Reference for NETBuilder® Family Software
Chapter 1 through Chapter 25

Software
Version 9.3

p/n 09-0863-002
Published May 1997

3Com Corporation ■ 5400 Bayfront Plaza ■ Santa Clara, California ■ 95052-8145

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty of any kind, either implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

UNITED STATES GOVERNMENT LEGENDS:
If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following restricted rights:

For units of the Department of Defense:
Restricted Rights Legend: Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) for Restricted Rights in Technical Data and Computer Software Clause at 48 C.F.R. 52.227-7013. 3Com Corporation, 5400 Bayfront Plaza, Santa Clara, California 95052-8145.

For civilian agencies:
Restricted Rights Legend: Use, reproduction, or disclosure is subject to restrictions set forth in subparagraph (a) through (d) of the Commercial Computer Software - Restricted Rights Clause at 48 C.F.R. 52.227-19 and the limitations set forth in 3Com Corporation's standard commercial agreement for the software. Unpublished rights reserved under the copyright laws of the United States.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, Boundary Routing, NETBuilder, and NETBuilder II, and SuperStack II are registered trademarks of 3Com Corporation.

CompuServe is a registered trademark of CompuServe, Inc. IBM, AS/400, LAN Net Manager, OS/2, PS/2, and VTAM are registered trademarks of International Business Machines Corporation. Advanced Peer-to-Peer Networking and APPN are trademarks of International Business Machines Corporation. XNS is a trademark of Xerox Corporation. VAX, DEC, and DECnet are registered trademarks of Digital Equipment Corporation. TeleVideo is a registered trademark of TeleVideo Corporation. NetWare, Novell, and UNIX are registered trademarks of Novell, Inc. Banyan and VINES are registered trademarks of Banyan Systems. Telenet is a trademark of Telenet Communications Corporation. SPARCsystem is a trademark of SPARC International, Inc. licensed exclusively to Sun Microsystems, Inc. SunOS is a trademark of Sun Microsystems, Inc. Link level compression uses Stac LZS compression software, copyrighted by Stac Electronics, (© Stac Electronics, 1991-1995) and protected by one or more patents, including US patent 5,126,739. Stac and LZS compression are registered trademarks of Stac Electronics. AppleTalk and Macintosh are registered trademarks of Apple Corporation. Honeywell is a registered trademark of Honeywell Corporation.

Other brand and product names may be registered trademarks or trademarks of their respective holders.

Guide written by Ramona Boersma, Mike Figone, Linda Lininger, Andrew Mann, and Carol Tatick. Edited by Pat Vaughn and Amy Guzules. Technical illustration by Debra Knodel. Production by Debra Knodel.

Printed on recycled paper.

CONTENTS

ABOUT THIS GUIDE

Audience 1
How to Use This Guide 1
Conventions 2

1 COMMANDS

ADD 1-1
AddUser 1-2
ANameLookup 1-2
APING 1-4
APpnPING 1-5
AtmToFr 1-6
AuditLog 1-6
BACkwards 1-7
Broadcast 1-7
CHange 1-8
ChangeDir 1-8
Connect 1-9
COpy 1-10
DEFine 1-11
DEFRag 1-13
DELete 1-13
DELeteUser 1-13
DIal 1-14
DirectoryManage 1-16
DisConnect 1-16
DiscoverRoutes 1-17
DiscRouteRs 1-18
DiskFiles 1-18
DLTest 1-19
DO 1-24
DteToIp 1-24
Echo 1-24
EraseDump 1-25
EXPire 1-25
FLush 1-26
FORMAT 1-26
FORwards 1-26
FrToAtm 1-27
GET 1-27
HangUp 1-29
InStall 1-29
IpToDte 1-30
LIsten 1-30
LOGout 1-31
MacAddrConvert 1-31
MakeDir 1-32
MEnu 1-32
MONitor 1-33
  Firmware Monitor 1-33
    NETBuilder II with CEC Module 1-34
    SuperStack II and OfficeConnect Bridge/Routers 1-34
  Debug Monitor (DPE Only) 1-34
MRInfo 1-35
MTraceRoute 1-35
NetwarePING 1-37
NetwareTraceRoute 1-37
NetwareView 1-38
OPING 1-38
OTraceRoute 1-39
PassWord 1-39
PathSwitch 1-40
PAuse 1-40
PING 1-40
PUT 1-41
PutDump 1-42
ReaD 1-43
ReBoot 1-44
REMote 1-44
RemoveDir 1-46
RemoveFile 1-47
ReName 1-47
RESTart 1-48
RESume 1-48
RLOGin 1-49
RZ 1-50
SAve 1-50
SAVEbgp 1-52
SecCheck 1-52
SET 1-53
SETDefault 1-53
SHow 1-54
SHowDefault 1-57
SpyRing 1-58
SWitch 1-58
SysconF 1-59
SYSgen 1-60
SysInfo 1-60
SysPassWord 1-61
SZ 1-61
TELnet 1-62
TEst 1-62

TraceRoute 1-63
TRansmit 1-64
UnBindDSA 1-64
UNDefine 1-64
UNSave 1-65
UserManage 1-65
VPing 1-66
VTp 1-66

2 GLOBAL PARAMETERS

CurrentPorts 2-1
CurrentServices 2-2
GREP 2-2
History 2-3
InterAction 2-3
PRIvilege 2-3
ScreenLength 2-4

3 AC SERVICE PARAMETERS

CONFiguration 3-1
CONTrol 3-1
EXPirationTimer 3-2
LOGINs 3-2
RESolutionOrder 3-2

4 APPLETALK SERVICE PARAMETERS

AarpCache 4-2
AarpCouNT 4-2
AarpTIMe 4-2
ADDRess 4-3
AllRoutes 4-4
AMTagingTime 4-5
CONFiguration 4-6
CONTrol 4-6
DefaultZone 4-8
DIAGnostics 4-9
EntityFilter 4-9
EntityFilterNum 4-12
NAmes 4-13
NbpLookupTimer 4-14
NetFilter 4-14
NetFilterType 4-15
NetRange 4-15
NetZoneMapping 4-16
PortZone 4-16
RouteAgingTime 4-17
RouterName 4-17
RouteUpdateTime 4-18
SMDSGroupAddr 4-18
StartupNET 4-19
StartupNODe 4-19
X25PROFileid 4-19
X25ProtID 4-20
ZONe 4-20
ZoneAdvFilterNm 4-21
ZoneNetMapping 4-21

5 APPN SERVICE PARAMETERS

AdjLenDef 5-2
AdjLinkSta 5-3
AdjNodeStatus 5-6
AppnLOG 5-7
ConfigCOS 5-8
CONFiguration 5-8
CONNection 5-8
ConnNetworkChar 5-10
ConnNetworkDef 5-11
CONTrol 5-12
COS 5-12
COSDef 5-12
COSNodeChar 5-13
COSNodeRow 5-13
COSTgChar 5-14
COSTgRow 5-15
DIRectory 5-16
DirectoryEntry 5-17
DlurDefaults 5-18
DlurLinkSta 5-18
DluRStatus 5-20
DluSStatus 5-21
DownStreamLU 5-21
HprTimer 5-21
ISRsessions 5-22
LinkStaCHar 5-23
LinkStaCONTrol 5-25
LocalNodeName 5-27
LocalNodeResist 5-28
Mode 5-28
ModetoCosMap 5-28
NNtopology 5-29
PortCHar 5-29
PortCONTrol 5-30
PortDef 5-31
QueuePriority 5-33
RTP 5-33
RTPStats 5-34
SdlcAdjLinkSta 5-35
SdlcDlurLinkSta 5-37
TG 5-40
TreeCache 5-41

6 ARP SERVICE PARAMETERS
CONFiguration 6-1
CONTrol 6-1
HoldTime 6-2
OverBlocked 6-2
RarpClientState 6-2
RarpCONTrol 6-3
RequestFormat 6-4

7 ATM SERVICE PARAMETERS
CONFiguration 7-1
CONTrol 7-1
KeepAliveTime 7-2
LoopMode 7-2
PermVirCircuit 7-2
SwitchVersion 7-4
TrafficShaper 7-4
VCIBits 7-5
VirCirLoopMode 7-5
VirCirLoopTime 7-6
VPIBits 7-6

8 ATMLE SERVICE PARAMETERS
AgeTime 8-1
ARPRoute 8-2
ArpRspTime 8-2
ATMAddress 8-2
CntrlTime 8-2
CONFiguration 8-3
ConnTime 8-3
CONTrol 8-3
DelayTime 8-4
ElanName 8-4
FlushTime 8-5
LanType 8-5
LECSAddr 8-5
LESAddr 8-5
MaxData 8-6
MaxRetry 8-6
MaxUnkFrm 8-6
MaxUnkFtm 8-7
PrimaryMAC 8-7
STATUS 8-7
SwitchTime 8-7
VccTime 8-7

9 ATUN SERVICE PARAMETERS
AddrLOCation 9-1
BroadCastAddr 9-2
CUADDRess 9-2
CUCONFig 9-2
CUCONTrol 9-2
CUInfo 9-3
CUPOrt 9-4
CUSTatus 9-4
FrameChars 9-4
FrameGap 9-5
FrameSize 9-5
IdleTimer 9-6
LocalMac 9-6
LocalSap 9-6
PortCONFig 9-6
PortCONTrol 9-7
PortCU 9-8
RemoteMac 9-9
RemoteSap 9-9

10 AUDITLOG SERVICE PARAMETERS
CONFiguration 10-1
CONTrol 10-1
LocalFacility 10-2
LogServerAddr 10-2

11 BCN SERVICE PARAMETERS
CONFiguration 11-1
CONTrol 11-1
IbmStatus 11-2
LclNonIbmDlci 11-2
RemNonIbmDlci 11-3
RemoteLanType 11-3
X25ProtID 11-3

12 BGP SERVICE PARAMETERS
AggregateExcept 12-2
AggregateRange 12-2
AsFilter 12-3
ASPath 12-4
AsPolicyAll 12-4
AsPolicyExt 12-5
AsPolicyInt 12-6
AsPolicyPeer 12-7
CONFiguration 12-8
CONTrol 12-8
CurrentPeeR 12-8
DEBug 12-9
DefaultNet 12-9
DefaultWeight 12-10
DisplayFilter 12-10
HoldTime 12-11
InteriorPolicy 12-11
LocalAS 12-12
MaxPeers 12-12
NetworkFilter 12-12
NetPolicyAll 12-13
NetPolicyExt 12-14

NetPolicyInt 12-14
NetPolicyPeer 12-15
PEER 12-16
PeerAS 12-16
PeerControl 12-17
PeerIpAddress 12-17
PeerMetric 12-17
PeerVersion 12-18
PeerWeight 12-18
ROUte 12-18

13 BOOTPC SERVICE PARAMETERS
CONFiguration 13-1
CONTrol 13-1
RequestStatus 13-2
RetryCount 13-2
RetryInterval 13-2

14 BRIDGE SERVICE PARAMETERS
AgeTime 14-1
AllRoutes 14-2
APPletalk 14-3
ATMNeighbor 14-3
BLimitTimer 14-4
BroadCastLimit 14-4
CONFiguration 14-4
CONTrol 14-5
DatalinkAddrFmt 14-6
DlciNeighbor 14-7
DStSecurity 14-7
FunctionalAddr 14-8
MultiCastAddr 14-8
ROUte 14-8
RouteTableSize 14-11
RptStationHop 14-12
SMDSGroupAddr 14-12
SRcSecurity 14-13
TransparentBRidge 14-13
X25Neighbor 14-14
X25PROFileid 14-14
X25ProtID 14-14

15 BSC SERVICE PARAMETERS
BscCU 15-1
CONFiguration 15-2
CONTrol 15-2
CUCONTrol 15-2
Role 15-3

16 CLNP SERVICE PARAMETERS
CONFiguration 16-1
CONTrol 16-1
DefaultTTL 16-2
ERgeneration 16-2
ES 16-3
IS 16-3
MTU 16-4
NetEntityTitle 16-4
RDgeneration 16-4
X25PROFileid 16-5

17 DECNET SERVICE PARAMETERS
ADDRess 17-2
AddressMap 17-3
AdvertisePolicy 17-4
AdvToNeighbor 17-5
AllEndNodesTR 17-6
AllRoutersTR 17-6
AllRoutes 17-7
CONFiguration 17-7
CONTrol 17-7
COST 17-8
GatewayControl 17-8
HelloTime 17-9
InterNetRoute 17-9
IVPrefix 17-10
MaxAReaCost 17-11
MaxAReaHops 17-11
MaxAReaNumber 17-12
MaxCost 17-12
MaxHops 17-12
MaxNodeNumber 17-13
MaxPseudoAreas 17-13
MaxVisits 17-14
Neighbor 17-14
NETwork 17-15
NodeType 17-15
PolicyControl 17-15
PRIOrity 17-16
PseudoAreaPrefix 17-16
RcvFromNeighbor 17-16
ReceivePolicy 17-17
RoutingTime 17-18
SMDSGroupAddr 17-19
STATUS 17-19
VAdvertisePolicy 17-20
X25PROFileid 17-21
X25ProtID 17-21

18 DIR SERVICE PARAMETERS
NAME 18-1
RESolutionOrder 18-1

19 DLSw Service Parameters
AccessAct 19-2
BoundAccessNode 19-2
CircuitBal 19-3
CIRcuits 19-3
CONFiguration 19-4
CONNections 19-4
CONNectStats 19-4
CONTrol 19-4
Display 19-5
DlswLOG 19-5
FradMap 19-6
Interface 19-6
LimitDataGrams 19-7
LimitNBeXplorers 19-7
LimitSnaeXplorers 19-7
MacCache 19-8
MaxTRaceData 19-8
McastStats 19-9
McastTcpIdle 19-9
MOde 19-9
MulticastAddr 19-10
MulticastRetry 19-10
NameCache 19-11
NBBcastResend 19-11
NBBcastTimeout 19-11
NBLocalAccess 19-11
NBRemAccess 19-12
PEer 19-12
PeerMacAdd 19-13
PeerNBName 19-13
PortGroup 19-14
PRiorityCRiteria 19-14
PRioSTATistics 19-15
SnaAlertsToTraps 19-16
SnaLocalAccess 19-16
SnaRemAccess 19-17
SnaTopoCollect 19-18
SnaTopoDisplay 19-18
TRaceData 19-20
TrapCONTrol 19-20

20 DVMRP Service Parameters
AggregateExcept 20-1
AggregateRange 20-2
BoundaryAddr 20-3
CacheTime 20-3
CONFiguration 20-4
CONTrol 20-4
DestGroup 20-4
ForwardTable 20-5
MEtric 20-6
MOspf 20-6
NEighbor 20-7
NeighborRouter 20-7
PolicyControl 20-8
Prune 20-9
RateLimit 20-9
RouteTable 20-9
TUnnel 20-10
UpdateTime 20-10

21 ESIS Service Parameter
CONFiguration 21-1
CONTrol 21-1
HoldTime 21-2
MulticastES 21-2
MulticastES8025 21-2
MulticastIS 21-3
MulticastIS8025 21-3
UpdateTime 21-3

22 FDDI Service Parameters
BufferErrors 22-2
CurrentPAth 22-2
DownNeighbor 22-2
DupAddress 22-2
FrameCounts 22-3
FrameErrorRatio 22-3
InsertPolicy 22-3
InsertedStatus 22-3
LCTFailCount 22-3
LEMCount 22-3
LLCService 22-4
MACAction 22-4
MACPlacement 22-4
MaintLineStateA 22-4
MaintLineStateB 22-5
OpticalBypass (Switch) 22-5
PCConnectState 22-5
PCControlA 22-6
PCControlB 22-6
PCMState 22-6
PMF 22-7
PortNeighbor 22-7
RemDisconnect 22-7
RMTState 22-8
SMTAddress 22-8
SMTVersion 22-8
StationAction 22-9
StationCONFig 22-9
StationID 22-10
TNEGotiated 22-10
TREQuest 22-10
UpNeighbor 22-10
UserData 22-11
WrapAB 22-11

23 FILTER SERVICE PARAMETERS

- CONFiguration 23-1
- CONTrol 23-1
- DefaultAction 23-2
- DIAGnostics 23-2
- MASK 23-2
- MNEmonics 23-5
- POLicy 23-6
- SELection 23-9
- StationGroup 23-10

24 FIREWALL SERVICE PARAMETERS

- ARCHIE 24-2
- CONFiguration 24-2
- CONTrol 24-3
- DefAction 24-4
- DNSSvrSvr 24-4
- FILters 24-5
- FTPIn 24-7
- FTPOut 24-8
- FTPSession 24-9
- GopherIn 24-10
- GopherOut 24-10
- HTTPIn 24-11
- HTTPOut 24-12
- ICMP 24-13
- InFilter 24-13
- Log 24-14
- NFS 24-15
- NNTPIn 24-16
- NNTPOut 24-16
- NTP 24-17
- OSPF 24-18
- OutFilter 24-19
- POPIn 24-19
- POPOut 24-20
- RIP 24-21
- SMTPIn 24-22
- SMTPOut 24-23
- SNMP 24-24
- Syslog 24-25
- TELnetIn 24-25
- TELnetOut 24-26
- TFTP 24-27
- WAISIn 24-28
- WAISOut 24-28

25 FR SERVICE PARAMETERS

- AllDlci 25-1
- AtmMode 25-1
- BackupPVC 25-2
- COMPressType 25-2
- CONFiguration 25-3
- CONTrol 25-3
- DEbit 25-3
- DIAGnostics 25-4
- DLCIR 25-4
- DLciStat 25-4
- DRTrigger 25-4
- ErrorThreshold 25-5
- FSEInterval 25-5
- KATime 25-5
- MonitoredEvent 25-5
- PDNtype 25-5

26 GATEWAY SERVICE PARAMETERS

- CONFiguration 26-1
- ConnHistory 26-1
- CONtrol 26-2
- IPX25Map 26-3
- PadSession 26-4
- PSelX25Map 26-5
- SubAddrMap 26-5

27 IDP SERVICE PARAMETERS

- AllRoutes 27-1
- CONFiguration 27-2
- CONTrol 27-2
- NETnumber 27-2
- ROUte 27-3
- SMDSGroupAddr 27-4
- X25CallUsrData 27-4
- X25PROFileid 27-4
- X25ProtID 27-5

28 IISIS SERVICE PARAMETERS

- CONTrol 28-1
- DefaultMetric 28-2
- ExteriorPolicy 28-2
- InteriorPolicy 28-3
- StaticPolicy 28-4

29 IP SERVICE PARAMETERS

- ADDRess 29-2
- AllRoutes 29-3
- CONFiguration 29-4
- CONTrol 29-5
- DefaultTTL 29-6
- FilterAddrs 29-6
- FilterDefAction 29-10
- FIlters 29-10
- ICMPGenerate 29-12
- ICMPReply 29-12
- LaPosteDD 29-12

LaPosteNN 29-13
LaPostePort 29-13
LaPostePP 29-13
LaPostePRefix 29-13
NETaddr 29-13
QueuePriority 29-15
ReassemblyTime 29-15
RemoteAddress 29-15
ROUte 29-16
SecAuthIn 29-17
SecAuthOut 29-18
SecCONTrol 29-19
SecFileServer 29-20
SecLabelDefault 29-20
SecLabelSys 29-21
SecLabelValues 29-21
SecLabelXtra 29-22
SecLEVel 29-22
SMDSGroupAddr 29-23
X25PROFileid 29-23
X25ProtID 29-23

30 IPNAME SERVICE PARAMETERS
CAChe 30-1
CONFiguration 30-1
DomainName 30-2
NAME 30-2
NameServiceType 30-3
PrimaryNameServer 30-3
SecondaryNameServer 30-3

31 IPX SERVICE PARAMETERS
ADDRess 31-1
AllRoutes 31-2
AllServers 31-3
CONFiguration 31-3
CONTrol 31-3
Delay 31-4
DIAGnostics 31-4
InternalNET 31-5
MaxHop 31-5
MTU 31-5
NETnumber 31-6
PathSplit 31-7
ROUte 31-7
RouterName 31-9
SERver 31-9
SMDSGroupAddr 31-9
SPoofCONTrol 31-10
X25PROFileid 31-11
X25ProtID 31-11

32 ISIS SERVICE PARAMETERS
ADJacencies 32-2
AreaAddress 32-3
CONFiguration 32-4
CONTrol 32-4
CsnpTime 32-5
DISHelloTime 32-6
HelloPassWord 32-6
HelloTime 32-6
L1BufferSize 32-7
L2BufferSize 32-7
L1DefaultMetric 32-7
L2DefaultMetric 32-7
L1Multicast 32-8
L2Multicast 32-8
L1PassWord 32-8
L2PassWord 32-8
L1Priority 32-9
L2Priority 32-9
L1Route 32-9
L2Route 32-10
LinkStateData 32-10
LspBroadcastTime 32-11
LspMAxTime 32-11
LspMInTime 32-11
LspRtxTime 32-12
MODE 32-12
Neighbors 32-12
PathSplit 32-13
PrefixRoute 32-13
PsnpTime 32-14
SMDSGroupAddr 32-14
SMDSID 32-15
SystemID 32-15
SystemName 32-15
TRACE 32-16

33 LAPB SERVICE PARAMETERS
CONFiguration 33-1
CONTrol 33-1
FrameSeq 33-2
InterfaceType 33-2
N2 33-2
T1 33-2
T3 33-3
WindowSize 33-3

34 LLC2 SERVICE PARAMETERS
CONFiguration 34-1
CONTrol 34-2
LlcLOG 34-2
MaxFrame 34-3
MaxTRaceData 34-3

ReceiveWindow 34-3
RetryCount 34-3
SESSions 34-3
TImerAck 34-4
TImerInact 34-4
TImerReply 34-4
TRaceData 34-4
TransmitWindow 34-5
TUNnelControl 34-5
TUNnelDisplay 34-5
TUNnelInterface 34-5
TUNnelMAcadd 34-6
TUNnelMOde 34-7
TUNnelPeer 34-7
TUNnelPRiority 34-7
TUNnelVRing 34-8

35 LNM Service Parameters
CONTrol 35-1
ExcSftErrTh 35-2
FrCopErrTh 35-2
FreqErrTh 35-2
ImpSftErrTh 35-2
LostFrTh 35-3
MinDecErrTh 35-3
NumAltMgrs 35-3
PassWord 35-4
RcvCnTFErrTh 35-4
RcvConErrTh 35-4
SftErrRptTimer 35-4
TblFlErrTh 35-5
TokErrTh 35-5
VirBrNum 35-5
VirRingNum 35-5

36 MIP Service Parameters
CONFiguration 36-1
CONTrol 36-1
LocalGroups 36-1
PaceMode 36-2
QueryInterval 36-2
SMDSGroupAddr 36-3
THreshold 36-3

37 MOSPF Service Parameters
CONFiguration 37-1
CONTrol 37-1
DestGroup 37-2
Dvmrp 37-3
ForwardTable 37-4
MABR 37-5
PolicyControl 37-5

38 NLSP Service Parameters
ADJacencies 38-1
AreaAddress 38-2
BufferSize 38-3
CONFiguration 38-3
CONTrol 38-4
Cost 38-4
CsnpTime 38-5
DISHelloTime 38-5
HelloPassWord 38-6
HelloTimeLan 38-6
HelloTimeWan 38-7
HoldTimeFactor 38-7
LinkStateData 38-7
LspBcastTime 38-8
LspMAxTime 38-8
LspMInTime 38-9
LspRtxTime 38-9
Multicast 38-10
Multicast8025 38-10
Neighbors 38-10
PRIOrity 38-11
PsnpTime 38-11
SPFHolddown 38-12
SystemID 38-12
SystemName 38-13
TRACE 38-13

39 NRIP Service Parameters
AdvertisePolicy 39-1
AdvToNeighbor 39-2
CONFiguration 39-3
CONTrol 39-4
DefaultMetric 39-5
HoldTimeFactor 39-6
MaxResrcRteNmbr 39-6
PolicyControl 39-6
RcvFromNeighbor 39-7
ReceivePolicy 39-7
UpdateTime 39-9

40 OSIAPPL Service Parameters
CONFiguration 40-1
CONNections 40-1
DSAAddress 40-2
DSAType 40-2
DuaState 40-2
NAme 40-2
NameSourceOrder 40-3
UnbindTimer 40-3
VtpDataConcat 40-3

41 OSPF Service Parameters

AreaId 41-2
AreaRanges 41-2
CONFiguration 41-3
CONTrol 41-3
Cost 41-4
DEBUG 41-4
DefaultMetric 41-5
Delay 41-5
DemandInterface 41-6
DirectPolicy 41-7
ExteriorPolicy 41-7
HelloTime 41-8
InterfaceStatus 41-8
InteriorPolicy 41-9
LinkStateData 41-10
Neighbor 41-10
NeighborStatus 41-11
PassWord 41-13
ReceivePolicy 41-13
RetransmitTime 41-13
RouterDeadTime 41-14
RouterID 41-14
ROUTerPriority 41-15
SPFHolddown 41-15
StaticPolicy 41-15
StubDefaultMetric 41-16
VirtualLink 41-16

42 PATH Service Parameters

BAud 42-2
CLock 42-3
CmdCharSet 42-4
CONFiguration 42-4
CONNector 42-5
CONTrol 42-6
DataBits 42-7
DialCarrierTime 42-7
DialCONTrol 42-8
DialMode 42-9
DialPool 42-9
DUplex 42-10
ENCoding 42-10
ExDevType 42-11
LAyout 42-11
LineType 42-12
LocalDialNo 42-13
LocalSubAddr 42-14
MacAddress 42-14
NAme 42-15
Pad 42-16
PARity 42-16
PhantomPower 42-17
RateAdaption 42-17
RxParity 42-18
SPIDdn1 42-18
SPIDdn2 42-19
StayAliveAction 42-19
StayAliveTimer 42-20
StopBits 42-20
SwitchType 42-20
TinyGramcomp 42-21
TxIdle 42-21
TxParity 42-22

43 PORT Service Parameters

AutoDial 43-2
BODIncrLimit 43-2
BODTHreshold 43-3
COMPressType 43-3
CONFiguration 43-4
CONTrol 43-5
DefaultPriority 43-5
DIAGnostics 43-6
DialCONFig 43-6
DialCONTrol 43-8
DialDebouncTime 43-8
DialHistory 43-9
DialIdleTime 43-9
DialInitState 43-9
DialNoList 43-10
DialRcvrState 43-12
DialRetryCount 43-12
DialRetryTime 43-13
DialSamplPeriod 43-13
DialSTatus 43-14
IfDescr 43-16
LinkCompStat 43-16
LogicalNET 43-16
NAme 43-17
NORMalBandwidth 43-17
OWNer 43-19
PathPreference 43-21
PAths 43-22
ProtMacAddrFmt 43-23
PROTocolRsrv 43-25
QueueCONTrol 43-27
QueueInterLeave 43-27
QueuePATtern 43-28
QueuePriority 43-28
QueueStatistics 43-29
QueueThrottle 43-29
VirtualPort 43-30
WEProfileList 43-32

44 PPP SERVICE PARAMETERS

AuthLocalUser 44-1
AuthProTocol 44-1
AuthRemoteUser 44-2
AuthReptIntvl 44-2
CONFiguration 44-2
MaxRcvUnit 44-2
MlpCONTrol 44-3
MlpmaxRxRecUnit 44-3
MlpSTATIstics 44-3
STATUS 44-3

45 PROFILE SERVICE PARAMETERS

CONFiguration 45-1
ProfileID 45-2
ProfileType 45-2
X25ClosedUsrGrp 45-3
X25COMPressType 45-3
X25CONTrol 45-4
X25CUDSuffix 45-4
X25FastSelect 45-5
X25NSF 45-5
X25PacketSiZe 45-6
X25ProfileName 45-6
X25ReverseChrg 45-6
X25ThruputClass 45-7
X25VCLimit 45-7
X25VCQueueSize 45-7
X25VCTimer 45-8
X25WindowSiZe 45-8

46 RDP SERVICE PARAMETERS

CONFiguration 46-1
CONTrol 46-1
LifeTime 46-2
MAxInterval 46-2
MInInterval 46-2
RouterList 46-3

47 RIPIP SERVICE PARAMETERS

AdvertisePolicy 47-1
AdvToNeighbor 47-3
CONFiguration 47-4
CONTrol 47-4
DefaultMetric 47-6
ExteriorPolicy 47-6
ImportMetric 47-8
InteriorPolicy 47-9
RcvFromNeighbor 47-9
RcvSubnetMask 47-11
ReceivePolicy 47-12
StaticPolicy 47-12
UpdateTime 47-13

48 RIPXNS SERVICE PARAMETERS

ADDRess 48-1
CONFiguration 48-2
CONTrol 48-2
UpdateTime 48-3

49 SAP SERVICE PARAMETERS

AdvertisePolicy 49-1
AdvToNeighbor 49-2
CONFiguration 49-3
CONTrol 49-4
HoldTimeFactor 49-5
PolicyControl 49-5
PreferredServer 49-5
RcvFromNeighbor 49-6
ReceivePolicy 49-7
UpdateTime 49-8

50 SCH SERVICE PARAMETERS

ActiveSCHedule 50-1
CONFiguration 50-1
CONTrol 50-2
EbmeCONFig 50-2
EbmeCONTrol 50-2
EbmeEVent 50-3
EVent 50-3

51 SDLC SERVICE PARAMETERS

CUAddr 51-2
CUCONFig 51-2
CUCONTrol 51-2
CUInfo 51-3
CULocalMac 51-3
CULocalSap 51-3
CUMAXout 51-4
CUMOde 51-4
CUNAme 51-4
CUPollTimer 51-4
CUPOrt 51-5
CURemoteMac 51-5
CURemoteSap 51-5
CUStatus 51-6
CUType 51-6
CUXId 51-7
CUXidDefined 51-7
HostMac 51-7
MaxTRaceData 51-7
PCallTimer 51-8
PCONFig 51-8
PCONtrol 51-8
PDatMode 51-8
PIdleDiscTimer 51-9

PMaxData 51-9
PMinFrameDelay 51-9
PMODulo 51-9
PortCU 51-10
PRetryTimer 51-10
PROle 51-10
PT1Retry 51-11
PT1Timer 51-11
SdlcLOG 51-11
SuppressDM 51-11
TRaceData 51-12
TrapCONTrol 51-12
XidKeepAlive 51-12

52 SHDLC SERVICE PARAMETERS
PEer 52-1

53 SMDS SERVICE PARAMETERS
CONFiguration 53-1
CONTrol 53-1
SMDSGroupAddr 53-2
SMDSIndivAddr 53-2

54 SNA SERVICE PARAMETERS
CONFiguration 54-1
DefaultPU 54-1
LinkStaCONT 54-2
LocalNodeName 54-2
PortCONTrol 54-2
PortDef 54-2
PUStatus 54-3
SdlcLinkSta 54-3
SNaLOG 54-4
SscpLinkSta 54-5

55 SNMP SERVICE PARAMETERS
COMmunity 55-1
CONFiguration 55-2
CONTrol 55-2
MANager 55-2

56 SR SERVICE PARAMETERS
AllRoutes 56-1
BridgeNumber 56-2
CONFiguration 56-3
DIAGnostics 56-3
GatewayControl 56-3
GatewayVRing 56-4
HoldTime 56-4
LargestFrameSize 56-5
MaxAreRDLimit 56-5
MaxSteRDLimit 56-6
MinAccessPrior 56-6
Mode 56-6
RingNumber 56-7
ROUte 56-7
RouteDiscovery 56-8
SrcRouBridge 56-9
WanRoutes 56-10

57 STP SERVICE PARAMETERS
ADDRess 57-1
BridgePriority 57-2
CONFiguration 57-2
CONTrol 57-2
ForwardDelay 57-3
HelloTime 57-3
MaxAge 57-4
PathCost 57-4
PortPArams 57-5
PortPriority 57-5

58 SYS SERVICE PARAMETERS
ADDRess 58-2
ALias 58-3
AUditTrailType 58-4
CONFiguration 58-4
CONNectionUsage 58-4
CPUboardInfo 58-5
DATE 58-5
DpmSTATistics 58-6
DSTime 58-6
FILESELection 58-7
FileServerAddr 58-7
GetConfigFiles 58-7
GLobalPARams 58-8
IOboardInfo 58-8
MacAddrDispMode 58-8
MacAddrFormat 58-9
MACros 58-9
MPMessages 58-10
NetAccess 58-10
NetMAP 58-10
NetMapTime 58-11
NMMacro 58-11
NMPrompt 58-11
PROMpt 58-12
RemoteManager 58-12
SampleOption 58-12
SampleTime 58-13
STatControl 58-13
STATistics 58-14
SysCallerID 58-15
SysCONtact 58-15
SYSgen 58-15

SysLOCation 58-15
SysNAMe 58-16
SystemMessages 58-16
TelnetManager 58-16
TimeZone 58-17
UIBinary 58-17
UIEcho 58-18
VERSion 58-18
WatchDogTimer 58-18
WelcomeString 58-19

59 TCP SERVICE PARAMETERS
CONFiguration 59-1
CONNections 59-1
CONTrol 59-2
DelayedAckTime 59-2
KeepAliveLimit 59-2
KeepAliveTime 59-3
MaxSegmentSize 59-3
RetransmitLimit 59-3
SYNRetrys 59-3
WINdow 59-3

60 TCPAPPL SERVICE PARAMETERS
LIStenerPorts 60-1
RLogSendName 60-2

61 TERM SERVICE PARAMETERS
AllSessions 61-4
AUToDisconnect 61-4
AUToListen 61-4
BAud 61-5
BReakAction 61-5
BReakChar 61-6
BUffersize 61-7
COLumns 61-7
CRPad 61-7
DataForward 61-8
DefaultParams 61-8
DeVice 61-9
ECHOData 61-10
ECHOMask 61-10
ECMChar 61-10
ERAse 61-11
FlowCtrlFrom and FlowCtrlTo 61-11
FlushVC 61-12
FunctionalUnit 61-12
IdleTimer 61-12
InitMacro 61-13
InterActTerm 61-13
LFInsertion 61-14
LFPad 61-14
LineERase 61-14
LocalEDit 61-15
MaxSessions 61-15
NetAScii 61-15
PARAmeters 61-16
PARIty 61-16
PROFile 61-16
ReprintLine 61-17
ROWs 61-17
SavedParams 61-17
SESsions 61-18
TERMType 61-18
VERBatim 61-18
WordERAse 61-19
XmitBinary 61-19
XON and XOFF 61-19

62 UDPHELP SERVICE PARAMETERS
ActivePorts 62-1
AuthDHCPServer 62-2
BootpMaxHops 62-2
BootpThreshold 62-3
CONFiguration 62-3
CONTrol 62-3
ForwardAddress 62-3
Name 62-5
TTLOverride 62-6

63 VIP SERVICE PARAMETERS
ADDRess 63-1
AllRoutes 63-2
CONFiguration 63-2
CONTrol 63-2
HeaderFormat 63-3
Metric 63-4
Neighbor 63-4
RtrName 63-5
SMDSGroupAddr 63-5
STATUS 63-6
SymbolicNames 63-6
UpdateTime 63-6
WideAreaNbr 63-7
X25PROFileid 63-7
X25ProtID 63-7

64 WE SERVICE PARAMETERS
CONFiguration 64-1
DevCONTrol 64-1
DevSTATistics 64-2
DialPathLimit 64-2
ErrorThreshold 64-3
FullStatusFreq 64-3
KeepAliveInt 64-4
ProFiles 64-4

65 X25 SERVICE PARAMETERS
CONFiguration 65-1
CONTrol 65-1
IncomingSVCs 65-2
NbrPROFile 65-2
OutgoingSVCs 65-2
PDNetworkType 65-3
PVC 65-3
STATUS 65-3
Trace 65-3
TwowaySVCs 65-4
X25Address 65-4
X25PROFileid 65-4
X25STATistics 65-5

66 XSWITCH SERVICE PARAMETERS
CONFiguration 66-1
CONTrol 66-1
SWitchedVC 66-1
TUNnelPassWord 66-2
TUNnelPort 66-2
X25Prefix 66-3
XSWPVC 66-3

A SYSCONF COMMAND MENUS
NETBuilder II with DPE A-1
Serial Ports A-1
Primary Boot Source and Secondary Boot Source A-2
Boot Filename A-2
Config File Source A-3
IP Addresses A-3
FTP login parameters A-3
Test Boot Source A-4
Perform Test Boot A-4
Clear Test Boot Timer A-4
Boot Sources A-5
Primary A-5
Primary and Secondary A-5
Secondary A-5
Dump Destination A-5
No Full Dump A-6
Single PC Card Full Dump to Drive A or B A-6
Multiple PC Card Full Dump to Drive A or B A-6
Recovery Procedure A-6
Halt A-6
Halt System A-7
Reboot A-7
Reboot System A-7
Dump and Reboot A-7
Selective Dump and Reboot A-7
MP Boot Source A-8
Local A-8
Default File Source A-8
Boot Statistics A-8
NETBuilder II with CEC A-9
Serial Ports A-9
Self-Test A-10
Start-Up Action A-10
Enter Monitor A-10
Local A-10
Try Boot Once A-10
Try Boot Forever A-11
Primary Boot Source and Secondary Boot Source A-11
Boot Device A-11
Default File Source A-13
Maximum Retries A-13
I/O Module Parameters A-13
Boot Protocol A-14
IP Addresses A-14
MAC Address A-15
ARP Format A-15
FTP login parameters A-16
Test Boot Source A-16
Perform Test Boot A-16
Clear Test Boot Timer A-17
Boot Sources A-17
Primary A-17
Primary and Secondary A-17
Secondary A-17
Dump Destination A-18
Local A-18
Network A-18
Recovery Procedure A-19
Halt and Halt System A-19
Reboot A-19
Reboot System A-19
Dump and Reboot A-19
Selective Dump and Reboot A-19
MP Boot Source A-20
Local A-20
Default File Source A-20
Boot Statistics A-20
SuperStack II NETBuilder and OfficeConnect NETBuilder A-21
Upgrade Menu A-21
Console Port A-21
Self-Test A-22
Primary Boot Source and Secondary Boot Source A-22
Boot Filename A-22
Default File Source A-22
IP Addresses A-23
FTP login parameters A-23

Test Boot Source A-23
Perform Test Boot A-24
Clear Test Boot Timer A-24
Boot Sources A-24
Primary A-24
Primary and Secondary A-25
Secondary A-25
Dump Destination A-25
Do not dump A-25
Network A-25
Boot Statistics A-26

B FIRMWARE COMMANDS

Entering the Boot Monitor B-1
Commands B-1
Boot B-1
Boot Utility B-2
Display Files B-2
Help B-2
Recovery Action B-3
Reboot B-4
Show Version B-4

INDEX

3COM CORPORATION LIMITED WARRANTY

ABOUT THIS GUIDE

This guide provides a comprehensive reference to NETBuilder® software commands and syntax.

If the information in the release notes that shipped with your software differs from the information in this guide, follow the release notes.

Before you use the information in this guide, you must first install, check, and boot the bridge/router according to the hardware installation guide:

The SuperStack II NETBuilder bridge/routers were formerly referred to as NETBuilder Remote Office bridge/routers.

In addition to installing the hardware, you must also install and configure the NETBuilder software on the bridge/router. This procedure is explained in the software guide specific to each platform. If you are upgrading software from an earlier version, refer to *Upgrading NETBuilder Family Software*.

This guide is intended primarily for command reference. For procedures about operating and configuring your bridge/router software for bridging, routing, and wide area protocols, according to your network needs, refer to *Using NETBuilder Family Software.*

In this guide, the term bridge/router is used regardless of whether the system is configured as a bridge or a router or both.

Audience

This guide is intended for network administrators who:

- Have experience planning, maintaining, and troubleshooting local or wide area networks.
- Are familiar with network protocols, bridging and routing, and network management.
- Are responsible for configuring and operating NETBuilder Bridge/Routers.

How to Use This Guide

The chapters in this guide are organized according to NETBuilder software services. For information about command function, syntax, and parameters, refer to the chapter for the corresponding service.

Chapter 1 describes system-wide commands.

Chapter 2 describes global parameters that affect the system environment. Global parameters do not belong to a service.

Chapter 3 through **Chapter 66** provide descriptions of all services available in NETBuilder software and their related parameters. The services are in alphabetical order from Chapter 3 (AC Service) through Chapter 66 (XSWitch Service). The parameters within each service chapter are also listed in alphabetical order.

Appendix A and **Appendix B** describe the SysconF command and the firmware monitor utility.

Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

Table 1 Notice Icons

Icon	Type	Description
ℹ	Information Note	Information notes call attention to important features or instructions.
⚠	Caution	Cautions alert you to personal safety risk, system damage, or loss of data.
⚡	Warning	Warnings alert you to the risk of severe personal injury.

Table 2 Text Conventions

Convention	Description
"Enter" vs. "Type"	When the word "enter" is used in this guide, it means type something, then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says "type."
"Syntax" vs. "Command"	When the word "syntax" is used in this guide, it indicates that the general form of a command syntax is provided. You must evaluate the syntax and supply the appropriate port, path, value, address, or string; for example: Enable RIPIP by using the following syntax: `SETDefault !<port> -RIPIP CONTrol = Listen` In this example, you must supply a port number for !<port>. When the word "command" is used in this guide, it indicates that all variables in the command have been supplied and you can enter the command as shown in text; for example: Remove the IP address by entering the following command: **`SETDefault !0 -IP NETaddr = 0.0.0.0`** ℹ For consistency and clarity , the full form syntax (upper- and lowercase letters) is provided. However, you can enter the abbreviated form of a command by typing only the uppercase portion and supplying the appropriate port, path, address, value, and so forth. You can enter the command in either upper- or lowercase letters at the prompt.
Text represented as `screen display`	`This typeface` is used to represent displays that appear on your terminal screen, for example: `NetLogin:`
Text represented as **`commands`**	**`This typeface`** is used to represent commands that you enter, for example: **`SETDefault !0 -IP NETaddr = 0.0.0.0`**
Keys	When specific keys are referred to in the text, they are called out by their labels, such as "the Return key" or "the Escape key," or they may be shown as [Return] or [Esc]. If two or more keys are to be pressed simultaneously, the keys are linked with a plus sign (+), for example: Press [Ctrl]+[Alt]+[Del].
Italics	*Italics* are used to denote *new terms* or *emphasis*.

1 COMMANDS

This chapter describes the system commands. For each command, the descriptions include:

- Full syntax
- Privilege level
- Command function, format, and system response

When applicable, examples and lists of related commands are provided.

Some commands can be entered without any parameters; others operate on parameters. The exact command syntax for modifying or displaying a particular parameter may be different from the general syntax. For detailed information on using a command with a particular parameter and exact syntaxes, refer to the appropriate service chapter in this guide.

If you have Network Manager privilege, you can view a summary of the commands on the screen by entering a question mark (?) at the system prompt.

Depending on your software package and platform, some commands discussed in this chapter may not be available.

The commands are listed alphabetically in this chapter.

ADD

Syntax

```
ADD [!<port>] [-<service>] <set-name> <set-member>
```

Minimum Privilege Level

Network Manager

Description

The ADD command adds an object to a set. The exact function of this command depends on the set on which it operates. The modified set is saved to disk.

When the new list takes effect depends on the set. One of the following situations occurs:

- The list takes effect immediately.
- The list takes effect after a reboot.

For more information, refer to the appropriate service chapter in this guide.

Depending on the parameter, ADD is sometimes used with !<filterid> or !<logid> instead of !<port>. For more information on using the system parameters, refer to the appropriate service chapter.

Normal Response

Depends on the parameter.

Related Commands

DELete
SHow
SHowDefault

AddUser

Syntax

```
AddUser [<username>]
```

Minimum Privilege Level “Root” user with Network Manager privilege

Prerequisites You must enter the following command to use any user accounts added with AddUser:

`SETDefault -AC RESolutionOrder = Local`

Description The AddUser command creates a user account in the bridge/router database. The bridge/router uses this database to authenticate the user when there is an access request from the console port, Telnet connection, or from an X.25 pad incoming connection.

X.25 users only need to create user accounts if access control is enabled. Only users with recognized accounts can access the gateway.

Each account establishes an account name (initials, for example), access privilege, full name, and password. The user name, full name, and password consist of simple character strings. Account names and passwords are case-sensitive.

The Maximum Privilege field assigns the user access privilege. Entering NetMgr allows the user the maximum access privileges. Entering User allows only user access privileges. Each field has a maximum length:

Account name	15 characters
Full name	23 characters
Maximum Privilege	User/NetMgr
Password	15 characters

Remove user accounts from the NETBuilder database with the DELeteUser or UserManage command (also described in this chapter). The UserManage command also can be used to create user accounts.

Normal Response If the account name is not entered on the command line, the system prompts for the account name, along with the full name and password. The password is not displayed as it is typed; instead, a new prompt appears.

Related Commands DELeteUser
EXPire
PassWord
UserManage

ANameLookup

Syntax

```
ANameLookup “<entity-name>” [maxmatch]
```

Minimum Privilege Level User

Description The ANameLookup command is an AppleTalk command that performs an entity name lookup for named entities present in the distributed AppleTalk named-entity database (for more information on entity names, refer to Chapter 14 in *Using NETBuilder Family Software*).

The router waits a specified amount of time for responses before terminating the lookup procedure and displaying the results. The response time ranges from 1 to 300 seconds; the default is 10 seconds. You can adjust this default time interval by changing the NbpLookupTimer parameter. For more information, refer to "NbpLookupTimer" on page 4-14.

This command, in combination with the APING command, can be used to determine connectivity between the router on which this command is executed and other AppleTalk nodes with named services. For instance, AppleTalk-based file servers, printers, and routers can be located within specified zones.

You can specify the maximum number of name matches to look for because the name pattern specified may result in multiple responses. The default is 100.

Special wild-card characters are permitted in the object and type fields of the entity name value. An equal sign (=) by itself in either field signifies that all possible values are permitted. A tilde (~) indicates zero or more characters of any value. The zone field must contain a fully specified zone name and cannot have wild cards. The type field for a 3Com AppleTalk port entity name is always 3ComRouter.

If the total returned is equal to the max match (explicitly entered or the default of 100), the following string is appended to the line:

```
Max Matches returned, there can be more.
```

To interrupt the ANameLookup command, press the Break key.

The ANameLookup command and other third-party name lookup software will not find registered names of all 3Com router ports connected to Frame Relay and X.25 AppleTalk networks unless the router from which the name lookup was issued has established virtual circuits to all of the routers.

Normal Response Depends on the parameter.

Example The ANameLookup command attempts to locate all instances of 3Com AppleTalk ports in the B500MKT zone. This command presents up to 30 entity names in up to 10 seconds (default).

```
ANameLookup "=:3ComRouter@B500MKT" 30
Resolving...
"NB-0800002123456-1:3ComRouter@B500MKT" (20.45.2)
"B500-BACKBONE:3ComRouter@B500MKT" (20.45.2)
Total matches: 2
Elapsed Time: 10.0 seconds
```

The first response is a default entity name in the format used by the system. The object field is the datalink address qualified by port number 1.

The second response is for the same port, which has the same socket address of network 20, node 45, and socket 2. The entity name was created using the RouterName parameter.

APING

Syntax `APING {“<entity-name>” | <node-address>} [timeout (1–300 seconds)]`

Minimum Privilege Level User

Description The APING command determines whether or not a specified AppleTalk device is operating without connecting to that device. The specified device must support AppleTalk Echo Protocol (AEP). Use either the AppleTalk node address (net.node) or the AppleTalk entity name in the command.

To successfully perform the APING command, one AppleTalk port must be actively routing and must be connected to an AppleTalk network (not configured as CONTrol = NonAppleTalk). An AppleTalk node address associated with the bridge/router must exist in order to receive the APING response.

If you specify an entity name, APING first attempts to resolve the name into an AppleTalk node address and then issues the echo requests to the node address. This name-to-address resolution succeeds only if the target node registers the name on the AppleTalk Internet using the Name Binding Protocol (NBP) registration procedures.

APING sends an echo request packet to the destination device. Either a response from the specified device is received or the time-out value (in seconds) is exceeded. The default time-out value is 20 seconds. The maximum time-out value is 300 seconds. The AppleTalk router can send and respond to an APING command or its equivalent (available in third-party AppleTalk tools.)

When you specify an entity name, you can also use the time-out value (if specified) to determine the length of time to wait for the name resolution process to complete.

Elapsed time values include the local system processing times and may be significantly higher than actual packet round-trip time. Under heavy system load, times may be longer due to the priority of system processes. Since Echo packet delivery is not guaranteed, (Datagram Delivery Protocol (DDP) based), a response may not always return, especially in a busy networking environment.

To interrupt the APING command, press the Break key.

APING will not get a reply to 3Com router ports on Frame Relay and X.25 AppleTalk networks unless static configuration of addresses and virtual circuits exists to provide connectivity. The lack of multicast support in the Frame Relay cloud results in a no response to APING.

Example To determine if “Mac5:workstation@azone” is operating, enter:

`APING “Mac5:workstation@azone”`

The entity address resolves to 11.50.4 in 0.5 seconds.

```
Resolving...
“Mac:workstation@azone” (11.50.4)
Elapsed Time : 0.50 seconds
Pinging... 11.50 is alive.
Elapsed Time : 0.50 seconds
```

Normal Response If the specified device responds within the specified time, the <node-address> is alive message appears.

APpnPING

Syntax

```
APpnPING [<netid>.]<partner_lu_name> [Mode = <name>] [Size =
  <num>] [Consec = <num>] [Iterations=<num>] [Echo = Yes | No]
  [Userid = <string> [Password = <string>]]
```

Minimum Privilege Level User

Description The APpnPING command performs an Advanced Program-to-Program Communication (APPC) ping to another logical unit (LU) in the Advanced Peer-to-Peer Networking (APPN) network to determine if a route exists to that LU. The partner LU name can be entered either as a fully qualified or not-fully qualified LU name. This command is equivalent to the IBM Aping command (but do not confuse it with the NETBuilder® APING command, which is used for AppleTalk).

When you enter the APpnPING command, it runs until completion. One way to interrupt the process is to bring down the link through which the APPC ping is flowing, if it is known.

Although APpnPING may require some time to complete (for example, if Iterations is set to a large number), the system user interface reappears immediately. You can enter other commands while the APPC ping is taking place. You can enter multiple APpnPING commands, and up to five APPC pings can be taking place concurrently.

Values

<netid> Specifies the network ID of the partner LU you are pinging to. If the network ID is specified, a period is required between the network ID and the partner LU name.

<partner_lu_name> Specifies the partner LU you are pinging to.

Mode Specifies the mode that will be used for the APPC ping session. Valid modes include #CONNECT, #BATCH, #BATCHSC, #INTER, or #INTERSC. The default mode is #INTER.

Size Specifies the size of the data. The default size is 100 bytes.

Consec Specifies how many times to repeat the data within the same APPC ping request. For example, if the data size is 100 bytes and the Consec value at 3, when you send the ping request, the data will be 300 bytes. The default consec value is 1.

Iterations Specifies the number of times the APPC ping is sent. The default number of iterations is 2.

Echo Specifies whether the APPC ping receiver at the other end sends an echo back to the local node. The default value for Echo is Yes.

Userid Enters a user identification of up to 10 characters. The string is case-sensitive.

Password Enters an optional password to be used with the user identification. The password can be up to 10 characters long and is case-sensitive.

Example To perform an APPC ping to a partner LU named US3COMHQ.NN1 using the BATCH mode, a message size of 200 bytes, and a consec value of 3, and to have the ping sent 4 times, enter:

```
APpnPING US3COMHQ.NN1 Mode=#BATCH Size=200 Consec=3 Iterations=4
```

AtmToFr

Syntax `AtmToFr <VPI.VCI>`

Minimum Privilege Level User

Description The AtmToFr command converts a decimal VPI.VCI address under Asynchronous Transfer Mode (ATM) to the corresponding decimal data link connection identifier (DLCI) address under Frame Relay. This command is used for configuring an ATM network under the FR Service.

Values

<VPI.	Specifies a number between 0 and 255.
VCI>	Specifies a number between 0 and 65535.

Normal Response The normal response is the decimal DLCI address.

Related Commands FrToAtm

AuditLog

Syntax `AuditLog [<priorityLevel>] “<message>”`

Minimum Privilege Level User

Prerequisite You must set the -AuditLog LogServerAddr parameter to use a log file.

Description The AuditLog command generates a log message containing the specified message text and sends it to the network management station specified by the -AuditLog LogServerAddr parameter. If the -AuditLog LogServerAddr parameter is specified as 0.0.0.0, no messages are sent to the buffer for the log file. You do not need to configure the CONTrol parameter to activate this parameter.

Values

<priorityLevel> Determines the default messages sent to the log file. You can allocate a priority level to track an individual type of message. The following priority levels are available:

- LogEMerg
- LogINfo
- LogCRitical
- LogERror
- LogWArning
- LogNOtice
- LogALert
- LogDEbug

<message> May be any length if the overall length of the typed command, including the trailing quote, is less than 128 characters. The message must be enclosed in double quotes. The smallest message allowed (a pair of double quotes) generates an empty message.

BACkwards

The BACkwards command is available only if you are connected as a PAD-attached terminal to IP Internet-attached Telnet, Rlogin, or OSI servers.

Syntax

```
BACkwards
```

Minimum Privilege Level

User

Description

The BACkwards command helps manage multiple sessions from packet assembler/disassembler (PAD) attached terminals to Internet Protocol (IP) Internet-attached Telnet, Rlogin, or Open System Interconnection (OSI) servers. You can use BACkwards when the bridge/router functions as an X.25 connection service gateway for incoming extended connections.

This command resumes the session that precedes the current session. The preceding session is the one with the next lowest number to the current session that is listed in the session list. If the current session is the lowest-numbered session in the list, the preceding session is the highest-numbered session on the session display.

To display the session list, use the SHow -TERM SESsions command.

For example, if there are four active sessions (numbered 1, 2, 3, and 6; sessions 4 and 5 were previously deleted) on a port and the current session is number 1, the preceding session is number 6.

BACkwards does not allow you to skip sessions. For example, if there are four sessions and the current session is number 1 and the previous session was number 3, the BACkwards command does not jump back to number 3. Use the RESume command instead; for example, to get to session number 3, enter:

```
RESume 3
```

Related Commands

FORMAT
RESume
SWitch

Broadcast

The Broadcast command is available only if you are connected as a PAD-attached terminal to IP Internet-attached Telnet, Rlogin, or OSI servers.

Syntax

```
Broadcast [!<port>] “<string>”
```

Minimum Privilege Level

Network Manager

Description

The Broadcast command transmits string text messages over ports on the bridge/router. Follow the rules for specifying strings described in *New Installation for NETBuilder II Software*. You can use the Broadcast command when the bridge/router is functioning as an X.25 connection service gateway and receiving incoming connection requests.

If a port number (0–127 are valid on a NETBuilder II system) is not specified, the message is sent to all gateway ports that are not in listen mode and that have been configured for BroadcastON by the -TERM InterActTerm parameter. If a port number is specified and if reception of broadcast messages is disabled for the specified port (that is, if the -TERM InterActTerm parameter is set to BroadcastOFF), the gateway returns an error message. Broadcasts occur on active ports and those ports with the -TERM DeVice parameter set to Terminal.

If the InterActTerm parameter for the destination port is set to Verbose, the message is prefixed by the following text:

```
Broadcast from <user>:
```

If the InterActTerm parameter is set to Brief, the message text is displayed without the prefix.

Example 1 The following command transmits the specified text only to port 1 of the gateway:

```
Broadcast !1 “Printing requests are due by 1700 today”
```

Example 2 The following command issued from port 136 sends the message to all active ports (-TERM DeVice = Terminal) on the gateway:

```
Broadcast “Meeting in the lunch room in 5 minutes”
```

The following message is displayed on the destination ports:

```
Broadcast from port 136:
Meeting in the lunch room in 5 minutes
```

Normal Response A new prompt appears on the requesting port, and the message text appears on the destination ports.

CHange

Syntax

```
CHange -FIlter StationGroup <oldstationgroupname>
  <newstationgroupname>
```

Minimum Privilege Level Network Manager

Description The CHange command in the FIlter Service changes the name of an old station group to a new station group.

Related Commands ADD
DELete
SHow

ChangeDir

Syntax

```
ChangeDir [<device>:] [<path>]
```

Minimum Privilege Level Network Manager

Description The ChangeDir command changes the default directory. All subsequent file commands apply to the new directory. If no parameters are specified, the command changes the directory to the default file source when the system was booted. This directory is in effect only while the system is running. If you reboot the system, the directory defaults to the root directory on drive A.

Values

<device>	Specifies the local storage device, which can be a or b.
<path>	Indicates the new working directory.

Connect

The Connect command is available only if you are connected as a PAD-attached terminal to IP Internet-attached Telnet, Rlogin, or OSI servers.

Syntax

```
Connect <target> [,<target>]...[ECM]
```

For IP:

```
<target> = <IP address | name>
```

For OSI:

```
<target> = <PSAP address | name>
```

Minimum Privilege Level

User

Description

The Connect command requests a connection when the bridge/router is functioning as an X.25 connection service gateway. When the Connect command is executed from the bridge/router user interface, a connection from an X.25 PAD-attached terminal to a Transmission Control Protocol/Internet Protocol (TCP/IP) or OSI host is made.

In the Connect command syntax, if an address is substituted for <target>, an Internet address or an presentation service access point (PSAP) address can be used. The rules governing Internet addresses are described in *New Installation for NETBuilder II Software*. For information on Internet addressing, refer to Appendix D in *Using NETBuilder Family Software*; for information on PSAP addressing, refer to Appendix E in *Using NETBuilder Family Software*. The gateway recognizes explicit TCP/IP or PSAP and then attempts to make the connection using the appropriate protocol. The Connect command can be used in the following form:

```
Connect <address>
Connect <address>, <address>, <address>
```

If you specify a name in the preceding command syntax, the <target> accepts an Internet name or a Domain name for IP or a directory name or X.500 name for OSI. For more information on how the gateway attempts to establish a TCP Service connection, refer to “TELnet” on page 1-62 and “RLOGin” on page 1-49.

After you complete the connection initialization, the port is placed in data transfer mode. If the enter command mode (ECM) option is appended to the <target>, the port is left in command mode instead of the data transfer mode.

Connect rejects the following invalid Internet addresses:

- Unassigned addresses (0.0.0.0)
- Broadcast or loopback addresses (host fields all zeros or ones)

Example 1

In this example, a command requests a connection from a terminal to the name “tahoe.” A connection is made between the PAD-attached terminal and the address represented by “tahoe,” and both the originating and destination ports are in data transfer mode after the successful connection.

```
Connect tahoe
```

Example 2

In this example, a command requests a connection to the address represented by “accounting.” If it fails, a connection to 129.2.1.5 is attempted. When the connection is complete, the port is placed into command mode.

```
Connect accounting, 129.2.1.5 ECM
```

Example 3

In this example, a command requests a connection to “host1”; if it fails, try “host2”; if “host2” fails, try “host3.”

```
Connect host1, host2, host3
```

Example 4

In this example, a command requests a connection to a remote management port on a 3Com bridge/router, which is represented by the PSAP address “/49/005308000212345601!1.128”.

```
Connect /49/005308000212345601!1.128
```

Normal Response

A successful connection is indicated by a message similar to one of the following messages:

```
Connecting using OSI...connected session 2, ECM Char is ^^
```

Related Commands

DisConnect
RLOGin
TELnet
VTp

COpy

Syntax

```
COpy [<device>:]<src_filename> [<device>:][<dest_filename>]
```

Minimum Privilege Level

Network Manager

Description

The COpy command copies boot and configuration files from a local device to a remote device, from a remote device to a local device, or from a local device to a local device (for example, backing up a file from one location in a device to another location).

Copying from a local device to a local device applies to the NETBuilder II bridge/router and the SuperStack II bridge/router only.

Values

<device>: Specifies the device that the source file resides on and the device that you want the source file copied to. You can specify either the IP address of a remote Trivial File Transfer Protocol (TFTP) server or a local drive identifier. NETBuilder II bridge/routers have drives A and B. The flash PROM on the SuperStack II NETBuilder and OfficeConnect NETBuilder bridge/routers is drive A.

If you do not specify a device, the system assumes the default drive and prompts you to continue.

<src_ filename> Specifies the name of the source file that you want to copy. You can precede the filename with the directory pathname. If a directory pathname is not complete, the system tries to access the file on the source device’s default directory.

The COpy command cannot use a destination directory without a filename unless the destination directory is terminated with a slash to preserve the original filename.

Specify * if you want to copy all files and directories.

The filename can also contain metacharacters. @M indicates 12 characters of the media access control (MAC) address of the input/output (I/O) port used for the remote booting of the system. @m indicates the last 6 characters of the MAC address of the I/O port used for the remote booting of the system. If a local floppy is used as the system's boot source, @M and @m expands to a null character stream.

<dest_ filename> Specifies an optional name for the destination file. You can precede the filename with a directory pathname. If a directory pathname is not specified, the system copies the file to the default location on the destination device. If you do not specify a destination filename, the system uses the filename specified in the source filename (it does not use the pathname).

The filename can also contain metacharacters. @M indicates 12 characters of the MAC address of the I/O port used for the remote booting of the system. @m indicates the last 6 characters of the MAC address of the I/O port used for the remote booting of the system. If a local floppy is used as the system's boot source, @M and @m expands to a null character stream.

Example 1 To copy a file called macros/schedule that resides on a local bridge/router with a floppy drive to a remote file server with an IP address of 129.142.10.10, enter:

```
COpy macros/schedule 129.142.10.10:3Com/@m/macros/
```

An I/O port with a MAC address of 080002030A68 was used for booting the system from a remote boot server. This file is copied to the following location on the remote file server's default directory:

3Com/030A68/macros

Example 2 To copy a file called boot.29k from a flash memory drive to a floppy drive on a NETBuilder II bridge/router, enter:

```
COpy a:boot.29k b:boot.sav
```

The new copy of the file will be called boot.sav.

Normal Response The system displays messages that indicate the status of the copy and transfer processes. For every 10,000 bytes of file transferred, the system displays a period (.).

DEFine

Syntax `DEFine <macroname> = (<text>)`

Minimum Privilege Level Network Manager

Description The DEFine command creates a macro file and specifies its contents. When a new macro is created with the same name as an existing macro, the new macro contents replace the old ones. Table 1-1 shows the commands used to manipulate macros.

Table 1-1 Commands Used with Macros

Command	Function
DEFine <macroname>	Defines a macro.
DO <macroname>	Executes a macro.
FLush <macros>	Clears the contents of the macro cache on the system.
SHow MACros	Displays a list of macro names defined on the local system.
SHow MACros macroname	Displays the contents for the specified macro file.
UNDefine <macroname>	Removes a macro file.

Macro Names

For the NETBuilder II bridge/router, a macro name can be up to 14 characters long; a name longer than 14 characters is truncated. The first character of a macro name must be alphabetic. Upper- and lowercase letters in macro names are not distinguished.

Macro Contents

Macro contents must begin with a left parenthesis, as shown in the syntax. If the definition requires more than one line, press the Return key after the opening parenthesis. After you press the Return key, the Macro: prompt appears on the next line. All characters entered between the opening and closing parentheses are part of the macro. Nested parentheses in balanced pairs are allowed. Any time before the closing parenthesis is entered, you can press the Break key to cancel the DEFine command.

The text of the macro must conform to the conventions for entering strings listed in *New Installation for NETBuilder II Software*. A single macro can contain no more than 256 characters. The normal system prompt returns when you end the macro with the final closing parenthesis.

A macro can contain any valid system commands. In addition, macros can branch to other statements, accept input, and pass arguments. The bridge/routers support more powerful macro features such as variables, conditional statements, macro caching, and shared macros. For more information, refer to Appendix G in *Using NETBuilder Family Software*. A macro can include the DO command to call up other macros, including calls to itself.

Executing Macros

Each line of a macro is not printed on the terminal screen. To display each line, just before the line is executed, set the InterAction parameter to MacroEcho at the beginning of the macro.

Press the Break key to cancel the execution of a macro after it has started unless the InterAction parameter for that port has been set to NoMacroBreak. For more information, refer to "InterAction" in Chapter 2.

Example

The following example defines a macro called route that enables various routing functions on the system:

```
DEFine route = (
  SETDefault -BRidge CONTrol = Bridge
  SETDefault -IDP CONTrol = Route
  SETDefault -IP CONTrol = ROute
  SETDefault -CLNP CONTrol = Route
  )
```

To execute this macro, enter:

```
DO route
```

Related Commands

DO
FLush MACros
SHow MACros
UNDefine

DEFRag

Syntax

```
DEFRag [<device>:]
```

Minimum Privilege Level Network Manager

Description The DEFRag command reclaims *dirty space* on a flash memory card. Dirty space is memory that has been written and cannot be used again until it has been erased. If you do not specify a device, drive A will be used.

Normal Response A system prompt appears.

DELete

Syntax

```
DELete [!<port>] [-<service>] <set-name> <set-member>
```

Minimum Privilege Level Network Manager

Description The DELete command usually deletes an object from a list. The only exception is the DELete -TCP CONNections command, which aborts a Transmission Control Protocol (TCP) session. For more information, refer to “CONNections” on page 59-1. The exact function of this command depends on the parameter.

The change is saved to the disk.

When the DELete command takes effect depends on the set used with the command.

Depending on the parameter, the DELete command is sometimes used with !<filterid> or !<logid> instead of !<port>. For more information on using the system parameters, refer to the appropriate service parameters chapter in this guide.

Normal Response A system prompt appears.

Related Commands

ADD
SHow
SHowDefault

DELeteUser

Syntax

```
DELeteUser <username>
```

Minimum Privilege Level “Root” user with Network Manager privilege

Description The DELeteUser command removes the specified user from the user account database of the local server. This command only applies to local access control. The UserManage command also removes user accounts.

Normal Response A new prompt appears.

Related Commands

AddUser
UserManage
EXPire

DIal

Syntax

For non-ISDN interfaces

Port-based dialing:

```
DIal !<port> [-PORT] ["<dial-string>"]
```

Path-based dialing:

```
DIal !<path> -PATH ["<dial-string>"]
```

For ISDN interfaces

Port-based dialing:

```
DIal !<port> [-PORT] ["<dial-string>"]
```

Path-based dialing:

```
DIal !<connectorID.channel ID> -PATH ["<dial-string>"]
```

Minimum Privilege Level Network Manager

Default Port-based dialing

Description ***Port-based dialing*** The port-based DIal command dials on a port or virtual port using a specific dial string or using no dial string.

If you use the DIal command with only the port number specified, the software looks for the highest-priority phone number listed for the port through the -PORT DialNoList command. If the highest-prioritized phone number is not available, the system tries another phone number specified for the port if more than one phone number is configured. The path preference list determines which paths can be selected for the call. If a DTR modem is used, the software looks for the DTR phone number before looking at the dial number list.

The system finds a path by first checking if a path is in the path preference list. If it is, the highest priority path in the list consistent with the phone number is used. If no path is found in the preference list, the system determines whether the port can use the dynamic dial pool. If the dynamic dial pool is available, the system checks for an available path that matches the device type set in the -PATH ExDevType parameter for the phone number entry in the dynamic dial path pool, binds it to the port, and makes the call.

If no phone numbers are configured in the dial number list and no path is a DTR dial modem, the call attempt fails and an error message is displayed.

Paths that are attached to data terminal ready (DTR) modems should not be configured as dynamic paths. If they are configured in this way, they are ignored.

If you specify a port number and a dial string, you can temporarily override the phone numbers in the phone list for outbound calls; however, the telephone number has to be listed in the -PORT DialNoList parameter.

Port-based dialing *without* the dial string brings up the port with the bandwidth set as specified in the NORMalBandwidth parameter. Port-based dialing *with* the dial string dials the telephone number and brings up the port with the bandwidth set as specified in the NORMalBandwidth parameter. Additional paths may be brought up using the resources listed in the -PORT DialNoList parameter.

Path-based dialing The path-based DIal command dials on the specified path. The path number specified must be a static path; dynamic paths are not supported.

If you issue the DIal command without a phone number specified, the system uses the highest-prioritized phone number from the -PORT DialNoList parameter for the path that is statically bound to the port. If the attached modem is DTR, then the telephone number stored in the modem is used. If you set the -PATH DialMode parameter to V.25bis, you must have at least one number in the dial number list, or you will receive an error message when attempting to dial.

Path-based dialing *without* the dial string dials using the specified path with the telephone number from the -PORT DialNoList parameter and brings up the port with the bandwidth set as specified in the NORMalBandwidth parameter. Path-based dialing *with* the dial string dials for the specified path the telephone number specified by the dial string and brings up the port with the bandwidth set as specified in the NORMalBandwidth parameter. If you specify a dial string, you can temporarily override the phone numbers in the phone list or the number specified with the -PORT DialNoList parameter. You can test phone numbers on a per-static path basis. If you want to test phone numbers on specific dynamic paths, test them as static paths first.

When specifying a dial string in an Integrated Services Digital Network (ISDN) environment, you can include a phone number, and if applicable, a subaddress. If specifying a phone number and subaddress, specify the phone number, followed by a semicolon (;), followed by the subaddress.

General (applies to port- and path-based dialing) All DIal commands, whether path- or port-based, share the following common characteristics:

- The DIal command triggers bandwidth management to evaluate bandwidth on the port and take appropriate action, either allocate additional resources to meet the normal bandwidth specification, or hang up some path resources.
- The DIal command can only be executed on ports enabled with a positive bandwidth specified with the -PORT NORMalBandwidth parameter.
- The dial string specified in the DIal command must also be listed in the -PORT DialNoList parameter.

The DIal command does not bring up additional paths to provide disaster recovery or bandwidth-on-demand.

The DIal command retries the dial string to establish the connection the number of times specified in the -PORT DialRetryCount parameter. (The DialRetryCount algorithm determines how many times to dial again.) The -PORT DialIdleTime parameter monitors the line for inactivity. If the port is idle for the duration of DialIdleTime, then all outbound dial paths are disconnected.

When using non-V.25bis modems or terminal adapters (TAs), the phone numbers must be stored in the modem. The dial number and dial string stored on the bridge/router are ignored.

DirectoryManage

The DirectoryManage command is available only with software packages that support OSI.

Syntax

```
DirectoryManage
```

Minimum Privilege Level

Network Manager

Description

The DirectoryManage command is a menu-driven interface that adds, removes, or lists names in the X.500 directory. You can use this command when the bridge/router functions as an X.25 connection service gateway for incoming connections from PAD-attached terminals to LAN-attached Virtual Terminal Protocol (VTP) hosts. The gateway cannot implement the X.500 directory service, but can participate in it.

For information on how to add, remove, and list names in the X.500 directory, refer to "X.500 Directory Service" in *Using NETBuilder Family Software*.

The DSAAddress parameter must be configured and the DSAType parameter must be verified to match the X.500 server type before the X.500 directory can be modified. For more information, refer to "DSAAddress" on page 40-2 and "DSAType" on page 40-2.

Related Commands

Connect
VTp
UnBindDSA

Related OSIAPPL Service Parameters

DSAAddress
DSAType
DuaState
NameSourceOrder
UnbindTimer

DisConnect

The DisConnect command is available only if you are connected as a PAD-attached terminal to IP Internet-attached Telnet, Rlogin, or OSI servers.

Syntax

```
DisConnect [!<port>] [<session number>]
```

Minimum Privilege Level

User privilege to specify the session number
Network Manager privilege to specify the port

Description

The DisConnect command disconnects a session. You can use this command when the bridge/router is functioning as an X.25 connection service gateway and is receiving incoming connections from PAD-attached terminals to IP Internet-attached Telnet, Rlogin, or OSI servers.

If you specify a session number, the DisConnect command disconnects the specified session. If you do not specify a session number, the current session is disconnected. If you specify a port number, a network manager can disconnect any session on the specified port. Port numbers 0–127 are valid on the NETBuilder II system.

Normal Response

The following message appears:

```
Disconnecting ... disconnected
```

Related Commands

Connect
RLOGin
TELnet
VTp

DiscoverRoutes

Syntax

```
DiscoverRoutes <media address> [!<port>] [<timeout> (1–120 sec)]
 [AllRouteExp] [Xid] [Save]
```

Minimum Privilege Level Network Manager

Description The DiscoverRoutes command allows routes to a remote station to be determined and displayed. A route can be optionally selected among the learned routes and cached as either a discovered route or a static route. Up to 16 routes can be recorded and displayed in order of arrival. The DiscoverRoutes command can be accessed only through the command line interface.

The DiscoverRoutes command applies only to ports (token ring, Fiber Distributed Data Interface (FDDI), and high-speed serial (HSS) running Frame Relay, Switched Multimegabit Data Service (SMDS), or Point-to-Point Protocol (PPP)) with the end system source routing option enabled with the -SR RouteDiscovery parameter.

For each route discovered, the following information is displayed:

Number Assigned route number.

Port Associated port number.

LFS Largest frame size.

Delay Round-trip delay in milliseconds.

Routes Route descriptor in a forward direction. A transparent spanning tree route is indicated by the string “Transparent.” A source route is indicated by a sequence of ring numbers and bridge numbers, where the ring number is preceded by a colon (:) and the bridge number is preceded by an ampersand (&).

The following screen display indicates that a source-routed packet was initiated at Ring 25 and forwarded through Bridge 2 onto Ring 4 before reaching its destination:

```
Station Address = %xxxx, Number of Routes = 2
Number     Port        LFS            Delay     Routes
1          3           4399           4         Transparent
2          3           4399           5         :25&2:4
```

Values <media address> Specifies the media address of a remote station as 12 hexadecimal digits preceded by a percent sign (%)

Precede the media address with Cmac to specify that the media address is in canonical format and Ncmac to specify that the media address is in noncanonical format:

```
[Cmac | Ncmac] %xxxxxxxxxxxx
```

If you specify the port number but not Cmac nor Ncmac, the current setting of the -SYS MacAddrFormat parameter determines whether the MAC addresses are displayed in canonical or noncanonical format.

<port> Specifies the port number of the network interface that can reach the remote station. If the port number is not specified, a route discovery packet is transmitted on all interfaces that support end system route discovery.

<timeout> Specifies the time interval in seconds to wait for responses to the route discovery packet. The default is 5 seconds.

AllRouteExp Specifies that the route discovery TEST/XID frames are transmitted as All Route Explorer frames. By default, the less expensive Spanning Tree Explorer frame is used to traverse the source routed network through the spanning tree path.

Xid Specifies that XID frames are used as the route discovery packet. The default route discovery packet is a TEST frame.

Save Selects the save option. If one or more routes exist for the remote station, a prompt appears to request the route number to save and to determine whether the route is to be cached as a dynamic or a static route. You can display the saved route with the SHow -SR AllRoutes command.

DiscRouteRs

Syntax

```
DiscRouteRs [!<port>|<source IP>] [Broadcast] [<timeout (1-30
  seconds)>]
```

Minimum Privilege Level Network Manager

Description The DiscRouteRs command discovers neighboring RDP routers. To discover neighboring routers, you can specify either the outgoing port number or one of the system IP addresses for systems in host mode (!0) to send router solicitations from. After the command is entered, the system transmits router solicitations every second until the time set using the timeout option. During the timeout period, any router advertisements that are received are displayed.

Values

!<port> Specifies the outgoing port number to send route solicitations from.

<source IP> Specifies the source IP address sent with router solicitations. If you do not specify a source IP address, router solicitations are sent with the actual source IP address of the system.

Broadcast If Broadcast is specified, the IP destination address is set to limited broadcast address (255.255.255.255). If Broadcast is not specified, the IP destination address is set to the all-routers address (224.0.0.2).

<timeout> Specifies the time in seconds to stop transmitting router solicitations. The default is 15 seconds if no port or source IP is specified. If a source IP address is specified, the default is five seconds.

DiskFiles

Syntax

```
DiskFiles [<device>:][<path>]
```

Minimum Privilege Level Network Manager

Description The DiskFiles command displays a listing of all files in a root or subdirectory on the local storage device when the configuration file source has been set to the local device. If a NETBuilder II bridge/router is being booted remotely and the configuration file source has been set to the boot device and File Transfer Protocol (FTP) has been selected as the remote file access protocol, the DiskFiles command displays a listing of all files in the remote subdirectory containing the configuration files.

Do not use the DiskFiles command on a card that you have formatted for a memory dump using the EraseDump command. The DiskFiles command shows a file system access error message, but the card is formatted correctly for a memory dump.

Values

<device> Specifies a local storage device. NETBuilder II bridge/routers have drives A and B. The flash PROM on the SuperStack II NETBuilder and OfficeConnect NETBuilder bridge/routers is drive A.

If you do not specify a device, the system assumes the default drive and prompts you to continue.

<path> Specifies a listing of files that exist in a particular subdirectory.

If you do not specify a path, the system displays a listing of files in the configuration file source directory that was defined for the boot source.

When specifying the path option, you can specify metacharacters, that is, @M indicates the 12 characters of a MAC address; @m indicates the last six characters of a MAC address.

DLTest

Syntax

```
DLTest [Abort | DestAddr | PArameters | PktCount | PktSize | RAte
 | RcvCheck | SrcAddr | START | STATistics | StatUs | TestMode |
 TestDuration | ZeroStats]
```

Minimum Privilege Level Network Manager

Description

The DLTest command initiates the data link test (DLT) over a local area network (LAN) or high-speed serial (HSS) path, specify how the test is run, and display the test results. The exact syntax and function of the command depend on the option you select.

The DLT helps you determine whether a bridge/router can properly exchange packets with another device that supports the DLT Protocol. The HSS DLT performs a loopback operation for you to test the physical connection between an HSS path and a channel service unit and digital service unit (CSU/DSU) or modem. Only one DLT at a time can be run on a bridge/router. The bridge/router on which you initiate the test accepts only the echoed packets from the destination device.

The HSS DLT operates in a non-intrusive way, for example, the under-test interface is affected but all other interfaces work normally. The test detects line errors if packets cannot be transmitted or received and records the number of packets misordered, lost, duplicated, or corrupted. The test also calculates the round-trip delay of packets. The statistics obtained from the test are stored in the bridge/router and are displayed by the DLTest STATistics command.

For proper operation of DLTest over Ethernet, token ring, or FDDI, you must set the source address to the MAC address of the port from which the DLTest traffic is generated (Ethernet, FDDI, or token ring MAC I/O board). The default DLTest source address is the MAC address of the main processor module. Do not change the default DLTest source address for HSS ports. On the HSS port carrying data traffic, you must set a static bridge route for the destination address of the receiving station.

CAUTION: *Normal bridging and routing functions are interrupted on the under-test interface while HSS DLT is running. Bridging and routing functions are not interrupted while LAN DLT is running; however, system performance may be impacted.*

Values

Abort — Stops the DLTest packet transmission.

DestAddr — Sets the address of the destination bridge/router or station to which the DLTest packets are transmitted. The destination must be a station that runs the DLT Protocol and the address must be a MAC address.

For a bridge/router that performs bridging only, add the destination address as a static route to the bridge routing table before executing over a remote port. This ensures that the destination address of the remote port does not age out of the route table during execution of the test. For loopback testing, the destination address is not required.

For either bridging only or routing only, the destination address selected must be one of the addresses used on the network.

PArameters — Displays the values of the DLTest parameters that the test uses on its next run. New values that are set while the test is running do not affect the current test, but take effect at the next test. Use the DLTest STATistics parameter to see the current DLTest parameter values.

PktCount — Specify the following options:

DLTest PktCount <decimal>	Sets the number of packets to be sent out.
DLTest PktCount Infinite	Continues the test until a DLTest Abort command is entered. The default is Infinite.

PktSize — Sets the size of the transmitted packets, the minimum-to-maximum packet size range, and the size of each increment. Use the following options to set these values:

DLTest PktSize <pk size>

DLTest PktSize <min pk size>-<max pk size>

DLTest PktSize <min pk size>-<max pk size> <increment>

The packet size is interface-type-dependent. The packet size for Ethernet and HSS can range from 60 to 1,450 bytes. The default minimum packet size is 60 bytes; the default maximum is 1,450 bytes. The packet size for token ring can range from 18 to 4,442 bytes. The default minimum packet size is 18 bytes; the default maximum is 1,450 bytes. The default increment size is 1 byte.

When packet transmission starts, the packet size increases by <increment> bytes from the minimum to the maximum size. After the maximum size is reached, the packet size returns to the minimum, and transmission continues until all packets are sent out or the test is aborted.

The maximum packet size does not need to be a multiple of the increment size. If the maximum size is not a multiple of the increment size, the packet size returns to the minimum before the maximum packet size is reached.

RAte — Specify the following options:

DLTest RAte <decimal> Sets the number of packets to be transmitted per second. The default is 10 packets per second.

DLTest MaxRate Causes DLTest to transmit the packets as fast as possible.

The test transmission rate depends on the packet size. As the packet size increases, the transmission rate decreases.

If the packet size is 60 bytes, the maximum test transmission rate is approximately 677 packets per second on an Ethernet network. If the packet size is 18 bytes, the maximum test transmission rate is approximately 800 packets per second on a token ring network.

For HSS loopback, the transmission rate is calculated based on the baud rate and maximum packet size.

RcvCheck Determines whether the test examines the packets received from the destination and how it examines them.

Specify the following options:

DLTest RcvCheck None The test does not examine the received packets (default value).

DLTest RcvCheck Length The test checks whether the received packets have length errors.

DLTest RcvCheck Data The packets are checked for both length errors and data corruption.

SrcAddr Defines the source address of the test. For the source station, which transmits the DLTest packets, this address is the MAC address of the port on which the packets are transmitted. For the destination station, which receives the DLTest packets, this address is the MAC address of the port on which the packets are received. On a NETBuilder II system, the address needs to be set manually.

START Starts the DLTest. All DLTest statistics are zeroed at the start of a new test. You must assign a value to DestAddr before starting the test except when TestMode is set to Loopback.

The optional values for <sendingport> and <receivingport> may be used when a loopback test is being performed between two ports on the same device. The <sendingport> value designates the sending port and the <receivingport> value designates the receiving port.

STATistics Displays the test parameter values and statistics for the current test including the following:

Transmit statistics

Number of transmitted packets
Number of transmitted bytes
Average transmission rate

Receive statistics

Number of received packets
Number of received bytes
Maximum, minimum, average, and current incoming packet rate
Maximum, minimum, and average round-trip delay

Good packets

Receive error statistics
Number of lost, misordered, and duplicated packets
Number of received packets with a length error
Number of received packets whose data is corrupted

The following is an example of the screen display:

```
DLTEST PARAMETERS
src address = %080002A0089D   dest address = %000000000000
transmit rate (pkt/sec)    10 transmit packet count         Infinite
min xmit pkt size (bytes)  60 max xmit pkt size (bytes)     1450
packet size increment      1  rcv checking mode             None
test mode                  NoRemoteEcho
TRANSMIT STATISTICS
number of packets          0  number of bytes
ave xmit rate (pkt/sec)    0
RECEIVE STATISTICS
number of packets          0  number of bytes               0
max rcv pkt rate (pkt/sec) 0  ave rcv pkt rate (pkt/sec)    0
min rcv pkt rate (pkt/sec) 0  cur rcv pkt rate (pkt/sec)    0
max round trip delay (ms)  0  good packets                  0
min round trip delay (ms)  0  ave round trip delay (ms)     0
RECEIVE ERROR STATISTICS
lost packets               0  misordered packets            0
length error packets       0  data corrupted packets        0
```

The statistics displayed by the DLTest STATistics parameter are slightly different for loopback mode than for non-loopback mode.The following paragraphs define the terms used in the statistical displays:

Receive error statistics
The DLTest STATistics command displays the receive error statistics, which show the number of lost, misordered, and duplicated packets, and packets with the wrong length or corrupted data. A packet can be counted as both lost and misordered. This can occur because a packet not received is counted as a lost packet, but if it arrives later, it is counted as a misordered packet. Similarly, the same packet can be counted as both duplicated and misordered.

Round-trip delay
The DLTest STATistics command displays the average, minimum, and maximum round-trip delay in milliseconds under Receive Statistics. The round-trip delay of a packet includes the local bridge/router delay, network delay, and remote device delay.

To estimate the delay time when a bridge/router forwards a packet from one end station to another, divide the value of round-trip delay by two. The statistics are updated at regular intervals between 1 and 10 seconds.

StatUs
Specify the following options:

Idle
DLTest is not running.

Running (as initiator)
The system has initiated a DLTest and is transmitting packets

Running (as target)
The system is receiving DLTest packets. It is the destination of a DLTest initiated on another system.

TestMode — Specify the following options:

- RemoteEcho — The destination device echoes the DLTest packets to the source of the test.
- NoRemoteEcho — DLTest acts as a one-way traffic generator (default value).
- LoopBack — Tests the physical connection between a HSS path and a CSU/DSU or modem. During a loopback test, test packets that are transmitted across the HSS path are looped back by the CSU/DSU or modem attached to the HSS path. The LoopBack option may also be used in an ISDN configuration where data is transmitted on one bearer channel and looped back by the other.

  The CSU/DSU or modem must be configured for loopback operation before starting the HSS DLT.

  Whenever DLTest is started in LoopBack mode, a test checks if the currently selected packet rate (PktCount) and the packet size (PktSize) exceeds the bandwidth of the serial line being used for the DLTest. If the PktCount and PktSize exceed the serial line bandwidth, the loopback test is started, but the following warning message is displayed:

```
Warning: Current PktCount/PktSize exceeds serial line bandwidth.
```

To run a loopback test on a high-speed serial path, follow these steps:

TestDuration — Specifies the number of seconds a test should run. If not specified, an infinite time duration is assumed.

A discrepancy between the number of packets transmitted and received may occur as a result of using the TestDuration option. This discrepancy may occur because when running the test with a specified duration, the test ends abruptly as soon as the time duration expires.

A discrepancy between the number of packets transmitted and received may occur as a result of using the TestDuration option. This discrepancy may occur because when running the test with a specified duration, the test ends abruptly as soon as the time duration expires.

ZeroStats — Zeros out the DLTest statistics whether or not a test is running.

The CSU/DSU or modem must be configured for loopback operation before starting the HSS DLT.

DO

Syntax

```
DO <macro name>[+<macro name>] [<params>]
```

Minimum Privilege Level User

Description The DO command executes a specified macro that you have previously created using the DEFine command. You can enter the macro name in either upper- or lowercase letters.

Press the Break key to interrupt the execution of a macro unless the InterAction parameter has been set to NoMacroBreak. For more information about the InterAction parameter, refer to Chapter 2.

Use the plus sign (+) to link several macro files to form a final, large macro. Do not include a blank space before or after the plus sign in the command line.

The parameters are optional, depending on the function of the macro. If the macro operates on or modifies a particular parameter, include the parameter. For more information on macros, refer to "DEFine" on page 1-11.

Normal Response Each command in the macro file and the system responses to the commands do not appear on the screen as the macro is executed unless the InterAction parameter is set to MacroEcho. To echo the commands in the macro file, set the InterAction parameter to MacroEcho. For information on setting the InterAction parameter, refer to Chapter 2.

Other normal responses depend on the contents of the macro. Error messages can be generated if a command contained in the macro fails.

Related Commands

DEFine
FLush MACros
SHow MACros
UNDefine

DteToIp

Syntax

```
DteToIp [!<port>] <PDN type> <DTE address>
```

Minimum Privilege Level Network Manager

Description The DteToIp command converts the <PDN type> X.25 address to an IP address for the provided PDN type. The public data network (PDN) type can be one of the following: DDN, BFE, or LaPoste.

Echo

Syntax

```
Echo [-n] "<string>"
```

Minimum Privilege Level User

Description The Echo command prints a specified string on the terminal screen. Specify the string according to the syntax recommendations described in *New Installation for NETBuilder II Software*. If the specified string is too long to fit in the system buffer, the string is truncated at 80 characters, and an error message appears.

If the -n option is specified, Echo does not append a new line to the string (by default, a new line is always appended). The -n option provides another method to conveniently include prompts within conditional macros (in addition to the $> output variable).

The Echo command is most commonly used within a macro. The string is sent to the terminal executing the macro even if normal echoing is turned off by the InterAction parameter. For information on setting the InterAction parameter, refer to Chapter 2.

Normal Response The specified string is displayed on the terminal, followed by a new prompt. If the command is executed within a macro, the new prompt appears once macro execution is complete.

Related Commands DEFine

EraseDump

This command is used only by the NETBuilder II bridge/router with DPE.

Syntax

```
EraseDump <device>:
```

Minimum Privilege Level Network Manager

Description The EraseDump command erases and prepares a flash memory card for a full dump.

Do not use the DiskFiles command or the firmware DF command on a card that you have formatted for a memory dump using the EraseDump command. The DiskFiles and DF commands show a file system access error message, but the card is formatted correctly for a memory dump.

Related Commands PutDump
SysconF

EXPire

Syntax

```
EXPire <username>
```

Minimum Privilege Level “Root” user with Network Manager privilege

Description The EXPire command invalidates a particular account password.

If the EXPire command is not used, a password expires when the specified time on a timer elapses. Use the EXPirationTimer parameter to set this timer, or enter:

```
SHow -AC EXPirationTimer
```

If you are unsure about the security of a password, use the EXPire command immediately to change a password for each user account created. You also can use the UserManage command to force a password to expire. For more information, refer to “UserManage” on page 1-65.

This command applies only to local access control.

Normal Response A new prompt appears.

Related Commands AddUser
DELeteUser
SETDefault -AC EXPirationTimer
SHow -AC EXPirationTimer
UserManage

FLush

Syntax

```
FLush [!<port>] [-<service>] <param-name>
```

Minimum Privilege Level Network Manager

Description The FLush command removes dynamic information (information learned from the network) from tables created by the system. The function of this command can vary depending on the parameter on which it operates.

The FLush -SYS MACros command clears the contents of the macro cache on the system. Caching macros enables the system to access a macro file quickly without accessing the local diskette or sending another request over the network to the file server. The bridge/router automatically stores the macros in the cache as they are requested. The number of macros the system stores depends on the size of the cache.

The system can keep the contents of the cache active for several days. If the network manager obsoletes or changes macro files on the macro file server, the macros that are still present in the system cache become invalid.

The FLush -SYS MACros command can also prevent discrepancies between the DO <macroname> and SHow -SYS MACros commands. The DO command first searches the cache for the file and then examines the local diskette or macro file server. Conversely, the SHow -SYS MACros command always reads the macro file from the local diskette or macro file server, not from the cache. If the file stored in the cache is not the same as the one on the diskette or file server, you execute a file other than the one displayed by the SHow command.

When you use the FLush -SYS STATistics [-<service>] syntax, several seconds may pass before statistics sampling is restarted.

Normal Response A system prompt appears.

Related Commands SHow
SHowDefault

FORMAT

Syntax

```
FORMAT [<device>:]
```

Minimum Privilege Level Network Manager

Description The FORMAT command formats the media in the specified device. If no device is specified, drive A is used.

Normal Response A confirmation prompt appears.

FORwards

The FORwards command is available only if you are connected as a PAD-attached terminal to IP Internet-attached Telnet, Rlogin, or OSI servers.

Syntax

```
FORwards
```

Minimum Privilege Level User

Description The FORwards command helps manage multiple sessions from PAD-attached terminals to IP Internet-attached Telnet, Rlogin, or OSI servers. You can use the FORwards command when the bridge/router functions as an X.25 connection service gateway for incoming extended connections.

The FORwards command connects you to the session with the next highest session number from the current session. If the current session has the highest session number, FORwards connects you to the session with the lowest session number. For example, if there are four active sessions (numbered 1, 2, 3, and 6; sessions 4 and 5 were previously deleted) on a port and the current session is number 6, the FORwards command connects you to number 1, which is the next highest session. Use the SHow -TERM SESsions command to display the list of session connections.

The FORwards command does not allow sessions to be skipped. For example, if there are four sessions, and the current session is number 1 and the previous session was number 3, the FORwards command does not jump forward to 3. Use the RESume command instead; for example, to get to session number 3, enter:

```
RESume 3
```

Related Commands BACkwards
RESume
SWitch

FrToAtm

Syntax

```
FrToAtm <DLCI address>
```

Minimum Privilege Level User

Description The FrToAtm command converts a decimal DLCI address under Frame Relay to the corresponding decimal VPI.VCI address under ATM. The DLCI address is a number between 0 and 1023. You can configure an ATM network under the FR Service.

Normal Response The normal response is the decimal VPI.VCI address.

Related Commands AtmToFr

GET

Syntax

```
GET [<IP address>:][<src_path>/]<src_filename>
  [<device>:][<dest_path>/][<dest_filename>]
```

Minimum Privilege Level Network Manager

Description The GET command copies boot and configuration files from a remote device to the local storage device using the services of an FTP server. The FTP logon information that is needed to connect to the FTP server must have already been defined through the SysconF command or the firmware SF command.

Values

<IP address>	Specifies the IP address of the remote FTP server.
<src_path>	Specifies the path where the source file to be transferred resides. An absolute path can be specified by entering slash (/) or backslash (\) as the first character. If a slash or backslash is not the first character, the path is assumed to be a relative path. The specified path is a path relative to the root directory or to the directory specified with the ChangeDir command.

You can specify metacharacters when specifying the source path, that is, @M indicates the 12 characters of a MAC address; @m indicates the last six characters of a MAC address.

If <src_path> is not specified, the default directory is the root directory or the directory specified with the ChangeDir command.

<src_filename> Specifies the name of the source file that you want to transfer to the local storage device. You can specify metacharacters when specifying the filename, that is, @M indicates the 12 characters of a MAC address; @m indicates the last six characters of a MAC address. You can use an asterisk (*) to get all files in the <src_path> directory; however, if you use an asterisk with this option, <dest_filename> cannot be used.

<device> Specifies a local storage device. NETBuilder II bridge/routers have drives A and B. The flash PROM on the SuperStack II NETBuilder and OfficeConnect NETBuilder bridge/routers is drive A.

If you do not specify a device, the system assumes the default drive and prompts you to continue.

<dest_path> Specifies the path where the copied file will reside. An absolute path can be specified be entering slash (/) or backslash (\). If a slash or backslash is not the first character, the path is assumed to be a relative path.

The specified path is a path relative to the root directory or to the directory specified with the ChangeDir command.

You can specify metacharacters when specifying the destination path, that is, @M indicates the 12 characters of a MAC address; @m indicates the last six characters of a MAC address. Since DOS conventions apply, names that exceed eight characters are truncated to meet DOS requirements.

If <dest_path> is not specified, the default directory is the root directory or the directory specified with the ChangeDir command.

<dest_filename> Specifies the DOS name of the file on the local storage device. If no filename is specified, the source file name will be converted into a DOS-compatible filename.

Example 1 To transfer a file called 3Com.nm/rbcs/data/image/boot.29k in the login directory at the file server whose address is 129.213.10.10 to the directory called image on the local flash memory drive, enter the following command (assuming local boot and FTP login parameters have been set up):

```
GET 129.213.10.10:/tftp/image/NBII/CP/sw/90/boot.29k a:image
```

Example 2 To transfer a file called 3Com.nm/030A68/bin/mp6e.29k in the remote configuration directory at the file server (assume 030A68 is the last six digits of the MAC address of the boot port) to a file called mp8.0 on the floppy disk drive, enter the following command (assuming remote configuration and FTP login parameters have been set up):

```
GET 3Com.nm/@m/bin/mp6e.29k b:mp8.0
```

Normal Response The system displays messages that indicate the status of the copy and transfer process. For every 10,000 bytes of file transferred, the system displays a period (.).

Related Commands COpy
PUT

HangUp

Syntax

For non-ISDN interfaces

Port-based disconnecting:

```
Hangup !<port> [-PORT]
```

Path-based disconnecting:

```
HangUp !<path> -PATH
```

For ISDN interfaces

Port-based disconnecting:

```
Hangup !<port> [-PORT]
```

Path-based disconnecting:

```
HangUp !<connectorID.channelID> -PATH
```

Minimum Privilege Level Network Manager

Default Port-based hangup

Description The HangUp command disconnects a dial-up path manually (path-based disconnecting) or allows you to disconnect all phone connections on the specified port (port-based disconnecting). By default, port-based disconnecting is performed. This command can hang up calls on dynamic paths or static paths. If the path is dynamic and is currently bound to a port, the HangUp command disconnects the call, unbinds the path, and places the path back into the dial pool.

Bandwidth management compares the bandwidth of the current port against the bandwidth set with the -PORT NORMalBandwidth parameter for actions such as hanging up the line or changing the NORMalBandwidth setting, and makes any required adjustments.

This command can disconnect a dial-up path used for disaster recovery or bandwidth-on-demand tuning. If disaster recovery or bandwidth-on-demand is configured and an additional path is activated (due to failure or bandwidth overload of the line), when the HangUp command is issued on the additional path, the call is disconnected. BOD will bring up the lines again only if congestion persists. If you do not want the additional path to be reconnected after disconnection, you must change the dial-up configuration before or immediately after you issue the HangUp command.

InStall

The InStall command is supported on any 3Com hardware platform that runs the Boundary Routing system architecture software. For a complete listing of possible platforms, refer to Chapter 32 in *Using NETBuilder Family Software*.

Syntax

```
InStall
```

Minimum Privilege Level Network Manager

Description The InStall command returns you to the boundary router's System Configuration menu after you exit from the boundary router menu interface to access the command line interface. You must enter the InStall command at the Network Manager prompt (NETBuilder #).

Normal Response The boundary router System Configuration menu is displayed again.

IpToDte

Syntax

```
IpToDte [!<port>] <PDN Type> <IP address>
```

Minimum Privilege Level Network Manager

Description The IpToDte command converts the <PDN Type> IP address to an X.25 address for the provided PDN type. The PDN type can be one of the following: DDN, BFE, or LaPoste.

LIsten

Syntax

```
LIsten [!<port>]
```

Minimum Privilege Level User

Network Manager to specify the port number (only valid when the X.25 connection service is present)

Description The LIsten command terminates the user interface session, whether that session is initiated through the local console port, the network management port (using Telnet or VTP), or a PAD port of the X.25 connection service. When entering the LIsten command with User privilege, the only affected port is the one on which the command was issued.

When issued on the local console, an at sign (@) is displayed. To log back in, press the Return key at the at sign (@) prompt, and the Netlogin: prompt appears.

The NetLogin: prompt does not reappear if the InterAction parameter is set to NoLOGin. For information on setting the InterAction parameter, refer to Chapter 2.

When issued on the network management port through Telnet or VTP, the Telnet session is closed. When issued on a PAD port, all Telnet, Rlogin, and VTP sessions are closed and the X.25 call is cleared.

With Network Manager privilege and the presence of the X.25 connection service software, you can specify a port number with the LIsten command. In this case, the LIsten command disconnects all sessions on a port and puts the port in listen mode if it is in command or data transfer mode. Valid port numbers are 0–127 for the NETBuilder II system.

Only ports in listen mode can accept connections from another device.

If this command is entered from a PAD port during connection service, any existing IP/OSI connection is closed and the X.25 call is cleared.

Example With Network Manager privilege, this command terminates all existing sessions on port 3 and puts port 3 on the gateway into listen mode. Depending on the application, data can be lost in open files when a session is terminated with the LIsten command.

```
LIsten !3
```

Normal Response When the LIsten command is entered from the console port, the at sign (@) appears. A prompt appears if the specified port number is not the port from which the LIsten command was entered.

Related Commands LOGout

LOGout

The LOGout command is available only with software packages that support X.25.

Syntax

```
LOGout [!<port>]
```

Minimum Privilege Level

User
Network Manager to specify the port number

Description

The LOGout command clears a port's user profile from the bridge/router memory. You can use the LOGout command to disconnect a session between an X.25 PAD-attached terminal (through the bridge/router functioning as an X.25 connection service gateway) and an IP Internet-attached Telnet, Rlogin, or OSI servers.

If a port is in command or data transfer mode, the LOGout command places the port in listen mode. If no port number is included, the LOGout command affects the port on which the command is entered. The network manager can include a port number with the LOGout command to indicate that the specified port is to be placed in listen mode. Valid port numbers are 0–127 for the NETBuilder II system.

Depending on the application, data can be lost in open files when a session is terminated with the LOGout command.

Only ports in listen mode can accept connections from another device.

If the AutoListen timer expires, the user profile is cleared and the port is placed in listen mode. This has the same result as executing the LOGout command; .

Example

The following command logs out port 3 of the gateway on which the command is entered. You must have Network Manager privilege before you can log out users on other ports.

```
LOGout !3
```

Normal Response

If a terminal is attached to the console port, the LOGout command usually causes a single at sign (@) to appear on the screen. The PAD prompt appears if the specified port number is not the port from which the LOGout command was entered.

MacAddrConvert

Syntax

```
MacAddrConvert <MacAddress>
```

Minimum Privilege Level

User

Description

The MacAddrConvert command converts a media access control (MAC) address in canonical format to noncanonical format and vice versa.

Example

To convert a canonical MAC address to a noncanonical MAC address, enter the command as shown in the following example:

```
MacAddrConvert 08005AB6C731
```

A display of the address converted into noncanonical format appears as follows:

```
%10005A6DE38C
```

When entering the MAC address, do not enter the percent sign (%) prefix.

MakeDir

Syntax

```
MakeDir [<device>:][<path>]<subdirectory name>
```

Minimum Privilege Level Network Manager

Description The MakeDir command creates a subdirectory on a local storage device when the configuration file source has been set to the local device. If a NETBuilder II bridge/router is being booted remotely, the configuration file source has been set to the boot device, and FTP has been selected as the remote file access protocol, the MakeDir command allows you to create a subdirectory in the remote directory containing the configuration files.

Values

<device> Specifies a local storage device. NETBuilder II bridge/routers use drives A and B. The flash memory on the SuperStack II NETBuilder and OfficeConnect NETBuilder bridge/routers is drive A.

If you do not specify a device, the system assumes the default drive and prompts you to continue.

<path> Creates a subdirectory that is not at the configuration file source directory level. You can create up to four subdirectory levels. For example, to create the subdirectory "secondlevel" that is in subdirectory "firstlevel," specify "firstlevel/secondlevel."

When specifying the path option, you can specify metacharacters. @M indicates the 12 characters of a MAC address; @m indicates the last six characters of a MAC address.

You must specify the name of the new subdirectory.

Normal Response A system displays a message that indicates the subdirectory was created.

Related Commands

DiskFiles
RemoveDir
ReName

MEnu

Syntax

```
MEnu [-<service>] [<param-name>]
```

Minimum Privilege Level Network Manager

Description The MEnu command can display three levels of menus. From these menus you can display and modify parameters and be prompted for the appropriate sequence to enter.

If the CurrentServices parameter is set to ALL, the Main menu appears after you enter the MEnu command, allowing you to choose a service.

Depending on your hardware and software configuration, the list of available services on the Main menu may differ.

If the CurrentServices parameter is set to a particular service, the Main menu displays only that service. For example, if the current service is PORT, only the PORT Service entry appears in the Main menu.

If you specify the service in the MEnu command, the parameters in the specified service are displayed, not the ones in the current service. For example, if the current service is PORT, and you enter MEnu -PATH, the PATH Service menu containing parameters in the PATH Service is displayed.

The Environment parameters are not accessible through the MEnu command. To manipulate these parameters (for example, the InterAction and PRIvilege parameters), enter the appropriate command at the system prompt. Environment parameters are available regardless of the current service.

In the service menu, the parameters are numbered. The commands that can be used to modify the parameters are enclosed in parentheses. If no commands follow a parameter, as in the case of the CONFiguration parameter in the PORT Service menu, the parameter can only be displayed.

If you select a configurable parameter from the service menu, another menu displays information on that parameter and prompts you for the port number (if appropriate) and command.

When entering the MEnu command, if you include the parameter to be modified or displayed, the first two levels of the service menu are skipped.

For example, if you enter MEnu -PATH NAme, the following menu appears:

```
==================== SHow -PATH NAme ==================
Path !1 NAme = Path1
Path !2 NAme = Path2
========= -PATH NAme parameter menu (Level 3)==========
1  - SetD
Select (1-1) ... <CR> to Exit ====>
```

MONitor

Syntax `MONitor`

Minimum Privilege Level “Root” user with Network Manager privilege

Description The MONitor command enters the firmware monitor for all platforms except the NETBuilder II bridge/router with DPE. If you have a DPE module, the MONitor command enters the software debug monitor. Refer to the section that applies to your platform.

Firmware Monitor

The monitor utility allows you to perform the following tasks:

- Use commands to boot the system, perform system housekeeping tasks, or perform diagnostic tasks
- Modify firmware parameters to customize the operation of your system; for example, defining the boot sources
- Display product information encoded on the EEPROM

***CAUTION**: The MONitor command halts normal system operation.*

Most monitor commands, except for booting the system, system housekeeping, and diagnostics, can be performed using the SysconF command without halting the system. However, because the monitor is in firmware, it is accessible even when the system software is unavailable.

Normal Response

The following message appears after you enter the MONitor command:

```
WARNING: Monitor mode halts normal operations. Confirm (Y/N)?
```

To enter monitor mode, enter:

Y

The monitor prompt (>) appears.

NETBuilder II with CEC Module

To resume normal system operation for a NETBuilder II with CEC module, enter:

Go

To resume normal operation after using monitor commands that interact with memory, such as CO and DU, reinitialize and reboot the system by pressing the front panel Reset switch or by entering:

RS

SuperStack II and OfficeConnect Bridge/Routers

To resume normal system operation for a SuperStack II or OfficeConnect bridge/router, you must reset the system by entering:

RS

Debug Monitor (DPE Only)

The MONitor command enters the debug monitor. The debug monitor is one of three configuration tools for the DPE module along with the boot monitor and the SysconF command. See Appendix B for a description of the firmware boot monitor utility. The SysconF command is described in Appendix A.

Unlike the CEC monitor utility which repeats functionality in the SysconF command, functionality is divided among the three DPE configuration tools.

CAUTION: *The MONitor command halts normal system operation.*

Options

The following commands are available in the debug monitor:

Go	Returns to the software prompt.
RS	Resets system.
DU	Performs manual dump (when entered due to fatal error).
DM, DH, or DB	Displays memory.
FX or FS	Finds hex/string in memory.
IG	Initializes gdb for later attach.

Normal Response

To enter the debug monitor, enter:

Y

The monitor prompt (>) appears.

To resume normal system operation, enter:

Go

To resume normal operation after using monitor commands that interact with memory, such as DU, reinitialize and reboot the system by pressing the front panel Reset switch or by entering:

RS

MRInfo

Syntax

```
MRInfo <target IP> [!<port>] [<timeout (0–120 seconds)>]
```

Minimum Privilege Level Network Manager

Description The MRInfo command finds neighboring multicast-capable routers, and requests neighboring router information and interface-state information.

The MRInfo command first sends an AskNeighbors packet to request information from neighboring routers. If a reply is received with a non-zero value in the group address field, an AskNeighbors2 packet is sent to request interface state information. The AskNeighbors or AskNeighbors2 packet is sent every second until a reply packet is received or a timeout occurs. If no timeout is specified, the default is 5 seconds.

The following information is displayed as a result of the MRInfo command:

Neighbor's IP address The sending router's address as seen by the neighbor's neighbor list.

Neighbor's neighbor The IP address of the neighboring router.

Metric The cost of the interface.

Threshold The TTL that a packet must have to be forwarded to any of the neighbors in the Neighbor's neighbor field.

Status Provides status messages as follows:

- Leaf Indicates that the router is a leaf node.
- PIM Indicates that the router is running the Protocol Independent Multicast (PIM) Protocol.
- Down Indicates that the router's interface is down.
- Dis Indicates that the router's interface is disabled.
- Tun Indicates that the router's interface is a tunnel interface with IP-over-IP encapsulation (neighbors are reached through a tunnel).
- Tun(sr) Indicates that the router's interface is a tunnel interface that uses Loose Source Route Option.
- Querier Indicates that the router is the subnet's query router.

Values

<target IP> Specifies the IP address of the target device.

<port> Specifies the outgoing port number. If the <target IP> is a multicast IP address, the !<port> must be specified.

<timeout> Specifies the time in seconds for a reply to occur. A value between 0 and 120 seconds can be specified. If no value is specified, the default is 5 seconds.

MTraceRoute

Syntax

```
MTraceRoute <source> <destination> [G <group>] [H <reports>]
  [!<port>] [T <timeout>] [W <gateway>] [R <Resp addr>]
  [L <Resp ttl>]
```

Minimum Privilege Level Network Manager

Description

The MTraceRoute command traces a branch of a multicast tree from a specified receiver to the source. A router receiving a multicast trace route request packet adds its forwarding information associated with the requested pair (source, group) to the request packet and then forwards the packet to the upstream router. The router that receives the packet with the maximum number of reports reached, or the requesting source falls within one of the router's local subnets, sends a multicast trace route response to the address that is provided in the original request packet.

The following information is displayed as a result of the MTraceRoute command:

Hops	The number of hops to the destination system.
IP subnet	The IP address of the router.
Protocol	The multicast routing protocol being used (DVMRP, MOSPF, Protocol Independent Multicast (PIM) Protocol, or Core-Based Trees (CBT) Protocol.
Threshold	The threshold required to forward packets.
Delay Time	The cumulative delay for the trace route query to reach this router.
ErrorFlag	The error status and meaning are displayed:

No Error	No error.
Wrong Interface	The query packet arrived on the interface that is not on the forwarding tree.
Pruned	A pruned message was sent to the upstream router for this group.
Output Pruned	The query packet arrived on the interface that is pruned for the pair (source, group).
Scoped	The query packet arrived on an interface that is scoped.
No Route	No route exists to the source.
No Forwarding	The query packet arrived on an interface that is not forwarding.
No Space	No space is available for the new report.
Old Router	The router does not support multicast trace route.

Values

<source>	The IP address of the source and group to be queried.
<destination>	The IP address of the receiver to which the multicast tree is being traced. This address must fall in one of the neighboring router's subnets, and the virtual interface associated with the subnet must be on the forwarding tree for the queried source. If !<port> or R <Resp addr> is not specified, <destination> must be set to one of the local subnets and determines the outgoing port to which multicast trace route query packets are sent.
<group>	The group address of the source and group to be queried. This address must be preceded with the keyword G. The default group address is 224.2.0.1 (MBONE audio).
<reports>	The maximum number of hops for the query packet to travel. This number must be preceded with the keyword H. The default is 32 hops maximum.

If no response packet is received before the timeout, the query packet is sent in a hop-to-hop mode, similar to a unicast trace route. The query packet is sent out with the Number of Reports set to one and then increased by one until it reaches the maximum hop count or no response packet is received.

<port> Specifies the outgoing port for the query packet.

If no port number is specified, the outgoing port is determined by the <destination> or by W <gateway> if it is provided.

<timeout> Indicates the time in seconds to wait for a response packet.

The timeout range is from 0 to 120 seconds.

The default timeout value is 5 seconds.

<gateway> The IP address of the last hop router on the path from the source to the destination. Using this address allows you to send out a unicast query packet directly to a specific router.

This address must be preceded with the keyword W.

If <gateway> is not provided, the query packet is sent to the group address if the destination is not on any directly connected subnet. The packet is sent to 224.0.0.2 (all routers) if the destination is directly connected.

<Resp addr> The address to which the response packet is sent.

This address must be preceded with the keyword R.

This address can be the sender's local IP address from which the query packet is transmitted or one of the multicast addresses to which the sender listens.

<Resp ttl> The value to be placed into the TTL field of the IP header of the response packet. The value ranges from 1 to 255.

This value must be preceded with the keyword L.

The default is 1 if the packet is destined for 224.0.0.2.

The default is 64 if the packet is destined to a multicast address; otherwise, the default is set to 255.

NetwarePING

Syntax

```
NetwarePING &<network>%<host> [timeout (1–300 seconds)]
```

Minimum Privilege Level User

Description The NetwarePING command determines connectivity to an Internet Packet Exchange (IPX) node on the network, including other 3Com bridge/routers.

NetwareTraceRoute

Syntax

```
NetwareTraceRoute &<network>%<host>
```

Minimum Privilege Level User

Description The NetwareTraceRoute command is a troubleshooting tool used for locating malfunctioning devices. When you specify a destination IPX address, this command probes all the intermediate routers and servers traversed along the path before reaching the final destination node, measures round trip delays, and displays the results.

Error Messages (Optional)

```
Can’t trace route to &300%080002001234 now - try later.
```

Example

In this example, the destination node is 3 hops away. The trace route requester has tried trace route requests four times including those routes on the local network and one diagnostic request because the target server does not support NetWare trace route. Enter:

`NetwareTraceRoute &00000101%000000000001`

```
NetwareTraceRoute to &00000101%000000000001 ...
Hops  Next Router Address      Round Trip Delays
0     <skipping a router>      * * *
1     &00000200%080002A00AF0    3 ms  5 ms  4 ms
2     <skipping a router>      * * *
3     <skipping a router>      * * *
3     &00000101%000000000001    6 ms  7 ms  6 ms
```

Only the second router responded to the trace route request. Non-participating routers are shown by the <skipping a router> value. If the target server supported the trace route protocol, there is not a diagnostic request.

NetwareView

Syntax

```
NetwareView &<network>%<host> [timeout (1–300 seconds)]
```

Minimum Privilege Level

User

Description

The NetwareView command obtains configuration information from a NetWare server. This command uses NetWare diagnostic request and response packet types.

Normal Response

The following is a sample display of a target server configuration received by the NetwareView command:

```
Major version: 1
Minor version: 0
SPX Diagnostic Socket: 4002
Number of Components: 3
Component ID: 0 (IPX/SPX)
Component ID: 1 (Router Driver)
Component ID: 6 (File Server/Router)
Number of Local Networks: 2
Local Network Type: 1 (Non-dedicated File Server (virtual board)
Network Address1 &0000DADA
Node Address1 %000000000001
Local Network Type: 0 (LAN/WAN board)
Network Address2 &00000303
NodeAddress2 %2608C4C5755
```

OPING

Syntax

```
OPING <NSAP address | name> [timeout (1–300 seconds)]
```

Minimum Privilege Level

User

Description

The OPING command determines whether or not a particular OSI device is operating without connecting to that device. The device is specified by its network service access point (NSAP) address or name. For information on NSAP addressing, refer to Appendix E in *Using NETBuilder Family Software*.

The OPING command triggers transmission of an echo request (ERQ) protocol data unit (PDU) that accepts one of the following responses:

- Echo reply PDU (ERP)
- Error report PDU (ERR)

If the ERQ PDU does not receive a response within the amount of time specified by the time-out value elapses, the destination is considered unreachable. The default time-out value is 5 seconds.

Normal Response If the device responds within the specified time, a message similar to the following appears:

```
destination is alive
```

OTraceRoute

Syntax

```
OTraceRoute <NSAP address>
```

Minimum Privilege Level User

Description This OSI command traces a path to an OSI destination. The display provides the OSI address of each gateway used to forward packets to a particular destination.

You must specify the NSAP address of the OSI destination that you want to trace.

Normal Response A display similar to the following appears:

```
TTL       Next_Hop_Address
1         /47/0004/00351100080020031C4B00
```

Related Commands OPING

PassWord

Syntax

```
PassWord
```

Minimum Privilege Level User

Description The PassWord command changes your password. After you enter the PassWord command, the system prompts you for the old password. If you enter a password that does not match the password in the database, the system immediately displays a system prompt.

When you enter the password that matches the password in the database, the system prompts you for the new password, which is limited to 15 characters. After you enter the new password, you are prompted to retype it for verification. The system saves the new password on the disk and displays the service prompt. The new password immediately takes effect. For confirmation, you are prompted twice for the password.

Normal Response The password is changed, and a new prompt appears.

Related Commands EXPire
UserManage

PathSwitch

Syntax

```
PathSwitch <RTP name>
```

Minimum Privilege Level User

Description The PathSwitch command for APPN High Performance Routing (HPR) allows you to initiate a nondisruptive path switch to switch an RTP connection to another path. The name of the RTP connection is required to perform the path switch.

When you initiate a path switch, the system determines which path is the most desirable for the RTP connection at the time, and then switches to it. If the current path is the most desirable path for the RTP connection, then the RTP connection remains on the current path. An RTP connection can only switch paths through HPR nodes; you cannot switch an RTP connection to a path where one or both partner nodes is performing Intermediate Session Routing (ISR) only.

To obtain a list of RTP connection names, enter the SHow -APPN RTP command.

Normal Response You will receive a confirmation that the path switch took place, or an error message stating that the path switch attempt did not succeed.

PAuse

Syntax

```
PAuse [<seconds>]
```

Minimum Privilege Level User

Description The PAuse command causes the command interface to pause for a specified number of seconds. This command is normally used within a macro.

If the number of seconds is not specified, the command interface pauses for one second. The maximum length of a pause is one day (86,400 seconds). Use the Break key to interrupt the PAuse command.

Normal Response The command interface for the current session pauses for the number of seconds specified.

Related Commands DEFine

PING

Syntax

```
PING <IP address> [timeout (0–300 seconds)]
```

Minimum Privilege Level User

Description The PING command determines whether or not a specified IP device is operating without having to connect to that device. The specified device must support the Internet Control Message Protocol (ICMP). Use the Internet address of the destination in the command.

PING sends ICMP echo request messages to the destination device at a rate of one per second until there is a response or until the specified time-out value (in seconds) is exceeded. The default time-out value is 20 seconds. The maximum time-out value is 300 seconds. The system can send, as well as respond to, a PING command. To interrupt the PING command, press the Break key. A timeout value of 0 (zero) seconds may be specified.

You may want to use the PING command to check whether an IP host on the network is up and running when you are using the system only for bridging.

Normal Response If the host responds within the specified time, the <IP address> is alive message appears.

PUT

Syntax

```
PUT [<device>:][<src_path>/]<src_filename>
  [<IP address>:][<path>/][<dest_filename>]
```

Minimum Privilege Level Network Manager

Description The PUT command transfers boot and configuration files from the local storage device to a remote device using the services of an FTP server. The FTP logon information that is needed to connect to the FTP server must be defined using the SysconF software command or the SF firmware command before using the PUT command.

Values

<device> Specifies the local storage device if your bridge/router has more than one.

Only the NETBuilder II bridge/router can have two local storage devices: one floppy disk drive and one flash memory drive. If the bridge/router has only a single local storage device, this parameter can be set to A or left unassigned.

On the NETBuilder II bridge/router with both floppy disk drive and flash memory drives, the floppy disk drive is referred to as device B and the flash memory drive as device A. If the bridge/router has multiple local storage devices and you do not specify a device, the system assumes the default drive and prompts you to continue.

<src_path> Specifies the path where the source file is located. An absolute path can be specified by entering slash (/) or backslash (\) as the first character. If a slash or backslash is not the first character, the path is assumed to be a relative path.

The specified path is a path relative to the root directory or to the directory specified with the ChangeDir command.

You can specify metacharacters when specifying the destination path, that is, @M indicates the 12 characters of a MAC address; @m indicates the last six characters of a MAC address.

If <src_path> is not specified, the default directory is the root directory or the directory specified with the ChangeDir command.

<src_filename> Specifies the name of the source file that you want to transfer to the local storage device. Specify an asterisk (*) to transfer all files in the <src_filename> directory. <dest_filename> cannot be specified when an asterisk is used.

<IP address> Specifies the IP address of the remote FTP server.

<dest_path> Specifies the subdirectory where the file will be copied to. If the configuration file source has been set to local or the bridge/router was booted from the local device, the specified path is relative to the configuration file source directory.

The specified path is a path relative to the root directory or to the directory specified with the ChangeDir command.

When specifying the source relative path, you can use metacharacters, that is, @M indicates the 12 characters of a MAC address; @m indicates the last six characters of a MAC address.

If <dest_path> is not specified, the default directory is the root directory or the directory specified with the ChangeDir command.

<dest_filename> Specifies the name of the file at the remote device. If no file name is specified, the source file name will be used.

Example 1 To transfer a file called boot.29k on the flash memory drive to 3Com.nm/rbcs/data/image in the login directory at the file server at 129.213.10.10, enter the following command (assuming that the FTP login parameters have been set up):

```
PUT a:boot.29k 129.213.10.10:/tftpboot/image/NBII/CP/SW/90/boot.29k
```

Example 2 To transfer a file called mp6e.29k on the floppy disk drive to 3Com.nm/030A68/bin/mp6e_saved in the login directory at the file server (assume 030A68 is the last six digits of the MAC address of the boot port), enter the following command (assuming that FTP login parameters have been set up):

```
PUT mp6e.29k 3Com.nm/@m/bin/mp6e_saved
```

Normal Response The system displays messages that indicate the status of the copy and transfer process. For every 10,000 bytes of file transferred, the system displays a period (.).

Related Commands COpy
GET

PutDump

This command is used by the NETBuilder II bridge/router with DPE only.

Syntax

```
PutDump <device>: [<IP address>:][<path>/]<dest_filename>
```

Minimum Privilege Level Network Manager

Prerequisite Use the SysconF command to set the FTP logon information that is needed to connect to the FTP server.

Description The PutDump command transfers a memory dump from a local flash memory card to a remote server using FTP.

This command may be used to transfer the full dump to 3Com for technical support.

Values

<device> Specifies the local flash memory drive, a or b.

<IP address> Specifies the IP address of the remote FTP server. If you do not specify the IP address, the server address configured using SysconF is used.

<path> Specifies the subdirectory where the file is copied to.

<dest_filename> Specifies the name of the file at the remote device.

Related Commands EraseDump
PUT
SysconF

ReaD

The ReaD command is available only if you are connected as a PAD-attached terminal to IP Internet-attached Telnet, Rlogin, or OSI servers.

Syntax

```
ReaD [!<config file>] <filename>
```

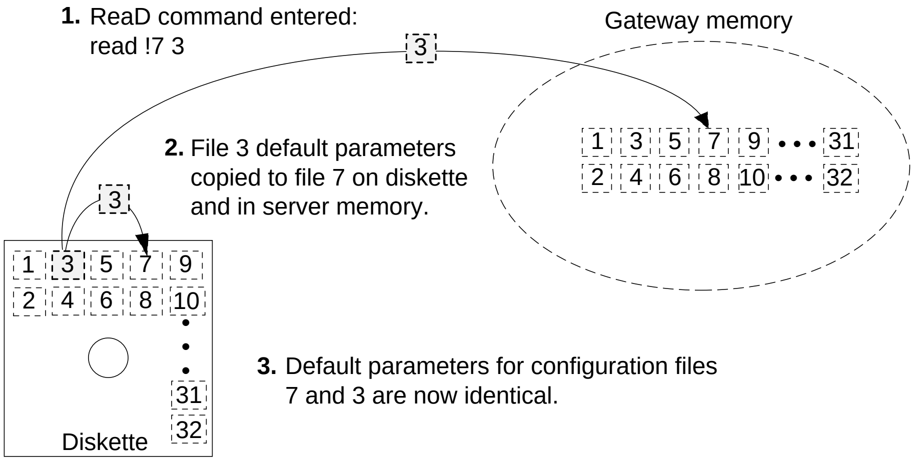
Minimum Privilege Level Network Manager

Description The ReaD command copies the parameter values from the specified configuration file (<filename>) on diskette to replace the default parameter values for the specified configuration file (!<config file>) both in memory and on the diskette. If no configuration file is specified, the current session's default parameters are overwritten by the values specified in <filename>. You can use this command when the bridge/router functions as an X.25 connection service gateway and accepts incoming connection requests from PAD-attached terminals to IP Internet-attached Telnet or Rlogin servers.

On a gateway that boots from its own diskette, verify that the diskette is in the disk drive before entering the command.

Figure 1-1 is a diagram showing the operation of the ReaD command, ReaD !7 3. In this example, the default parameters for configuration file 7 are replaced by the ones for configuration file 3, both in memory and on the diskette. After the ReaD command, the default parameters for configuration files 7 and 3 are the same. When an incoming automatic connection request is made that specifies configuration 7 as the call user data, the gateway port is initialized with the new session parameters that were copied from configuration file 3.

The specified filename can be an alphanumeric name. The gateway does not differentiate between upper- and lowercase in filenames. The filename also can be a number from 1 to 32. Regardless of whether the gateway boots from a local disk drive, each gateway has its own set of numbered files.



1. ReaD command entered:
read !7 3
Gateway memory
3
2. File 3 default parameters copied to file 7 on diskette and in server memory.
3
1 3 5 7 9 • • • 31
2 4 6 8 10 • • • 32
1 3 5 7 9
2 4 6 8 10
31
32
Diskette
3. Default parameters for configuration files 7 and 3 are now identical.

Figure 1-1 Effects of the ReaD Command

Example 1 This command creates new default parameter values for configuration file 8 by reading the parameters currently stored as defaults for configuration file 9 into configuration file 8. To ensure that the in-memory and disk copies of the default values are identical, the ReaD command automatically saves the new values to configuration file 8 on disk.

```
ReaD !8 9
```

Example 2 This command first copies the alternate configuration file (a set of parameters appropriate for connection to a host) named “finance” into the in-memory default configuration file 6, and then saves the in-memory default values to the diskette as file 6.

```
ReaD !6 finance
```

Normal Response The prompt appears.

Related Commands SAve
SETDefault

ReBoot

Syntax

```
ReBoot [slot]
```

Minimum Privilege Level Network Manager

Description The ReBoot command reboots your bridge/router. You can use the slot number with the ReBoot command to select and reset a multiprocessor I/O module that has halted after a crash. You can specify a slot between 1 and 8.

The system response to the ReBoot command depends on its firmware configuration. For firmware configuration information, refer to the appropriate installation guide.

CAUTION: *Rebooting stops the normal operation of the system.*

Normal Response After you enter the ReBoot command, a display similar to the following appears:

```
NETBuilder Power-up
CPU-4 Megs Private RAM, 2 Megs Shared RAM, -Passed N3 MMON rev.00I
Ethernet Controller 1 - Passed    Station Address - 080002A031B7
Ethernet Controller 2 - Passed    Station Address - 080002A031B8
HSS Card - not present.
Booting from Floppy
```

REMote

Syntax

```
REMote [<IP address> | [&<network>]%<host>] [<command>]
```

The <command> syntax is available with IP, but not with Xerox Network Systems (XNS). Remote XNS is not supported on the SuperStack II bridge/router platform.

Minimum Privilege Level Network Manager

Description The REMote command provides access to the commands available on the specified 3Com gateway server, communications server, network control server, internetwork bridge, or bridge/router. The address specified must be an IP address or an XNS address. The REMote command is not subject to the password and may allow access by unauthorized users. You can disable the use of REMote with the NetAccess parameter.

If you connect remotely to a 3Com bridge/router using an XNS address, you can use the address of any of its ports. On a wide area configuration, you can connect remotely using the high-speed serial line through which you communicate with the system, provided that a network number has been assigned to that line.

After you enter the REMote command, the Remote prompt (Remote:) appears where you can enter any command available on the device to which you connect remotely. For information on the availability of commands in remote mode for the specific device, refer to the appropriate manual. You can also enter a question mark (?) at the Remote: prompt to see a list of the commands that can be used. If you enter a command that is not available, the following message appears:

```
Command not accessible through remote.
```

The appearance of the Remote: prompt does not indicate communication with the specified device. The attempt to communicate with that device happens only after you enter a command at the prompt.

Press the Break key to exit remote mode.

The following system commands cannot be used in remote mode:

IP Service commands:

- PING
- TraceRoute

SYS Service commands:

- DEFine
- DO
- LIsten
- PAuse
- REMote
- SHow History
- SysconF
- UNDefine

You may experience a time-out failure if you use the REMote command to transmit a large quantity of data in a single transaction over a serial line operating at a baud rate of 448 kbps or lower.

If the output from a single command is large (for example, the output from the SHow -SYS STATistics command), the User Datagram Protocol (UDP), upon which REMote is based, sends the data as one large UDP packet. The IP Protocol fragments the packet; if fragments are lost, a timeout failure occurs. To avoid timeout failures, use the REMote command over serial lines that operate at a baud rate of 1536 kbps or higher, or use the TELnet command.

If you enter the REMote command and a command is included, the single command is executed in remote, and the system prompt appears. For example, enter the following command to display the software version of a system whose IP address is 129.12.2.3:

```
REMote 129.12.2.3 SHow -SYS VERSion
```

For a system to be accessed remotely from another device, the -SYS NetAccess and -SYS RemoteManager parameters must be set appropriately.

CAUTION: *The software allows NetAccess to be disabled without giving any warning messages. After assigning NoRemote, NoTelnet, or NoConsole to NetAccess, you can no longer access the bridge/router parameters to perform* *software configuration. You must boot the bridge/router with a bridge/router diskette that contains an enabled NetAccess parameter before you can regain access.*

For reference information on these parameters, refer to “NetAccess” on page 58-10 and to “RemoteManager” on page 58-12. For configuration information, refer to “Preventing Remote Access” on page 53-10 and “Restricting Remote Access” on page 53-10 in *Using NETBuilder Family Software*.

The changes made to NetAccess and RemoteManager take effect immediately. Suppose you have successfully used the REMote command on system A to access system B, and at the Remote: prompt, you enter:

```
SETDefault -SYS NetAccess = NoRemote
```

The Remote: prompt still appears. But when you enter a command, an error message appears because you configured system B as inaccessible for the REMote command.

Example 1 To access the device with Internet address 129.12.2.3 in remote mode, enter:

```
REMote 129.12.2.3
```

Example 2 To access the device with network number 3145 and MAC address %080002009999 in remote mode, enter:

```
REMote &3145%080002009999
```

Example 3 To display the software version on the device with address 129.12.2.3 in remote mode, enter:

```
REMote 129.12.2.3 SHow -SYS VERSion
```

Normal Response The Remote: prompt appears.

Related Commands SETDefault NetAccess
SHow NetAccess
ADD RemoteManager
DELete RemoteManager
SHow RemoteManager

RemoveDir

Syntax `RemoveDir [<device>:][<path>/]<subdirectory name>`

Minimum Privilege Level Network Manager

Description The RemoveDir command removes an empty subdirectory on the NETBuilder II and SuperStack II bridge/router from the local storage device when the configuration file source has been set to the local device. If a NETBuilder II is being booted remotely, the configuration file source has been set to boot device, and FTP has been selected as the remote file access protocol, then the RemoveDir command removes an empty subdirectory in the remote directory containing the configuration files.

Values <device> Specifies a local storage device. NETBuilder II bridge/routers use drives A and B. The flash memory on the SuperStack II NETBuilder and OfficeConnect NETBuilder bridge/routers is drive A.

If you do not specify a device, the system assumes the default drive and prompts you to continue.

<path> Removes an empty subdirectory that is not at the configuration file source level. For example, to remove the subdirectory "secondlevel" that is in subdirectory "firstlevel," specify "firstlevel/secondlevel."

When specifying the path option, you can specify metacharacters. @M indicates the 12 characters of a MAC address; @m indicates the last 6 characters of a MAC address.

You must specify the complete pathname of the subdirectory.

Normal Response A system displays a message that indicates the subdirectory was removed.

Related Commands DiskFiles
MakeDir
ReName

RemoveFile

Syntax

```
RemoveFile [<device>:][<path>/]<filename>
```

Minimum Privilege Level Network Manager

Description The RemoveFile command deletes files in a root or subdirectory on the local storage device when the configuration file source has been set to the local drive. If a NETBuilder II bridge/router is being booted remotely and the configuration file source has been set to boot device and FTP has been selected as the remote access protocol, then the RemoveFile command deletes a file in the remote subdirectory containing the configuration files.

Values

<device> Specifies a local storage device. NETBuilder II bridge/routers use drives A and B. The flash memory on the SuperStack II NETBuilder and OfficeConnect NETBuilder bridge/routers is drive A.

If you do not specify a device, the system assumes the default drive and prompts you to continue.

<path> Specifies the complete path of the file you want to delete.

<filename> Specifies the complete filename of the file you want to delete. The filename can contain metacharacters: @M indicates 12 characters of a MAC address, while @m indicates t he last 6 characters of a MAC address. Specify an asterisk (*) if you want to delete all configuration files. Specify *.* to remove all files with an extension, including the boot file.

ReName

Syntax

```
ReName [<device>:][<path>/]<old name> <new name>
```

Minimum Privilege Level Network Manager

Description The ReName command changes the name of a subdirectory or file on the bridge/router local storage device when the configuration file source has been set to the local device. If a NETBuilder II bridge/router is being booted remotely and the configuration file source has been set to boot device and FTP has been selected as the remote access protocol, then the ReName command changes the name of a subdirectory or file in the remote subdirectory containing the configuration files.

Values

<device> Specifies a local storage device. NETBuilder II bridge/routers use drives A and B. The flash memory on the SuperStack II NETBuilder and OfficeConnect NETBuilder bridge/routers is drive A.

If you do not specify a device, the system assumes the default drive and prompts you to continue.

<path> Specifies a subdirectory or file that is not at the configuration file source level. When specifying the path option, you can use metacharacters, that is, @M indicates the 12 characters of a MAC address; @m indicates the last 6 characters of a MAC address.

You must specify the old name of the subdirectory or file and the new name.

Normal Response A system prompt appears.

Related Commands DiskFiles

RESTart

Syntax

```
RESTart
```

Minimum Privilege Level Network Manager

Description The RESTart command reloads Internet firewall filters after you have made changes to the filters. When the filters are reinitialized, the system detects syntax errors and provides the line number, the offending keyword, and other applicable help information. If there is a syntax error in the filter file, none of the defined filters will take effect.

RESume

The RESume command is available only if you are connected as a PAD-attached terminal to IP Internet-attached Telnet, Rlogin, or OSI servers.

Syntax

```
RESume [<session number>]
```

Minimum Privilege Level User

Description The RESume command helps manage multiple sessions from PAD-attached terminals to IP Internet-attached Telnet, Rlogin, or OSI servers.

The RESume command is useful only if a connection exists on the local port by changing the local port from command mode to data transfer mode and resuming communications for the specified session. If you do not specify a session number, the current session or the session that was active most recently is resumed. To display the session list, enter:

```
SHow -TERM SESsions
```

Normal Response The session is resumed.

Related Commands

SWitch
FORMAT
BACkwards

RLOGin

The RLOGin command is available only if you are connected as a PAD-attached terminal to IP Internet-attached Telnet, Rlogin, or OSI servers.

Syntax

```
RLOGin <address | name> [,<address | name>] ... [-l <username>]
  [ECM]
```

Minimum Privilege Level User

Description The RLOGin command makes TCP connections when the bridge/router is functioning as an X.25 connection service gateway. When the RLOGin command is executed from the bridge/router's user interface, a connection from a PAD-attached terminal to an IP Internet-attached Rlogin server occurs.

The RLOGin command makes a TCP connection to the specified host using the Rlogin Protocol. The Rlogin Protocol is widely used between UNIX hosts because it transports more of the UNIX terminal environment (for example, sends the terminal type, number of columns, and number of rows) than does the Telnet Protocol. In addition, UNIX hosts can be configured not to require user entry of passwords with connections that originate from trusted hosts.

This implementation of Rlogin supports the Rlogin client only and supports passing of the terminal type, screen size, and username information to the destination. The client username (user name on the client side), server username (username to be used for login on the server side), terminal type, and baud rate is communicated to the Rlogin server during the connection setup. The number of rows and columns may also be communicated to the server, if the server requests this information.

The username used to log on during network login (local access control) is used as the value for the client username and server username. If access control is disabled, then an empty string is sent for these fields.

If the username is explicitly specified with the -l (the letter "l") option, then that username is used for the server username. If the -l option is not specified, then the client username and the Rlogin server username are the same.

Other parameter values affect the way the RLOGin command works. If the parameter -TCPAPPL RLogSendName is set to No, an empty string is sent as the client username. This usually means that you are prompted for a password to log on the remote host. The -TERM TERMType parameter communicates the terminal type to the server.

Example 1 This command initiates an Rlogin connection to a host called "unix1." The gateway port enters the data transfer mode after the connection is made.

```
RLOGin unix1
```

Example 2 This command initiates an Rlogin connection to a host with an IP address 129.213.1.2. The username "abc" is used for the remote logon. The port remains in command mode after the connection is made.

```
RLOGin 129.213.1.2 -L abc ECM
```

Example 3 This command attempts an Rlogin connection to a host with an IP address 129.213.1.2; if that connection fails, an Rlogin connection to a host named "unix1" is attempted. The username "abc" is used for the remote logon. The port remains in data transfer mode after the connection is made.

```
RLOGin 129.213.1.2, unix1 -L abc
```

Normal Response

If the ECM option is specified, the NETBuilder prompt appears. If no ECM option is specified, the gateway port enters the data transfer mode, and the prompt from the host to which you connected may appear.

Related Commands

DisConnect
SETDefault -TCPAPPL RLogSendName
SETDefault -TERM COLumns
SETDefault -TERM ROWs
SETDefault -TERM TERMType

RZ

This command is used by the NETBuilder II bridge/router with DPE only.

Syntax

```
RZ [Timeout=<timeout>]
```

Minimum Privilege Level

Network Manager

Description

The RZ command readies the bridge/router to receive a Zmodem file transfer from a PC over the CONSOLE port.

Configure the Serial Ports parameter in the SysconF command to the highest baud rate setting your communications program allows. Also change to the directory where you want the transferred files to appear by using the ChangeDir command.

Table 1-2 lists the supported applications.

Table 1-2 Supported ZMODEM Packages

Software	Versions
Windows95 HyperTerminal	1.0
ProComm Plus for Windows	2.00
ProComm Plus for Windows	1.02
ProComm Plus for DOS	2.01
CrossTalk for Windows	2.0, 3.0 (not 2.1)

Values

<timeout> Specifies the length of time in tenths of seconds before the connection times out waiting for a response from the PC. The timeout value can be between 10 and 1000. The bridge/router waits eight times the specified timeout value before timing out. The default is 100 tenths of seconds.

SAve

The SWitch command is available only if you are connected as a PAD-attached terminal to IP Internet-attached Telnet, Rlogin, or OSI servers.

Syntax

```
SAve [!<port>] DefaultParameters | PARAmeters <filename>
```

Minimum Privilege Level

Network Manager

Description

The SAve command writes the default or the active parameter values for a port configuration to the diskette on the gateway under the specified filename. If the port number is not specified, the port number you are connected to (the current port) is used. Valid port numbers are 0–127 on the NETBuilder II system.

While accessing the gateway remotely through the Telnet Protocol, the SAve command can only be used with a port number.

On a gateway that boots from its own diskette, verify that the diskette is in the disk drive before entering the command.

If the command line specifies DefaultParameters, the port's default configuration table is written to the file specified by filename. If the command line specifies PARAmeters, the port's active configuration table is written to the file specified by filename. The filename can be either alphanumeric or a number.

Values <filename> Alphanumeric:

A file with an alphanumeric name is considered an alternate configuration, not a default configuration. For example, you can save the active parameters for port 2 to a file named "xyz" on the disk. But the next time you boot the gateway, the file named "2" (if it exists), not "xyz," is copied to memory as the default configuration file for port 2. Upper- and lowercase letters in filenames are not distinguished.

Numeric:

The number can be any number from 0–127 on a NETBuilder II system. You can save the active or default port configuration to another number. For example, you can save port configuration file 2 to "04." If configuration file "04" exists, it is overwritten by the contents of port configuration file 2.

Figure 1-2 shows the operation of the SAve command.

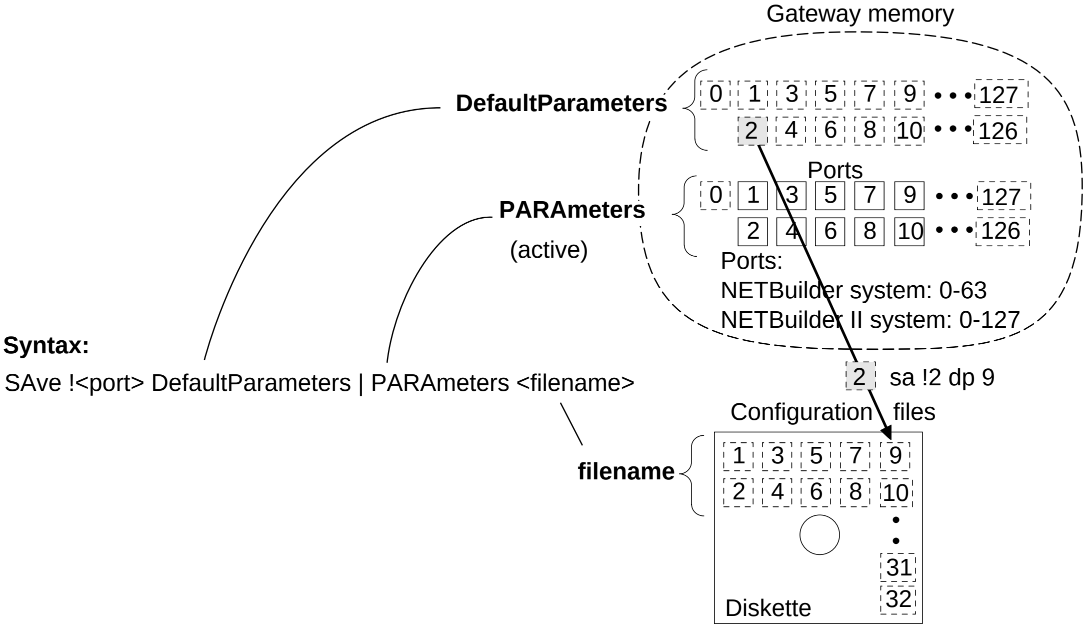


Figure 1-2 Effects of the SAve Command

To maintain consistency between the default parameter values in memory and on disk, use the ReaD command immediately after a SAve command. For example, after the SAve command is executed in Figure 1-2, file 9 on disk is different from file 9 in memory. To make them consistent, enter the following command to copy file 9 from disk to memory:

```
ReaD !9 9
```

Example 1

This command writes the active configuration file for the current session on the gateway port to the file “port4.conf” on the disk.

```
SAve PARAmeters port4.conf
```

Example 2

The first command in this example copies the default parameter file for configuration file 1 to the default parameter file for configuration file 5. The two SETDefault commands alter the current values of the BReakAction and ECMChar parameters. The last command new active parameter values on port 5 to filename 5 on diskette. Current and default configuration tables of configuration file 1 remain unchanged.

```
ReaD !5 1
SETDefault !5 -TERM BReakAction = inband
SETDefault !5 -TERM ECMChar = ^C
SAve !5 PARAmeters 5
```

Normal Response

The prompt appears.

Related Commands

ReaD
SETDefault

SAVEbgp

Syntax

```
SAVEbgp [All]
```

Minimum Privilege Level

Network Manager

Description

The SAVEbgp command forces an immediate save of Border Gateway Protocol (BGP) parameters. Unlike other services, the BGP Service does not automatically save settings to nonvolatile storage when a SETDefault, ADD, or DELete operation is performed. The settings usually are only saved to disk every ten operations.

Use the SAVEbgp command to save only the files that need saving, that is, the files that changed since the last save. To force a save of all BGP-related files to disk, enter:

```
SAVEbgp All
```

SecCheck

Syntax

```
SecCheck [!<port>]
```

Minimum Privilege Level

Network Manager

Description

The SecCheck command is a diagnostic tool that determines whether IP security option misconfigurations exist and generates warning messages about them. The SecCheck command does not check for all possible misconfigurations, but makes sure the values for SecLabelSys and SecLabelDefault are consistent with values for SecLEVel and SecAuthOut.

The SecCheck command ensures that your setup is consistent for the system, not whether the values or levels configured are what you intended. The SecCheck command does not check whether the configuration is consistent with other values over the network.

If this command is executed without a port number, all ports are checked. If this command is executed with a port number, only the IP security configurations for the specified port are checked.

For more information on configuring your system for IP security options, refer to Chapter 8 in *Using NETBuilder Family Software*.

Normal Response Warning messages are generated. If no messages are displayed, the security configuration is correct.

SET

Syntax

```
SET [!<port>] [-<service>] <param-name> = <value> ...
```

Minimum Privilege Level User or Network Manager, depending on parameter

Description The SET command function changes the value of a parameter in the system memory. The function of the command depends on the parameter on which it operates. The new value takes effect immediately, but the value is not stored on the disk. The next time you boot the bridge/router, the default value is used instead of the new value you assigned with SET.

For Environment parameters, the active value affects only the current session. The next time you log on, the active value is, in effect, the default. This allows users who are logged on to the system to have a different environment for interacting with the system.

Except for the -SYS DATE parameter, the minimum privilege level for setting these parameters is User.

Depending on the parameter, the SET command is sometimes used with !<path> instead of !<port>. For information on using parameters, refer to the appropriate parameter.

Normal Response A system prompt appears.

Related Commands SETDefault
SHow

SETDefault

Syntax *For non-ISDN interfaces*

```
SETDefault [!<port>] [!<path>] [-<service>] <param-name> =
 <value> ...
```

For ISDN interfaces

```
SETDefault [!<port>] [!<connectorID.channelID>] [-<service>]
 <param-name> = <value> ...
```

Minimum Privilege Level Network Manager

Description The SETDefault command changes the value of a parameter and stores it to the disk. The function of the command depends on the parameter on which it operates.

For most parameters, the new value takes effect immediately; some parameters take effect only after you reenable the port or path; some parameters take effect only after a reboot. In these cases, after you use SETDefault, a message appears stating that you must reboot the system for the change to take effect.

New values for the InterAction and ScreenLength parameters (refer to Chapter 2) take effect in the next Telnet session or after the next login to the console port.

Depending on the parameter, the SETDefault command is sometimes used with !<path> instead of !<port>. For information on using the system parameters, refer to the appropriate parameter.

Normal Response

If the new value takes effect immediately or after the next logon, a system prompt appears. If the new value takes effect after reboot, the following message appears:

```
Note: you must reboot for this parameter to take effect
```

Related Commands

SET
SHow
SHowDefault

SHow

Syntax

For non-ISDN interfaces

```
SHow [!<port> | !*] [-<service>] <param-name> ...
SHow [!<path> | !*] [-<service>] <param-name> ...
```

For ISDN interfaces

```
SHow [!<port> | !*] [-<service>] <param-name> ...
SHow [!<connectorID.channelID> | !<connectorID>.*] [-<service>]
  <param-name> ...
```

Minimum Privilege Level

User or Network Manager, depending on the parameter

Description

The SHow command displays one of the following types of information:

- The value of a configuration parameter in memory
- Information related to the system's current configuration or function (for example, statistics, routing table information, configuration information)

The actual display depends on the parameter it is used with. You can also use the SHow command with the GREP command to filter the output of the information you are displaying. For more information, refer to "GREP" on page 2-2.

The SHow -SYS STATistics command does not display all statistics when you are in remote mode through the REMote command.

For some parameters, no port number or path number should be entered. For many parameters, the port or path number can be used. For these parameters, you have three choices for displaying information:

- Information for a specific path or port

  To display this information, enter the SHow command followed by the specific port number.

  For example, to use this syntax to show the IP network address of port 4, enter:

  ```
  SHow !4 -IP NETaddr
  ```

- Information for all paths or ports

  To display this information, enter the SHow command followed by the !* wildcard syntax.

  For example, to use this syntax to show the IP network address of all ports, enter:

  ```
  SHow !* -IP NETaddr
  ```

- Information for a given parameter

  To display this information, enter the SHow command without using a specific path or port number, or wildcard syntax. In this case, the default display is shown.

  For example, to show the default display for the NETaddr parameter in the IP Service, enter:

  ```
  SHow -IP NETaddr
  ```

When you enter the SHow command for these parameters, but you do not specify path or port syntax, the path or port information displayed depends on the service and the system configuration. Table 1-3 shows the default display when you enter the SHow command with parameters in different services.

Table 1-3 Default Displays for SHow and SHowDefault Commands

Service	Default Paths/Ports Displayed
AppleTalk	Ports configured with the SETDefault -AT CONTrol = ROute command.
APPN	Ports defined as APPN ports using the SETDefault -APPN PortDef command (SHow only).
ARP	Ports that have a NET address assigned.
BCN	Ports physically present in the system.
BOOTPC	Ports configured with the SETDefault -BOOTPC CONTrol command.
BRidge	Ports physically present in the system when the port is enabled and transparent bridging or source routing is enabled for the port. Or it displays information for ports physically present when global bridging is enabled.
CLNP	Ports physically present in the system.
DECnet	Ports configured with SETDefault -DEC CONTrol = ROute command.
DVMRP	Ports physically present in the system.
ESIS	Ports physically present in the system.
FDDI	Paths where the FDDI card is physically present in the system.
FR	Ports physically present in the system when the port owner is set to FR.
Gateway	Ports physically present in the system.
IDP	Ports that have an XNS NETnumber assigned.
IP	Ports that have an IP NET address assigned.
IPX	Ports that have an IPX NETnumber assigned.
ISIS	Ports physically present in the system.
LAPB	Paths physically present in the system when LAPB is enabled.

(continued)

Table 1-3 Default Displays for SHow and SHowDefault Commands (continued)

Service	Default Paths/Ports Displayed
LLC2	Ports physically present in the system.
MIP	Ports physically present in the system.
NLSP	Ports configured with the SETDefault -NLSP CONTrol command.
NRIP	Ports configured with the SETDefault -NRIP CONTrol command.
OSPF	Ports that have an IP NET address assigned.
PATH	Paths physically present in the system.
PORT	Ports physically present in the system.
PPP	Ports physically present in the system when the port owner is set to PPP.
PROFile	All the configured profiles.
RIPIP	Ports that have an IP NET address assigned.
RIPXNS	Ports for which the -RIPXNS CONTrol parameter is enabled.
SAP	Ports configured with the SETDefault -SAP CONTrol command.
SMDS	Ports physically present in the system that are enabled and the port owner is set to SMDS.
SR	Ports with source route bridging or route discovery enabled.
STP	Ports physically present in the system when the port is enabled and transparent bridging or source routing is enabled for the port. Or it displays information for ports physically present when global bridging is enabled.
VIP	Ports configured with the SETDefault !<port> -VIP CONTrol = Route command.
XSWitch	Ports that have at least one X.25 address prefix assigned.
X25	Ports physically present in the system when the port owner is set to X25, and X.25 is enabled.

Table 1-4 shows variations of the SHow command syntax in some services. For some parameters, the SHow command syntax is different from the general syntax in Table 1-4. For information on the syntax, refer to the appropriate service parameter chapter.

Table 1-4 Variations in SHow Command Syntax

Service	Parameter	Syntax
SYS	MACros	`SHow MACros [<macro name>]`
SYS	NetMAP	`SHow [!<port>] NetMAP [Long] [xns | tcp]`
SYS	STATistics	`SHow STATistics [-<service>] [<option>]`
IP	AllRoutes	`SHow -IP AllRoutes [<IP address> | A | B | C | N | S | H | L | R | ST]`
IP	ADDRess	`SHow -IP ADDRess [<IP address>] [External | Internal | Broadcast | Local]`
OSPF	LinkStateData	`SHow [!<areaid>] -OSPF LinkStateData [Router | Network | Summary | External | Long | <LS id>]`

Related Commands

ADD
DELete
SET
SETDefault
SHowDefault

SHowDefault

Syntax

For non-ISDN interfaces

```
SHowDefault [!<port> | !*] [-<service>] <param-name> ...
SHowDefault [!<path> | !*] [-<service>] <param-name> ...
```

For ISDN interfaces

```
SHowDefault [!<port> | !*] [-<service>] <param-name> ...
SHowDefault [!<connectorID.channelID> | !<connectorID>.*]
 [-<service>] <param-name> ...
```

Minimum Privilege Level Network Manager

Description The SHowDefault command displays the value of a parameter that is stored on the disk. The actual display depends on the parameter. The following two types of parameters can be displayed:

- Parameters whose active and default values could be different. The ScreenLength parameter, which can be modified by both SET and SETDefault, is an example.
- The parameters that display system information on the disk, which can be different from the active information being used. For example, in the PATH Service, you can define the baud rate for a specified serial line path. The information about the command is not being used directly but is used for internal calculations. The information is stored on the disk and can be displayed by the SHowDefault -PATH BAud command.

For some parameters, no port number or path number should be entered. For others, the port number or path number is optional.

If the port or path number is entered, information relevant to the referenced port or path is displayed. If the wildcard character is entered, information relevant to all ports or paths is displayed. If no port or path syntax is entered, the system provides the default display. The default displays provided differ depending on the service. For more information on the default displays for specific services, refer to Table 1-3 in the description for the SHow command.

You can also use the SHow command with the GREP command to filter the output of the information you are displaying. For more information, refer to “GREP” on page 2-2.

The parameters used with the SHowDefault command are a subset of the parameters used with the SHow command.

Related Commands ADD
DELete
SETDefault
SHow

SpyRing

Syntax

```
SpyRing !<port> [Canonical | NonCanonical]
```

Default Canonical

Minimum Privilege Level Network Manager

Description The SpyRing command displays MAC addresses of stations attached to the local token ring interface.

Values Select one of the following values:

Canonical	The MAC address is displayed in canonical format.
NonCanonical	The MAC address is displayed in noncanonical format.

Related Commands MacAddrConvert

SWitch

The SWitch command is available only if you are connected as a PAD-attached terminal to IP Internet-attached Telnet, Rlogin, or OSI servers.

Syntax

```
SWitch [<session number>]
```

Minimum Privilege Level User

Description The SWitch command helps manage multiple sessions from PAD-attached terminals to IP Internet-attached Telnet, Rlogin, or OSI servers. You can use the SWitch command when the bridge/router functions as an X.25 connection service gateway for incoming extended connections.

The SWitch command suspends the current session and switches to the specified session on the port. A session is referred to by its session number. If you do not specify a session number, the most recently active session becomes active. The port remains in command mode until the RESume command is entered.

To display the sessions in the order of most recently used, with the current session at the top, enter:

```
SHow -TERM SESsions
```

The current session is the one acted on by the SET command or by RESume and DisConnect if no session is specified.

To prevent the SWitch command from being interpreted as a switch statement, abbreviate it as sw when used in a macro.

Normal Response A display similar to the following is generated:

```
Switched to session 1 with 192.10.100.50.
```

Related Commands

BACkwards
FORMAT
RESume
SET

SysconF

This section describes the main System Configuration menu displayed when entering the SysconF command. See Appendix A for a full description of each menu and submenu option.

Syntax

```
SysconF [<number>]
```

Minimum Privilege

“Root” user with Network Manager privilege

Description

The SysconF command displays a menu of configurable firmware parameters for the NETBuilder II system. Configuring these firmware parameters allows you to customize the operation of the bridge/router.

If you enter only SysconF, a menu of options is displayed. If you enter SysconF with the number of a menu option, only that specific menu item is displayed.

You cannot use the SysconF command when you access the bridge/router using the REMote command.

Except for the NETBuilder II with DPE module, you can also configure the firmware parameters by entering the MONitor command to use the firmware monitor utility.

The advantage of configuring the firmware through the bridge/router software using SysconF is that it can be done while the software is running. Using the MONitor command halts the bridge/router software.

Normal Response

A menu appears that allows you to configure the firmware parameters for your system. The following tables show the menus for each platform.

Table 1-5 NETBuilder II with DPE SysconF Main Menu

```
1. Serial Ports
2. Primary Boot Source
3. Secondary Boot Source
4. Test Boot Source
5. Boot Sources
6. Dump Destination
7. Recovery Procedure
8. MP Boot Source
9. Boot Statistics
```

Table 1-6 NETBuilder II with CEC SysconF Main Menu

```
1. Serial Ports
2. Self-Test
3. Start-Up Action
4. Primary Boot Source
5. Secondary Boot Source
6. Test Boot Source
7. Boot Sources
8. Dump Destination
9. Recovery Procedure
10. MP Boot Source
11. Boot Statistics
```

Table 1-7 SuperStack II NETBuilder and OfficeConnect NETBuilder SysconF Main Menu

```
1. Upgrade Menu
2. Console Port
3. Self-Test
4. Primary Boot Source
5. Secondary Boot Source
6. Test Boot Source
7. Boot Sources
8. Dump Destination
9. Boot Statistics
```

See Appendix A for a full description of each menu and submenu option.

Related Commands MONitor

SYSgen

The SYSgen command is only available for the NETBuilder II bridge/router with CEC.

Syntax `SYSgen [!<port>] [-<service>] <param-name> = <value> ...`

Minimum Privilege Level Network Manager

Description The SYSgen command changes the value of a parameter and stores the new value to disk. The new value takes effect immediately.

To show the results of the SYSgen command, enter:

`SHow -SYS SYSgen`

For more information, refer to "SHow" on page 1-54 and "SYSgen" on page 58-15.

Normal Response A system prompt appears.

SysInfo

Syntax `SysInfo [<number>]`

Minimum Privilege Level Network Manager

Description The SysInfo command shows CPU, firmware version, RAM size, drive information, and MAC addresses of the NETBuilder bridge/router.

For the NETBuilder II bridge/router with CEC module, the SysInfo command accesses the System Information menu. If you know which menu item you want to access, you can enter the number with the command to go straight to that menu item.

You cannot use the SysInfo command when you access the NETBuilder II bridge/router with the REMote command.

Normal Response The system information is displayed, or a menu appears that allows you to access the system information.

SysPassWord

Syntax `SysPassWord`

Minimum Privilege Level “Root” user with Network Manager privilege

Description The SysPassWord command brings up a menu that allows you to set or reset the Network Manager and User privilege password. The Network Manager password must be set before you set the User password and the User password must be cleared before you reset the Network Manager password. This menu also allows you to enable or disable SNMP control over the Network Manager and User privilege passwords.

SZ

This command is used by the NETBuilder II bridge/router with DPE only.

Syntax `SZ [Timeout=<timeout>] <filelist>`

Minimum Privilege Level Network Manager

Description The SZ command uses Zmodem file transfer to send specified files to a PC over the CONSOLE port.

Configure the Serial Ports parameter in the SysconF command to the highest baud rate setting your communications program allows. Also change to the files directory by using the ChangeDir command.

Table 1-8 lists the supported applications:

Table 1-8 Supported Zmodem Packages

Software	**Versions**
Windows95 HyperTerminal	1.0
ProComm Plus for Windows	2.00
ProComm Plus for Windows	1.02
ProComm Plus for DOS	2.01
CrossTalk for Windows	2.0, 3.0 (not 2.1)

Values

<timeout> Specifies the length of time in tenths of seconds before the connection times out waiting for a response from the PC. The timeout value can be between 10 and 1000. The default is 100 tenths of seconds.

<filelist> Specifies the files you want to send. Separate each filename with a space. Specify an asterisk (*) if you want to send all configuration files. Specify `*.*` to send all files with an extension, including the boot file.

TELnet

Syntax

```
TELnet <IP address> | <NSAP address>
```

Default No default

Minimum Privilege Level User

Description The TELnet command establishes a standard Telnet connection between the bridge/router and any IP or OSI NSAP address reachable from the bridge/router, with the following limitations:

- You cannot use Internet or OSI names as arguments to the TELnet command; only IP or OSI NSAP addresses are allowed.
- The TELnet command does not support multiple sessions. You must disconnect the session in progress before initiating a new session.
- The escape character ^[returns control to the command mode, at which time only two options are available: Disconnect or resume the current session.

While using a Telnet connection from the console port to another system, you will still receive console messages from the bridge/router from which the Telnet connection was established.

TEst

Syntax

```
TEst
```

Minimum Privilege Level Network Manager

Description The TEst command tests your IP firewall filters with test packets. Prompts similar to the following are displayed, depending on which protocol you specify:

```
Protocol [0]:
From [0.0.0.0]:
To [0.0.0.0]:
Direction [Out]:
Port [!1]:
```

The system then reports whether the packet was permitted or denied.

Values Protocol The following protocols are available:

- TCP
- UDP
- ICMP
- Any IP protocol number. Refer to RFC-1700 for a complete list of protocols and their assigned numbers. For instance, if you type 89, OSPF is specified.

TraceRoute

Syntax

```
TraceRoute <IP Address> [<tos> [SourceRoute]]
```

Minimum Privilege Level

Network Manager

Description

The TraceRoute command traces a path to a TCP/IP destination. It provides you with the IP address of each gateway used to forward packets to a particular destination. It also provides the round-trip time to each gateway along the path.

The TraceRoute command cannot be used in remote mode.

You must specify the IP address of the TCP/IP destination you want to trace.

Values

<tos> Specifies the type of service (TOS) to be used. Based on the type of links that interconnect the route, a metric can be assigned for each TOS value. Type of service values from 0 through 7 are supported, although only values 1, 2, and 4 are defined in RFC 791. Table 1-9 describes these TOS values. The default value is 0.

SourceRoute If you use the SourceRoute option, the software determines if Loose or Strict source route is desired. Loose source route allows intermediate nodes to forward to the next entry in the source address even if next entry is not directly connected to the node. For example, if the source route list is A, B, C, D, the route must traverse A, B, C, D, but other routes such as A, F, B, C, X, D are considered valid.

With Strict source route, the intermediate node drops the packet if the next entry is not directly connected to it. For example, if the source route list is A, B, C, D, then only A, B, C, D must be traversed.

Although the 3Com IP router supports other vendors' implementation of the TOS function, it does have its own implementation.

Table 1-9 TOS Values

TOS Value	Description
TOS 0*	Default
TOS 1	High reliable links
TOS 2	High throughput links
TOS 4	Low delay links

* For TOS 0 links, the software does not try to alter the reliability or throughput on this link.

Example

To obtain TraceRoute information for the path to a TCP/IP destination whose IP address is 192.65.73.133 using TOS 0, enter the following command:

```
TraceRoute 192.65.73.133 0Normal Response
```

A display similar to the following appears:

```
TraceRoute to 192.65.73.133 using TOS 0
TTL   Next Hop Address  RTTs
1     129.213.96.96      7 ms     5 ms     5 ms
2     129.213.112.102    9 ms     5 ms     5 ms
3     192.65.73.133      8 ms     6 ms     6 ms
```

Related Commands

PING

TRansmit

Syntax

```
TRansmit [-n] "<string>" | Break
```

Minimum Privilege Level User

Description The TRansmit command is used within a macro definition to instruct the gateway to transmit the specified "string" or break signal to the destination of the current session. If the -n option is specified, TRansmit does not append a new line to the "string" (by default, a new line is always appended). The bridge/router uses this command when it functions as an X.25 connection service gateway and accepts incoming connection requests from PAD-attached terminals to IP Internet-attached Telnet or Rlogin servers.

One TRansmit command can be used to send either a "string" or a break (the word Break is entered), but not both. The BReakAction parameter in "BReakAction" on page 61-5 describes the difference between an in-band and out-of-band break.

The string text must be entered according to the rules described in *New Installation for NETBuilder II Software*.

Example 1 This command transmits the login string "myusername" to the destination of the session that is current at the time the macro containing the command is executed. The -n option prevents a new line from being added to the string.

```
TRansmit -n "myusername"
```

Example 2 This command transmits a break signal to the device at the other end of the current session.

```
TRansmit Break
```

Normal Response Normal responses to the TRansmit command depend on the response of the LAN-attached device to the transmitted text. Locally, the prompt appears. Because TRansmit is given in command mode, you stay in command mode.

UnBindDSA

The LOGout command is available only with software packages that support OSI.

Syntax

```
UnBindDSA
```

Minimum Privilege Level Network Manager

Description The UnBindDSA command disconnects the Directory User Agent (DUA) of the bridge/router from the Directory System Agent (DSA). Use this command when the bridge/router functions as an X.25 connection service gateway for incoming connection requests from PAD-attached terminals to LAN-attached OSI hosts.

Related Commands DirectoryManage

UNDefine

Syntax

```
UNDefine <macro name>
```

Minimum Privilege Level Network Manager

Description The UNDefine command deletes a macro from the macro directory. This command does not distinguish between upper- and lowercase letters in macro names.

Normal Response A new prompt appears.

Related Commands
DEFine
DO
FLush MACros
SHow MACros

UNSave

The UNSave command is available only with software packages that support X.25.

Syntax

```
UNSave <filename>
```

Minimum Privilege Level

Network Manager

Description

The UNSave command deletes the specified port configuration file. If the gateway boots locally, the file is deleted from the gateway's own diskette. If the server boots from an TFTP server and obtains files from this boot source, the UNSave command deletes the specified file from the TFTP server disk.

Normal Response

A new prompt appears.

UserManage

Syntax

```
UserManage
```

Minimum Privilege Level

"Root" user with Network Manager privilege

Description

The UserManage command provides a simple, menu-driven program that creates, modifies, removes, lists, and prints user accounts. You can add a maximum of 128 users on the NETBuilder II system.

Menu Options

You can access the following User Manager Menu options:

New account — Provides the same function as the AddUser command. It allows you to create user accounts on the system. User accounts must be set up on the server before a user is granted access to the system, assuming the UserLogin parameter for the port being accessed in turned on.

Each account establishes the account name (initials, for example), full name, and password. The communication server prompts you for each of these parameters. When a password is entered at the password prompt, it is not echoed on the terminal screen as it is typed.

The account name, full name, and password consist of simple character strings. Each field has a maximum length: username, 14 characters; full name, 23 characters; password, 15 characters. Account names and passwords are case-sensitive.

Remove account — Provides the same function as the DELeteUser command. It allows you to delete a user account from the database. The system responds to this request by prompting for the account name to be removed.

Expire account password — Provides the same function as the EXPire command by forcing a particular account password to expire.

List all accounts — Displays a list of all user accounts on the database.

Print account — Prompts you for an account name and then displays the full name associated with that account and the last login time.

Related Commands

AddUser
DELeteUser
EXPire
PassWord

VPing

Syntax

```
VPing <server addr>(decimal) [timeout (1–300 seconds)]
```

Minimum Privilege Level User

Description The VPing command specifies whether a specified VINES server can operate without connecting to the server. The target device must be a VINES server or router since VINES Echo Request and Reply is implemented on the server side only. You must specify the server's serial number in decimal format. No subnet ID is required.

VPing sends an echo request packet to the target server and waits until either a response from the specified server is received, or the time-out value is exceeded. The default time-out value is 20 seconds. The maximum time-out value is 300 seconds. To interrupt the VPing command, press the Break key.

The target server must be running VINES 5.0 or greater, and NETBuilder software version 6.2 or greater.

Normal Response The following message appears if the target server responds within the specified time:

```
Pinging... 2901599 is alive
```

VTp

The VTp command is available only if you are connected as a PAD-attached terminal to an IP Internet-attached OSI server.

Syntax

```
VTp <address | name> [,<address | name>...] [<profile>] [ECM]
```

Minimum Privilege Level User

Description The VTp command establishes an OSI connection to a specified PSAP address or name when the bridge/router is functioning as an X.25 connection service gateway. When the VTp command is executed from the bridge/router user interface, a connection request from an X.25 PAD-attached terminal to LAN-attached OSI host occurs.

If a list of addresses or names is entered, the gateway tries one address or name after another in the given order until a connection is made.

Values

<address | name>	Designates the destination PSAP address or name. The second address or name ([,<address | name>]) listed on the command line, allows you to try more than one destination. If a name is used, it is resolved through the X.500 or file name service depending on the values set by the -OSIAPPL NameSourceOrder parameter. Two or more addresses or names can be specified.
<profile>	Specifies TELnet, X3, TRansparent, and Default as the four possible virtual terminal profile (VTP) options that can be selected for connections. The default is TELnet.
ECM	Causes the port to remain in command mode after the connection is made.

Example 1 This command connects to a device named “nb_englab” using the TRansparent profile. If the connection to “nb_englab” cannot be completed, a connection to “nb2_mkt” is attempted.

```
VTp nb_englab, nb2_mkt TRansparent
```

Example 2 This command connects to port 1 of a 3Com device with the OSI address /47/0004/0035110008000201f00801 using the X3 profile.

```
VTp /47/0004/0035110008000201f00801!1 X3
```

2 GLOBAL PARAMETERS

This chapter describes global parameters which determine the characteristics of the bridge/router and affect the way you interact with it. Global parameters do not belong to a service, and you do not include a service name with global commands. Table 2-1 lists the global parameters and commands.

Global parameters are not available using the menu-driven interface.

Table 2-1 Global Parameters and Commands

Parameters	Commands
CurrentPorts	SET, SHow
CurrentServices	SET, SHow
GREP	any command
History	SHow
InterAction	SET, SETDefault, SHow, SHowDefault
PRIvilege	SET, SHow
ScreenLength	SET, SETDefault, SHow, SHowDefault

CurrentPorts

Syntax

```
SET CurrentPorts = ALL | (<port> [,<port>])
SHow CurrentPorts
```

Default All

Description The CurrentPorts parameter specifies the port or ports to which the SHow and SHowDefault commands apply and affects the display of these commands.

Specify port numbers that are meaningful for your hardware platform. For example, you can specify 1–8B on the NETBuilder II bridge/router with Ethernet 2-Port 10BASE-FL module installed, 1–8C on the NETBuilder II bridge/router with high-speed serial (HSS) V.35 3-Port module installed, and 1–8F on the NETBuilder II bridge/router with Ethernet 6-Port module installed.

When you set the CurrentPorts parameter with a multiport module installed, individual connectors are distinct, and you must enter their letter designations individually. For example, if you specify port 1, the software assumes you mean port 1A, not all connectors on port 1.

Values

ALL	Displays information for all ports.
<port>	Specifies the port or ports for which you want to display information. Information for paths mapped to the specified ports is also displayed.

CurrentServices

Syntax

```
SET CurrentServices = ALL | (<service> [,<service>])
SHow CurrentServices
```

Default All

Description The CurrentServices parameter specifies the service or services to which subsequent commands apply. Setting CurrentServices makes a parameter unambiguous (service-specific) and simplifies command syntax. You can list information for a maximum of 24 services.

Values

ALL Displays parameters for all services. For example, if you want information about all parameters, regardless of service, set CurrentServices to All, then enter SHow ? (include a space before the question mark).

<service> Specifies the service or services.

Example 1 To set the current service to BRidge in order to configure the bridge/router bridging characteristics, enter:

```
SET CurrentServices = BRidge
```

Then, to add a route in the bridge routing table and then show the table, enter:

```
ADD !1 ROUte %02608CA4E004
SHow AllRoutes
```

If you did not set CurrentServices to the BRidge Service, you would need to include -BRidge in each of these commands. Otherwise, an error message appears, because the ROUte and AllRoutes parameters also exist in other services.

GREP

Syntax

```
<COMMAND> <command syntax> | GREP [-v] [-i] <grep pattern>
```

Minimum Privilege Level Network Manager

Description The GREP parameter searches the command output for specified text and displays only the matching text. The GREP parameter can be used with any UI command by typing the command, a pipe (|) GREP, and the grep pattern.

For example, if you want to see only the RAM information on your OfficeConnect NETBuilder bridge/router, enter:

```
SysInfo | GREP RAM
```

Only the following is displayed:

```
RAM size 8380412 bytes
```

You can use regular expressions in your grep pattern as described in Appendix K in *Using NETBuilder Family Software*.

Values

-v Displays all information that does not contain (inverted search) the specified <grep pattern>.

-i Ignores the case.

<grep pattern> Specifies the character string on which the search is being performed.

History

Syntax
```
SHow History
```

Default No default

Description The History parameter displays the nine most recently entered bridge/router commands and is useful for command substitution. For a full description of command substitution used with the History parameter, refer to *New Installation for NETBuilder II Software*.

InterAction

Syntax
```
SET InterAction = ([MacroEcho | NoMacroEcho], [MacroBreak |
   NoMacroBreak], [LOGin | NoLOGin])
SETDefault InterAction = ([MacroEcho | NoMacroEcho], [MacroBreak |
   NoMacroBreak], [LOGin | NoLOGin])
SHow InterAction
SHowDefault InterAction
```

Default NoMacroEcho, MacroBreak, LOGin

Description The InterAction parameter controls the interaction between you and the bridge/router. It can be set with either the SET or SETDefault command. Values assigned by the SET command take effect immediately. Values assigned by the SETDefault command take effect in the next session.

Values

MacroEcho | NoMacroEcho	Determines whether macros are echoed on the screen as they are executed.
MacroBreak | NoMacroBreak	Determines whether the Break key can be used to stop execution of a macro. In macros that temporarily raise the privilege level to Network Manager, setting NoMacroBreak prevents a user from breaking out of the macro and remaining in Network Manager privilege level.
LOGin | NoLOGin	Determines whether login is required when you try to access the bridge/router commands and parameters. It affects access through both the local port and Telnet. If LOGin is selected and a user logs in, the privilege level is based on the password the user enters (Network Manager privilege password or User privilege password). For further information, refer to “SysPassWord” on page 1-61. If NoLOGin is selected, the privilege level is automatically set to User.

PRIvilege

Syntax
```
SET PRIvilege = User | NetMgr
SHow PRIvilege
```

Default NetMgr

Description The PRIvilege parameter specifies the privilege level of the current session.

Values

User Permits you to display or modify the active values of some bridge/router parameters.

NetMgr Allows access to all bridge/router commands and parameters. You can display or modify both active and default values of all parameters. After you perform root login, your privilege level is NetMgr.

ScreenLength

Syntax

```
SET ScreenLength = None | <lines> (6–100)
SETDefault ScreenLength = None | <lines> (6–100)
SHow ScreenLength
SHowDefault ScreenLength
```

Default 24

Description The ScreenLength parameter controls the number of lines displayed by a command on each screen if the display generated by that command exceeds one screen. The value assigned by the SET command takes effect immediately. The value assigned by the SETDefault command takes effect in the next session.

Values

<lines> Indicates the number of lines, from 6 to 100, displayed by a command if the display generated by that command exceeds one screen.

None Specifies that the display scrolls until output from the command is completed.

Example The following command limits the screen display to six lines:

```
SET ScreenLength = 6
```

The following display is the first six lines of a typical help menu generated by the ? command when ScreenLength is set to 6:

```
----------------------Configuration Commands-------------------
ADD     [!<port>] [-<service>] <set-name> <set-member>
DELete  [!<port>] [-<service>] <set-name> <set-member>
FLush   [!<port>] [-<service>] <param-name>
MEnu    [!<service>] <param-name>
--<CR> to continue, Q to quit--
```

Press the Return key to display the next screen of information. To exit the display, press Q and then the Return key.

3

AC Service Parameters

This chapter describes the parameters in the AC Service. The AC Service parameters can limit access to the NETBuilder bridge/router to authorized users. The bridge/router uses these parameters when there is an access request from the console port or from an incoming Telnet request. Table 3-1 lists the AC Service parameters and commands.

Table 3-1 AC Service Parameters and Commands

Parameters	Commands
CONFiguration	SHow
CONTrol	SETDefault, SHow, SHowDefault
EXPirationTimer	SETDefault, SHow
LOGINs	SHow
RESolutionOrder	SETDefault, Show

CONFiguration

Syntax

```
SHow -AC CONFiguration
```

Default No default

Description The CONFiguration parameter displays all the active values of the AC non-port-specific parameters. LOGINs is not displayed because it is port-specific. To display this parameter, use individual SHow parameter commands.

CONTrol

Syntax

```
SETDefault -AC CONTrol = [Enable | Disable]
SHow -AC CONTrol
SHowDefault -AC CONTrol
```

Default Enable

Description The CONTrol parameter enables or disables local access control. This parameter control is only available in the CX package (gateway).

Values

Enable Enables local access control for X.25 PAD incoming connection requests. When local access control is enabled, you must first log in to a gateway port to access the network. When the port displays the NetLogin prompt, enter your username. The gateway then prompts for the password and checks the account name and the password against the user account information in the gateway database.

Disable Disables local access control. When CONtrol is disabled, there is no access control for PAD users. The user interface prompt is displayed for all incoming X.25 PAD users.

For more information, refer to *Using NETBuilder Family Software*.

EXPirationTimer

Syntax

```
SETDefault -AC EXPirationTimer = <days>(1–512)
SHow -AC EXPirationTimer
```

Default 90 days

Description The EXPirationTimer parameter specifies when the current password should expire. It is valid only when local access control is enabled.

LOGINs

Syntax

```
SHow [!<port>] -AC LOGINs
```

Default No default

Description The LOGINs parameter displays a list of users who are logged in to the NETBuilder bridge/router through a console port or Telnet connection. In the CX package, the LOGINs parameter also displays a list of users who are logged in to the specified active port on the gateway. Without the port number, the command shows the users on all the ports.

Valid port numbers on the NETBuilder II system are 0–127 (CX package).

RESolutionOrder

Syntax

```
SETDefault RESolutionOrder=[NONE|Local]
```

Default Local

Description The RESolutionOrder parameter allows the user to select a sequence of access control schemes for access authentications. If NONE is configured, the local access control is not executed, so only those users logging in as root will have access to the box. If Local is configured, the local access control is enabled and any user whose access request can be authenticated locally will have access to the NETBuilder bridge/router.

4

APPLETALK SERVICE PARAMETERS

This chapter describes the parameters in the AppleTalk Service. Table 4-1 lists the AppleTalk Service parameters and commands.

Table 4-1 AppleTalk Service Parameters and Commands

Parameters	Commands
AarpCache	FLush, SHow
AarpCouNT	SETDefault, SHow, SHowDefault
AarpTIMe	SETDefault, SHow, SHowDefault
ADDRess	ADD, DELete, SHow
AllRoutes	FLush, SHow
AMTagingTime	SETDefault, SHow, SHowDefault
CONFiguration	SHow, SHowDefault
CONTrol	SETDefault, SHow, SHowDefault
DefaultZone	SETDefault, SHow, SHowDefault
DIAGnostics	FLush, SHow
EntityFilter	ADD, DELete, SHow
EntityFilterNum	ADD, DELete, SHow
NAmes	SHow
NbpLookupTimer	SETDefault, SHow, SHowDefault
NetFilter	ADD, DELete, SHow
NetFilterType	SETDefault, SHow, SHowDefault
NetRange	SETDefault, SHow, SHowDefault
NetZoneMapping	SHow
PortZone	SETDefault, SHow, SHowDefault
RouteAgingTime	SETDefault, SHow, SHowDefault
RouterName	SETDefault, SHow, SHowDefault
RouteUpdateTime	SETDefault, SHow, SHowDefault
SMDSGroupAddr	SETDefault, SHow, SHowDefault
StartupNET	SETDefault, SHow, SHowDefault
StartupNODe	SETDefault, SHow, SHowDefault
X25PROFileid	SETDefault, SHow
X25ProtID	SETDefault, SHow, SHowDefault
ZONe	ADD, DELete, SHow, SHowDefault
ZoneAdvFilterNm	ADD, DELete, SHow, SHowDefault
ZoneNetMapping	SHow

AarpCache

Syntax

```
FLush [!<port>] -AppleTalk AarpCache
SHow [!<port> | !*] -AppleTalk AarpCache [Hex]
```

Default No default

Description The AarpCache parameter displays or flushes the contents of the AppleTalk Address Resolution Protocol (AARP) cache. The AARP cache maintains the mapping between AppleTalk node addresses, media addresses, and the port through which the nodes can be reached.

Statically configured AppleTalk node addresses and media addresses are not removed from the AARP cache by the FLush command. Cache entries that are not statically configured are aged out of the cache. The time-to-live (TTL) column in the AARP cache represents the number of seconds before aging out occurs. (You can change the TTL value using the -AppleTalk AMTagingTime parameter. For more information, refer to "AMTagingTime" on page 4-5.)

Values Hex Displays the AppleTalk node addresses in hexadecimal mode.

AarpCouNT

Syntax

```
SETDefault !<port> -AppleTalk AarpCouNT = <number> (1–255)
SHow [!<port> | !*] -AppleTalk AarpCouNT
SHowDefault [!<port> | !*] -AppleTalk AarpCouNT
```

Default 10 (5 if port is configured for Switched Multimegabit Data Service (SMDS))

Description The AarpCouNT parameter determines the maximum number of times the AARP retransmits an AARP request or AARP probe when it does not receive a response. This parameter takes effect immediately.

To avoid having a router on a large network acquire the same address as another node, you may need to increase the value of the AarpCouNT parameter from the default value. Increasing the value of the AarpCount parameter increases the chances of delivering packets to other nodes on busy networks if their entries have been aged out of the AARP cache.

AarpTIMe

Syntax

```
SETDefault !<port> -AppleTalk AarpTIMe = <number> (1–10)
SHow [!<port> | !*] -AppleTalk AarpTIMe
SHowDefault [!<port> | !*] -AppleTalk AarpTIMe
```

Default 1 (5 if port is configured for SMDS)

Description The AarpTIMe parameter specifies (in units of 200 milliseconds) the time interval that AARP waits for a response to an AARP request or AARP probe before retransmitting the request or probe packet. This parameter takes effect immediately.

ADDRess

Syntax

```
ADD -AppleTalk ADDRess (<appletalk-node-address> | !<port>)
  <media-address>
DELete -AppleTalk ADDRess All | ((<appletalk-node-address> |
  !<port>) <media-address>)
SHow -AppleTalk ADDRess [Hex]
```

Default No default

Description The ADDRess parameter statically maps media addresses to ports or AppleTalk node addresses. This parameter is used to establish media addresses for out ports of the router connected to non-AppleTalk links or AppleTalk node address to media address pairings for media over which the AARP is not used, such as X.25 or Frame Relay. For detailed information regarding routing AppleTalk over X.25 and Frame Relay interfaces, refer to Chapter 14 in the *Using NETBuilder Family Software*.

You can configure as many address mappings for each bridge/router as desired.

No limit exists to the number of address mappings that you can configure for each bridge/router. However, large numbers of configured neighbor entries on X.25, SMDS, and Frame Relay ports in combination with large AppleTalk Internet topologies and slow WAN links can result in configurations that exceed the processing or memory capability of the bridge/router.

On an active Frame Relay, X.25, or SMDS port, additions and deletions of configured neighboring routers are dynamic. As a result, you do not need to re-enable AppleTalk routing for the changes to take effect. Refer to “CONTrol” on page 4-6.

You can configure different media type addresses for the same port or corresponding to the same node address. The entries for the type of media that is currently configured for the port are used and others are ignored.

Values

<appletalk-node-address> The form of an AppleTalk node address is <network-number>.<node-id> (for example, 20.198). The network number must be in the network range defined for an AppleTalk network out one of the ports. The valid network range is 1–65,279. The valid node ID range is 1–253. A node ID value must be unique across all nodes on a network using the same network number.

<media-address> Specifies an X.25 DTE address, a Frame Relay data link connection identifier (DLCI), an SMDS address, or a MAC address. For information on addressing conventions, refer to *Using NETBuilder Family Software.*

All Removes all current entries that are visible when using the SHow -AppleTalk ADDRess command from a static routing table.

Hex Displays the AppleTalk node addresses in hexadecimal mode.

Example 1 To add and specify mapping between an AppleTalk node address (4.23) and corresponding X.25 data terminal ready (DTE) address (#311040800245), enter:

```
ADD -AppleTalk ADDRess 4.23 #311040800245
```

Example 2 To add and specify mapping between an AppleTalk node address (3.25) and corresponding Frame Relay DLCI (@920), enter:

```
ADD -AppleTalk ADDRess 3.25 @920
```

or

```
ADD -AppleTalk ADDRess 3.25 DLCI 920
```

Example 3 To remove an X.25 DTE address (#311040800245) previously specified as reachable through port 3, enter:

```
DELete -AppleTalk ADDRess !3 #311040800245
```

Example 4 To display the current contents of the address mapping table, enter:

```
SHow -AppleTalk ADDRess
```

The following is a sample display:

```
Port Node-Address  Media-Address
-    4.56          08000201915B (Appletalk Static)
-    15.30         #311040800245 (AppleTalk Static)
-    17.30         #311040800246 (Appletalk Static)
4    -             @920 (Non-Appletalk Static)
```

If an AppleTalk static entry is in use, the Port column contains a port label instead of a hyphen.

AllRoutes

Syntax

```
FLush [!<port>] -AppleTalk AllRoutes
SHow [!<port> | !*] -AppleTalk AllRoutes [Hex] [<network range>]
```

Default No default

Description The AllRoutes parameter discards all current entries from the routing table, except the entries for directly connected AppleTalk networks. The router rebuilds the routing table based on new routing information obtained from other routers. If a port number is specified, then only routes that are associated with the specified port number are discarded. If no port number is specified, then all routes for all ports are purged. This parameter also displays the current contents of the AppleTalk Routing Table.

To reestablish new AppleTalk network information for the directly connected network, you need to disable AppleTalk routing on all AppleTalk routers connected to the network, to change seed information, and then to enable all routers again. For more information, refer to “CONTrol” on page 4-6.

Values

Hex	Displays the AppleTalk node addresses and network numbers in hexadecimal representation instead of decimal.
<network range>	Specifying a range limits the display to only those networks that have network ranges that overlap with the given network range. The specified network range must use valid network numbers in the range 1–65,279. Not specifying a range is equivalent to specifying a range of 1–65,279.

The following paragraphs describe the elements in the AppleTalk Routing Table:

Type	Indicates extended or nonextended network. Nonextended network types are usually LocalTalk networks.
Status	Indicates freshness of routing information. When the router receives new or fresh route information, the status is updated to Good. Every time the RouteAging Timer expires, the status drops one level, from Good to Suspect, then to Bad (1) and finally to Bad (2). If a route has a status of Bad (2) when the aging timer expires, it is removed from the routing table, (refer to "RouteAgingTime"on page 4-17.)
Hops	Indicates the number of Internet AppleTalk routers the port must pass through to reach the network.
Port	Indicates the port out of which packets must be sent to reach the network.
Next Hop /MediaAddress	Supplies the AppleTalk and data link addresses of the next router in the route to the network. Addresses in parentheses indicate the local router port address for the directly connected network. A next router node address will not be present if it is on a non-AppleTalk network. For Point-to-Point (PPP) ports, "PPP" appears instead of the data link address. For Frame Relay, directly connected networks will have "Frame Relay" because there is no local Frame Relay address.

AMTagingTime

Syntax

```
SETDefault !<port> -AppleTalk AMTagingTime = <seconds> (1–65535)
SHow [!<port> | !*] -AppleTalk AMTagingTime
SHowDefault [!<port> !*] -AppleTalk AMTagingTime
```

Default 1800 seconds (30 minutes)

Description The AMTagingTime parameter specifies the time interval (in seconds) that is used to evaluate the validity of entries in the AARP cache. An entry is deleted from the table when this time interval elapses without receiving any information that would cause the entry to be updated or confirmed. This parameter takes effect immediately.

The AARP cache contains mappings between AppleTalk node addresses and data link addresses on directly connected AppleTalk networks. Generally, the cache contains entries for non-router AppleTalk nodes to which the AppleTalk router has most recently sent packets. There is a separate table of data link addresses of other AppleTalk routers maintained in the routing database.

With the -AppleTalk CONTrol parameter set to NoAarpLearn (the default), mappings only stay in the cache for the number of seconds specified by the AMTagingTime parameter. After the specified time, an entry for a node is added only when a packet must be delivered to that node address.

With the -AppleTalk CONTrol parameter set to AarpLearn, mappings are added to the cache for the sender of every DDP packet received, so AARP cache entries remain as long as packets arrive from a node.

The AARP cache is limited to 1,000 node-to-address mappings.

If the AARP cache is full, new entries are not added until one or more of the existing entries are aged out. If the AMTagingTime is set too high, there may be periods where the benefits of the AARP cache are not available in the delivery of packets to some non-router nodes. This means that during some periods, every packet destined for a non-router node generates one or more AARP request packets to determine the data link address to use as the destination address in the MAC header. If more packets arrive at the router for that node before the AARP request is responded to, they may be dropped.

By keeping the AMTagingTime low, use of the cache is spread more evenly over a larger set of non-router node addresses. However, a value that is too low may generate excessive AARP requests. This can be an important consideration when the total number of non-router AppleTalk devices in use at any one time on all the directly connected AppleTalk networks is greater than 1,000.

When large streams of data are moving toward a particular end node, if you need to perform an AARP request for a significant number of packets, you may need to do numerous retries at the transport protocol level using AppleTalk Transaction Protocol (ATP) or AppleTalk Data Stream Protocol (ADSP).

If the total number of non-router AppleTalk devices in use at any one time on all the directly connected AppleTalk networks is less than or equal to 1,000, there is no advantage to setting a low value for AMTagingTime. Setting a high value reduces the occurrences of AARP requests to almost none, resulting in improved performance.

CONFiguration

Syntax

```
SHow [!<port> | !*]-AppleTalk CONFiguration
SHowDefault [!<port> | !*] -AppleTalk CONFiguration
```

Default No default

Description The CONFiguration parameter displays the current AppleTalk configuration parameter values. The SHow command displays the current applicable values of the parameters. The SHowDefault command displays the default values. Some of the default values may be different from the current applicable values, and take effect the next time AppleTalk routing is enabled on this router or if the router is rebooted.

CONTrol

Syntax

```
SETDefault !<port> -AppleTalk CONTrol = ([ROute | NoROute],
  [AppleTalk | NoAppleTalk], [SeedCheck | NoSeedCheck],
  [SeedingAllowed | NoSeedingAllowed], [EntityFilter |
  NoEntityFilter], [NetFilter | NoNetFilter], [ArpLearn |
  NoArpLearn], [Checksum | NoChecksum], [ZoneAdvFilter |
  NoZoneAdvFilter])
SHow [!<port> | !*] -AppleTalk CONTrol
ShowDefault [!<port> | !*] -AppleTalk CONTrol
```

Default NoROute, AppleTalk, SeedCheck, SeedingAllowed, NoEntityFilter, NoNetFilter, NoAarpLearn, NoChecksum, NoZoneAdvFilter

Description The CONTrol parameter determines how the AppleTalk router operates.

Some of the following values take effect only after AppleTalk routing is re-enabled. To re-enable AppleTalk routing, you must set the value of the -AppleTalk CONTrol parameter to NoROute and then reset the value of this parameter to ROute.

Values

ROute | NoROute
Determines whether or not the AppleTalk routing capability is enabled. The ROute option starts the AppleTalk port startup. If successful, the router can route through that port. The NoROute option disables routing on a port, flushing all routes that were reachable through that port from the routing table. This option takes effect immediately. For more information, refer to Chapter 14 in the *Using NETBuilder Family Software*.

AppleTalk | NoAppleTalk
Determines whether an attached network, a Point-to-Point Protocol/Phone Line Gateway (PPP/PLG) link, or a set of configured public data network (PDN) X.25, or Frame Relay addresses out of the specified port is treated as an AppleTalk network. SMDS can be treated as either an AppleTalk network or a NoAppleTalk network. A router can be attached to a non-AppleTalk backbone network with no AppleTalk end systems, but only AppleTalk routers. This option takes effect only after AppleTalk routing is re-enabled.

SeedCheck | NoSeedCheck
The default value SeedCheck means that the port does not become active if differences exist between the locally configured seed information and information obtained from other routers residing on the network connected to that port. Information on seeding conflicts is available using the SHow -AppleTalk DIAGnostics command. A value of NoSeedCheck enables a router to use its locally configured seed information regardless of detected conflicting information. SeedCheck is ignored if the -AppleTalk CONTrol value NoSeedingAllowed is in effect, of if seeding information is incompletely configured.

SeedingAllowed | NoSeedingAllowed
If SeedingAllowed and ROute are selected and seed information is configured, the router acts as a primary source of information for network number range, default zone, and zone list information for a directly connected network. Use NoSeedingAllowed to disable the use of seeding information that was configured when routing was enabled. This option takes effect only after AppleTalk routing is re-enabled.

EntityFilter | NoEntityFilter
Determines whether Network Entity filtering is performed. NoEntityFilter prevents the use of configured EntityFilter information for a port. This option takes effect immediately. (Refer to “EntityFilter”on page 4-12.)

NetFilter | NoNetFilter
Determines whether filtering of packets based on the destination or source network number occurs. NoNetFilter prevents use of configured NETFilter information for a port. This option takes effect immediately. (Refer to “NetFilter”on page 4-14.)

AarpLearn | NoAarpLearn
Determines whether or not the router is in AARP learning mode. This option is only meaningful on interface types where the AARP is defined as Ethernet, token ring, Fiber Distributed Data Interface (FDDI), or SMDS. In learning mode, AARP intercepts and gleans address resolution information from all incoming packets. In nonlearning mode, AARP only receives those packets destined to the router. It also negatively affects performance because all incoming packets are inspected. AarpLearn takes effect immediately and tends to use more shared memory for cache entries.

Checksum | NoChecksum
If Checksum is selected, a Datagram Delivery Protocol (DDP) checksum is generated for all outgoing packets. This option only controls checksum generation for packets sourced from the router; it does not affect the verification of checksums in incoming DDP packets. If NoChecksum is selected, a checksum is not generated for DDP outgoing packets. This option takes effect immediately.

ZoneAdvFilter | NoZoneAdvFilter
Use the configured zone advertisement filter to filter zones returned in the ZIP ZoneList request. If NoZoneAdvFilter is selected, all zones are returned in the zone list in response to a ZIP ZoneList request.

DefaultZone

Syntax

```
SETDefault !<port> -AppleTalk DefaultZone = "<zone-string>" (1–32
  char)
SHow [!<port> | !*] -AppleTalk DefaultZone
SHowDefault [!<port> | !*] -AppleTalk DefaultZone
```

Default " " (null string)

Description The DefaultZone parameter designates a default zone name that can be used for nodes on an AppleTalk network attached to the specified router port. This must be done if the router is being configured to seed the network attached to the specific port.

You can also use this parameter to add a zone and indicate that it is the default in one step.

This parameter takes effect the next time AppleTalk is re-enabled on the specified port and the router determines it is a seed router for the directly connected network. If full seed information is not configured, the configured default zone is not used.

Values "<zone-string>"
Special characters in the Macintosh character set can be specified using escape sequences. The backslash (\) character is used for escape sequences and must be followed by two hexadecimal digits that represent the character code. To insert a backslash in the string, use two backslashes (\\). This value is not case-sensitive and can be 1 to 32 characters in length. Refer to the table for the Macintosh extended character set in Chapter 7 in the *Using NETBuilder Family Software*.

DIAGnostics

Syntax

```
FLush [!<port>] -AppleTalk DIAGnostics
SHow [!<port> | !*] -AppleTalk DIAGnostics
```

Default No default

Description The DIAGnostics parameter displays messages for a number of conditions, including faulty configuration of the local AppleTalk router or external AppleTalk devices as well as informational messages.

For example, if the port is configured with the SETDefault !<port> -AppleTalk CONTrol = NoROute syntax, the “AppleTalk is configured NOROUTE” message appears. If nothing unusual is detected on an actively routing AppleTalk port, the only message displayed on your screen is one indicating that AppleTalk Phase 2 routing is enabled; otherwise, information describing some specific condition is displayed. In many cases, if the condition is related to information from another device, the data link address of the last device to cause the condition is displayed.

The types of information displayed include the following:

- Various reasons that AppleTalk may not be routing over the port including seed router information conflicts, waiting for a seed router to provide seed information, and port interface down
- Notification of incomplete configuration of seed information
- Invalid data in Routing Table Maintenance Protocol (RTMP) routing information packets
- Seed information conflicts with other routers at startup and during operation
- Network range conflicts with existing routing table entries
- Most recent network aged out of routing table (not necessarily an error condition)
- Counts of insufficient memory (zone and routing table entries) and buffers (for output of routing and zone information)
- Shortage of buffers, which may occur during peak load conditions (software is self-adjusting)
- Insufficient memory due to an overloaded system or a combination of too many protocols or routes

For more information on the use of diagnostics, refer to Chapter 14 in the *Using NETBuilder Family Software*.

EntityFilter

Syntax

```
ADD -AppleTalk EntityFilter <number> <entity name> [<network
  range>]
DELete -AppleTalk EntityFilter <number>
SHow -AppleTalk EntityFilter
```

Default No default

Description The EntityFilter parameter defines or removes an entity filter specification. Entity filtering restricts access to named resources on a network. AppleTalk Services on the network are accessed by using their entity names. Entity filtering uses these names as the primary criterion for filtering.

Special wildcard characters are permitted in all fields of the entity filter specification. An equals sign (=) by itself in a field signifies that all possible values match. A tilde (~) indicates zero or more characters of any value match.

Multiple *negative* entity filters are not useful. A packet is dropped if any one negative filter specification is met. For example, the following two filter patterns, if specified with the negative attribute, filter all NBP requests: =:=@zone1 and =:=@zone2. What is not filtered by one is filtered by the other.

Entity filtering has a limitation that results from the method of returning entity names in Name Binding Protocol (NBP) replies. The limitation is caused by using the asterisk (*) in the zone field on NBP replies. For NBP replies from a multizone network, the zone field cannot be determined because there is no way to determine the zone of the replying entity. This makes it impossible to apply the entity filtering.

The bridge/router attempts to prevent the received NBP requests and replies from continuing. A filter with an "=" zone field (object:type@=) works on filtering replies because an NBP reply always has fully specified object and type fields. In this case, an NBP request =:type@zone generated from a Macintosh computer gets through this filter, but the NBP reply is filtered.

Any positive filter with a fully specified zone field and wild object and type fields (=:=@ZoneA) is filtered upon receipt of the request, because the filter is applied at the zone level, and all NBP requests will have a fully specified zone field.

Any filter with a fully specified zone field and object or type fields with no wildcard characters has the potential of leaking back an NBP reply. For example, a filter of "=:type@ZoneA" can filter requests with matching type field and zone field. A request of "=:=@ZoneA" can get past the filter because "=:type@ZoneA" is filtering a specified type, which does not match the wild "=" type in the request. If the network from which the reply is received has multiple zones, the reply may be of the specified type from ZoneA; but since the reply may have a "*" zone field, the zone cannot be determined. Only if there is just one zone associated with the network can an "*" be taken as ZoneA, making the filter effective.

In Figure 4-1, an endnode "E" sending an NBP Broadcast Request of "=:=@ZoneA" for ZoneA results in the following combinations of entity filters applied to port B.

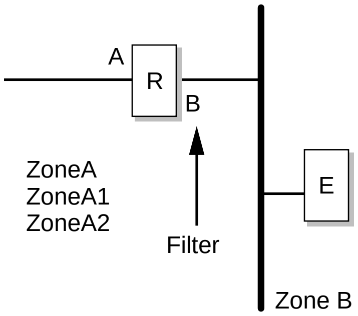


Figure 4-1 Application of Entity Filters

- Filter 1: "=:=@ZoneA"

  "=:=@ZoneA" NBP requests are filtered.

- Filter 2: “object:type@ZoneA”

  The “=:=@ZoneA” NBP request are not filtered. The specific “object” and “type” do not match. The reply from ZoneA/ZoneA1/ZoneA2 is routed back to endnode “E” even if the reply matches the filter specification because the “*” in the zone field of the reply cannot be resolved to a specific zone. The filter is effective only if port A has a single zone.

- Filter 3: “~object~:~type~@ZoneA”

  The wildcards “~” in the object or type field have the same result as Filter 2.

- Filter 4: “=:~type~@ZoneA”

  Same as Filter 2.

- Filter 5: “~object~:=@ZoneA”

  Same as Filter 2.

- Filter 6: “object:type@=”

  The “=:=@ZoneA” request goes through, but the reply is filtered because the zone is not relevant due to the wildcard in the filter. The reply will have a fully specified object and type.

- Filter 7: “~object~:~type~@=”

  Same as Filter 6.

- Filter 8: “~object~:=@=”z

  Same as Filter 6.

- Filter 9 : “=:~type~@=”z

  Same as Filter 6.

A filter number can be any value between 1 and 32 inclusive. The number represents a slot in an EntityFilter table displayed by the SHow command.

Values

<entity name> An entity name is a character string consisting of three fields: object, type, and zone in that order with a colon (:) and an at sign (@) separating the fields; for example, “Printer 002:LaserWriter@Mkt.” Each field is a string of a maximum of 32 characters. Entity names are not case-sensitive.

<network range> The filtering criteria can be further qualified by specifying a network number range. This requires that an entity name not only belong to a filtered set, but also that the node associated with the entity name be on a network that is included in the specified network number range.

Specifying an entity filter involves the following processes:

- Configuring the filtering criteria and associating it with a filter number by specifying the entity name and, optionally, a network number range qualifier.
- Associating the filtering criteria with a port along with a positive or negative filter type attribute.

Filtering may adversely affect the expected performance of the router.

Example 1 In the following example of entity filtering, assume that bridge/router A has three interfaces:

- Interface 1 is connected to a network that contains two pools of resources in the separate zones MARKETING and FINANCE. These resources could include a collection of printers, file servers, and communications servers.
- Interfaces 2 and 3 are connected to two network segments that contain users that access the resources in zones MARKETING and FINANCE.

  The requirement is to partition the pool of resources in such a way that all users on the segment attached to interface 2 can only access resources in zone MARKETING, and all users on the segment attached to interface 3 can only access resources in zone FINANCE.

  In addition, the FINANCE zone is associated with multiple network ranges, but users on the segment attached to interface 2 should only be restricted from accessing resources on the network range 10–20 in the zone FINANCE.

  Apply the entity filters at interfaces 2 and 3. At interface 2, the filtered set are all entities from a network range of 10–20 in zone FINANCE. At interface 3, the filtered set are all entities in zone MARKETING. Configuring the filters requires the following:

- Filter specification associated with filter number 1 (“=:=@MARKETING”)
- Filter specification associated with filter number 2 (“=:=@FINANCE” range of 10–20
- Filter number 1 added to interface 3 with the POSITIVE filter type attribute
- Filter number 2 added to interface 2 with the POSITIVE filter type attribute

To configure the filters as shown above, enter:

```
ADD -AppleTalk EntityFilter 1 “=:=@MARKETING”
ADD -AppleTalk EntityFilter 2 “=:=@FINANCE” 10-20
ADD !3 -AppleTalk EntityFilterNum 1 Positive
ADD !2 -AppleTalk EntityFilterNum 2 Positive
```

Refer also to “EntityFilterNum” on page 4-12 and Chapter 14 in *Using NETBuilder Family Software*.

EntityFilterNum

Syntax

```
ADD !<port> -AppleTalk EntityFilterNum <number> [Positive
  |Negative] [ClientIN |ClientOut | ClientBoth]
DELete !<port> -AppleTalk EntityFilterNum <number>
SHow [!<port> | !*] -AppleTalk EntityFilterNum
```

Default Positive, Client Both

Description The EntityFilterNum parameter associates an entity filter specification with a port through the filter number entered using the EntityFilter parameter, and specifies whether the filter specification should be interpreted as a positive or a negative filter. The ADD command takes effect immediately if the EntityFilter option is currently set using the SETDefault !<port> -AppleTalk CONTrol syntax.

Values Positive Indicates that the entity filter names that match the entity filter specification for the port are to be filtered.

Negative Indicates that the entity filter names that do not match the entity filter specification for the port are to be filtered.

ClientIn Indicates NBP Requests entering the !<port> are filtered.
Indicates NBP Replies exiting the !<port> are filtered.

ClientOut Indicates NBP Requests exiting the !<port> are filtered.
NBP Replies entering the !<port> are filtered.

ClientBoth Indicates NBP Requests entering/exiting the !<port> are filtered.
Indicates NBP Replies entering/exiting the !<port> are filtered.

NAmes

Syntax `SHow [!<port> | !*] -AppleTalk NAmes [Hex]`

Default No default

Description The NAmes parameter displays the contents of the NBP Name Table maintained by the router. This table contains the AppleTalk entity names and the corresponding AppleTalk Internet socket address of all network entities registered on this router. These names are accessible from another 3Com router using the ANameLookup command, which provides a method to verify connectivity.

Name entries must be checked for previous existence in a zone before being claimed by a node. The entries can be registered, or in a state of preregistration (waiting lookup, waiting lookup confirm, and waiting registration).

Values Hex Displays the AppleTalk node addresses in hexadecimal mode.

Example Use the SHow command to display the contents of the Name Table maintained by the router:

```
--------------------------------NameTable------------------------------------
Port   DDP Address  StatusEntity Name
1      10.20.2      Registered        “080002019155-1:3ComRouter@B300 MKT”
1      10.20.2      Registered        “ROUTER-100:3ComRouter@B300 MKT”
2      20.33.2      Registered        “08000201915APLTLK-2:3ComRouter@B300 FIN
1      10.20.2      Registered        “ROUTER-100:3ComRouter@B300 MKT”
```

The first and third name table entries show the default name format automatically registered by the AppleTalk router for all active ports connected to AppleTalk networks. The router port names are always registered on the AppleTalk Echo Protocol (AEP) socket number 2. The Entity name is the media address followed by a hyphen and then the port number. The type is always 3ComRouter and the zone is the active PortZone.

The second name table entry is an example of adding an alias (a different name for the same AppleTalk Internet socket address) for a router port using the RouterName parameter.

NbpLookupTimer

Syntax

```
SETDefault -AppleTalk NbpLookupTimer = <seconds> (1–300)
SHow -AppleTalk NbpLookupTimer
SHowDefault -AppleTalk NbpLookupTimer
```

Default 10

Description The NbpLookupTimer parameter specifies the maximum length of time the router waits for confirmation of NBP name lookups. This time-out value is used in both the ANameLookup and APING commands to locate named entities.

The AppleTalk NBP supports a distributed name database that provides the conversion of entity names to numeric addresses. Name binding provides a way of translating names that do not change as often to addresses that have the potential of changing each time the host machine is rebooted.

A longer time-out value increases the success rate in locating an entity name on a large AppleTalk Internet for ANameLookup and APING. It also increases the wait for returning results.

NetFilter

Syntax

```
ADD !<port> -AppleTalk NetFilter <network-range>
DELete !<port> -AppleTalk NetFilter {ALL | <network-range>}
SHow [!<port> | !*] -AppleTalk NetFilter
```

Default No default

Description The NetFilter parameter adds or deletes network ranges that are used to filter packets originating from or destined for networks. Network filtering for a port does not affect the router's interactions with devices on the net directly connected to the port if that network is in the filtered network set.

When adding network ranges to the filter, consolidation of filter ranges may occur depending upon the current entries and the entries added. For example, if the ranges 1 through 4 and 8 through 10 already have been added, and a new range, 5 through 7, is added, the three ranges collapse into a single entry with the range 1 through 10.

When deleting ranges, the ranges must be fully contained in an existing range. Subrange deletions are permitted. Extending the example above, if you request that the range 6 through 7 be deleted, then two entries are created, one for range 1 through 5 and the other for range 8 through 10. The NetFilterType parameter allows positive and negative filtering on a per-port basis.

A maximum of 64 entries can be added to the NetFilter table for a port. All additions and deletions take effect immediately if the NetFilter option of the -AppleTalk CONTrol parameter is in effect.

Filtering may adversely affect the expected performance of the router.

Values

<network-range> A range of AppleTalk network numbers assigned to a network. Valid network ranges are subsets of 1–65,279.

ALL Used with the DELete command to delete all network ranges.

Example 1 To add a filter at port 1 to filter out packets originating from or destined to networks in the range of 1–4, enter:

```
ADD !1 -AppleTalk NetFilter 1-4
```

Example 2 To add a filter at port 2 to filter out packets originating from or destined to networks not in the range of 10 –20, enter:

```
DELete !2 -AppleTalk NetFilter ALL
ADD !2 -AppleTalk NetFilter 10-20
SETDefault -AppleTalk NetFilterType = Negative
```

NetFilterType

Syntax

```
SETDefault !<port> -AppleTalk NetFilterType = [Positive |
  Negative]
SHow [!<port> | !*] -AppleTalk NetFilterType
SHowDefault [!<port> | !*] -AppleTalk NetFilterType
```

Default Positive

Description The NetFilterType parameter determines whether network ranges (configured using the NetFilter parameter) are specified for positive or negative filtering on an AppleTalk routing port.

The use of positive or negative filtering is based on which requires the fewest ranges. For example, if you want to filter all networks except 30–40, use 30–40/Negative. This also could have been specified as 1–29, 41–65279/Positive; however, this approach is less efficient.

To activate network filtering, be sure that the Netfilter is enabled for this port through the CONTrol command.

Values

Positive Indicates that packets bearing network numbers identified in the network filters are discarded.

Negative Indicates that packets bearing network numbers not found in the network filters are discarded. Negative filtering is disabled if network filter ranges are not defined.

Filtering may adversely affect the expected performance of the router.

NetRange

Syntax

```
SETDefault !<port> -AppleTalk NetRange = <network-range>
SHow [!<port> | !*] -AppleTalk NetRange
SHowDefault [!<port> | !*] -AppleTalk NetRange
```

Default 0–0

Description The NetRange parameter specifies the legal range of network numbers that are used on the AppleTalk cable to which the router port is attached. The default (0–0) is allowed as input to disable the parameter.

For an AppleTalk router to assume the role of a seed router, the NetRange parameter must be set and zone list information must be specified.

The SHow command displays the current range of network numbers in use on the specified ports.

The SHowDefault command displays the configured range that may be used as seed information the next time the ports are enabled again by using the route control. For more information on specifying seed information and the AppleTalk router startup process, refer to Chapter 14 in *Using NETBuilder Family Software*.

This parameter takes effect the next time AppleTalk is enabled.

Values	<network-range>	A range of AppleTalk network numbers assigned to a network. Valid network ranges are 1–65,279.

NetZoneMapping

Syntax

```
SHow -AppleTalk NetZoneMapping [<number> (1-65279)]
```

Default No default

Description The NetZoneMapping parameter displays all the zones associated with a network. If an optional network number is specified, only those zones for the network on which the given network number is valid are displayed. If a network number is not specified, then the network range to zone mapping is displayed for all known networks. If a network zone list has not been acquired from another router, there may not be any zones listed. This is a temporary condition resulting from dropped zone-related request or reply packets. If the condition persists, use the SHow -AppleTalk DIAGnostics command for more information. Refer also to "ZoneAdvFilterNm"on page 4-21.

Values	<number>	Indicates a number within an AppleTalk network range.

Example The following sample display specifies the zones contained in a specified network number range of 10 through 20:

```
SHow -AppleTalk NetZoneMapping 10

----------------Network to Zone Mapping--------------
Network number range: 10-20 (0x000A-0x0014)
Total zones: 2
"B200 FINANCE"      "B300 MKT"
```

PortZone

Syntax

```
SETDefault !<port> -AppleTalk PortZone = "<zone-string>" (1–32 char)
SHow [!<port> | !*] -AppleTalk PortZone
SHowDefault [!<port> | !*] -AppleTalk PortZone
```

Default " " (null string)

Description The PortZone parameter specifies the zone name to be used by network entities residing on the specified port of this router (refer to "NAmes" on page 4-13). For example, the router registers the router name using this zone name on the specified port. The value configured through this parameter is used the next time the specified port is enabled for AppleTalk routing.

If a port zone is not explicitly defined for a port or the configured value is not in the active zonelist for the local network, the active default zone for the local network is used.

Ensure that the specified zone is in the configured zone list that is active for the network out the specified port.

Values “<zone-string>” Indicates characters in the Macintosh character set that can be specified using escape sequences. The backslash (\) character is used for escape sequences and must be followed by two hexadecimal digits that represent the character code. To insert a backslash in the string, use two backslashes (\\). This value is not case-sensitive and can be 1 to 32 characters in length. Refer to the table for the Macintosh extended character set in Chapter 14 in *Using NETBuilder Family Software.*

RouteAgingTime

Syntax

```
SETDefault -AppleTalk RouteAgingTime = <seconds> (20–300)
SHow -AppleTalk RouteAgingTime
SHowDefault -AppleTalk RouteAgingTime
```

Default 20

Description The RouteAgingTime parameter specifies the length of time (in seconds) that elapses between AppleTalk routing table validity checks. When the validity timer expires, every network entry in the routing table is transitioned to the next least reliable state. When the router receives new information, the status is updated to Good. Every time the route aging timer expires, the status drops one level, from Good to Suspect, then to Bad (1) and then to Bad (2). If a route has a status of Bad (2) when the aging timer expires, it is removed from the routing table.

3Com recommends that you do not change the default. Increasing this value may result in nonexistent routes remaining in the table for an extended time. Reducing it too low may result in an increase in router-generated traffic caused by an increased need to reacquire zone information from neighboring routers. If other vendors’ routers are on the network and they are configured with different broadcast and aging times, unreliable routing may result. \

This parameter takes effect immediately.

RouterName

Syntax

```
SETDefault !<port> -AppleTalk RouterName = “<object-string>”
  (1–32 char)
SHow [!<port> | !*] -AppleTalk RouterName
SHowDefault [!<port> | !*] -AppleTalk RouterName
```

Default “ “ (null string)

Description The RouterName parameter specifies the object portion of an AppleTalk entity name identifying an active AppleTalk router port in addition to the default name automatically registered by the router.

The actual entity name constructed from an AppleTalk router name specified as “XXX” with a portzone of “YYY” would be “XXX:3ComRouter@YYY”. Entity names are used as a convenient form of AppleTalk addressing.

The specified router name also is returned as the port description string in the AppleTalk management information base (MIB) (at port DESC). For related information, refer to “PortZone” on page 4-16, “NAmes” on page 4-13, “ANameLookup” on page 1-2 and “APING” on page 1-4.

This parameter takes effect immediately.

Values “<object-string>” Special characters in the Macintosh character set can be specified using escape sequences. The backslash (\) character is used for escape sequences and must be followed by two hexadecimal digits that represent the character code. To insert a backslash in the string, use two backslashes (\\). This value is not case-sensitive and can be 1 to 32 characters in length. Refer to the table for the Macintosh extended character set in Chapter 14 in *Using NETBuilder Family Software*.

RouteUpdateTime

Syntax

```
SETDefault -AppleTalk RouteUpdateTime = <seconds> (1–300)
SHow -AppleTalk RouteUpdateTime
SHowDefault -AppleTalk RouteUpdateTime
```

Default 10

Description The RouterUpdateTime parameter determines how often the router broadcasts AppleTalk routing information to all enabled AppleTalk ports. The router update time has an effective range of two seconds. Uneven values are rounded up to the next even number. For example, specifying 11 has the same effect as specifying 12.

Do not increase this parameter from its default value if other AppleTalk routers on the directly connected AppleTalk networks contain shorter routing table aging intervals. Unstable routes may result.

This parameter takes effect immediately.

SMDSGroupAddr

Syntax

```
SETDefault !<port> -AppleTalk SMDSGroupAddr = $<E0–EFFFFFFFFFFFFFFF>
  | None
SHow [!<port> | !*] -AppleTalk SMDSGroupAddr
SHowDefault [!<port> | !*] -AppleTalk SMDSGroupAddr
```

Default No default

Description The SMDSGroupAddr parameter configures the group address to be used as the AppleTalk broadcast and zone multicast datalink addresses on the specified port. For AppleTalk routing to occur over SMDS, the port must be configured with OWNer = SMDS and the -SMDS SMDSIndivAddr and the -AppleTalk SMDSGroupAddr parameters with valid individual and group addresses. If an address is not configured, a display of port diagnostic information through the -AppleTalk DIAGnostics parameter will indicate this fact as the reason for not routing.

Values	<E0–EFFFFFFFFFFFFFFF>	Indicates the format for an SMDS group address. The group address routes data to all devices in the SMDS network configured with the same group address. The group address begins with the letter E and is followed by 1 to 15 hex digits of the network number.
	None	Removes a group address that was previously assigned to a port.

StartupNET

Syntax

```
SETDefault !<port> -AppleTalk StartupNET = <number> (0–65279)
SHow [!<port> | !*] -AppleTalk StartupNET
SHowDefault [!<port> | !*] -AppleTalk StartupNET
```

Default 0

Description The StartupNET parameter specifies the tentative network number the AppleTalk router uses during dynamic node address acquisition when enabling a port. This number is used as a starting point only. If this network number cannot be used (the node IDs are all in use, or the network number is not in the active network range for the connected network), then the router continues the process of determining a valid network number and saves the final value in the configuration file for use the next time it has to perform the node address acquisition process. This final value is tried first the next time the port is enabled if the StartupNET value is zero at that time or cannot be used again.

To view the network number currently used for the port AppleTalk node address, use the SHow command.

StartupNODe

Syntax

```
SETDefault !<port> -AppleTalk StartupNODe = <number> (0–253)
SHow [!<port> | !*] -AppleTalk StartupNODe
SHowDefault [!<port> | !*] -AppleTalk StartupNODe
```

Default 0

Description The StartupNODe parameter specifies the tentative node ID to begin the process of dynamic AppleTalk node address acquisition for the specified router port. Apply this parameter to specify a starting value. If for any reason this value does not provide an unused node address, the router attempts to find a unique node ID and saves the new value for use the next time the router has to perform the address acquisition process. This final value is tried first at the next port enable time if the StartupNODe value is zero at that time or cannot be used again.

Use the SHow command to view the node ID currently in use for a specified port.

X25PROFileid

Syntax

```
SETDefault [!<port>] -AppleTalk X25PROFileid = <number>(0-9999)
SHow [!<port> | !*] -AppleTalk X25PROFileid
```

Default 0

Description The X25PROFileid parameter defines an X.25 user profile that is used when X.25 virtual circuits are set up to carry AppleTalk packets. A value of 0 indicates that no specific X.25 user profile is configured for AppleTalk packets.

X25ProtID

Syntax

```
SETDefault !<port> -AppleTalk X25ProtID = <protocol id> (1 octet)
SHow [!<port> | !*] -AppleTalk X25ProtID
SHowDefault [!<port> | !*] -AppleTalk X25ProtID
```

Default 0xCA

Description The X25PortID parameter specifies a protocol identifier for all outgoing X.25 call request packets to indicate that subsequent packets transmitted are AppleTalk packets.

The value of this AppleTalk parameter must be the same on all connected AppleTalk routers, or the incoming calls will be rejected. The chosen value must not conflict with that used by other protocols. The default is 0XCA.

The protocol identifiers (PIDs) are entered in hexadecimal (between 0 and FF).

ZONe

Syntax

```
ADD !<port> -AppleTalk ZONe "<zone-string>" (1–32 char)
DELete !<port> -AppleTalk ZONe (ALL | <zone-string> (1–32 char))
SHow [!<port> | !*] -AppleTalk ZONe
SHowDefault [!<port> | !*] -AppleTalk ZONe
```

Default No default

Description The ZONe parameter adds or deletes a zone name on the AppleTalk router zone list for the local AppleTalk network connected to a given port. The zone list is the list of zones that the router associates with the local network if it is serving as a seed router for the network attached to the port.

The available bridge/router memory space determines the upper limit on the number of zones you can configure in seed zone lists across all ports. If the zone name added is the first for a specified port, then the zone is the default zone for the network. If a deleted zone is the default zone for the network, the default zone changes to the first (alphabetically) of the remaining zones in the port zone list.

For setting the default zone from list of zones, refer to "DefaultZone" on page 4-8. For information on changing zone lists for an AppleTalk network, refer to Chapter 14 in the *Using NETBuilder Family Software*.

Values

"<zone-string>"	Indicates characters in the Macintosh character set that can be specified using escape sequences. The backslash (\) character is used for escape sequences and must be followed by two hexadecimal digits representing the character code. To insert a backslash in the string, use two backslashes (\\). This value is not case-sensitive and can be 1 to 32 characters in length. Refer to the table for the Macintosh extended character set in Chapter 14 in *Using NETBuilder Family Software.*
ALL	Used with the DELete command to delete all zone names from an AppleTalk router zone list.

ZoneAdvFilterNm

Syntax

```
ADD !<port> -AppleTalk ZoneAdvFilterNM <number> [Positive |
  Negative]
DELete !<port> ZoneAdvFilterNm <number>
ShowDefault [!<port> | !*] -AppleTalk ZoneAdvFilterNm
```

Default Positive

Description The ZoneAdvFilterNM parameter selects an entity filter for zone advertisement filtering. The entity filter is configured through the EntityFilter parameter in the AppleTalk Service. Only zone-specific entity filters of the "=:=@<zone>" type (where <zone> is a zone name) can be selected.

You can configure zone advertisement filtering on specific ports. This action allows some zones to be "hidden" on some ports but advertised on other ports.

Values

<port>	Specifies an AppleTalk port.
<number>	AppleTalk entity filter number. The entity filter number must identify an entity filter of type "=:=@zone" (configured using entity filter parameter).
Positive	Indicates positive filtering.
Negative	indicates negative filtering

ZoneNetMapping

Syntax

```
SHow -AppleTalk ZoneNetMapping [“<zone-string>” (1-32 chars)]
```

Default No default

Description The ZoneNetMapping parameter displays all the network ranges associated with a given zone. If no zone name is specified, then the zone to network range mapping is displayed for all known zones in the AppleTalk internetwork (refer also to "NetZoneMapping" on page 4-21).

Values

"<zone-string>"	Special characters in the Macintosh character set can be specified using escape sequences. The backslash (\) character is used for escape sequences and must be followed by two hexadecimal digits that represent the character code. To insert a backslash in the string, use two backslashes (\\). This value is not case-sensitive and can be 1 to 32 characters in length. Refer to the table for the Macintosh extended character set in Chapter 14 in *Using NETBuilder Family Software*.

5 APPN SERVICE PARAMETERS

This chapter describes all the parameters in the APPN Service. Parameters in this service are used to define Advanced Peer-to-Peer Networking (APPN) network nodes and end nodes, configure adjacent link stations, and to configure customized classes of service to meet specialized network needs.

Table 5-1 lists the APPN Service parameters and the commands.

Table 5-1 APPN Service Parameters and Commands

Parameters	Commands
AdjLenDef	ADD, DELete, SHow
AdjLinkSta	ADD, DELete, SHow
AdjNodeStatus	SHow
AppnLOG	SHow
ConfigCOS	ADD, DELete, SHow
CONFiguration	SHow
CONNection	SHow
ConnNetworkChar	SETDefault, SHow
ConnNetworkDef	ADD, DELete, SHow
CONTrol	SET. SETDefault, SHow
COS	SHow
COSDef	SET, SHow
COSNodeChar	SHow
COSNodeRow	ADD, DELete, SHow
COSTgChar	SHow
COSTgRow	ADD, DELete, SHow
DIRectory	SHow
DIrectoryEntry	ADD, DELete, SHow
DlurDefaults	SETDefault, SHow
DlurLinkSta	ADD, DELete, SHow
DluRStatus	SHow
DluSStatus	SHow
DownStreamLU	SHow
HprTimer	SETDefault, SHow
ISRsessions	SHow
LinkStaCHar	SETDefault, SHow
LinkStaCONTrol	SET, SHow
LocalNodeName	SETDefault, SHow
LocalNodeResist	SETDefault, SHow
Mode	SHow

(continued)

Table 5-1 APPN Service Parameters and Commands (continued)

Parameters	Commands
ModetoCosMap	ADD, DELete, SHow
NNtopology	SHow
PortCHar	SETDefault, SHow
PortCONTrol	SET, SHow
PortDef	SETDefault, SHow
QueuePriority	SETDefault, SHOw
RTP	SHow
RTPStats	SHow
SdlcAdjLinkSta	ADD, DELete, SHow
SdlcDlurLinkSta	ADD, DELete, SHow
TG	SHow
TreeCache	SHow

AdjLenDef

Syntax

```
ADD -APPN AdjLenDef [adjnetid.]<adjcpname> [adjlu ...]
DELete -APPN AdjLenDef [adjnetid.]<adjcpname> [adjlu ...]
SHow -APPN AdjLenDef [[netid.]cpname]
```

Default No default

Description The AdjLenDef parameter statically defines logical units (LUs) in adjacent low entry networking (LEN) end nodes into the network node's directory database. There are two situations in which you may need to statically define LEN end node LUs into the directory database:

- When a link activates with a LEN node, the LEN end node sends XID3 packets to the network node server. The LU name of the control point (CP) name field is automatically added to the network node server directory. However, if there are additional LUs in the LEN end node, then static configuration for those LUs is required.
- If the LEN end node's LU name does not match the CP name of the XID3, then static configuration is required.

Values

adjnetid.	Enters the net ID of the adjacent LEN node. When you enter the net ID, you must enter a period following it. The adjacent CP name follows the period without a space. If you do not enter the net ID, the net ID of the network node will be used.
<adjcpname>	Enters the nonqualified CP name of the adjacent LEN node.
adjlu	Enters the name of the LUs associated with the adjacent LEN node. The LU name can be from one to eight characters. You can enter up to four LU names when entering the command. To enter additional LUs, reenter the command. You can define up to 256 LUs for all adjacent LEN nodes defined.

Using the DELete command, you can delete individual LUs by specifying the LU name. If no LUs are specified with the DELete command, *all* LUs belonging to the adjacent LEN node will be deleted.

AdjLinkSta

Syntax

```
ADD !<port> -APPN AdjLinkSta <type>(NN|EN|Learn)
  <max_btu_size>(99-8912) [[Cmac|Ncmac] dest media addr]
  [Sap=<num>] [CPName=[netid.]cpname] [Nodeid=<ID>]
  [LinkName=<name>] [TGprof=<name>] [AutoStart=(Yes|No)]
  [CPSess=(Yes|No)] [HPR=(Yes|No)] [ErrorRecovery=(Yes|No)]
DELete !<port> -APPN AdjLinkSta <LinkName>
SHow [!<port>] -APPN AdjLinkSta [LinkName]
```

Default No default

Description The AdjLinkSta parameter defines an adjacent link station as a destination and defines the type of node being linked to, the destination address, and the node name associated with the link station. To send and receive traffic from all adjacent nodes (both network nodes and end nodes), you must configure the other nodes as adjacent link stations.

Once the adjacent link station is activated, if the APPN node is active and you want to make any configuration changes using this parameter or the LinkStaCHar parameter, you must first deactivate the link using the LinkStaCONTrol parameter. If the APPN node is not active, you do not need to deactivate the link.

You can set this parameter for virtual ports. To use virtual ports, the physical port that the virtual port is on must be configured for Frame Relay by entering the SETDefault !<port> -PORT OWNer = FrameRelay command. The DLC type configured using the SETDefault !<port> -APPN PortDef command must also be set to Frame Relay.

Values

NN|EN|Learn Specifies whether the destination is a network node (NN) or an end node (EN). Specify Learn if you do not know the node type and all you know is the node's media address. If you specify Learn, do not specify a CP name.

<max_btu_size> Enters the maximum number of bytes in a basic transmission unit (BTU) that can be sent to this destination. The acceptable range for network nodes is 99 to 8,912, while the acceptable range for end nodes is 256 to 8,912.

If you set the type to Learn, do not set the value to less than 256, because you do not know if the node is a network node or an end node. If the learned node is an end node and you set the value to less than 256, the link may not come up. If the link can support HPR (HPR=Yes), the maximum BTU size must be at least 768.

For optimal buffer utilization, the recommended maximum BTU size is 1,500 for Ethernet and for bridging LLC2 over serial lines using Source Route Transparent bridging. For token ring and all other media, including bridging over serial lines using Source Route bridging, the recommended maximum is 5,005.

<dest media addr>

Enters the destination media address. The destination media address is required if the port data link control (DLC) type is LLC2, Frame Relay, Data Link Switching (DLSw), or Synchronous Data Link Control (SDLC). The media address is not required if the port DLC type is Point-to-Point Protocol (PPP). If the port DLC type is Frame Relay, the media address is the DLCI.

If you have specified the -SYS MacAddrFormat parameter as noncanonical, enter the address in noncanonical format. If you have not changed the -SYS MacAddrFormat, enter the address in noncanonical format but add the prefix "Ncmac." Although you can enter the address in canonical format, SNA environments normally use noncanonical format. If Ncmac or Cmac is not specified, the format specified with the -SYS MacAddrFormat parameter is used.

Sap

Enters the service access point (SAP) of the remote node in the destination host. The valid range in hexadecimal of SAP values for this parameter is from 0x4 to 0xEC in multiples of 4. The default SAP value is 4. The SAP is always displayed using the hexadecimal value, but is not shown with the 0x prefix.

CPName

Enters the control point name of the adjacent link station. If the net ID is different than the net ID of the local node specified using the LocalNodeName parameter, you can specify the net ID. If you enter the net ID, you must type a period immediately following it, then type the CP name immediately following the period to create the fully qualified CP name. The CP name can be up to eight characters in length, and valid characters are A–Z, 0–9, $, @, #. The name cannot start with a number, a space or a period. This value is optional.

Nodeid

Enters the eight-digit hex identification that is used to identify the node. This value is optional. The node ID corresponds to the IDNUM of the IBM node ID format IDBLK/IDNUM.

<LinkName>

Specifies the name assigned to the link. All link names must be unique on the local network node. For example, you cannot use the same link name on more than one port, and you cannot use the same link name for two types of links (such as for adjacent link stations or DLUr link stations) at the same time. The link name is limited to eight characters, and cannot start with special characters. If no link name is specified, the system assigns a link name LINKXXXX where XXXX is a number between 0001 and 9999.

TGprof

Specifies the transmission group profile assigned to the link station. The TG profile is a set of default values that apply to the link if chosen. When a TG profile is chosen, the proper capacity and propagation delay values will be assigned to the link station based on the link speed of the media. If no profile for the link station is specified, then the profile specified for the port using the PortDef parameter is used; if no TG profile for the port is specified the system automatically picks a profile corresponding to the port's baud rate.

If the port is not active and the baud rate is unknown, then the system defaults to the Ser64 profile. Table 5-2 lists the TG profiles you can specify, and the corresponding link values. Once you specify a TG profile, if you then specify a different value for capacity or propagation delay using the LinkStaCHar parameter, then the TG profile value is overridden and the value assigned by the LinkStaCHar parameter is used.

Table 5-2 TG Profile Values

TG Profile	Link Type	Effective Capacity	Propagation Delay
TR4	LAN	4M (0x76)	LAN (0x4C)
TR16	LAN	16M (0x85)	LAN
Eth10	LAN	10M (0x80)	LAN
Eth100	LAN	100M (0x9A)	LAN
FDDI	LAN	100M (0x9A)	LAN
Ser9.6	WAN	9600 (0x30)	Telephone (0x71)
Ser19.2	WAN	19200 (0x38)	Telephone
Ser56	WAN	56000 (0x44)	Telephone
Ser64	WAN	64000 (0x45)	Telephone
Ser256	WAN	256000 (0x55)	Telephone
SerT1	WAN	T1 (0x69)	Telephone

AutoStart

Specifies whether AutoStart will be supported. If you specify yes, the link is automatically activated when the local network node is enabled and is restarted automatically if the link stops. If you specify no, the link is not automatically started and you must activate the link by entering the SET -APPN LinkStaCONTrol command. The default value is yes. In the SHow -APPN AdjLinkSta display, AutoStart support is shown in the “AS” column.

CPSess

Specifies whether CP-CP sessions are activated with the adjacent node. If you specify yes, CP-CP sessions will be activated with the node, and if you specify no, they will not. The default value is no if the adjacent node type is a network node, and yes if the adjacent node type is an end node or the node type is set to LEARN. In the SHow -APPN AdjLinkSta display, CP-CP session support is shown in the “CP” column.

HPR

Specifies if the link station supports High Performance Routing (HPR) on this link. If you specify “Yes,” then HPR will be supported on the link between the local node and the adjacent link station. If you specify “No,” HPR is not supported and the link uses Intermediate Session Routing (ISR). The default is Yes, meaning HPR is supported by default. If you want the adjacent link station to support only ISR, you must specify No.

ErrorRecovery For HPR links only, specifies if link level error recovery is used for an *outgoing* connection on the link. If you specify "Yes," error recovery is preferred, but can be negotiated down. If you specify "No," error recovery for HPR does not take place. If you want link level error recovery for the *incoming* connection, then you must set the ErrorRecovery value for the PortDef parameter (see page 5-31). The default is the ErrorRecovery value defined using the PortDef parameter (the port that the adjacent link station belongs to). If you use link level error recovery, additional overhead is created on your links. This value is only valid if the HPR value is set to "Yes."

Example To add an adjacent link station on port 1 that is a network node using a maximum BTU size of 1033, with a noncanonical MAC address of 100040C08ACE, a fully qualified control point name of "HQ.SnJose," enter:

```
ADD !1 -APPN AdjLinkSta NN 1033 N100040C08ACE CPName=HQSnJose
```

AdjNodeStatus

Syntax

```
SHow -APPN AdjNodeStatus [Name=[netid.]nodename] [Type=(EN|NN|VRN)]
```

Default No default

Description The AdjNodeStatus parameter displays the current status of the adjacent nodes on the network as well as the status of the CP-CP sessions between the local network node and the adjacent nodes. You can specify the display to show only adjacent nodes for a net ID, or you can specify the display to show only nodes of specific types.

Values Name Specifies the name to display the status of a specific node only. Optionally, you can specify the net ID, followed by a period, then followed by the node name.

Type Specifies the type of node for displaying only nodes of a certain type. Specify EN to display the status of adjacent end nodes and LEN end nodes only. Specify NN to display the status of adjacent network nodes only. Specify VRN to display the status of adjacent virtual routing nodes for connection networks only.

Example The following is an example of the display obtained by entering the SHow -APPN AdjNodeStatus command. Table 5-3 describes the meanings of the headings and status messages included in the display.

```
================================ SHow -APPN AdjNodeStatus =======================
-----------------------------------Adjacent Node Status---------------------------
CP Name            Type   TG Num   Status      VRN Address   CP Sess    Sap   RSN
US3COMHQ.ACSCFG    EN     1       OPERATIVE                  NO               2
US3COMHQ.#3COMPC1  EN     1       OPERATIVE                  YES              2
US3COMHQ.HOST3COM  NN     1       OPERATIVE                  YES              2
US3COMHQ.S100367A  NN     1       OPERATIVE                  YES              2
US3COMHQ.CUBE      NN     1       OPERATIVE                  YES              2
US#COMHQ.BEACH     NN     1       OPERATIVE                  YES              2
US3COMHQ.IBM4      NN     1       INOPERATIVE                YES              4
```

Table 5-3 AdjNodeStatus Display Meanings

Display Heading	Meaning
CP Name	CP name of the adjacent node.
Type	Node type of the adjacent node.
TG Num	Number assigned to the transmission group between the local node and the adjacent node. If you have parallel TGs between the local node and an adjacent node, one would be designated 1 and the other 2; also, with parallel TGs, one TG could be up while the other could be down.
Status	Status of the adjacent node. Operative indicates the node is operating, while Inoperative indicates the node is not. Quiescing means the node is in the process of shutting down.
VRN Address	Data link control (DLC) address (MAC and SAP address) of the connection to the virtual routing node (VRN).
CP Sess	Indicates whether CP-CP sessions are supported between the node and its adjacent partner.
Sap	SAP portion of the DLC address of the connection to the virtual routing node.
RSN	Resource Sequence Number (RSN) for the adjacent node that indicates how up-to-date the information regarding the node is. The higher the RSN number is, the more up-to-date the information.

LEN end nodes will display as end nodes; however, the CP status will display inactive even if the link is active because LEN end nodes do not have a control point.

AppnLOG

Syntax `SHow -APPN AppnLOG`

Default No default

Description The AppnLOG parameter displays a log of APPN activity messages captured on the bridge/router and stored in a buffer. The display shows the most recent activity messages, up to a limit of 256. Table 5-4 lists the event types captured in the log, and the corresponding message displayed. The lowercase “a” in the table denotes the various node or link names as part of the message.

Table 5-4 APPN Log Event Types and Messages

Event Type	Message displayed
Local network node activated	LOCAL NETWORK NODE *aaaaaaaa.aaaaaaaa* is STARTED
Local network node deactivated	LOCAL NETWORK NODE *aaaaaaaa.aaaaaaaa* is STOPPED
Link station activated	Link *aaaaaaaa* to *aaaaaaaa.aaaaaaaa* is UP
Link station deactivated	Link *aaaaaaaa* to *aaaaaaaa.aaaaaaaa* is DOWN
Downstream PU activated	Pipe to *aaaaaaaa.aaaaaaaa* is UP
Downstream PU deactivated	Pipe to *aaaaaaaa.aaaaaaaa* is DOWN
Downstream LU activated	SSCP_PU session for dspu *aaaaaaaa.aaaaaaaa* on link *aaaaaaaa* is UP
Downstream LU deactivated	SSCP_PU session for dspu *aaaaaaaa.aaaaaaaa* on link *aaaaaaaa* is DOWN

(continued)

Table 5-4 APPN Log Event Types and Messages (continued)

Event Type	Message displayed
CP-CP session activated	CONWINNER CP-CP session with *aaaaaaaa.aaaaaaaa* is UP
	CONLOSER CP-CP session with *aaaaaaaa.aaaaaaaa* is UP
CP-CP session deactivated	CONWINNER CP-CP session with *aaaaaaaa.aaaaaaaa* is DOWN
	CONLOSER CP-CP session with *aaaaaaaa.aaaaaaaa* is DOWN
RTP connection activated	RTP connection *aaaaaaaa.aaaaaaaa* is UP
RTP connection deactivated	RTP connection *aaaaaaaa.aaaaaaaa* is DOWN
RTP connection switched path	RTP connection *aaaaaaaa.aaaaaaaa* did a path switch

ConfigCOS

Syntax

```
ADD -APPN ConfigCOS <cos name> <transmit priority>
  [SNA defined COS name]
DELete -APPN ConfigCOS <cos name>
SHow -APPN ConfigCOS
```

Default No default

Description The ConfigCOS parameter creates a customized class of service (COS), assigns a name to the class of service, and sets the appropriate transmission priority.

Values

<cos name>	Enters the desired class of service name. The name can be up to eight characters long.
<transmit priority>	Enters the desired transmission priority associated with this class of service. Select one of the following values: High, Medium, and Low.
SNA defined COS name	Specifies whether a SNA-defined COS will be used for this COS. If you enter this optional value, the default node row and transmission group row characteristics assigned to the Systems Network Architecture (SNA) default are automatically assigned to the new class of service name you create.

CONFiguration

Syntax

```
SHow -APPN CONFiguration
```

Default No default

Description The CONFiguration parameter displays complete information on the APPN Service parameter settings as well as information on the APPN network configuration. The display includes individual displays such as adjacent link stations, link station characteristics, and class of service definitions.

CONNection

Syntax

```
SHow -APPN CONNection [[netid.]cpname | ALL]
```

Default Shows connections to and from the local network node only.

Description The CONNection parameter displays information about connections in the APPN network. The display includes connections associated with the network node topology only. The display shows the following:

- Links for the specified network node
- All links the network node is aware of

The display does not include connections between other network nodes and their associated end nodes.

Values netid. Specifies the net ID, although it is not required. If you do specify the net ID, you must enter a period after it, followed by the CP name with no space after the period. Net ID needs to be specified if the CP name has a different net ID than the local network node.

cpname | ALL Specifies a CP name to be displayed. If you specify a CP name, you display a list of connections to the node with that CP name. If you specify ALL, you display a list of all connections for both the local topology and the network topology.

When entering a CP name, you can enter either a non-qualified name (such as NB2GREEN) or a fully qualified name (such as US3COMHQ.NB2GREEN).

If no value is specified, then only connections to the local network node are displayed.

To obtain the following display (showing all connections for both local and network topologies), enter the SHow -APPN CONNection ALL command. Table 5-3 describes the meanings of the headings and status messages included in the display.

```
======================SHow -APPN CONNection======================
-------------------------Connection Topology----------------------
Node name                Partner name       TG num State  RSN
US3COMHQ.CN7(VRN)        US3COMHQ.CUBE      1      UP     2
US3COMHQ.CN5(VRN)        US3COMHQ.IBM4      1      UP     26
US3COMHQ.CUBE            US3COMHQ.IBM4      1      UP     20
US3COMHQ.CN5(VRN)        US3COMHQ.COM20E    1      UP     2
US3COMHQ.CUBE            US3COMHQ.COM20E    1      UP     2
US3COMHQ.IBM4            US3COMHQ.CUBE      1      UP     8
*US3COMHQ.COM20E         US3COMHQ.IBM4      1      DOWN   12
```

Table 5-5 CONNection Display Meanings

Display Heading	Meaning
Node name	Node name for the connection. This will always be a network node, but may not necessarily be a 3Com bridge/router network node. If VRN is displayed, this indicates the node is acting as a virtual routing node. If the node name has an asterisk in front of it (as shown in the last line of the example), this indicates that the entry is not paired with its partner node in both directions, meaning the information may be stale in the network. If a node name is shown with an asterisk and the state is up, connectivity with the node may not be possible.
Partner name	Node name for the node at the remote end of the connection.

(continued)

Table 5-5 CONNection Display Meanings (continued)

Display Heading	Meaning
TG num	Number assigned to the transmission group between the two nodes. If you have parallel TGs between two nodes, one would be designated 1 and the other 2; also, with parallel TGs, one TG could be up while the other could be down.
State	Status of the connection: up or down. If both nodes are up, then the connection state will be up. If at least one node is down, then the connection state will be down.
RSN	Resource Sequence Number (RSN) for the TG. This indicates how up-to-date the information regarding the TG is. The higher the RSN number is, the more up-to-date the information. If you have two entries in the display showing the same TG, the entry with the higher RSN is more up-to-date. If the topology is stable, the RSN for the different network nodes would normally match.

ConnNetworkChar

Syntax

```
SETDefault -APPN ConnNetworkChar = <cn name> [EffectCap=<string>]
  [ConnectCost=<0-255>] [ByteCost=<0-255>] [Security=<string>]
  [PropDelay=<string>] [Usd1=<0-255>] [Usd2=<0-255>] [Usd3=<0-255>]
SHow -APPN ConnNetworkChar <cn_name>
```

Default No default

Description The ConnNetworkChar parameter specifies TG characteristics for a connection network. You can specify any value you want to change; any value not specified will not be affected.

Values

<cn name> Specifies the name assigned to the connection network.

EffectCap Specifies the highest bit transmission rate that the TG can obtain. Specify one of the following values: MINimum, MAXimum, 2400, 4800, 9600, 19200, 56000, 64000, 2560000, T1, 4M, 10M, 16M, 25M, 100M, or 155M. The default values are those used by the connection network's TG profile. You must enter this value using one of these strings; however, these strings map to specific hex values. For information on mapping the hex values to these strings, see Table 5-2 on page 5-5.

ConnectCost Specifies the relative cost per unit time of using a TG. Valid values are from 0–255. The default is 0.

ByteCost Specifies the relative cost per byte for using a TG. Valid values are from 0–255. The default is 0.

Security Specifies the level of security available on the TG. Specify one of the following strings: NONsecure, PKTswtnet, UNDgndcbl, SECurcnd, GUArdcnd, ENCryptd, guardRAD, or MAX. The default values are those used by the connection network's TG profile. You must enter this value using one of these strings; however, these strings map to specific hex values. For information on mapping the hex values to these strings, see Table 5-11 on page 5-24.

PropDelay Specifies the length of time in microseconds for a signal to propagate from one end of the TG to the other. Specify one of the following strings: MINimum, LAN, TELephone, PKTswitch, SATellite, or MAXimum. The default values are those used by the connection network's TG profile.You must enter this value using one of these strings; however, these strings map to specific hex values. For information on mapping the hex values to these strings, see Table 5-12 on page 5-25.

Usd1 Specifies the value for user-defined parameter 1. The user-defined parameters represent TG characteristics defined by the network administrator. Valid values are from 0–255. The default is 128. These values also apply to user-defined parameters 2 and 3.

Usd2 Specifies the value for user-defined parameter 2.

Usd3 Specifies the value for user-defined parameter 3.

ConnNetworkDef

Syntax

```
ADD !<port> -APPN ConnNetworkDef [netid.]<cn name>
   [TG profile name]
DELete !<port> -APPN ConnNetworkDef [netid.]<cn name>
SHow -APPN ConnNetworkDef [[netid.]cn name]
```

Default No default

Description The ConnNetworkDef parameter adds or deletes connection network definitions. If the node is active, the addition or deletion is dynamic. The optional TG profile_name specifies the default TG characteristics for the connection network. Because the connection network can be defined for multiple ports, the profile only needs to be specified on the first ADD command.

Values netid. Specifies the net ID of the connection network. If you specify the net ID, you must type a period immediately following the name, and then the cn_name must immediate follow the period. If you do not specify the net ID, the net ID of the local network node is used.

<cn name> Specifies the name assigned to the connection network. If you enter the net ID, you must type a period immediately after it, then type the connection network (CN) name immediately after the period to create the fully qualified CN name. The CN name can be up to eight characters in length, and valid characters are A–Z, 0–9, $, @, #. The name cannot start with a number, a space or a period. This value is optional.

TG profile name Specifies the TG profile assigned to the connection network. The TG profile is a set of default values that apply to the connection network if chosen. When a TG profile is specified, the proper capacity and propagation delay values are assigned to the link station based on the link speed of the media.

If no profile for the link station is specified, then the profile specified for the port using the PortDef parameter is used. If a TG profile for the port is not specified, then the system automatically picks a profile corresponding to the port's baud rate. If the port is not active and the baud rate is unknown, then the system defaults to the Ser64 profile. For a list of TG profiles, see Table 5-2 on page 5-5.

CONTrol

Syntax

```
SET -APPN CONTrol = Enable|Disable [<type>(Immediate|Orderly)]
SETDefault -APPN CONTrol = Enable|Disable [<type>(Immediate|
  Orderly)]
SHow -APPN CONTrol
```

Default Disable (default for Disable is Immediate)

Description The CONTrol parameter enables the bridge/router to serve as an APPN network node. You can use the SETDefault command to initially enable the network node. When the network node is enabled, use the SET command to disable the network node without changing the configuration file.

If you plan to configure both APPN and DECnet on the same bridge/router, DECnet routing must be configured on the bridge/router before APPN is enabled because the DECnet configuration can change the bridge/router's MAC addresses.

Values

Enable | Disable	Enable allows the bridge/router to serve as an APPN network node. If used with the SETDefault command, the network node automatically comes up when the bridge/router is rebooted. Disable stops the bridge/router from serving as an APPN network node.
type	Specifies the type of deactivation that occurs if you disable the network node. You do not specify the type when enabling the node. If you specify Immediate, the links are deactivated first, then the ports on the network node, and then the network node itself. If you specify Orderly, the node first is advertised as "Quiesced," then the session limits are reset on all modes. After all ISR sessions have ended, all endpoint sessions and all CP-CP sessions are unbound. The links are first deactivated, followed by the ports on the network node, and then followed by the network node itself.

COS

Syntax

```
SHow -APPN COS
```

Default No default

Description The COS parameter displays information regarding the classes of service that are available to the network node. If no customized classes of service have been created, the display shows the SNA defaults. The display shows the COS name, the priority for the COS (low, medium, high or network), the number of node and TG rows for the COS. The column in the display #trees indicates the number of route trees computed and cached for that COS.

COSDef

Syntax

```
SET -APPN COSDef = <cos name>
SHow -APPN COSDef
```

Default No default

Description The COSDef parameter defines a customized class of service to the local node. Until this parameter is set, the class of service first created using the ConfigCOS parameter does not take effect.

COSNodeChar

Syntax

```
SHow -APPN COSNodeChar
```

Default No default

Description The COSNodeChar parameter displays all the class of service node row characteristics the local node knows about. These include the following:

- Customized class of service node tables configured using the COSNodeRow parameter
- SNA default class of service node tables

If a customized class of service has been created but not defined to the system using the COSDef parameter, the system will not yet know it, and will not be shown on this display.

COSNodeRow

Syntax

```
ADD -APPN COSNodeRow <cos name> <weight>(0–255) [Congestion=min
   (Yes|No),max (Yes|No)] [Resistance=min,max]
DELete -APPN COSNodeRow <cos name> <row num>
SHow -APPN COSNodeRow [cosname]
```

Default No default

Description The COSNodeRow parameter defines the characteristics of the class of service (COS) node row. You can define the characteristics of a node row in the node table. Weight is determined by the congestion state and resistance (desirability of routing). Node rows are sorted in ascending weight order. Using the SHow command, you can display all node rows for user-configured classes of service. If you enter the class of service name, you display only the node rows for the specific class of service.

In the values specifying minimum and maximum values, you must specify both, separated by a comma (but no space). In the value that takes in decimal values (resistance), you can use hexadecimal values if preceded with “0x” (for example, 0x100).

Values Select the following values using the ADD command:

<cos name> Specifies the class of service name. The name can be up to eight characters long.

<weight> Specifies the weight associated with the row. Valid values are from 0–255.

Congestion Specifies the minimum and maximum congestion values for the node. For both the minimum and maximum values, specify either Yes (congested) or No (uncongested) for both minimum and maximum values. The default value for minimum congestion is No (uncongested), and the default value for maximum congestion is Yes (congested).

If you set the minimum congestion value to No and the maximum congestion to No, if the node on the desired path is congested, it will not satisfy the requirements of the entry. If you set the minimum congestion to No and the maximum congestion to Yes (the default), the node is considered a "wide open" gate and satisfies the requirements of the entry. If you set both the minimum and maximum congestion values to Yes, only a congested node satisfies the entry requirements; this combination is not recommended. If you set the minimum congestion to Yes and the maximum congestion to No, it is illegal. No nodes can satisfy the entry requirements.

Resistance Specifies the minimum and maximum resistance values for the row. A value between 0–255 indicates both the minimum resistance (the lowest acceptable route addition resistance), and the maximum resistance (the highest acceptable route addition resistance) for this row. The default for the minimum resistance is 0. The default for the maximum resistance is 255.

CAUTION: *If you are creating a customized class of service table, make sure that you configure the last node row in the table to include both the minimum and maximum values for all characteristics. Otherwise, you risk creating a situation in which none of the node rows in the table apply. Select the following values using the DELete command:*

<cos name>	Specifies the class of service name with the row to be deleted.
<row num>	Specifies the row number to be deleted.

Example To add a COS node row to the COS named COSA in which the weight is 255, the minimum congestion is Yes and the maximum congestion is Yes, and the minimum resistance is 128 and the maximum resistance is 255, enter:

```
ADD -APPN COSNodeRow COSA 255 Congestion=Yes,Yes Resistance=128,255
```

COSTgChar

Syntax

```
SHow -APPN COSTgChar
```

Default No default

Description The COSTgChar parameter displays all the following class of service TG row characteristics that the local node knows about:

- Customized class of service TG tables configured using the COSTgRow parameter
- SNA default class of service TG tables

If a customized class of service has been created but not defined to the system using the COSDef parameter, the system will not yet know it, and will not be shown on this display.

COSTgRow

Syntax

```
ADD -APPN COSTgRow <cos name> <weight>(0-255)
  [ConnectCost=min,max] [ByteCost=min,max] [Security=min,max]
  [PropDelay=min,max] [EffectCap=min,max] [Usd1=min,max]
  [Us2=min,max] [Usd3=min,max]
DELete -APPN COSTgRow <cos name> <row num>
SHow -APPN COSTgRow [cosname]
```

Default No default

Description The COSTgRow parameter defines the characteristics of the class of service transmission group (TG) table rows in the COS database. You can define the weight of the transmission group associated with a class of service, and the characteristics of the CP-CP sessions of the TG. With the SHow command, you can display all transmission group rows for user-configured classes of service. If you enter the class of service name, you display only the transmission group rows for the specific class of service.

In options specifying both minimum and maximum values, you must specify both, separated by a comma (but no space). In all values of this parameter that use decimal values (connection cost, byte cost, and Usd1, Usd2 and Usd3), you can use hexadecimal values if preceded with “0x” (for example, 0x100).

Values Select the following values using the ADD command:

<cos name>	Specifies the class of service name. The name can be up to eight characters long.
<weight>	Specifies the weight of the row of the TG table. Valid values are 0–255.
ConnectCost	Specifies the minimum and maximum connection cost for the TG. Valid values for both are 0-255. The default minimum connection cost is 0, and the default maximum connection cost is 255.
ByteCost	Specifies the lowest and highest acceptable cost per byte value for the row. Valid values for both are 0–255. The default minimum byte cost is 0, and the default maximum byte cost is 255.
Security	Specifies the lowest and highest acceptable values of security for the row. You can choose from one of the following seven values for both: NONsecure, PKTswtnet, UNDgndcbl, SECurecnd, GUArdcnd, ENCryptd, and guardRAD. The default for the minimum security value is NONsecure, and the default for the maximum security value is guardRAD.
PropDelay	Specifies the minimum and maximum propagation delay value in microseconds. Specify one of the following strings for each: MIN, LAN TELephone, PKTswitch, SAT AND MAX. The default minimum value is MIN, and the default maximum value is MAX.
EffectCap	Specifies the minimum and maximum encode effective capacity of the TG. Specify one of the following values for both: MINimum, MAXimum, 1200, 4800, 9600, 19200, 56000, 64000, T1, 4M, 10M, 16M, 100M. Each unit represents 300 bps. The default minimum value is MINimum (0), and the default maximum value is MAXimum (0xFF).

Usd1 Specifies the minimum and maximum values for user-defined parameter 1. The user-defined parameters represent TG characteristics defined by the network administrator. Valid values for both are from 0–255. The default is 0 for the minimum value and 255 for the maximum value. These values also apply to user-defined parameters 2 and 3.

Usd2 Specifies the minimum and maximum values for user-defined parameter 2.

Usd3 Specifies the minimum and maximum values for user-defined parameter 3.

CAUTION: *If you are creating a customized class of service table, make sure that you configure the last TG row in the table to include both the minimum and maximum values for all characteristics. Otherwise, you risk creating a situation in which none of the TG rows in the table apply.*

Select the following values using the DELete command:

<cos name> Enters the class of service name that has the row to be deleted.

<row num> Enters the row number to be deleted.

Example To add a TG row to the COS named “COSA” with a weight of 128, minimum and maximum connection cost of 128 and 128, minimum and maximum byte cost of 128 and 128, minimum and maximum security value of ENCrypted, minimum delay of NEGligible and maximum delay of LONG, and minimum capacity of 19200 and maximum capacity of 64000, enter:

```
ADD -APPN COSTgRow COSA 128 Connection=128,128 Byte=128,128
Security=ENCrypted,ENCrypted PropDelay=NEGligible,LONG
EffectCap=19200,64000
```

DIRectory

Syntax `SHow -APPN DIRectory`

Default No default

Description The DIRectory parameter displays directory table information for your APPN network. The display shows all local LUs, LUs in the domain of the local network node, and all LUs discovered that are still in the cache. The display includes entries entered through the DirectoryEntry and AdjLenDef parameters, and entries learned through other APPN nodes.

The following display is obtained by entering the SHow -APPN DIRectory command:

```
=========================== SHow -APPN DIRectory ===========================
-----------------------------------Directory-----------------------------------
Resource Name      Type      Parent Name        Type   Entry Location  Type
US3COMHQ.CUBE      NNCP                         LOCAL  HOME
US3COMHQ.CUBE      LU        US3COMHQ.CUBE      NNCP   LOCAL           HOME
US3COMHQ.LEN1      ENCP      US3COMHQ.CUBE      NNCP   DOMAIN          HOME
US3COMHQ.LU10      LU        US3COMHQ.LEN1      ENCP   DOMAIN          HOME
US3COMHQ.NN1       NNCP                                X_DOMAIN        HOME
US3COMHQ.EN1       ENCP      US3COMHQ.NN1       NNCP   X_DOMAIN        HOME
US3COMHQ.LU7*      WILDCARD  US3COMHQ.NN1              X_DOMAIN        HOME
```

Table 5-6 explains the headings in the directory display.

Table 5-6 Directory Display Meanings

Display Heading	Meaning
Resource Name	Name of the resource as listed in the directory database.
Type	Resource type of the entry. NNCP indicates the entry is a Network Node Control Point, while ENCP indicates the entry is an End Node Control Point. LU indicates the entry is a logical unit. WILDCARD indicates the entry is a wildcard entry. If the resource type is an NNCP, then it will not have a parent resource.
Parent Name	Parent name of the resource entry.
Type	Parent type of the resource. NNCP Indicates the parent is a network node control point and ENCP indicates the parent is an end node control point.
Entry Location	Location of the entry. Local indicates the resource is located on the network node, while Domain indicates the entry is on another node in the domain served by the local network node. XDomain indicates the entry is on a node in a domain served by a *remote* network node.
Type	Indicates whether the directory entry is a home entry, a cached entry, or a registered entry.

DirectoryEntry

Syntax

```
ADD -APPN DirectoryEntry [netid.]<resource name> <type(LU|EN|NN|
  Wild)> [[netid.]<parent_name> <parent_type(EN | NN)>]
  [[netid.]<grandparent_name> <grandparent_type(NN)>]
DELete -APPN DirectoryEntry [netid.]<resource name> <type(LU|EN|
  NN|Wild)>
SHow -APPN DirectoryEntry [[netid.]resource name]
```

Default No default

Description The DirectoryEntry parameter preloads an entry into the APPN Directory Cache. In the syntax EN is short for EN Control Point and NN is short for NN Control Point. When deleting wildcard entries, the lu_name must match the wildcard name exactly (that is, LU* will not match LU7*). When you use the SHow command, you display a list of user-configured entries.

Values

netid.	Specifies the net ID of the directory entry. If you specify the net ID, you must type a period immediately following the name, and then the lu_name must immediate follow the period. If you do not specify the net ID, the net ID of the local network node will be used.
<resource name>	Specifies the name of the directory entry resource.
<type>	Specifies the type of node where the directory entry resides. Specify LU if the resource is an LU. Specify EN if the resource is an end node or LEN end node control point. Specify NN for a network node control point. Specify Wild when entering or deleting wildcard entries. If the resource type is not an NN, then it requires a parent (including name and type) in the same command.
<parent_name>	Specifies the name of the parent for the resource.

<parent_type> Specifies the type of the parent. Specify EN if the parent is an end node or LEN end node control point, or NN if the parent is a network node control point. If the parent type is not an NN, then it requires a grandparent (including name and type) in the same command.

<grandparent_name> Specifies the grandparent name of the resource.

<grandparent_type> Specifies the type of the grandparent. The grandparent type must be NN.

Table 5-7 lists the hierarchy of parents and grandparents required for the different resource types.

Table 5-7 Hierarchy of Directory Entries

Resource Type	Parent	Required Grandparent
NN	none	none
EN/LU/WILD	NN	none
LU/WILD	EN	NN

Example To add an LU resource named LU22 in which EN22 is the parent and HQ.NNGREEN is the grandparent, enter:

```
ADD -APPN DirectoryEntry LU22 LU EN22 EN NNGREEN NN
```

DlurDefaults

Syntax

```
SETDefault -APPN DlurDefaults [Dlus=(<[netid.]name>|UNdef)]
  [Backup=(<[netid.]name>|UNdef)]
SHow -APPN DlurDefaults
```

Default No DLUs or backup DLUs

Description The DlurDefaults parameter specifies the default Dependent LU Server (DLUs) name and a backup DLUs name. If you want to reset the DLUs or backup DLUs enter the name as UNdef.

Values

dlus Specifies the name of the default DLUs. To reset the DLUs name, enter UNdef.

backup Specifies the name of the backup DLUs. To reset the DLUs name, enter UNdef.

DlurLinkSta

Syntax

```
ADD !<port> -APPN DlurLinkSta <max_btu_size(256-8912)> <[Cmac |
  Ncmac] dest media addr> <dspu name> [Sap=<num>] [Nodeid=<ID>]
  [LinkName=<name>] [Dlus=<[netid.]name|UNdef>]
  [Backup=<[netid.]name|UNdef>] [TGprof=<name>]
  [AutoStart=(Yes|No)] [CPSess=(Yes|No)] [PU2=(Yes|No)]
  [HPR=(Yes|No)] [ErrorRecovery=(Yes|No)]
DELete !<port> -APPN DlurLinkSta <LinkName>
SHow [!<port>] -APPN DlurLinkSta [LinkName]
```

Default No default

Description The DlurLinkSta parameter specifies a LinkStation for downstream DLUr nodes. Using the ADD command, you specify a DLUr link station for a port, including the DLUr's destination address and downstream physical unit name (DSPU).

Values

<max_btu_size> Specifies the maximum BTU size for the DLUr link station. The value range is 256-8912.

<dest media addr> Specifies the destination MAC address for the DLUr link station. If you have specified the -SYS MacAddrFormat parameter as noncanonical, enter the address in noncanonical format; if you have not changed the -SYS MacAddrFormat parameter, enter the address in noncanonical format but add the prefix "NcMac."

<dspu name> Specifies the downstream PU (DSPU) name. If the host will be activate the session with the DLUr link station, then the DSPU name you configure here must match the name on the host configuration.

Sap Enters the service access point (SAP) of the DLUr link station. The valid range in hexadecimal of SAP values for this parameter is from 0x4 to 0xEC in multiples of 4. The default SAP value is 0x04. Note that the SAP is always displayed using the hexadecimal value, but is not shown with the 0x prefix.

Nodeid Specifies the node ID that is checked by the XID. The node ID must be entered in hex and must include all eight hex digits. A node ID of 0x00000000 means that the Node ID will not be checked.

<LinkName> Specifies the name assigned to the link. All link names must be unique on the local network node. For example, you cannot use the same link name on more than one port, and you cannot use the same link name for two types of links (such as for adjacent link stations or DLUr link stations) at the same time. The link name is limited to eight characters, and cannot start with special characters. If no link name is specified, the system assigns a link name LINKXXXX where XXXX is a number between 0001 and 9999. When deleting a DLUr link station, you must specify the link name.

Dlus Specifies the primary DLUs name used by this DLUr link station. If no primary DLUs is specified, then the DLUs configured with the DlurDefaults parameter are used. To remove the primary DLUs name, enter Undef.

Backup Specifies the backup DLUs name used by this DLUr link station. If no backup DLUs is specified, then the backup DLUs configured with the DlurDefaults parameter are used.To remove the backup DLUs name, enter Undef.

TGprof Specifies the TG profile assigned to the DLUr link station. The TG profile is a set of default values that apply to the link if chosen. When a TG profile is specified, the proper effective capacity and propagation delay values are assigned to the link station based on the link speed of the media. For a list of TG profiles, see Table 5-2 on page 5-5.

AutoStart

If you specify Yes, the link is automatically activated when the local network node is enabled, and is restarted automatically if the link stops. If you specify No, the link is not automatically started and you will have to activate the link using the SET -APPN LinkStaCONTrol command. The default value is yes. In the SHow -APPN DlurLinkSta display, AutoStart support is shown in the “A” column.

CPSess

Specifies whether CP-CP sessions is activated with the adjacent node. If you specify yes, CP-CP sessions are activated with the node, and if you specify no, they are not. The default value is no if the adjacent node type is a network node, and yes if the adjacent node type is an end node or the node type is set to LEARN. In the SHow -APPN DlurLinkSta display, CP-CP session support is shown in the “CP” column.

PU2

Specifies whether the link station is a PU 2.0 node or a PU 2.1 node. If you specify Yes, the link supports communication to PU 2.0 nodes but supports DLUr services only (and not APPN services). If you specify No, the link supports communication to PU 2.1 nodes and can support both APPN and DLUr over the same link. The default is No.

If you specify Yes, the link can be activated by the host. If you specify No, the link cannot be activated by the host. Specify Yes if the downstream node does not support APPN, or you do not want APPN services from the local network node.

HPR

Specifies whether the link station supports High Performance Routing (HPR) on this link. If you specify Yes, then HPR is supported on the link between the local node and the DLUR link station. If you specify No, HPR is supported, and the link uses Intermediate Session Routing (ISR). The default is Yes, which means HPR is supported by default, so if you want the adjacent link station to support only ISR, you must specify No. If HPR is set to Yes, then PU2 must be set to No.

ErrorRecovery

For HPR links only, specifies whether link-level error recovery is used for an *outgoing* connection on the link. If you specify Yes, error recovery is preferred, but can be negotiated down. If you specify No, error recovery for HPR will not take place. If you want link level error recovery for the *incoming* connection, then you must set the ErrorRecovery value for the PortDef parameter (see page 5-31). The default is the ErrorRecovery value defined using the PortDef parameter (the port the adjacent link station belongs to). If you use link-level error recovery, additional overhead is created on your links. This value is only valid if the HPR value is set to “Yes.”

DluRStatus

Syntax

```
SHow -APPN DluRStatus [[netid.]dlur_name]
```

Default No default

Description The DluRStatus parameter shows the status of all DLUr PUs downstream from the local network node. You can also display the status of a specific DLUr PU. To display the status of DLUr LUs downstream from the local use, use the DownStreamLU parameter.

DluSStatus

Syntax `SHow -APPN DluSStatus [[netid.]dlus_name]`

Default No default

Description The DluSStatus parameter shows the status of all DLUs pipes for the local network node. You can also display the status of a specific DLUs.

DownStreamLU

Syntax `SHow -APPN DownStreamLU [dslu_name]`

Default No default

Description The DownStreamLU parameter displays a list of sessions with dependent LUs downstream from the local node (all LUs that reside on PU 2.0 nodes and all dependent LUs residing on PU 2.1 nodes). You can also display information on a single downstream LU. To display a list of sessions with other types of LUs, use the -APPN ISRsessions parameter.

The following is an example of the display obtained by entering the SHow -APPN DownStreamLU command:

```
-------------------------DownStream LU Sessions---------------------------
DSLU       NAU  DSPU      SSCP-LU  PLU-SLU           Upstream   Downstream
name            name      Status   Status   LFSID    Linkname   Linkname
LU31HB12   02   PU31HB1   ACTIVE   ACTIVE   000103   LINK0001   LINK0064
LU31HB13   03   PU31HB1   ACTIVE   INACTIVE 000000
LU31HB14   04   PU31HB1   ACTIVE   INACTIVE 000000
LU31HB15   05   PU31HB1   ACTIVE   INACTIVE 000000
```

Table 5-8 explains the headings in the downstream LU display.

Table 5-8 DownStreamLU Display Meanings

Display Heading	Meaning
DSLU name	Downstream LU name.
NAU	Network Addressable Unit
DSPU name	Downstream PU name.
SSCP-LU Status	Status of pipe between SSCP on the host and the downstream LU
PLU-SLU Status	Status of the link between the primary logical unit (PLU) and secondary logical unit (SLU)
LFSID	Local Form Session Identifier
Upstream Linkname	Name of the link between the local node and upstream LU
Downstream Linkname	Name of the link between the local node and the downstream LU

HprTimer

Syntax

```
SetDefault -APPN HprTimer = [AliveTimer=<30-600>]
  [PathSwitchTimerLow=<240-960>][PathSwitchTimerMed=<120-480>]
  [PathSwitchTimerHigh=<60-240>][PathSwitchTimerNtwk=<30-120>]
SHow -APPN HprTimer
```

Default AliveTimer is 180; PathSwitchTimer is 120

Description The HprTimer parameter defines the timer settings in seconds for the Rapid Transport Protocol (RTP) connection. Changing this parameter only affects new RTP connections, and has no effect on existing RTP connections. The local network node must be an RTP endpoint for the RTP connection for the settings to take effect.

Values

AliveTimer Specifies the duration before a keepalive probe is sent on an idle line. The default is 180 seconds. The valid range is from 30 to 600 seconds.

PathSwitchTimer Low Specifies the duration that an RTP endpoint tries for a new RTP connection when a path switch takes place on a connection with low priority. The default is 200 seconds. The valid range is from 240 to 960 seconds.

PathSwitchTimerMed Specifies the duration that an RTP endpoint tries for a new RTP connection when a path switch takes place on a connection with medium priority. The default is 240 seconds. The valid range is from 120 to 480 seconds.

PathSwitchTimerHigh Specifies the duration that an RTP endpoint tries for a new RTP connection when a path switch takes place on a connection with high priority. The default is 120 seconds. The valid range is from 60 to 240 seconds.

PathSwitchTimerNtwk Specifies the duration that an RTP endpoint tries for a new RTP connection when a path switch takes place on a connection with network priority. The default is 60 seconds. The valid range is from 30 to 120 seconds.

ISRsessions

Syntax `SHow -APPN ISRsessions`

Default No default

Description The ISRsessions parameter displays the status of Intermediate Session Routing (ISR) sessions, or the full session between two endpoint LUs. Because the local network node is an intermediate point between the two endpoints on the session, the display shows both the part of the session incoming to the network node and the part of the session outgoing from it.

Example The following is an example of the display obtained by entering the SHow -APPN ISRsessions command:

```
=========================== SHow -APPN ISRsessions ==========================
-----------------------------------ISR Sessions-------------------------------
Originator     COS        Limit   Primary          Secondary
CP name        name       Res     LFSID   Linkname  LFSID      Link name
US3COMHQ.IBM4  SNASVCMG   NO      010201  LINK0000  000201     @I000001
US3COMHQ.IBM4  #INTER     NO      010202  LINK0000  000202     @I000001
```

Table 5-9 explains the headings in the ISR sessions display.

Table 5-9 ISRsessions Display Meanings

Display Heading	Meaning
Originator CP name	Control point name of the node that sends out the BIND for that session.
COS name	Class of service named used for the ISR session.
Limit Res	Indicates whether the ISR session is over a limited resource.
Primary LFSID	Primary Local Form Session Identifier (LFSid). The first two digits of the LFSid (the ODAI bit) indicates which node was assigned the values in the transmission header. For more information on the ODAI bit format, refer to the IBM document, *APPN Architecture and Product Implementations Tutorial*.
Primary Link name	Name of the link for the primary stage of the session.
Secondary LFSID	Secondary Local Form Session Identifier (LFSid). The ODAI bit in the LFSid indicates which node was assigned the values in the transmission header.
Secondary Link name	Name of the link for the secondary stage of the session.

LinkStaCHar

Syntax

```
SETDefault -APPN LinkStaCHar = <LinkStation name>
  [EffectCap=<string>] [ConnectCost=<0-255>] [ByteCost=<0-255>]
  [Security=<string>] [PropDelay=<string>] [Usd1=<0-255>]
  [Usd2=<0-255>] [Usd3=<0-255>]
SHow -APPN LinkStaCHar [LinkStation name]
```

Default No default

Description The LinkStaCHar parameter defines the characteristics of the link to an adjacent link station. The characteristics used to define adjacent link stations also determine the characteristics of transmission groups (TGs). Once the adjacent link station is activated, if you want to make any changes using this parameter or the AdjLinkSta parameter, you must first deactivate the link using the LinkStaCONTrol parameter.

CAUTION: *If you change any of the default characteristics for a link to a network node, the characteristic must also be changed on the partner network node. For example, if you set the security level of the TG as GUarded on the local node, then you must also configure the security level as GUarded on the partner node. Otherwise, the characteristic is valid in one direction only, from the local node to the partner node; the characteristic on the link in the opposite direction does not match.*

Values

<LinkStation name> Specifies the name assigned to the link by the system, or by specifying the link name with the ADD -APPN AdjLinkSta command.

EffectCap Specifies the highest bit transmission rate that the TG can obtain. Specify one of the following values: MINimum, MAXimum, 2400, 4800, 9600, 19200, 56000, 64000, 2560000, T1, 4M, 10M, 16M, 25M, 100M, or 155M. The default values are those used by the link station's TG profile. You must enter this value using one of these strings; however, these strings map to specific hex values. For information on mapping the hex values to these strings, see Table 5-10. If you have previously specified an effective capacity by assigning a TG profile to the port the link is on, the effective capacity you specify for the adjacent link station would be used, and would override the capacity specified by the TG profile.

Table 5-10 Effective Capacity Values

String	Hex Value Equivalent
MIN	0x00
2400	0x20
4800	0x28
9600	0x30
14400	0x34
19200	0x38
56000	0x43
64000	0x45
256000	0x55
T1	0x69
4M	0x75
10M	0x80
16M	0x85
25M	0x8A
100M	0x9A
155M	0x9F
MAX	0xFF

ConnectCost — Specifies the relative cost per unit time of using a TG. Valid values are from 0–255. The default is 0.

ByteCost — Specifies the relative cost per byte for using a TG. Valid values are from 0–255. The default is 0.

Security — Specifies the level of security available on the TG. Specify one of the following strings: NONsecure, PKTswtnet, UNDgndcbl, SECurcnd, GUArdcnd, ENCryptd, guardRAD, or MAX. The default values are those used by the link station's TG profile. You must enter this value using one of these strings; however, these strings map to specific hex values. For information on mapping the hex values to these strings, see Table 5-11.

Table 5-11 Security Values

String	Hex Value Equivalents
NONsecure	0x01
PKTswtnet	0x20
UNDgndcbl	0x40
SECurecnd	0x60
GUArdcnd	0x80
ENCryptd	0xA0
guardRAD	0xC0
MAX	0xC0 (for TG characteristics)
	0xFF (for COS tables)

PropDelay — Specifies the duration for a signal to propagate from one end of the TG to the other. Specify one of the following strings: MINimum, LAN, TELephone, PKTswitch, SATellite, or MAXimum. You must enter this value using one of these strings; however, these strings map to specific hex values.

For information on mapping the hex values to these strings, see Table 5-12. If you have previously specified a propagation delay by assigning a TG profile to the port the link is on, the effective capacity you specify for the adjacent link station would be used, and would override the delay specified by the TG profile.

Table 5-12 Propagation Delay Values

String	Hex Value Equivalent
MINimum	0x00
LAN	0x4C
TELephone	0x71
PKTswitch	0x91
SATellite	0x99
MAXimum	0xFF

Usd1 — Specifies the value for user-defined parameter 1. The user-defined parameters represent TG characteristics defined by the network administrator. Valid values are from 0–255. The default is 128. These values also apply to user-defined parameters 2 and 3.

Usd2 — Specifies the value for user-defined parameter 2.

Usd3 — Specifies the value for user-defined parameter 3.

Example To define the characteristics of a link named “ENGREEN1” for an effective capacity of 9600, a byte cost of 128, and a security value of SECurcnd, enter:

```
SETDefault -APPN LinkStaCHar = ENGREEN1 EffectCap=9600 ByteCost=128
Security=SECurecnd
```

You can enter the options for this parameter in any combination. You can configure one option, some options, or all of them with each command. For example, you can define the same characteristics on the link by entering the following three commands:

```
SETDefault -APPN LinkStaCHar = ENGREEN1 EffectCap=9600
SETDefault -APPN LinkStaCHar = ENGREEN1 ByteCost=128
SETDefault -APPN LinkStaCHar = ENGREEN1 Security=SECurecnd
```

LinkStaCONTrol

Syntax

```
SET -APPN LinkStaCONTrol = <LinkName> <Activate | Deactivate
  [Orderly | Immediate]>
SHow -APPN LinkStaCONTrol [linkname]
```

Default No default Description

The LinkStaCONTrol parameter dynamically activates or deactivates a specific link without taking the physical port up or down. (To take an APPN port up or down, use the PortCONTrol parameter described in this chapter.) This parameter activates and deactivates both regular adjacent link stations and DLUr link stations. To display the names of the links to any adjacent link stations, and the status of those links, use the SHow command.

This parameter uses the SET command, which means the changes you make are dynamic to that link.

Values

<LinkName>	Enters the link name assigned to the link between the network node and the adjacent node. The link name is assigned by the local network node or by assigning a link name with the AdjLinkSta or DlurLinkSta parameters. To determine which link name to use, enter the SHow -APPN LinkStaCONTrol command.
Activate | Deactivate	Enter Activate to take up a previously deactivated link to an adjacent link station. Enter Deactivate to take down a link to an adjacent link station.
Orderly | Immediate	If you specify Deactivate to take down a link, you can specify either Orderly or Immediate. If you specify Orderly, the link is deactivated when all ISR sessions are stopped. If you specify Immediate, all sessions are first stopped and then the link is deactivated.

Example 1 To deactivate a link on port 3 named “LINK002” and take the sessions down in an orderly manner, enter:

```
SET !3 -APPN LinkStaCONTrol = LINK002 Deactivate Orderly
```

When you activate or deactivate a link to an adjacent link station (and the link supports CP-CP sessions), you receive messages similar to the following two messages on the console indicating that the CP-CP session has been activated or deactivated:

```
CONLOSER CP-CP SESSION WITH US3COMHQ.GOLD IS UP
CONWINNER CP-CP SESSION WITH US3COMHQ.GOLD IS UP
```

If deactivating a link to an adjacent link station, the link will be deactivated until you reactivate it.

Example 2 To reactivate a link to an adjacent link station you previously deactivated, use:

```
SET !<port> -APPN LinkStaCONTrol
```

Specify the Activate value. For example, to reactivate the link to link station “LINK002” deactivated in Example 1, enter:

```
SET !3 -APPN LinkStaCONTrol = LINK002 Activate
```

If you try to activate or deactivate a link over an APPN port that is not active, you will receive the following warning:

```
WARNING: Port is not active.  Use set !<port> -appn PortCONTrol =
  Activate
```

Example 3 The following is an example of the display obtained using the SHow LinkStaCONTrol command. The display shows adjacent link stations, DLUr link stations, and link stations learned from remote sites. Table 5-13 describes the meanings of the headings and status messages included in the display.

```
=================== SHow -APPN LinkStaCONTrol ===================
-------------Current Defined Link Stations and Status-------------
Port     LinkName    AdjCPName        Type     #Sess    LinkStatus
!1       @I000001    US3COMHQ.COM20E  NN       4        ACTIVE
!1       LINK0000    US3COMHQ.IBM4    NN       4        ACTIVE
!1       LINK0064                              0        INACTIVE
```

Table 5-13 LinkStaCONTrol Display Meanings

Display Heading	Meaning
Port	Port on the local network node the link is on.
LinkName	Name assigned to the link by the local network node or by assigning a link name using the AdjLinkSta parameter. If the name includes the @ character, this indicates an incoming link station that is not locally defined.
AdjCPName	Adjacent control point at the other end of the link.
Type	Node type of the adjacent control point, either NN or EN.
#Sess	Number of CP-CP sessions between the local node and the adjacent control point. If there are no CP-CP sessions between the local node and adjacent control point, that does not mean the link is inactive. The link may still be active without CP-CP sessions.
LinkStatus	Status of the link. Inactive means the link is inactive. Active means the link is active. PEND_ACTIVE means the link is in the process of coming up while PEND_INACTIVE means the link is in the process of going down.

LocalNodeName

Syntax

```
SETDefault -APPN LocalNodeName = <netid.cpname> [node_id]
SHow -APPN LocalNodeName
```

Default No default

Description The LocalNodeName parameter defines the local node name assigned to the node. The local node name plus network ID creates the full control point (CP) name.

Values <netid.cpname> Specifies the <netid>, the unique network identifier used to identify the network node throughout the APPN network. The ID can be up to eight characters in length, and valid characters are A–Z, 0-9, $,@, #. The field cannot start with a number. You must enter a period and no space between the <netid> and the <cpname>.

The <cpname> is the unique local node name assigned to the node, also known as the nonqualified CP name. The network ID plus this CP name creates the fully qualified CP name. The ID can be up to eight characters in length, and valid characters are A–Z, 0–9, $,@, #. The field cannot start with a number.

node_id	Specifies the local node ID number that consists of the lower 20 bits. This identification is used in the XID when link station negotiation takes place. When two nodes are negotiating a link station, the node with the higher value for the XID will be the primary link station. This value also is used for LEN end nodes, which use this value instead of the CP name during link activation. The node ID is also used to identify the node for NetVIEW alerts. The field requires a five-digit hexadecimal value, and the default is 0. This value is optional. The node ID is the IDNUM of the SNA node ID format BLKID/IDNUM. The BLKID used is the block number assigned to 3Com. The block number assigned to 3Com is "E06." You do not need to configure the 3Com block number on the NETBuilder bridge/router, but you may need it for configuring other systems to communicate with the NETBuilder bridge/router.

LocalNodeResist

Syntax

```
SETDefault -APPN LocalNodeResist = <node_resistance> (0–255)
SHow -APPN LocalNodeResist
```

Default 128

Description The LocalNodeResist parameter determines how the local node advertises the desirability of routing (resistance) through the node. A value of 0 indicates to the network that routing is highly desirable, while 255 indicates that it is not.

Mode

Syntax

```
SHow -APPN Mode [mode_name]
```

Default No default

Description The Mode parameter displays the mapping of modes to class of service names for all modes, including default IBM modes.

ModetoCosMap

Syntax

```
ADD -APPN ModetoCosMap <cos_name> <mode_name> [mode_name ...]
DELete -APPN ModetoCosMap <cos_name> <mode_name> [mode_name ...]
SHow -APPN ModetoCosMap [<cos_name>]
```

Default No default

Description The ModetoCosMap parameter adds or deletes a list of mode names associated with a given COS name. You can specify up to four mode names for each add or delete command, and you can enter the command multiple times for the same COS name.

Values

<cos_name>	Enters the COS name to which you add or delete mode names.
<mode_name>	Enters the mode name you add to a COS name or delete from a COS name. You can enter up to four mode names for each command. The mode name must be eight characters or less.

NNtopology

Syntax `SHow -APPN NNtopology`

Default No default

Description The NNtopology parameter displays topology information for the network nodes on your network that are directly reachable from the network node. The display shows basic information about the nodes such as the node name, node type, and the number of transmission groups the node owns.

The SHow -APPN NNtopology command displays the following information:

```
================== SHow -APPN NNtopology ======================
----------------------Network Node-----------------------------
 Node name       Type   RAR  Status       Function support  RSN
US3COMHQ.CN5     VRN    128  UNCONGESTED  ISR               0
US3COMHQ.CN7     VRN    128  UNCONGESTED  ISR               0
US3COMHQ.CUBE    NN     128  UNCONGESTED  ISR               2
US3COMHQ.IBM4    NN     128  UNCONGESTED  ISR               2
US3COMHQ.COM20E  NN     128  UNCONGESTED  ISR               2
```

Table 5-14 explains the meanings of the NNtopology display.

Table 5-14 NNTopology Display Meanings

Display Heading	Meaning
Node name	Network node name.
Type	Indicates whether the network node is real or virtual (used for connection networks).
RAR	Route Addition Resistance, or desirability of routing associated with the network node.
Status	Indicates whether the network node was congested the last time the node was checked.
Function support	Type of function the node is performing. ISR indicates the node is performing Intermediate Session Routing. CDR indicates the node is a Central Directory Server. BORDER indicates the node is performing the border node function. HPR indicates the node is HPR-capable (but not RTP-capable). RTP indicates the node is RTP-capable (note that even though the node is RTP-capable, it may not be performing RTP at the time).
RSN	Resource Sequence Number for the node. Indicates how up-to-date the information regarding the node is. The higher the RSN number is, the more up-to-date the information.

PortCHar

Syntax

```
SETDefault !<port> -APPN PortCHar = [EffectCap=<string>]
  [ConnectCost=<0-255>] [ByteCost=<0-255>] [Security=<string>]
  [PropDelay=<string>] [Usd1=<0-255>] [Usd2=<0-255>] [Usd3=<0-255>]
SHow [!<port>] -APPN PortCHar
```

Default No default

Description The PortCHar parameter defines TG characteristics for a port. You can specify any value you want to change; any value not specified is not changed. Once the APPN port is activated, if you want to make any configuration changes using this parameter or the PortDef parameter, you must first deactivate the port using the PortCONTrol parameter.

Values

EffectCap — Specifies the highest bit transmission rate that the TG can obtain. Specify one of the following values: MINimum, MAXimum, 2400, 4800, 9600, 19200, 56000, 64000, 2560000, T1, 4M, 10M, 16M, 25M, 100M, or 155M. You must enter this value using one of these strings; however, these strings map to specific hex values. For information on mapping the hex values to these strings, see Table 5-10 on page 5-24.

ConnectCost — Specifies the relative cost per unit time of using a TG. Valid values are from 0–255. The default is 0.

ByteCost — Specifies the relative cost per byte for using a TG. Valid values are from 0–255. The default is 0.

Security — Specifies the level of security available on the TG. Specify one of the following strings: NONsecure, PKTswtnet, UNDgndcbl, SECurcnd, GUArdcnd, ENCryptd, guardRAD, or MAX. The default is NONsecure. You must enter this value using one of these strings; however, these strings map to specific hex values. For information on mapping the hex values to these strings, see Table 5-11 on page 5-24.

PropDelay — Specifies the length of time in microseconds for a signal to propagate from one end of the TG to the other. Specify one of the following strings: MINimum, LAN, TELephone, PKTswitch, SATellite, or MAXimum. You must enter this value using one of these strings; however, these strings map to specific hex values. For information on mapping the hex values to these strings, see Table 5-12 on page 5-25.

Usd1 — Specifies the value for user-defined parameter 1. The user-defined parameters represent TG characteristics defined by the network administrator. Valid values are from 0–255. The default is 128. These values also apply to user-defined parameters 2 and 3.

Usd2 — Specifies the value for user-defined parameter 2.

Usd3 — Specifies the value for user-defined parameter 3.

PortCONTrol

Syntax

```
SET !<port> -APPN PortCONTrol = (<Activate [NoLinkStations] |
  Deactivate [Orderly | Immediate]>)
SHow -APPN PortCONTrol
```

Default No default

Description The PortCONTrol parameter dynamically activates or deactivates a port being used for APPN traffic. When you take the APPN port down, you also automatically take down all the link stations on that port, and when you reactivate the port, you automatically reactivate the link stations on that port. By specifying the Nolinkstations value, you can activate the port without affecting the link stations. To activate or deactivate specific link stations on a port, use the LinkStaCONTrol parameter.

This parameter uses the SET command, which means the changes you make are dynamic to that port.

The SHow command displays the current status of active and inactive APPN ports.

Values

Activate | Deactivate
: Use Activate to take the APPN port up and Deactivate to take the APPN port down.

NoLinkStations
: Specifies whether link stations should be automatically activated. When you activate the port specify NoLinkStations to prevent any auto start link stations on the port from being activated when the port is activated. The NoLinkStations option applies only when you activate ports, and only to link stations set with the AutoStart=Yes setting for the AdjLinkSta parameter.

Orderly | Immediate
: Specifies how to deactivate linkstations. If you specify Deactivate to take down a port, you can specify either Orderly or Immediate. If you specify Orderly, the bridge/router waits for all LLC2 sessions on the port to terminate before deactivating the port. If you specify Immediate, all sessions are first terminated, then all LLC2 sessions are terminated, and finally the port is deactivated. If you do not specify either, then an Immediate deactivation takes place.

PortDef

Syntax

```
SETDefault !<port> -APPN PortDef = <DLC type>
  (LLC2|FR|PPP|DLSW|SDLC|UNdef) <max_btu_size>(99-8192)
  [ActLimit=<limit>(1-512)] [TGprof=<name>] [HPR=(Yes|No)]
  [ErrorRecovery=(Yes|No)] [DatMode=(Half|Full)]
  [ROle=(Neg|Pri|Sec)]
SHow [!<port>] -APPN PortDef
```

Default No default

Description The PortDef parameter defines the characteristics of the local APPN port, including the type of communications used, the maximum basic transmission unit (BTU) size, and optionally, the activation limit and TG profile. After the APPN port is activated, if you want to make any configuration changes using this parameter or the PortCHar parameter, you must first deactivate the port using the PortCONTrol parameter. Re-enabling the CONTrol parameter in the PORT Service does not change the configuration. Without re-enabling the APPN CONTrol or APPN PortCONTrol parameters, the link on the port whose definition was modified is not activated. This parameter does not support virtual ports.

Values

<DLC type>
: Selects the data link control communication type that is used on the port. Enter SDLC for synchronous data link control traffic. Enter LLC2 for token ring, Ethernet, and FDDI. Enter FR for Frame Relay, PPP for Point-to-Point links, or DLSw for using Data Link Switching over an IP network. If you specify the DLC type as DLSw, the port number specified must be !0. Do not specify !0 if using a DLC type other than DLSw. To remove a port definition entry, enter UNdef.

If a port has been previously defined for a particular DLC type, you need to remove the port definition entry using UNdef before specifying the new DLC type.

If you specify the DLC type as SDLC, then use the SdlcAdjLinkSta parameter or the SdlcDlurLinkSta parameter to add adjacent link stations or DLUr link stations to the port.

<max_btu_size>
Enters the maximum number of bytes in a BTU that can be received on the port. The acceptable range is 99–8192. To determine the maximum BTU size to use, first you determine the appropriate request/response unit (RU) size, then add an additional nine bytes (three bytes for the request header (RH) plus six bytes for transmission header). The RU size plus the additional nine bytes comprise the BTU size. For optimal buffer utilization, the recommended maximum BTU size for Ethernet and if bridging LLC2 over serial lines using source route transparent (SRT) bridging is 1,500. For token ring and all other media, including bridging over serial lines using source route (SR) bridging, the recommended maximum is 5,005.

ActLimit
Specifies the activation limit, or the number of LLC2 sessions allowed on the port. The valid range for all DLC types other than SDLC is 1-512. The default value is 32.

If you specify the DLC type as SDLC, then this value is valid only if ROle is set to Primary. The valid range for SDLC ports is 1-254. If the SDLC port ROle is Secondary or Negotiable, then the activation limit is set to 1 internally.

TGprof
Specifies the TG profile assigned to the port. The TG profile is a set of default values that apply to the port if chosen. When a TG profile is specified, the proper capacity and propagation delay values is assigned to the port based on the link speed of the media. If a TG profile for the port is not specified, then the system automatically uses a profile matching the port baud rate. If the port is not active and the baud rate is unknown, then the system defaults to the Ser64 profile. For a list of TG profiles, see Table 5-2 on page 5-5.

HPR
Specifies whether HPR is supported on the port. If you specify "Yes," HPR can take place over the port. If you specify "No," HPR is not supported on the port and Intermediate Session Routing (ISR) is used. Using this option, you can have some ports supporting HPR and other ports supporting ISR at the same time. The default is Yes.

ErrorRecovery
For HPR links only, specifies if link level error recovery is used on this port for an *incoming* connection. If you specify "Yes," error recovery is preferred on the port, but it can be negotiated down. If you specify "No," error recovery is not supported on the port. If you want link level error recovery for the *outgoing* connection, then you must set the ErrorRecovery value for the AdjLinkSta parameter (see page 5-3). The default is Yes if the DLC type is set to DLSw or SDLC (SDLC requires error recovery; do not change it to No). The default is No if the DLC type is set to LLC2, FR, or PPP. If you use link level error recovery, this creates additional overhead on your links. This value is only valid if the HPR value is set to "Yes."

DatMode
Specifies the data transmission mode of the port to half duplex or full duplex. This value applies to the port and all link stations on that port. Set this value to match the capabilities of the attached device. The de- fault is half duplex. This value is only valid if you set the DLC type to SDLC.

Some IBM and SNA documents refer to half duplex as “two-way alternate,” and full duplex as “two-way simultaneous.”

ROle
Specifies whether the role of the SDLC port is primary or secondary, or whether the role is negotiable (Neg). The default is Neg. This value is only valid if you set the DLC type to SDLC

QueuePriority

Syntax

```
SETDefault -APPN QueuePriority = <H|M|L|DEFault>
SHOw -APPN QueuePriority
```

Default Medium

Description The QueuePriority parameter assigns a priority to an APPN-routed packet destined for a wide area network using PPP, PLG, Frame Relay, or SMDS. Possible priorities include high, medium, or low. If this parameter is set to default, the system uses the setting of the -PORT DefaultPriority parameter. For more information on the -PORT DefaultPriority parameter, refer to Chapter 43. For more information on data prioritization, refer to Chapter 41 in *Using NETBuilder Family Software*.

You can display the setting of this parameter by entering the SHow -APPN QueuePriority command.

RTP

Syntax

```
SHow -APPN RTP [name]
```

Default No default

Description The RTP parameter displays RTP connections. If you do not specify a name, then all RTP connections are displayed.

The following is an example of the display obtained by entering the SHow -APPN RTP command:

```
==================================== SHow -APPN RTP ===================================

Name          Link        Dest                COS     BTU     #SESS     ALIVE(val,t_out)

1. 3C000001   LINK001     US3COMHQ.CUBE       #INTER  1033    2         180     4
(US3COMHQ.IBM4 - GOLD - SILVER - CUBE)
2. 3C000003   LINK0001    US3COMHQ.PEBBLE     3INTER  1033    4         180     6
(US3COMHQ.IBM4 - GOLD - SILVER - CUBE - PEBBLE)
```

The first line of the display shows specific information for the RTP connection. The second line of the display shows the Route Selection Control Vector (RSCV) list of the RTP path. For the first entry, the RSCV list contains the network name in addition to the node name. For subsequent nodes in the path, if the node belongs in the same network as the preceding node, the network name is not displayed.

Table 5-15 explains the meanings of the RTPStats display.

Table 5-15 RTP Display Meanings

Display Heading	Meaning
Name	The RTP connection name.
Link	The first hop link name
Dest	The destination node name
COS	The class of service name.
BTU	The maximum BTU size.
#Sess	The number of active sessions.
ALIVE (val,t_out)	Values for the ALIVE timer. The first number, val, indicates the ALIVE timer setting (in seconds) for the RTP connection. The second number, t_out, indicates the number of timeouts, or the number of times the ALIVE timer expired, on the RTP connection.

RTPStats

Syntax `SHow -APPN RTPStats [name]`

Default No default

Description The RTPStats parameter displays statistics for RTP connections. If you do not specify a name, then statistics for all RTP connections are displayed.

The following is an example of the display obtained by entering the SHow -APPN RTPStats command:

```
================================= SHow -APPN RTPStats =============================

Name            Up_time   Pkt_sent    S_rate (max,now,min) out_SC  Round_trip
RTP Partner               Pkt_rcvd    R_rate (max,now,min) in_SC   Retx        Gap
1. 3C000001     22:31:53  460         983 983 491          1       209
US3COMHQ.IBM7             456         356 356 356          0       0           0
2. 3C000002     22:31:52  469         983 983 491          1       140
US3COMHQ.IBM7             461         754 744 744          0       0           0
```

Table 5-16 explains the meanings of the RTPStats display.

Table 5-16 RTPStats Display Meanings

Display Heading	Meaning
Name	The RTP connection name.
RTP Partner	The RTP connection partner.
Up_time	The up time or the total duration that the RTP connection is active.
Pkt_sent	The number of packets sent on the RTP connection.
Pkt_rcvd	The number of packets received on the RTP connection.
S_rate	The send rate (in kbps) on the RTP connection. The first number is the maximum send rate, the second number is the current send rate, and the third number is the minimum send rate.
R_rate	The receive rate (in kbps) on the RTP connection. The first number is the maximum receive rate, the second number is the current receive rate, and the third number is the minimum receive rate.
out_sc	The number of session control frames sent on the RTP connection.
in_sc	The number of session control frames received on the RTP connection.

(continued)

Table 5-16 RTPStats Display Meanings (continued)

Display Heading	Meaning
Round_trip	The round trip time between RTP endpoints (in milliseconds). The first number is the smoothed, or average, round-trip time. The second number is the last measured round-trip time.
Retx	The number of packets resent because of a loss in transit.
Gap	The total number of gaps (indicating lost frames) detected.

SdlcAdjLinkSta

Syntax

```
ADD !<port> -APPN SdlcAdjLinkSta <type>(NN|EN|Learn)
  <max_btu_size>(99-8912) <station addr>(Hex 1-FE)
  [CPName=<[netid.]cpname] [Nodeid=<ID>] [LinkName=<name>]
  [TGprof=<name>] [AutoStart=(Yes|No)] [CPSess=(Yes|No)]
  [HPR=(Yes|No)] [ErrorRecovery=(Yes|No)] [SendWindow=<num>]
  [ContactTimer=<num>] [NoRspTimer=<num>]
  [NoRspTimRetry=<num>]
DElete !<port> -APPN SdlcAdjLinkSta <LinkName>
SHow [!<port>] -APPN SdlcAdjLinkSta [LinkName]
```

Default No default

Description The SdlcAdjLinkSta parameter defines for SDLC traffic an adjacent link station as a destination and defines the type of node being linked to, the destination station address, and the node name associated with the link station. To send and receive SDLC traffic from an adjacent SDLC node, both partner nodes must configure each other as SDLC adjacent link stations using the SdlcAdjLinkSta parameter.

After the SDLC adjacent link station is activated, if the APPN node is active and you want to make any configuration changes using this parameter or the LinkStaCHar parameter, you must first deactivate the link using the LinkStaCONTrol parameter. If the APPN node is not active, you do not need to deactivate the link.

APPN over SDLC connections is supported on all types of HSS-3 Port Modules, including V.35, RS-232, and RS-449.

Values

NN|EN|Learn	Specifies whether the destination is a network node (NN) or an end node (EN). Specify Learn if you do not know the node type and all you know is the node's media address; if you specify Learn, do not specify a CP name.
<max_btu_size>	Enters the maximum number of bytes in a basic transmission unit (BTU) that can be sent to this destination. The acceptable range for network nodes is 99 to 8,912, while the acceptable range for end nodes is 256 to 8,912. If you set the type to Learn, do not set the value to less than 256, since you do not know if the node is a network node or an end node. If the learned node is an end node and you set the value to less than 256, the link may not come up.
<station addr>	Specifies the station address (or polling address) of the adjacent link station. Valid address values are Hex 01 through Hex FE.

CPName

Enters the control point name of the adjacent link station. If the net ID is different than the net ID of the local node specified using the LocalNodeName parameter, you can specify the net ID. If you enter the net ID, you must type a period immediately following it, then type the CP name immediately following the period to create the fully qualified CP name. The CP name can be up to eight characters in length, and valid characters are A–Z, 0–9, $, @, #. The name cannot start with a number, a space or a period. This value is optional.

Nodeid

Enters the eight-digit hex identification that is used to identify the node. This value is optional. The node ID corresponds to the IDNUM of the IBM node ID format IDBLK/IDNUM.

<LinkName>

Specifies the name assigned to the link. All link names must be unique on the local network node. For example, you cannot use the same link name on more than one port, and you cannot use the same link name for two types of links (such as for adjacent link stations or DLUr link stations) at the same time. The link name is limited to eight characters, and cannot start with special characters. If no link name is specified, the system will assign a link name LINKXXXX where XXXX is a number between 0001 and 9999.

TGprof

Specifies the TG profile assigned to the link station. The TG profile is a set of default values that apply to the link if chosen. When a TG profile is chosen, the proper effective capacity and propagation delay values are assigned to the link station based on the link speed of the media. If no profile for the link station is specified, then the profile specified for the port using the PortDef parameter is used; if no TG profile for the port is specified, then the system automatically picks a profile corresponding to the port’s baud rate.

If the port is not active and the baud rate is unknown, then the system defaults to the Ser64 profile. For a list of valid TG profile values, see Table 5-2 on page 5-5.

AutoStart

If you specify Yes, the link is automatically activated when the local network node is enabled, and is restarted automatically if the link stops. If you specify No, the link is not automatically started and you have to activate the link by entering SET -APPN LinkStaCONTrol. The default value is Yes. In the SHow -APPN SdlcAdjLinkSta display, AutoStart support is shown in the “A” column.

CPSess

Specifies whether CP-CP sessions will be activated with the adjacent node. If you specify Yes, CP-CP sessions are activated with the node, and if you specify No, they are not activated. The default value is No if the adjacent node type is a network node, and Yes if the adjacent node type is an end node or the node type is set to LEARN. In the SHow -APPN SdlcAdjLinkSta display, CP-CP session support is shown in the “CP” column.

HPR	Specifies if the link station supports HPR on this link. If you specify Yes, then HPR is supported on the link between the local node and the adjacent link station. If you specify No, HPR is not supported. The default is Yes, meaning HPR is supported by default, so if you want the SDLC adjacent link station to support only ISR, you must specify No.
ErrorRecovery	For HPR links only, specifies if link level error recovery is used for an *outgoing* connection on the link. If you specify Yes, error recovery is preferred, but can be negotiated down. If you specify No, error recovery for HPR does not take place. If you want link level error recovery for the *incoming* connection, then you must set the ErrorRecovery value for the PortDef parameter (see page 5-31). If you use link level error recovery, additional overhead occurs on your links. This value is only valid if the HPR value is set to Yes.
SendWindow	Specifies the send window size (in number of frames). The valid range is from 1 to 12. The default is 4. The receive window size is always 7 if the send window size is less than or equal to 7; in this case, the normal sequence numbering (Modulo 8) is used. The receive window size is always 12 if the send window size is greater than 7 but less than 12; in this case, the extended sequence numbering (Modulo 128) is used.
ContactTimer	Specifies the number of seconds to wait between attempts to contact a failed or newly activated adjacent link station. The valid range is from 0 to 300 seconds. The default is 1 second. This value is valid on primary ports only.
NoRspTimer	Also known as the T1 timer, this value specifies the no-response time-out in milliseconds for the SDLC port on the bridge/router. If the link station does not receive a response to a poll or message before this timer expires, then the transmission is retried until the retry count is exhausted. The valid range is from 0 to 10,000 milliseconds. The default is 1000 milliseconds. This value is valid on primary ports only.
NoRspTimRetry	Specifies the number of times the bridge/router attempts to complete a protocol exchange with a connected device before stopping the attempts. The valid range is from 1 to 25. The default is 3. This value is valid on primary ports only.

SdlcDlurLinkSta

Syntax

```
ADD !<port> -APPN SdlcDlurLinkSta <max_btu_size>(265-8912)
   <station addr>(Hex 1-FE) <dspu name> [Nodeid=<ID>]
   [LinkName=<name>] [Dlus=[netid.]name] [Backup=[netid.]name]
   [TGprof=<name>] [AutoStart=(Yes|No)] [PU2=(Yes|No)]
   [HPR=(Yes|No)] [CPSess=(Yes|No)] [SendWindow=<num>]
   [ContactTimer=<num>] [NoRspTimer=<num>]
   [NoRspTimRetry=<num>]
DElete !<port> -APPN SdlcDlurLinkSta <LinkName>
SHow [!<port>] -APPN SdlcDlurLinkSta [LinkName]
```

Default No default

Description The SdlcDlurLinkSta parameter specifies for SDLC traffic a link station for downstream DLUr nodes. Using the ADD command, you specify a DLUr link station for a port, including the DLUr's station address and downstream physical unit name (DSPU).

APPN over SDLC connections is supported on all types of HSS-3 Port Modules, including V.35, RS-232, and RS-449.

Values

<max_btu_size>	Specifies the maximum BTU size for the DLUr link station. The value range is 256-8912.
<station addr>	Specifies the station address (or polling address) of the DLUr link station. Enter the address in hex.
<dspu name>	Specifies the downstream physical unit (DSPU) name. If the host activates the session with the DLUr link station, then the DSPU name you configure here must match the name on the host configuration.
Nodeid	Specifies the node ID that is checked by the XID. The node ID must be entered in hex and must include all eight hex digits. A node ID of 0x00000000 means that the Node ID will not be checked.
<LinkName>	Specifies the name assigned to the link. All link names must be unique on the local network node. For example, you cannot use the same link name on more than one port, and you cannot use the same link name for two types of links (such as for adjacent link stations or DLUr link stations) at the same time. The link name is limited to eight characters, and cannot start with special characters. If no link name is specified, the system assigns a link name LINKXXXX where XXXX is a number between 0001 and 9999. When deleting a DLUr link station, you must specify the link name.
Dlus	Specifies the primary DLUs name used by this DLUr link station. If no primary DLUs is specified, then the DLUs configured with the DlurDefaults parameter are used.
Backup	Specifies the backup DLUs name used by this DLUr link station. If no backup DLUs is specified, then the backup DLUs configured with the DlurDefaults parameter are used.
Tgprof	Specifies the TG profile assigned to the DLUr link station. The TG profile is a set of default values that apply to the link if chosen. When a TG profile is specified, the proper effective capacity and propagation delay values will be assigned to the link station based on the link speed of the media. For a list of TG profiles, see Table 5-2 on page 5-5.
AutoStart	If you specify Yes, the link is automatically activated when the local network node is enabled, and is restarted automatically if the link stops. If you specify No, the link is not automatically started and you have to activate the link by entering SET -APPN LinkStaCONTrol. The default value is Yes.

PU2 Specifies whether the link station is a PU 2.0 node or a PU 2.1 node. If you specify Yes, the link will support communication to PU 2.0 nodes but will support DLUr services only (and not APPN services). If you specify No, the link will support communication to PU 2.1 nodes and can support both APPN and DLUr over the same link. The default is No.

If you specify Yes, the link can be activated by the host. If you specify No, the link cannot be activated by the host. Specify Yes if the downstream node does not support APPN, or you do not want APPN services from the local network node.

HPR Specifies if the link station supports HPR on this link. If you specify Yes, then HPR is supported on the link between the local node and the adjacent link station. If you specify No, HPR is not supported. The default is Yes, meaning HPR is supported by default, so if you want the SDLC DLUr link station to support only ISR, you must specify No.

CPSess Specifies whether CP-CP sessions are activated with the adjacent node. If you specify Yes, CP-CP sessions are activated with the node, and if you specify No, they are not activated. The default value is No if the adjacent node type is a network node, and Yes if the adjacent node type is an end node or the node type is set to LEARN.

SendWindow Specifies the send window size in number of frames. The valid range is from 1 to 12. The default is 4.

The receive window size is always 7 if the send window size is less than or equal to 7; in this case, the normal sequence numbering (Modulo 8) is used. The receive window size is always 12 if the send window size is greater than 7 but less than 12; in this case, the extended sequence numbering (Modulo 128) is used.

ContactTimer Specifies the number of seconds to wait between attempts to contact a failed or newly activated adjacent link station. The default is 1 second. This value is valid on primary ports only.

NoRspTimer Also known as the T1 timer, this value specifies the no-response time-out in milliseconds for the SDLC port on the bridge/router. If the link station does not receive a response to a poll or message before this timer expires, then the transmission is retried until the retry count is exhausted. The default is 1,000 milliseconds. This value is valid on primary ports only.

NoRspTimRetry Specifies the number of times the bridge/router attempts to complete a protocol exchange with a connected device before stopping the attempts. The default is 3. This value is valid on primary ports only.

TG

Syntax `SHow -APPN TG [<node name> | ALL]`

Default No default

Description The TG parameter displays all information in the transmission group (TG) topology database. If the network node specified does not own any TG, then a message indicates that no transmission group is defined for the specified node.

This display may include TGs that no longer exist which have not been removed from the database. For a list of active connections only, enter SHow -APPN CONNection.

Values <node name> | ALL Enters the specific network node name to display transmission group information for that network node only. Enter ALL to display TG information for all network nodes.

When entering a node name, you can enter either a fully qualified name (such as US3COMHQ.NB2BLUE), or a name that is not qualified (such as NB2BLUE).

If no value is specified, then all transmission groups owned by this node are displayed.

Example To display the transmission group information for a network node called US3COMHQ.CN7, enter:

`SHow -APPN TG US3COMHQ.CN7`

A display similar to the following appears:

```
========================= SHow -APPN TG =========================
------------------Network Node Transmission Group-----------------
Owning node name (type) = US3COMHQ.CN7       (VRN)
TG partner CP name (type) = US3COMHQ.CUBE      (NN)
TG number = 1
Days left before deletion = 15
RSN = 2
TG Status = OPERATIVE
Effective Capacity = 56000
Cost per connect time = 68
Cost per byte = 68
Propagation Delay = 68
User defined parameter 1 = 68
User defined parameter 2 = 68
User defined parameter 3 = 68
```

This example shows only one TG. If you enter the command without specifying a network node, then the display will show all TGs.

Table 5-17 explains the headings in the transmission group display.

Table 5-17 Transmission Group Display Meanings

Display Heading	Meaning
Owning Node name (type)	Name of the node (and node type) to which the transmission group belongs.
TG partner CP name	Control point name assigned to the network node's transmission group partner. The network node's transmission group partner is the end node.
TG number	Number assigned to the transmission group. If you have parallel TGs between two nodes, one TG would be designated 1 and the other 2; also, with parallel TGs, one TG could be up while the other could be down.
Days left before deletion	Number of days left before the entry will be deleted from the TG database. APPN deletes the information after 15 days. If the value shown is 15, then the entry is new; the lower the value, the older the entry.
RSN	Resource Sequence Number. This indicates how up-to-date the information regarding the TG is. The higher the RSN number is, the more up-to-date the information.
TG Status	State of the TG. Possible states include Operative, Inoperative, or Quiescing. Quiescing indicates the TG is in the process of shutting down. All of the status messages also indicate whether there is or is not CP-CP sessions over the TG.
Effective Capacity	The effective link speed and throughput the link on the transmission group can handle without getting overloaded. The number shown is rounded, so the capacity displayed may not be exactly the amount entered at configuration.
Cost per byte	Relative cost per byte for the link.
Security	Level of security for the transmission group.
Propagation delay	Time in microseconds for a signal to propagate from one end of the transmission group to another.
User defined parameter 1, 2, 3	Values assigned to the user-defined parameters.

TreeCache

Syntax `SHow -APPN TreeCache [COS name]`

Default No default

Description The TreeCache parameter displays the Topology and Route Selection tree cache for different classes of service. If you do not specify a COS name, the display shows all the SNA-defined COS tree caches.

The following is an example of the display obtained using the SHow -APPN TreeCache:

```
-----------------------Network Node Tree Cache-------------------
Cached tree for COS #INTER ..
(0) node = US3COMHQ.CUBE      (total wt = 60)
  (1) node = US3COMHQ.CN5       (total_wt = 90)
    (2) node = US3COMHQ.SPHERE    (total_wt = 180)
  (1) node = US3COMHQ.IBM4      (total_wt = 150)
```

The display shows the information regarding the route for the specific COS. The "total_wt" shown is the weight of the route to the corresponding node, including the weight of the node itself. The nodes are displayed in the order they are traversed on the route to the destination node.

Because the tree cache may not be cached if there is an ongoing session using a specific COS, you can force a tree cache calculation by performing an

APpnPING to itself (the local node). For example, to obtain the tree cache for the COS #BATCH on local node US3COMHQ.LOCAL, enter:

```
ApnPING US3COMHQ.LOCAL Mode=#batch
```

After performing the ApnPING, display the tree cache for the COS #BATCH by entering:

```
SHow -APPN TreeCache #BATCH
```

6

ARP SERVICE PARAMETERS

This chapter describes the Address Resolution Protocol (ARP) Service parameters. The ARP Service is related to the following services: FR, IP, OSPF, RIPIP, and TCP.

Table 6-1 lists the ARP service parameters and commands.

Table 6-1 ARP Service Parameters and Commands

Parameters	Commands
CONFiguration	SHow
CONTrol	SETDefault, SHow
HoldTime	SETDefault, SHow
OverBlocked	SETDefault, SHow
RarpClientState	SHow
RarpCONTrol	SETDefault, SHow
RequestFormat	SETDefault, SHow

CONFiguration

Syntax

```
SHow [!<port> | !*] -ARP CONFiguration
```

Default No default

Description The CONFiguration parameter displays the ARP parameter values for the specified port.

CONTrol

Syntax

```
SETDefault !<port> -ARP CONTrol = ([Proxy | NoProxy], [InArp |
   NoInArp])
SHow [!<port> | !*] -ARP CONTrol
```

Default NoProxy, InArp

Description The CONTrol parameter determines whether an ARP proxy is used on the specified port. When the Local Management Interface (LMI) value is enabled in the Frame Relay Service, the CONTrol parameter also determines when the ARP Service automatically discovers an IP address for the data link connection identifier (DLCI).

Values

Proxy	Sets ARP to respond to proxy requests with the media access control (MAC) (Ethernet) address of the router’s interface on which the request came. This situation occurs only if the target network or subnet is in the IP Routing Table.
NoProxy	Sets ARP to ignore the proxy request.

InArp Sets ARP to automatically discover IP addresses for the DLCI over a Frame Relay network.

NoInArp Sets ARP to not discover IP protocol addresses for the DLCI over a Frame Relay network.

HoldTime

Syntax

```
SETDefault !<port> -ARP HoldTime = <hours>(1–24)
SHow [!<port> | !*] -ARP HoldTime
```

Default 24

Description The HoldTime parameter determines the amount of time (in hours) an entry can stay in the ARP Table. When the specified time elapses, the entry is deleted. When one-sixteenth of the time elapses, ARP considers this entry to be aged.

If a packet is destined for an address that has become aged, the router sends an ARP request, using a unicast address, to the destination to verify whether it is still operational.

OverBlocked

Syntax

```
SETDefault -ARP OverBlocked = [OFF | ON]
SHow -ARP OverBlocked
```

Default OFF

Description The OverBlocked parameter sends ARP requests and responses over ports that are in a nonforwarding state in !0 mode. The OverBlocked values take effect for NoInARP only; they have no relationship to InARP operation.

Values

ON Sends ARP requests and responses over ports that are in a nonforwarding state in !0 mode.

OFF Does not send ARP requests and responses over ports that are in a nonforwarding state in !0 mode.

RarpClientState

Syntax

```
SHow -ARP RarpClientState
```

Default Idle

Description The RarpClientState parameter indicates whether the RARP client is idle, waiting for an RARP reply, or waiting for an ICMP reply. If the client is waiting for an RARP reply, the display also states the number of RARP requests it has transmitted. Possible responses to the SHow -ARP RarpClientState are “Idle,” “Awaiting for Rarp reply (<number of transmissions>),” and “Awaiting for ICMP subnet reply.”

RarpCONTrol

Syntax

```
SETDefault -ARP RarpCONTrol = ([RarpClient | NoRarpClient],
   [RarpServer | NoRarpServer])
SHow -ARP RarpCONTrol
```

Default NoRarpClient, NoRarpServer

Description The RarpCONTrol parameter enables or disables the RARP client and server.

The Reverse ARP (RARP) protocol allows a diskless machine or a machine without a configured IP address to obtain an IP address from a server. The machine without an IP address is called the *RARP client*; the responding server is called the *RARP server*.

Both ARP and RARP use the same IP address translation table for the server. You can add RARP entries to the IP Address Translation Table by using the -IP ADDRess parameter. For more information, refer to Chapter 29.

Rarp Client When the system is configured as the RARP client and the line comes up, the system initiates an RARP request only:

- When routing is disabled, or
- When the RARP client option is enabled, and its IP configuration file does not contain an IP address.

Retransmissions of the request occur until one of the previous three conditions fail or a RARP response is received from the RARP server. The RARP client saves only one RARP response and discards any duplicate responses. The IP address is saved in port 0 mode in the routing table. The address is never saved in the IP configuration file. Before accepting a response, the RARP client verifies that no IP address has been assigned to the IP configuration file.

After receiving an IP address, the RARP client initiates an Internet Control Message Protocol (ICMP) Address Mask request to the RARP server to obtain the subnet mask. If no ICMP response is received, the client continues sending the request for ten attempts. If the tenth retransmission fails, the client assigns the class of the IP address to be the subnet mask. If the server responds, the client obtains the subnet mask. After receiving the subnet mask, the client sets the default gateway to be the RARP server.

RARP Server When the system is configured as the RARP server, it can receive an RARP request from a machine (RARP client) that needs an address. The RARP server searches the addresses in the IP Address Translation Table to find a match for the source hardware address in the request. If the RARP server finds a match, it sends the IP address corresponding to the match to the client. If no match is found, the RARP server discards the request.

The RARP server can also respond to an ICMP Address Mask request. When the RARP server receives and IP address, it returns the subnet mask of that address if the ICMPReply parameter is set to Mask. For information about the ICMPReply parameter, refer to Chapter 29.

Values

RarpClient | NoRarpClient	Selects the RarpClient option for the client machine. Setting the value to NoRarpClient and then to RarpClient causes the client to send a RARP request and provides manual control for situations in which the client needs to learn a new IP address because of network reconfigurations.
RarpServer | NoRarpServer	Selects the RarpServer option for the server machine. For example, the RarpServer option can be used for a central node in a Boundary Routing® configuration. For information about Boundary Routing, refer to Chapter 32 in *Using NETBuilder Family Software*.

RequestFormat

Syntax

```
SETDefault !<port> -ARP RequestFormat = Auto | Both | Ethernet | Snap
SHow [!<port> | !*] -ARP RequestFormat
```

Default Ethernet

Description The RequestFormat parameter specifies the header format used for ARP request packets.

Values

Auto	Allows the system to determine the default request format based on the media type of the interface.
Both	ARP sends two ARP request packets, one with Ethernet format and one with the IEEE 802.2 and IEEE 802.3 formats (see the description for Snap that follows). It also dynamically learns the header format supported by the destination system.
Ethernet	ARP sends request packets with an Ethernet Version 2 header.
Snap	The ARP request packet is encapsulated with a Subnetwork Access Protocol (SNAP) header. If the interface type is Ethernet and the value of the RequestFormat parameter is set to Snap, two ARP requests (each with a SNAP header), are sent out. The first ARP request is for type 1, and the second ARP request is for type 6. The type 6 request is for IBM RS6000-type machines. The Snap option is useful for protocols that do not have regular Destination Service Access Point (DSAP) and Source Service Access Point (SSAP) addresses, for example, AppleTalk.

7 ATM SERVICE PARAMETERS

This chapter describes parameters in the Asynchronous Transfer Mode (ATM) Service used for bridging and routing over ATM.

Table 7-1 lists the ATM Service parameters and commands.

Table 7-1 ATM Service Parameters and Commands

Parameters	Commands
CONFiguration	SHow
CONTrol	SETDefault, SHow
KeepAliveTime	SETDefault, SHow
LoopMode	SETDefault, SHow
PermVirCircuit	ADD, DELete, SHow
SwitchVersion	SETDefault, Show
TrafficShaper	SETDefault, SHow
VCIBits	SETDefault, SHow
VirCirLoopMode	SETDefault, SHow
VirCirLoopTime	SETDefault, SHow
VPIBits	SETDefault, SHow

CONFiguration

Syntax

```
SHow [!<port> | !*] -ATM CONFiguration
```

Default No default

Description The CONFiguration parameter displays the current ATM Service parameters settings for a single port or all ports.

CONTrol

Syntax

```
SETDefault !<port> -ATM CONTrol = SVC | NoSVC
SHow [!<port> | !*] -ATM CONTrol
```

Default SVC

Description The CONTrol parameter enables or disables switched virtual circuits (SVC) on the specified port.

Values

SVC	Indicates that SVCs are enabled.
NoSVC	Indicates that SVCs are disabled.

KeepAliveTime

Syntax

```
SETDefault !<port> -ATM KeepAliveTime = <seconds>(1–60)
SHow [!<port> | !*] -ATM KeepAliveTime
```

Default 2 seconds

Description The KeepAliveTime parameter specifies the time interval at which the interface is checked to determine whether it is connected to the ATM switch using the method specified by the LoopMode parameter.

The KeepAliveTime parameter can be modified at any time, but the new setting does not take effect until the ATM interface is reset (the path must be re-enabled).

LoopMode

Syntax

```
SETDefault !<port> -ATM LoopMode = AssumeConnected | DetectFraming
   | LoopBack
SHow [!<port> | !*] -ATM LoopMode
```

Default AssumeConnected

Description The LoopMode parameter specifies the method that determines whether or not the ATM interface is connected to the ATM switch. you can specify how often the ATM network status is checked with the KeepAliveTime parameter.

The LoopMode parameter can be modified at any time, but the new setting does not take effect until the ATM interface is reset (the path must be re-enabled).

Values

AssumeConnected	Assumes the specified interface is connected to the ATM switch. No periodic checking is performed.
DetectFraming	Connects the specified interface is to the ATM switch if successful framing of received data is detected (the Synchronous Optical Network (SONET) equivalent of carrier detection).
LoopBack	Connects the specified interface is to the ATM switch if loopbacks to the ATM switch are successful.

PermVirCircuit

Syntax

```
ADD !<port> -ATM PermVirCircuit <vcid> <vpi.vci> [LLCSNAP | [NULL
   | IP | IPX]] [<shaper_id>]
DELete !<port> -ATM PermVirCircuit <vcid> | ALL
SHow [!<port> | !*] -ATM PermVirCircuit
```

Default Encapsulation type is LLCSNAP; shaper ID is 1

Description The PermVirCircuit parameter adds, deletes, or displays the permanent virtual circuit (PVC) on a virtual port. A PVC must be configured for each communicating ATM end node. The virtual circuit characteristics configured for each PVC must match in the NETBuilder II bridge/router, the ATM switch, and the remote end node. For software version 9.0 and later, PVCs support AAL5 for data communications.

Use the DELete command to terminate the PVC connection associated with this virtual circuit ID and to remove the PVC from the configuration file. The DELete command can delete a single PVC connection or all connections. Before deleting a PVC, all protocol users of the PVC must delete the neighbor configuration associated with the PVC.

Use the SHow command to display all PVC status on a specified port or on all ports.

Values

!<port> Specifies a virtual port number.

<vcid> Virtual circuit identifier (VCID) is a unique user-assigned numeric identifier to be assigned to the PVC for a remote node and represents its configured virtual circuit characteristics. The network and bridge protocols use the local VCID as the ATM address of the remote node (similar to the DLCI of a Frame Relay PVC).

Valid VCID numbers range from 1 to 1,024.

<vpi.vci> Specifies the virtual path identifier (VPI) and the virtual channel identifier (VCI) pair that denotes a single point-to-point ATM virtual circuit. The virtual circuit can support either unidirectional or bidirectional traffic.

The VPI is an 8-bit number that ranges from 0 to 255 and is supplied by the service provider.

The VCI is a 16-bit number that ranges from 0 to 65,535 and is supplied by the service provider.

VPI.VCIs from 0.0 through 0.32 are reserved virtual circuits and are not allowed as user virtual circuits. The VPI and VCI values must be compatible with the configured value for the VPIBits and the VCIBits parameter.

LLCSNAP | NULL Specifies the encapsulation type for the user protocol data. Either LLCSNAP or NULL can be specified.

Use LLCSNAP to support multiple protocol traffic to be carried within a single ATM virtual circuit. This encapsulation type allows the same PVC to be used by different network or bridge protocols on the bridge/router, for example, IP and IPX.

Use NULL to support only a single protocol to run on a virtual circuit. This encapsulation type allows the PVC to be used only by the specified protocol, such as IP or IPX.

IP | IPX Specifies the virtual circuit-specific protocol. For release 9.0, only IP and IPX are supported.

<shaper_id> Specifies the traffic shaper for outgoing traffic on the virtual circuit. Traffic shaping is based on the peak/average rates, burst count, and priority level specified for the assigned traffic shaper. For more information, refer to "SwitchVersion" on page 7-4.

ALL Deletes all PVC connections assigned to the port.

SwitchVersion

Syntax

```
SETDefault !<port> -ATM SwitchVersion = [UNI30 | UNI31]
```

Default No default

Description The SwitchVersion parameter specifies the version of the User Network Interface (UNI) that is supported by the ATM switch.

Values

UNI30	Specifies that the ATM switch supports UNI version 3.0.
UNI31	Specifies that the ATM switch supports UNI version 3.1.

TrafficShaper

Syntax

```
SETDefault -ATM TrafficShaper = <id>(1–14) <peak>(1–155,000)
  <avg>(1–155,000) [<burst>(1–255)] [High | Low]
SHow -ATM TrafficShaper [<shaper_id>(1–14)]
```

Default Burst = 32; priority = High

Description The TrafficShaper parameter defines a set of traffic-shaping attributes that are associated with each PVC to support flexible outbound traffic flow control per the specified peak rate, average rate, burst count, and priority levels.

You can configure up to 14 default traffic shapers on each NETBuilder II bridge/router. The default traffic shapers can be modified at any time, but the new shaper attributes do not take effect until the ATM interface is reset (the path must be re-enabled). Table 7-2 shows the predefined traffic shapers attributes.

Table 7-2 Predefined Traffic Shaper Attributes

ID	Peak Rate (kbps)	Average Rate (kbps)	Burst	Priority
1	50,000	50,000	32	High
2	75,000	75,000	32	High
3	60,000	60,000	32	High
4	40,000	40,000	32	High
5	30,000	30,000	32	High
6	20,000	20,000	32	High
7	10,000	10,000	32	High
8	50,000	50,000	32	Low
9	75,000	75,000	32	Low
10	60,000	60,000	32	Low
11	40,000	40,000	32	Low
12	30,000	30,000	32	Low
13	20,000	20,000	32	Low
14	10,000	10,000	32	Low

For software version 9.0 and later, only AAL5 data application traffic (not voice and video application traffic) is supported.

For more information on using traffic shapers, refer to "Traffic Shapers" on page 47-14 in *Using NETBuilder Family Software*.

Values

<id> or <shaper_id>	Identifies the traffic shaper to be modified. Valid IDs are from 1 to 14.
<peak>	Specifies the peak bit rate in kilobits per second. Valid rates are from 1 to 155,000.
<avg>	Specifies the average bit rate in kilobits per second. Valid rates are from 1 to 155,000.
<burst>	Specifies the burst count in 53-byte cells. Valid numbers are from 1 to 255.
High | Low	Specifies the priority level. Valid priorities are High or Low. Virtual circuit traffic associated with a high-priority shaper are serviced first. If several traffic shapers have the same priority, they are serviced in a round-robin process and considered to be equal priority.

VCIBits

Syntax

```
SETDefault !<port> -ATM VCIBits = <vci_bits>(1-16)
SHow [!<port> | !*] -ATM VCIBits
```

Default 10

Description The VCIBits parameter specifies the number of effective VCI bits to be used for all the virtual circuits associated with the specified ATM interface. Adjust this parameter to the VCI size supported by the ATM switch. You may also need to adjust the VPIBits parameter to the size supported by the ATM switch; refer to "VPIBits" on page 7-6. The combined number of VPI and VCI bits must not exceed the maximum 24 bits.

The VCIBits parameter can be modified at any time, but the new setting does not take effect until the ATM interface is reset (the path must be re-enabled).

VirCirLoopMode

Syntax

```
SETDefault !<port> -ATM VirCirLoopMode = ENabled | DISabled
SHow [!<port> | !*] -ATM VirCirLoopMode
```

Default DISabled

Description The VirCirLoopMode parameter enables or disables the F5 end-to-end loop back to determine end-to-end connection status for all the virtual circuits associated with the specified virtual port.

The frequency of checking the end-to-end connection status is specified using the VirCirLoopTime parameter. If the F5 loopback is disabled, the virtual circuit is assumed to be connected and periodic F5 loopback is not initiated to probe end-to-end connectivity.

VirCirLoopTime

Syntax

```
SETDefault !<port> -ATM VirCirLoopTime = <seconds>(1–60)
SHow [!<port> | !*] -ATM VirCirLoopTime
```

Default 5 seconds

Description The VirCirLoopTime parameter specifies the time interval in seconds to initiate the F5 loopback to determine the end-to-end connection status.

The VirCirLoopTime parameter can be modified at any time, but the new setting does not take effect until the ATM virtual port is reset (the port must be re-enabled).

VPIBits

Syntax

```
SETDefault !<port> -ATM VPIBits = <vpi_bits>(1–8)
SHow [!<port> | !*] -ATM VPIBits
```

Default 6

Description The VPIBits parameter specifies the number of effective VPI bits to be used for all the virtual circuits associated with the specified ATM interface. Adjust this parameter to the VPI size supported by the ATM switch. You may also need to adjust the VCIBits parameter to the size supported by the ATM switch; refer to "VCIBits" on page 7-5. The combined number of VPI and VCI bits must not exceed the maximum 24 bits.

The VPIBits parameter can be modified at any time, but the new setting does not take effect until the ATM interface is reset (the path must be re-enabled).

8 ATMLE SERVICE PARAMETERS

This chapter describes parameters in the Asynchronous Transfer Mode LAN Emulation (ATMLE) Client Service used to emulate the services of a connectionless LAN network over ATM.

Table 8-1 lists the ATMLE Service parameters and commands.

Table 8-1 ATMLE Service Parameters and Commands

Parameters	Commands
AgeTime	SETDefault, SHowDefault
ArpRoute	FLUSH, SHow
ArpRspTime	SETDefault, SHowDefault
ATMAddress	SHowDefault
CntrlTime	SETDefault, SHowDefault
CONFiguration	SHowDefault
ConnTime	SETDefault, SHowDefault
CONTrol	SETDefault, SHowDefault
DelayTime	SETDefault, SHowDefault
ElanName	SETDefault, SHowDefault
FlushTime	SETDefault, SHowDefault
LanType	SETDefault, SHowDefault
LECSAddr	SETDefault, SHowDefault
LESAddr	SETDefault, SHowDefault
MaxData	SETDefault, SHowDefault
MaxRetry	SETDefault, SHowDefault
MaxUnkFRM	SETDefault, SHowDefault
MaxUnkFTM	SETDefault, SHowDefault
PrimaryMAC	SHowDefault
STATUS	SHow
SwitchTime	SETDefault, SHowDefault
VccTime	SETDefault, SHowDefault

AgeTime

Syntax

```
SETDefault !<vport> -ATMLE AgeTime = <seconds> (10-300)
SHowDefault !<vport> -ATMLE AgeTime
```

Default 300 seconds

Description The AgeTime parameter displays the maximum inactivity time for an entry in the LE_ARP Table.

The LE_ARP Table holds the MAC address while the data direct VCC is being set up between LAN emulation clients. The AgeTime parameter specifies the maximum aging time for an entry in the LE_ARP Table. The LAN Emulation Client resets this timer when it receives a packet from the BUS (Multicast forward VCC) or through a remote LAN Emulation Client (data direct VCC) with the entries MAC address.

If an entry ages out, the LAN emulation client (LEC) does not remove the entry from the LE_ARP Table, but sends a LE_ARP request to verify that the MAC address is still reachable. If the LE_ARP response is not received, then the entry is removed from the table.

ARPRoute

Syntax

```
FLUSH -ATMLE ArpRoute
SHow -ATMLE ArpRoute
```

Default No default

Description The ARPRoute parameter displays the current contents of the LE_ARP Table. The table displays the LEC index and the MAC address order.

The FLUSH command removes all the entries from the LE_ARP Table.

ArpRspTime

Syntax

```
SETDefault <!vport> -ATMLE ArpRspTime = <seconds> (1-30)
SHowDefault <!vport> -ATMLE ArpRspTime
```

Default 4 seconds

Description The ArpRspTime parameter specifies the maximum amount of time that the LEC waits for a response to a LE_ARP request. If the LE_ARP response does not arrive within the LE_ARP response time, the MAC address is removed from the LE_ARP Table. The LE_ARP request is usually generated when a unicast packet is received and there is no entry in the LE_ARP Table. The LE_ARP request is also generated to verify that a MAC/ATM address mapping is still valid when AgeTime or DelayTime has expired.

ATMAddress

Syntax

```
SHowDefault !<vport> -ATMLE ATMAddress
```

Default No default

Description The ATMAddress parameter displays the local ATM address of a specific LAN emulation client or all the configured LAN emulation clients.

CntrlTime

Syntax

```
SETDefault !<vport> -ATMLE CntrlTime = <seconds> (10-300)
SHowDefault !<vport> -ATMLE CntrlTime
```

Default 120 seconds

Description The CntrlTime parameter specifies the control time-out period (in seconds) for request and response control frames between the LAN emulation client and the ATM Service. The following control frames are affected by this parameter:

- Configuration Response Frame - LEC configuration phase
- Join Response Frame - LEC join phase
- LE_ARP Reply Frame - BUS connect phase and operational phase

Values <seconds> Specifies the number of seconds to wait before timing out a response frame from the ATM services.

CONFiguration

Syntax

```
SHowDefault !<vport> -ATMLE CONFiguration
```

Default No default

Description The CONFiguration parameter displays the configured parameters for a specific LAN emulation client or all the LAN emulation clients configured on the specified virtual port.

ConnTime

Syntax

```
SETDefault !<vport> -ATMLE ConnTime = <seconds> (10-300)
SHowDefault !<vport> -ATMLE ConnTime
```

Default 10 seconds

Description The ConnTime parameter specifies the maximum amount of time to wait for the READY_IND control frame on the data direct VCC after the LEC has requested the connection manager to send a connection response to the calling remote LEC. The READY_IND control frame was sent by the calling remote LEC after it received the connection confirm and the calling remote LEC is ready to receive data packets. If the READY_IND control ram wait period expires, the LEC reacts to the event as though it was received and starts sending data packets on the data direct VCC.

Values <seconds> Specifies the connection completion time to wait for a READY_IND control frame to complete the connection establishment.

CONTrol

Syntax

```
SETDefault !<vport> -ATMLE CONTrol = [MANual | AUTOmatic], [Proxy
  | NoProxy]
```

Default AUTOmatic

Description The CONTrol parameter specifies the addressing method, either MANual or AUTOmatic, that is used during the LAN emulation client initialization.

Values MANual Indicates the LEC initialization process will check the configured LES-ATM addresses and use the address for the LE_JOIN state and skip the CONFI_LEC states.

AUTOmatic	Indicates the LEC initialization process goes through the CONF_LEC states to retrieve the LES ATM address and joins the emulated LAN.
Proxy	Indicates that ATMLE will receive LE_ARP requests for MAC addresses not registered with the LES. Proxy should be set when global Bridging is enabled and the ATMLE virtual port has transparent bridging enabled.
NoProxy	Indicates that ATMLE will only receive LE_ARP requests for its local MAC address/local ATM address pair registered with the LES. ATMLE may not receive the LE_ARP Request if the LES responds for registered MAC addresses. NoProxy should be set when the ATMLE virtual port is configured for routing only.

DelayTime

Syntax

```
SETDefault !<vport> -ATMLE DelayTime = <seconds> (4 - 30)
SHowDefault !<vport> -ATMLE DelayTime
```

Default 4 seconds

Description The DelayTime parameter specifies the maximum amount of time for a LEC owned remote MAC address in the LE_ARP Table. These entries are MAC addresses that are learned to be reachable through a remote LEC connected to the ATM network. The entries of MAC addresses belonging to LECs connected to the ATM network (ATM end-stations) are not affected by this aging timer. The LEC uses this aging timer for the LEC-owned remote MAC addresses as long as the LEC receives a LE_TOPOLOGY Request with the “Topology Change” flag set. When an LE_TOPOLOGY Request is received with the “Topology Change” flag cleared, the LEC uses the AgeTime parameter again for the remote MAC entries.

Values

<seconds>	Specifies the inactivity period for a LEC-owned remote MAC entry in the LE_ARP Table.

ElanName

Syntax

```
SETDefault !<vport> -ATMLE ElanName = <string (1-60 char)>
  [Validate | NoValidate]
SHowDefault !<vport> -ATMLE ElanName
```

Default NoValidate

Description The ElanName parameter is the name of the emulated LAN that the LAN emulation client joins. If unspecified, the name is returned in the join response frame from the LES during the LES join phase. If the name is specified, this parameter allows the LEC to select which emulated LAN it wants to join. If the option Validate is specified, the LE_JOIN_RESPONSE Elan_Name must match the configured value. If the strings do not match, the LEC must change to the IDLE state.

Values

<string>	Specifies the name of the ELAN. From one to sixty characters may be used.
Validate	When specified, the LE_JOIN_RESPONSE Elan Name must match the configured value.
NoValidate	Specifies that no elan name matching must be performed.

FlushTime

Syntax

```
SETDefault !<vport> -ATMLE FlushTime = <seconds> (1-4)
SHowDefault !<vport> -ATMLE FlushTime
```

Default 4 seconds

Description The FlushTime parameter specifies the maximum amount of time to wait for the LE_FLUSH response after the LE_FLUSH request has been sent.

Values

<seconds>	The maximum LE_FLUSH response wait period.

LanType

Syntax

```
SETDefault !<vport> -ATMLE LanType = ETHernet
SHowDefault !<vport> -ATMLE LanType
```

Default ETHernet

Description The LanType parameter specifies the type of LAN.

Values

ETHernet	Specifies that the LAN type of the emulated LAN is Ethernet/IEEE 802.3.

LECSAddr

Syntax

```
SETDefault !<vport> -ATMLE LECSAddr = <atm address>
SHowDefault !<vport> -ATMLE LECSAddr
```

Default None

Description The LECSAddr parameter specifies the ATM address of the LAN emulation configuration server (LECS). If the LAN emulation client is in manual mode, and the LECS ATM address is configured, the LEC uses this ATM address to connect to the LECS instead of using the UME to retrieve the LECS ATM address. The LEC can select the LECS. Configuring the LECS ATM address also overrides the use of the configured LES ATM address. If the LEC is in automatic mode, the configured LECS ATM address is ignored.

Values

<atm address>	Specifies the LAN emulation configuration server (LECS) ATM address.

LESAddr

Syntax

```
SETDefault !<vport> -ATMLE LESAddr = <atm address>
SHowDefault !<vport> -ATMLE LESAddr
```

Default No default

Description The LESAddr parameter specifies the ATM address of the LAN emulation server. If the LAN emulation client is in manual mode and the LES ATM address is configured, the LEC bypasses the LEC Connect Phase and LEC Configuration Phase and goes directly into the LEC join phase. If unspecified, the LES ATM address is returned in the LECS configuration response frame. This allows the LEC to select which emulated LAN it wants to join. If the LEC is in automatic mode or the LEC is in manual mode but the LECS ATM address is configured, the configured LES ATM address is ignored.

Values <atm address> Specifies the LAN emulation server ATM address.

MaxData

Syntax

```
SETDefault !<vport> -ATMLE MaxData = [UNspecified | 15165 | 4544
 | 9234 | 18190]
SHowDefault !<vport> -ATMLE MaxData
```

Default 1516

Description The MaxData parameter specifies the maximum data frame size between the LEC and the BUS that can be sent or received on the multicast send VCC and received on the multicast forward VCC. This parameter also specifies the maximum data frame size between the LEC and the remote LEC that can be sent or received on the data direct VCC.

Values

1516	Specifies a maximum of 1516 bytes on the SVCs. Used for Ethernet/IEEE 802.3 LAN emulation.
4544	Specifies a maximum of 4544 bytes on the SVCs. Used for token ring IEEE 802.5 4 Mbps operation.
9234	Specifies a maximum of 9234 bytes on the SVCs. Used for RFC 1626 (Default IP MTU for use over AAL5) operations.

MaxRetry

Syntax

```
SETDefault !<vport> -ATMLE MaxRetry = <count> (0-2)
SHowDefault !<vport> -ATMLE MaxRetry
```

Default 1 retry

Description The MaxRetry parameter specifies the maximum number of retries that will be executed.

Values <count> Specifies the LE_ARP maximum retry count.

MaxUnkFrm

Syntax

```
SETDefault !<vport> -ATMLE MaxUnkFRM = <count> (1 - 10)
SHowDefault !<vport> -ATMLE MaxUnkFRM
```

Default 1 frame

Description The MaxUnkFrm parameter specifies the maximum number of unknown frames (unicast packets) to the same destination MAC address that can be sent to the BUS multicast send VCC within the period specified.

Values <count> Specifies the maximum number of unicast packets to the same destination MAC address within the time period specified using the MaxUnkFtm parameter.

MaxUnkFtm

Syntax

```
SETDefault !<vport> -ATMLE MaxUnkFTM = <seconds> (1-60)
SHowDefault !<vport> -ATMLE MaxUnkFTM
```

Default 1 second

Description The MaxUnkFtm parameter specifies the period within which the LEC cannot send any more than the number of unknown unicast frames that are specified.

Values <seconds> Indicates the period in which the number of unknown unicast packets must not exceed the number specified.

PrimaryMAC

Syntax

```
SHowDefault !<vport> -ATMLE PrimaryMac
```

Default No default

Description The PrimaryMac parameter displays the primary MAC address for the virtual port.

STATUS

Syntax

```
SHow !<port> -ATMLE STATus [Verbose]
```

Default No default

Description The STATUS parameter displays the status of the NetBuilder II LAN emulation client.

Values Verbose Displays the connection number and VPI/VCI associated with the connections established with the LECS, LES, and BUS. LE_ARP statistics and LEC control frame statistics are also displayed.

SwitchTime

Syntax

```
SETDefault !<vport> -ATMLE SwitchTime = <seconds> (1-8)
SHowDefault !<vport> -ATMLE SwitchTime
```

Default 6 seconds

Description The SwitchTime parameter specifies the transmit inactivity period for an entry in the LE_ARP Table that allows the LEC to switch data paths without using the LE_FLUSH request/LE_FLUSH response procedure. Because no data packets have been sent during the switch period, the LEC is assured that switching data paths do not affect unicast data packet sequencing.

Values <seconds> Specifies the transmit inactivity period for a LEC-owned entry in the LE_ARP Table that allows the LEC to bypass sending the LE_FLUSH request before switching data paths.

VccTime

Syntax

```
SETDefault !<vport> -ATMLE VccTime = <minutes> (0 ... 65535)
```

```
SHowDefault !<vport> -ATMLE VccTime
```

Default 20 minutes

Description The VccTime parameter specifies the VCC time-out period. The LEC releases the data direct VCC when the VCC was not used by the LEC to transmit or receive any data frames before this period expires. This timer causes the LEC to remove the entry in the CEC BRT, but the LEC does not remove it from the LE_ARP Table. The entry needs to reestablish the data direct VCC before it can forward data packets again.

Values	<minutes>	Specifies the inactivity time period for a data direct VCC. This timer does not affect any other VCCs opened by the LEC.

9 ATUN SERVICE PARAMETERS

This chapter describes the parameters in the ATUN Service. The parameters in this service are used to operate paths in asynchronous mode while tunneling port data to remote control units (CUs).

Table 9-1 lists the ATUN Service parameters and commands.

Table 9-1 ATUN Service Parameters and Commands

Parameters	Commands
AddrLOCation	SETDefault, SHow
BroadCastAddr	SETDefault, SHow
CUADDRess	SETDefault, SHow
CUCONFig	SHow
CUCONTrol	SETDefault, SHow
CUInfo	SHow, FLush
CUPOrt	SHow
CUSTatus	SHow
FrameChars	ADD, DELete, SHow
FrameGap	SETDefault, SHow
FrameSize	SETDefault, SHow
IdleTimer	SETDefault, SHow
LocalMac	SETDefault, SHow
LocalSap	SETDefault, SHow
PortCONFig	SHow
PortCONTrol	SETDefault, SHow
PortCU	ADD, DELete, SHow
RemoteMac	SETDefault, SHow
RemoteSap	SETDefault, SHow

AddrLOCation

Syntax

```
SETDefault !<port> -ATUN AddrLOCation = <offset> (0-1024)
SHow [!<port>] -ATUN AddrLOCation
```

Default 0

Description The AddrLOCation parameter sets which data byte of received frames should be considered an address byte. This value is specified as an offset from the first byte of the frame: 0 indicates the first byte, 1 the second byte, and so forth. If a frame is received with fewer bytes than the offset required to locate the address, it is assumed to be an incorrect frame and is discarded. If you disable addressing using the -ATUN PortCONTrol parameter, the AddrLOCation parameter is ignored.

BroadCastAddr

Syntax

```
SETDefault !<port> -ATUN BroadCastAddr = <value> (0-255)
SHow [!<port>] -ATUN BroadcastAddr
```

Default 0

Description The BroadCastAddr parameter defines a special value for the address byte, which indicates an "all stations" destination. If you enable broadcast addressing with the -ATUN PortCONTrol parameter Address and BCAddr options, frames with an address byte that matches the BroadCastAddr value are forwarded to all active tunnels associated with the port.

CUADDRess

Syntax

```
SETDefault !<CU name> -ATUN CUADDRess = <value>(0-255) [-<value> (0-255)]
SHow [!<CU name>] -ATUN CUADDRess
```

Default 0

Description The CUADDRess parameter sets which frames are sent over the tunnel associated with the CU. When you use addressing on the port (set with the PortCONTrol parameter), an address byte is extracted from each frame (as determined by the AddrLOCation parameter). The frame is then directed to the CU whose address range includes this value.

The CUADDress values for all enabled CUs on a port must not overlap. An addressed frame is mapped to a single CU only. Broadcast capability (sending a frame to any CUs on the port) is available explicitly by broadcast addressing or implicitly by ignoring the address and broadcasting all frames.

When entering the address, the range must be specified using the low end of the range first followed by the high end of the range (for example 30 to 47 is set as 30-47); you cannot specify the range as 47-30.

CUCONFig

Syntax

```
SHow [!<CU name>] -ATUN CUCONFig
```

Default No default

Description The CUCONFig parameter displays the entire configuration of a CU. If no CU name is specified, information for all CUs is displayed.

CUCONTrol

Syntax

```
SETDefault !<CU name> -ATUN CUCONTrol = (Enabled | Disabled)
SHow [!<CU name>] -ATUN CUCONTrol
```

Default Disabled

Description The CUCONTrol parameter enables and disables individual CUs.

Values	Enabled | Disabled	Enabled allows the CU. If CUCONTrol is changed from Enabled to Disabled when the tunnel is active, the tunnel is disconnected. Whether the CU initiates a connection or waits for a connection depends on the CentralSite | RemoteSite setting of the PortCONTrol parameter (refer to page 9-7).

CUInfo

Syntax

```
SHow [!<CU name>] -ATUN CUInfo [<port>]
FLush [!<CU name>] -ATUN CUInfo [<port>]
```

Default No default

Description The CUInfo parameter displays information about the CU. If a CU name is not included (or the * wildcard character is used), the information for all CUs is displayed. If a port number is included at the end of the command, information for all CUs on the port is displayed.

The display includes the following:

- The current CUSTatus value
- The time of the last connect or disconnect event
- The reason for the last disconnect
- The number of packets and bytes forwarded, and the number of packets discarded, in each direction on the tunnel for the CU

The counts shown in the display are accumulated for the current tunnel connection; if the tunnel is currently down (no circuit) the counts are the totals for the previous connection. Counts can be reset to 0 using the FLush command.

Table 9-2 describes the meanings of the headings and status messages included in the CUInfo display.

Table 9-2 CUInfo Display Meanings

Display Heading	Meaning
Port-to-Tunnel	Shows accumulated values for data from the asynch port, directed at the CU (addressed or broadcast).
Tunnel-to-Port	Shows accumulated values from the CU tunnel, implicitly directed at the asynch port.
Forwarded	The number of packets or bytes forwarded.
Discarded	The number of packets discarded. FlowControl indicates the number of packets discarded to flow-control (overflow) of the port or tunnel. No Circuit indicates the number of packets discarded because the tunnel was not up. No Memory indicates the number of packets discarded because there was insufficient memory to copy the data to the tunnel. The No Circuit and No Memory packet counts only apply to data from Port-to-Tunnel.

CUPOrt

Syntax

```
SHow [!<CU name>] -ATUN CUPOrt
```

Default No default

Description The CUPOrt parameter displays the number of the port that the specified CU is assigned to. If no CU name is specified, all CUs are displayed, grouped, and ordered by port.

CUSTatus

Syntax

```
SHow [!<CU name>] -ATUN CUSTatus
```

Default No default

Description The CUSTatus parameter displays the current status of a specified CU, or the state of all configured CUs.

Table 9-3 lists the possible CU states shown in the display and their meanings.

Table 9-3 CUSTatus Display Status Message Meanings

Status Message	Meaning
Disabled (CUCONTrol Disabled)	The CU is non-operational; the CUCONTrol parameter is disabled.
Disabled (PortCONTrol Disabled)	The CU is non-operational; the CUCONTrol parameter is Enabled, but the PortCONTrol parameter is disabled.
Disabled (Port or Path is Unavailable)	The CU is non-operational. The CUCONTrol and PortCONTrol parameters are both Enabled, but the ATUN Service is not able to use the port because the -PORT OWNer parameter is not set to ATUN, or because the -PORT or -PATH CONTrol parameters are disabled.
Disabled (Port or Path is Down)	The CU is non-operational. The CUCONTrol and PortCONTrol parameters are Enabled, and ATUN is the -PORT OWNer, but the port is down. The -PORT or -PATH CONTrol parameters may be disabled, or the system may not be receiving any control signals (such as DTR or DCD) from the asynch device.
Enabled (Trying to initiate circuit)	The CU is trying to initiate a circuit with its peer. (Produces DLSw CANUREACH messages and/or LLC2 TEST frames).
Enabled (Waiting for peer to initiate circuit)	The CU is on a CentralSite port, and is waiting for its peer to initiate a circuit.
Connecting (exchanging peer XID or CONNECT)	A circuit has been established for this CU by DLSw; the CU is exchanging setup frames with its peer. These appear as DLSw XIDFRAME or CONNECT messages, and/or LLC2 XID or SABME/UA frames.
Connected to NB/ATUN peer	The circuit is CONNECTED and ready for transport of asynch data. (Setup frames indicate that the configured CU peer is an ATUN port.)

FrameChars

Syntax

```
ADD !<port> -ATUN FrameChars <char>...
DELete !<port> -ATUN FrameChars <char>...
SHow [!<port>] -ATUN FrameChars
```

Default No default

Description The FrameChars parameter specifies a set of special characters that indicate the end of a frame. This framing mechanism can be used for protocols with a frame format that includes an end-of-frame character, including situations where the nature of the transmitter makes the IdleTimer too inefficient (too long) or unusable (too short).

You can include up to eight characters when specifying the command. When entering numerics, you can use decimal, hex, octal, or binary.

You cannot use the null character (value 0).

Example 1 To configure a carriage return (decimal 13) as the end of a frame for port 1, enter:

```
ADD !1 -ATUN FrameChars 13
```

Example 2 To configure a carriage return as the end of a frame using hex, enter:

```
ADD !1 -ATUN FrameChars %D
```

Example 3 To configure a carriage return as the end of a frame using the appropriate ASCII control characters, enter:

```
ADD !1 -ATUN FrameChars ^M
```

FrameGap

Syntax

```
SETDefault !<port> -ATUN FrameGap = <milliseconds> (0-1000)
SHow [!<port>] -ATUN FrameGap
```

Default 0

Description The FrameGap parameter sets the minimum amount of idle time to leave between frames transmitted by the bridge/router. This parameter can be used when the attached device recognizes frames using an idle timer. The bridge/router receives data for the port from one or more tunnels; the variable-latency characteristics of the tunnels may cause multiple frames to arrive back-to-back. If you configure the FrameGap parameter, the bridge/router guarantees that the frames are separated when transmitted out the port.

This timer is expressed in milliseconds, but the implemented granularity varies. The configured value defines minimum interframe gap; the actual gap may be longer.

FrameSize

Syntax

```
SETDefault !<port> -ATUN FrameSize = <bytes> (1-1024)
SHow [!<port>] -ATUN FrameSize
```

Default 1024

Description The FrameSize parameter sets the maximum number of bytes that should be collected before forwarding. When the specified number of bytes has been received, the data is forwarded as a single frame.

The FrameSize parameter should not be only forwarding configured conditions, or data may misframe on receipt. The IdleTimer parameter should usually be set to “mop up” any trailing partial frames (remaining data less than FrameSize). The exception is if you set a frame size of 1.

You can use this parameter with non-framed data to control tunneling efficiency. Larger frames are more efficient with less relative overhead, but may increase latency. The overhead of small frames also can cause latency.

You also can use the FrameSize parameter when the attached device sends fixed-sized frames. The parameter reduces latency by forwarding the frame upon complete reception, instead of the idle timer expiration set with the IdleTimer parameter.

If a device sends variable-length frames, and addressing is used, or framing is important at the receiver, set the FrameSize parameter to no less than the maximum possible frame.

IdleTimer

Syntax

```
SETDefault !<port> -ATUN IdleTimer = <milliseconds> (0-5000)
SHow [!<port>] -ATUN IdleTimer
```

Default 10

Description The IdleTimer parameter specifies the maximum inter-character delay before the bridge/router considers the accumulated frame to be complete, and the frame is forwarded. Setting 0 disables the timer completely, and forwarding then depends on the FrameSize or FrameChars parameter settings. This action is not recommended in most cases.

Although expressed in milliseconds, the timer granularity is implemented in terms of character times. For example, at a speed of 1200 bps, one character takes 8 to 10 milliseconds of transmission time, so the configured value will be rounded up to a multiple of 10.

LocalMac

Syntax

```
SETDefault !<CU name> -ATUN LocalMac = <address>
SHow [!<CU name>] -ATUN LocalMac
```

Default 000000000000

Description The LocalMac parameter sets the MAC address for the local tunnel endpoint. The value specified must match the RemoteMac parameter of the peer CU configuration. The local MAC must be in the Locally Administered Address (LAA) range.

LocalSap

Syntax

```
SETDefault !<CU name> -ATUN LocalSap = <sap> (hex 04-ec[by 4])
SHow [!<CU name>] -ATUN LocalSap
```

Default E8

Description The LocalSap parameter sets the SAP for the local tunnel endpoint. The value specified must match the RemoteSap parameter of the peer CU configuration.

PortCONFig

Syntax

```
SHow [!<port>] -ATUN PortCONFig
```

Default No default

Description The PortCONFig parameter displays the asynchronous tunneling configuration of the port.

PortCONTrol

Syntax

```
SETDefault !<port> -ATUN PortCONTrol = ([Enabled | Disabled],
  [CentralSite | RemoteSite], [Address | NoAddress], [BCAddr |
  NoBCaddr], [ForcePoll | NoForcePoll], [TestEcho | NoTestEcho])
SHow [!<port>] -ATUN PortCONTrol
```

Default Disabled, RemoteSite, NoAddress, NoBCaddr, NoForcePoll, NoTestEcho

Description The PortCONTrol parameter determines the general configuration of the ATUN port.

Values

Enabled | Disabled — Enabled indicates that enabled CUs associated with the port will accept or initiate tunnels with their configured peers. Disabled indicates that the CUs on the port will not accept or initiate tunnels. When the PortCONTrol parameter is changed from Enabled to Disabled, any active tunnels for CUs on the port are disconnected. The default is disabled.

CentralSite | RemoteSite — CentralSite indicates that the port is on a central site, meaning that multiple CUs can be defined on the port. RemoteSite indicates that the port is on a remote site, meaning that only one CU can be defined on the port. The default is RemoteSite.

A CU on a remote site port will initiate a tunnel, while a CU on a central site port will wait for its peer to initiate the tunnel. You can have a tunnel with remote site ports at both ends, but you cannot have a tunnel with central site ports at both ends because neither side will initiate the session.

Address | NoAddress — Indicates whether addressing is used on the port. Address indicates that each received frame (as set by the -ATUN FrameSize, FrameChars, and IdleTimer parameters) is directed to a tunnel with a specific address configured with the -ATUN AddrLOCation, CUADDress or BroadCastAddr parameters. NoAddress indicates that each received frame is sent on every tunnel. In most configurations, Address should be set for central site ports when appropriate (depending on the protocol frame format being used), and NoAddress should be set for remote site ports. The default is NoAddress.

BCAddr | NoBCAddr — BCAddr indicates that frames whose address matches the -ATUN BroadCastAddr parameter are forwarded to all configured CUs (all tunnels) on the port. NoBCAddr indicates that all frames are forwarded to all configured CUs on the port. This option applies only when the Address option is selected. The default is NoBCAddr.

ForcePoll | NoForcePoll	When set to ForcePoll, the bridge/router keeps track of which tunnel a frame was last sent to. Data arriving from that tunnel is forwarded to the port; data from other tunnels is discarded. If the last frame from the port was sent to all tunnels (either no addressing or broadcast), any tunnel may transmit data to the port. If the last frame from the port was addressed to a nonexistent CU, no tunnel may transmit. This restriction is per-tunnel instead of per-address. The bridge/router will not distinguish between different addresses within a single CU address range definition. When set to NoForcePoll, the bridge/router will not keep track of which tunnel a frame was last sent to. The ForcePoll value filters out delayed responses or spurious data from other tunnels when a polling host has polled a specific tunnel and is expecting a response only from that tunnel. Protocols and devices that do not operate in a pure master and slave mode should not use this parameter (for example, devices that do not allow unsolicited data from remote sites).
TestEcho | NoTestEcho	TestEcho places the port in a special test mode. When set to TestEcho, asynch data received is echoed back out the port. The data stream is still framed as set with the configured ATUN parameters, but addressing is not used. ATUN statistics count valid and error frames separately, but all frames are echoed. In TestEcho mode, any data received from a CU tunnel is also echoed back to the tunnel. These frames are counted in the CUInfo display. When set to NoTestEcho, the port operates normally. Data from the port is forwarded to CU tunnels according to the configuration and data from the tunnels is forwarded to the port.

PortCU

Syntax

```
ADD !<port> -ATUN PortCU <CU name>...
DELete !<port> -ATUN PortCU <CU name>...
SHow [!<port>] -ATUN PortCU
```

Default No default

Description The PortCU parameter defines CU names and assigns them to ports. You can define or remove multiple CUs by entering a single command. A CU name is a string of up to eight alphanumeric characters. CU names must be unique on the bridge/router. A port with -ATUN PortCONTrol set to RemoteSite may only have one CU assigned.

A specific configuration will have practical limits to the number of CUs dependent on asynch and WAN link speeds, tunnel concentration, and device response-time constraints. The configuration limit on the number of CUs assigned to a port is 256 because of the constraint on non-overlapping CU addresses, but the practical limit will be significantly lower.

RemoteMac

Syntax

```
SETDefault !<CU name> -ATUN RemoteMac = <address>
SHow [!<CU name>] -ATUN RemoteMac
```

Default 000000000000

Description The RemoteMac parameter sets the MAC address for the remote tunnel endpoint. The value specified must match the LocalMac parameter of the peer CU configuration. The local MAC must be in the LAA range.

RemoteSap

Syntax

```
SETDefault !<CU name> -ATUN RemoteSap = <sap> (hex 04-ec[by 4])
SHow [!<CU name>] -ATUN RemoteSap
```

Default E8

Description The RemoteSap parameter sets the SAP for the remote tunnel endpoint. The value specified must match the LocalSap parameter of the peer CU configuration.

10 AUDITLOG SERVICE PARAMETERS

This chapter describes all the parameters in the AuditLog Service. The AuditLog Service sends log messages to a Syslog daemon running on a specified network management station when a message variable is specified with the AUDitLog command. Table 10-1 lists the AuditLog Service parameters and commands.

Table 10-1 AuditLog Service Parameters and Commands

Parameters	**Commands**
CONFiguration	SHow
CONTrol	SETDefault, SHow
LocalFacility	SETDefault, SHow
LogServerAddr	SETDefault, Show

CONFiguration

Syntax

```
SHow -AuditLog CONFiguration
```

Default No default

Description The CONFiguration parameter displays the values of the AuditLog Service parameters.

CONTrol

Syntax

```
SETDefault -AuditLog CONtrol = [AuditTrail |NoAuditTrail],
  [COnfig|NoCOnfig], [ MEssages|NoMessages], [SEcurity|NoSEcurity]
SHow -AuditLog CONTrol
```

Default NoAuditTrail, NoCOnfig, NoMEssages, NoSEcurity

Description The CONTrol parameter selects whether or not the AuditLog Service logs events in each of four categories to the network management station. Each category of log messages is assigned a preset Syslog priority level as follows:

AuditTrail	LogINfo
COnfig	LogWarning
MEssage	LogNotice
SEcurity	LogALert

Values

AuditTrail Log Audit Trail messages using the SYSLOG daemon to the network management station identified by the LogServerAddr parameter. This class of messages is logged to Remote Boot and Configuration Services (RBCS) servers. For more information about audit trail messages, see the RBCS manpages.

No AuditTrail Specifies that no log Audit Trail messages are recorded.

COnfig	Logs commands and parameters that successfully changed configurations.
NoCOnfig	Does not log configuration change commands.
MEssages	Indicates Log System Service Messages and Dial History messages (under the POrt Service).
NoMEssages	Specifies no log System Messages or Dial History messages.
SEcurity	Specifies log messages concerning failed login attempts, failed set privilege, or invalid SNMP community strings.
NoSEcurity	Indicates to not log security-related messages.

LocalFacility

Syntax

```
SETDefault -AuditLog LocalFacility = <0-7>
SHow -AuditLog LocalFacility
```

Default 7

Description The LocalFacility parameter specifies a value representing the Syslog facility (LOCAL0 through LOCAL7) to which log messages are directed. This parameter may be applied to all log message categories.

LogServerAddr

Syntax

```
SETDefault -AuditLog LogServerAddr = <IP address>
SHow -AuditLog LogServerAddr
```

Default 0.0.0.0

Description The LogServer parameter specifies the Internet Protocol (IP) address of a network management station intended to store the log file. The network management station must have the syslog daemon running and be configured with the correct syslog.conf configuration file.

11

BCN Service Parameters

This chapter describes the parameters in the Boundary Routing at Central Node (BCN) Service. Table 11-1 lists the BCN Service parameters and commands.

Table 11-1 BCN Service Parameters and Commands

Parameters	Commands
CONFiguration	SHow, SHowDefault
CONTrol	SETDefault, SHow, SHowDefault
IbmStatus	SHow
LclNonIbmDlci	SETDefault, SHow
RemNonIbmDlci	SETDefault, SHow
RemoteLanType	SETDefault, SHow, SHowDefault
X25ProtID	SETDefault, SHow, SHowDefault

CONFiguration

Syntax

```
SHow [!<port> | !*] -BCN CONFiguration
SHowDefault [!<port> | !*] -BCN CONFiguration
```

Default No default

Description The CONFiguration parameter displays the Boundary Routing settings for the specified port or all ports.

CONTrol

Syntax

```
SETDefault !<port> -BCN CONTrol = ([Enabled | Disabled],
[CentralMac | NoCentralMac], [SmartFiltering |
NoSmartFiltering],[IbmTraffic | NoIbmTraffic])
SHow [!<port> | !*] -BCN CONTrol
SHowDefault [!<port> | !*] -BCN CONTrol
```

Default Disabled, NoCentralMac, NoSmartFiltering, NoIbmTraffic

Description The CONTrol parameter enables or disables the following on a Boundary Routing port:

- Boundary Routing of non-IBM traffic
- Use of a reserved media access control (MAC) address
- Smart filtering in an Internetwork Packet Exchange (IPX) environment
- Boundary Routing of IBM traffic

For more information on each of these features, refer to Chapter 32 in *Using NETBuilder Family Software*.

If you enable or disable the Boundary Routing of non-IBM or IBM traffic or the use of a reserved MAC address, you must re-enable the -PORT CONTrol parameter for configuration to take effect. If you enable or disable smart filtering in an IPX environment, you must re-enable the -BCN CONTrol parameter for the configuration to take effect.

Values

Enabled | Disabled	Enables or disables Boundary Routing on the specified port of the central node. By default, Disabled is selected for all ports.
CentralMac | NoCentralMac	Enables or disables the use of an internally saved MAC address for the Boundary Routing port on the central and alternate central nodes. Use of this MAC address depends on the protocols being run and may be required when configuring a Boundary Routing environment for network resiliency.
SmartFiltering | NoSmartFiltering	Enables or disables smart filtering if you are using the IPX protocol in your Boundary Routing topology. Smart filtering reduces or eliminates periodic broadcast packets generated by IPX routing and packets generated by protocol islands to reduce WAN costs in small remote offices and use bandwidth more efficiently.
IbmTraffic | NoIbmTraffic	Enables or disables Boundary Routing of IBM traffic on the specified port of the central node. By enabling Boundary Routing of IBM traffic, you are activating smart polling, which extends the existing smart filtering feature to IBM Boundary Routing topologies. You are also activating local termination and the automatic prioritization of Systems Network Architecture (SNA) and NetBIOS traffic.

IbmStatus

Syntax

```
SHow [!<port> | !*] -BCN IbmStatus
```

Default No default

Description The IbmStatus parameter displays the status of the Boundary Routing ports over which IBM traffic is running. A display appears only if the -BCN CONTrol parameter has been set to IbmTraffic.

LclNonIbmDlci

Syntax

```
SETDefault !<virtual port ID> -BCN LclNonIbmDlci = <dlci number
(16-991)>
SHow !<virtual port ID> -BCN LclNonIbmDlci
SHowDefault [!<port> | !*] -BCN LclNonIbmDlci
```

Default 0

Description The LclNonIbmDlci parameter configures the DLCI that will be used for non-SNA traffic at the central site. When this parameter is set to the default value of 0, a single PVC is used for all traffic types. Any other value indicates that dual PVCs will be used.

RemNonIbmDlci

Syntax

```
SETDefault !<virtual port ID> -BCN RemNonIbmDlci = <dlci number
(16-991)>
SHow !<virtual port ID> -BCN RemNonIbmDlci
SHowDefault [!<port> | !*] -BCN RemNonIbmDlci
```

Default 0

Description The RemNonIbmDlci parameter configures the Frame Relay Data Link Connection Identifier (DLCI) that will be used for non-IBM traffic at remote site (leaf node) when using a dual PVC configuration. The DLCI is transmitted to the remote site using the Simple Management Network Protocol (SNMP).

Before the settings (or changes) to this parameter can take effect, the port must be enabled (or re-enabled) using the -PORT CONTrol parameter.

RemoteLanType

Syntax

```
SETDefault !<port> -BCN RemoteLanType = ETHernet | TokenRing
SHow [!<port> | !*] -BCN RemoteLanType
SHowDefault [!<port> | !*] -BCN RemoteLanType
```

Default ETHernet

Description The RemoteLanType parameter identifies for a port the type of media to which the Boundary Routing peripheral node is connected. You can configure this parameter on a NETBuilder II bridge/router only; it is not configurable on a SuperStack II boundary router.

The SHow -BCN RemoteLanType command displays the media type for all ports; the SHow !<port > -BCN RemoteLanType command displays the media type for the specified port. For more information, refer to Chapter 32 in *Using NETBuilder Family Software*.

Value		
	ETHernet | TokenRing	Indicates that the peripheral node is connected to an Ethernet LAN or a token ring LAN.

X25ProtID

Syntax

```
SETDefault !<port> -BCN X25ProtID = <protocol id> (octet)
SHow [!<port> | !*] -BCN X25ProtID
SHowDefault [!<port> | !*] -BCN X25ProtID
```

Default 0xDD

Description The X25ProtID parameter specifies a protocol identifier to be included in outgoing X.25 call requests. The protocol identifier indicates that only boundary-routed packets are exchanged over the virtual circuit that is established after the call is completed. Enter a hex value between 1 and 0xFF.

When a packet reaches its destination, the destination 3Com bridge/router verifies this protocol identifier against its own protocol identifier. If they match, the incoming call is accepted. If they do not match, the call is rejected (that is, either Boundary Routing is not running on the destination device or Boundary Routing is running on the destination device but is using a different protocol identifier). The chosen value must not conflict with that used by other protocols.

12

BGP SERVICE PARAMETERS

This chapter describes the Border Gateway Protocol (BGP) Service parameters. BGP is an interdomain routing protocol that distributes network reachability information between autonomous systems (AS). Table 12-1 lists the BGP Service parameters and commands.

Table 12-1 BGP Service Parameters and Commands

Parameters	Commands
AggregateExcept	ADD, DELete, SHow
AggregateRange	ADD, DELete, SHow
AsFilter	ADD, DELete, SHow
ASPath	SHow
AsPolicyAll	ADD, DELete, SHow
AsPolicyExt	ADD, DELete, SHow
AsPolicyInt	ADD, DELete, SHow
AsPolicyPeer	ADD, DELete, SHow
CONFiguration	SHow
CONTrol	SETDefault, SHow
CurrentPeeR	SET, SHow
DEBug	SETDefault, SHow
DefaultNet	ADD, DELete, SHow
DefaultWeight	SETDefault, SHow
DisplayFilter	SET, SHow
HoldTime	SETDefault, SHow
InteriorPolicy	ADD, DELete, SHow
LocalAS	SETDefault, SHow
MaxPeers	SETDefault, SHow
NetworkFilter	ADD, DELete, SHow
NetPolicyAll	ADD, DELete, SHow
NetPolicyExt	ADD, DELete, SHow
NetPolicyInt	ADD, DELete, SHow
NetPolicyPeer	ADD, DELete, SHow
PEER	ADD, DELete, SHow
PeerAS	SETDefault, SHow
PeerControl	SETDefault, SHow
PeerIpAddress	ADD, DELete, SHow
PeerMetric	SETDefault, SHow
PeerVersion	SHow
PeerWeight	SETDefault, SHow
ROUte	SHow

Unlike other services, the BGP Service does not automatically save settings to nonvolatile storage when a SETDefault, ADD, or DELete operation is performed. The parameters are only saved to disk every ten operations. If you want to force an immediate save of BGP parameters, use the SAve command after you use the SETDefault, ADD, and DELete operations.

AggregateExcept

Syntax

```
ADD -BGP AggregateExcept <IP address> {<mask> | <prefix length>}
DELete -BGP AggregateExcept {<IP address> {<mask> |
  <prefix length>}} | All
SHow -BGP AggregateExcept
```

Default No default exception

Description The AggregateExcept parameter adds, deletes, and displays a list of constituent routes that BGP explicitly advertises even if it falls within the aggregate range.

The route is specified by the pair of Internet Protocol (IP) address and mask.

Use the ADD command to add a list of routes to be explicitly advertised. Use the DELete command to remove a single route or all routes. Use the SHow command to display the list of exception routes.

Values

<IP address>	Specifies the IP address in dotted decimal notation of the route that BGP advertises.
<mask>	Specifies the network mask to be applied to the IP address. The network mask can be specified using dotted decimal notation.
<prefix length>	Provides an alternate method to specify a network mask. Specifies the length in bits of the IP address prefix (the number of left-most contiguous 1s in the network mask).
All	Allows all aggregate exception routes to be deleted.

AggregateRange

Syntax

```
ADD -BGP AggregateRange <IP address> {<mask> | <prefix length>}
  [Aggregator]
DELete -BGP AggregateRange {<IP address> {<mask> |
  <prefix length>}} | All
SHow -BGP AggregateRange
```

Default No default range

Description The AggregateRange parameter adds, deletes, and displays a list of supernets that BGP advertises. All of the subnets within the specified supernet range are aggregated into the associated supernet, except for the subnets specified by the AggregateExcept parameter.

Use the ADD command to add a list of supernets. Use the DELete command to delete supernet routes. Use the SHow command to display the list of supernets.

Use the NetPolicyAll parameter to list more specific routes that need to be explicitly advertised. For different type of peers (all, external, internal, peers), different sets of network policy lists can be specified. For more information, refer to "NetPolicyAll" on page 12-13, "NetPolicyExt" on page 12-14, "NetPolicyInt" on page 12-14, and "NetPolicyPeer" on page 12-15.

Values

<IP address> Specifies the IP address in dotted decimal notation of the supernet that BGP advertises.

<mask> Specifies the network mask to be applied to the IP address. The network mask can be specified using dotted decimal notation.

<prefix length> An alternate method of specifying a network mask. Specifies the length in bits of the IP address prefix (the number of left-most contiguous 1s in the network mask).

Aggregator Specifies if the optional transitive AS path attribute AGGREGATOR is included in the updates of this aggregate route. Using this keyword allows the BGP speaker performing route aggregation to advertise its own AS as the autonomous system that performed the aggregation.

All Allows all supernets to be deleted.

AsFilter

Syntax

```
ADD -BGP AsFilter <AsfilterID> "<regular expression>"
DELete -BGP AsFilter <AsfilterID> | ALL
SHow -BGP AsFilter [<AsfilterID>] [Long]
```

Default No default

Description The AsFilter parameter adds, deletes, or displays filters. Filters are made up of the AS-path regular expression. AS path filters are used in conjunction with the AsPolicyPeer, AsPolicyExt, AsPolicyInt, and AsPolicyAll parameters.

Each AS number in the AS path has a leading and trailing blank. These blanks must be included in any AS filter definition. For example, AS45 must be written _45_ (the blank spaces are represented here as underscores (_); you must enter a blank space for each underscore). For example, to create filter 4 that identifies an AS-PATH attribute containing the AS Sequence <AS5, AS46, AS32>, enter:

```
ADD -BGP AsFilter 4 "<_5_ _46_ _32_>".
```

To add an AS filter, the filterID must be specified. To overwrite an existing AS filter, delete it first and then add the new filter.

When deleting AS filters, you can delete a specific filter by specifying the filter ID or all filters by using the keyword ALL.

You can display a specific AS filter by specifying the filter ID or display all filters by using the SHow -BGP AsFilter command. When you use the SHow command with the Long option, the software displays each filter and the peers that are using them. Also displayed are unused filters and filters that peers refer to but are not currently defined.

If a policy is deleted that is still in use by a peer, the peer configuration is left unchanged. Policies that are no longer available in the peer configuration are marked with an asterisk.

For complete information on regular expressions, refer to Appendix K in *Reference for NETBuilder Family Software*.

ASPath

Syntax

```
SHow -BGP ASPath [Debug] [Filter]
```

Default No default

Description The ASPath parameter displays all the AS paths stored in the AS path database. For each path stored, networks that are associated with this path and the BGP peers that are using this AS path are displayed.

When displaying AS paths, the following syntax is used:

```
<>: AS SEQUENCE
[]: AS SET
```

Values

Debug Displays detailed information about the path attributes associated with AS paths.

Filter Applies the setting of the DisplayFilter parameter to filter the AS path database display.

Example A display similar to the following is generated with the SHow -BGP ASPath command:

```
--------------------------------ASPaths-------------------------
Total Path Attributes = 288
<>: AS Sequence; []: AS Set
{< 704  701  690  2149 >}
{< 704  701  690  174 >}
{< 704  701  1280  174 >}
{< 704 >[ 701  1239  35  3365 ]}
```

AsPolicyAll

Syntax

```
ADD -BGP AsPolicyAll <AsfilterID> [Permit | Deny [In | Out |
  Both]] | [Weight <weight>]
DELete -BGP AsPolicyAll [<AsfilterID> [Permit | Deny | Weight]]
  | All
SHow -BGP AsPolicyAll [<AsfilterID>]
```

Default No policies are defined for all peers.

Description The AsPolicyAll parameter applies an AS policy to all peers. Two kinds of policies are possible: weights and permit/deny. Weight policies control the route selection process and permit/deny policies to filter incoming and outgoing routes.

When adding a policy, you must specify an AsfilterID and the policy type (weight or permit/deny). To create a filter, refer to “AsFilter” on page 12-3.

Values

Permit | Deny | Weight Controls the route selection process. Permit or deny policies can be applied to incoming routes, outgoing advertisements, or to both. Weight policies are implicitly applied only to incoming routing updates. All policies in a particular direction (in/out) must either be permit or deny. A mix of permit and deny policies causes ambiguity and the entire policy list will be ignored.

<weight> The weight specified in the parameter is a numeric value.

In | Out | Both — Identifies how the policy should be applied. In indicates that the policy should be applied to incoming route updates. Out indicates that the AS policy should be applied to outgoing advertisements. Both indicates that the network filter should be applied to both directions.

When you define a set of permit policies, any route that does not match any of the permit policies is discarded (or not advertised). Similarly, when all the policies in a given direction are deny policies, only those routes that match are discarded and all other routes are allowed.

When you define a set of weight policies, an incoming route may match one or more policies. For each policy that matches the AS path of a route, the corresponding weight specified for that policy is added to the AS path. The sum of the default weight, or PeerWeight if specified, and all matching weight policies are stored on AS path.

When multiple routes to a network are available, the cumulative weight of each AS path is compared, and the route with the greater weight is selected as the primary route.

AsPolicyExt

Syntax

```
ADD -BGP AsPolicyExt <AsfilterID> [Permit | Deny [In | Out |
  Both]] | [Weight <weight>]
DELete -BGP AsPolicyExt [<AsfilterID> [Permit | Deny | Weight]] |
  All
SHow -BGP AsPolicyExt [AsfilterID]
```

Default No policies are defined for external peers.

Description The AsPolicyExt parameter applies an AS policy to peers that are configured with AS numbers other than the local AS. These peers are communicating through an “external” BGP session.

Two kinds of policies are possible: weights and permit/deny. You can use weight policies control the route selection process and permit/deny policies filter incoming and outgoing routes.

When adding a policy, you must specify an AsfilterID and the policy type (weight or permit/deny). To create a filter, refer to “AsFilter” on page 12-3.

Values

Permit | Deny | Weight — Controls the route selection process. Permit or deny policies can be applied to incoming routes, outgoing advertisements, or to both. Weight policies are implicitly applied only to incoming routing updates. All policies in a particular direction (in/out) must either be permit or deny. A mix of permit and deny policies causes ambiguity and the entire policy list will be ignored.

<weight> — The weight specified in the parameter is a numeric value.

In | Out | Both — Identifies how the policy should be applied. In indicates that the policy should be applied to incoming route updates. Out indicates that the AS policy should be applied to outgoing advertisements. Both indicates that the network filter should be applied to both directions.

When you define a set of permit policies, any route that does not match any of the permit policies is discarded (or not advertised). Similarly, when all the policies in a given direction are deny policies, only those routes that match are discarded and all other routes are allowed.

When you define a set of weight policies, an incoming route may match one or more policies. For each policy that matches the AS path of a route, the corresponding weight specified for that policy is added to the AS path. The sum of the default weight, or PeerWeight if specified, and all matching weight policies are stored on AS path.

When multiple routes to a network are available, the cumulative weight of each AS path is compared, and the route with the greater weight is selected as the primary route.

AsPolicyInt

Syntax

```
ADD -BGP AsPolicyInt <AsfilterID> [Permit | Deny [In | Out |
  Both]] | [Weight <weight>]
DELete -BGP AsPolicyInt [<AsfilterID> [Permit | Deny | Weight]]
  | All
SHow -BGP AsPolicyInt [<AsfilterID>]
```

Default No policies are defined for internal BGP sessions.

Description The AsPolicyInt parameter applies AS policy to peers running internal BGP, which are configured to have the same AS number as the local AS. these peers they are communicating through an “external” BGP session.

Two kinds of policies are possible: weights and permit/deny. Weight policies control the route selection process and permit/deny policies filter incoming and outgoing routes.

When adding a policy, you must specify an AsfilterID and the policy type (weight or permit/deny). To create a filter, refer to “AsFilter” on page 12-3.

Values

Permit | Deny | Weight	Controls the route selection process. Permit or deny policies can be applied to incoming routes, outgoing advertisements, or to both. Weight policies are implicitly applied only to incoming routing updates. All policies in a particular direction (in/out) must either be permit or deny. A mix of permit and deny policies causes ambiguity and the entire policy list will be ignored.
<weight>	The weight specified in the parameter is a numeric value.
In | Out | Both	Identifies how the policy should be applied. In indicates that the policy should be applied to incoming route updates. Out indicates that the AS policy should be applied to outgoing advertisements. Both indicates that the network filter should be applied to both directions.

When you define a set of permit policies, any route that does not match any of the permit policies is discarded (or not advertised). Similarly, when all the policies in a given direction are deny policies, only those routes that match are discarded and all other routes are allowed.

When you define a set of weight policies, an incoming route may match one or more policies. For each policy that matches the AS path of a route, the corresponding weight specified for that policy is added to the AS path. The sum of the default weight, or PeerWeight if specified, and all matching weight policies are stored on AS path.

When multiple routes to a network are available, the cumulative weight of each AS path is compared, and the route with the greater weight is selected as the primary route.

AsPolicyPeer

Syntax

```
ADD [!<IP address>] -BGP AsPolicyPeer <AsfilterID> [Permit | Deny
  [In | Out | Both]] | [Weight <weight>]
DELete [!<IPaddress>] -BGP AsPolicyPeer [<AsfilterID> [Permit |
  Deny | Weight]] | All
SHow [!<IP address>] -BGP AsPolicyPeer [<AsfilterID>]
```

Default No policies are defined per peer.

Description The AsPolicyPeer parameter applies AS policy to a specific peer.

Two kinds of policies are possible: weights and permit/deny. Weight policies control the route selection process and permit/deny policies filter incoming and outgoing routes.

When adding a policy, you must specify an AsfilterID and the policy type (weight or permit/deny). To create a filter, refer to “AsFilter” on page 12-3.

Values

Permit | Deny | Weight	Controls the route selection process. Permit or deny policies can be applied to incoming routes, outgoing advertisements, or to both. Weight policies are implicitly applied only to incoming routing updates. All policies in a particular direction (in/out) must either be permit or deny. A mix of permit and deny policies causes ambiguity and the entire policy list will be ignored.
In | Out | Both	Identifies how the policy should be applied. In indicates that the policy should be applied to incoming route updates. Out indicates that the AS policy should be applied to outgoing advertisements. Both indicates that the network filter should be applied to both directions.
<weight>	The weight specified in the parameter is a numeric value.

When you define a set of permit policies, any route that does not match any of the permit policies is discarded (or not advertised). Similarly, when all the policies in a given direction are deny policies, only those routes that match are discarded and all other routes are allowed.

When you define a set of weight policies, an incoming route may match one or more policies. For each policy that matches the AS path of a route, the corresponding weight specified for that policy is added to the AS path. The sum of the default weight, or PeerWeight if specified, and all matching weight policies are stored on AS path.

When multiple routes to a network are available, the cumulative weight of each AS path is compared, and the route with the greater weight is selected as the primary route.

CONFiguration

Syntax

```
SHow -BGP CONFiguration
```

Default No default

Description The CONFiguration parameter displays all the BGP configurations.

CONTrol

Syntax

```
SETDefault -BGP CONTrol = ([Enable | Disable], [AGgregate |
  NoAGgregate])
SHow -BGP CONTrol
```

Default Disable, NoAGgregate

Description The CONTrol parameter controls the overall behavior of BGP, including BGP route aggregation.

Values

Enable | Disable

Enables or disables the BGP Protocol. The Enable value causes the router to initiate a BGP session for each configured peer that has been enabled and allows other routers to initiate BGP sessions with this router.

The Disable value causes all existing BGP sessions to terminate. All routes learned through BGP in the routing table are deleted. Any incoming BGP connection attempts are rejected.

When BGP is enabled, setting the parameter to Enable is the same as disabling and reenabling BGP.

AGgregate | NoAGgregate

Enables or disables BGP route aggregation. The AGgregate value causes the router to aggregate the eligible subnets into the supernet based on the settings of the AggregateExcept and AggregateRange parameters.

NoAGgregate prevents the router from aggregating any routes.

CurrentPeeR

Syntax

```
SET -BGP CurrentPeeR = <IP address> | None
SHow -BGP CurrentPeeR
```

Default 0.0.0.0

Description The CurrentPeeR parameter sets the peer context for any commands that are being executed. You can set the peer context within a command on a per command basis or set the current peer.

If the IP address is not specified for a command, the current peer is used for parameters that apply on a per-peer basis.

DEBug

Syntax

```
SETDefault -BGP DEBug = ([All | None], [State | NoState],
  [Msg |NoMsg], [Memory | NoMemory], [Error | NoError], [Timer
  | NoTimer], [Unreach | NoUnreach], [RtEntry | NoRtEntry],
  [RteRror | NoRteRror], [RtState | NoRtState], [RtXtra |
  NoRtXtra])
SHow -BGP DEBug
```

Default None

Description The DEBug parameter traces various events and displays them on the console. This parameter is only used for diagnostic purposes to trace errant BGP code behavior and is meant only for internal code development by 3Com engineers.

Values

All	Traces all events.
State	Traces connection state machine changes.
Msg	Traces and displays messages.
Memory	Traces the freeing and allocation of buffer memory.
Error	Traces and displays connection management errors.
Timer	Traces and displays timer expiration.
Unreach	Traces unreachables.
RtEntry	Provides entry point tracing of BGP code.
RteRror	Displays routing table management errors.
RtState	Displays routing state machine changes.
RtXtra	Displays additional information for the routing table.

DefaultNet

Syntax

```
ADD -BGP DefaultNet <IP address>
DELete -BGP DefaultNet <IP address> | ALL
SHow -BGP DefaultNet
```

Default No default routes are configured.

Description The DefaultNet parameter selectively configures, deletes, or displays a default route in the BGP Routing Table. This parameter is beneficial when a particular BGP implementation does not advertise a default route.

If there is no route for a particular destination address in the BGP Routing Table, then the system checks to see if any default networks were configured. The configured address may not be a directly connected network. For each configured default network, the system checks to determine if a route exists for the configured default network. The configured default network is reachable through an entry that exists in the BGP Routing Table. If a route exists, the system uses the next-hop for the route to the default network address in the BGP Routing Table to route the packet. If all default networks have been scanned and no route is found, then the software continues with the normal route look-up precedence as described in "Multipath Routing" on page 6-40 in *Using NETBuilder Family Software*.

To configure a default network, use the ADD command and specify an IP address.

To remove a default network, use the DELete command and specify the desired IP address. To remove all default networks, use the DELete command and specify the keyword ALL.

To display all default networks, use the SHow command.

DefaultWeight

Syntax

```
SETDefault -BGP DefaultWeight = <number>(-2000 – 2000)
SHow -BGP DefaultWeight
```

Default 0

Description The DefaultWeight parameter configures the default weight to be applied to each route when computing route weights. This default weight is used in combination with peer specific weight (PeerWeight) and route specific weights (using AS policies) to determine the exact weight of a route. The resulting weight is stored along with a route. Routes with the highest weight are the routes to be advertised to neighbors.

If you change this parameter, all route selection processes must be recomputed. Because the route selection process has to be recomputed, 3Com recommends that all BGP sessions be restarted when policies or weights are modified.

DisplayFilter

Syntax

```
SET -BGP DisplayFilter = "<regular expression>"
SHow -BGP DisplayFilter
```

Default " "

Description The DisplayFilter parameter filters the display of the ROUte and ASPath parameters to show only the information that you specify with the regular expression in the SET -BGP DisplayFilter command.

After specifying a regular expression with the SET -BGP DisplayFilter command, and when the SHow -BGP ROUte Filter or SHow -BGP ASPath Filter commands are issued, the display is filtered based on the value of the DisplayFilter parameter. For information about regular expressions, refer to Appendix K in *Using NETBuilder Family Software*.

For every ROUte entry or for every ASPath entry, the regular expression specified by DisplayFilter is applied. If a match is found, the entry is displayed. Otherwise, the entry is not displayed.

If no DisplayFilter is specified, or the Filter option for the ROUte or ASPath parameter is not used, then all entries are displayed.

Example 1 To display only the routing entries with the next-hop gateway address of 129.213.16.9, enter:

```
SET -BGP DisplayFilter = "129.213.16.9"
SHow -BGP ROUte Filter
```

Only entries that have "129.213.16.9" in the BGP Routing Table are displayed.

The entry “129.213.16.9” may occur in fields other than the next-hop gateway, and these entries will also be displayed.

Example 2 To display only the ASPath entries that have AS 701 followed by AS 3057, enter:

```
SET -BGP DisplayFilter = “_701_ _3057_”
SHow -BGP ASPath Filter
```

Each AS number in the AS path has a leading and trailing blank. Blank spaces are represented here as underscores (_). When two spaces are shown together, a space has been inserted between the underscores, for example _ _. You must enter a blank space for each underscore shown.

HoldTime

Syntax

```
SETDefault -BGP HoldTime = <seconds>(0–65535)
SHow -BGP HoldTime
```

Default 180 seconds

Description The HoldTime parameter defines the interval of time (seconds) that a router waits before declaring a peer dead after receiving the last keepalive message. When a peer is declared dead, all the routes learned from that peer are deleted from the routing table. All other peers are unreachable for these routes.

If the HoldTime parameter is set to 0, the keepalive mechanism is disabled. However, even when disabled, a non-zero hold time is used while the connection is being established, to prevent the connection from hanging.

InteriorPolicy

Syntax

```
ADD -BGP InteriorPolicy <NetfilterID> [Permit | Deny]
DELete -BGP InteriorPolicy [<NetfilterID> [Permit | Deny]] | All
SHow -BGP InteriorPolicy [<filterid>]
```

Default No default (No policy is configured and all interior or intra-AS routes are imported into BGP.)

Description The InteriorPolicy parameter specifies a network or a range of networks that can be imported into BGP from an Interior Gateway Protocol (IGP) such as Routing Information Protocol (RIP), or Open Shortest Path Firtst (OSPF), including directly connected networks and statically configured routes.

The filter ID used is an ID of a filter defined by the ADD NetworkFilter command. An operation specified with the filter ID indicates if this route should or should not be imported into the BGP Routing Table from the IGP Routing Table.

You must specify the policy as either all “permit” filters or all “deny” filters. All policies in a particular direction (in/out) must either be permit or deny. A mix of permit and deny policies causes ambiguity and the entire policy list is ignored.

When you define a set of permit policies, only those networks that do not match the same interior policy are discarded (or not advertised through BGP). Similarly, when all the policies in a given direction are deny policies, only those routes that match the interior policy are discarded and all others are allowed.

LocalAS

Syntax

```
SETDefault -BGP LocalAS = <AS Number>(0–65535)
SHow -BGP LocalAS
```

Default 0

Description The LocalAS parameter defines the AS number used by this BGP speaker in the OPEN message and in all routing updates as the originating AS number.

The local AS number determines if a peer is connected through an "internal" BGP session (same AS number as the peer) or an "external" BGP session (different AS numbers).

MaxPeers

Syntax

```
SETDefault -BGP MaxPeers = <number>(0–128)
SHow -BGP MaxPeers
```

Default 32 peers

Description The MaxPeers parameter controls the maximum number of peers supported and is used to optimize the memory use of the router when maintaining neighbor state machines. To change this number, you must shut down all BGP activity by disabling BGP.

Increasing the value of the MaxPeers parameter directly affects memory use per route learned through BGP. 3Com recommends that this number be increased only when absolutely necessary.

NetworkFilter

Syntax

```
ADD -BGP NetworkFilter <NetfilterID> <network address> <mask>
DELete -BGP NetworkFilter <NetfilterID> | ALL
SHow -BGP NetworkFilter [<NetfilterID>] [Long]
```

Default No default (no network filters defined)

Description The NetworkFilter parameter adds, deletes, and displays network filters. These filters are made up of two components: the *network address* and the *mask*.

The network address and mask are used to determine if a network route qualifies for the operation. Each bit in a mask that is set to 0 indicates a wildcard or "don't care" position for the mask.

When displaying network filters, you can display a specific filter by specifying the filter ID or display all filters by using the SHow -BGP NetworkFilter command. When you use the SHow command with the Long option, the software displays each filter and the peers that are using them. Also displayed are unused filters and filters that peers refer to but are not currently defined.

If a policy is deleted that is still in use by a peer, the peer configuration is left unchanged. However, policies that are no longer available in the peer configuration are marked with an asterisk.

Example 1 To allow incoming routes to network 192.2.100.0 to be accepted for peer 10.0.0.2, enter:

```
ADD -BGP NetworkFilter 1 192.2.100.0 255.255.255.0
ADD -BGP !10.0.0.2 NetPolicyPeer 1 Permit In
```

If this was the only permit policy defined, all other routes from peer 10.0.0.2 would be discarded.

Example 2 To configure this router to not advertise any network numbers that have 192 as the first byte when sending updates to peer 10.0.0.2, enter:

```
ADD -BGP NetworkFilter 2 192.0.0.0 255.0.0.0
ADD -BGP !10.0.0.2 NetPolicyPeer 2 Deny Out
```

NetPolicyAll

Syntax

```
ADD -BGP NetPolicyAll <NetfilterID> {Permit | Deny [In | Out |
  Both]} | Explicit
DELete -BGP NetPolicyAll {<NetfilterID> [Permit | Deny |
  Explicit]} | All
SHow -BGP NetPolicyAll [<NetfilterID>]
```

Default No default

Description The NetPolicyAll parameter applies network policies to all peers. Network policies are used to filter the receipt and advertisement of routes based on the network address specified in a routing update.

When adding a policy, you must specify a <NetfilterID> and the policy type: permit or deny.

You can delete all policies by specifying the keyword All, policies of a specific <NetfilterID>, or policies of a specific <NetfilterID> and specific direction.

Values

<NetFilterID>	Specifies the name of a filter policy.
Permit | Deny	Controls network policies. Permit or deny policies can be applied to incoming routes, outgoing advertisements, or to both. All policies in one direction (in or out) must either be permit or deny. A mix of permit and deny policies causes ambiguity and the entire policy list is ignored.
Explicit	If Explicit is specified, the selected routes are explicitly advertised, even though they are included in the aggregate range. Explicit policies are implicitly applied only to outgoing constituent routes of aggregates.
In | Out | Both	Identifies how the policy should be applied. In indicates that the policy should be applied to incoming route updates. Out indicates that the network filter should be applied to outgoing advertisements. Both indicates that the network filter should be applied to both directions.

When you define a set of permit policies, any route that does not match any of the permit policies is discarded (or not advertised). Similarly, when all the policies in a given direction are deny policies, only matching routes are discarded and all other routes are allowed.

NetPolicyExt

Syntax

```
ADD -BGP NetPolicyExt <NetfilterID> {Permit | Deny [In | Out |
  Both]} | Explicit
DELete -BGP NetPolicyExt {<NetfilterID> [Permit | Deny |
  Explicit]} | All
SHow -BGP NetPolicyExt [<NetfilterID>]
```

Default No default

Description The NetPolicyExt parameter applies network policies to all peers that are in an AS different from the local AS, These peers are running external BGP sessions. Network policies are used to filter the receipt and advertisement of routes based on the network address specified in a routing update.

When adding a policy, you must specify a <NetfilterID> and the policy type: permit or deny.

You can delete all policies by specifying the keyword All, policies of a specific <NetfilterID>, or policies of a specific <NetfilterID> and specific direction.

Values

<NetFilterID> Specifies the name of a filter policy.

Permit | Deny Controls network policies. Permit or deny policies can be applied to incoming routes, outgoing advertisements, or to both. All policies in one direction (in or out) must either be permit or deny. A mix of permit and deny policies causes ambiguity and the entire policy list is ignored.

Explicit If Explicit is specified, the selected routes are explicitly advertised, even though they are included in the aggregate range. Explicit policies are implicitly applied only to outgoing constituent routes of aggregates.

In | Out | Both Identifies how the policy should be applied. In indicates that the policy should be applied to incoming route updates. Out indicates that the network filter should be applied to outgoing advertisements. Both indicates that the network filter should be applied to both directions.

When you define a set of permit policies, any route that does not match any of the permit policies is discarded (or not advertised). Similarly, when all the policies in a given direction are deny policies, only matching routes are discarded and all other routes are allowed.

NetPolicyInt

Syntax

```
ADD -BGP NetPolicyInt <NetfilterID> {Permit | Deny [In |Out |
  Both]} | Explicit
DELete -BGP NetPolicyInt {<NetfilterID> [Permit | Deny |
  Explicit]} | All
SHow -BGP NetPolicyInt [<NetfilterID>]
```

Default No default

Description The NetPolicyInt parameter applies network policies to all peers that are the same AS as the local peer. These peers are running internal BGP sessions.

Network policies are used to filter the receipt and advertisement of routes based on the network address specified in a routing update.

When adding a policy, you must specify a <NetfilterID> and the policy type: permit or deny.

You can delete all policies by specifying the keyword All, policies of a specific <NetfilterID>, or policies of a specific <NetfilterID> and specific direction.

Values

<NetFilterID> Specifies the name of a filter policy.

Permit | Deny Controls network policies. Permit or deny policies can be applied to incoming routes, outgoing advertisements, or to both. All policies in one direction (in or out) must either be permit or deny. A mix of permit and deny policies causes ambiguity and the entire policy list is ignored.

Explicit If Explicit is specified, the selected routes are explicitly advertised, even though they are included in the aggregate range. Explicit policies are implicitly applied only to outgoing constituent routes of aggregates.

In | Out | Both Identifies how the policy should be applied. In indicates that the policy should be applied to incoming route updates. Out indicates that the network filter should be applied to outgoing advertisements. Both indicates that the network filter should be applied to both directions.

When you define a set of permit policies, any route that does not match any of the permit policies is discarded (or not advertised). Similarly, when all the policies in a given direction are deny policies, only matching routes are discarded and all other routes are allowed.

NetPolicyPeer

Syntax

```
ADD [!<IP address>] -BGP NetPolicyPeer <NetfilterID> {Permit |
  Deny [In | Out | Both]} | Explicit
DELete [!<IP address>] -BGP NetPolicyPeer {<NetfilterID> [Permit |
  Deny | Explicit]} | All
SHow -BGP NetPolicyPeer [<NetfilterID>]
```

Default No default

Description The NetPolicyPeer parameter applies network policies to a specific peer. Network policies are used to filter the receipt and advertisement of routes based on the network address specified in a routing update.

When adding a policy, you must specify a <NetfilterID> and policy type: permit or deny.

You can delete all policies by specifying the keyword All, policies of a specific <NetfilterID>, or policies of a specific <NetfilterID> and specific direction.

Values

<NetFilterID> Specifies the name of a filter policy.

Permit | Deny Controls network policies. Permit or deny policies can be applied to incoming routes, outgoing advertisements, or to both. All policies in one direction (in or out) must either be permit or deny. A mix of permit and deny policies causes ambiguity and the entire policy list is ignored.

Explicit	If Explicit is specified, the selected routes are explicitly advertised, even though they are included in the aggregate range. Explicit policies are implicitly applied only to outgoing constituent routes of aggregates.
In | Out | Both	Identifies how the policy should be applied. In indicates that the policy should be applied to incoming route updates. Out indicates that the network filter should be applied to outgoing advertisements. Both indicates that the network filter should be applied to both directions.

When you define a set of permit policies, any route that does not match any of the permit policies is discarded (or not advertised). Similarly, when all the policies in a given direction are deny policies, only matching routes are discarded and all other routes are allowed.

PEER

Syntax

```
ADD -BGP PEER <IP address> <AS Number>
DELete -BGP PEER <IP address>
SHow -BGP PEER [<IP address>] [Long]
```

Default No peers

Description The PEER parameter adds, deletes, or displays a peer configuration. Deleting a peer deletes all peer-specific configuration information associated with that peer, for example, Network Policies, AS Policies, Weight, Version, Metric, and IP addresses. When using the ADD and DELete commands, the IP address must be specified.

When using the SHow command, the IP address is optional. If the IP address is not specified, all BGP peers are displayed. When you specify the Long option, a complete display of all the configurations relevant to that peer is displayed, including Current state, Control, IP addresses, Network Policies, AS Policies, Version, Weight, and Metric.

The SHow -BGP PEER display shows the current mapping of Peer ID to IP address to AS number and shows the current state of the peer, for example, disabled, open, connecting.

There can only be one peer per IP address and one IP address per peer.

PeerAS

Syntax

```
SETDefault [!<IP address>] -BGP PeerAS = <AS Number>(0–65535)
SHow [!<IP address>] -BGP PeerAS
```

Default Assigned when peer is created.

Description The PeerAS parameter modifies the AS number assigned to a peer when it is first created.

PeerControl

Syntax

```
SETDefault [!<IP address>] -BGP PeerControl = ([Enable | Disable])
SHow [!<IP address>] -BGP PeerControl
```

Default Disable

Description The PeerControl parameter individually enables or disables a specific peer. When a peer is created with the ADD -BGP PEER command, the peer is initially set up to be disabled. You need to add relevant policies for that peer and then enable the peer.

You can disable a peer by setting the control to disable. If the peer is active at the time, the session is closed and all routing information learned from that session is removed from the routing table.

If a peer is already enabled and you set the PeerControl parameter to enable, you are performing the same step as disabling and reenabling the peer.

PeerIpAddress

Syntax

```
ADD [!<IP address>] -BGP PeerIpAddress <IP address>
DELete [!<IP address>] -BGP PeerIpAddress <IP address>
SHow [!<IP address>] -BGP PeerIpAddress
```

Default Initially the list of peers is determined by those peers added using the ADD -BGP PEER command.

Description The PeerIpAddress parameter adds a set of IP addresses that are considered to be equivalent. This parameter does not allow you to create new peers. You create new peers using the ADD -BGP PEER command. After a set of peers has been defined, the you can add additional IP addresses, which are equivalent to the peers already defined.

Making peers equivalent is useful if a connection can be accepted from multiple IP addresses (but need to be considered exactly equivalent), and saves the effort of defining a separate filter or policy database for a each member of a set of equivalent peers.

PeerMetric

Syntax

```
SETDefault [!<IP address>] -BGP PeerMetric = <number>(0–10000)
SHow [!<IP address>] -BGP PeerMetric
```

Default 0 (Disabled)

Description The PeerMetric parameter configures the metric to be used when advertising routes. The metric is sent as part of a BGP routing update as the Multi-Exit-DISC attribute (BGP-4).

This metric is used by BGP in the route-selection process. Routes with lower values of this metric are preferred over routes with higher values of the metric.

Setting the metric to 0 disables the generation of the attribute. When you change this value, you need to re-advertise of all routes to a peer by shutting down and restarting the BGP session with the particular peer whose metric has been changed.

PeerVersion

Syntax

```
SHow -BGP PeerVersion
```

Default No peers configured

Description The PeerVersion parameter displays the BGP version number. Only version 4 is currently supported.

PeerWeight

Syntax

```
SETDefault [!<IP address>] -BGP PeerWeight = <weight>(-2000 –
  2000)
SHow [!<IP address>] -BGP PeerWeight
```

Default 0

Description The PeerWeight parameter configures the specific weight to be applied when computing route weights. If you do not configure a peer with a specific weight, the default value is used.

The PeerWeight parameter is used to give certain neighbors higher or lower priority when comparing multiple routes through different neighbors to a network. A higher value weight results in routes through that neighbor selected over other routes.

When you change the PeerWeight setting, the route-selection procedures are recomputed. As a result, if any new paths are computed to have a better path weight, a BGP update packet is issued to all BGP peers to inform them of this change. Only peers with the configured peer weight are displayed.

ROUte

Syntax

```
SHow -BGP ROUte [<IP address> | I | E] [Debug] [Filter]
```

Default No default

Description The ROUte parameter displays a table of all the routes learned through BGP and routes imported into BGP through configuration of the InteriorPolicy parameter. Before a route is advertised, the relevant policies are applied to this table. A route in this table is advertised only if the polices allow.

Values

<IP address>	Displays the route entry if there is a route to the specified address.
I	Displays interior routes learned through BGP.
E	Displays external routes learned through BGP.
Debug	Displays more detailed information about each entry. This option can be used for debugging as well as for providing a more detailed look at some of the routing entry attributes.
Filter	If the Filter option is specified, the setting of the DisplayFilter parameter is applied to filter the BGP Routing Table display.

Example The SHow ROUte command generates a table similar to the following:

```
---------------------------BGP Routing Table-----------------------------
Total Networks = 7, Total Paths 7, Total Path Attributes 4
ASPath:    <>: AS Sequence;       []: AS Set
Destination     Mask           Gateway       Peer          ASPath
128.49.0.0      255.255.0.0    198.6.253.13  198.6.253.13  {< 704  701  690  22 >}
128.160.0.0     255.255.0.0    198.6.253.13  198.6.253.13  {< 704  701  690  22 >}
128.206.0.0     255.255.0.0    198.6.253.13  198.6.253.13  {< 704  701  1239  2572 >}
129.34.0.0      255.255.0.0    198.6.253.13  198.6.253.13  {< 704  701  690  1747 >}
129.72.0.0      255.255.0.0    198.6.253.13  198.6.253.13  {< 704  701  1239  2902 >}
129.131.0.0     255.255.0.0    198.6.253.13  198.6.253.13  {< 704  701  690  22 >}
129.213.128.0   255.255.252.0  --            --            InteriorPol
Total Networks Displayed = 7
```

The meaning of the display elements and column headings are as follows:

Total Networks
Total number of distinct destinations that have an existing route in the BGP Routing Table.

Total Paths
Count of all the various paths or routes to all the destination networks. A given destination network may have more than one path to reach it.

Total Path Attributes
Count of the total number of distinct path attributes that exist. Several routes may have the same set of path attributes. To view the distinct set of path attributes, enter:

SHow -BGP ASPath

Destination
Destination network for which a route exists.

Mask
Network mask for this destination.

Gateway
Next-hop address for this destination.

Peer
Router to which the BGP session is established.

ASPath
AS numbers traversed to reach destination.

Total Networks Displayed
Count of the number of networks.

13

BOOTPC SERVICE PARAMETERS

This chapter describes the BOOTPCLient (BOOTPC) Service parameters. BOOTP Client provides a way for a network device to retrieve all of its Internet Protocol (IP) address-related information. BOOTP Client is implemented on each interface and is user-configurable.

Table 13-1 lists the BOOTPC Service parameters and commands.

Table 13-1 BOOTPC Service Parameters and Commands

Parameters	Commands
CONFiguration	SHow
CONTrol	SETDefault, SHow
RequestStatus	SHow
RetryCount	SETDefault, SHow
RetryInterval	SETDefault, SHow

CONFiguration

Syntax

```
SHow [!<port>] -BOOTPC CONFiguration
```

Default No default

Description The CONFiguration parameter displays all the current parameter values associated with the BOOTP Client. If you specify a particular port, only the parameter values associated with that port are displayed.

CONTrol

Syntax

```
SETDefault !<port> -BOOTPC CONTrol = [Enable | Disable]
SHow [!<port>] -BOOTPC CONTrol
```

Default Enable

Description The CONTrol parameter controls how the system handles BOOTREQUEST packets.

If the CONTrol parameter is set to Enable and the port is up, BOOTP Client is activated and the system sends out a BOOTREQUEST packet to acquire its IP address for that port. If the parameter is set to Disable, any BOOTREQUEST packet waiting in a queue to be transmitted through the port is removed and any BOOTREPLY packet received through the port is discarded.

For Enable to take effect on a specific port, the following conditions must be met:

- If you set a non-zero client, there should be no IP address configured for this port when the system is in router mode and no IP address configured for !0 mode.
- If you set a !0 client, no IP address should be configured.

If port !0 is specified, it assumes the system is entering *host mode* and BOOTREQUEST packets are sent through all the IP interfaces. The IP address extracted from the first BOOTREPLY packet, no matter which interface receives this reply packet, is set as the whole unit's network address. All of the following reply packets are discarded. If the -IP CONTrol parameter is set to ROute, it is reset to NoROute when the IP address is obtained from BOOTREPLY packet.

The SHow command displays the current value of the parameter.

RequestStatus

Syntax

```
SHow [!<port>] -BOOTPC RequestStatus
```

Default No default

Description The RequestStatus parameter displays the current BOOTP Client state as follows:

Idle	No activity.
Wait for BOOTREPLY	BOOTREQUEST packet sent out, waiting for reply packet.
No BOOTREPLY received	No valid reply packet received before time-out and retries.
Got an IP address	Received BOOTREPLY with your own IP address.

RetryCount

Syntax

```
SETDefault !<port> -BOOTPC RetryCount = <value> (0–40)
SHow [!<port>] -BOOTPC RetryCount
```

Default 5

Description The RetryCount parameter controls how many times the BOOTREQUEST packet is sent before receiving a BOOTREPLY packet. If you set this parameter to 0, the BOOTREQUEST packet is transmitted indefinitely until the BOOTREPLY packet is received.

You must re-enable the port if you want the new setting to take effect immediately.

RetryInterval

Syntax

```
SETDefault !<port> -BOOTPC RetryInterval = <seconds> (1–10)
SHow [!<port>] -BOOTPC RetryInterval
```

Default 1

Description The RetryInterval parameter controls the starting timer that retransmits a BOOTREQUEST packet. A BOOTREQUEST packet is retransmitted until a BOOTREPLY packet is received or until it reaches its timeout value (see RetryCount parameter above). The default starting timer is 1 second and the allowable maximum value is 10 seconds. This timer is doubled for each retransmission until it reaches 10 minutes.

You must re-enable the CONTrol parameter for the new setting to take effect immediately.

14

BRIDGE SERVICE PARAMETERS

This chapter describes BRidge Service parameters for operating your bridge/router as a bridge. Table 14-1 lists the BRidge Service parameters and commands.

Table 14-1 BRidge Service Parameters and Commands

Parameters	Commands
AgeTime	SETDefault, SHow
AllRoutes	FLush, SHow
APPletalk	SETDefault, SHow
ATMNeighbor	ADD, DELete, SHow
BLimitTimer	SETDefault, SHow
BroadCastLimit	SETDefault, SHow
CONFiguration	SHow
CONTrol	SETDefault, SHow
DatalinkAddrFmt	SETDefault, SHow, SHowDefault
DlciNeighbor	ADD, DELete, SHow
DStSecurity	SETDefault, SHow
FunctionalAddr	ADD, DELete, SHow
MultiCastAddr	ADD, DELete, SHow
ROUte	ADD, DELete, SHow
RouteTableSize	SETDefault, SHow
RptStationHop	SETDefault, SHow, SHowDefault
SMDSGroupAddr	SETDefault, SHow, SHowDefault
SRcSecurity	SETDefault, SHow
TransparentBRidge	SETDefault, SHow
X25Neighbor	ADD, DELete, SHow
X25PROFileid	SETDefault, SHow
X25ProtID	SETDefault, SHow, SHowDefault

AgeTime

Syntax

```
SETDefault -BRidge AgeTime = <seconds> (10–1000000)
SHow -BRidge AgeTime
```

Default 300

Description The AgeTime parameter specifies the number of seconds a device can be dormant before it is deleted from the routing table. A device is considered dormant if it is not transmitting packets. For more information on how the bridge learns about other devices on the extended network and creates entries in the routing table, refer to Chapter 3 in *Using NETBuilder Family Software*.

AllRoutes

Syntax

```
FLush [!<port>] -BRidge AllRoutes
SHow [!<port> | !*] -BRidge AllRoutes [<address_mask> [<start>
   [<count>]]]
```

Default No default

Description The AllRoutes parameter displays the routing table, including learned and user-defined routes. The FLush command removes all the learned entries.

The following display is generated by the SHow command:

```
No.  Station Address    Port           Depth   Age      WAN ID
1    %080002A00AEF      Local          0       Local    –
2    %080002A00AF0      Local          0       Local    –
3    %FFFFFFFFFFFF      PortsAndLocal  0       Static   –
4    %080001001111      2              0       Static   –
5    %080002003589      1              0       Young    –
6    %080002A000A0      1              0       Young    –
7    %080002013E98      1              0       Young    –
8    %0207010037FE      1              0       Young    –
9    %080002001234      3              0       Young    128
-- Entries displayed = 9  Total table entries = 49
```

In this display, No. indicates the order in which the routes are displayed in the routing table. Station Address is the media access control (MAC) address of the learned or user-defined device. Port is the port to which packets for that destination are forwarded. Depth indicates the number of entries in the routing table containing the same low-order 16-bit MAC address. Age indicates the approximate fraction of AgeTime since the bridge knew of a packet from that station. WanID is the specified wide area network address, for example, a Frame Relay data link control identifier (DLCI), an switched multimegabit data service (SMDS) individual address, an X.25 DTE address, or an ATM virtual channel identifier (VCID) of a permanent virtual circuit (PVC). For more information about the WanID, refer to “ROUte” on page 14-8.

In the Port field, a PortsAndLocal entry indicates the multicast or broadcast address that is provided to the local bridge/router and forwarded to other ports.

The following list explains the possible values for Age:

Local Address belonging to the bridge/router that is displaying the routing table.

Static Address is a user-defined address.

Young Less than one-third of the time specified by the AgeTime parameter has elapsed.

Middle More than one-third of the time specified by the AgeTime parameter has elapsed.

Values <address_mask> Displays only the entry for a particular address or range of addresses. The address must be a MAC address in hexadecimal preceded by a percent sign (%), with the leading zeros significant. The address mask may include one or more asterisks (*). The asterisk represents a wildcard character, which means “any value.” For example:

```
SHow !1 -BRidge AllRoutes %0800*
```

This example displays all entries in the routing table on port 1 that contain addresses that start with %0800.

<start>	Starting entry number. For example, if the value for start is 21, the display contains entries starting with entry number 21.
<count>	Number of entries to be displayed.

Example The following command displays 10 entries in the routing table on port 1, starting from entry number 21. The asterisk in the address mask field indicates that entries are displayed regardless of MAC address. The address mask field is mandatory because the start and count fields are specified, and the command is field-position-sensitive.

```
SHow !1 -BRidge AllRoutes * 21 10
```

APPletalk

Syntax

```
SETDefault -BRidge APPletalk = Enable | Disable
SHow -BRidge APPletalk
```

Default Enable

Description The APPletalk parameter enables the bridge to forward packets between Ethernet and fiber distributed data interface (FDDI) networks with proper encapsulation, according to recommended IEEE practice. When this parameter is set to Enable, the original format of both AT-1 (Ethernet) and AT-2 (subnetwork access protocol) (SNAP) packets is preserved when bridging between Ethernets over an FDDI backbone. If the APPletalk parameter is disabled, AT-2 packets are converted to Ethernet format after going across the FDDI backbone.

ATMNeighbor

Syntax

```
ADD !<port> -BRidge ATMNeighbor = <VCID>
DELete !<port> -BRidge ATMNeighbor = <VCID>
SHow [!<port> | !*] -BRidge ATMNeighbor
```

Default No default (no ATM neighbors are configured)

Description The ATMNeighbor parameter specifies the local VCID of the PVC for each neighbor on the ATM network that supports transparent bridging. You can configure a maximum of 256 ATM bridge neighbors on a single virtual port. VCIDs are mapped to the VPI.VCI and configured using the -ATM PermVirCircuit parameter. For more information, refer to “PermVirCircuit” on page 7-2.

You can add neighbors by using the ADD command. If the VCID is already in the Bridge Neighbor Table, no change occurs.

You can delete the VCIDs that are no longer needed from the table one at a time by using the DELete command.

You can display the contents of the Bridge Neighbor Table for either a specified port or for all ports using the SHow command.

BLimitTimer

Syntax
```
SETDefault -BRidge BLimitTimer = [<milliseconds> (400 | 600 | 800 |
   1000) | Disabled ]
```

Default Disabled

Description The BLimitTimer parameter selects the timer interval for the broadcast limit mechanism that limits the maximum rate at which broadcast and multicast packets are forwarded through bridged ports. This parameter is useful in large bridged network environments where high levels of broadcast traffic can affect the performance of some network devices. This parameter can be used in both transparent bridging and source route bridging environments. In source route bridging environments, you can use this parameter to reduce explorer frames for unicast and multicast broadcast packets.

The broadcast limit mechanism works by counting the number of broadcast and multicast packets received during each timer interval. Broadcast and multicast packets are forwarded during a timer interval until the broadcast limit threshold (described later in this chapter) for the port is reached. Once the threshold has been reached, no additional broadcast or multicast packets are forwarded on the port until the start of the next timer interval. At that point, broadcast and multicast forwarding is resumed. This parameter works in conjunction with the BroadcastLimit parameter described in this chapter.

The broadcast limit mechanism is disabled when the BLimitTimer parameter is set to Disabled. The total number of packets discarded by the broadcast limit mechanism and the number of timer intervals in which packets were discarded are displayed in bridge statistics (refer to Appendix H in *Using NETBuilder Family Software*.

Enabling the broadcast limit mechanism can adversely affect system performance.

BroadCastLimit

Syntax
```
SETDefault !<port> -BRidge BroadCastLimit = <packets per second>
   (0–100000)
SHow [!<port> | !*] -BRidge BroadCastLimit
```

Default 0

Description The BroadCastLimit parameter sets the maximum rate (in packets per second) at which broadcast packets are forwarded through a bridged port. The BroadCastLimit affects both broadcast and multicast packets, and is used with the BLimitTimer parameter described earlier in this section. Setting BroadCastLimit to 0 disables this feature on the port. This parameter can be used for both transparent bridging and source route bridging environments.

CONFiguration

Syntax
```
SHow -BRidge CONFiguration
```

Default No default

Description The CONFiguration parameter displays current and default values for the CONTrol and AgeTime parameters and the status of ports and paths.

The first part of the screen shows the current values of CONTrol and AgeTime. The remaining lines indicate the status of each port and its associated paths. These lines include the following types of information

Name String currently assigned to the port or path.

State State of the port determined by the spanning tree algorithm. The state is Listening immediately after the bridge is booted or after Bridge is selected for the CONTrol parameter, and then transitions to Learning. If the spanning tree algorithm determines that the port should forward packets, the state becomes Forwarding; otherwise, it becomes Blocking. If NoBridge is selected for the CONTrol parameter, the state is Blocking. For more information, refer to "CONTrol" on page 14-5.

Type Whether the port is attached to an Ethernet, token ring, or FDDI network, or remotely through a wide area connection.

Status For ports, the status is either Reachable or Unreachable. Reachable indicates that the network to which the port is connected can be reached through at least one of its paths. Unreachable indicates that the network cannot be reached because all its paths are down.

For paths, the status can be one of the following:

DOWN The path is out of operation.

LOOPBACK This status is specific to serial lines. Packets sent out on this line are received back by the bridge. This occurs, for example, on lines that have a modem on which the loopback setting has not been disabled. You can use loopback detection to verify the basic functionality of an interface.

Up The path is in normal operation.

The date and time following the path status indicate when the path's status last changed.

SRcSec Source explicit forwarding and blocking states. The value can be one of the following:

None Forwards all packets.

Fwd Forwards only packets from sources permanently entered in the routing table.

Blk Blocks only packets from sources permanently entered in the routing table.

DStSec Destination explicit forwarding and blocking states. The value can be one of the following:

None Forwards all packets.

Fwd Forwards only packets to destinations permanently entered in the routing table.

Blk Blocks only packets to destinations permanently entered in the routing table.

CONTrol

Syntax

```
SETDefault -BRidge CONTrol = ([Aging | NoAging], [Bridge | NoBridge],
    [FOrward | NoFOrward], [Learn | NoLearn], [IPFragment |
    NoIPFragment], [FireWall | NoFireWall])
SHow -BRidge CONTrol
```

Default Aging, NoBridge, FOrward, LEarn, NoIPFragment, NoFireWall

In bridge-only software, the default value is Bridge.

Description The CONTrol parameter determines whether the bridge performs bridging and establishes the characteristics of the bridging function. The values apply to the global bridging function, not to a particular interface.

Values

Aging | NoAging	Determines whether nodes that have not transmitted packets for a specified time are deleted from the routing table. The time is specified by the AgeTime parameter. Select Aging in a new installation or where nodes can be moved from one network to another. To improve performance, select NoAging. If NoLEarn is selected, NoAging is selected automatically. Selecting LEarn has no effect on Aging or NoAging.
Bridge | NoBridge	Whether the bridge performs the bridging function. When Bridge is selected, the bridge participates in the spanning tree configuration. Select NoBridge only when you want the bridge to operate as a router with no concurrent bridging.
FOrward | NoFOrward	Whether the bridge forwards packets. Selecting NoFOrward allows isolation of attached networks for network management or diagnostic purposes. Select NoFOrward as a temporary measure to isolate faults.
LEarn | NoLEarn	Whether the bridge creates and updates entries in its routing tables. For information on the relationship between learning and aging, refer to the discussion of Aging | NoAging.
IPFragment | NoIPFragment	Whether fragmentation occurs whenever an MTU mismatch is encountered in the forwarding path for transparently bridged packets. The default is NoIPFragment.
FireWall | NoFireWall	Important only when the system is performing both bridging and routing. Before setting this value, refer to the descriptions in Chapter 3 of *Using NETBuilder Family Software*.

3Com recommends setting -BRidge CONTrol to FireWall if IP or AppleTalk filters are defined.

DatalinkAddrFmt

Syntax

```
SETDefault !<port> -BRidge DatalinkAddrFmt = Performance | Standard
SHow [!<port> | !*] -BRidge DatalinkAddrFmt
SHowDefault [!<port> | !*] -BRidge DatalinkAddrFmt
```

Default Performance

Description The DatalinkAddrFmt parameter determines how the bridge interprets the MAC header type for different data link address formats when handling bridged packets over WAN interfaces. Normally, the MAC header in bridged encapsulated packets over WAN media is in canonical format. However, some implementations, such as token ring (802.5) and FDDI, normally use noncanonical format. This parameter can be used to configure the bridge/router to automatically convert different MAC header formats if necessary. This parameter applies on serial interfaces only.

Values

Performance Connects two 3Com bridges. You can use Standard mode when connecting two 3Com bridges, but it is not recommended because of the effect on performance.

Standard Connects a 3Com bridge to a bridge from another vendor. In this mode, the 3Com bridge conforms to the standards used by the other bridge.

DlciNeighbor

Syntax

```
ADD !<port> -BRidge DlciNeighbor = <dlci>
DELete !<port> -BRidge DlciNeighbor = <dlci> | All
SHow [!<port> | !*] -BRidge DlciNeighbor
```

Default No default

Description The DlciNeighbor parameter adds a data link connection identifier (DLCI) neighbor to the static DLCI Neighbor Table. If the DLCI is already in the table, no change occurs. You can delete DLCIs that are no longer needed from the table one at a time, or you can delete all entries for the specified port by specifying the All option. If LMI protocol is running consortium LMI, the valid range for subscriber numbers is 16–1022. For other LMI protocols, the range is 16–991.

The SHow command displays the contents of the DLCI Neighbor Table for either a specified port or all ports. In addition to static entries, the SHow command displays DLCIs that are dynamically learned by the bridge/router if the -FR CONTrol parameter is set to either LMI or ANsiLMI (ANsiLMI is the default setting). For information on the -FR CONTrol parameter, refer to Chapter 25. The static table takes precedence over the dynamic table; entries in the dynamic table are used only when the static DLCI Table for the port is empty.

DStSecurity

Syntax

```
SETDefault !<port> -BRidge DStSecurity = None | Fwd | Blk
SHow [!<port> | !*] -BRidge DStSecurity
```

Default None

⚠ **CAUTION:** *Before you use the DStSecurity parameter, read the description and examples in Chapter 3 in Using NETBuilder Family Software. Using this parameter incorrectly may cause the bridge to discard packets you want to forward or to forward packets that you want to discard.*

Description The DStSecurity parameter is a security feature that controls packets sent to specific destinations on a per-port basis. This parameter is used in conjunction with the routing table.

A packet is forwarded or discarded based on the following criteria:

- The value of the DStSecurity parameter
- Whether the packet's destination address is a static entry in the routing table

After you have decided which packets should be forwarded and which should be discarded, set the DStSecurity feature to a value that requires configuring the minimum number of static entries.

Packets that meet forwarding conditions are not guaranteed to be forwarded; they can be subject to blocking because of other constraints such as filtering or source explicit blocking.

Setting DStSecurity to either Fwd or Blk can adversely affect performance.

Values

None	Allows packets to be forwarded to any destination.
Fwd	Allows only packets for destination addresses listed as static entries in the Bridge Routing Table to be forwarded.
Blk	Allows only packets for destination addresses listed as static entries in the Bridge Routing Table to be blocked.

FunctionalAddr

Syntax

```
ADD -BRidge FunctionalAddr = %<address> MultiCastAddr = %<address>
DELete -BRidge FunctionalAddr All | %<address>
SHow -BRidge FunctionalAddr
```

Default 3Com maintains a table of functional-address-to-multicast-address mappings for well-known protocols. These defaults cannot be deleted. The default display and entry is canonical format.

Description The FunctionalAddr parameter adds functional-address-to-multicast-address mappings, and is used in a bridging environment where communication between end stations on different LAN media (for example, FDDI and Ethernet) is necessary.

MultiCastAddr

Syntax

```
ADD -BRidge MultiCastAddr = %<address> FunctionalAddr = %<address>
DELete -BRidge MultiCastAddr All | %<address>
SHow -BRidge MultiCastAddr
```

Default 3Com maintains a table of multicast-address-to-functional-address mappings for well-known protocols. These defaults cannot be deleted. The default display and entry is in canonical format.

Description The MultiCastAddr parameter adds multicast-address-to-functional-address mappings, and is used in a bridging environment where communication between end stations on different LAN media (for example, FDDI and Ethernet) is necessary.

ROUte

Syntax

```
ADD [!<port>] -BRidge ROUte All | <MAC address> [[SMDS | DTE | DLCI |
   ATM <WanID>] Off]
DELete [!<port>] -BRidge ROUte All | <MAC address>
SHow [!<port> | !*] -BRidge ROUte
```

Default No default

Description The ROUte parameter modifies the routing table used by the bridge. This parameter affects only user-defined (static) entries in the routing table.

Routing table entries indicate where packets containing the specified destination address should be forwarded. The routing table can contain two types of entries: those the bridge learns from the network, called learned (dynamic) entries, and those you assign using the ADD -BRidge ROUte command, called user-assigned (static) entries.

Learned entries are subject to dynamic change or deletion whenever Aging and LEarn are selected for the CONTrol parameter. Static entries are saved on the local floppy disk or flash memory drive. These entries can only be changed or deleted using the ADD or DELete -BRidge commands. If you are using a floppy disk, make sure the disk is in the drive before entering commands such as ADD, DELete, and SHow.

To change all dynamically learned entries in the Bridge Routing Table to static entries, enter:

```
ADD -BRidge ROUte All
```

To delete all static entries except the local and broadcast entries, enter:

```
DELete -BRidge ROUte All
```

⚠ **CAUTION:** *When you change the owner for any WAN port, you must delete all static routes that were configured for the previous owner and WAN type. Use the DELete -BRidge ROUte command to delete these routes. Failing to delete the routes can cause a crash (fatal error) in NETBuilder software.*

ADD and DELete commands support both canonical and noncanonical data entry, as follows:

```
ADD !<port> -BRidge ROUte %<address>
ADD !<port> -BRidge ROUte mac <address>
ADD !<port> -BRidge ROUte ncmac <address>
DELete !<port> -BRidge ROUte %<address>
DELete !<port> -BRidge ROUte mac <address>
DELete !<port> -BRidge ROUte ncmac <address>
```

Canonical entry is the default. For example, to add a static route in canonical format, enter:

```
ADD !1 -BRidge ROUte %02608CA4E004
```

or

```
ADD !1 -BRidge ROUte mac 02608CA4E004
```

To add a static route in noncanonical format, enter:

```
ADD !1 -BRidge ROUte ncmac 400631250720
```

Values All When used with the ADD command, specifies that all learned entries are marked as static entries in the routing table. When used with the DELete command, specifies that all static entries are deleted from the routing table.

<MAC address> Destination MAC address.

With the ADD command you can specify one of the following optional values after the address:

SMDS — SMDS individual address of the neighbor. The dollar sign ($) can be used in place of the word SMDS.

DTE — Data terminal equipment (DTE) address for X.25. The pound sign (#) can be used in place of the word DTE.

DLCI — Data link connection identifier (DLCI) for Frame Relay. The at sign (@) can be used in place of the word DLCI.

ATM — Asynchronous Transfer Mode (ATM) virtual circuit ID (VCID) of the PVC for the ATM neighbor. The and sign (&) can be used in place of the word ATM. VCIDs are mapped to the VPI.VCI and configured using the -ATM PermVirCircuit parameter. For more information, refer to "PermVirCircuit" on page 7-2.

<WanID> — WAN to which packets containing the specified MAC address should be forwarded. The WanID is based on the type of address prefix. For example, if the keyword DTE is specified, the WanID is an X.25 DTE address such as 31104152222.

Off — Disables forwarding of any packet containing the specified address as its destination address.

All packets containing the broadcast address %FFFFFFFFFFFF are forwarded to all attached networks. This entry in the user-assigned (static) table cannot be modified or deleted from the table.

Servers that generate few packets may be deleted from the routing table during the bridge's aging and learning processes. If such a server needs to receive packets, assign an entry to the routing table to specify the routing to that server. Otherwise, the bridge must relearn the server's address. Example 1 for the ROUte parameter shows a typical command used to add an address to the routing table.

The default maximum number of available entries in a routing table varies between 8,167 and 8,171, depending on the configuration. You can change the default size using the RouteTableSize parameter. For more information, refer to "RouteTableSize" on page 14-11.

To create a static route in the routing table, enter the ADD -BRidge ROUte command. Each static entry in the routing table contains a MAC address and a location. It indicates where packets containing that address as the destination address should be forwarded.

Example 1 The following example creates a user-assigned routing table entry that forwards all packets containing the destination address %080002001359 to port 1:

```
ADD !1 -BRidge ROUte %080002001359
```

Example 2 The following example creates a user-assigned routing table entry that disables forwarding of all packets containing the multicast address %AB1234567890. Disabling such packets decreases traffic across the bridge and on destination networks.

```
ADD -BRidge ROUte %AB1234567890 Off
```

Example 3 The following example adds to the routing table an address to a Frame Relay port with a DLCI value of 128 and a MAC (Ethernet) address of %080002001234. Any time a packet with this destination address is forwarded to port 3, which is configured as a Frame Relay port, the DLCI value entered is inserted into the packet as the destination DLCI.

```
ADD !3 -BRidge ROUte %080002001234 DLCI 128
```

Example 4 The following example marks all learned entries in the bridge routing table as bridge static routes. The change from learned to static entries is limited to routes that are learned on individual ports. In addition, the change is made on a sequential basis from the start of the routing table. If the routing table has more learned entries than the maximum size allotted for static routes, only the first of those entries that fit within the static entry limits (512 for the SuperStack II NETBuilder and 2,048 for the NETBuilder II bridge/router) are changed into static entries.

```
ADD -BRidge ROUte All
```

RouteTableSize

Syntax

```
SETDefault -BRidge RouteTableSize = <number> (1–8) or (1–64)
   or (1–2)
SHow -BRidge RouteTableSize
```

Default 8 for NETBuilder II bridge/router
1 for SuperStack II NETBuilder

Description The RouteTableSize parameter configures the size of a bridge's routing table, in multiples of 1,024 entries. The size can vary from 1,024 to 65,535 entries, depending on your NETBuilder platform and its configuration. The size determines the maximum number of stations that can be learned by the bridge. Setting RouteTableSize to 1 configures a maximum of 1,024 entries, 2 configures a maximum of 2,048 entries, and so on.

You can set this parameter to the following values:

- NETBuilder II bridge/router with connection services: 1–8
- NETBuilder II bridge/router without connection services: 1–64
- SuperStack II NETBuilder: 1–2

After changing the RouteTableSize parameter, you must disable bridging (if it is currently enabled) and then re-enable bridging before the parameter value takes effect.

In some configurations, there may not be enough memory available to support a bridge routing table as large as specified by the RouteTableSize parameter. If this is the case, the software displays a message similar to the following: "Bridge Routing Table size reduced to <n> entries," where <n> is the actual number of entries allocated.

Example 1 To configure the bridge table size to 10,240 entries, enter:

```
SETDefault -BRidge RouteTableSize = 10
```

RptStationHop

Syntax

```
SETDefault -BRidge RptStationHop = Enable | Disable
SHow -BRidge RptStationHop
SHowDefault -BRidge RptStationHop
```

Default Disable

Description The RptStationHop parameter keeps track of stations that move from one port to another because of physical movement or external loopback. The movement of a station from one port to another is called an event. A station moving from port 1 to port 2 and then back to port 1 would create two events. If there are events in the sampling interval, the bridge reports them by sending a message to the console. If RptStationHop is enabled and there are no events during the sampling interval, no message is sent. The sample interval is fixed at 10 seconds.

The following example shows the display generated by the SHow -SYS SystemMessages command:

```
Fri May 27 12:05:49 1994 Station Hop
Report:136 events in last 10 secs
```

Displaying system messages can cause performance degradation in packet forwarding. Enable RptStationHop only if you need it.

SMDSGroupAddr

Syntax

```
SETDefault !<port> -BRidge SMDSGroupAddr = $<E0–E999999999999999> |
  None
SHow [!<port> | !*] -BRidge SMDSGroupAddr
SHowDefault [!<port> | !*] -BRidge SMDSGroupAddr
```

Default None

Description The SMDSGroupAddr parameter specifies an SMDS group address that is used by the transparent bridging software when transmitting packets to bridges connected to the SMDS network. You must configure this parameter to use transparent bridging over SMDS. The value is used as the SMDS network destination address when transmitting spanning tree Bridge Protocol Data Units (BPDUs), all bridged broadcast and multicast packets, and bridged packets containing a destination address that has not yet been learned.

For transparent bridging to occur over SMDS, -PORT OWNer must be set to SMDS and -BRidge SMDSGroupAddr must be configured with a valid SMDS group address.

Values

<E0–E999999999999999>	The format for an SMDS group, or multicast, address. The group address type is used to route data to all bridges with the same group address. The group address begins with the letter E and is followed by the 15 digits of the network number. If the number is less than 15 digits long, it is padded on the right with Fs.
None	Removes a group address previously assigned to a port.

SRcSecurity

Syntax

```
SETDefault !<port> -BRidge SRcSecurity = None | Fwd | Blk
SHow [!<port> | !*] -BRidge SRcSecurity
```

Default None

CAUTION: *Before you use the SRcSecurity feature, read the description and examples in Chapter 3 in Using NETBuilder Family Software.Using this feature incorrectly can cause the bridge to discard packets that you want to forward or to forward packets that you want to discard.*

Description The SRcSecurity parameter is a security feature that controls packets sent from specific station sources on a per-port basis. This parameter is used in conjunction with the routing table.

A packet is forwarded or discarded based on the following criteria:

- The value of the SRcSecurity parameter
- Whether the packet's source address is a static entry in the routing table

After you have decided which packets should be forwarded and which should be discarded, set the SRcSecurity feature to a value that requires configuring the minimum number of static entries.

Packets that meet forwarding conditions are not guaranteed to be forwarded; they can be subject to blocking because of other constraints such as filtering or destination explicit blocking.

Setting the SRcSecurity parameter to Fwd or Blk can adversely affect performance.

Values

None	Forwards packets from any address.
Fwd	Forwards only packets from addresses listed on the bridge routing table.
Blk	Blocks only packets from addresses listed on the bridge routing table.

TransparentBRidge

Syntax

```
SETDefault !<port> -BRidge TransparentBRidge = TransparentBRidge |
  NoTransparentBRidge
SHow [!<port> | !*] -BRidge TransparentBRidge
```

Default TransparentBRidge

Description The TransparentBRidge parameter enables or disables bridging on a per-port basis. This parameter is useful if you want bridging on local ports to remain enabled, but want to disable it on WAN ports.

Use the SETDefault -BRidge CONTrol = Bridge command initially to enable the bridging function on all ports. After that, to disable bridging on the ports where it is not required, use the following syntax:

```
SETDefault !<port> -BRidge TransparentBRidge = NoTransparentBRidge
```

This parameter does not apply to SuperStack II NETBuilder models 32x and 52x.

X25Neighbor

Syntax

```
ADD !<port> -BRidge X25Neighbor = <dte_addr> (1–15 digits)
DELete !<port> -BRidge X25Neighbor = <dte_addr> (1–15 digits)
SHow [!<port> | !*] -BRidge X25Neighbor
```

Default No default

Description The X25Neighbor parameter specifies the DTE address of each neighbor that supports transparent bridging. A maximum of 10 neighboring DTEs can be configured from each port supporting bridging over X.25.

X25PROFileid

Syntax

```
SETDefault !<port> -BRidge X25PROFileid = <user profile id> (0–255)
SHow [!<port> | !*] -BRidge X25PROFileid
```

Default 0

Description The X25PROFileid parameter defines an X.25 user profile that is used when X.25 virtual circuits are set up to carry bridged packets. A value of 0 indicates that no X.25 user profile is configured for bridged packets.

X25ProtID

Syntax

```
SETDefault !<port> -BRidge X25ProtID = <protocol id> (1 octet)
SHow [!<port> | !*] -BRidge X25ProtID
SHowDefault [!<port> | !*] -BRidge X25ProtID
```

Default 0xDD

Description The X25ProtID parameter specifies a protocol identifier to be included in an outgoing X.25 call request to indicate that only transparent bridge packets are exchanged over the virtual circuit established when the call is completed. Enter a hexadecimal value between 1 and FF.

When a packet reaches its destination, the destination bridge verifies this protocol identifier against its own protocol ID. If they match, the incoming call is accepted. The call is rejected if they do not match. For example, either transparent bridging is not running on the destination device, or transparent bridging is running on the destination device but is using a different protocol ID. The X25ProtID value must not conflict with the value used by other protocols.

15

BSC SERVICE PARAMETERS

This chapter describes the parameters in the BSC Service. The parameters in this service are used to provide support for Binary Synchronous Communications (BSC, also known as BISYNC) in IBM environments.

Table 15-1 lists the BSC Service parameters and commands.

Table 15-1 BSC Service Parameters and Commands

Parameters	Commands
BscCU	ADD, DELete, SHow
CONFiguration	SHow
CONTrol	SETDefault, SHow
CUCONTrol	SETDefault, SHow
Role	SETDefault, SHow

BscCU

Syntax

```
ADD !<port> -BSC BscCU <cu name> <cu addr> <local mac> <remote mac>
  [Lsap=<value>] [Rsap=<value>] [ENable]
DELete !<port> -BSC BscCU <cu name> | ALL
SHow [!<port>] -BSC BscCU
```

Default No default

Description The BscCU parameter adds or deletes BSC control unit (CU) definitions on a port. With the DELete command, you can delete a single CU definition or all CU definitions. You can only delete CUs that have been disabled (refer to “CUCONTrol” on page 15-2).

Values

<cu name> Enters the CU name. The name can be up to 8 characters. The CU name must be unique on the bridge/router, and it cannot be the name “ALL.” The name is not case-sensitive, but is always displayed how you enter it.

<cu addr> Enters the BSC device address for the CU. Valid values are from 0 to 31 decimals. You can also enter the CU address in EBCDIC format. The CU address must be unique on the port.

<local mac> Enters the MAC address that the other side of the tunnel sends to. The MAC address must be entered in noncanonical format. The local MAC must be in the locally administered address (LAA) range. For more information, refer to Chapter 28 in *Using NETBuilder Family Software*.

<remote mac>	Enters the MAC address that the local bridge/router sends to when BSC traffic is received on the line. The MAC address must be entered in noncanonical format. The remote MAC must be in the LAA range.
Lsap	Enters the local Service Access Point (SAP) number. The value must be in multiples of 4. The default is 4.
Rsap	Enters the remote SAP number. The value must be in multiples of 4. The default is 4.
ENable	ENable allows you to enable the CU without disabling it. The CU will end up in the Enabled state. If you do not specify ENable, you can enable the CU independently using the CUCONTrol parameter.
ALL	Used with the DELete command only. ALL allows you to delete all configured CUs on a port. If any CUs are active on the port, the bridge/router will not allow you to delete any CUs on that port.

CONFiguration

Syntax

```
SHow -BSC CONFiguration
```

Default No default

Description The CONFiguration parameter displays the current BSC configuration.

CONTrol

Syntax

```
SETDefault !<port> -BSC CONTrol = Enable | Disable
SHow [!<port>] -BSC CONTrol
```

Default Disable

Description The CONTrol parameter enables or disables a port for BSC services. If the port is disabled, none of the CUs on that port become active. All ports are disabled for this parameter by default. If a BSC port is disabled, all active CUs on the port are automatically deactivated.

CUCONTrol

Syntax

```
SETDefault !<CU name> -BSC CUCONTrol = <Enable | Disable>
SHow [!<CU name>] -BSC CUCONTrol
```

Default Enable

Description The CUCONTrol parameter enables and disables a CU. If the CU is enabled and the BSC port is enabled, the DLSw circuit for the CU can be established. After the circuit is established, BSC traffic flows when the real primary starts polling. If the CU is disabled, the DLSw circuit is disconnected, and no BSC traffic flows to or from the CU. If the bridge/router is the secondary, polls are ignored by the CU if the CUCONTrol parameter is disabled on the bridge/router. If the bridge/router is the primary, no polls are sent to this CU if it is disabled.

Role

Syntax

```
SETDefault !<port> -BSC Role = Primary | Secondary
SHow [!<port>] -BSC Role
```

Default Secondary

Description The Role parameter defines whether the role of the local BSC port is primary or secondary for the devices it is connecting to.

Values

Primary	Indicates the role of the BSC port on the local bridge/router is primary. At a remote site, the bridge/router role should be set to primary because it acts as a primary and talks to a real secondary CU.
Secondary	Indicates the role of the BSC port on the local bridge/router is secondary. At the host (central) site, the bridge/router role should be set to secondary because it acts as one or more secondary device, and talks to a real primary/host.

16 CLNP SERVICE PARAMETERS

This chapter describes the Connectionless Network Protocol (CLNP) Service parameters that are used for Open System Interconnection (OSI) routing. CLNP parameters are related to the ESIS, ISIS, and IISIS services. Table 16-1 lists the CLNP Service parameters and commands.

Table 16-1 CLNP Service Parameters and Commands

Parameters	Commands
CONFiguration	SHow
CONTrol	SETDefault, SHow
DefaultTTL	SETDefault, SHow
ERgeneration	SETDefault, SHow
ES	ADD, DELete, SHow
IS	SHow
MTU	SETDefault, SHow, SHowDefault
NetEntityTitle	SHow
RDgeneration	SETDefault, SHow
X25PROFileid	SETDefault, SHow

CONFiguration

Syntax

```
SHow -CLNP CONFiguration
```

Default No default display

Description The CONFiguration parameter displays the values of the CLNP parameters, the End System Table, and the Intermediate System Table.

CONTrol

Syntax

```
SETDefault -CLNP CONTrol = ([Route | NoRoute], [ChecKSum | NoChecKSum],
  [SEGment | NoSEGment], [QOS | NoQOS], [ErrReport | NoErrReport],
  [PartialRecRte | NoPartialRecRte])
SHow -CLNP CONTrol
```

Default NoRoute, NoChecKSum, SEGment, NoQOS, ErrReport, NoPartialRecRte

Description The CONTrol parameter determines whether the router performs CLNP routing and determines other characteristics of the CLNP packets.

Values other than Route or NoRoute have no effect on the routing function. CLNP cannot modify a packet format while switching packets. All other values determine the CLNP packet format when the router is originating its own packets.

Values

Route | NoRoute — Route enables the CLNP routing function immediately. A router with CLNP enabled is an intermediate system (IS) to all directly attached networks and sends intermediate system hello (ISH) packets to those networks. Selecting Route automatically enables the End System-to-Intermediate System and ISIS protocols immediately. NoRoute disables CLNP routing immediately and disables ESIS and ISIS protocols.

ChecKSum | NoChecKSum — ChecKSum indicates that the checksum field in CLNP packets originated by the router is computed. NoChecKSum indicates that the checksum field is left as zero.

SEGment | NoSEGment — SEGment indicates that CLNP packets originated by the router include segmentation parts. NoSEGment indicates that the CLNP PDUs cannot be segmented on route to its destination.

QOS | NoQOS — QOS indicates that the CLNP packets originated by the router include the quality of service option. NoQOS indicates that CLNP packets do not include the quality of service option.

ErrReport | NoErrReport — ErrReport indicates that the error report flag is set in the CLNP packets originated by the router. NoErrReport indicates that the error report flag is not suppressed in CLNP packets generated by the end system.

PartialRecRte | NoPartialRecRte — PartialRecRte indicates that CLNP packets originated by the router include the Partial Recording of Route option. NoPartialRecRte indicates that the Partial Recording of Route option is not included.

DefaultTTL

Syntax

```
SETDefault -CLNP DefaultTTL = <half-seconds> (1–255)
SHow -CLNP DefaultTTL
```

Default 48

Description The DefaultTTL parameter specifies the time-to-live (TTL) field in CLNP packets originated by the router.

This parameter applies only to CLNP packets originated by the router.

ERgeneration

Syntax

```
SETDefault -CLNP ERgeneration = [Disable | <millisecond> (60–900)]
SHow -CLNP ERgeneration
```

Default 60

Description The ERgeneration parameter controls the frequency of Error Packets Protocol Data Units (ER PDUs) that can be originated by the router. Error packets are generated by the router to report error events such as destination unreachable or lifetime expired. The ERgeneration parameter prevents the router from generating too many error packets, which can saturate the network.

Values	Disable	Halts generation of all ER PDUs by the router.
	60–900	Specifies in milliseconds the minimal interval between transmission of ER PDUs.

ES

Syntax

```
ADD !<port> -CLNP ES <NSAP address> <SNPA>
DELete !<port> -CLNP ES <NSAP address>
SHow [!<port> | !*] -CLNP ES
```

Default No default (no end systems known to the router)

Description The ES parameter specifies a list of end systems (ESs) known to the router. The ES list changes over time for the following reasons:

- The router constantly learns from the networks through the ESIS protocol. The learned end systems entries are called dynamic entries.
- You can add or delete end systems using the ADD and DELete commands. The entries resulting from this configuration are called static entries. Possible reasons for configuring the ES list include the following:
  - The ES does not support the ESIS protocol.
  - A specific routing path is desired for a particular ES.

Static routes always take precedence over dynamic routes.

To add an ES, use the ADD command. You can specify up to 64 static ES entries.

The Subnetwork Point of Attachment (SNPA) is the media address of the next hop. It may be one of the following:

- The media address of the ES
- The media address of another IS that knows how to route packets to the ES

To delete an ES, use the DELete command.

IS

Syntax

```
SHow -CLNP IS
```

Default No default (no intermediate systems known to the router)

Description The IS parameter specifies a list of intermediate systems known to the router. The IS list changes over time because the router constantly learns from the networks through the ESIS protocol. The learned intermediate systems entries are called dynamic entries.

An IS learns the existence of and establishes adjacency with other neighboring ISs through the ISIS Protocol. An IS is not required to learn about other ISs through the ESIS Protocol, but the information may be useful to users.

MTU

Syntax

```
SETDefault !<port> -CLNP MTU = [Default | 512–4500]
SHow [!<port> | !*] -CLNP MTU
SHowDefault [!<port> | !*] -CLNP MTU
```

Default

1,497 (Ethernet and serial lines)
4,439 (token ring)
4,475 (FDDI)
9,185 (SMDS)

Description

The MTU parameter specifies (in bytes) the maximum transmission unit (MTU) of a CLNP packet on a medium. For example, the default maximum transmission unit of a CLNP packet on Ethernet is 1,497 bytes. The SHow -CLNP MTU command displays the current MTU size. The current MTU size is either the lower value of the MTU size setting or the MTU of the media. The SHowDefault -CLNP MTU command displays user settings of MTU sizes.

NetEntityTitle

Syntax

```
SHow -CLNP NetEntityTitle
```

Default

/49/0053 <Ethernet address of interface 1>00

Description

The NetEntityTitle parameter shows the address used by the router for CLNP and ESIS functions. The address is used in the following ways:

- When the router transmits ISH PDUs
- In ER PDUs generated by the router
- In the Recording of Route option if the CLNP PDU includes this option

The Network Entity Title (NET) is implicitly determined by the -ISIS AreaAddress parameter. It is automatically computed by taking the numerically lowest area address and concatenating it with six octets of MAC address and one octet value of 00 for N-selector. No user configuration is necessary. For more information, refer to “AreaAddress” on page 32-3.

The NET is subject to change when the AreaAddress is changed.

RDgeneration

Syntax

```
SETDefault -CLNP RDgeneration = [Disable | <millisecond> (60–900)]
SHow -CLNP RDgeneration
```

Default

60

Description

The RDgeneration parameter controls the frequency of redirect packets protocol data units (RD PDUs) that can be originated by the router. RD PDUs are generated by an IS and sent to an ES informing the ES that it should use another IS for reaching the destination because there is a better route toward the destination.

A router may need to generate RD PDUs and periodically send them to an ES to assist the ES in selecting the best next-hop IS.

The RDgeneration parameter prevents the router from generating too many RD PDUs, which can saturate the network.

Values

Disable	Selecting Disable halts generation of all ER PDUs by the router.
60–900	Selecting a number from 60 through 900 specifies in milliseconds the minimal interval between transmission of ER PDUs.

X25PROFileid

Syntax

```
SETDefault [!<port>] -CLNP X25PROFileid = <user profile id>
 (0–255)
SHow [!<port> | !*] -CLNP X25PROFileid
```

Default 0

Description The X25PROFileid parameter defines an X.25 user profile that will be used when X.25 virtual circuits are set up to carry CLNP packets. A value of 0 indicates that no specific X.25 user profile is configured for CLNP packets.

17 DECnet Service Parameters

This chapter describes all the parameters that are related to DECnet Phase IV routing and DECnet Phase IV-to-Phase V transition. Table 17-1 lists the DECnet Service parameters and commands.

Table 17-1 DECnet Service Parameters and Commands

Parameters	Commands
ADDRess	SETDefault, SHow
AddressMap	ADD, DELete, SHow
AdvertisePolicy	ADD, DELete, SHow
AdvToNeighbor	ADD, DELete, SHow
AllEndNodesTR	SETDefault, SHow
AllRoutersTR	SETDefault, SHow
AllRoutes	SHow
CONFiguration	SHow
CONTrol	SETDefault, SHow
COST	SETDefault, SHow
GatewayControl	SETDefault, SHow
HelloTime	SETDefault, SHow
InterNetRoute	SETDefault, SHow
IVPrefix	SETDefault, SHow
MaxAReaCost	SETDefault, SHow
MaxAReaHops	SETDefault, SHow
MaxAReaNumber	SETDefault, SHow
MaxCost	SETDefault, SHow
MaxHops	SETDefault, SHow
MaxNodeNumber	SETDefault, SHow
MaxPseudoAreas	SETDefault, SHow
MaxVisits	SETDefault, SHow
Neighbor	ADD, DELete, SHow
NETwork	SETDefault, SHow
NodeType	SETDefault, SHow
PolicyControl	SETDefault, SHow
PRIOrity	SETDefault, SHow
PseudoAreaPrefix	SETDefault, SHow
RcvFromNeighbor	ADD, DELete, SHow
ReceivePolicy	ADD, DELete, SHow
RoutingTime	SETDefault, SHow
SMDSGroupAddr	SETDefault, SHow
STATUS	SHow

(continued)

Table 17-1 DECnet Service Parameters and Commands (continued)

Parameters	Commands
VAdvertisePolicy	ADD, DELete, SHow
X25PROFileid	SETDefault, SHow
X25ProtID	SETDefault, SHow

ADDRess

Syntax

```
SETDefault -DECnet ADDRess = None |
  <area number>.<node number>(1–63).(1–1023) [<network>(0–15)]
SHow -DECnet ADDRess [<network>(0–15)]
```

Default Network 0

Description The ADDRess parameter specifies the DECnet address to be used by the router on the attached DECnet Phase IV network. When you assign an address to a router, the area number cannot exceed the value configured for the MaxAReaNumber parameter, and the node number cannot exceed the value configured for the MaxNodeNumber parameter. For more information refer to “MaxAReaNumber” on page 17-12 and “MaxNodeNumber” on page 17-13.

There is no default value for the ADDRess parameter. A DECnet address must be specified.

DECnet routing must be configured before the OSI protocol or APPN. Configuring DECnet routing changes the MAC address of the associated interfaces. If OSI or APPN routing is configured before DECnet routing is enabled, the OSI Protocol will not recognize the new MAC address.This restriction applies to the entire bridge/router, not just individual ports.

Values

None	Removes the DECnet address assigned to the specified network. All interfaces associated with the network will reset the network address back to the original MAC address.
<area number>	Specifies the area number to which the router belongs. Enter an area number between 1 and 63. It must not exceed the value specified for the MaxAReaNumber parameter.
<node number>	Specifies the node number assigned to the router. Each router must have a node number that is unique within the area. Enter a node number between 1 and 1023. It must not exceed the value specified for the MaxNodeNumber parameter.
<network >	Specifies the network number of the attached DECnet Phase IV network. Enter a network number between 0 and 15. The default value is 0. The specified DECnet address is assigned to all router interfaces associated with the network. When specifying the DECnet address, separate the area number from the node number with a period (.).

To display the current address configured for a DECnet network enter the SHow command.

AddressMap

Syntax

```
ADD -DECnet AddressMap <virtual DECnet address>@<network>
  <real DECnet address>@<network>
DELete -DECnet AddressMap All | [<virtual
DECnet address>]@<network>
SHow -DECnet AddressMap [@<network>]
```

The user-defined virtual DECnet address must not already exist in the associated network.

Default No default (no entries configured)

Description The AddressMap parameter defines an address translation entry that maps the real address on one DECnet network to a virtual address on another DECnet network.

Values

<virtual DECnet address> Specifies a virtual DECnet address, containing an area number with a range of 1–63 and a node number with a range of 0–1,023. A node number of 0 indicates a virtual area and is applicable only if the router is a level 2 area router on the associated network. A node number of asterisk (*) specifies that all virtual addresses within the specified area have a matching node number as the active real addresses on the associated network. A virtual address must be unique and may not be a duplicate of any existing real DECnet address on the associated network.

<real DECnet address> Specifies a real DECnet address, containing an area number with a range of 1–63 and a node number with a range of 0–1,023. A node number of 0 indicates a real area and is applicable only if the router is a level 2 router on the associated network. A node number of asterisk (*) specifies all active real addresses are mapped into a virtual address with a matching node number.

<network > Specifies the network number of the DECnet Phase IV network associated with the specified virtual/real address. The network associated with the specified virtual address and its corresponding real address must be distinct and within the range of 0–7.

All Indicates all translation entries.

Addresses with an area number that exceeds the value of the MaxAreaNumber parameter for the associated network or with a node number that exceeds the value of the MaxNodeNumber parameter for the associated network are allowed and saved in the configuration file, but the address translation entry is not added to the active list.

Example 1 To map the virtual address 1.7 on network 0 to the real address 1.207 on network 2, enter:

```
ADD -DECnet AddressMap 1.7@0 1.207@2.
```

Example 2 To delete the specific address translation entry for the virtual address 1.7 on network 0, enter:

```
DELete -DECnet AddressMap1.7@0
```

AdvertisePolicy

Syntax

```
ADD !<port> -DECnet AdvertisePolicy All |
  list of [~]<DECnet address>[–<DECnet address>]
DELete !<port> -DECnet AdvertisePolicy All |
  list of [~]<DECnet address>[–<DECnet address>]
SHow [!<port> | !*] -DECnet AdvertisePolicy
```

A route entry with an area number that is greater than the MaxAReaNumber and a node number that is greater than the MaxNodeNumber is allowed and saved on the configuration file, but it is not added to the active advertise list.

Default No default (no advertise policies defined)

Description The AdvertisePolicy parameter determines which routes are advertised to adjacent routers on the port specified. You can specify up to 32 route entries per port.

To include only specific routes in route advertisements, use the ADD command to add one or more DECnet addresses or ranges to the port's advertise list. To exclude specific routes in route advertisements, use the ADD command with the tilde (~) prefix added to the route entry to indicate an inverse route.

Normal routes and inverse routes are mutually exclusive and are not allowed to intermix in the AdvertisePolicy parameter or in the existing advertise list.

To remove a DECnet address or range from the route list, use the DELete command. Use the All value to indicate all specified routes.

The SHow command displays the list of route entries in the specified port's advertise list. If the optional port number is not specified, advertise lists are displayed for all ports with routing configured. Inverse routes are indicated by a tilde (~) prefix.

If the AdvertisePolicy parameter is enabled on a port with an empty advertise list, then routing updates are not sent.

Values

<DECnet address>	Specifies a DECnet address that is included or excluded in the AdvertisePolicy parameter. An excluded DECnet address is indicated by the tilde (~) prefix. A list of addresses, each separated by a comma, can be specified. The DECnet address and the DECnet address range can both be included in a route list. The DECnet address contains an area number with a range of 1–63 and a node number with a range of 0–1023. A node number of 0 indicates an area route. A DECnet address with a value of 0.0 specifies the route to the nearest level 2 router. To specify a range of DECnet addresses, type the lower DECnet address, a dash, and the higher address, using the following format: <area number.node number> - <area number.node number>
All	Indicates all routes.

If an address range is specified and the area numbers of the two addresses are not identical, it represents a range of areas and the two node number values are ignored.

Example 1 To advertise nodes 20.1, 20.4 and 20.10 through 20.50 on port 2, enter:

```
ADD !2 -DECnet AdvertisePolicy 20.1, 20.4, 20.10-20.50
```

Example 2 To not advertise reachability for nodes 2.2 through 2.100 and areas 5 and 6, enter:

```
ADD !2 -DECnet AdvertisePolicy ~2.2-2.100, ~5.0, ~6.0
```

Example 3 To advertise all nodes reachable on port 1, enter:

```
ADD !1 -DECnet AdvertisePolicy All
```

Example 4 To remove areas 6, 25 through 27 and nodes 22.1 through 22.100 from the advertise list for port 5, enter the following command. The reachability information for these nodes and areas will no longer be advertised on port 5.

```
DELete !5 -DECnet AdvertisePolicy 6.0, 22.1-22.100, 25.0-27.0
```

AdvToNeighbor

Syntax

```
ADD !<port> -DECnet AdvToNeighbor All |
 list of <DECnet address>[–<DECnet address>]
DELete !<port> -DECnet AdvToNeighbor All |
 list of <DECnet address>[–<DECnet address>]
SHow [!<port> | !*] -DECnet AdvToNeighbor
```

Default No default (no neighbors configured to advertise to)

Description The AdvToNeighbor parameter specifies a list of adjacent routers to which routing update messages are sent. You can specify up to 32 entries per port. Inverse entries, indicated by the tilde (~) prefix, are not permitted in the AdvToNeighbor parameter.

To add one or more DECnet addresses or ranges to the neighbor list, use the ADD command. If the neighbor list for a port exists, routing updates sent on the port are sent to the specific set of routers on the list.

Routing updates are not sent if the AdvToNeighbor parameter is enabled on a port with an empty neighbor list.

To remove one or more DECnet addresses or ranges from a port’s neighbor list, use the DELete command. The All value indicates all adjacent routers and may be used to remove all entries in a neighbor list before new entries are added.

The SHow command displays the list of neighbors to which routing update messages are sent. If you do not specify a port, this information is displayed for all ports that have routing enabled.

Values

<DECnet address>	Specifies a DECnet address that is included or excluded in the AdvertisePolicy parameter. A list of addresses, each separated by a comma, can be specified. The DECnet address and the DECnet address range can both be included in a route list.

The DECnet address contains an area number with a range of 1–63 and a node number with a range of 0–1023. A node number of 0 indicates an area route. A DECnet address with a value of 0.0 specifies the route to the nearest level 2 router. An example of a DECnet address is:

```
<area number.node number>
```

To specify a range of DECnet addresses, type the lower DECnet address, a dash, and the higher address, using:

```
<area number.node number> - <area number.node number>
```

The area numbers of the two addresses must be identical.

All — Indicates all routes.

Example 1 To send routing updates to adjacent router 20.5 on port 1, enter:

```
ADD !1 -DECnet AdvToNeighbor 20.5
```

Example 2 To remove 22.1 from the neighbor list on port 5, enter the following command. Routing updates sent on port 5 will not be sent to adjacent router 22.1.

```
DELete !5 -DECnet AdvToNeighbor 22.1
```

AllEndNodesTR

Syntax

```
SETDefault !<port> -DECnet AllEndNodesTR = %<functional address>
  [Ncmac | Mac]
SHow [!<port> | !*] -DECnet AllEndNodesTR
```

Default %030010000000 (canonical)
%C00008000000 (noncanonical)

Description The AllEndNodesTR parameter specifies the multidestination functional address that is used by the designated router to transmit router hellos to all adjacent DECnet Phase IV end nodes on token ring LANs. This parameter is also used by the router to listen for end node hellos from adjacent Phase IV end nodes.

Values

%<functional address >	Indicates a 48-bit multidestination address. This address can consist of either a Ncmac or Mac address.
Ncmac	Indicates functional address specified in noncanonical format.
Mac	Indicates functional address specified in canonical format. This is the default.

Example To specify the multidestination functional address for port 2, enter:

```
SETDefault !2 -DECnet AllEndNodesTR = %C00040000000 n
```

AllRoutersTR

Syntax

```
SETDefault !<port> -DECnet AllRoutersTR = <functional address>
 [Ncmac | Mac]
SHow [!<port> | !*] -DECnet AllRoutersTR
```

Default 030008000000 (canonical)
C00010000000 (noncanonical)

Description The AllRoutersTR parameter specifies the multidestination functional address that must be used to reach all adjacent Phase IV router nodes on token ring LANs.

Values

<functional address> Indicates a 48-bit multidestination function address. This address can consist of either an Ncmac or Mac address.

Ncmac Indicates functional address specified in noncanonical format.

Mac Indicates functional address specified in canonical format. This is the default.

AllRoutes

Syntax

```
SHow -DECnet AllRoutes [L1 | L2] [<network>(0–7)]
```

Default All Level 1 and Level 2 routes for network 0

Description The AllRoutes parameter displays the current DECnet Routing Table for the specified network.

Values

L1 Displays only Level 1 intra-area routes.

L2 Displays only Level 2 inter-area routes.

<network > Specifies a network number to select a specific network. Enter a network number between 0 and 7. The default is 0.

For Level 1(RoutingIV) routers, only the DECnet Intra-Area Routing Table is displayed. For Level 2 (Area) routers, both the DECnet Routing Table and the DECnet Inter-Area Routing Table are displayed.

CONFiguration

Syntax

```
SHow [!<port> | !*] -DECnet CONFiguration [<network>(0–7)]
```

Default Network 0

Description The CONFiguration parameter displays the current DECnet routing configuration for a specified network.

Values

<network > Specifies a network number to select a specific network. Enter a network number between 0 and 7. The default is 0.

CONTrol

Syntax

```
SETDefault !<port> -DECnet CONTrol = ([ROute | NoROute], [Trigger |
  NoTrigger])
SHow [!<port> | !*] -DECnet CONTrol
```

Default NoROute, Trigger

Description The CONTrol parameter enables or disables DECnet routing on a specified port.

DECnet routing cannot be enabled if the OSI Protocol or APPN already is enabled for routing. You must first disable the OSI Protocol or APPN, then enable DECnet routing. After you enable DECnet routing, you can re-enable the OSI routing protocols or APPN. This restriction applies to the entire bridge/router, not just individual ports.

To display the current value of the CONTrol parameter for a specified port, enter:

```
SHow -DECnet CONTrol
```

If you do not specify a port, this information is displayed for all ports that have routing enabled.

Values

ROute — Enables DECnet routing on the specified port. All ports with DECnet routing enabled can send and receive routing updates and Hello messages.

NoROute — Disables DECnet routing on the specified port. Routing messages and Hello messages are not sent or received on the port.

Trigger — Causes DECnet to send trigger update packets. A trigger update is sent when the metric of one or more route has changed. Trigger updates allow the routing database to be more responsive to network configuration changes.

NoTrigger — Causes DECnet to send only complete update packets at the interval specified by the RoutingTime parameter.

COST

Syntax

```
SETDefault !<port> -DECnet COST = <number>(1–25)
SHow [!<port> | !*] -DECnet COST
```

Default 10

Description The COST parameter specifies the cost for a particular port. Specify a value between 1 and 25.

To display the cost for a particular port, use the SHow command. If you do not specify a port, this information is displayed for all ports that have routing enabled.

GatewayControl

Syntax

```
SETDefault -DECnet GatewayControl = ([GateWay | NoGateWay], [PseudoArea
  | NoPseudoArea], [VAdvertisePolicy | NoVAdvertisePolicy])
SHow -DECnet GatewayControl
```

Default NoGateWay, NoPseudoArea, NoVAdvertisePolicy

Description The GatewayControl parameter enables and disables the DECnet Phase IV to Phase V translation, the pseudo area mapping function, and filtering of Phase IV routes in Phase V link state advertisements (LSA). Pseudo area mapping functions can be activated only when the Phase IV to Phase V translation function is enabled through this parameter.

To display the current gateway control status, use the SHow command.

Values

GateWay	Enables the DECnet Phase IV to Phase V translation.
NoGateWay	Disables the DECnet Phase IV to Phase V translation.
PseudoArea	Enables the pseudo area mapping function.
NoPseudoArea	Disables the pseudo area mapping function.
VAdvertisePolicy	Enables filtering of Phase IV routes that are advertised in Phase V Link State Packets.
NoVAdvertisePolicy	Disables filtering of Phase IV routes that are advertised in Phase V Link State Packets

HelloTime

Syntax

```
SETDefault [!<port>] -DECnet HelloTime = <seconds>(5–8191)
SHow [!<port> | !*] -DECnet HelloTime
```

Default 15

Description The HelloTime parameter specifies the time interval in seconds at which the router sends hello messages to adjacent nodes.

To display the current value for the HelloTime parameter, enter the following command on the port specified:

```
SHow -DECnet HelloTime
```

InterNetRoute

Syntax

```
SETDefault -DECnet InterNetRoute = Disable | AddressMap |
 <list of networks>
SHow -DECnet InterNetRoute
```

Default Disable

Description The InterNetRoute parameter enables and disables internetwork routing between the specified networks.

Address translation is disabled if you enable internetwork routing when the list of networks value is specified.

To display the current value for the InterNetRoute parameter, use the SHow command.

Values

Disable	Disables internetwork routing.
AddressMap	Enables user-defined address translation to allow internetwork routing between selected nodes on different networks.
<list of networks>	Enables internetwork routing between specified networks. Nodes on one network may communicate with all nodes on the other specified networks. Each of the specified networks must reside in a different DECnet area.

IVPrefix

Syntax

```
SETDefault -DECnet IVPrefix = <NSAP prefix>
SHow -DECnet IVPrefix
```

Default No default (no prefixes configured)

Description The IVPrefix parameter specifies the common Phase IV Network Service Access Point (NSAP) Prefix that is used across a DECnet routing domain for DECnet Phase IV to Phase V transition support. Connectivity between Phase IV and Phase V systems in the routing domain is possible only when the Phase V system is configured with a matching NSAP Prefix.

When you enable the DECnet gateway function, the OSI area address of the gateway must match one of the area addresses configured for the OSI router. The OSI area address of the gateway is formed by appending the local Phase IV area number to the area prefix configured with the IVPrefix parameter.

Values <NSAP prefix> Specifies the NSAP address, which consists of the following:

Authority format identifier (AFI). This part identifies the authority responsible for allocating IDI field values, format, and whether domain specific part (DSP) syntax is specified with binary or decimal digits.This identifier is always preceded with a slash in 3Com syntax.

Initial domain identifier (IDI). This part identifies the network addressing authority responsible for determining the format of the DSP field. It contains up to 15 decimal digits depending on the format established in AFI.

If you are specifying an initial domain identifier less than 12 digits long, you must use a slash (/) after the identifier. The final slash informs the system that a full IDI has been specified. Otherwise, the system will pad the number with leading zeros to use all 12 digits.

Domain specific part (DSP) prefix. This prefix consists of decimal or hexadecimal digits. If the DSP is in hexadecimal, it must contain an even number of digits. Only the upper portion of the domain specific part up to, but not including the area field, is specified.

If the DECnet gateway is enabled, the Phase IV NSAP prefix defined with the SETDefault command takes effect immediately. A change in the Phase IV prefix may result in newly reachable addresses or a previously reachable address becoming inaccessible. This situation is indicated by the DECnet and ISIS displays.

The SHow command displays the current value of the Phase IV NSAP prefix. The Phase IV DECnet address is in decimals, while the OSI area address is in hexadecimals.

MaxAReaCost

Syntax

```
SETDefault -DECnet MaxAReaCost = <number>(1–1022) [<network>(0–7]
SHow -DECnet MaxAReaCost [<network>(0–7)]
```

Default 1022

Description The MaxAReaCost parameter specifies the maximum cost possible in a path to a reachable area. If the path cost to a destination area is determined to be higher than this value, the destination area is considered unreachable.

The MaxAReaCost parameter applies only to a Level 2 router, which can route packets within its area, as well as to other areas.

3Com recommends using the following formula to determine a value for the MaxAReaCost Parameter: MaxAReaCost = MaxAReaHops * 25. For information on assigning a value for the MaxAReaHops parameter, refer to "MaxAReaHops" on page 17-11.

To display the current value for the MaxAReaCost parameter, use the SHow command.

Values <network> Specifies the number of the network to which this MaxAreaCost value is assigned. Enter a network number between 0 and 7. The network number is required only if multiple independent networks are configured. Default is 0.

MaxAReaHops

Syntax

```
SETDefault -DECnet MaxAReaHops = <number>(1–30) [<network>(0–7)]
SHow -DECnet MaxAReaHops [<network>(0–7)]
```

Default 30

Description The MaxAReaHops parameter specifies the maximum number of hops possible in a path to a reachable area in the network. If the number of hops in the path to another area exceeds the value of this parameter, that area is considered to be unreachable.

The suggested value for the MaxAReaHops parameter is twice the distance (in hops) of the worst-case longest path.

The MaxAReaHops parameter applies only to a Level 2 router, which can route packets within its area, as well as to other areas.

To display the current value for the MaxAReaHops parameter, use the SHow command.

Values <network> Specifies the number of the network to which this MaxAreaHops value is assigned. Enter a network number between 0 and 7. The network number is required only if multiple independent networks are configured. Default is 0.

MaxAReaNumber

Syntax

```
SETDefault -DECnet MaxAReaNumber = <number>(1–63) [<network>(0–7)]
SHow -DECnet MaxAReaNumber [<network>(0–7)]
```

Default 63

Description The MaxAReaNumber parameter specifies the maximum number of areas allowed on the network. Packets received from or forwarded to an area with a number higher than the value specified for MaxAReaNumber are discarded.

To display the current and default values for the MaxAReaNumber parameter, use the SHow command.

Values

<network>	Specifies the number of the network to which this MaxAreaNumber value is assigned. Enter a network number between 0 and 7. The network number is required only if multiple independent networks are configured. Default is 0.

MaxCost

Syntax

```
SETDefault -DECnet MaxCost = <number>(1–1022) [<network>(0–7)]
SHow -DECnet MaxCost [<network>(0–7)]
```

Default 1022

Description The MaxCost parameter specifies the maximum cost possible for a path to a reachable node within the area. If the cost to a destination node exceeds this value, the destination is considered unreachable.

3Com recommends using the following formula to determine a value for the MaxCost parameter: MaxCost = MaxHops * 25. For information on assigning a value for the MaxHops parameter, refer to “MaxHops. “

To display the current value for the MaxCost parameter, use the SHow command.

Values

<network>	Specifies the number of the network to which this MaxCost value is assigned. Enter a network number between 0 and 7. The network number is required only if multiple independent networks are configured. Default is 0.

MaxHops

Syntax

```
SETDefault -DECnet MaxHops = <number>(1–30) [<network>(0–7)]
SHow -DECnet MaxHops [<network>(0–7)]
```

Default 30

Description The MaxHops parameter specifies the maximum number of hops allowed in a path to a reachable node within the area. If the cost to a destination node exceeds this value, the destination is considered unreachable.

To display the current value for the MaxHops parameter, use the SHow command.

The suggested value for MaxHops is twice the worst-case longest path in hops.

Values <network> Specifies a network number to select a specific network. Enter a network number between 0 and 7. Default is 0.

MaxNodeNumber

Syntax

```
SETDefault -DECnet MaxNodeNumber = <number>(1–1023)
<network>(0–7)]
SHow -DECnet MaxNodeNumber [<network>(0–7)]
```

Default 255

Description The MaxNodeNumber parameter specifies the maximum number of nodes allowed within an area. Packets received from or forwarded to a node with a node number higher than the MaxNodeNumber parameter value are discarded.

To display the current value for the MaxNodeNumber parameter, use the SHow command.

Values <network> Specifies a network number to select a specific network. Enter a network number between 0 and 7. The default is 0.

MaxPseudoAreas

Syntax

```
SETDefault -DECnet MaxPseudoAreas = <number>(2–8)
SHow -DECnet MaxPseudoAreas
```

Default 2

Description The MaxPseudoAreas parameter specifies the maximum number of pseudo areas that are allowed in a single DECnet area. The MaxPseudoAreas value and the local DECnet Phase IV address, (<area number.node number>), determine the local pseudo area ID. The pseudo area ID is appended to the area prefix configured with the PseudoAreaPrefix parameter to form the OSI area address for the local pseudo area.

The MaxPseudoAreas value must be a power of 2 to be compatible with the Phase IV address structure.

The MaxPseudoAreas value must be identical on the gateway router of all participating pseudo areas. In addition, all nodes in a pseudo area must be assigned a DECnet address that is within the range of addresses allotted for the pseudo area.

To display the current value of the MaxPseudoAreas, use the SHow command.

MaxVisits

Syntax

```
SETDefault -DECnet MaxVisits = <number>(1–63) [<network>(0–7)]
SHow -DECnet MaxVisits [<network>(0–7)]
```

Default 63

Description The MaxVisits parameter specifies the maximum number of hops that a packet can transverse before the packet is considered to be looping.

3Com recommends using the following formula to determine a value for the MaxVisits parameter: MaxVisits = MaxHops + K (where 1<K ≤ MaxHops). For information on assigning a value for the MaxHops parameter, refer to “MaxHops” on page 17-12.

To display the current value for the MaxVisits parameter, use the SHow command.

Values

<network >	Specifies a network number to select a specific network. Enter a network number between 0 and 7. The default is 0.

Neighbor

Syntax

```
ADD !<port> -DECnet Neighbor <DECnet address> <media address>
DELete !<port> -DECnet Neighbor <DECnet address>
SHow [!<port> | !*] -DECnet Neighbor
```

Default None (no neighbors configured)

Description The Neighbor parameter adds X.25 or Frame Relay neighbor addresses by mapping the media address to corresponding data terminal equipment (DTE) or data link connection identifier (DLCI) addresses.

To remove an entry from the DECnet Neighbor Table, use the DELete command.

To display DECnet neighbors on a particular port, use the SHow command.

Values

<DECnet address>	Specifies a DECnet address, such as 3.55. The area number has a range of 1–63 and the node number has a range of 0–1023.
<media address>	Specifies the media address. You can use one of the following media addresses: To add an X.25 neighbor, use an X.25 DTE address. The X.25 DTE address is prefixed by #. To add a Frame Relay neighbor, use a Frame Relay DLCI. The Frame Relay DLCI has an @ prefix.

NETwork

Syntax

```
SETDefault !<port> -DECnet NETwork = <network>(0–7)
SHow [!<port> | !*] -DECnet NETwork
```

Default 0

Description The NETwork parameter specifies the DECnet network number associated with the indicated port. Up to seven independent DECnet networks can be defined for the router.

To display the DECnet network for a particular port, use the SHow command.

NodeType

Syntax

```
SETDefault -DECnet NodeType = [Area | RoutingIV] [<network>(0–7)]
SHow -DECnet NodeType [<network>(0–7)]
```

Default RoutingIV

Description The NodeType parameter specifies the type of routing that you want the router to perform.

To display the current value for the NodeType parameter, use the SHow command.

Values

Area	Specifies a Level 2 router. A Level 2 router can route packets within its own area, as well as to other areas.
RoutingIV	Specifies a Level 1 router. A Level 1 router can route packets only within its own area.
<network >	Specifies a network number to select a specific network. Enter a network number between 0 and 7. The default is 0.

PolicyControl

Syntax

```
SETDefault !<port> -DECnet PolicyControl = ([AdvertisePolicy |
  NoAdvertisePolicy],[ReceivePolicy|NoReceivePolicy],[AdvToNeighbor
  | NoAdvToNeighbor], [RcvFromNeighbor | NoRcvFromNeighbor])
SHow [!<port> | !*] -DECnet PolicyControl
```

Default NoAdvertisePolicy, NoReceivePolicy, NoAdvToNeighbor, NoRcvFromNeighbor

Description The PolicyControl parameter enables and disables DECnet route filtering on a per-port basis.

Values

AdvertisePolicy	Enables the AdvertisePolicy filter.
NoAdvertisePolicy	Disables the AdvertisePolicy filter.
ReceivePolicy	Enables the ReceivePolicy filter.
NoReceivePolicy	Disables the ReceivePolicy filter.
AdvToNeighbor	Enables the AdvToNeighbor filter.
NoAdvToNeighbor	Disables the AdvToNeighbor filter.
RcvFromNeighbor	Enables the RcvFromNeighbor filter.
NoRcvFromNeighbor	Disables the RcvFromNeighbor filter.

PRIOrity

Syntax

```
SETDefault [!<port>] -DECnet PRIOrity = <number>(1–127)
SHow [!<port> | !*] -DECnet PRIOrity
```

Default 64

Description The PRIOrity parameter specifies the priority of the router on each port. The value of this parameter is used to determine the designated router on the LAN. The router with the highest priority is the designated router on the attached LAN. If two or more routers have the same priority assigned, the router with the highest node ID is chosen.

To display the current value for the PRIOrity parameter, use the SHow command.

PseudoAreaPrefix

Syntax

```
SETDefault -DECnet PseudoAreaPrefix = <area prefix>
SHow -DECnet PseudoAreaPrefix
```

Default A default area prefix does not exist.

Description The PseudoAreaPrefix parameter specifies the common GOSIP-compliant area prefix that is used across a DECnet area for the pseudo area routing support. This value is attached as a prefix to a subarea’s pseudo area ID to form the pseudo area address for the subarea. The pseudo area enables intra-area traffic to be routed across a partitioned OSI area using the inter-domain routing mechanisms. When a packet destined for a pseudo area is received at a subarea’s gateway router, the pseudo area translation algorithm is invoked.

Coordinate the assignment of the PseudoAreaPrefix among the gateway routers of all the participating subareas so a common area prefix is used. In addition, the appropriate address prefix routes must be statically configured at both the gateway routers and the peer neighbor backbone routers to achieve connectivity among the subareas.

The PseudoAreaPrefix parameter is activated by the GatewayControl parameter.

To display the current value of the PseudoAreaPrefix, use the SHow command.

The SHow -DECnet CONFiguration command displays the OSI pseudo area address assumed by the local subarea. The local pseudo area ID is computed from the MaxPseudoAreas value and the local DECnet Phase IV address.

RcvFromNeighbor

Syntax

```
ADD !<port> -DECnet RcvFromNeighbor All | list of [~]<DECnet
  address>[–<DECnet address>]
DELete !<port> -DECnet RcvFromNeighbor All | list of <DECnet
  address>[–<DECnet address>]
SHow [!<port> | !*] -DECnet RcvFromNeighbor
```

Default No default (no routers configured from which to receive routing updates)

Description

The RcvFromNeighbor parameter specifies the list of adjacent routers from which to accept routing updates. This list is called the trusted neighbor list and it can be specified for each port. Routing information reported by the trusted neighbors is accepted. You can specify up to 32 entries per port.

If the RcvFromNeighbor parameter is enabled on a port with no configured RcvFromNeighbor values, then all routing updates received on the port are ignored.

To add a DECnet address or range to the port's trusted neighbor list, use the ADD command. To exclude routing updates from a specific set of adjacent routers, use the ADD command with the tilde (~) prefix to indicate an inverse entry. Routing updates received on the port are accepted except those that originate from the inverse trusted neighbors.

Trusted neighbors and inverse trusted neighbors are mutually exclusive and are not allowed to intermix in the RcvFromNeighbor parameter or in the existing trusted neighbor list.

To remove a DECnet address or range from a port's trusted neighbor list, use the DELete command. Use the All value to indicate all adjacent routers. The All value also may be used to remove all the entries in a trusted neighbor list before new entries are added.

The SHow command displays the list of entries in the trusted neighbor list. If the optional port number is not specified, trusted neighbor lists are displayed for all ports with routing configured. Inverse entries are indicated by the tilde (~) prefix.

Values

<DECnet address> Specifies the DECnet address that is included or excluded in the AdvertisePolicy parameter. An excluded DECnet address is indicated by the tilde (~) prefix. A list of addresses, each separated by a comma, can be specified. The DECnet address and the DECnet address range can both be included in a route list.

The DECnet address contains an area number with a range of 1–63 and a node number with a range of 0–1023. A node number of 0 indicates an area route. A DECnet address with a value of 0.0 specifies the route to the nearest level 2 router.

To specify a range of DECnet addresses, type the lower DECnet address, a dash, and the higher DECnet address, using:

```
<area number.node number> - <area number.node number>
```

When an address range is specified, the area numbers of the two addresses must be identical.

All Indicates all neighbors.

ReceivePolicy

Syntax

```
ADD !<port> -DECnet ReceivePolicy All |
  list of [~]<DECnet address>[–<DECnet address>]
DELete !<port> -DECnet ReceivePolicy All |
  list of <DECnet address>[–<DECnet address>]
SHow [!<port> | !*] -DECnet ReceivePolicy
```

Default No default (no receive policies configured)

Description The ReceivePolicy parameter specifies which routes, reported in the routing updates by adjacent routers, are accepted and cached in the local routing tables. The ReceivePolicy parameter is specified per port. You can specify up to 32 route entries per port.

If the ReceivePolicy parameter is enabled on a port with no configured ReceivePolicy values, then all routing updates received on the port are ignored.

To accept only specific routes reported in adjacent routers' routing updates, use the ADD command to add a DECnet address or range to the port's receive list. To exclude specific routes in adjacent routers' routing updates, use the ADD command with the tilde (~) prefix to indicate an inverse route.

A receive list contains either normal or inverse routes. If an inverse route exists in a receive list and you want to change the receive list to a normal route, you must first use the DELete command to remove all of the existing routes in that receive list. Then add normal routes to the receive list. Follow the same procedure to change a receive list to include only inverse routes.

To remove a DECnet address or range from the route list, use the DELete command. Use the All value to indicate all routes.

The SHow command displays the list of route entries in the specified receive list. If the optional port number is not specified, receive lists are displayed for all ports with routing configured. Inverse routes are indicated by a tilde (~) prefix.

A route entry with area number that is greater than the MaxAReaNumber and node number that is greater than the MaxNodeNumber is allowed and saved on the configuration file, but it is not added to the active advertise list.

Values

<DECnet address>	Specifies the DECnet address that is included or excluded in the AdvertisePolicy parameter. An excluded DECnet address is indicated by the tilde (~) prefix. A list of addresses, each separated by a comma, can be specified. The DECnet address and the DECnet address range can both be included in a route list. The DECnet address contains an area number with a range of 1–63 and a node number with a range of 0–1023. A node number of 0 indicates an area route. A DECnet address with a value of 0.0 specifies the route to the nearest level 2 router. To specify a range of DECnet addresses, type the lower DECnet address, a dash, and the higher DECnet address, using: `<area number.node number> - <area number.node number>`
~	When an address range is specified and the area numbers of the two addresses are not identical, it represents a range of areas and the two node number values are ignored.
All	Indicates all routes.

RoutingTime

Syntax

```
SETDefault [!<port>] -DECnet RoutingTime = <seconds>(5–65535)
SHow [!<port> | !*] -DECnet RoutingTime
```

Default 120

Description The RoutingTime parameter specifies the time interval (in seconds) at which the router will send routing updates to adjacent router nodes.

To display the current value for the RoutingTime parameter, use the SHow command.

SMDSGroupAddr

Syntax

```
SETDefault !<port> -DECnet SMDSGroupAddr = $<E0–E999999999999999> | None
SHow [!<port> | !*] -DECnet SMDSGroupAddr
```

Default None (no group address configured)

Description The SMDSGroupAddr parameter configures an SMDS group address that is used as the DECnet multicast address on the specified port. The port must be configured with the -PORT OWNer set to SMDS and the -DECnet SMDSGroupAddr configured with a valid group address for DECnet routing to occur over SMDS.

Values

<E0–E999999999999999>	Specifies the SMDS group, or multicast, address. The group address is used to multicast DECnet, hello, and routing messages to all routers configured with the same group address. The group address begins with the letter E and is followed by the 15 digits of the SMDS network number; if the number is less than 15 digits, it is padded on the right with Fs.
None	Removes a group address previously assigned to a port.

STATUS

Syntax

```
SHow -DECnet STATUS [<network>(0–7)] [All]
```

Default Network 0

Description The STATUS parameter displays the current state of DECnet routing on each port, plus the correct status of the Phase IV to Phase V gateway.

The DECnet routing status categories may include the following:

ROute	DECnet routing is enabled on the port.
NoROute	DECnet routing is not enabled on the port.
Running	DECnet routing is enabled and active on the port.
Down	The router has declared the port down.

Values

<network>	Specifies a network number to select a specific network. Enter a network number between 0 and 7. The default is 0.
All	Specifies the status of all ports be displayed. Default is to display all active ports on network 0 with DECnet routing enabled.

VAdvertisePolicy

Syntax

```
ADD -DECnet VAdvertisePolicy All | AllNeighbors | list of |
  [~]<DECnet address> [–<DECnet address>]
DELete -DECnet VAdvertisePolicy All | AllNeighbors | list of |
  <DECnet address> [–<DECnet address>]
SHow -DECnet VAdvertisePolicy
```

Default No default (no Phase IV to Phase V link state advertisements configured)

Description The VAdvertisePolicy parameter controls which Phase IV routes are announced in Phase V link state advertisements. This parameter is only activated when Phase IV to Phase V translation is operational.

To include only specific routes in route advertisements, use the ADD command to add one or more DECnet addresses or ranges to the port's advertise list. To exclude specific Phase IV routes in LSP advertisements, use the ADD command with the tilde (~) prefix added to the route entry to indicate an inverse route.

Normal routes and inverse routes are mutually exclusive and are not allowed to intermix in the AdvertisePolicy parameter or in the existing advertise list.

To remove a DECnet address or range from the route list, use the DELete command. Use the All value to indicate all specified routes.

To display the list of route entries in the router's list, use the SHow command. Inverse routes are indicated by a tilde (~) prefix.

A route entry with an area number that is greater than the MaxAReaNumber and a node number that is greater than the MaxNodeNumber is allowed and saved on the configuration file, but it is not added to the active advertise list.

Values

<DECnet address>	Specifies the DECnet address that is included or excluded in the AdvertisePolicy parameter. An excluded DECnet address is indicated by the tilde (~) prefix. A list of addresses, each separated by a comma, can be specified. The DECnet address and the DECnet address range can both be included in a route list. The DECnet address contains an area number with a range of 1–63 and a node number with a range of 0–1023. A node number of 0 indicates an area route. To specify a range of DECnet addresses, type the lower DECnet address, a dash, and the higher DECnet address, using: <area number.node number> - <area number.node number>
~	If an address range is specified and the area numbers of the two addresses are not identical, it represents a range of areas and the two node number values are ignored.
All	Indicates all routes.
AllNeighbors	Indicates all neighbors.

X25PROFileid

Syntax

```
SETDefault !<port> -DECnet X25PROFileid = <user profile
 id>(0–9999)
SHow [!<port> | !*] -DECnet X25PROFileid
```

Default 0

Description The X25PROFileid parameter defines an X.25 user profile that will be used when X.25 virtual circuits are set up to carry DECnet packets. A value of 0 indicates that no specific X.25 user profile is configured for DECnet packets.

X25ProtID

Syntax

```
SETDefault !<port> -DECnet X25ProtID = <protocol id>(1 octet)
SHow [!<port> | !*] -DECnet X25ProtID
```

Default OxDE

Description The X25ProtID parameter specifies a protocol identifier to be included in all outgoing X.25 call request packets to indicate that subsequent packets transmitted on the virtual circuit are DECnet packets. As a packet arrives at its destination, the destination router verifies this DECnet protocol identifier against its own DECnet protocol ID (PID). If they match, the incoming packet is accepted. If they do not match, the DECnet packet is discarded. The chosen value must not conflict with that used by other protocols.

The PIDs are entered in hexadecimal.

18 DIR SERVICE PARAMETERS

This chapter describes all the parameters in the DIR Service. The DIR Service displays names and determines the order in which the name resolvers are queried. The bridge/router uses these parameters when functioning as an X.25 connection service gateway for incoming automatic and extended connections.

Table 18-1 lists the DIR Service parameters and commands.

Table 18-1 DIR Service Parameters and Commands

Parameters	Commands
NAME	SHow
RESolutionOrder	SETDefault, SHow

NAME

Syntax

```
SHow -DIR NAME [<name>]
```

Default No default

Description The NAME parameter displays names in the IPName Service or the NAme parameter in the OSIAPPL Service. You do not need to know which name resolver is used for the name resolution. The order in which the gateway tries the IP and OSI name resolvers depends on the RESolutionOrder parameter. If the IP name resolver is used, the result of this command is the same as SHow -IPName NAME. If the OSI name resolver is used, the result is the same as SHow -OSIAPPL NAme.

RESolutionOrder

Syntax

```
SETDefault RESolutionOrder = <protocol> [<protocol> ...] (From
 IP, OSI)
SHow -DIR RESolutionOrder
```

Default IP, then OSI

Description The RESolutionOrder parameter defines the order of name resolvers to be used to resolve a name in an incoming connection request.

Specify both name resolvers for incoming connections made with the Connect command. The Connect command is not protocol-specific, and the name used with it can identify a Telnet host or a VTP host. You can set this parameter to IP when using the TELnet or RLOGin command. When using the VTp command set this parameter to OSI.

Example To set the resolution order to IP and then OSI, enter the following command:

```
SETDefault -DIR RESolutionOrder = IP OSI
```

After configuring the resolution order, you enter “Connect host1” on your X.25 PAD-attached terminal. The gateway queries the IP resolver first. If the IP resolver cannot resolve the name, the gateway queries the OSI resolver.

19 DLSw Service Parameters

This chapter describes all the parameters that are related to data link switching (DLSw) tunneling of Systems Network Architecture (SNA) and NetBIOS traffic over Transmission Control Protocol/Internet Protocol (TCP/IP). Table 19-1 lists the DLSw Service parameters and commands.

Table 19-1 DLSw Service Parameters and Commands

Parameters	Commands
AccessAct	SETDefault, SHow
BoundAccessNode	ADD, DELete, SHow
CircuitBal	SETDefault, SHow
CIRcuits	SHow
CONFiguration	SHow
CONNections	SHow
CONNectStats	SHow, Flush
CONTrol	SETDefault, SHow
Display	SHow
DlswLOG	SHow
FradMap	ADD, DELete, SHow
Interface	SETDefault, SHow
LimitDatagrams	SETDefault, SHow
LimitNBeXplorers	SETDefault, SHow
LimitSnaeXplorers	SETDefault, SHow
MacCache	FLush, SHow
MaxTRaceData	SETDefault, SHow
McastStats	SHow, Flush
McastTcpIdle	SETDefault, SHow
MOde	SETDefault, SHow
MulticastAddr	ADD, DELete, SHow
MulticastRetry	SETDefault, SHow
NameCache	FLush, SHow
NBBcastResend	SETDefault, SHow
NBBcastTimeout	SETDefault, SHow
NBLocalAccess	ADD, DELete, SHow
NBRemAccess	ADD, DELete, SHow
PEer	ADD, DELete, SETDefault, SHow
PeerMacAdd	ADD, DELete, SHow
PeerNBName	ADD, DELete, SHow
PortGroup	ADD, DELete, SHow

(continued)

Table 19-1 DLSw Service Parameters and Commands

Parameters	Commands
PRiorityCRiteria	ADD, DELete, SETDefault, SHow
PRioritySTATistics	SHow, FLush
SnaAlertsToTraps	SETDefault, SHow
SnaLocalAccess	ADD, DELete, SHow
SnaRemAccess	ADD, DELete, SHow
SnaTopoCollect	SETDefault
SnaTopoDisplay	SHow
TRaceData	FLush, SHow
TrapCONTrol	SETDefault, SHow

AccessAct

Syntax

```
SETDefault -DLSw AccessAct = ([LocalSnaForward |
   LocalSnaDiscard], [LocalNBForward | LocalNBDiscard],
   [RemoteSnaForward | RemoteSnaDiscard], [RemoteNBForward |
   RemoteNBDiscard])
SHow -DLSw AccessAct
```

Default LocalSnaDiscard, LocalNBDiscard, RemoteSnaDiscard, RemoteNBDiscard

Description The AccessAct parameter defines access filter actions for SNA frames and NetBIOS names. If the access filter matches, then the frames are either forwarded or discarded. The values for this parameter are dependent on the settings of the -DLSw NBLocalAccess, NBRemAccess, SnaLocalAccess and SnaRemAccess parameters described in this chapter.

Values

LocalSnaForward | LocalSnaDiscard	Discards or forwards to DLSw the list of MAC addresses specified by the SNALocalAccess parameter (see page 19-16).
LocalNBForward | LocalNBDiscard	Forwards to DLSw or discards only the list of names specified by the NBLocalAccess parameter (see page 19-11).
RemoteSnaForward | RemoteSnaDiscard	Discards or forwards to DLSw only the list of MAC addresses specified in the SnaRemAccess parameter (see page 19-17).
RemoteNBForward | RemoteNBDiscard	Discards or forwards to DLSw only the list of names specified in the NBRemAccess parameter (see page 19-12).

BoundAccessNode

Syntax

```
ADD !<Vport> -DLSw BoundAccessNode <ban dlci mac addr>
   [<bni mac addr>]
DELete !<Vport> -DLSw BoundAccessNode <bni dlci mac addr> | ALL
SHow -DLSw BoundAccessNode
```

Default No default

Description The BoundAccessNode parameter displays, activates, or deactivates the boundary access node (BAN) configuration on a virtual port. You must specify the BAN DLCI media access control (MAC) address. You can also specify the boundary node indicator (BNI) MAC address, overriding the default, which is 0x4FFF00000000 in noncanonical format.

Values

<ban dlci mac addr>	Provides an address that stations on the LAN use to connect to the host.
<bni mac addr>	Provides the FEP MAC address used between the router and the FEP.

CircuitBal

Syntax

```
SETDefault -DLSw CircuitBal = <Enable | Disable> [<cache refresh
   timeout> (0-240 minutes)]
SHow -DLSw CircuitBal
```

Defaults Disable

Description The CircuitBal parameter controls whether the NETBuilder II bridge/router supports circuit balancing, a feature that enables the bridge/router to distribute circuits evenly across available routes. You can use the cache refresh timeout value to set the interval between each route discovery broadcast. If you set the cache refresh timeout value to zero, the cache refresh timer is disabled, and there is no route discovery broadcasting. This parameter also displays whether circuit balancing is enabled.

Values

Enable | Disable	Controls whether circuit balancing is enabled.
<cache refresh timeout>	Sets the interval in minutes between each route discovery broadcast. If circuit balancing is enabled, the default is 60 minutes.

CIRcuits

Syntax

```
SHow -DLSw CIRcuits
```

Default No default

Description The CIRcuits parameter displays the actual data link switching circuits. For each circuit, the local and remote MAC address and SAP are displayed. This parameter also displays the state of the circuit, the IP address, the data link correlators, and the port number used by the LLC2, BAN, SDLC, or FRAD link connection. A question mark in the port number display indicates an unknown port number.

The MAC addresses displayed using this parameter are in noncanonical format.

The CIRcuits states include:

DISC	No circuit or connection is established.
RESOLVE	The circuit is waiting for a name resolution or a test request on the LAN.
CONT_PEND	Waiting for contact confirmation.
CONN_PEND	Waiting for a response to a contact message.

CIRC_EST	The end-to-end circuit has been established. Logical link control (LLC) Type 1 services are available.*
CIRC_PEND	Waiting for an SSP REACH_ACK response to an ICANREACH message.
CONNECTD	The end-to-end circuit has been established and logical link control (LLC) Type 2 service is available.*
RES_PEND	Waiting for a DL HALTED to restart the line.
DIS_PEND	Waiting for a HALT_DL SSP message.

* Circuits are in these main states most of the time.

CONFiguration

Syntax
```
SHow -DLSw CONFiguration
```

Default No default

Description The CONFiguration parameter displays the current settings for all DLSw configuration parameters.

The MAC addresses displayed using this parameter are in noncanonical format.

CONNections

Syntax
```
SHow -DLSw CONNections
```

Default No default

Description The CONNections parameter displays the current status of configured connections as well as any nonconfigured connections (nonsecured mode). The number of circuits in each active IP connection are also displayed. The states are as follows:

ACTIVATING	Trying to connect to a peer data link switch router.
CAPEX	Practitioner capability exchange flows.
ACTIVE	Connected to a data link switch and ready to pass data.
DEACTIVATING	In process of disconnecting.
INACTIVE	Not trying to connect. Waiting for a time-out.

CONNectStats

Syntax
```
FLush -DLSw CONNectStats
SHow -DLSw CONNectStats [peer address]
```

Default No default

Description The CONNectStats parameter displays the peer connection and circuit statistics for all DLSw connections. Optionally, you can display the connection statistics for a specific peer address only.

CONTrol

Syntax
```
SETDefault -DLSw CONTrol = ([EnableSNA | DisableSNA],
   [EnableNetBios | DisableNetBios])
SHow -DLSw CONTrol
```

Default EnableSNA, DisableNetBios

Description The CONTrol parameter defines the type of frame to be tunneled by data link switching.

Values

EnableSNA | DisableSNA	EnableSNA enables link switching of SNA traffic to all data link switches. DisableSNA disables SNA traffic data link switching to all data link switches.
EnableNetBios | DisableNetBios	EnableNetBios enables data link switching of NetBIOS traffic to all data link switches. DisableNetBios disables data link switching of NetBIOS traffic to all data link switches.

Setting the IP address to 0.0.0.0 disables all tunneling.

Display

Syntax `SHow -DLSw Display`

Default No default

Description The Display parameter combines the output of the CONNections, CIRcuits, MacCache, and NameCache parameters.

The MAC addresses displayed using this parameter are in noncanonical format.

DlswLOG

Syntax `SHow -DLSw DlswLOG`

Default No default

Description The DlswLOG parameter displays a log of DLSw activity messages captured on the bridge/router and stored in a buffer. The display shows the most recent activity message. Table 19-2 lists the event types captured in the log, and the corresponding messages displayed. In each message, *hhhhhhhhhhhh* represents either the local MAC address (LMAC) or remote MAC address (RMAC) while “xx” represents a hex value for either the local SAP (LSAP) or remote SAP (RSAP). The *nnn.nnn.nnn.nnn* variable represents an IP address.

Table 19-2 DLSw Log Event Types and Messages

Event Type	Message
Circuit activated	Circuit Up LMAC *hhhhhhhhhhhh* LSAP *xx* RMAC *hhhhhhhhhhhh* RSAP *xx* IP *nnn.nnn.nnn.nnn*
Circuit deactivated	Circuit Down LMAC *hhhhhhhhhhhh* LSAP *xx* RMAC *hhhhhhhhhhhh* RSAP *xx* IP *nnn.nnn.nnn.nnn*
(continued)	
Circuit failed	Circuit Failed LMAC *hhhhhhhhhhhh* LSAP *xx* RMAC *hhhhhhhhhhhh* RSAP *xx* IP *nnn.nnn.nnn.nnn*
Circuit could not get buffers	Circuit No Buffers LMAC *hhhhhhhhhhhh* LSAP *xx* RMAC *hhhhhhhhhhhh* RSAP *xx* IP *nnn.nnn.nnn.nnn*
Tunnel activated	Tunnel Up IP *nnn.nnn.nnn.nnn*
Tunnel deactivated	Tunnel Down IP *nnn.nnn.nnn.nnn*
Tunnel failed	Tunnel Failed IP *nnn.nnn.nnn.nnn*

Table 19-2 DLSw Log Event Types and Messages (continued)

Event Type	Message
Capabilities exchange accepted	CapEx Ack IP *nnn.nnn.nnn.nnn* Vectors: *xx xx* ...
Capabilities exchange rejected	CapEx Nack IP *nnn.nnn.nnn.nnn* Vectors: *xx xx* ...

FradMap

Syntax

```
ADD !<port> -DLSw FradMap <src mac> <src sap> <fep mac> <fep sap>
   <DLCI> <code point>
DELete !<port> -DLSw FradMap <src mac> <src sap> <fep mac>
SHow [!<port> | !*] -DLSw FradMap
```

Default No default (no addresses in the FradMap Table)

Description The FradMap parameter defines the address mapping for Frame Relay access to a front-end processor using the BNI frame format (the other format is BAN). The FradMap Table is searched when a frame is being switched out through a Frame Relay port.

Values

<src mac>	Specifies the address of the device attempting a connection with the front end processor. This address must be entered in noncanonical format.
<src sap>	Specifies the service access point number used by the device to establish connection. This hex number should be in the range of 4-EC and divisible by 4.
<fep mac>	Specifies the user-assigned address used by the bridge/router to represent the front-end processor (FEP). This address must be entered in noncanonical format.
<fep sap>	Specifies the service access point number used by the front-end-processor to represent the device.This hex number should be in the range of 4-FC and divisible by 4.
<DLCI>	Specifies the data link connection identifier, which is the value assigned by the Frame Relay service on the port to identify the virtual circuit.
<code point>	Specifies the hex value describing the traffic type of the Frame Relay session. Traffic types include 82 (FID2), 83 (APPN) and 84 (NetBIOS).

Interface

Syntax

```
SETDefault -DLSw Interface = <local DLSw IP address>
SHow -DLSw Interface
```

Default No default (no interface configured)

Description The Interface parameter selects a local port IP address to be used for data link switching communication. The address must be the same as one of the addresses defined using the SETDefault !<port> -IP NETaddr syntax. Only one local IP address can be defined. Make sure that the address is for a LAN port.

Values

<local DLSw IP address>	Specifies the local IP address to be used for DLSw communications.

Setting the IP address to 0.0.0.0 disables all tunneling.

LimitDataGrams

Syntax

```
SETDefault -DLSw LimitDataGrams = <# of datagrams sent/second>
   (0-500)
SHow -DLSw LimitDataGrams
```

Default 50

Description The LimitDataGrams parameter limits the number of NetBIOS explorer datagrams that DLSw on the local bridge/router responds to. When the bridge/router receives these NetBIOS explorer datagrams, it sends an SSP frame to a peer DLSw station. When an explorer datagram is received, SSP frame responses are sent to all DLSw peers. With large networks with many DLSw peers, these large SSP frame broadcasts can consume bridge/router buffers and memory. This parameter can limit the impact of large numbers of explorer datagrams. DLSw waits 15 seconds for a reply to an explorer frame.

When calculating the number of network messages generated, the number of datagrams you set using the parameter must be multiplied by the number of active peers, since the bridge/router sends a datagram to each peer.

LimitNBeXplorers

Syntax

```
SETDefault -DLSw LimitNBeXplorers = <# of unacknowledged netbios
   explorers>(0-500)
SHow -DLSw LimitNBeXplorers
```

Default 50

Description The LimitNBeXplorers parameter limits the number of NetBIOS NAME_QUERY explorer frames that DLSw on the local bridge/router responds to. When the bridge/router receives these name query frames, it sends an SSP frame to a peer DLSw station. If the peer address is unknown, SSP frame responses are sent to all DLSw peers. With large networks with many DLSw peers, these large SSP frame broadcasts can consume bridge/router buffers and memory. This parameter can limit the impact of large numbers of NetBIOS explorer frames. DLSw waits 15 seconds for a reply to an explorer frame.

When calculating the number of network messages generated, the number of SSP frames responses you set using the parameter must be multiplied by the number of active peers, since the bridge/router sends an SSP frame response to each peer.

LimitSnaeXplorers

Syntax

```
SETDefault -DLSw LimitSnaeXplorers = <# of unacknowledged
   explorers>(0-500)
SHow -DLSw LimitSnaeXplorers
```

Default 50

Description The LimitSnaeXplorers parameter limits the number of SNA test frames that DLSw on the local bridge/router responds to. When the bridge/router receives these SNA test frames, it sends an SSP frame to a peer DLSw station. If the peer address is unknown, SSP frame responses are sent to all DLSw peers. With large networks with many DLSw peers, these large SSP frame broadcasts can consume bridge/router buffers and memory. This parameter can limit the impact of large numbers of SNA test frames. DLSw waits 15 seconds for a reply to an explorer frame.

When calculating the number of network messages generated, the number of SSP frames responses you set using the parameter must be multiplied by the number of active peers, since the bridge/router sends an SSP frame response to each peer.

MacCache

Syntax

```
FLush -DLSw MacCache
SHow -DLSw MacCache
```

Default No default

Description The MacCache parameter displays the list of statically defined and dynamically learned MAC addresses and the peer IP address where these MAC addresses reside. The FLush -DLSw MacCache parameter deletes all the dynamically learned entries from its cache.

The MAC addresses displayed using this parameter are in noncanonical format.

MaxTRaceData

Syntax

```
SETDefault -DLSw MaxTRaceData = <max_bytes_traced> (0-76)
SHow -DLSw MaxTRaceData
```

Default 16

Description The MaxTRaceData parameter sets the maximum number of bytes of DLSw data captured using the Trace facility. The value sets the number of bytes captured over and above the DLSw message headers. The number of bytes of data captured affects the types of data captured; the higher the value entered, the more detailed trace data is captured. The number entered is rounded up to the nearest four. For example, if you enter the value as 29, the number is rounded up to 32.

McastStats

Syntax

```
SHow -DLSw McastStats
Flush -DLSw McastStats
```

Default No default

Description The McastStats parameter displays the frame count statistics for SSP traffic.

When viewing the display, if the multicast address is 224.0.10.1, the traffic is probably NetBIOS traffic because it is used to send and receive frames. If the address is 224.0.10.3, the traffic is probably used to send frames for SNA client-server traffic. If the address is 224.0.10.4, then the traffic is probably used to receive frames for SNA client-server traffic.

McastTcpIdle

Syntax

```
SETDefault -DLSw McastTcpIdle = <timer duration (1-255)>
SHow -DLSw McastTcpIdle
```

Default 3 minutes

Description The McastTcpIdle parameter specifies the amount of time (in minutes) that the TCP connection stays up without a circuit using it. This parameter applies only to the TCP connections with DLSw peers that have also implemented the multicast feature. This parameter takes effect immediately.

MOde

Syntax

```
SETDefault -DLSw MOde = ([Secure | NonSecure], [DefaultPRioritized |
   DefaultNoPRioritized], [Multicast | NoMulticast] )
SHow -DLSw MOde
```

Default NonSecure, DEFaultNoPRioritized, NoMulticast

Description The MOde parameter sets the mode of operation of the bridge/router.

Values

Secure | NonSecure	Controls whether the bridge/router is in Secure or NonSecure state. When the bridge/router is in Secure state, the tunnel client accepts only connection requests from configured DLSw tunnel peer routers (using the ADD -DLSw PEer command). When the bridge/router is in NonSecure state, the system accepts all DLSw tunnel connection requests received from any bridge/router.
DefaultPRioritized | DefaultNoPRioritized	Controls default prioritization for all tunnels by making all traffic either prioritized or not prioritized.
Multicast| NoMulticast	Controls whether DLSw multicast is supported. The default is NoMulticast.

NoPRioritized traffic can still be prioritized compared to other traffic types.

MulticastAddr

Syntax

```
ADD -DLSw MulticastAddr <IP multicast address | DEFault> <traffic
   type (SNA | NetBios | ALL)> [usage (Tx|Rx|TxRx)]
DELete -DLSw MulticastAddr <IP multicast address> | DEFault
SHow -DLSw MulticastAddr
```

Default The default address is 224.0.10.0.

Description The MulticastAddr parameter specifies the IP multicast addresses that the data link switch listens on, sends to, or both.

Values

<IP multicast address | DEFault>	Specifies the Class D multicast address. Enter the appropriate address, or enter DEFault to use the default multicast address, 224.0.10.0.
<traffic type>	Specifies the type of traffic that the multicast address applies to. Enter SNA if the specified IP multicast address applies to SNA traffic only. Enter NetBios if the specified IP multicast address applies to NetBIOS traffic only. Enter ALL if the specified IP multicast address applies to both SNA and NetBIOS traffic.
usage	Specifies whether the data link switch transmits or receives on the IP multicast address. Enter Tx if the data link switch transmits on the IP multicast address. Enter Rx if the data link switch receives on the IP multicast address. Enter TxRx if the data link switch transmits and receives on the IP multicast address.

MulticastRetry

Syntax

```
SETDefault -DLSw MulticastRetry = <SNA | NetBios> <retry interval
   (1-5)> <retry count (0-5)>
SHow -DLSw MulticastRetry
```

Default No default

Description The MulticastRetry parameter specifies the retry interval (in seconds) that the bridge/router waits before trying to resend SSP frames, and the number of times that the multicast is retried.

Values

SNA | NetBios	Specifies the traffic type for the retry interval. Enter SNA for SNA traffic or NetBios for NetBIOS traffic.
retry interval	Enters the retry interval in seconds. The valid range is from 1-5. The default is 3 seconds.
retry count	Enters the number of retries. The valid range is from 0 to 5. The default is 3.

NameCache

Syntax

```
FLush -DLSw NameCache
SHow -DLSw NameCache
```

Default No default

Description The NameCache parameter displays the list of statically defined and dynamically learned peer NetBIOS names and the peer IP address where each name resides. The FLush -DLSw NameCache parameter deletes dynamically learned names from its cache.

NBBcastResend

Syntax

```
SETDefault -DLSw NBBcastResend = <number> (0–30)
SHow -DLSw NBBcastResend
```

Default 3

Description The NBBcastResend parameter configures the number of times that NetBIOS name query frames are retransmitted out the LLC connection. The NBBcastResend parameter uses the NBBcastTimeout value to determine the time interval between each retry. When 0 is specified, the message is sent only once with no retries. Enter a number between 0 and 30. This parameter, in conjunction with the NBBcastTimeout parameter, determines how often DLSw sends a name query across a TCP tunnel.

NBBcastTimeout

Syntax

```
SETDefault -DLSw NBBcastTimeout = <seconds> (1–30)
SHow -DLSw NBBcastTimeout
```

Default 5

Description The NBBcastTimeout parameter configures the time-out between subsequent retries of the broadcast of NetBIOS name query frames used in conjunction with the NBBcastResend parameter. Enter a number between 1 and 30. This parameter, in conjunction with the NBBcastResend parameter, determines how often DLSw sends a name query across a TCP tunnel.

NBLocalAccess

Syntax

```
ADD !<filterid> -DLSw NBLocalAccess <src name> <dest name>
DELete !<filterid> -DLSw NBLocalAccess <src name>
SHow -DLSw NBLocalAccess
```

Default No default (no filters defined)

Description The NBLocalAccess parameter defines access filters for frames received from the local LAN. When DLSw receives a NetBIOS UI frame, it searches its tables for matching names. The action taken is determined by the value of the AccessAct parameter (see page 19-2) where RemoteNBDiscard indicates to discard the message and RemoteNBForward indicates to forward the frame to the local LAN.

The MAC addresses displayed using this parameter are in noncanonical format.

Values

<filterid> Specifies the ID for the filter being used in the command.

<src name> Specifies the Source NetBIOS name for the filtered source-destination pair.

<dest name> Specifies the Destination NetBIOS name for the filtered source-destination pair.

NBRemAccess

Syntax

```
ADD !<filterid> -DLSw NBRemAccess <src name> <dest name>
DELete !<filterid> -DLSw NBRemAccess <src name> <dest name>
SHow -DLSw NBRemAccess
```

Default No default (no filters defined)

Description The NBRemAccess parameter defines the access filters used for frames received from peer DLSw nodes. This table is searched for matching names when a NetBIOS NQ, DATAFRAME, or DGRMFRAME message is received from a peer. The action taken is determined by the value of the AccessAct parameter (see page 19-2) where RemoteNBDiscard indicates to discard the message and RemoteNBForward indicates to forward the frame to the local LAN.

Values

<filterid> Specifies the ID for the filter being used in the command.

<src name> Specifies the source NetBIOS name for the filtered source-destination pair.

<dest name> Specifies the destination NetBIOS name for the filtered source-destination pair.

PEer

Syntax

```
ADD !<tunnelid> -DLSw PEer <peer DLSw IP address> [PRIO | NoPRIO]
   [<init bw>] [Enable | Disable] [ NOrmal | QUiesce |
   NoBroadcast ] [“<peer name>”]
DELete !<tunnelid> -DLSw PEer <peer DLSw IP address>
SETDefault !<tunnelid> -DLSw PEer = <peer DLSw IP address> [PRIO
   | NoPRIO] [init bw] [Enable | Disable | OnDemand] [ NOrmal |
   QUiesce | NoBroadcast ] [“<peer name>”]
SHow -DLSw PEer
```

Default The default value for initial bandwidth is 8,000 bytes per second.

Description The PEer parameter enters the DLSw tunnel peer router’s IP address in the local bridge/router’s database. Select a tunnel ID to identify each peer. To add a new peer, use the ADD -DLSw PEer command. To modify the PRIO or NoPRIO and Enable or Disable status of an active peer use the SETDefault -DLSw PEer command When you set the Mode parameter to Secure, DLSw only establishes connections with routers defined as peers. NOrmal, Quiesce, or NoBroadcast values specify the operation mode of the tunnel.

Values

<tunnelid> Identifies the tunnel that connects to the peer DLSw at <peer IP address>.

<peer IP address> Identifies the address of the data link switch peer router.

PRIO | NoPRIO	Controls whether prioritization is enabled or disabled for individual tunnel links. The mode parameter determines the default.
inil bw	Sets the initial bandwidth in bytes per second for the tunnel. Do not set initial bandwidth higher than 8000.
Enable | Disable | OnDemand	Controls whether the connection is enabled or disabled. By default, the local data link switch enables the connection. When you specify Enable, the local data link switch automatically initiates a connection to the peer. When you specify Disable, the data link switch does not initiate the connection or accept an incoming connection from the peer. When you specify OnDemand, the data link switch does not initiate connection to the peer, but it does accept incoming connections from the peer. This option is used when DLSw is in Secure mode (for use with DLSw multicast). The default is Enable.
"<peer name>"	Identifies the name of the remote session partner. Use quotation marks (" ") to bracket the string. The string is limited to 16 characters.
NOrmal | Quiesce | NoBroadcast	Sets the mode of operation of the tunnel. NOrmal is the default. When you specify Quiesce, the tunnel does not explore for or accept new circuits (sessions between end-stations). When you specify NoBroadcast, the tunnel does not broadcast explorer packets but does accept and answer explorer packets from the remote station. The default is NOrmal.

When you set the Mode Parameter to Secure, DLSw only establishes connections with routers defined as peers.

PeerMacAdd

Syntax

```
ADD !<tunnelid> -DLSw PeerMacAdd <peer mac address>
DELete !<tunnelid> -DLSw PeerMacAdd <peer mac address>
SHow -DLSw PeerMacAdd
```

Default No default (no statically configured remote peer MAC addresses)

Description The PeerMacAdd parameter statically configures the MAC addresses of systems that are reachable through a DLSw tunnel peer router. Each MAC address is configured to map to the Internet address of the tunnel peer bridge/router.

The MAC addresses displayed using this parameter are in noncanonical format.

Values

<tunnelid>	Identifies the tunnel within the local bridge/router software that defines the peer data link switch IP address.
<peer mac address>	Specifies a hex number six bytes long.

PeerNBName

Syntax

```
ADD !<tunnelid> -DLSw PeerNBName <peer netbios name>
DELete !<tunnelid> -DLSw PeerNBName <peer netbios name>
```

```
SHow -DLSw PeerNBName
```

Default No default (no statically configured remote peer NetBIOS names)

Description The PeerNBName parameter statically defines NetBIOS names residing at specific peer IP locations. It also allows static assignment of names.

Values

<tunnelid>	Identifies a tunnel within the local bridge/router software that defines the peer data link switch IP address.
<peer netbios name>	Specifies a unique logical name from 1 to 15 characters long that identifies the NetBIOS peer.

PortGroup

Syntax

```
ADD !<port_group_id> -DLSw PortGroup <port> [,...] ["<string>"]
DELete !<port_group_id> -DLSw PortGroup [<port> [,...] | ALL]
SHow !<port_group_id> -DLSw PortGroup
```

Default No default

Description The PortGroup parameter defines a DLSw port group and adds ports to a port group. By configuring port groups, you can group many incoming ports from a remote site and funnel these ports to a single port grouping that you can send over a single data link switch to a central site. You can configure up to eight port groups on a single bridge/router. When the first port group is configured, DLSw local switching is enabled.

Values

<port>	Specifies a port number assigned to the port group. You can assign up to 16 ports to a port group.
"<string>"	Specifies an optional string that can be assigned to a port group. The string can be up to seven characters long.

PRiorityCRiteria

Syntax

```
ADD !<instanceid> -DLSw PRiorityCRiteria <tunnelid> <percentage>
   [High | Medium | Low] {<LocalMac> <LocalSap> <RemoteMac>
   <RemoteSap> [LocalLocAddr <LocAddr> | RemoteLocAddr
   <LocAddr>]}|UI
DELete !<instanceid> -DLSw PRiorityCRiteria <tunnelid>
SETDefault !<instanceid> -DLSw PRiorityCRiteria <tunnelid>
   <percentage> [High | Medium | Low] [LocalLocAddr <LocAddr> |
   RemoteLocAddr <LocAddr>]
SHow -DLSw PRiorityCRiteria <tunnelid>
```

Default Medium

Description The PRiorityCRiteria parameter defines a traffic type based on a MAC address, a SAP address, or a logical unit (LU). This parameter also controls priority assignments and bandwidth allocations, and displays them for each tunnel ID.

All MAC addresses, including addresses of Ethernet end-stations, must be entered in noncanonical format. If you define a priority criteria for all SNA traffic and other priority criteria for individual SNA devices by specifying their MAC addresses, the definitions for individual devices take precedence over the global definition.

Values

<instanceid> Specifies the priority criteria identifier that identifies the traffic type.

<tunnelid> Identifies the data link switch tunnel to which the priority criteria identifier applies.

<percentage> Specifies the percentage of bandwidth for the traffic type.

High | Medium | Low Sets the processing order of traffic types.

<LocalMac> Identifies the MAC address of the local workstation.

<LocalSap> Identifies, in hexadecimal, the SAP address of the local workstation. Can be set to SNA or NetBIOS to represent all SNA SAP or NetBIOS traffic, respectively. The SAP address must be a multiple of 4.

LocalLocAddr <LocAddr> | RemoteLocAddr <LocAddr> LocalLocAddr and RemoteLocAddr identify the local or remote LU. <LocAddr> identifies, in hexadecimal, the local LU address.

<RemoteMac> Identifies the MAC address of the remote workstation.

<RemoteSap> Identifies, in hexadecimal, the SAP address of the remote workstation. Can be set to SNA or NetBIOS to represent all SNA SAP or NetBIOS traffic, respectively. The SAP address must be a multiple of 4.

UI Specifies that all broadcasting frame types (TEST, NetBIOS name query/recognized, NetBIOS status, and UI datagrams) are included. If you enter a value for UI, do not enter values for <LocalMac>, <LocalSap>, <RemoteMac>, <RemoteSap>, <LocAddr>, LocalLocAddr, or RemoteLocAddr.

All values except <instanceid> and <percentage> can have a wildcard value of "*." When <tunnelid> is set to "*," the ADD command is applied to all DLSw tunnels that do not have any explicit priority criteria defined. This criteria is called global prioritization.

You can identify traffic from a specific downstream LU by specifying <LocAddr>, even if the LU is not local to your NETBuilder bridge/router. Be sure to specify the MAC address associated with the LU.

PRioSTATistics

Syntax

```
FLush -DLSw PRioSTATistics [<peer IP address>]
SHow -DLSw PRioSTATistics [<peer IP address>]
```

Default No default

Description The PRioSTATistics parameter displays or flushes DLSw prioritization statistics for each DLSW tunnel.

Values <peer IP address> Identifies the DLSW tunnel peer IP address. If you do not enter a value for this variable, statistics for all tunnels are displayed or flushed.

SnaAlertsToTraps

Syntax

```
SETDefault -DLSw SnaAlertsToTraps = [Send | SendAlert | Disabled]
SHow -DLSw SnaAlertsToTraps
```

Default Disabled

Description The SnaAlertsToTraps parameter enables or disables the conversion of SNA alerts to SNMP traps. This parameter also displays the current state of the alert conversion feature.

Values

Send Enables the conversion of SNA alerts to SNMP traps and sends the traps to the SNMP manager. When you enable SNA Traps, SNA alerts issued for all SNA LUs and PUs connected to each bridge/router port are converted to SNMP traps and sent to SNMP managers. The Send value only obtains a portion of the alert information. To obtain information for the entire alert, use the SendAlert value.

SendAlert Enables the conversion of SNA alerts to SNMP traps and sends the entire SNA alert information as the NetView host will see it.

Disabled Directs a bridge/router to ignore all SNA alerts.

SnaLocalAccess

Syntax

```
ADD !<filter id> -DLSw SnaLocalAccess <src addr> <src mask>
   <dest addr> <dest mask>
DELete !<filterid> -DLSw SnaLocalAccess <src addr>
SHow -DLSw SnaLocalAccess
```

Default No default (no filters defined)

Description The SnaLocalAccess parameter defines the access filters used for frames received from the local LAN segment of the network. When an LLC test frame is received from a local LAN segment, a search is performed and the frame is forwarded or discarded depending on the access action specified. Forward indicates forwarding test frames to a remote peer data link switch.

The MAC addresses displayed using this parameter are in noncanonical format.

Values

<filterid> Specifies the ID for the filter being used in the parameter.

<src addr> Specifies the Source MAC address for the filtered source-destination pair. This is the address of the originating LLC frame. This address is also the source address of the original (first) test frame.

<src mask> Specifies the bit mask to be applied to establish whether the source MAC address in the frame matches the source MAC address specified. When you set each bit in the bit mask to 1, all bits in the address must match. When you set each bit in the bit mask to 0, a match is not required. Each bit can be set separately. There are six bytes, and you are allowed to use all the bits.

<dest addr> Specifies the destination MAC address for the filtered source-destination pair. This is the destination address of the originating LLC frame.

<dest mask> Specifies the destination MAC address for the filtered source-destination pair. Setting each bit in the bit mask to 1 means that all bits in the address must match. When you set each bit in the bit mask to 0, a match is not required. Each bit can be set separately. There are six bytes, and you are allowed to use all the bits.

SnaRemAccess

Syntax

```
ADD !<filterid> -DLSw SnaRemAccess <src addr> <src mask> <dest
   addr> <dest mask>
DELete !<filterid> -DLSw SnaRemAccess <src addr>
SHow -DLSw SnaRemAccess
```

Default No default (no filters defined)

Description The SnaRemAccess parameter defines the access filters used for frames received from the data link switch. This address table is searched when a CANUREACH frame is received. A search is performed whether to forward or discard based on the access action that has been specified. Forward indicates forwarding to the local LAN segment.

The MAC addresses displayed using this parameter are in noncanonical format

Values

<filterid> Specifies the ID for the filter being used in the parameter.

<src addr> Specifies the source MAC address for the filtered source-destination pair. The source address is the address of the remote system’s MAC address. This is usually the source address of the original test frame.

<src mask> Specifies the bit mask used to establish whether the source MAC address in the frame matches the source MAC address specified. When you set each bit in the bit mask to 1, all bits in the address must match. When you set each bit in the bit mask to 0, a match is not required. Each bit can be set separately. There are six bytes, and you are allowed to use all the bits.

<dest addr> Specifies the destination MAC address for the filtered source-destination pair.

<dest mask> Specifies the destination bit mask for the filtered source-destination pair. Setting each bit in the bit mask to 1 means that all bits in the address must match. Setting each bit in the bit mask to 0 means that a match is not required. Each bit can be set separately. There are six bytes, and you are allowed to use all the bits.

SnaTopoCollect

Syntax

```
SETDefault -DLSw SnaTopoCollect = (EnablePu | EnablePuLu |
   Disable)
```

Default Disable

Description The SnaTopoCollect parameter enables and disables the collection of end-station topology information at the PU and LU level. To display the information collected, enter:

```
SHow -DLSw SnaTopoDisplay
```

Values

EnablePu Collects end-station information for physical units (PUs) only. When you display the topology collection results using the SnaTopoDisplay parameter, only PU information is shown.

EnablePuLu Collects end-station information for physical units (PUs) and logical units (LUs). When you display the topology collection results using the SnaTopoDisplay parameter, both PU and LU information is shown.

Disable Turns off the collection of end-station topology information. If you disable the collection function and then later display the topology information using the SnaTopoDisplay parameter, the display will not be current.

SnaTopoDisplay

Syntax

```
SHow -DLSw SnaTopoDisplay
```

Default No default

Description The SnaTopoDisplay parameter displays end-station topology information collected by DLSw. The display shows the end-station PU topology if you enabled PU collection with the SnaTopoCollect parameter, or end-station topology information for both PUs and LUs if you enabled LU collection with the same parameter.

When an SNMP Manager such as SunNet Manager or OpenView is used, more information about each end station is displayed than is available through the NETBuilder SnaTopoDisplay parameter display.

Table 19-3 lists the different headings and their meanings in the SNA topology display.

Table 19-3 SnaTopoCollect Display Meanings

Display Heading	Meaning
PU Name	The name of the end-station SNA physical unit (PU) as derived from the XID exchange, or as SET by an SNMP manager. The PU name may or may not be present.
Node ID	The Block Num/ID Num pair (as derived from the XID) that uniquely identifies an SNA node.
NodeType	The SNA PU type of the end station. NN indicates network node, EN indicates End Node, and 1, 2, 2.1 indicates the node is Type 1, Type 2.0, or Type 2.1, respectively. The designation 4/5 indicates the end station is a front-end processor or a host.
Dep. LU	Indicates whether the PU has dependent LUs. If the PU does not have any dependent LUs, the display for the PU will be shorter than PUs with dependent LUs. The topology collection facility does not collect information about independent LUs.
MAC Addr	The MAC or SAP address of the DLSw end station in noncanonical format.
Port Num	The port number of the NETBuilder that connects to the end station.
DLC Type	The data link control type of the connection. Valid entries are TOK (Token Ring), ETH (Ethernet), or SDLC.
Status	The status of the end station. The values can vary depending on the end station type. The valid states are: XID NEGOTIATION: This is the initial state of all SNA end stations during initialization. It indicates that an XID negotiation is in progress. ACTIVE/Wait ACTPU: Indicates that an end-station with dependent LUs has completed XID negotiation and is awaiting an ACTPU request from a host. ACTIVE: An end station with dependent LUs has received an ACTPU request and returned a positive response. If the end station has no dependent LUs (meaning one that doe not expect an ACTPU), this state indicates that XID negotiation has successfully completed. INACTIVE: An end station with dependent LUs has received an ACTPU request from the host. PEND ACTIVE: An end station with dependent LUs has received an ACTPU request but has not responded yet.
The following fields display only when an end station has dependent LUs associated with it:	
Active LU	The number of dependent LUs associated with the end station that have received ACTLU commands and have returned a positive response.
Bound LU	The number of dependent LUs that have received BIND requests and have returned a positive response.
LU Name	The name of the local LU. This name appears only if the LU was indicated in a BIND request received by the LU or if the LU was SET from an SNMP management station.
Add	The local address of the dependent LU on the end-station. This is a simple number identifying the LU and is not a physical address. The values range from 1 to 254.
T	Indicates the LU. The type appears only if the LU has received a BIND.
State	Indicates the current state of the LU. The valid states are: INACTIVE: LU was not activated (or was inactivated) by a host. PNDACT: Host has attempted to activate the LU (by sending an ACTLU command), and the LU has not yet returned a response. ACTIVE: The LU has received an ACTLU request and has returned a positive response. PNDINACT: Host is deactivating the LU (by sending a DACTLU request) and the response has not yet been returned by the LU. PNDBIND: LU has received a BIND request but has not yet responded. BOUND: LU has received a BIND request and has returned a positive response. PNDUNBND: LU has received an UNBIND request and has not yet responded.
Pri. LU	If the LU is bound, this field contains the name of the primary LU for the session.

TRaceData

Syntax

```
SHow -DLSw TRaceData
```

Default No default

Description The TRaceData parameter displays all DLSw entries in the trace buffer.

TrapCONTrol

Syntax

```
SETDefault -DLSw TrapCONTrol = ([TunnelUp | NoTunnelUp],
   [TunnelDown | NoTunnelDown], [CircuitUp | NoCircuitUp],
   [CircuitDown | NoCircuitDown]) | ALL | None
SHow -DLSw TrapCONTrol
```

Default NoTunnelUp, TunnelDown, NoCircuitUp, CircuitDown

Description The TrapCONTrol parameter defines control of the transmission of SNMP traps for the DLSw Service. If the control is enabled, the specific trap is sent to the SNMP Service for transmission; if the control is disabled, the trap is blocked from being sent to SNMP.

Whether the trap is sent or not is dependent on how the -SNMP COMmunity, -SNMP CONTrol, and -SNMP MANager parameters are configured. For more information about parameters in the SNMP Service, refer to Chapter 55.

Values

TunnelUp | NoTunnelUp	TunnelUp sends an SNMP trap to activate a tunnel. NoTunnelUp blocks an SNMP trap to activate a tunnel.
TunnelDown | NoTunnelDown	TunnelDown sends an SNMP trap to deactivate a tunnel. NoTunnelDown blocks an SNMP trap to deactivate a tunnel.
CircuitUp | NoCircuitUp	CircuitUp sends an SNMP trap to activate a circuit. NoCircuitUp blocks an SNMP to activate a circuit.
CircuitDown | NoCircuitDown	CircuitDown sends an SNMP trap to deactivate a circuit. NoCircuitDown blocks an SNMP trap to deactivate a circuit.
ALL	ALL is equivalent to entering TunnelUp, TunnelDown, CircuitUp and CircuitDown, enabling transmission of all DLSw SNMP traps.
None	None is equivalent to entering NoTunnelUp, NoTunnelDown, NoCircuitUp, NoCircuitDown, disabling transmission of all DLSw SNMP traps.

20 DVMRP SERVICE PARAMETERS

This chapter describes the Distance Vector Multicast Routing Protocol (DVMRP) Service parameters. The DVMRP Service is related to the Multicast Internet Protocol (MIP) and the Multicast Open Shortest Path First (MOSPF) Services. Table 20-1 lists the DVMRP Service parameters and commands.

Table 20-1 DVMRP Service Parameters and Commands

Parameters	Commands
AggregateExcept	ADD, DELete, SHow
AggregateRange	ADD, DELete, SHow
BoundaryAddr	ADD, DELete, SHow
CacheTime	SETDefault, SHow
CONFiguration	SHow, SHowDefault
CONTrol	SETDefault, SHow
DestGroup	ADD, DELete, SHow
ForwardTable	SHow
MEtric	SETDefault, SHow
MOspf	ADD, DELete, SHow
NEighbor	ADD, DELete, SHow, SHowDefault
NeighborRouter	SHow
PolicyControl	SETDefault, SHow
Prune	SETDefault, SHow
RateLimit	SETDefault, SHow, SHowDefault
RouteTable	FLush, SHow
TUnnel	SETDefault, SHow
UpdateTime	SETDefault, SHow

Some parameters in this service can be applied per port by using the !<port> syntax or per tunnel by using the !<tunnel ID> syntax. Valid port tunnel IDs are from 1 to 32 and must be preceded with an upper- or lowercase T.

AggregateExcept

Syntax

```
ADD -DVMRP AggregateExcept <subnet>/<mask>
DELete -DVMRP AggregateExcept {<subnet>/<mask> | ALL}
SHow -DVMRP AggregateExcept [<subnet>/<mask>]
```

Default No default exception route

Description The AggregateExcept parameter adds, deletes, and displays a list of constituent routes that DVMRP explicitly advertises even if it falls within the aggregate range.The route is specified by the subnet and mask. The -DVMRP CONTrol parameter must be set to Aggregate for this parameter to take effect.

To add a list of routes to be explicitly advertised, use the ADD command. To remove a single route or all routes, use the DELete command. To display the list of exception routes, use the SHow command.

Values

<subnet>/<mask> Specifies a range of addresses to add, delete, or display. The range of addresses are the constituent routes that DVRMP advertises.

Specify the subnet in dotted decimal notation. The subnet is the route that DVMRP advertises.

Specify the network mask to be applied to the network address. The mask is an integer between 0 and 32. It is a counter of the number of leading 1s in the subnet mask.

For example, if mask = 8, it represents the subnet mask 255.0.0.0 in decimal form. If mask = 10, it represents the subnet mask 255.192.0.0.

ALL Allows all aggregate exception routes to be deleted.

AggregateRange

Syntax

```
ADD -DVMRP AggregateRange <subnet>/<mask> [<metric>]
DELete -DVMRP AggregateRange {<subnet>/<mask> | ALL}
SHow -DVMRP AggregateRange [<subnet>/<mask>]
```

Default No default range; the default metric is 0

Description The AggregateRange parameter adds, deletes, and displays a list of supernets that DVMRP advertises to neighboring routers. All of the subnets within the specified supernet range are aggregated into the associated supernet, except for the subnets specified by the AggregateExcept parameter. The -DVMRP CONTrol parameter must be set to Aggregate for this parameter to take effect.

To add a list of supernets, use the ADD command. To delete supernet routes, use the DELete command. To display the list of supernets, use the SHow command.

Values

<subnet>/<mask> Specifies a range of addresses to add, delete, or display. The range of addresses are the supernets that DVMRP advertises.

Specify the subnet in dotted decimal notation. The subnet is the supernet that DVMRP advertises.

Specify the network mask to be applied to the network address. The mask is an integer between 0 and 32. It is a counter of the number of leading 1s in the subnet mask.

For example, if mask = 8, it represents the subnet mask 255.0.0.0 in decimal form. If mask = 10, it represents the subnet mask 255.192.0.0.

<metric>	The cost associated with the supernet to be advertised. If the metric is not specified or is set to 0, DVMRP picks the minimum cost among all the individual routes that fall within their associated supernet.
ALL	Allows all supernets to be deleted.

BoundaryAddr

Syntax

```
ADD {!<port> | !<tunnel ID>} -DVMRP BoundaryAddr <IP addr> [<subnet
  mask>]
DELete {!<port> | !<tunnel ID>} -DVMRP BoundaryAddr {<IP addr> | ALL}
SHow [!<port> | !<tunnel ID> | !*] -DVMRP BoundaryAddr [<IP addr>]
```

Default No default IP address.
255.255.255.255 is the default subnet mask.

Description The BoundaryAddr parameter adds, deletes, and displays a set of multicast destinations that are not reachable through this router port or tunnel. The packet is filtered when it is received from a port or tunnel and before it is transmitted to a port or tunnel.

A group of multicast addresses (239.xxx.xxx.xxx) has been set aside for use in private networks; these addresses are known as *scoped addresses*. Any traffic on a scoped address does not cross the boundary router. The NETBuilder software does not limit blocking to these scoped addresses; you can configure any set of multicast address to be blocked.

The DELete -DVMRP BoundaryAddr command deletes a single scoped address, a set of scoped addresses, or all the scoped addresses associated with the specified port.

The SHow -DVMRP BoundaryAddr command displays the boundary address for the specified port or all boundary addresses if no port number is specified.

Values

<IP addr>	The IP address to be scoped.
<subnet mask>	The subnet mask applied to the address. The default subnet mask is 255.255.255.255.

CacheTime

Syntax

```
SETDefault -DVMRP CacheTime = <seconds>(300–86400)
SHow -DVMRP CacheTime
```

Default 300 seconds

Description The CacheTime parameter specifies how long to keep a (source, group) pair in the forwarding table after the last packet has been received.

A router sends a Prune message to its parent router to detach itself from a delivery tree if and only if it has no members for that group on any directly connected subnets, and it has received Prune messages from each of its child interfaces for that group. When a Prune message is sent to the upstream router, the router holds the Prune message for the period specified by the smaller of the Prune Lifetime field and the value of the CacheTime parameter.

The range of this parameter is from 5 minutes (300 seconds) to 1 day (86,400 seconds).

CONFiguration

Syntax

```
SHow [!<port> | !<tunnel ID> | !*] -DVMRP CONFiguration
SHowDefault [!<port> | !<tunnel ID> | !*] -DVMRP CONFiguration
```

Default No default

Description The CONFiguration parameter displays the current settings of the parameters associated with the DVMRP Service.

CONTrol

Syntax

```
SETDefault {!<port> | !<tunnel ID>} -DVMRP CONTrol = ([Enable |
  Disable], [Aggregate | NoAggregate])
SHow [!<port> | !<tunnel ID> | !*] -DVMRP CONTrol
```

Default Disable, NoAggregate

Description The CONTrol parameter controls the overall behavior of DVMRP, including DVMRP route aggregation.

Values

Enable | Disable	Enables or disables the DVMRP Protocol.
Aggregate | NoAggregate	Enables or disables DVMRP route aggregation. The Aggregate value causes the router to aggregate the eligible subnets into the supernet based on the settings of the AggregateExcept and AggregateRange parameters. The NoAggregate value prevents the router from aggregating any routes.

DestGroup

Syntax

```
ADD -DVMRP DestGroup <subnet>/<mask> [Accept | Reject]
DELete -DVMRP DestGroup {<subnet>/<mask> | ALL}
SHow -DVMRP DestGroup [<subnet>/<mask>]
```

Default No default subnet or mask; Accept

Description The DestGroup parameter controls data packet forwarding between DVMRP and MOSPF domains. The -DVMRP PolicyControl parameter must be set to DestGroupfor this parameter to take effect. For more information, refer to “PolicyControl” on page 20-8.

Values

<subnet>/<mask>	Specifies the multicast IP network address in dotted decimal notation of the destination group whose data packets are accepted or rejected. The first byte of the subnet must be in the range of 224–239. The mask is applied to the network address and is an integer between 0 and 32. It is a counter of the number of leading 1s.

	For example, if mask = 8, it represents the subnet mask 255.0.0.0 in decimal form. If mask = 10, it represents the subnet mask 255.192.0.0.
Accept | Reject	Specifies whether data packets are accepted and forwarded, or rejected and dropped, between the two domains. If data packets do not fall within any specified subnet/mask address range, the data packets are accepted and forwarded. The Accept option causes the following actions by the multicast router: ▪ If the multicast router receives a packet from the MOSPF domain with a destination address that matches this destination group filter, then the multicast router accepts it and forwards it into the DVMRP domain. ▪ If the multicast router receives a packet from the DVMRP domain with a destination address that matches this destination group filter, then the multicast router accepts it and forwards it into the MOSPF domain. The Reject option causes the following actions by the multicast router: ▪ If the multicast router receives a packet from the MOSPF domain with a destination address that matches this destination group filter, then the multicast router rejects it and drops the packet and never forwards it into the DVMRP domain. ▪ If the multicast router receives a packet from the DVMRP domain with a destination address that matches this destination group filter, then the multicast router rejects it and drops the packet and never forwards it into the MOSPF domain.
ALL	Allows all destination groups to be deleted.

ForwardTable

Syntax

```
SHow -DVMRP ForwardTable [<subnet>[/<mask>]] [<group>]
```

Default No default

Description The ForwardTable parameter displays the current cache (forwarding) table for each (source, group) pair.

If you specify only <subnet>[/<mask>], which forms the subnet address range, then the display includes all the groups' entries associated with this subnet address range. If you specify only <group>, then the display includes all the subnets associated with this <group>. If you specify both <subnet> and <group>, then only the forwarding table entries for these subnet ranges are shown.

Values	<subnet>/<mask>	Specifies an address range to be displayed. <mask> is an integer between 0 and 32. It is the number of leading 1s in the subnet mask. If <mask> is not specified, the natural subnet mask is applied.
	<group>	The Class D multicast address of a group.

MEtric

Syntax

```
SETDefault {!<port> | !<tunnel ID>} -DVMRP MEtric = <value> (1–31)
SHow [!<port> | !<tunnel ID> | !*] -DVMRP MEtric
```

Default 1

Description The MEtric parameter specifies and displays the cost for the specified port. The metric is an administrative metric assigned to a subnet.

For multiple routes to the same source, the route with the lowest metric is selected. A route with a metric of 32 is considered unreachable (the value set for infinity is 32).

MOspf

Syntax

```
ADD -DVMRP MOspf <subnet>/<mask> [Aggregate | Individual | Reject]
  [<metric>]
DELete -DVMRP MOspf {<subnet>/<mask> | ALL}
SHow -DVMRP MOspf [<subnet>/<mask>]
```

Default

No default subnet or mask
Aggregate
Metric =1

Description The MOspf parameter allows routes learned from an MOSPF domain, except external routes, to be advertised into the DVMRP domain. If the routes are accepted, multicast packets from the MOSPF domain can be forwarded to the DVMRP domain if the -DVMRP PolicyControl parameter is set to Mospf. For more information, refer to “PolicyControl” on page 20-8.

Routes imported from an MOSPF domain have higher priority than those learned from the DVMRP Protocol; consequently, routes imported from MOSPF overwrite the existing DVMRP route regardless of the metric.

To define a policy for routes learned from an MOSPF domain to be advertised into the DVMRP domain as aggregated routes, individual routes, or to be rejected from the DVMRP domain, use the ADD command. When adding a policy, Aggregate and a metric of 1 are selected by default.

To remove a specific policy or all policies, use the DELete command.

To display all the policies or a single policy, use the SHow command.

Values

<subnet>/<mask>	Identifies an address range to which all MOSPF source networks are compared. If an MOSPF source network falls within the address range, the Aggregate, Individual, or Reject keywords determine the action. The mask is an integer between 0 and 32. It is a counter of the number of leading 1s in the subnet mask. For example, if mask = 8, it represents the subnet mask 255.0.0.0 in decimal form. If mask = 10, it represents the subnet mask 255.192.0.0.
Aggregate	All MOSPF source networks are aggregated by a single route subnet/mask, which summarizes multiple networks using supernetting. The aggregation occurs before the route is imported into the DVMRP domain.
Individual	Specifies that each MOSPF source network is advertised as learned into the DVMRP domain.
Reject	Specifies that the MOSPF source network is not advertised into the DVMRP domain.
<metric>	Indicates the administrative cost from 1 to 31 that is assigned to the subnet. A route with a metric of 32 is considered unreachable (the value set for infinity is 32). The default metric is 1.
ALL	Deletes all the configured policy's routes and then deletes all the routes learned from the MOSPF domain in the DVMRP Routing Table.

NEighbor

Syntax

```
ADD !<port> -DVMRP NEighbor {<FR_DLCI> | <X.25 DTE>}
DELete !<port> -DVMRP NEighbor {{<FR_DLCI> | <X.25 DTE>} | ALL}
SHow [!<port> | !*] -DVMRP NEighbor [<FR_DLCI> | <X.25 DTE>]
SHowDefault [!<port> | !*] -DVMRP NEighbor [<FR_DLCI> | <X.25 DTE>]
```

Default No default

Description The NEighbor parameter adds deletes, or displays neighbor addresses over an X.25 or Frame Relay network. By default, the router does not attempt to send route reports or to forward multicast packets over X.25 or Frame Relay networks unless you correctly configure this parameter. To establish the connection, you also need to configure the remote router.

Values

<FR_DLCI>	The data link connection identifier (DLCI) associated with the permanent virtual circuit. For example, @123.
<X.25 DTE>	The data terminal equipment (DTE) address associated with the remote router. For example, #31107645500.
ALL	Allows you to delete all the neighbors for the specified port.

NeighborRouter

Syntax

```
SHow [!<port> | !<tunnel ID> | !*] -DVMRP NeighborRouter [<IP addr>]
```

Default No default

Description The NeighborRouter parameter displays neighboring router information. If <IP addr> is specified, only neighboring router information with this IP address is displayed.

Elements in the display include the following items:

IP Address	Internet Protocol (IP) address of neighboring router.
GenerationID	Generation ID of neighboring router.
Version	Multicast router version of neighboring router.
TTL	Time-to-live (TTL) indicates how much time (in seconds) left before removing the neighboring router from table.
Status	If the neighboring router is running a UNIX routed version 3.5 or greater, Status indicates whether the neighboring router is a leaf node, and whether it supports prune, generation ID, and multicast trace route. The ~ before the status means the neighboring router does not support the specified item.

PolicyControl

Syntax

```
SETDefault -DVMRP PolicyControl = ([Mospf | NoMospf], [DestGroup |
  NoDestGroup])
SHow -DVMRP PolicyControl
```

Default NoMospf, NoDestGroup

Description The PolicyControl parameter determines if the router should perform inter-AS multicast forwarding with MOSPF and whether data packets should be forwarded between the DVMRP and MOSPF domains.

The PolicyControl parameter only allows the DVMRP domain to accept MOSPF-sourced multicast packets. For the MOSPF domain to accept DVMRP-sourced multicast packets, a similar configuration must be completed in the MOSPF Service. Failure to do so results in half-duplex communication. For more information, refer to “Dvmrp” on page 37-3 and “PolicyControl” on page 37-5.

Values

Mospf | NoMospf	When set to Mospf, routes learned, except external routes, from the MOSPF domain are considered a valid source subnet for the DVMRP domain. When set to NoMospf, inter-AS multicast forwarding with MOSPF is disabled. To enable source routes to be imported from the MOSPF domain, you must also configure the MOspf parameter. For more information, refer to “MOspf” on page 20-6.
DestGroup | NoDestGroup	When set to DestGroup, data packets are forwarded between DVMRP and MOSPF domains according to the lists established by the -DVMRP DestGroup parameter. For more information, refer to “DestGroup” on page 20-4. When set to NoDestGroup, no filtering is performed, and all data packets are forwarded between domains.

Prune

Syntax

```
SETDefault -DVMRP Prune = [Enable | Disable]
SHow -DVMRP Prune
```

Default Enable

Description The Prune parameter enables or disables the prune mechanism when running the DVMRP routing protocol. The SHow command displays the current value of the parameter.

Values

Enable	When pruning is enabled, the router uses the Reverse Path Multicasting (RPM) algorithm.
Disable	When pruning is disabled, the router uses the Truncated Reverse Path Broadcasting (TRPB) algorithm for multicast routing.

RateLimit

Syntax

```
SETDefault {!<port> | !<tunnel ID>} -DVMRP RateLimit = <Kbits/second>
  (0–100000)
SHow [!<port> | !<tunnel ID> | !*] -DVMRP RateLimit
SHowDefault [!<port> | !<tunnel ID> | !*] -DVMRP RateLimit
```

Default 0

Description The RateLimit parameter specifies and displays the bandwidth in kilobits per second (kbps) that is allocated for the multicast datagram traffic. If the value of this parameter is set to 0, then no limit is applied to the given interface, and the interface uses its full bandwidth.

If the value of this parameter is set to exceed the interface’s bandwidth, a warning message appears, and the result is the same as setting the value to 0.

RouteTable

Syntax

```
FLush -DVMRP RouteTable
SHow -DVMRP RouteTable [<subnet>[/<mask>]] [Long]
```

Default No default

Description The RouteTable parameter flushes or displays the current multicast routing table.

If you specify <subnet>[/<mask>], the routing table for the specified address range is displayed. The mask is an integer between 0 and 32; it is the number of leading 1s in the subnet mask. If a mask is not specified, the natural subnet mask is applied.

If Long is specified, the display shows a lists of ports that connect to child subtrees and leaf subnets.

The FLush -DVMRP RouteTable command deletes all the entries learned from the DVMRP Protocol in the routing table.

TUnnel

Syntax

```
SETDefault !<tunnel ID> -DVMRP TUnnel = <local-end IP>
  <remote-end IP> [<ttl> (1–255)] | None
```

SHow [!<tunnel ID>] -DVMRP TUnnel [<local-end IP> [<remote-end IP>]]

Default 64 (default TTL)

Description The TUnnel parameter creates, deletes, or displays a virtual point-to-point link between a pair of multicast routers that are separated by (unicast) routers, which do not support IP multicasting.

Up to 32 tunnels can be configured using the SETDefault command. To configure a tunnel, you must provide the local IP address and remote IP address.

If IP (unicast) routing is not enabled, you must configure a static route for the remote end of the tunnel.

The added tunnel is immediately activated if the associated CONTrol parameter is set to Enable. To disable a tunnel without deleting it, set the CONTrol parameter to Disable.

IP multicast packets are encapsulated for transmission through a tunnel so that they look like normal unicast packets to intervening routers. The encapsulation is added to an entry when entering a tunnel and stripped off when exiting from a tunnel. The IP-over-IP (with the protocol number set to 4) encapsulation is used for transmitting packets through a tunnel. The IP TTL field of the newly encapsulated packet is configurable through <ttl> and is set to 64 by default.

The SHow command displays all current tunnels or the specified tunnel.

Values

<local-end IP>	The IP address of the local router. This address must be agreed upon with the remote router.
<remote-end IP>	The IP address of the remote router. This address must be unique. You cannot assign tunnels with different local IP addresses and the same remote IP address. The remote IP address also cannot belong to one of the directly connected subnets if the underlying subnet has broadcast or multicast capability.
<ttl>	Configures the time-to-live of the newly encapsulated packet. This value is set to 64 by default.
None	Deletes a tunnel.

UpdateTime

Syntax

```
SETDefault -DVMRP UpdateTime = <seconds> (5–5400)
SHow -DVMRP UpdateTime
```

Default 60 seconds

Description The UpdateTime parameter specifies how often to send route report messages containing the complete routing table.

It derives the time for how long a route is considered valid (RouteExpirationTime) and how long a route exists (GarbageCollectionTime) without confirmation. The RouteExpirationTime is equal to three times the value of this parameter, and the GarbageCollectionTime is equal to five times the value of this parameter.

This parameter can also derive the NeighborExpireTime (how long a neighbor is considered "up" without confirmation) and when to consider the associated virtual interface as a leaf link (LeafConfirmationTime). The NeighborExpireTime is set to two times the value of this parameter plus 20 seconds, and the LeafConfirmationTime is set to three times the value of this parameter plus 20 seconds.

21

ESIS Service Parameter

This chapter describes the End System-to-Intermediate System (ESIS) Service parameters used for Open System Interconnection (OSI) routing. The ESIS parameters are related to the CLNP and ISIS Services. Table 21-1 lists the ESIS Service parameters and the commands.

Table 21-1 ESIS Service Parameters and Commands

Parameters	Commands
CONFiguration	SHow
CONTrol	SETDefault, SHow
HoldTime	SETDefault, SHow
MulticastES	SETDefault, SHow
MulticastES8025	SETDefault, SHow
MulticastIS	SETDefault, SHow
MulticastIS8025	SETDefault, SHow
UpdateTime	SETDefault, SHow

CONFiguration

Syntax

```
SHow -ESIS CONFiguration
```

Default No default display

Description The CONFiguration command displays the values of the parameters in the ESIS Service.

CONTrol

Syntax

```
SETDefault -ESIS CONTrol = ([ChecKSum | NoChecKSum], [FastConfig |
  NoFastConfig], [RefreshRedirect | NoRefreshRedirect])
SHow -ESIS CONTrol
```

Default NoChecKSum, FastConfig, RefreshRedirect

Description The CONTrol parameter determines how the ESIS routing protocol operates.

Values

ChecKSum| NoChecKSum	Specifies whether the checksum is computed for the intermediate system hello protocol data units (ISH PDUs) and end system hello protocol data units (ESH PDUs) generated by the router. The Checksum field is 0 if NoChecKSum is selected. ISH PDUs and ESH PDUs generated by the router. The Checksum field is 0 if NoChecKSum is selected.

FastConfig | NoFastConfig	Determines how fast each system on the network learns about each other's presence. When an IS or ES is introduced to the network, it sends out a hello PDU. A system, upon receiving this PDU from the new system, responds with its own hello PDU, which is unicast packets for the new system. This ensures that all systems on the network can learn about the new network configuration quickly.
RefreshRedirect | NoRefreshRedirect	This option applies only when the router serves as an ES. When the router receives packets from an end system, it refreshes its age timer in its routing table that applies to this particular end system. Only entries that are created by the ESIS Redirect PDUs can be refreshed.

HoldTime

Syntax

```
SETDefault -ESIS HoldTime = <seconds> (1–16000)
SHow -ESIS HoldTime
```

Default 140

Description The HoldTime parameter specifies the value (in seconds) in the Holding Time field in the ESH or ISH PDU sent by the router.

The greater the value of HoldTime, the longer it takes to age out entries in the routing table (which are created by the ISH or ESH PDUs). A greater HoldTime value results in a more stable network, but one that responds more slowly to network topology changes.

3Com recommends that the HoldTime value be slightly more than twice the value of the UpdateTime parameter. For more information, refer to "UpdateTime" on page 21-3.

MulticastES

Syntax

```
SETDefault -ESIS MulticastES = <multicast address>
SHow -ESIS MulticastES
```

Default %09002B000004

Description The MulticastES parameter specifies the multicast address used by the router to send or receive ISH PDUs. It is the group address representing all the end systems on the network. To ensure proper communication between systems, the MulticastES value on all end systems and intermediate systems on the network should be the same. This parameter is only used on Ethernet and Fiber Distributed Data Interface (FDDI) interfaces.

MulticastES8025

Syntax

```
SETDefault -ESIS MulticastES8025 = <multicast address>
SHow -ESIS MulticastES8025
```

Default %030000000200

Description The MulticastES8025 parameter specifies the multicast address used by the router to send or receive ISH PDUs. It is the group address representing all the end systems on the network. To ensure proper communication between systems, the MulticastES8025 value on all end systems and intermediate systems on the network should be the same. This parameter is only used on token ring interfaces.

This parameter value is in canonical format, which is also known as big-endian format.

MulticastIS

Syntax
```
SETDefault -ESIS MulticastIS = <multicast address>
SHow -ESIS MulticastIS
```

Default %09002B000005

Description The MulticastIS parameter specifies the multicast address used by the router to send or receive ESH PDUs. It is the group address representing all the intermediate systems on the network. To ensure proper communication between systems, the MulticastIS value on all end systems and intermediate systems on the network should be the same. This parameter is only used on Ethernet and FDDI interfaces.

MulticastIS8025

Syntax
```
SETDefault -ESIS MulticastIS8025 = <multicast address>
SHow -ESIS MulticastIS8025
```

Default %030000000100

Description The MulticastIS8025 parameter specifies the multicast address used by the router to send or receive End System Hello Protocol Data Units (ESH PDUs). It is the group address representing all the intermediate systems on the network. To ensure proper communication between systems, the MulticastIS8025 value on all end systems and intermediate systems on the network should be the same. This parameter is only used on token ring interfaces.

This parameter value is in canonical format, which is also known as big-endian format.

UpdateTime

Syntax
```
SETDefault -ESIS UpdateTime = <seconds> (1–16000)
SHow -ESIS UpdateTime
```

Default 60

Description The UpdateTime parameter specifies the interval (in seconds) between sending out ESH or ISH PDUs from the router.

The smaller the value of UpdateTime, the more frequently ESH and ISH PDUs are sent. Frequent hello packets consume more network bandwidth but allow the network to respond faster to topology changes.

ESH or ISH PDUs can be sent more frequently than the UpdateTime parameter specifies in the following situations:

- After the router is turned on, it sends out a series of hello packets in a short period of time, which allows other nodes on the network to quickly learn about the router's presence.
- After you change the value of NetEntityTitle, the router immediately sends out hello packets.
- After you change the value of MulticastES, MulticastIS, HoldTime, or UpdateTime, the router immediately sends out hello packets.

22 FDDI SERVICE PARAMETERS

The FDDI Service supports Fiber Distributed Data Interface (FDDI) station management. Table 22-1 lists the FDDI Service parameters and commands.

Table 22-1 FDDI Service Parameters and Commands

Parameters	Commands
BufferErrors	SHow
CurrentPAth	SHow
DownNeighbor	SHow
DupAddress	SHow
FrameCounts	SHow
FrameErrorRatio	SHow
InsertPolicy	SETDefault, SHow
InsertedStatus	SHow
LCTFailCount	SHow
LEMCount	SHow
LLCService	SHow
MACAction	SET
MACPlacement	SHow
MaintLineStateA	SET, SHow
MaintLineStateB	SET, SHow
OpticalBypass	SHow
PCConnectState	SHow
PCControlA	SET
PCControlB	SET
PCMState	SHow
PMF	SETDefault, SHow
PortNeighbor	SHow
RemDisconnect	SHow
RMTState	SHow
SMTAddress	SHow
SMTVersion	SETDefault, SHow
StationAction	SET
StationCONFig	SHow
StationID	SHow
TNEGotiated	SHow
TREQuest	SETDefault, SHow
UpNeighbor	SHow
UserData	SETDefault, SHow
WrapAB	SETDefault, SHow

The SMTAddress, UpNeighbor, and DownNeighbor parameter displays show addresses in both most significant bit (MSB) and canonical forms. The MSB form is shown first, and the canonical form is shown in parentheses.

BufferErrors

Syntax
```
SHow !<path> -FDDI BufferErrors
```

Default No default

Description The BufferErrors parameter displays the current elasticity buffer error count (a decimal value between 0 and 4,294,967,295) for both ports of a physical (PHY) layer protocol board.

CurrentPAth

Syntax
```
SHow !<path> -FDDI CurrentPAth
```

Default No default

Description The CurrentPAth parameter displays the path type associated with a media access controller (MAC). The following are possible CurrentPAth values returned by this command:

Isolated	The MAC is not on any path.
Primary	The MAC is placed on the primary path. In a Thru state, this indicates that the MAC receives on the A port and sends on the B port.
Secondary	The MAC is placed on the secondary path. In a Thru state, this indicates that the MAC receives on the B port and sends on the A port.

DownNeighbor

Syntax
```
SHow !<path> -FDDI DownNeighbor
```

Default No default

Description The DownNeighbor parameter displays the downstream neighbor's long individual MAC address (12 hex characters).

DupAddress

Syntax
```
SHow !<path> -FDDI DupAddress
```

Default No default

Description The DupAddress parameter displays the setting of the duplicate address flag. The duplicate address flag is set to the Detected state when a frame is detected with a MAC address that is a duplicate of the receiving station's MAC address. Possible displayed settings of the duplicate address flag are as follows:

Detected	Duplicate address detected.
Not Detected	Duplicate address not detected.

FrameCounts

Syntax

```
SHow !<path> -FDDI FrameCounts
```

Default No default

Description The FrameCounts parameter displays the received and sent frames of the specified path.

FrameErrorRatio

Syntax

```
SHow !<path> -FDDI FrameErrorRatio
```

Default No default

Description The FrameErrorRatio parameter displays an indication of the error rate detected at a MAC, relative to the number of frames processed. The value returned is a decimal number between 0 and 65,535.

InsertPolicy

Syntax

```
SETDefault !<path> -FDDI InsertPolicy = [Insert | DoNotInsert]
SHow !<path> -FDDI InsertPolicy
```

Default Insert

Description The InsertPolicy parameter sets the insertion policy for a station's attachment to the ring if an optical bypass switch is in use. If there is no optical bypass switch, this parameter has no effect.

The SHow command displays the current insertion policy.

InsertedStatus

Syntax

```
SHow !<path> -FDDI InsertedStatus
```

Default No default

Description The InsertedStatus parameter displays whether or not an attachment is currently inserted onto the ring, or is optically bypassed.

LCTFailCount

Syntax

```
SHow !<path> -FDDI LCTFailCount
```

Default No default

Description The LCTFailCount parameter displays the current link confidence test failure count for both PHY components on a PHY board.

LEMCount

Syntax

```
SHow !<path> -FDDI LEMCount
```

Default No default

Description The LEMCount parameter displays the current link error monitor count for both PHY components on a PHY board.

LLCService

Syntax

```
SHow !<path> -FDDI LLCService
```

Default No default

Description The LLCService parameter displays the state of the logical link control (LLC) service provided by a MAC. Possible displayed states of the LLC service are as follows:

Available	LLC service is available.
NotAvailable	LLC service is not available.

MACAction

Syntax

```
SET !<path> -FDDI MACAction = [EnableLLC | DisableLLC | ConnectMAC
  | DisconnectMAC]
```

Default No default

Description The MACAction parameter enables or disables the LLC service provided by a MAC, and connects or disconnects a MAC to and from the ring. This parameter can only be set.

Values

EnableLLC	Enables LLC service.
DisableLLC	Disables LLC service.
ConnectMAC	Connects the MAC to the ring.
DisconnectMAC	Disconnects the MAC from the ring.

MACPlacement

Syntax

```
SHow !<path> -FDDI MACPlacement
```

Default No default

Description The MACPlacement parameter displays the path ID of the MACs whose transmit path exits the station through the ports on a PHY board.

MaintLineStateA

Syntax

```
SET !<path> -FDDI MaintLineStateA = [Quiet | Idle | Master | Halt
  | Active]
SHow !<path> -FDDI MaintLineStateA
```

Default Quiet

Description The MaintLineStateA parameter sets the maintenance line state of port A using the SET command. The maintenance line state is the state of the port's transmitter, and the receiver line state is the state of the port's receiver. The SHow command displays the current maintenance line state and receiver line state of port A.

The PCControlA parameter (refer to "PCControlA" on page 22-6) must be used to set port A to maintenance state before port A's line state can be changed.

Values

Quiet	Sends or receives quiet symbols.
Idle	Sends or receives idle symbols.
Master	Sends or receives alternating Halt and Quiet symbols.
Halt	Sends or receives halt symbols.
Active	Sends or receives an FDDI frame.

MaintLineStateB

Syntax

```
SET !<path> -FDDI MaintLineStateB = [Quiet | Idle | Master | Halt
  | Active]
SHow !<path> -FDDI MaintLineStateB
```

Default Quiet

Description The MaintLineStateB parameter sets the maintenance line state of port B using the SET command. The SHow command displays the current maintenance line state of port B.

The PCControlB parameter must be used to set port B to maintenance state before the port B line state can be changed.

Values

Quiet	Sends or receives quiet symbols.
Idle	Sends or receives idle symbols.
Master	Sends or receives alternating Halt and Quiet symbols.
Halt	Sends or receives halt symbols.
Active	Sends or receives an FDDI frame.

OpticalBypass (Switch)

Syntax

```
SHow !<path> -FDDI OpticalBypass
```

Default No default

Description The OpticalBypass parameter displays whether or not an optical bypass switch is present on the physical attachment board. Possible displayed settings for the optical bypass switch are as follows:

Present	Optical bypass switch is installed.
Not Present	No optical bypass switch.

PCConnectState

Syntax

```
SHow !<path> -FDDI PCConnectState
```

Default No default

Description The PCConnectState parameter displays the current connection state for both PHY components on a PHY board. the physical values are DisabledPHY, ConnectingPHY, and StandbyPHY. These values represent the following states:

- DisabledPHY is disabled.
- ConnectingPHY is ready to connect or is in the process of connecting to a neighbor.
- StandbyPHY is in standby mode (dual-homing). This mode occurs on the A PHY when the B PHY is connected to a master port. If the B PHY fails, the A PHY is changed to an active state.

PCControlA

Syntax

```
SET !<path> -FDDI PCControlA = [Maint | Normal]
```

Default Normal

Description The PCControlA parameter sets the connection control mode for port A of the PHY interface.

Values

Maint	Sets the port to maintenance state. This value takes the port out of operational state and allows use of the MaintLineStateA parameter to manually control the transmitter of the port.
Normal	Indicates normal operating mode.

PCControlB

Syntax

```
SET !<path> -FDDI PCControlB = [Maint | Normal]
```

Default Normal

Description The PCControlB parameter sets the connection control mode for port B of the PHY interface.

Values

Maint	Sets the port to maintenance state. This state takes the port out of operational state and enables the MaintLineStateB parameter to manually control the transmitter of the port.
Normal	Indicates normal operating mode.

PCMState

Syntax

```
SHow !<portID> -FDDI PCMState
```

Default No default

Description The PCMState parameter displays the current physical connection management (PCM) state for both ports of a PHY board. Possible values returned by this command are as follows:

Off	Initial state.
Break	Initiating a connection.
Trace	Localizing a Stuck Beacon condition.

Connect	Waiting for a connection sequence to begin. This is the normal PCMState when a port is ready to connect.
Next	State used to separate signaling in Signal state.
Signal	State used for exchange of configuration information.
Join	First in sequence for active connection.
Verify	Second in sequence for active connection.
Active	Third in sequence for active connection. This is the normal PCMState when a port is operational.
Maint	Maintenance state.

PMF

Syntax

```
SETDefault !<path> -FDDI PMF = <hex bytes with PMF Set request>
SHow !<path> -FDDI PMF <hex bytes with PMF Get request>
```

Default No default

Description The PMF parameter simulates receipt of a Station Management (SMT) parameter management frame Get request on the specified path. The requested parameter is specified by encoding the parameter management frame (PMF) Get request starting with the parameter encoding.

The SETDefault command simulates receipt of an SMT parameter management frame Set request on the specified path. The requested parameter is specified by encoding the PMF Set request starting with the parameter encoding.

PortNeighbor

Syntax

```
SHow !<path> -FDDI PortNeighbor
```

Default No default

Description The PortNeighbor parameter displays the type of port neighbor that communicates with each of the ports on the PHY board. This command produces a response for both port A and port B. Possible displayed settings of the port neighbor and their meanings are as follows:

A	Neighbor is port A.
B	Neighbor is port B.
Slave	Neighbor operates as a slave; not a normal condition.
Master	Neighbor operates as a master.
Unknown	Indicates a possible fiber disconnect or other error condition.

RemDisconnect

Syntax

```
SHow !<path> -FDDI RemDisconnect
```

Default No default

Description The RemDisconnect parameter displays the current value of the Remote Disconnect Flag. When set (value = Yes), this flag indicates that the station has been remotely disconnected. Possible displayed settings of the Remote Disconnect Flag and their meanings are as follows:

Yes	Station was remotely disconnected.
No	Station has not been remotely disconnected since power-up.

RMTState

Syntax

```
SHow !<path> -FDDI RMTState
```

Default No default

Description The RMTState parameter displays the current Ring Management state for a MAC. Possible displayed settings of the current Ring Management state are as follows:

Isolated	Initial state.
NonOp	Ring is not operational. MAC is participating in ring recovery.
RingOp	Ring is operational.
Detect	MAC is in the process of detecting duplicate address conditions that prevent ring operation.
NonOpDup	Ring is not operational due to presence of another MAC with the same address as this MAC.
RingOpDup	Ring is operational, but another MAC with the same address as this MAC has been detected.
Directed	MAC is sending directed Beacon frames to the Status Report Frame multicast address.
Trace	Trace has been initiated.

SMTAddress

Syntax

```
SHow !<path> -FDDI SMTAddress
```

Default The preset SMT address (12 hex characters) on the MAC board in your bridge/router.

Description The SMTAddress parameter displays the Station Management (SMT) MAC address (12 hex characters).

SMTVersion

Syntax

```
SETDefault !<path> -FDDI SMTVersion = [Version6.2 | Version7.2 |
 Auto]
SHow !<path> -FDDI SMTVersion
```

Default Auto

Description The SMTVersion parameter sets or displays the version of SMT to be used on the system. This parameter specifies the format for the SMT frames to be used on the ring.

Values

Version6.2	The system recognizes and formats frames in accordance with the SMT Version 6.2 ANSI standard.
Version7.2	The system recognizes and formats frames in accordance with the SMT Version 7.2 ANSI standard.

Auto	The system conforms to the operational version of SMT based on the last received valid Parameter Management Request frame. The system conforms to the version of SMT being used by the management stations on the ring. If multiple FDDI management stations are present on the ring and are operating with different SMT versions, this setting may cause problems with Status Report frames. In this case, the specific version of SMT should be specified.

StationAction

Syntax

```
SET !<path> -FDDI StationAction = [Connect | Disconnect | PathTest
 | SelfTest]
```

Default No default

Description The StationAction parameter specifies the function of the station.

Values

Connect	Initiates station connection sequence. Clears the Remote Disconnect flag. If the station and ring are functioning properly, Connect causes the station to be inserted into the ring.
Disconnect	Causes the station to remove itself from the FDDI ring. The station remains out of the ring until a local or remote Connect action is performed or until the system is reinitialized.
PathTest	Causes the station to test all internal paths. The station must be disconnected for this to happen.
SelfTest	Causes a self-test of individual station components.

StationCONFig

Syntax

```
SHow !<path> -FDDI StationCONFig
```

Default No default

Description The StationCONFig parameter displays the current configuration state of the station. Possible displayed settings generated by this command and their meanings are as follows:

Isolated	Isolated from ring.
WrapS	Normal state for single-attached station (SAS). Not currently used.
WrapA	Wrap A state. This state occurs if the A port is active, the B port is inactive, and the station’s paths are not configured for concatenation. In this state, only the primary path is connected to the A port. This state only occurs if the station's requested path values have been modified by an FDDI management station.
WrapB	Wrap B state. This state occurs if the B port is active, the A port is inactive, and the station’s paths are not configured for concatenation. In this state, only the secondary path is connected to the B port. This state only occurs if the station's requested path values have been modified by an FDDI management station.

WrapAB	Wrapped through both A and B ports. The station receives the token from A port input and transmits the token out the A port output; the station receives the token from B port input and transmits the token out the B port output.
CWrapA	Concatenated Wrap A state. This state occurs if the A port is active, the B port is inactive, and the station's requested paths are configured to concatenate the primary and secondary paths (default). All MACs on the primary and secondary paths are included in the token path entering the A port and exiting the A port.
CWrapB	Concatenated Wrap B state. This state occurs if the B port is active, the A port is inactive, and the station's requested paths are configured to concatenate the primary and secondary paths (default). All MACs on the primary and secondary paths are included in the token path entering the B port and exiting the B port.

StationID

Syntax

```
SHow !<path> -FDDI StationID
```

Default No default

Description The StationID parameter shows the 16-hex-character value assigned as station identification. The SMT address of the first MAC in the station is used for the last 6 bytes of the station ID.

TNEGotiated

Syntax

```
SHow !<path> -FDDI TNEGotiated
```

Default No default

Description The TNEGotiated parameter displays the target token rotation time (in milliseconds) as negotiated in the Claim process.

TREQuest

Syntax

```
SETDefault !<path> -FDDI TREQuest = <milliseconds> (1–200)
SHow !<path> -FDDI TREQuest
```

Default 165

Description The TREQuest parameter sets the time (in milliseconds) that a station uses as its bid for target token rotation time in the Claim process.

UpNeighbor

Syntax

```
SHow !<path> -FDDI UpNeighbor
```

Default No default

Description The UpNeighbor parameter displays an upstream neighbor's individual MAC address (12 hex characters).

UserData

Syntax

```
SETDefault !<path> -FDDI UserData = “<string>”
SHow !<path> -FDDI UserData
```

Default UserData = <null string>

Description The UserData parameter modifies the station’s user data string. Quotation marks are required around the variable. The SHow command displays the current user data string.

WrapAB

Syntax

```
SETDefault !<path> -FDDI WrapAB = [Yes | No]
SHow !<path> -FDDI WrapAB
```

Default No

Description The WrapAB parameter sets or resets the station’s WrapAB flag. This flag controls the behavior of a dual MAC station when the station is connected to the master ports of one or more concentrators. In this case, both ports of the station are functioning as single MAC stations to be used simultaneously if both links are active. If this option is not set, the B port takes precedence and the A port functions as a standby port in case the B port fails (dual homing).

Set this option if the station’s ports are connected to two different concentrators on different rings. Do not set the option if the station’s ports are connected to the same concentrator or to two different concentrators on the same ring.

The SHow command displays the current setting for the station’s WrapAB flag.

Values

Yes	Determines that a dual MAC station will allow both ports to become simultaneously active when connected to master ports.
No	Determines that port B takes precedence over port A and is the standby port if port B fails.

23 FIlter Service Parameters

This chapter describes all parameters related to packet filtering, logging, sequencing, and packet fair-bandwidth allocation. Table 23-1 lists the FIlter Service parameters and commands.

Table 23-1 FIlter Service Parameters and Commands

Parameters	Commands
CONFiguration	SHow
CONTrol	SETDefault, SHow
DefaultAction	SETDefault, SHow
DIAGnostics	SHow
MASK	ADD, DELete, SHow
MNEmonics	SHow
POLicy	ADD, DELete, FLush, SHow
SELection	SETDefault, SHow
StationGroup	ADD, CHange, DELete, SHow

CONFiguration

Syntax

```
SHow -FIlter CONFiguration
```

Default No default

Description The CONFiguration parameter displays all relevant configuration parameters for the FIlter Service: control, masks, policies, and default action.

CONTrol

Syntax

```
SETDefault -FIlter CONTrol = ([Enabled | Disabled], [MatchOne |
   CheckAll])
SHow -FIlter CONTrol
```

Default Disabled, MatchOne

Description The CONTrol parameter disables or enables the FIlter Service.

Values

Enabled | Disabled	Specifies whether filtering is enabled or disabled.
MatchOne | CheckAll	The MatchOne value determines which policy should be applied if several policies are defined. Packets are checked against policies that are arranged on the decision tree (For more information, refer to “DIAGnostics” on page 23-2.) In this case, the first policy on the decision tree matching the packet is applied, and no other policies are checked.

The CheckAll value determines which policy or policies should be applied if there are several policies defined. Packets are checked against policies that are arranged on the decision tree (For more information, refer to “DIAGnostics” on page 23-2.) In this case, all policies are checked, and policies that match the packet are applied, unless they are mutually exclusive. For example, three policies may be applied: forward, count, and sequence. If two mutually exclusive policies, forward and discard, are both met, then the discard policy is applied.

DefaultAction

Syntax

```
SETDefault -FIlter DefaultAction = [Forward | Discard]
SHow -FIlter DefaultAction
```

Default Forward

Description The DefaultAction parameter specifies the action applied to a packet if it does not match any of the policies configured. For example, imagine that two policies are defined. The first policy specifies that Internet Protocol (IP) packets are forwarded. The second policy specifies that Xerox Network Systems (XNS) packets are discarded. When an AppleTalk packet is encountered, the action specified for DefaultAction is taken.

Values	
Forward | Discard	Specifies how to handle packets that do not match. If DefaultAction is set to forward, the packet that does not match the configured policies is forwarded. If DefaultAction is set to discard, the packet that does not match the configured policies is discarded.

DIAGnostics

Syntax

```
SHow -FIlter DIAGnostics
```

Default No default

Description The DIAGnostics parameter shows the current active policies on the internal decision tree.

MASK

Syntax

```
ADD -FIlter MASK <maskname> <location> [<operation>] <pattern>
   <location>:= <mnemonic format> |
   <numerical format><mnemonic format>:=<protocol>.<field>
   <numerical format>:=[<protocol >.DATA+][%]<offset>[:[%]<length>]
   <operation>:=<operator><operand><operator>:=<bitwise or>|<bitwise
   and> | <bitwise exclusive or> <operand>:=<numerical value>
   <pattern>:=<comparison><match><comparison>:=(equal to|not equal to
   | greater than | greater than or equal to | less than | less than
   or equal to | inclusive range) <match>:=different values for
   different <locations>
DELete -FIlter MASK <maskname> | ALL
SHow -FIlter MASK [<maskname> | BuiltIn]
```

Default No default

Description The MASK parameter defines the criteria used to identify and select a packet. You can define a mask using a set of predefined, built-in criteria, or you can use numerical syntax. For a complete list of predefined masks, refer to Chapter 4 in *Using NETBuilder Family Software*. The criteria defined in the MASK parameter are location, operation, and pattern. The mask has a true value if the condition is matched and a false value if the condition is not matched.

To delete all user-defined masks, use DELete -FIlter MASK ALL. A user-defined mask is not deleted if it is used by any policy. If a user-defined mask cannot be deleted, the message “Can’t delete - <maskname still in use>” appears on the display. If you use the SHow -FIlter MASK command without specifying any values, both user-defined and built-in masks are displayed.

Values <maskname> Specifies the mask name, which is the user-defined string that identifies the mask consisting of a maximum of 15 printable alphanumeric characters. The mask name must begin with an alphanumeric character. Only four extra characters are valid for names. These characters are an underscore (_), period (.), hyphen (-), and ampersand (&).

Reserved words and names of built-in masks are not legal names. Reserved words are all, among, and, at, betw, between, from, to, forward, discard, count, prioritize, and sequence. All names are case-insensitive.

<location> Specifies the position in the packet where the operation takes place. Using the command syntax, you can specify the location either in mnemonic or numerical form. Both mnemonic and numerical syntax forms are listed here.

<mnemonic format> Consists of the following syntax: <protocol>.<field>

<numerical format> Consists of the following syntax:<protocol >.DATA+] [%] <offset> [: [%] <length>] where <offset> and <length> can be specified in decimal or hexadecimal format.

When predefined mnemonics are used, the offset and the number of bytes are implied. When a numerical value is used, the offset and number of bytes are explicitly specified. Enter the offset and number of bytes according to the following guidelines:

When specified as hexadecimal, precede the value by a percent sign (%). Otherwise, the values are in decimal format.

Use the correct number of hexadecimal digits for your intended mask size, or explicitly specify the length. The following list shows the corresponding number of digits for three mask sizes:

Number of Hex Digits	**Mask Size**
Two	One byte
Four	One word
Eight	Two words

When <protocol>.DATA+ is not specified in numerical form, the format indicates a bridge filter, and the offset counts from the start of the data link header.

The <numerical format> field cannot be used when the <protocol> is DLSW, LLC2, or SDLC.

<protocol> Indicates the starting point or offset in the packet if a filter has been assigned. This value can also indicate which protocol packets should be forwarded or discarded. If DataLink is specified, the filter is applied to bridged packets only. If Internet Packet Exchange (IPX) is specified, the filter is applied to IPX only. If you specify the protocol as DLSW, LLC2, or SDLC, then the only action supported for the -POLicy parameter is Trace.

<field> Specifies the area within the protocol header.

<operation> Indicates a conversion to be applied to the selected area within a packet. The result of the conversion is then used as a comparison with a given result. The operation consists of an operator and an operand. The operators allowed are logical, bitwise operators, and require an operand. Some mnemonics do not support an operation.

<operator> Specifies an operator used in the ADD -FIlter MASK command. The command includes optional logical operators bitwise AND, bitwise EXclusive OR, and bitwise OR. Table 23-3 summarizes the operators, their meanings, and their effects.

Table 23-2 Logical Operations in the ADD-Filter MASK Command

Symbol	Name	Example
&	bitwise and	11010111
		AND 10011001
		10010001
|	bitwise or	10010111
		OR 00100010
		10110111
^	bitwise exclusive or	10010111
		XOR 00100010
		10110101

The <operator> field cannot be used when the <protocol> is DLSW, LLC2, or SDLC.

<pattern> Specifies a set of conditions within the packet that is compared to an expected value. The pattern consists of a comparison and an expected value. A comparison indicates how to match similarities of the selected portions of the packet with the selected result. Some mnemonics do not support all comparisons. A comparison is represented by one of the symbols in Table 23-3.

Table 23-3 Comparison Symbols

Symbol	Meaning
=	equal
>	greater than
<	less than
-	inclusive range
!	not equal
>=	greater than or equal to
<=	less than or equal to

When the <protocol> is DLSW, LLC2 or SDLC, the <, <=, >, >= comparison symbols cannot be used.

BuiltIn

Specifies a built-in mask, which contains a predefined set of qualifications and a specified expected value. For tables listing built-in masks, refer to Chapter 4 in *Using NETBuilder Family Software*

Messages

You may see the following messages when defining masks:

```
Mask <maskname> is added
Mask <maskname> is deleted
Mask <maskname> already exists
Mask <maskname> does not exist
Invalid operation
Invalid field
Can’t delete - still in use
Can’t add - max. entry
<maskname> is a built-in mask
<maskname> is a policy
<maskname> is a reserved word
<maskname> still in use
Invalid syntax: Mnemonic <fieldname> allows only ‘=’ and ‘!=’
<maskname> can’t be traced
<maskname> can only be traced
<data format> can’t be used with IBM protocols
```

MNEmonics

Syntax

```
SHow -FIlter MNEmonics
```

Default

No default

Description

The MNEmonics parameter displays all possible options for a location that can be used to define a mask.

POLicy

Syntax

```
ADD -FIlter POLicy <p_name> <action> <maskname> [<context>]
   <action> = (PROTocolRsrv <tag> | Count | Discard | DodDiscard |
   Forward | Sequence | Prioritize | Trace) <1–255><masks>:=<maskname>[,
   <maskname>...]<context>:=[AT<list of ports>]|[TO <list of ports>]
   | [FROM <list of ports>] | [FROM <list of ports> TO <list of ports>]
   | [BETWEEN <list of ports> AND <list of ports>] | [AMONG <list of
   ports>] <list of ports>:=ALL | <portid> | <range of ports>[,
   <list of ports>] <range of ports>:=<portid> - <portid>
DELete -FIlter POLicy <policyname> | ALL
FLush -FIlter POLicy [<policyname>]
SHow -FIlter POLicy [<policyname>]
```

Default No default

Description The POLicy parameter specifies filtering rules and assigns an action if the rules are met. This parameter combines selection criteria (specified as masks through the MASK parameter) with a system context (specified as ports) and then assigns an action. You can specify up to four selection criteria (masks). The action associated with the policy is taken only if a packet meets all selection criteria and the context is valid.

The FLush -FIlter POLicy command flushes the statistics of the POLicy parameter. The SHow -FIlter POLicy command displays all the configured policies or a specified policy. The number of packets and byte counts also are displayed. The DELete -FIlter POLicy ALL command deletes all of the defined policies.

Values **<p_name>**

A policy name is the user-defined string that identifies the policy. You can use up to 15 printable alphanumeric characters to define the policy name. The policy name must begin with an alphanumeric character. Only four extra characters are valid for names. These characters are an underscore (_), period (.), hyphen (-), and ampersand (@).

The order in which you enter policy names is not the order in which they are used or displayed in the software. The software arranges the policies in the most efficient way and rearranges masks within a policy. For example, the following display appears when you enter SHow -Filter POLicy:

```
7 policies defined.
id name    action          masks
============================================================
p0 IP12    : Discard IP    FROMCS1 TOCS2 AT all (0, 0)
p1 IP13    : Discard IP    FROMCS1 TOCS3 AT all (0, 0)
p2 IP21    : Discard IP    FROMCS2 TOCS1 AT all (0, 0)
p3 IP23    : Discard IP    FROMCS2 TOCS3 AT all (0, 0)
p4 IP12SR  : Discard IP    FROMCS1 TOCS2 ALLRT AT all (0, 0)
p5 XNSBC   : Discard XNS BC AT all (0, 0)
p6 IPXBC Discard IPX BC AT !2, !4 (0, 0)
```

When you enter SHow -FIlter DIAGnostics, the following display appears:

```
masks  policy
==========================
BC     IPXBC
       XNSBC
IP     IP12SR
       IP12
       IP13
       IP21
       IP23
```

In this example, IPXBC is entered last, but it is the first policy on the decision tree. In the same policy, the BC mask appears before IPX even though these masks were entered in a different order. The IPXBC and XNSBC policies have the BC mask in common. The IP mask is also common to IP12, IP13, IP21, and IP23.

Reserved words and names of built-in masks are not legal names. Reserved words are all, among, and, at, betw, between, from, to, forward, discard, count, prioritize, and sequence. All names are case-insensitive.

<action>

An action is the operation that is performed when selection criteria are met. The values and definitions for <action> are listed in Table 23-4.

Table 23-4 Actions Taken in the POLicy Parameter

Action	Definition
PROTocolRsrv <tag>	Specifies protocol reservation as the action option and specifies a tag to identify the packets transmitting from the WAN port that will receive the amount of reserved bandwidth designated by the protocol reservation procedure. The procedure also specifies the matching tag, the conditions to be met, and the percentage of bandwidth to be received by the identified packets. Do not specify the PROTocolRsrv action with a specific port number. The protocol reservation tag can be any case-insensitive alphanumeric sequence of 15 characters maximum. The tag does not need to be unique because multiple FilterAddrs definitions can use the same tag. The protocol reservation configuration procedure can vary for different packet types. For detailed information on how to configure protocol reservation for all packet types, refer to Chapter 49 in *Using NETBuilder Family Software*.
Count	The packet is counted when it is forwarded.
Discard	The packet is discarded when matching is completed.
DodDiscard	For a DOD port, if the dial-up path is down, the packet is discarded and does not cause the dial-up path to be raised. If the path is up, the packet is forwarded, but will not be considered as “user” traffic that keeps a dial-up path up. For a non-DOD port, the action taken is similar to the Forward action.
Forward	The packet is forwarded when matching is completed.
Sequence	The packet is forwarded in the order it is received.
Prioritize	The packet is assigned to a high-, medium-, or low-queue depending on how you configured this action.
Trace	The packet is sent to the trace facility for diagnosing conditions for IBM-related protocols. The action is only valid if the protocol set with the -FIlter MASK parameter is DLSW, LLC2, or SDLC.

<maskname>

The <maskname> value includes a list of masks to which the POLicy parameter applies. Using the masks convention within the POLicy syntax, you must define the mask name that determines to which masks the filter applies.

Masks uses the following syntax convention:

```
ADD -FIlter POLicy <policyname> <action> <[maskname], [maskname]>
   <context>
```

Select the mask name by using either the MASK parameter or a built-in mask.

If policies with the same masks but different actions are defined, the software reorders the policies defined so that policies with the discard action are checked before policies with other actions.

For more information on the MASK parameter, refer to "MASK" on page 23-2. For more information on built-in masks, refer to Chapter 4 in *Using NETBuilder Family Software.*

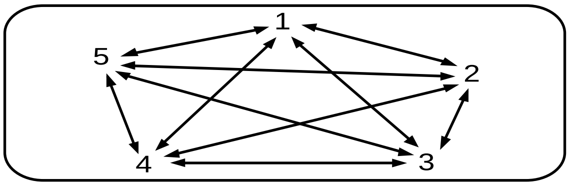
<context>

The <context> value applies a filter only to packets traveling between specific ports in a specified direction. The following syntax conventions are used to define context:

```
ADD POLicy <policyname> <action> [<mask applicability>[AT
   <list of ports>] | [TO <list of ports>] | [FROM <list of ports> TO
   <list of ports>] | [BETWEEN <list of ports> AND <list of ports>] |
   [AMONG <list of ports>]]
```

The following values are associated with context:

AT	Apply this action if the packet is received from or destined to the specified ports.
TO	Apply this action if the packet is destined to the specified ports.
FROM	Apply this action if the packet is received from the specified port.
FROM...TO	Apply this action if the packet is received from the ports specified after FROM and destined to the ports specified after TO.

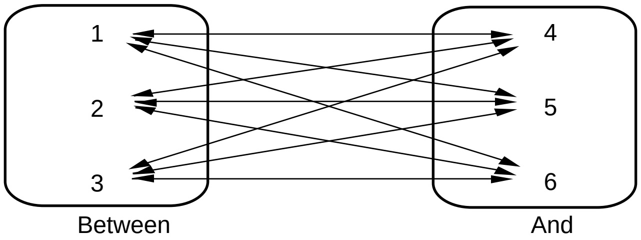


Among

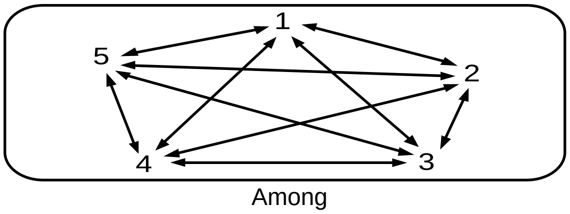
If the context is not specified, AT ALL is the default value. AT ALL signifies "at every port of the platform." If the action is "sequence," the only valid context direction is TO. If the action is neither "sequence" nor "bandwidth," and the context is not specified, AT ALL is the default value.

For the DLSw protocol, the <context> value is not allowed. For the LLC and SDLC protocols, only AT, TO, and FROM actions are allowed.

BETWeen...AND Apply this action if the packet is received from the ports specified after BETWeen and destined to the ports specified after AND, or vice versa.



AMONG Apply this action if the packet is received from and destined to the specified ports.



Messages You may see the following messages appear when defining policies:

```
Policy <policyname> is added
Policy <policyname> is deleted
Policy <policyname> already exists
Policy <policyname> does not exist
Can’t add - max. entry
<policyname> is a built-in mask
<policyname> is a mask
<policyname> is a reserved word
Mask <maskname> does not exist
Invalid action
Invalid context
StationGroup
```

SELection

Syntax

```
SETDefault -FIlter SELection = ALL | <BRidge> [,<IPX>] [,DLSW] [,LLC]
   [,SDLC]
SHow -FIlter SELection
```

Default BRidge

Description The SELection parameter allows you to select which services the filter function is used for. When you select a protocol, you can specify that any configured policies for that protocol are filtered. When you deselect the protocol, you can retain the policies and masks configured for that protocol without applying the filter function to them. A combination of the values configured for the SELection and CONTrol parameters determines the state of the filtering function.

Values

<BRidge Selects the BRidge Service for filtering.

<IPX> Selects the IPX Service for filtering.

All Selects both the BRidge and IPX Services for filtering.

DLSW Selects the DLSw Service to be used for filtering.

LLC Selects the LLC2 Service to be used for filtering.

SDLC Selects the SDLC Service to be used for filtering.

For NETBuilder bridge/router platforms without IBM components, the DLSw, LLC and SDLC options will not be accepted or displayed.

StationGroup

Syntax

```
ADD -FIlter StationGroup <stationgroupname> [<address>]
CHange -FIlter StationGroup <oldstationgoupname> <newstationgroupname>
DELete -FIlter StationGroup <stationgroupname> [<address> | ALL]
SHow -FIlter StationGroup [<stationgroupname>]Default
```

Default No default

Description The StationGroup parameter groups a set of station addresses for easy reference. With the StationGroup parameter you can:

- Group logically related stations into a group
- Give the station group a name
- Create a mask by referencing the station group name
- Create a POLicy by referencing such a mask

A group is created when the station group name is used for the first time. Addresses can be entered in either canonical or noncanonical format in all commands where applicable.

A station becomes a member of a group when its media access control (MAC) address is added to the collection of MAC addresses of other group members. You can use a specific address in more than one station group at a time. Reserved words and names of built-in masks, user-defined masks, and policies are not legal names. You can change the name of any group using the CHange command. A station can be a member of one group or several groups (for example, accounting, macintosh, and bldg_100).

The maximum number of station groups is 16. The maximum number of MAC addresses is 511. The maximum number of MAC addresses that may belong to all station groups is platform-dependent: you can use 511 addresses on a NETBuilder system and 2,047 on a NETBuilder II system. The maximum number of MAC addresses that can belong to one particular station group is also 511 on a NETBuilder system and 2,047 on a NETBuilder II system.

You can create an empty group (a group without any members) without specifying any address in order to reserve a place for a future group. For example, you may plan to use a new group in the future but currently do not have the physical stations or addresses belonging to that group. Using the StationGroup parameter, you can create a place for that group and add the station addresses later.

You can also create an empty group by deleting all addresses from an existing nonempty group. You can keep the group name and add new addresses later. An empty group still exists in the system.

To delete a group from the system, you must first delete all members of that group and all masks that are defined for members in that group. Only empty groups and groups that are not referenced in any mask can be deleted.

Defining a POLicy in terms of an empty station group may adversely affect performance, because the filtering rules will not be met.

Table 23-5 lists the StationGroup commands and their uses.

Table 23-5 StationGroup Commands and Uses

Command	Use
ADD -FIlter StationGroup <stationgroupname> <address>	Creates a group and adds an address to it, or adds an address to an existing group.
ADD -FIlter StationGroup <stationgroupname>	Creates an empty group.
DELete -FIlter StationGroup <stationgroupname> <address>	Deletes an address from a group.
DELete -FIlter StationGroup <stationgroupname> ALL	Deletes all addresses from a group.
DELete -FIlter StationGroup <stationgroupname>	Deletes a group.
SHow -FIlter StationGroup	Shows all station groups with names and number of members.
SHow -FIlter StationGroup <stationgroupname>	Shows all addresses of a specific group name.
CHange -FIlter StationGroup <old stationgroupname> <newstationgroupname>	Changes the name of a group into a new name.

Values <stationgroupname> Specifies a user-defined string that identifies the station group. It consists of 15 printable ASCII characters. Every station group name must begin with an alphabet character.

<address> Specifies the MAC address mapped to the station group.

Reserved words and names of built-in masks are not legal names. Reserved words are all, among, and, at, betw, between, from, to, forward, discard, count, prioritize, and sequence. All names are case-insensitive.

Messages Table 23-6 lists the StationGroup messages.

Table 23-6 StationGroup Messages

Message	Comment
`Group <name > does not exist`	Attempt to show or delete a non-existing group.
`<name> is a defined <type>`	Attempt to reuse the name of an existing mask or policy as a group name.
`<name> is a built-in mask`	Attempt to reuse the name of an existing built-in mask as a group name.
`No StationGroups defined`	Response to a SHow command when there are no station groups defined.
`Group <name> has no members`	Attempt to show the contents of an empty group.
`Invalid address`	Invalid MAC address.

(continued)

Table 23-6 StationGroup Messages (continued)

Message	Comment
`Can’t add - max number of addresses exists`	Maximum address count reached.
`Address <addr> is already a member of group <name>`	Attempt to add an address, but that address is already in that group.
`There are no addresses in any of StationGroups`	Attempt to delete an address, but there are no addresses in any group.
`Group <name > is empty`	Attempt to delete an address from an empty group
`Address <addr> is not a member of group <name>`	Attempt to delete an address from a group, but the address is not in that group.
`Group <name> is NOT created`	Unable to create a group.
`Group <name> does not exist`	Attempt to change a non-existing group.
`Group <name> already exists`	Attempt to change a group into an existing group name.
`Can’t delete - group <name> is not empty`	Attempt to delete a non-empty group.
`Can’t delete - group <name> is used in a mask`	Attempt to delete a group that is used in a mask.
`Can’t delete - group <name> is not empty and it is used in a mask`	Attempt to delete a non-empty group that is also used in a mask.

24 FireWall Service Parameters

This chapter describes parameters in the FireWall Service. Table 24-1 lists the FireWall Service parameters and commands.

Table 24-1 FireWall Service Parameters and Commands

Parameter	Command
ARCHIE	ADD, DELete
CONFiguration	SHow
CONTrol	SETDefault, SHow
DefAction	SETDefault, SHow
DNSSvrSvr	ADD, DELete
FILters	ADD, DELete, SHow
FTPIn	ADD, DELete
FTPOut	ADD, DELete
FTPSession	SHow
GopherIn	ADD, DELete
GopherOut	ADD, DELete
HTTPIn	ADD, DELete
HTTPOut	ADD, DELete
ICMP	ADD, DELete
InFilter	SETDefault, SHow
Log	SETDefault, SHow
NFS	ADD, DELete
NNTPIn	ADD, DELete
NNTPOut	ADD, DELete
NTP	ADD, DELete
OSPF	ADD, DELete
OutFilter	SETDefault, SHow
POPIn	ADD, DELete
POPOut	ADD, DELete
RIP	ADD, DELete
SMTPIn	ADD, DELete
SMTPOut	ADD, DELete
SNMP	ADD, DELete
SysLog	ADD, DELete
TELnetIn	ADD, DELete
TELnetOut	ADD, DELete
TFTP	ADD, DELete
WAISIn	ADD, DELete
WAISOut	ADD, DELete

ARCHIE

Syntax

```
ADD !<port> -FireWall ARCHIE Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
DELete !<port> -FireWall ARCHIE Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
```

Default No default

Description The ARCHIE parameter allows you to search through indexes of anonymous FTP servers for file names that match certain expressions. Archie is a UDP-based Internet service.

Values

Permit	Permits Archie packets.
Deny	Denies Archie packets.
Log [0–7]	Each packet, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.
From <IPaddr/mask>	Applies only to packets with source IP addresses falling within the address range.
To <IPaddr/mask>	Applies only to packets with destination IP addresses falling within the address range.
NextHop <IP addr>	Forwards the qualified packets to another IP address instead of the destination IP address in the packet. The destination address in the packet is not modified, only the forwarding direction is affected. This value is useful only with received packets on the interface, before routing decisions have been made.

Equivalent Generic Filter Rules (assuming Permit)

Incoming filters	Permit [From<source>] [To<dest>] [NextHop<IP addr>] UDP Dst = 1525
	Permit [From<dest>] [To<source>] [NextHop<IP addr>] UDP Src = 1525
Outgoing filters	Permit [From<source>] [To<dest>] UDP Dst = 1525
	Permit [From<dest>] [To<source>] UDP Src = 1525

CONFiguration

Syntax

```
SHow [!<port>] -FireWall CONFiguration
```

Default No default

Description The CONFiguration parameter displays all the current settings on a particular interface and also displays many vital statistics.

The display is divided into four groups and is in the order of execution priority. The first priority includes all of the options in the CONTrol parameter, such as SrcSpoofing and SrcRouting. The second priority includes all of the service-dependent parameters, for example, FTPOut, TELnetOut, and SNMP. The third priority displays the generic filters including InFilter and OutFilter. The last priority displays the DefAction parameter settings.

Other useful statistics are also displayed, such as the number of packets permitted, denied, and or logged. The display also shows the activation time and the idle time since that last parameter execution in some cases.

CONTrol

Syntax

```
SETDefault -FireWall CONTrol = ([Filter | NoFilter],
  [IgnoreSrcSpoofing | DenySrcSpoofing], [IgnoreTinyFragment |
  DenyTinyFragment], [IgnoreSrcRoute | DenySrcRoute],
  [IgnoreRecordRoute | DenyRecordRoute], [IgnoreTimeStamp |
  DenyTimeStamp], [IgnoreIPTunnel | DenyIPTunnel], [GenerateICMP |
  SuppressICMP])
SHow -FireWall CONTrol
```

Default NoFilter, IgnoreSrcSpoofing, DenyTinyFragment, DenySrcRoute, DenyRecordRoute, DenyTimeStamp, DenyIPTunnel, SuppressICMP

Description The CONTrol parameter determines the firewall function characteristics.

Values

Filter | NoFilter	Enables or disables filtering operations on a particular interface. If Filter is selected, all filtering functions are enabled. If NoFilter is selected, filtering functions on the interface are disabled.
IgnoreSrcSpoofing | DenySrcSpoofing	Specifies whether packets are subject to source-spoofing checks. This is a CPU-intensive option and generally results in performance degradation. You should disable this option except on interfaces where external, untrusted traffic is received. The source address of incoming packets is checked against the routing table. If the routing information shows that the source address is unreachable, or reachable on different interfaces, then it is a SrcSpoofing attack.
IgnoreTinyFragment | DenyTinyFragment	Specifies whether tiny TCP fragment checks (RFC 1858) are performed.
IgnoreSrcRoute | DenySrcRoute	Specifies whether or not the received packet should be dropped if the source-route option is present in the IP header.
IgnoreRecordRoute | DenyRecordRoute	Specifies whether or not the received packet should be dropped if the record-route option is present in the IP header.
IgnoreTimeStamp | DenyTimeStamp	Specifies whether or not the received packet should be dropped if the time-stamp option is present in the IP header.

IgnoreIPTunnel | DenyIPTunnel	Specifies whether or not IP tunnel packets are allowed. IP tunnel packets are IP-over-IP encapsulation.
GenerateICMP | SuppressICMP	For denied packets, this option specifies whether or not the router should generate ICMP destination administratively unreachable messages (ICMP type 13). To prevent flooding, the bridge/router generates no more than 10 ICMP messages per second.

DefAction

Syntax

```
SETDefault !<port> -FireWall DefAction = ([Permit | Deny], [Log
  | NoLog])
SHow -FireWall DefAction
```

Default Deny, NoLog

Description The DefAction parameter controls the basic set up of your firewall. This parameter applies to both incoming and outgoing traffic.

DefAction is the last priority in firewall screening, however, it is the most important in defining the security policy of your organization. Packets that do not match any other filter are handled by DefAction. DefAction permits or denies all non-specified packets. The Deny value provides the maximum protection against unknown services. The Permit value allows unknown services to pass through the firewall. This is more risky than deny but it offers more convenience to users.

Values

Permit	Everything that is not specifically denied is permitted.
Deny	Blocks everything not specifically permitted.
Log	Generates log messages on all packets, whether permitted or denied.
NoLog	Generates no log messages.

DNSSvrSvr

Syntax

```
ADD !<port> -FireWall DNSSvrSvr Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
DELete !<port> -FireWall DNSSvrSvr Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
```

Default No default

Description The DNSSvrSvr parameter permits or denies DNS server-to-server connections. When this parameter is enabled, both incoming and outgoing server-to-server queries are enabled. Unlike other parameters in the FireWall Service, there is no directional sense (either in or out) associated with this parameter.

DNS server-to-server connection involves both UDP and TCP packets; both cases are handled by this parameter.

Values

Permit	Permits server-to-server connections.
Deny	Denies server-to-server connections.

Log [0–7] Specifies a connection request. Each request, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.

From <IPaddr/mask> Applies only to packets with source IP addresses falling within the address range.

To <IPaddr/mask> Applies only to packets with destination IP addresses falling within the address range.

NextHop <IP addr> Forwards the qualified packets to another IP address instead of the destination IP address in the packet. The destination address in the packet is not modified, only the forwarding direction is affected. This value is useful only with received packets on the interface, before routing decisions have been made.

Equivalent Generic Filter Rules (assuming Permit)

Incoming filters

Permit [From<source>] [To<dest>] [NextHop<IP addr>] TCP Src >1023 Dst = 53

Permit [From<dest>] [To<source>] [NextHop<IP addr>] TCP Src = 53 Dest >1023 Estab

Permit [From<source>] [To<dest>] [NextHop<IP addr>] UDP Src = 53 Dest = 53

Permit [From<dest>] [To<source>] [NextHop<IP addr>] UDP Src = 53 Dest = 53

Outgoing filters

Permit [From<dest>] [To<source>] TCP Src = 53 Dest >1023 Estab

Permit [From<source>] [To<dest>] TCP Src >1023 Dest = 53

Permit [From<source>] [To<dest>] UDP Src =53 Dest = 53

Permit [From<dest>] [To<source>] UDP Src = 53 Dest = 53

FILters

Syntax

```
ADD -FireWall FILters <filter name> (<rules>)
DELete -FireWall FILters <filter name>
SHow -FireWall FILters <filter name>
```

Default No default

Description The FILters parameter allows you to define specialized filters. Each filter may have several rules. The SHow -FireWall FILters command displays the names, sizes, and creation dates of all the filters currently stored on the disk. Filters must be individually deleted from the system. When you delete a filter, it is removed from local storage and also from memory. When you use the DELete command, any interface that is currently using that filter immediately ceases applying its rules.

The FILters parameter allows you to define and modify filters. The InFilter and OutFilter parameters control the execution of the filters that are assigned to an interface to perform input or output packet filtering.

Values

<filter name> Assigns a name to a filter. The syntax of the filter name is the same as a DOS filename, that is, it can be up to eight characters in length followed by up to a three-character extension. The name is case-insensitive; upper- and lowercase letters can be used. If a new filter is created with the same name as an existing filter, the new filter replaces the old.

A filter must have a least one rule defined within it.

<rules> Specifies filter rules on a per-interface basis and can be applied to incoming traffic, outgoing traffic, or both. The order in which rules are executed is user-defined, and there is no limit to the number of rules within a filter if there is sufficient memory. The syntax for specifying a rule is as follows:

```
Permit | Deny [Log[0–7]] [From <IPaddr/mask>]
 [To <IPaddr/mask>] [NextHop <IPaddr>]
 [<protocol>] [<options>]
```

Permit Allows the packet to pass though.

Deny Discards the packet.

Log Specifies a connection request. Each request, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.

From <IPaddr/mask>, To <IPaddr/mask> Compares the source and destination IP address in the packet. The <mask> field is a number between 0 and 32 and specifies the number of bits in the <IPaddr> field that is significant for comparison. For example: 129.213.0.0/16 is all addresses in the range from 129.213.0.0 to 129.213.255.255, 129.213.1.2/32 is the host itself, 0.0.0.0/0 is all the IP addresses, and 224.0.0.0/4 is all the class D multicast addresses from 224.0.0.0 to 239.255.255.255.

Next Hop <IPaddr> Instructs the routing software to forward the qualified packets to another IP address instead of the destination IP address in the packet. The destination IP address in the packet is not modified, only the forwarding direction is affected. This value is only useful on received packets on the interface, that is, when assigned to the InFilter parameter.

<protocol> Specifies protocol values. Possible protocol values are TCP, UDP, ICMP, or any numerical value between 1 and 255.

<options> This value is protocol-dependent.

If TCP is specified, the syntax for <options> is:

```
[Src <compare> <port>] [Dst <compare> <port>]
 [Estab]
```

Src indicates a comparison should be made with the source TCP port number, Dst indicates a comparison should be made with the destination TCP port number, and Estab indicates that the packet should be tested to see if it is for an established TCP connection. If you specify this option, then packets trying to create new TCP connections will not match. This is done by checking the ACK bit inside the TCP header. The ACK bit is set in all TCP packets except in the very first TCP packet trying to create a new TCP connection. The <compare> option can be one of several comparison operators: > (greater than), < (less than), or = (equal). The <port> option is any numerical decimal number between 0 and 65535.

If UDP is specified, the syntax for <options> is:

```
[Src <compare> <port>] [Dst <compare> <port>]
```

Src indicates a comparison should be made with the source UDP port number, and Dst indicates a comparison should be made with the destination UDP port number. The <compare> option can be one of several comparison operators: > (greater than), < (less than), or = (equal). The <port> option is any numerical decimal number between 0 and 65535.

If ICMP is specified, the syntax for <options> is <ICMP type> where <ICMP type> is a numerical decimal number (0–255) specifying ICMP message types. For example, Echo Request - 8, Echo response - 0, Destination unreachable - 3, Source quench - 4, Redirect - 5, Time exceeded - 11, and Parameter problem - 12.

FTPIn

Syntax

```
ADD !<port> -FireWall FTPIn Permit | Deny [Log[0–7]] [From
 <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
DELete !<port> -FireWall FTPIn Permit | Deny [Log[0–7]] [From
 <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
```

Default No default

Description The FTPIn parameter determines whether incoming FTP connections are permitted or denied. This parameter applies to both traditional (PORT) and passive (PASV) FTP sessions. The FTPIn parameter monitors the TCP port number and direction by decoding the command channel, allowing a time-limited window for the right TCP connection; it behaves like an application-level gateway (refer to “FTPSession”).

Values

Permit	Permits incoming FTP connections.
Deny	Denies incoming FTP connections.

Log [0–7] Specifies a connection request. Each request, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.

From <IPaddr/mask> Applies only to packets with source IP addresses falling within the address range.

To <IPaddr/mask> Applies only to packets with destination IP addresses falling within the address range.

NextHop <IP addr> Forwards the qualified packets to another IP address instead of the destination IP address in the packet. The destination address in the packet is not modified, only the forwarding direction is affected. This value is useful only with received packets on the interface, before routing decisions have been made.

Equivalent Generic Filter Rules (assuming Permit)

Incoming filters

Permit [From<source>] [To<dest>] [NextHop<IP addr>] TCP Src >1023 Dst = 21

Permit [From<source>] [To<dest>] [NextHop<IP addr>] TCP Src = <variable 1> Dst = 20 Estab

Permit [From<source>] [To<dest>] [NextHop<IP addr>] TCP Src = <variable 2> Dst = <variable 2>

Outgoing filters

Permit [From<dest>] [To<source>] TCP Src = 21Dst >1023 Estab

Permit [From<dest>] [To<source>] TCP Src = 20 Dst = <variable 1>

Permit [From<dest>] [To<source>] TCP Src = <variable 2> Dst = <variable 2>

<variable 1> depends on the PORT command; <variable 2> depends on the PASV command.

FTPOut

Syntax

```
ADD !<port> -FireWall FTPOut Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
DELete !<port> -FireWall FTPOut Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
```

Default No default

Description The FTPOut parameter determines whether outgoing FTP connections are permitted or denied. This parameter applies to both traditional (PORT) and passive (PASV) FTP sessions. The FTPOut parameter monitors the TCP port number and direction by decoding the command channel, allowing a time-limited window for the right TCP connection; it behaves like an application-level gateway (refer to “FTPSession”).

Values

Permit: Permits outgoing FTP connections.

Deny: Denies outgoing FTP connections.

Log [0–7]: Specifies a connection request. Each request, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.

From <IPaddr/mask>: Applies only to packets with source IP addresses falling within the address range.

To <IPaddr/mask>: Applies only to packets with destination IP addresses falling within the address range.

NextHop <IP addr>: Forwards the qualified packets to another IP address instead of the destination IP address in the packet. The destination address in the packet is not modified, only the forwarding direction is affected. This value is useful only with received packets on the interface, before routing decisions have been made.

Equivalent Generic Filter Rules (assuming Permit)

Incoming filters

Permit [From<dest>] [To<source>] TCP Src = 21Dst >1023 Estab

Permit [From<dest>] [To<source>] TCP Src = 20 Dst = <variable 1>

Permit [From<dest>] [To<source>] [NextHop<IP addr>] TCP Src = <variable 2> Dst = <variable 2>

Outgoing filters

Permit [From<source>] [To<dest>] TCP Src >1023 Dst =21

Permit [From<source>] [To<dest>] TCP Src = <variable 1> Dst = 20 Estab

Permit [From<source>] [To<dest>] TCP Src = <variable 2> Dst = <variable 2>

<variable 1> depends on the PORT command; <variable 2> depends on the PASV command.

FTPSession

Syntax `SHow -FireWall FTPSession`

Default No default

Description The FTPSession parameter displays the currently active FTP sessions. Each FTP session can have two TCP connections active at the same time: the command channel, which passes commands and responses between client and server, and the data channel, which transfers the data. This parameter displays detailed information for both the command and data channels.

GopherIn

Syntax

```
ADD !<port> -FireWall GopherIn Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
DELete !<port> -FireWall GopherIn Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
```

Default No default

Description The GopherIn parameter permits or denies incoming Gopher connections. Gopher is a menu-oriented, text-based tool that helps users find a variety of information on the Internet.

Values

Permit	Permits incoming Gopher connections.
Deny	Denies incoming Gopher connections.
Log [0–7]	Specifies a connection request. Each request, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.
From <IPaddr/mask>	Applies only to packets with source IP addresses falling within the address range.
To <IPaddr/mask>	Applies only to packets with destination IP addresses falling within the address range.
NextHop <IP addr>	Forwards the qualified packets to another IP address instead of the destination IP address in the packet. The destination address in the packet is not modified, only the forwarding direction is affected. This value is useful only with received packets on the interface, before routing decisions have been made.

Equivalent Generic Filter Rules (assuming Permit)

Incoming filter	Permit [From<source>] [To<dest>] [NextHop<IP addr>] TCP Src >1023 Dst = 70
Outgoing filter	Permit [From<dest>] [To<source>] TCP Src = 70 Dst >1023 Estab

GopherOut

Syntax

```
ADD !<port> -FireWall GopherOut Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
DELete !<port> -FireWall GopherOut Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
```

Default No default

Description The GopherOut parameter permits or denies outgoing Gopher connections. Gopher is a menu-oriented, text-based tool that helps users find a variety of information on the Internet.

Values

Permit	Permits outgoing Gopher connections.
Deny	Denies outgoing Gopher connections.
Log [0–7]	Specifies a connection request. Each request, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.
From <IPaddr/mask>	Applies only to packets with source IP addresses falling within the address range.
To <IPaddr/mask>	Applies only to packets with destination IP addresses falling within the address range.
NextHop <IP addr>	Forwards the qualified packets to another IP address instead of the destination IP address in the packet. The destination address in the packet is not modified, only the forwarding direction is affected. This value is useful only with received packets on the interface, before routing decisions have been made.

Equivalent Generic Filter Rules (assuming Permit)

Incoming filter	Permit [From<dest>] [To<source>] [NextHop<IP addr>] TCP Src = 70 Dst >1023 Estab
Outgoing filter	Permit [From<source>] [To<dest>] TCP Src >1023 Dst = 70

HTTPIn

Syntax

```
ADD !<port> -FireWall HTTPIn Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
DELete !<port> -FireWall HTTPIn Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
```

Default No default

Description The HTTPIn parameter permits or denies incoming HyperText Transfer Protocol (HTTP) connections. HTTP is the primary application protocol for the World Wide Web (WWW). This protocol provides users access to WWW files.

Values

Permit	Permits incoming HTTP connections.
Deny	Denies incoming HTTP connections.
Log [0–7]	Specifies a connection request. Each request, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.
From <IPaddr/mask>	Applies only to packets with source IP addresses falling within the address range.

To <IPaddr/mask> Applies only to packets with destination IP addresses falling within the address range.

NextHop <IP addr> Forwards the qualified packets to another IP address instead of the destination IP address in the packet. The destination address in the packet is not modified, only the forwarding direction is affected. This value is useful only with received packets on the interface, before routing decisions have been made.

Equivalent Generic Filter Rules (assuming Permit)

Incoming filter Permit [From<source>] [To<dest>] [NextHop<IP addr>] TCP Src >1023 Dst = 80

Outgoing filter Permit [From<dest>] [To<source>] TCP Src = 80 Dst >1023 Estab

HTTPOut

Syntax

```
ADD !<port> -FireWall HTTPOut Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>]
DELete !<port> -FireWall HTTPOut Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>]
```

Default No default

Description The HTTPOut parameter permits or denies outgoing HyperText Transfer Protocol (HTTP) connections. HTTP is the primary application protocol for the World Wide Web (WWW). This protocol provides users access to WWW files.

Values

Permit Permits outgoing HTTP connections.

Deny Denies outgoing HTTP connections.

Log [0–7] Specifies a connection request. Each request, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.

From <IPaddr/mask> Applies only to packets with source IP addresses falling within the address range.

To <IPaddr/mask> Applies only to packets with destination IP addresses falling within the address range.

NextHop <IP addr> Forwards the qualified packets to another IP address instead of the destination IP address in the packet. The destination address in the packet is not modified, only the forwarding direction is affected. This value is useful only with received packets on the interface, before routing decisions have been made.

Equivalent Generic Filter Rules (assuming Permit)

Incoming filter Permit [From<dest>] [To<source>] [NextHop<IP addr>] TCP Src = 80 Dest >1023 Estab

Outgoing filter Permit [From<source>] [To<dest>] TCP Src >1023 Dst = 80

ICMP

Syntax

```
ADD !<port> -FireWall ICMP Permit | Deny [Log[0–7]] [From
 <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
DELete !<port> -FireWall ICMP Permit | Deny [Log[0–7]] [From
 <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
```

Default No default

Description The ICMP parameter permits or denies Internet Control Message Protocol (ICMP) packets through the firewall. There are many ICMP message types including echo request, reply, and destination unreachable. Some ICMP messages, such as redirect, may be considered risky.

Values

Permit	Permits ICMP packets.
Deny	Denies ICMP packets.
Log [0–7]	Each packet, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.
From <IPaddr/mask>	Applies only to packets with source IP addresses falling within the address range.
To <IPaddr/mask>	Applies only to packets with destination IP addresses falling within the address range.
NextHop <IP addr>	Forwards the qualified packets to another IP address instead of the destination IP address in the packet. The destination address in the packet is not modified, only the forwarding direction is affected. This value is useful only with received packets on the interface, before routing decisions have been made.

Equivalent Generic Filter Rules (assuming Permit)

Incoming filter	Permit [From<source>] [To<dest>] [NextHop<IP addr>] ICMP
Outgoing filter	Permit [From<source>] [To<dest>] ICMP

InFilter

Syntax

```
SETDefault !<port> -FireWall InFilter = <filter name>
SHow -FireWall InFilter
```

Default No default

Description The InFilter parameter allows you to associate a user-defined filter (identified by its name) with the input filter on an interface. If <filter name> is empty, no filters are associated with the interface. If <filter name> is not found on local storage, no filtering actions are taken.

Filters are defined by the Filters parameter (refer to page 24-5).

Values <filter name> Assigns a name to a filter. The syntax of the filter name is the same as a DOS filename, that is, it can be up to eight characters in length followed by up to a three-character extension. The name is case-insensitive; upper- and lowercase letters can be used. If a new filter is created with the same name as an existing filter, the new filter replaces the old.

Log

Syntax

```
SETDefault -FireWall Log = ([Syslog | NoSyslog], [Console |
 NoConsole], [SUmmary | DEtail], [SrcSpoofing | NoSrcSpoofing],
 [TinyFragment | NoTinyFragment], [SrcRoute | NoSrcRoute],
 [RecordRoute | NoRecordRoute], [TimeStamp | NoTimeStamp],
 [IPTunnel | NoIPTunnel])
SHow -FireWall Log
```

Default NoSyslog, NoConsole, SUmmary, SrcSpoofing, TinyFragment, SrcRoute, RecordRoute, TimeStamp, IPTunnel

Description The Log parameter determines which messages are recorded and whether these messages are sent to syslog, to the local console, or both. To avoid log message flooding, only TCP connection request packets are logged. Because of the lack of connection information, non-TCP packets are logged individually. The Log parameter does not generate more than 10 log messages per second. Excessive messages are suppressed; the next message contains a suppress count.

Values

Syslog | NoSyslog	Determines if the log messages are delivered to a log server with syslog. If Syslog is selected, you must also configure the log server IP address using the LogServerAddr parameter in the AuditLog Service.
Console | NoConsole	Determines if log messages are delivered to the local console.
SUmmary | DEtail	If SUmmary is selected, the logging messages contain just the summary of the IP header. If DEtail is selected, the first 64 bytes of each packet is also logged.
SrcSpoofing | NoSrcSpoofing	Determines whether to log denied source-spoofing packets.
TinyFragment | NoTinyFragment	Determines whether to log denied tiny TCP fragments.
SrcRoute | NoSrcRoute	Determines whether to log denied source-route packets.
RecordRoute | NoRecordRoute	Determines whether to log denied record-route packets.
TimeStamp | NoTimeStamp	Determines whether to log denied packets with time-stamp options.
IPTunnel | NoIPTunnel	Determines whether to log denied IP-over-IP tunnel packets.

NFS

Syntax

```
ADD !<port> -FireWall NFS Permit | Deny [Log[0–7]] [From
 <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
DELete !<port> -FireWall NFS Permit | Deny [Log[0–7]] [From
 <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
```

Default No default

Description The NFS parameter permits or denies NFS traffic. NFS traffic traditionally uses UDP port number 2049 as the server port. When you enable NFS traffic, UDP access to port number 2049 and UDP port number 111 are opened up. Port 111 is the port mapper service, which tells NFS clients the port number of the NFS server.

Values

Permit	Permits NFS traffic.
Deny	Denies NFS traffic.
Log [0–7]	Each packet, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.
From <IPaddr/mask>	Applies only to packets with source IP addresses falling within the address range.
To <IPaddr/mask>	Applies only to packets with destination IP addresses falling within the address range.
NextHop <IP addr>	Forwards the qualified packets to another IP address instead of the destination IP address in the packet. The destination address in the packet is not modified, only the forwarding direction is affected. This value is useful only with received packets on the interface, before routing decisions have been made.

Equivalent Generic Filter Rules (assuming Permit)

Incoming filters	Permit [From<source>] [To<dest>] [NextHop<IP addr>] UDP Dst = 111
	Permit [From<dest>] [To<source>] [NextHop<IP addr>] UDP Src = 111
	Permit [From<source>] [To<dest>] [NextHop<IP addr>] UDP Dest = 2049
	Permit [From<dest>] [To<source>] [NextHop<IP addr>] UDP Src = 2049
Outgoing filters	Permit [From<dest>] [To<source>] UDP Src = 111
	Permit [From<source>] [To<dest>] UDP Dest = 111
	Permit [From<source>] [To<dest>] UDP Dest = 2049
	Permit [From<dest>] [To<source>] UDP Src = 2049

NNTPIn

Syntax

```
ADD !<port> -FireWall NNTPIn Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
DELete !<port> -FireWall NNTPIn Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
```

Default No default

Description The NNTPIn parameter permits or denies incoming Network News Transfer Protocol (NNTP) connections. NNTP is used to transfer Usenet news across the Internet.

Values

Permit	Permits incoming NNTP connections.
Deny	Denies incoming NTTP connections.
Log [0–7]	Specifies a connection request. Each request, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.
From <IPaddr/mask>	Applies only to packets with source IP addresses falling within the address range.
To <IPaddr/mask>	Applies only to packets with destination IP addresses falling within the address range.
NextHop <IP addr>	Forwards the qualified packets to another IP address instead of the destination IP address in the packet. The destination address in the packet is not modified, only the forwarding direction is affected. This value is useful only with received packets on the interface, before routing decisions have been made.

Equivalent Generic Filter Rules (assuming Permit)

Incoming filter	Permit [From<source>] [To<dest>] [NextHop<IP addr>] TCP Src >1023 Dst = 119
Outgoing filter	Permit [From<dest>] [To<source>] TCP Src = 119 Dst >1023 Estab

NNTPOut

Syntax

```
ADD !<port> -FireWall NNTPOut Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
DELete !<port> -FireWall NNTPOut Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
```

Default No default

Description The NNTPOut parameter permits or denies outgoing Network News Transfer Protocol (NNTP) connections. NNTP is used to transfer Usenet news across the Internet.

Values

Permit Permits outgoing NNTP connections.

Deny Denies outgoing NNTP connections.

Log [0–7] Specifies a connection request. Each request, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.

From <IPaddr/mask> Applies only to packets with source IP addresses falling within the address range.

To <IPaddr/mask> Applies only to packets with destination IP addresses falling within the address range.

NextHop <IP addr> Forwards the qualified packets to another IP address instead of the destination IP address in the packet. The destination address in the packet is not modified, only the forwarding direction is affected. This value is useful only with received packets on the interface, before routing decisions have been made.

Equivalent Generic Filter Rules (assuming Permit)

Incoming filter Permit [From<dest>] [To<source>] [NextHop<IP addr>] TCP Src = 119 Dst >1023 Estab

Outgoing filter Permit [From<source>] [To<dest>] TCP Src >1023 Dst = 119

NTP

Syntax

```
ADD !<port> -FireWall NTP Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
DELete !<port> -FireWall NTP Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
```

Default No default

Description The NTP parameter permits or denies Network Time Protocol (NTP) packets through the firewall. NTP is a UDP-based service. NTP servers listen on UDP port 123 while NTP clients use a UDP port number greater than 1023. It is possible for an NTP server to query another NTP server. In that case, both the source and destination use UDP port 123.

Values

Permit Permits NTP packets.

Deny Denies NTP packets.

Log [0–7] Each packet, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.

From <IPaddr/mask> Applies only to packets with source IP addresses falling within the address range.

To <IPaddr/mask> Applies only to packets with destination IP addresses falling within the address range.

NextHop <IP addr> Forwards the qualified packets to another IP address instead of the destination IP address in the packet. The destination address in the packet is not modified, only the forwarding direction is affected. This value is useful only with received packets on the interface, before routing decisions have been made.

Equivalent Generic Filter Rules (assuming Permit)

Incoming filters

Permit [From<source>] [To<dest>] [NextHop<IP addr>] UDP Src = 123 Dst = 123

Permit [From<dest>] [To<source>] [NextHop<IP addr>] UDP Src = 123 Dest = 123

Permit [From<source>] [To<dest>] [NextHop<IP addr>] UDP Src >1023 Dest = 123

Permit [From<dest>] [To<source>] [NextHop<IP addr>] UDP Src = 123 Dest >1023

Outgoing filters

Permit [From<source>] [To<dest>] UDP Src = 123 Dst = 123

Permit [From<dest>] [To<source>] UDP Src = 123 Dest = 123

Permit [From<source>] [To<dest>] UDP Src >1023 Dest = 123

Permit [From<dest>] [To<source>] UDP Src = 123 Dest >1023

OSPF

Syntax

```
ADD !<port> -FireWall OSPF Permit | Deny [Log[0–7]] [From
 <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
DELete !<port> -FireWall OSPF Permit | Deny [Log[0–7]] [From
 <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
```

Default No default

Description The OSPF parameter permits or denies Open Shortest Path First (OSPF) packets through the firewall. OSPF packets are IP packet type 89. Some OSPF packets have an IP multicast address as their destination address (for example, 224.0.0.5 or 224.0.0.6). OSPF packets can also be unicast between neighbors.

Values

Permit Permits OSPF packets.

Deny Denies OSPF packets.

Log [0–7] Each packet, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.

From <IPaddr/mask>	Applies only to packets with source IP addresses falling within the address range.
To <IPaddr/mask>	Applies only to packets with destination IP addresses falling within the address range.
NextHop <IP addr>	Forwards the qualified packets to another IP address instead of the destination IP address in the packet. The destination address in the packet is not modified, only the forwarding direction is affected. This value is useful only with received packets on the interface, before routing decisions have been made.

Equivalent Generic Filter Rules (assuming Permit)

Incoming filter	Permit [From<source>] [To<dest>] 89
Outgoing filter	Permit [From<source>] [To<dest>] 89

OutFilter

Syntax

```
SETDefault !<port> -FireWall OutFilter <filter name>
SHow -FireWall OutFilter
```

Default No default

Description The OutFilter parameter associates a user-defined filter (identified by its name) with the output filter on an interface. If <filter name> is empty, no filters are associated with the interface. If <filter name> is not found on local storage, no filtering actions are taken.

Filters are defined by the Filters parameter (refer to page 24-5).

Values

<filter name>	Specifies a filter name. The syntax of the filter name is the same as a DOS file name, that is, it can be up to eight characters in length followed by up to a three-character extension. The name is case-insensitive; upper- and lowercase letters can be used. If a new filter is created with the same name as an existing filter, the new filter replaces the old.

POPIn

Syntax

```
ADD !<port> -FireWall POPIn Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
DELete !<port> -FireWall POPIn Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
```

Default No default

Description The POPIn parameter permits or denies incoming Post Office Protocol (POP) packets. POP is a client-server protocol for accessing user electronic mailboxes. POP is a TCP-based service.

Values

Permit	Permits incoming POP connections.
Deny	Denies incoming POP connections.

Log [0–7] Specifies a connection request. Each request, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.

From <IPaddr/mask> Applies only to packets with source IP addresses falling within the address range.

To <IPaddr/mask> Applies only to packets with destination IP addresses falling within the address range.

NextHop <IP addr> Forwards the qualified packets to another IP address instead of the destination IP address in the packet. The destination address in the packet is not modified, only the forwarding direction is affected. This value is useful only with received packets on the interface, before routing decisions have been made.

Equivalent Generic Filter Rules (assuming Permit)

Incoming filters Permit [From<source>] [To<dest>] [NextHop<IP addr>] TCP Src >1023 Dst = 109

Permit [From<source>] [To<dest>] [NextHop<IP addr>] TCP Src >1023 Dest = 110

Outgoing filters Permit [From<dest>] [To<source>] TCP Src = 109 Dst >1023 Estab

Permit [From<dest>] [To<source>] TCP Src = 110 Dest >1023 Estab

POPOut

Syntax

```
ADD !<port> -FireWall POPOut Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
DELete !<port> -FireWall POPOut Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
```

Default No default

Description The POPOut parameter permits or denies outgoing Post Office Protocol (POP) connections. POP is a client-server protocol for accessing user electronic mailboxes. POP is a TCP-based service.

Value

Permit Permits outgoing POP connections.

Deny Denies outgoing POP connections.

Log [0–7] Specifies a connection request. Each request, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.

From <IPaddr/mask> Applies only to packets with source IP addresses falling within the address range.

To <IPaddr/mask> Applies only to packets with destination IP addresses falling within the address range.

NextHop <IP addr> Forwards the qualified packets to another IP address instead of the destination IP address in the packet. The destination address in the packet is not modified, only the forwarding direction is affected. This value is useful only with received packets on the interface, before routing decisions have been made.

Equivalent Generic Filter Rules (assuming Permit)

Incoming filters

Permit [From<dest>] [To<source>] [NextHop<IP addr>] TCP Src = 109 Dst >1023 Estab

Permit [From<dest>] [To<source>] [NextHop<IP addr>] TCP Src = 110 Dest >1023 Estab

Outgoing filters

Permit [From<source>] [To<dest>] TCP Src >1023 Dst = 109 Estab

Permit [From<source>] [To<dest>] TCP Src >1023 Dest = 110

RIP

Syntax

```
ADD !<port> -FireWall RIP Permit | Deny [Log[0–7]] [From <IPaddr/mask>]
  [To <IPaddr/mask>] [NextHop <IPaddr>]
DELete !<port> -FireWall RIP Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
```

Default No default

Description The RIP parameter permits or denies Routing Information Protocol (RIP) packets through the firewall. RIP is a UDP-based service. RIP servers listen on port 520 and clients usually use a port greater than 1023 as the source. If a server sends an update to another server, they both may use port 520 as the source and destination port.

Values

Permit Permits RIP packets.

Deny Denies RIP packets.

Log [0–7] Each packet, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.

From <IPaddr/mask> Applies only to packets with source IP addresses falling within the address range.

To <IPaddr/mask> Applies only to packets with destination IP addresses falling within the address range.

	NextHop <IP addr>	Forwards the qualified packets to another IP address instead of the destination IP address in the packet. The destination address in the packet is not modified, only the forwarding direction is affected. This value is useful only with received packets on the interface, before routing decisions have been made.
Equivalent Generic Filter Rules (assuming Permit)	Incoming filters	Permit [From<source>] [NextHop<IP addr>] UDP Src = 520 Dst = 520
		Permit [From<dest>] [To<source>] [NextHop<IP addr>] UDP Src = 520 Dst >1023
		Permit [From<source>] [To<dest>] [NextHop<IP addr>] UDP Src >1023 Dst = 520
	Outgoing filters	Permit [From<source>] UDP Src = 520 Dst = 520
		Permit [From<dest>] [To<source>] UDP Src = 520 Dest >1023
		Permit [From<source>] [To<dest>] UDP Src >1023 Dest = 520

SMTPIn

Syntax

```
ADD !<port> -FireWall SMTPIn Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
DELete !<port> -FireWall SMTPIn Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
```

Default No default

Description The SMTPIn parameter permits or denies incoming Simple Mail Transfer Protocol (SMTP) packets. SMTP is the Internet standard protocol for sending and receiving electronic mail.

Values	Permit	Permits incoming SMTP connections.
	Deny	Denies incoming SMTP connections.
	Log [0–7]	Specifies a connection request. Each request, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.
	From <IPaddr/mask>	Applies only to packets with source IP addresses falling within the address range.
	To <IPaddr/mask>	Applies only to packets with destination IP addresses falling within the address range.

NextHop <IP addr>	Forwards the qualified packets to another IP address instead of the destination IP address in the packet. The destination address in the packet is not modified, only the forwarding direction is affected. This value is useful only with received packets on the interface, before routing decisions have been made.

Equivalent Generic Filter Rules (assuming Permit)

Incoming filter	Permit [From<source>] [To<dest>] [NextHop<IP addr>] TCP Src >1023 Dst = 25
Outgoing filter	Permit [From<dest>] [To<source>] TCP Src = 25 Dst > 1023 Estab

SMTPOut

Syntax

```
ADD !<port> -FireWall SMTPOut Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
DELete !<port> -FireWall SMTPOut Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
```

Default No default

Description The SMTPOut parameter permits or denies outgoing Simple Mail Transfer Protocol (SMTP) connections. SMTP is the Internet standard protocol for sending and receiving electronic mail.

Values

Permit	Permits outgoing SMTP connections.
Deny	Denies outgoing SMTP connections.
Log [0–7]	Specifies a connection request. Each request, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.
From <IPaddr/mask>	Applies only to packets with source IP addresses falling within the address range.
To <IPaddr/mask>	Applies only to packets with destination IP addresses falling within the address range.
NextHop <IP addr>	Forwards the qualified packets to another IP address instead of the destination IP address in the packet. The destination address in the packet is not modified, only the forwarding direction is affected. This value is useful only with received packets on the interface, before routing decisions have been made.

Equivalent Generic Filter Rules (assuming Permit)

Incoming filter	Permit [From<dest>] [To<source>] [NextHop<IP addr>] TCP Src = 25 Dst >1023 Estab
Outgoing filter	Permit [From<source>] [To<dest>] TCP Src > 1023 Dst = 25

SNMP

Syntax

```
ADD !<port> -FireWall SNMP Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
DELete !<port> -FireWall SNMP Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
```

Default No default

Description The SNMP parameter permits or denies Simple Network Management Protocol (SNMP) packets through the firewall. SNMP is a UDP-based protocol designed to manage network equipment such as bridges, routers, and hubs.

Values

Permit	Permits SNMP packets.
Deny	Denies SNMP packets.
Log [0–7]	Each packet, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.
From <IPaddr/mask>	Applies only to packets with source IP addresses falling within the address range.
To <IPaddr/mask>	Applies only to packets with destination IP addresses falling within the address range.
NextHop <IP addr>	Forwards the qualified packets to another IP address instead of the destination IP address in the packet. The destination address in the packet is not modified, only the forwarding direction is affected. This value is useful only with received packets on the interface, before routing decisions have been made.

Equivalent Generic Filter Rules (assuming Permit)

Incoming filters	Permit [From<source>] [To<dest>] [NextHop<IP addr>] UDP Dst = 161
	Permit [From<dest>] [To<source>] [NextHop<IP addr>] UDP Src = 161
	Permit [From<source>] [To<dest>] [NextHop<IP addr>] UDP Dest = 162
	Permit [From<dest>] [To<source>] [NextHop<IP addr>] UDP Src = 162
Outgoing filters	Permit [From<source>] [To<dest>] UDP Dst = 161
	Permit [From<dest>] [To<source>] UDP Src = 161
	Permit [From<source>] [To<dest>] UDP Dest = 162
	Permit [From<dest>] [To<source>] UDP Src = 162

Syslog

Syntax

```
ADD !<port> -FireWall Syslog Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
DELete !<port> -FireWall Syslog Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
```

Default No default

Description The Syslog parameter reports status and usage information to a UNIX machine, where the daemon (syslogd) resides. The firewall also uses syslog to report log messages (refer to “Log”). The Syslog parameter is a UDP-based service.

Values

Permit	Permits syslog packets.
Deny	Denies syslog packets.
Log [0–7]	Each packet, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.
From <IPaddr/mask>	Applies only to packets with source IP addresses falling within the address range.
To <IPaddr/mask>	Applies only to packets with destination IP addresses falling within the address range.
NextHop <IP addr>	Forwards the qualified packets to another IP address instead of the destination IP address in the packet. The destination address in the packet is not modified, only the forwarding direction is affected. This value is useful only with received packets on the interface, before routing decisions have been made.

Equivalent Generic Filter Rules (assuming Permit)

Incoming filter	Permit [From<source>] [To<dest>] [NextHop<IP addr>] Dst = 514
Outgoing filter	Permit [From<source>] [To<dest>] Dst = 514

TELnetIn

Syntax

```
ADD !<port> -FireWall TELnetIn Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
DELete !<port> -FireWall TELnetIn Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
```

Default No default

Description The TELnetIn parameter permits or denies incoming Telnet connections.

Values

Permit	Permits incoming Telnet connections.
Deny	Denies incoming Telnet connections.

Log [0–7]	Specifies a connection request. Each request, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.
From <IPaddr/mask>	Applies only to packets with source IP addresses falling within the address range.
To <IPaddr/mask>	Applies only to packets with destination IP addresses falling within the address range.
NextHop <IP addr>	Forwards the qualified packets to another IP address instead of the destination IP address in the packet. The destination address in the packet is not modified, only the forwarding direction is affected. This value is useful only with received packets on the interface, before routing decisions have been made.

Equivalent Generic Filter Rules (assuming Permit)

Incoming filter	Permit [From<source>] [To<dest>] [NextHop<IP addr>] TCP Src >1023 Dst = 23
Outgoing filter	Permit [From<dest>] [To<source>] TCP Src = 23 Dst >1023 Estab

TELnetOut

Syntax

```
ADD !<port> -FireWall HTTPOut Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
DELete !<port> -FireWall HTTPOut Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
```

Default No default

Description The TELnetOut parameter determines whether outgoing TELnet connections are permitted or denied.

Values

Permit	Permits outgoing Telnet connections.
Deny	Denies outgoing Telnet connections.
Log [0–7]	Specifies a connection request. Each request, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.
From <IPaddr/mask>	Applies only to packets with source IP addresses falling within the address range.
To <IPaddr/mask>	Applies only to packets with destination IP addresses falling within the address range.

NextHop <IP addr>	Forwards the qualified packets to another IP address instead of the destination IP address in the packet. The destination address in the packet is not modified, only the forwarding direction is affected. This value is useful only with received packets on the interface, before routing decisions have been made.

Equivalent Generic Filter Rules (assuming Permit)

Incoming filter	Permit [From<dest>] [To<source>] [NextHop<IP addr>] TCP Src = 23 Dst >1023 Estab
Outgoing filter	Permit [From<source>] [To<dest>] TCP Src > 1023 Dst = 23

TFTP

Syntax

```
ADD !<port> -FireWall TFTP Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
DELete !<port> -FireWall TFTP Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
```

Default No default

Description The TFTP parameter permits or denies UDP-based Trivial File Transfer Protocol (TFTP) packets through the firewall. TFTP is a simplified file transfer protocol.

Values

Permit	Permits TFTP packets.
Deny	Denies TFTP packets.
Log [0–7]	Each packet, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.
From <IPaddr/mask>	Applies only to packets with source IP addresses falling within the address range.
To <IPaddr/mask>	Applies only to packets with destination IP addresses falling within the address range.
NextHop <IP addr>	Forwards the qualified packets to another IP address instead of the destination IP address in the packet. The destination address in the packet is not modified, only the forwarding direction is affected. This value is useful only with received packets on the interface, before routing decisions have been made.

Equivalent Generic Filter Rules (assuming Permit)

Incoming filters	Permit [From<source>] [To<dest>] [NextHop<IP addr>] UDP Dst = 69 Permit [From<dest>] [To<source>] [NextHop<IP addr>] UDP Src = 69
Outgoing filters	Permit [From<source>] [To<dest>] UDP Dst = 69 Permit [From<dest>] [To<source>] UDP Src = 69

WAISIn

Syntax

```
ADD !<port> -FireWall WAISIn Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
DELete !<port> -FireWall WAISIn Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
```

Default No default

Description The WAISIn parameter permits or denies incoming Wide Area Information Service (WAIS) connections through the firewall. WAIS is a TCP-based service. WAIS clients use random ports above 1023; WAIS servers usually use port 210.

Values

Permit	Permits incoming WAIS connections.
Deny	Denies incoming WAIS connections.
Log [0–7]	Specifies a connection request. Each request, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.
From <IPaddr/mask>	Applies only to packets with source IP addresses falling within the address range.
To <IPaddr/mask>	Applies only to packets with destination IP addresses falling within the address range.
NextHop <IP addr>	Forwards the qualified packets to another IP address instead of the destination IP address in the packet. The destination address in the packet is not modified, only the forwarding direction is affected. This value is useful only with received packets on the interface, before routing decisions have been made.

Equivalent Generic Filter Rules (assuming Permit)

Incoming filter	Permit [From<source>] [To<dest>] [NextHop<IP addr>] TCP Src >1023 Dest = 210
Outgoing filter	Permit [From<dest>] [To<source>] TCP Src = 210 Dst >1023 Estab

WAISOut

Syntax

```
ADD !<port> -FireWall WAISOut Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
DELete !<port> -FireWall WAISOut Permit | Deny [Log[0–7]] [From
  <IPaddr/mask>] [To <IPaddr/mask>] [NextHop <IPaddr>]
```

Default No default

Description The WAISOut parameter permits or denies Wide Area Information Service (WAIS) connections through the firewall. WAIS is a TCP-based service. WAIS clients use random ports above 1023; WAIS servers usually use port 210.

Values	Permit	Permits outgoing WAIS connections.
	Deny	Denies outgoing WAIS connections.
	Log [0–7]	Specifies a connection request. Each request, whether permitted or denied, is independently logged. You can select log message priorities: Log(0), emergency, is the highest priority and Log(7), debug, is the lowest priority. These priorities are meaningful when using syslog to write to the log server. If a priority is not specified, then the default priority, Log(6) (informational), is applied.
	From <IPaddr/mask>	Applies only to packets with source IP addresses falling within the address range.
	To <IPaddr/mask>	Applies only to packets with destination IP addresses falling within the address range.
	NextHop <IP addr>	Forwards the qualified packets to another IP address instead of the destination IP address in the packet. The destination address in the packet is not modified, only the forwarding direction is affected. This value is useful only with received packets on the interface, before routing decisions have been made.
Equivalent Generic Filter Rules (assuming Permit)	Incoming filter	Permit [From<dest>] [To<source>] [NextHop<IP addr>] TCP Src = 210 Dst >1023 Estab
	Outgoing filter	Permit [From<source>] [To<dest>] TCP Src >1023 Dst = 210

25 FR SERVICE PARAMETERS

This chapter describes parameters in the Frame Relay (FR) Service. Table 25-1 lists the FR Service parameters and commands.

Table 25-1 FR Service Parameters and Commands

Parameters	Commands
AllDlci	SHow
AtmMode	SETDefault, SHow
BackupPVC	ADD, DELete, SHow
COMPressType	SETDefault, SHow
CONFiguration	SHow
CONTrol	SETDefault, SHow
DEbit	SETDefault, SHow
DIAGnostics	FLush, SHow
DLCIR	SETDefault, SHow
DLciStat	FLush, SHow
DRTrigger	SETDefault, SHow
ErrorThreshold	SETDefault, SHow
FSEInterval	SETDefault, SHow
KATime	SETDefault, SHow
MonitoredEvent	SETDefault, SHow
PDNtype	SETDefault, SHow

AllDlci

Syntax

```
SHow [!<port> | !*] -FR AllDlci
```

Default No default

Description The AllDlci parameter displays all the data link connection identifiers (DLCIs) that are active on the Frame Relay network.

AtmMode

Syntax

```
SETDefault !<port> -FR AtmMode = ([Disabled | Enabled], [AAL5 |
   AAL34])
SHow [!<port> | !*] -FR AtmMode
```

Default Disable, AAL5

Description The AtmMode parameter enables or disables asynchronous transfer mode (ATM) running under the FR Service.

Values

Enable | Disable	Enable specifies logical link control/Subnetwork Access Protocol (LLC/SNAP) encapsulation; this is the normal ATM mode. Disable specifies Network Layer Protocol Identifier (NLPID) encapsulation; this is the normal Frame Relay mode. To allow connectivity between a 3Com bridge/router running ATM and another router that supports Frame Relay but not ATM, disable this mode.
AAL34 | AAL5	Use AAL34 when connecting to an ATM digital service unit (DSU) that supports only ATM Adaptation Layer AAL3-4. Use AAL5 when connecting to an ATM DSU that supports AAL5.

BackupPVC

Syntax

```
ADD !<port> -FR BackupPVC <PortNo>@<DLCI>
DELete !<port> -FR BackupPVC <PortNo>@<DLCI>
SHow [!<port> | !*] -FR BackupPVC
```

Default No default

Description The BackupPVC parameter adds or deletes a secondary permanent virtual circuit (PVC) to or from a virtual port. This secondary PVC backs up the primary PVC defined for the virtual port.

The SHow command displays all the primary and secondary PVCs and their status. If a virtual port number is specified, it displays the status of the primary and secondary PVCs attached to the specified virtual port. If a virtual port number is not specified, it displays the status of the primary and secondary PVCs attached to all the virtual ports.

Example To add a backup PVC to virtual port 1, where 4 is the physical port on which Frame Relay is running and 35 is the DLCI, enter the following command:

```
ADD !V1 -FR BackupPVC 4@35
```

COMPressType

Syntax

```
SETDefault !<port> -FR COMPressType = <dlci> [DEFault | NONE |
   PerPacket]
SHow [!<port> | !*] -FR COMPressType
```

Default DEFault

Description The COMPressType parameter selects the compression for each individual DLCI. This parameter overrides the compression type configured for the PORT Service.

Values

DEFault | NONE | PerPacket	The DEFault setting uses the compression type configured on the PORT Service. NONE specifies that no compression will be performed. PerPacket sets per-packet data compression. For complete information on link-level compression, refer to Chapter 39 in *Reference for NETBuilder Family Software*.

CONFiguration

Syntax

```
SHow [!<port> | !*] -FR CONFiguration
```

Default No default

Description The CONFiguration parameter displays current FR Service configuration information for each bridge/router port. The display includes the CONTrol parameter setting, the DLCIs attached to the Frame Relay network, the status of each virtual port, and the active DLCI for that port. If you set the value of the -FR CONTrol parameter to NTTLMI, the DLCI and committed information rate (CIR) values of each port are also displayed.

If you want to display configuration information for a particular port only, include the port number in the SHow CONFiguration command. If you do not specify a port number, information for all active Frame Relay ports is displayed.

CONTrol

Syntax

```
SETDefault !<port> -FR CONTrol = [NoLMI | LMI | ANsiLMI | NTTLMI]
SHow [!<port> | !*] -FR CONTrol
```

Default ANsiLMI

Description The CONTrol parameter determines whether the Line Management Interface (LMI) Protocol runs over a specified port. You must use the -PORT OWNer parameter to enable the FR Service.

Values

NoLMI | LMI | ANsiLMI | NTTLMI	Allows you to enable or disable LMI over a particular interface. LMI allows the bridge/router to learn about all the nodes that are reachable on a particular interface. If LMI is selected, the Consortium LMI Protocol runs between the bridge/router and the data communications equipment (DCE). If ANsiLMI is selected, the Annex-D Protocol runs between the bridge/router and the DCE. If NTTLMI is selected, the NTT LMI Protocol runs between the bridge/router and the DCE. If LMI protocol is running consortium LMI, the valid range for subscriber numbers is 16–1022. For other LMI protocols, the range is 16–991.

DEbit

Syntax

```
SETDefault !<port> -FR DEbit = [NoPRiority | PRiority]
SHow [!<port> | !*] -FR DEbit
```

Default NoPRiority

Description The DEbit parameter specifies whether the discard eligibility DE bit in a packet header is reset for all packets or only for high priority packets.

Values

NoPRiority	Resets the DE bit for all packets.
PRiority	Resets the DE bit for high priority packets only.

DIAGnostics

Syntax

```
FLush -FR DIAGnostics
SHow -FR DIAGnostics
```

Description The DIAGnostics parameter displays diagnostics information maintained by the system. SHow currently displays one diagnostic message that pertains to the reception of out-of-range DLCIs in the control packet. The range of DLCIs acceptable to the system is 16-1022.

DLCIR

Syntax

```
SETDefault !<port> -FR DLCIR = <dlci> <cir>
SHow [!<port> | !*] -FR DLCIR
```

Default No default

Configure this parameter only if you set the value of the -FR CONTrol parameter to NTTLMI.

Description The DLCIR parameter controls the throughput of a DLCI if congestion occurs over a Frame Relay network. If a Frame Relay network becomes congested, the 3Com bridge/router reduces the throughput to a level appropriate to the Frame Relay service provider.

Values

<dlci> Specifies a DLCI number assigned by your Frame Relay service provider. Valid entries include 16 to 1022.

<cir> Specifies a CIR value assigned by your Frame Relay service provider. Valid entries include 0, 16, 32, 64, 128, 192, 256, 512, 768 kbps. Specifying 0 implies that no CIR value was assigned by the Frame Relay service provider. In this instance, the bridge/router uses an internal value to provide minimum service. If you specify a higher value than the value assigned by your Frame Relay service provider, the DLCI may perform erratically, that is, it may drop packets.

The SHow command allows you to display the DLCIR parameter setting for a particular port. If you do not specify a port with the SHow command, the DLCIR parameter settings for all ports are shown.

DLciStat

Syntax

```
FLush [!<port>] -FR DLciStat
SHow [!<port> | !*] -FR DLciStat
```

Default No default

Description The DLciStat parameter displays the DLCI status and statistics for all the active Frame Relay ports. The FLush command zeros out the statistic values displayed by the SHow command.

DRTrigger

Syntax

```
SETDefault !<port> -FR DRTrigger = ([PVC | LINE])
SHow [!<port> | !*] -FR DRTrigger
```

Default PVC

Description The DRTrigger parameter specifies whether a PVC or the dial-up link triggers dial recovery when the link goes down.

ErrorThreshold

Syntax

```
SETDefault !<port> -FR ErrorThreshold = (1–10)
SHow [!<port> | !*] -FR ErrorThreshold
```

Default 3

Description The ErrorThreshold parameter specifies the maximum number of unanswered status enquiry messages the bridge accepts before shutting down the path.

FSEInterval

Syntax

```
SETDefault !<port> -FR FSEInterval = (1–255)
SHow [!<port> | !*] -FR FSEInterval
```

Default 6

Description The FSEInterval parameter indicates the number of status enquiry intervals that pass before full status enquiry messages (FSE) are issued. The FSE interval defines the number of keepalive messages sent before sending the full status enquiry message.

KATime

Syntax

```
SETDefault !<port> -FR KATime = <seconds> (5–30)
SHow [!<port> | !*] -FR KATime
```

Default 10

Description The KATime parameter specifies the amount of time (in seconds) between transmission of keepalive packets.

MonitoredEvent

Syntax

```
SETDefault !<port> -FR MonitoredEvent = (1–10)
SHow [!<port> | !*] -FR MonitoredEvent
```

Default 4

Description The MonitoredEvent parameter specifies the maximum number of responses to full status or link integrity verification messages unacknowledged before the specified path shuts down.

PDNtype

Syntax

```
SETDefault !<port> -FR PDNtype = PRIvate | SPRint | MCI
SHow [!<port> | !*] -FR PDNtype
```

Default PRIvate

Description The PDNtype parameter configures a port to communicate with a particular type of public data network (PDN). Retaining the default value of this parameter (PRIvate) is the same as setting the value to SPRint.

INDEX

Symbols

- ? command B-2

A

- AarpCache parameter, AppleTalk Service 4-2
- AarpCouNT parameter, AppleTalk Service 4-2
- AarpTIMe parameter, AppleTalk Service 4-2
- AC Service
  - logged-in users, displaying 3-2
  - parameter list 3-1
- AccessAct parameter, DLSw Service 19-2
- ActivePorts parameter, UDPHELP Service 62-1
- ActiveSCHedule parameter, SCH Service 50-1
- ADD 23-6
- ADD command 1-1
- ADDRess parameter
  - AppleTalk Service 4-3
  - DECnet Service 17-2
  - IP Service 29-2
  - IPX Service 31-1
  - RIPXNS Service 48-1
  - STP Service 57-1
  - SYS Service 58-2
  - VIP Service 63-1
- Address Resolution Protocol. *See* ARP Service
- addresses
  - ARP table 29-2
  - boundary, for multicasting 20-3
  - convert
    - DLCI to VPI.VCI 1-27
    - PDN-type IP to X.25 1-30
    - PDN-type X.25 to IP 1-24
    - VPI.VCI to DLCI 1-6
  - discovering IP 6-2
  - displaying 1-57
    - AppleTalk 4-4
    - Frame Relay 25-1
    - IP 1-56, 29-2, 29-13
    - IPX Service 31-1
    - IS-IS 32-3, 32-12, 32-13
  - DSA 40-2
  - formats
    - matching to end systems 43-23
    - SMDS 53-2
  - Frame Relay 32-12
  - Internet 29-2
  - MAC
    - and path type 22-2
    - converting canonical to noncanonical 1-31
    - display mode 58-8
    - displaying 1-58
- addresses (continued)
  - MAC (continued)
    - downstream neighbor, FDDI 22-2
    - duplicate, FDDI 22-2
    - format 1-31, 43-23, 58-9
    - SMT 22-8
    - STP multicast 57-1
    - upstream neighbor, FDDI 22-10
  - mapping
    - DECnet to X.25 17-14
    - functional to multicast 14-8
    - IP to X.25 26-3
    - multiple DECnet networks 17-3
    - X.25 subaddress to IP or PSAP 26-5
  - mapping IP to
    - Frame Relay DLCIs 29-2
    - MAC 29-2
    - X.25 29-2
  - network 29-13
  - router
    - DECnet 17-2
    - VIP 63-1
  - SMDS group 53-2
  - SMDS group. *See also* SMDSGroupAddr parameter
  - SMDS individual 53-2
  - subnet mask 29-14
  - translation table 29-2
- AddressMap parameter, DECnet Service 17-3
- AddrLOCation parameter, ATUN Service 9-1
- AddUser command 1-2
- ADJacencies parameter
  - ISIS Service 32-2
  - NLSP Service 38-1
- AdjLenDef parameter, APPN Service 5-2
- AdjLinkSta parameter, APPN Service 5-3
- AdjNodeStatus parameter, APPN Service 5-6
- AdvertisePolicy parameter
  - DECnet Service 17-3, 17-4
  - NRIP Service 39-1
  - RIPIP Service 47-1
  - SAP Service 49-1
- AdvToNeighbor parameter
  - DECnet Service 17-5
  - NRIP Service 39-2
  - RIPIP Service 47-3
  - SAP Service 49-2
- AgeTime parameter
  - ATMLE Service 8-1
  - BRidge Service 14-1
- AggregateExcept parameter
  - BGP Service 12-2
  - DVMRP Service 20-1
- AggregateRange parameter
  - BGP Service 12-2
  - DVMRP Service 20-2
- aggregation
  - BGP 12-2
  - DVMRP 20-2
  - RIPIP 47-5
- ALias parameter, SYS Service 58-3
- aliases for commands 58-3
- All Route Explorer frames 56-5
- AllDlci parameter, FR Service 25-1
- AllEndNodesTR parameter, DECnet Service 17-6
- AllRoutersTR parameter, DECnet Service 17-6
- AllRoutes parameter
  - AppleTalk Service 4-4
  - BRidge Service 14-2
  - DECnet Service 17-7
  - IDP Service 27-1
  - IP Service 29-3
  - IPX Service 31-2
  - SR Service 56-1
  - VIP Service 63-2
- AllServers parameter, IPX Service 31-3
- AllSessions parameter, TERM Service 61-4
- AMTagingTime parameter, AppleTalk Service 4-5
- ANameLookup command 1-2
- APING command 1-4
- AppleTalk
  - bridging between Ethernet and FDDI 14-3
  - device, checking 1-4
  - entity name lookup 1-2
- AppleTalk Address Resolution Protocol (AARP). *See* AppleTalk Service
- AppleTalk Echo Protocol (AEP) 1-4
- APPleTalk parameter, BRidge Service 14-3
- AppleTalk Service
  - AARP cache
    - displaying and flushing 4-2
    - entries, interval for validating 4-5
  - AARP request or probe 4-2
  - addresses
    - displaying 4-4
    - mapping to media addresses 4-3
    - SMDS group 4-18
    - socket 4-13
  - configuring 4-6
  - creating an X.25 profile 4-19
  - debugging 4-9
  - displaying current configuration 4-6
  - entity filtering
    - defining 4-9
    - enabling 4-7
    - filter number 4-12
  - names
    - router 4-17
    - zone 4-8

- AppleTalk Service (continued)
  - NBP Name Table
    - displaying 4-13
    - maximum lookup time 4-14
  - network number
    - for startup 4-19
    - range for cable attachment 4-15
  - network number-based filtering
    - enabling 4-7
    - network ranges 4-14
    - positive and negative 4-15
  - node ID for startup 4-19
  - packets
    - filtering 4-7
    - update interval 4-18
  - parameter list 4-1
  - routes
    - aging time 4-17
    - displaying and flushing 4-3
    - learning 4-8
  - routing
    - AARP cache, validating entries 4-5
    - over non-AppleTalk data link 4-7
    - over X.25 4-20
  - routing table, displaying 4-4
  - troubleshooting 4-9
  - X.25, protocol identifier 4-20
  - zones
    - adding 4-20
    - default 4-8
    - deleting 4-20
    - mapping 4-16
    - port 4-16
- APPN Service
  - adding directory entries 5-17
  - adjacent LEN nodes,defining 5-2
  - adjacent link stations
    - activating and deactivating 5-25
    - setting characteristics 5-23
  - adjacent nodes,verifying status 5-6
  - APPN ports
    - activating and deactivating 5-30
    - defining 5-31
  - class of service
    - adding and deleting 5-8
    - defining on the node 5-12
    - display 5-12
    - mapping to mode names 5-28
    - mode name display 5-28
    - node row 5-13
    - TG row 5-14
  - configuration display 5-8
  - connection display 5-8
  - connection network
    - characteristics configuration 5-10
    - configuration 5-11
    - definitions 5-11
  - directory display 5-16
  - DLUr
    - adding PU 2.0 and 2.1 nodes 5-18
    - downstream LU display 5-21
    - status display 5-20
  - DLUs
    - specifying defaults 5-18
    - status display 5-21
  - HPR timer 5-21
- APPN Service (continued)
  - ISR sessions 5-22
  - local node name 5-27
  - local node resistance 5-28
  - network node
    - directory display 5-16
    - enabling and disabling 5-12
    - name for local node 5-27
    - resistance 5-28
    - topology display 5-29
  - parameter displays 5-8
  - parameter list 5-1
  - pinging to other LUs 1-5
  - QueuePriority parameter 5-33
  - registering LUs 5-2
  - RTP connection statistics 5-34
  - RTP connections 5-33
  - SDLC adjacent link stations 5-35
  - SDLC DLUr link stations 5-37
  - TG topology display 5-40
  - tree cache display 5-41
- AppnLOG parameter, APPN Service 5-7
- APpnPING command 1-5
- ARCHIE parameter, IPFirewall Service 24-2
- area addresses
  - DECnet 17-2, 17-16
  - ISIS 32-3
  - OSPF 41-2
- AreaAddress parameter
  - ISIS Service 32-3
  - NLSP Service 38-2
- AreaId parameter, OSPF Service 41-2
- AreaRanges parameter, OSPF Service 41-2
- ARP Format firmware parameter, NETBuilder II A-15
- ARP Service
  - ARP table, inactive entry 6-2
  - displaying current configuration 6-1
  - IP address discovery 6-1
  - proxy requests 6-1
  - RARP client 6-3
  - RARP server 6-3
  - request packets, header format 6-4
  - Reverse ARP Protocol (RARP) 6-3
- ARPRoute parameter, ATMLE Service 8-2
- ArpRspTime parameter, ATMLE Service 8-2
- AsFilter parameter, BGP Service 12-3
- ASPath parameter, BGP Service 12-4
- AsPolicyAll parameter, BGP Service 12-4
- AsPolicyExt, BGP Service 12-5
- AsPolicyInt parameter, BGP Service 12-6
- AsPolicyPeer parameter, BGP Service 12-7
- asynchronous communications. *See* ATUN Service
- asynchronous path
  - configuring parity used, with PARity parameter 42-17
- ATM Service
  - CONTrol parameter 7-1
  - creating permanent virtual circuit 7-2
  - displaying current configuration 7-1
  - F5 loopback
    - enabling 7-5
    - time interval to initiate 7-6
- ATM Service (continued)
  - loop mode
    - configuring 7-2
    - time interval for checking interface 7-2, 8-4
  - number of VCI bits 7-5
  - number of VPI bits 7-6
  - parameter list 7-1
  - traffic shaping attributes 7-4
- ATMAddress parameter, ATMLE Service 8-2
- ATMLE Service
  - control time-out period 8-2
  - display LAN emulation client configuration paramteters 8-3
  - enabling LAN emulation client 8-3
  - LE_ARP table contents 8-2
  - local ATM address 8-2
  - maximum inactivity period 8-1
  - parameter list 8-1
- AtmMode parameter, FR Service 25-1
- ATMNeighbor parameter, BRidge Service 14-3
- AtmToFr command 1-6
- ATUN Service
  - address location offset 9-1
  - broadcast address byte 9-2
  - CU
    - address 9-2
    - configuration display 9-2
    - information display 9-3
  - CU port display 9-4
  - CU status display 9-4
  - enabling and disabling ATUN ports 9-7
  - enabling and disabling CUs 9-2
  - end of frame characters 9-4
  - frame size maximum 9-5
  - idle time frame gap 9-5
  - local MAC address 9-6
  - local SAP 9-6
  - maximum inter-character delay 9-6
  - parameter list 9-1
  - port configuration display 9-6
  - port CU definition 9-8
  - remote MAC address 9-9
  - remote SAP 9-9
- AUDit command 1-6
- audit trail messages, time/date stamp 58-4
- AUditTrailType parameter, SYS Service 58-4
- AuthDHCPServer parameter, UDPHELP Service 62-2
- AuthLocalUser parameter, PPP Service 44-1
- AuthProTocol parameter, PPP Service 44-1
- AuthRemoteUser parameter, PPP Service 44-2
- AuthReptIntvl parameter, PPP Service 44-2
- AutoDial parameter, PORT Service 43-2
- AUToDisconnect parameter, TERM Service 61-4
- AUToListen parameter, TERM Service 61-4
- automatic connections, incoming. *See* incoming connections
- automatic connections, outgoing. *See* outgoing connections

B

- B channel data rate
  - setting with RateAdaption parameter 42-17
- BackupPVC parameter, FR Service 25-2
- BACkwards command 1-7
- bandwidth
  - assigning to packets transmitting from WAN port 43-25
- bandwidth for multicast traffic 20-9
- BAud parameter
  - PATH Service 42-2
  - TERM Service 61-5
- baud rate 42-2
  - calculation for port cost 63-4
  - terminal device 61-5
- BCN Service
  - IBM Boundary Routing status
    - displaying 11-2
- BCN service
  - backup central node address 11-1
  - remote LAN media type 11-3
  - smart filtering 11-1
  - X.25 protocol identifier 11-3
- BGP Service
  - AS number
    - defining 12-12
    - modifying 12-16
  - AS paths, displaying 12-4
  - AS policy 12-4 to 12-7
  - cost, route 12-17
  - debugging 12-9
  - displaying current configuration 12-8
  - enabling 12-8
  - filtering the display 12-10
  - filters
    - AS 12-3
    - network 12-12
  - interior policy 12-11
  - network policy 12-13 to 12-15
  - peers
    - configuration, modifying 12-16
    - current 12-8
    - enabling and disabling 12-17
    - expiration time 12-11
    - IP addresses, adding 12-17
    - maximum 12-12
  - routes
    - advertising 12-15
    - aggregate exception 12-2
    - aggregate range 12-2
    - default route and weight 12-9, 12-10
    - displaying 12-18
    - specific weight, defining 12-18
  - saving settings to disk 1-52
  - tracing events 12-9
  - version number 12-18
- Binary Synchronous Communications (BISYNC). *See* BSC
- BISYNC. *See* BSC
- BLimitTimer parameter, BRidge Service 14-4
- BODIncrLimit parameter, PORT Service 43-2
- BODTHreshold parameter, PORT Service 43-3
- Boot command B-1
- Boot Device firmware parameter A-11, A-22
- boot monitor B-1
- boot path B-1
- Boot Protocol firmware parameter A-14
- Boot Sources firmware parameter A-5, A-17, A-24
- Boot Statistics firmware parameter A-8, A-20, A-26
- boot, test A-4, A-17, A-24
- booting
  - from RBCS 58-7
  - system 1-44
- BOOTPC Service 13-1
  - display current BOOTP Client state 13-2
  - number of BOOTREQUEST packets sent 13-2
  - retransmission interval for BOOTREQUEST packets 13-3
- BootpMaxHops parameter, UDPHELP Service 62-2
- BootpThreshold parameter, UDPHELP Service 62-3
- Border Gateway Protocol. *See* BGP Service
- BoundAccessNode parameter, DLSw Service 19-2
- Boundary Routing
  - displaying
    - current configuration 11-1
    - IBM status 11-2
  - enabling 11-1
  - installing menu interface 1-29
  - port status 44-4
  - remote LAN media type 11-3
  - X.25 protocol identifier 11-3
- BoundaryAddr parameter, DVMRP Service 20-3
- BReakAction parameter, TERM Service 61-5
- BReakChar parameter, TERM Service 61-6
- bridge/router
  - accessing by
    - remote 1-44
    - Rlogin 1-49
    - Telnet 1-62
  - accessing through
    - console port 58-10
    - remote 58-10, 58-12
    - Telnet 58-10, 58-17
  - booting 1-44
  - commands 1-1
  - files
    - NCS/RBCS address 58-7
    - storing 58-7
  - hardware information, displaying
    - CPU 58-5
    - DPMs 58-6
    - I/O modules 58-8
  - location 58-15
  - macro
    - cache 58-9
    - names 58-11
  - memory, managing 58-4
  - name 58-16
  - operating as a bridge. *See* BRidge Service, SR Service, and STP Service
  - user interaction environment 2-1
- BRidge Service 14-1, 14-5
  - addresses
    - mapping functional to multicast 14-8
    - masks 14-2
    - neighbor 14-14
    - SMDS group 14-12
  - ATM neighbors 14-3
  - bridge
    - enabling 14-6
    - operating as router 14-6
  - configuring 14-5
  - creating an X.25 profile 14-14
  - displaying current configuration 14-4
  - FireWall/NoFireWall option 14-6
  - Frame Relay neighbors 14-7
  - MAC header interpretation over WAN 14-6
  - multicast, forwarding rate 14-4
  - neighbors
    - ATM 14-3
    - Frame Relay 14-7
    - SMDS 14-12
    - X.25 14-14
  - packets
    - aging 14-6
    - broadcast, forwarding rate 14-4
    - destination explicit forwarding and blocking 14-5
    - forwarding 14-6, 14-10
    - forwarding between Ethernet and FDDI 14-3
    - multicast, forwarding rate 14-4
    - source explicit forwarding and blocking 14-5
  - root bridge 57-3, 57-4
  - routes, learning 14-6
  - routing table
    - adding static routes 14-9
    - deleting learned routes 14-2
    - displaying 14-2
    - modifying 14-9
    - size 14-11
    - time for deleting a device 14-1
  - security
    - destination explicit forwarding and blocking 14-7
    - source explicit forwarding and blocking 14-13
  - SMDS neighbors 14-12
  - station movement 14-12
  - translation bridging 14-3
  - transparent bridging
    - disabling on specific ports 14-13
    - enabling 14-6
    - over ATM 14-3
    - over Frame Relay 14-7
    - over SMDS 14-12
    - over X.25 14-14
  - X.25
    - neighbors 14-14
    - protocol identifier 14-14
    - user profile definition 14-14
- bridge/router, accessing through Telnet 58-17
- BridgeNumber parameter,SR Service 56-2

BridgePriority parameter, STP Service 57-2
Broadcast command 1-7
BroadCastAddr parameter, ATUN Service 9-2
BroadCastLimit parameter, BRidge Service 14-4
BSC Service
  configuration display 15-2
  CU definitions 15-1
  defining primary and secondary devices 15-3
  enabling and disabling BSC ports 15-2
  enabling and disabling CUs 15-2
  parameter list 15-1
BscCU parameter, BSC Service 15-1
BT command B-1
BufferErrors parameter, FDDI Service 22-2
BufferSize parameter, NLSP Service 38-3
BUffersize parameter, TERM Service 61-7

C

cache
  AARP
    displaying and flushing 4-2
    entries, interval for validating 4-5
  Domain name 30-1
  DVMRP
    display forwarding table entries 20-5
    source group entry time 20-3
  macro
    clearing contents 58-9
    flushing 1-26
CAChe parameter, IPName Service 30-1
CacheTime parameter, DVMRP Service 20-3
CBPDU, transmission interval 57-3
CHange command 1-8
ChangeDir command 1-8
character
  determining stop bits appended on asynchronous path 42-20
  setting value of parity bit checked 42-18
CircuitBal parameter, DLSw Service 19-3
CIRcuits parameter, DLSw Service 19-2, 19-3
CLNP Service
  configuring 16-1
  creating an X.25 profile 16-5
  displaying current configuration 16-1
  End Systems (ES) list 16-3
  Intermediate Systems (IS) list 16-3
  Network Entity Title (NET) 16-4
  packets
    controlling generation of error 16-2
    controlling generation of redirect 16-4
    maximum transmission unit 16-4
    time-to-live 16-2
  parameter list 16-1
CLock parameter, PATH Service 42-3
clock, setting 58-5
Closed User Group (CUG) 45-3
CmdCharSet parameter, PATH Service 42-4
CntrlTime parameter, ATMLE Service 8-2
COLumns parameter, TERM Service 61-7
commands
  ? B-2
  aliases 58-3
  Boot B-1
  BT B-1
  description 1-1
  DF B-2
  Display Files B-2
  displaying
    recent 2-2
    summary of 1-1
  H B-2
  Help B-2
  MONitor B-3
  RA B-3
  RB B-4
  Reboot B-4
  Recovery Action B-3
  SHow 61-1
  SysconF B-1
COMmunity parameter, SNMP Service 55-1
COMPressType parameter
  FR Service 25-2
  PORT Service 43-3
Config File Source firmware parameter A-3, A-13, A-22
ConfigCOS parameter, APPN Service 5-8
configuration display. *See* CONFiguration parameter
configuration files
  copying
    between devices 1-10
    parameter values 1-43
  deleting 1-65
  retrieving from server 58-7
  saving current parameter values 1-50
CONFiguration parameter
  AC Service 3-1
  AppleTalk Service 4-6
  APPN Service 5-8
  ARP Service 6-1
  ATM Service 7-1
  ATMLE Service 8-3
  AuditLog Service 10-1
  BCN service 11-1
  BGP Service 12-8
  BOOTPC Service 13-1
  BRidge Service 14-4
  BSC Service 15-2
  CLNP Service 16-1
  DECnet Service 17-7
  DLSw Service 19-4
  DVMRP Service 20-4
  ESIS Service 21-1
  FIlter Service 23-1
  FR Service 25-3
  Gateway Service 26-1
  IDP Service 27-2
  IP Service 29-4
  IPFirewall Service 24-2
  IPName Service 30-1
  IPX Service 31-3
  ISIS Service 32-4
  LAPB Service 33-1
  LLC2 Service 34-1
  MIP Service 36-1
CONFiguration parameter (continued)
  MOSPF Service 37-1
  NLSP Service 38-3
  NRIP Service 39-3
  OSIAPPL Service 40-1
  OSPF Service 41-3
  PATH Service 42-4
  PORT Service 43-4
  PPP Service 44-2
  PROFile Service 45-1
  RDP service 46-1
  RIPIP Service 47-4
  RIPXNS Service 48-2
  SAP Service 49-3
  SCH Service 50-1
  SMDS Service 53-1
  SNA Service 54-1
  SNMP Service 55-2
  SR Service 56-3
  STP Service 57-2
  SYS Service 58-4
  TCP Service 59-1
  UDPHELP Service 62-3
  VIP Service 63-2
  WE Service 64-1
  XSWitch Service 66-1
configuring individual services. *See* CONTrol parameter
Connect command 1-9
connection control mode, FDDI 22-6
CONNection parameter, APPN Service 5-8
connections
  OSI 1-66
  remote 1-44
  Rlogin 1-49
  TCP
    automatic login 60-2
    displaying 59-1
  through remote 58-10, 58-12
  through Telnet 58-10, 58-16, 58-17
  tunnel 20-10, 34-2
  when failed, setting time before reconnection
    with DialRetryTime parameter 43-13
CONNections parameter
  DLSw Service 19-4
  OSIAPPL Service 40-1
  TCP Service 59-1
CONNectionUsage Parameter, SYS Service 58-4
CONNector parameter, PATH Service 42-5
CONNectStats parameter, DLSw Service 19-4
ConnHistory parameter, Gateway Service 26-1
ConnNetworkChar parameter, APPN Service 5-10
ConnNetworkDef parameter, APPN Service 5-11
ConnTime
  ATMLE Service 8-3
console port, for accessing bridge/router 58-10

- CONTrol parameter
  - AC Service 3-1
  - AppleTalk Service 4-6
  - APPN Service 5-12
  - ARP Service 6-1
  - ATMLE Service 8-3
  - AuditLog Service 10-1
  - BCN service 11-1
  - BGP Service 12-8
  - BOOTPC Service 13-1
  - BRidge Service 14-5
  - BSC Service 15-2
  - CLNP Service 16-1
  - DECnet Service 17-7
  - DLSw Service 19-5
  - DVMRP Service 20-4
  - ESIS Service 21-1
  - FIlter Service 23-1
  - Firewall Service 24-3
  - FR Service 25-3
  - Gateway Service 26-2
  - IDP Service 27-2
  - IISIS Service 28-1
  - IP Service 29-5
  - IPX Service 31-3
  - ISIS Service 32-4
  - LAPB Service 33-1
  - LLC2 Service 34-2
  - LNM Service 35-1
  - MIP Service 36-1
  - MOSPF Service 37-1
  - NLSP Service 38-4
  - NRIP Service 39-4
  - OSPF Service 41-3
  - PATH Service 42-6
  - PORT Service 43-5
  - RDP service 46-1
  - RIPIP Service 47-4
  - RIPXNS Service 48-2
  - SAP Service 49-4
  - SCH Service 50-2
  - SMDS Service 53-1
  - SNMP Service 55-2
  - STP Service 57-2
  - TCP Service 59-2
  - UDPHELP Service 62-3
  - VIP Service 63-2
  - X25 Service 65-1
  - XSWitch Service 66-1
- CONTrol parameter, ATM Service 7-1
- COpy command 1-10
- COS parameter, APPN Service 5-12
- COSDef parameter, APPN Service 5-12
- COSNodeChar parameter, APPN Service 5-13
- COSNodeRow parameter, APPN Service 5-13
- cost
  - default route
    - OSPF Service 41-5, 41-16
    - RIPIP Service 47-6
  - demand interface circuit 41-6
  - path, STP Service 57-4
  - port
    - DECnet Service 17-8
    - DVMRP Service 20-6
    - ISIS Service 32-7
    - OSPF Service 41-4
    - VIP Service 63-4
- cost (continued)
  - routes
    - BGP Service 12-17
    - OSPF Service 41-5, 41-9, 41-16
    - RIPIP Service 47-6, 47-9, 47-12
- Cost parameter
  - NLSP Service 38-4
  - OSPF Service 41-4
- COST parameter, DECnet Service 17-8
- COSTgChar parameter, APPN Service 5-14
- COSTgRow parameter, APPN Service 5-15
- CPUboardInfo parameter, SYS Service 58-5
- CRPad parameter, TERM Service 61-7
- CsnpTime parameter
  - ISIS Service 32-5
  - NLSP Service 38-5
- CUAddr parameter, SDLC Service 51-2
- CUAddress parameter, ATUN Service 9-2
- CUCONFig parameter, ATUN Service 9-2
- CUCONFiguration parameter, SDLC Service 51-2
- CUCONTrol parameter
  - BSC Service 15-2
- CUCONTrol parameter, ATUN Service 9-2
- CUCONTrol parameter, SDLC Service 51-2
- CUInfo parameter, ATUN Service 9-3
- CULocalMac parameter, SDLC Service 51-3
- CULocalSap parameter, SDLC Service 51-3
- CUMode parameter, SDLC Service 51-4
- CUNAme parameter, SDLC Service 51-4
- CUPOrt parameter, ATUN Service 9-4
- CUPOrt parameter, SDLC Service 51-5
- CURemoteMac parameter, SDLC Service 51-5
- CURemoteSap parameter, SDLC Service 51-5
- current tunnel sessions, displaying 19-5
- CurrentPAth parameter, FDDI Service 22-2
- CurrentPeeR parameter, BGP Service 12-8
- CurrentPorts, Environment parameter 2-1
- CurrentServices, Environment parameter 2-2
- CUSTatus parameter, ATUN Service 9-4
- CUType parameter, SDLC Service 51-6
- CUXid parameter, SDLC Service 51-7
- CUXidDefined parameter, SDLC Service 51-7

D

- data compression
  - configuring for X.25 profiles 45-3
  - tinygram on paths 42-21
- data link switch tunneling. *See* DLSW Service
- Data Link Test. *See* DLT
- DataBits parameter
  - PATH Service 42-7
- DataBits parameter, PATH Service 42-7
- DataForward parameter, TERM Service 61-8
- DatalinkAddrFmt parameter, BRidge Service 14-6
- DATE parameter, SYS Service 58-5
- daylight saving time, setting 58-6
- DEbit parameter, FR Service 25-3
- debug monitor 1-34, B-3
- DEBug parameter, BGP Service 12-9
- DEBUG parameter, OSPF Service 41-4
- debugging
  - AppleTalk Service 4-9
  - BGP Service 12-9
  - FIlter Service 23-2
  - FR Service 25-3, 25-4
  - ISIS Service 32-16
  - OSPF Service 41-5
  - PORT Service 43-6
- DECnet Service
  - addresses
    - adding to trusted neighbor list 17-16
    - defining translation 17-3
    - for route advertisements 17-3, 17-4
    - multidestination functional 17-6
    - SMDS group 17-19
    - specifying 17-2
  - area
    - numbers 17-2
    - to pseudo area translation 17-16
  - areas
    - internetworking between 17-9
    - maximum allowed 17-12
    - pseudo, maximum 17-13
  - defining address translation entry 17-4
  - displaying current configuration 17-7
  - enabling 17-7
  - hops, maximum
    - before looping 17-14
    - to reachable area 17-11
    - to reachable node 17-12
  - internetworking between different areas 17-9
  - neighbors
    - adding X.25 or Frame Relay addresses 17-14, 17-15
    - sending updates to 17-5
    - trusted, list 17-16
  - nodes, maximum 17-13
  - packets
    - hello, transmission interval 17-9
    - update 17-5
  - path cost
    - to reachable area 17-11
    - to reachable node 17-12
  - Phase IV
    - adjacent end nodes 17-6
    - adjacent router nodes 17-6
    - NSAP prefix 17-10, 17-11
    - route filtering 17-9
    - routes, specifying in Phase V LSAs 17-20
    - to Phase V translation 17-8
  - port
    - cost 17-8
    - status 17-19
  - pseudo area mapping function 17-8
  - router
    - address, assigning 17-2
    - priority 17-16
  - routes
    - advertising to adjacent routers 17-3
    - filtering 17-15
    - receive policy 17-18

- DECnet Service (continued)
  - routing
    - over X.25 17-21
    - specifying Level 1 or Level 2 17-15
    - update interval 17-19
  - routing table, displaying 17-7
  - X.25
    - protocol identifier 17-21
    - user profile 17-21
- DefAction parameter, Firewall Service 24-4
- DefaultAction parameter, FIlter Service 23-2
- DefaultMetric parameter
  - IISIS Service 28-2
  - NRIP Service 39-5
  - OSPF Service 41-5
  - RIPIP Service 47-6
- DefaultNet parameter, BGP Service 12-9
- DefaultParams parameter, TERM Service 61-8
- DefaultPriority parameter
  - PORT Service 43-5
- DefaultPU parameter, SNA Service 54-1
- DefaultTTL parameter
  - CLNP Service 16-2
  - IP Service 29-6
- DefaultWeight parameter, BGP Service 12-10
- DefaultZone parameter, AppleTalk Service 4-8
- DEFine command 1-11
- DEFRag command 1-13
- Delay parameter
  - IPX Service 31-4
  - OSPF Service 41-5
- DelayedAckTime parameter, TCP Service 59-2
- DelayTime parameter
  - ATMLE Service 8-4
- DELete command 1-13
- DELeteUser command 1-13
- DemandInterface parameter, OSPF Service 41-6
- Designated Intermediate System (DIS) 32-6
- DestGroup parameter
  - DVMRP Service 20-4
  - MOSPF Service 37-2
- DevCONTrol parameter
  - WE Service 64-1
- device
  - checking
    - AppleTalk 1-4
    - OSI 1-38
    - using PING command 1-40
  - type, specifying 61-9
- DeVice parameter, TERM Service 61-9
- DevSTATistics parameter, WE Service 64-2
- DF command B-2
- DIAGnostics parameter
  - AppleTalk Service 4-9
  - FIlter Service 23-2
  - FR Service 25-4
  - IPX Service 31-4
  - PORT Service 43-6
  - SR Service 56-3
- DIal command 1-14
- DialCarrierTime parameter, PATH Service 42-7
- DialCONFig parameter, PORT Service 43-6
- DialCONTrol parameter
  - PATH Service 42-8
  - PORT Service 43-8
- DialDebouncTime parameter, PORT Service 43-8
- DialHistory parameter, PORT Service 43-9
- DialIdleTime parameter, PORT Service 43-9
- dialing
  - path-based 1-15
  - port-based 1-14
- DialInitState parameter, PORT Service 43-9
- DialMode parameter, PATH Service 42-9
- DialNoList parameter, PORT Service 43-10
- DialPathLimit parameter, WE Service 64-2
- DialPool parameter, PATH Service 42-9
- DialRcvrState parameter, PORT Service 43-12
- DialRetryCount parameter, PORT Service 43-12
- DialRetryTime parameter, PORT Service 43-13
- DialSamplTime parameter, PORT Service 43-13
- DialSTatus parameter, PORT Service 43-14
- dial-up lines
  - and paths
    - attributes 42-8
    - connecting 1-14
    - device type connected to the path 42-11
    - disconnecting 1-29
    - line type, setting 42-12, 42-17
    - path-based 1-15
    - wait for carrier signal 42-7
  - and ports
    - attributes 43-8
    - configurations 43-6
    - connecting 1-14
    - connecting paths 43-2
    - dial number list 43-10
    - dial path resources 43-22
    - dial status 43-14
    - disconnecting 1-29
    - dynamic dial path usage preference 43-21
    - idle time before disconnect 43-9
    - number of retries 43-12
    - PPP virtual ports 43-31
    - time between samples 43-13
    - time-stamped dial history 43-9
    - wait before connect, disconnect 43-8
    - wait before retry 43-13
- DIR Service
  - name resolution order 18-1
  - parameter list 18-1
- DIRectory parameter, APPN Service 5-16
- Directory Service. *See* DIR Service
- Directory System Agent (DSA) 1-64, 40-2
- Directory User Agent (DUA) 1-64, 40-2
- DIRectoryEntry parameter, APPN Service 5-17
- DirectoryManage command 1-16
- DirectPolicy parameter, OSPF Service 41-7
- DisConnect command 1-16
- discovering neighboring RDP routers 1-18
- DiscoverRoutes command 1-17
- DiscRouteRs command 1-18
- DISHelloTime parameter
  - ISIS Service 32-6
  - NLSP Service 38-5
- DiskFiles command 1-18
- Display Files command B-2
- Display parameter, DLSw Service 19-5
- DisplayCircuit parameter, DLSw Service 19-5
- DisplayFilter parameter, BGP Service 12-10
- Distance Vector Multicast Routing Protocol Service. *See* DVMRP Service
- DLCI, displaying 25-1
- DlciNeighbor parameter, BRidge Service 14-7
- DLciStat parameter, FR Service 25-4
- DLSw Service
  - adding peer router addresses 19-12
  - Boundary Access Node (BAN) 19-2
  - circuit balancing 19-3
  - collecting end-station topology information 19-18
  - configuration, displaying 19-4
  - configuring
    - displaying current 19-4
    - NetBIOS timeout 19-11
    - resends 19-11
  - connections, displaying 19-4
  - converting SNA alerts to traps 19-16
  - defining
    - access actions for remote traffic 19-17
    - access filters 19-11, 19-12
    - filters for determining access 19-2
    - local DLSw IP address 19-6
    - NetBIOS names 19-14
    - SNA local access actions 19-16
  - displaying
    - circuits 19-3
    - current configuration 19-4
    - current connections 19-4
    - end-station topology information 19-18
    - log of activity messages 19-5
    - MAC addresses 19-8
    - NetBIOS names 19-11
    - peer addresses 19-12
  - end-station topology information
    - collecting 19-18
    - displaying 19-18
  - FR-to-FEP address mapping 19-6
  - multicast address configuration 19-10
  - multicast retry interval 19-10
  - multicast statistics display 19-9
  - parameter list 19-1
  - port groups 19-14
  - traces
    - displaying trace entries 19-20
    - maximum number of bytes captured 19-8
  - tunnel connections
    - controlling 19-9
    - enabling 19-4

- DLSw Service (continued)
  - tunnel DLSw connections
    - assigning traffic priorities 19-14
    - displaying 19-5, 19-14, 19-15
    - MAC addresses for tunnel peers 19-13
- DlswLOG parameter, DLSw Service 19-5
- DLT
  - LoopBack mode 1-23
  - statistics, displaying 1-22
- DLTest command 1-19
- DlurDefaults parameter, APPN Service 5-18
- DlurLinkSta parameter, APPN Service 5-18
- DluRStatus parameter, APPN Service 5-20
- DluSStatus parameter, APPN Service 5-21
- DNSSvrSvr parameter, Firewall Service 24-4
- DO command 1-24
- Domain name service 30-3
- DomainName parameter, IPName Service 30-2
- DownNeighbor parameter, FDDI Service 22-2
- DownStreamLU parameter, APPN Service 5-21
- DpmSTATistics parameter, SYS Service 58-6
- DRTrigger parameter, FR Service 25-4
- DSAAddress parameter, OSIAPPL Service 40-2
- DSAType parameter, OSIAPPL Service 40-2
- DSTime parameter, SYS Service 58-6
- DStSecurity parameter, BRidge Service 14-7
- DteToIp command 1-24
- dual MAC station, Wrap AB flag 22-11
- DuaState parameter, OSIAPPL Service 40-2
- Dump Destination firmware parameter, NETBuilder II A-5, A-18, A-25
- dumping memory B-3
- DupAddress parameter, FDDI Service 22-2
- DUplex parameter, PATH Service 42-10
- Dvmrp parameter, MOSPF Service 37-3
- DVMRP Service
  - bandwidth for multicast traffic 20-9
  - boundary addresses for scoping 20-3
  - cost 20-6
  - displaying current configuration 20-4
  - enabling 20-4
  - forwarding table
    - displaying 20-5
    - source group entry time 20-3
  - neighbors
    - configuring X.25 or Frame Relay 20-7
    - displaying router information 20-7
  - policies
    - advertising MOSPF sourced networks 20-6
    - enabling inter-AS forwarding 20-8
    - filtering destination group data packets 20-4, 20-8
  - pruning 20-9
  - routes, aggregate exception and range 20-1
  - routing table
    - displaying 20-9
    - update time 20-10
  - tunneling through unicast routers 20-10

E

- EbmeCONFig parameter, SCH Service 50-2
- EbmeCONTrol parameter, SCH Service 50-2
- EbmeEVent parameter, SCH Service 50-3
- Echo command 1-24
- echo option, setting 58-18
- ECHOData parameter, TERM Service 61-10
- ECHOMask parameter, TERM Service 61-10
- ECMChar parameter, TERM Service 61-10
- EGP, learned routes
  - OSPF-reported 41-7
  - RIP-reported 47-6
- ElanName parameter, ATMLE Service 8-4
- ENCoding parameter, PATH Service 42-10
- End System Hello Protocol Data Units (ESH PDUs) 21-3
- End-System-to-Intermediate System. *See* ESIS Service
- entities, named 1-2
- EntityFilter parameter, AppleTalk Service 4-9
- EntityFilterNum parameter, AppleTalk Service 4-12
- Environment parameters 2-1
  - configuring 2-3
  - port information, displaying 2-1
  - privilege level, setting
    - User and Network Manager 2-3
  - recent commands, displaying 2-3
  - screen length 2-4
  - services, setting 2-2
- ERAse parameter, TERM Service 61-11
- EraseDump command 1-25
- ERgeneration parameter, CLNP Service 16-2
- Error Packets Protocol Data Units (ER PDUs) 16-2
- ErrorThreshold parameter, FR Service 25-5
- ErrorThreshold parameter, WE Service 64-3
- ES parameter, CLNP Service 16-3
- ESIS Service 21-1
  - hold time, setting for ESH and ISH PDUs 21-2
  - interval for transmitting ESH and ISH PDUs 21-3
  - multicast address (Ethernet and FDDI interfaces)
    - for ESH PDUs 21-3
    - for ISH PDUs 21-2
  - multicast address (token ring interfaces)
    - for ESH and ISH PDUs 21-3
- Ethernet
  - bridging over FDDI backbone 14-3
  - designated router 17-16
- EVent parameter, SCH Service 50-3
- ExcSftErrTh parameter, LNM Service 35-2
- ExDevType parameter, PATH Service 42-11
- EXPirationTimer parameter, AC Service 3-2
- EXPire command 1-25
- extended connections, incoming. *See* incoming connections
- extended connections, outgoing. *See* outgoing connections
- ExteriorPolicy parameter
  - IISIS Service 28-2
  - OSPF Service 41-7
  - RIPIP Service 47-6

F

- FDDI Service
  - buffer error count 22-2
  - dual MAC station wrap AB flag 22-11
  - frame
    - count 22-3
    - error ratio 22-3
  - link confidence test (LCT) failure count 22-3
  - link error monitor (LEM) count 22-4
  - MAC 22-4
    - connecting to ring 22-4
    - downstream neighbor address 22-2
    - duplicate address flag 22-2
    - LLC, enabling and disabling 22-4
    - path ID 22-4
    - path type display 22-2
    - ring management state 22-8
    - station Wrap AB flag 22-11
    - upstream neighbor address 22-10
  - optical bypass switch setting, displaying 22-5
  - parameter list 22-1
  - physical connection control (PCC) state 22-5
  - physical connection management (PCM) state 22-6
  - port A
    - connection control mode 22-6
    - maintenance line state 22-4
  - port B
    - connection control mode 22-6
    - maintenance line state 22-5
  - port neighbor type 22-7
  - receiver line state, definition 22-4
  - Remote Disconnect Flag 22-8
  - ring attachment and policy 22-3
  - SMT
    - MAC address 22-8
    - parameter management frame (PMF) 22-7
    - version, setting 22-8
  - station 22-9
    - function, specifying 22-9
    - identification 22-10
    - user data string, modifying 22-11
  - Target Token Rotation Time 22-10
- files
  - boot, copying between devices 1-10
  - configuration. *See* configuration files
  - deleting 1-47
  - displaying 1-18
  - renaming 1-47
- FILESELection parameter, SYS Service 58-7
- FileServerAddr parameter, SYS Service 58-7
- FIlter Service
  - creating an X.25 profile 23-6
  - debugging 23-2
  - displaying current configuration 23-1
  - masks
    - built-in 23-3
    - location options 23-5
    - user-defined 23-3
  - packets, filtering
    - forwarding, discarding 19-14, 23-2

- FIlter Service (continued)
  - policies
    - active, displaying 23-2
    - defining 23-6
    - statistics, flushing 23-6
  - station groups 23-10
- FilterAddrs parameter, IP Service 29-6
- FilterDefAction parameter, IP Service 29-10
- filtering
  - AppleTalk routing
    - entity 4-7, 4-9, 4-12
    - network number-based 4-7, 4-14
  - BGP routing 12-12
  - DECnet routing 17-15
  - IP routing 29-5, 29-6, 29-10
  - routing updates from trusted neighbors 47-12
- FILters parameter, Firewall Service 24-5
- FIlters parameter, IP Service 29-10
- FireWall Service
  - defining filters 24-5
  - parameter list 24-1
  - setting up logs 24-14
- firmware monitor 1-33
- firmware parameters
  - ARP Format A-15
  - Boot Device A-11, A-22
  - Boot Protocol A-14
  - Boot Sources A-5, A-17, A-24
  - Boot Statistics A-8, A-20, A-26
  - Config File Source A-13, A-22
  - Dump Destination A-5, A-18, A-25
  - I/O module A-14
  - IP Addresses A-3, A-15, A-23
  - Maximum Retries A-13
  - Primary and Secondary Boot Sources A-2, A-11, A-14, A-22
  - Self-test A-10, A-22
- FlowCtrlFrom parameter, TERM Service 61-11
- FlowCtrlTo parameter, TERM Service 61-11
- FLush command 1-26
- FlushTime parameter, ATMLE Service 8-5
- FlushVC parameter, TERM Service 61-12
- FORMAT command 1-26
- ForwardAddress parameter, UDPHELP Service 62-3
- ForwardDelay parameter, STP Service 57-3
- FORwards command 1-26
- ForwardTable parameter
  - DVMRP Service 20-5
  - MOSPF Service 37-4
- FR Service
  - compression 25-2
  - configuring public data network 25-5
  - dial recovery trigger 25-4
  - displaying current configuration 25-3
  - DLCI
    - displaying 25-1
    - status for ports 25-4
  - enabling
    - Line Management Interface (LMI) Protocol 25-3
  - keepalive packets 25-5
  - messages 25-5
- FR Service (continued)
  - neighbor addresses
    - BRidge Service 14-7
    - DECnet Service 17-14
    - DVMRP Service 20-7
    - RIPXNS Service 48-1
  - packet discard eligibility 25-3
  - PDN type, setting 25-5
  - troubleshooting 25-4
- FradMap parameter, DLSw Service 19-6
- FrameChars parameter, ATUN Service 9-4
- FrameCounts parameter, FDDI Service 22-3
- FrameErrorRatio parameter, FDDI Service 22-3
- FrameGap parameter, ATUN Service 9-5
- frames
  - FDDI
    - count 22-3
    - error ratio 22-3
    - SMT parameter management 22-7
  - source route bridging
    - All Route Explorer 56-5
    - maximum size for transmission 56-5
    - outgoing, minimum access priority 56-6
    - Spanning Tree Explorer 56-6
- FrameSeq parameter, LAPB Service 33-2
- FrameSize parameter, ATUN Service 9-5
- FrCopErrTh parameter, LNM Service 35-2
- FreqErrTh parameter, LNM Service 35-2
- FrToAtm command 1-27
- FSEInterval parameter, FR Service 25-5
- FTPIn parameter, Firewall Service 24-7
- FTPOut parameter, Firewall Service 24-8
- FTPSession parameter, Firewall Service 24-9
- full dump B-3
- Full Status Enquiry Message 25-5
- FullStatusFreq parameter, WE Service 64-3
- FunctionalAddr parameter, BRidge Service 14-8
- FunctionalUnit parameter, TERM Service 61-12

G

- Gateway Service
  - connection history 26-1
  - connection service requests, establishing 26-2
  - enabling gateway functions 26-2
  - incoming connections 26-2
  - outgoing connections 26-2
    - assigning IP addresses 26-3
    - configuring OSI P-Selectors 26-5
  - parameter list 26-1
  - X.25 subaddress
    - mapping to IP or PSAP 26-5
    - processing 26-2
  - X.25 to IP address mapping table 26-3
- GatewayControl parameter
  - DECnet Service 17-8
  - SR Service 56-3
- GatewayVRing parameter, SR Service 56-4
- GET command 1-27
- GetConfigFiles parameter, SYS service 58-7
- global and local switching. *See* XSWitch Service
- GLobalPARams parameter, SYS Service 58-8
- GopherIn parameter, Firewall Service 24-10
- GopherOut parameter, Firewall Service 24-10
- GREP parameter, Environment 2-2
- group ports 43-16
- GS/X25-XNS, call user data area 27-4

H

- H command B-2
- HangUp command 1-29
- hardware information, displaying
  - CPU 58-5
  - DPMs 58-6
  - I/O modules 58-8
- HeaderFormat parameter, VIP Service 63-3
- hello packets. *See* packets
- HelloPassWord parameter
  - ISIS Service 32-6
  - NLSP Service 38-6
- HelloTime parameter
  - DECnet Service 17-9
  - ISIS Service 32-6
  - OSPF Service 41-8
  - STP Service 57-3
- HelloTimeLan parameter, NLSP Service 38-6
- HelloTimeWan parameter, NLSP Service 38-7
- Help command B-2
- History, Environment parameter 2-3
- HoldTime parameter
  - ARP Service 6-2
  - BGP Service 12-11
  - ESIS Service 21-2
  - SR Service 56-4
- HoldTimeFactor parameter
  - NLSP Service 38-7
  - NRIP Service 39-6
  - SAP Service 49-5
- hops
  - in spanning tree algorithm 57-2
  - maximum
    - for All Route Explorer frames 56-5
    - for Spanning Tree Explorer frames 56-6
    - to reachable area and node 17-11
- HostMac parameter, SDLC Service 51-7
- HprTimer parameter, APPN Service 5-21
- HTTPIn parameter, Firewall Service 24-11
- HTTPOut parameter, Firewall Service 24-12

I

- I/O module
  - displaying messages 58-10
  - firmware parameter, NETBuilder II A-14
- IbmStatus parameter, BCN Service 11-2
- ICMP
  - echo request 1-40
  - generation of 29-12
  - request packets 29-12
  - Time Exceeded message 29-15

- ICMP parameter, Firewall Service 24-13
- ICMP Router Discovery Protocol. *See* RDP Service.
- ICMPGenerate parameter, IP Service 29-12
- ICMPReply parameter, IP Service 29-12
- IdleTimer parameter, ATUN Service 9-6
- IdleTimer parameter, TERM Service 61-12
- IDP Service
  - creating an X.25 profile 27-4
  - displaying current configuration 27-2
  - dynamic routes, flushing 27-1
  - enabling 27-2
  - packets, checksum 27-2
  - routing
    - over SMDS 27-4
    - over X.25 27-5
  - SMDS group address 27-4
  - static routes 27-3
    - deleting 27-1
    - displaying 27-1
  - X.25
    - call user data 27-4
    - protocol identifier 27-5
  - XNS. *See also* XNS routing
    - network number
    - routing table, displaying
- IEN name service 30-2
- IfDescr parameter, PORT Service 43-16
- IGMP Query message interval 36-2
- IISIS Service
  - default route cost 28-2
  - parameter list 28-1
  - routing protocol policy list 28-2, 28-3, 28-4
- ImportMetric parameter, RIPIP Service 47-8
- ImpSftErrTh parameter, LNM Service 35-3
- incoming connection requests, name resolver order 18-1
- incoming connections 30-2, 30-3
  - automatic
    - Rlogin connections, preventing 59-1
  - automatic and extended 26-2
  - extended
    - resuming next highest session 1-27
    - resuming preceding session 1-7
    - Rlogin connections, preventing 60-2
- IncomingSVCs parameter, X25 Service 65-2
- InFilter parameter, Firewall Service 24-13
- InitMacro parameter, TERM Service 61-13
- InsertedStatus parameter, FDDI Service 22-3
- InsertPolicy parameter, FDDI Service 22-3
- InStall command 1-29
- Integrated Intermediate System to Intermediate System. *See* IISIS Service
- InterAction, Environment parameter 2-3
- InterActTerm parameter, TERM Service 61-13
- Interface parameter, DLSw Service 19-6
- InterfaceStatus parameter, OSPF Service 41-8
- InterfaceType parameter, LAPB Service 33-2
- InteriorPolicy parameter
  - BGP Service 12-11
  - IISIS Service 28-3
  - OSPF Service 41-9
  - RIPIP Service 47-9
- Intermediate System Hello Protocol Data Units (ISH PDUs) 21-2
- InternalNET parameter, IPX Service 31-5
- Internet addresses. *See* IP addresses
- Internet Control Message Protocol. *See* ICMP
- Internet Datagram Protocol. *See* IDP Service
- Internet Packet Exchange Protocol. *See* IPX Service and SAP Service
- Internet Protocol Name Service. *See* IPName Service
- Internet Protocol. *See* IP Service
- InterNetRoute parameter, DECnet Service 17-9
- IOboardInfo parameter, SYS Service 58-8
- IP Addresses firmware parameter A-3, A-14, A-23
- IP addresses. *See also* IP Service
- IP addresses. *See* IP Service
- IP security. *See* IP Service
- IP Service
  - Address Translation Table 29-2 to 29-3
  - addresses
    - adding 29-2
    - connecting to 1-9
    - deleting 29-2
    - displaying 1-56, 29-3
    - mapping port to IP 29-15
    - SMDS group 29-23
    - subnet masks 29-14
  - configuring 29-5
  - creating an X.25 profile 29-23
  - description 29-1
  - displaying current global configuration 29-4
  - filters
    - creating 29-11
    - default action 29-10
    - deleting 29-11
    - enabling 29-5
    - policy 29-6
  - ICMP Protocol 29-12
  - ICMP Time Exceeded message 29-15
  - IP networks, configuring 29-13
  - load splitting 29-5
  - network traffic, restricting 29-6
  - packets
    - discarding 29-6
    - filtering 29-5, 29-6, 29-10
    - ICMP generation 29-12
    - ICMP replies 29-12
    - queue priority 29-15
    - source route 29-5
    - time-to-live 29-6
  - parameter list 29-1
  - routes
    - displaying 29-3
    - dynamic, flushing 29-3
    - static, adding 29-16
  - routing
    - over SMDS 29-23
    - over X.25 29-23
  - routing table
    - description 29-4
    - displaying 29-3, 29-16
- IP Service (continued)
  - security
    - classification level 29-22
    - enabling 29-5
    - for packets from file server 29-20
    - labels, adding strings to 29-22
    - labels, default 29-20
    - labels, system 29-21
    - options, additional 29-19
    - options, checking 1-53
    - protection authority flags 29-17, 29-18
  - X.25
    - LaPoste IP address-to-X.121 address conversion 29-12 to 29-13
    - protocol identifier 29-23
- IPName Service
  - addresses 30-3
  - database names, modifying 30-2
  - displaying current configuration 30-1
  - domain name
    - adding 30-2
    - clearing 30-1
    - configuring 30-2
    - displaying 30-1
  - IEN name server
    - primary 30-2
    - secondary 30-3
  - name service type 30-3
  - parameter list 30-1
- IpToDte command 1-30
- IPX Service
  - addresses
    - host to media address mapping, modifying 31-1
    - SMDS group 31-9
  - cost of path 31-4
  - creating an X.25 profile 31-11
  - default route 31-8
  - defining user profile over X.25 31-11
  - deleting static servers 31-9
  - diagnostics 31-4
  - displaying current configuration 31-3
  - enabling
    - IPX routing 31-3
    - load splitting 31-7
  - encapsulation formats 31-6
  - forwarding WAN broadcast packets 31-3
  - maximum hops under NLSP 31-5
  - NetWare server configuration information 1-38
  - network number 31-6
  - node connectivity 1-37
  - packet size 31-5
  - packets, WAN broadcast 31-4
  - parameter list 31-1
  - route discovery 1-37
  - router
    - internal network number 31-5
    - symbolic name 31-9
  - routing over
    - ATM 31-1
    - Frame Relay 31-1
    - SMDS 31-1, 31-9
    - X.25 31-1, 31-11

- IPX Service (continued)
  - routing table
    - adding static routes 31-7
    - displaying 31-2
    - flushing dynamic routes 31-2
  - server table 31-3
  - specifying gateways to reach servers 31-9
  - spoofing NCP KeepAliveRequest 31-10
  - spoofing on dial-on-demand lines 31-10
  - spoofing SPX watchdog packet 31-10
  - X.25, protocol identifier 31-11
- IPX25Map parameter, Gateway Service 26-3
- IS parameter, CLNP Service 16-3
- ISDN
  - addresses 42-13, 42-14
  - configuring
    - baud rate 42-2
    - date rate transfer 42-17
    - service profile identifiers and directory numbers 42-18, 42-19
    - switch type 42-20
  - TAs, specifying type 42-11
  - virtual ports, creating 43-30
- ISIS Service
  - addresses
    - IS area 32-3
    - multicast, Level 1 router 32-8
    - multicast, Level 2 router 32-8
    - neighbor 32-12
    - NSAP 32-3
    - NSAP, prefixes 32-13
    - SMDS group 32-14
  - current configuration, displaying 32-4
  - debugging 32-16
  - Designated Intermediate System (DIS) 32-5
  - enabling 32-4
  - Intermediate System (IS)
    - adjacencies 32-2
    - Level 1 or Level 2, designating 32-12
  - link state PDU database, displaying 32-10
  - load splitting 32-13
  - packets
    - CSNP, transmission interval 32-5
    - hello, DIS transmission interval 32-6
    - hello, IS transmission interval 32-6
    - hello, password 32-6
    - LSP 32-11, 32-12
    - maximum size, Level 1and 2 routing 32-7
    - PSNP, transmission interval 32-14
  - password
    - hello packet 32-6
    - Level 1 area 32-8
    - Level 2 backbone 32-8
  - port
    - cost, Level 1 and 2 router 32-7
    - priority, Level 1 and 2 router 32-9
  - routing
    - Level 1 and Level 2 32-4
    - over SMDS 32-14
- ISIS Service (continued)
  - routing table, displaying 32-9
  - SMDS interoperability between routers 32-15
  - stub network, enabling 32-5
  - system
    - ID 32-15
    - name 32-15
  - transit network, enabling 32-5
- ISRsessions parameter, APPN Service 5-22
- IVPrefix parameter, DECnet Service 17-10

K

- KATime parameter, FR Service 25-5
- KeepAliveInt parameter, WE Service 64-4
- KeepAliveLimit parameter, TCP Service 59-2
- KeepAliveTime parameter, TCP Service 59-3
- KeepAliveTime paramter, ATM Service 7-2, 8-4

L

- L1BufferSize parameter, ISIS Service 32-7
- L1DefaultMetric parameter, ISIS Service 32-7
- L1Multicast parameter, ISIS Service 32-8
- L1PassWord parameter, ISIS Service 32-8
- L1Priority parameter, ISIS Service 32-9
- L1Route parameter, ISIS Service 32-9
- L2BufferSize parameter, ISIS Service 32-7
- L2DefaultMetric parameter, ISIS Service 32-7
- L2Multicast parameter, ISIS Service 32-8
- L2PassWord parameter, ISIS Service 32-8
- L2Priority parameter, ISIS Service 32-9
- L2Route parameter, ISIS Service 32-10
- LAN emulation client 8-5
- lan emulation server 8-5
- LanType parameter, ATMLE Service 8-5
- LAPB Service
  - enabling 33-1
  - frames 33-2 to 33-3
  - parameter list 33-1
  - path interface type, DCE and DTE 33-2
- LaPosteDD parameter, IP Service 29-12
- LaPosteNN parameter, IP Service 29-13
- LaPostePort parameter, IP Service 29-13
- LaPostePP parameter, IP Service 29-13
- LaPostePRefix parameter, IP Service 29-13
- LargestFrameSize parameter
  - SR Service 56-5
- LAyout parameter
  - PATH Service 42-11
- LclNonIbmDlci parameter, BCN Service 11-2
- LCNs 65-2, 65-4
- LCTFailCount parameter, FDDI Service 22-3
- learned routes. *See* routes
- LEC. See LAN emulation client 8-5
- LECSAddr parameter, ATMLE Service 8-5
- LEMCount parameter, FDDI Service 22-3
- LES. See lan emulation server 8-5
- LESAddr parameter, ATMLE Service 8-5
- Level 1 router. *See* ISIS Service
- Level 2 router. *See* ISIS Service
- LFInsertion parameter, TERM Service 61-14
- LFPad parameter, TERM Service 61-14
- LifeTime parameter
  - RDP service 46-2
- LimitDataGrams parameter, DLSw Service 19-7
- LimitNBeXplorers parameter, DLSw Service 19-7
- LimitSnaeXplorers parameter, DLSw Service 19-7
- Line Management Interface (LMI) Protocol, enabling
  - FR Service 25-3
  - SMDS Service 53-1
- LineERase parameter, TERM Service 61-14
- LineType parameter, PATH Service 42-12
- Link Access Procedure Balanced Mode. *See* LAPB Service
- Link Control Protocol (LCP) 44-3
- Link Integrity Verification message 25-5
- Link State Advertisement. *See* LSA
- LinkCompStat parameter
  - PORT service 43-16
- LinkStaCHar parameter, APPN Service 5-23
- LinkStaCONT parameter
  - SNA Service 54-2
- LinkStaCONTrol parameter, APPN Service 5-25
- LinkStateData parameter
  - ISIS Service 32-10
  - NLSP Service 38-7
  - OSPF Service 41-10
- LIsten command 1-30
- listen mode 1-30
- LIStenerPorts parameter, TCPAPPL Service 60-1
- LLC2 Service
  - displaying current configuration 34-1
  - frames
    - information field length 34-3
    - maxium retransmittals 34-3
    - retransmission time 34-4
    - retransmit window size 34-5
  - parameter list 34-1
  - sessions
    - disconnecting inactive 34-4
    - displaying 34-3
  - tunnel connections
    - controlling 34-7
    - displaying current tunnel sessions 34-5
    - enabling 34-2
    - incoming request for 34-5
    - LLC2 over TCP/IP 58-4
    - MAC addresses for tunnel peer end station 34-6
    - packet priority 34-7
    - to peer network, enabling 34-5
    - tunnel peer address 34-7
    - virtual ring number 34-8
- LlcLOG parameter, LLC2 Service 34-2
- LLCService parameter, FDDI Service 22-4
- LMI Protocol
  - enabling FR Service 25-3
  - enabling SMDS Service 53-1

- LNM Service
  - Excessive Soft Error threshold 35-2
  - Frame Copied Error threshold 35-2
  - Frequency Error threshold 35-2
  - Impending Soft Error threshold 35-2
  - LAN Net Manager support
    - enabling and disabling 35-1
    - number of alternate managers 35-3
    - setting the password 35-4
  - Lost Frame threshold 35-3
  - Minimum Decrement Error threshold 35-3
  - Receiver Congestion Errors threshold 35-4
  - Receiver Congestion Table Full Error threshold 35-4
  - Soft Error Report Timer 35-4
  - Table Full Error threshold 35-5
  - Token Error threshold 35-5
- load splitting
  - in IP routing 29-5
  - in OSI routing 32-13
- local access control. *See* AC Service
- local and global switching. *See* XSWitch Service
- LocalAS parameter, BGP Service 12-12
- LocalDialNo parameter, PATH Service 42-13
- LocalEDit parameter, TERM Service 61-15
- LocalFacility parameter, AuditLog Service 10-2
- LocalGroups parameter, MIP Service 36-1
- LocalMac parameter, ATUN Service 9-6
- LocalNodeName parameter
  - APPN Service 5-27
  - SNA Service 54-2
- LocalNodeResist parameter, APPN Service 5-28
- LocalSap parameter, ATUN Service 9-6
- LocalSubAddr parameter
  - PATH Service 42-14
- Log parameter, Firewall Service 24-14
- logical channel numbers. *See* LCNs
- logical networks 43-16
- LogicalNET parameter, PORT Service 43-16
- LOGINs parameter, AC Service 3-2
- LOGout command 1-31
- LogServerAddr parameter, AuditLog Service 10-2
- loopback test 1-23
- LoopMode parameter, ATM Service 7-2
- LostFrTh parameter, LNM Service 35-3
- LSA
  - area, flooding 41-2
  - database, displaying 41-10
  - delay time 41-5
  - transmission interval 41-13
- LspBcastTime parameter, NLSP Service 38-8
- LspBroadcastTime parameter, ISIS Service 32-11
- LspMAxTime parameter
  - ISIS Service 32-11
  - NLSP Service 38-8
- LspMInTime parameter, NLSP Service 38-9
- LspRtxTime parameter
  - ISIS Service 32-12
  - NLSP Service 38-9

M

- MABR parameter, MOSPF Service 37-5
- MAC
  - addresses
    - reassigning to a CEC module 42-15
    - reassigning to a physical port 42-15
  - path type 22-2
  - ring management state 22-8
  - service data unit frame size 56-5
- MAC Address firmware parameter, SysconF command A-15
- MACAction parameter, FDDI Service 22-4
- MacAddrConvert command 1-31
- MacAddrDispMode parameter, SYS Service 58-8
- MacAddress parameter, PATH Service 42-15
- MacAddrFormat parameter, SYS Service 58-9
- MacCache parameter, DLSw Service 19-7, 19-8
- MACPlacement parameter, FDDI Service 22-4
- macros
  - bridge/router
    - cache 58-9
    - names 58-11
  - creating 1-12
  - deleting 1-64
  - displaying 1-56
  - event-based command/macro execution
    - displaying current configuration 50-2
    - enabling 50-2
    - specifying an event 50-3
  - executing 1-24
  - file contents 1-12
  - flushing 1-26
  - port initialization 61-13
  - strings, echoing 1-24
  - strings, transmitting 1-64
- MACros parameter, SYS Service 58-9
- MaintLineStateA parameter, FDDI Service 22-4
- MaintLineStateB parameter, FDDI Service 22-5
- MakeDir command 1-32
- MANager parameter, SNMP Service 55-2
- mapping
  - addresses. *See* addresses
  - IP to X.25 29-2
  - paths to ports 43-22
- mapping IP to
  - X.25 26-3
- MASK parameter, FIlter Service 23-2
- masks
  - defining 23-2
- MaxAge parameter, STP Service 57-4
- MaxAReaCost parameter, DECnet Service 17-11
- MaxAReaHops parameter, DECnet Service 17-11
- MaxAReaNumber parameter, DECnet Service 17-12
- MaxAreRDLimit parameter
  - SR Service 56-5
- MaxCost parameter, DECnet Service 17-12
- MaxData parameter
  - ATMLE Service 8-6
- MaxFrame parameter, LLC2 Service 34-3
- MaxHop parameter, IPX Service 31-5
- MaxHops parameter, DECnet Service 17-12
- Maximum Retries firmware parameter A-13
- MAxInterval parameter
  - RDP service 46-2
- MaxNodeNumber, DECnet Service 17-13
- MaxPeers parameter, BGP Service 12-12
- MaxPseudoAreas parameter, DECnet Service 17-13
- MaxRcvUnit parameter, PPP Service 44-2
- MaxResrcRteNmbr parameter, NRIP Service 39-6
- MaxRetry parameter
  - ATMLE Service 8-6
- MaxSegmentSize parameter, TCP Service 59-3
- MaxSessions parameter, TERM Service 61-15
- MaxSTeRDLimit parameter, SR Service 56-6
- MaxTRaceData parameter
  - DLSw Service 19-8
  - LLC2 Service 34-3
  - SDLC Service 51-7
- MaxUnkFrm parameter, ATMLE Service 8-6
- MaxUnkFtm parameter, ATMLE Service 8-7
- MaxVisits parameter, DECnet Service 17-15
- McastStats parameter, DLSw Service 19-9
- McastTcpIdle parameter, DLSw Service 19-9
- media access control. *See* MAC
- memory dump B-3
- MEnu command 1-32
- menus
  - accessing 1-32
  - Directory Manager 1-16
- messages
  - audit trail. *See* audit trail messages
  - I/O module, displaying 58-10
  - ICMP Router Advertisement
    - lifetime of 46-2
    - maximum interval between 46-2
    - minimum interval between 46-2
  - ICMP Router Solicitation 46-1
  - string text, transmitting 1-7
  - system, displaying 58-16
  - Time Exceeded 29-15
  - welcome string 58-19
- MEtric parameter, DVMRP Service 20-6
- Metric parameter, VIP Service 63-4
- MinAccessPrior parameter, SR Service 56-6
- MinDecErrTh parameter, LNM Service 35-3
- MInInterval parameter, RDP Service 46-2
- MIP Service
  - displaying current configuration 36-1
  - enabling 36-1
  - local group membership
    - IGMP query interval 36-2
    - registering 36-1
  - minimum threshold 36-3
  - multicast datagram TTL 36-3
  - prioritizing traffic 36-2
  - SMDS group address 36-3
- MLN 43-16
- MIpCONTrol parameter, PPP Service 44-3

MlpmaxrxRecUnit parameter, PPP Service 44-3
MlpSTATIstics parameter, PPP Service 44-3
MNEmonics parameter, FIlter Service 23-5
Mode parameter
    APPN Service 5-28
    SR Service 56-6
MOde parameter, DLSw Service 19-9
MODE parameter, ISIS Service 32-12
modems, DTR 1-14
ModetoCosMap parameter, APPN Service 5-28
modifying and displaying neighbors, RIP-IP 47-3
monitor
    boot B-1
    debug B-3
    firmware 1-33
MONitor command 1-33, B-3
monitor mode 1-34
MonitoredEvent parameter, FR Service 25-5
MOspf parameter, DVMRP Service 20-6
MOSPF Service
    displaying
        current configuration 37-1
        forwarding table 37-4
    enabling 37-1
    forwarding interarea multicast traffic 37-5
    policies
        advertising DVMRP sourced networks 37-3
        enabling inter-AS forwarding 37-5
        filtering destination group data packets 37-2, 37-6
MPMessages parameter, SYS Service 58-10
MRInfo command 1-35
MTraceRoute command 1-35
MTU parameter
    CLNP Service 16-4
    IPX Service 31-5
Multicast Internet Protocol. *See* MIP Service
multicast local group membership 36-2
Multicast Open Shortest Path First Service. *See* MOSPF Service
Multicast parameter, NLSP Service 38-10
Multicast8025 parameter, NLSP Service 38-10
MultiCastAddr parameter, BRidge Service 14-8
MulticastAddr parameter, DLSw Service 19-10
MulticastES parameter, ESIS Service 21-2
MulticastES8025 parameter, ESIS Service 21-2
multicasting, IP
    datagram bandwidth 20-9
    datagram TTL 36-3
    finding multicast-capable routers 1-35
    forwarding datagrams 37-1
    tracing a tree 1-36
MulticastIS parameter, ESIS Service 21-3
MulticastIS8025 parameter, ESIS Service 21-3
MulticastRetry parameter, DLSw Service 19-10
multiple logical networks 43-16

N

N2 parameter, LAPB Service 33-2
Name Binding Protocol. *See* NBP
NAME parameter
    DIR Service 18-1
    IPName Service 30-2
NAme parameter
    PATH Service 42-15
    PORT Service 43-17
Name parameter, UDPHELP Service 62-5
name resolution, defining resolution order 18-1, 40-3
name services. *See* IPName Service
NameCache parameter, DLSw Service 19-10, 19-11
names
    community 55-1, 55-2
    domain 30-1
    end system (ES) 32-15
    entity, AppleTalk 1-2
    intermediate system (IS) 32-15
    macro 58-11
    NBP 4-13, 4-14
    node 58-15
    path 42-15
    port 43-17
    router
        AppleTalk 4-17
        IPX 31-9
        VINES 63-5
    station group, changing 1-8
    symbolic 63-6
    X.500 directory, modifying 1-16
    zone, AppleTalk 4-20
NAmes parameter, AppleTalk Service 4-13
NameServiceType parameter, IPName Service 30-3
NameSourceOrder parameter, OSIAPPL Service 40-3
National Specific Facilities (NSF) 65-2
NBBcastResend parameter, DLSw Service 19-11
NBBcastTimeout parameter, DLSw Service 19-11
NBLocalAccess parameter, DLSw Service 19-11
NBP Name Table, displaying 4-13
NbpLookupTimer parameter, AppleTalk Service 4-14
NBRemAccess parameter, DLSw Service 19-12
NCS
    addresses 58-7
    audit trail messages on 58-4
NEBuilder II with DPE
    system configuration
        IP address setting A-3
neighbor
    addresses,adding 41-11
    adjacencies, directly connected 41-11
Neighbor parameter
    DECnet Service 17-14
    OSPF Service 41-10
    VIP Service 63-4
NEighbor parameter, DVMRP Service 20-7
NeighborRouter parameter, DVMRP Service 20-7
neighbors
    ATM
        BRidge Service 14-3
        IPX Service 31-1
        NLSP Service 38-10
        RIPIP Service 47-3
    DECnet 17-16
    DLCI, adding 14-7
    FDDI
        downstream 22-2
        port 22-7
        upstream 22-10
    FR, DVMRP Service 20-7
    IPX 31-1
    NRIP 39-2, 39-7
    OSPF 41-11
    RIP-IP 47-12
    SAP 49-2, 49-6
    static 41-11
    VIP 63-7
    X.25
        BRidge Service 14-14
        DECnet Service 17-14
        DVMRP Service 20-7
        IPX Service 31-1
        OSPF Service 41-11
        RIPXNS Service 48-1
        VIP Service 63-4
Neighbors parameter
    ISIS Service 32-12
    NLSP Service 38-10
NeighborStatus parameter, OSPF Service 41-11
NetAccess parameter, SYS Service 1-45, 58-10
NETaddr parameter, IP Service 29-13
NetAScii parameter, TERM Service 61-15
NETBuilder II
    firmware parameters. *See* firmware parameters
    virtual ports 61-2
NETBuilder II with DPE
    system configuration
        boot source A-2
        memory storage location A-5
        MP module software images A-8
        recovery options A-6
        serial ports baud rate A-1
NETBuilder with DPE
    system configuration
        statistics display A-8
NetEntityTitle parameter, CLNP Service 16-4
NetFilter parameter, AppleTalk Service 4-14
NetFilterType parameter, AppleTalk Service 4-15
NetMap packets 58-11
NetMAP parameter, SYS Service 58-10
NetMapTime parameter, SYS Service 58-11
NETnumber parameter
    IDP Service 27-2
    IPX Service 31-6
NetPolicyAll parameter, BGP Service 12-13
NetPolicyExt parameter, BGP Service 12-14
NetPolicyInt parameter, BGP Service 12-14

- NetPolicyPeer parameter, BGP Service 12-15
- NetRange parameter, AppleTalk Service 4-15
- NetWare Link Service Protocol. *See* NLSP Service
- NetWare Routing Information Protocol. *See* NRIP Service
- NetWare server configuration information 1-38
- NetwarePING command 1-37
- NetwareTraceRoute command 1-37
- NetwareView command 1-38
- network
  - devices, checking 1-38, 1-40
  - map, displaying 58-10
  - numbers
    - AppleTalk 4-15, 4-19
    - DECnet 17-15
    - IP 29-13
    - IPX 31-6
    - OSPF 41-7, 41-9, 41-13, 41-14
    - SMDS 53-2
    - VIP 63-1
    - XNS 27-3
  - statistics 58-14
- Network Control Protocol (NCP) 44-3
- Network Control Server. *See* NCS
- network management
  - community names 55-1, 55-2
  - macros 58-11
  - SNMP 55-1
  - system prompt 58-11
  - through remote 58-12
  - through Telnet 58-17
- Network Manager
  - password, setting 1-61
  - privilege level, setting 2-3
- NETwork parameter, DECnet Service 17-15
- NetworkFilter parameter, BGP Service 12-12
- NetZoneMapping parameter, AppleTalk Service 4-16
- NFS parameter, Firewall Service 24-15
- NLSP Service
  - addresses
    - area 38-2
    - multicast router addresses on Ethernet and FDDI networks 38-10
    - multicast router addresses on token ring networks 38-10
    - neighbor 38-10
  - adjacencies, displaying 38-1
  - areas
    - configuring 38-2
    - network capacity or cost 38-4
  - designated router priority 38-11
  - displaying current configuration 38-3
  - enabling and disabling 38-4
  - hello
    - interval of DIS router 38-5
    - passwords 38-6
    - transmission frequency on a LAN and a WAN 38-6
  - LSPs
    - broadcast rate for routing packets 38-8
    - database viewing 38-7
- NLSP Service (continued)
  - LSPs (continued)
    - maximum interval between regeneration 38-8
    - minimum interval between event-driven LSPs 38-9
  - names, assigning to interested systems 38-13
  - neighbor addresses 38-10
  - packets
    - CSNP routing packet transmissions 38-5
    - maximum rate on broadcast networks 38-8
    - routing packet size 38-3
  - parameter list 38-1
  - PSNP transmission frequency 38-11
  - server ID, specifying 38-12
  - tracing adjacency, LSP, SNP, DIS and hello events 38-13
- NMMacro parameter, SYS Service 58-11
- NMPrompt parameter, SYS Service 58-11
- NNtopology parameter, APPN Service 5-29
- NNTPIn parameter, Firewall Service 24-16
- NNTPOut paramter, Firewall Service 24-16
- node management 58-15, 58-16
- NodeType parameter, DECnet Service 17-15
- non-disruptive path switching (for APPN HPR) 1-40
- NORMalBandwidth parameter
  - PORT Service 43-17
- NRIP Service
  - default route, advertising 39-5
  - displaying current configuration 39-3
  - enabling 39-4
  - IPXWAN, enabling 31-4
  - neighbor list, defining
    - for receiving updates 39-7
    - for route and service reachability 39-2
  - NRIP updates 39-4, 39-5, 39-9
  - parameter list 39-1
  - policies
    - enabling, disabling 39-6
    - route advertisement 39-1
    - route receive 39-7
    - routes reported 39-8
    - service advertisement 39-1
    - service receive 39-7
- NSAP addresses
  - prefixes 17-10
  - structure 32-3
- NTP parameter, Firewall Service 24-17
- NumAltMgrs parameter, LNM Service 35-3

O

- object
  - adding to a set 1-1
  - deleting from list 1-13
- Open Shortest Path First. *See* OSPF Service
- Open Systems Interconnect. *See* OSI routing
- Open Systems Interconnection Applications. *See* OSIAPPL Service
- OPING command 1-38
- OpticalBypass parameter, FDDI Service 22-5
- or 30-1
- OSI routing
  - addresses, NSAP 32-3, 32-13
  - device, checking 1-38
  - ISIS Service parameters 32-1
  - tracing paths 1-39
- OSIAPPL Service
  - concatenating outgoing deliver PDUs 40-3
  - displaying
    - current configuration 40-1
    - OSI connection information 40-1
  - DSA address or name for X.500 40-2
  - DUA connections
    - abort time 40-3
    - status 40-2
  - name resolution, defining resolution order 40-3
  - parameter list 40-1
- OSPF parameter, Firewall Service 24-18
- OSPF Service
  - advertising networks into the OSPF domain 41-7
  - area addresses 41-2
  - area ranges 41-2
  - creating neighbor lists 41-4
  - demand interface circuit 41-6
  - displaying current configuration 41-3
  - enabling 41-3
  - link state advertisements (LSA)
    - advertising, summary of 41-2
    - area flooding 41-2
    - database 41-10
    - delay time 41-5
    - transmission interval 41-13
  - neighbor
    - addresses, adding 41-11
    - status 41-11
  - network numbers, adding to
    - exterior routing protocol policy list 41-7
    - interior routing protocol policy list 41-9
    - policy list 41-13
    - policy list of static routes 41-15
  - packets, hello transmission interval 41-8
  - parameter list 41-1
  - port
    - area ID 41-2
    - cost 41-4
    - delay time 41-5
    - password 41-13
    - status 41-9
  - router
    - adding, to virtual link list 41-16
    - designated 41-15
    - setting downtime interval 41-14
    - specifying an ID 41-14
  - routes
    - default, cost 41-5, 41-16
    - learned, by exterior routing protocols 41-7
    - learned, by interior routing protocols 41-9
  - routing table, reducing size of 41-2
  - tracing 41-5

- OTraceRoute command 1-39
- OutFilter parameter, Firewall Service 24-19
- outgoing connections, automatic and extended 26-2
- OutgoingSVCs parameter, X25 Service 65-2
- OverBlocked parameter, ARP Service 6-2
- OWNer parameter
  - PORT Service 43-19

P

- PaceMode parameter, MIP Service 36-2
- packets
  - AARP 4-2
  - acknowledgment 59-2
  - AskNeighbors 1-35
  - BOOTREQUEST
    - number of times to send 13-2
    - retransmission time 13-3
  - broadcast
    - AppleTalk Service 4-18
    - BRidge Service 14-4
    - LSP 32-11
    - NetMap 58-11
    - PSNP 32-14
    - RIP-XNS 48-3
    - UDPHELP Service 62-4
    - VIP Service 63-6
  - CLNP 16-4
  - CSNP 32-5
  - destination explicit forwarding and blocking 14-5
  - encapsulation
    - between Ethernet and FDDI 14-3
    - types 63-3
  - filtering
    - AppleTalk Service 4-9
    - Filter Service 23-1
    - IP Service 29-5, 29-6, 29-10
    - RIP-IP routing updates 47-12
  - hello
    - CBPDU 57-3
    - DECnet 17-8
    - DIS multicasts 32-6
    - ESH PDUs 21-3
    - IS multicasts 32-6
    - ISH PDUs 21-3
    - Level 1and 2, IS 32-8
    - NLSP 38-6
    - OSPF 41-8
    - password 32-6
  - ICMP generation 29-12
  - keepalive
    - enabling/disabling 59-2
    - FR Service 25-5
    - transmission quantity 59-2
  - prioritizing WAN packets
    - with DefaultPriority parameter 43-6
  - request
    - ARP 6-2, 6-4
    - echo, AppleTalk 1-4
    - ICMP 29-12
    - RIP-IP 47-4
  - time-to-live
    - CLNP Service 16-2
    - IP Service 29-6
    - MIP Service 36-3
- packets (continued)
  - transmission
    - error statistics 1-22
    - testing 1-19
  - update
    - DECnet 17-17
    - DVMRP 20-10
    - ES-IS 21-3
    - NRIP 39-9
    - RIP-IP 47-4, 47-13
    - RIP-XNS 48-2, 48-3
    - SAP 49-8
    - VIP RTP 63-7
  - WAN broadcast
    - IPX 31-3
    - NRIP 39-4
    - SAP 49-4, 49-5
  - X.25 protocol identifier. *See* X.25
- Pad parameter
  - PATH Service 42-16
- PadSession parameter, Gateway Service 26-4
- parameters
  - default values
    - displaying 1-57
    - setting 1-53
  - values
    - copying 1-43
    - displaying 1-54
    - saving 1-50
    - setting 1-53
    - storing 1-60
- PARAmeters parameter, TERM Service 61-16
- parity bit value
  - appended to each character transmitted on asynchronous path 42-22
- PARity parameter
  - PATH Service 42-17
- PARity parameter, PATH Service 42-16
- PARIty parameter, TERM Service 61-16
- Partial Sequence Number PDU (PSNP), transmitting 32-14
- PassWord command 1-39
- PassWord parameter
  - LNM Service 35-4
  - OSPF Service 41-13
- passwords
  - changing 1-39
  - invalidating 1-25
  - Level 1 and 2 32-8
  - port, OSPF 41-13
  - setting 1-61
  - tunnel 66-2
- PATH Service
  - bandwidth-on-demand aggregation 42-8
  - configuring 42-6
  - continuous flags, sending 42-21
  - data bits, received and transmitted 42-7
  - dial-up lines
    - communications status, displaying 42-10
    - device type connected to the path 42-11
    - dial pool status, displaying 42-10
    - line type, setting 42-12, 42-17
- PATH Service (continued)
  - dial-up lines (continued)
    - path attributes 42-8
    - transmission encoding method, displaying 42-10
    - wait for carrier signal 42-7
  - disaster recovery paths 42-8
  - Ethernet controller chip, reset 42-19
  - graphical layout, displaying 42-11
  - ISDN lines
    - baud rate 42-2
    - setting HDLC lines for 42-16
  - Local Address Administration (LAA)
    - reassigning a CEC module MAC address 42-15
    - reassigning a physical port's MAC address 42-15
  - modem type 42-9
  - name, assigning to path 42-15
  - packets
    - Ethernet, compressing 42-21
    - stay alive, transmission interval 42-20
  - parameter list 42-1
  - serial lines
    - baud rate 42-2
    - connector type 42-5
    - setting HDLC flags for 42-16
    - transmit clock 42-2, 42-3
  - setting the baud rate 42-2
  - TA type 42-11
  - unbind a static path from a port 42-8
  - unrestricted path 42-9
  - V.25bis command format 42-4
- PathCost parameter, STP Service 57-4
- PathPreference parameter
  - PORT Service 43-21
- paths
  - cost, STP bridging 57-4
  - dial-up
    - connecting 1-14
    - disconnecting 1-29
  - ID 22-4
  - mapping to ports 43-22
  - tracing 1-39, 1-63
  - type and MAC 22-2
- PAths parameter, PORT Service 43-22
- PathSplit parameter
  - IPX Service 31-7
  - ISIS Service 32-13
- PathSwitch command 1-40
- PathTest 22-9
- Patricial Tree Memory 39-6
- PAuse command 1-40
- PCallTmr parameter, SDLC Service 51-8
- PCConnectState parameter, FDDI Service 22-5
- PCControlA parameter, FDDI Service 22-6
- PCControlB parameter, FDDI Service 22-6
- PCMState parameter, FDDI Service 22-6
- PCONFig parameter, SDLC Service 51-8
- PCONtrol parameter, SDLC Service 51-8
- PDatMode parameter, SDLC Service 51-8
- PDNetworkType parameter, X25 Service 65-3
- PDNtype parameter, FR Service 25-5

- PEER parameter, BGP Service 12-16
- PEer parameter, DLSw Service 19-12
- PEer parameter, SHDlc Service 52-1
- PeerAS parameter, BGP Service 12-16
- PeerControl parameter, BGP Service 12-17
- PeerIpAddress parameter, BGP Service 12-17
- PeerMacAdd parameter, DLSw Service 19-13
- PeerMetric parameter, BGP Service 12-17
- PeerNBName parameter, DLSw Service 19-13, 19-14
- PeerVersion parameter, BGP Service 12-18
- PeerWeight parameter, BGP Service 12-18
- permanent virtual circuits. See PVCs 65-3
- PermVirCircuit parameter, ATM Service 7-2
- PhantomPower parameter
  - PATH Service 42-17
- physical connection management (PCM) state 22-6
- PING command 1-40
- PMaxData parameter, SDLC Service 51-9
- PMaxOut parameter, SDLC Service 51-4
- PMF parameter, FDDI Service 22-7
- PMODulo parameter, SDLC Service 51-9
- Point-to-Point Protocol. *See* PPP Service
- policy list, OSPF Service 41-7, 41-9, 41-13
- POLicy parameter, FIlter Service 23-6
- PolicyControl parameter
  - DECnet Service 17-15
  - DVMRP Service 20-8
  - MOSPF Service 37-5
  - NRIP Service 39-6
  - SAP Service 49-5
- polled asynchronous communication. *See* ATUN Service
- POPIn parameter, Firewall Service 24-19
- POPOut parameter, Firewall Service 24-20
- PORT 43-25
- port groups 43-16
- PORT Service
  - address formats, matching to end systems 43-23
  - bandwidth increment limit 43-2
  - bandwidth-on-demand
    - allocating maximum 43-2
    - threshold 43-3
  - bandwith assignment
    - to packets transmitting from WAN port 43-25
  - compression
    - statistics 43-16
    - types of 43-3
  - current configuration, displaying 43-4
  - dial control state
    - call indicator, bandwidth management mode 43-9
    - call receiver 43-12
  - dial-up lines
    - attributes 43-8
    - bandwidth-on-demand status 43-15
    - bandwidth-on-demand threshold 43-3
    - configurations 43-6
    - connecting paths 43-2
    - dial number list 43-10
    - dial path resources 43-22

- PORT Service (continued)
  - dial-up lines (continued)
    - dial status 43-14
    - dial-on-demand status 43-14
    - disaster recovery status 43-15
    - dynamic dial path usage preference 43-21
    - idle time before disconnect 43-9
    - manual dial status 43-15
    - number of retries 43-12
    - PPP virtual ports 43-31
    - time between samples 43-13
    - time-stamped dial history 43-9
    - wait before connect, disconnect 43-8
    - wait before retry 43-13
  - displaying WAN queue statistics for protocol reservation 43-29
  - enabling 43-5
  - group ports 43-16
  - logical networks 43-16
  - packets
    - controlling medium- and low-priority packets 43-29
    - default priority 43-5
    - displaying queue priority for IP and LLC2 43-28
    - forwarding ratio, setting 43-25, 43-27
    - queue, setting 43-28
  - parameter list 43-1
  - ports
    - configuring groups 43-16
    - configuring queueing 43-27
    - configuring virtual ports 43-30
    - mapping paths to 43-22
    - naming 43-17
    - ownership 43-19
    - SNMP MIB object IfDescr 43-16
  - setting bandwidth automatically 43-17
  - troubleshooting 43-6
- PortCHar parameter, APPN Service 5-29
- PortCONFig parameter, ATUN Service 9-6
- PortCONTrol parameter
  - APPN Service 5-30
  - ATUN Service 9-7
  - SNA Service 54-2
- PortCU parameter, ATUN Service 9-8
- PortCU parameter, SDLC Service 51-10
- PortDef parameter
  - APPN Service 5-31
  - SNA Service 54-2
- PortGroup parameter, DLSw Service 19-14
- PortNeighbor parameter, FDDI Service 22-7
- PortPArams parameter, STP Service 57-5
- PortPriority parameter, STP Service 57-5
- ports
  - buffer size 61-7
  - configuration files
    - copying 1-43
    - deleting 1-65
    - parameter values, saving 1-50, 1-61
  - configuring queueing 43-27

- ports (continued)
  - cost
    - DECnet Service 17-8
    - DVMRP Service 20-6
    - ISIS Service 32-7
    - OSPF Service 41-4
    - VIP Service 63-4
  - defining for APPN 5-31
  - dial-up
    - connecting 1-14
    - disconnecting 1-29
  - enabling 43-5
  - group 43-16
  - initializing 61-2, 61-13
  - interface type 33-2
  - interfaces, obtaining path cost 57-4
  - mapping dynamic paths to 43-22
  - mapping static paths to 43-22
  - numbers 2-1
  - PAD, displaying session information 26-4
  - priority
    - ISIS Service 32-9
    - SR Service 56-6
    - STP Service 57-5
  - status
    - DECnet Service 17-19
    - FR Service 25-4
    - OSPF Service 41-8
    - PPP Service 44-3
    - VIP Service 63-6
    - X25 Service 65-3
  - virtual 61-2
  - with name tags
    - to assign bandwidth to packets 43-25
- PortZone parameter, AppleTalk Service 4-16
- PPP Service
  - authentication interval time 44-2
  - CHAP, selecting 44-1
  - displaying current configuration 44-2
  - enabling MLP 44-3
  - maximum packet length 44-3
  - MLP-related statistics 44-3
  - packets, maximum size 44-2
  - PAP
    - assigning userid/password 44-1
    - controlling access to central host 44-2
    - selecting 44-1
  - parameter list 44-1
- PreferredServer parameter, SAP Service 49-5
- PrefixRoute parameter, ISIS Service 32-13
- Presentation Service Access Point (PSAP) 40-2
- PRetryTimer parameter, SDLC Service 51-10
- Primary and Secondary Boot Sources firmware parameter A-2, A-11, A-22
- PrimaryMAC parameter
  - ATMLE Service 8-7
- PrimaryNameServer parameter, IPName Service 30-3
- prioritizing WAN packets
  - with DefaultPriority parameter 43-6

- PRIOrity parameter
  - DECnet Service 17-16
  - NLSP Service 38-11
- PRiorityCRiteria parameter, DLSw Service 19-14
- PRioritySTATistics parameter, DLSw Service 19-15
- PRioSTATistics parameter, DLSw Service 19-15
- PRirorityCRiteria parameter, DLSw Service 19-14
- privilege level, setting 2-3
- PRIvilege, Environment parameter 2-3
- PROFile parameter, TERM Service 61-16
- PROFile Service
  - call setup parameters 45-4
  - charge reversal 45-6
  - data compression type 45-3
  - number of bytes per packet 45-5
  - parameter list 45-1
  - specifying
    - a set of users 45-3
    - default rate 45-7
    - maximum number of virtual circuits 45-7
    - National Specific Facilities 45-5
    - number of packets queued 45-7
    - packet size 45-6
    - time before clearing a VC 45-8
  - user profile, naming 45-6
  - window size 45-8
  - X.25 profile 45-2
- ProfileID parameter, PROFile Service 45-2
- ProFiles parameter, WE Service 64-4
- PROle parameter, SDLC Service 51-10
- prompt
  - Network Manager 58-11
  - Remote 1-45
  - user privilege 58-11
- PROMpt parameter, SYS Service 58-12
- ProtMacAddrFmt parameter
  - PORT Service 43-23
- Protocol Data Units (PDUs)
  - concatenating outgoing deliver 40-3
- protocol identifier. *See* X.25
- protocol reservation
  - IP filtering procedure
    - IP FilterAddrs parameter, PROTocolRsrv= action option 29-8
  - IP packet filtering policy 29-6
  - mnemonic filtering 23-6
  - name tags to assign bandwidth to packets 43-25
  - -PORT PROTocolRsrv parameter syntax 43-25
  - reserving bandwidth rules 43-25, 43-26
  - setting bandwidth percentage 43-25
  - WAN queue statistics displays 43-29
- PROTocolRsrv 23-7, 29-8
- PROTocolRsrv parameter, PORT Service 43-25
- prune 20-9
- Prune parameter, DVMRP Service 20-9
- PSelX25Map parameter, Gateway Service 26-5
- PseudoAreaPrefix parameter, DECnet Service 17-16
- PsnpTime parameter
  - ISIS Service 32-14
  - NLSP Service 38-11
- PT1Retry parameter, SDLC Service 51-11
- PT1Timer parameter, SDLC Service 51-11
- PUStatus parameter, SNA Service 54-3
- PUT command 1-41
- PutDump command 1-42
- PVC parameter, X25 Service 65-3
- PVCs
  - configured on LCNs to DTE address 65-3
  - traffic over dual Frame Relay 11-2, 11-3

Q

- QueryInterval parameter, MIP Service 36-2
- QueueCONTrol 43-27
- QueueCONTrol parameter
  - PORT Service 43-27
- QueueInterLeave parameter
  - PORT Service 43-25, 43-27
- QueuePriority parameter
  - APPN Service 5-33
  - IP Service 29-15
  - PORT Service 43-28
- QueueStatistics parameter
  - PORT Service 43-29
- QueueStatistics parameter, PORT Service 43-29
- QueueThrottle parameter, PORT Service 43-29

R

- RA command B-3
- RarpClientState parameter, ARP Service 6-2
- RarpCONTrol parameter, ARP Service 6-3
- RateAdaption parameter, PATH Service 42-17
- RateLimit parameter, DVMRP Service 20-9
- RB command B-4
- RBCS
  - addresses 58-7
  - audit trail messages 58-4
  - booting from 58-7
- RcvCnTFErrTh parameter, LNM Service 35-4
- RcvConErrTh parameter, LNM Service 35-4
- RcvFromNeighbor parameter
  - DECnet Service 17-16
  - NRIP Service 39-7
  - RIPIP Service 47-9
  - SAP Service 49-6
- RcvSubnetMask parameter, RIPIP Service 47-11
- RDgeneration parameter, CLNP Service 16-4
- RDP Service
  - default router 46-3
  - disabling 46-1
  - enabling 46-1
  - IP broadcasted packets 46-1
  - multicasted packets 46-1
  - participating routers, selecting 46-3
- RDP Service (continued)
  - Router Advertisement message
    - lifetime of 46-2
    - maximum interval between 46-2
    - minimum interval between 46-2
  - Router Solicitation message 46-1
  - timers 46-2
  - verifying configuration 46-1
- ReaD command 1-43
- ReassemblyTime parameter, IP Service 29-15
- ReBoot command 1-44
- Reboot command B-4
- ReceivePolicy parameter
  - DECnet Service 17-17
  - NRIP Service 39-7
  - OSPF Service 41-13
  - RIPIP Service 47-12
  - SAP Service 49-7
- ReceiveWindow parameter, LLC2 parameter 34-3
- Recovery Action command B-3
- RemDisconnect parameter, FDDI Service 22-7
- RemNonIbmDlci parameter, BCN Service 11-3
- REMote command 1-44, 58-12
- Remote Disconnect Flag 22-8
- RemoteAddress parameter, IP Service 29-15
- RemoteLanType parameter
  - BCN service 11-3
- RemoteMac parameter, ATUN Service 9-9
- RemoteManager parameter, SYS Service 1-45, 58-12
- RemoteSap parameter, ATUN Service 9-9
- RemoveDir command 1-46
- RemoveFile command 1-47
- ReName command 1-47
- ReprintLine parameter, TERM Service 61-17
- RequestFormat parameter, ARP Service 6-4
- RequestStatus parameter, BOOTPC Service 13-2
- RESolutionOrder parameter, DIR Service 18-1
- RESTart command 1-48
- RESume command 1-48
- RetransmitLimit parameter, TCP Service 59-3
- RetransmitTime parameter, OSPF Service 41-13
- RetryCount parameter
  - BOOTPC Service 13-2
  - LLC2 Service 34-3
- RetryInterval parameter
  - BOOTPC Service 13-2
- ring speed 42-2
- RingNumber parameter, SR Service 56-7
- RIP parameter, Firewall Service 24-21
- RIPIP Service 47-1
  - addresses
    - adding to and deleting from a trusted neighbor list 47-10
    - directed or limited broadcast 47-5
  - configuring 47-4
  - displaying current configuration 47-4

RIPIP Service (continued)
- filtering
  - routing updates from trusted neighbors 47-12
  - static routes 47-12
- packets 47-4, 47-5
- policies
  - exterior 47-6
  - interior 47-9
  - network 47-1
  - receive 47-12
  - static route 47-12
- routes
  - advertised, displaying 47-1
  - aging time 47-13
  - default, cost 47-6
  - expiration time 47-13
  - imported, cost conversion formula 47-8
  - learned by BGP 47-6
  - learned by EGP 47-6
  - learned by OSPF 47-9
- routes, adding to
  - advertise policy list 47-2
  - exterior policy list 47-7
  - interior policy list 47-9
  - receive policy list 47-12
- routes, deleting from
  - advertise policy list 47-2
  - exterior policy list 47-7
  - interior policy list 47-9
  - receive policy list 47-12
- split horizon with poison reverse 47-5
- unnumbered links 47-5
- update Frame Relay, X.25, or ATM neighbor list 47-6
- variable length subnet masks
  - aggregate/deaggregate scheme 47-5
  - range table mask scheme 47-11

RIPXNS Service
- configuring 48-2
- displaying current configuration 48-2
- neighbor addresses, adding 48-1
- packets
  - broadcast, transmission interval 48-3
  - trigger update 48-2
  - update, to neighbors 48-1
- parameter list 48-1

RLOGin command 1-49

Rlogin connections
- from PAD-attached terminal 1-49
- preventing 60-2
- TCP 1-49

RLogSendName parameter, TCPAPPL Service 60-2

RMTState parameter, FDDI Service 22-8

Role parameter, BSC Service 15-3

ROUte parameter
- BGP Service 12-18
- BRidge Service 14-8
- IDP Service 27-3
- IP Service 29-16
- IPX Service 31-7
- SR Service 56-7

RouteAgingTime parameter, AppleTalk Service 4-17

RouteDiscovery parameter, SR Service 56-8

router
- address 17-2, 63-1
- adjacencies 38-1
- adjacent 32-2
- default 46-3
- designated
  - on Ethernet 17-16
  - OSPF 41-15
- name 4-17, 63-5

Router Discovery Protocol service. *See* RDP service.

RouterDeadTime parameter, OSPF Service 41-14

RouterID parameter, OSPF Service 41-14

RouterList parameter
- RDP service 46-3

RouterName parameter
- AppleTalk Service 4-17
- IPX Service 31-9

ROUTerPriority parameter, OSPF Service 41-15

routes
- aggregation
  - BGP 12-2
  - DVMRP 20-2
  - RIPIP 47-5
- cost
  - DVMRP Service 20-6
  - OSPF Service 41-5, 41-9, 41-16
  - RIPIP Service 47-2, 47-6, 47-7, 47-9, 47-12, 47-13
- discovering 1-17
- displaying
  - AppleTalk Service 4-6
  - BGP Service 12-18
  - BRidge Service 14-2
  - DECnet Service 17-7
  - IDP Service 27-1, 27-3
  - IP Service 29-3
  - IPX Service 31-2, 31-7
  - ISIS Service 32-9, 32-10
  - SR Service 56-1
  - VIP Service 63-2
- learning
  - AppleTalk Service 4-8
  - BRidge Service 14-6
  - IP, with BGP 47-6
  - IP, with EGP 47-6
  - IP, with OSPF 41-7, 41-9, 47-9
  - SR Service 56-2
- tracing 1-63

RouteTable parameter, DVMRP Service 20-9

RouteTableSize parameter, BRidge Service 14-11

RouteUpdateTime parameter, AppleTalk Service 4-18

routing
- AppleTalk 4-1
- DECnet 17-1
- IP 29-1
- IPX 31-1
- OSI 21-1, 28-1
- PPP 44-2

routing (continued)
- SMDS 53-1
- VINES 63-1
- XNS 27-2

Routing Information Protocol for IP. *See* RIPIP Service

Routing Information Protocol for XNS. *See* RIPXNS Service

RoutingTime parameter, DECnet Service 17-18

ROWs parameter, TERM Service 61-17

RptStationHop parameter, BRidge Service 14-12

RTP parameter, APPN Service 5-33

RTPStats parameter, APPN Service 5-34

RtrName parameter, VIP Service 63-5

RTS signal control
- DUplex parameter 42-10

RxParity parameter
- PATH Service 42-18

RxParity parameter, PATH Service 42-18

RZ command 1-50

S

SampleOption parameter, SYS Service 58-12

SampleTime parameter, SYS Service 58-13

SAP Service
- advertising services 49-1
- age out time 49-5
- displaying current configuration 49-3
- enabling 49-4, 49-5
- neighbor list, defining
  - for receiving updates 49-6
  - for route and service reachability 49-2
- packets, WAN broadcast 49-4
- parameter list 49-1
- policies
  - enabling, disabling 49-5
  - route receive 49-7
  - service receive 49-7
- preferred server 49-5
- server 49-2
- updates
  - Auto 49-4
  - controlling 49-4
  - transmission interval 49-8

SAve command 1-50

SAVEbgp command 1-52

SavedParams parameter, TERM Service 61-17

SCH Service
- daily schedule
  - displaying 50-4
  - events, assigning to day or date 50-1
  - modifying 50-3
- displaying current configuration 50-1
- enabling scheduling 50-2
- event-based command/macro execution
  - displaying current configuration 50-2
  - enabling 50-2
  - specifying an event 50-3
- parameter list 50-1

scoping 20-3
ScreenLength, Environment parameter 2-4
SDLC Service, parameter list 51-1
SdlcAdjLinkSta parameter, APPN Service 5-35
SdlcDlurLinkSta parameter, APPN Service 5-37
SdlcLinkSta parameter, SNA Service 54-3
SdlcLOG parameter, SDLC Service 51-11
SecAuthIn parameter, IP Service 29-17
SecAuthOut parameter, IP Service 29-18
SecCheck command 1-52
SecCONTrol parameter, IP Service 29-19
SecFileServer parameter, IP Service 29-20
SecLabelDefault parameter, IP Service 29-20
SecLabelSys parameter, IP Service 29-21
SecLabelValues parameter, IP Service 29-21
SecLabelXtra parameter, IP Service 29-22
SecLEVel parameter, IP Service 29-22
SecondaryNameServer parameter, IPName Service 30-3
security
- for bridges 14-7, 14-13
- IP 29-5

Self-test firmware parameter A-10, A-22
serial lines
- baud rate 42-2
- clock 42-3

SERver parameter, IPX Service 31-9
sessions
- changing current 1-58
- connection commands
  - Connect 1-9
  - RLOGin 1-49
  - TELnet 1-62
  - VTp 1-66
- disconnecting
  - multiple 1-30, 1-31
  - single 1-16
- displaying
  - all 61-18
  - LAN side 61-4
  - LLC2 34-3
- idle time 61-4
- initializing 61-2
- resuming
  - current 1-48
  - next highest 1-27
  - preceding 1-7
- switching 1-58

SESSions parameter, LLC2 Service 34-3
SESsions parameter, TERM Service 61-18
SET command 1-53
SETDefault command 1-53
SftErrRptTimer parameter, LNM Service 35-4
SHDlc Service, PEer parameter 52-1
SHow command 1-54
SHowDefault command 1-57
Simple Network Management Protocol. *See* SNMP Service
SMDS Service 53-1
- assigning SMDS individual address 53-2
- displaying current configuration 53-1
- Line Management Interface (LMI) Protocol, enabling 53-1
- Subscriber Network Interface address 53-2

SMDSGroupAddr parameter
- AppleTalk Service 4-18
- BRidge Service 14-12
- DECnet Service 17-19
- IDP Service 27-4
- IP Service 29-23
- IPX Service 31-9
- ISIS Service 32-14
- MIP Service 36-3
- SMDS Service 53-2
- VIP Service 63-5

SMDSID parameter, ISIS Service 32-15
SMDSIndivAddr parameter, SMDS Service 53-2
SMT
- addresses
  - displaying 22-8
  - in FDDI station ID 22-10
- version, setting 22-8

SMTAddress parameter, FDDI Service 22-8
SMTPIn parameter, Firewall Service 24-22
SMTPOut parameter, Firewall Service 24-23
SMTVersion parameter, FDDI Service 22-8
SNA
- DLCI for traffic over dual Frame Relay PVCs 11-3
- traffic over dual Frame Relay PVCs 11-2

SNA Service
- activating and deactivating a link station 54-2
- activating and deactivating an SNA port 54-2
- configuration display 54-1
- default PU definition 54-1
- defining SNA ports 54-2
- local node name definition 54-2
- log display 54-4
- parameter list 54-1
- PU status display 54-3
- SDLC link station definition 54-3
- SSCP link station definition 54-5

SnaAlertstoTraps parameter, DLSw Service 19-16
SnaLocalAccess parameter, DLSw Service 19-16
SNaLOG parameter, SNA Service 54-4
SnaRemAccess parameter, DLSw Service 19-17
SnaTopoCollect parameter, DLSw Service 19-18
SnaTopoDisplay parameter, DLSw Service 19-18
SNMP parameter, Firewall Service 24-24
SNMP Service 55-1
- community name
  - manager list 55-2
  - modifying 55-1
- configuring 55-2
- traps, generating 55-2

software version number, displaying 58-18
source route bridging, reducing broadcast traffic 14-4
source route packets, in IP routing 29-5
Source Route. *See* SR Service
Spanning Tree Explorer frames 56-6
Spanning Tree Explorer. *See* STE

Spanning Tree Protocol. *See* STP Service
Specifies 29-8
SPIDdn1 parameter, PATH Service 42-18
SPIDdn2 parameter, PATH Service 42-19
SPoofCONTrol parameter, IPX Service 31-10
SpyRing command 1-58
SR Service
- bridge number 56-2
- configuration error display 56-3
- displaying current configuration 56-3
- encapsulation tracking 56-4
- end system source routing, enabling 56-8
- frames
  - All Route Explorer, RD limit 56-5
  - maximum size for MAC service data unit 56-5
  - outgoing, minimum access priority 56-6
  - Spanning Tree Explorer, RD limit 56-5
- LAN ID for port 56-7
- packet translation modes 56-3
- port ring number 56-7
- ring number for transparent bridge packets 56-4
- route discovery for end system packets 56-8
- routes
  - displaying
    - all 56-1
    - SRT 56-2
  - flushing 56-1
  - inactive entries hold time 56-4
  - learned source routes, flushing 56-10
  - static, adding 56-7
- routes, displaying
  - discovered 56-2
  - learned source 56-10
  - static 56-2
  - static, for remote end station 56-7
- source route bridging
  - enabling 56-9
  - mode, setting 56-6
- Source Route Transparent bridge mode 56-1

SrcRouBridge parameter, SR Service 56-9
SRcSecurity parameter, BRidge Service 14-13
SRTG 56-3, 56-4
SscpLinkSta parameter, SNA Service 54-5
StartupNET parameter, AppleTalk Service 4-19
StartupNODe parameter, AppleTalk Service 4-19
static routes
- adding, deleting, and displaying 31-7
  - OSPF Service 41-15
  - RIPIP Service 47-12
  - SR Service 56-7

StaticPolicy parameter
- IISIS Service 28-4
- OSPF Service 41-15
- RIPIP Service 47-12

- Station Management. *See* SMT
- StationAction parameter, FDDI Service 22-9
- StationCONFig parameter, FDDI Service 22-9
- StationGroup parameter, FIlter Service 23-9
- StationID parameter, FDDI Service 22-10
- statistics
  - boot A-8, A-20, A-26
  - displaying 58-14
  - flushing 58-14
  - sampling time 58-13
- STATistics parameter, SYS Service 58-14
- Status Enquiry Messages 25-5
- STATUS parameter
  - ATMLE Service 8-7
  - DECnet Service 17-19
  - PPP Service 44-3
  - VIP Service 63-6
  - X25 Service 65-3
- StayAliveAction, PATH Service 42-19
- StayAliveTimer parameter
  - PATH Service 42-20
- StayAliveTimer parameter, PATH Service 42-19
- STE 56-5
- stop bits
  - determining stop bits appended to character
    - on asynchronous path 42-20
- StopBits parameter
  - PATH Service 42-20
- StopBits parameter, PATH Service 42-20
- STP Service 57-1
  - displaying current configuration 57-2
  - enabling 57-2
  - hops 57-3
  - multicast address restrictions 57-1
  - multicast MAC address 57-1
  - path cost 57-5
  - port
    - identifier priority field 57-5
    - parameters, displaying 57-5
    - wait before changing states 57-3
  - root bridge
    - identifier priority field 57-2
    - interval to transmit CBPDU 57-3
    - maximum wait time for CBPDU 57-4
- strings
  - echoing in macros 1-24
  - transmitting 1-64
- StubDefaultMetric parameter, OSPF Service 41-16
- SubAddrMap parameter, Gateway Service 26-5
- subdirectories
  - creating 1-32
  - removing 1-46
- subnet masks, RIPIP variable length
  - aggregate/deaggregate scheme 47-5
  - range table mask scheme 47-11
- Subnetwork Access Protocol (SNAP) packet encapsulation 63-3
- Subscriber Network Interface address 53-2
- SuppressDM parameter, SDLC Service 51-11
- SWitch command 1-58
- Switched Multimegabit Data Service. *See* SMDS Service
- SWitchedVC parameter, XSWitch Service 66-1
- SwitchTime parameter, ATMLE Service 8-7
- SwitchType parameter, PATH Service 42-20
- SymbolicNames parameter, VIP Service 63-6
- SYNRetrys parameter, TCP Service 59-3
- Syntax 6-1
- SYS Service
  - accessing bridge/router 58-10
  - addresses
    - bridge/router, broadcast interval 58-11
    - MAC 58-2, 58-8, 58-9
    - NCS 58-7
    - RBCS 58-7
  - audit trail message, time/date stamp format 58-4
  - clock, setting 58-5
  - command aliases 58-3
  - connection service level 58-4
  - displaying
    - current configuration 58-4
    - DPM statistics 58-6
  - echo option, setting 58-18
  - hardware information
    - Communications Engine Card (CEC) 58-5, 58-6
    - I/O modules 58-5, 58-6, 58-8
  - macro
    - cache 58-9
    - names 58-11
  - memory, managing 58-4
  - NCS
    - file storage 58-7
  - network management
    - macros 58-11
    - prompt 58-11
    - through remote 58-12
    - through Telnet 58-16
  - network map, displaying 58-10
  - node
    - management contact name 58-15
    - name 58-16
    - physical location 58-15
  - parameter list 58-1
  - parameters, displaying 58-8
  - prompt
    - Network Manager privilege 58-11
    - user privilege 58-12
  - RBCS, file storage 58-7
  - remote system identification with PPP 58-15
  - software version number, displaying 58-18
  - statistics
    - displaying 58-14
    - sampling time 58-13
    - types gathered 58-12
  - SysConf file, displaying 58-15
  - system clock, setting 58-5
  - system messages, displaying 58-16
  - time zones, setting displacement for 58-6, 58-17
  - watchdog timer 58-19
  - welcome message string 58-19
- SysCallerID parameter, SYS Service 58-15
- SysconF command 1-59, B-1
- SysConf file 58-15
- SysCONtact parameter, SYS Service 58-15
- SYSgen command 1-60
- SYSgen parameter, SYS Service 58-15
- SysInfo command 1-60
- SysLOCation parameter, SYS Service 58-15
- Syslog parameter, Firewall Service 24-25
- SysNAMe parameter, SYS Service 58-16
- SysPassWord command 1-61
- system crash B-3
- SystemID parameter
  - ISIS Service 32-15
  - NLSP Service 38-12
- SystemMessages parameter, SYS Service 58-16
- SystemName parameter
  - ISIS Service 32-15
  - NLSP Service 38-13
- SZ command 1-61

T

- T1 parameter, LAPB Service 33-2
- T3 parameter, LAPB Service 33-3
- Table 3-1
- Target Token Rotation Time 22-10
- TblFlErrTh parameter, LNM Service 35-5
- TCP Applications Service. *See* TCPAPPL Service
- TCP connections. *See* TCP Service, TCPAPPL Service, and TERM Service
- TCP Service 59-1
  - acknowledgment packets, delay time 59-2
  - connections 59-1
  - data segment
    - maximum size 59-3
    - retransmission limit 59-3
  - keepalive packets 59-2, 59-3
  - maximum window size 59-3
  - TCP sessions, deleting 59-1
- TCP/IP connections
  - enabling 1-9
  - incoming, name services 30-1
- TCP/IP destinations, tracing 1-63
- TCPAPPL Service
  - parameter list 60-1
  - Rlogin connections 60-2
  - user-defined service ports 60-1
- Telnet
  - binary transmission request 61-19
  - connections
    - allowing 58-10
    - deleting 59-1
    - from console port 1-62
- TELnet command 1-62
- TELnetIn parameter, Firewall Service 24-25
- TelnetManager parameter, SYS Service 58-16
- TELnetOut parameter, Firewall Service 24-26
- TERM Service
  - baud rate 61-5
  - Break Functional Unit, enabling 61-12

- TERM Service (continued)
  - character
    - carriage return, nulls insert 61-7
    - changing to command mode 61-10
  - configuration files, displaying 61-17
  - configuration table list, displaying 61-17
  - device type 61-9
  - echoing
    - input data 61-10
    - linefeed 61-14
  - flow control
    - between gateway and local device 61-11
    - characters 61-20
  - incoming connections
    - binary transmission request 61-19
    - break character 61-5
    - character sequence following Return 61-15
    - default configuration file 61-2
    - echoing specific characters 61-10
    - erase character 61-11
    - interaction environment 61-13
    - line-erase character 61-14
    - local editing during data transfer 61-15
    - maximum sessions 61-15
    - mode, changing 61-10
    - port idle time, setting 61-4
    - port initialization macros 61-13
    - reprint-line character 61-17
    - terminal display dimensions 61-7, 61-17
    - terminal type 61-18
    - verbatim character 61-18
    - word-erase character 61-19
    - X.25 to TCP/IP 61-1
  - internal buffer size 61-7
  - linefeed 61-14
  - outgoing connections
    - default configuration file 61-2
    - TCP/IP to X.25 61-1
    - Virtual Terminal Profiles, selecting 61-16
  - packets
    - flushing 61-12
    - forwarding 61-8
    - transmission interval 61-12
  - parameter
    - active values, displaying 61-16
    - classification 61-3
    - default values, displaying 61-8
  - parity, setting 61-16
  - sessions
    - current, disconnecting inactive 61-4
    - displaying 61-4, 61-18
    - inactive time 61-4
  - Urgent Information Exchange Functional Unit, enabling 61-12
- TERMType parameter, TERM Service 61-18
- test boot A-4, A-17, A-24
- TFTP parameter, Firewall Service 24-27
- TG parameter, APPN Service 5-40
- This 4-1
- THreshold parameter, MIP Service 36-3
- time and date, setting 58-5
- time zones 58-6, 58-17
- TImerAck parameter, LLC2 Service 34-4
- TImerInactivity parameter, LLC2 Service 34-4
- TImerReply parameter, LLC2 Service 34-4
- TimeZone parameter, SYS Service 58-17
- TinyGramcomp parameter
  - PATH Service 42-21
- TNEGotiated parameter, FDDI Service 22-10
- token ring line, baud rate 42-2
- TokErrTh parameter, LNM Service 35-5
- TRACE parameter
  - ISIS Service 32-16
  - NLSP Service 38-13
- Trace parameter, X25 Service 65-3
- TRaceData parameter
  - LLC2 Service 34-4
  - SDLC Service 51-12
- TRaceData parameter, DLSw Service 19-20
- TraceRoute command 1-63
- tracing
  - multicast tree 1-36
  - OSI destinations 1-39
  - TCP/IP destinations 1-63
- traffic congestion path resources
  - limiting with BODIncrLimit parameter 43-2
- traffic priorities, displaying 19-14
- traffic priority statistics, displaying 19-15
- TrafficShaper parameter, ATM Service 7-4
- translation bridging, AppleTalk packets 14-3
- Transmission Control Protocol. *See* TCP Service
- transmit clock, setting 42-3
- TRansmit command 1-64
- TransmitWindow parameter, LLC2 Service 34-5
- transparent bridging
  - disabling per-port 14-13
  - enabling 14-6
  - over ATM 14-3
  - over Frame Relay 14-7
  - over SMDS 14-12
  - over X.25 14-14
  - reducing broadcast traffic 14-4
- TransparentBRidge parameter, BRidge Service 14-13
- TrapCONTrol parameter
  - DLSw Service 19-20
  - SDLC Service 51-12
- TreeCache parameter, APPN Service 5-41
- TREQuest parameter, FDDI Service 22-10
- troubleshooting
  - AppleTalk Service 4-9
  - Filter Service 23-2
  - FR Service 25-3, 25-4
  - ISIS Service 32-16
  - PORT Service 43-6
  - X25 Service 65-4
- TTLOverride parameter
  - UDPHELP Service 62-6
- tunnel connections to SNA networks. *See* LLC2 Service
- TUnnel parameter, DVMRP Service 20-10
- TUNnelControl parameter, LLC2 Service 34-5
- TUNnelDisplay parameter, LLC2 Service 34-5
- TUNnelInterface parameter, LLC2 Service 34-5
- TUNnelMAcadd parameter, LLC2 Service 34-6
- TUNnelMOde parameter, LLC2 Service 34-7
- TUNnelPassWord parameter, XSWitch Service 66-2
- TUNnelPeer parameter, LLC2 Service 34-7
- TUNnelPort parameter, XSWitch Service 66-2
- TUNnelPriority parameter, LLC2 Service 34-7
- TUNnelVRing parameter, LLC2 Service 34-8
- TwowaySVCs parameter, X25 Service 65-4
- TxIdle parameter, PATH Service 42-21
- TxParity parameter
  - PATH Service 42-22
- TxParity parameter, PATH Service 42-22

U

- UDPHELP Service 62-1
  - active port list 62-1
  - authorized BOOTP/DHCP server list 62-2
  - boot request packets
    - forwarding priority 62-3
    - maximum hop count 62-2
  - broadcast packets
    - forwarding 62-4
    - overriding time-to-live value 62-6
  - displaying current configuration 62-3
  - enabling 62-3
  - network and server IP addresses 62-4
  - ports, naming 62-5
- UIBinary parameter, SYS Service 58-17
- UIEcho parameter, SYS Service 58-18
- UnBindDSA command 1-64
- UnbindTimer parameter, OSIAPPL Service 40-3
- UNDefine command 1-64
- Universal time support 58-6, 58-17
- UNSave command 1-65
- UpdateTime parameter
  - DVMRP Service 20-10
  - ESIS Service 21-3
  - NRIP Service 39-9
  - RIPIP Service 47-13
  - RIPXNS Service 48-3
  - SAP Service 49-8
  - VIP Service 63-6
- UpNeighbor parameter, FDDI Service 22-10
- user accounts
  - adding to database 1-2
  - deleting 1-13
  - local access control 3-1
  - logged-in users, displaying 3-2
  - managing 1-65
  - names 1-2
  - passwords
    - changing 1-39
    - expiration time 3-2
    - invalidating 1-25
    - setting 1-61
  - privilege level, setting 2-3
  - removing from database 1-13
- User Datagram Protocol Broadcast Helper. *See* UDPHELP Service
- UserData parameter, FDDI Service 22-11
- UserManage command 1-65

V

- VAdvertisePolicy parameter, DECnet Service 17-20
- ValidAddress parameter, X25 Service 65-2, 65-3
- VccTime parameter, ATMLE Service 8-7
- VCIBits parameter, ATM Service 7-5
- VERBatim parameter, TERM Service 61-18
- VERSion parameter, SYS Service 58-18
- VINES Internet Protocol. *See* VIP Service
- VINES routing, checking connectivity 1-66
- VIP Service
  - addresses
    - neighbor, displaying 63-4
    - router 63-1
    - SMDS group 63-5
    - WAN neighbors 63-7
  - configuring 63-2
  - names
    - router 63-5
    - symbolic 63-6
  - packets
    - broadcast, transmission interval 63-6
    - encapsulation type 63-3
    - update, to WAN neighbors 63-7
  - parameter list 63-1
  - port
    - cost 63-4
    - status 63-6
  - routes 63-2
  - routing over
    - Frame Relay 63-7
    - SMDS 63-5
    - X.25 63-7
  - Routing Update Protocol (RTP) 63-4
  - X.25 63-7
- VirBrNum parameter, LNM Service 35-5
- VirCirLoopMode parameter, ATM Service 7-5
- VirCirLoopTime parameter, ATM Service 7-6
- VirRingNum parameter, LNM Service 35-6
- virtual ports 61-2
- VirtualLink parameter, OSPF Service 41-16
- VirtualPort parameter, PORT Service 43-30
- VPIBits parameter, ATM Service 7-6
- VPing command 1-66
- VTp command 1-66
- VtpDataConcat parameter, OSIAPPL Service 40-3

W

- WAISIn parameter, Firewall Service 24-28
- WAISOut parameter, Firewall Service 24-28
- WAN 42-6, 43-4, 43-7, 43-11, 64-1
  - broadcast packets
    - IPX 31-4
    - SAP 49-4
  - learned source routes 56-10
  - MAC header interpretation 14-6
  - neighbors, VINES 63-7
- WAN Extender
  - available virtual paths for dial-up paths 42-8
  - LAPB restriction 43-3
  - Not Set clock value 42-4
  - path number displayed 43-14
  - paths binding to ports 42-4
  - selecting as port owner 43-20
  - supplies send or receive timing clock 42-3
- WanRoutes parameter, SR Service 56-10
- WatchDogTimer parameter, SYS Service 58-18
- WE Service
  - configuring 64-1
  - keep alive timer 64-4
  - limiting available paths 64-2
  - Rebooting the WAN Extender device 64-1
  - retrieving WAN Extender information 64-4
  - setting the error threshold 64-3
  - statistics 64-2
- WelcomeString parameter, SYS Service 58-19
- wide area interface line type
  - setting with LineType parameter 42-12
- WideAreaNbr parameter, VIP Service 63-7
- WINdow parameter, TCP Service 59-3
- WindowSize parameter
  - LAPB Service 33-3
- WordERAse parameter, TERM Service 61-19
- WrapAB parameter, FDDI Service 22-11

X

- X.25
  - addresses, mapping 26-3
  - call user data area 27-4
  - neighbors
    - BRidge Service 14-14
    - DECnet Service 17-14
    - DVMRP Service 20-7
    - IPX Service 31-1
    - ISIS Service 32-13
    - OSPF Service 41-10
    - RIPXNS Service 48-1
    - VIP Service 63-4
  - packets, protocol identifier
    - AppleTalk Service 4-20
    - BRidge Service 14-14
    - DECnet Service 17-21
    - IDP Service 27-5
    - IP Service 29-23
    - IPX Service 31-11
    - VIP Service 63-7
  - PAD session information, displaying 26-4
- X.25 local and global switching. *See* XSWitch Service
- X.500 directory service, DSA address or name 40-2
- X25 Service
  - calls 45-4
  - Closed User Group (CUG)
    - communication 45-2, 45-3
    - default override 65-2, 65-3
  - configuring 45-4
  - creating an X.25 profile 65-4
  - LCNs 65-2, 65-4
  - line status 65-3
  - parameter list 65-1
  - PDN type, setting 65-3
  - port
    - activity, displaying 65-5
    - DTE address 65-4
  - profile ID for neighboring DTE 65-2
  - PVCs 65-3
  - troubleshooting 65-3
- X25Address parameter, X25 Service 65-4
- X25CallUsrData parameter, IDP Service 27-4
- X25ClosedUsrGrp parameter, PROFile Service 45-3
- X25COMPressType parameter, PROFile Service 45-3
- X25CONTrol parameter, PROFile Service 45-4
- X25FastSelect parameter, PROFile Service 45-5
- X25Neighbor parameter, BRidge Service 14-14
- X25NSF parameter, PROFile Service 45-5
- X25PacketSiZe parameter, PROFile Service 45-6
- X25Prefix parameter, XSWitch Service 66-3
- X25PROFileid parameter
  - AppleTalk Service 4-19
  - BRidge Service 14-14
  - CLNP Service 16-5
  - DECnet Service 17-21
  - IDP Service 27-4
  - IP Service 29-23
  - IPX Service 31-11
  - VIP Service 63-7
  - X25 Service 65-4
- X25ProfileName parameter, PROFile Service 45-6
- X25ProfileType parameter, PROFile Service 45-2
- X25ProtID parameter
  - AppleTalk Service 4-20
  - BCN service 11-3
  - BRidge Service 14-14
  - DECnet Service 17-21
  - IDP Service 27-5
  - IP Service 29-23
  - IPX Service 31-11
  - VIP Service 63-7
- X25ReverseChrg parameter, PROFile Service 45-6
- X25STATistics parameter, X25 Service 65-5
- X25ThruputClass parameter, PROFile Service 45-7
- X25VCLimit parameter, PROFile Service 45-7
- X25VCQueueSize parameter, PROFile Service 45-7
- X25VCTimer parameter, PROFile Service 45-8
- X25WindowSiZe parameter, PROFile Service 45-8
- XidKeepAlive parameter, SDLC Service 51-12
- XmitBinary parameter, TERM Service 61-19

XNS routing
  assigning network number 27-2
  displaying configuration information 27-2
  error checking 27-2
  RIP parameters for XNS. *See* RIPXNS Service
  XNS Static Routing Table 27-1, 27-3
XOFF parameter, TERM Service 61-19
XON parameter, TERM Service 61-19
XSWitch Service
  global and local switching 66-1
  mapping address prefixes 66-3
  parameter list 66-1
  switched virtual circuits 66-1
  tunnel 66-2
  X25Prefix table 66-3

Z

Zmodem
  commands 1-50, 1-61
  sending files over CONSOLE port 1-61
  supported packages 1-61
ZONe parameter, AppleTalk Service 4-20
ZoneAdvFilterNm parameter, AppleTalk Service 4-21
ZoneNetMapping parameter, AppleTalk Service 4-21