Reference for NETBuilder® Family Software
Chapter 26 through Appendix B

Software
Version 9.3

p/n 09-1236-000
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 Unpublished rights reserved under the copyright laws of the United States.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

26 GATEWAY SERVICE PARAMETERS

27 IDP SERVICE PARAMETERS

28 IISIS SERVICE PARAMETERS

29 IP SERVICE PARAMETERS

30 IPNAME SERVICE PARAMETERS

31 IPX SERVICE PARAMETERS

B FIRMWARE COMMANDS

INDEX

3COM CORPORATION LIMITED WARRANTY

26 GATEWAY SERVICE PARAMETERS

This chapter describes the parameters for configuring the bridge/router to function as an X.25 connection service gateway for incoming (Telnet, Virtual Terminal Protocol (VTP), or Rlogin) and outgoing (Telnet or VTP) connections. Table 26-1 lists the Gateway Service parameters and commands.

Table 26-1 Gateway Service Parameters and Commands

Parameters	Commands
CONFiguration	SHow
ConnHistory	FLush, SHow
CONTrol	SETDefault, SHow
IPX25Map	ADD, DELete, SHow
PadSession	SHow
PSelX25Map	FLush, SETDefault, SHow
SubAddrMap	FLush, SETDefault, SHow

CONFiguration

Syntax

```
SHow !<path> -Gateway CONFiguration
```

Default No default

Description The CONFiguration parameter displays the current configuration of the gateway.

ConnHistory

Syntax

```
FLush [!<path> | !*] -Gateway ConnHistory
SHow [!<path> | !*] -Gateway ConnHistory
```

Default No default

Description The ConnHistory parameter displays a history that the Gateway Service maintains of the status of the last few sessions. This history includes the following information:

- Direction of the connection
- The client address and the host address
- Type of connection, for example, extended or automatic
- Type of configuration or profile used (if applicable)
- Reason for the termination of the connection

The history buffer is a circular buffer with limited capacity (12 records per path); older entries are overwritten when space is needed to record the history of more recent sessions.

You use the SHow command to view the contents of the history buffer.

The FLush command provides a way to erase the connection history buffer information so the buffer can begin to catch the new records.

CONtrol

Syntax

```
SETDefault !<path> -Gateway CONTrol = ([Enable | Disable], [InExt
  | NoInExt], [OutExt | NoOutExt], [InAuto | NoInAuto], [OutAuto |
  NoOutAuto], [DDXP | NoDDXP], [SubAddr | NoSubAddr], [DSA |
  NoDSA], [Trace | NoTrace])
SHow [!<path> | !*] -Gateway CONTrol
```

Default Disable, InExt, OutExt, InAuto, OutAuto, NoDDXP, SubAddr, NoDSA, NoTrace (Automatically enabled when the X.25 packet layer is up).

Description The CONTrol parameter enables or disables the gateway function and controls the type of connection.

Values

Enable | Disable — Enables and disables the gateway functions on the specified path. Once enabled, X.25 connection service is available for use. If disabled, all currently established sessions on that path are not terminated. No further sessions can be established until the Enable option is set.

InExt | NoInExt — Allows and disallows establishment of incoming extended connections. If NoInExt is selected, the NETBuilder user interface is inaccessible.

OutExt | NoOutExt — Allows and disallows establishment of outgoing extended connection service requests to X.25-attached hosts. If NoOutExt is selected, the packet assembler/disassembler (PAD) emulation user interface is inaccessible.

InAuto | NoInAuto — Allows and disallows acceptance of incoming automatic connection service requests from X.25 PAD-attached terminals.

OutAuto | NoOutAuto — Allows and disallows establishment of outgoing automatic connection service requests to X.25-attached hosts.

DDXP | NoDDXP — Allows and disallows support for the Japanese public data network and connections between a PAD and X.25 host.

SubAddr | NoSubAddr — When SubAddr is selected, the Gateway Service processes the subaddress. When NoSubAddr is selected, no subaddress is processed. If the subaddress is processed by the incoming call service, it is used as extra information in the single step (automatic) incoming connection.

The subaddress is used as a key to find the targeted Internet Protocol/presentation service access point (IP/PSAP) address in the SubAddrMap table. If the IP or PSAP address can be found, the gateway directly makes a Telnet connection to that IP address.

If the IP or PSAP address cannot be found in the SubAddrMap table, this subaddress is treated as the “config file” when initiating the port. If the subaddress is used and an IP or PSAP address is found to make the connection, the default port config file is still the config file “1.”

DSA | NoDSA	Allows and disallows addressing support for the Honeywell Corporation Distributed Systems Architecture (DSA). DSA addressing is supported only for incoming connections to an Open Systems Interconnection (OSI) host.
Trace | NoTrace	Enables and disables tracing. When enabled, messages are printed to the console for certain key events and decisions made by the gateway.

IPX25Map

Syntax

```
ADD [!<config file>] -Gateway IPX25Map <IP address>
  {<x25addr string> | PAD}
DELete [!<config file>] -Gateway IPX25Map {<IP address>
  [<x25addr string> | PAD] | ALL}
SHow -Gateway IPX25Map [<IP address>]
```

Default No default

The NETaddr parameter in the IP Service corresponds to the IPX25Map parameter; if you change the NETaddr parameter, you must make sure this value matches the IPX25Map parameter value.

Description The IPX25Map parameter configures a list of IP addresses in a table for use during outgoing connection establishment. The table includes:

- Configuration file number that initializes the port and session
- IP address
- X.25 address string (facilities)
- Keyword PAD

When creating the table, you can specify a configuration file to initialize the session during outgoing connections. If you do not specify a configuration file, then configuration file 2 is used as the default. In most cases, you can use configuration file 2 without modification; the default settings of the TERM Service parameters are acceptable for most outgoing connections. If you require different settings than the defaults already provided, use one of the configuration files numbered 3 through 32.

Configuration file 1 is the default for incoming connections and must not be used for outgoing connections. If you use an odd-numbered configuration file for an outgoing connection, make sure you change the DeVice parameter from Terminal to Host using the SETDefault !configfile -TERM DeVice = Host command, or the connection attempt will fail.

For information on parameters specifically needed for outgoing connections, refer to Chapter 61.

You must assign an IP address that is on the same network or subnetwork to which the gateway is attached. An IP address assigned to an X.25 address for establishing an automatic outgoing connection must be valid on some IP subnet to which the gateway is attached. For example, if the gateway has two LAN ports and is configured to route IP packets between these two ports, the gateway will be attached to two IP subnets, and an IP address assigned to an IPX25Map entry must be derived from one of these subnets.

After assigning the IP address in the IPX25Map command line, you can substitute PAD commands for the X.25 address string to specify combinations of the following:

- An X.25 destination address
- A specific path
- Facilities to be requested with the call
- Call user data to be sent with the call

In the IPX25Map command line, you can specify the keyword PAD instead of a string of commands. If you specify PAD and a user makes a connection request to the corresponding Internet address, the gateway places the user in the PAD emulation user interface. For more information on PAD emulation mode, refer to “Extended Connections” on page 49-10 in *Using NETBuilder Family Software*.

To delete a single entry from the table, use the DELete -Gateway IPX25Map command and specify the IP address. You also can specify the X.25 address string or the keyword PAD with the IP address. To delete all entries in the table, use the DELete -Gateway IPX25Map ALL command.

To display all entries in the table, use the SHow -Gateway IPX25Map command. You also can display connection information for a single IP address by specifying the address with the SHow command.

Example 1 To map the IP address 129.213.112.120 to the X.25 destination 31104150222 enter:

```
ADD -Gateway IPX25Map 129.213.112.120 311041502222
```

When you make a connection to 129.213.112.120 from an IP Internet-attached terminal, the gateway places a call to 311041502222, an X.25 destination address. Because no configuration file was specified, the connection is initialized with the contents of configuration file 2 (the default). Configuration file 2 contains appropriate TERM Service parameters needed for host connections.

Example 2 To specify reverse charge request and closed user group facilities when the call is placed, enter:

```
ADD !4 -Gateway IPX25Map 129.213.112.121 R,G09*311041502222
```

When you make a connection to 129.213.112.121 from an IP Internet-attached terminal, the gateway places a call to 311041502222 and requests reverse charging (R) and closed user group (G09*). The contents of configuration file 4 initializes the connection.

PadSession

Syntax `SHow [!<xport>] -Gateway PadSession`

Default No default

Description The PadSession parameter displays the session information associated with all the sessions currently active on the specified PAD port, for example, an X.25 line, including both outgoing and incoming Telnet connections. If no !xport is specified, then the sessions on all the ports on which Gateway Service is active are displayed. You can specify the optional session ID to selectively view the information pertaining to that one session. Session information includes the following:

- Session ID
- Client (source) address
- Host (destination) address
- Session protocol on the LAN
- Associated configuration file or profile (if applicable)
- Duration of the session
- Number of bytes transmitted
- Number of bytes received
- Logical channel number (LCN) of the virtual circuit used for the session

This parameter displays gateway-to-X.25 session information for the X.25 side of the connection; the AllSessions parameter in the TERM Service displays gateway-to-host session information for the LAN side of an incoming and outgoing connection.

Valid xport numbers on the NETBuilder II system are 0–127.

PSelX25Map

Syntax

```
SETDefault !<P-Sel> -Gateway PSelX25Map = {[!<conf file>]
(<x.25 addr string> | PAD) | None}
SHow [!<P-Sel>] -Gateway PSelX25Map
FLush -Gateway PSelX25Map
```

Default No default

Description The PSelX25Map parameter configures the list of OSI P-selectors that establish an outgoing connection and to associate the P-selector with the X.25 connection set information required to connect to a WAN-attached host.

When the gateway receives a VTP connection request from a LAN-attached client with a destination P-selector that matches one of the addresses in this list, the gateway uses the corresponding X.25 connection information to initiate a connection with the WAN-attached host. If PAD is specified, then the gateway places the terminal in the PAD emulation user interface.

SubAddrMap

Syntax

```
FLush -Gateway SubAddrMap
SETDefault !<subaddr #> -Gateway SubAddrMap = {(<IPaddr> |
  <PSAPaddr>) | None}
SHow [!<subaddr #>] -Gateway SubAddrMap
```

Default No default

Description The SubAddrMap parameter maps a subaddress to an IP address or PSAP address used for incoming connections from a PAD. Each entry of this parameter maps an internal subaddress to the IP address or PSAP address used for the second-step connection in the single-step incoming connection. The subaddress is used only if you set the CONTrol parameter to the SubAddr value.

Values	<subaddr#>	Specifies a two-byte value ranging from 0–32. After you map a subaddress to an IP/PSAP address, you cannot use that subaddress without reassigning it. For example, if you map subaddress 01 to an IP address, then later map 01 to another IP address, the first IP address is overwritten.
	<IPaddr/PSAPaddr>	Specifies the address to which you are mapping the subaddress.
	None	Deletes an IP address or PSAP address to the SubAddrMap mapping.

27 IDP SERVICE PARAMETERS

This chapter describes the Internet Datagram Protocol (IDP) parameters. Table 27-1 lists the IDP Service parameters and commands.

Table 27-1 IDP Service Parameters and Commands

Parameters	Commands
AllRoutes	FLush, SHow
CONFiguration	SHow, SHowDefault
CONTrol	SETDefault, SHow, SHowDefault
NETnumber	SETDefault, SHow, SHowDefault
ROUte	ADD, DELete, SHow, SHowDefault
SMDSGroupAddr	SETDefault, SHow, SHowDefault
X25CallUsrData	SETDefault, SHow, SHowDefault
X25PROFileid	SETDefault, SHow, SHowDefault
X25ProtID	SETDefault, SHow, SHowDefault

AllRoutes

Syntax

```
FLush -IDP AllRoutes
SHow -IDP AllRoutes [Short | Long | <NETnumber>]
```

Default Short

Description The AllRoutes parameter displays the XNS Routing Table, which lists all the Xerox Network Systems (XNS) networks known to the router. Entries marked with an asterisk (*) are static entries.

Use the FLush command to remove all dynamically learned entries in the routing table. Static entries are not removed by the FLush command. The XNS Static Routing Table size is not limited; as long as space exists on the diskette, static routes can be added.

Values

Short	Produces a short-form routing display that shows only network numbers and hop counts.
Long	Generates a long-form routing table that includes port numbers, network numbers, gateway addresses, and hop counts.
<NETnumber>	Generates a routing table display that includes the port number, gateway address, and hop counts for the specified network number.

CONFiguration

Syntax

```
SHow [!<port> | !*] -IDP CONFiguration
SHowDefault [!<port> | !*] -IDP CONFiguration
```

Default No default display

Description The CONFiguration parameter displays active configuration information as follows:

- Values of the CONTrol parameter
- Values of the SMDSGroupAddr if the Switched Multimegabit Data Service (SMDS) interface is enabled
- Number of attached networks controlled by the NETnumber parameter
- Number of static routes in the routing table controlled by the ROUte parameter
- X.25 configuration parameter information for each port if the X.25 interface is enabled

When no port number is specified, the CONFiguration parameter displays user-configurable information only for those ports whose XNS network number is assigned. When a port number is specified, configuration information for that specific port is displayed. To display all configuration information, use the `!*` wildcard syntax.

CONTrol

Syntax

```
SETDefault -IDP CONTrol = ([Route | NoRoute], [Checksum | NoChecksum])
SHow -IDP CONTrol
SHowDefault -IDP CONTrol
```

Default NoRoute, NoChecksum

Description The CONTrol parameter determines whether the router performs XNS routing and whether checksum is used in the packets.

Values

Route | NoRoute	If Route is selected, the router performs XNS routing. If NoRoute is selected, the router does not perform IDP routing.
Checksum | NoChecksum	If Checksum is selected, error checking is performed to detect data corruption on the received packets. NoChecksum does not provide this service, but provides higher network performance.

NETnumber

Syntax

```
SETDefault !<port> -IDP NETnumber = &<number> (0–FFFFFFFE)
SHow [!<port>| !*] -IDP NETnumber
SHowDefault [!<port>| !*] -IDP NETnumber
```

Default No default (no XNS network numbers assigned)

Description The NETnumber parameter specifies the XNS network number assigned to a port. Multiple network numbers are not allowed on a port. For example, even if you have assigned multiple paths to port 3, you can assign only one network number to that port. Network numbers consist of eight hexadecimal digits. You can omit leading zeros in a network number. For example, &00001234 has the same meaning as &1234.

For more information on ports, refer to Chapter 1 in *Reference for NETBuilder Family Software*.

ROUte

Syntax

```
ADD -IDP ROUte &<remote network> &<network> <media address> <hops>
DELete -IDP ROUte &<remote network>
SHow -IDP ROUte
SHowDefault -IDP ROUte
```

Default No default (no static routes configured)

Description The ROUte parameter adds, deletes, or displays static routes. The XNS Static Routing Table size is not limited; as long as space exists on the diskette, static routes can be added.

Values Select different values with the ADD command in the following order:

First specify each of the following values in the order shown:

<&remote network> Refers to the identifier of the destination network.

<&network> The network number of the directly connected network through which the router can reach the remote destination.

Specify one of the following formats for the <media address> option:

<%host> Media access control (MAC) (Ethernet) address of the closest router through which the XNS network can be reached. MAC can be used in place of %.

<#X25 address> Data terminal equipment (DTE) address that is used for adding X.25 static routes. It indicates the DTE address of the closest router through which the network can be reached. DTE can be used in place of #.

<@DLCI> Data link connection identifier (DLCI) that is used for adding Frame Relay static routes. DLCI can be used in place of @.

$SMDS addr Switched Multimegabit Data Service individual address of the neighbor router on the SMDS network that is used for adding static routes. SMDS can be used in place of $.

Specify:

<hops> Number of gateways that a packet has to pass through before it can reach the destination network. The maximum number of hops is 15. Any network that is 16 or more hops away is considered unreachable.

Example To add a static route to the routing table on Router 1 for an Ethernet network (&3145) that is two hops away, enter:

```
ADD -IDP ROUte &3145 &3140%080002015980 2
```

SMDSGroupAddr

Syntax

```
SETDefault !<port> -IDP SMDSGroupAddr = $<E0–E999999999999999> |
  None
SHow [!<port> | !*] -IDP SMDSGroupAddr
SHowDefault [!<port> | !*] -IDP SMDSGroupAddr
```

Default None (no group address configured)

Description The SMDSGroupAddr parameter configures an SMDS group address that is used as the XNS multicast address on the specified port. The port must be configured with the -PORT OWNer set to SMDS and the -IDP SMDSGroupAddr configured with a valid group address for XNS routing to occur over SMDS.

Values

<E0–E999999999999999>	Specifies the format for an SMDS group, or multicast, address. The group address type is used to route data to all routers 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, it is padded on the right with Fs.
None	Removes a group address previously assigned to a port.

X25CallUsrData

Syntax

```
SETDefault !<port> -IDP X25CallUsrData = {<number> (1–FFFFFFFE) |
  None}
SHow [!<port> | !*] -IDP X25CallUsrData
SHowDefault [!<port> | !*] -IDP X25CallUsrData
```

Default None

Description The X25CallUsrData parameter is used when a router is talking to a GS/X.25-XNS. The GS/X.25-XNS checks the call user data area when it receives a call connection request.

Use the SHow command to display the X25CallUsrData parameter value for a particular port. If no port number is specified, the value for all ports will be shown.

Values

<1–FFFFFFFE>	Sets the value of X25CallUsrData to the network number of the router's port that is to be connected to the GS/X.25-XNS.
None	Use the value None if you do not need to set any call user data. For example, if another bridge/router is at the remote end, you can use the value None.

X25PROFileid

Syntax

```
SETDefault [!<port>] -IDP X25PROFileid = <number> (0–255)
```

```
SHow [!<port> | !*] -IDP X25PROFileid
SHowDefault [!<port> | !*] -IDP 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 Internet Datagram Protocol (IDP) (XNS) packets. A value of 0 indicates that no specific X.25 user profile is configured for IDP (XNS) packets.

X25ProtID

Syntax

```
SETDefault !<port> -IDP X25ProtID = <protocol id> (1 octet)
SHow [!<port> | !*] -IDP X25ProtID
SHowDefault [!<port> | !*] -IDP X25ProtID
```

Default 0xC0

Description The X25ProtID parameter applies to routing XNS over an X.25 public data network (PDN). This parameter specifies a protocol identifier to be included in all outgoing packets. Enter a value between 1 and FF.

When a packet reaches its destination, the destination DTE verifies this protocol identifier against its own protocol ID. If they match, the incoming packet is accepted. If they do not match, the packet is discarded. The chosen value must not conflict with that used by other protocols.

28 IISIS SERVICE PARAMETERS

This chapter describes the Integrated Intermediate System to Intermediate System (IISIS) Service Parameters used for Internet Protocol (IP) and Open System Interconnect (OSI) routing. The IISIS parameters are related to the IP and ISIS Services. Table 28-1 lists the IISIS parameters and commands.

Table 28-1 IISIS Service Parameters and Commands

Parameters	Commands
CONTrol	SETDefault, SHow
DefaultMetric	SETDefault, SHow
ExteriorPolicy	ADD, DELete, SHow
InteriorPolicy	ADD, DELete, SHow
StaticPolicy	ADD, DELete, SHow

CONTrol

Syntax

```
SETDefault -IISIS CONTrol = [Disable | Enable]
SHow -IISIS CONTrol
```

Default Disable

Description The CONTrol parameter enables or disables Integrated IS-IS operation for IP mode.

To run Integrated IS-IS in IP mode, you must perform two additional steps:

- Enable the IP routing by setting the value of the -IP CONTrol parameter to ROute.
- Configure at least one IP address using the -IP NETaddr parameter.

Integrated IS-IS automatically monitors the two requirements. If the requirements are satisfied, Integrated IS-IS in IP mode is then enabled. For more information, refer to Chapter 6 in *Using NETBuilder Family Software*.

Values Disable | Enable

Disable turns off the IP mode operation of the IS-IS Protocol immediately but does not impact the OSI mode operation if it is currently running.

Enable turns on the Integrated IS-IS operation immediately. If the IS-IS Protocol is not running yet, Enable allows it to run in the IP-only mode. If the IS-IS Protocol is already running for the OSI family (that is, in the OSI-only mode), Enable turns it into the dual IP and OSI mode immediately.

DefaultMetric

Syntax

```
SETDefault -IISIS DefaultMetric = [Disable | <metric> (1–63)
 [Internal | External]]
SHow -IISIS DefaultMetric
```

Default None

Description The DefaultMetric parameter configures the cost of a default route. Using this parameter, the router can be configured to announce a default route into the IS-IS routing domain. A default route is an advertisement for network 0.0.0.0 with subnet mask 0.0.0.0.

This parameter is effective only on a Level 2 router. For more information on designating a router as either Level 1 or Level 2, refer to “MODE” on page 32-12.

Values

Disable	Indicates that no default route will be advertised.
<metric>	Indicates a value between 1 and 63.
Internal | External	If you select Internal, the metric type in the advertisement is tagged as internal. An internal metric is comparable to other path costs, and is added to the total path cost as part of the criteria used to measure distance and cost. If you select External, the metric type in the advertisement is tagged as external. An external metric is more expensive than any other metric, and is used as the sole criterion in determining distance and cost. If you do not specify Internal or External, Internal is the default. Internal routes have higher precedence over external routes. An external route is not chosen if an alternate internal route is available. For example, an internal default route announcement prevents the use of any route with external metric, whether or not the route is host route, subnet route or default route.

ExteriorPolicy

Syntax

```
ADD -IISIS ExteriorPolicy All | None | [~]<IP address> <metric>
 [Internal | External]
DELete -IISIS ExteriorPolicy All | <IP address>
SHow -IISIS ExteriorPolicy
```

Default None (no routes will be advertised)

Description The ExteriorPolicy parameter adds an IP network number to an exterior routing protocol policy list. The list is used to cross-check with routes learned from other exterior routing protocols, such as Exterior Gateway Protocol (EGP) and Border Gateway Protocol (BGP). If these routes are reachable, they will be further advertised into the IS-IS domain.

Up to 64 network numbers can be added. This parameter is effective only on a Level 2 router.

Values

All | None — All specifies that all routes from exterior routing protocols are advertised. When used with the DELete command, All removes all networks from the policy list. None specifies that no routes will be advertised.

~ — Indicates that all networks except the ones in the policy list are advertised.

<IP address> — The IP network number you are adding to the exterior routing protocol policy list.

<metric> — A value between 1 to 63. If metric 0 is specified, the metric value from the exterior routing domain is used. If the value is higher than 63, 63 is used.

Internal | External — If you select Internal, the metric type in the advertisement is tagged internal. An internal metric is comparable to other path costs, and is added to the total path cost as part of the criteria used to measure distance and cost. If you select External, the metric type in the advertisement is tagged external. An external metric is more expensive than any other metric. If no metric is specified, 0 is the default.

If Internal or External is not specified, Internal is the default

InteriorPolicy

Syntax

```
ADD -IISIS InteriorPolicy All | None | [~]<IP address> <metric>
 [Internal | External]
DELete -IISIS InteriorPolicy All | <IP address>
SHow -IISIS InteriorPolicy
```

Default None (no routes will be advertised)

Description The InteriorPolicy parameter adds an IP network number to an interior routing protocol policy list. The list is used to cross-check with routes learned from other interior routing protocols, such as Open Shortest Path First (OSPF) and Routing Information Protocol (RIP). If these routes are reachable, they are further advertised into the IS-IS domain.

Up to 64 network numbers can be added. This parameter is effective only on a Level 2 router.

Values

All | None — All specifies that all routes from other routing protocols are advertised. When used with the DELete command, All removes all networks from the policy list. None specifies that no routes from other routing protocols are advertised.

~ — All networks except the ones in the policy list are advertised.

<IP address> — The IP address you are adding to the interior routing protocol policy list.

<metric> — *A* value between 1 to 63. If metric 0 is specified, the metric value (OSPF cost or RIP cost) from the interior routing domain is used. If the value is higher than 63, 63 is used.

Internal | External	Internal tags the metric type in the advertisement internal. An internal metric is comparable to other path costs, and is added to the total path cost as part of criterion used to measure distance/cost. When you specify External, the metric type in the advertisement is tagged as external. An external metric is more expensive than any other metric.

If no metric is specified, 0 is the default. If Internal or External is not specified, Internal is the default.

StaticPolicy

Syntax

```
ADD -IISIS StaticPolicy All | None | [~]<IP address> <metric>
 [Internal | External]
DELete -IISIS StaticPolicy All | <IP address>
SHow -IISIS StaticPolicy
```

Default None (no routes will be advertised)

Description The StaticPolicy parameter adds an IP network number to an static routing protocol policy list. The list is used to cross-check with all the static routes configured into the router. If these routes are reachable, they are further advertised into the IS-IS domain.

Up to 64 network numbers can be added. This parameter is effective only on a Level 2 router.

Values

All | None	All specifies that all routes from static route table are advertised. When used with the DELete command, All removes all networks from the policy list. None specifies that no routes are advertised.
~	All networks except the ones in the policy list are advertised.
<IPaddress>	The IP network number you are adding to the static routing policy list.
<metric>	*A* value between 1 to 63. If metric value 0 is specified, the metric from the static routes are used. If the value is higher than 63, 63 is used.
Internal | External	When you specify Internal, the metric in the advertisement is tagged as internal. An internal metric is comparable to other path costs, and is added to the total path cost as part of criterion used to measure distance/cost. When you specify External, the metric type in the advertisement is tagged as external. An external metric is more expensive than any other metrics.

If no metric is specified, 0 is the default. If Internal or External is not specified, Internal is the default.

29

IP Service Parameters

This chapter describes the Internet Protocol (IP) Service parameters. The IP Service is related to the ARP, OSPF, RIPIP, and TCP Services. Table 29-1 lists the IP Service parameters and commands.

Table 29-1 IP Service Parameters and Commands

Parameters	Commands
ADDRess	ADD, DELete, FLush, SHow, SHowDefault
AllRoutes	FLush, SHow
CONFiguration	SHow
CONTrol	SETDefault, SHow
DefaultTTL	SETDefault, SHow
FilterAddrs	ADD, DELete, SHow
FilterDefAction	SETDefault, SHow
FIlters	ADD, DELete, SHow
ICMPGenerate	SETDefault, SHow
ICMPReply	SETDefault, SHow
LaPosteDD	SETDefault, SHow
LaPosteNN	SETDefault, SHow
LaPostePort	SHow
LaPostePP	SETDefault, SHow
LaPostePRefix	SETDefault, SHow
NETaddr	ADD, DELete, SETDefault, SHow
QueuePriority	SETDefault, SHow
ReassemblyTime	SETDefault, SHow
RemoteAddress	SETDefault, SHow
ROUte	ADD, DELete, SHow
SecAuthIn	ADD, DELete, SHow
SecAuthOut	ADD, DELete, SHow
SecCONTrol	SETDefault, SHow
SecFileServer	SETDefault, SHow
SecLabelDefault	SETDefault, SHow
SecLabelSys	SETDefault, SHow
SecLabelValues	SETDefault, SHow
SecLabelXtra	SETDefault, SHow
SecLEVel	SETDefault, SHow
SMDSGroupAddr	ADD, DELete, SHow, SHowDefault
X25PROFileid	SETDefault, SHow
X25ProtID	SETDefault, SHow

ADDRess

Syntax

```
ADD -IP ADDRess <IP address> <media address> [Ethernet | Ieee |
  Snap [Report]]
DELete -IP ADDRess <IP address>
FLush -IP ADDRess
SHow -IP ADDRess [<IP address>] [External | Internal | Broadcast
  | Local]
SHowDefault -IP ADDRess
```

Default No default

Description The ADDRess parameter controls and displays the Address Translation Table, which is the same as the Address Resolution Protocol (ARP) Table. You can add as many Internet addresses as desired to the Address Translation Table.

Adding an Address. To add an Internet address to the table, use the ADD command syntax. The <IP address> in the syntax is the Internet address you are adding to the IP Address Translation Table. The [media address] is configured for the Internet address specified. If the <media address> is a MAC address, precede it with either a percent sign (%) or the letters MAC. If the <media address> is an X.25 address, precede it with either a pound sign (#) or the letters data terminal equipment (DTE). If the <media address> is a Frame Relay data link connection identifier (DLCI), precede it with either an at sign (@) or the letters DLCI. If the <media address> is an SMDS individual address, precede it with either a dollar sign ($) or the letters SMDS. If the media address is a local ATM virtual circuit identifier (VCID) of a permanent virtual circuit (PVC), precede it with an and sign (&). VCIDs are mapped to the VPI.VCI and configured using the -ATM PermVirCircuit parameter. For more information, refer to "PermVirCircuit" on page 7-2.

The Ethernet, IEEE, and Subnetwork Access Protocol (SNAP) values are for the Ethernet header format. The value is required only when the media address is a MAC address.

If R or Report is specified, the ARP agent responds to the ARP request for the specified Internet address with the configured media address and header format. This feature is useful for systems that do not support ARP or for environments in which a single ARP server is used.

The default is Ethernet header format; ARP agent support (the Report value) is disabled.

Deleting an Address. DELete -IP ADDRess removes static entries created by the ADD -IP ADDRess command.

The ADD -IP ADDRess and DELete -IP ADDRess commands change the ARP table on the disk and in memory, and the new table takes effect immediately if the IP address is on one of the attached networks with the valid reader format.

To remove all dynamic entries in the table, use the FLush command.

Values <IP address> Specifies the Internet address to be added to the IP Address Translation Table.

<media address>	Specifies the X.25, Frame Relay, Switched Multimegabit Data Service (SMDS), Asynchronous Transfer Mode (ATM), or media access control (MAC) address.
External	Indicates the Internet address of a system on one of the attached networks.
Internal	Applies only to Internet addresses assigned to ports of a communications server that is not local.
Broadcast	Indicates the broadcast address or addresses associated with the configured IP network.
Local	Indicates the address associated with one of the router interfaces.
Report	Indicates to ARP whether ARP should perform ARP agent functions (proxy ARP) for the specified IP address.

Displaying the Address Translation Table. You can use the SHow -IP ADDRess and the SHowDefault -IP ADDRess commands to show the IP Address Translation Table. The display generated by the SHowDefault -IP ADDRess command may be different from the one generated by the SHow -IP ADDRess command.

To display the IP Address Translation Table that is being used, use:

```
SHow -IP ADDRess [<IP address>] [External | Internal | Broadcast
  | Local]
```

The information in the SHowDefault -IP ADDRess display becomes active as soon as you connect the router to the network and configure its ports.

AllRoutes

Syntax

```
FLush -IP AllRoutes
SHow -IP AllRoutes [<IP address> | A | B | C | N | S | H | L |
  R | ST] [LOng]
```

Default No default

Description The AllRoutes parameter clears and displays both static entries and dynamic entries in the routing table.

If you enter the SHow -IP AllRoutes command without any of the optional values described below, the system displays a routing table with the following elements:

- Class A, B, or C networks
- Network routes, subnet routes, or host routes
- Local networks (directly connected to the router) or remote networks

Enter the SHow -IP AllRoutes command with one or more of the optional values described below (except for the LOng value) to display specific types of information.

Only dynamic RIP entries can be removed using the FLush command; dynamic OSPF entries are not removed.

Values

<IP address>	Displays only the entry for that particular Internet address.
A, B, C	Displays class A, B, or C networks, respectively.

N, S, H Displays network routes, subnet routes, or host routes, respectively.

L, R Displays local networks (directly connected to the router) or remote networks, respectively.

ST Displays static routes only.

LOng Displays the complete OSPF area ID.

For information on how the router learns the routes, refer to Chapter 6 in *Using NETBuilder Family Software*.

Example The following display is generated by the SHow -IP AllRoutes command:

```
------------------------------IP Routing Table----------------------------
Total Routes = 6, Total Direct Networks = 2,
Destination  Mask             Gateway       Metric Status   TTL  Source
10.0.0.0     255.0.0.0        UnNumbered !3 1      Up       60   RIP
11.11.11.11  255.255.255.255  60.0.0.4      3      --       --   Static
                              UnNumbered !3 5      Up       60   RIP
20.0.0.0     255.0.0.0        UnNumbered !3 1      Up       60   RIP
50.0.0.0     255.0.0.0        50.0.0.3      0      Up       --   Connected
60.0.0.0     255.0.0.0        60.0.0.3      0      Up       --   Connected
```

The following are descriptions of fields in the routing table:

Destination Specifies the destination of the packets. It could be a host or a network address.

Gateway Specifies the address to which the router forwards the packet, or if the gateway is unnumbered, the number of the interface to which the unnumbered gateway is connected.

Metric Is a measure of the cost of reaching a destination.

TOS Indicates a type of service (TOS) that applies to the route. The TOS column is provided only in the LOng display.

Status Indicates the status of the route. If route source is connected, the status is either Up or Down. If the route source is RIP, the status could be Up, Garbage-Collection, or Hold-Down. If the route source is OSPF, it is always UP. If it is a static route, no status is reported.

TTL Specifies a time-to-live (TTL) applies only to routes dynamically learned through RIP. It indicates how much time (in seconds) is left before the route is deleted from the routing table.

Source Indicates whether the route is a static route, a directly connected network, or a dynamic route learned through RIP, OSPF, or Integrated IS-IS.

CONFiguration

Syntax `SHow [!<port> | !*] -IP CONFiguration`

Default No default

Description The CONFiguration parameter displays the global IP configuration parameters for all ports and the information on the directly connected networks.

CONTrol

Syntax

```
SETDefault -IP CONTrol = ([ROute | NoROute], [RelaySrcRoute |
  NoRelaySrcRoute], [SplitLoad | NoSplitLoad], [Filtering |
  NoFiltering], [SECurity | NoSECurity], [FwdSubnetBcast |
  NoFwdSubnetBcast], [FwdAllSubnetBcast | NoFwdAllSubnetBcast])
SHow -IP CONTrol
```

Default NoROute, NoRelaySrcRoute, NoSplitLoad, NoFiltering, NoSECurity, FwdSubnetBcast, NoFwdAllSubnetBcast

Description The CONTrol parameter determines whether the system performs IP routing and how the routing function is performed. The values within each pair are mutually exclusive. The values specified apply to the global IP routing function, not just to a particular interface.

Values

ROute | NoROute	Determines whether IP routing is performed.
RelaySrcRoute | NoRelaySrcRoute	If RelaySrcRoute is specified, the router forwards (relays) packets that contain the Loose or Strict source route option. If NoRelaySrcRoute is specified, these packets are discarded.
SplitLoad | NoSplitLoad	Determines whether load splitting is performed. If SplitLoad is specified, the traffic load is distributed among a set of least-equal-cost paths. These paths are selected on a round-robin basis. If a path is unreachable, it is not considered a candidate for load splitting.
Filtering | NoFiltering	Determines whether IP packet filtering is performed. If Filtering is specified, each IP packet is verified against the filter list before it is forwarded. Filtering can reduce router performance, because each packet needs to be verified against the filter list.
SECurity | NoSECurity	Globally enables/disables IP security for the system. If NoSECurity is selected, the system does not check for IP security options in the IP header. If security options are present, they are ignored.
FwdSubnetBcast | NoFwdSubnetBcast	Determines whether or not a system forwards packets with IP addresses that are subnet broadcast addresses, (the host field of the destination IP address is set to all 1s). The packet is normally routed toward the remote subnet. Upon reaching the last hop, if the router is set to FwdSubnetBcast, the packet is broadcasted using the hardware broadcast mechanism to all hosts on the subnet. For example, a subnet broadcast directed to 10.1.255.255 with a 16-bit subnet mask reaches every host on subnet 1.
FwdAllSubnetBcast| NoFwdAllSubnetBcst	Determines whether or not the system forwards all subnet broadcast packets. The all subnet broadcast packet is configured with both the subnet field *and* the host field set to all 1s in the destination address.

When set to FwdAllSubnetBcast, the IP packet is routed toward the destination IP network. Upon reaching its destination, the router broadcasts the packet using the hardware broadcast mechanism on all directly connected subnets of the destination IP network. Downstream routers receive the packet and broadcast it further downstream to other routers. The time-to-live field is decremented along the way to prevent the packet from looping forever.

For example, an all subnet broadcast to 10.255.255.255 is broadcast to every subnet on network 10. If subnet 10.255 already exists on the network, the all subnet broadcast is ignored and a directed broadcast to all host on subnet 255 occurs.

DefaultTTL

Syntax

```
SETDefault -IP DefaultTTL = <seconds>(1–255)
SHow -IP DefaultTTL
```

Default 30

Description The DefaultTTL parameter specifies the default number of seconds that pass before an IP packet is discarded and applies only to packets sourced by the local router. The number of seconds is approximately equal to the number of hops. The IP client may specify a different number for each packet or specify that the packet use the default (for example, the value of DefaultTTL).

FilterAddrs

Syntax

```
ADD -IP FilterAddrs <adr1> [<dir>] <adr2> [<action> [<protocol>
  [<filterID>]]] <action>=PROTocolRsrv=<tag>| Discard |
  DODdiscard | Forward | QPriority = {H | M | L} |
  X25Profile=<profile>
  <protocol> = DLSW | FTP | IP | IPDATA | ICMP | SMTP | TCP |
  TELNET | UDP
DELete -IP FilterAddrs <adr1> [<dir>] <adr2> [<action> [<protocol>
  [<filterID>]]]
SHow -IP FilterAddrs [<adr1> <addr2>]
```

Default No default

Description The FilterAddrs parameter specifies a packet filtering policy. You can restrict network traffic on a per-address basis. The FIlterAddrs parameter specifies to which addresses and protocols a packet filter should be applied. You can specify the ADD -IP FilterAddrs command as many times as desired. A policy must be defined in order for IP packet filtering to function. A filter requires a corresponding policy; a policy does not require a corresponding filter.

The FilterAddrs parameter works in conjunction with the FIlters parameter. Use the FIlters parameter to create custom filters for particular types of packets. For information on creating custom packet filters, refer to “FIlters” on page 29-10.

The system sorts the packet filter policies that you create using the ADD -IP FilterAddrs in a particular order. First, the system looks at the source and destination IP addresses. The system places policies with more specific source and destination IP addresses higher in the list than policies with less specific source and destination IP addresses. For example, if you specify source and destination IP addresses of 20.0.0.0 and 0.0.0.0 and source and destination addresses of ALL and ALL, the system places the policy containing the addresses 20.0.0.0 and 0.0.0.0 higher in the list than a policy containing the addresses ALL and ALL because the addresses are more specific. If you add a policy containing the addresses 20.0.0.1 and ALL, the system places this policy higher in the list than the previously discussed policies because the addresses are more specific.

If different policies contain the same source and destination IP addresses, the system then looks at the protocol specified by each of these policies. The system has an established hierarchy for the protocols. The hierarchy is as follows:

- Internet Protocol (IP)
- IPDATA
- Internet Control Message Protocol (ICMP)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- File Transfer Protocol (FTP)
- TELNET
- Simple Mail Transfer Protocol (SMTP)
- Data Link Switching (DLSw)
- Number (if more than one number is specified, the system puts in numerical order)

To display the policy for a particular filter, use SHow -IP FilterAddrs. If you do not specify a pair of addresses, all policies are displayed. The policies are displayed in the order described in the preceding paragraphs.

Values <adr1/adr2> Specifies the source (adr1) and destination (adr2) addresses for a policy. Specify <adr1> and <adr2> using the following syntax:

```
<adr1> or <adr2> = <IP address> [<mask>] | ALL
```

The syntax is described as follows:

<IP address> A specific IP address.

<mask > An optional range of IP addresses. Each bit set to 1 in a mask specifies that the corresponding bit position in the address is not checked. For example, if you have a policy with an address of 129.213.0.0 and mask of 0.0.255.255, specified as 129.213.0.0/0.0.255.255, the following is a match:

129.213.0.1
129.213.1.0
129.213.1.1

The following do not match:

128.213.0.0
128.213.1.1

If you do not specify a mask, the system assumes 0.0.0.0.

- ALL — Indicates all IP addresses. All is the default value.

<dir> Indicates the flow of direction. The following options are available:

- > — The policy operates in the direction from <adr1> to <adr2> where <adr1> is the source IP address and <adr2> is the destination IP address.
- <> — The policy operates bidirectionally between <adr1> and <adr2>. This is the default value.
- < — The policy operates in the direction from <adr2> to <adr1> where <adr2> is the source IP address and <adr1> is the destination IP address.

<action> Specifies the action to be performed when the policy matches a packet. You can specify different actions for the same pair of addresses. The following options are available:

- PROTocolRsrv=<tag> — Specifies a tag for IP packets using protocol reservation. 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.

  Bandwidth reservation for designated packets (protocol reservation) can be accomplished through a mnemonic filtering procedure or an IP filtering procedure. For more information, refer to the PROTocolRsrv and QueueCONTrol parameters in Chapter 43. For information about the mnemonic filtering procedure, refer to Chapter 4 in *Using NETBuilder Family Software*, and to the -FIlter POLicy parameter in Chapter 23. For information about the IP filtering procedure, refer to Chapter 6 in *Using NETBuilder Family Software*.
- Discard — Discards the packet when matching is satisfied. This is the default value.
- 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 is not considered as “user” traffic that keeps a dial-up path up.

  For a non-DOD port, the action taken is similar to that of the Forward action.
- Forward — Forwards the packet when matching is satisfied.

QPriority — Setting QPriority to a value of either High, Medium, or Low places packets matching this FilterAddrs policy on the corresponding LMF transmission queue for non-X.25 links.

<X25Profile> — Specifies the intended X.25 user profile ID. For more information, refer to “X25PROFileid” on page 29-23.

<protocol> Indicates the starting point for the offset of a condition if any filters have been assigned to the policy. The format for a filter condition is described in “FIlters” on page 29-10.

This value also can indicate which protocol packets should be forwarded or discarded. You can specify only one protocol per ADD -IP FilterAddrs command.

IP — Starting point is at the beginning of the IP header.

IPDATA — Starting point is at the byte following the IP header.

If IP options are present, the offset is the byte immediately following the IP options.

ICMP — Starting point is at the beginning of the ICMP header. Protocol number in the IP header is checked. If matched, the associated filter is applied.

TCP — Starting point is at the beginning of the TCP header. Protocol number in the IP header is checked. If matched, the associated filter is applied.

UDP — Starting point is at the beginning of the UDP header. Protocol number in the IP header is checked. If matched, the associated filter is applied.

FTP — Starting point is at the beginning of the TCP header. Port number in the TCP header is checked. If matched, the associated filter is applied.

TELNET — Starting point is at the beginning of the TCP header. Port number in the TCP header is checked. If matched, the associated filter is applied.

SMTP — Starting point is at the beginning of the SMTP header. Port number in the TCP header is checked. If matched, the associated filter is applied.

DLSw — Starting point is at the beginning of the DLSw header. Port number in the TCP header is checked. If matched, the associated filter is applied.

<number> — Protocol number is in decimal format. Protocol number in the IP header is checked. If matched, the associated filter is applied.

<filterID> Specifies a filter to which the FilterAddrs policy applies. Filters are identified by their filterid and are defined using the FIlters parameter. You can specify one filterid per ADD -IP FilterAddrs command.

If no filter is assigned to a policy, packet filtering is performed based on the arguments and protocols. By default, no filter is assigned.

Example 1 To create a policy that discards any packets sourced from or destined to host 129.10.0.1, enter:

```
ADD -IP FilterAddrs ALL<> 129.10.0.1
```

Example 2 To delete the policy with address pair All, 129.10.0.1, enter:

```
DELete -IP FilterAddrs ALL 129.10.0.1
```

For more information on using the filtering feature, refer to “FIlters” on page 29-10. For examples of prioritization using the FilterAddrs parameter, refer to Chapter 6 in *Using NETBuilder Family Software*.

FilterDefAction

Syntax

```
SETDefault -IP FilterDefAction = ([Forward | Discard])
SHow -IP FilterDefAction
```

Default Forward

Description The FilterDefAction parameter specifies the action performed on the packets that do not match any FilterAddrs conditions.

FIlters

Syntax

```
ADD !<filterid> -IP FIlters <condition> [,<condition>...]
  <condition> = <%offset>: [<operator>] <%pattern>
DELete !<filterid> -IP FIlters ALL | <condition> [,<condition>...]
  <condition> = <%offset>: [<operator>] <%pattern>
SHow -IP [!<filterid>] FIlters
```

Default No default

Description The FIlters parameter creates, deletes, and modifies custom filters. Filters restrict the flow of IP traffic on a per-packet basis. The IP packet filtering function allows you to define custom filters that will forward or discard packets that meet all conditions of the filter.

FIlters works in conjunction with the FilterAddrs parameter. Use FilterAddrs to establish a filter policy, which can then be assigned to a filter created with the ADD -IP FIlters command. For more information on establishing a filter policy, refer to “FilterAddrs” on page 29-6.

Use SHow -IP FIlters to display a particular defined filter. If no filterid is specified, all defined filters are displayed.

IP packet filtering reduces the router’s performance, because each packet must be verified against filtering criteria before it can be forwarded.

Creating a Filter. You can create up to 64 custom IP packet filters using the ADD syntax. The filter ID identifies a particular filter. Assign a filter ID between 1 and 64. The ADD command works in one of two ways:

- An ADD command with a filter ID that does not exist creates a new filter with that ID.
- An ADD command with a filter ID already assigned to a filter modifies that filter.

Filter Conditions. Each filter can contain as many conditions as desired. A packet must meet all of the conditions of the filter in order to be forwarded or discarded. If more than one condition is specified, use commas to separate the conditions. The comma indicates the logical "and" operator. The list of conditions has the following format:

```
<%offset>: [<operator>] <%pattern> [,...]
```

The following list explains each element of the condition list format:

<%offset>: Must be entered in hexadecimal, preceded by a percent sign (%) and followed by a colon (:). The offset is relative to the starting point specified by the ADD -IP FilterAddrs command.

<operator> Specifies an optional logical operator argument. Refer to Table 29-2 for a list of logical operators. The default logical operator is represented by the equal sign (=).

<%pattern> Must be preceded by a percent sign (%) and entered in hexadecimal with a maximum of 8 hex digits.

Table 29-2 Logical Operators in the ADD FIlters Command

Symbol	Name	Condition Requirements
&	and	The result of the bitwise "and" operation is not 0.
|	or	The result of the bitwise "or" operation is not 0.
=	equal	The value of offset is equal to the pattern.
!	not equal	The value of the offset is not equal to the pattern.
>	greater than	The value of the offset is greater than the pattern.
<	less than	The value of the offset is less than the pattern.

Adding a Filter. For more information on adding a filter and the packet filtering feature in general, refer to Chapter 6 in *Using NETBuilder Family Software*.

Deleting a Filter. You can use the DELete -IP FIlters command in the following ways:

- To remove one or more conditions from the list of conditions already assigned to a particular filter
- To remove all conditions already assigned to a particular filter using the value ALL, which deletes the entire filter

3Com recommends that you delete filters you no longer need.

ICMPGenerate

Syntax

```
SETDefault !<port> -IP ICMPGenerate = ([Redirect | NoRedirect],
  [DestUnreachable | NoDestUnreachable], [TimeExceed |
  NoTimeExceed])
SHow [!<port> | !*] -IP ICMPGenerate
```

Default Redirect, DestUnreachable, TimeExceed

Description The ICMPGenerate parameter controls the origin of certain ICMP packets and can be selectively disabled on a per-port basis.

Values

Redirect | NoRedirect	Controls whether ICMP ReDirect packets are issued on the port.
DestUnreachable | NoDestUnreachable	Controls whether ICMP Destination Unreachable packets are issued on the port.
TimeExceed | NoTimeExceed	Controls whether ICMP TimeExceed packets are issued on the port.

ICMPReply

Syntax

```
SETDefault -IP ICMPReply = ([Info | NoInfo], [Mask | NoMask])
SHow -IP ICMPReply
```

Default NoInfo, NoMask

Description The ICMPReply parameter determines whether the router responds to ICMP Information request packets and ICMP Address Mask request packets.

Values

Info | NoInfo	Determines whether the router responds to Information request packets.
Mask | NoMask	Determines whether the router responds to Address Mask request packets.

Both the Address Mask and Information request packets are answered after confirmation that the source address is on the network. Address Mask requests are answered with the subnet mask configured for the interface receiving the request.

The Address Mask and Information requests with source route options are ignored. Unspecified source Internet addresses (0.0.0.0) are allowed. The ICMP replies are broadcast (but unicast at the MAC level).

LaPosteDD

Syntax

```
SETDefault -IP LaPosteDD = <min> - <max>
SHow -IP LaPosteDD
```

Default 1–99

Description The LaPosteDD parameter controls the range of DD, the administrative department in France.

The LaPoste parameters provide you with the ability to control and customize the LaPoste IP Address-to-X.121 Address conversion algorithm. The X.25 address for the LaPoste network is always seven decimal digits long and can be represented as x D D N N P P.

LaPosteNN

Syntax
```
SETDefault -IP LaPosteNN = <min> - <max>
SHow -IP LaPosteNN
```

Default 0–99

Description The LaPosteNN parameter controls the range of NN, the X.25 node number.

LaPostePort

Syntax
```
SHow -IP LaPostePort
```

Default No default

Description The LaPostePort parameter displays the port that is actively attached to the LaPoste network. “Active” means that the PD network type is LaPoste, this port is in the UP state, and the IP address is Class A.

LaPostePP

Syntax
```
SETDefault -IP LaPostePP = <min> - <max>
SHow -IP LaPostePP
```

Default 0–35

Description The LaPostePP parameter controls the range of PP, which is the X.25 port number on the X.25 node.

LaPostePRefix

Syntax
```
SETDefault -IP LaPostePRefix = <number> (0–9)
SHow -IP LaPostePRefix
```

Default 9

Description The LaPostePRefix parameter controls the value of x, the prefix of the DTE address.

NETaddr

Syntax
```
ADD !<port> -IP NETaddr <IP address> [<subnet mask> [Ones | Zeros
  [MTU]]] | UnNumbered
DELete !<port> -IP NETaddr <IP address>
SETDefault !<port> -IP NETaddr = <IP address> [<subnet mask> [Ones
  | Zeros [MTU]]] | UnNumbered
SHow [!<port> | !*] -IP NETaddr
```

Default No default

Description The NETaddr parameter assigns an IP address to the specified port and configures a directly connected IP network or subnet on a specified port.

Use SETDefault to configure the primary address to be used as a source address for originating packets. Use the ADD command to configure secondary addresses. If you do not use SETDefault, the first ADD command specifies the primary address. If a subsequent SETDefault command is entered, the SETDefault address becomes primary, and the first ADD address becomes secondary.

When NETaddr is configured for port 0, the router is affected in the following ways:

- The Internet address specified is assigned to all interfaces. This means that the entire router has a single IP address.
- Any IP networks previously configured on an interface are no longer considered configured networks.
- The router becomes an IP host. If you want the router to perform IP routing, you must not configure NETaddr on port 0. Typically, the router should be an IP host when it is performing bridging or when it is routing other protocols and bridging IP packets, as opposed to routing functions or network management functions that require the IP protocol stack.

  For example, you would configure NETaddr on port 0 if the router were configured for bridging only and you wanted to use Telnet or Simple Network Management Protocol (SNMP) to access the router.
- The Internet address is the address of the system on the specified port.

Values <IP address> The IP address to be assigned to the port.

<subnet mask> Specifies the way in which the subnet mask is specified depends on whether the IP network is subnetted:

If the IP network is subnetted, the subnet mask value is required. The mask must be in dotted decimal format as a contiguous string of left-justified 1 bits.

If the IP network is not subnetted, the subnet mask must be the same as the network mask. The following list shows the appropriate network mask for each class of network:

Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

If no subnet mask is specified, it is assumed to be the same as the network mask. Therefore, if the network is not subnetted, you do not need to include the subnet mask.

Ones | Zeros Specifies the Ones or Zeros options configure the IP broadcast address for packets that originate from this router. Ones indicates that the host portion of the Internet address contains all 1 bits. Zeros indicates that it contains all 0 bits. For packets that are received, all broadcast formats are recognized.

MTU Specifies that the maximum transmission unit (MTU) is the maximum size frame that is supported by the underlying network. Specify it in bytes.

UnNumbered When the UnNumbered option is specified, the router transmits and receives IP packets over the port without assigning an IP address to the port. This option is meaningful only over PPP links.

If the Internet address specified is 0.0.0.0, then the primary IP network or subnet previously configured for the specified port is no longer considered configured for that port. Because no network is configured for this particular port, any received IP packet is discarded. To unconfigure a port, set its address to 0.0.0.0.

By default, the subnet mask is the same as the network mask. By default, the Ones option is selected. The specification of optional Ones | Zeros and an optional MTU value requires the entry of a subnet mask.

SHow -IP NETaddr displays the status and address information for the directly connected IP networks. When a port number is specified, the directly connected IP networks for that port are displayed; when no port number is specified, configured networks on all ports are displayed.

QueuePriority

Syntax

```
SETDefault -IP QueuePriority = <H | M | L | DEFault>
SHow -IP QueuePriority
```

Default DEFault

Description The QueuePriority parameter assigns a priority to an IP-routed packet destined for a wide area network using Point-to-Point Protocol (PPP), phone line gateway (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 bandwidth allocation, refer to Chapter 32 in *Using NETBuilder Family Software*.

You can also display the setting of this parameter with the SHow command.

ReassemblyTime

Syntax

```
SETDefault -IP ReassemblyTime = <seconds>(1–255)
SHow -IP ReassemblyTime
```

Default 15

Description The ReassemblyTime parameter specifies the number of seconds that the IP layer waits for all IP fragments of an IP datagram to be received. This parameter applies only to packets specifically destined for the local router. If any fragment is not received in the time specified, an ICMP Time Exceeded message is sent to the system from which the fragments originated.

RemoteAddress

Syntax

```
SETDefault !<port> -IP RemoteAddress = <IPaddress>
SHow [!<port> | !*] -IP RemoteAddress
```

Default No default

Description The RemoteAddress parameter maps a port, instead of a MAC address, to an IP address in a Boundary Routing configuration. The port corresponds to the interface on which a RARP request is received, and the IP address corresponds to the IP address supplied by the local router to the peripheral node.

The Reverse Address Resolution Protocol (RARP) server first searches the RARP IP Address Translation Table for a match for the source hardware address in the request. If a match is found, the RARP server sends a reply (the IP address) to the RARP client. If the RARP server cannot find an address match and Boundary Routing is enabled on the port on which the request was received, the RARP server checks whether an IP remote address was assigned to the port over which the RARP request was received. If one is found, that IP address is sent to the RARP client.

For more information, refer to "ADDRess" on page 29-2.

ROUte

Syntax

```
ADD -IP ROUte <IP address> [<mask>] {<gateway> | !<port>} <metric>
  [Override]
DELete -IP ROUte <IP address> [<mask>] {<gateway> | !<port>}
SHow -IP ROUte [<IP address>]
```

Default No default

Description The ROUte parameter enters a static route into the IP routing table and displays the contents of the IP Routing Table. The routes that you add and delete through this parameter are called "static routes." You can add as many static routes as desired.

Values

<IP address>	Can be the address of a network, a subnet, or a host route specification. If <IP address> is 0.0.0.0, the route is called the "default route."
<mask>	A mask can be specified while adding static routes. Mask 0.0.0.0 is displayed for the default route. Routes with natural masks display the natural masks. If an optional mask is specified with the DELete command, a static entry is deleted only if it matches the specified address/mask. If a mask is not specified with the DELete command, and multiple entries exist with the same destination address but different masks, the first entry that matches the given destination address is deleted.
<gateway>	The address of the first gateway through which a forwarded packet passes before reaching its destination.
!<port>	The !<port> syntax specifies the next hop over a numbered or unnumbered PPP link. Because only one destination exists over this serial link, once the local router's outgoing port ID is specified, the remote IP address (gateway address) is no longer necessary. When the port number is specified, the port owner must be PPP for the command to take effect.
<metric>	Represents the number of hops required for the packet to reach its destination. The permissible values range from 0 through 255.
Override	Allows a learned route (dynamic route) to take precedence over a static route. That is, the router can use a gateway other than the one specified to forward a packet to the specified destination Internet address. If Override is not specified, the router uses the static route to forward packets to this Internet address.

To display the static routes configured, use SHow -IP ROUte. If the gateway address is on a directly connected network, the route is usable and is stored in the IP Routing Table; otherwise, it is saved only on disk. Table 29-3 lists the type of routes affected by various commands using the ROUte and AllRoutes parameters.

Table 29-3 Types of Routes Affected by Various Commands

Commands	Type of Route
ADD ROUte	Static
DELete ROUte	Static
SHow ROUte	Static
FLush AllRoutes	Dynamic
SHow AllRoutes	Static and dynamic

Example 1 The following is an example of the ADD -IP ROUte command:

```
ADD -IP ROUte 129.213.0.0 128.1.1.1 5 O
```

This example adds the address 129.213.0.0 to the routing table. The first gateway that a packet destined for this address has to pass through is 128.1.1.1. To reach the host, the packet has to pass through five routers. Because the Override option is included, the router may forward the packet using a learned route.

Example 2 The following is an example of the ADD -IP ROUte command specifying a mask:

```
ADD -IP ROUte 130.10.112.0 255.255.252.0 10.0.0.24 4
```

This example adds the address 130.10.112.0 to the routing table. Because the mask is present, the route is not a host route, but a route to a subnet with address 130.10.112.0. The first gateway that a packet destined for this address has to pass through is 10.0.0.24. To reach the subnet, the packet has to pass through four routers.

Example 3 To delete a static route, use the DELete command. You can delete both valid and invalid routes with the DELete command. The following is an example of the DELete -IP ROUte command:

```
DELete -IP ROUte 129.213.0.0 128.1.1.1
```

SecAuthIn

Syntax

```
ADD !<port> -IP SecAuthIn <authority> [<authority>...] [ANY]
  <authority> = GENSER | SIOP | SCI | NSA | DOE | NONE | <value>
DELete !<port> -IP SecAuthIn <authority> [<authority>...] [ANY]
  <authority> = GENSER | SIOP | SCI | NSA | DOE | NONE | <value>
SHow [!<port> | !*] -IP SecAuthIn
```

Default GENSER

Description The SecAuthIn parameter creates, modifies, or displays table entries per port of protection authority flags, which can be present in a datagram received by a NETBuilder system using IP security options. The protection authority flags identify the agency that specifies the protection rules for the receiving and processing of information contained in the datagram received by a specific port. Each entry in the table can be a combination of multiple protection authority flags.

When IP security options are enabled with the SETDefault -IP CONTrol parameter, the system compares the protection authority flags in the IP header of the incoming datagram with the protection authority flags in the IP Security Configuration Table for the port. If the protection authority flags match, in addition to the classification level specified by the SETDefault -IP SecLEVel command, the system can receive the datagram and begin processing it. If the ANY value is specified in addition to other protection authority flags in a table entry, then the system accepts incoming datagrams that are a subset of the protection authority flags in the table entry.

If the protection authority flags in the incoming datagram's header do not match the IP Security Configuration Table entries for the specified port, the system drops the datagram and generates an ICMP.

The table can contain as many entries as desired for the system.

Values	GENSER, SIOP, SCI,NSA,DOE	Identifies various protection authorities. More than one protection authority can be specified.
	NONE	No protection authority flags are set.
	ANY	If ANY is set, the protection authority flags in an incoming datagram need only to be a subset of the protection authority flags in the table entry. If ANY is not set, an exact match is required.
	<value>	A two-byte hexadecimal number that can be specified for the protection authority instead of entering the actual protection authority name. It must follow the rules for specifying a valid protection authority flag field. If only the upper byte is needed, the lower byte must be all zeros and bit 7 of the upper byte must be zero. If any of the bits in the lower byte is nonzero, bit 7 in the upper byte must be 1.

SecAuthOut

Syntax

```
ADD !<port> -IP SecAuthOut <authority> [<authority>...] [ANY]
  <authority> = GENSER | SIOP | SCI | NSA | DOE | NONE | <value>
DELete !<port> -IP SecAuthOut <authority> [<authority>...] [ANY]
  <authority> = GENSER | SIOP | SCI | NSA | DOE | NONE | <value>
SHow [!<port> | !*] -IP SecAuthOut
```

Default GENSER

Description The SecAuthOut parameter creates, modifies, or displays table entries per port of protection authority flags, which can be present in a datagram transmitted by a NETBuilder system using IP security options. The protection authority flags identify the agency that specifies the protection rules for the transmission of information contained in the datagram. This parameter does not apply to end system configurations.

When you enable IP security options using the SETDefault -IP CONTrol parameter, the system compares the protection authority flags in the IP header of the datagram to be transmitted with the protection authority flags in the IP Security Configuration Table for the port. If the protection authority flags match, in addition to the classification level specified by the SETDefault -IP SecLEVel command, the system can transmit the datagram over the specified port. If the ANY value is specified in addition to other protection authority flags in a table entry, then the system can transmit datagrams that are a subset of the protection authority flags in the table entry.

If the protection authority flags in the header of the datagram that are to be transmitted do not match the IP Security Configuration Table entries for the specified port, the system drops the datagram and an ICMP message is sent.

The table can contain as many entries as desired for the system.

Values

GENSER, SIOP, SCI, NSA, DOE — Identifies various protection authorities. More than one protection authority can be specified.

NONE — No protection authority flags are set.

ANY — If ANY is set, the protection authority flags in a transmitted datagram need only to be a subset of the protection authority flags in the table entry. If ANY is not set, an exact match is required.

<value> — A two-byte hexadecimal number that can be specified for the protection authority instead of entering the actual protection authority name. It must follow the rules for specifying a valid protection authority flag field. If only the upper byte is needed, the lower byte must be all zeros and bit 7 of the upper byte must be zero. If any of the bits in the lower byte is nonzero, bit 7 in the upper byte must be 1.

SecCONTrol

Syntax

```
SETDefault !<port> -IP SecCONTrol = ([EXTended | NoEXTended],
  [LabelXtraAdd | NoLabelXtraAdd], [LabelAdd | NoLabelAdd],
  [BasicFirst | NoBasicFirst], [LabelStrip | NoLabelStrip],
  [LabelExtStrip | NoLabelExtStrip])
SHow [!<port> | !*] -IP SecCONTrol
```

Default

NoEXTended, NoLabelXtraAdd, NoLabelAdd, NoBasicFirst, NoLabelStrip, NoLabelExtStrip

Description

The SecCONTrol parameter configures IP security options (see the “Values” section).

The BasicFirst | NoBasicFirst, LabelAdd | NoLabelAdd, and LabelStrip | NoLabelStrip value pairs do not apply to end system configurations.

Values

EXTended | NoEXTended — Allows or disallows datagrams with extended security options to be received from or transmitted to a particular port.

LabelXtraAdd | NoLabelXtraAdd — If LabelXtraAdd is specified, the label specified by the parameter SecLabelXtra is added as the first option to all IP packets leaving that port.

BasicFirst | NoBasicFirst — Ensures that the basic security option is always transmitted as the first option in the datagram if set to BasicFirst. If the basic security option is not the first option, then it is moved to make it the first option. If set to NoBasicFirst, the options are transmitted as they are. Use the BasicFirst option for devices that require the security option to be the first option.

LabelAdd | NoLabelAdd — Ensures that all datagrams leaving the specified port have labels attached to them if set to LabelAdd. If an outgoing datagram does not have a label, the default label, computed for the datagram on receipt, is attached to it before transmission. If set to NoLabelAdd, then datagrams without labels are allowed to be transmitted. The default label is not attached to the datagram.

LabelStrip | NoLabelStrip — Strips any basic security option present in the datagram before transmission through that port if set to LabelStrip. Stripping is done after all security processing has been done. If set to NoLabelStrip, the label is transmitted as is.

LabelExtStrip | NoLabelExtStrip — Strips the first (and only the first) extended security option in an IP packet leaving the port.

SecFileServer

Syntax

```
SETDefault -IP SecFileServer = Yes | No
SHow -IP SecFileServer
```

Default No

Description The SecFileServer parameter enables or disables security option processing when communicating with a file server that is identified by the -SYS FileServerAddr parameter. If you want the NETBuilder system to perform security processing of packets received from the file server, change the default to Yes.

Values

Yes — Enables security processing of packets received from or being sent to the file server.

No — Disables security processing of packets received from the file server. Any security options in datagrams that are received from the file server are ignored. The system strips security options from datagrams before transmission to the file server.

SecLabelDefault

Syntax

```
SETDefault !<port> -IP SecLabelDefault = NONE | <level> <auth>
  [<auth> ...]
<level> = TopSECret | SECret | CONFidential | UNCLass
<authority> = GENSER | SIOP | SCI | NSA | DOE | NONE | <value>
SHow [!<port> | !*] -IP SecLabelDefault
```

Default NONE

Description The SecLabelDefault parameter configures a port with a classification level and protection authority to be associated with incoming datagrams. If set to NONE, each datagram must have a label. If the port is configured for a particular label, a datagram without a label is accepted, and the label configured for the port is attached to the datagram before any processing is started. The label is not automatically attached to the datagram on transmission; use the SecCONTrol parameter with the LabelAdd value to attach it.

The SecLabelDefault parameter is useful for networks that have systems that cannot generate datagrams with labels. This parameter does not apply to end system configurations.

Values		
	TopSECret, SECret, CONFidential, UNCLass	If a datagram is received that has no label, a label with one of these classification levels will be generated for it.
	GENSER, SIOP, SCI, NSA, DOE	Identifies various protection authorities. More than one protection authority can be specified.
	NONE	The datagram label has no protection authority flags.
	<value>	Indicates a two-byte hexadecimal number that can be specified for the protection authority instead of entering the actual protection authority name. It must follow the rules for specifying a valid protection authority flag field. If only the upper byte is needed, the lower byte must be all zeros and bit 7 of the upper byte must be zero. If any of the bits in the lower byte is nonzero, bit 7 in the upper byte must be 1.

SecLabelSys

Syntax

```
SETDefault !<port> -IP SecLabelSys = NONE | <level> <auth>
  [<auth>...]
<level> = TopSECret | SECret | CONFidential | UNCLass
<authority> = GENSER | SIOP | SCI | NSA | DOE | NONE | <value>
SHow [!<port> | !*] -IP SecLabelSys
```

Default UNCLass GENSER

Description The SecLabelSys parameter configures a port with a label (classification level and protection authority) for datagrams originated by the system, such as the PING command. The setting of this parameter must form a label that is legal as specified by SecLEVel and SecAuthOut.

The value of this parameter also determines the security labels to be used in ICMP error messages that are generated as a result of security option processing.

Values		
	TopSECret, SECret, CONFidential, UNCLass	The datagram originated by the system and sent through a specified port must have one of these classification levels.
	GENSER, SIOP, SCI, NSA, DOE	Identifies various protection authorities. More than one protection authority can be specified.
	NONE	Indicates that no protection authority flags are set.
	<value>	Indicates a two-byte hexadecimal number that can be specified for the protection authority instead of entering the actual protection authority name. It must follow the rules for specifying a valid protection authority flag field. If only the upper byte is needed, the lower byte must be all zeros and bit 7 of the upper byte must be zero. If any bit in the lower byte is nonzero, bit 7 in the upper byte must be 1.

SecLabelValues

Syntax

```
SETDefault -IP SecLabelValues = RFC1038 | RFC1108
SHow -IP SecLabelValues
```

Default RFC1108

Description The SecLabelValues parameter allows you to use either RFC 1108 or RFC 1038 in an internetwork; you cannot use both.

When processing IP security options, RFC 1108 is followed by default. The constants (byte values) used for the classification levels and the protection authority flags in RFC 1038 and RFC 1108 are different, making them incompatible. The process for handling basic IP security options is the same in the two RFCs except for a few differences as to when ICMP messages are generated.

The implementation in this software follows RFC 1108. Setting this parameter to RFC 1038 only causes the SecLabelValues defined for that RFC to be used.

Values	RFC1108	Causes the system to use constants defined in RFC 1108.
	RFC1038	Causes the system to use constants defined in RFC 1038.

SecLabelXtra

Syntax

```
SETDefault -IP SecLabelXtra = “<string>”
SHow -IP SecLabelXtra
```

Default “133/13/252/0/0/0/0/0/0/0/0/0/0/1/1/1/”

Description The SecLabelXtra parameter contains a string that can be added to any IP packet. If SecCONTrol for a port is set to LabelXtraAdd, the SecLabelXtra string is added to the beginning of the option list for any IP packet leaving the port.

The string is specified as values of individual bytes given as a decimal number, each byte separated by a slash (/). The total number of bytes specified must be a multiple of four. The IP option NOOP (value 1) can be specified to make the length a multiple of four bytes.

The string must end with a slash (/). Because no syntax checking is done, the string must be correctly specified.

If no value is to be specified, set it to an empty string by entering:

```
SETDefault -IP SecLabelXtra = “ ”
```

SecLEVel

Syntax

```
SETDefault !<port> -IP SecLEVel = <min-level> [<max-level>]
<level> = TopSECret | SECret | CONFidential | UNCLass
SHow [!<port> | !*] -IP SecLEVel
```

Default UNCLass (min-level and max-level)

Description The SecLEVel parameter specifies a single classification level or range of classification levels within which the classification level of any datagram entering or leaving a specified port must fall. If the maximum level is not specified, then it takes the same value as the minimum level.

Values	TopSECret | SECret |CONFidential | UNCLass	Specifies a classification level or range of levels for a port.

SMDSGroupAddr

Syntax

```
ADD -IP SMDSGroupAddr <IP address> $<E0–E999999999999999>
DELete -IP SMDSGroupAddr <IP address>
SHow -IP SMDSGroupAddr
SHowDefault -IP SMDSGroupAddr
```

Default No default

Description The SMDSGroupAddr parameter defines a multicast address for use by routing protocols within a logical IP subnetwork (LIS) on the SMDS network. An LIS is a group of SMDS nodes running IP that all use the same IP subnet for the SMDS interface. A 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, the software pads it on the right with Fs.

Values

<IP address>	Specifies the IP network address, for example, 129.2.0.0.
<E0–E999999999999999>	Specifies the format for an SMDS group, or multicast, address. The group address type is used to route data to all routers 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, it is padded on the right with Fs. An SMDS group address is the only valid address that can be used with this parameter.

X25PROFileid

Syntax

```
SETDefault [!<port>] -IP X25PROFileid = <user profile id> (0–9999)
SHow [!<port> | !*] -IP 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 IP packets. A value of 0 indicates that no specific X.25 user profile is configured for IP packets.

X25ProtID

Syntax

```
SETDefault !<port> -IP X25ProtID = <protocol id> (1 octet)
SHow [!<port> | !*] -IP X25ProtID
```

Default 0xCC

Description The X25ProtID parameter applies to routing IP over an X.25 public data network (PDN). It specifies a protocol identifier to be included in all outgoing X.25 call request packets indicating that subsequent packets transmitted are IP packets. Enter a value between 1 and FF.

When a packet reaches its destination, the destination router verifies this protocol identifier against its own protocol ID. If they match, the incoming packet is accepted. If they do not match (IP is not running on the destination device), the packet is discarded. The value must not conflict with the values used by other protocols.

30 IPName Service Parameters

This chapter describes all the parameters in the Internet Protocol Name (IPName) Service. The IPName Service determines how names are resolved for Transmission Control Protocol/Internet Protocol (TCP/IP) connections. The bridge/router uses these parameters when functioning as an X.25 connection service gateway for incoming automatic and extended connections to IP Internet-attached TCP/IP hosts that support Telnet or Rlogin.

Table 30-1 lists the IPName Service parameters and commands.

Table 30-1 IPName Service Parameters and Commands

Parameters	Commands
CAChe	FLush, SHow
CONFiguration	SHow
DomainName	SETDefault, SHow
NAME	ADD, DELete, SHow
NameServiceType	SETDefault, SHow
PrimaryNameServer	SETDefault, SHow
SecondaryNameServer	SETDefault, SHow

CAChe

Syntax

```
FLush -IPName CAChe
SHow -IPName CAChe
```

Default No default

Description The CAChe parameter clears or displays the domain name cache. Caching allows the domain name resolver to quickly retrieve name and address associations from the local cache. The gateway automatically stores the names and addresses in the cache as they are requested.

The gateway can keep the contents of the cache active for several days. The resolver automatically deletes entries from the cache when they become outdated; that is, when the timeout value associated with each entry expires.

If you obsolete or change domain names on the domain name server, the name/address associations still present in the cache are invalid. By using the FLush -IPName CAChe command, you can quickly clear the contents of the domain name cache on the gateway. CAChe can operate only when -IPName NameServiceType is set to domain.

CONFiguration

Syntax

```
SHow -IPName CONFiguration
```

Default No default

Description The CONFiguration parameter displays the values of the IPName parameters.

DomainName

Syntax

```
SETDefault -IPName DomainName = “<string>”
SHow -IPName DomainName
```

Default No default

Description The DomainName parameter specifies the default domain string for all domain names entered on the gateway. These defaults are automatically appended to the local name unless overridden when the name is entered. This parameter can operate only when -IPName NameServiceType is set to Domain.

Domain names consist of labels separated by periods (“.”) and are limited to 128 characters. For example, the name “eng.3com” specifies that eng is a subdomain of 3com. The gateway appends the default domain name to all names that do not contain a period.

Example To set the default domain name, enter the following command:

```
SETDefault -IPName DomainName = “eng.3com”
```

After this command is executed, enter this Connect command:

```
Connect host1
```

The gateway sends “host1.eng.3com” out in the Domain request. However, the default domain name is not appended to the name request after this command.

When you include a period in the command, it signifies a different domain, as shown in the following command:

```
Connect host1.xyz
```

NAME

Syntax

```
ADD -IPName NAME <Internet-name> <Internet-address>
DELete -IPName NAME <Internet-name>
SHow -IPName NAME [Internet-name]
```

Default No names defined

Description The NAME parameter assigns a name to an address, deletes a name from the database, or displays the names in the database.

The ADD and DELete commands apply only when -IPName NameServiceType is set to Ien, and when the PrimaryNameServer or SecondaryNameServer is set to the address of the gateway. This parameter is useful only if the gateway can be an IEN name server. You can use SHow -IPName NAME no matter what the -IPName NameServiceType is.

If Domain name service is used, a database that acts as the name server must be present on the network. The ADD and DELete commands are not useful in this situation because the gateway supports only the Domain name resolver portion of the Domain name service, not the database.

ADD -IPName NAME assigns a name to an address and includes this name and address pair in the IEN name database. DELete -IPName NAME deletes a name from the database.

SHow -IPName NAME * displays all the names in the database. The asterisk (*) applies to IEN116 only. To display the Internet address of a specific Internet name, use SHow -IPName NAME followed by the Internet name.

NameServiceType

Syntax

```
SETDefault -IPName NameServiceType = [Ien | Domain]
SHow -IPName NameServiceType
```

Default Domain

Description The NameServiceType parameter specifies the type of name service running on the gateway. The gateway examines the NameServiceType parameter when resolving a command that specifies a name, such as the Connect or SHow -IPName NAME commands.

Values

Ien	Indicates the name-to-address request is resolved using the Internet Engineering Notes (IEN) protocol. The IEN name service can be maintained on the gateway disk.
Domain	Indicates the name-to-address request is resolved using the Domain Name Service requirements.

PrimaryNameServer

Syntax

```
SETDefault -IPName PrimaryNameServer = <nameserver Internet
  address>
SHow -IPName PrimaryNameServer
```

Default 0.0.0.0

Description The PrimaryNameServer parameter specifies the address of the gateway's primary name server. All Internet and Domain name requests are sent first to the name server specified by this parameter.

For the IEN name servers, if PrimaryNameServer is undefined (that is, 0.0.0.0), the gateway refers name requests to the boot source (local floppy).

For Domain name servers, if the PrimaryNameServer address is undefined (that is, 0.0.0.0) or contains the address of the gateway, the name service skips to the secondary name server. If the secondary name server is also undefined, queries are sent to the address of the file server (refer to "FileServerAddr" on page 58-7).

SecondaryNameServer

Syntax

```
SETDefault -IPName SecondaryNameServer =
  <nameserver Internet address>
SHow -IPName SecondaryNameServer
```

Default 0.0.0.0

Description The SecondaryNameServer parameter specifies the address of the secondary name server. The gateway sends all Internet name requests to the name server specified by this parameter if no response from the primary name server is received.

31

IPX SERVICE PARAMETERS

This chapter describes all the parameters that are related to Internetwork Packet Exchange (IPX) Protocol routing. Table 31-1 lists the IPX Service parameters and commands.

Table 31-1 IPX Service Parameters and Commands

Parameters	Commands
ADDRess	ADD, DELete, FLush, SHow, SHowDefault
AllRoutes	FLush, SHow
AllServers	FLush, SHow
CONFiguration	SHow
CONTrol	SETDefault, SHow, SHowDefault
Delay	SETDefault, SHow, SHowDefault
DIAGnostics	FLush, SHow
InternalNET	SETDefault, SHow, SHowDefault
MaxHop	SETDefault, SHow
MTU	SETDefault, SHow, SHowDefault
NETnumber	ADD, DELete, SETDefault, SHow, SHowDefault
PathSplit	SETDefault, SHow
ROUte	ADD, DELete, SHow, SHowDefault
RouterName	SETDefault, SHow, SHowDefault
SERver	ADD, DELete, SHow
SMDSGroupAddr	SETDefault, SHow, SHowDefault
SPoofCONTrol	SETDefault, SHow, SHowDefault
X25PROFileid	SETDefault, SHow, SHowDefault
X25ProtID	SETDefault, SHow, SHowDefault

ADDRess

Syntax

```
ADD !<port> -IPX ADDRess <media address> [%<host>]
DELete !<port> -IPX ADDRess <media address>
FLush !<port> -IPX ADDRess
SHow [!<port> | !*] -IPX ADDRess
SHowDefault [!<port> | !*] -IPX ADDRess
```

Default No default (IPX Address Mapping table is empty)

Description The ADDRess parameter modifies and displays the list of host address-to-media address mapping. It is a port-dependent parameter.

ADDRess maps the media access control (MAC) address of a remote host to the corresponding X.25, Frame Relay, data link connection identifier (DLCI), Switched Multimegabit Data Service (SMDS) address, or Asynchronous Transfer Mode (ATM) virtual circuit identifier (VCID).

The IPX Protocol can run dynamically over SMDS by configuring the SMDSGroupAddr parameter. For more information, refer to Chapter 44 in Using NETBuilder Family Software.

The host address consists of the MAC address (12 hexadecimal digits) preceded by a percent sign (%).

You must configure ADDRess if you want IPX to pass routing information over X.25, Frame Relay, or ATM. When no addresses are configured and neighbor policies are disabled, IPX RIP traffic is not passed over X.25, Frame Relay, or ATM. Refer to Chapter 13 in Using NETBuilder Family Software.

Values You can specify the following <media address> formats with the ADD command:

<#X.25 address>	Adds X.25 neighbors. It indicates the data terminal equipment (DTE) address of the closest router through which the network can be reached.
<@DLCI>	Adds Frame Relay neighbors.
<$SMDS address>	Use an SMDS individual address to add SMDS neighbors, for example, $c14087645400. Because the IPX Protocol dynamically learns SMDS neighbors, there is no need to add neighbors that use an SMDS group address.
<&VCID>	Use the local VCID of the permanent virtual circuit (PVC) to statically add ATM neighbors. The VCID is an alias that identifies the ATM address VPI.VCI and is configured using the -ATM PermVirCircuit parameter. For more information, refer to “PermVirCircuit” on page 7-2.

AllRoutes

Syntax

```
FLush -IPX AllRoutes
SHow -IPX AllRoutes [Short | Long | <NETnumber>]
```

Default Short

Description The AllRoutes parameter displays all known routes in the routing table, including static, dynamic, and default. If a default route is currently in use, the display indicates its existence with the keyword “default” in the display. Default routes are also listed first in the display.

FLush -IPX AllRoutes removes all dynamically learned routes from the routing table. Static entries are not removed by the FLush command. The IPX Routing Table display includes port numbers, network numbers, gateway addresses, hop counts, and the delay or cost involved. Asterisks in column 1 indicate static routes.

Values

Short	Produces a short-form routing display that shows only network numbers and hop counts.
Long	Generates a long-form routing table that includes port numbers, network numbers, gateway addresses, hop counts, and costs.
<NETnumber>	Generates a routing table display that includes the port number, gateway address, hop counts, and costs for the specified network number.

AllServers

Syntax

```
FLush -IPX AllServers
SHow -IPX AllServers [Short | Long | Best | <string>]
```

Default Short

Description The AllServers parameter displays all known servers in the IPX Server Table, which shows port numbers, server types, server addresses, hop counts, and server names.

The FLush AllServers command removes all service information from the Service Advertisement Protocol (SAP) Table and sends out SAP requests over the serial lines (if any) to learn new server information. Incremental (nonperiodic) SAP updates instead of periodic updates, which occur every 60 seconds by default, can be used on the serial interfaces in order to reduce the SAP traffic, and is configurable using -SAP CONTrol.

Values

Short Produces a short-form display of only server names and hop counts.

Long Generates a long-form display including port numbers, server types, server addresses, hop counts, and server names.

Best Displays the closest servers in long form.

<string> Generates a server table display including port number, server type, server address, and hop count for the specified server name, which is enclosed in quotes, for example, “Engineering_Server.”

CONFiguration

Syntax

```
SHow [!<port> | !*] -IPX CONFiguration
```

Default No default

Description The CONFiguration parameter displays the current IPX configuration parameters. If no port number is specified, SHow -IPX CONFiguration displays active information; active means CONTrol is set to ROute and NETnumber is configured. In the sample display below, CONTrol is not set to ROute and the following message is displayed:

```
IPX is not enabled. Please configure CONTrol and assign NETnumbers
```

Assuming CONTrol is set to ROute, it displays active configuration information for ports assigned with IPX network numbers. This has been changed in an effort to reduce console output. In the case of static routes, address mapping, policies and neighbors, even headers are suppressed if their corresponding tables are empty.

CONTrol

Syntax

```
SETDefault !<port> -IPX CONTrol = ([ROute | NoROute], [WanBcast |
  NoWanBcast], [Checksum | NoChecksum], [IpxWan | NoIpxWan])
SHow [!<port> | !*] -IPX CONTrol
SHowDefault [!<port> | !*] -IPX CONTrol
```

Default NoROute, WanBcast, NoChecksum, NoIpxWan

Description The CONTrol parameter enables or disables IPX routing for the router, and specifies whether WAN broadcast packets (packet type = 0x14) are forwarded. Some application programs, such as NetBIOS, require that broadcast packets be propagated throughout an Internet. The IPX router forwards these packets when CONTrol is set to WanBcast.

When communicating with a bridge/router running a software version prior to 7.0 on a WAN link, the -IPX CONTrol parameter must be set to NoIpxWan and the -NRIP CONTrol parameter set to PEriodic. Be sure the -SAP CONTrol parameter is set to NoPEriodic. For more information, refer to "CONTrol" on page 49-4.

Values

ROute | NoROute	If ROute is selected, IPX routing is enabled. If NoROute is selected, IPX routing is disabled.
WanBcast |NoWanBcast	Specifies whether WAN broadcast is supported.If WanBcast is selected, IPX router makes copies of the WAN broadcast packets and forwards them to all ports other than the one received on. If NoWanBcast is selected, IPX router drops packets to prevent excessive traffic. When WAN broadcast packets go beyond 8 hops without reaching their destination, they are discarded, regardless of these settings.
Checksum | NoChecksum	If Checksum is selected, a checksum is generated in outgoing IPX packets. If NoChecksum is selected, a checksum is not added to the outgoing IPX packets.
IpxWan | NoIpxWan	If IpxWan is selected, IPXWAN is enabled on the specified port. If NoIpxWan is selected, IPXWAN is disabled on the specified port. The InternalNET and RouterName parameters must also be configured.

Delay

Syntax

```
SETDefault [!<port>] -IPX Delay = <ticks>(1-65535) | Default
SHow [!<port> | !*] -IPX Delay
SHowDefault [!<port> | !*] -IPX Delay
```

Default Computed based on the media baud rate. For all LAN media, the value is 1. For low speed serial lines, the value can be higher.

Description The Delay parameter sets the cost of a path. A tick is 1/18th of a second.

DIAGnostics

Syntax

```
FLush [!<port>] -IPX DIAGnostics
SHow [!<port> | !*] -IPX DIAGnostics
```

Default No default

Description The DIAGnostics parameter displays the current status of the IPX router. This parameter reports most of the potential configuration errors, run timer errors, incompatibility issues, boundary conditions, and resource allocation failures that may occur in IPX, NetWare Routing Information Protocol (NRIP), and SAP.

InternalNET

Syntax

```
SETDefault -IPX InternalNET = &<number> (0–FFFFFFFD)
SHow -IPX InternalNET
SHowDefault -IPX InternalNET
```

Default No default (no internal network number assigned)

Description The InternalNET parameter assigns an internal network number to the router. The router uses this internal number during IPXWAN negotiation; the router with the lowest internal network number becomes the slave to the router with the highest internal network number (the master) during link establishment and information exchange.

The InternalNET number must be unique throughout the IPX Internet. This network number is advertised in NRIP updates to other routes.

If you intend to run the NetWare Link Services Protocol (NLSP) as your routing protocol, or if you use NetwarePING for diagnostics, you must first configure the InternalNET parameter. These protocols use this network as a source address in many packets.

MaxHop

Syntax

```
SETDefault -IPX MaxHop = <hop count> (16–255)
SHow -IPX MaxHop
```

Default 16

Description The MaxHop parameter specifies the maximum number of hops allowed for forwarding IPX packets. NLSP allows discovery of routes more than 16 hops away and forwarding of packets to those destinations. Setting MaxHop to a value greater than 16 allows you to take advantage of this feature of NLSP in order to build large IPX networks.

With traditional RIP and SAP protocols, IPX packets travel only up to 16 routers (hops) before being discarded. RIP and SAP protocols also use the number 16 to mean that a destination is unreachable. Changing MaxHop has no effect on the operation of RIP or SAP. These protocols still treat 16 as infinity (unreachable).

All NLSP routers should be configured to the higher MaxHop count; otherwise, IPX packets may not travel beyond 16 routers.

MTU

Syntax

```
SETDefault !<port> -IPX MTU = <number> (576-1500)
SHow [!<port> | !*] -IPX MTU
SHowDefault [!<port> | !*] -IPX MTU
```

Default 576

Description The MTU parameter affects only the size of routed packets that originate from the same router. Higher values allow the router to send larger packets. Setting this parameter does not affect the handling of user data packets. The router accepts and forwards all IPX packets up to the maximum size supported by the underlying media.

NETnumber

Syntax

```
ADD !<port> -IPX NETnumber &<number> (0–FFFFFFFD) [Ethernet | Ieee
  | Llc | Snap | X25 | PPP | Frame | SMDS | ATM]
DELete !<port> -IPX NETnumber &<number>
SETDefault !<port> -IPX NETnumber = &<number> (0–FFFFFFFD)
  [Ethernet | Ieee | Llc | Snap | X25 | PPP | Frame | SMDS | ATM]
SHow [!<port> | !*] -IPX NETnumber
SHowDefault [!<port> | !*] -IPX NETnumber
```

Default No default (no NETnumber assigned)

Description The NETnumber parameter specifies the IPX network number assigned to a port and determines the header format to be used by that port.

Enter a unique network number between &1 and &FFFFFFFD. The network numbers &0, &FFFFFFFE, and $FFFFFFFF are reserved.

To delete a network number from a port, use one of the following syntaxes:

```
SETDefault !<port> -IPX NETnumber = 0
DELete !<port> -IPX NETnumber &<netnumber>
```

To configure a network number, assign any unique network number between &1 and &FFFFFFFD to that port, and select a header format from the list of values that follows.

You can configure NETnumber with the SETDefault or ADD command. The network number added using SETDefault is called a primary network and takes precedence over a secondary network. Primary networks are marked with asterisks (*). Networks that are added with the ADD command are called secondary networks, and priority is given according to the order in which networks are added.

On Ethernet ports, you can add up to four different networks per port, but they need different header formats. To delete a primary network number, use:

```
SETDefault !<port> -IPX NETnumber
```

To delete a secondary network, use:

```
DELete !<port> -IPX NETnumber
```

NETBuilder supports four encapsulation formats on Ethernet (Ethernet V2, IEEE, logical link control (LLC), and Subnetwork Access Protocol (SNAP)), three on token ring (IEEE, LLC, and SNAP), and three on FDDI (IEEE, LLC, and SNAP). For more information on which encapsulation formats are available and how to configure them, refer to “Configuring Secondary Networks with Different Header Formats” on page 13-2 of *Using NETBuilder Family Software.*

Values

Ethernet	Ethernet V2 headers are used on outgoing packets.
Ieee	An IEEE 802.3 header is immediately followed by IPX data packets used on outgoing packets. This is the default value on Ethernet and phone line gateway (PLG) lines.
Llc	IPX data packets are encapsulated in the IEEE 802.3 header followed by IEEE 802.2 (LLC) header. The destination service access point (DSAP) and source service access point (SSAP) for IPX is 0xE0.
Snap	IPX packets are encapsulated in the SNAP header. 0x8137 is reserved for the IPX protocol identifier.

X25	IPX packets are encapsulated in the X.25 header format.
PPP	IPX packets are encapsulated in Point-to-Point Protocol (PPP) header format.
Frame	IPX packets are encapsulated in the header format.
SMDS	IPX packets are encapsulated in the SMDS header format.
ATM	IPX packets are encapsulated in the ATM header format.

The router can receive incoming packets with either of the header types listed.

The default header format for Ethernet is IEEE 802.3. On serial ports, header formats are optional. Depending on the port ownership, IPX automatically configures the header format.

If ownership of the path changes (for example, to X.25 or PPP), the header format automatically changes to accommodate the new owner for the primary network.

To display IPX network numbers currently configured for a particular port, use the SHow command. If you do not specify a port number, the IPX network number for all ports is shown.

PathSplit

Syntax

```
SETDefault -IPX PathSplit = <number> (1–4)
SHow -IPX PathSplit
```

Default 1

Description The PathSplit parameter enables load splitting. When a routing table is computed, the system always computes up to the specified PathSplit number of equal minimum cost paths toward any destination. When forwarding IPX data packets, the router may split traffic evenly among these paths.

Configuring PathSplit to 1 disables load splitting. Settings 2 through 4 specify the maximum number of paths for load splitting.

ROUte

Syntax

```
ADD !<port> -IPX ROUte {&<remote network> | Default} [<network>]
  <media address> <hops> [Override] [hdrfmt]
DELete !<port> -IPX ROUte &<remote network> | Default
SHow [!<port> | !*] -IPX ROUte
SHowDefault [!<port> | !*] -IPX ROUte
```

Default No default (no static IPX routes configured)

Description The ROUte parameter adds, deletes, or displays static routes in the routing table.

Values You can select the different values with the ADD command in the following order:

First, specify each of the following values in the order presented:

<&remote network>	Refers to the identifier of the destination network.

Default
Allows you to enter a static default route, which is subsequently added to the routing table and propagated by NRIP or NetWare Link Services Protocol (NLSP.) When a default route has been specified, packets destined to networks not explicitly known or listed in the routing table are routed to the default router for subsequent routing. Only one default route can be added per port.

<&network>
Specifies the directly connected network through which the router can reach the remote destination.

Then specify one of the following formats for the <media address> option:

<%host>
Specifies the MAC (Ethernet) address of the closest router through which the IPX network can be reached. This is the WAN ports MAC address. MAC can be used in place of %.

<#X.25 address>
Specifies the DTE address that is used for adding an X.25 neighbor. It indicates the DTE address of the closest router through which the network can be reached. DTE can be used in place of #.

<@DLCI>
Specifies the DLCI address that is used for adding Frame Relay neighbors. DLCI can be used in place of @.

<$SMDS addr>
Specifies the SMDS individual address of the neighbor router on the SMDS network and is used to configure a static route. SMDS can be used in place of $. For configuration information, refer to Chapter 13 in *Using NETBuilder Family Software*.

<&VCID>
Specifies Asynchronous Transfer Mode 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.

You can also specify the following values:

<hops>
Specifies the number of hops or routers required for the packet to reach its destination. The hops value must be a number from 1 to 15.

[Override]
Static routes configured with this option become the lowest precedence routes. When available, other routes such as RIP and NLSP learned routes will override the static route configured with the Override option.

Only routes toward the same destination can override each other. If no other routes are available, routes configured as static override routes are then used.

Without the Override option, static routes are usually the highest precedence routes overriding all other dynamic routes.

<hdrfmt>
Specifies a header format such as Ethernet, Ieee, Llc, Snap and so forth. For a complete listing, refer to "NETnumber" on page 31-6.

RouterName

Syntax

```
SETDefault -IPX RouterName = “<string>”
SHow -IPX RouterName
SHowDefault -IPX RouterName
```

Default Concatenation of the prefix “3Com_Router_” and the last 4 bytes of the router MAC address. For example, 3Com_Router_0203073F.

Description The RouterName parameter assigns a symbolic name to the router. The router name must be unique throughout the IPX Internet and can be up to 48 characters in length. The router uses this name during IPXWAN negotiation to build NRIP and SAP information request and response packets. The router does not use this name internally; the name is for network management use only.

Because the IPX router does not provide any service (unlike a NetWare server) and a well-known service type is not available for a router, the router name is not advertised in SAP updates.

SERver

Syntax

```
ADD -IPX SERver <sname> <type> <snet>%<shost>:<sskt> <hops>
DELete -IPX SERver <sname> <type>
SHow -IPX SERver
SHowDefault -IPX SERver
```

Default No default (no IPX static servers defined)

Description The SERver parameter adds or deletes the static server and specifies the server address through which the server is located.

Values

<sname> Specifies the server name <string>.

<type> Defines a 16-bit number specifying the type of service located on a given host.

<snet> Specifies the network number identifier of the destination network.

<shost> Specifies the MAC (Ethernet) address of the closest router through which the IPX network can be reached. MAC can be used in place of %.

<sskt> Specifies the slot number.

<hops> Refers to the number of gateways that a packet has to pass through before it can reach the destination network. The maximum number of hops is 15. Any network that is 16 or more hops away is considered unreachable.

Example To add the static server MOBILE_SERVER401 to the network, enter:

```
ADD -IPX SERver “MOBILE_SERVER401” 4 &00000401%000000000001:0451 2
```

SMDSGroupAddr

Syntax

```
SETDefault !<port> -IPX SMDSGroupAddr = $<E0–E999999999999999> |
  None
SHow [!<port> | !*] -IPX SMDSGroupAddr
SHowDefault [!<port> | !*] -IPX SMDSGroupAddr
```

Default No default (no group address configured)

Description

The SMDSGroupAddr parameter configures an SMDS group address that is used as the IPX multicast address on the specified port. The port must be configured with -PORT OWNer set to SMDS and -IPX SMDSGroupAddr configured with a valid group address for IPX routing to occur over SMDS.

Values

<E0–E999999999999999>	Specifies the SMDS group, or multicast, address format. The group address type routes data to all routers with the same group address. The group address begins with the letter E followed by the 15 digits of the 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.

SPoofCONTrol

Syntax

```
SETDefault !<port> -IPX SPoofCONTrol = ([NcpWatchDog |
  NoNcpWatchDog] [Spx1WatchDog | NoSpx1WatchDog])
SHow [!<port> | !*] -IPX SPoofCONTrol
SHowDefault [!<port> | !*] -IPX SPoofCONTrol
```

Default

NcpWatchDog; NoSpx1WatchDog

Description

The SPoofCONTrol parameter helps control IPX traffic over dial-on-demand (DOD) lines. The bridge/router software responds to an incoming NetWare Communication Protocol (NCP) KeepAliveRequest or Sequenced Packet Exchange 1(SPX1) watchdog packets that are to be routed out a DOD port and spoofs packets (sends them back to the originating endnode) on behalf of the intended client.

The maximum number of spoofed connections supported on the router are not limited; the bridge/router software can spoof as many connections as needed over the DOD line.

For conceptual information about spoofing, refer to “IP over a DOD Link” on page 37-24 in *Using NETBuilder Family Software*.

Spoofing does not apply to non-DOD ports; enabling or disabling spoofing on these ports has no effect. Spoofing is limited to NetWare 3.0 and 4.0 NCP KeepAlive and SPX1 watchdog packets.

Values

NcpWatchDog	Enables NCP KeepAlive spoofing on the specified port. If you enable spoofing (NcpWatchDog) on a DOD line and the bridge/router receives an incoming KeepAliveRequest packet, the packet is handled as follows: If the path is down, the IPX spoofing software generates the appropriate KeepAliveResponse packet, transmits it to the originating server, and discards the request packet without ever bringing up the DOD line. If the path is up, the IPX spoofing software routes the KeepAliveRequest packet out the DOD port, but does not keep the DOD line up.
NoNcpWatchDog	Disables KeepAlive spoofing on the specified port.

If you disable spoofing (NoNcpWatchDog) on a DOD port, KeepAliveRequest packets are routed out the DOD port without any special treatment.

Spx1WatchDog Enables SPX1 spoofing on the specified port.

If you enable spoofing (Spx1WatchDog) on a DOD line and the bridge/router receives an incoming SPX1 watchdog packet, the packet is handled as follows:

If the path is down, SPX1 watchdog packets are recycled as a spoofed packet and sent back to the originating endnode.

If the path is up, the SPX1 spoofing software routes the watchdog packet out the DOD port, but will not hold the DOD line up.

NoSpx1WatchDog Disables SPX1 spoofing on the specified port.

If you disable spoofing (NoNcpWatchDog) on a DOD port, SPX1 watchdog packets are routed out the DOD port without any special treatment.

X25PROFileid

Syntax

```
SETDefault !<port> -IPX X25PROFileid = <number> (0–255)
SHow [!<port> | !*] -IPX X25PROFileid
SHowDefault [!<port> | !*] -IPX 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 IPX packets. A value of 0 indicates that no specific X.25 user profile is configured for IPX packets.

X25ProtID

Syntax

```
SETDefault !<port> -IPX X25ProtID = IETF | <protocol id> (1 octet)
SHow [!<port> | !*] -IPX X25ProtID
SHowDefault [!<port> | !*] -IPX X25ProtID
```

Default 0xEE

Description The X25ProtID parameter applies to routing IPX over an X.25 public data network. It specifies a protocol identifier to be included in all outgoing packets. Enter a value between 1 and FF.

When an X.25 call setup is attempted, this protocol ID is sent as the call user data and the destination DTE verifies this protocol identifier against its own configured protocol ID. If it matches, the incoming call is accepted; otherwise, it is discarded. The chosen value must not conflict with that used by other protocols.

Values IETF Specifies if the call and user data encoding is compliant to RFC 1356. It provides interoperability for multi-vendor connectivity over X.25. Because 3Com routers maintain backward compatibility with older software, configuring IETF between 3Com routers is not required.

32 ISIS SERVICE PARAMETERS

This chapter describes the Intermediate System-to-Intermediate System (ISIS) Service parameters used for Open System Interconnection (OSI) routing. ISIS parameters are related to the CLNP, ESIS, and IISIS Services. Table 32-1 lists the ISIS Service parameters and commands.

Table 32-1 ISIS Service Parameters and Commands

Parameters	Commands
ADJacencies	SHow
AreaAddress	ADD, DELete, SHow, SHowDefault
CONFiguration	SHow
CONTrol	SETDefault, SHow
CsnpTime	SETDefault, SHow
DISHelloTime	SETDefault, SHow
HelloPassWord	SETDefault, SHow
HelloTime	SETDefault, SHow
L1BufferSize	SETDefault, SHow
L2BufferSize	SETDefault, SHow
L1DefaultMetric	SETDefault, SHow
L2DefaultMetric	SETDefault, SHow
L1Multicast	SETDefault, SHow
L2Multicast	SETDefault, SHow
L1PassWord	SETDefault, SHow
L2PassWord	SETDefault, SHow
L1Priority	SETDefault, SHow
L2Priority	SETDefault, SHow
L1Route	SHow
L2Route	SHow
LinkStateData	SHow
LspBroadcastTime	SETDefault, SHow
LspMAxTime	SETDefault, SHow
LspMInTime	SETDefault, SHow
LspRtxTime	SETDefault, SHow
MODE	SETDefault, SHow
Neighbors	ADD, DELete, SHow
PathSplit	SETDefault, SHow
PrefixRoute	ADD, DELete, SHow, SHowDefault
PsnpTime	SETDefault, SHow
SMDSGroupAddr	SETDefault, SHow, SHowDefault

(continued)

Table 32-1 ISIS Service Parameters and Commands (continued)

Parameters	Commands
SMDSID	SETDefault, SHow
SystemID	SETDefault, SHow
SystemName	ADD, DELete, SHow
TRACE	SETDefault, SHow

ADJacencies

Syntax `SHow -ISIS ADJacencies`

Default No default (the adjacency database is empty)

Description The ADJacencies parameter displays the current intermediate system (IS) adjacencies. An IS can have multiple adjacencies to a particular IS for the following reasons:

- There can be separate and independent L1ONLY and L2ONLY adjacencies toward the same IS.
- Adjacencies learned from different interfaces are treated independently.
- Adjacencies can be learned from different media access control (MAC) addresses, suggesting that the IS has multiple interfaces on the same LAN.

To display end system (ES) adjacencies, use the -CLNP ES parameter.

The SHow -ISIS ADJacencies command generates a screen display similar to the following:

```
SYSTEM-ID    state    SNPA              Type     prior Port  lifetime
Saturn       UP       %080002013E8F     L2ONLY   64    2     95
Mars         UP       %080002012E8F     L1ONLY   126   2     95
```

The following list explains the possible adjacency states:

UP Indicates that the adjacency is available for exchanging routing information.

INIT Indicates that the adjacency is not yet fully established. An adjacency in the INIT state for an extended period of time usually indicates a network problem.

The following list explains the possible adjacency types:

L1ONLY Indicates that the adjacency can exchange Level 1 (L1) routing packets.

L2ONLY Indicates that the adjacency can exchange Level 2 (L2) routing packets.

L1+2 Indicates that the adjacency can exchange both L1 and L2 routing packets. This can only happen over a point-to-point link when both ISs are L2.

AreaAddress

Syntax

```
ADD -ISIS AreaAddress <NSAP Address> (/<afi>/<idi>/<dsp prefix>)
DELete -ISIS AreaAddress <NSAP Address> (/<afi>/<idi>/<dsp prefix>)
SHow -ISIS AreaAddress
SHowDefault -ISIS AreaAddress
```

Default /49/0053

Description The AreaAddress parameter adds, deletes, and displays area addresses for each IS. Up to three area addresses can be added to an IS. AreaAddress is a network service access point (NSAP) address without the last seven octets. It is made up of three parts: address format identifier (AFI), initial domain identifier (IDI), and domain specific part (DSP), which are assigned by an appropriate authority. The maximum size of an AreaAddress is 13 octets.

3Com does not recommend using multiple area addresses. Multiple area addresses are available primarily for area address transitions, such as introducing a new area to replace an old one, merging two areas into one, or separating one area into two areas.

3Com recommends that each site use an officially assigned area address from an appropriate addressing authority. If such an address is not yet available, you can continue to use the default AFI value 49. The 0053 value can be replaced by a new value for each area in your network. Because AFI value 49 is not guaranteed to be universally unique, these networks cannot be interconnected with other routing domains.

Values

<NSAP Address> Specifies the NSAP address, which consists of the following parts:

<afi>

AFI identifies the authority responsible for allocating IDI field values, format, and whether DSP syntax is specified with binary or decimal digits. This identifier is always preceded with a slash in 3Com syntax.

<idi>

IDI 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.

<dsp prefix>

This prefix consists of decimal or hexadecimal digits. If the DSP is in hexadecimal, it must contain an even number of digits.

The SHow command displays the computed area addresses for the IS home area. The SHowDefault command displays the statically configured AreaAddress for the IS. Figure 32-1 illustrates the uses of the AreaAddress command syntaxes.

If the OSI routing function is not enabled by the -CLNP CONTrol parameter, the SHow -ISIS AreaAddress parameter displays an empty table.

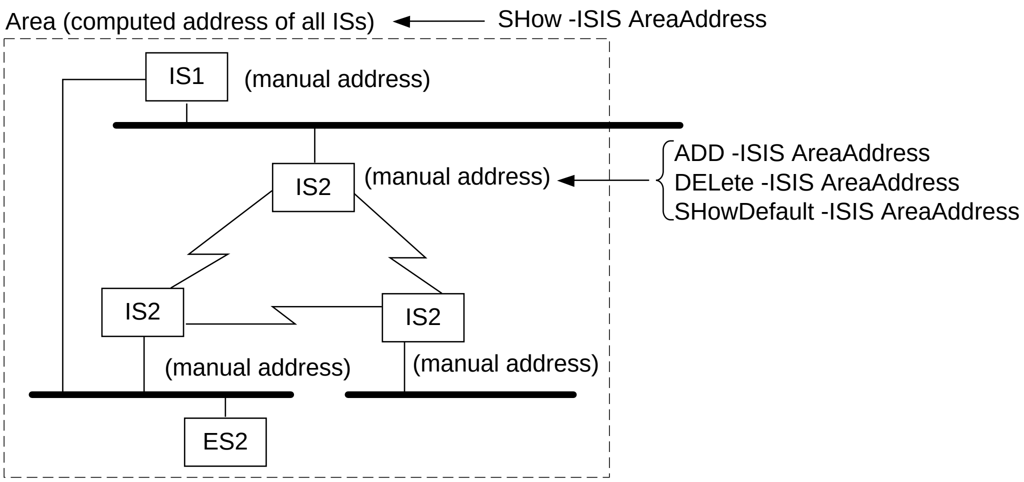


Figure 32-1 AreaAddress Command Syntaxes

CONFiguration

Syntax `SHow -ISIS CONFiguration`

Default No default

Description The CONFiguration parameter displays the following ISIS configuration information for the router:

- AreaAddress parameter value
- MODE parameter setting
- CONTrol parameter setting for each port
- PathSplit parameter value
- ISIS adjacency database

CONTrol

Syntax

```
SETDefault !<port> -ISIS CONTrol = ([Enable | Disable], [L1andL2 |
  L2only], [Transit | Stub])
SHow [!<port> | !*] -ISIS CONTrol
```

Default Enable, L1andL2, Transit

Description The CONTrol parameter enables or disables ISIS routing on each port, and determines whether the port performs Level 1 and Level 2 routing, or Level 2 routing.

For ISIS routing to occur, the -CLNP CONTrol parameter must be set to Route.

Values

Enable | Disable — Enables ISIS routing on the specified port. The ESIS routing protocol is enabled automatically on ports with -ISIS CONTrol set to Enable. The Disable value disables ISIS routing on the specified port. ISIS packets received on the port are ignored. Transmission of hello packets and other routing packets, such as Link State Protocol (LSP), Complete Sequence Number Protocol Data Unit (CSNP), and Partial Sequence Number Protocol Data Unit (PSNP), is disabled. ESIS is automatically disabled.

L1andL2 | L2only — When L1andL2 is selected, both L1 and L2 routing are enabled on the port. Intra-area and interarea routing are performed. This option is effective only when the value Enable is selected. When L2only is selected, only L2 routing is enabled on the port. Interarea routing is performed. This option is effective only when the value Enable is selected. The L2only setting is only effective when the MODE parameter is set to L2. For more information, refer to "MODE" on page 32-12.

Transit | Stub — A transit network is a LAN with ES and two or more IS present. A transit network requires both the IS-IS and ES-IS protocol running on it. A stub network is a LAN with ESs, but no other ISs present. A stub network is sometimes referred to as a "leaf" network. A stub network only needs the ES-IS protocol running on it. This yields significant bandwidth savings. If Transit is selected, both ES-IS and IS-IS protocols are enabled on the specified port. If Stub is selected, only the ES-IS protocol is enabled on the port.

CsnpTime

Syntax

```
SETDefault -ISIS CsnpTime = <seconds> (1–600)
SHow -ISIS CsnpTime
```

Default 10

Description The CsnpTime parameter specifies the time interval (in seconds) between transmission of CSNPs. CSNPs are routing packets sent out by a Designated Intermediate System (DIS) to summarize all the LSPs in its database. CSNPs are received by other direct neighboring ISs on the same LAN and are used to maintain synchronization of link state databases among all ISs.

The CsnpTime value applies to both Level 1 and Level 2 routing. It is effective only on LAN interfaces on a router that is elected as the DIS. A DIS is the IS with the highest priority on the LAN. For more information on setting the priority for each IS, refer to "L1Priority" on page 32-9 and "L2Priority" on page 32-9.

A smaller CsnpTime value provides faster synchronization of link state databases, but requires more network bandwidth consumption.

DISHelloTime

Syntax

```
SETDefault !<port> -ISIS DISHelloTime = <seconds> (1–65535)
SHow [!<port> | !*] -ISIS DISHelloTime
```

Default 1

Description The DISHelloTime parameter determines the time in seconds between multicasts of hello packets on a DIS. It applies only to an IS that is elected as the DIS. A DIS is the IS with the highest priority on the LAN. For more information on setting the priority for each IS, refer to "L1Priority" on page 32-9 and "L2Priority" on page 32-9.

Hello packets are used to determine which systems are up and which adjacencies to maintain. Setting the DISHelloTime parameter value higher reduces traffic on the network, but it takes longer to detect a failed DIS on the network.

If the DIS resigns as DIS, it uses the HelloTime parameter value to determine the rate of multicast for hello packets. For information on configuring the HelloTime parameter, refer to "HelloTime" on page 32-6.

DISHelloTime applies to Level 1 and Level 2 routing. It is effective only on LAN interfaces.

HelloPassWord

Syntax

```
SETDefault !<port> -ISIS HelloPassWord = None | “<password
  (1–16 characters)>”
SHow [!<port> | !*] -ISIS HelloPassWord
```

Default None

Description The HelloPassWord parameter specifies passwords for hello packets. There is one for each interface. If a password is specified, that password is transmitted in the outgoing hello packets (including level 1 hello, level 2 hello, and point-2-point hello packets). The same password is used for verifying received hello packets (of the interface).

HelloTime

Syntax

```
SETDefault !<port> -ISIS HelloTime = <seconds> (3–21845)
SHow [!<port> | !*] -ISIS HelloTime
```

Default 3

Description The HelloTime parameter sets the time in seconds between multicasts of hello packets by an IS. Hello packets are used to determine the existence and location of other directly reachable ISs. Setting a high HelloTime value reduces traffic on the network, but it takes longer to detect a failed IS on the network.

HelloTime applies to Level 1 and Level 2 routing. It is effective on LAN and point-to-point interfaces.

On a LAN interface, if an IS is elected as DIS, the frequency of multicast hello packets is controlled by the DISHelloTime parameter.

L1BufferSize

Syntax

```
SETDefault -ISIS L1BufferSize = <bytes> (512–1492)
SHow -ISIS L1BufferSize
```

Default 1492

Description The L1BufferSize parameter determines the maximum size (in bytes) allowable for Level 1 routing packets originated from the IS. Packets that exceed the limits set by the L1BufferSize parameters are fragmented into smaller pieces.

The L1BufferSize parameter affects the Level 1 packets including, CSNP, PSNP, and LSP packets.

L2BufferSize

Syntax

```
SETDefault -ISIS L2BufferSize = <bytes> (512–1492)
SHow -ISIS L2BufferSize
```

Default 1492

Description The L2BufferSize parameter determines the maximum size (in bytes) allowable for Level 2 routing packets originated from the IS. Packets that exceed the limits set by the L2BufferSize parameters are fragmented into smaller pieces.

L2BufferSize affects the Level 2 packets, including CSNP, PSNP, and LSP packets.

L1DefaultMetric

Syntax

```
SETDefault !<port> -ISIS L1DefaultMetric = <number> (1–63)
SHow [!<port> | !*] -ISIS L1DefaultMetric
```

Default 20

Description The L1DefaultMetric parameter sets a cost to a particular port on a L1 router and applies only to intra-area routing. It is used as a measurement of the port's capacity. Higher values indicate higher costs (lower capacity, lower baud rate).

The cost is used by the router to calculate the least-cost path to a destination. Setting the value higher instructs the IS to avoid using the port for forwarding traffic if other lower cost routes are available.

L2DefaultMetric

Syntax

```
SETDefault !<port> -ISIS L2DefaultMetric = <number> (1–63)
SHow [!<port> | !*] -ISIS L2DefaultMetric
```

Default 20

Description The L2DefaultMetric parameter sets a cost to a particular port on a L2 router and applies only to interarea routing. It is used as a measurement of the port's capacity. Higher values indicate higher costs (lower capacity, lower baud rate).

The cost is used by the router to calculate the least-cost path to a destination. Setting the value higher instructs the IS to avoid using the port for forwarding traffic if there are other lower cost routes available.

L1Multicast

Syntax

```
SETDefault -ISIS L1Multicast = <multicast address>
SHow -ISIS L1Multicast
```

Default %0180C2000014

Description The L1Multicast parameter specifies the multidestination address to which the L1 IS transmits hello packets and routing packets. The IS also receives L1 hello packets and routing packets on this address. L1 multicast addresses are for L1 routers.

This parameter is effective only on LAN interfaces.

3Com does not recommend changing the value of this parameter. The multidestination address should be the same for all ISs within the routing domain.

L2Multicast

Syntax

```
SETDefault -ISIS L2Multicast = <multicast address>
SHow -ISIS L2Multicast
```

Default %0180C2000015

Description The L2Multicast parameter specifies the multidestination address to which the L2 IS transmits hello packets and routing packets. The IS also receives L2 hello packets and routing packets on this address. L2 multicast addresses are for L2 routers.

This parameter is effective only on LAN interfaces.

3Com does not recommend changing the value of this parameter. The multidestination address should be the same for all ISs within the routing domain.

L1PassWord

Syntax

```
SETDefault -ISIS L1PassWord = None | “<password (1–16 characters)>”
SHow -ISIS L1PassWord
```

Default None (no password configured)

Description The L1PassWord parameter sets a password for the Level 1 area. Because a router can be homed to only one area, there is only one password defined.

L2PassWord

Syntax

```
SETDefault -ISIS L2PassWord = None | “<password (1–16 characters)>”
SHow -ISIS L2PassWord
```

Default None (no password configured)

Description The L2PassWord parameter sets a password for the Level 2 backbone. There is only one password defined (for the router). This password is included in all Level 2 link state packets and sequence packets that are transmitted. The same password is also used to verify received (Level 1) link state packets and sequence packets.

L1Priority

Syntax

```
SETDefault !<port> -ISIS L1Priority = <number> (1–127)
SHow [!<port> | !*] -ISIS L1Priority
```

Default 63

Description The L1Priority parameter assigns a priority value to the L1 IS for a particular LAN port. Among all the L1 ISs on the same LAN, the IS with the highest priority is elected as the DIS.

Higher values indicate higher priority. If two or more ISs have the same high priority, the IS with the numerically highest MAC address is elected as the DIS.

L1Priority is effective only on LAN interfaces, and only for Level 1 routing.

L2Priority

Syntax

```
SETDefault !<port> -ISIS L2Priority = <number> (1–127)
SHow [!<port> | !*] -ISIS L2Priority
```

Default 63

Description The L2Priority parameter assigns a priority value to the L2 IS for a particular LAN port. Among all the L2 ISs on the same LAN, the IS with the highest priority is elected as the DIS.

Higher values indicate higher priority. If two or more ISs have the same high priority, the IS with the numerically highest MAC address is elected as the DIS.

L2Priority is effective only on LAN interfaces, and only for Level 2 routing.

L1Route

Syntax

```
SHow -ISIS L1Route [<SystemID>]
```

Default No default (Level 1 routing table is empty)

Description The L1Route parameter displays the contents of the Level 1 routing table, which lists all reachable ISs and ESs within the area. Systems are listed by their six-octet ID value (SystemID).

SHow -ISIS L1Route displays a summary of all reachable systems in the area. SHow L1Route SystemID displays the routing information for a particular system, including information about all possible minimum cost routes and information about all ISs along the routes.

For information and an example display, refer to Chapter 16 in *Using NETBuilder Family Software*.

Multiple paths to the same destination can exist. In this case, the IS does load splitting among these paths, based on the value configured for the PathSplit parameter. For more information, refer to “PathSplit” on page 32-13.

L2Route

Syntax `SHow -ISIS L2Route`

Default No default (Level 2 routing table is empty)

Description The L2Route parameter displays the contents of the Level 2 routing table. The L2 routing table contains information for interarea routing, including:

- All areas (identified by AreaAddress) reachable within the L2 routing domain
- Total metric to each area
- Outgoing port number to each area
- Next hop IS for reaching the area

For each AreaAddress that is in the IS home area, the metric is 0.

For information and an example display, refer to Chapter 16 in *Using NETBuilder Family Software*.

LinkStateData

Syntax `SHow -ISIS LinkStateData [<SystemID> [:##[:##]]]`

Default No default (link state database is empty)

Description The LinkStateData parameter displays the current Link State PDU database. The Link State Protocol Data Unit (PDU) database includes the Level 1 database and the Level 2 database (if it exists).

Use SHow to display the Link State PDU database for a particular LSP. If you do not specify an LSP ID, summary information for all LSPs is displayed.

Example The following is an example of a display generated by SHow -ISIS LinkStateData:

```
----------------------Level 1 Link State Database--------------------------
LSP-ID         sequence  remaining  P    H    attach  IS    data    checksum
               number     lifetime  bit  bit  bit     type  length
Micky:00:00    17B           309    0    0    1         L2  47      A569(OK)
Micky:01:00    17B           309    0    0    0         L1  14      E45D(OK)
Micky:02:00    17C           309    0    0    0         L1  25      CC7C(OK)
Donald:00:00   53            970    0    0    1         L2  36      A3E8(OK)
```

The display elements are as follows:

LSP-ID Identifies an LSP by its eight-octet ID value. The first six octets indicate the originating IS by its system ID or isystem name if one has been assigned. For more information on system names, refer to "SystemName" on page 32-15. The seventh octet indicates whether the LSP is generated for a pseudonode. The eighth octet indicates whether the packet has been fragmented. A zero for the eighth octet indicates that the packet has not been fragmented.

sequence number Indicates (in hexadecimal numbers) how many times the particular LSP has been reissued by the originating IS.

remaining lifetime	Amount of time remaining (in seconds) before the LSP is aged out.
P bit	Indicates whether the originating IS supports the partition repair option.
H bit	Indicates whether the originating IS suffers from memory overflow.
attach bit	Indicates whether the IS can reach other areas in the L2 routing domain or other routing domains.
IS type	Indicates whether the IS is a Level 1 (intra-area) or Level 2 (interarea) router.
data length	Length of the data contents in decimal value.
checksum	Indicates the checksum value contained in the LSP PDU. If the value is good, OK is displayed.

LspBroadcastTime

Syntax

```
SETDefault -ISIS LspBroadcastTime = <milliseconds> (1–1000)
SHow -ISIS LspBroadcastTime
```

Default 33

Description The LspBroadcastTime parameter specifies the minimum interval between transmissions of LSP, CSNP, and PSNP routing packets on a LAN. This parameter guarantees that an IS does not send more than (1000/LspBroadcastTime) routing packets within any one second.

LSPBroadcastTime applies to Level 1 and Level 2 routing. It is effective only on LAN interfaces.

LspMAxTime

Syntax

```
SETDefault -ISIS LspMAxTime = <seconds> (60–900)
SHow -ISIS LspMAxTime
```

Default 900

Description The LspMAxTime parameter specifies the maximum amount of time in seconds between LSP packet regeneration. Because all LSPs carry an initial lifetime of 1,200 seconds, you will need to regenerate LSPs periodically before the lifetime expires.

LSP packets can be regenerated before the LspMAxTime timer expires because of other events, such as a link going up or down or an adjacency going up or down. When such an event occurs, the LSP packet contents are modified and transmitted, but the LspMAxTime timer is not reset.

LspMAxTime applies to Level 1 and Level 2 routing.

LspMInTime

Syntax

```
SETDefault -ISIS LspMInTime = <seconds> (5–300)
SHow -ISIS LspMInTime
```

Default 30

Description The LspMInTime parameter sets a minimum time interval (in seconds) at which LSPs are regenerated. In addition to regular periodic generation of LSPs, the following events can trigger immediate modification and generation on an LSP:

- An adjacency or port goes from up state to down state or vice versa
- A change in a port's metric
- A change of AreaAddress
- A change in designated IS status
- Addition or deletion of a prefix route

Excessive LSP generation can consume a large amount of CPU power and network bandwidth The LspMInTime parameter prevents LSPs from being generated excessively.

LspRtxTime

Syntax

```
SETDefault -ISIS LspRtxTime = <seconds> (5–30)
SHow -ISIS LspRtxTime
```

Default 5

Description The LspRtxTime parameter determines the minimum time between transmission and retransmission of routing packets on a point-to-point link. Each transmission must be explicitly acknowledged by the receiving IS. If the LspRtxTime time (in seconds) expires before receiving an acknowledgment, the same packet is retransmitted.

LspRtxTime applies to both the L1 and L2 routing process. It is effective only on point-to-point links.

MODE

Syntax

```
SETDefault -ISIS MODE = [Level1 | Level2]
SHow -ISIS MODE
```

Default Level1

Description The MODE parameter designates the intermediate system as either a Level 1 or Level 2 IS.

Values Level1 The IS performs only intra-area routing.

Level2 The IS performs both intra-area and interarea routing.

For intra-area routing, all Level 1 routers within an area must be directly connected.

For interarea routing, all Level 2 routers within a routing domain must be directly connected.

Neighbors

Syntax

```
ADD !<port> -ISIS Neighbors [#<DTE address> | @<DLCI>]
DELete !<port> -ISIS Neighbors [#<DTE address> | @<DLCI>]
SHow [!<port> | !*] -ISIS Neighbors
```

Default No default (no neighbors are configured)

Description The Neighbors parameter adds, deletes, and displays neighbors' addresses over an X.25 or Frame Relay network. Up to 28 neighbors can be entered.

Neighbors takes effect immediately; the router initiates the following actions when a neighbor is added:

- Establishes a connection toward the destination address, if a connection is not open
- Begins sending hello packets toward the remote router
- Starts exchanging routing information, if the adjacency establishment procedure is successful

For the remote router to accept the adjacency, the Neighbors parameter of the remote router needs to be configured accordingly.

PathSplit

Syntax

```
SETDefault -ISIS PathSplit = <number> (1–4)
SHow -ISIS PathSplit
```

Default 4

Description The PathSplit parameter determines whether load splitting is performed. Setting PathSplit to 1 disables load splitting. A value between 2 and 4 specifies the maximum number of paths available for load splitting.

PathSplit applies to Level 1 and Level 2 routing.

PrefixRoute

Syntax

```
ADD !<port> -ISIS PrefixRoute [<NSAP Prefix> | Default] [%<MAC> |
  #<DTE address> | @<DLCI> | $<SMDS address> | ALGORITHM]
DELete !<port> -ISIS PrefixRoute [<NSAP Prefix> | Default]
SHow [!<port> | !*] -ISIS PrefixRoute
SHowDefault [!<port> | !*] -ISIS PrefixRoute
```

Default No default (no address prefixes are configured)

Description The PrefixRoute parameter configures NSAP address prefixes, which are sued to set up static routes to other routing domains. PrefixRoute only applies if MODE is set to Level2. For information, refer to "MODE" on page 32-12**.**

Values You can select one of the following values. DELete specifies either <NSAP Prefix> or Default.

<NSAP Prefix> | Default The prefix of the NSAP address. It can be part of /AFI/IDI/DSP. Default acts as a wild card and will match any NSAP address. Default has the lowest priority and is only chosen when matching to all other prefix addresses fails.

In addition, one of the following values can be specified with the ADD command:

<MAC> Indicates the MAC address for a particular node on a LAN or point-to-point interface. Each node must have a unique MAC address.

<DTE address> Allows you to configure the address of a remote domain border router in order to route OSI packets over X.25 networks. The remote domain is reachable through a public data network (PDN). You can specify the uppercase letters DTE or use the pound (#) sign before the address.

<DLCI> Specifies a Frame Relay data link connection identifier (DLCI), which is used only on a Frame Relay interface. You can specify the uppercase letters DLCI or use the at (@) sign before the address.

<SMDS address> Specifies the Switched Multimegabit Data Service (SMDS) unicast address, which is used only on an SMDS network. You can specify the uppercase letters SMDS or use the dollar sign ($) before the address.

ALGORITHM Allows the router to automatically extract X.121, E.163, and E.164 addresses from the destination NSAP address. The addresses are used as the next hop for forwarding the packet over X.25, SMDS, or Integrated Services Digital Network (ISDN) networks. This option can be useful in a large scale OSI over X25, SMDS, or ISDN networks, where systems attaching to the network have their X.25, SMDS, or ISDN addresses embedded in their NSAP addresses. This option is only allowed for AFI values 36, 37, 52, 53, 42, 43, 56, 57, 44, 45, 58, and 59.

The SHow command displays all NSAP prefixes currently reachable within the L2 routing domain. SHowDefault command displays the statically configured prefix information for the IS.

PsnpTime

Syntax

```
SETDefault -ISIS PsnpTime = <seconds> (1–65535)
SHow -ISIS PsnpTime
```

Default 2

Description The PsnpTime parameter specifies the time interval (in seconds) between successive transmission of PSNPs. PSNP packets are sent on point-to-point links to acknowledge receipt of LSPs. They are also transmitted on LAN interfaces to synchronize all the LSPs in the router’s database with the database on the DIS.

The PsnpTime value applies to both Level 1 and Level 2 routing. It is effective on both LAN and point-to-point links.

A smaller PsnpTime value provides faster synchronization of link state databases, but may require more network bandwidth consumption.

SMDSGroupAddr

Syntax

```
SETDefault !<port> -ISIS SMDSGroupAddr = $<E0–E999999999999999> None
SHow [!<port> | !*] -ISIS SMDSGroupAddr
SHowDefault [!<port> | !*] -ISIS SMDSGroupAddr
```

Default None (no SMDS group address is configured)

Description The SMDSGroupAddr parameter configures an SMDS group address that is used as the multicast address on the specified port. The port must be configured with

-PORT OWNer set to SMDS and the -ISIS SMDSGroupAddr configured with a valid group address for the ISIS Protocol to operate over SMDS.

Both the Level 1 and Level 2 ISIS Protocols use the same group address.

Values

<E0–E999999999999999>	Specifies the format for an SMDS group, or multicast, address. The group address type is used to route data to all routers with the same group address. The group address begins with the letter E followed by the 15 digits of the 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.

SMDSID

Syntax

```
SETDeault -ISIS SMDSID = UseMacAddress | UseSystemID
SHow -ISIS SMDSID
```

Default UseMacAddress

Description The SMDSID parameter provides interoperability between 3Com NETBuilder bridge/routers and Cisco routers. Because there is no accepted standard for SMDS, the two companies' proprietary methods are not compatible.

The default value, UseMacAddress, selects 3Com-compatible mode. UseSystemID selects Cisco-compatible mode.

SystemID

Syntax

```
SETDefault -ISIS SystemID = [<SystemID> | Default]
SHow -ISIS SystemID
```

Default Default

Description The SystemID parameter specifies an ISIS system ID for the router. When the value is Default, ISIS extracts the MAC address of the first LAN interface on the router and use it as the SystemID value. Otherwise, ISIS uses the user-specified value.

The System ID is a six-octet binary value identical to a LAN address. It cannot be all zeros.

SystemName

Syntax

```
ADD -ISIS SystemName <SystemName> <System ID>
DELete -ISIS SystemName <SystemName>
SHow -ISIS SystemName
```

Default No default (SystemName Table is empty)

Description The SystemName parameter assigns a name to an ES or IS so that ISIS displays the system by name, instead of by its 6-octet hexadecimal number. SystemName affects displays generated with the following ISIS parameters: TRACE, L1Route, L2Route, ADJacencies, and LinkStateData. SystemName has no other effect on ISIS operation.

Values

<SystemName>	Specifies the name assigned to an end system or an intermediate system.
<System ID>	Specifies the ID of an end system or an intermediate system. The system ID is a 6-octet number; it is not necessarily a MAC address.

TRACE

Syntax

```
SETDefault -ISIS TRACE = (None, ADJAcency, LSP, SNP, DIS, Hello)
SHow -ISIS TRACE
```

Default None

Description The TRACE parameter displays various real-time events on the local console terminal for debugging purposes. It applies to Level 1 and Level 2 routing.

Values

None	No events are displayed on the local console terminal. This value is useful for resetting the TRACE parameter so that no tracing is performed.
ADJAcency	Displays when an adjacency goes up or down.
LSP	A display appears on the local console terminal when an LSP is sent or received.
SNP	Displays when a CSNP or PSNP is sent or received.
DIS	Displays when the IS becomes or resigns as DIS.
Hello	Displays when a hello packet is sent or received.
None	No events are displayed on the local console terminal. This value is useful for resetting the TRACE parameter so that no tracing is performed.

Enabling TRACE significantly slows routing efficiency. This parameter is intended for debugging purposes.

33 LAPB SERVICE PARAMETERS

This chapter describes the Link Access Procedure, Balanced (LAPB) Service parameters. 3Com's implementation is based on the CCITT X.25 Level 2 specification; see this document for more information. Table 33-1 lists the LAPB Service parameters and commands.

Table 33-1 LAPB Service Parameters and Commands

Parameters	Commands
CONFiguration	SHow, SHowDefault
CONTrol	SETDefault, SHow, SHowDefault
FrameSeq	SETDefault, SHow, SHowDefault
InterfaceType	SETDefault, SHow, SHowDefault
N2	SETDefault, SHow, SHowDefault
T1	SETDefault, SHow, SHowDefault
T3	SETDefault, SHow, SHowDefault
WindowSize	SETDefault, SHow, SHowDefault

CONFiguration

Syntax

```
SHow [!<path> | !*] -LAPB CONFiguration
SHowDefault [!<path> | !*] -LAPB CONFiguration
```

Default No default

Description The CONFiguration parameter displays the LAPB parameter values on a path-by-path basis.

CONTrol

Syntax

```
SETDefault !<path> -LAPB CONTrol = Enable | Disable
SHow [!<path> | !*] -LAPB CONTrol
SHowDefault [!<path> | !*] -LAPB CONTrol
```

Default Disable

Description The CONTrol parameter enables or disables the LAPB Service. For parameter changes to take effect immediately, you must toggle the path by enabling it. When you enable the path, NETBuilder first disables it and then enables it.

The SHow command displays CONTrol settings for a particular path. If no path is specified, the CONTrol values for all paths are shown.

Values

Enable	Enables LAPB over the specified path.
Disable	Disables LAPB over the specified path.

FrameSeq

Syntax

```
SETDefault !<path> -LAPB FrameSeq = Basic | Extended
SHow [!<path> | !*] -LAPB FrameSeq
SHowDefault [!<path> | !*] -LAPB FrameSeq
```

Default Basic

Description The FrameSeq parameter specifies basic or extended sequencing.

Values

Basic	Enables numbered frames to range from 0–7.
Extended	Enables numbered frames to range from 0–127.

InterfaceType

Syntax

```
SETDefault !<path> -LAPB InterfaceType = DTE | DCE
SHow [!<path> | !*] -LAPB InterfaceType
SHowDefault [!<path> | !*] -LAPB InterfaceType
```

Default DTE

Description The InterfaceType parameter specifies the interface type of the path. Most public data networks (PDNs) function as data communications equipment (DCE), so the default value of this parameter is acceptable. If you want to configure the bridge/router in a private network, one device must function as the DCE and the other as the data terminal equipment (DTE).

Values

DTE	Indicates that the specified path on the bridge/router is configured for interaction with a PDN configured as Level 2 DCE.
DCE	Indicates that the specified path on the bridge/router is configured for interaction with a PDN configured as Level 2 DTE.

N2

Syntax

```
SETDefault !<path> -LAPB N2 = <1–255>
SHow [!<path> | !*] -LAPB N2
SHowDefault [!<path> | !*] -LAPB N2
```

Default 10

Description The N2 parameter specifies the maximum number of times a frame is sent after a time-out.

T1

Syntax

```
SETDefault !<path> -LAPB T1 = <100–1000000>
SHow [!<path> | !*] -LAPB T1
SHowDefault [!<path> | !*] -LAPB T1
```

Default 3000

Description The T1 parameter specifies the maximum time (in milliseconds) that the LAPB Protocol waits for an acknowledgment once a frame is transmitted. Any value you enter for the T1 parameter is internally divided by 250 milliseconds. As a result, any value you enter less than 250 actually equals zero.

T3

Syntax

```
SETDefault !<path> -LAPB T3 = <0–1000000>
SHow [!<path> | !*] -LAPB T3
SHowDefault [!<path> | !*] -LAPB T3
```

Default 0

Description The T3 parameter specifies the maximum period of line idle time. When this time expires, the link is assumed to be down and LAPB attempts to set up the link again. If the value of this parameter is set to 0, LAPB does not bring the idle link down. Any value you enter for the T3 parameter is internally divided by 250 milliseconds. As a result, any value you enter less than 250 actually equals zero.

WindowSize

Syntax

```
SETDefault !<path> -LAPB WindowSize = <1–127>
SHow [!<path> | !*] -LAPB WindowSize
SHowDefault [!<path> | !*] -LAPB WindowSize
```

Default 7

Description The WindowSize parameter specifies the maximum number of frames LAPB sends without an acknowledgment.

34

LLC2 SERVICE PARAMETERS

This chapter describes the parameters related to Logical Link Control, type 2 (LLC2) tunneling to and from Systems Network Architecture (SNA) networks. Table 34-1 lists the LLC2 Service parameters and commands.

Table 34-1 LLC2 Service Parameters and Commands

Parameters	Commands
CONFiguration	SHow
CONTrol	SETDefault, SHow
LlcLOG	SHow
MaxFrame	SETDefault, SHow
MaxTRaceData	SETDefault, SHow
ReceiveWindow	SETDefault, SHow
RetryCount	SETDefault, SHow
SESSions	SHow
TImerAck	SETDefault, SHow
TImerInact	SETDefault, SHow
TImerReply	SETDefault, SHow
TRaceData	FLush, SHow
TransmitWindow	SETDefault, SHow
TUNnelControl	SETDefault, SHow
TUNnelDisplay	SHow
TUNnelInterface	ADD, DELete, SHow
TUNnelMAcadd	ADD, DELete, SHow
TUNnelMOde	SETDefault, SHow
TUNnelPeer	ADD, DELete, SHow
TUNnelPRiority	SETDefault, SHow
TUNnelVRing	SETDefault, SHow

CONFiguration

Syntax

```
SHow [!<port> | !*] -LLC2 CONFiguration
```

Default No default

Description The CONFiguration parameter displays the current settings for LLC2 and tunneling. The display shows the LLC2 data link parameter settings, the tunnel interfaces configured, the tunnel media addresses configured, the tunnel virtual ring setting, and any current LLC2 settings.

CONTrol

Syntax

```
SETDefault !<port> -LLC2 CONTrol = ([Enable | Disable])
SHow [!<port> | !*] -LLC2 CONTrol
```

Default Disable

Description The CONTrol parameter defines the local LLC2 support, and specifies which port or ports on the bridge/router will serve as the LLC2 end system.

The !n syntax in the CONTrol parameter usually indicates the port number. In the LLC2 Service, the !n syntax indicates the tunnel identification number in the parameters that begin with TUN.

You can also configure this parameter for wide area ports if you need to enable the peer data exchange feature in an IBM Boundary Routing topology. For information on this feature, refer to Chapter 32 in *Using NETBuilder Family Software*.

Values Enable | Disable Configures the port that connects the bridge/router to the SNA network on which the end station or host is located. The Enable value allows a port to accept an LLC2 connection from an end system and forwards it through a tunnel to the peer SNA network, and the reverse. The Disable value disables the port so that it cannot accept or receive connections from an LLC2 end system.

LlcLOG

Syntax

```
SHow -LLC2 LlcLOG
```

Default No default

Description The LlcLOG parameter displays a log of LLC2 activity messages captured on the bridge/router and stored in a buffer. The display shows the most recent activity messages. Table 34-2 lists the event types captured in the log and the corresponding message that is displayed. In each message, *hhhhhhhhhhhh* represents a MAC address, *xx* represents a SAP *nnn.nnn.nnn.nnn* and represents an IP address.

Table 34-2 LLC2 Log Event Types and Messages

Event Type	Message Displayed
Session activated	Session Up LMAC *hhhhhhhhhhhh* LSAP *xx* RMAC *hhhhhhhhhhhh* RSAP *xx* IP *nnn.nnn.nnn.nnn*
Session deactivated	Session Down LMAC *hhhhhhhhhhhh* LSAP *xx* RMAC *hhhhhhhhhhhh* RSAP *xx* IP *nnn.nnn.nnn.nnn*
Session failed	Session Failed LMAC *hhhhhhhhhhhh* LSAP *xx* RMAC *hhhhhhhhhhhh* RSAP *xx* IP *nnn.nnn.nnn.nnn*

MaxFrame

Syntax

```
SETDefault !<port> -LLC2 MaxFrame = <size>(128–4399)
SHow [!<port> | !*] -LLC2 MaxFrame
```

Default 1,500

Description The MaxFrame parameter sets the maximum length of an information field. The value range is 128 to 4,399 bytes.

MaxTRaceData

Syntax

```
SETDefault -LLC2 MaxTRaceData = <max_bytes_traced> (0-76)
SHow -LLC2 MaxTRaceData
```

Default 16

Description The MaxTraceData parameter sets the maximum number of bytes of LLC2 data captured using the Trace facility. The value sets the number of bytes captured over and above the LLC2 address and control bytes. The number of bytes captured affects the types of data captured; the higher the value entered, the more detailed is the trace data that 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.

ReceiveWindow

Syntax

```
SETDefault !<port> -LLC2 ReceiveWindow = <size>(1–128)
SHow [!<port> | !*] -LLC2 ReceiveWindow
```

Default 7

Description The ReceiveWindow parameter sets the receive window size of information frames. The value range is 1 to 128.

RetryCount

Syntax

```
SETDefault !<port> -LLC2 RetryCount = <retrys>(1–255)
SHow [!<port> | !*] -LLC2 RetryCount
```

Default 7

Description The RetryCount parameter defines the maximum number of times to retransmit after expiration of the reply timer. The value range is 1 to 255.

SESSions

Syntax

```
SHow -LLC2 SESSions
```

Default No default

Description The SESSions parameter displays any current LLC2 sessions, including any active remote LLC2 sessions. This parameter only displays sessions at the LLC2 level. To display sessions for configured tunnels, use SHow -LLC2 TUNnelDisplay. For more information, refer to "TUNnelDisplay" on page 34-5.

TImerAck

Syntax

```
SETDefault !<port> -LLC2 TImerAck = <milliseconds>(0–500)
SHow [!<port> | !*] -LLC2 TImerAck
```

Default 0 milliseconds

Description The TImerAck parameter is used as the acknowledge timer and specifies the amount of time the bridge/router waits before acknowledging the received information frame. This is a link performance parameter. The connection is considered stopped after retrying the RetryCount.

The timer range is 0 to 500 milliseconds.

TImerInact

Syntax

```
SETDefault !<port> -LLC2 TImerInact = <milliseconds>(3000–180000)
SHow [!<port> | !*] -LLC2 TImerInact
```

Default 60,000 milliseconds

Description The TImerInact parameter defines the time the bridge/router waits to receive a frame from the other end before disconnecting a session. Make sure the TImerInact value entered is at least five times the value entered for the TImerReply parameter.

The timer range is 3,000 to 180,000 milliseconds.

TImerReply

Syntax

```
SETDefault !<port> -LLC2 TImerReply = <milliseconds>(500–60000)
SHow [!<port> | !*] -LLC2 TImerReply
```

Default 3,000 milliseconds

Description The TImerReply parameter sets the reply timer value. This is the length of time the bridge/router waits for a response to a command frame or for an acknowledgment of an information frame. After this timer expires, the bridge/router retransmits the command for a number of times specified in the RetryCount parameter. If this is still unsuccessful, the link is stopped.

The timer range is 500 to 60,000 milliseconds.

TRaceData

Syntax

```
SHow -LLC2 TRaceData
```

Default No default

Description The TRaceData parameter displays all LLC2 entries in the trace buffer.

TransmitWindow

Syntax

```
SETDefault !<port> -LLC2 TransmitWindow = <size>(1–128)
SHow [!<port> | !*] -LLC2 TransmitWindow
```

Default 7

Description The TransmitWindow parameter sets the retransmit window size of information frames. The value range is 1 to 128.

TUNnelControl

Syntax

```
SETDefault !<tunnelid> -LLC2 TUNnelControl = <Enable | Disable> [<local
  network IP address>]
SHow [!<tunnelid>] -LLC2 TUNnelControl
```

Default Enable

Description The TUNnelControl parameter opens or closes the tunnel connection to the peer network address for a tunnel identified by the tunnel identification number.

Values

Enable | Disable	Opens or closes the tunnel connection to the peer network address.
<local network IP address>	Specifies the IP address of the local bridge/router. This is only required when the !0 syntax has been used on a bridge/router to enable tunnel connections from any network (not just configured tunnel peers) to any port on the bridge/router.

TUNnelDisplay

Syntax

```
SHow -LLC2 TUNnelDisplay
```

Default No default display

Description The TUNnelDisplay parameter shows the status of any configured tunnels, including any active sessions for specific tunnels. This parameter only displays sessions for configured tunnels. To display information for LLC2 sessions only, use SHow -LLC2 SESSions. For more information, refer to "SESSions" on page 34-3.

TUNnelInterface

Syntax

```
ADD !<tunnelid> -LLC2 TUNnelInterface <local network IP address>
  [tunnel transport port] [LOCAL_TERM | TRANSPARENT]
DELete !<tunnelid> -LLC2 TUNnelInterface <local network IP address>
SHow [!<tunnelid>] -LLC2 TUNnelInterface
```

Default No default

Description The TUNnelInterace parameter requests tunneling support from the transport port of the tunnel client. After this parameter is configured, the tunnel service dynamically sets up a tunnel connection when it receives a connection request. Depending on the current state of the tunnel client, the tunnel client can accept or reject the connection request. Tunnel configuration can then be performed on one side of the tunnel, while the tunnel peer waits for the connection requests.

The tunnel identification number uniquely identifies the tunnel on the local bridge/router. When the data packet is sent through the tunnel connection, the local network address is used as the source network address. Using the local network address as the source network address is important because loops in the network topology can cause the source network address to change. For example, the best path for the peer network address changes to another port because a router in the network topology is down.

The tunnel client should consistently provide the same source network address so that the peer router can positively identify the source of the data packet in a tunnel connection. When you configure the tunnel connection on both sides of the tunnel, you enter the local network address and peer network address configuration one way on one peer router, and in reverse on the other peer router.

Values <local network address> Specifies the Internet address for the local bridge/router where the tunnel originates. This is used as the source network address when the data packet is sent through the tunnel connection. This address must be configured in the IP service before the tunneling function can be enabled.

tunnel transport port Specifies the tunnel transport port number. The default number is TCP port number decimal 2049 or hex 0801.

LOCAL_TERM | TRANSPARENT LOCAL_TERM state indicates that the LLC2 session for the tunnel peer is terminated locally. The LOCAL_TERM value is the default. TRANSPARENT state indicates that no local acknowledgment of the peer connection takes place; all data is passed to the other side of the tunnel as is.

TUNnelMAcadd

Syntax

```
ADD !<tunnelid> -LLC2 TUNnelMAcadd <peer mac address> [sap] [high sap]
DELete !<tunnelid> -LLC2 TUNnelMAcadd <peer mac address>
SHow [!<tunnelid>] -LLC2 TUNnelMAcadd
```

Default No default

Description The TUNnelMAcadd parameter statically configures the media access control (MAC) addresses of all SNA hosts or end stations that are reachable through a tunnel peer router. Each MAC address is mapped to the Internet address of the tunnel peer bridge/router. The number of end stations you can configure for each tunnel peer network address depends on which bridge/router hardware platform you are using. Sap and high sap values indicate the SAP ranges available. The default includes both, enabling the full SAP range.

Token ring applications normally use noncanonical MAC addresses. To convert MAC addresses from noncanonical to canonical format, use the MacAddrConvert command. When configuring MAC addresses using the TUNnelMAcadd parameter, you must enter the address in canonical format.

TUNnelMOde

Syntax

```
SETDefault -LLC2 TUNnelMOde = ([TunnelEnable | TunnelDisable],
  [TunnelSecure |TunnelNonSecure])
SHow -LLC2 TUNnelMOde
```

Default TunnelEnable, TunnelSecure

Description The TUNnelMOde parameter controls whether LLC2 tunneling is available on the bridge/router, and controls the types of tunnel connection requests the bridge/router will accept.

Values

TunnelEnable | TunnelDisable	The TunnelEnable state allows the bridge/router to make tunnel connections to tunnel peer routers, and receive tunnel connection requests from tunnel peer routers. The TunnelDisable state allows you to disable the bridge/router so that no tunnel connections can be sent or received.
TunnelSecure | TunnelNonSecure	When the bridge/router is in TunnelSecure state, the tunnel client only accepts connection requests from configured tunnel peer routers (using the ADD TunnelPeer user interface command). When the bridge/router is in TunnelNonSecure state, it accepts all tunnel connection requests received from other bridge/routers.

TUNnelPeer

Syntax

```
ADD !<tunnelid> -LLC2 TUNnelPeer <peer network IP address>
  [“peer name”]
DELete !<tunnelid> -LLC2 TUNnelPeer <peer network IP address>
SHow [!<tunnelid>] -LLC2 TUNnelPeer
```

Default No default

Description The TUNnelPeer parameter sets the tunnel peer router’s network address. The tunnel ID is unique for an ADD -LLC2 TUNnelInterface and ADD -LLC2 TUNnelPeer pair when a point-to-point tunnel connection is being configured. The tunnel connection is not made until the tunnel is enabled using the SETDefault -LLC2 TUNnelControl command.

Values

<peer network IP address>	Specifies the Internet address of the tunnel peer bridge/router.
“peer name”	Specifies an optional string used to name the tunnel peer bridge/router. Use quotation marks (“ ”) to bracket the string. The string is limited to 16 characters.

TUNnelPRiority

Syntax

```
SETDefault -LLC2 TUNnelPRiority = <H | M | L | DEFault>
SHow -LLC2 TUNnelPRiority
```

Default DEFault

Description The TUNnelPRiority parameter assigns a priority to an LLC2 packet that is tunneled over an Internet protocol (IP) internetwork. Possible priorities include high, medium, or low. If this parameter is set to default, the system uses the -IP QueuePriority setting. For more information on -IP DefaultPriority, refer to Chapter 29. For more information on data prioritization, refer to Chapter 41 in *Using NETBuilder Family Software*.

The priority of LLC2 tunnel packets is maintained across 3Com bridge/routers through the use of the type of service (TOS) field in the IP header.

You can also display the setting of this parameter with the SHow command.

TUNnelVRing

Syntax

```
SETDefault -LLC2 TUNnelVRing = <Number>(1–4095)
SHow -LLC2 TUNnelVRing
```

Default 92 (decimal)

Description The TUNnelVRing parameter sets the virtual ring number for the Internet. This allows token ring networks on both ends of the tunnel to interpret the Internet as an intermediate token ring network. The virtual ring number must be configured on the peer bridge/routers at both ends of the tunnel.

The value range is 1 to 254.

35 LNM SERVICE PARAMETERS

This chapter describes the parameters that provide the bridge/router with LAN Net Manager (LNM) support, an IBM network management application that monitors and performs some configuration of token ring networks. Table 35-1 lists the LNM Service parameters and commands.

Table 35-1 LNM Service Parameters and Commands

Parameters	Commands
CONTrol	SETDefault, SHow, SHowDefault
ExcSftErrTh	SETDefault, Show, SHowDefault
FrCopErrTh	SETDefault, SHow, SHowDefault
FreqErrTh	SETDefault, SHow, SHowDefault
ImpSftErrTh	SETDefault, SHow, SHowDefault
LostFrTh	SETDefault, SHow, SHowDefault
MinDecErrTh	SETDefault, SHow, SHowDefault
NumAltMgrs	SETDefault, SHow, SHowDefault
PassWord	SETDefault, SHow
RcvCnTFErrTh	SETDefault, SHow, SHowDefault
RcvConErrTh	SETDefault, SHow, SHowDefault
SftErrRptTimer	SETDefault, SHow, SHowDefault
TblFlErrTh	SETDefault, SHow, SHowDefault
TokErrTh	SETDefault, SHow, SHowDefault
VirBrNum	SETDefault, SHow, SHowDefault
VirRingNum	SETDefault, SHow, SHowDefault

CONTrol

Syntax

```
SETDefault -LNM CONTrol = (Enabled | Disabled)
SHow -LNM CONTrol
SHowDefault -LNM CONTrol
```

Default Disabled

Description The CONTrol parameter enables and disables LAN Net Manager support. If enabled, the bridge/router accepts and responds to requests from LAN Net Manager. If disabled, the system neither responds to requests from LAN Net Manager nor sends notifications to LAN Net Manager stations. If this feature is disabled when reporting links to LAN Net Manager stations are established, the links are gracefully terminated (as defined by IBM) by the system before disabling the feature.

ExcSftErrTh

Syntax

```
SETDefault !<port> -LNM ExcSftErrTh = <number> (0–127)
SHow [!<port> | !*] -LNM ExcSftErrTh
SHowDefault [!<port> | !*] -LNM ExcSftErrTh
```

Default 10

Description The ExcSftErrTh parameter sets the Excessive Soft Error threshold for the stations in the Ring Error Monitor’s Isolating table. When a station’s weight exceeds the Excessive Soft Error threshold, a Weight-Exceeded notification is sent to all LAN Net Manager stations configured to receive these notifications.

The Ring Error Monitor maintains two thresholds for the stations in its Isolating table: Excessive Soft Error thresholds and Impending Soft Error thresholds. For information on setting the Impending Soft Error thresholds, refer to “ImpSftErrTh” on page 35-2.

FrCopErrTh

Syntax

```
SETDefault !<port> -LNM FrCopErrTh = <number> (0–127)
SHow [!<port> | !*] -LNM FrCopErrTh
SHowDefault [!<port> | !*] -LNM FrCopErrTh
```

Default 50

Description The FrCopErrTh parameter sets a threshold for the Frame Copied Error soft error counter kept by the Ring Error Monitor. When this threshold is crossed, a notification is sent to those LAN Net Manager stations that monitor this token ring port. If this parameter’s value is 0, the Ring Error Monitor does not generate notification frames for this type of non-isolating error.

FreqErrTh

Syntax

```
SETDefault !<port> -LNM FreqErrTh = <number> (0–127)
SHow [!<port> | !*] -LNM FreqErrTh
SHowDefault [!<port> | !*] -LNM FreqErrTh
```

Default 50

Description The FreqErrTh parameter sets a threshold for the Frequency Error soft error counter kept by the Ring Error Monitor. When this threshold is crossed, a notification is sent to those LAN Net Manager stations that monitor this token ring port. If this parameter’s value is 0, the Ring Error Monitor does not generate notification frames for this type of non-isolating error.

ImpSftErrTh

Syntax

```
SETDefault !<port> -LNM ImpSftErrTh = <number> (0–127)
SHow [!<port> | !*] -LNM ImpSftErrTh
SHowDefault [!<port> | !*] -LNM ImpSftErrTh
```

Default 5

Description The ImpSftErrTh parameter sets the Impending Soft Error threshold for the stations in the Ring Error Monitor's Isolating table. When a station's weight exceeds the Impending Soft Error threshold, a Pre-Weight-Exceeded notification is sent to all LAN Net Manager stations configured to receive these notifications.

The Ring Error Monitor maintains two thresholds for the stations in its Isolating Table: Excessive Soft Error thresholds and Impending Soft Error thresholds. For information on setting the Excessive Soft Error thresholds, refer to "ExcSftErrTh" on page 35-2.

LostFrTh

Syntax

```
SETDefault !<port> -LNM LostFrTh = <number> (0–127)
SHow [!<port> | !*] -LNM LostFrTh
SHowDefault [!<port> | !*] -LNM LostFrTh
```

Default 50

Description The LostFrTh parameter sets a threshold for the Lost Frames soft error counter kept by the Ring Error Monitor. When this threshold is crossed, a notification is sent to those LAN Net Manager stations that monitor this token ring port. If this parameter has a value of 0, the Ring Error Monitor does not generate notification frames for this type of Non-Isolating Error.

MinDecErrTh

Syntax

```
SETDefault !<port> -LNM MinDecErrTh = <number> (0–127)
SHow [!<port> | !*] -LNM MinDecErrTh
SHowDefault [!<port> | !*] -LNM MinDecErrTh
```

Default 50

Description The MinDecErrTh parameter sets a threshold for the number of times the Ring Error Monitor attempts to set its decrement value below the minimum value allowed. When this threshold is crossed, a notification is sent to those LAN Net Manager stations that monitor this token ring port. If this parameter has a value of 0, the Ring Error Monitor does not generate notification frames for this type of non-isolating error.

NumAltMgrs

Syntax

```
SETDefault -LNM NumAltMgrs = <number> (0–5)
SHow -LNM NumAltMgrs
SHowDefault -LNM NumAltMgrs
```

Default 4

Description The NumAltMgrs parameter specifies the maximum number of alternate LAN Net Manager stations supported by the bridge/router. The total number of reporting links supported is one greater than the value of this parameter (the number of alternate managers plus one controlling manager).

PassWord

Syntax

```
SETDefault -LNM PassWord = “<string>”
SHow -LNM PassWord
```

Default 00000000

Description The PassWord parameter sets and displays the password that is used by LAN Net Manager stations when establishing reporting links. This must be the same password entered in the IBM LAN Manager application under System Parameters. The same password is used regardless of whether the type of reporting link is controlling or observing. The password can be up to eight characters in length, and any ASCII character can be used.

RcvCnTFErrTh

Syntax

```
SETDefault !<port> -LNM RcvCnTFErrTh = <number> (0–127)
SHow [!<port> | !*] -LNM RcvCnTFErrTh
SHowDefault [!<port> | !*] -LNM RcvCnTFErrTh
```

Default 50

Description The RcvCnTFErrTh parameter sets a threshold for the number of times a receiver-congestion table-full condition may be encountered by the Ring Error Monitor. This condition is detected when all entries in the receiver-congestion table are in use, and a Report Soft Error MAC frame containing a non-zero value for receiver-congestion errors is received from a station for which there is no entry in the table.

RcvConErrTh

Syntax

```
SETDefault !<port> -LNM RcvConErrTh = <number> (0–127)
SHow [!<port> | !*] -LNM RcvConErrTh
SHowDefault [!<port> | !*] -LNM RcvConErrTh
```

Default 50

Description The RcvConErrTh parameter sets a threshold for the Receiver Congestion Errors soft error counter kept by the Ring Error Monitor. When this threshold is crossed, a notification is sent to those LAN Net Manager stations that monitor this token ring port. If the parameter’s value is 0, the Ring Error Monitor does not generate notification frames for this type of Non-Isolating Error.

SftErrRptTimer

Syntax

```
SETDefault -LNM SftErrRptTimer = <number> (1—65,535)
SHow -LNM SftErrRptTimer
SHowDefault -LNM SftErrRptTimer
```

Default 200

Description The SftErrRptTimer parameter specifies the value of the Soft Error Report Timer returned to all ring stations and Lan Net Manager stations that request it. The Soft Error Report Timer parameter indicates the time-out value (in units of 10 milliseconds) for the ring station’s T (soft_error_report) timer. This timer specifies the minimum interval of time between Report Soft Error MAC frames are sent to the REM. Waiting a minimum amount of time allows stations to collect multiple error counts into one transmission during periods of high numbers of errors, which avoids additional congestion.

TblFlErrTh

Syntax

```
SETDefault !<port> -LNM TblFlErrTh = <number> (0–127)
SHow [!<port> | !*] -LNM TblFlErrTh
SHowDefault [!<port> | !*] -LNM TblFlErrTh
```

Default 50

Description The TblFlErrTh parameter sets a threshold for the number of times the Ring Error Monitor may encounter an isolating-table-full condition. When this threshold is crossed, a notification is sent to those LAN Net Manager stations that monitor this token ring port. If this parameter’s value is 0, the Ring Error Monitor does not generate notification frames for this type of non-isolating error.

TokErrTh

Syntax

```
SETDefault !<port> -LNM TokErrTh = <number> (0–127)
SHow [!<port> | !*] -LNM TokErrTh
SHowDefault [!<port> | !*] -LNM TokErrTh
```

Default 50

Description The TokErrTh parameter sets a threshold for the Token Error soft error counter kept by the Ring Error Monitor. When this threshold is crossed, a notification is sent to those LAN Net Manager stations that monitor this token ring port. If this parameter has a value of 0, the Ring Error Monitor does not generate notification frames for this type of non-isolating error.

VirBrNum

Syntax

```
SETDefault !<port> -LNM VirBrNum = <number> (0–15)
SHow [!<port> | !*] -LNM VirBrNum
SHOwDefault [!<port> | !*] -LNM VirBrNum
```

Default 0

Description The VirBrNum parameter specifies the value assigned to the virtual bridge associated with the specified port. When bridging more than two token ring networks, virtual bridges are required because of limitations imposed by LAN Net Manager.

VirRingNum

Syntax

```
SETDefault -LNM VirRingNum = [None | <number> (1–4095)]
SHow -LNM VirRingNum
SHowDefault -LNM VirRingNum
```

Default None

Description The VirRingNum parameter specifies the ring number of the virtual ring presented to a LAN Net Manager station. When bridging more than two token rings, a virtual ring is needed because of limitations of LAN Net Manager. The default value None means that the bridge/router has not been configured as a virtual ring. You must configure the bridge/router as a virtual ring, using a nonzero virtual ring number, to provide LAN Net Manager support.

36 MIP SERVICE PARAMETERS

This chapter describes the Multicast Internet Protocol (MIP) Service parameters. The MIP Service is related to the Distance Vector Multicast Routing Protocol (DVMRP) and the Multicast Open Shortest Path First (MOSPF) Services. Table 36-1 shows the MIP Service parameters and commands.

Table 36-1 MIP Service Parameters and Commands

Parameters	Commands
CONFiguration	SHow, SHowDefault
CONTrol	SETDefault, SHow
LocalGroups	ADD, DELete, FLush, SHow, SHowDefault
PaceMode	SETDefault, SHow
QueryInterval	SETDefault, SHow
SMDSGroupAddr	ADD, DELete, SHow, SHowDefault
THreshold	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.

CONFiguration

Syntax

```
SHow [!<port> | !<tunnel ID> | !*] -MIP CONFiguration
SHowDefault [!<port> | !<tunnel ID> | !*] -MIP CONFiguration
```

Default No default

Description The CONFiguration parameter displays the current settings of parameters in the MIP Service. It also displays which multicast routing protocol is running.

CONTrol

Syntax

```
SETDefault -MIP CONTrol = [Enable | Disable]
SHow -MIP CONTrol
```

Default Disable

Description The CONTrol parameter enables or disables multicast routing, and displays whether multicast routing is in service.

LocalGroups

Syntax

```
ADD !<port> -MIP LocalGroups <Group addr>
DELete !<port> -MIP LocalGroups {<Group addr> | ALL}
FLush [!<port>] -MIP LocalGroups [<Group addr>]
SHow [!<port> | !*] -MIP LocalGroups [<Group addr>]
SHowDefault [!<port> | !*] -MIP LocalGroups [<Group addr>]
```

Default No default

Description The LocalGroups parameter adds, deletes, flushes, and displays local group memberships. The router learns local group memberships through the Internet Group Management Protocol (IGMP) group report messages from the host, and also when groups are statically added with the ADD command.

Even though the system is not running as a host, you can register to a group or a set of groups so that any multicast packets destined to the configured group will be forwarded to the LAN by the router even though no member is on the LAN.

Use ADD to register to a group; groups added in this way are considered static entries. Use the DELete command to delete static entries and unregister from a group. The DELete -MIP LocalGroups ALL command unregisters all the static groups. These commands can be used for debugging purposes.

FLush removes all the groups learned from the IGMP; groups learned from IGMP are considered dynamic entries.

The SHow and SHowDefault commands display all local group membership for all ports or for the specified port.

Values

<Group addr>	The Class D multicast address of the group to be added, deleted, flushed, or displayed.
ALL	Unregisters all groups when used with the DELete command.

PaceMode

Syntax

```
SETDefault !<port> -MIP PaceMode = [Enable | Disable]
SHow [!<port> | !*] -MIP PaceMode
```

Default Disable

Description The PaceMode parameter maps multicast IP addresses to MAC addresses with the Universal/Local bit set in the IEEE 48-bit address. For example, it maps to 03-00-5E-xx-xx-xx instead of 01-00-5E-xx-xx-xx.

With PaceMode enabled, data sent from the router through a set of pace-enabled switches is tagged as high priority and goes to the head of the transmit queue for transmission and the head of the receive queue when the packet arrives at its destination. PaceMode moves delay-sensitive traffic (such as voice and video) ahead of delay-tolerant data traffic (e-mail).

QueryInterval

Syntax

```
SETDefault !<port> -MIP QueryInterval = <seconds>(5–5400)
SHow [!<port> | !*] -MIP QueryInterval
```

Default 120 seconds (implies that the MembershipExpirationTime = 260)

Description The QueryInterval parameter specifies how often an IGMP Query message is sent to request local group membership. Only the designated router sends the queries onto the associated network. The designated router is elected if it has the lowest IP address on that network (when running the DVMRP Protocol) or the one with the highest router priority (when running the MOSPF Protocol).

The QueryInterval parameter also derives the time (MembershipExpirationTime) which indicates how long a local group membership is valid without confirmation. The MembershipExpirationTime value is set to two times the value of this parameter plus 20 seconds.

The SHow command shows the query interval and whether the router is the designated router for the specified port. If it is, the word Querier is displayed.

SMDSGroupAddr

Syntax

```
ADD -MIP SMDSGroupAddr <IP addr> $<E0–E999999999999999>
DELete -MIP SMDSGroupAddr {<IP addr> [$<E0–E999999999999999>] |
  ALL}
SHow -MIP SMDSGroupAddr [<IP addr>]
SHowDefault -MIP SMDSGroupAddr [<IP addr>]
```

Default No default (the Switched Multimegabit Data Service (SMDS) group address table is empty)

Description The SMDSGroupAddr parameter adds, deletes, or displays an SMDS group address for use in forwarding multicast IP packets to nodes on SMDS networks that have the same IP subnet. This parameter allows you to separate the multicast IP packets from unicast IP packets.

When multicast IP packets are to be forwarded on an SMDS interface and no corresponding group address is configured with this parameter, the system tries to locate the corresponding group address that is configured using the -IP SMDSGroupAddr parameter.

Values

<IP addr>	Refers to the IP network address, for example, 129.2.0.0
<E0–E999999999999999>	The format of an SMDS group address. The group address type is used to route data to all routers 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, it is padded on the right with Fs. An SMDS group address is the only valid address that can be used with this parameter.
ALL	Used with the DELete command to delete all the IP networks and SMDS group address mappings.

THreshold

Syntax

```
SETDefault {!<port> | !<tunnel ID>} -MIP THreshold =
  <value>(1–255)
SHow [!<port> | !<tunnel ID> | !*] -MIP THreshold
```

Default 1

Description The THreshold parameter specifies the minimum threshold required for a multicast datagram to be forwarded out the given interface. The time-to-live (TTL) value of the received multicast datagram is compared to the threshold value. If the TTL value is less than the threshold, the datagram is discarded. If the TTL value is greater than or equal to the threshold, the router forwards the datagram on the specified interface.

The threshold can provide scope control for the following TTL values, which are not standards but accepted conventions:

- Datagrams with initial TTL 0 are restricted to the same host.
- Datagrams with initial TTL 1 are restricted to the same subnet.
- Datagrams with initial TTL 32 are restricted to the same site.
- Datagrams with initial TTL 64 are restricted to the same region.
- Datagrams with initial TTL 128 are restricted to the same continent.
- Datagrams with initial TTL 255 are unrestricted in scope.

37 MOSPF Service Parameters

This chapter describes the Multicast Open Shortest Path First (MOSPF) Service parameters. The MOSPF Service is related to the DVMRP, the MIP, and the OSPF Services. Table 37-1 lists the MOSPF Service parameters and commands.

Table 37-1 MOSPF Service Parameters and Commands

Parameters	Commands
CONFiguration	SHow
CONTrol	SETDefault, SHow
DestGroup	ADD, DELete, SHow
Dvmrp	ADD, DELete, SHow
ForwardTable	FLush, SHow
MABR	SETDefault, SHow
PolicyControl	SETDefault, SHow

CONFiguration

Syntax

```
SHow [!<port> | !*] -MOSPF CONFiguration
```

Default No default

Description The CONFiguration parameter displays the current settings of the MOSPF Service parameters.

CONTrol

Syntax

```
SETDefault !<port> -MOSPF CONTrol = [Enable | Disable], [Multicast|
 Unicast]
SHow [!<port> | !*] -MOSPF CONTrol
```

Default Disable, Multicast

Description The CONTrol parameter determines whether multicast IP packets are forwarded on the interface.

3Com recommends all interfaces be configured as Enable, Multicast. All routers must be configured identically, on a subnet, or incorrect multicast routing may result.

Values

Enable | Disable	Enable allows multicast Internet Protocol (IP) packets to be forwarded on the interface. When Enable is selected, two more options, Multicast or Unicast, are available.

Disable prevents multicast IP packets from being forwarded on the interface. Received multicast IP packets are also not forwarded. The Disable value on an interface only disables data traffic forwarding on that interface; the router can continue to claim to be MOSPF-capable to all neighbors on that interface.

Multicast | Unicast

Multicast allows multicast IP packets to be forwarded over the media as data-link level multicast packets. This value is only effective on LAN-type interfaces such as Ethernet, token ring, Fiber Distributed Data Interface (FDDI), and Switched Multimegabit Data Service (SMDS). On WAN interfaces with no multicast capability, all multicast packets are encapsulated as unicast IP packets.

Unicast allows multicast IP packets to be forwarded as data-link unicast packets using media access control (MAC) level unicast addresses. When Unicast is selected, hosts residing on the interface do not receive multicast IP packets; Internet Group Management Protocol (IGMP) group membership is not monitored, and IGMP queries are not sent by the router. Use the Unicast value only to ban hosts from receiving multicast IP packets or when multiple types of multicast routing protocols, such as Distance Vector Multicast Routing Protocol (DVMRP), are running on the same subnet.

DestGroup

Syntax

```
ADD -MOSPF DestGroup <subnet>/<mask> [Accept | Reject]
DELete -MOSPF DestGroup <subnet>/<mask>
SHow -MOSPF DestGroup
```

Default No default subnet or mask; Accept

Description The DestGroup parameter controls data packet forwarding between MOSPF and DVMRP domains. For this parameter to take effect, the -MOSPF PolicyControl parameter must be set to DestGroup. For more information, refer to “PolicyControl” on page 37-5.

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.

Specifies the mask to be 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.

Accept causes the following actions by the multicast router:

- 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.
- 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.

Reject causes the following actions by the multicast router:

- 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.
- 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.

Dvmrp

Syntax

```
ADD -MOSPF Dvmrp <subnet>/<mask> [Aggregate | Individual | Reject]
  [<metric>] [Type1 | Type2]
DELete -MOSPF Dvmrp <subnet>/<mask>
SHow -MOSPF Dvmrp
```

Default

No default (the table is empty)
No default subnet or Mask
Aggregate
Metric = 65535
Type1

Description

The Dvmrp parameter allows routes learned from a DVMRP domain to be accepted (advertised) into the MOSPF domain. The selected routing information is advertised as external link state advertisements (LSAs).

If the routes are accepted, multicast packets originated from those sources can be forwarded into an MOSPF domain if the -MOSPF PolicyControl parameter is set to Dvmrp. For more information, refer to “PolicyControl” on page 37-5.

Values

<subnet>/<mask>

Identifies an address range to which all DVMRP source networks are compared. If a DVMRP 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.

A particular address may fall into multiple subnet/mask ranges. In this situation, the most specific match (the highest mask bits) is chosen. 0.0.0.0/0 is always the lowest priority range.

Aggregate

All DVMRP source networks are aggregated by a single route <subnet>/<mask>, which summarizes multiple networks using supernetting.

The Aggregate option can significantly reduce the external routing information imported into the OSPF domain. Typical MBONE routing tables contain thousands of routes, so this option can dramatically reduce the memory or CPU overhead in your OSPF routers.

Individual

Each DVMRP source network is advertised as learned into the MOSPF domain.

Reject

The DVMRP source network is not advertised into the MOSPF domain. If a particular source network is rejected (not advertised), multicast packets originated from that source network are not forwarded into the MOSPF domain.

<metric>

A value between 0 and 65,535. The default is 65535.

Type1 | Type2

If Aggregate or Individual is selected, the source subnet information can be advertised as either a Type1 or Type2 external LSA. Type1 is preferred over Type2 regardless of the metric.

The router scans through the entire DVMRP routing table of sources. For each route, it finds all possible matches in the DVMRP table. If there is no match, the route is ignored. If there is a match or multiple matches, the most specific match (the one with the longest subnet mask) is chosen.

If Reject is selected, the router examines the next route. Otherwise, the route is advertised as an OSPF external LSA with the specified metric and type.

ForwardTable

Syntax

```
FLush -MOSPF ForwardTable
SHow -MOSPF ForwardTable [<destination>]
```

Default No default

Description The ForwardTable parameter flushes or displays the current forwarding cache built by MOSPF. If <destination> is specified, only entries toward the particular destination, or IP address, are displayed.

The MOSPF forwarding table is built only when the router attempts to forward IP multicast packets. The table shows packets the router has recently processed including those successfully forwarded or discarded. The forwarding table varies from router to router because not all routers forward multicast packets. Routers may periodically flush the forwarding table and also when topology changes are made.

MABR

Syntax

```
SETDefault -MOSPF MABR = Enable | Disable
SHow -MOSPF MABR
```

Default Enable

Description The MABR parameter determines whether the router performs interarea multicast forwarding.

For this parameter to take effect, the router must be an OSPF Area Border Router (ABR). Not all ABRs need to be multicast-capable or interarea multicast forwarders.

Values

Enable When enabled, the router summarizes group membership information from nonbackbone areas into the backbone. The router declares itself as a wildcard multicast receiver to all its attached nonbackbone areas to attract multicast packets of all destinations. The router forwards multicast packets between areas. This router must be an OSPF ABR for the parameter to take effect.

Disable When disabled, the router does not relay group membership LSAs between areas. It does not declare itself as a wildcard multicast receiver.

PolicyControl

Syntax

```
SETDefault -MOSPF PolicyControl = ([Dvmrp | NoDvmrp], [DestGroup |
  NoDestGroup])
SHow -MOSPF PolicyControl
```

Default NoDvmrp, NoDestGroup

Description The PolicyControl parameter determines whether the router needs to perform inter-AS multicast forwarding, whether the DVMRP-sourced packets are accepted as valid, and whether data packets need to be forwarded between the MOSPF and DVMRP domains.

This parameter only allows the MOSPF domain to accept DVMRP-sourced multicast packets. This limitation may be sufficient if you only have hosts that listen to multicast traffic in the MOSPF domain. If you have hosts that transmit multicast traffic in the MOSPF domain, a similar configuration must be completed in the DVMRP Service, otherwise half-duplex communication occurs. For more information, refer to “MOspf” on page 20-6 and “PolicyControl” on page 20-8.

MOSPF and OSPF are designed to operate within an autonomous system. These protocols are not suited for an inter-AS role. If an MOSPF domain is to become a transit domain for DVMRP, you must configure tunnels between those DVMRP border routers to complete the connection.

Values

Dvmrp | NoDvmrp

When set to Dvmrp, the router functions as an inter-AS multicast forwarder and declares itself as a wild-card multicast receiver to all its attached areas to attract multicast packets of all destinations. The router imports the routes sourced from DVMRP into MOSPF as external LSAs. The routes that are imported are configured through the Dvmrp parameter. For more information, refer to "Dvmrp" on page 37-3.

DestGroup | NoDestGroup

When set to DestGroup, data packets are forwarded between MOSPF and DVMRP domains according to the lists established by -MOSPF DestGroup parameter. For more information, refer to "DestGroup" on page 37-2. If no lists are established, the default action is to forward the packet between domains.

When set to NoDestGroup, no filtering is performed, and all data packets are forwarded between domains.

38 NLSP SERVICE PARAMETERS

This chapter describes all the parameters that are related to NetWare Link Services Protocol (NLSP) routing. Table 38-1 lists the NLSP Service parameters and commands.

Table 38-1 NLSP Service Parameters and Commands

Parameters	Commands
ADJacencies	SHow
AreaAddress	ADD, DELete, SHow, SHowDefault
BufferSize	SETDefault, SHow
CONFiguration	SHow
CONTrol	SETDefault, SHow
Cost	SETDefault, SHow
CsnpTime	SETDefault, SHow
DISHelloTime	SETDefault, SHow
HelloPassWord	SETDefault, SHow
HelloTimeLan	SETDefault, SHow
HelloTimeWan	SETDefault, SHow
HoldTimeFactor	SETDefault, SHow
LinkStateData	SHow
LspBcastTime	SETDefault, SHow
LspMAxTime	SETDefault, SHow
LspMInTime	SETDefault, SHow
LspRtxTime	SETDefault, SHow
Multicast	SETDefault, SHow
Multicast8025	SETDefault, SHow
Neighbors	ADD, DELete, SHow
PRIOrity	SETDefault, SHow
PsnpTime	SETDefault, SHow
SPFHolddown	SETDefault, SHow
SystemID	SETDefault, SHow
SystemName	ADD, DELete, SHow
TRACE	SET, SHow

ADJacencies

Syntax `SHow -NLSP ADJacencies`

Default No default (NLSP adjacency database is empty)

Description The ADJacencies parameter displays the current router adjacencies.

Router adjacencies include adjacencies learned from both LANs and WAN links. An adjacency can be in the UP state, meaning the adjacency is available for exchanging routing information. An adjacency not yet fully established is displayed in INIT state. An adjacency in INIT state for an extended period usually indicates network problems.

There are three possible adjacency types: L1ONLY, L2ONLY, and L1+2. An L1ONLY adjacency can only exchange Level 1 routing packets. An L2ONLY adjacency can only Only L2 routing packets. An L1+2 adjacency can exchange both levels of routing packets. This is a Level 1-only implementation, L2ONLY and L1+2 will not show up.

A particular router can have multiple adjacencies because of the following situations:

- There can be separate L1ONLY and L2ONLY adjacencies toward the same router. Adjacencies of different levels are treated independently.
- Adjacencies can be learned from local interfaces; each are treated independently.
- Adjacencies can be learned from different source MAC addresses because the router has multiple interfaces to the same LAN.

Adjacencies are established through the protocol data unit (PDU) exchanges. All adjacencies have a remaining lifetime timer associated with them. An adjacency is deleted if the PDU is not received and the timer expires. The timer value is determined by the source router. For more information, refer to “HelloTimeLan” on page 38-6, “HelloTimeWan” on page 38-7, “DISHelloTime” on page 38-5, and “HoldTimeFactor” on page 38-7.

AreaAddress

Syntax

```
ADD -NLSP AreaAddress <net> <mask>
DELete -NLSP AreaAddress <net> <mask>
SHow -NLSP AreaAddress
SHowDefault -NLSP AreaAddress
```

Default 00000000 00000000

Description The AreaAddress parameter configures a group of networks as an area for a router. Up to three area addresses may be added to the router.

The area address is a pair of 32-bit integers: the first is an Internetwork Packet Exchange (IPX) network number, the second is a mask. The mask has a number of leading 1 bits, followed by 0 bits. All the 1 bits must be contiguous. An example of area address is 12345600 FFFFFF00.

Area addresses have the following attributes:

- An IPX network number identifying the area.

  In an area address of 12345600 FFFFFF00, 12345600 is the IPX number of the area.
- A mask identifying a range of networks that reside within the area.

For example, all network numbers in the range 12345600 to 123456FF reside within the area. It is not necessary that all of the networks are operational.

- All network numbers within the area must fall within the address range.

  With an area address of 12345600 FFFFFF00, all IPX networks must begin with 123456XX.

The following are area displays:

- The SHow -NLSP AreaAddress command displays the computed area addresses for the router's home area.

  The computed area addresses for the router's home area is accomplished by taking all the advertised area addresses of all the routers (including this router) in the area. If the set of addresses exceed three, numerically higher addresses are dropped.

- The SHowDefault -NLSP AreaAddress command displays the statically configured area address of this router.

  Neighboring routers compare each other's area addresses to determine if they should establish adjacencies. Routers with noncompatible area addresses do not communicate or exchange routing information. This parameter must be properly configured on all routers.

  The default value, 00000000 00000000, means all IPX networks can reside within the area.

  Up to three area addresses can be configured on each router. A numerical relationship between the areas addresses is not necessary. Addresses can overlap each other if necessary. Multiple area addresses can produce graceful address transition, that is, if the network is undergoing IPX address consolidation.

BufferSize

Syntax

```
SETDefault -NLSP BufferSize = <bytes> (576–4096)
SHow -NLSP BufferSize
```

Default 512

Description The BufferSize parameter determines the maximum size of routing packets (LSP, CSNP, and PSNP) that can originate a router. If a particular routing packet exceeds the buffer size limit, the router fragments the packet. If you increase the BufferSize parameter, the router's efficiency is increased and the amount of memory used is reduced. The BufferSize includes IPX packet headers, but does not include link level MAC headers.

CONFiguration

Syntax

```
SHow -NLSP CONFiguration
```

Default No default

Description The CONFiguration parameter displays the values of the AreaAddress, CONTrol, Cost, and ADJacencies parameters.

CONTrol

Syntax

```
SETDefault !<port> -NLSP CONTrol = ([Enable | Disable], [DynamicNbr |
   NoDynamicNbr])
SHow [!<port> | !*] -NLSP CONTrol
```

Default Disable, DynamicNbr on nonbroadcast multiaccess (NBMA) interfaces

Description The CONTrol parameter selectively enables or disables the NLSP routing protocol on a per-interface basis. If some router interfaces are connected to networks that you do not want to run NLSP on use this parameter.

Disabling an interface disables the transmission of hello packets PDUs and other routing packets (LSP, CSNP, and PSNP). When NLSP packets are received on those interfaces, they are also ignored by the service.

Disabling an interface does not disable the IPX Protocol on the interface. IPX packets continue to be accepted from (forwarded to) the interface. If NRIP or SAP are enabled on an interface, you must also enable NLSP on the interface.

Values

Enable | Disable	Enables or disables the NLSP routing protocol.
DynamicNbr | NoDynamicNbr	The DynamicNbr option is only available on ports that are NBMA networks, such as X.25 and Frame Relay. This option is not displayed for non-NBMA networks. Neighbor learning is enabled by default on an NBMA interface. When Neighbor learning is enabled, the dynamic neighbor list is automatically created, and NLSP operates correctly without requiring you to configure static neighbor information. Use the Neighbor parameter to display the learned dynamic neighbors.

Cost

Syntax

```
SETDefault !<port> -NLSP Cost = Default | <number> (1–63)
SHow [!<port> | !*] -NLSP Cost
```

Default The default values are automatically determined by the bit-per-second rate of the media and vary for each type of media as follows:

- 20 for Ethernet
- 19 for 16 MB token ring
- 25 for 4 MB token ring
- 14 for FDDI
- 40 for a 64 KB serial line (PPP, Frame Relay or X.25)
- 27 for 10 MB serial line (PPP, Frame Relay, X.25)

Description The Cost parameter sets the capacity of networks in an area. Higher values indicate lower capacity. You can adjust the parameter with any factor. Interfaces with identical baud rates need not have the same cost. A preferred interface can have a lower cost value relative to other interfaces, and a preferred router can have lower cost values compared to other routers.

You can individually configure the parameters for each interface. The Cost parameter affects the outcome of the decision process for route computation.

CsnpTime

Syntax

```
SETDefault -NLSP CsnpTime = <seconds> (1–600)
SHow -NSLP CsnpTime
```

Default 30 seconds

Description The CsnpTime parameter controls the transmission of the CSNP NLSP routing packet.

Two types of NLSP routing packets maintain the synchronization of link state databases among all the routers in the area. These packets are referred to CSNP and Partial Sequence Number PDU (PSNP). The transmission intervals of these packets are controlled by the CsnpTime and PsnpTime parameters. For more information, refer to "PsnpTime" on page 38-11.

When a new link state PDU is generated, it is immediately propagated or flooded throughout the routing domain. LSPs can get lost, corrupted, or misdelivered during flooding. Routers use the CSNP for resolving these situations. The synchronization procedure is different on LANs and on point-to-point links.

On a LAN, the highest priority router is elected as a designated router. The Designated Intermediate System (DIS) periodically sends out CSNPs summarizing all the LSPs it has in its database. Other routers compare the CSNP information with their local databases as follows:

- If everything is in sync, they take no action.
- If some LSP entries in the DIS are old or missing, those LSPs are sent back to the DIS (using PSNP), which brings the DIS up to date.
- If some LSP entries are newer, they request DIS to resend them through PSNP packets.

CsnpTime is effective only on LAN interfaces, and only when the router is elected as the DIS. A smaller CsnpTime value guarantees faster synchronization but at the expense of higher network bandwidth consumption.

DISHelloTime

Syntax

```
SETDefault -NLSP DISHelloTime = <seconds> (1–100)
SHow -NLSP DISHelloTime
```

Default 10 seconds

Description The DISHelloTime parameter controls the interval of the hello packets (Intermediate System-to- Intermediate System hello packet (IIH) PDUs) sent by a designated DIS router on the LAN. A DIS is a router with the highest priority (see "PRIOrity" on page 38-11) on a LAN. The DIS router periodically sends out hello packets on all its interfaces. By sending or receiving hello packets, routers learn the existence and location of other directly reachable routers. If a router resigns as DIS, it uses the HelloTimeLan parameter for its IIH transmission interval. Refer to "HelloTimeLan" on page 38-6.

Each IIH PDU carries a lifetime value, which is HoldTimeFactor times the value of HelloTimeLan parameter (or DISHelloTime). If the lifetime value expires before further IIH PDUs are received, the router is considered down. If you set the

DISHelloTime parameter higher, the network bandwidth consumption is reduced by IIH PDUs. If you set it lower, a failed router is discovered sooner because the lifetime value is small.

Routers are not required to carry identical hello time values; you can configure each router with different values. Configure unstable networks (routers) with smaller values so that topology changes (for example, a failing router) can be detected quickly.

DISHelloTime is effective only on LAN interfaces, and only when the router is elected as DIS.

HelloPassWord

Syntax

```
SETDefault !<port> -NLSP HelloPassWord = None | “<password (1–16
   characters)>”
SHow [!<port> | !*] -NLSP HelloPassWord
```

Default None (no password configured)

Description The HelloPassWord parameter specifies passwords for hello packets. You can specify one password for each interface. If a password is specified, that password is transmitted in the outgoing hello packets. The same password verifies hello packets received on the interface. Mismatched passwords cause routers to reject each other and are reported as authentication errors.

The HelloPassWord authentication is 3Com’s proprietary addition to the NLSP Protocol. When you interoperate with other vendors’ products, it is recommended that these passwords be set to None.

HelloTimeLan

Syntax

```
SETDefault !<port> -NLSP HelloTimeLan = <seconds> (1–100)
SHow [!<port> | !*] -NLSP HelloTimeLan
```

Default 20 seconds

Description The HelloTimeLan parameter controls the interval frequency of hello packet transmissions on a LAN for non-DIS routers. If a router does not operate as a DIS, it uses this parameter for its IIH transmission interval. Otherwise, it uses DISHelloTime for the hello interval.

Routers periodically send hello packets (IIH PDUs) to all of their interfaces. By sending and receiving hello packets, routers learn the existence and location of other directly reachable routers. If you set the HelloTimeLan parameter higher, the network bandwidth consumption by IIH PDUs is reduced. If you set it lower, a failed router is detected sooner because the lifetime value is smaller.

Routers are not required to carry identical hello time values. You can configure each router with different values. Configure unstable networks (routers) with smaller values so that topology changes (for example, a failing router) can be detected quickly.

HelloTimeWan

Syntax

```
SETDefault !<port> -NLSP HelloTimeWan = <seconds> (1–100)
SHow [!<port> | !*] -NLSP HelloTimeWan
```

Default 20 seconds

Description The HelloTimeWan parameter controls the interval or frequency of hello packet transmission on a WAN. A router periodically sends out hello packets (IIH PDUs) onto all its interfaces. By sending and/or receiving hello packets, routers learn the existence and location of other directly reachable routers.

If the HelloTimeWan setting is higher, the network bandwidth consumption by IIH PDUs is reduced. If it is lower, a failed router is detected sooner because the lifetime value is small.

Routers are not required to carry identical hello time values. You can configure each router with different values. Configure unstable networks (routers) with smaller values so that topology changes (for example, a failing router) can be detected quickly.

HoldTimeFactor

Syntax

```
SETDefault -NLSP HoldTimeFactor = <number> (2–20)
SHow -NLSP HoldTimeFactor
```

Default 3

Description The HoldTimeFactor parameter determines the age time for hello packets. The age time is determined by the sender and is explicitly encoded in the hello packets. For example, if the sender has a hello interval of 10 seconds, and HoldTimeFactor of 4, then each hello packet is remembered for 40 (10 X 4) seconds.

LinkStateData

Syntax

```
SHow -NLSP LinkStateData <LSP ID>
```

Default No default (link state database is empty)

Description The LinkStateData parameter displays the contents of the current Link State PDU database. It shows summary information of the L1 link state database if it exists. The following is the summary information given by the LinkStateData parameter:

- An LSP identifier that is an 8-octet hexadecimal ID value.

  The first 6 octets are the system ID of the originating router. If SystemName (see “SystemName” on page 38-13) is configured, then the name of each router is displayed instead of the 6-octet hexadecimal value. The 7th octet indicates whether the LSP is generated for a pseudonode. A zero 7th octet indicates the LSP is generated for the router itself. The 8th octet is usually zero, unless the LSP has been fragmented into multiple pieces (see “BufferSize” on page 38-3), which causes all LSPs with identical leading 7 octets to be considered as one.
- A sequence number that is a 4-octet hexadecimal number.

- An overflow bit to indicate if the originating router is having a memory shortage.
- An attach bit that is applicable only to non-pseudonode, L2 routers.

  This bit indicates whether the router can reach other areas in the L2 routing domain or other routing domains.
- A router type number specifying that the router is either an L1 router or L2 router.
- A data length number specifying the length of the data contents as a decimal value.
- A checksum value that is 2 octets of a hexadecimal value.

Example To see a detailed display of data section of an LSP named Micky, enter:

```
SHow -NLSP LinkStateData Micky
SHow -NLSP LinkStateData Micky:00
SHow -NLSP LinkStateData Micky:00:00
```

The software displays detailed contents of all LSPs with matching 6, 7, or 8 leading octets.

```
-------------------Level 1 Link State Database----------------------
LSP-ID     sequence  remaining overflow    router  data  checksum
           number    lifetime  attach bit  bit     type  length
M86:00:00  17B       309       0           1       L1    47A569(OK)
M86:01:00  17B       309       0           0       L1    14E45D(OK)
M86:02:00  17C       309       0           0       L1    25CC7C(OK)
M79:00:00   53       970       0           1       L1    36A3E8(OK)
```

LspBcastTime

Syntax

```
SETDefault -NLSP LspBcastTime = <milliseconds> (1–1000)
SHow -NLSP LspBcastTime
```

Default 33 milliseconds

Description The LspBcastTime parameter is used only on LAN interfaces and controls the maximum rate of transmitting routing packets (LSP, CSNP, and PSNP) on broadcast networks. It specifies the minimal interval between successive transmissions. This parameter prevents slow routers from being overwhelmed by excessive updates and guarantees that a router does not send more than 1,000 LspBcastTime routing packets within any one second. Transmitted updates can be sent one after the other back-to-back.

LspMAxTime

Syntax

```
SETDefault -NLSP LspMAxTime = <seconds> (1–50000)
SHow -NLSP LspMAxTime
```

Default 7,200 seconds

Description The LspMAxTime parameter specifies the maximum interval between LSP regeneration. All the link state PDUs (LSPs) generated by an router carry a lifetime of 7,200 seconds. You need to periodically regenerate LSPs before the lifetime expires, even if there are no topology changes since the last time the LSPs were issued.

At the expiration of LspMAxTime, the router goes through its complete LSP database verifying the data located in memory. The router also recalculates all of its routing table, making sure corrupted routes do not persist.

Other events, such as a link or an adjacency going up or down, can trigger LSP generation before the LspMAxTime timer expires. Those events cause LSP contents to be modified and immediately reissued. LSP generation driven by events does not reset the LspMAxTime timer.

LspMInTime

Syntax

```
SETDefault -NLSP LspMInTime = <seconds> (1–30)
SHow -NLSP LspMInTime
```

Default 5 seconds

Description The LspMInTime parameter controls the minimum interval between the generation of LSPs driven by events to prevent flooding caused by continuously generated packets. Excessive LSP generations can consume network bandwidth and CPU cycles that occur when the constant update of the routing tables is necessary.

A router can regenerate an LSP when the following events occur:

- An adjacency or port is up or down.
- A change in port cost.
- A change in area address.
- A change in designated router status.
- A change in learned Routing Information Protocol (RIP) and Service Advertising Protocol (SAP) entries, if the router put them into the NLSP routing domain.

These events cause the contents of the LSP to change. Those affected LSPs are immediately regenerated and flooded throughout the network.

LspRtxTime

Syntax

```
SETDefault -NLSP LspRtxTime = <seconds> (5–30)
SHow -NLSP LspRtxTime
```

Default 5 seconds

Description The LspRtxTime parameter specifies the minimum interval between retransmissions of an update on a point-to-point link. There is no limit on how fast a router can flood updates onto a point-to-point link. Each update must be explicitly acknowledged by the receiving router. If acknowledgment is not received within the link state protocol retransmit time, then the update is retransmitted.

This parameter is only effective on point-to-point links.

Multicast

Syntax

```
SETDefault -NLSP Multicast = Default | <multicast address>
SHow -NLSP Multicast
```

Default %09001BFFFFFF

Description The Multicast parameter displays the multicast address for routers on an Ethernet or Fiber Distributed Data Interface (FDDI) network that are transmitting hello (IIH) and routing packets (LSP, CSNP, and PSNP). Routers must also listen for multicasts from that address. The multidestination addresses need to be consistent among all routers within the routing domain or routing problems can occur. This parameter applies to LAN interfaces only; the multidestination address is displayed as a hexadecimal number in canonical format. If you have routers on an Ethernet or FDDI network that can receive multicast packets, you can set this parameter to broadcast address FFFF FFFF FFFF. The Default option restores the default value of the multicast address after modification.

Multicast8025

Syntax

```
SETDefault -NLSP Multicast8025 = Default | <multicast address>
SHow -NLSP Multicast8025
```

Default %09001BFFFFFF (canonical)
%C0001000000 (noncanonical)

Description The Multicast8025 parameter displays the multicast address for routers on a token ring network that are transmitting hello (IIH) and routing packets (LSP, CSNP, and PSNP). Routers must also listen for multicasts from that address. The multidestination addresses must be consistent among all routers within the routing domain or routing problems can occur.

This parameter applies to token ring interfaces only, the multidestination address is displayed in canonical format. If you have routers on a token ring network that cannot receive multicast packets, you can set this parameter to broadcast address FFFF FFFF FFFF. The Default option restores the default value of the multicast address after modification.

Neighbors

Syntax

```
ADD !<port> -NLSP Neighbors [#<DTE address> | @<DLCI> | &<VCID>]
DELete !<port> -NLSP Neighbors [#<DTE address> | @<DLCI> | &<VCID>]
SHow [!<port> | !*] -NLSP Neighbors
```

Default No default (no neighbors configured)

Description The Neighbors parameter adds or deletes neighbor addresses over an X.25, Frame Relay, or Asynchronous Transfer Mode (ATM) network. You can enter up to 28 neighbors. By default, NLSP does not attempt to establish an adjacency over X.25, Frame Relay, or ATM networks unless you specify the appropriate neighbor information. To allow the remote router to accept the adjacency, the Neighbors parameter of the remote router must also be configured.

Neighbors takes effect immediately. The router initiates the following actions when a neighbor is added:

- Establishes a virtual circuit toward the destination address, if a virtual circuit is not open.
- Begins sending hello packets toward the remote router.
- Starts exchanging routing information with the remote router if establishing the adjacency was successful.

Values		
	#<DTE address>	Adds X.25 neighbors.
	@<DLCI>	Adds Frame Relay neighbors.
	&<VCID>	The local VCID of the PVC statically adds ATM neighbors. The VCID is an alias that identifies the ATM address VPI.VCI and configured using the -ATM PermVirCircuit parameter. For more information, refer to "PermVirCircuit" on page 7-2.

The display shows both the static and dynamically learned neighbors with the dynamically learned neighbors indicated by the (dynamic) suffix. Only static neighbors can be deleted.

PRIOrity

Syntax

```
SETDefault !<port> -NLSP PRIOrity = <number> (1–127)
SHow [!<port> | !*] -NLSP PRIOrity
```

Default 44

Description The PRIOrity parameter sets the priority of a router and is effective only on LAN interfaces. This parameter can be independently configured for each interface. A router can become a designated router on multiple interfaces.

A LAN-designated router is the highest priority router on the LAN. PRIOrity determines the priority of being elected as the DIS on a LAN. Higher values indicates higher priority. Among all routers that have the same priority, numerically higher MAC addresses determine the highest priority.

To prevent constantly changing the DIS on a particular LAN, for example, because a router is going up and then down, the DIS raises its priority value by 20. This router remains as the designated router until another router comes up with higher priority. Then the old DIS resigns and restores its previous priority value (reduces its priority by 20).

PsnpTime

Syntax

```
SETDefault -NLSP PsnpTime = <seconds> (1–60)
SHow -NLSP PsnpTime
```

Default 1 second

Description The PsnpTime parameter controls the transmission intervals or frequency at which the PSNP are transmitted on both LAN and point-to-point interfaces.

There are two kinds of NLSP routing packets that maintain the synchronization of link state database among all the routers in the area. These packets are referred to as CSNP and PSNP. The transmission intervals of these packets are controlled by the CsnpTime and PsnpTime parameters. Refer to "CsnpTime" on page 38-5.

When a new link state PDU is generated, it is immediately propagated or flooded throughout the routing domain. LSPs can get lost, corrupted, or misdelivered in the flooding procedure. Routers use CSNP for resolving these errors. The synchronization procedure is different on LANs and point-to-point links.

On a LAN, the highest priority router is elected as a designated router. The DIS periodically sends out CSNPs summarizing all the LSPs it has in its database. Other routers compare the information in the CSNP with their local databases as follows:

- If everything is in sync, then take no action.
- If some LSP entries in DIS are old or missing, those LSPs are sent back to the DIS, which brings the DIS up to date.
- If some LSP entries in DIS are newer, a PSNP is sent back describing only those entries. The PSNP prompts the DIS transmitting those LSPs.

On a point-to-point link, all the LSPs transmitted must be explicitly acknowledged by a PSNP from the other router. Unacknowledged LSPs are retransmitted (refer to "LspRtxTime" on page 38-9).

SPFHolddown

Syntax

```
SETDefault -OSPF SPFHolddown = <seconds> (0-60)
SHow -OSPF SPFHolddown
```

Default 5

Description The SPFHolddown parameter prevents continuous OSPF computations from using up the available CPU time. This parameter limits OSPF computations to one computation per the SPFHolddown time value.

Setting SPFHolddown to a lower number allows instant reaction to network topology changes. Setting it to a higher number conserves CPU usage. Higher values tend to stabilize the network by slowing down topology changes.

To display the SPFHolddown parameter value, use the SHow command.

SystemID

Syntax

```
SETDefault -NLSP SystemID = [<SystemID> | Default]
SHow -NLSP SystemID
```

Default The factory-shipped MAC address on the Communications Engine Card (CEC) (NETBuilder II bridge/router) or the MAC address of the first LAN interface (SuperStack II) identifier. Each NLSP router must have a globally unique identifier.

Description The SystemID parameter specifies and displays the NLSP server.

SystemName

Syntax

```
ADD -NLSP SystemName <SystemName> <SystemID>
DELete -NLSP SystemName <SystemName>
SHow -NLSP SystemName
```

Default No default (SystemName table is empty)

Description The SystemName parameter selects specific systems and assigns names to them. This parameter makes the TRACE, ADJacencies, and LinkStateData parameter displays more effective because you can assign names to routers instead of using the 6-octet hexadecimal numbers as router identifiers. This parameter has no impact on the protocol operation.

TRACE

Syntax

```
SET -NLSP TRACE = (None, ADJAcency, LSP, SNP, DIS, Hello)
SHow -NLSP TRACE
```

Default None

Description The TRACE parameter displays events in real-time on the locally attached console terminal.

Values

None	Disables all of the displays.
ADJAcency	Indicates when an adjacency goes UP or DOWN.
LSP	Indicates when an LSP is received/sent.
SNP	Indicates when either a CSNP or PSNP is received/sent.
DIS	Indicates when the router becomes/resigns as a DIS.
Hello	Indicates when a hello packet is received/sent.

The TRACE parameter significantly slows down the routing efficiency. This parameter is designed mostly for debugging purposes.

39

NRIP Service Parameters

This chapter describes all the parameters that are related to NetWare Routing Information Protocol (NRIP) routing. Table 39-1 lists the NRIP Service parameters and commands.

Table 39-1 NRIP Service Parameters and Commands

Parameters	Commands
AdvertisePolicy	ADD, DELete, SHow, SHowDefault
AdvToNeighbor	ADD, DELete, SHow, SHowDefault
CONFiguration	SHow
CONTrol	SETDefault, SHow, SHowDefault
DefaultMetric	SETDefault, SHow
HoldTimeFactor	SETDefault, SHow, SHowDefault
MaxResrcRtnmbr	SETDefault, SHow, SHowDefault
PolicyControl	SETDefault, SHow, SHowDefault
RcvFromNeighbor	ADD, DELete, SHow, SHowDefault
ReceivePolicy	ADD, DELete, SHow, SHowDefault
UpdateTime	SETDefault, SHow, SHowDefault

AdvertisePolicy

Syntax

```
ADD !<port> -NRIP AdvertisePolicy [~]{<route> | Default},
  [<list of routes>]
DELete !<port> -NRIP AdvertisePolicy {All | Default |
  <list of routes>}
SHow [!<port> | !*] -NRIP AdvertisePolicy
SHowDefault [!<port> | !*] -NRIP AdvertisePolicy
```

Default No default (no route advertise policies defined)

Description The AdvertisePolicy parameter specifies which routes are advertised on the port to adjacent routers.

The lists of routes can be entered as part of one command with each route separated by a comma (,). For example, <list of routes>:=[~]<route>, [list of routes>].

To include only specific routes for advertisement, use the ADD command. To exclude specific routes from advertisement, use the ADD command with the tilde (~) prefix added to the route entry. When ~ is used for one route specification, it must be used for all. If exclusion lists are mixed with inclusion lists, an error message appears.

When you need to change a list from one type (inclusion or exclusion) to the other, the current list must first be deleted before the new list can be added.

To remove a specific route (including a default route), a list of routes, or the entire list of configured routes, use the DELete command. The All option deletes all the route policies for the specified interface.

The SHow command displays the configured list of routes in the advertise policy. If no port number is specified, then all advertise policy entries are displayed. When a port number is specified, only those advertise policy entries that are associated with that port are displayed.

Values

Default	Advertises default routes on the specified port to adjacent routers.
<list of routes>	Indicates a single Internetwork Packet Exchange (IPX) network number or a range of IPX network numbers, separated by a hyphen, that includes the low and high network numbers in that range. For example: <route>:=<net number>|<net range> <net range>:=<net number>-<net number> <net number>:=[&]<32-bit hex number> (1–FFFFFFFD)

Example 1 To set up a policy specifying that all routes in the range 10 through 100 are advertised on interface 1, enter:

```
ADD !1 -NRIP AdvertisePolicy &10 - &100
```

Example 2 To set up a policy specifying that routes to network 200 are advertised on interface 1, enter:

```
ADD !1 -NRIP AdvertisePolicy &200
```

Example 3 To delete all the route advertisement policies that have been configured for interface 1, enter:

```
DELete !1 -NRIP AdvertisePolicy All
```

Example 4 To set up an exclusion list where all routes except those to networks 10, 20 and 30 are advertised on interface 3, enter:

```
ADD !3 -NRIP AdvertisePolicy ~&10, ~&20, ~&30
```

AdvToNeighbor

Syntax

```
ADD !<port> -NRIP AdvToNeighbor <network>%<mac address> [...]
DELete !<port> -NRIP AdvToNeighbor ALL | <network>%<mac address>
  [...]
SHow [!<port> | !*] -NRIP AdvToNeighbor
SHowDefault [!<port> | !*] -NRIP AdvToNeighbor
```

Default No default (no neighbors configured to advertise to)

Description The AdvToNeighbor parameter specifies which neighbors on each interface receive route reachability information. You can enter a list of neighbors as part of a single command with each neighbor separated by a comma. For example:

```
<network>%<mac address>, <network>%<mac address>, <network>%<mac
  address>
```

The list of neighbors is used when broadcasting route reachability information and when responding to a specific route query from a specific station. If the requesting station address is not part of the neighbor list, then no response is sent.

Inverse entries are not allowed for the AdvToNeighbor list. When an AdvToNeighbor list is specified and enabled through the PolicyControl parameter, instead of through the regular NRIP broadcasts, the router sends the NRIP message as a separate unicast messages to each neighbor listed.

To add to the neighbor list, use the ADD command.

To remove neighbors from a port's neighbor list, use the DELete command and specify the port number and the neighbor address, or specify the port number and the keyword ALL to delete multiple entries for the same port.

The SHow command displays the list of entries in the neighbor list. If the optional port number is not specified, all active neighbor lists are displayed. The display shows both the static and dynamically learned neighbors with the static neighbors indicated by the * symbol. Only static neighbors can be deleted.

Values

<network>	Supply the network number in the following format:
	`[%]<48-bit MAC address in native format> |`
	`MAC <48-bit MAC address in canonical format> |`
	`NcMac <48-bit MAC address in canonical format>`

%<mac address>	The 48-bit MAC address of the host. The MAC address must be entered in the same format (canonical or noncanonical) as used by the host.

CONFiguration

Syntax

```
SHow [!<port> | !*] -NRIP CONFiguration
```

Default No default

Description The CONFiguration parameter displays the current NRIP configuration parameters. If no port number is specified, the SHow -NRIP CONFiguration command displays active information.

Active means the -NRIP CONTrol parameter is set to Listen, and the -IPX CONTrol parameter is set to ROute. If the -IPX CONTrol parameter is not set to ROute, the following message is displayed:

```
IPX is not enabled. Please configure CONTrol and assign NETnumbers
```

Assuming -IPX CONTrol is set to ROute, the active configuration information for ports assigned with IPX network numbers is displayed. For static routes, address mapping, and policies and neighbors, even headers are suppressed if their corresponding tables are empty.

CONTrol

Syntax

```
SETDefault !<port> -NRIP CONTrol = (Auto, [Talk | NoTalk], [Listen
  | NoListen], [Trigger | NoTrigger], [POison | NoPOison],
  [NewNbrMap | OldNbrMap], [PEriodic | NoPEriodic], [DynamicNbr |
  NoDynamicNbr])
SHow [!<port> | !*] -NRIP CONTrol
SHowDefault [!<port> | !*] -NRIP CONTrol
```

Default Auto, Trigger, NoPOison, NewNbrMap, PEriodic, and DynamicNbr on nonbroadcast multiaccess (NBMA) interfaces

Description The CONTrol parameter enables or disables the NRIP Service for the router.

Values

Auto	If Auto is selected, the Talk | NoTalk and Listen | NoListen values are not displayed in the user interface. The Talk and Listen modes are dynamically determined by the software and the current network topology when Auto is selected. Use the SHow -IPX DIAGnostics command to display the current Talk | Listen mode. If Talk | NoTalk or Listen | NoListen are selected, the Auto state is inactive. The Auto setting is useful when the NLSP is enabled. With NLSP, the router stops transmitting updates if it determines no routers or file servers are interested in them (for example, all routers are running NLSP). If NLSP is not enabled, Auto implies both Talk and Listen.
Talk | NoTalk	If Talk is selected, NRIP broadcasts to its neighbors and dynamically maintains the routing table. If NoTalk is selected, regular NRIP updates do not occur.
Listen | NoListen	If Listen is selected, NRIP receives NRIP information from its neighbors and dynamically maintains the routing table. If NoListen is selected, dynamic learning does not occur.
Trigger | NoTrigger	If Trigger is selected, NRIP updates are sent as soon as the topology changes are detected, allowing all routers to advertise their routing tables to each other. If NoTrigger is selected, topology changes are not sent immediately, but routers that are detected are included in their regular updates.
POison | NoPOison	If POison is selected, the router advertises all routes to all neighbors, but when advertising a route to a neighbor that has advertised the same route, the router sets the hop count to infinity (16) to prevent the recipient from adding the route to its routing table. Poison reverse speeds convergence but adds to network overhead. If NoPOison is selected, the router omits routes learned from one neighbor from NRIP updates sent to that neighbor. NoPOison has the advantage of minimizing network overhead in large network configurations at the expense of slower convergence.

NewNbrMap | OldNbrMap

If OldNbrMap is selected, old X.25 or Frame Relay neighbor mapping is used. If NewNbrMap is selected, new X.25 or Frame Relay neighbor mapping is used. The X.25 addresses and Frame Relay DLCIs can be mapped in two different ways: by using IPX network numbers as previously implemented (OldNbrMap) or by using the Ethernet address of the remote router currently implemented (NewNbrMap). This option is set to NewNbrMap by default, but you must select OldNbrMap to interoperate with a neighbor running earlier than 5.0 bridge/router software.

PEriodic | NoPEriodic

If PEriodic is selected, the IPX router periodically generates NRIP updates. To stop periodic NRIP updates, select the NoPEriodic option. When NoPEriodic is set, the IPX router shuts off periodic NRIP updates and switches to incremental updates. When selecting this option, make sure that all participating routers use the same option. NoPEriodic can be used for all media.

Noisy and expensive network chatting of NRIP updates can be eliminated by setting the CONTrol parameter to NoPEriodic. This setting is recommended in a stable and reliable network. Periodic NRIP updates are recommended where frequent topology changes occur.

DynamicNbr | NoDynamicNbr

Neighbor learning is enabled by default on an NBMA interface. With Neighbor learning enabled, the dynamic neighbor list is automatically created, and NRIP operates correctly without requiring you to configure static neighbor information. Use the AdvToNeighbor parameter to display the learned dynamic neighbors.

With DynamicNbr on, NRIP includes dynamically learned neighbors in the AdvToNeighbor table. Dynamic AdvToNeighbor neighbors then stay in the AdToNeighbor table and are considered “trusted neighbors”. These dynamically learned neighbors can only be deleted by resetting -NRIP CONTrol to NoDynamicNbr.

The DynamicNbr option is only available on ports that are NBMA networks, such as X.25 and Frame Relay. This option is not displayed for non-NBMA networks.

DefaultMetric

Syntax

```
SETDefault !<port> -NRIP DefaultMetric = Disable | <hops(1–15)>
  [<ticks>]
SHow [!<port> | !*] -NRIP DefaultMetric
```

Default Disable

Description The DefaultMetric parameter specifies whether NRIP advertises the default route on the specified port. Use the SHow command to display the current setting for a specified port or for all ports.

Values		
	Disable	Turns off default route advertisement.
	<hops>	Enables default route advertisement within the corresponding hop count. The hop count must be in the range of 1 to 15.
	<ticks>	A measurement of the delay for a destination that is specified with a number between 1 and 65535. By default, this value is 1. The ticks value allows the router to select the line with the lowest delay if more than one route to the same destination exists. The lower the tick value, the lower the delay.

HoldTimeFactor

Syntax

```
SETDefault -NRIP HoldTimeFactor = <number> <1-24>
SHow -NRIP HoldTimeFactor
SHowDefault -NRIP HoldTimeFactor
```

Default 3

Description The HoldTimeFactor parameter calculates the aging-out time. For each Routing Information Protocol (RIP) entry learned from a particular port, the age-out time is calculated by multiplying the UpdateTime of the port and the HoldTimeFactor. The learned RIP entry is aged out if no further update for that service is received within the age-out timeframe.

MaxResrcRteNmbr

Syntax

```
SETDefault -NRIP MaxResrcRteNmbr = <max resource route number>
SHow -NRIP MaxResrcRteNmbr
SHowDefault -NRIP MaxResrcRteNmbr
```

Default 0 (no limit on the number of route numbers)

Description The MaxResrcRteNmbr parameter provides a soft reset to IPX to free all the memory in the Patricial Tree. IPX routing tables are stored in the Patricial Tree and large numbers of routing tables can use up available memory.

Using this parameter, you set the maximum number of route resources to be stored in the Patricial Tree. When the maximum number is reached, the Patricial Tree is deleted and all the routes stored are removed, freeing up the memory and resetting IPX. 3Com recommends that the maximum resource route number be set to twice the normal routing table size. For example, if the regular routing table size is 3,000, set the maximum resource route number to 6,000.

PolicyControl

Syntax

```
SETDefault !<port> -NRIP PolicyControl = ([AdvPolicy |
  NoAdvPolicy], [RcvPolicy | NoRcvPolicy], [PolicyOverride |
  NoPolicyOverride], [AdvToNbr | NoAdvToNbr], [RcvFromNbr |
  NoRcvFromNbr])
SHow [!<port> | !*] -NRIP PolicyControl
SHowDefault [!<port> | !*] -NRIP PolicyControl
```

Default All policies are disabled.

Description The PolicyControl parameter enables and disables the use of policy parameters, such as AdvertisePolicy and ReceivePolicy. If a policy is enabled and the corresponding policy list is empty, the policy is still applied. For example, if RcvPolicy is selected and the RcvPolicy list for routes is empty, then no routes are accepted. Similarly, if RcvFromNbr is selected and the RcvFromNbr list is empty, then none of the NRIP updates from any neighbor are accepted.

To enable policies Use the SETDefault command. To display the current policies configured for the router use the SHow command.

RcvFromNeighbor

Syntax

```
ADD !<port> -NRIP RcvFromNeighbor <list of MAC addresses>
DELete !<port> -NRIP RcvFromNeighbor ALL | <list of MAC addresses>
SHow [!<port> | !*] -NRIP RcvFromNeighbor
SHowDefault [!<port> | !*] -NRIP RcvFromNeighbor
```

Default No default (no neighbors configured from which to receive advertisements)

Description The RcvFromNeighbor parameter defines the neighbors (next hop routers) from which NRIP advertisements will be accepted on the specified interface.

The lists of neighbors can be entered as part of one command. For example:

```
<list of MAC addresses>, <list of MAC addresses>, <list of MAC
  addresses>
```

Use a tilde (~) before the neighbor specification to exclude it from the list of neighbors. When you use ~ for one neighbor specification, it must be used for all. If exclusion lists are mixed with inclusion lists, an error message is issued. When you must change a list from one type (inclusion or exclusion) to the other, the current list must first be deleted before the new list can be added. For more information, refer to “Configuring Other Policy Settings” on page 13-26 in *Using NETBuilder Family Software*.

Values

<list of MAC addresses>	The 48-bit media access control (MAC) address of the host. The MAC address must be entered in the same format (canonical or noncanonical) as used by the host. For example:
	`[%]<48-bit MAC address in native format> |`
	`Mac <48-bit MAC address in canonical format> |`
	`NcMac <48-bit MAC address in noncanonical format>`

ReceivePolicy

Syntax

```
ADD !<port> -NRIP ReceivePolicy [~]{<route> | Default},
  [<list of routes>]
DELete !<port> -NRIP ReceivePolicy {All | Default |
  <list of routes>}
SHow [!<port> | !*] -NRIP ReceivePolicy
SHowDefault [!<port> | !*] -NRIP ReceivePolicy
```

Default No default (no route receive policies defined)

Description

The ReceivePolicy parameter specifies which routes reported in the routing updates by adjacent routers are accepted on the specified interface and cached in the local routing tables. The ReceivePolicy parameter is specified per port.

To accept only specific routes reported in adjacent routers' routing updates, use the ADD command to add a list of routes 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 port's receive list can contain only normal or inverse routes. If an inverse route exists in a port's receive list and you want to change that route to a normal route, use the DELete command to remove all of the existing routes in that port's advertise list. Follow the same procedure to change a normal route or an inverse route.

To remove a route 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 port's receive list. If a port number is specified, the receive lists for the specified port are displayed. If a port number is not specified, all existing receive lists are displayed. Inverse routes are indicated by a tilde (~) prefix.

Values

Default The keyword Default specifies that default routes reported in the routing updates by adjacent routers are accepted on the specified interface and cached in the local routing table.

<list of routes> This specification can be either a single IPX network number or a range of IPX network numbers separated by a hyphen, inclusive of the low and high ends of the range. For example:

```
<route>:=<net number> | <net range>
<net range>:=<net number>– <net number>
<net number>:= [&]<32-bit hex number>(1-FFFFFFFD)
```

Example 1

To set up a policy where routes in the range 10 through 100 are accepted on interface 1, enter:

```
ADD !1 -NRIP ReceivePolicy &10 - &100
```

Example 2

To set up a policy where routes (in addition to those routes in the previous example) to network 200 are accepted on port 1, enter:

```
ADD !1 -NRIP ReceivePolicy &200
```

Example 3

To delete all the route acceptance policies configured for port 1, enter:

```
DELete !1 -NRIP ReceivePolicy All
```

Example 4

To set up an exclusion list where all routes except those to networks 10, 20, and 30 are accepted on port 3, enter:

```
ADD !3 -NRIP ReceivePolicy ~&10, ~&20, ~&30
```

UpdateTime

Syntax

```
SETDefault !<port> -NRIP UpdateTime = <seconds> (10–65535)
SHow [!<port> | !*] -NRIP UpdateTime
SHowDefault [!<port> | !*] -NRIP UpdateTime
```

Default 60

Description The UpdateTime parameter specifies how often the router sends NRIP regular updates to the specified port to exchange routing information (in seconds). Permissible values range from 10 to 65,535 seconds, but UpdateTime must be synchronized with other routers and server update time value. Novell servers also use a default of 60 seconds.

To display the current value for this parameter use the SHow command.

40 OSIAPPL SERVICE PARAMETERS

This chapter describes the parameters in the Open System Interconnection Applications (OSIAPPL) Service. Table 40-1 lists the OSIAPPL Service parameters and commands.

Table 40-1 OSIAPPL Service Parameters and Commands

Parameters	Commands
CONFiguration	SHow
CONNections	SHow
DSAAddress	SETDefault, SHow
DSAType	SETDefault, SHow
DuaState	SHow
NAme	ADD, DELete, SHow
NameSourceOrder	SETDefault, SHow
UnbindTimer	SETDefault, SHow
VtpDataConcat	SETDefault, SHow

CONFiguration

Syntax

```
SHow -OSIAPPL CONFiguration
```

Default No default

Description The CONFiguration parameter displays the values of the OSIAPPL parameters.

CONNections

Syntax

```
SHow -OSIAPPL CONNections
```

Default No default

Description The CONNections parameter displays information regarding the Open Systems Interconnection (OSI) connections present in the gateway. The following information is displayed:

ID — The connection identifier.

I/A — The gateway is either the initiator (I) or the acceptor (A) of the connection.

Elapsed Time — The length of time the connection has been established in day:hour:minute:second (day:hr:min:sec) format.

PSAP address — The presentation service access point (PSAP) addresses of the caller and the called destination, respectively.

DSAAddress

Syntax

```
SETDefault -OSIAPPL DSAAddress = [<PSAP address> | <name> | None]
SHow -OSIAPPL DSAAddress
```

Default None

Description The DSAAddress parameter sets the Directory System Agent (DSA) address or name.

Values

PSAP address	The PSAP of the DSA address contains the network service access point (NSAP) address and a full set of (N)-selector values: T-selector, S-selector, and P-selector. For more information on PSAP and NSAP addressing, refer to Appendix E in *Using NETBuilder Family Software*.
<name>	This value specifies a name to be resolved to the PSAP address of a DSA. The name and its corresponding PSAP address must first be added using the ADD -OSIAPPL NAme command. For information on how to assign a logical name to a physical address, refer to "NAme" in this chapter. Restrictions on the name value are also explained.
None	No DSA address or name has been specified.

DSAType

Syntax

```
SETDefault -OSIAPPL DSAType = [Standard | Quipu]
SHow -OSIAPPL DSAType
```

Default Quipu

Description The DSAType parameter specifies a vendor DSA. The DSA maintains a directory of names and their corresponding PSAP addresses, and handles directory access requests from users or other DSAs. 3Com supports the X.500 standards DSA and the ISODE (QUIPU) DSA.

Values

Standard	This value specifies the X.500 standards of the OSI Directory.
Quipu	This value specifies the ISODE public domain software of the OSI Directory.

DuaState

Syntax

```
SHow -OSIAPPL DuaState
```

Default No default

Description The DuaState parameter shows whether the gateway is disconnected or connected to a DSA, and the address of the DSA to which it is connected.

NAme

Syntax

```
ADD -OSIAPPL NAme <name> <PSAP address>
DELete -OSIAPPL NAme <name>
SHow -OSIAPPL NAme [<name>]
```

Default No default

Description The NAme parameter assigns a logical name to a physical address. The information is saved on the gateway diskette.

The SHow -OSIAPPL NAme command displays all file-based names. The SHow -OSIAPPL NAme command displays the PSAP address associated with the name.

If the name field on the command line does not meet the following conditions it is ignored:

- The length of the name must be no more than 14 characters.
- The name must start with a letter.
- Characters that can be used legitimately to succeed the first letter are a letter, a digit, or one of the following symbols: underscore (_), period (.), hyphen (-), or at (@). All other characters are ignored.

NameSourceOrder

Syntax

```
SETDefault -OSIAPPL NameSourceOrder = <name> [<name> ...] (From X.500,
  File)
SHow -OSIAPPL NameSourceOrder
```

Default X.500

Description The NameSourceOrder parameter indicates the order in which multiple name resolvers are queried in order to map names to addresses. The two name resolvers available at this time are X.500 and File.

If X.500 is selected, a computer that supports the X.500 protocol must be on the network so that names and addresses of network resources can be added, removed, or displayed from the gateway. If File is selected, the database is stored on the gateway diskette.

This parameter does not apply to the DirectoryManage command. The DirectoryManage command always uses X.500 as its name resolver, regardless of whether X.500 is a value of NameSourceOrder.

UnbindTimer

Syntax

```
SETDefault -OSIAPPL UnbindTimer = <minutes> (1–1440)
SHow -OSIAPPL UnbindTimer
```

Default 1440

Description The UnbindTimer parameter indicates how long a Directory User Agent (DUA) connection remains idle before it is aborted. The time limit ranges from 1 minute to 1440 minutes (24 hours).

VtpDataConcat

Syntax

```
SETDefault -OSIAPPL VtpDataConcat = [OFF | ON]
SHow -OSIAPPL VtpDataConcat
```

Default OFF

Description The VtpDataConcat parameter concatenates outgoing deliver protocol data units (PDUs) to the data PDUs when set to ON. By concatenating the PDUs, less traffic occurs on the network.

41

OSPF Service Parameters

This chapter discusses the Open Shortest Path First (OSPF) Service parameters. The OSPF Service is related to the ARP, BGP, IP, RIPIP, and TCP Services. Table 41-1 lists the OSPF Service parameters and commands.

Table 41-1 OSPF Service Parameters and Commands

Parameters	Commands
AreaId	SETDefault, SHow
AreaRanges	ADD, DELete, SHow
CONFiguration	SHow
CONTrol	SETDefault, SHow
Cost	SETDefault, SHow
DEBUG	SET, SHow
DefaultMetric	SETDefault, SHow
Delay	SETDefault, SHow
DemandInterface	SETDefault, SHow, SHowDefault
DirectPolicy	SETDefault, SHow
ExteriorPolicy	ADD, DELete, SHow
HelloTime	SETDefault, SHow
InterfaceStatus	SHow
InteriorPolicy	ADD, DELete, SHow
LinkStateData	SHow
Neighbor	ADD, DELete, SHow
NeighborStatus	SHow
PassWord	SETDefault, SHow
ReceivePolicy	ADD, DELete, SHow
RetransmitTime	SETDefault, SHow
RouterDeadTime	SETDefault, SHow
RouterID	SETDefault, SHow
ROUTerPriority	SETDefault, SHow
SPFHolddown	SETDefault, SHow
StaticPolicy	ADD, DELete, SHow
StubDefaultMetric	SETDefault, SHow
VirtualLink	ADD, DELete, SHow

AreaId

Syntax

```
SETDefault !<port> -OSPF AreaId = <n.n.n.n> [Transit | Stub]
SHow [!<port> | !*] -OSPF AreaId
```

Default 0.0.0.0

Description The AreaId parameter configures an area ID for a specified port. If all ports on the router are configured with the same area ID, the router acts as an intra-area OSPF router only. If different area IDs are used on different ports, the router acts as an area border router (ABR). Specify the area D in dotted decimal format, such as 0.0.0.0.

To display the area ID assigned to a particular port, use:

```
SHow !<port> -OSPF AreaId
```

To display the area ID for all ports, use:

```
SHow -OSPF AreaId
```

You must use area ID 0.0.0.0 only for interfaces that are attached to the backbone network.

Values

<n.n.n.n>	Specify an AreaId value between 0.0.0.0 and 255.255.255.255.
Transit	Floods external link state advertisements into the area. This is the default value.
Stub	Does not flood external link state advertisements into the area. This value cannot be configured when area ID is 0.0.0.0.

AreaRanges

Syntax

```
ADD -OSPF AreaRanges <areaID> <IP address> <mask> [Advertise |
  DontAdvertise]
DELete -OSPF AreaRanges <areaID> <IP address>
SHow -OSPF AreaRanges
```

Default No default (area range table is empty)

Description The AreaRanges parameter reduces the routing table size and link state database size of OSPF domains. It is useful in a large routing domain, where route aggregation from each area can reduce the routing information in the backbone, and subsequently in all areas. This parameter is effective only on an ABR. An ABR is a router with interfaces into multiple areas. A maximum of 31 entries are allowed in the AreaRanges Table.

Values

<areaID>	Identifies the source OSPF area to which the <IPaddress> and <mask> are applied to perform route aggregation. More than one set of IP addresses and masks can be associated with each area.
<IPaddress> <mask>	Describes a range of IP addresses. For example, 10.0.0.0 255.0.0.0 describes the 10.0.0.0 to 10.255.255.255 address range.

Many network/subnet/host routes fall within the same <IPaddress> <mask> pair, and all these routes are aggregated into a single summary LSA. Routes that do not fall into any <IPaddress> <mask> pair are advertised individually.

A particular network can fall into multiple <IPaddress> <mask> ranges. In this case, the most specific match (highest mask value) is chosen. The address range 0.0.0.0 0.0.0.0 has the lowest priority.

Advertise — Advertises the aggregate.

DontAdvertise — Suppresses the summary link state advertisement (LSA). Use this option to intentionally hide some networks from other networks within an area.

CONFiguration

Syntax

```
SHow [!<port> | !*] -OSPF CONFiguration
```

Default No default

Description The CONFiguration parameter displays values for all OSPF-related parameters. If you do not specify a port, parameter values for all ports as well as global OSPF parameters are shown.

CONTrol

Syntax

```
SETDefault !<port> -OSPF CONTrol = ([Enable | Disable], [DynamicNbr |
  NoDynamicNbr], [NonMesh | FullMesh])
SHow [!<port> | !*] -OSPF CONTrol
```

Default Disable, DynamicNbr, NonMesh

Description The CONTrol parameter enables or disables OSPF routing for a specified port. The NonMesh | FullMesh option supports the point-to-multipoint interface. Neighbor learning is enabled by default on nonbroadcast multi-access (NBMA) interfaces, which means that neighbor lists are automatically created and OSPF operates correctly without static neighbor information. Neighbor learning can be disabled (NoDynamicNbr) for security reasons so that only those statically configured neighbors are trusted.

OSPF runs only when IP routing is enabled. OSPF only advertises directly connected networks when it is enabled for direct networks and an IP address has been configured.

To display the CONTrol parameter value for a particular port, use the SHow command. If no port number is specified, the CONTrol parameter value is shown for all ports that have been configured with an IP network number.

Values Enable | Disable — If OSPF is enabled on a port, the router attempts to become adjacent with other OSPF routers on the network. If CONTrol is disabled, the port is not considered to be part of any configured area.

DynamicNbr | NoDynamicNbr — Determines how OSPF Frame Relay, X.25, and ATM neighbor lists get created. If DynamicNbr is selected, the router exchanges information with all routers whose NBMA address is known and stored in the IP address table. If NoDynamicNbr is selected, a router exchanges routing information with manually configured neighbors.

NonMesh | FullMesh — Determines whether a designated router (DR) can be elected for an NBMA interface. This option applies only to Frame Relay, X.25, and ATM ports. If you set this option for a port other than a Frame Relay, X.25, or ATM port, for example, an Ethernet port, the setting does not take effect.

All neighboring routers must be configured with the same mode: FullMesh or NonMesh.

NonMesh causes the OSPF router to attempt to establish a point-to-point adjacency with each neighbor through the specified port.

FullMesh causes a designated router to be selected from among the attached routers. All of the neighboring routers must be fully connected with each other with a mesh of virtual circuits.

For correct operation, all routers on the Frame Relay, X.25, or ATM network must be consistently configured.

Cost

Syntax

```
SETDefault !<port> -OSPF Cost = <1–65535> | Default | Infinity
SHow [!<port> | !*] -OSPF Cost
```

Default

100,000,000 / media baud rate
For example, Ethernet is 100,000,000 / 10,000,000 = 10.
For ATM, the default cost is 1.

Description

The Cost parameter sets the cost for a specified port. The cost is an administrative metric assigned to a network. You can specify a cost between 1 and 65,535.

To display the Cost parameter value for a particular port, use the SHow command. If you do not specify a port, the cost for all ports that have been configured with an IP network number is displayed.

Values

<1–65535> — Specify a cost between 1 and 65,535.

Default — Causes the software to automatically compute the value based on the media baud rate. The formula used is as follows:

cost = 100,000/baud rate (bits per second)

Infinity — When specified and OSPF is the only routing protocol used on the network, the network is not used for data traffic.

DEBUG

Syntax

```
SET -OSPF DEBUG = All | None | [~] (IO | State | Error | Timer |
 SPT)
SHow -OSPF DEBUG
```

Default

None

Description The DEBUG parameter enables different levels of OSPF tracing. If tracing is enabled, flags appear on the local console depending on what level of tracing you select. If there is no local console attached to the RS-232 port, the DEBUG parameter should be set to None so that tracing is not performed.

Values

All — All flags are turned on.

None — No tracing is performed. Nothing is logged.

~ — Used in combination with another option to disable logging for that option. For example, if you enter SET -OSPF DEBUG All and then enter SET -OSPF DEBUG ~Error, all levels of tracing are performed except Errors.

IO — Logs packets transmitted and received.

State — Logs interface and neighbor finite state machine events.

Error — Logs all abnormal errors.

Timer — Logs expirations of OSPF-related timers.

SPT — Logs shortest path tree (SPT) calculations, such as nodes added to the SPT and networks added to routing tables.

DefaultMetric

Syntax

```
SETDefault -OSPF DefaultMetric = [Disable | <metric> (1–65535)
 [Type1 | Type2]]
SHow -OSPF DefaultMetric
```

Default Disable

Description The DefaultMetric parameter sets the cost for a default route. If any value other than Disable is specified, the router generates an external LSA for network 0.0.0.0. This information is propagated throughout the routing domain.

Network 0.0.0.0 is advertised with a metric type of "what is configured."

Values

Disable — Disables the DefaultMetric parameter.

<metric> — Specifies the metric value between 1 through 65,535.

Type1 — An external metric that is the sum of the external metric and the link state metric. Type1 metric is the preferred over Type2 and should be used if the cost to reach the Autonomous System Boundary Router (ASBR) is the criterion used to measure distance. The default route is advertised with a Type1 metric.

Type2 — The configured metric is used as the sole criterion in determining the cost for using the default route.

Delay

Syntax

```
SETDefault !<port> -OSPF Delay = <seconds><1–65,535>
SHow [!<port> | !*] -OSPF Delay
```

Default 1

Description The Delay parameter specifies the delay time (in seconds) for a specified port. The value for the Delay parameter is added to all LSAs that are originated and sent over the given network. This allows an LSA to be aged manually when being transmitted over slow media. Set the Delay parameter value accordingly for different speed links.

To display the Delay parameter value for a specified port, use the SHow command. If you do not specify a port number, the Delay parameter value is shown for all ports that have been configured with an IP network number.

DemandInterface

Syntax

```
SETDefault !<port> -OSPF DemandInterface = Passive | Enable
SHow [!<port> | !*] -OSPF DemandInterface
SHowDefault [!<port> | !*] -OSPF DemandInterface
```

Default Passive

Description The DemandInterface parameter determines whether to treat the interface as a demand circuit. A demand circuit is characterized as a point-to-point or point-to-multipoint link, such as an Integrated Services Digital Network (ISDN) circuit, an X.25 switched virtual circuit (SVC) or Frame Relay SVC neighbor, or a dial-up line.

A demand circuit allows OSPF to operate more efficiently by saving bandwidth and reducing cost. When there are no network topology changes, OSPF hello packets and routing-refresh information are suppressed, which allows the data link connection to be closed when not carrying application traffic.

Use the SETDefault command to enable the demand interface. Use the SHowDefault command to display the configured value and SHow command to display the run-time value of this parameter.

⚠ **CAUTION:** *Do not configure any interface on any router in a single OSPF area as a demand circuit (DC) interface unless all routers in that area have been upgraded to at least software version 8.3. Non-DC-aware routers become confused by link state advertisements (LSAs) using the DoNotAge bit in the link state age field. The LSA appears to expire and those routers are constantly flushing the LSA from their link state database and rerunning the Dijkstra algorithm, as well as informing all the routers they have adjacencies with of the routing changes. This affects every router in an area that cannot understand DC-style LSAs.*

Values

Passive	OSPF treats the interface as a regular circuit until the neighbor is willing to treat the point-to-point link as a demand circuit.
Enable	OSPF treats the interface as a demand circuit and tries to negotiate with the neighbor at the other end to suppress hello packets if the link is a point-to-point link.

The following values can be displayed with the SHow command:

True	OSPF currently treats the specified interface as a demand circuit. Hellos may be suppressed if the link is a point-to-point link.
False	OSPF currently treats the specified interface as a regular circuit, not a demand circuit, and periodically sends hello packets and refreshes link state advertisements.

DirectPolicy

Syntax

```
SETDefault !<port> -OSPF DirectPolicy = ([Advertise |
 DontAdvertise], [Type1 | Type2])
SHow [!<port>] -OSPF DirectPolicy
```

Default DontAdvertise, Type1

Description The DirectPolicy parameter determines whether the networks (on the port) should be advertised into the OSPF domain or not. This parameter applies to directly attached networks of the router. It can be configured independently for each port. If you select “Advertise” , you can specify if the network should be advertised as Type1 or Type2 OSPF external routes.

For security reasons, you may not want to advertise a local network into the OSPF domain. This is accomplished by disabling OSPF on the port, and selecting DontAdvertise option for this parameter.

You sometimes may not want to run OSPF on a port, but still want to advertise it to other OSPF routers. For example, turning off OSPF on a system running Boundary Routing software on a WAN port can save line bandwidth. This is accomplished by selecting the Advertise option.

The DirectPolicy parameter is useful only on ports where -OSPF CONTrol is disabled. If OSPF is enabled, the network is always advertised. The metric of the advertisement can be adjusted by the -OSPF Cost parameter.

ExteriorPolicy

Syntax

```
ADD -OSPF ExteriorPolicy All | None | [~]<IP address> <metric>
 [Type1 | Type2]
DELete -OSPF ExteriorPolicy All | <IP address>
SHow -OSPF ExteriorPolicy
```

Default None

Description The ExteriorPolicy parameter adds an IP network number to an exterior routing protocol policy list. The list is used to cross-check with routes learned from other exterior routing protocols such as Border Gateway Protocol (BGP). If routes are reachable, they are further advertised into the OSPF domain.

DELete removes either a single IP address or all addresses from the policy list.

Values

All	Specifies that all routes are advertised by OSPF. When used with the DELete command, All removes all addresses from the policy list. No exterior routes are advertised.
None	Does not advertise routes by OSPF when used with the ADD command.
~	Advertises all addresses except for the ones on the policy list.
<IP address>	Specifies an IP network number, a subnet number, or a host address.
<metric>	Specifies the advertised cost of the route. If set to 0, the metric in the routing table is used.
Type1	Indicates a metric comparable to the link state metric.
Type2	Indicates the external metric.

Example 1 To add IP network number 129.213.0.0 to the policy list, enter:

```
ADD -OSPF ExteriorPolicy 129.213.0.0
```

OSPF reports this network only if it was learned through BGP. The configured metric (in this case 0) indicates that the metric in the routing table should be used and be reported with a metric type of Type1. This enables receivers of this LSA to use the advertised cost and the link state cost (to reach this system) as the metric value stored in the routing table.

Example 2 To add 128.1.0.0 to the list to be advertised with metric 1 and metric Type2, enter:

```
ADD -OSPF ExteriorPolicy 128.1.0.0 1 Type2
```

HelloTime

Syntax

```
SETDefault !<port> -OSPF HelloTime = <seconds> (1–65,535)
SHow [!<port> | !*] -OSPF HelloTime
```

Default 10

Description The HelloTime parameter sets the interval (in seconds) at which the router sends hello packets on the given network. Hello packets are sent to neighbor routers to maintain adjacencies.

Set the HelloTime parameter to the same value for all routers on the same network.

The HelloTime parameter works together with the RouterDeadTime parameter. If a router does not send a hello message for a period of time specified by the RouterDeadTime parameter, the router is considered down. If you reconfigure the value of the HelloTime parameter, be sure to check the value of the RouterDeadTime parameter. The value of the RouterDeadTime parameter should be a greater multiple of the value of the HelloTime parameter. For example, if the value of the HelloTime parameter is 15 seconds, then the value of the RouterDeadTime parameter should be approximately 45 seconds. For more information on this parameter, refer to “RouterDeadTime” on page 41-14.

To display the HelloTime value for a particular port, use the SHow command. If you do not specify a port, the HelloTime values for all ports that have been configured with an IP network number are displayed.

InterfaceStatus

Syntax

```
SHow [!<port> | !*] -OSPF InterfaceStatus
```

Default No default

Description The InterfaceStatus parameter displays the status of a specified interface that is running OSPF. If no port number is specified, the status for all ports is displayed.

Example The following is a sample screen display generated by the SHow -OSPF InterfaceStatus command.

```
-------------------------OSPF Interface Status---------------------
Interface Address   Port  State    Area ID  DR             BDR
1.0.0.1             2     DRother  0.0.0.0  1.0.0.2        1.0.0.3
129.213.112.254     2     DR       0.0.0.1  129.213.32.1   129.213.32.9
```

Possible interface states are as follows:

Down The interface is not operational. This router enters this state if the lower layers indicate that the interface is not operational or an IP address for the interface is not configured or is incorrectly configured.

Loopback Indicates either hardware or software loopback, which causes the router to advertise this link as a host route that includes its own IP address.

Waiting The interface is waiting to recognize the designated router (DR) and backup designated router (BDR).

PTP The interface has been determined to be a point-to-point link. This applies to serial interfaces as well as virtual links.

DRother Indicates that the router is neither DR nor BDR for the interface.

Backup Indicates that the router has been elected as BDR for the interface.

DR Indicates that the router has been elected DR for the interface.

InteriorPolicy

Syntax

```
ADD -OSPF InteriorPolicy All | None | [~]<IP address> <metric>
 [Type1 | Type2]
DELete -OSPF InteriorPolicy All | <IP address>
SHow -OSPF InteriorPolicy
```

Default None

Description The InteriorPolicy parameter adds an IP network number to an interior routing protocol policy list. The list is used to cross-check routes from other interior routing protocols such as Routing Information Protocol (RIP) or Integrated Integrated System-to-Integrated System (IS-IS). If the routes are reachable, they are further advertised into the OSPF domain.

The DELete command removes either a single IP address or all addresses from the policy list. If you delete all addresses from the list, no interior routes are advertised.

Values All OSPF advertises all RIP or Integrated IS-IS learned routes. When used with the DELete command, All removes all addresses from the policy list, and no interior routes are advertised.

None No RIP or integrated IS-IS learned routes are advertised.

~ Advertises all addresses except for the ones on the policy list.

<IP address> Can be an IP network number, a subnet number, or a host address.

<metric> The advertised cost of the route. If set to 0, the metric in the routing table is used.

Type1	Indicates a metric comparable to the link state metric.
Type2	Indicates the external metric. The specified addresses are advertised only if they exist in the routing table.

Example To add IP network number 129.213.0.0 with 0 metric to the interior routing protocol policy list, which is then advertised into the OSPF routing domain, enter:

```
ADD -OSPF InteriorPolicy 129.213.0.0 0
```

OSPF reports this network only if it was learned through RIP or Integrated IS-IS.

LinkStateData

Syntax

```
SHow -OSPF LinkStateData [AreaId] [Router | Network | Summary |
  External | Long | Title <LS Id>]
```

Default No default

Description The LinkStateData parameter displays the link state database for a particular area. If you do not specify an area ID, information for all areas is displayed, including external LSAs.

The SHow LinkStateData command values determine the type of display that is generated.

Values

AreaId	Specifies the area ID and display the link state database.
Router	Displays only router link state advertisements.
Network	Displays only network link state advertisements.
Summary	Displays only summary link state advertisements.
External	Displays only AS external link state advertisements.
Long	Displays the long form, including the LSA body and link state header.
Title	Displays a summary of the link state database. This display includes general information, such as the size and database checksum. Individual entries in the database are not displayed.
<LS Id>	Displays LSA with specified link state IDs. This value can be entered as a hexadecimal value to locate a router ID or in dotted decimal format to locate a network, summary, or external LSA.

If display options are used in combination, they should be separated by spaces.

When displaying an LSA, the true age value may begin with “DNAg+,” which means Do Not Age, if the circuit is a demand circuit. The checksum sum of the link state database may not be same between routers across demand circuits.

Neighbor

Syntax

```
ADD !<port> -OSPF Neighbor All | <IP address>
DELete !<port> -OSPF Neighbor All | <IP address>
SHow [!<port> | !*] -OSPF Neighbor
```

Default All

Description Neighbor adds or deletes a neighbor address to or from the neighbor list for a specified port. Neighbors that are dynamically learned, but not configured statically, cannot be deleted using the user interface or SNMP. If an attempt is made through the user interface to delete a dynamic neighbor, an error message is displayed giving the reason why the command failed.

If an OSPF neighbor whose NBMA address exists in the IP address table is statically added, it is treated as a static neighbor. If this neighbor is deleted using the user interface or SNMP, it may still be in the neighbor list as long as neighbor learning is enabled and its address mapping entry exists.

OSPF neighbors are useful in the following circumstances:

- If you want only an acceptable set of routers to run OSPF; for example, if you do not want to run OSPF with routers from another organization.
- If the underlying network does not support multicast addressing.

The value All indicates that multicasting will be used for the port, if possible.

Use SHow to display the current list of neighbors for a specified port. If you do not specify a port number, the neighbor list is displayed for all ports that have been configured with an IP network number.

Values

All When used with the ADD command, All initiates multicast addressing if the network is multiaccess and supports broadcast addressing. When used with the DELete command, all neighbors are removed from the neighbor list, and multicasting goes into effect. For NBMA interfaces, All means all dynamic neighbors.

<IP address> Specifies a particular address to be added to or deleted from the neighbor list. If specific neighbor addresses are configured, all OSPF packets are unicast directly to those neighbors. Those neighbors should be configured with a neighbor list that includes this router.

DynamicNbr Only for NBMA interfaces. When static neighbors are configured, and DynamicNbr is enabled, DynamicNbr is displayed after the IP addresses of all the configured neighbors that are dynamically learned.

None Only for NBMA interfaces. None is displayed if no static neighbors are configured and DynamicNbr is disabled.

NeighborStatus

Syntax `SHow [!<port> | !*] -OSPF NeighborStatus`

Default No default

Description The NeighborStatus parameter shows the status of directly connected neighbor adjacencies for a specified port. If neighbor learning is enabled (-OSPF CONTrol = DynamicNbr), the output of this parameter may include neighbors statically configured or dynamically learned. Static neighbors are distinguished in a display by an asterisk (*). If you do not specify a port, all neighbors on all ports are displayed.

Example To display neighbors for port 1, enter:

```
SHow !1 -OSPF NeighborStatus
```

A display similar to the following appears:

```
-------------------------OSPF NeighborStatus-------------------------
Neighbor Address  Router ID   State     Priority Rxmit Q  Sum Q  Req Q
129.213.16.22     0x02001122  Full      10       0        0      0      (DR)
129.213.16.21     0x02001121  Full      10       1        0      0      (BDR)
129.213.16.44     0x02001120  Exchange  1        0        20     0
```

The following list explains the possible states for OSPF neighbors:

Down The neighbor is declared down because the directly connected network has gone down or because a hello packet was not received before the router dead time expired.

Init A hello packet is received, but the router has not indicated its reception of that hello packet.

Attempt An adjacency is attempting to be established, and a hello packet is sent.

ExStart Two neighbors have decided to become fully adjacent and are negotiating to determine how the database exchange process will operate.

Exchange The neighbor is in database exchange state. Each neighbor describes what is in its link state database.

Loading Database exchange process is complete. Updated link state database downloading is occurring.

2Way Two-way communication exists between the system and the neighbor. Two routers that are neither designated routers nor backup designated routers are always in 2Way state with each other.

Full Two-way communication exists, and the routers have synchronized their databases. The DR and BDR are fully adjacent with all routers.

The following list explains the other columns in the display:

Priority Used for electing the DR and BDR.

Rxmit Q The number of unacknowledged LSAs in the retransmission queue for a particular neighbor. All LSAs must be acknowledged by the receiving neighbor.

Sum Q Number of unacknowledged LSAs in the summary queue. The summary queue is used during exchange state to describe a router's database.

Req Q Number of LSAs on the request list. The request list is created once the exchange process is complete and it is determined that the neighbor has more recent link state information.

In order for routers to become neighbors, the HelloTime, RouterDeadTime, and PassWord parameters for all routers must be identically set.

PassWord

Syntax

```
SETDefault !<port> -OSPF PassWord = None | “<password>”
SHow !<port> -OSFP PassWord
```

Default None

Description The PassWord parameter sets a password for a particular port. The password is used for security purposes. To maintain security, the password is not displayed.

Each router on a particular network must have the same password or no adjacencies form.

If you enter the SHow -OSPF PassWord command, the following message is displayed:

```
Password cannot be shown
```

ReceivePolicy

Syntax

```
ADD -OSPF ReceivePolicy All | None | [~]<IP address> [<metric>]
DELete -OSPF ReceivePolicy All | <IP address>
SHow -OSPF ReceivePolicy
```

Default All

Description The ReceivePolicy parameter adds IP addresses to a policy list. A policy list filters routes learned from external LSA packets. This parameter does not affect the protocol handling of external LSAs. All external LSAs are received, stored, and further flooded as appropriate. Only qualified external LSAs are accepted in the routing table.

Values

All	Accepts all external LSAs in the local routing table. When used with the DELete command, All removes all addresses from the policy list. All routes received from LSAs are stored in the routing table.
None	Does not accept external LSAs in the local routing table.
~	All addresses except for the ones on the policy list are accepted in a local routing table.
<IP address>	Specifies an IP network number, a subnet, or a host address.
<metric>	Specifies the value stored as the metric in the routing table. If set to 0, the metric from the route is stored in the routing table.

RetransmitTime

Syntax

```
SETDefault !<port> -OSPF RetransmitTime = <seconds> (1–65,535)
SHow [!<port> | !*] -OSPF RetransmitTime
```

Default 5

Description The RetransmitTime parameter specifies a time interval (in seconds) between LSA transmissions.

If you do not specify a port number in the SHow -OSPF RetransmitTime command, the RetransmitTime parameter value for all ports that have been configured with an IP network number is shown.

RouterDeadTime

Syntax

```
SETDefault !<port> -OSPF RouterDeadTime = <seconds> (1–65,535)
SHow [!<port> | !*] -OSPF RouterDeadTime
```

Default 40

Description The RouterDeadTime parameter specifies a time interval (in seconds) that is used for determining when a router is down. Each time a hello packet is received from a neighbor, the RouterDeadTime interval for that router is reset.

The RouterDeadTime value should be the same for all routers on the same network.

The RouterDeadTime parameter works together with the HelloTime parameter; that is, if a router does not send a hello message for a period of time specified by the RouterDeadTime parameter, the router is considered down. If you reconfigure the value of the RouterDeadTime parameter, make certain that you check the value of the HelloTime parameter. The value of the RouterDeadTime parameter should be a greater multiple of the value of the HelloTime parameter. For example, if the value of the HelloTime parameter is 15 seconds, then the value of the RouterDeadTime parameter should be approximately 45 seconds. For more information on this parameter, refer to "HelloTime" on page 41-8.

To display the RouterDeadTime parameter value for a particular port, use the SHow command. If you do not specify a port, the RouterDeadTime value for all ports configured with an IP network number is displayed.

RouterID

Syntax

```
SETDefault -OSPF RouterID = Default | !<port> | <IP address>
SHow -OSPF RouterID
```

Default Default

Description The RouterID parameter specifies the router ID to be used by OSPF. The router ID must be unique throughout the OSPF domain to ensure correct operation of the routing protocol.

For this parameter to take effect, OSPF must be shut down and restarted.

Values

Default	OSPF uses the lower 4 bytes of the CEC MAC address (for the NETBuilder II platform) or the MAC address of the first LAN interface (SuperStack II NETBuilder platform) as its router ID. The Default value represents the behavior of all previous versions of software.
!<port>	OSPF uses the IP address on the specified port to be its router ID. If no IP address is configured on the port, OSPF uses the CEC MAC address
<IP address>	OSPF uses the value you specify for the router ID. You can specify an IP address of one of the router's ports or any convenient value.

ROUTerPriority

Syntax

```
SETDefault !<port> -OSPF ROUTerPriority = <number> (0–255)
SHow [!<port> | !*] -OSPF ROUTerPriority
```

Default 1

Description The ROUTerPriority parameter sets the priority for the router on the specified port. The ROUTerPriority value is used to elect a designated router (DR) for the multiaccess network.

If a router is assigned the priority value of 0, it is not eligible to become the designated router for that network, but can become the backup designated router (BDR) for the network.

If the value of the ROUTerPriority parameter is greater than the current designated router DR value, the router attempts to assert itself as DR for the network. If the value is lower than the current DR value and the router is not the DR, no action is taken.

To display the ROUTerPriority parameter value for a specified port, use the SHow command. If you do not specify a port number, the ROUTerPriority parameter value for all ports configured with an IP network number is shown.

SPFHolddown

Syntax

```
SETDefault -OSPF SPFHolddown = <seconds> (0-60)
SHow -OSPF SPFHolddown
```

Default 5

Description The SPFHolddown parameter prevents continuous OSPF computations from using up the available CPU time. This parameter limits computations to one per the SPFHolddown time value.

Setting SPFHolddown to a lower number allows instant reaction to network topology changes. Setting it to a higher number conserves CPU usage. Higher values tend to stabilize the network by slowing down topology changes.

To display the SPFHolddown parameter value, use the SHow command.

StaticPolicy

Syntax

```
ADD -OSPF StaticPolicy All | None | [~]<IP address> <metric>
 [Type1 | Type2]
DELete -OSPF StaticPolicy All | <IP address>
SHow -OSPF StaticPolicy
```

Default None

Description The StaticPolicy parameter adds an IP network number to a policy list of static configured routes. The list is used to cross-check locally configured static routes. If the routes are available, they are further advertised into the OSPF domain.

Values

	All	OSPF advertises all static routes. When used with the DELete command, All removes all addresses from the policy list. No static routes are advertised.
	None	No static routes are advertised by OSPF.
	~	Advertises all addresses except for the ones in the policy list.
	<IP address>	Specifies an IP network number, a subnet number, or a host address.
	<metric>	The advertised cost of the route. If set to 0, the metric in the routing table is used.
	Type1	Indicates a metric comparable to the link state metric.
	Type2	Indicates the external metric. The specified addresses are advertised only if they exist in the routing table.

StubDefaultMetric

Syntax

```
SETDefault -OSPF StubDefaultMetric = [Disable | <metric>
 (1–65535)]
SHow -OSPF StubDefaultMetric
```

Default 1

Description The StubDefaultMetric parameter specifies whether or not the router should generate the default route (to IP destination 0.0.0.0) into the stub areas. This parameter applies if the router is configured as an ABR with interfaces into different areas (some of which are stub areas). If a default route is generated into a stub area, the route does not generate summary LSAs in the stub area, significantly reducing the link state database size in the stub area. This parameter applies only to stub areas.

Values

Disable	The router does not generate the default route into stub areas.
<metric>	The router generates the default route into the stub areas with the cost (metric) you specify. Enter a value between 1 and 65,535.

VirtualLink

Syntax

```
ADD !<port> -OSPF VirtualLink None | <router id> [<rxmit
 interval>]
DELete !<port> -OSPF VirtualLink All | None | <router id>
SHow [!<port> | !*] -OSPF VirtualLink
```

Default None

Description The VirtualLink parameter adds or deletes routers to or from the virtual link list for the area to which the specified port belongs. A virtual link provides connection to areas in the autonomous system that are not directly connected to the backbone. A virtual link is required when an ABR has an interface that is not in the backbone area (AreaId 0), or when it is connected to the backbone and provides access to other ABRs that do not have access to the network. Up to eight virtual links can be established per port.

Virtual links cannot be configured if the port is in area 0. To configure a virtual link, both routers must have the other configured with the ADD command.

To display the virtual links for a particular port, use the SHow command. If you do not specify a port, the virtual links for all ports that have been configured with an IP address are displayed.

Values

None	No virtual links are configured for the area.
<rxmit interval>	Specifies a time interval (in seconds) at which LSAs are sent over the virtual link. To change the time interval for an existing entry, use the ADD command to specify the new time interval.
All	Removes all routers from the virtual link list for the area.
<router id>	Specifies a particular router to be added to or deleted from the virtual link list for the area. This value is entered in hexadecimal.

42

PATH SERVICE PARAMETERS

This chapter describes the PATH Service parameters. For descriptions of paths and ports, refer to Chapter 1 in *Using NETBuilder Family Software.* Table 42-1 lists the PATH Service parameters and commands.

Table 42-1 PATH Service Parameters and Commands

Parameters	Commands
BAud	SETDefault, SHow, SHowDefault
CLock	SETDefault, SHow, SHowDefault
CmdCharSet	SETDefault, SHow, SHowDefault
CONFiguration	SHow, SHowDefault
CONNector	SETDefault, SHow, SHowDefault
CONTrol	SETDefault, SHow, SHowDefault
DataBits	SETDefault, SHow, SHowDefault
DialCarrierTime	SETDefault, SHow, SHowDefault
DialCONTrol	SETDefault, SHow, SHowDefault
DialMode	SETDefault, SHow, SHowDefault
DialPool	SHow
DUplex	SETDefault, SHow, SHowDefault
ENCoding	SETDefault, SHow, SHowDefault
ExDevType	SETDefault, SHow, SHowDefault
LAyout	SHow, SHowDefault
LineType	SETDefault, SHow, SHowDefault
LocalDialNo	SETDefault, SHow, SHowDefault
LocalSubAddr	SETDefault, SHow, SHowDefault
MacAddress	SETDefault, SHow, SHowDefault
NAme	SETDefault, SHow, SHowDefault
Pad	SETDefault, SHow, SHowDefault
PARity	SETDefault, SHow, SHowDefault
PhantomPower	SETDefault, SHow, SHowDefault
RateAdaption	SETDefault, SHow, SHowDefault
RxParity	SETDefault, SHow, SHowDefault
SPIDdn1	SETDefault, SHow, SHowDefault
SPIDdn2	SETDefault, SHow, SHowDefault
StayAliveAction	SETDefault, SHow, SHowDefault
StayAliveTimer	SETDefault, SHow, SHowDefault
StopBits	SETDefault, SHow, SHowDefault
SwitchType	SETDefault, SHow, SHowDefault
TinyGramcomp	SETDefault, SHow, SHowDefault
TxIdle	SETDefault, SHow, SHowDefault
TxParity	SETDefault, SHow, SHowDefault

BAud

Syntax

For non-ISDN interfaces

For NETBuilder II bridge/router:

```
SETDefault !<path> -PATH BAud = <kbps> (1.2–52000)
SHow [!<path> | !*] -PATH BAud
SHowDefault [!<path> | !*] -PATH BAud
```

For all other platforms:

```
SETDefault !<path> -PATH BAud = <kbps> (1.2–16000)
SHow [!<path> | !*] -PATH BAud
SHowDefault [!<path> | !*] -PATH BAud
```

For software packages that support asynchronous communications:

```
SETDefault !<path> -PATH BAud = <kbps> (0.110-16000)
SHow [!<path> | !*] -PATH BAud
SHowDefault [!<path> | !*] -PATH BAud
```

For ISDN interfaces

```
SETDefault !<connectorID.channelID> -PATH BAud = <kbps> (1.2–16000)
SHow [!<connectorID.channelID> | !<connectorID>.*] -PATH BAud
SHowDefault [!<connectorID.channelID> | !<connectorID>.*] -PATH BAud
```

Default

64 kbps for serial lines and Integrated Services Digital Network (ISDN) lines that are not in NTT HSD128K mode

128 kbps for ISDN lines in NTT HSD128K mode

4,000 kbps for token ring

Description

The BAud parameter sets the baud rate for a specified token ring, serial, or ISDN line path. If the transmit clock is derived internally, or if the path is an asynch path, the value of BAud is used to set the speed of the clock. Otherwise, the BAud parameter changes only internal calculations to perform load sharing, spanning tree configurations, default costing for Open Shortest Path First (OSPF), and queue size determinations. However, even if the clock is derived externally, 3Com recommends that you set its value as close as possible to the actual baud rate at which the line operates, to achieve the best possible performance from your bridge/router. The baud rate is expressed in kilobits per second (kbps).

The auto startup feature automatically detects:

- Modem connectivity
- The wide area connector type (for SuperStack II NETBuilder bridge/routers only)
- The data link connection for a particular port (can detect the Point-to-Point Protocol and Frame Relay only)
- The type of line

These elements are detected when the platform boots. This feature also enables the associated path.

When you change this parameter value, you need to re-enable the corresponding path for the new parameter value to take effect.

The following baud rates are supported for asynchronous connectivity only (-PORT OWNer set to ATUN):

0.110	0.135	0.150
0.200	0.300	0.600

The following baud rates are supported for both asynchronous connectivity (-PORT OWNer set to ATUN), and BSC (-PORT OWNer set to BSC):

1.2	1.8	2.4
3.6	4.8	7.2
9.6	19.2	38.4

On software packages that support asynchronous connectivity, use baud rates lower than 1.2 kbps for asynch paths only. For all other functions, rates lower than 1.2 kbps are not allowed.

CLock

Syntax

```
SETDefault !<path> -PATH CLock = TestMode | External | Internal | Auto
SHow [!<path> | !*] -PATH CLock
SHowDefault [!<path> | !*] -PATH CLock
```

Default External

Description The CLock parameter determines how the bridge/router derives its transmit clock. This parameter applies only to serial interfaces. For the new value to take effect on all NETBuilder bridge/routers except the OfficeConnect models, you must re-enable the corresponding path.

On the OfficeConnect NETBuilder bridge/routers, clocking is detected automatically through the Flex-WAN cable; you cannot set clocking on the Flex-WAN port.

Values

TestMode Indicates the bridge/router derives the transmit clock from the on-board clock oscillator. TestMode does not support all baud rates. You cannot use the TestMode setting when you are configuring SuperStack II NETBuilder bridge/routers or NETBuilder II HSS V.35 3-Port WAN interfaces. This value does not apply to SuperStack II NETBuilder bridge/router models 32x and 52x.

Internal Indicates the bridge/router derives both the transmit and receive clocks from the on-board clock oscillator. This value applies to SuperStack II NETBuilder bridge/router (models 32x and 52x only). It also applies to a NETBuilder II HSS RS-232 3-Port DTE/DCE module if you change one of the module ports to DCE so that the port can connect to a DTE device.

External Indicates the bridge/router derives the transmit clock from the send or receive timing clock supplied by the digital service unit/channel service unit (DSU/CSU); by an attached modem; or for a NETBuilder II bridge/routers by an attached WAN Extender. For NETBuilder II bridge/routers deriving their transmit clock from a WAN Extender, the physical path of the NETBuilder II bridge/router has the clock set to External and not the virtual paths provided by the WAN Extender.

Auto — Indicates the default setting for the OfficeConnect NETBuilder bridge/router Flex-WAN cable. Clocking is detected automatically when this connector is attached and cannot be set by the user.

You must change the path clock setting from External to Internal if you change the port on the HSS RS-232 3-Port DTE/DCE module to DCE to connect to a DTE device. If you change this setting, you must also use a different cable. For more information, refer to the WAN Cabling and Connectivity Guide. You can find this guide on the 3Com Corporation World Wide Web site by entering: http://www.3com.com/.

The CLock parameter displays a "Not Set" value for Ethernet paths, WAN Extender virtual paths, and empty slots on all NETBuilder bridge/routers except the OfficeConnect models. For OfficeConnect NETBuilder bridge/routers, the CLock parameter displays "Auto" if no Flex-WAN connector is attached.

CmdCharSet

Syntax

```
SETDefault !<path> -PATH CmdCharSet = ASCII | EBCDIC
SHow [!<path> | !*] -PATH CmdCharSet
SHowDefault [!<path> | !*] -PATH CmdCharSet
```

Default ASCII

Description The CmdCharSet parameter defines how an external WAN device expects the V.25 bis commands to be formatted, either with ASCII or EBCDIC character sets. This parameter is only valid for V.25 bis dialing.

CONFiguration

Syntax *For non-ISDN interfaces*

```
SHow [!<path> | !*] -PATH CONFiguration
SHowDefault [!<path> | !*] -PATH CONFiguration
```

For ISDN interfaces

```
SHow [!<connectorID.channelID> | !<connectorID>.*] -PATH CONFiguration
SHowDefault [!<connectorID.channelID> | !<connectorID>.*] -PATH
  CONFiguration
```

Default No default

Description The CONFiguration parameter shows the values of the PATH parameters for a specified path. If no path number is specified, parameters for all paths are displayed.

To display the active configuration information, use SHow -PATH CONFiguration. To display the configuration information on the disk, use SHowDefault -PATH CONFiguration.

The Ctrl column shown in the display indicates whether the path is enabled or disabled. The State column shows the status of the path.

Because WAN Extender virtual paths do not bind to a port until a connection is established, the Conn column on the Current Path Parameters display will not show a value for a virtual path unless the virtual path is connected.

For dial-up lines, a connection is established when an outgoing call is completed or when an incoming call is accepted. For channelized lines, the connection is established when the NETBuilder II bridge/router synchronizes with the WAN Extender.

CONNector

Syntax *For all NETBuilder systems except SuperStack II NETBuilder bridge/router models 42x and 52x*

```
SETDefault !<path> -PATH CONNector = V35 | RS232 | RS449 | G703 | HSSI
  | X21
SHow [!<path> | !*] -PATH CONNector
SHowDefault [!<path> | !*] -PATH CONNector
```

For SuperStack II NETBuilder bridge/router models 42x

```
SETDefault !<connectorID> -PATH CONNector = AUTO | RS232 | V36 | RS449 |
  X21
SHow [!<connectorID>] -PATH CONNector
SHowDefault [!<connectorID>] -PATH CONNector
```

For SuperStack II NETBuilder bridge/router models 52x

```
SETDefault !<connectorID> -PATH CONNector = AUTO | RS232 | V35 | RS449 |
  X21
SHow [!<connectorID>] -PATH CONNector
SHowDefault [!<connectorID>] -PATH CONNector
```

For all OfficeConnect NETBuilder bridge/routers

```
SETDefault !<path> -PATH CONNector = Auto
SHow [!<path> | !*] -PATH CONNector
SHowDefault [!<path> | !*] -PATH CONNector
```

Default V35 for all NETBuilder systems except SuperStack II NETBuilder bridge/router models 32x, 42x, and 52x

AUTO for SuperStack II NETBuilder bridge/router models 42x and all OfficeConnect NETBuilder bridge/routers

RS449 for SuperStack II NETBuilder bridge/router models 32x and 52x

Description The CONNector parameter specifies the connector type for a serial interface. When you change this parameter state, you need to re-enable the corresponding path for the new parameter value to take effect.

This parameter does not apply to SuperStack II NETBuilder bridge/router models 2xx. On SuperStack II NETBuilder bridge/router models 32x, 42x, and 52x, this parameter applies only to the connector marked “B” (also referred to as the universal serial connector or USC); all other connector types on these models are fixed and cannot be changed.

On OfficeConnect NETBuilder bridge/routers, the connector type is determined automatically through the Flex-WAN cable and cannot be set using the CONNector parameter.

Values **V35, V36, RS232, RS449, G703, HSSI, AUTO, or X21**

All values are self-explanatory except for AUTO.

The G703 value is only available on the NETBuilder II bridge/router; the AUTO value is available only on all SuperStack II NETBuilder bridge/routers.

The AUTO value configures the software to automatically sense the type of wide area connector you have cabled without user intervention.

The AUTO value must be explicitly set for software versions 8.3 and earlier. For all software releases, both the -PATH CONNector command and the -PORT OWNer command must be set to AUTO in SuperStack II NETBuilder bridge/router models 32x and 52x for the auto connector to properly detect the path configurations.

The auto startup feature automatically detects modem connectivity, the wide area connector type, the data link connection for a particular port (can detect PPP and Frame Relay only), the type of line, and enables the associated path. These attributes are detected when the platform boots.

For empty slots and nonserial ports on all NETBuilder bridge/routers except the OfficeConnect models, the CONNector parameter displays a “Not Set” value. For OfficeConnect NETBuilder bridge/routers, the CONNector parameter displays AUTO followed by (N/C) if the Flex-WAN connector is not connected, or AUTO followed by the connector type.

CONTrol

Syntax

For all NETBuilder systems except SuperStack II NETBuilder bridge/routers

```
SETDefault !<path> -PATH CONTrol = ([Enabled | Disabled],
  [ItcmCompatible | NoItcmCompatible], [T1Mode | NoT1Mode], [Crypto |
  NoCrypto], [CRC32 | CRC16])
SHow [!<path> | !*] -PATH CONTrol
SHowDefault [!<path> | !*] -PATH CONTrol
```

For SuperStack II NETBuilder bridge/routers

```
SETDefault !<connectorID.channelID> -PATH CONTrol = ([Enabled |
  Disabled], [Crypto | NoCrypto], [CRC32 | CRC16])
SHow [!<connectorID.channelID> | !<connectorID>.*] -PATH CONTrol
SHowDefault [!<connectorID.channelID> | !<connectorID>.*] -PATH CONTrol
```

Default

NoItcmCompatible, NoT1Mode, NoCrypto

All paths are enabled; CRC is set to 16 bit

Description

The CONTrol parameter enables or disables a path on the bridge/router. By disabling and enabling the path, all the values associated with the CONTrol parameter take effect.

Values

Enabled | Disabled	Enables or disables a path. Enabled and Disabled are the only options available for WAN Extender virtual paths.
ItcmCompatible | NoItcmCompatible	The ItcmCompatible value should be enabled if your bridge/router is attached through a serial link to a Series/1-based bridge or bridge/router (IB/3, BR/3) that contains an Integrated T1 Controller Module (ITCM) board. For example, enable the ItcmCompatible option if a path on your bridge/router is attached to an ITCM board path on a Series/1 device.

T1Mode | NoT1Mode

This value applies only to leased lines. It does not apply to switched lines such as Frame Relay, X.25, or SMDS.

When some digital service units (DSUs) are configured for 1.544 Mbps, the one's density of the line is not ensured. In this situation, you can set this parameter to the T1Mode option so that the system ensures the one's density of the line. Do not select T1Mode and ItcmCompatible at the same time. If you do, change the setting from T1Mode to NoT1Mode. If the line goes down, you must disable and then enable the path or reset the bridge/router and the Series/1- based bridge or bridge/router at the same time to recover the line.

Crypto | NoCrypto

The Crypto value causes the system to attempt to resynchronize with attached KG81/94 devices. This value applies only to the RS-449 interface of a wide area bridge/router. Although an RS-449 interface is used between a NETBuilder II bridge/router and a WAN Extender, only the Enabled and Disabled options are available for WAN Extender virtual paths.

CRC16 | CRC32

CRC16 is a 16-bit cyclic redundancy check (CRC) that is used on serial lines. If you set the CONTrol parameter to CRC32, a 32-bit CRC is used. Both ends of the path need to have the same CRC value settings. The SMDS Protocol requires the CRC value where the CRC between the router and DSU is optionally set to 16/32. 32-bit CRC is an option on SMDS ports.

DataBits

Syntax

```
SETDefault !<path> -PATH DataBits = 5 | 6 | 7 | 8
SHow [!<path> | !*] -PATH DataBits
SHowDefault [!<path> | !*] -PATH DataBits
```

Default 8

Description The DataBits parameter determines the number of data bits in each character transmitted or received on an asynchronous path. This parameter applies only when the -PORT OWNer parameter is set to ATUN.

DialCarrierTime

Syntax *For non-ISDN interfaces*

```
SETDefault !<path> -PATH DialCarrierTime = <seconds> (30–300)
SHow [!<path> | !*] -PATH DialCarrierTime
SHowDefault [!<path> | !*] -PATH DialCarrierTime
```

For ISDN interfaces

```
SETDefault !<connectorID.channelID> -PATH DialCarrierTime = <seconds>
  (50–300)
SHow [!<connectorID.channelID> | !<connectorID>.*] -PATH DialCarrierTime
SHowDefault [!<connectorID.channelID> | !<connectorID>.*] -PATH
  DialCarrierTime
```

Default 120

Description The DialCarrierTime parameter defines the number of seconds the system must wait for the carrier signals on the connected line. If this timer expires before the carrier is detected, the interface is disconnected; the system retries the call after the retry timer times out.

DialCONTrol

Syntax *For non-ISDN interfaces*

```
SETDefault !<path> -PATH DialCONTrol = ([DYNamic | STAtic],
  [DisasterRcvry | NoDisasterRcvry | UnReSTricted], [Answer |
  NoAnswer], [Originate | NoOriginate])
SHow [!<path> | !*] -PATH DialCONTrol
SHowDefault [!<path> | !*] -PATH DialCONTrol
```

For ISDN interfaces

```
SETDefault !<connectorID.channelID> -PATH DialCONTrol = ([DYNamic |
  STAtic], [DisasterRcvry | NoDisasterRcvry | UnReSTricted],
  [ Answer |NoAnswer], [Originate| NoOriginate])
SHow [!<connectorID.channelID> | !<connectorID>.*] -PATH DialCONTrol
SHowDefault [!<connectorID.channelID> | !<connectorID>.*] -PATH
  DialCONTrol
```

When configuring a NETBuilder II bridge/router to use a WAN Extender, the WAN Extender virtual paths available for dial-up paths are set automatically to the default values for the -PATH DialCONTrol parameter except that the virtual paths are automatically set to DYNamic and not STAtic (the default setting).

Default STAtic, UnReSTricted, Answer, Originate

Description The DialCONTrol parameter sets the path attributes for the dial-up paths. This parameter is a bit-mapped control parameter.

Values

DYNamic | STAtic

STAtic makes the selected path available only to its corresponding port and is the default. A static path is not part of the dynamic dial pool. DYNamic unbinds a path from its corresponding port and adds the path to the dynamic dial pool. Placing a path in the dial pool allows the path to be used by any dial port. For a dial path to become a dynamic dial path, the -PATH LineType parameter must be set to Dialup. To take a dynamic path out of the dial pool, set the -PATH DialCONTrol parameter to STAtic, and rebind the path to a port using the ADD -PORT PAths command.

DisasterRcvry | NoDisasterRcvry | UnReSTricted

The DisasterRcvry value allows the dial path to be used for disaster recovery purposes only; it cannot be used for normal or bandwidth-on-demand aggregation.

The NoDisasterRcvry value assigns the dial path only for normal bandwidth or bandwidth-on-demand aggregation; it cannot be used for disaster recovery. This value is most often assigned to the least reliable line in the network.

	The UnReSTricted value (the default) assigns the dial path for any purpose: disaster recovery or bandwidth aggregation.
Answer | NoAnswer	The Answer value allows the dial-up line to accept incoming calls. Use NoAnswer when you do not want the dial-up line to accept incoming calls. These values apply to both static and dynamic paths. For dial-up port control, refer to "DialRcvrState" on page 43-12.
Originate | NoOriginate	The Originate value allows the dial-up path to originate calls. Use NoOriginate when you do not want the dial-up path to originate calls. These values apply to both static and dynamic paths.

When you change the parameter state to Answer | NoAnswer or to Originate | NoOriginate, you need to enable the corresponding port or path for the new parameter value to take effect.

Example In this example, you assign paths 3 and 4 to port 3. You then assign path 3 as an unrestricted leased line and path 4 as the dial-up disaster recovery line by entering:

```
ADD !3 -PORT PAths 3,4
SETDefault !3 -PATH LineType = Leased
SETDefault !3 -PATH DialCONTrol = (STAtic, UnReSTricted)
SETDefault !4 -PATH LineType = Dialup
SETDefault !4 -PATH DialCONTrol = (STAtic, DisasterRcvry, Answer,
Originate)
```

DialMode

Syntax

```
SETDefault !<path> -PATH DialMode = V25bis | DTRdial
SHow [!<path> | !*] -PATH DialMode
SHowDefault [!<path> | !*] -PATH DialMode
```

Default V25bis

Description The DialMode parameter configures a data terminal equipment (DTE) path for a V.25bis-compatible modem or a modem that initiates and terminates calls by raising or lowering the data terminal ready (DTR) signal.

When you change this parameter state, you need to enable the corresponding port or path for the new parameter value to take effect.

DialPool

Syntax

```
SHow -PATH DialPool
```

Default No dynamic dial paths in the dial pool

Description The DialPool parameter displays the dial pool status and configuration. This display includes the following:

- All paths in the dial pool
- All dynamic paths, both physical and virtual

- The last time the path was used
- The time when the current path became active
- The external device type
- The ports that have reserved the dial paths through the -PORT PathPreference parameter

Because WAN Extender virtual dial paths cannot be reserved for specific ports with the -PORT PathPreference parameter, the entry of a SHow -PATH DialPool command displays the virtual paths provided by WAN Extender to the dial-up pool, but does not display the reservation of WAN Extender virtual paths to a particular port.

DUplex

Syntax

```
SETDefault !<path> -PATH DUplex = Full | Half | Auto
SHow [!<path> | !*] -PATH DUplex
SHowDefault [!<path> | !*] -PATH DUplex
```

Default Auto

Description The DUplex parameter specifies the physical characteristics of the communications method used to control the request-to-send (RTS) signal on the serial line. Selecting the full-duplex transmission mode can eliminate the turnaround time and maximize the line use. Half duplex is necessary if the attached modem or device configuration requires half-duplex operations. Depending on the interface, Auto specifies either full or half duplex:

- When using Fast Ethernet, Auto is set to half duplex.
- When using Synchronous Data Link Control (SDLC), Auto is set to full duplex.
- When using the Flex-WAN cable on the OfficeConnect NETBuilder bridge/router, Auto is set to full duplex mode, and is the recommended setting.

Before changes to this parameter can take effect, -PATH CONTrol must be enabled.

ENCoding

Syntax

```
SETDefault !<path> -PATH ENCoding = NRZ | NRZI
SHow [!<path> | !*] -PATH ENCoding
SHowDefault [!<path> | !*] -PATH ENCoding
```

Default NRZ

Description The ENCoding parameter specifies the transmission encoding method for a serial line. The coding method you specify for the serial line must match the attached communication device. Use non-return to zero (NRZ) encoding for digital devices and non-return to zero inverted (NRZI) for analog devices.

Before changes to this parameter can take effect, -PATH CONTrol must be enabled.

ExDevType

Syntax

```
SETDefault !<path> -PATH ExDevType = Modem | Bri | Sw56
SHow [!<path> | !*] -PATH ExDevType
SHowDefault [!<path> | !*] -PATH ExDevType
```

Default Modem (if DTE connector type; otherwise “-” is displayed)

Description The ExDevType parameter specifies and displays the external device type attached to a DTE connector, for example, an HSS module or DTE connector on the SuperStack II NETBuilder bridge/router models 42x. This parameter is used with the dial-up path selection algorithm for matching destination phone numbers with dynamic dial ports.

For the NETBuilder II bridge/router with HSS modules installed, the connector type is a DTE connector type such as RS-232 or RS-449. In this configuration, the ExDevType parameter can be set to Modem, Bri, or Sw56.

For the SuperStack II NETBuilder bridge/router models 42x, the setting of this parameter depends on the connector type. For path 2.*, the connector type is Bri, and the ExDevType parameter does not apply. The system can identify the connector type without user intervention. For path 3, the connector type is a DTE connector type such as RS-232; the ExDevType parameter can be set to Modem, Bri, or Sw56.

For NETBuilder II bridge/routers with a WAN Extender, the ExDevType setting for the WAN Extender physical path is set automatically to WE by the device driver. This setting can be viewed, but not changed with the ExDevType parameter.

Only paths that have DTE connector types can have the ExDevType parameter defined. Other paths do not use this parameter, and a hyphen (-) is displayed as their value.

Values

Modem	Specifies the path is connected to an analog modem.
Bri	Specifies the path is connected to a digital modem (a terminal adapter for Integrated Services Digital Network (ISDN) connectivity).
Sw56	Specifies the path is connected to a SW56 DSU/CSU.

LAyout

Syntax

```
SHow -PATH LAyout
SHowDefault -PATH LAyout
```

Default No default

Description The LAyout parameter displays the arrangement of slots, module types, and path assignments on the bridge/router.

LineType

Syntax

For all NETBuilder systems except SuperStack II NETBuilder bridge/routers with ISDN interfaces

```
SETDefault !<path> -PATH LineType = [Leased | Dialup]
SHow [!<path> | !*] -PATH LineType
SHowDefault [!<path> | !*] -PATH LineType
```

For SuperStack II NETBuilder bridge/routers with ISDN interfaces

```
SETDefault !<connectorID.channelID> -PATH LineType = [Auto | Leased |
  Dialup | HSD64 | HSD128 | Digi64S]
SHow [!<connectorID.channelID> | !<connectorID>.*] -PATH LineType
SHowDefault[!<connectorID.channelID>|!<connectorID>.*]-PATHLineType
```

Default

Leased for all NETBuilder systems, except the SuperStack II NETBuilder bridge/router, without ISDN interfaces. Auto is the default for SuperStack II NETBuilder bridge/routers with ISDN interfaces.

Description

The LineType parameter sets the type of line being used on your wide area interface. When you change the LineType setting, you must reenable the path for the change to take effect.

The LineType parameter for a WAN Extender virtual path is set automatically by the WAN Extender device driver. The driver sets the LineType parameter to Dial-up for a dial-up path and to Leased for a channelized path. You can display these settings, but you cannot change them. The Linetype parameter for a physical path to which the WAN Extender is connected must be set to Leased.

Values

Leased Applies only to DTE interfaces. Specifies the line type as a leased line.

Dialup Specifies the line type as a dial-up line.

Auto Applies only to SuperStack II NETBuilder bridge/routers. Configures the software to recognize the type of line automatically without user intervention. If specified for a DTE interface, the dial mode is automatically detected to be either V.25 bis or DTR, regardless of the setting of the -PATH DialMode parameter.

The auto startup feature automatically detects modem connectivity, the DTE connector type (for SuperStack II NETBuilder bridge/router models 42x only), the data link connection for a particular port (can detect PPP and Frame Relay only), the type of line, and enables the associated path. The detection of these elements takes place when the platform boots. If auto line detection brings up a DTR line, the line stays up until you bring it down manually using the HangUp command.

An ambiguity may occur in detecting leased lines versus DTR mode dial-up lines if data carrier detected/data set ready (DCD/DSR) is on. If you keep the system in auto mode, the physical connection will be made. However, the line type reported may not be correct because auto-line-type detection may not be able to distinguish a leased line from a DTR mode dial-up line.

When the auto startup facility is used with Matracom ISDN Model 820 devices on SuperStack II NETBuilder bridge/routers, LineType is set by default to Auto, but the line is detected as leased instead of dial-up. The central site can still *place a call to the remote unit and perform the initial configuration, because the remote site answers automatically when the call is placed. The central site can then complete normal reconfiguration.*

HSD64 Applies only to ISDN interfaces. Specifies the Japanese NTT ISDN permanent circuit 64K service.

HSD128 Applies only to ISDN interfaces. Specifies the Japanese NTT ISDN permanent circuit 128K service. When you specify this option for a particular channel path, that path automatically uses both B channels to provide a single 128 kbps path. The other channel path cannot be used by the protocols.

Digi64S Applies only to ISDN interfaces. Specifies the ISDN 64 kbps leased line service Digital64S for ISDN BRI non-switched connections.

LocalDialNo

Syntax *For ISDN interfaces only*

```
SETDefault !<connectorID.channelID> -PATH LocalDialNo = “<string>”
SHow [!<connectorID.channelID> | !<connectorID>.*] -PATH LocalDialNo
SHowDefault [!<connectorID.channelID> | !<connectorID>.*] -PATH
  LocalDialNo
```

Default No phone number configured

Description The LocalDialNo parameter specifies a phone number provided by your telecommunications carrier for an ISDN path.

The phone number string can be composed of a maximum of 30 characters. Valid characters include the digits 0 through 9, an asterisk (*), and the pound sign (#). Because the software ignores all other characters except those previously mentioned, you can also specify special characters, such as parentheses and dashes, to distinguish the different elements that compose a phone number and text characters to embed descriptive text in the string.

When specifying a phone number, each character entered, whether the software considers it valid or ignores it, counts toward the maximum allowable number of characters.

An example of specifying a phone number for ISDN path 2.1 is as follows:

```
SETDefault !2.1 -PATH LocalDialNo = “Los Angeles Office 1-213-555-1000”
```

In this command, the phone number consists of long distance dial prefix 1 (assume that the bridge/router being configured is located in Santa Clara), and phone number 213-555-1000. The descriptive text indicates that the phone and subaddress numbers are for the Los Angeles office.

For hints on how to configure this parameter, refer to Chapter 35 in *Using NETBuilder Family Software*.

If you assign the same phone number to more than one ISDN path in your point-to-point or point-to-multipoint configuration, you need to specify a subaddress, which resembles a phone extension, using the -PATH LocalSubAddr parameter. For more information on subaddresses, refer to Chapter 35 in *Using NETBuilder Family Software*.

Not all telecommunications carriers allow you to assign the same phone number to multiple paths. When you contact your carrier to acquire support services, verify that they support this feature. You must also specify that you will be using subaddresses.

For the configuration of this parameter to take effect, you must re-enable the channel using the -PATH CONTrol parameter. For more information, refer to "CONTrol" on page 42-6.

LocalSubAddr

Syntax

```
SETDefault !<connectorID.channelID> -PATH LocalSubAddr = "<string>"
SHow [!<connectorID.channelID> | !<connectorID>.*] -PATH LocalSubAddr
SHowDefault [!<connectorID.channelID> | !<connectorID>.*] -PATH
  LocalSubAddr
```

Default No subaddress configured

Description The LocalSubAddr parameter configures a subaddress to the phone number you specified for an ISDN path using the -PATH LocalDialNo parameter. A subaddress resembles a phone extension. When specifying a subaddress, valid characters include up to 20 ASCII characters.

You need to specify a subaddress if you have assigned the same phone number to more than one ISDN path in your point-to-point or point-to-multipoint configuration. The telecommunications carrier does not provide a subaddress; you must create your own.

Not all telecommunications carriers allow you to assign the same phone number to multiple paths. When you contact your carrier to acquire support services, verify that they support this feature. You must also specify that you will be using subaddresses.

For more information on subaddresses, refer to Chapter 35 in *Using NETBuilder Family Software*.

For the configuration of this parameter to take effect, you must re-enable the channel using the -PATH CONTrol parameter. For more information, refer to "CONTrol" on page 42-6.

MacAddress

Syntax

```
SETDefault !<path> -PATH MacAddress = %<MAC address> |
  Mac <MAC address> | Ncmac <MAC address> | Reset
SHow [!<path>| !*] -PATH MacAddress
SHowDefault [!<path>| !*] -PATH MacAddress
```

Default The media access control (MAC) address burned into the adapter's PROM is the default for each interface.

Changing the MAC address using the MacAddress parameter is supported only on token ring paths.

Description The MacAddress parameter changes the MAC address assigned to a physical LAN interface. The default MAC address is burned into the PROM of the interface, but with this parameter you can reassign a new MAC address.

You may need to reassign the MAC address in connection-oriented environments such as Systems Network Architecture (SNA) because the originator of the session request must configure the destination MAC address before a connection can be established. By reassigning the MAC address to a port, you can also hot-swap modules and use the same MAC address so that end stations do not need to be reconfigured. You can enter the MAC address in either native format, canonical format, or noncanonical format.

You must re-enable the path after setting this parameter.

The address you assign cannot be a broadcast address and cannot match the smart filtering MAC address and all of the Bridge Protocol Data Unit (BPDU) addresses. You can use the same media address that already exists on one of the bridge/router interfaces, but you will receive a warning message.

You can also assign a different MAC address to the CEC module of the NETBuilder II bridge/router for APPN environments. To do this, specify !0 as the path when entering the command so the new MAC address is assigned for the bridge/router, and not for individual ports. If you change the CEC address by specifying !0 for the MacAddress parameter, you must reboot the bridge/router for the change to take effect.

Values

%<MAC address>	Enters the MAC address in canonical format. Do not enter a space between the percent symbol (%) and the address.
Mac <MAC address>	Enters the MAC address in canonical format. Enter a space between the keyword Mac and the address.
Ncmac <MAC address>	Enters the MAC address in noncanonical format. Enter a space between the keyword Ncmac and the address.
Reset	Returns the MAC address to the original address burned into the adapter's PROM.

To convert a MAC address from canonical to noncanonical format and vice versa, use the MacAddrConvert command. Bits 0 and 1 (the two most significant bits in a noncanonical address) must be set to 0 and 1, respectively. Bit 0 is the multicast bit, and bit 1 is the upper/lower bit. For more information, refer to "MacAddrConvert" on page 1-31 in Chapter 1.

NAme

Syntax *For non-ISDN interfaces*

```
SETDefault !<path> -PATH NAme = "<string>"
SHow [!<path> | !*] -PATH NAme
SHowDefault [!<path> | !*] -PATH NAme
```

For ISDN interfaces

```
SETDefault !<connectorID.channelID> -PATH NAme = "<string>"
SHow [!<connectorID.channelID> | !<connectorID>.*] -PATH NAme
SHowDefault [!<connectorID.channelID> | !<connectorID>.*] -PATH NAme
```

Default For non-ISDN interfaces, Path_n (where n is the path number; for example, Path_1, Path_2, Path_3, Path_4)

For ISDN interfaces, Path_n.x (where n is the connector number and x is the B channel number; for example, Path_2.1, Path_2.2)

Description The NAme parameter assigns a name to the specified path. The name is subject to the following restrictions:

- The name string can contain a maximum of eight characters, the first of which must be alphabetic.
- No blank spaces are allowed. The only non-alphanumeric characters allowed are the asterisk (*), underscore (_), period (.), and hyphen (-).
- Two paths cannot have the same name, but a path name can be the same as an existing port name.
- Alphabetic characters are stored and displayed as entered. Names are case-insensitive when compared on entry with previously entered names. For example, path2 and PATH2 are evaluated as the same name.

After you assign a name to a port, you can use the name as an instance identifier in subsequent commands, replacing <path> for non-ISDN interfaces and <connectorID.channelID> for ISDN interfaces.

Pad

Syntax *For non-ISDN interfaces*

```
SETDefault !<path> -PATH Pad = <number> (0–100)
SHow [!<path> | !*] -PATH Pad
SHowDefault [!<path> | !*] -PATH Pad
```

For ISDN interfaces

```
SETDefault !<connectorID.channelID> -PATH Pad = <number> (0–100)
SHow [!<connectorID.channelID> | !<connectorID>.*] -PATH Pad
SHowDefault [!<connectorID.channelID> | !<connectorID>.*] -PATH Pad
```

Default 0

Description The Pad parameter sets the number of high-level data link control (HDLC) flags that will be inserted between frames on a serial or ISDN line.

By setting this parameter, you can prevent the NETBuilder II bridge/router from overrunning NETBuilder or SuperStack II NETBuilder bridge/routers when these devices are connected back-to-back over a serial or ISDN line. Increasing the number of flags prevents the NETBuilder II system from sending back-to-back frames.

When you change this parameter state, you need to enable the corresponding port or path for the new parameter value to take effect.

PARity

Syntax

```
SETDefault !<path> -PATH PARity = Even | Odd | Mark | Space | None
SHow [!<path> | !*] -PATH PARity
SHowDefault [!<path> | !*] -PATH PARity
```

Default None

Description The PARity parameter configures the parity used on an asynchronous path. When the path is configured, it transmits and receives using the specified parity. If asymmetric parity is required, the RxParity and TxParity parameters can be used to configure receive and transmit parity independently. If asymmetric parity is in use, then when you display the PARity parameter, it will display the values configured by the RxParity and TxParity parameters. This parameter applies only when the -PORT OWNer parameter is set to ATUN.

Values

Even	Indicates that the parity bit is appended to make the total parity even.
Odd	Indicates that the parity bit is appended to make the total parity odd.
Mark	Indicates that the parity bit appended is always one.
Space	Indicates that the parity bit appended is always zero.
None	Indicates that no parity bit is appended.

PhantomPower

Syntax *For ISDN interfaces only*

```
SETDefault !<connectorID> -PATH PhantomPower= Disable| Enable
SHow [!<connectorID>] -PATH PhantomPower
SHowDefault [!<connectorID>] -PATH PhantomPower
```

Default Enable

Description The PhantomPower parameter disables or enables the detection of phantom power that may be available from your ISDN line. The PATH CONTrol parameter must be set to Enable before this parameter takes effect.

Users in the United States who are connecting their 3Com bridge/router to an NT1 switch, which does not supply phantom power, should set this parameter to Disable before initiating ISDN dialup.

RateAdaption

Syntax

```
SETDefault !<connectorID.channelID> -PATH RateAdaption = Auto | Rate64
  | Rate56
SHow [!<connectorID.channelID> | !<connectorID>.*] -PATH RateAdaption
SHowDefault [!<connectorID.channelID> | !<connectorID>.*] -PATH
  RateAdaption
```

Default Auto

Description The RateAdaption parameter specifies a method that determines the data rate to be used on a particular B channel.

The RateAdaption parameter applies to ISDN interfaces only.

Values

Auto For US Switch Types incoming calls, when rate adaption is set to Auto, calls will be connected at either 56K or 64K.

For US Switch Types outgoing calls, when rate adaption is set to Auto if the dial number list's baud rate is configured to be greater than 56, the initial call is made at 64K and the retry is made at 56K. If the dial number list baud rate is less than or equal to 56, the initial call is made at 56K and the retry is made at 64K.

For non-US Switch Types incoming calls, when rate adaption is set to Auto, a call is connected at either 56K or 64K.

For non-US Switch Types outgoing calls, when rate adaption is set to Auto, calls are made at 64K only.

Rate64 For US Switch Types incoming calls, when rate adaption is set to Rate64, calls are connected at 64K only.

For US Switch Types outgoing calls, when rate adaption is set to Rate64, calls are made at 64K only.

For non-US Switch Types incoming calls, when rate adaption is set to Rate64, calls are connected at 64K only.

For non-US Switch Types outgoing calls, when rate adaption is set to Rate64, calls are made at 64K only.

Rate56 For US Switch Types incoming calls, when rate adaption is set to Rate56, calls are connected at 56K only.

For US Switch Types outgoing calls, when rate adaption is set to Rate56, calls are made at 56K only.

For non-US Switch Types incoming calls, when rate adaption is set to Rate56, calls are connected at 56K only.

For non-US Switch Types outgoing calls, when rate adaption is set to Rate56, calls are made at 56K only.

RxParity

Syntax

```
SETDefault !<path> -PATH RxParity = Even | Odd | Mark | Space | Tx
SHow [!<path> | !*] -PATH RxParity
SHowDefault [!<path> | !*] -PATH RxParity
```

Default Tx

Description The RxParity parameter determines the value of the parity bit checked for each character received on an asynchronous path. When a character is received with incorrect parity, the character is discarded. This parameter applies only when the -PORT OWNer parameter is set to ATUN.

Values

Even Checks for even parity.

Odd Checks for odd parity.

Mark Checks for a parity bit value of one.

Space Checks for a parity bit value of zero.

Tx Checks for parity matching the current setting of the -PATH TxParity parameter.

SPIDdn1

Syntax *For ISDN interfaces only*

```
SETDefault !<connectorID> -PATH SPIDdn1 = “<string>”
SHow [!<connectorID>] -PATH SPIDdn1
SHowDefault [!<connectorID>] -PATH SPIDdn1
```

Default No SPIDs configured

Description The SPIDdn1 parameter specifies the Service Profile Identifiers (SPIDs) and directory numbers (DNs) provided by a North American telecommunications carrier for North American BRI ISDN dial-up modes for which the ISDN line has been provisioned as a fully initializing terminal (FIT). A DN is a phone number that is used to determine if an incoming call is accepted.

This parameter does not apply to European or Japanese dial-up or non-dial-up modes. If a SPID was not specified for a North American ISDN switch, the ISDN line was not provisioned as FIT, and the SPID negotiation with the switch will not be attempted.

Some North American switches require one SPID, while others require two. If two SPIDs are required, you must configure the -PATH SPIDdn2 parameter.

The DNs may be needed for some DMS100 or NI1 switches to support the FIT registration. DNs are provided by your telecommunications carrier along with the SPID when you acquire your services.

A SPID string can contain a maximum of 20 digits; a DN string can contain up to 16 digits. When specifying both a SPID and DN, enter the SPID string first, then a semicolon (;) to separate the SPID and DN strings, then the DN string. When specifying a SPID string only, you do not need to enter a semicolon.

For more information on acquiring services from your telecommunications carrier, refer to Chapter 35 in *Using NETBuilder Family Software*.

For the configuration of this parameter to take effect, you must re-enable the channel using the -PATH CONTrol parameter. For more information, refer to “CONTrol” on page 42-6 of this guide.

SPIDdn2

Syntax *For ISDN interfaces only*

```
SETDefault !<connectorID> -PATH SPIDdn2 = “<string>”
SHow [!<connectorID>] -PATH SPIDdn2
SHowDefault [!<connectorID>] -PATH SPIDdn2
```

Default No SPIDs configured

Description The SPIDdn2 parameter functions in the same way as the SPIDdn1 parameter; you can refer to “SPIDdn1” on page 42-18 for information.

StayAliveAction

Syntax

```
SETDefault !<path> -PATH StayAliveAction = Reset | NoReset
SHow [!<path> | !*] -PATH StayAliveAction
SHowDefault [!<path> | !*] -PATH StayAliveAction
```

Default NoReset

Description The StayAliveAction parameter enables the Ethernet driver to reset the Ethernet controller chip for the specified path if no data is received during the interval determined by the StayAliveTimer parameter. If the default value of NoReset is used, the driver does not reset the chip.

The default value of NoReset is normally satisfactory unless you suspect a path has stopped receiving data. You can examine path statistics by entering:

```
FLush
```

and

```
SHow -SYS STATistics -PATH
```

The StayAliveAction parameter can be set only on NETBuilder II bridge/router single-port and dual-port Ethernet modules. If you attempt to set this parameter on other types of NETBuilder II bridge/router ports, or on SuperStack II NETBuilder bridge/router ports, you will receive error messages.

StayAliveTimer

Syntax

```
SETDefault !<path> -PATH StayAliveTimer = <seconds> (0–255)
SHow [!<path> | !*] -PATH StayAliveTimer
SHowDefault [!<path> | !*] -PATH StayAliveTimer
```

Default 2

Description The StayAliveTimer parameter defines the interval of time between transmission of stay-alive packets by the driver. A value of 0 disables the transmission of these packets. This parameter is valid only for Ethernet paths.

The StayAlive parameter timer is issued every <integer> seconds with a default of 2 seconds. The actual interval between stay-alive packets reflects the user set values under low and medium traffic rates. As the traffic rate increases, the actual interval becomes larger than the user set value.

During extreme Ethernet activity, the StayAliveTimer may not be sent out. This action reduces unnecessary traffic. Carrier loss (that is, the Ethernet cable being disconnected) is detected within the amount of time specified for the StayAliveTimer value within 10 percent of the accuracy of the system clock.

StopBits

Syntax

```
SETDefault !<path> -PATH StopBits = 1 | 1.5 | 2
SHow [!<path> | !*] -PATH StopBits
SHowDefault [!<path> | !*] -PATH StopBits
```

Default 1

Description The StopBits parameter determines the number of stop bits appended to each character on an asynchronous path. This parameter applies only when the -PORT OWNer parameter is set to ATUN.

SwitchType

Syntax *For ISDN interfaces only*

```
SETDefault !<connectorID> -PATH SwitchType = ETSI | NTT | KDD | NI1 |
  ATT5ESS | DMS100 | VN3 | AUSTEL
SHow [!<connectorID>] -PATH SwitchType
SHowDefault [!<connectorID>] -PATH SwitchType
```

Default ETSI

Description The SwitchType parameter specifies the type of switch to which your ISDN path interfaces.

Values

ETSI	Specifies the European ETSI standard ISDN switch. This selection is valid only if the -PATH LineType parameter is set to Dialup or Auto.

NTT Specifies the Japanese NTT ISDN switch. This selection is valid only if the -PATH LineType parameter is set to Dialup or Auto. The services supported include:

NTT INS_C Specifies the dialup service that uses one B1 64 Kbps channel

HSD128 Specifies the permanent circuit 128K service

HSD64 Specifies the permanent circuit 64K service

NI1 Specifies the North American National ISDN 1 switch. This selection is valid only if the -PATH LineType parameter is set to Dialup or Auto.

ATT5ESS Specifies the AT&T 5ESS ISDN switch. This selection is valid only if the -PATH LineType parameter is set to Dialup or Auto.

DMS100 Specifies the Northern Telecom DMS 100 ISDN switch. This selection is valid only if the -PATH LineType parameter is set to Dialup or Auto.

VN3 Specifies the French VN3 ISDN switch. This selection is valid only if the -PATH LineType parameter is set to Dialup or Auto.

AUSTEL Specifies the Australian ISDN switch. This selection is valid only if the -PATH LineType parameter is set to Dialup or Auto.

TinyGramcomp

Syntax *For non-ISDN interfaces*

```
SETDefault !<path> -PATH TinyGramcomp = Enabled | Disabled
SHow [!<path> | !*] -PATH TinyGramcomp
SHowDefault [!<path> | !*] -PATH TinyGramcomp
```

For ISDN interfaces

```
SETDefault !<connectorID.channelID> -PATH TinyGramcomp = Enabled
  | Disabled
SHow [!<connectorID.channelID> | !<connector>.*] -PATH
  TinyGramcomp
SHowDefault [!<connectorID.channelID> | !<connectorID>.*] -PATH
  TinyGramcomp
```

Default Disabled

Description The TinyGramcomp parameter compresses all bridged Ethernet packets that are 64 bytes and are padded with trailing zeros. When the packet is sent on a serial line, the receiving side reinserts the zeros before forwarding the packet to an Ethernet LAN.

This parameter is effective only on serial and ISDN ports and is normally used in Digital Equipment Corporation (DEC) and local area transport (LAT) terminal-to-host environments.

TxIdle

Syntax

```
SETDefault !<path> -PATH TxIdle = Flag | Mark
SHow [!<path> | !*] -PATH TxIdle
SHowDefault [!<path> | !*] -PATH TxIdle
```

Default Flag

Description The TxIdle parameter determines if the bridge/router sends continuous flags or stops the transmission process when it is not sending frames. When transmitting multiple frames, the bridge/router sends flags between frames regardless of the setting of this parameter. Changes to this parameter do not take effect until after the Path Service CONTrol parameter is enabled.

Values

Flag — Causes the bridge/router to send continuous flags on the transmit line after the transmission of the last frame of the transaction (the frame that contains the poll/final bit). The transmission of flags keeps the line up for further transmissions.

Mark — When the DUplex parameter is set to half-duplex, the TxIdle Parameter must be set to this value allowing the half-duplex transactions to occur. When the last frame is sent, no flags are sent and the RTS signal is lowered after the abort signal, setting the system up for the second half of the transmission.

TxParity

Syntax

```
SETDefault !<path> -PATH TxParity = Even | Odd | Mark | Space |
  None
SHow [!<path> | !*] -PATH TxParity
SHowDefault [!<path> | !*] -PATH TxParity
```

Default None

Description The TxParity parameter determines the value of the parity bit appended to each character transmitted on an asynchronous path. This parameter is valid only when the -PORT OWNer parameter is set to ATUN.

Values

Even — Specifies that the parity bit is appended to make the total parity even.

Odd — Specifies that the parity bit is appended to make the total parity odd.

Mark — Specifies that the parity bit appended is always one.

Space — Specifies that the parity bit appended is always zero.

None — Specifies that no parity bit is appended.

43

PORT SERVICE PARAMETERS

This chapter describes parameters in the PORT Service. PORT Service parameters determine the characteristics of the bridge/router's ports. For descriptions of ports, refer to Chapter 1 in *Using NETBuilder Family Software.*

Table 43-1 lists the PORT Service parameters and commands.

Table 43-1 PORT Service Parameters and Commands

Parameters	Commands
AutoDial	SETDefault, SHow, SHowDefault
BODIncrLimit	SET, SETDefault, SHow, SHowDefault
BODTHreshold	SETDefault, SHow, SHowDefault
COMPressType	SETDefault, SHow, SHowDefault
CONFiguration	SHow, SHowDefault
CONTrol	SETDefault, SHow, SHowDefault
DefaultPriority	SETDefault, SHow
DIAGnostics	SHow
DialCONFig	SHow, SHowDefault
DialCONTrol	SETDefault, SHow, SHowDefault
DialDebouncTime	SETDefault, SHow, SHowDefault
DialHistory	SHow
DialIdleTime	SETDefault, SHow, SHowDefault
DialInitState	SETDefault, SHow, SHowDefault
DialNoList	ADD, DELete, SHow
DialRcvrState	SETDefault, SHow, SHowDefault
DialRetryCount	SETDefault, SHow, SHowDefault
DialRetryTime	SETDefault, SHow, SHowDefault
DialSamplPeriod	SETDefault, SHow, SHowDefault
DialSTatus	SHow
IfDescr	SETDefault, SHow
LinkCompStat	FLush, SHow
LogicalNET	ADD, DELete, SHow, SHowDefault, FLush
NAme	SETDefault, SHow, SHowDefault
NORMalBandwidth	SET, SETDefault
OWNer	SETDefault, SHow, SHowDefault
PAths	ADD, DELete, SHow, SHowDefault
PathPreference	ADD, DELete, SHow
ProtMacAddrFmt	SETDefault, SHow, SHowDefault
PROTocolRsrv	ADD, DELete, SHow
QueueCONTrol	SETDefault, SHow

(continued)

Table 43-1 PORT Service Parameters and Commands (continued)

Parameters	Commands
QueueInterleave	SETDefault, SHow, SHowDefault
QueuePATtern	SHow
QueuePriority	SHow
QueueStatistics	FLush, SHow
QueueThrottle	SETDefault, SHow, SHowDefault
VirtualPort	ADD, DELete, SHow, SHowDefault
WEProfileList	ADD. DE:ete. SHow

AutoDial

Syntax

```
SETDefault !<port> -PORT AutoDial = Enabled | Disabled
SHow [!<port> | !*] -PORT AutoDial
SHowDefault [!<port> | !*] -PORT AutoDial
```

Default Disabled

Description The AutoDial parameter connects all dial-up paths assigned to a port as soon as these paths are available. At system startup, AutoDial is checked for each port. If it is enabled, then any dial-up lines configured for the port are connected using the preset dial numbers.

Dialing begins as soon as AutoDial is enabled or when the system boots. If a call is on the line when AutoDial is enabled, it is terminated, except for calls going through ports configured for dial-on-demand (DOD) mode.

BODIncrLimit

Syntax

```
SETDefault !<port> -PORT BODIncrLimit = <kbps> (>=0)
SHow [!<port> | !*] -PORT BODIncrLimit
SHowDefault [!<port> | !*] -PORT BODIncrLimit
```

Default 0

Description The BODIncrLimit parameter limits the path resources a port may use for handling traffic congestion. The port can add path resources until it is at or above the specified incremental limit.

This parameter enables bandwidth-on-demand (BOD) and specifies the bandwidth levels that can be *incrementally* allocated for a port above the normal bandwidth specification for all serial lines being used by a port.

When a positive value is specified with the NORMalBandwidth parameter, and the current port bandwidth meets or exceeds the bandwidth specified, the BOD algorithm is activated to monitor traffic. The bandwidth manager can allocate additional bandwidth up to the limit specified by the BODIncrLimit parameter.

This parameter affects only system bandwidth management settings.

Values kbps Specifies the value for the BOD increment limit in kilobits per second.

The default value is 0, which disables the BOD algorithm. A positive value enables the BOD algorithm for configurations using system bandwidth management.

BODTHreshold

Syntax

```
SETDefault !<port> -PORT BODTHreshold = <%>(0–100)
SHow [!<port> | !*] -PORT BODTHreshold
SHowDefault [!<port> | !*] -PORT BODTHreshold
```

Default 100

Description The BODTHreshold parameter controls when an additional dial path configured for bandwidth-on-demand (BOD) comes up or goes down. The trigger-up and trigger-down mechanisms are based on a percentage of the outgoing traffic rate. The mechanism is triggered up when the outgoing traffic rate exceeds the percentage of the port bandwidth specified by BODTHreshold during the first sample period specified with the DialSamplPeriod parameter. The mechanism is triggered down when the rate of traffic runs below the specified percentage of the port bandwidth during the second sample period set in the DialSamplPeriod parameter.

For example, assume NORMalBandwidth is set to 64 kbps, BODIncrLimit is set to 128 kbps, BODTHreshold is set to 50 percent, and the DialSamplPeriod parameter command specifies two sample periods at 30 and 60 seconds. With this configuration, the BOD algorithm is triggered on when traffic exceeds 32 kbps for 30 seconds. When traffic returns to less than 32 kbps for longer than 60 seconds, the BOD algorithm is triggered off.

Changes to this parameter take effect immediately.

COMPressType

Syntax

```
SETDefault !<port> -PORT COMPressType = NONE | HIStory | PerPacket
SHow [!<port> | !*] -PORT COMPressType
SHowDefault [!<port> | !*] -PORT COMPressType
```

Default NONE

Description The COMPressType parameter defines the type of data compression performed on the port.

Values

NONE | HIStory | PerPacket	The NONE value indicates that compression is not enabled. The HIStory value indicates that packets are compressed using a link-level history-based algorithm. The PerPacket value flushes the history buffer before each packet is compressed, and each packet is compressed individually. When a compression type is selected for a port, that type is enabled for all paths and virtual circuits associated with the port. For information on history-based and per-packet link-level compression algorithms, refer to Chapter 39 in *Using NETBuilder Family Software*.

LAPB cannot run on WAN Extender connections. If HIStory-based compression is selected, no HIStory-based compression occurs. Only PerPacket compression can be used on the WAN Extender links.

CONFiguration

Syntax

```
SHow [!<port> | !*] -PORT CONFiguration
SHowDefault [!<port> | !*] -PORT CONFiguration
```

Default No default

Description The CONFiguration parameter displays configuration information for each port, virtual port, or group port. The display includes port number and name, some CONTrol parameter values (Enabled and Disabled states and Boundary Routing status), state, owner of the port (indicating the protocol running on the path), and path corresponding to the port.

A physical path that has been designated for dial-up and a WAN Extender dial-up or channelized virtual path that was bound to a port upon establishing a connection (State is UP) shows SCID “SysCallerID” in the Paths column if a text string is being used to identify the remote site. The Paths column shows SCID “SysCallerID” for both ISDN and non-ISDN.

To display active configuration information, enter:

`SHow -PORT CONFiguration`

To display configuration information on disk, enter:

`SHowDefault -PORT CONFiguration`

Examples The following is a sample display generated by entering:

`SHow -PORT CONFiguration`

```
..................Current Port Parameters.................
Port  Name     Ctrl      State Owner      Bandwidt  Paths
                                            h
1     Port_1  Ena       Up    ETH        10000     1
2     Port_2  Ena       Up    TOK        4000      2
3     Port_3  Ena       Up    Auto (PPP) 192       3
4     Port_4  Ena       Dwn   WE         4096      4
V1    Port_V1 Ena       Up    FRM        64        4@21
V2    Port_V2 Ena       Up    PPP        128       SCID”SanDiego”
V3    Port_V3 Ena       Up    PPP        128       v1v2SCID”NewYork
                                                   ”
V4    Port_V4 Ena       Up    PPP        128       v3v4SCID“SanJose
                                                   ”
V5    Port_V5 Ena       Up    ETH        64        1%080002031234
```

The following is a sample display generated by entering:

`SHowDefault -PORT CONFiguration`

```
..................Saved Port Parameters.................
Port   Name      Ctrl           State   Owner  Paths
1      Port_1    Ena            Up      ETH    1
2      Port_2    Ena            Up      TOK    2
3      Port_3    Ena            Up      Auto   3
4      Port_4    Ena            Dwn     WE     4
V1     Port_V1   Ena            Up      FRM    4@21
V2     Port_V2   Ena            Up      PPP    SCID”SanDiego”
V3     Port_V3   Ena            Up      PPP    v1v2SCID”NewYork”
V4     Port_V4   Ena            Up      PPP    v3v4SCID“SanJose”
V5     Port_V5   Ena            Up      ETH    1%080002031234
```

State refers to the state of the port. The following are possible states:

Up The port is operational.

Dis The port has been disabled.

Dwn The port has been enabled but is not operational. When a cable is attached to a line network or data link layer protocol negotiation is successful, the state goes from Dwn to Up.

Owner indicates the protocol running over the path mapped to the port. The following are possible owners:

ETH	Ethernet
TOK	Token ring
FDDI	Fiber Distributed Data Interface (FDDI)
PPP	Point-to-Point Protocol (PPP)
PLG	3Com's proprietary protocol, Phone Line Gateway (PLG)
FRM	Frame Relay
BSC	Binary Synchronous Communications
ATUN	Asynchronous (asynch) communications
SHDLC	Synchronous Data Link Control (SDLC) or High-Level Data Link Control (HDLC)
SMDS	Switched Multimegabit Data Service (SMDS)
X25	X.25 Protocol
WE	WAN Extender. Owner of physical ports only.
SDLC	Synchronous Data Link Control
ATM	Asynchronous Transfer Mode
LoopBack	Loopback testing
Auto	The path mapped to the port is a high-speed serial (HSS) path. The software automatically determines the port owner. Possible owners include PPP and Frame Relay.

For the active configuration information, the current bandwidth capability of each port is displayed.

CONTrol

Syntax

```
SETDefault !<port> -PORT CONTrol = Enabled | Disabled
SHow [!<port> | !*] -PORT CONTrol
SHowDefault [!<port> | !*] -PORT CONTrol
```

Default Enabled

Description The CONTrol parameter enables or disables a port on the bridge/router, including virtual ports and group ports.

DefaultPriority

Syntax

```
SETDefault -PORT DefaultPriority = High | Medium | Low
SHow -PORT DefaultPriority
```

Default Medium

Description The DefaultPriority parameter determines the priority of an unprioritized packet destined for a wide area network using PPP, PLG, Frame Relay, or SMDS. A packet is considered unprioritized if any of the following conditions are met:

- It does not have a system-assigned priority.
- You retain the default setting or set the -LLC2 TUNnelPRiority or -IP QueuePriority parameter to Default.
- You did not set up a mask and prioritization policy for a particular type of packet.

For information on prioritizing data, refer to Chapter 41 of *Using NETBuilder Family Software*.

Values

High | Medium | Low	Specifies that the priority of an unprioritized packet is either High, Medium, or Low.

DIAGnostics

Syntax

```
SHow [!<port> | !*] -PORT DIAGnostics
```

Default No default

Description The DIAGnostics parameter monitors auto-owner detection. If the owner has been manually configured to a value other than Auto for a port, this parameter does not display information for that port. This parameter also displays information related to smart filtering in a Boundary Routing environment.

If auto-owner detection is operating and you enter the following command, the owner is shown as Auto:

```
SHowDefault -PORT OWNer
```

The owner is shown as Trying <owner> or Detected <owner> if you enter:

```
SHow -PORT OWNer
```

or

```
SHow -PORT CONFiguration
```

The Trying syntax indicates that auto-owner detection is trying the owner. The Detected syntax indicates that auto owner has detected the owner.

If multiple paths are assigned to a port, auto-owner detection tries PPP, but not Frame Relay.

DialCONFig

Syntax

```
SHow [!<port>] -PORT DialCONFig
SHowDefault [!<port>] -PORT DialCONFig
```

Default No default

Description The DialCONFig parameter generates a display in two parts: one part shows the configured values for the PORT Service parameters and the other part shows the configured values for the PATH Service parameters.

The SHow command displays all runtime configuration values, including the current port bandwidth in kbps and the percentage of bandwidth utilization. The SHowDefault command shows the configuration file values.

The following list explains the information in the Port portion of the display:

Port Indicates the port number.

State Indicates the packet-per-minute (PPM) state of the port.

DIS Indicates the dial-initiator state, dial-on-demand (DOD) or manual dial (MD).

DRS Indicates the dial-receiver state, either answer (ANS) or no answer (NOANS).

DR A Yes or No indicates whether or not disaster recovery is configured.

NORMB Indicates the NORMalBandwidth parameter setting configured.

BODIL Indicates the BOD increment limit configured.

BODTH% Indicates the BOD threshold configured.

CurB Indicates the current total port bandwidth (SHow command only).

CurUtil% Indicates the current total percentage of bandwidth utilization configured. The total bandwidth utilization is equal to the traffic rate divided by port bandwidth (SHow command only).

The following list explains the information in the Path portion of the display:

Port Indicates the port number.

State Indicates the bandwidth manager state of the path.

Baud Indicates the baud rate configured for the path.

Dial Control Config Indicates the DialCONTrol parameters set for the path; see Table 43-2 for the valid parameters.

Dial String Lists the numbers entered in the dial number list with the DialNoList parameter.

Table 43-2 Valid Settings Displayed in the Dial Control Config Column

Parameter	Description
Leased	Indicates a WAN Extender virtual path used as a leased channelized connection. Leased only appears after the NETBuilder II bridge/router synchronizes with the WAN Extender.
Dialup	Indicates the physical dial path or WAN Extender virtual path is set to Dialup.
NDr	Indicates the physical dial path or virtual path is set to NoDisasterRcvry.
Dr	Indicates the physical dial path or virtual path is set to DisasterRcvry.
Unrst	Indicates the physical dial path or virtual path is set to UnReSTricted.
Sta	Indicates the physical dial path is set to Static.
Dyn	Indicates the physical dial path or WAN Extender virtual path is set to Dynamic.
Ans	Indicates the physical dial path or WAN Extender virtual path is set to Answer mode.
NoAns	Indicates the physical dial path or WAN Extender virtual path is set to NoAnswer mode.
Orig	Indicates the physical dial path or WAN Extender virtual path is set to Originate mode.
NoOrig	Indicates the physical dial path or WAN Extender virtual path is set to NoOriginate mode.

Other displays indicate when DialPool and WAN Extender are configured. The path label indicates the caller ID. The dial number list path preference list are also shown.

DialCONTrol

Syntax

```
SETDefault !<port> -PORT DialCONTrol = ([DisasterRcvry |
  NoDisasterRcvry])
SHow [!<port> | !*] -PORT DialCONTrol
SHowDefault [!<port> | !*] -PORT DialCONTrol
```

Default NoDisasterRcvry

Description The DialCONTrol parameter controls port attributes for a dial-up port in the event the bandwidth set for a leased line drops below what has been set as the normal bandwidth.

Values

DisasterRcvry | The DisasterRcvry value searches for a DisasterRcvryOnly dial path to back up the failed leased line path when a line path failure drops the port bandwidth below the normal bandwidth setting. If there is no DisasterRcvry dial path available, it searches for an UnReSTricted dial path to use.

NoDisasterRcvry If the NoDisasterRcvry value is selected under system bandwidth management, the bandwidth manager searches for an UnReSTricted or NoDisasterRcvry dial path when a leased line drops the port bandwidth to below the Normal setting to bring the port back to the defined bandwidth.

If the NoDisasterRcvry value is selected under manual bandwidth management while the dial path is under control of the bandwidth manager, no action is taken when a leased line drops the port bandwidth to below the Normal bandwidth setting, unless the port was manually dialed. If the DisasterRcvry option is selected, the bandwidth manager searches first for a DisasterRcvry-only line, then an UnReSTricted dial path to bring the port back to the NORMalBandwidth parameter setting.

If the user dialed the port manually, the port is under bandwidth management control. A dropped line causes bandwidth management to add more paths to meet the bandwidth target.

DialDebouncTime

Syntax

```
SETDefault !<port> -PORT DialDebouncTime = <seconds>, <seconds> (0–3600)
SHow [!<port> | !*] -PORT DialDebouncTime
SHowDefault [!<port> | !*] -PORT DialDebouncTime
```

Default 30, 30

Description The DialDebouncTime parameter sets the elapsed time (in seconds) to wait after the dial path is disconnected or connected before the additional dial-up path is connected or disconnected. This parameter is used only for disaster recovery.

The first value is the time in seconds the dial path must remain disconnected before the additional path is connected. The second value is the time in seconds the dial path must remain connected before the additional path is disconnected.

DialHistory

Syntax

```
SHow -PORT DialHistory
```

Default No default

Description The DialHistory parameter displays a time-stamped dial history for all ports. The information in the display can be used for troubleshooting purposes.

DialIdleTime

Syntax

```
SETDefault !<port> -PORT DialIdleTime = <seconds> (0–3600)
SHow [!<port> | !*] -PORT DialIdleTime
SHowDefault [!<port> | !*] -PORT DialIdleTime
```

Default 180

Description The DialIdleTime parameter sets the time in seconds before all dial-up lines in a port are disconnected if the port is not in use. If the DIal command has been given and no packets are transmitted or received on the port during the idle period, all dial lines of the port are disconnected.

If DialIdleTime is set to zero, all dial-up lines remain connected regardless of traffic on the port. Use the HangUp command to disconnect the port manually.

For bandwidth-on-demand, use the sample periods to specify the congestion alleviation criteria that disconnect the dial-up paths.

DialInitState

Syntax

```
SETDefault !<port> -PORT DialInitState = NoDialOut | ManualDial |
  DialOnDemand
SHow [!<port> | !*] -PORT DialInitState
SHowDefault [!<port> | !*] -PORT DialInitState
```

Default ManualDial

Description The DialInitState parameter determines which bandwidth management mode (system or manual) is enabled, and sets the call-initiator dial control state for the port. Once a state is set, you must re-enable the port for it to take effect.

Values

NoDialOut Indicates the local bridge/router cannot initiate calls.

ManualDial Enables manual bandwidth management mode where you define specific bandwidth requirements. The local bridge/router can initiate calls by the user invoking the DIal command any time during operation and can bring up the dial-up lines when the AutoDial parameter is enabled. If DialIdleTime is nonzero, a manual dial idle timer starts when the DIal command brings up the line. If there is no traffic on the port and the timer expires, all the dial lines of the port automatically go down. If DialIdleTime is zero, the idle timer does not run, and all the dial lines of the port remain up until a HangUp command is issued or the lines are disconnected by the remote system.

DialOnDemand Enables system bandwidth-management mode. Enough dial lines to reach normal bandwidth are initially brought up, then taken down and brought up automatically by the system based on traffic demand. A DOD idle timer runs according to the value in DialIdleTime. If there is no traffic on the port and the timer expires, all dial lines on the port go down. New traffic on the port brings the lines up again.

DialNoList

Syntax

```
ADD !<port> -PORT DialNoList “<phone no>" [Baud = <rate>
  (1.2–16000)] [Type = Modem | Bri | Sw56 | WE | WEH0][Pos =
  <number>]
DELete !<port> -PORT DialNoList "<dial stream>"
SHow [!<port> | !*] -PORT DialNoList
```

Default No default (the DialNoList is empty)

Description The DialNoList parameter adds, deletes, edits, and displays a list of phone numbers with their associated attributes (baud rate, phone number, and position in the list).

A port chooses a phone number from its dial number list, and then tries to find a path that can use that phone number. Because different types of external devices can be connected to a path, a phone number is valid only for a particular phone technology. For example, Integrated Services Digital Network (ISDN) numbers normally cannot be used on the analog public telephone network in the United States. The -PATH ExDevType parameter indicates the accessible technology of a path.

Make sure you configure the external device type for all DTE paths available for dialing. The default for the -PATH ExDevType parameter is Modem, and the default type for the phone number is also modem. However, if you attach a path to this port through the path preference list, the software uses this path based on the external device type as the new port default.

With static or dynamic port and path bindings, the software uses the phone numbers from the dial number list first. If the highest prioritized phone number is not available, the software tries the next phone number configured for the port, if any.

If no phone number is available for the port or no phone numbers are configured in the dial number list, the call attempt fails.

To append a phone number to the list, use:

```
ADD !<port> -PORT DialNoList “<phone no>”
```

By using the Baud, Type, and Pos keywords, you can specify the baud rate, device type, and position in the list; otherwise, default values are used. You can edit an existing number in the list to give it different baud rate, type, or position, but you cannot change the phone number. To change a phone number, delete the entry and then add the new number.

When you specify a position, the phone number is inserted at the specified place.

If you delete a phone number from the list while it is being dialed, the call is completed; however, the number will not be available for any subsequent calls.

Values

<phone no> Specifies a phone number for all device types except WE and WEHO. For V.25 bis dialing, the phone number can include the dial prefix, country code, and area code, which are sent to the modem. You can configure up to 16 phone numbers per port.

If you specify WE or WEH0 as the Type value, the value entered for <phone no> is actually the NETBuilder II system port number to which the WAN Extender is connected and the WAN Extender remote site's profile ID. (The remote site's profile has the remote site's phone number.)

For DTR dialing, the dial number list is not needed, since the outgoing telephone number is stored in the modem.

For ISDN dialing, the phone number usually includes the dial prefix, country code, area code, and possibly a subaddress assigned to your ISDN interface. If you specify a subaddress, you must separate the phone number from the subaddress with a semicolon (;). With ISDN phone numbers, you can use hyphens (-) to separate the prefix, country code, and area code.

Baud Specifies the baud rate. Acceptable values range from 1.2 to 16,000 kbps. The default baud rate is 9.6 kbps if the device type is Modem, 64 kbps if the device type is Bri, 56 kbps if the device type is Sw56, 64 kbps if the device type is WE, and 384 kbps if the device type is WEH0. It is important that the path and dial number list baud rate match.

Type Specifies the switch type. If all paths in the dial pool have the -PATH ExDevType parameter set to Modem, the default type is Modem. If all paths in the dial pool have the -PATH ExDevType parameter set to Bri, the default type is Bri. If the -PATH ExDevType parameter for the paths in the dial pool is a mixture of Modem and Bri, the default type is Modem.

Sw56 Specifies Switch 56 with 56 kbps virtual paths to be used for terminal adapters or channel service unit/digital service unit (CSU/DSU) switched-56 modems.

WE Specifies that WAN Extender 64 kbps virtual paths are used to make a call. After a connection is established, the actual baud rate is determined and displayed. If you specify WE as the Type value, the value entered for <phone no> is the NETBuilder II system port number to which the WAN Extender is connected and the WAN Extender remote site's profile ID. (The remote site's profile has the remote site's phone number.)

For more information, refer to Chapter 36 in *Using NETBuilder Family Software*, the *WAN Extender 2T/2E Installation Guide*, and the *WAN Extender Manager User's Guide*.

WEH0 Specifies that WAN Extender 384 kbps virtual paths are used to make a call. If you specify WEH0 as the Type value, the value entered for <phone no) is the NETBuilder II system port number that the WAN Extender is connected to and the WAN Extender remote site's profile ID. (The remote site's profile has the remote site's phone number.)

For more information about WEH0, refer to Chapter 36 in *Using NETBuilder Family Software*, the *WAN Extender 2T/2E Installation Guide*, and the *WAN Extender Manager User's Guide*.

Pos Specifies the position of the phone number in the dial numbers list. If a position is specified, the phone number is inserted at that position. If the list is smaller than the specified position, the phone number is appended to the end of the list. If no position is specified, the phone number is appended to the end of the list.

DialRcvrState

Syntax

```
SETDefault !<port> -PORT DialRcvrState = NoAnswer | Answer
SHow [!<port> | !*] -PORT DialRcvrState
SHowDefault [!<port> | !*] -PORT DialRcvrState
```

Default Answer

Description The DialRcvrState parameter determines whether the port answers calls. Once the parameter value is set, you must re-enable the port for it to take effect.

Values NoAnswer Specifies that the bridge/router does not answer calls.

Answer Specifies that the bridge/router is prepared to answer calls.

DialRetryCount

Syntax

```
SETDefault !<port> -PORT DialRetryCount = <number> (0–20)
SHow [!<port> | !*] -PORT DialRetryCount
SHowDefault [!<port> | !*] -PORT DialRetryCount
```

Default 9

Description The DialRetryCount parameter specifies the number of times to retry the call if the call attempt fails. If this parameter is 0, the call is not retried.

If dialing is based on a static port and path binding, the software first tries to make the call. If the attempt fails to bring the path up, the software tries the call again using the same or different path. It may try the same phone number as on the first attempt or dial another number configured through the -PORT DialNoList parameter. Depending on the error code, other phone numbers may be tried. The call attempts continue until the dial retry count is reached.

The software can also try different phone numbers specified in the phone list through the -PORT DialNoList parameter. The call attempts continue until the dial retry count is reached. If the retry count is too low, not all phone numbers and paths in the dial pool are tried. If the retry count is too high, the software may cycle through phone numbers or paths more than once.

The internal retry counter is reset to zero if the call is connected successfully, the -PORT DialRetryCount parameter is modified, or a user issues a DIal command. These actions restart call attempts. A disable command followed by an enable command also resets the internal counter.

DialRetryTime

Syntax

```
SETDefault !<port> -PORT DialRetryTime = <seconds> (5–120)
SHow [!<port> | !*] -PORT DialRetryTime
SHowDefault [!<port> | !*] -PORT DialRetryTime
```

Default 30

Description The DialRetryTime parameter sets the initial time (in seconds) to wait before attempting to reconnect after a connection has failed because a carrier was not detected, or the path did not come up. After each attempt fails, a random number between 0 and 45 seconds is added or subtracted from the DialRetryTime value for the next connection attempt, until the number of attempts reaches the DialRetryCount value. This action is taken to prevent multiple call collisions.

For the NTT switch type, the DialRetryTime parameter defaults to 60 seconds. 0 to 5 seconds is added or subtracted for the next connection attempt.

Example The following command sets the DialRetryTime parameter to 60 seconds. If the first call attempt fails, the initial value is increased or decreased by 0 to 45 seconds and the call attempt is repeated:

```
SETDefault !4 -PORT DialRetryTime = 60
```

DialSamplPeriod

Syntax

```
SETDefault !<port> -PORT DialSamplPeriod = <seconds>, <seconds>
  (0–300)
SHow [!<port> | !*] -PORT DialSamplPeriod
SHowDefault [!<port> | !*] -PORT DialSamplPeriod
```

Default 0, 60

Description The DialSamplPeriod parameter sets the time (in seconds) to sample before taking an action to bring paths up or down, based on traffic load for bandwidth-on-demand.

The first sample time determines when to bring up additional dial paths; the second sample time determines when to bring down this additional path. If traffic for the duration of the first sample time exceeds the threshold set by the -PORT BODTHreshold parameter for the port, the additional paths are connected to alleviate traffic congestion. If traffic for the duration of the second sample time falls below the threshold set by the -PORT BODTHreshold parameter for the port, the additional paths are disconnected to remove excess capacity.

DialSTatus

Syntax `SHow [!<port> | !*] -PORT DialSTatus`

Default No default

Description The DialSTatus parameter shows the current status and dial path status information for the specified dial port or for all dial ports. A message is displayed for each port describing its state under the bandwidth manager. The display includes the path number and its state (up, down, or disabled). If the port is to be used for an outgoing call, the dial string (phone number) is displayed. This parameter also displays port-level dial diagnostic messages that can be used for troubleshooting disaster recovery and BOD configurations.

The following information is displayed in the port bandwidth and utilization display:

CurB The current total port bandwidth.

CurUtil% The current total percentage of bandwidth utilization configured. The total bandwidth utilization is equal to the traffic rate divided by CurB.

The following information is displayed for each path bound to the port:

Path The path number. The path number appears for WAN Extender virtual paths only if the path is up.

State The bandwidth manager path state. See Table 43-3 on page 43-14 for path state messages shown in the DialStatus display.

Baud The path bandwidth as reported by the system. If the path is not up or the driver cannot report the bandwidth, the runtime configuration value is reported instead.

Dial Ctrl The path's runtime DialCONTrol setting.

Dial String The dial string used on the path. If the path is a WAN Extender virtual path and the path is up, the network port is shown.

Table 43-3 lists the dial-on-demand messages shown in the DialSTatus display.

Table 43-3 Dial-on-Demand DialSTatus Messages

Message
`Port is down, no bandwidth.`
`Port is coming down.`

`Port is coming up.`
`If dead again timer is on: Port is down, Max retry count has exceeded, wait 1 hour.`

`Port is Up for the first time.`
`Port is Up, but NORMalBandwidth requirement has not been met yet.`
`Port is Up, NORMalBandwidth is met.`
`Port is Up, but dial paths are idling out.`
`Port is Up but dial paths are Down, monitoring traffic to bring up dial paths.`

Table 43-4 lists the manual dial messages shown in the DialSTatus display.

Table 43-4 Manual Dial DialSTatus Message

Message
`Port is down, no bandwidth.`

`Port is coming up.`
`If dead again timer is on: Port is down, Max retry count has exceeded, wait 1 hour.`

`Port is Up, but NORMalBandwidth requirement has not been met yet.`
`Port is Up, NORMalBandwidth is met.`
`Port is Up, leased line paths are up but dial paths have idled out.`

Table 43-5 lists the disaster recovery messages shown in the DialSTatus display.

Table 43-5 Disaster Recovery DialSTatus Messages

Situation	Message
Disaster recovery is disabled.	No message.
Disaster recovery is enabled but port has no leased line path configured.	No message
Disaster recovery is enabled; all leased lines paths are up.	`Leased lines are Up`
Disaster recovery is enabled, the port has a leased line path down, and the current bandwidth is less than that specified for NORMalBandwidth.	`Leased lines are Down, NORMBandwidth is not met`
Disaster recovery is enabled, the port has a leased line path down, and the current bandwidth is greater than or equal to that specified for NORMalBandwidth.	`Leased lines are Down, but NORMBandwidth is met`

Table 43-6 lists the bandwidth-on-demand messages shown in the DialSTatus display.

Table 43-6 Bandwidth-on-Demand DialSTatus Messages

Bandwidth Situation	Message
UI BODincrLiMit = 0 or MD mode	No message.
Port down or current bandwidth is less than normal.	`Congestion monitoring disabled.`
Current bandwidth is normal.	`No BOD bandwidth applied. Monitoring for congestion.`
Current bandwidth is above normal with no congestion.	`BOD bandwidth is applied. Monitoring for congestion.`
Congestion detected, but first sample timer has not expired.	`Congestion detected. Monitoring for persistent congestion.`
Current bandwidth is at the maximum limit (Normal + BODincrLiMit).	`Congestion detected. Cannot allocate additional bandwidth.`
Excess bandwidth capacity, but the second sample timer has not expired.	`Excess bandwidth capacity detected. Monitoring for persistent excess capacity.`
BOD algorithm has taken action to add or subtract bandwidth, but the action has not yet completed.	`BOD bandwidth being updated. Waiting for BOD bandwidth update to complete.`

IfDescr

Syntax

```
SETDefault !<port> -PORT IfDescr = "<string>>”
SHow [!<port> | !*] -PORT IfDescr
```

Default Depends on the type of port

Description The IfDescr parameter describes a port by assigning a value to the Simple Network Management Protocol (SNMP) management information base (MIB) object IfDescr. You can enter your own customized value or use the default value, which is generated by the software based on the type of port. The string is limited to ASCII characters and can be no longer than 255 characters.

You can remove the customized value and revert to the software-generated value by entering a zero-length string.

LinkCompStat

Syntax

```
FLush !<port> -PORT LinkCompStat
SHow [!<port> | !*] -PORT LinkCompStat
```

Default No default

Description The LinkCompStat parameter displays the total number of bytes transferred across the link when data compression is used. Error counts, compression ratio, and number of raw and compressed bytes are displayed. This parameter also allows you to flush link compression statistics.

LogicalNET

Syntax

```
ADD !<port> -PORT LogicalNET ETHernet <port> [,…]["<string>"
  (1–50 characters)]
DELete !<port> -PORT LogicalNET <port> [,…] | ALL
FLush -PORT LogicalNET STATistics
SHow [!<port>] -PORT LogicalNET [CONFiguration] | DIAGnostics]
SHow -PORT LogicalNET STATistics
SHowDefault [!<port>] -PORT LogicalNET [CONFiguration]
```

Default No default

Description The LogicalNET parameter adds ports to a port group (logical network), deletes ports from a port group, and shows the current configuration, diagnostics, and statistics. Deleting the last port in a port group, or deleting all ports in a port group, removes the port group.

Port groups cannot overlap: the same port cannot be configured as part of two different port groups.

Values

<port>	Specifies the group port that interfaces to the logical network. Its number also identifies the port group. This port is always numbered as if it were a virtual port (V*n*), but it cannot be an existing virtual port.
ETHernet	Identifies the media type. Only Ethernet is support for version 8.2.
<port> [,…]	The ports assigned to the port group. These ports are called member ports. They cannot be virtual ports.

CONFiguration Shows the current port group configuration.

DIAGnostics Shows diagnostic information to help in configuration or with connectivity problems. The display includes the group's primary port and MAC address. The primary port is the logical connection between the multiple logical network (MLN) external routing function and its internal bridging function. The primary port is configured automatically, and is usually the lowest numbered member port that is in the Up state.

The group port MAC address is the one to which packets for the port group must be addressed. It is also configured automatically, and is usually the MAC address of the lowest numbered available member port (the port does not have to be up). The primary port and the port used to configure the MAC address can be different from each other and can change dynamically.

STATistics Shows activity on the group port and member ports.

"<string>" Specifies an optional descriptive name you can attach to the port group. The description is shown as part of the port group configuration display.

NAme

Syntax

```
SETDefault !<port> -PORT NAme = "<string>"
SHow [!<port> | !*] -PORT NAme
SHowDefault [!<port> | !*] -PORT NAme
```

Default Port_n (where n is the port number; for example, Port_1, Port_2, Port_3, Port_4)

Description The NAme parameter assigns a name to a port, virtual port, or group port, subject to the following restrictions:

- The name string can contain a maximum of eight characters, the first of which must be alphabetic.
- No blank spaces are allowed. The only non-alphanumeric characters allowed are the asterisk (*), underscore (_), period (.), and hyphen (-).
- Two ports cannot have the same name, but a port name can be the same as an existing path name.
- Alphabetic characters are stored and displayed as entered. Names are case-insensitive when compared on entry with previously entered names. For example, port2 and PORT2 are evaluated as the same name.

After you assign a name to a port, you can use the name as an instance identifier in subsequent commands, replacing the <port> value.

NORMalBandwidth

Syntax

```
SETDefault !<port> -PORT NORMalBandwidth = <kbps> (>=0)
```

Default There is no default set for this parameter in the configuration file. If no values are specified, the system determines a runtime default (see Table 43-7).

Table 43-7 Runtime Default Bandwidth Settings

Paths in Port	Setting
Only dynamic dial paths	64 kbps
Static dial path without leased line path	Baud rate of the highest preferred static dial path in the path preference list
Leased line path and static dial path	Total baud rate of the leased line paths
Leased line paths only	Total baud rate of the leased line paths

Description The NORMalBandwidth parameter specifies the amount of bandwidth the port will bring up when it is enabled (system bandwidth management mode) or when the port is dialed (manual bandwidth management mode).

This parameter indicates the normal operating bandwidth for the port to be operating at if there are no path failures or traffic congestion. The value specified for the NORMalBandwidth parameter can be met with a combination of leased and dial lines, or static and dynamic lines. A port uses the dial paths available to it to achieve and maintain the specified normal bandwidth.

The value expressed for NORMalBandwidth can be set to a smaller or larger value than the aggregated leased line bandwidth. If the exact amount of bandwidth cannot be brought up for the port, the bandwidth manager tries to bring up additional, not less, bandwidth.

Under system bandwidth management, if the NORMalBandwidth parameter is set to a value *larger* than the port's current bandwidth capability, the system attempts to simultaneously bring up a bundle of lines to meet the normal bandwidth specification. When the port reaches the normal bandwidth level, it continues operation based on traffic demand.

Under system bandwidth management, if the NORMalBandwidth parameter is set to a value *smaller* than a leased line's actual bandwidth capability, the system does not bring up any additional bandwidth when the port is enabled. For disaster recovery, bandwidth management only brings up backup bandwidth at the value specified for NORMalBandwidth and not the amount of the port's bandwidth capability (assuming no congestion). Setting NORMalBandwidth to a smaller value can preserve available dial path resources if backup lines are needed, especially if the leased lines have high bandwidth capability.

Under manual bandwidth management, if the value set for the NORMalBandwidth parameter is *larger* than the port's bandwidth capability, the system attempts to simultaneously bring up a bundle of lines to meet the bandwidth specification when the port is dialed. When the port reaches the bandwidth set with NORMalBandwidth, it maintains that value until the dial idle timer expires, at which time all dial path resources are brought down.

Under manual bandwidth management, if the value set for the NORMalBandwidth parameter is *smaller* than the leased line's actual bandwidth capability, the bandwidth manager only brings up backup bandwidth at the value specified for NORMalBandwidth and not the amount of the port's bandwidth capability when the leased line fails.

Values <kbps> Specifies the bandwidth value in kilobits per second.

OWNer

Syntax

```
SETDefault !<port> -PORT OWNer = ETHernet | TokenRing | FDDI |
  PPP | PLG | FrameRelay | BSC | ATUN | SHDLC | SMDS | X25 |
  WanExtender | SDLC | ATM | LoopBack | Auto
SHow [!<port>] -PORT OWNer
```

Default See Table 43-8.

Description The OWNer parameter assigns an owner to the path mapped to a port. If multiple paths are mapped to a port, then all paths have the same owner.

The SETDefault syntax shows a superset of all options for all bridge/router models. The specific options available depend on the bridge/router model used.

On power-up, the default port owner is determined by the hardware platform you have and whether the port is a LAN or WAN port. See Table 43-8 to determine the default owner for each port.

Table 43-8 Default Port Owner

Bridge/Router	Default Owner for LAN Ports	Default Owner for WAN Ports
NETBuilder II bridge/router	Depends on I/O module. If Ethernet, Ethernet is default owner; if Token Ring, Token Ring is default owner.	PPP If an ATM module is installed, ATM is the default owner.
SuperStack II NETBuilder bridge/router model 2xx	Ethernet	Auto
SuperStack II NETBuilder bridge/router model 32x	Token Ring	Auto
SuperStack II NETBuilder bridge/router model 42x	Ethernet	Auto for DTE serial ports; PPP for ISDN ports
SuperStack II NETBuilder bridge/router model 52x	Token Ring	Auto for serial ports; PPP for ISDN ports

If you have a NETBuilder II bridge/router, before entering the SETDefault !<port> -PORT OWNer syntax, confirm that an appropriate interface card is inserted in the path slot mapped to the port. The value takes effect immediately only if it matches the board type in the chassis. If the value does not match the board, the value is saved to disk.

Values

ETHernet	Specifies Ethernet as port owner.
TokenRing	Specifies token ring as port owner.
FDDI	Specifies Fiber Distributed Data Interface (FDDI) as port owner.
PPP	Specifies Point-to-Point Protocol (PPP) as port owner.
PLG	Specifies 3Com's proprietary protocol, Phone Line Gateway (PLG) as port owner.
FrameRelay	Specifies Frame Relay as port owner.
BSC	Specifies Binary Synchronous Communications (BSC) as port owner. The BSC value applies only to certain SuperStack II NETBuilder models. A port may run BSC only if the port is mapped to a single path.
ATUN	Specifies asynch tunneling as port owner. The ATUN value applies only to certain SuperStack II NETBuilder models. A port may run ATUN only if the port is mapped to a single path.

SHDLC Specifies SHDLC as port owner. SHDLC is a feature that enables bridge/routers to tunnel Synchronous Data Link Control (SDLC) or High-Level Data Link Control (HDLC) frames across IP networks by using DLSw.

SMDS Specifies Switched Multimegabit Data Service (SMDS) as port owner.

X25 Specifies X.25 Protocol as port owner.

WanExtender Specifies WAN Extender as port owner. Select WAN Extender as port owner if the port is tied to a physical path to which the WAN Extender is connected. This port remains in a down state to prevent misuse by upper layer protocols.

For more information about WAN Extender, refer to Chapter 36 in *Using NETBuilder Family Software*, the *WAN Extender 2T/2E Installation Guide*, and the *WAN Extender Manager User's Guide*.

SDLC Specifies SDLC as port owner. This value applies to the NETBuilder II bridge/router and SuperStack II NETBuilder bridge/router as follows:

A port may run SDLC only if the port is mapped to a single path. SDLC supports only leased lines for this release. The -PATH LineType parameter must be set to leased. OWNer cannot be set to SDLC on a port whose line type is set to Auto or Dial.

On the NETBuilder II bridge/router, SDLC may be used only on HDWAN ports and cannot be configured on other port types.

On the SuperStack II NETBuilder bridge/router, SDLC may be used only on WAN serial ports and cannot be configured on a LAN or ISDN port.

ATM Specifies Asynchronous Transfer Mode (ATM) as the port owner. The ATM value applies only to a NETBuilder II bridge/router with an ATM module installed.

LoopBack Specifies Loopback testing.

Auto Allows automatic detection to be triggered by enabling, then disabling, the path or port. You must also explicitly configure the connector for automatic detection using the -PATH CONNector command; both commands must be set for proper operation.

This value applies to SuperStack II NETBuilder bridge/router only. The auto startup feature provides automatic PPP or Frame Relay data link recognition during the boot process.

The auto startup feature does not apply to SMDS, PLG, SDLC, ATM, and X.25 protocols. You must configure the owner manually for these protocols using:

```
SETDefault !<port> -PORT OWNer
```

The auto startup feature automatically detects modem connectivity, DTE connector type (for SuperStack II NETBuilder bridge/router models 42x only), data link connection for a port (PPP and Frame Relay only), and type of line, and enables the associated path. Detection of these elements takes place when the platform boots.

Example To assign Frame Relay as owner to port 3 on a NETBuilder II bridge/router, enter:

```
SETDefault !3 -PORT OWNer = FrameRelay
```

The preceding command takes effect only if the board in slot 3 is a high-speed serial board. If the board in slot 3 is an Ethernet board, the command does not take effect, but the value is saved to disk and is effective next time you boot the bridge/router. For information on inserting a different board, refer to the appropriate hardware documentation accompanying your NETBuilder II bridge/router.

PathPreference

Syntax *For non-ISDN interfaces*

```
ADD !<port> -PORT PathPreference <path> [,...] [Pos = <1- number>]
DELete !<port> -PORT PathPreference <path> [,...]
SHow [!<port>] | !*] -PORT PathPreference
```

For ISDN interfaces

```
ADD !<port> -PORT PathPreference <connectorID.channelID> [,…]
  [Pos = <number>]
DELete !<port> -PORT PathPreference <connectorID.channelID> [,…]
SHow [!<port> | !*] -PORT PathPreference
```

Default No default (the path preference list is empty or as set using -PORT Paths parameter)

Description For dynamic physical paths, the PathPreference parameter restricts the use of a path to only those ports that contain the path in their path list. Multiple paths can belong to a path preference list, and the port picks the first available path in order of the list. If all paths in its path preference list are busy, a port can pick a path not in the list.

For static physical paths, the PathPreference parameter specifies the priority sequence of selection for use by a port. When a static path is added to a port, it is inserted at the end of the path preference list by default. When a static path is deleted from a port, it is also automatically deleted from the list.

Leased lines cannot be included in the list because the bandwidth manager does not have a choice of bringing the line up or down. Leased-line paths are brought up when the port is enabled (by default).

The PathPreference parameter applies to only dial paths.

Values

<path> or <connectorID.channelID>	Specifies a single path or connector and B channel or multiple paths or connector and B channels (when separated by commas) that the dial port can use. By default, the paths or connector and B channels are appended to the end of the prioritized list in the order specified.
Pos	Specifies a position for the path in the path list. When specified with a nonzero number, the path at that position in the current list is deleted, and the new path is inserted at the specified position.

PAths

Syntax *For non-ISDN interfaces*

```
ADD !<port> -PORT PAths <path> [,…] | SysCallerID "<IncomingCallID>”
DELete !<port> -PORT PAths <path> [,…] | SysCallerID
  "<IncomingCallID>”
```

For ISDN interfaces

```
ADD !<port> -PORT PAths <connectorID.channelID [,…]> | SCID
  "<SysCallerID>"
DELete !<port> -PORT PAths <connectorID.channelID> [,…] | SCID
  "<SysCallerID>"
SHow [!<port> | !*] -PORT PAths
SHowDefault [!<port> | !*] -PORT PAths
```

Default Each port is mapped to the corresponding path: port 1 to path 1, port 2 to path 2, and so forth. WAN Extender virtual paths are not mapped to virtual ports.

Description The PAths parameter assigns a static path or multiple static paths to the specified port. This parameter also assigns a dial path pool, a WAN Extender dial-up virtual path, or a WAN Extender channelized virtual path to the specified port.

When a static dial path is added to a port, it is automatically inserted at the end of the list established by the PathPreference parameter.

You can display the path list (the configured path resources) for the specified port or all ports by using the SHow command.

When entering ADD or DELete for ISDN interfaces, you cannot use the <connectorID>.* wildcard syntax. You must enter commands to add a mapping to or delete a mapping from each B channel instead of one command for both B channels. For example, instead of entering:

`ADD !2 -PORT PAths 2.*…,`

you must enter:

`ADD !2 -PORT PAths 2.1…`

and

`ADD !2 -PORT PAths 2.2….`

You can configure this parameter only for a WAN port. For the ADD command to take effect, you must re-enable the associated paths using:

```
SETDefault !<path> -PATH CONTrol = Enabled
```

Adding multiple paths on a port can cause unpredictable problems if both empty and non-empty path slots are assigned to the same port. To avoid problems, make sure all path slots assigned to the port are occupied.

For troubleshooting and diagnostic purposes, the bridge/router generates system messages when a path is in loopback state. By placing your locally or remotely attached modem into loopback, you can check the integrity of the path. Refer to “SystemMessages” on page 58-16.

Values

<path> or <connectorID.channelID>

Represents an individual physical path or connector B such as a channel, leased line, or static dial path. Using a path or connector/B channel number that has already been assigned to the dynamic dial pool is not allowed.

SCID "<SysCallerID>"

Specifies a text string to identify a remote site, such as a regional office in Seattle (SCID "Seattle"). It enables the specified port to use the dynamic dial-path pool, a WAN Extender dial-up virtual path, or a WAN Extender channelized virtual path to connect with the remote site.

Only ports configured with PPP as the port owner can use the dial pool. Software searches the path preference list first then uses paths in the dial pool.

ProtMacAddrFmt

Syntax

```
SETDefault !<port> -PORT ProtMacAddrFmt = ([DefaultARP | CanonARP |
  NonCanonARP], [DefaultIPX | CanonIPX | NonCanonIPX], [DefaultXNS |
  CanonXNS | NonCanonXNS])
SHow [!<port> | !*] -PORT ProtMacAddrFmt
SHowDefault [!<port> | !*] -PORT ProtMacAddrFmt
```

Default

For token ring ports:

DefaultARP (NC), DefaultIPX (NC), DefaultXNS (NC)

For Ethernet ports, FDDI ports, and HSS ports:

DefaultARP (C), DefaultIPX (C), DefaultXNS (C)

Description

The ProtMacAddrFmt parameter sets the address format used by various protocols to match formats of systems connected to the network. When this parameter is used on NETBuilder bridge/routers, end systems on token ring networks can communicate with end systems on Ethernet or FDDI networks in a bridged environment, if the IP protocol is used between those end systems. In this environment, Address Resolution Protocol (ARP) protocol data unit (PDU) addresses are translated from noncanonical format on token ring networks to canonical format on Ethernet and FDDI networks. This translation does not occur when Internetwork Packet Exchange (IPX) or Xerox Network Systems (XNS) protocols are used in a bridged environment. All protocols (ARP, IPX, XNS) work correctly in a routed environment.

In a Boundary Routing environment where end systems on token ring networks need to communicate with end systems on Ethernet or FDDI networks, set the ARP, IPX, and XNS formats (as appropriate) to noncanonical on the WAN port of the central node.

The default values of this parameter are sufficient for most situations because the bridge/router detects the media type and performs the conversion as needed. If the default values do not work, you must set the parameter to match the address format. You usually need to do this only on token ring and serial interfaces.

When bridging over serial lines from a NETBuilder II bridge/router to a token ring bridge/router, use this parameter to modify the ARP format on the NETBuilder II bridge/router serial interface to noncanonical format.

The setting of ARP, IPX, and XNS values affects end system packets generated within the bridge/router, bridged packets, and routed packets as follows:

- ARP: End systems, bridged, routed instead of bridged, routed
- IPX: End systems, routed
- XNS: End systems, routed

IPX and XNS settings do not influence bridged packets.

Values

DefaultARP | CanonARP | NonCanonARP

The DefaultARP value sets the address format on token ring ports to noncanonical. On Ethernet ports, FDDI ports, and HSS ports, DefaultARP sets the address format to canonical.

The CanonARP value sets the address format for ARP packets to canonical.

The NonCanonARP value sets the address format for ARP packets to noncanonical.

The ARP values are used with IP bridging and IP routing.

DefaultIPX | CanonIPX | NonCanonIPX

The DefaultIPX value sets the address format to canonical on Ethernet ports, FDDI ports, and HSS ports.

The CanonIPX value sets the address format for IPX packets to canonical.

The NonCanonIPX value sets the address format for IPX packets to noncanonical.

IPX values are used with IPX routing.

DefaultXNS | CanonXNS | NonCanonXNS

The DefaultXNS value sets the address format on token ring ports to noncanonical. On Ethernet ports, FDDI ports, and HSS ports, DefaultXNS sets the address format to canonical.

The CanonXNS value sets the address format for XNS packets to canonical.

The NonCanonXNS value sets the address format for XNS packets to noncanonical.

XNS values are used with XNS routing.

Example 1 To bridge ARP packets over serial lines from a NETBuilder II bridge/router to a SuperStack II NETBuilder bridge/router, modify the ProtMacAddrFmt parameter on the NETBuilder II bridge/router port to noncanonical. For example, modify port 3 by entering:

```
SETDefault !3 -PORT ProtMacAddrFmt = NonCanonArp
```

Example 2 To route IPX packets over serial lines from a NETBuilder II bridge/router to a SuperStack II NETBuilder bridge/router, modify the ProtMacAddrFmt parameter on the NETBuilder II bridge/router port to noncanonical. For example, modify port 4 by entering:

```
SETDefault !4 -PORT ProtMacAddrFmt = NonCanonIPX
```

PROTocolRsrv

Syntax

```
ADD !<port> -PORT PROTocolRsrv <name_tag> <percentage share> (1-95)
  <name_tag> = <15-character PROTocolRsrv tag> | DLSW | DLSWPeer
  <peer_ip_address>}
DELete !<port> -PORT PROTocolRsrv <name_tag>
SHow [!<port> | !*] -PORT PROTocolRsrv
```

For WAN Extender ports:

```
ADD !<vport> -PORT PROTocolRsrv <name_tag> <percentage share> (1-95)
  <name_tag> = {<15-character PROTocolRsrv tag> | DLSW | DLSWPeer
  <peer_ip_address>}
DELete !<vport> -PORT PROTocolRsrv <name_tag>
SHow [!<vport> | !*] -PORT PROTocolRsrv
```

Default

Each port has a default queue, which has at least 5 percent of the available bandwidth that is reserved for all untagged packets.

Description

The PROTocolRsrv parameter assigns a percentage of bandwidth to designated packets transmitting from a WAN logical port (and virtual ports on a WAN Extender only) and meeting specified conditions. The packets are identified by a name tag that is selected as part of the protocol reservation configuration.

The PROTocolRsrv parameter is used as a part of the protocol reservation procedure to configure a WAN logical port with a name tag (usually a name that identifies the protocol packet type or specified condition) and its associated reserved bandwidth. After you complete this configuration and set other parameters, if the system transmits a packet that contains a matching name tag, the system provides a queue with the percentage of bandwidth reserved for its protocol type.

You configure the bandwidth reservation for particular packets (protocol reservation) with different procedures for different protocols. For example, a mnemonic filtering procedure that uses FIlter Service parameters, such as FIlter POLicy and FIlter MASK, is used to configure all bridged and IPX-routed packets. The IP fIltering procedure, which uses the IP Service parameters such as FilterAddrs, is applied to IP-routed packets.

To configure protocol reservation for DLSw packets on a WAN port that is at the end point of a DLSw tunnel, select the DLSw option and enter the percentage of bandwidth assigned to it on the -PORT PROTocolRsrv parameter.

You do not need to enter a tag because DLSw, like DLSwPeer, are reserved name tags, which means that they have built-in name tags. For DLSw, the tags indicate bandwidth reservation for all DLSw traffic.

To enter the protocol reservation for packets destined for a DLSw peer, select the DLSwPeer value, entering the allotted bandwidth and entering the peer's IP address on the -PORT PROTocolRsrv parameter. You do not need to enter a tag because DLSwPeer has a built-in tag that identifies the packets destined for the peer IP address that will receive the extra bandwidth.

To configure protocol reservation for DLSw packets on a bridge/router WAN port that forwards traffic as part of the normal IP-packet forwarding use an IP filtering procedure.

For detailed information about configuring WAN ports for protocol reservation for all protocol packet types supported, refer to Chapter 38 in *Using NETBuilder Family Software*.

In allocating bandwidth percentages be aware of the following rules:

- Each port has a default queue, which has at least 5 percent of the available bandwidth. If the total configured bandwidth percentages for the logical port exceed 95 percent, the values are balanced by the system so that the default queue still has its default allotment of 5 percent of the available bandwidth. The rest of the bandwidth is distributed among the entries configured for the port in a ratio to the percentages that were configured for each. This balancing and distribution of bandwidth is called *normalization*. Any fractional remainders that are left as a result of normalization are allotted to the default bandwidth provided for all untagged packets.
- If bandwidth percentages are configured to a general entry and an entry that is a subset of the general entry, the bandwidth allocation to the subset entry is exclusive of the general entry. For example, if 30 percent of bandwidth is reserved for all IP traffic, and 10 percent is reserved for Telnet traffic, the bandwidth reserved for the Telnet traffic is exclusive of the bandwidth allocated to the IP traffic (a total of 10 percent is reserved only for Telnet and 30 percent is reserved for all IP traffic other than Telnet).
- If the total configured bandwidth percentages are less then 95 percent, the non-allocated bandwidth is added to the default to be given to the configured protocols or for untagged traffic on a first-come first-served basis.

  For example, if you configure protocol reservation for a WAN port with the following bandwidth allocations, the remaining 25 percent of the bandwidth is added to the default to be used for SNA traffic, NetBIOS traffic, or for untagged traffic, whatever traffic needs it first:

  - 50 percent of the bandwidth for SNA traffic
  - 20 percent of the bandwidth for NetBIOS traffic
  - 5 percent is automatically set aside as default bandwidth for untagged traffic

Values

<port> Specifies the port that is assigned to reserve a particular percentage of bandwidth for the protocol that corresponds to the <name_tag> entered.

<name_tag> Specifies the name that is used by the system to identify which packets to allocate the configured bandwidth amount.

<percentage_share>(1-95) Specifies the bandwidth amount that is to be allocated in reserve to the packets with the name tag that matches the name tag that is assigned to the particular physical port by the -PORT Service ProtocolRsrv parameter.

DLSw — Indicates that all DLSw traffic will be allocated the percentage of bandwidth entered in the command. DLSw is a reserved name tag. This option applies to DLSw traffic transmitting from a WAN port that is at the end of a DLSw tunnel.

DLSwPeer — Indicates that all DLSw traffic with the designated peer IP address will receive the reserved bandwidth entered in the command. DLSwPeer is a reserved name tag. This option applies to DLSw traffic transmitting from a WAN port that is at the end of a DLSw tunnel.

<peer_ip_address> — Specifies the IP address of the DLSw peer that will receive the allocated bandwidth.

QueueCONTrol

Syntax

```
SETDefault !<port> -PORT QueueCONTrol = PriorityQueues |
  PROTocolRsrv | NOne
SHow [!<port> | !*] -PORT QueueCONTrol
SHowDefault [!<port> | !*] -PORT QueueCONTrol
```

Default PriorityQueues

Description The QueueCONTrol parameter configures queueing for each port.

Values

PriorityQueues — Specifies that each port uses priority queues to assign packets a high, medium, or low priority.

PROTocolRsrv — Specifies that queueing for the specified WAN port is set for protocol reservation. Setting -PORT QueueCONTrol to PROTocolRsrv is a step in the protocol reservation procedure that allocates a specified percentage of bandwidth for designated packet types transmitting through a designated WAN port and meeting specified conditions.

The tag to identify the packet types and the percentage of reserved bandwidth is set through the -PORT PROTocolRsrv parameter described in this chapter. The procedures to configure protocol reservation can vary with different packet types. Refer to Chapter 38 in *Using NETBuilder Family Software* for a complete description of the procedures to configure a WAN port for protocol reservation for all packet types.

NOne — Specifies that queuing for the specified port is not in effect.

QueueInterLeave

Syntax

```
SETDefault !<port> -PORT QueueInterLeave = <ratio1> <ratio2> (1–10)
SHow [!<port> | !*] -PORT QueueInterLeave
SHowDefault [!<port> | !*] -PORT QueueInterLeave
```

Default 3, 2

Description The QueueInterLeave parameter determines the forwarding ratio of packets in the high- to medium-priority queues and the forwarding ratio of packets in the medium- to low-priority queues. To determine the forwarding ratio of packets in the high- to medium-priority queues, specify a value for ratio1. To determine the forwarding ratio of packets in the medium- to low-priority queues, specify a value for ratio2.

The values you specify identify the number of high-priority packets that are transmitted for each medium-priority packet and the number of medium-priority packets that are transmitted for each low-priority packet. Valid entries for each ratio include 1 through 10.

The value of QueueInterLeave directs the software to select the closest matching eight-slot pattern for the queue. This pattern may differ slightly from the configured interleave factor. For information on the queue arbitration algorithm, refer to Chapter 41 in Using NETBuilder Family Software.

To display the current setting, use:

```
SHow !<port> -PORT QueueInterLeave
```

QueuePATtern

Syntax `SHow [!<port> | !*] -PORT QueuePATtern`

Default HHMHMHLH (5:2:1)

Description The QueuePATtern parameter displays the eight-slot queue pattern for the interleave factor configured by -PORT QueueInterLeave. This parameter also displays a ratio based on the queue pattern.

The following is a sample display for port 1:

```
HHMHMHLH (5:2:1)
```

The information in the display is based on the default value (3, 2) of the -PORT QueueInterLeave parameter. This display indicates that the first and second packets are sent from the high-priority queue, the third packet is sent from the medium-priority queue, and so on. Once the eighth packet is sent, the algorithm wraps to the beginning of the pattern.

If a packet is to be sent from the high-priority queue but that queue is empty, a packet from the medium-priority queue is sent instead. If the medium-priority queue is also empty, a packet from the low-priority queue is sent. If a packet is to be sent from the medium-priority queue but that queue is empty, a packet from the high-priority queue is sent instead. If a packet is to be sent from the low-priority queue but that queue is empty, a high-priority packet is sent instead.

QueuePriority

Syntax `SHow -PORT QueuePriority`

Default No default

Description The QueuePriority parameter displays the settings of the following parameters:

- -PORT DefaultPriority
- -IP QueuePriority
- -LLC2 TUNnelPRiority

The display summarizes the priority assigned to IP and LLC2 tunnel packets. The display also shows the default priority assigned to a packet if any of the following conditions are met:

- The packet does not have a system-assigned priority.
- The -LLC2 TUNnelPRiority or -IP QueuePriority parameter is set to DEFault.
- You did not set up a mask and prioritization policy for a particular type of packet

For more information on these parameters, refer to the following:

- The -PORT DefaultPriority parameter on page 43-5 in this chapter.
- The -IP QueuePriority parameter in Chapter 29 on page 29-15.
- The -LCC2 TUNnelPRiority parameter in Chapter 34 on page 34-7

QueueStatistics

Syntax

```
FLush !<port> -PORT QueueStatistics
SHow [!<port>] -PORT QueueStatistics
```

Default None

Description The QueueStatistics parameter displays WAN queue statistics for protocol reservation. By displaying the statistics, you can determine the status of the queue.

QueueThrottle

Syntax

```
SETDefault !<port> -PORT QueueThrottle = <number> (1–40) | OFF
SHow [!<port> | !*] -PORT QueueThrottle
SHowDefault [!<port> | !*] -PORT QueueThrottle
```

Default OFF

Description The QueueThrottle parameter controls the number of medium- and low-priority packets that are forwarded to the driver each time packets from the priority queues are forwarded to the wide area network. This parameter applies only to wide area ports.

You can use the QueueThrottle parameter to manage queue latency time. You can tune the parameter to a smaller value for better response time, or to a larger value for better bandwidth and CPU utilization. Each incremental value of the QueueThrottle parameter represents about 10 milliseconds of latency, and if the parameter is set to OFF, the latency time defaults to 100 milliseconds. For example, if QueueThrottle is set to 3, the predictable queueing latency of high priority traffic is around 30 milliseconds.

3Com recommends that you change the setting of this parameter from the default of OFF only if the forwarding of certain high-priority packets (for example, SNA packets) is being slowed down by an excess of medium- or low-priority packets (especially large packets) across a serial line.

Values

<number> Indicates the maximum number of medium- and low-priority packets that are forwarded to the queue. 3Com recommends setting the value between 1 and 20 if you are using a low-speed line (64K or below) and between 21 and 40 if you are using a high-speed line (for example, T1).

OFF Indicates that the number of medium- and low-priority packets forwarded to the serial line driver is limited by the number of packets the driver can accept.

VirtualPort

Syntax *For non-ISDN interfaces*

```
ADD !<port> -PORT VirtualPort {<path> {<FRDLCI> | <X.25 DTE> | SMDS
  | MPATM | ATMLE}} | {SCID"<SysCallerID>"}
DELete !<port> -PORT VirtualPort {<path> {<FRDLCI> | <X.25 DTE> |
  SMDS | MPATM}} | {SCID"<SysCallerID>"} | ALL
SHow [!<port> | !*] -PORT VirtualPort
SHowDefault [!<port> | !*] -PORT VirtualPort
```

For ISDN interfaces

```
ADD !<port> -PORT VirtualPort {<connectorID.channelID> {<FRDLCI> |
  <X.25 DTE> |SMDS}} | {SCID"<SysCallerID>"} |
DELete !<port> -PORT VirtualPort {<connectorID.channelID> {<FRDLCI>|
  <X.25 DTE> |SMDS}} | {SCID”<SysCallerID>”} | ALL
SHow [!<port> | !*] -PORT VirtualPort
SHowDefault [!<port> | !*] -PORT VirtualPort
```

Default No default

Description The VirtualPort parameter can be used to create, delete, and display virtual ports. You do not need to create virtual ports in numerical order, for example, you can create virtual port !V2 before !V1.

For information on platforms that support virtual ports and the number of ports you can create, see Table 1-1 in Chapter 1 in *Using NETBuilder Family Software*.

Virtual ports function in the same way as other ports, as a logical interface that represents a connection to a network.

Virtual ports can be used when bridging or routing over Frame Relay, Asynchronous Transfer Mode data exchange interface (ATM DXI), and X.25. If you are bridging or routing IP-OSPF, DECnet, XNS, or VINES over Frame Relay or X.25 in a partially meshed or nonmeshed topology, or Boundary Routing over Frame Relay or X.25, you must configure virtual ports. If you are routing IP-RIP, IPX, or AppleTalk over Frame Relay or X.25 in a partially meshed or nonmeshed topology, you can optionally configure virtual ports. If you are routing APPN and other protocol data over the same port to the same DLCI, you must configure virtual ports. If you are routing APPN only, virtual ports are not recommended. For more information on virtual ports, refer to Chapter 1 in *Using NETBuilder Family Software*.

Virtual ports are required when bridging or routing over ATM in fully meshed, partially meshed, and nonmeshed topologies. Partially meshed and nonmeshed topologies are supported but not recommended. For more information, refer to Chapter 47 in *Using NETBuilder Family Software*.

Virtual ports can also be used to increase the number of addresses available over SMDS, or to increase the number of dial ports to support multidestination dialing over PPP. PPP dial virtual ports use the dynamic dial pool for their path resources.

Although group ports (logical networks) are numbered as if they are virtual ports, you create them using the LogicalNET parameter, not the VirtualPort parameter.

Values

<port>	Specifies the virtual port number. Virtual ports are numbered V*n*, where n is a value from 1 through the maximum number supported on the platform.
<path> or <connectorID.channelID>	Specifies the path number or the connector and B channel numbers to which the virtual port is attached.
<FRDLCI >| <X.25 DTE> | <SMDS> | MPATM | ETHATM	The FRDLCI value specifies the DLCI associated with the permanent virtual circuit on a Frame Relay network, for example, @205. The X.25DTE value specifies the X.25 address associated with the permanent virtual circuit on an X.25 network, for example, #31107551234. The SMDS value specifies to use the word SMDS on an SMDS network; there is no circuit ID. The MPATM (multiprocessor ATM) value specifies that the virtual port owner is a multiprotocol encapsulation over ATM as defined in the "MultiProtocol Encapsulation Over ATM - RFC 1483." When set to this value, the NETBuilder II bridge/router virtual port sends and receives packets over ATM permanent virtual circuit (PVCs). The packets will be encapsulated in SNAP format when carrying packets of different protocols on the same PVC. Optionally, each PVC can be dedicated to a single protocol, in which case, the packets are sent with NULL encapsulation. The ETHATM value specifies that the virtual port owner is ATM LAN emulation client as defined by the ATM Forum specification "LAN Emulation Over ATM - Version 1.0." When set to the ETHATM value, the NETBuilder II bridge/router virtual port participates as a LAN emulation client in the LAN emulation environment.
SCID "<SysCallerID>"	Specifies a text string to identify a remote site, such as a regional office in Seattle (SCID "Seattle"). This value enables the specified virtual port to use the dynamic dial-path pool, a WAN Extender dial-up virtual path, or a WAN Extender channelized virtual path to find a path resource. Only ports configured with PPP as port owner can use the dial pool. This value is compatible with all dial-path pools. The incoming caller ID is the -SYS SysCallerID of the calling bridge/router and uses the same syntax as SysCallerID, which is a string up to 31 characters long and case-sensitive.
ALL	Use this value with the DELete command to remove the virtual port.

WEProfileList

Syntax

```
ADD !<port? -PORT WEProfileList “<HSSpath profileID>”
DELete !<port> -PORT WEProfileList “<HSSpath profileID>” | ALL
SHow [!<port> | !*] _PORT WEProfile:ist
```

Default None

Description The WEProfileList parameter allows remote bridge/routers to establish a connection over a channelized T1 or E1 through a WAN Extender to a NETBuilder II bridge/router without entering a SCID (SysCallerID) string.

Up to 16 separate path and profile entry combinations can be added per port, but only one combination is entered at a time.

You can also use this parameter to configure the NETBuilder II bridge/router to use a WAN Extender. Refer to Chapter 35 in *Using NETBuilder Family Software* for more information.

Values

<port>
Specifies the port through which the channelized T1 or E1 connection is made between the remote bridge/router and the central NETBuilder II bridge/router. The connection between the two bridge/routers is made through a WAN Extender

“<HSSpath protileID>” (1-256)
Specifies the profile ID that identifies the remote site to the central NETBuilder II bridge/router. The profile ID is configured to one or more leased lines as part of the WAN Extender configuration. Refer to the *WAN Extender 2E|2T Manager User’s Guide* for more details.

44

PPP Service Parameters

This chapter describes parameters in the Point-to-Point Protocol (PPP) Service. PPP is a standard protocol that provides serial line connectivity between two NETBuilder bridge/routers or between a NETBuilder bridge/router and a bridge/router built by another vendor running PPP. Table 44-1 lists the PPP Service parameters and commands.

Table 44-1 PPP Service Parameters and Commands

Parameters	Commands
AuthLocalUser	SETDefault, SHow, SHowDefault
AuthProTocol	SETDefault, SHow, SHowDefault
AuthRemoteUser	ADD, DELete, SHow, SHowDefault
AuthReptIntvl	SETDefault, SHow, SHowDefault
CONFiguration	SHow, SHowDefault
MaxRcvUnit	SETDefault, SHow, SHowDefault
MlpCONTrol	SETDefault, SHow, SHowDefault
MlpmaxRxRecUnit	SETDefault, SHow, SHowDefault
MlpSTATIstics	Flush, SHow
STATUS	SHow

AuthLocalUser

Syntax

```
SETDefault !<port> -PPP AuthLocalUser = ([“<userid>” | None],
   “<password>”)
SHow [!<port> | !*] -PPP AuthLocalUser
SHowDefault [!<port> | !*] -PPP AuthLocalUser
```

Default None

Description The AuthLocalUser parameter assigns a user ID and password pair to a local bridge/router to be used when the Password Authentication Protocol (PAP) is enabled. If you configure this parameter, you must re-enable the port for the change to take effect.

AuthProTocol

Syntax

```
SETDefault !<port> -PPP AuthProTocol = None | Pap | Chap
SHow [!<port> | !*] -PPP AuthProTocol
SHowDefault [!<port> | !*] -PPP AuthProTocol
```

Default None

Description The AuthProTocol parameter selects the authentication protocol used in PPP link establishment. If you configure this parameter, you must re-enable the port for the change to take effect.

AuthRemoteUser

Syntax

```
ADD !<port> -PPP AuthRemoteUser ([“<userid>” | None], “<password>”)
DELete !<port> -PPP AuthRemoteUser ([“<userid>” | None])
SHow [!<port> | !*] -PPP AuthRemoteUser
SHowDefault [!<port> | !*] -PPP AuthRemoteUser
```

Default None

Description The AuthRemoteUser parameter controls access to a central host by multiple sites that support PAP. For each site, specify its user ID and password by adding an AuthRemoteUser. If you configure this parameter, you must re-enable the port for the change to take effect.

AuthReptIntvl

Syntax

```
SETDefault !<port> -PPP AuthReptIntvl = <minutes> (0–255)
SHow [!<port> | !*] -PPP AuthReptIntvl
SHowDefault [!<port> | !*] -PPP AuthReptIntvl
```

Default 0 (No periodic challenge handshake authentication protocol (CHAP) challenges following the link control protocol (LCP) OPEN state)

Description The AuthReptIntvl parameter specifies an interval value in minutes to allow repeat authentication after a link is established. The parameter ensures that the identity of a peer does not change even after initial authentication has been completed. If you configure this parameter, you must re-enable the port for the change to take effect.

CONFiguration

Syntax

```
SHow [!<port> | !*] -PPP CONFiguration
SHowDefault [!<port> | !*] -PPP CONFiguration
```

Default No default

Description The CONFiguration parameter displays PPP Service configuration information for each bridge/router path. The display includes the compression type and the MaxRcvUnit parameter value for each path on the bridge/router.

MaxRcvUnit

Syntax

```
SETDefault !<port> -PPP MaxRcvUnit = <bytes> (1–4500)
SHow [!<port> | !*] -PPP MaxRcvUnit
SHowDefault [!<port> | !*] -PPP MaxRcvUnit
```

Default 1,524 (when bridging Ethernet packets over serial lines)
4,500 (when bridging token ring packets over serial lines)

Description The MaxRcvUnit parameter specifies the maximum packet size (in bytes) that can be received on a serial link. In special cases, when an maximum request unit (MRU) of less than 1,500 is selected, the bridge/router can still receive 1,500 byte packets. The bridge/router will not transmit packets that exceed the value of MaxRcvUnit negotiated by the remote port.

The maximum packet size should be established on both sides of the link. A smaller value than the default may be required for some protocols that cannot receive larger packets.

MlpCONTrol

Syntax

```
SETDefault !<port> -PPP MlpCONTrol = ([Enabled | Disabled],
   [Fragment | NoFragment], [LongSequencing | ShortSequencing])
SHow [!<port> | !*] -PPP MlpCONTrol
SHowDefault [!<port> | !*] -PPP MlpCONTrol
```

Default Disabled, Fragment, LongSequencing

Description The MlpCONTrol parameter enables or disables multilink protocol (MLP) negotiation, fragmentation, and sequencing on a specified port.

Values

Enabled | Disabled	Determines whether PPP negotiates the multilink operation for a given link during the LCP link establishment phase. If Enabled is selected, the bridge/router originates and accepts MLP negotiation. If Disabled is selected, the bridge/router neither originates nor accepts MLP negotiation.
Fragment | NoFragment	If Fragment is selected, MLP fragments the packets transmitted on the port. If NoFragment is selected, MLP sequences the packets and load balances them, but does not fragment them.
LongSequencing | ShortSequencing	Determines whether PPP uses a long sequence number scheme (4-byte MLP header) or a short sequence number scheme (2-byte header). This only applies to the receiver side of MLP.

MlpmaxRxRecUnit

Syntax

```
SETDefault !<port> -PPP MlpmaxRxRecUnit = <value> (1–1624)
SHow [!<port> | !*] -MLP MlpmaxRxRecUnit
SHowDefault [!<port> | !*] -MLP MlpmaxRxRecUnit
```

Default 1624 (4500 on NETBuilder II)

Description The MlpmaxRxRecUnit parameter specifies the maximum length of a packet that PPP can receive after reassembly on a specified port.

MlpSTATIstics

Syntax

```
FLush -PPP MlpSTATIstics
SHow [!<port> | !*] -PPP MlpSTATIstics
```

Default No default

Description The MlpSTATIstics parameter displays all MLP-related statistics for all paths belonging to a specified port. Statistics gathered by MLP can be cleared using the FLush command.

STATUS

Syntax

```
SHow -PPP STATUS [LCP | NCP]
```

Default No default

Description The STATUS parameter displays the current Link Control Protocol (LCP) state and Network Control Protocol (NCP) state. LCP manages the PPP link between the two end points. The NCPs manage the network-layer routing or bridging protocols (Bridging, TCP/IP, XNS, OSI, IPX, DECnet, AppleTalk, and VINES).

The following are possible LCP states:

INITIAL The lower protocol layer is down and there is no request to open a connection.

STARTING The open procedure has been initiated, but the lower layer is still down.

CLOSED The lower layer is up, but there is no request to open a connection.

STOPPED PPP has already sent a certain number of configuration requests and no response has been received. It is no longer sending configuration requests, but waits for them from the peer.

CLOSING An attempt is being made to terminate the connection. A terminate request has been sent but not yet acknowledged.

STOPPING The link is up and open but an attempt is being made to terminate the connection. A terminate request has been sent but not yet acknowledged. This state provides a well-defined opportunity to terminate a link before allowing new traffic. After the link has terminated, a new configuration may occur through the Stopped or Starting states.

REQSENT An attempt is being made to configure the connection. A configuration request packet has been sent, but an acknowledgment has not been received.

ACKRCVD A configuration request packet has been sent and an acknowledgment received, but a return acknowledgment has not yet been sent.

ACKSENT A configuration request packet and an acknowledgment have both been sent, but an acknowledgment has not been received.

OPENED A configuration request packet and an acknowledgment have both been sent and received.

The following are NCP states:

LISTEN Idle mode. The port is listening for communication to begin.

OPEN Negotiation between the two devices is complete.

REQSENT An attempt is being made to configure the connection. A configuration request packet has been sent, but an acknowledgment has not been received.

ACKRCVD A configuration request packet has been sent and an acknowledgment received, but a return acknowledgment has not yet been sent.

ACKSENT A configuration request packet and an acknowledgment have both been sent, but an acknowledgment has not been received.

DISABLD All packets received for this protocol will be rejected. This state is displayed when a NETBuilder II port is using Boundary Routing to communicate with remote office networks. For more information, refer to Chapter 32 in *Using NETBuilder Family Software*.

45

PROFILE SERVICE PARAMETERS

This chapter describes all the parameters in the PROFile Service. Table 45-1 lists the PROFile Service parameters and commands.

Table 45-1 PROFile Service Parameters and Commands

Parameters	Commands
CONFiguration	SHow, SHowDefault
ProfileID	DELete, SHow
ProfileType	ADD, SHow, SHowDefault
X25ClosedUsrGrp	SETDefault, SHow, SHowDefault
X25COMPressType	SETDefault, SHow, SHowDefault
X25CONTrol	SETDefault, SHow, SHowDefault
X25CUDSuffix	SETDefault, SHow, SHowDefault
X25FastSelect	SETDefault, SHow, SHowDefault
X25NSF	SETDefault, SHow, SHowDefault
X25PacketSiZe	SETDefault, SHow, SHowDefault
X25ProfileName	SETDefault, SHow, SHowDefault
X25ReverseChrg	SETDefault, SHow, SHowDefault
X25ThruputClass	SETDefault, SHow, SHowDefault
X25VCLimit	SETDefault, SHow, SHowDefault
X25VCQueueSize	SETDefault, SHow, SHowDefault
X25VCTimer	SETDefault, SHow, SHowDefault
X25WindowSiZe	SETDefault, SHow, SHowDefault

CONFiguration

Syntax

```
SHow [!<profile ID>] -PROFile CONFiguration [X25User | X25Dte]
SHowDefault [!<profile ID>] -PROFile CONFiguration [X25User |
  X25Dte]
```

Default No default

Description The CONFiguration parameter displays the values of the PROFile Service parameters.

To display all profile IDs and profile types, do not specify X25User or X25Dte options after CONFiguration. To display a specific profile, select either X25User or X25Dte as the profile type.

Values

!<profile ID>	Refers to a number from 1 to 255 identifying the X.25 profile to be changed. A value of 0 indicates the default data terminal equipment (DTE) profile.
X25User	If X25User is selected, the screen displays the contents of the X.25 user profiles currently configured in the PROFile Service.
X25Dte	If X25Dte is selected, the screen displays the contents of the X.25 DTE profiles currently configured in the PROFile Service.

ProfileID

Syntax

```
DELete -PROFile ProfileID [!<profile ID> | <ALL [X25User |
  X25Dte>] [Override]
SHow -PROFile ProfileID
```

Default No default

Description The ProfileID parameter identifies the profile ID number from 1 to 255 and the profile type to be deleted. A value of 0 cannot be used because 0 identifies the default profile, which cannot be deleted.

Values

!<profile ID> Refers to a number from 1 to 255 identifying the X.25 profile to be deleted. A value of 0 indicates the default DTE profile.

ALL Deletes all the profiles of the specified profile type.

X25User Deletes X25 User profiles. Identifies the profile ID as an X.25 user profile. The X.25 user profile contains a subset of the X. 25 DTE profile parameters that are used locally to prioritize traffic over a virtual circuit. The subset overrides the DTE profile for the port when the profiles are combined to build the X.25 call request.

An X.25 user profile allows each network protocol to define its own subset of X.25 DTE profile parameters that enable the virtual circuits to meet their specific congestion and throughput requirements.

X25Dte Deletes X25 DTE profiles. Identifies the configured profile ID as an X.25 DTE profile. The X.25 DTE profile contains the complete set of parameters that is used by the X.25 service to configure the call setup and throughput requirements for a virtual circuit. When the call request is built by the X.25 service, the X.25 user profile is combined with the X.25 DTE profile, and the X.25 user parameters from the X.25 user profile override the X.25 DTE profile parameters.

Override Deletes the profile even if the profile is in use. However, the default profile (!0) cannot be deleted even if the Override option is used.

ProfileType

Syntax

```
ADD !<profile ID> -PROFile ProfileType [X25User | X25Dte] [<seed
  profileID>] [<"string" (1–60 characters)>]
SHow !<profile ID> -PROFile ProfileType
SHowDefault !<profile ID> -PROFile ProfileType
```

Default No default

Description The ProfileType parameter creates an X.25 user or X.25 DTE profile. For more information on X.25 user and X.25 DTE profiles, refer to Chapter 45 in *Using NETBuilder Family Software*.

Values

<profile ID> Refers to a number from 1 to 255 identifying the X.25 profile to be deleted. A value of 0 indicates the default DTE.

X25User Identifies the profile ID as an X.25 user profile. The X.25 user profile contains a subset of the X.25 DTE profile parameters that are used locally to prioritize traffic over a virtual circuit. The subset overrides the DTE profile for the port when the profiles are combined to build the X.25 call request.

An X.25 user profile allows each network protocol to define its own subset of X.25 DTE profile parameters that enable the virtual circuits to meet their specific congestion and throughput requirements.

X25Dte	Identifies the configured profile ID as an X.25 DTE profile. The X.25 DTE profile contains the complete set of parameters that is used by the X.25 service to configure the call setup and throughput requirements for a virtual circuit. When the call request is built by the X.25 service, the X.25 user profile is combined with the X.25 DTE profile, and the X.25 user parameters from the X.25 user profile override the X.25 DTE profile parameters.
<seed profileID>	Selects a seed profile to be predefined with profile parameters. The seed profile ID is a number from 1 to 255 identifying the profile. The seed profile type must match the configured profile type.
<“string”>	Refers to the text string used to describe the profile and is limited to 60 characters.

X25ClosedUsrGrp

Syntax

```
SETDefault !<profile ID> -PROFile X25ClosedUsrGrp = <number>
  (0–9999)
SHow !<profile ID> -PROFile X25ClosedUsrGrp
SHowDefault !<profile ID> -PROFile X25ClosedUsrGrp
```

Default 0

Description The X25ClosedUsrGrp parameter specifies the closed user group (CUG) for the data terminal equipment (DTE) associated with the specified port. Access among public data network (PDN) users can be restricted by subdividing users into groups called closed user groups. A CUG is a set of PDN users. Each CUG is assigned a number between 1 and 9999, and only these groups can communicate with each other through the PDN. The default value 0 indicates that the DTE address associated with this port does not belong to any CUGs and can communicate with devices not belonging to the CUG. If you specify a CUG number other than 0, you can communicate only with devices in that CUG. Information regarding CUG assignments is provided to PDN subscribers at the time of subscription. You can specify which CUGs you want to communicate with on a specified interface.

Values

<profile ID>	Refers to a number from 1 to 255 identifying the X.25 profile to be changed. A value of 0 indicates the default DTE profile.
0–9999	Refers to the closed user group value.

X25COMPressType

Syntax

```
SETDefault !<profile ID> -PROFile X25COMPressType = DEFault | NONE
  | HIStory | PerPacket
SHow !<profile ID> -PROFile X25COMPressType
SHowDefault !<profile ID> -PROFile X25COMPressType
```

Default DEFault

Description The X25COMPressType parameter configures a data compression type to a selected profile. By default, all the virtual circuits on a path use the data compression type specified using the -PORT COMPressType parameter. The X25COMPressType parameter overrides the -PORT COMPressType parameter.

When X25COMPressType is set to any value other than the DEFault, the specified virtual circuit using the profile uses the selected data compression method. If the value is set to DEFault, then the virtual circuit uses X25COMPressType configured for the port.

Values

DEFault	Indicates that the selected virtual circuit using the profile will use the data compression method configured by the -PORT COMPressType parameter.
NONE	Indicates that the selected virtual circuit using the profile will not use data compression.
HIStory	Indicates that the selected virtual circuit using the profile will perform history link-level data compression.
PerPacket	Indicates that the selected virtual circuit using the profile will perform per-packet link-level data compression.

For more information about configuring data compression, refer to Chapter 39 in *Using NETBuilder Family Software*.

X25CONTrol

Syntax

```
SETDefault !<profile ID> -PROFile X25CONTrol = ([IncomingCall |
  NoIncomingCall], [OutgoingCall | NoOutgoingCall], [PSN | NoPSN],
  [TCN | NoTCN], [WSN | NoWSN])
SHow !<profile ID> -PROFile X25CONTrol
SHowDefault !<profile ID> -PROFile X25CONTrol
```

Default IncomingCall, OutgoingCall, NoPSN, NoWSN, NoTCN

Description The X25CONTrol parameter configures valid call setup parameters.

Values

<profile ID>	Refers to a number from 1 to 255 identifying the X.25 profile to be changed. A value of 0 indicates the default DTE profile.
IncomingCall | NoIncomingCall	IncomingCall allows incoming calls. NoIncomingCall does not allow incoming calls from the DTE to which the identified profile is mapped.
OutgoingCall | NoOutgoingCall	OutgoingCall enables outgoing calls. NoOutgoingCall does not allow outgoing calls from the DTE to which the identified profile is mapped.
PSN | NoPSN	PSN initiates the packet size negotiation in the outgoing call. NoPSN indicates that packet size negotiation is not initiated.
TCN | NoTCN	TCN initiates the throughput class negotiation in the outgoing call. NoTCN indicates that throughput class negotiation is not initiated.
WSN | NoWSN	WSN initiates the window size negotiation in the outgoing call. NoWSN indicates that window size negotiation is not initiated.

X25CUDSuffix

Syntax

```
SETDefault !<profile ID> -PROFile X25CUDSuffix = <“string”>
  (max 4 char)
SHow !<profile ID> -PROFile X25CUDSuffix
SHowDefault !<profile ID> -PROFile X25CUDSuffix
```

Default No default

Description The X25CUDSuffix parameter sends a 4-byte suffix in the call request packet configured for a user profile. If X25CUDSuffix is present in the incoming call request, it searches all user profile IDs registered for that protocol. If the match is found, it maps the matched user profile to the specified virtual circuit. You can use a maximum number of four characters enclosed in quotes for the X25CUDSuffix. A configured label of fewer than four bytes is padded by null characters.

X25FastSelect

Syntax

```
SETDefault !<profile ID> -PROFile X25FastSelect = ([Request |
 NoRequest], [Accept |NoAccept])
SHow !<profile ID> -PROFile X25FastSelect
SHowDefault !<profile ID> -PROFile X25FastSelect
```

Default NoRequest, NoAccept

Description The X25FastSelect parameter determines whether the call request packet can include more than 16 characters of user data. By default, the call request packet does not include more than 16 bytes of user data. Up to 128 bytes of user data can be included if the X25FastSelect parameter is enabled.

Values

profile ID Refers to a number from 1 to 255 identifying the X.25 profile to be changed. A value of 0 indicates the default DTE profile.

Request | NoRequest Request specifies that X25FastSelect can be used in outgoing calls. NoRequest specifies that X25FastSelect cannot be used in outgoing calls.

Accept | NoAccept Accept specifies X25FastSelect for incoming calls. NoAccept specifies that X25FastSelect is not allowed for incoming calls.

X25NSF

Syntax

```
SETDefault !<profile ID> -PROFile X25NSF = <“string”> (1–60 char)
SHow !<profile ID> -PROFile X25NSF
SHowDefault !<profile ID> -PROFile X25NSF
```

Default No default

Description The X25NSF parameter specifies the facilities to be passed in the call request. These facilities are required by the PDN. The value of National Specific Facilities (NSF) is expressed in hexadecimal string format, and the maximum length can be up to 60 characters for that specific DTE. This string is transmitted as part of the facilities in all call requests to that DTE.

Values

<profile ID> Refers to a number from 1 to 255 identifying the X.25 profile to be changed. A value of 0 indicates the default DTE profile.

<“string”> Refers to the text string used to specify the National Specific Facilities. The value is expressed in hexadecimal string format, and the limit is 60 characters.

Example To place the facilities “040801” in the call request to the DTE using profile 0, enter:

```
SETDefault !0 -PROFile X25NSF = “040801”
```

X25PacketSiZe

Syntax

```
SETDefault !<profile ID> -PROFile X25PacketSiZe = 16 | 32 | 64 |
  128 | 256 | 512 | 1024 |2048 | 4096
SHow !<profile ID> -PROFile X25PacketSiZe
SHowDefault !<profile ID> -PROFile X25PacketSiZe
```

Default 128

Description The X25PacketSiZe parameter specifies in bytes the packet size for the virtual circuit using the identified profile. The maximum packet size for the SuperStack II NETBuilder boundary router is 1024.

Values

<profile ID >	Refers to a number from 1 to 255 identifying the X.25 profile to be changed. A value of 0 indicates the default DTE profile.

X25ProfileName

Syntax

```
SETDefault !<profile ID> -PROFile X25ProfileName = <“string”> (1–60
  characters)
SHow !<profile ID> -PROFile X25ProfileName
SHowDefault !<profile ID> -PROFile X25ProfileName
```

Default No default

Description The X25ProfileName parameter names the X.25 user profile that you have defined. The number of characters in the name must be 60 or less.

Values

<profile ID>	Refers to a number from 1 to 255 identifying the X.25 profile to be changed. A value of 0 indicates the default DTE profile.
<“string”>	Refers to the text string used to describe the profile.

X25ReverseChrg

Syntax

```
SETDefault !<profile ID> -PROFile X25ReverseChrg = ([Request |
  NoRequest], [Accept | NoAccept])
SHow !<profile ID> -PROFile X25ReverseChrg
SHowDefault !<profile ID> -PROFile X25ReverseChrg
```

Default NoRequest, Accept

Description The X25ReverseCharge parameter determines whether charges for all connections from or to a particular DTE can be reversed.

Values

<profile ID>	Specifies a number from 1 to 255 identifying the X.25 profile to be changed. A value of 0 indicates the default DTE profile.
Request | NoRequest	Request specifies that calls going from the local bridge/router are charged to the destination; that is, the receiving end pays for the call. NoRequest means that calls going from the local bridge/router cannot be charged to the destination; that is, the originating end pays for the calls.

Accept | NoAccept Accept means that calls coming in to the local bridge/router are charged to their destination; that is, the local bridge/router pays for them. NoAccept means that incoming calls are not charged to their destination; that is, the remote bridge/router or originating end of the call pays for them.

X25ThruputClass

Syntax

```
SETDefault !<profile ID> -PROFile X25ThruputClass = 75 | 150 | 300 |
 600 | 1200 | 2400 | 4800 | 9600 | 19200 | 48000
SHow !<profile ID> -PROFile X25ThruputClass
SHowDefault !<profile ID> -PROFile X25ThruputClass
```

Default 9600

Description The X25ThruputClass parameter specifies the default throughput rate in bits per second.

Values <profile ID> Specifies a number from 1 to 255 identifying the X.25 profile to be changed.

X25VCLimit

Syntax

```
SETDefault !<profile ID> -PROFile X25VCLimit = <number> (0–15)
SHow !<profile ID> -PROFile X25VCLimit
SHowDefault !<profile ID> -PROFile X25VCLimit
```

Default 2

Description The X25VCLimit parameter specifies the maximum number of virtual circuits to a specific DTE address destination. For more information, refer to Chapter 45 in *Using NETBuilder Family Software*.

Values <profile ID> Specifies a number from 1 to 255 identifying the X.25 profile to be changed. A value of 0 indicates the default DTE profile.

0–15 Refers to the number of virtual circuits.

X25VCQueueSize

Syntax

```
SETDefault !<profile ID> -PROFile X25VCQueueSize = <number> (1–128)
SHow !<profile ID> -PROFile X25VCQueueSize
SHowDefault !<profile ID> -PROFile X25VCQueueSize
```

Default 10

Description The X25VCQueueSize parameter specifies the maximum number of packets that can be queued for a specific DTE address when the virtual circuit on the X.25 port is congested.

If the X25VCQueueSize value is low, additional virtual circuits can be established up to the number specified by the X25VCLimit parameter. If the X25VCQueueSize value is high, additional memory resources are required. For more information, refer to Chapter 45 in *Using NETBuilder Family Software*.

Values		
	<profile ID>	Specifies a number from 1 to 255 identifying the X.25 profile to be changed. A value of 10 indicates the default DTE profile.
	1–128	Refers to the number of packets queued.

X25VCTimer

Syntax

```
SETDefault !<profile ID> -PROFile X25VCTimer = <minutes> (1–512)
SHow !<profile ID> -PROFile X25VCTimer
SHowDefault !<profile ID> -PROFile X25VCTimer
```

Default 5

Description The X25VCTimer parameter specifies the maximum amount of time (in minutes) that can elapse when there is no activity on the X.25 virtual circuit before it is cleared. It applies to the first virtual circuit established for a DTE address.

If more than one virtual circuit is established for the same DTE address, all are cleared (except for the first one established) when the first virtual circuit is not experiencing congestion. For more information, refer to Chapter 45 in the *Using NETBuilder Family Software*.

Values		
	<profile ID>	Specifies a number from 1 to 255 identifying the X.25 profile to be changed. A value of 0 indicates the default DTE profile.
	1–512	The number of minutes before the virtual circuit is cleared.

X25WindowSiZe

Syntax

```
SETDefault !<profile ID> -PROFile X25WindowSiZe = <number> (1–127)
SHow !<profile ID> -PROFile X25WindowSiZe
SHowDefault !<profile ID> -PROFile X25WindowSiZe
```

Default 2

Description The X25WindowSiZe parameter determines the X.25 packet layer window size. The window determines how many packets can be sent on a virtual circuit without an acknowledgment from the other end.

Values		
	<profile ID>	Specifies a number from 1 to 255 identifying the X.25 profile to be changed. A value of 0 indicates the default DTE profile.
	1–7	If the -X25 CONTrol parameter is set to NoExtendedPacketSeq, the X25WindowSiZe parameter can be set to a value from 1 through 7.
	1–127	If the -X25 CONTrol parameter is set to ExtendedPacketSeq, the X25WindowSiZe parameter can be set to a value from 1 through 127.

46

RDP SERVICE PARAMETERS

This chapter describes the Internet Control Message Protocol (ICMP) Router Discovery Protocol (RDP) Service parameters. The RDP Service is related to the following protocols: IP and IP Multicasting. Table 46-1 lists the RDP Service parameters and commands.

Table 46-1 RDP Service Parameters and Commands

Parameters	Commands
CONFiguration	SHow
CONTrol	SETDefault, SHow
LifeTime	SETDefault, SHow
MAxInterval	SETDefault, SHow
MInInterval	SETDefault, SHow
RouterList	ADD, DElete, FLush, SHow

CONFiguration

Syntax

```
SHow [!<port>] -RDP CONFiguration
```

Default No default

Description The CONFiguration parameter displays the values associated with RDP Service.

CONTrol

Syntax

```
SETDefault !<port> -RDP CONTrol = ([Auto | Enable | Disable],
  [Multicast | Broadcast])
SHow [!<port>] -RDP CONTrol
```

Defaults Auto, Multicast

Description The CONtrol parameter enables or disables RDP and specifies the destination IP address to be used for sending ICMP Router Advertisement or Router Solicitation messages.

Values

Auto|Enable | Disable	With the Auto setting, RDP is enabled on LANs but disabled on WANs. Enable globally enables RDP while Disable globally disables RDP. The default is Auto.
Multicast | Broadcast	Determines whether packets are multicasted or broadcasted. The following rules determine settings: When the system is in host mode (!0 mode), set this value to Multicast to send router solicitations out with the IP destination set to the all-router address (224.0.0.2).

- When the system is in router mode, set this value to Multicast to send router advertisements out with the IP destination address set to the all-host address (224.0.0.1).
- In either host or router mode, set this parameter to Broadcast to send router solicitations or router advertisements out with the IP destination set to the limited broadcast IP address (255.255.255.255).

LifeTime

Syntax

```
SETDefault !<port> -RDP LifeTime = <seconds>(4-9000) | Default
SHow [!<port>] -RDP LifeTime
```

Default 1800 seconds (3 times the default value of MAxInterval); refer to "MAxInterval" on page 46-2.

Description The LifeTime parameter specifies the value for the lifetime field in router advertisements, and applies only when the router is in router mode.

The value of the lifetime field must not be less than the current value of MAxInterval.

MAxInterval

Syntax

```
SETDefault !<port> -RDP MAxInterval = <seconds>(4-1800) | Default
SHow [!<port>] -RDP MAxInterval
```

Default 600 seconds

Description The MAxInterval parameter specifies the maximum interval allowed between two router advertisements, and only applies when the system is in router mode.

The value of MAxInterval must not be greater than the current value of the LifeTime parameter (refer to "LifeTime" on page 46-2), nor less than the value set for MInInterval (refer to "MInInterval" on page 46-2). If either situation occurs, a warning message is displayed and the value of the LifeTime parameter is set to its default setting.

Setting MAxInterval to Default automatically sets the values of the LifeTime, MAxInterval, and MInInterval parameters to their default settings.

MInInterval

Syntax

```
SETDefault !<port> -RDP MInInterval = <seconds>(3-1800) | Default
SHow [!<port>] -RDP MInInterval
```

Default 450 seconds (75 percent of the default value of MAxInterval).

Description The MInInterval parameter specifies the minimum interval allowed between two router advertisements, and is only meaningful when the system is in router mode.

The value of MInInterval must not be greater than the current value of the MAxInterval parameter (refer to "MAxInterval" on page 46-2).

RouterList

Syntax

```
ADD -RDP RouterList <IP address>[NoAdvertise][<preference
 level>|Infinity]
DELete -RDP RouterList {<IP address>|ALL}
FLush -RDP RouterList
SHow -RDP RouterList
```

Default preference level = 0

Description The RouterList parameter specifies the list of routers that either learn from router advertisements or that advertise their address. The following rules determine the settings:

- When the system is in host mode, the RouterList parameter specifies the default routers that learn from router advertisements.
- When the system is in router mode, the RouterList parameter specifies the list of router addresses to be advertised or not be advertised. This parameter can also set the preferred router address as a default router on the same subnet. There is no limitation for adding router addresses, as long as system memory is available.

Values

<IP address> Indicates the Internet address to be included in the router list. When router advertisements are transmitted on a particular advertising interface, the system checks each IP address assigned to that interface against those placed in the router list. If the address is not in the list, then this address is included in the router advertisement; otherwise, this value depends on the advertise flag.

<NoAdvertise> Indicates not to advertise the router address. The default is to advertise.

<preference level> Indicates a 32-bit, signed, twos-complement integer that defines the hierarchy for selecting the default router. The higher the value, the higher the router preference is.

Infinity Indicates that the address is not to be picked up by hosts as a default router address and has a minimum value (0x80000000).

The SHow RouterList command displays the router list. The FLush command flushes the current router list and allows routes to be relearned. The DELete RouterList command can delete a particular IP address or all addresses from the router list.

47

RIPIP SERVICE PARAMETERS

This chapter describes the Routing Information Protocol/Internet Protocol (RIPIP) Service parameter. The RIPIP Service is related to the ARP, OSPF, IP, and TCP Services. Table 47-1 lists the RIPIP parameters and commands.

Table 47-1 RIPIP Service Parameters and Commands

Parameters	Commands
AdvertisePolicy	ADD, DELete, SHow
AdvToNeighbor	ADD, DELete, SHow
CONFiguration	SHow, SHowDefault
CONTrol	SETDefault, SHow
DefaultMetric	SETDefault, SHow
ExteriorPolicy	ADD, DELete, SHow
ImportMetric	ADD, DELete, SHow
InteriorPolicy	ADD, DELete, SHow
RcvFromNeighbor	ADD, DELete, SHow
RcvSubnetMask	ADD, DELete, SHow
ReceivePolicy	ADD, DELete, SHow
StaticPolicy	ADD, DELete, SHow
UpdateTime	SETDefault, SHow

All the RIPIP parameters (except for UpdateTime) are port-dependent, and valid port numbers can be used in all the commands involving these parameters. Port 0 is a valid port number for RIPIP parameters, but you should configure the parameters for port 0 only if you have defined NETaddr in the IP Service for port 0. In this case, the router is considered a host and cannot be used for IP routing. On port 0, only the CONTrol, ReceivePolicy, and RcvFromNeighbor parameters are relevant; none of the other RIPIP parameters take effect.

AdvertisePolicy

Syntax

```
ADD !<port> -RIPIP AdvertisePolicy All | None | [~]<IP address>
   [<metric>(0–15)]
DELete !<port> -RIPIP AdvertisePolicy All | <IP address>
SHow [!<port> | !*] -RIPIP AdvertisePolicy
```

Default All, 0

Description The AdvertisePolicy parameter modifies or displays the list of routes advertised by RIP. To be advertised, the route must be in this list and must exist in the IP Routing Table. There is no limit to the number of networks that can be added per port.

Values	All	Reports all routes learned regardless of the source.
	None	None of the routes learned regardless of the source are reported.
	<IP address>	Specifies the Internet address to be reported.
	~	When used in the ADD command, reports all routes except the one specified. In this format, no metric should be included in the command syntax. For example, if you enter the following command, all routes except 12.0.0.0 are advertised on port 1: **ADD !1 -RIPIP AdvertisePolicy ~12.0.0.0** The AdvertisePolicy list includes only the entry ~12.0.0.0 instead of all the routes being advertised.
	<metric>	If an Internet address is specified, the metric is optional. If you decide to specify a metric, specify a value between 1 and 15. This value can be based on bandwidth or utilization. The route and this specified metric are reported. If you decide not to specify a metric, specify 0.

Adding to a List. If a tilde (~) precedes the Internet address in the command, the command affects all Internet addresses configured for that port except the address specified. The following is an example:

```
ADD !2 -RIPIP AdvertisePolicy ~10.0.0.0
```

This example causes RIP to advertise all the routes on port 2 except 10.0.0.0.

If the AdvertisePolicy list already consists of networks that were added with ADD commands without tildes, and you are entering an ADD command that includes the tilde, this ADD command takes precedence.

The following is another example showing how a series of ADD commands affects the AdvertisePolicy list. Suppose you enter:

```
ADD !1 -RIPIP AdvertisePolicy 12.0.0.0 2
ADD !1 -RIPIP AdvertisePolicy 13.0.0.0 3
ADD !1 -RIPIP AdvertisePolicy 14.0.0.0 4
```

The list of routes on port 1 now contains 12.0.0.0 with metric 2, 13.0.0.0 with metric 3, and 14.0.0.0 with metric 4. Suppose later you enter :

```
ADD !1 -RIPIP AdvertisePolicy ~14.0.0.0
```

The original list of three routes is replaced by ~14.0.0.0.

Suppose you enter:

```
ADD !1 -RIPIP AdvertisePolicy 15.0.0.0
```

This most recently entered command overrides the existing values on the list. That is, the list now consists of 15.0.0.0 only, and RIP advertises only 15.0.0.0 on port 1.

Deleting from a List. To delete a route in the AdvertisePolicy list, use the DELete command. The following is an example that deletes a route:

```
DELete !1 -RIPIP AdvertisePolicy 15.0.0.0
```

RIP now does not advertise 15.0.0.0 on port 1.

If the AdvertisePolicy list contains an entry with a tilde, and you want to delete it, just specify the Internet network in the DELete command. You do not need to include the tilde.

For example, to indicate that all routes except 14.0.0.0 are advertised on port 1, enter:

```
ADD !1 -RIPIP AdvertisePolicy ~14.0.0.0
```

You can then later nullify this command by entering:

```
DELete !1 -RIPIP AdvertisePolicy 14.0.0.0
```

This DELete command removes ~14.0.0.0 from the AdvertisePolicy list. As a result, the router no longer advertises the routes that used to be advertised as a result of the previous ADD AdvertisePolicy command.

By default, RIP reports all networks.

AdvertisePolicy overrides StaticPolicy, InteriorPolicy, and ExteriorPolicy in deciding whether a route is to be reported.

AdvToNeighbor

Syntax

```
ADD !<port> -RIPIP AdvToNeighbor <IP address>
DELete !<port> -RIPIP AdvToNeighbor <IP address>
SHow [!<port> | !*] -RIPIP AdvToNeighbor
```

Default No default

Description The AdvToNeighbor parameter modifies and displays the list of neighbor addresses that RIP uses to determine to which neighbors it should send update packets.

RIP neighbors are routers that share a common network and participate in the RIP Protocol. Each RIP packet can be either broadcast or addressed individually to each neighbor.

If no neighbors are configured on the port, RIP broadcasts update packets on the port. Use the ADD and DELete commands to include or remove an address.

SHow displays the active neighbors. If a neighbor has been configured but is not directly connected, the bridge/router does not send out RIP updates. When this happens, this command lists the addresses of AdvToNeighbor and RcvFromNeighbor as NONE. Some neighbors on the disk may be invalid if they are not connected to the network to which the router's port is connected. Invalid neighbors can become valid after they have been directly connected.

By default, the AdvToNeighbor list is empty, and RIP broadcasts request and response packets on the network configured for the port.

AdvToNeighbor must be configured or DynamicNbr enabled on a serial port that is running X.25, Frame Relay, or ATM because these protocols do not support broadcast facilities. For each X.25, Frame Relay, or asynchronous transfer mode (ATM) neighbor configured, the IP address to corresponding media address (data terminal equipment (DTE) for X.25, datalink connection identifier (DLCI) for Frame Relay, virtual channel identifier (VCID) of a PVC for ATM) needs to be in the IP Address Table, either dynamically learned (InARP) or statically configured.

CONFiguration

Syntax

```
SHow [!<port> | !*] -RIPIP CONFiguration
SHowDefault [!<port> | !*] -RIPIP CONFiguration
```

Default No default

Description The CONFiguration command displays the values of all modifiable RIPIP parameters for a particular port. If no port number is specified, the parameters for all ports configured to support an IP network or subnet are displayed.

The SHow -RIPIP CONFiguration command displays the valid configured values. If a neighbor has been configured but is not directly connected, the bridge/router does not send out RIP updates. When this happens, this command lists the addresses of AdvToNeighbor and RcvFromNeighbor as NONE.

The SHowDefault -RIPIP CONFiguration command displays all the values that are stored on the disk, both valid and invalid. The values of the AdvToNeighbor and RcvFromNeighbor parameters are invalid if the specified IP addresses are not on a directly connected network or subnet.

The SHow -RIPIP CONFiguration command generates the following message if no IP address is configured for the specified port:

```
No active configuration
```

CONTrol

Syntax

```
SETDefault !<port> -RIPIP CONTrol = ([TAlk | NoTAlk], [Listen |
   NoListen], [Poison | NoPoison], [TRigger | NoTRigger],
   [SubnetAdvUnn | NetAdvUnn], [SubnetBcast | All1sBcast],
   [Aggregate | NoAggregate], [DeAggregate | NoDeAggregate],
   [DynamicNbr | NoDynamicNbr], [FullMesh | NonMesh])
SHow [!<port> | !*] -RIPIP CONTrol
```

Default NoTAlk, NoListen, Poison, NoTRigger, SubnetAdvUnn, SubnetBcast, NoAggregate, NoDeAggregate, DynamicNbr, NonMesh

Description The CONTrol parameter configures a set of parameters related to RIPIP.

Values

TAlk | NoTAlk	Determines whether RIP sends update and request packets. If you select TAlk, RIP sends update and request packets on the specified port. If you select NoTalk, no update and request packets are sent.
Listen | NoListen	Determines whether RIP receives and processes incoming update and request packets. Select Listen to enable the process or NoListen to disable receiving and processing incoming update and request packets. Listen | NoListen are the only values for CONTrol that are significant on port 0. If the router serves as a bridge, use these values on port 0 to determine whether it collects RIP information from the network.

Poison | NoPoison

If Poison is selected, the router advertises all routes to all neighbors, but when advertising a route to a neighbor that has advertised the same route, the router sets the metric to infinity (16) to prevent the recipient from adding the route to its routing table. Poison reverse speeds convergence but adds to network overhead.

If NoPoison is selected, the router omits routes learned from one neighbor from RIP updates sent to that neighbor. NoPoison has the advantage of minimizing network overhead in large network configurations at the expense of slower convergence.

TRigger | NoTRigger

Determines if RIP sends trigger update packets. TRigger update packets are sent when a route's metric has changed. By sending these update packets, RIP does not need to wait for the update interval, allowing earlier notification that a route's metric has changed.

NetAdvUnn | SubnetAdvUnn

NetAdvUnn summarizes all subnet routes into a natural IP network. NetAdvUnn is useful if the other end of an unnumbered link belongs to a different IP network. This option does not affect host routes or network routes. SubnetAdvUnn sends all subnet routes as is. SubnetAdvUnn is useful if the other end of an unnumbered link belongs to the same subnetwork. Both options are applicable only to unnumbered links.

SubnetBcast | All1sBcast

Determines whether RIP uses a directed or limited broadcast address as the destination IP addresses in its broadcast updates on the port specified by this parameter (a neighbor is not defined on this port). If you specify SubnetBcast, RIP uses directed broadcast addresses. If you specify All1sBcast, RIP uses the limited broadcast address 255.255.255.255.

Aggregate | NoAggregate

If Aggregate is selected on the outgoing port and if the subnet mask of the route is longer than the subnet mask of the outgoing interface, the border router adopts the shorter mask and zeros out all the bits in the host field (aggregate to a shorter mask). If NoAggregate is selected for the outgoing port, route aggregation is not performed.

DeAggregate | NoDeAggregate

If DeAggregate is selected on the outgoing port and if the subnet mask of the route is shorter than the mask of the outgoing interface, the border router adopts the longer mask and converts the route into a series of route advertisements that cover the full address space. If you select NoDeAggregate for the outgoing port, route deaggregation is not performed.

To use RIP with variable length subnet masks, use aggregation/deaggregation only in simple topologies, such as a single border router between the backbone and stub network. The backbone has a shorter mask with non-overlapping routes. All subnets with the same aggregate must be fully connected and contiguous. Do not use the aggregate/deaggregate scheme with unnumbered PPP links; use the -RIPIP CONTrol parameter's NetAdvUnn | SubnetAdvUnn values.

DynamicNbr | NoDynamicNbr	If DynamicNbr is selected, new addresses are learned through the Inverse Address Resolution Protocol (InARP) or static configuration, and RIP's AdvToNeighbor list is updated. If NoDynamicNbr is selected, RIP's AdvToNeighbor list is not updated with new addresses. This option only applies to Frame Relay, X.25, and ATM; it has no effect for other media types and is not displayed for other media.
FullMesh | NonMesh	If FullMesh is selected, regular split horizon is applied. If NonMesh is selected, next-hop split horizon is applied. These options apply only to Frame Relay, X.25, and ATM; it has no effect and is not displayed for other media types. When routing over IP in a nonmeshed topology over Frame Relay or X.25, you must set DefaultMetric on the root router to 15.

DefaultMetric

Syntax

```
SETDefault !<port> -RIPIP DefaultMetric = <metric>(0–15)
SHow [!<port> | !*] -RIPIP DefaultMetric
```

Default 0

Description The DefaultMetric parameter specifies whether RIP advertises the default route. The default route is the network with Internet address 0.0.0.0 and is reported with a metric equal to the value of this parameter. If DefaultMetric is 0, the default route is advertised with a metric equal to the value stored in the routing table only if the default route is dynamically learned and the policy allows this to occur.

When routing over IP in a nonmeshed topology over Frame Relay or X.25, you must set the DefaultMetric parameter on the root router to 15.

ExteriorPolicy

Syntax

```
ADD !<port> -RIPIP ExteriorPolicy All | None | [~]<IP address>
   [<metric>(0–15)]
DELete !<port> -RIPIP ExteriorPolicy All | <IP address>
SHow [!<port> | !*] -RIPIP ExteriorPolicy
```

Default None

Description The ExteriorPolicy parameter determines which routes learned by the Border Gateway Protocol (BGP) are reported by RIP. To add a network and its associated metric to the list, use the ADD command. There is no limit to the number of networks that can be added per port. When All is used in the ADD command, all routes learned from BGP are reported on this port.

A route specified by ExteriorPolicy is reported only if AdvertisePolicy is either All or contains the IP address specified by ExteriorPolicy.

Values

All	Reports all routes learned from BGP, provided those routes are allowed to be reported by the AdvertisePolicy.
None	None of the routes learned from BGP are reported.
<IP address>	Specifies the Internet address to be reported.

~ When used in the ADD command, all routes are reported except the one specified. In this format, no metric should be included in the command syntax. For example, if you enter the following command, all routes except 12.0.0.0 are advertised on port 1:

```
ADD !1 -RIPIP ExteriorPolicy ~12.0.0.0
```

The ExteriorPolicy list includes only the entry ~12.0.0.0 instead of all the routes being advertised.

<metric> If an Internet address is specified, the metric is optional. If you decide to specify a metric, specify a value between 1 and 15. This value can be based on bandwidth or utilization. The route and this specified metric are reported. If you decide not to specify a metric, specify 0.

You can also specify a metric for exterior policy routing protocols through the ImportMetric parameter. For more information, refer to "ImportMetric" on page 47-8.

Adding to the List. The following example shows how a series of ADD -RIPIP ExteriorPolicy commands affects the list of routes to be advertised. Enter:

```
ADD !1 -RIPIP ExteriorPolicy 12.0.0.0
ADD !1 -RIPIP ExteriorPolicy 13.0.0.0
ADD !1 -RIPIP ExteriorPolicy 14.0.0.0
```

The list of routes advertised on port 1 now contains 12.0.0.0, 13.0.0.0, and 14.0.0.0. RIP does not advertise any BGP routes other than these. Enter:

```
ADD !1 -RIPIP ExteriorPolicy ~14.0.0.0
```

The ExteriorPolicy list now contains the entry ~14.0.0.0, and RIP advertises all the BGP routes except 14.0.0.0 on port 1.

Enter:

```
ADD !1 -RIPIP ExteriorPolicy 15.0.0.0
```

Because the tilde is absent from this command, it overrides the previous ADD !1 ExteriorPolicy ~14.0.0.0 command. That is, the ~14.0.0.0 entry is replaced by 15.0.0.0 in the ExteriorPolicy list. The router now only advertises 15.0.0.0 on port 1.

The list of routes to be advertised is overridden by the most recent ADD -RIPIP ExteriorPolicy command if you switch from not using a tilde to using a tilde or vice versa.

Deleting from the List. To delete a route in the ExteriorPolicy list, use the DELete command. The following example deletes a route:

```
DELete !1 -RIPIP ExteriorPolicy 15.0.0.0
```

The router now does not advertise 15.0.0.0 on port 1.

If the ExteriorPolicy list contains an entry with a tilde and you want to delete it, specify the Internet address in the DELete command. You do not need to include the tilde. If you specify an IP address with an associated metric and you want to delete it, you do not need to include the metric value in the DELete command.

For example, to indicate that all routes except 14.0.0.0 are advertised on port 1 with metric 7 enter:

```
ADD !1 -RIPIP ExteriorPolicy ~14.0.0.0 7
```

You can later enter the following command to nullify it:

```
DELete !1 -RIPIP ExteriorPolicy 14.0.0.0
```

This DELete command removes ~14.0.0.0 from the ExteriorPolicy list. The router no longer advertises the routes that were advertised as a result of the previous ADD -RIPIP ExteriorPolicy command.

By default, the list of advertised routes is empty, which indicates that no BGP-derived routes are advertised.

SHow -RIPIP ExteriorPolicy displays the list of routes reported by RIP. If no routes exist in the list, none are displayed.

ImportMetric

Syntax

```
ADD -RIPIP ImportMetric <from protocol> Multiply | Divide <operand>
DELete -RIPIP ImportMetric <from protocol>
SHow -RIPIP ImportMetric
```

Default Multiply/Divide

From protocol	Operation	Operand
OSPF	Divide	4096
IISIS	Divide	64
BGP	Divide	1024
Static	Divide	1

Description The ImportMetric parameter allows you to manipulate the formula that RIP uses to convert a metric from the routing table into one that it understands. When an interior, exterior, or static policy is enabled on a port using InteriorPolicy, ExteriorPolicy, or StaticPolicy, RIP imports the appropriate type of route from another routing domain. If you do not specify a metric with InteriorPolicy, ExteriorPolicy, or StaticPolicy, then the imported route is reported with a metric calculated from the routing table.

The following are the default conversion formulas RIP uses:

- Interior policy
- RIP metric = (OSPF metric / 4096)
- RIP metric = (IISIS metric / 64)
- Exterior policy:
- RIP metric = (BGP metric / 1024)
- Static policy:
- RIP metric = (STATIC metric / 1)

If the conversion results in a value greater than or equal to 16, RIP advertises the route using the metric 16.

Values

<from protocol>	Specifies the routing protocol that learns the dynamic or static route that is being imported. You can specify OSPF, Integrated Intermediate System-to-Intermediate System (IISIS), BGP, or static.
<Multiply | Divide>	Determines how you want to manipulate the formula that RIP uses to convert the metrics.

<operand> Specifies the number in the conversion formula RIP uses that you multiply or divide the OSPF, IISIS, BGP, or static metric by.

InteriorPolicy

Syntax

```
ADD !<port> -RIPIP InteriorPolicy All | None | [~]<IP address>
   [<metric>(0–15)]
DELete !<port> -RIPIP InteriorPolicy All | <IP address>
SHow [!<port> | !*] -RIPIP InteriorPolicy
```

Default None

Description The InteriorPolicy parameter determines which routes learned by OSPF or Integrated IISIS are reported by RIP.

To add a network and its associated metric to the list, use the ADD command. There is no limit to the number of networks that can be added per port. When All is used in the ADD command, all routes learned from OSPF or Integrated IS-IS are reported on this port.

A route specified by InteriorPolicy is reported only if AdvertisePolicy is either All or contains the IP address specified by InteriorPolicy.

Values

All Reports all routes learned from OSPF or Integrated IS-IS, provided those routes are allowed to be reported by the AdvertisePolicy.

None None of the routes learned from OSPF or Integrated IS-IS are reported.

<IP address> Specifies the Internet address to be reported with the ADD command or deleted with the DELete command.

~ When used in the ADD command, reports all routes except for the one specified. In this format, no metric should be included in the command syntax. For example, if you enter the following command, all routes except 12.0.0.0 are advertised on port 1:

```
ADD !1 -RIPIP InteriorPolicy ~12.0.0.0
```

The InteriorPolicy list includes only the entry ~12.0.0.0 instead of than all the routes being advertised.

<metric> If an Internet address is specified, the metric is optional. If you decide to specify a metric, specify a value between 1 and 15. This value can be based on bandwidth or utilization. The route and this specified metric are reported. If you decide not to specify a metric, specify 0.

You can also specify a metric for interior policy routing protocols through the ImportMetric parameter. For more information, refer to “ImportMetric” on page 47-8.

InteriorPolicy functions in the same way as ExteriorPolicy. (For more information, refer to “ExteriorPolicy” on page 47-6.)

RcvFromNeighbor

Syntax

```
ADD !<port> -RIPIP RcvFromNeighbor [~]<IP address>
DELete !<port> -RIPIP RcvFromNeighbor <IP address>
SHow [!<port> | !*] -RIPIP RcvFromNeighbor
```

Default No default

Description The RcvFromNeighbor parameter modifies or displays the list of routers from which RIP accepts packets. It is a port-dependent parameter. If RcvFromNeighbor has been configured but no routers are directly connected, the bridge/router does not receive RIP updates. When this happens, this command lists the addresses of RcvFromNeighbor as NONE.

You can configure this parameter on port 0 to determine the set of routers from which the router, which serves as a bridge, collects RIP update packets.

Adding to a List. Add an address to the RcvFromNeighbor list using the ADD command syntax. If a tilde (~) precedes the Internet address in the ADD command, the command affects all Internet addresses configured for that port except the address specified, for example:

```
ADD !2 -RIPIP RcvFromNeighbor ~10.0.0.1
```

This example specifies that port 2 accepts all RIP packets received from all routers except the one with Internet address 10.0.0.1.

If the RcvFromNeighbor list already consists of addresses that were added with ADD commands without tildes, and you are entering an ADD command that includes a tilde, the latter ADD command takes precedence. The following example shows how a series of ADD commands affects the RcvFromNeighbor list. Enter:

```
ADD !1 -RIPIP RcvFromNeighbor 12.1.0.1
ADD !1 -RIPIP RcvFromNeighbor 12.2.0.2
ADD !1 -RIPIP RcvFromNeighbor 12.3.0.3
```

The RcvFromNeighbor list on port 1 now contains 12.1.0.1, 12.2.0.2, and 12.3.0.3. Suppose later you enter:

```
ADD !1 -RIPIP RcvFromNeighbor ~12.3.0.4
```

The original list of routers, which consists of three Internet addresses, is replaced by ~12.3.0.4, which indicates that RIP packets from all routers are accepted on port 1 except the ones that are sent by 12.3.0.4.

If you enter:

```
ADD !1 -RIPIP RcvFromNeighbor 12.4.0.4
```

This most recently entered command overrides the existing values on the list. That is, only RIP packets from 12.4.0.4 are accepted on port 1.

Deleting from a List. To delete an address from the RcvFromNeighbor list, use the DELete command. The following is an example that deletes an address from the list:

```
DELete !1 -RIPIP RcvFromNeighbor 15.0.0.1
```

Now RIP packets from 15.0.0.1 are not accepted on port 1.

If the RcvFromNeighbor list contains an entry with a tilde, and you want to delete it, specify the Internet address in the DELete command. You do not need to include the tilde.

For example, to indicate that all RIP packets are accepted except the ones from 14.0.0.1, enter:

```
ADD !1 -RIPIP AdvertisePolicy ~14.0.0.1
```

You can later enter the following command to nullify it:

```
DELete !1 -RIPIP AdvertisePolicy 14.0.0.1
```

This DELete command removes ~14.0.0.1 from the RcvFromNeighbor list. As a result, the router no longer accepts RIP packets from routers other than 14.0.0.1.

When all of the neighbors configured using RcvFromNeighbor have been deleted, the router resumes the default configuration of All.

By default, RIP accepts update packets from all neighbors.

RcvSubnetMask

Syntax

```
ADD -RIPIP RcvSubnetMask <IP address>-<IP address> <subnet mask>
DELete -RIPIP RcvSubnetMask <IP address>-<IP address>
SHow -RIPIP RcvSubnetMask
```

Default No default

Description The RcvSubnetMask parameter provides variable length subnet masks in your network in a range table mask scheme with RIPIP as the routing protocol. By providing the proper subnet mask for each known subnet, the receiving router can interpret an incoming route advertisement, assign an appropriate subnet mask to it, and determine the correct forwarding path.

The range table mask scheme can be used with more complex network topologies than those used for the route aggregate/deaggregate scheme (specified through the -RIPIP CONTrol parameter); no limit on the number of potential subnet masks exists, and overlapping routes can exist (10.2.0.0 255.255.0.0 and 10.2.2.0 255.255.255.0 can co-exist at the same time). The range table mask scheme should be used with routes learned over unnumbered Point-to-Point Protocol (PPP) links. For more information, refer to “Configuring RIPIP for Networks with Variable Length Subnet Masks” on page 6-10 in *Using NETBuilder Family Software*.

Values

<IP address>-<IP address>	Specifies an address range over which the following <subnet> applies. For example, 10.1.0.0–10.1.255.0 specifies that all routes within the range should be assigned the <subnet mask> value.
<subnet mask>	Specifies the subnet mask to be applied to the address range. You can configure any length subnet mask to any network number; the subnet mask can be longer or shorter than its natural mask. You are not, however, allowed to assign a subnet mask to the default route (0.0.0.0).

ReceivePolicy

Syntax

```
ADD !<port> -RIPIP ReceivePolicy All | None | [~]<IP address>
   [<metric>(0–15)]
DELete !<port> -RIPIP ReceivePolicy All | <IP address>
SHow [!<port> | !*] -RIPIP ReceivePolicy
```

Default All

Description ReceivePolicy filters routing updates from trusted neighbors. It allows you to control which RIP routes are received and stored in the routing table.

To add a network and its metric to the list, use the ADD command. There is no limit to the number of networks that can be added per port. When All is used in the ADD command, all routes learned from trusted neighbors are reported on this port.

Values

All	Receives or stores all routes reported by trusted neighbors in the routing table.
None	None of the routes reported by trusted neighbors are received or stored in the routing table.
<IP address>	Specifies the Internet address to be received with the ADD command or deleted with the DELete command.
~	When used in the ADD command, all routes are received except for the one specified. In this format, no metric should be included in the command syntax. For example, if you enter the following command, all routes except 12.0.0.0 will be received on port 1: **ADD !1 -RIPIP ReceivePolicy ~12.0.0.0**
<metric>	The metric is optional if either All or an Internet address is specified. If a metric value in the range of 1 to 15 is specified, the route is entered into the routing table with the specified metric. If the metric 0 is used, the route is reported with the metric in the received route.

StaticPolicy

Syntax

```
ADD !<port> -RIPIP StaticPolicy All | None | [~]<IP address>
   [<metric>(0-15)]
DELete !<port> -RIPIP StaticPolicy All | <IP address>
SHow [!<port> | !*] -RIPIP StaticPolicy
```

Default None

Description The StaticPolicy parameter filters the reporting of static routes. To add a network and its associated metric to the list, use the ADD command. There is no limit to the number of networks that can be added per port. When All is used in the ADD command, all routes that have been added with the ADD -IP ROUte command are reported on this port.

A static route specified by StaticPolicy is reported only if AdvertisePolicy is All or contains the IP address specified by StaticPolicy.

Values

All — Reports all static routes, provided those routes are allowed to be reported by the AdvertisePolicy.

None — None of the static routes are reported.

<IP address> — Specifies the Internet address to be reported with the ADD command or deleted with the DELete command.

~ — When used in the ADD command, all routes are reported except for the one specified. In this format, no metric should be included in the command syntax. For example, if you enter the following command, all routes except 12.0.0.0 are advertised on port 1:

```
ADD !1 -RIPIP StaticPolicy ~12.0.0.0
```

The StaticPolicy list includes only the entry ~12.0.0.0 instead of all the routes being advertised.

<metric> — If an Internet address is specified, the metric is optional. If you decide to specify a metric, specify a value between 1 and 15. This value can be based on bandwidth or utilization. The route and this specified metric are reported. If you decide not to specify a metric, specify 0.

You can also specify a metric for static routes through the ImportMetric parameter. For more information, refer to "ImportMetric" on page 47-8

UpdateTime

Syntax

```
SETDefault -RIPIP UpdateTime = <seconds>(5–5400)
SHow -RIPIP UpdateTime
```

Default 30

Description The UpdateTime parameter specifies the time interval in seconds within which RIP sends update packets.

This parameter determines how long a route learned through RIP stays in the IP Routing Table. For example, once a route is in the routing table, the router must receive a RIP update packet indicating the reachability of this route every 180 seconds (six times the value of UpdateTime). If no updates are received before the timer expires, the route changes from Up state to Garbage Collection state and it is eventually deleted from the routing table.

48

RIPXNS SERVICE PARAMETERS

This chapter describes the Routing Information Protocol (RIP) parameters for Xerox Network Systems (XNS) protocol routing. Table 48-1 lists the Routing Information Protocol for XNS (RIPXNS) Service parameters and commands.

Table 48-1 RIPXNS Service Parameters and Commands

Parameters	Commands
ADDRess	ADD, DELete, SHow, SHowDefault
CONFiguration	SHow
CONTrol	SETDefault, SHow, SHowDefault
UpdateTime	SETDefault, SHow, SHowDefault

ADDRess

Syntax

```
ADD !<port> -RIPXNS ADDRess %<host> <media address>
DELete !<port> -RIPXNS ADDRess %<host>
SHow [!<port> | !*] -RIPXNS ADDRess
SHowDefault [!<port> | !*] -RIPXNS ADDRess
```

Default No default (XNS Address Mapping Table is empty)

Description The ADDRess parameter modifies and displays the list of neighbor addresses that RIP uses to determine to which WAN neighbors it should send update packets. It is a port-dependent parameter. The port number is mandatory in the ADD and DELete command; it is optional in the SHow command. Any number of neighbors can be configured.

The address can be added by mapping the media access control (MAC) address of a remote host to the corresponding X.25, Frame Relay data link connection identifier (DLCI), or Switched Multimegabit Data Service (SMDS) address. If you map the MAC address of a remote host to the Frame Relay DLCI or SMDS address, you can enable dynamic address mapping by setting Frame Relay CONTrol to either LMI or ANsiLMI and adding an SMDS group address (-IDP SMDSGroupAddr), respectively. If a participating router is running earlier than 5.0 router software, select the OldNbrMap option of -RIPXNS CONTrol and add a neighbor address according to the new syntax.

You must configure a neighbor address if you want RIPXNS to pass routing information over X.25, Frame Relay, or SMDS. When no addresses are configured, RIPXNS traffic is not passed over X.25, Frame Relay, or SMDS.

To remove an entry from the XNS address table, use the DELete command.

Use SHow to display XNS neighbor addresses for a particular port. If you do not specify a port, neighbor addresses for all ports are shown.

Values

%<host> Specifies the host address, consisting of the Ethernet address (12 hexadecimal digits) preceded by a percent sign (%).

<media address> You can map the MAC address of a remote host to an X.25 or Frame Relay data link connection identifier, or SMDS address.

X25 addr Specifies the data terminal equipment (DTE) address used for adding X.25 neighbors. It indicates the DTE address of the closest router through which the network can be reached. You can use the uppercase letters DTE or the pound sign (#).

DLCI Specifies the DLCI used for adding Frame Relay neighbors. You can use the uppercase letters DLCI or the at sign (@).

SMDS Specifies an individual SMDS address used to add SMDS neighbors. Because XNS learns SMDS neighbors dynamically, when the -IDP SMDSGroupAddr is configured, you do not need to add neighbors that use an SMDS group address.

CONFiguration

Syntax

```
SHow [!<port> | !*] -RIPXNS CONFiguration
```

Default No default

Description The CONFiguration parameter displays the values of the configurable parameters (CONTrol, ADDRess, and UpdateTime) in the RIPXNS Service.

CONTrol

Syntax

```
SETDefault !<port> -RIPXNS CONTrol = ([Enabled | Disabled], [Trigger |
  NoTrigger], [Poison | NoPoison], [NewNbrMap | OldNbrMap], [GlobBcast |
  NoGlobBcast])
SHow [!<port> | !*] -RIPXNS CONTrol
SHowDefault [!<port> | !*] -RIPXNS CONTrol
```

Default Enabled, Trigger, NoPoison, NewNbrMap, GlobBcast

Description The CONTrol parameter enables or disables RIPXNS on each port. This parameter also lets you control the way routing tables are updated.

Values

Enabled | Disabled Enabled allows RIPXNS to learn and advertise routes on the specified port. Disabled does not allow RIPXNS to learn or advertise routes on the specified port.

For more information on the effects of different combinations of settings of the CONTrol parameters in Internet Datagram Protocol (IDP) and RIPXNS, refer to Chapter 18 in *Using NETBuilder Family Software*.

Trigger | No Trigger Determines if RIP sends trigger update packets. Trigger update packets are sent when a route's metric has changed. By sending these update packets, RIP does not need to wait for the update interval, allowing earlier notification that a route's metric has changed.

When the network topology has not changed, no triggered update packets are sent.

Poison | NoPoison — Determines how the router treats a routing table entry learned from another router when it returns information from its routing table to the router from which the entry was learned. For more information about using this option, refer to “Network Reachability and Split Horizon” on page 18-10 in *Using NETBuilder Family Software*.

NewNbrMap | OldNbrMap — Specifies the bridge/router’s support address mapping for all software versions. NewNbrMap is the default. If software version is earlier than 5.0, use option OldNbrMap.

GlobBcast | NoGlobBcast — When CONTrol is set to GlobBcast, XNS global broadcast packets (destination network = 0xFFFFFFFF) are forwarded to all interfaces except the incoming port. Extra checking is in place to prevent loopback packets.

The GlobBcast option is required to support some application programs that use global broadcasts. Enabling the GlobBcast option results in some network overhead.

UpdateTime

Syntax

```
SETDefault -RIPXNS UpdateTime = <seconds> (10–65535)
SHow -RIPXNS UpdateTime
SHowDefault -RIPXNS UpdateTime
```

Default 30

Description The UpdateTime parameter specifies how often the router sends broadcast packets to let other routers know about its routing table, and it determines the interval between RIPXNS updates.

49 SAP SERVICE PARAMETERS

This chapter describes all the parameters that are related to Service Advertising Protocol (SAP) routing. Table 49-1 lists the SAP Service parameters and commands.

Table 49-1 SAP Service Parameters and Commands

Parameters	Commands
AdvertisePolicy	ADD, DELete, SHow
AdvToNeighbor	ADD, DELete, SHow
CONFiguration	SHow
CONTrol	SETDefault, SHow
HoldTimeFactor	SETDefault, SHow
PolicyControl	SETDefault, SHow
PreferredServer	ADD, DELete, SHow, SHowDefault
RcvFromNeighbor	ADD, DELete, SHow
ReceivePolicy	ADD, DELete, SHow
UpdateTime	SETDefault, SHow

AdvertisePolicy

Syntax

```
ADD !<port> -SAP AdvertisePolicy [~]<services>, [<list of
  services>]
DELete !<port> -SAP AdvertisePolicy {All | <list of services>}
SHow [!<port> | !*] -SAP AdvertisePolicy
SHowDefault [!<port> | !*] -SAP AdvertisePolicy
```

Default No default (no service advertisement policies defined)

Description The AdvertisePolicy parameter specifies which services are advertised on the port to adjacent routers.

The lists of services can be entered as part of one command with each service separated by a comma (,). For example:

```
<list of services>:=[~]<service>,[<list of services>]
```

To include only specific services for advertisement, use the ADD command. To exclude specific services from advertisement, use the ADD command with the tilde (~) prefix added to the entry. When ~ is used for one service specification, it must be used for all. If exclusion lists are mixed with inclusion lists, an error message appears. When you need to change the service list from one type (inclusion or exclusion) to the other, the current list must first be deleted before the new list can be added.

The maximum number of characters allowed for the server name in the AdvertisePolicy parameter is 15. In software versions 7.2 and higher, when you add the server name (a maximum of 15 characters) and you reboot the NETbuilder, the policy has truncated the server name to 15 characters and appears to be counting the quotation mark as one of the characters allowing you only 14 characters for your server name.

The wildcard character, an asterisk (*), can be used to include or exclude entire ranges or classes of services. For example, to identify all services on all hosts in the range of network numbers from 4ABC to 4ABE, both inclusive, enter:

```
&4ABC-&4ABE:*:*
```

To remove a specific service, a list of service, or the entire list of configured services, use DELete. The All option deletes all the service policies for the specified interface.

The SHow command displays the configured list of services in the advertise policy. When SHow is used with a port number, only those advertise policy entries that are associated with that port are displayed. When a port number is not specified, all advertise policy entries for all the ports on the system are displayed.

Values <list of services> Represents the route, server address, service name, and the service type. For example:

<service>:=<route>:[<service type>]|[<route>]:"<server name>":[<service type>]

<server name> A string up to 15 characters including the single wildcard asterisk (*) character. The asterisk specifies a substring match. For example:

<server name>:=<string>(1–15 chars)

<service type> A 16-bit hexadecimal number describing the type of service that is located on a host. For example:

<service type>:=<16-bit hex number> (0-FFFF)

Example 1 To set up an exclusion list where all services except those that are located on network 40, those that are of type 3 (on any network, any host), and those that are located on any network, all services are advertised on interface 1, enter:

```
ADD !1 -SAP AdvertisePolicy ~&40:*:*, ~*:*:3
```

Example 2 To add all server names beginning with "LA" and "NY" that have the file service to a list of services being advertised on interface 2, enter:

```
ADD !2 -SAP AdvertisePolicy "LA*":4, "NY*":4
```

AdvToNeighbor

Syntax

```
ADD !<port> -SAP AdvToNeighbor <network>%<mac address> [...]
DELete !<port> -SAP AdvToNeighbor ALL | <network>%<mac address>
  [...]
SHow [!<port> | !*] -SAP AdvToNeighbor
SHowDefault [!<port> | !*] -SAP AdvToNeighbor
```

Default No default (no neighbors configured to advertise to)

Description The AdvToNeighbor parameter specifies which neighbors on each interface receive service reachability information. You can enter a list of neighbors as part of a single command with each neighbor separated by a comma. For example:

```
<network>%<mac address>, <network>%<mac address>, <network>%<mac
  address>
```

The list of neighbors is used when broadcasting service reachability information and when responding to a specific service query from a specific station. If the requesting station address is not part of the neighbor list, then no response is sent.

Inverse entries are not allowed for the AdvToNeighbor list. When an AdvToNeighbor list is specified and enabled through PolicyControl, instead of through the regular SAP broadcasts, the router sends the SAP messages as separate unicast messages to each neighbor listed.

To add to the neighbor list, use the ADD command.

To remove neighbors from the neighbor list of a port, use DELete and specify the port number and the neighbor address, or specify the port number and the keyword ALL to delete multiple entries for the same port.

The SHow command displays the list of entries in the neighbor list. If the optional port number is not specified, all active neighbor lists are displayed. The display shows both the static and dynamically learned neighbors with the static neighbors indicated by the * symbol. Only static neighbors can be deleted.

Values <network> Supply the network number in the following format:

```
[%]<48-bit MAC address in native format>
MAC <48-bit MAC address in canonical format>
NcMac <48-bit MAC address in canonical format>
```

%<mac address> The 48-bit media access control (MAC) address of the host. The MAC address must be entered in the same format (canonical or noncanonical) as used by the host.

CONFiguration

Syntax `SHow [!<port> |!*] -SAP CONFiguration`

Default No default display

Description The CONFiguration parameter displays the current SAP configuration parameters. If no port number is specified, active information is displayed. Active means the -IPX CONTrol is set to ROute and the -IPX NETnumber is configured. If -IPX CONTrol is not set to ROute, the following message is displayed:

```
IPX is not enabled. Please configure CONTrol and assign NETnumbers
```

Assuming -IPX CONTrol is set to ROute, the message displays active configuration information for ports assigned with IPX network numbers. This has been changed in an effort to reduce console output. In the case of static routes, address mapping, policies and neighbors, even headers are suppressed if their corresponding tables are empty.

CONTrol

Syntax

```
SETDefault !<port> -SAP CONTrol = (Auto, [Talk | NoTalk],
  [Listen | NoListen], [PEriodic | NoPEriodic], [DynamicNbr |
  NoDynamicNbr])
SHow [!<port> |!*] -SAP CONTrol
SHowDefault [!<port> |!*] -SAP CONTrol
```

Default Auto, PEriodic, and DynamicNbr on nonbroadcast multiaccess (NBMA) interfaces

Description The CONTrol parameter enables or disables whether SAP packets are updated or sent. The Internetwork Packet Exchange (IPX) router forwards these packets when CONTrol is set to Talk.

Values

Auto

If Auto is selected, the Talk | NoTalk and Listen | NoListen values are not displayed in the user interface. The Talk and Listen modes are dynamically determined by the software and the current network topology when Auto is selected. Use the SHow -IPX DIAGnostics command to display the current Talk | Listen mode.

When either Talk or NoTalk or Listen or NoListen are selected, the Auto state is inactive.

Talk | NoTalk

If Talk is selected, SAP sends services information to its neighbors and dynamically maintains the routing table. If NoTalk is selected, dynamic and regular SAP updates are not sent.

Listen | NoListen

If Listen is selected, the router receives SAP updates and updates packets. If NoListen is selected, the router does not receive SAP updates or update packets.

PEriodic | NoPEriodic

If PEriodic is selected, the IPX router periodically generates SAP updates. To stop periodic SAP update, select the NoPEriodic option. After you set NoPEriodic, the IPX router shuts off periodic SAP updates and switches to incremental updates. When selecting this option, make sure that all participating routers use the same option. NoPEriodic can be used for all media.

Noisy and expensive network chatting of SAP updates can be virtually eliminated by setting CONTrol to NoPEriodic. This setting is recommended in a stable and reliable network while periodic SAP updates are recommended where frequent topology changes occur.

DynamicNbr | NoDynamicNbr

Neighbor learning is enabled by default on an NBMA interface. With Neighbor learning enabled, the dynamic neighbor list is automatically created, and SAP operates correctly without requiring you to configure static neighbor information. Use the AdvToNeighbor parameter to display the learned dynamic neighbors.

With DynamicNbr on, SAP includes dynamically learned neighbors in the AdvToNeighbor table. Dynamic AdvToNeighbor neighbors then stay in the AdToNeighbor table and are considered “trusted neighbors”. These dynamically learned neighbors can only be deleted by resetting -SAP CONTrol to NoDynamicNbr.

The DynamicNbr option is only available on ports that are NBMA networks, such as X.25 and Frame Relay. This option is not displayed for non-NBMA networks.

When communicating with a bridge/router running a pre-7.0 software version on a WAN link, the -SAP CONTrol parameter must be set to NoPEriodic.

HoldTimeFactor

Syntax

```
SETDefault -SAP HoldTimeFactor = <number> <1-24>
SHow -SAP HoldTimeFactor
SHowDefault -SAP HoldTimeFactor
```

Default 3

Description The HoldTimeFactor parameter calculates the aging out time. For each SAP entry learned from a particular port, the age-out time is calculated by multiplying the UpdateTime of the port and the HoldTimeFactor. The learned SAP entry is aged out if no further update for that service is received within the age-out timeframe.

PolicyControl

Syntax

```
SETDefault !<port> -SAP PolicyControl = ([AdvPolicy |
  NoAdvPolicy], [RcvPolicy | NoRcvPolicy], [PolicyOverride |
  NoPolicyOverride], [BestSvrReply | NoBestSvrReply], [AdvToNbr |
  NoAdvToNbr], [RcvFromNbr | NoRcvFromNbr])
SHow [!<port> | !*] -SAP PolicyControl
SHowDefault [!<port> | !*] -SAP PolicyControl
```

Default All policies are disabled except BestSvrReply.

Description The PolicyControl parameter enables and disables the use of policy parameters, such as AdvertisePolicy and ReceivePolicy. If a policy is enabled and the corresponding policy list is empty, the policy is still applied. For example, if RcvPolicy is selected and the ReceivePolicy list is empty, then no services are accepted. If the RcvFromNbr is selected and RcvFromNeighbor list is empty, then none of the SAP updates from any neighbor are accepted.

To enable policies use the SETDefault command. To display the current policies configured for the router, use the SHow command.

Values

PolicyOverride | NoPolicyOverride	Overrides the configured policies when the router responds to specific SAP requests while applying them as configured for regular SAP updates. Do not use PolicyOverride for serial interfaces.
BestSvrReply | NoBestSvrReply	Controls whether or not the router is permitted to respond to “get nearest server” requests.

PreferredServer

Syntax

```
ADD !<port> -SAP PreferredServer “<server name>”
  [,“<server name>”...]
DELete !<port> -SAP PreferredServer ALL | “<server name>”
  [,“<server name>”...]
SHow [!<port> | !*] -SAP PreferredServer
SHowDefault [!<port>| !*] -SAP PreferredServer
```

Default No default (no preferred server configured)

Description The PreferredServer parameter offers a specific server (not the one selected on the basis of split-horizon and best-cost) in response to a client “get nearest server” request. You can use this feature when there are more users to serve than a primary server is licensed to handle, and there is a backup server available. Once a list of preferred servers is configured, the IPX router responds to “get nearest server” requests with one of the reachable preferred servers regardless of the server location or number of hops.

If no preferred server is available, the normal selection process of the nearest server takes place. The primary server and backup server can alternately serve all the users and lessen the burden on the primary server. When you add preferred servers be sure that at least one preferred server is reachable and that service advertise policies do not exclude them.

You can also use PreferredServer when a local server is configured to not respond to “get nearest server” requests and the designated primary boot server is multiple hops away. NetWare 4.0 clients and pre-4.0 clients specify different service types in their “get nearest server” requests. Pre-4.0 clients use File Server type (0x0004) while 4.0 clients are looking for Directory Name Server type (0x026B); appropriate preferred servers must be added.

SAP neighbors are routers that share a common network and participate in the SAP Protocol. Each SAP packet can be either broadcast or addressed individually to each neighbor.

If no neighbors are configured on the port, SAP broadcasts update packets on the port. To include or remove an address, use the ADD and DELete commands.

SHow displays the active neighbors. Some neighbors on the disk may be invalid if they are not connected to the network to which the router port is connected. Invalid neighbors can become valid after they have been directly connected. By default, the Neighbor list is empty.

Neighbors must be configured on a serial port that is running X.25, Frame Relay, or Asynchronous Transfer Mode (ATM) because these protocols do not support broadcast facilities. For each X.25, Frame Relay, or ATM neighbor configured, static entries must be added to the IPX Address Table with corresponding media addresses (data terminal equipment (DTE) for X.25, data link connection identifier (DLCI) for Frame Relay, or VCID for ATM).

Preferred servers should be configured for the local service when using dial, or the link will try to be established to remote sites.

RcvFromNeighbor

Syntax

```
ADD !<port> -SAP RcvFromNeighbor <list of MAC addresses>
DELete !<port> -SAP RcvFromNeighbor ALL | <list of MAC addresses>
SHow [!<port> | !*] -SAP RcvFromNeighbor
SHowDefault [!<port> | !*] -SAP RcvFromNeighbor
```

Default No default (no neighbors configured from which to receive advertisements)

Description The RcvFromNeighbor parameter defines neighbors (next hop routers) from which SAP advertisements will be accepted on the specified interface.

The lists of neighbors can be entered as part of one command. For example:

```
<list of MAC addresses>, <list of MAC addresses>, <list of MAC
  addresses>
```

Use a tilde (~) before the neighbor specification to exclude it from the list of neighbors. Inverse policy specifies that all SAP updates must be received from all neighbors, except for the ones explicitly configured in the RcvFromNeighbor list. When ~ is used for one neighbor specification, it must be used for all. If exclusion lists are mixed with inclusion lists, an error message is issued. When you need to change a list from one type (inclusion or exclusion) to the other, the current list must first be deleted before the new list can be added. For more information, refer to "Configuring Other Policy Settings" on page 13-26 in *Using NETBuilder Family Software*.

Values <list of MAC addresses> The 48-bit MAC address of the host. The MAC address must be entered in the same format (canonical or noncanonical) as used by the host. For example:

```
[%]<48-bit MAC address in native format>
Mac <48-bit MAC address in canonical format>
NcMac <48-bit MAC address in canonical format>
```

ReceivePolicy

Syntax

```
ADD !<port> -SAP ReceivePolicy [~]<service>, [<list of services>]
DELete !<port> -SAP ReceivePolicy {All | <list of services>}
SHow [!<port> | !*] -SAP ReceivePolicy
SHowDefault [!<port> | !*] -SAP ReceivePolicy
```

Default No default (no service receive policies defined)

Description The ReceivePolicy parameter specifies which services reported in the routing updates by adjacent routers are accepted on the specified interface and cached in the local routing tables. ReceivePolicy is specified per port.

To accept only specific services reported in adjacent routers' SAP updates, use the ADD command to add a list of services to the port receive list. To exclude specific services in adjacent routers' routing updates, use the ADD command with the tilde (~) prefix to indicate an inverse route or service.

The receive list of a port can contain only normal or inverse services. If an inverse service exists in a port receive list and you want to change that service to a normal route, use the DELete command to remove all of the existing services in that port advertise list. Follow the same procedure to change a normal service to an inverse service.

To remove a service from the services list, use the DELete command. To indicate all services use the All value.

SHow displays the list of service entries in the specified port receive list. If the optional port number is not specified, all existing receive lists are displayed. Inverse services are indicated by a tilde (~) prefix.

Values <list of services> This value consists of several elements (route, server address or server name, service type). For example:

```
<service:=<route>:<server address>:[<service type] |
  [<route>]:"<server name>":[<service type>]
```

<server address> The 48-bit MAC address of the host on which the service resides. The full 48-bit address must be specified. The server address must be entered in the same format (canonical or noncanonical) as advertised by the server. For example:

```
<server address>:=[%]<48-bit MAC address in native
format>| MAC <48-bit MAC address in canonical format> |
NcMac <48-bit MAC address in canonical format>
```

<server name> Up to 15 characters that can include the single wildcard asterisk (*) character to specify a substring match.

<service type> A 16-bit number that specifies the type of service that is located on a given host.

The wildcard character, asterisk (*), can be used to include or exclude entire ranges or classes of servers or services. For example:

*:080002451234:04 identifies a service with type 04 on a host whose MAC address is 080002451234, no matter what network this host resides on.

&4ABC:*:04 identifies all hosts on network number 4ABC that offer service type 04.

&4ABC:*:* identifies all services on all hosts on network number 4ABC.

&4ABC-&4ABE:*:* identifies all services on all hosts in the range of network numbers from 4ABC to 4ABE, both inclusive.

Example 1 To set up an exclusion list where all services except those located on network 40, those of type 4 (on any network and any host) and those located on a host with the MAC address 080002451234 (on any network and all services) are accepted on port 1, enter:

```
ADD !1 -SAP ReceivePolicy ~&40:*:*, ~*:*:4, *:080002451234:*
```

Example 2 To add server “SQL–DB” to the list of services accepted on port 1, enter:

```
ADD !1 -SAP ReceivePolicy “SQL–DB”
```

Example 3 To add all server names that begin with “LA” and “NY” that have the file service to the list of services accepted on port 2, enter:

```
ADD !2 -SAP ReceivePolicy “LA*”:4, “NY*”:4
```

UpdateTime

Syntax

```
SETDefault !<port> -SAP UpdateTime = <seconds> (10–65535)
SHow [!<port> | !*] -SAP UpdateTime
SHowDefault [!<port> | !*] -SAP UpdateTime
```

Default 60

Description The UpdateTime parameter specifies how often the router sends SAP regular updates from the specified port to exchange service information (specified in seconds). Permissible values range from 10 to 65,535 seconds, but UpdateTime must be synchronized with other servers’ update time value. Novell servers also use a default of 60 seconds.

To display the current value for this parameter, use the SHow command.

50 SCH Service Parameters

This chapter describes the parameters for scheduling events to be performed automatically by the bridge/router and for setting up an automatic back-up and port loopback recovery using event-based macro execution (EBME). Table 50-1 lists the SCH Service parameters and commands.

Table 50-1 SCH Service Parameters and Commands

Parameters	Commands
ActiveSCHedule	ADD, DELete, SHow
CONFiguration	SHow
CONTrol	SETDefault, SHow
EbmeCONTrol	SETDefault, SHow
EbmeCONFig	SHow
EbmeEVent	ADD, DELete, SHow
EVent	ADD, DELete, SHow

ActiveSCHedule

Syntax

```
ADD -SCH ActiveSCHedule <mm/dd | SUN | MON | TUE | WED | THU | FRI |
  SAT > <daily schedule>
DELete -SCH ActiveSCHedule <mm/dd | SUN | MON | TUE | WED | THU | FRI
  | SAT >
SHow -SCH ActiveSCHedule [mm/dd | <day of the week> | <daily schedule>
  | TODAY] day of the week: SUN | MON | TUE | WED | THU | FRI | SAT
```

Default ADD and DELete: None
SHow: All active schedules currently defined

Description The ActiveSCHedule parameter assigns, unassigns, and displays a daily schedule for a day of the week or a calendar date.

Values When used with the ADD command, the first argument to the ActiveSCHedule parameter must be either a calendar date in the format mm/dd or one of the following keywords: SUN, MON, TUE, WED, THU, FRI; the second argument must be the name of a daily schedule (previously defined using the EVent parameter).

If there is a daily schedule set for the calendar date corresponding to today and if you have also set a day of the week schedule corresponding to today, only the daily schedule for the calendar date is used, not the day of the week schedule.

CONFiguration

Syntax

```
SHow -SCH CONFiguration
```

Default No default

Description The CONFiguration parameter displays the current settings of the CONTrol parameter, all of the active schedules, and all of the available daily schedules.

CONTrol

Syntax

```
SETDefault -SCH CONTrol = ([Enabled | Disabled], [RealTimeClock
  | NoRealTimeClock], [Log | NoLog])
SHow -SCH CONTrol
```

Default Disable, RealTimeClock, NoLog

Description The CONTrol parameter enables or disables the scheduling function, specifies the use of the system's hardware clock (if any) or a clock emulated in bridge/router software, and enables or disables logging of scheduled event.

Values

Enabled | Disabled	Enables or disables the scheduling function.
RealTimeClock | NoRealTimeClock	RealTimeClock selects the system's hardware clock (NETBuilder II system only). NoRealTimeClock selects NETBuilder software clock emulation and locks out the Enable function until the software clock is reset. After resetting the clock, you can enable scheduling.
Log | NoLog	Log causes all commands or macros and the first 80 characters of each resulting system response message to be stored in the system log buffer. NoLog curtails logging. Output from macros is not logged regardless of the Log | NoLog setting.

EbmeCONFig

Syntax

```
SHow -SCH EbmeCONFig
```

Default No default

Description The EbmeCONFig parameter displays the current values of the EbmeCONTrol parameter, and all events and actions configured for a given port.

EbmeCONTrol

Syntax

```
SETDefault -SCH EbmeCONTrol = ([Enable | Disable], [RunOnBootFail
  | NoRunOnBootFail], [Log | NoLog])
SHow -SCH EbmeCONTrol
```

Default Disable, NoRunOnBootFail, NoLog

Description The EbmeCONTrol parameter enables or disables EBME.

Values

Enable | Disable	Enables and disables EBME.
RunOnBootFail | NoRunOnBootFail	When RunOnBootFail is specified, EBME is enabled when the primary connections fail to establish within 5 minutes after the bridge/router boots, the actions set for the PortDown event of the primary port occur if EBME is enabled. No action is taken with NoRunOnBootFail is specified.

Log | NoLog The Log value causes 80 characters of the output from an event-based command to be recorded in the system log buffer. For event-based macros, the macro name and a macro complete/incomplete message is recorded.

No action is taken with NoLog specified.

EbmeEVent

Syntax

```
ADD !<port> -SCH EbmeEVent <event_keywords> [<DebounceTimer>
  (1-32767sec)] [<command-string(1-80 char)> ]
DELete !<port> -SCH EbmeEVent <event_keywords> | ALL
SHow [!<port>] -SCH EbmeEVent
```

Default Debounce Timer = 15, command-string = Null

Description The EbmeEVent parameter specifies an event for a port, for example, port up or port down.

Macros invoked through EBME cannot require user input or contain the following commands: PING, TraceRoute, DEFine, LIsten, SHow History, or UNDefine. Be sure to verify your macros before using them.

Values

<event_keywords> Indicates the PortUp, PortDown, or LoopBack event for this command or macro.

For LoopBack to be detected, the STP Service needs to be enabled and the port needs to be in the bridge forwarding state.

<DebounceTimer> Sets the time in seconds to wait after receiving the port status change notification and before executing the user-defined command or macro.

<command-string> Specifies an arbitrary bridge/router UI command or executable macro, for example, DO <macroname>.

EVent

Syntax

```
ADD -SCH EVent <daily schedule> <hh:mm> <command-string>
DELete -SCH EVent <daily schedule> <hh:mm | event# | ALL>
SHow -SCH EVent [<daily schedule> | TODAY | ALL]
```

Default ADD and DELete: None
SHow: ALL

Description The EVent parameter creates, deletes, updates, or displays a daily schedule. A daily schedule consists of events. Events consist of a time of day and a command or macro. A daily schedule cannot be executed until it is assigned to a calendar date or day of the week, using ActiveSCHedule.

If a daily schedule name was previously defined, the ADD -SCH -EVent command adds events to the daily schedule, or modifies the event for the specified time. If a daily schedule name was not previously defined, the ADD -SCH EVent command creates a daily schedule under the specified name.

Values

<daily schedule>	You must assign a unique name to the daily schedule. The logical name can be 1–12 characters long and contain any combination of letters and numbers. The characters _, -, @, and * can be used, except as the first character of the daily schedule name. Reserved word values for the ActiveSCHedule parameter (for example, SUN, MON, TODAY) are not valid daily schedule names.
<hh:mm>	Specifies the time of day at which you want the event to occur, in the format hh:mm, where hh represents the hours in 24-hour format and mm represents the minutes. With DELete, you can specify the event number of the schedule to be deleted.
<command-string>	Specifies the desired command exactly as you would enter it on the command line. To execute a macro, use: `DO <macro name>`
ALL	Deletes all events of a schedule when used with the DELete command or allows you to display all events for a specified schedule.
TODAY	Displays the events for today for a specific schedule.

Example 1 To define the daily schedule “midnight” and specify that the macro “clocksync” will occur at 9:30 PM, enter:

```
ADD -SCH EVent midnight 21:30 DO clocksync
```

When this event occurs, the bridge/router receives the following message:

```
DO clocksync
```

Macros invoked through the scheduler cannot require user input or contain the following commands: PING, TraceRoute, DEFine, LIsten, SHow History, or UNDefine. If you schedule a macro that contains an illegal command, the scheduler will log the following error message (if you have enabled logging):

```
Command not accessible through scheduler
```

Example 2 To add another event to the daily schedule “midnight,” enter:

```
ADD -SCH EVent midnight 00:01 DO trace
```

You can schedule multiple events for the same time; each event is run consecutively.

51

SDLC SERVICE PARAMETERS

This chapter describes the parameters that are related to data link connectivity for local area and wide area traffic using the Synchronous Data Link Control (SDLC) Service. Table 51-1 lists the SDLC Service parameters and commands.

Table 51-1 SDLC Service Parameters and Commands

Parameters	Commands
CUAddr	SETDefault, SHow
CUCONFig	SHow
CUCONTrol	SETDefault, SHow
CUInfo	SHow, FLUSH
CULocalMac	SETDefault, SHow
CULocalSap	SETDefault, SHow
CUMAXout	SETDefault, SHow
CUMOde	SETDefault, SHow
CUNAme	SHow
CUPollTimer	SETDefault
CUPOrt	SETDefault, SHow
CURemoteMac	SETDefault, SHow
CURemoteSap	SETDefault, SHow
CUStatus	SHow
CUType	SETDefault, SHow
CUXId	SETDefault, SHow
CUXidDefined	SETDefault, SHow
HostMac	SETDefault, SHow
MaxTRaceData	SETDefault, SHow
PCallTimer	SETDefault, SHow
PCONFig	SHow
PCONtrol	SETDefault, SHow
PDatMode	SETDefault, SHow
PIdleDiscTimer	SETDefault
PMaxData	SETDefault, SHow
PMinFrameDelay	SETDefault
PMODulo	SETDefault, SHow
PortCU	ADD, DELete, SHow
PRetryTimer	SETDefault, SHow
PROle	SETDefault, SHow
PT1Retry	SETDefault, SHow
PT1Timer	SETDefault, SHow

(continued)

Table 51-1 SDLC Service Parameters and Commands (continued)

Parameters	Commands
SdlcLOG	SHow
SuppressDM	SET, SHow
TRaceData	SHow, FLush
TrapCONTrol	SETDefault, SHow
XidKeepAlive	SET, SHow

CUAddr

Syntax

```
SETDefault !<CU Name> -SDLC CUAddr = <value> (hex 01-FF)
SHow [!<CU Name> | !*] -SDLC CUAddr
```

Default C1

Description The CUAddr parameter specifies the poll address of the secondary control unit (CU). If the bridge/router is acting as the SDLC primary for this CU, the address must match the poll address recognized by the CU. If the bridge/router is acting as the SDLC secondary, the address must match the poll address configured by the SDLC primary, for example the Network Control Program (NCP).

Values

<address>	Enter the poll address of the secondary CU. Valid address values are Hex 01 through Hex FF.
<CU Name>	CU names must be a 1–8 alphanumerical character string. A name longer than 8 characters is rejected and a warning message appears.

CUCONFig

Syntax

```
SHow [!<CU Name> | !*] -SDLC CUCONFig
```

Default No default

Description The CUCONFig parameter displays the value of all CU-related parameters for the specified CU and the current state of the CU connection.

CUCONTrol

Syntax

```
SETDefault !<CU Name> -SDLC CUCONTrol = Enabled | Disabled
SHow [!<CU Name> | !*] -SDLC CUCONTrol
```

Default Disabled

Description The CUCONTrol parameter sets the state of the CU when the bridge/router is started or rebooted. Once enabled, the bridge/router continually tries to activate the CU at initial startup time (after a system reboot). If this parameter is disabled, the CU connection is disabled at startup. After the bridge/router has started, the state of the CU may be changed with this parameter.

Although the CU may be enabled by CUCONTrol, it cannot become active with frames being sent and received until PCONtrol (refer to "PCONtrol" on page 51-8) for the port, and the PORT and PATH CONTrol are enabled, and PORT OWNer is set to SDLC.

CUInfo

Syntax
```
SHow [!<CU Name> | !*] -SDLC CUInfo
FLUSH [!<CU Name> | !*] -SDLC CUInfo
```

Default No default

Description The CUInfo parameter displays counters and statistics for the current SDLC connection with the specified CU (or all CUs). If the CU is not currently active, counters are displayed from the last connection for that CU.

CULocalMac

Syntax
```
SETDefault !<CU Name> -SDLC CULocalMac = <MAC address>
SHow [!<CU Name> | !*] -SDLC CULocalMac
```

Default No default

Description The CULocalMac parameter specifies the LAN source address to use in logical link control 2 (LLC2) frames being sent by the bridge/router on behalf of the specified CU. This media access control (MAC) address is also compared with the destination MAC address of the local LLC2 frames received by the bridge/router to determine to which CU the frame is sent.

3Com recommends using a locally administered address. Refer to Chapter 28 in *Using NETBuilder Family Software*.

Values <MAC address> The MAC address of the CU. The SDLC Service interprets MAC addresses in the form: %123456789123 or noncanonical (token-ring) address form.

The display of MAC addresses for the CULocalMac parameter now includes both canonical and noncanonical format.

Restrictions No two CUs located on the same bridge/router can have the same CULocalMac and CULocalSap configuration. The system may not be able to correctly route received LLC2 packets to the intended CU. MAC addresses must be unique within a network.

CULocalSap

Syntax
```
SETDefault !<CU Name> -SDLC CULocalSap = <sap value> (Hex 04-EC)
SHow [!<CU Name> | !*] -SDLC CULocalSap
```

Default 0x04

Description The CULocalSap parameter sets the Service Access Point (SAP) being used for the local end of a LAN (LLC2) connection for the specified CU. The SAP value specified is used as the source SAP for LLC2 frames sent by the bridge/router for the CU. This value is also compared to the destination SAP on LLC2 frames received by the system to determine which CU should receive the frames.

Values <sap value> Enter the SAP value of the CU that is the source of the LLC2 frames.

Restrictions The SAP value for this parameter must be from 0x04 through 0xEC. The SAP value must be divisible by 4. No two CUs on the same bridge/router may have the same CULocalMac and CULocalSap combination.

CUMAXout

Syntax

```
SETDefault !<CU Name> -SDLC CUMAXout = <number> (1–7)
SHow [!CU Name> | !*] -SDLC CUMAXout
```

Default 4

Description The CUMAXout parameter specifies the maximum number of unacknowledged data frames that can be sent to the CU on the specified port. For example, if this value is set to 3, the bridge/router will send no more than three data frames to a CU before requesting an acknowledgment even if it has more data to send.

The value selected for this parameter should be consistent with the host configuration of the CUs attached to this port; the bridge/router should be configured to send no more frames than a CU can handle. Refer to your host configuration for this CU.

The CUMAXout parameter only applies when PMODulo (refer to "PMODulo" on page 51-9) is set to 8. If PMODulo is set to 128 a value of 12 is used for CUMAXout.

When modulo 128 sequencing is used, the bridge/router accepts no more than 12 unacknowledged I frames; if a station attempts to send the bridge/router more than 12 frames in a single polling cycle, the bridge/router disconnects the station.

Restrictions Values over 7 are not used unless PMODulo is 128.

CUMOde

Syntax

```
SETDefault !<CU Name> -SDLC CUMOde = Originate | Answer
SHow [!<CU Name> | !*] -SDLC CUMOde
```

Default Originate

Description The CUMOde parameter configures the CU to either originate a network connection request or answer a connection request from the network. This parameter must be set correctly to ensure that SDLC connections and LLC2 connections are initiated at the correct time and in the correct order. Refer to Chapter 22 in *Using NETBuilder Family Software*.

CUNAme

Syntax

```
SHow -SDLC CUNAme
```

Description The CUNAme parameter displays all of the CUs defined on the bridge/router.

CUPollTimer

Syntax

```
SETDefault !<CU Name> -SDLC CUPollTimer = <milliseconds>
 (200-1000)
```

Default 200

Description The CUPollTimer parameter specifies the minimum delay time in milliseconds before a station is polled. The poll delay occurs in the following cases:

- After a timeout so that other stations on a multidrop link can be polled between retries to a station. Refer to the PT1Timer parameter for information on setting the no-response timeout wait for an SDLC port.
- When a station sends no data in response to a poll, and no data is waiting for transmission to the station. When no data is flowing, the CUPollTimer parameter determines the poll frequency.

This parameter is used only on ports on which the PROle parameter is set to Primary.

CUPOrt

Syntax

```
SETDefault !<CU Name> -SDLC CUPOrt = <port number>
SHow [!<CU Name> | !*] -SDLC CUPOrt
```

Default The port number that is assigned by the PortCU parameter (refer to “PortCU” on page 51-10) becomes the default for the specified CU.

Description The CUPOrt parameter displays the port assignment you create with PortCU , or changes the port assignment of the CU specified by that definition.

Values <port number> The port to which the CU should be assigned.

CURemoteMac

Syntax

```
SETDefault !<CU Name> -SDLC CURemoteMac = <MAC address>
SHow [!<CU Name> | !*] -SDLC CURemoteMac
```

Default No default

Description The CURemoteMac parameter specifies the MAC address for the destination CU. When the system initiates an LLC2 connection (refer to “CUMOde” on page 51-4) for the specified CU, this value is used as the destination MAC address in the LLC2 frames.

Values

<MAC address>	The MAC address of the CU. The SDLC Service interprets MAC addresses in the form: %123456789123 or noncanonical (token ring) address form. If the value is set to 0, the value of the HostMac parameter is used. Refer to “HostMac” on page 51-7.

The display of MAC addresses for the CURemoteMac parameter now includes both canonical and noncanonical format.

CURemoteSap

Syntax

```
SETDefault !<CU Name> -SDLC CURemoteSap = <sap address> (Hex
 04-EC)
SHow [!<CU Name> | !*] -SDLC CURemoteSap
```

Default 0x04

Description The CURemoteSap parameter specifies the SAP for the destination CU. When the system initiates an LLC2 connection (refer to "CUMOde" on page 51-4) for the specified CU, this value is used as the destination SAP in the LLC2 frames. The valid values for the SAP address used by this parameter are from 0x04 to 0xEC and must be divisible by 4.

CUStatus

Syntax

```
SHow [!<CU Name> | !*] -SDLC CUStatus
```

Default No default

Description The CUStatus parameter shows the current status of a CU. The listed status information for the CU is Disabled, Disconnected, Connecting, Internal XID Exchange, XID Exchange, Set Mode State, Information Transfer State, Disconnecting.

The values displayed by CUStatus represent changes in the internal connection state and SDLC and DLSw connection. Actual sequences of states depend on specific configuration options, many are transitory and are rarely displayed.

The following describes the status information:

Disabled	Indicates that CUCONTrol or PCONtrol is disabled
Disconnect	The port and CU are enabled. If the CU is in Originate mode on a Primary port, with XID defined, it may be attempting to poll the CU with SNRM frames; otherwise, the CU may be waiting for the port or path to come up, or waiting for an incoming connection request from the LAN or DLSw (Answer mode).
Connecting	An Originate CU on a primary port with no XID defined may be attempting XID polling of the CU to establish contact; otherwise the CU may be waiting for initial contact (TEST frame).
Internal XID Exchange	The bridge/router is exchanging initial (null) XID frames with the remote station on behalf of the CU.
XID Exchange	The two stations (the CU and its remote partner) are exchanging XID frames.
Set Mode State	The bridge/router primary (secondary) is generating (waiting to respond to) an SNRM frame.
Information Transfer State	The connection between the CU and its remote partner is complete and is available for application data transfer.
Disconnecting	The bridge/router primary (secondary) is sending (waiting to receive) a DISC frame.

CUType

Syntax

```
SETDefault !<CU Name> -SDLC CUType = T2.0 | T1 | T2.1 | T4
SHow [!<CU Name> | !*] -SDLC CUType
```

Default T2.0

Description The CUType parameter defines the physical unit (PU) type category. If the bridge/router is acting as the SDLC primary for the CU specified, the type must be set to the actual CU type. If the system is acting as the SDLC secondary, the type must match the type expected by the SDLC primary, for example, the NCP for the specified CU.

CUXId

Syntax
```
SETDefault !<CU Name> -SDLC CUXId = <value> (8 Hexadecimal digits)
SHow [!<CU Name> | !*] -SDLC CUXId
```

Default 01700001

Description The CUXId parameter sets the CU exchange identification (XID) used by bridge/router to establish LLC2 and DLSw sessions. The XID configured with this parameter must match the XID definition on the host for the specified CU. This parameter is required only when the bridge/router is an SDLC primary unit for the specified CU and the CU does not respond to session identification requests (XIDs type 2.01 and type 1nodes).

When CUXIdDefined is set to Yes, the system uses the configured value in the LLC2 XID frame which is sent when the port connection is being established. If the CUXidDefined is set to No, the system attempts to obtain the XID from the CU itself.

CUXidDefined

Syntax
```
SETDefault !<CU Name> -SDLC CUXidDefined = No | Yes
SHow [!<CU Name> | !*] -SDLC CUXidDefined
```

Default No

Description The CUXidDefined parameter specifies whether the value of CUXId is used. If set to Yes, the CUXId value is used by the bridge/router when initiating LLC2 connections for T1 and T2.0 devices.

If set to No, the bridge/router attempts to solicit the XID value from the CU. For T2.1 devices, the CUXId value is never used.

HostMac

Syntax
```
SETDefault -SDLC HostMac = <address>
SHow [!<CU Name> | !*] -SDLC HostMac
```

Default 000000000000

Description The HostMac parameter is used to configure the remote CU. The MAC address is interpreted in noncanonical (token ring) format if the CURemoteMac parameter is not defined.

The display of MAC addresses for the HostMac parameter now includes both canonical and noncanonical format.

MaxTRaceData

Syntax
```
SETDefault -SDLC MaxTRaceData = <max_bytes_traced> (0-76)
SHow -SDLC MaxTRaceData
```

Default 16

Description The MaxTRaceData parameter sets the maximum number of bytes of SDLC data captured using the Trace facility. The value sets the number of bytes captured over and above the SDLC address and control bytes. The number of bytes affects the types of data captured; the higher the value entered, the more detailed the trace data that 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.

PCallTimer

Syntax

```
SETDefault !<port> -SDLC PCallTimer = <seconds> (0-300)
SHow [!<port> | !*] -SDLC PCallTimer
```

Default 1

Description The PCallTimer parameter sets the number of seconds to wait between attempts to contact a failed or newly activated secondary CU on the bridge/router. This parameter is used on primary ports only.

The default value for PCallTimer is used for the first 10 poll attempts. After 10 poll attempts, twice the default value is used. Each contact attempt (SNRM or XID) uses the configured PT1Timer to timeout the poll, then waits the number of seconds set with PT1Timer, or twice the number of seconds set with PCallTimer, before the next contact attempt. On a multidrop link, you may want to set the PCallTimer to a larger value.

PCONFig

Syntax

```
SHow [!<port> | !*] -SDLC PCONFig
```

Default No default

Description The PCONFig parameter displays the values of all port-related parameters for the ports specified and all CUs assigned to the ports.

PCONtrol

Syntax

```
SETDefault !<port> -SDLC PCONtrol = Enabled | Disabled
SHow [!<port> | !*] -SDLC PCONtrol
```

Default Disabled

Description The PCONtrol parameter determines the state of the SDLC port. When PCONTrol is enabled, the bridge/router continually tries to activate the port at initial startup time (after a system reboot). If this parameter is disabled, the port is disabled at startup. After startup, you may use this parameter to change the state of the SDLC port.

The PCONtrol, CUCONTrol (refer to “CUCONTrol” on page 51-2), PORT and PATH CONTrol, and PORT OWNer parameters are interdependent. For example, when ports are enabled through PCONtrol, the CUs configured for that port only become active with frames being sent and received if their CUCONTrol parameters are enabled. Also, the corresponding CONTrol parameters in the PATH and PORT Services must be enabled (refer to Chapter 42 and Chapter 43) and the PORT OWNer must be set to SDLC (refer to Chapter 43).

PDatMode

Syntax

```
SETDefault !<port> -SDLC PDatMode = Full | Half
SHow [!<port> | !*] -SDLC PDatMode
```

Default Half

Description The PDatMode parameter sets the communication mode of the port to two-way alternate (half duplex) or two-way simultaneous (full duplex). This parameter applies to the port. The physical duplex (Request-To-Send/Clear-To-Send) signalling is controlled by DUplex in the PATH Service (refer to Chapter 42) using the DUplex parameter.

The PDatMode parameter must be set to FULL for a primary multidrop port, allowing the bridge/router to send frames to one PU while receiving from another.

PIdleDiscTimer

Syntax

```
SETDefault !<port> -SDLC PldleDiscTimer = <seconds> (0-1000)
```

Default 0

Description The PIdleDiscTimer parameter specifies the number of seconds that a port remains active without receiving frames. If the specified amount of time passes and no frames are received on the port, all control units (CUs) are disconnected. Reconnection is attempted by the SDLC port after approximately 30 seconds. A value of 0 disables this parameter so that the port will never time out. The PIdleDiscTimer parameter provides a method for SDLC secondary ports to detect the loss of the primary port.

PMaxData

Syntax

```
SETDefault !<port> -SDLC PMaxData = <value> (265 | 521 | 1033 |
 2057)
SHow [!<port> | !*] -SDLC PMaxData
```

Default 1033

Description The PMaxData parameter specifies the maximum amount of data in bytes (including the transmission and request/response header) allowed for the CU in one data transfer. The setting of this parameter should be the same as the host configuration for the CU on the port.

PMinFrameDelay

Syntax

```
SETDefault !<port> -SDLC PMinFrameDelay = <milliseconds> (0-1000)
```

Default 0

Description The PMinFrameDelay parameter specifies the minimum delay that must be inserted between frame transmissions on the specified port. A value of 0 disables the inter-frame delay. This parameter is only useful on ports on which the PROle parameter is set to primary.

PMODulo

Syntax

```
SETDefault !<port> -SDLC PMODulo = 8 | 128
SHow [!<port> | !*] -SDLC PMODulo
```

Default 8

Description The PMODulo parameter sets the frame numbering used for all CUs configured for this port. For example, if 8 is selected, modulo-8 sequencing is used. That is, frames are numbered 0 through 7. If 128 is selected, modulo-128 sequencing is used. That is, frames are numbered 0 through 127. The setting of this parameter must be the same as the other SDLC devices configured for the port. If module 128 is set, the bridge/router can accept no more than 15 frames in a single poll cycle.

PortCU

Syntax

```
ADD !<port> -SDLC PortCU <CU Name> [<CU Name>...]
DELete !<port> -SDLC PortCU <CU Name> | ALL
```

Default No default

Description The PortCU parameter defines a CU, gives it a name, and assigns the CU to a port. Use ADD to set up a new CU on a port. You can specify more than one CU name to configure more than one CU at a time with ADD. Use DELete to remove a single CU from a port, or all of the CUs that are configured for that port.

Values

<CU Name>	Enter the name of the CU. The CU Name defined by this parameter is used to specify the CU when configuring various CU parameters. The defined names are may be up to 8 characters in length. CU names must be unique within the bridge/router.
ALL	The ALL value allows you to delete all of the CUs defined on a port.

PRetryTimer

Syntax

```
SETDefault !<port> -SDLC PRetryTimer = <seconds> (0-300)
SHow [!<port> | !*] -SDLC PRetryTimer
```

Default 30

Description The PRetryTimer parameter sets the time between attempts by the bridge/router to contact the network datalink (LLC2) partner defined by CURemoteMac and CURemoteSap for a CU whose CUMOde parameter is set to Originate. For example, if the PRetryTimer is set to 3 seconds, when contact is established, the bridge/router tries to establish contact with the LLC2 partner every 3 seconds until contact is established or contact with the SDLC partner is lost. If the contact is successfully established with the CU, the datalink connections are started. This parameter has no effect when applied to ports whose CUMOde parameter is set to Answer.

Do not set PRetryTimer to less than 20 seconds, or timing conflicts with DLSw may prevent sessions on that port from coming up.

PROle

Syntax

```
SETDefault !<port> -SDLC PROle = Primary | Secondary
SHow [!<port> | !*] -SDLC PROle
```

Default Primary

Description The PROle parameter specifies the role for the SDLC port. The role applies to the port and all the CUs configured for the port. If the port is primary, then all the CUs attached to this port must be secondary.

PT1Retry

Syntax

```
SETDefault !<port> -SDLC PT1Retry = <number> (1-25)
SHow [!<port> | !*] -SDLC PT1Retry
```

Default 3

Description The PT1Retry parameter sets the number of times the bridge/router attempts to complete a protocol exchange (that is, poll) with a connected device before considering that device a failed device. This parameter tunes the system performance by not prematurely failing devices because of a temporary loss of response. This parameter is used on primary ports only.

PT1Timer

Syntax

```
SETDefault !<port> -SDLC PT1Timer = <milliseconds> (0-10000)
SHow [!<port> | !*] -SDLC PT1Timer
```

Default 1000

Description The PT1Timer parameter sets the no-response timeout wait for an SDLC port on the bridge/router. If the CU does not send a response to a poll or message from the SDLC port before the T1 timer stops, the transmission is retried until the retry count setting completes. This parameter is used on primary ports only.

SdlcLOG

Syntax

```
SHow -SDLC SdlcLOG
```

Default No default

Description The SdlcLOG parameter displays a log of SDLC activity messages captured on the bridge/router and stored in a buffer. The display shows the most recent activity messages. Table 51-2 lists the event types captured in the log, and the corresponding message displayed.

Table 51-2 SDLC Log Event Types and Messages

Event Type	Message Displayed
Control unit activated	Control Unit Up Addr *hh* Name *aaaaaaaa* Port !*pp*
Control unit deactivated	Control Unit Down Addr *hh* Name *aaaaaaaa* Port !*pp*
Control unit failed	Control Unit Failed Addr *hh* Name *aaaaaaaa* Port !*pp*

SuppressDM

Syntax

```
SET -SDLC SuppressDM = Yes | No
SHow -SDLC SuppressDM
```

Default No

Description The SuppressDM parameter disables DM responses from an enabled secondary/answer CU if the following occurs:

- The CUMOde parameter is set to Answer
- The PROle parameter is set to secondary
- The CU is not ready to respond to XIDs or SNRMs because there is no DLSw circuit yet

If you specify Yes, then the DM responses are suppressed. If you specify No, then the NETBuilder bridge/router sends a DM response to an XID or SNRM for an enabled secondary/answer CU that is not ready (has no established DLSw circuit).

TRaceData

Syntax

```
SHow -SDLC TRaceData
```

Default No default

Description The TRaceData parameter displays all SDLC entries in the trace buffer.

TrapCONTrol

Syntax

```
SETDefault -SDLC TrapCONTrol = ([PortUp | NoPortUp], [PortDown |
 NoPortDown], [CUUp | NoCUUp], [CUDown | NoCUDown]) | ALL | None
SHow -SDLC TrapCONTrol
```

Default NoPortUp, PortDown, NoCUUp, CUDown

Description The TrapCONTrol parameter defines control of the transmission of SNMP traps for the SDLC Service. If the control is enabled, the specific trap is sent to the SNMP Service for transmission; if the control is disabled, the particular 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

PortUp | NoPortUp	PortUp sends an SNMP trap to activate an SDLC port. NoPortUp blocks an SNMP trap to activate an SDLC port.
PortDown | NoPortDown	PortDown sends an SNMP trap to deactivate an SDLC port. NoPortDown blocks an SNMP trap to deactivate an SDLC port.
CUUp | NoCUUp	CUUp sends an SNMP trap to activate an SDLC control unit. NoCUUp blocks an SNMP to activate an SDLC control unit.
CUDown | NoCUDown	CUDown sends an SNMP trap to deactivate an SDLC control unit. NoCUDown blocks an SNMP trap to deactivate an SDLC control unit.
ALL	ALL is equivalent to entering PortUp, PortDown, CUUp, and CUDown, which enables transmission of all SDLC SNMP traps.
None	None is equivalent to entering NoPortUp, NoPortDown, NoCUUp, and NoCUDown, which disables transmission of all SDLC SNMP traps.

XidKeepAlive

Syntax

```
SET -SDLC XidKeepAlive = Enabled | Disabled
SHow -SDLC XidKeepAlive
```

Default Disabled

Description The XidKeepAlive parameter controls whether XIDs are sent over a DLSw circuit while waiting for the host poll. If you specify Enabled, then the CU configuration in the NETBuilder bridge/router sends NUL XID messages across the DLSw circuit, keeping the circuit alive longer, in order to receive the host poll. This is helpful in situations where the host poll rate of a secondary/answer CU is slow and does not coincide with the “ready” time of the CU (when a DLSw circuit is in place). If you specify Disabled, these XIDs are not sent.

These XIDs are sent only for the amount of time configured using the -SDLC PRetryTimer parameter. After that, the DLSw circuit is allowed to time out as usual.

This parameter was developed and tested in a PU 1 environment with a slow-polling host. The XidKeepAlive parameter is not recommended for general use, and may be removed in future software releases.

52 SHDLC SERVICE PARAMETERS

This chapter describes the parameters related to tunneling synchronous data link control (SDLC) or high-level data link (HDLC) control frames through Transmission Control Protocol/Internet Protocol (TCP/IP). Table 52-1 lists the SHDLC parameters and commands.

Table 52-1 SHDlc Service Parameters and Commands

Parameter	Commands
PEer	SETDefault, SHow

PEer

Syntax

```
SETDefault !<port> -SHDlc PEer = <peer mac address (noncanonical)>
  | None
SHow -SHDlc PEer
```

Default No default

Description The PEer parameter sets the MAC address of the peer port that the -SHDlc Service is going to use. This parameter also displays the connect state of the circuit associated with the peer port.

The MAC addresses displayed using this parameter are in noncanonical format.

Values

<peer mac address>	Identifies the MAC address of the peer port the SHDlc Service is going to use. You must enter the MAC address in noncanonical format.
None	Specifies that the SHDlc Service is not going to use a peer port and clears the previously configured peer MAC address.

53 SMDS SERVICE PARAMETERS

This chapter describes the parameters in the SMDS Service, which is related to the Switched Multimegabit Data Service. Table 53-1 lists the SMDS Service parameters and commands.

Table 53-1 SMDS Service Parameters and Commands

Parameters	Commands
CONFiguration	SHow, SHowDefault
CONTrol	SETDefault, SHow, SHowDefault
SMDSGroupAddr	SHow
SMDSIndivAddr	SETDefault, SHow, SHowDefault

CONFiguration

Syntax

```
SHow [!<port> | !*] -SMDS CONFiguration
SHowDefault [!<port> | !*] -SMDS CONFiguration
```

Default No default

Description The CONFiguration parameter displays current SMDS configuration information for each port or virtual port. The display includes the CONTrol setting and the interface attached to the digital service unit/channel service unit (DSU/CSU) network.

If you want to display configuration information for a particular port only, include the port number in the SHow or SHowDefault CONFiguration command. If you do not specify a port number, information for all SMDS-owned ports is displayed.

CONTrol

Syntax

```
SETDefault !<port> -SMDS CONTrol = ([LMI | NoLMI], [OldDXI | NewDXI])
SHow [!<port> | !*] -SMDS CONTrol
SHowDefault [!<port> | !*] -SMDS CONTrol
```

Default NoLMI, NewDXI

Description The CONTrol parameter determines whether the Line Management Interface (LMI) Protocol runs over a specified port and which Data Exchange Interface (DXI) standard is supported. A virtual port inherits its CONTrol value from the parent port. You cannot directly configure the CONTrol value of a virtual port. You must use the -PORT OWNer parameter to enable or disable SMDS.

If you are using network switching equipment (DCE) that does not run the LMI Protocol, set CONTrol to NoLMI.

Values	LMI | NoLMI	Specifies that the LMI Protocol runs between the router data terminal equipment (DTE) and the CSU/DSU (DCE). The LMI Protocol improves reliability between the DTE and DCE by exchanging heartbeat packets every 5 to 30 seconds, depending on the configuration. If the LMI Protocol is disabled, the line between the router and the CSU/DSU is assumed to be up. The LMI Protocol is disabled by default
	OldDXI | NewDXI	OldDXI should be configured when running in an SMDS environment supporting the DXI 2.1 standard. NewDXI should be configured when running in an SMDS environment supporting the DXI 3.2 standard.

SMDSGroupAddr

Syntax

```
SHow [!<port> | !*] -SMDS SMDSGroupAddr
```

Default No default

Description The SMDSGroupAddr parameter shows the SMDS group addresses used by each port or virtual port and the routing protocols using these addresses. If no port is specified, then all are shown.

For information related to multicast or group addresses, refer to "SMDSGroupAddr" in the following chapters:

- Chapter 4, "AppleTalk Service Parameters"
- Chapter 14, "BRidge Service Parameters"
- Chapter 17, "DECnet Service Parameters"
- Chapter 27, "IDP Service Parameters"
- Chapter 29, "IP Service Parameters"
- Chapter 31, "IPX Service Parameters"
- Chapter 32, "ISIS Service Parameters"
- Chapter 36, "MIP Service Parameters"
- Chapter 63, "VIP Service Parameters"

SMDSIndivAddr

Syntax

```
SETDefault !<port> -SMDS SMDSIndivAddr = $C0<address>
  (C0–C999999999999999) | None
SHow [!<port> | !*] -SMDS SMDSIndivAddr
SHowDefault [!<port> | !*] -SMDS SMDSIndivAddr
```

Default None

Description The SMDSIndivAddr parameter assigns an SMDS individual address to a port or virtual port. When a device is attached to an SMDS network, the network manager assigns it an SMDS address, called a Subscriber Network Interface address. This address is 15 digits long and resembles a telephone number.

Values

C0–C999999999999999

Specifies the format for an SMDS individual, or unicast, address. The individual address type is used to route data to a specific node. It begins with the letter C and is followed by the 15 digits of the network number. If the number is shorter than 15 digits, it is padded on the right with Fs. The digit that follows the C is the country code.

For packets received on the SMDS port, in addition to checking the address syntax, the software checks the first digit (country code). If the first digit is a 1, then the software flags the packet as an error if 10 digits do not follow the country code. This error appears as a syntactic error and can be display using:

```
SHow -SYS STATistics -SMDS
```

This address checking applies to both individual and group addresses.

None

Removes an individual address that was previously assigned to a port.

54

SNA Service Parameters

This chapter describes all the parameters in the SNA Service. Parameters in this service are used to allow network management applications to communicate with NetView.

Table 54-1 lists the SNA Service parameters and commands.

Table 54-1 SNA Service Parameters and Commands

Parameters	Commands
CONFiguration	SHow
DefaultPU	SETDefault, SHow
LinkStaCONT	SET, SHow
LocalNodeName	SETDefault, SHow
PortCONTrol	SET, SHow
PortDef	SETDefault, SHow
PUStatus	SHow
SDlcLinkSta	ADD, DELete, SHow
SNaLOG	SHow
SscpLinkSta	ADD, DELete, SHow

CONFiguration

Syntax

```
SHow -SNA CONFiguration
```

Default No default

Description The CONFiguration parameter displays the SNA configuration.

DefaultPU

Syntax

```
SETDefault -SNA DefaultPU <pu name>
SHow -SNA DefaultPU
```

Default No default

Description The DefaultPU parameter defines the default PU name. The DefaultPU parameter is required when applications are added that support the sending of unsolicited ALERTS. The PU name must match one of the PU names defined with the SscpLinkSta parameter.

LinkStaCONT

Syntax

```
SET -SNA LinkStaCONT = <linkname> Activate|Deactivate
SHow -SNA LinkStaCONT [linkname]
```

Default No default

Description The LinkStaCONT parameter activates or deactivates a specific link station. Using the SHow command, you can display all link stations or a single link station.

LocalNodeName

Syntax

```
SETDefault -SNA LocalNodeName <netid.cpname> <node_id>
SHow -SNA LocalNodeName
```

Default No default

Description The LocalNodeName parameter specifies the Netid and CP name that the local node will use. This name is carried on all XID3s sent from the local node. This parameter can be set only when the local node is not active. If you are going to use XID3s, then set this parameter before starting the node. The node ID is entered in hex.

PortCONTrol

Syntax

```
SET !<port> -SNA PortControl = <Activate|Deactivate>
SHow -SNA PortControl
```

Default For Activate, the default is to bring up all AutoStart link stations.

Description The PortCONTrol parameter activates and deactivates specific SNA ports.

PortDef

Syntax

```
SETDefault !<port> -SNA PortDef = <DLC type>
  (LLC2|FR|PPP|DLSW|SDLC|UNdef) [ActLimit=<limit(1-16)]
  [DatMode=(Half|Full)] [ROle=(Neg|Pri|Sec)]
SHow [!<port>] -SNA PortDef
```

Default No default

Description The PortDef parameter defines a port to be used by SNA.

Values

<DLC type> Specifies the data link control (DLC) type that will be used by SNA. Specify LLC2 for a token ring, Ethernet, FDDI, Boundary Access Node (BAN), and PPP links. Specify FR for Frame Relay links for Boundary Network Node (BNN), DLSW for DLSw links, or SDLC for SDLC links. If you specify DLSW as the DLC type, then you must specify the port number as !0 (no other DLC type can be used for !0). If you specify SDLC as the DLC type, then you may need to configure some -PORT and -PATH service parameters.

ActLimit Specifies the number of link stations that can be active over the port. The default is 16.

DatMode — Specifies the communication mode of the port. Specify Half for two-way alternate mode (half duplex) or Full for two-way simultaneous mode (full duplex). This value is valid only when the DLC type is set to SDLC.

ROle — Specifies the role for the SDLC port. Specify Neg if the port will negotiate the role with the other SDLC link station. Specify Pri if the port will be the primary port, or Sec if the port will be the secondary port, in the SDLC link transmission. This value is valid only when the DLC type is set to SDLC.

PUStatus

Syntax

```
SHow -SNA PUStatus [puname]
```

Default No default

Description The PUStatus parameter displays the current PU status for all configured PUs. Although the local node is just one PU, it can look like multiple local PUs depending on the configuration. Each SSCP link station represents one local PU.

SdlcLinkSta

Syntax

```
ADD !<port> -SNA SDlcLinkSta <pu name> <station addr>(Hex 1-FE)
  [Nodeid=0x00000000-0xFFFFFFFF] [LinkName=name]
  [AutoStart=(Yes|No)] [Xid3=(Yes|No)] [SendWindow=<num>]
  [ContactTimer=<num>] [NoRspTimer=<num>] [NoRsptimRetry=<num>]
DELete !<port> -SNA SDlcLinkSta <linkname>
Show [!<port>] -SNA SDlcLinkSta [linkname]
```

Default No default

Description The SdlcLinkSta parameter adds or deletes SDLC link stations to a Session Services Control Point (SSCP). Using this parameter, you define a local physical unit (PU) that is going to use the link to communicate with an SSCP. If the node is active, the SDLC link station is added dynamically.

Values

<pu name> — Specifies the physical unit that will use the link to communicate with a SSCP. The PU name must match the PU name configured on the SSCP, and the name must be unique on the local node.

<station addr> — Specifies the station address (or polling address) of the SDLC adjacent link station. Valid address values are Hex 01 through Hex FE.

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. The default node ID is 0x00000000.

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 at the same time (such as for adjacent link stations or DLUr link stations). 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 0000 and 9999.
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 the SET -SNA LinkStaCONTrol command. The default value is Yes.
Xid3	Specifies whether an XID3 should be sent instead of an XID0 during session negotiation. If you specify Yes, XID3 will be sent. If you specify No, XID0 will be sent. This value is valid only if the LocalNodeName parameter is configured. The default value is No.
SendWindow	Specifies the send window size, or the number of frames sent before the local node waits for an acknowledgment. The valid range is from 1 to 12. The default is 4.
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 1 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.

SNaLOG

Syntax

```
SHow -SNA SNaLOG
```

Default No default

Description The SNaLOG parameter displays a log of link and SSCP-PU activity. Displays include whether the node is up or down, the link is up or down, or the SSCP-PU session is up or down.

SscpLinkSta

Syntax

```
ADD !<port> -SNA SscpLinkSta <pu name> <dest media addr>
 [Sap=<num>] [Nodeid=0x00000000-0xFFFFFFFF] [LinkName=name]
 [AutoStart=(Yes|No)] [Xid3=(Yes|No)]
DELete !<port> -SNA SscpLinkSta <linkname> | <media addr> [<sap>]
Show [!<port>] -SNA SscpLinkSta [linkname]
```

Default No default

Description The SscpLinkSta parameter adds or deletes link stations to a SSCP. Using this parameter, you define a local PU that will use the link to communicate with the SSCP. If the node is active, the SSCP link station is added dynamically.

Values

<pu name> Specifies the physical unit that will use the link to communicate with a SSCP. The PU name must match the PU name configured on the SSCP, and the name must be unique on the local node.

<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.

<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.

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. The default node ID is 0x00000000.

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 0000 and 9999.

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 the SET -SNA LinkStaCONTrol command. The default value is Yes.

When you specify the AutoStart option, the link station restarts after a catastrophic failure. The link station also automatically restarts after the link station is deactivated by entering the SET -SNA LinkStaCONT = <linkname> Deactivate command.

Xid3

Specifies whether an XID3 should be sent instead of an XID0 during session negotiation. If you specify Yes, an XID3 is sent. If you specify No, XID0 is sent. This value is valid only if the LocalNodeName parameter is configured. The default value is No.

55

SNMP SERVICE PARAMETERS

This chapter describes the parameters in the Simple Network Management Protocol (SNMP) Service. The SNMP parameters determine how you can use another device to access and modify the configuration of the bridge/router. Table 55-1 lists the SNMP Service parameters and commands.

Table 55-1 SNMP Service Parameters and Commands

Parameters	Commands
COMmunity	ADD, DELete, SHow
CONFiguration	SHow
CONtrol	SETDefault, SHow
MANager	ADD, DELete, SHow

If the bridge/router is used as a Transmission Control Protocol/Internet Protocol (TCP/IP) node on the network, you may need to specify the Internet address for the bridge/router using the -IP NETaddr parameter even if the bridge/router performs Xerox Network Systems (XNS) routing. An Internet address is necessary for the bridge/router to participate in SNMP network management.

COMmunity

Syntax

```
ADD -SNMP COMmunity <“com.name”> [TRiv] [RO | RW] [GEnr | AUth |
  ALl | NOne]
DELete -SNMP COMmunity <“com.name”>
SHow -SNMP COMmunity
```

Default ANYCOM, TRiv, RO, NOne

Description The COMmunity parameter modifies the list of communities. A community is named by a string of octets and is used for authenticating SNMP messages. A request is valid only if the community name is included in the list. A maximum of six community names is allowed in the request list.

Values

<“com.name”> Represents the community name. This string can be up to 16 characters long; only alphanumeric characters are allowed, and the string must be enclosed within a pair of quotation marks (“ ”).

Optionally, specify one or more of the following values after the community name with the ADD command.

TRiv Specifies the authentication scheme. The Trivial scheme is selected by default.

RO | RW	Specifies the access to the management information base (MIB). RO means read-only; RW means read-write access. By default, RO is selected.
GEnr | AUth	Specifies the type of trap to be generated. GEnr means general traps only. AUth means authentication fail traps only.
ALl | NOne	ALl means both general and authentication and enterprise-specific traps as well as enterprise-specific traps. NOne (the default) means no traps are generated for managers using this community string.

There is a reserved com.name called ANYCOM. It allows requests with any community name to be handled. When the community list is checked upon the arrival of a request, the entry under ANYCOM is checked last. If an entry under any other community name is found, the information in that entry is used instead of that under ANYCOM. If traps are configured for ANYCOM, the community name field in the trap PDU is left blank.

The name ANYCOM is case-sensitive and must be entered in uppercase letters in order to function as expected.

CONFiguration

Syntax

```
SHow -SNMP CONFiguration
```

Default No default

Description The CONFiguration parameter displays the values of CONTrol and the SNMP Configuration Table.

CONTrol

Syntax

```
SETDefault -SNMP CONTrol = ([Manage | NoManage], [Trap | NoTrap])
SHow -SNMP CONTrol
```

Default Manage, NoTrap

Description The CONTrol parameter determines how the SNMP agent operates.

Values

Manage | NoManage	Enables or disables response to incoming requests.
Trap | NoTrap	Enables or disables trap generation. Traps can be generated even if NoManage is selected. Authentication failure traps are not generated because all incoming requests are ignored.

MANager

Syntax

```
ADD -SNMP MANager <“com.name”> <IP address> [<mask>]
DELete -SNMP MANager <“com.name”> <IP address>
SHow -SNMP MANager
```

Default No default

Description The MANager parameter modifies the list of managers for a community name. If the manager list is empty, any request with a matching community name is allowed. If a manager list is specified, any incoming Internet address must match the Internet address and mask combination in the specified Internet address list. A maximum of ten manager entries per community name are allowed.

Values

<“com.name” > Specifies the community name whose Internet address list should be updated.

<IP address> Specifies any Internet address.

<mask> Specifies the mask, which is used as a wild card and is specified in the Internet address format. By default, *mask* is 0.0.0.0.

The bits in the mask and the Internet address have a one-to-one mapping. For example, if a bit in the mask is 1, then the corresponding bit in the incoming Internet address can be 1 or 0. If the bit in the mask is 0, the corresponding bit in the incoming Internet address must match the corresponding bit in the Internet address specified in the ADD MANager command.

Example To add a manager to the list, enter:

```
ADD -SNMP MANager “public” 129.213.16.1
```

The following is a sample of the SNMP Configuration Table:

```
-------------------SNMP Configuration Table-----------------------
Community  Authentication Access  Traps   Managers       Masks
public     Trivial        R       None    192.123.19.0   0.0.0.255
                                          129.213.16.1   0.0.0.0
3Com       Trivial        R+W     Non     130.213.128.0  0.0.127.255
trap       Trivial        R       GE+AU   129.213.19.24  0.0.0.0
```

Using the above table, the following requests with community name “public” are valid:

- A request with the first three bytes of the manager Internet address as 192.123.19
- A request from a manager with Internet address 129.213.16.1

With community name “3Com,” the requests from managers with the first two bytes of the Internet address as 130.213 and with the highest bit in the third byte set to 1 are considered valid.

If traps are specified, you cannot use wild cards. Traps are generated to all Internet addresses specified in the list.

To delete a manager entry in the list, use the DELete command.

To display the SNMP Configuration Table, use the SHow command. The SNMP Configuration Table displayed is the same as the one displayed by the SHow -SNMP COMmunity command.

56

SR SERVICE PARAMETERS

This chapter describes the Source Route (SR) Service parameters for operating source route bridging and end system source routing. When configuring parallel bridges, 3Com recommends that you configure both bridges in the same bridge mode, source route (SR) or source route transparent (SRT), in order to prevent unexpected blocking of one type of traffic.

Table 56-1 lists the SR Service parameters and commands.

Table 56-1 SR Service Parameters and Commands

Parameters	Commands
AllRoutes	FLush, SHow, SHowDefault
BridgeNumber	SETDefault, SHow
CONFiguration	SHow, SHowDefault
DIAGnostics	SHow
GatewayControl	SETDefault, SHow, SHowDefault
GatewayVRing	SETDefault, SHow, SHowDefault
HoldTime	SETDefault, SHow, SHowDefault
LargestFrameSize	SETDefault, SHow, SHowDefault
MaxAreRDLimit	SETDefault, SHow, SHowDefault
MaxSteRDLimit	SETDefault, SHow, SHowDefault
MinAccessPrior	SETDefault, SHow, SHowDefault
Mode	SETDefault, SHow
RingNumber	SETDefault, SHow, SHowDefault
ROUte	ADD, DELete, SHow, SHowDefault
RouteDiscovery	SETDefault, SHow, SHowDefault
SrcRouBridge	SETDefault, SHow, SHowDefault
WanRoutes	FLush, SHow

AllRoutes

Syntax

```
FLush [!<port> | !*] -SR AllRoutes [Dec | Hex] [<route>] [Discover |
  Static]<route>: ’:’<ring number>’&’<bridge number>... | Transparent
SHow [!<port> | !*] -SR AllRoutes [Dec | Hex] [<route>] [Discover |
  Static] [<count>] <route>: ’:’<ring number>’&’<bridge number>... |
  Transparent
SHowDefault [!<port> | !*] -SR AllRoutes [Dec | Hex]
```

Default All routes in the routing table in decimal format

Description The AllRoutes parameter allows routes in the routing table to be flushed or displayed in decimal or hexadecimal format. The SHowDefault command displays static routes defined by the ADD -SR ROUte command. The SHow command displays static and discovered routes.

Dynamically learned routes used by LLC2 do not appear in the routing table. Therefore, you can not display, flush, or delete RIFs used by LLC2.

Values

Dec | Hex — Specifies whether decimal or hexadecimal format is flushed or displayed by the use of these keywords. Decimal is the default display format.

<route> — Specifies either a transparent route or a complete or partial source route as a sequence of rings and bridges in the order in which a source packet traverses the source route bridged network.

A route is specified in the following format:

:<ring number>’&’<bridge number>

The colon (:) precedes the ring number; the ampersand (&) precedes the bridge number, for example: 25&24.

Only routes that match the specified route are flushed or displayed. The following is an example of a route where the source route packet initiated at Ring 25, was forwarded through Bridge 2 onto Ring 4 before reaching its end system destination: 25&2:4

A valid route must begin with a ring number that matches the ring number assigned to its associated port. If the last element specified in *route* is a bridge number, that element is ignored.

Discover | Static — Discover specifies only dynamic routes learned through the route discovery process are flushed or displayed. Static specifies only manually configured routes using the ADD ROUte command are flushed or displayed.

<count> — Specifies the number of entries to be displayed.

Transparent — Transparent specifies that only SRT routes be displayed.

The default is all entries in the routing table.

BridgeNumber

Syntax

```
SETDefault -SR BridgeNumber = <number> (0–15) | 0x<number> (0–F)
SHow -SR BridgeNumber
```

Default 3

Description The BridgeNumber parameter determines the bridge number to be used by the source route bridge.

For optimum performance, assign unique bridge numbers to 3Com token ring bridges on a given ring whenever possible. The token ring interface accepts all the frames that have the LAN-In ID (ring-in number) followed by the bridge number. Frames that do not have a known LAN-Out ID (ring-out number) following the LAN-In ID and bridge number are discarded. No functionality is lost when this advice is not followed. Changing the BridgeNumber causes all dynamically learned routes (end system source routes, or WAN routes learned on the Frame Relay, SMDS, or X.25 interface) to be flushed.

IBM bridges support hexadecimal-only format for bridge and ring numbers. 3Com token ring bridges support entry of both decimal and hexadecimal format for these parameters. Hexadecimal format entry must be preceded by a 0x.

To display the current value of BridgeNumber, enter the SHow command. The decimal format is displayed along with the hexadecimal format in parentheses.

CONFiguration

Syntax

```
SHow [!<port> | !*] -SR CONFiguration
SHowDefault [!<port> | !*] -SR CONFiguration
```

Default No default

Description The CONFiguration parameter displays the current SR Service values for source route bridging, end system source route discovery, and source route transparent bridging gateway (SRTG). If a port number is specified, the display for port-related parameter values is limited to that port.

DIAGnostics

Syntax

```
SHow [!<port> | !*] -SR DIAGnostics
```

Default No default

Description The DIAGnostics parameter displays the current status of source route bridging and of the source route transparent bridging gateway. This parameter displays the common and potential configuration errors.

GatewayControl

Syntax

```
SETDefault !<port> -SR GatewayControl = ([Enabled | Disabled],
  [IeeeMode | EtherMode], [AutoMode | NoAutoMode])
SHow [!<port> | !*] -SR GatewayControl
SHowDefault [!<port> | !*] -SR GatewayControl
```

Default Disabled, IeeeMode, AutoMode

Description The GatewayControl parameter controls the behavior of the SRTG. This parameter does not apply to SuperStack II NETBuilder bridge/router models 32x and 52x.

Values

Enabled | Disabled	When enabled, SRTG bridges packets between source route and transparent bridge domains. When disabled, SRTG does not bridge packets between source route and transparent bridge domains.
IeeeMode | EtherMode	This pair of options determines how LLC-based packets from source route domains are translated as they are bridged to Ethernet LANs. If IeeeMode is selected, LLC-based protocol packets are translated into IEEE 802.2 frames when they are bridged to Ethernet. If EtherMode is selected, LLC-based protocol packets are translated into Ethernet Version II frame using a protocol packet type of 0x80D5 when they are bridged to Ethernet.

AutoMode | NoAutoMode	This pair of options determines whether SRTG automatically keeps track of each station's encapsulation format. When AutoMode is selected, SRTG automatically keeps track of each station's encapsulation formats. When NoAutoMode is selected, SRTG does not keep track of each station's encapsulation format.

If SRTG is configured with NoAutoMode, SRTG does not keep track of each transparent bridging station's encapsulation type. The final encapsulation format is decided by the setting of the IeeeMode or EtherMode settings. If EtherMode is selected, Ethernet II encapsulation with protocol type of 0x80D5 is used. Otherwise, LLC2-based packets are translated into the IEEE 802.3 format.

If AutoMode is selected, different packet translation rules are used for known and unknown stations. For known stations, the IeeeMode | EtherMode setting is ignored and the encapsulation format learned for those stations is used. For unknown stations, LLC-based packets are translated into both 802.3 and Ethernet Version II frames. Because non-LLC-based packets are not supported in this release, the DSAP field in the token ring 802.2 frame must be a multiple of 4's (that is, 00, 04, 08, so on), except for 0xBC and 0xE0, which are reserved for Banyan VINES and IPX, respectively.

GatewayVRing

Syntax

```
SETDefault -SR GatewayVRing = [None | <number>(1–4095) |
  0x<number> (1–FFF)]
SHow -SR GatewayVRing
SHowDefault -SR GatewayVRing
```

Default None

Description The GatewayVRing parameter configures a virtual ring number for the transparent bridging domain and its ports, and views them as a single virtual ring. SRTG inserts the virtual ring number and its own bridge number as a pair to the RIF field before bridging transparent packets to the source route domain. The SRTG software can then determine on which ring to bridge packets from the source route domain on the return path.

The ring number can be entered in decimal or hexadecimal but must be preceded by a 0x when entered in hexadecimal. This parameter must be configured to activate the SRTG feature.

The GatewayVRing parameter does not apply to SuperStack II NETBuilder bridge/router models 32x and 52x.

HoldTime

Syntax

```
SETDefault !<port> -SR HoldTime = <minutes> (1–1440)
SHow [!<port> | !*] -SR HoldTime
SHowDefault [!<port> | !*] -SR HoldTime
```

Default 15 minutes

Description The HoldTime parameter specifies the time interval in minutes that an inactive route entry can reside in the routing table.

LargestFrameSize

Syntax

```
SETDefault !<port> -SR LargestFrameSize = <number> (0–7)
SHow [!<port> | !*] -SR LargestFrameSize
SHowDefault [!<port> | !*] -SR LargestFrameSize
```

Default 3 (4,399 octets)

Description The LargestFrameSize parameter specifies the maximum size frame that can be sent and received on a port. The source route bridge negotiates the largest frame size of all transit routes down to this size. This parameter should be used to regulate the amount of data transmitted by end systems to prevent timeouts due to slow network links. If the connected network contains low-speed WAN links, a lower largest frame size value should be assigned. Table 56-2 shows how the base values specified in IEEE 802.1D are supported.

Table 56-2 Frame Size Values

LargestFrame Size Parameter Setting	Data Unit Length (Frame Size)
0	516 octets
1	1,470 octets
2	2,052 octets
3	4,399 octets
4*	8,130 octets
5*	11,407 octets
6*	17,749 octets
7*	41,600 octets

* These values are not supported.

Extended values listed in the IEEE specification are not currently supported.

MaxAreRDLimit

Syntax

```
SETDefault !<port> -SR MaxAreRDLimit = <number> (0–8)
SHow [!<port> | !*] -SR MaxAreRDLimit
SHowDefault [!<port> | !*] -SR MaxAreRDLimit
```

Default 8

Description The MaxAreRDLimit parameter specifies the maximum number of routing designators (RDs) (or hop count) allowed for an All Route Explorer (ARE) frame received on the specified port. The ARE is discarded after this limit is exceeded. The RD is a two-octet field in the routing information that designates a ring number (LAN ID) and bridge number.

The maximum All Route Explorer route designators (MaxAreRDLimit) allowed in a source route bridging environment is eight. This means that the maximum number of bridges or hops that can be daisy-chained in a source route bridge configuration is seven.

MaxSteRDLimit

Syntax

```
SETDefault !<port> -SR MaxSteRDLimit = <number> (0–8)
SHow [!<port> | !*] -SR MaxSteRDLimit
SHowDefault [!<port> | !*] -SR MaxSteRDLimit
```

Default 8

Description The MaxSteRDLimit parameter specifies the maximum number of RDs allowed for a spanning tree explorer (STE) frame received on the specified port. When MaxSteRDLimit is set to N (where N = 0–8), if an STE packet has crossed N–1 or fewer previous bridges, the packet is forwarded; otherwise, it is dropped.

MinAccessPrior

Syntax

```
SETDefault !<port> -SR MinAccessPrior = <number> (0–6)
SHow [!<port> | !*] -SR MinAccessPrior
SHowDefault [!<port> | !*] -SR MinAccessPrior
```

Default 4

Description The MinAccessPrior parameter determines the minimum access priority used for outgoing frames on a specified port. The lowest priority is 0; the highest is 6. End systems usually have a low access priority, while bridges have a medium. This allows bridges, which typically handle larger volumes of data, to get the token faster than end systems. If the user priority of the frame is greater than the minimum access priority, the user priority is used as the access priority. The user priority of the frame is determined by the access priority of an incoming token ring frame.

Mode

Syntax

```
SETDefault -SR Mode = [IEEE | PassiveBridging]
SHow -SR Mode
```

Default IEEE

Description The mode parameter defines the mode of source route bridging. The SHow command displays the current mode. If you select passive bridging, the same ring number must be assigned to all ports with the source route bridging enabled.

The Mode parameter does not apply to SuperStack II NETBuilder bridge/router models 32x and 52x.

Values

IEEE	The explorer frames are modified, and the forwarding path of the specifically routed frames is determined from the routing information (RI) field.
PassiveBridging	All source-routed frames are bridged across the spanning tree paths without examining or updating the source route information in the routing information field (RIF) of the MAC header.

RingNumber

Syntax

```
SETDefault !<port> -SR RingNumber = [None | <number> (1–4095) |
  0x<number> (1–FFF)]
SHow [!<port> | !*] -SR RingNumber
SHowDefault [!<port> | !*] -SR RingNumber
```

Default None

Description The RingNumber parameter determines the ring number or LAN ID for the specified port. This parameter must be defined before source route bridging is allowed on the port. A ring number must be assigned to a Frame Relay, SMDS, X.25, or Point-to-Point port in order to support source route bridging over these WAN interfaces. On a Frame Relay, SMDS, or X.25 port, the SR Service learns Frame Relay DLCIs, the SMDS individual address, or the X.25 DTE address associated with all remote bridges and their attached ring numbers. If you change the RingNumber value, the learned Frame Relay, SMDS, or X.25 routes are flushed.

IBM bridges support hexadecimal-only format for bridge and ring numbers. 3Com token ring bridges support entry of both decimal and hexadecimal format for these parameters. Hexadecimal format entry must be preceded by a 0x.

The SHow command displays the current value of the RingNumber parameter for a specific port or for all ports when the !* syntax is specified. The decimal format is displayed along with the hexadecimal format in parentheses.

ROUte

Syntax

```
ADD !<port> -SR ROUte <media address> [Override] [Dec | Hex]
  [<route> [<largestframesize>]]
DELete !<port> -SR ROUte <media address>
SHow [!<port> | !*] -SR ROUte [[Cmac | Ncmac] %<media address>]
  [Dec | Hex]
SHowDefault [!<port> | !*] -SR ROUte [[Cmac | Ncmac] %<media
  address>] [Dec |Hex]
```

Default No default

Description The ROUte parameter configures, deletes, and displays a static route for a remote end system.

Values

<media address> Specifies the media address of a remote station. Must be 12 hexadecimal digits and preceded by a percent sign (%).

Use the Cmac keyword when the media address is entered in canonical format and the Ncmac keyword when the media address is entered in noncanonical format.

If neither Cmac nor Ncmac is specified, the current setting of the -SYS MacAddrFormat parameter is used.

Override Specifies that the static route can be replaced by a learned route if the route has been determined to be inoperational.

Dec | Hex Specifies that the route information is entered or displayed in decimal (Dec keyword) or hexadecimal format (Hex keyword).

<route> Specifies a source route as a sequence of rings and bridges in the order in which a source-routed packet traverses the source route bridged network. The route is specified as follows:

```
:<ring_number>&<bridge_number>[:<ring_number>] ...,
```

A ring number must be preceded by a colon (:), and a bridge number must be preceded by an ampersand (&). The following is an example of a route where the source route packet initiated at Ring 25 was forwarded through Bridge 2 onto Ring 4 before reaching its end system destination: 25&2:4

A valid route must begin with a ring number that matches the ring number assigned to the specified port. If the last element specified in <route> is a bridge number, that element is ignored. Default is a transparent spanning tree route.

<largestframesize> Specifies the largest size MAC frame that can be transmitted to the indicated end system using this route. An integer value of 0 through 7 may be assigned. The default value is 3. The base values specified in IEEE 802.1D are supported; however, extended values are not currently supported. Enter one of the following numbers for the largest frame size value:

0 for 516 bytes
1 for 1,470 bytes
2 for 2,052 bytes
3 for 4,399 bytes
4 for 8,130 bytes (not supported)
5 for 11,407 bytes (not supported)
6 for 17,749 bytes (not supported)
7 for 41,600 bytes (not supported)

RouteDiscovery

Syntax

```
SETDefault !<port> -SR RouteDiscovery = ([All | None] | [AppleTalk
  | NoAppleTalk], [CLNP | NoCLNP], [DECnet | NoDECnet], [DLTest |
  NoDLTest], [IP | NoIP], [IPX | NoIPX], [LLC2 | NoLLC2], [VINES |
  NoVINES])
SHow [!<port> | !*] -SR RouteDiscovery
SHowDefault [!<port> | !*] -SR RouteDiscovery
```

Default None

Description The RouteDiscovery parameter specifies whether end system source routing is enabled on the port, and which routing protocols are being source routed over the port.

Values All All indicates that route discovery is initiated for all end system packets (AppleTalk, Connectionless Network Protocol (CLNP), DECnet, DLTest, Internet Protocol (IP), Internetwork Packet Exchange (IPX), Logical Link Control, type 2 (LLC2), or VINES) if a route to the destination end system does not exist in the local routing table.

None

None indicates that all end system packets are transmitted as transparent frames, which can reach end systems in transparent bridged or SRT bridged environments.

AppleTalk | NoAppleTalk

AppleTalk indicates that route discovery is initiated for AppleTalk end system packets. This discovery process occurs when a route to the end system does not exist in the local routing table. NoAppleTalk indicates that AppleTalk end system packets are transmitted as transparent frames.

CLNP | NoCLNP

CLNP indicates that route discovery is initiated for CLNP end system packets. This discovery process occurs when a route to the end system does not exist in the local routing table. NoCLNP indicates that CLNP end system packets are transmitted as transparent frames.

DECnet | NoDECnet

DECnet indicates that route discovery is initiated for DECnet end system packets. This discovery process occurs when a route to the end system does not exist in the local routing table. NoDECnet indicates that DECnet end system packets are transmitted as transparent frames.

DLTest | NoDLTest

DLTest indicates that route discovery is initiated for DLTest end system packets. This discovery process occurs when a route to the end system does not exist in the local routing table. NoDLTest indicates that DLTest end system packets are transmitted as transparent frames.

IP | NoIP

IP indicates that route discovery is initiated for IP end system packets. This discovery process occurs when a route to the end system does not exist in the local routing table. NoIP indicates that IP end system packets are transmitted as transparent frames.

IPX | NoIPX

IPX indicates that route discovery is initiated for IPX end system packets. This discovery process occurs when a route to the end system does not exist in the local routing table. NoIPX indicates that IPX end system packets are transmitted as transparent frames.

LLC2 | NoLLC2

LLC2 indicates that route discovery is initiated for LLC2 end system packets. This discovery process occurs when a route to the end system does not exist in the local routing table. NoLLC2 indicates that LLC2 end system packets are transmitted as transparent frames.

VINES | NoVINES

VINES indicates that route discovery is initiated for VINES end system packets. This discovery process occurs when a route to the end system does not exist in the local routing table. NoVINES indicates that VINES end system packets are transmitted as transparent frames.

SrcRouBridge

Syntax

```
SETDefault !<port> -SR SrcRouBridge = ([SrcRouBridge |
  NoSrcRouBridge])
SHow [!<port> | !*] -SR SrcRouBridge
SHowDefault [!<port> | !*] -SR SrcRouBridge
```

Default SrcRouBridge

Description The SrcRouBridge parameter enables source route bridging over a port.

Values	SrcRouBridge | NoSrcRouBridge	SrcRouBridge specifies that all source-routed packets not addressed to the bridge/router are bridged. NoSrcRouBridge specifies that all source-routed packets not addressed to the bridge/router are to be discarded.

WanRoutes

Syntax

```
FLush [!<port>| !*] -SR WanRoutes
SHow [!<port> | !*] -SR WanRoutes
```

Default No default (no WAN routes)

Description The WanRoutes parameter displays or flushes all learned remote routes. Each remote source route for a Frame Relay port has an associated Frame Relay address or data link connection identifier (DLCI). Each source route for an SMDS port has an associated SMDS individual address. Each source route for an X.25 port has an associated X25 DTE address.

FLush clears out all source routes learned across a Frame Relay, SMDS, or X.25 ring. This forces the end systems to redo the route discovery, since the SR bridge discards all traversing frames to and from the ring until the routes are relearned from the explorer frames. The learned routes are automatically flushed when the RingNumber or BridgeNumber is changed, or when source route bridging is turned off.

SHow displays all the currently learned source routes and the associated DLCI, SMDS individual address, or X.25 DTE address for each learned route. If the port is specified, the display for port-related parameter values is limited to that port.

57

STP Service Parameters

This chapter describes Spanning Tree Protocol (STP) Service parameters for operating your bridge/router as a bridge. Table 57-1 lists the STP Service parameters and commands.

Table 57-1 STP Service Parameters and Commands

Parameters	Commands
ADDRess	SETDefault, SHow
BridgePriority	SETDefault, SHow
CONFiguration	SHow
CONTrol	SETDefault, SHow
ForwardDelay	SETDefault, SHow
HelloTime	SETDefault, SHow
MaxAge	SETDefault, SHow
PathCost	SETDefault, SHow
PortPArams	SHow
PortPriority	SETDefault, SHow

If you configure logical networks, the group port does not participate in the Spanning Tree Protocol. Ports that belong to the group can still participate in the spanning tree algorithm with external bridges. You can configure STP Service parameters for logical networks at the global level or the member port level, but not on group ports.

ADDRess

Syntax

```
SETDefault -STP ADDRess = Default (%0180C2000000) | <multicast address>
SHow -STP ADDRess
```

Default %0180C2000000

Description The ADDRess parameter sets or shows the multicast media access control (MAC) address used by bridges running STP.

Do not use multicast addresses %0180C2000001 to %0180C00000F. These addresses are reserved IEEE addresses, and IEEE-conforming bridges do not forward them.

CAUTION: *Changing the STP ADDRess parameter can cause interoperability problems with IEEE 802.1D standard bridges. 3Com does not recommend this action unless you fully understand its effects.*

BridgePriority

Syntax

```
SETDefault -STP BridgePriority = Default (32768) | <number> (0–65535)
SHow -STP BridgePriority
```

Default 32768

Description The BridgePriority parameter sets the priority field of the bridge identifier. The STP algorithm considers the value of the bridge identifier when selecting the root bridge, root port, designated bridge, and port states. The lower the numerical value of the identifier, the higher the priority. For more information about the root bridge and root port, refer to Chapter 3 in *Using NETBuilder Family Software.*

You can enter a hexadecimal value for BridgePriority by using the percent sign (%). For example, %8001 (hexadecimal) is the equivalent of 32769 (decimal).

The format of the bridge identifier consists of Priority (2 bytes) and Datalink address (6 bytes).

CONFiguration

Syntax

```
SHow -STP CONFiguration
```

Default No default

Description The CONFiguration parameter displays current STP values that apply to the entire bridge.

CONTrol

Syntax

```
SETDefault -STP CONTrol = ([Enabled | Disabled], [HopReduce |
  NoHopReduce], [AutoMode | SRTMode | SRMode])
SHow -STP CONTrol
```

Default Enabled, NoHopReduce, AutoMode

Description The CONTrol parameter enables or disables STP and determines whether hop reduction takes place when the bridge configures the extended network.

Values

Enabled | Disabled	Enabled determines whether the STP algorithm is used. Select Disabled only if there are bridges on the network running earlier software versions, and the loop detection algorithm in these versions is causing problems. **CAUTION:** *If Disabled is selected, there is no guarantee that the network topology is loop-free. An extended network with loops can severely degrade performance, to the point of complete network failure, because of infinite packet circulation.*
AutoMode | SRTMode | SRMode	AutoMode automatically selects the appropriate STP mode. SRTMode forces the use of source route transparent STP mode. SRMode forces the use of source route STP mode.

HopReduce | NoHopReduce

Determines whether a bridge considers the number of hops needed to forward a packet to the root bridge when it selects a root port.

If HopReduce is selected, the bridge increases its root path cost by 1. If all bridges select HopReduce and other variables are equal, the cost of forwarding a packet from one bridge to the root increases as the packet passes through more bridges (that is, the packet needs more hops) before arriving at the root. As a result, if two ports have exactly the same root path cost but a different hop count, the one with the lower hop count is selected as the root port.

If NoHopReduce is selected and two ports have the same root path cost, the port that offers the least number of hops may not be chosen as the root port.

It is unusual for two or more ports to have the same root path cost but different hop counts from the root. If this situation occurs, select HopReduce to ensure that the port that is fewer hops away from the root is selected as the root port. If you use this feature, you must select HopReduce on all bridges on the extended network.

ForwardDelay

Syntax

```
SETDefault -STP ForwardDelay = <seconds> (4–30)
SHow -STP ForwardDelay
```

Default 15

Description The ForwardDelay parameter takes effect when a bridge is operating as the root bridge. Any bridge that is not the root bridge uses the root bridge ForwardDelay value. The value specifies the time in seconds that any port has to wait before it changes from listening to learning state and from learning to forwarding state. This delay is necessary so every bridge on the network can receive information about the topology change before the port starts to forward packets. During this time, the port also listens to the protocol for any information that might make it return to blocking state; otherwise, temporary data loops may result.

Set the ForwardDelay parameter so that the following condition is met:

2 x (ForwardDelay - 1) ≥ MaxAge

or equivalently:

ForwardDelay ≥ (MaxAge/2) + 1

For more information, refer to “MaxAge” on page 57-4.

HelloTime

Syntax

```
SETDefault -STP HelloTime = Default (2) | <seconds> (1–10)
SHow -STP HelloTime
```

Default Default (2)

Description The HelloTime parameter specifies the time interval in seconds at which a root bridge transmits a configuration bridge protocol data unit (CBPDU). This parameter takes effect when a bridge is operating as the root bridge. Any bridge that is not the root bridge uses the root bridge HelloTime value.

Set the HelloTime parameter so that the following condition is met:

MaxAge ≥ 2 x (HelloTime + 1)

or equivalently:

HelloTime ≤ (MaxAge/2) - 1

For more information, refer to “MaxAge” on page 57-4.

MaxAge

Syntax

```
SETDefault -STP MaxAge = <seconds> (6–40)
SHow -STP MaxAge
```

Default 20

Description The MaxAge parameter takes effect when a bridge is operating as the root bridge. Any bridge that is not the root bridge uses the root bridge MaxAge value. This value specifies the maximum time (in seconds) a bridge waits without receiving a CBPDU before attempting a reconfiguration. Under normal circumstances, the bridge ports (except for the designated ports) should receive CBPDUs at regular intervals.

If a network problem causes the loss of CBPDUs for a duration greater than or equal to the MaxAge value, STP information in the last BPDU received at these ports is ignored. The MaxAge value guarantees that ports are receiving timely BPDUs from the root bridge; otherwise, the extended network automatically reconfigures.

For example, if the MaxAge of the root bridge is 20 seconds and a BPDU is lost on the network, after 20 seconds ports that normally receive BPDUs age out the STP information obtained from the last BPDU.

Any port that ages out the information becomes the designated port for the LAN to which it is attached. If it is a root port, a new root port is selected from among the bridge ports.

Follow these guidelines when setting MaxAge:

- MaxAge should be several times greater than HelloTime to avoid the protocol information being aged out prematurely. For example, if MaxAge is two seconds and HelloTime is four seconds, a bridge port times out protocol information received two seconds earlier. In this situation, it is premature to time out the information because the next BPDU may still arrive properly. As a rule, MaxAge should be greater than or equal to the following value:

  2 x (HelloTime + 1)
- MaxAge should be less than or equal to the following value:

  2 x (ForwardDelay – 1)

PathCost

Syntax

```
SETDefault !<port> -STP PathCost = Default | <number> (1–65535)
SHow -STP PathCost
```

Default Depends on interface (refer to Table 57-2)

The PathCost parameter is already configured at the factory according to the type of network interface for local bridges. 3Com does not recommend reconfiguring this parameter.

Description The PathCost parameter sets the path cost of each port. The path cost is inversely proportional to the speed of the network interface used at that port.

Table 57-2 shows path costs for some interfaces. To obtain the path cost for other interfaces, divide 1,000 Mbps by the speed of the interface.

Table 57-2 Path Costs for Various Port Interfaces

Type	Speed	Path Cost
FDDI	100 Mbps	10
Ethernet	10 Mbps	100
Token Ring	4 Mbps	250
Token Ring	16 Mbps	63
Broadband	5 Mbps	200
T1	1.544 Mbps	651
T1 (2)	1.544 Mbps	326
DDS	56 kbps	17867

If you specify Default for PathCost, the appropriate value for the network interface is selected. If you set the baud rate for a serial path, the baud rate information is used to calculate the path cost.

PortPArams

Syntax

```
SHow -STP PortPArams
```

Default No default

Description The PortPArams parameter displays values of port-related STP parameters and other information on the spanning tree topology.

PortPriority

Syntax

```
SETDefault !<port> -STP PortPriority = Default (128) | <number> (0–255)
SHow [!<port> | !*] -STP PortPriority
```

Default Default (128)

Description The PortPriority parameter sets the priority field in the port identifier. The STP algorithm considers the port identifier when it selects the root port for each bridge. The lower the numerical value of the identifier, the higher the priority.

You can enter a hexadecimal value for PortPriority using the percent sign (%). For example, 127 (decimal) is the same as %7F (hexadecimal).

The format of the port identifier consists of Priority (1 byte) and Port Number (1 byte).

58

SYS SERVICE PARAMETERS

This chapter describes the SYS Service parameters that affect the entire system but are not configurable per session. Some SYS parameters affect the way you interact with the bridge/router, and some display system information. Table 58-1 lists the SYS Service parameters and commands.

The LogServerAddr parameter has been removed from the SYS Service and added to the AuditLog Service.

Table 58-1 SYS Service Parameters and Commands

Parameters	Commands
ADDRess	SHow
ALias	ADD, DELete, SHow
AUditTrailType	SETDefault, SHow
CONFiguration	SHow
CONNectionUsage	SETDefault, SHow
CPUboardInfo	SHow
DATE	SET, SHow
DpmSTATistics	FLush, SHow
DSTime	SETDefault, SHow
FILESELection	SYSgen, SHow
FileServerAddr	SYSgen, SHow
GetConfigFiles	SETDefault, SHow
GLobalPARams	SHow
IOboardInfo	SHow
MacAddrDispMode	SETDefault, SHow
MacAddrFormat	SETDefault, SHow
MACros	FLush, SHow
MPMessages	SHow
NetAccess	SETDefault, SHow
NetMAP	SHow
NetMapTime	SETDefault, SHow
NMMacro	SETDefault, SHow
NMPrompt	SETDefault, SHow
PROMpt	SETDefault, SHow
RemoteManager	ADD, DELete, SHow
SampleOption	SETDefault, SHow
SampleTime	SETDefault, SHow

(continued)

Table 58-1 SYS Service Parameters and Commands (continued)

Parameters	Commands
STatControl	SETDefault, SHow
STATistics	FLush, SHow
SysCallerID	SETDefault, SHow
SysCONtact	SETDefault, SHow
SYSgen	SHow
SysLOCation	SETDefault, SHow
SysNAMe	SETDefault, SHow
SystemMessages	FLush, SHow
TelnetManager	ADD, DELete, SHow
TimeZone	SETDefault, SHow
UIBinary	SETDefault, SHow
UIEcho	SET, SETDefault, SHow, SHowDefault
VERSion	SHow
WatchDogTimer	SETDefault, SHow
WelcomeString	SETDefault, SHow

ADDRess

Syntax `SHow -SYS ADDRess`

Default Depends on your equipment

Description The ADDRess parameter displays the physical media access control (MAC) addresses of the ports on your bridge/router.

To obtain the MAC address of an high-speed serial (HSS) port on a NETBuilder II bridge/router, enter the SHow -SYS IOboardInfo command instead of the SHow -SYS ADDRess command.

Depending on the hardware platform being used, the MAC address used for WAN ports will be different. Table 58-2 identifies the MAC addresses for physical WAN ports, and Table 58-3 identifies the MAC addresses for virtual WAN ports.

Table 58-2 MAC Addresses for Physical WAN Ports

NETBuilder Platform	WAN Port MAC Address
NETBuilder II	MAC address of WAN interface*
SuperStack II NETBuilder	MAC address of WAN interface

* NETBuilder II V.35 HSS Fab 107, Rev. 106 (1992) and earlier do not have a MAC address; the NETBuilder II CEC MAC address is used.

Table 58-3 MAC Addresses for Virtual WAN Ports

NETBuilder Platform	WAN Port MAC Address
NETBuilder II	CEC MAC address
SuperStack II NETBuilder	MAC address of LAN Interface 1

ALias

Syntax

```
ADD -SYS ALias <alias name> <arguments...>
DELete -SYS ALias <alias name>
SHow -SYS ALias
```

Default No default

Description The ALias parameter defines a list of aliases that you can substitute for bridge/router commands.

Values

<alias name> Indicates the alias you should enter in place of the actual command.

<arguments...> Indicates a command that the alias represents.

For example, you can create an alias called “bridge” to represent the SETDefault -BRidge CONTrol command by entering:

```
ADD -SYS ALias bridge SETDefault -BRidge CONTrol
```

Define an alias called “iproute” by entering:

```
ADD -SYS ALias iproute SETDefault -IP CONTrol =
(ROute, NoRelaySrcRoute)
```

After defining the alias “iproute,” the SETDefault -IP CONTrol command executes each time you enter “iproute.”

The rules for specifying an alias name include the following:

- It must begin with a letter (from A to Z).
- It is case-sensitive. For example, the alias named a is different from the alias named A.
- Alias names can be up to 11 characters.

Each time you enter a command, the bridge/router compares the first word of the command to the alias list. If a match is found, the command is processed according to the definition of the alias. For example, suppose you enter these commands:

```
ADD -SYS ALias abc SETDefault -BRidge CONTrol
abc = NoBridge
```

Because the alias list contains the alias abc, the preceding commands have the same effect as the following command:

```
SETDefault -BRidge CONTrol = NoBridge
```

Aliases can be nested so that an alias definition contains the name of another alias. For example, suppose you enter:

```
ADD -SYS ALias aa SHow -BRidge CONFiguration
ADD -SYS ALias bb aa ar
```

If you enter bb, the system displays the bridge configuration information followed by its routing table.

Be sure that an alias does not nest itself. Otherwise, when you attempt to execute the alias, this error message appears:

```
Alias loop
```

AUditTrailType

Syntax

```
SETDefault -SYS AUditTrailType = [Local | Universal]
SHow -SYS AUditTrailType
```

Default Local

Description The AUditTrailType parameter determines the format of the time and date stamp that is included with each audit trail message the bridge/router generates.

AUditTrailType applies only if there is a server on the attached network. Audit trail messages are generated by various network events and are logged in the server audit trail.

Values

Local	Specifies the time stamp for audit trail messages is the local time on the bridge/router when the event occurred.
Universal	Specifies the time stamp for audit trail messages is in Universal time, reflecting the Greenwich mean time when the event occurred. 3Com recommends using Universal time if your network spans multiple time zones.

CONFiguration

Syntax

```
SHow -SYS CONFiguration
```

Default Refer to "GetConfigFiles" on page 58-7.

Description The CONFiguration parameter displays various SYS Service parameter values. The display generated is the same as the display generated by the SHow -SYS GLobalPARams command.

CONNectionUsage

Syntax

```
SETDefault -SYS CONNectionUsage = [Low | Medium | High]
SHow -SYS CONNectionUsage
```

Default High for systems using the Dual Processor Engine (DPE), Low for all other systems

Description The CONNectionUsage parameter preallocates additional internal connection control structures for the system in anticipation of a greater demand for connection services. As with any dynamic memory allocation scheme, it is difficult to guarantee enough resources for any process when there are multiple processes in competition for the same memory pool. ConnectionUsage helps the system manage the memory pool by obtaining the level of connection services expected.

You do not need to configure CONNectionUsage unless the router is supporting a protocol that uses connection services; for example, when Logical Link Control, type 2 (LLC2) tunneling over Transmission Control Protocol/Internet Protocol (TCP/IP) (LLC2 tunneled over IP connection services) is used on the router.

After CONNectionUsage sets the expected connection service level, the new level does not occur until after the system is rebooted.

When configuring the connection service level, the expected level may not be achieved when the Bridge Routing Table is also being configured. If it is more important to maintain the Bridge Routing Table size, then the connection service level should be reduced. If the connection service level is important, then the Bridge Routing Table size should be reduced. When the default size of the Bridge Routing Table is used, increasing the connection services level will not cause any memory collisions between them.

Values

Low	Indicates that there is no need to preallocate additional connection control structures to support connection services for the router.
Medium	Indicates that there is not a high level of connection services expected, but additional connection control structures should be allocated.
High	Indicates that there will be a high level of connection services expected and the router should preallocate additional connection control structures to support the load.

CPUboardInfo

Syntax

```
SHow -SYS CPUboardInfo
```

Default No default

Description The CPUboardInfo parameter displays the following information for the Communications Engine Card (CEC) and I/O modules:

- Assembly information, including model, serial number, assembly number, and so on
- Maximum current consumption of electricity
- Start address and size of volatile and nonvolatile memory

You can also display this information using the SysInfo command. For more information on this command, refer to Chapter 1.

DATE

Syntax

```
SET -SYS DATE = yy/mm/dd hh:mm[:ss]
SHow -SYS DATE
```

Default No default

Description The DATE parameter sets the system clock. Enter the time in 24-hour-clock time. The clock is used by network management reports and should be set after each system boot. Unusually frequent disk activity can cause the clock to drift by a few seconds per year.

Although DATE is set with SET, it requires local Network Manager privilege level.

Depending on your network environment, you may need to set DSTime and TimeZone before setting DATE.

DpmSTATistics

Syntax

```
FLush -SYS DpmSTATistics
SHow [!<port|slot>] -SYS DpmSTATistics [POrt | SLot] [SRc |
  DEst] [<protocol>]
```

Default SLot, SRc, SUmmary

Description The DpmSTATistics parameter displays information about the forwarding behavior of the distributed protocol modules (DPMs) and gives details about how unicast and multicast network traffic was handled by the DPM. The statistics are valid only for traffic originating from an I/O module that supports DPMs. A count of the packets forwarded to the destination ports, slots, or CEC is displayed. When the parameter is used with the FLush command, all DPM statistics are zeroed out.

Values

!<port | slot> The port or slot instance for which statistics are required. If no instance is specified, statistics are displayed for all ports or slots.

POrt | SLot Determines if the display should be on a per-port or per-slot basis. The default is per-slot.

SRc | DEst When the SRc value is specified, data is displayed about packets transmitted from the specified slots or ports, or ports or slots which are the source of the packets. The DEst value displays data about packets received on the specified slots or ports, or the ports or slots that are the destination of the packets.

<protocol> The following keywords can be used for protocol:

SUmmary | ALl | BRidge | IP | IPX

SUmmary summarizes the data for all protocols by adding numbers for all protocols and displaying only one set of statistics. The SUmmary value is the default. ALl displays statistics about all known protocols that have a distributed protocol module. When BRidge, IP or IPX is specified, statistics are displayed only for the protocol listed.

DSTime

Syntax

```
SETDefault -SYS DSTime = [–]<minutes> (–120 to 120)
SHow -SYS DSTime
```

Default 0

Description The DSTime parameter specifies the displacement, in minutes, from non-daylight saving time. The DSTime parameter, along with the TimeZone parameter, allows the bridge/router to support Universal time for network communications spanning different time zones.

Set the displacement in minutes. Values of this parameter can be ±120 minutes (2 hours).

When you set your clock ahead in the spring (if your locality observes daylight saving time), set the DSTime parameter ahead by the same amount. For example, if you set the clock ahead by 60 minutes at the beginning of daylight saving time and reset the clock back 60 minutes at the end of daylight saving time, the DSTime parameter is set to 60 in the spring for daylight saving and reset to 0 at the end of daylight saving time.

In most cases, DSTime should be set to 60 during daylight saving time, and reset to 0 when daylight saving time ends.

FILESELection

Syntax

```
SHow -SYS FILESELection
SYSgen -SYS FILESELection = [Localfloppy | Remote]
```

Default Localfloppy

Description The FILESELection parameter specifies whether the configuration or boot files used by the bridge/router are stored on a local diskette or remotely.

Before using FILESELection with the Remote value, you must first SYSgen the file server address using FileServerAddr. If you do not SYSgen the file server address first, the following error message appears on your screen:

```
SYSgen FileServer Address first
```

Values

Localfloppy	Indicates that the bridge/router files are stored on the local diskette.
Remote	Indicates that the bridge/router files are stored remotely.

FileServerAddr

Syntax

```
SHow -SYS FileServerAddr
SYSgen -SYS FileServerAddr = <address>
```

Default 0.0.0.0

Description The FileServerAddr parameter applies to bridge/routers that are booted from a server. It specifies the address of the server on which the bridge/router configuration files are stored.

Only a server configured for TCP/IP can be used as a file server for the bridge/router.

GetConfigFiles

Syntax

```
SETDefault -SYS GetConfigFiles = [OFF | ON]
SHow -SYS GetConfigFiles
```

Default OFF

Description The GetConfigFiles parameter retrieves configuration files from a central site server. To find these files, the system must first receive a BOOTREPLY packet through the BOOTP process.

After the system retrieves the files, it resets GetConfigFiles to OFF and reboots. If GetConfigFiles is set to ON during booting, the system enters the auto startup process and tries to retrieve configuration files from the server. Successful retrieval overwrites the local configuration files. If you do not want the files overwritten, set GetConfigFiles to OFF.

GLobalPARams

Syntax

```
SHow -SYS GLobalPARams
```

Default No default

Description The GLobalPARams parameter displays the values of SYS Service parameters.

IOboardInfo

Syntax

```
SHow -SYS IOboardInfo
```

Default No default

Description The IOboardInfo parameter displays information for the I/O modules installed in a NETBuilder II bridge/router slot; interface type, model, serial and assembly numbers, revision level, and MAC address. Multiprocessor I/O board information is displayed differently.

If you have an HSS or HSSI+ module installed in your NETBuilder II bridge/router and you enter the SHow -SYS IOboardInfo command, the MAC address that displays for the HSS or HSSI+ port is assigned by 3Com.

You can also display this information using the SysInfo command. For more information on this command, refer to Chapter 1.

If you assign a new MAC address using the -PATH MacAddress parameter, the new MAC address assigned will not be shown in this display. The IOboardInfo display shows only the MAC address burned onto the PROM of the I/O module.

MacAddrDispMode

Syntax

```
SETDefault -SYS MacAddrDispMode = [Brief | Full]
SHow -SYS MacAddrDispMode
```

Default Brief

Description The MacAddrDispMode parameter sets the display mode for MAC addresses when they appear in displays using the SHow command.

Values

Brief Indicates that all displays of MAC addresses occur in the MacAddrFormat currently applicable for the associated port. This parameter only applies to the following BRidge and FIlter Service displays:

```
SHow -BRidge FunctionalAddr
SHow -BRidge MultiCastAddr
SHow -BRidge AllRoutes
SHow -BRidge ROUte
SHow -FIlter StationGroup <stationgroupname>
```

Full Indicates that all displays of MAC addresses occur in both canonical and noncanonical formats. The noncanonical format is displayed on a new line, exactly below the MAC address in canonical format in the first line.

MacAddrFormat

Syntax

```
SETDefault !<port> -SYS MacAddrFormat = [Canonical | Default |
  Noncanonical]
SHow [!<port> | !*] -SYS MacAddrFormat
```

Default Canonical

Description The MacAddrFormat parameter determines whether MAC addresses are displayed in canonical or noncanonical format. Setting this parameter to Default ensures that when the media type changes on a port, the system displays the MAC addresses in a format that is appropriate for that media type (see Table 58-4.)

Table 58-4 Default MAC Address Display by Media Type

Media Type	Displayed As
Token ring	Noncanonical
Ethernet	Canonical
FDDI	Noncanonical
HSS	Canonical

MAC addresses are always displayed in canonical format when they are not associated with a specific port (that is, local ports and addresses), which occurs using SHow -BRidge AllRoutes.

If a MAC address includes letters in the string, the address is in canonical format. To convert an address in canonical format to noncanonical format, or vice versa, use MacAddrConvert.

MACros

Syntax

```
FLush -SYS MACros
SHow -SYS MACros [<macro name>]
```

Default No default

Description The MACros parameter, when used with the FLush command, clears the contents of the macro cache on the local bridge/router. Caching macros enables the bridge/router to access a macro file quickly without having to send a request over the network to the file server or local diskette. The bridge/router automatically stores the macros in the cache as they are requested. The number of macros the bridge/router can store depends on the cache size.

The bridge/router can keep the contents of the cache active for several days. If you obsolete or change macro files on the macro file server, the macros still present in the cache on the bridge/router are invalid. The FLush -SYS MACros command allows you to quickly clear invalid macros.

FLush -SYS MACros also helps prevent discrepancies between DO <macroname> and SHow -SYS MACros <macroname>. DO command first searches the cache for the file and then examines the local diskette or macro file server. SHow -SYS MACros always reads the macro file from the local diskette or macro file server. If the file stored in the cache is not the same as the one on the diskette or file server, you get different results for different files.

SHow -SYS MACros displays all the macros defined on the bridge/router. If the name of a macro is specified, the contents of that macro are displayed.

For more information on macros, refer to the DEFine, DO, and UNDefine commands in Chapter 1.

MPMessages

Syntax

```
SHow !<slot> -SYS MPMessages
```

Default No default

Description The MPMessages parameter displays a log of system messages and errors for all of the I/O modules installed in a NETBuilder II bridge/router. The log shows the 16 most recent messages displayed for the system. All messages are date- and time-stamped.

NetAccess

Syntax

```
SETDefault -SYS NetAccess = ([Remote | NoRemote], [Console |
  NoConsole], [Telnet | NoTelnet])
SHow -SYS NetAccess
```

Default NoRemote, Console, Telnet

Description The NetAccess parameter determines how a bridge/router can be accessed from another network device. The NetAccess parameter defaults to NoRemote for security because no password is required. Remote access may be enabled by setting NetAccess to Remote.

Values

Remote | NoRemote	Determines whether another device can make a remote connection to the bridge/router using the REMote command. For more information on this command, refer to "REMote" on page 1-44.
Console | NoConsole	Determines whether you can interact with the bridge/router through its console port.
Telnet | NoTelnet	Determines whether another device can use the Telnet Protocol to access the bridge/router.

CAUTION: *The software allows NetAccess to be disabled without giving any warning messages. NoRemote is the remote connection default. 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.*

NetMAP

Syntax

```
SHow [!<port> | !*] -SYS NetMAP [Long] [xns | tcp]
```

Default No default

Description The NetMAP parameter displays the network map. If no port number is specified, the bridge/router displays the netmap for each port.

Values

Long Without the Long option, the netmap includes only the Ethernet and Internet addresses of each 3Com device participating in the NetMAP Protocol that is on the network. With the Long option, the netmap also displays the version of the software that runs on each of these devices.

xns Indicates that the netmap display includes the XNS network number and MAC address of the 3Com devices that support the XNS Protocol.

tcp Indicates that the netmap display includes the MAC and Internet addresses of the 3Com devices that support the TCP/IP Protocol.

If neither the tcp nor the xns value is selected, the bridge/router displays the tcp option. If a 3Com device appears on both displays, that device supports both XNS and TCP/IP Protocols.

NetMapTime

Syntax

```
SETDefault -SYS NetMapTime = <number> (0 to 120 seconds)
SHow -SYS NetMapTime
```

Default 0

Description The NetMapTime parameter determines how often the bridge/router broadcasts its address on the attached network. The default is 0, which keeps the bridge/router from broadcasting its NetMap packets.

NMMacro

Syntax

```
SETDefault -SYS NMMacro = “<string>”
SHow -SYS NMMacro
```

Default “ ” (null string)

Description The NMMacro parameter assigns a name to a macro that is automatically executed when you log in to the bridge/router.

The DEFine command described in Chapter 1 describes how to create macros.

NMPrompt

Syntax

```
SETDefault -SYS NMPrompt = “<string>”
SHow -SYS NMPrompt
```

Default “NETBuilder #”

Description The NMPrompt parameter specifies the string (maximum of 14 characters) that the bridge/router uses as the prompt on the local device (starting in column 1) to indicate that the port has Network Manager privilege. If you set the prompt for greater than 14 characters, it is truncated to 14, and the message “String truncated” appears.

This prompt appears only when CurrentServices is set to more than one service or to ALL. For example, if you set CurrentServices to SR, the following prompt appears instead of the prompt specified by NMPrompt:

```
SR service#
```

PROMpt

Syntax

```
SETDefault -SYS PROMpt = "<string>"
SHow -SYS PROMpt
```

Default "NETBuilder > "

Description The PROMpt parameter specifies the string (maximum of 14 characters) that the bridge/router uses as the prompt on the local device (starting in column 1) to indicate that the port has User privilege. If you set the prompt for greater than 14 characters, it is truncated to 14, and the message "String truncated" appears.

RemoteManager

Syntax

```
ADD -SYS RemoteManager <IP address>
DELete -SYS RemoteManager <IP address>
SHow -SYS RemoteManager
```

Default *.*.*.*

Description The RemoteManager parameter specifies the Internet addresses of devices that can connect to the bridge/router through the REMote command, which is described in Chapter 1. The default value of RemoteManager is *.*.*.* (four wild card characters), which indicates that any device can access the bridge/router through the REMote command.

No remote access is allowed if all addresses, including the default value, are deleted. You can configure a maximum of three RemoteManager addresses.

SampleOption

Syntax

```
SETDefault -SYS SampleOption = (None, Sample, Minute, Hour, Day)
SHow -SYS SampleOption
```

Default None

Description The SampleOption parameter specifies the types of statistics that the system gathers. You can display the statistics using the SHow -SYS STATistics command.

By default, the system gathers only the current sample (statistics for period of time determined by the -SYS SampleTime parameter) and accumulated statistics. You can configure the system to gather the following types of statistics:

None The system retains the default setting for this parameter; it gathers only the current sample and accumulated statistics as described above.

Sample The system gathers statistics for the busiest sample time period since the previous midnight or since the FLush -SYS STATistics -<service> command was last entered, whichever is later. The length of sampling time is determined by the -SYS SampleTime parameter. The default value is 15 seconds.

Minute	The system gathers statistics for the previous minute. It also gather statistics for network activity during the busiest one-minute interval since the previous midnight or since the FLush -SYS STATistics -<service> command was entered, whichever is later.
Hour	The system gathers statistics for the previous hour.
Day	The system gathers statistics for the previous day.

Configuring the system to gather statistics beyond what it gathers by default may consume large amounts of data memory, which reduces the memory available for the routing tables.

SampleTime

Syntax

```
SETDefault -SYS SampleTime = [5 | 10 | 15 | 20 | 30 | 60]
SHow -SYS SampleTime
```

Default 15

Description The SampleTime parameter specifies the time during which statistics are collected for display by the SHow STATistics -SYS command. In the SHow STATistics -SYS command, if the CurrentSample option is specified, the bridge/router displays the statistics collected in the last time interval defined by SampleTime.

You must reboot the system to have the new SampleTime setting take effect.

STatControl

Syntax

```
SETDefault - SYS STatControl = [Enable|Disableclear|DisableFreeze]
Show -SYS STatControl
```

Default Enable

Description The STatControl parameter specifies whether or not statistics are collected for the system.

Values

Enable	Collects statistics for all services in the system.
Disableclear	Stops collection of statistics, clears all data collected, and frees system memory.
DisableFreeze	Stops collection of statistics but does not clear previous data collected. When you reenable STatControl after a DisableFreeze, all previous data will be cleared and new statistics are collected.

Using Disableclear to stop statistics collection frees more system memory for other functions, such as routing tables.

STATistics

Syntax

```
Flush -SYS STATistics [-<service>]
SHow -SYS STATistics [-<service>] [<option>]
```

Default No default

Description The STATistics parameter displays or clears statistics gathered by the system. You can display or clear statistics for a particular service or for all services.

Unlike most service-related commands, the service name for this parameter name follows rather than precedes it. The SHow -SYS STATistics -<service> command displays statistics related to the operation of the bridge/router since it was booted.

If you do not specify a service with STATistics , statistics for all services are displayed.

The -SYS FLush STATistics -<service> syntax clears the accumulated, minute, and sample statistics.

If you do specify a service with the STATistics parameter, only that service is affected. For example, if you enter the FLush -SYS STATistics -PORT command at 5 p.m., the port statistics collected before 5 p.m. are deleted. The bridge/router then accumulates port statistics starting from 5 p.m.

The FLush -SYS STATistics -<service> command may take several seconds before statistics sampling is restarted.

For a listing of services for which you can display information, and information on interpreting statistics, refer to Appendix H in *Using NETBuilder Family Software*.

The types of statistics displayed are determined by the -SYS SampleOption setting. You can override the -SYS SampleOption setting by specifying one or more of these options:

Sample Displays the statistics for the busiest sample time period since the previous midnight or since FLush STATistics -<service> was last entered, whichever is later. The length of the sampling time is determined by SampleTime. The default value is 15 seconds.

CurrentSample Displays statistics for the most recent sample time period. The length of this period is determined by SampleTime. The default value is 15 seconds.

CurrentMinute Displays the statistics for the minute before the command is entered.

Minute Summarizes network activity during the busiest one-minute interval since the most recent midnight or since FLush STATistics -<service> was last entered.

LastHour Displays statistics for the previous hour.

Day Summarizes the average load for the prior day.

If you do not specify an option with SHow -SYS STATistics, the system displays statistics accumulated since FLush -SYS STATistics was last entered.

SysCallerID

Syntax

```
SETDefault -SYS SysCallerID = “<string>”
SHow -SYS SysCallerID
```

Default “”(null string)

Description The SysCallerID parameter enters a text string as an identification for your system. PPP uses this identification as a “caller ID” to identify itself to its peer when establishing a PPP Link Control Protocol (LCP) link. This identification allows the central site router to map incoming calls from remote sites to the proper port when the dynamic dial path pool is being used. For more information, refer to Chapter 34 in *Using NETBuilder Family Software*.

The SysCallerID parameter is limited to 31 characters. If you enter a longer string, it is truncated. This parameter should be administratively assigned and be unique across the network.

SysCONtact

Syntax

```
SETDefault -SYS SysCONtact = “<string>”
SHow -SYS SysCONtact
```

Default “ ” (null string)

Description The SysCONtact parameter specifies a string that identifies the name of a contact person responsible for this managed node. You can also specify information on how to contact the person, such as a telephone number or address.

You need Network Manager privilege to use the SETDefault -SYS SysCONtact command.

SYSgen

Syntax

```
SHow -SYS SYSgen
```

Default No default

Description The SYSgen parameter displays the parameters stored in the SysConf file. These parameters are modified by the SYSgen command.

SysLOCation

Syntax

```
SETDefault -SYS SysLOCation = “<string>”
SHow -SYS SysLOCation
```

Default “ ” (null string)

Description The SysLOCation parameter specifies the physical location of the node.

SysNAMe

Syntax

```
SETDefault -SYS SysNAMe = “<string>”
SHow -SYS SysNAMe
```

Default “ ” (null string)

Description The SysNAMe parameter specifies the administratively assigned name for the node. This is normally the fully qualified domain node of the node.

SystemMessages

Syntax

```
FLush -SYS SystemMessages
SHow -SYS SystemMessages
```

Default No default

Description The SystemMessages parameter displays the 64 most recent system messages sent to the console port. Each message is numbered and includes the date and time the message was generated. When used with the FLush command, SystemMessages deletes all system messages. New incoming messages are numbered at 1.

Example 1 In the following example, the bridge/router has booted successfully:

```
System Initialized and Running
```

Example 2 In the following example, too many transitions from up state to down state have occurred on the specified path within 30 seconds. The bridge/router does not use the path until it has been up continuously for 30 seconds.

```
Path "n" Faulty
```

Example 3 If the bridge/router is used as a bridge, as in the following example, the spanning tree algorithm detects a loop on the extended network, and the specified port is blocked to eliminate the loop. The port remains operational (for example, it can still route packets if routing is enabled), but the bridge does not forward any packets from that port.

```
Port "n" Loop Detected
```

Example 4 In the following example, the bridge/router has received on path “n” one of the packets it transmitted on that path. This situation occurs when the path is connected to a device that loops the packets back to the bridge/router (for example, when the device is malfunctioning or is set to Loopback for troubleshooting purposes). The path is operational, but the bridge/router does not use the path to forward packets until the loop is corrected.

```
Path "n" Physical loop back detected
```

TelnetManager

Syntax

```
ADD -SYS TelnetManager <IP address>
DELete -SYS TelnetManager {<IP address> | ALL}
SHow -SYS TelnetManager
```

Default *.*.*.* (Telnet requests from all address are accepted.)

Description The TelnetManager parameter specifies IP addresses of devices that can connect to the bridge/router using the Telnet Protocol. You can use the TelnetManager parameter to provide limited security at the Telnet level for network management purposes.

You can add a maximum of six entries to the IP address list. Wild card format is allowed at each byte position of the address.

You can delete addresses one at a time by specifying the address, or delete all addresses by specifying the keyword ALL.

All addresses that are added or deleted take effect immediately. Deleting an address does not affect an existing Telnet connection to the address that is already established.

You can display the IP address list using the SHow command.

The default value of `*.*.*.*` (indicates 255.255.255.255) in the address list allows the bridge/router to accept Telnet connections from every station.

TimeZone

Syntax

```
SETDefault -SYS TimeZone = [–]<minute> (–720 to 720)
SHow -SYS TimeZone
```

Default 480

Description The TimeZone parameter specifies the number of minutes displacement west of Greenwich, England of the bridge/router site. A negative number for this parameter indicates how many minutes displacement east of Greenwich the site is located. Values of this parameter can be ±720 minutes. Only numerical values are allowed.

TimeZone, along with DSTime, allows the server to support Universal time for network communications that span different time zones.

UIBinary

Syntax

```
SETDefault -SYS UIBinary = [OFF | ON]
SHow -SYS UIBinary
```

Default OFF

Description The UIBinary parameter allows or disallows, the server to initiate negotiation for binary transmission when a Telnet connection is made to the bridge/router user interface. This parameter ensures completeness because of various behaviors observed in Telnet client implementations with the end-of-line treatment in local echo mode. The default OFF is satisfactory for most systems, but some clients may operate better in binary mode when connecting to the bridge/router user interface port.

Values

OFF | ON	Allows (ON) or disallows (OFF) the system to initiate the negotiation for binary transmission when a Telnet connection is made to the user interface.

UIEcho

Syntax

```
SET -SYS UIEcho = [OFF | ON]
SETDefault -SYS UIEcho = [OFF | ON]
SHow -SYS UIEcho
SHowDefault -SYS UIEcho
```

Default ON

Description The UIEcho parameter enables or disables the user interface Echo capability when connecting to the network management port. If Telnet is the connection protocol, setting this parameter is the same as the negotiate Telnet Echo option on behalf of the Telnet server.

When this parameter is OFF, the system expects its network partner (the Telnet client implementation) to provide echo and editing.

When this parameter is ON, the system echoes the inputs from its network partner and processes the editing characters accordingly.

The following editing characters are recognized:

Erase	[Ctrl] + [H] (BackSpace), [Ctrl] + [?] (Delete)
EraseWord	[Ctrl] + [W]
EraseLine	[Ctrl] + [U], [Ctrl] + [X]
ReprintLine	[Ctrl] + [R]
Verbatim	[Ctrl] + [V]

Unrecognized control characters are echoed as their equivalent ASCII characters. For example, [Ctrl] + C is echoed as '^C'. For terminals that require editing characters other than the ones supported, set this parameter to OFF.

If there are multiple network management sessions, each session can have its own UIEcho value. However, there is only one default value of this parameter for the whole system. The default value is used as the starting value when a network management session is first established.

Values

OFF | ON	Echo and editing are disabled (OFF) or enabled (ON).

VERSion

Syntax

```
SHow -SYS VERSion
```

Default No default

Description The VERSion parameter displays the bridge/router software and firmware release number, the boot time, the boot source, and copyright information. Only User privilege is required.

WatchDogTimer

Syntax

```
SETDefault -SYS WatchDogTimer = [Reset | Disable]
SHow -SYS WatchDogTimer
```

Default Enabled

Description The WatchDogTimer parameter enables or disables the watchdog timer operation when the parameter is configured for SuperStack II NETBuilder systems. If the system has never previously been configured for watchdog, the software automatically enables the hardware watchdog timer. Watchdog configuration is stored in the system EEPROM, not on floppy configuration files.

WelcomeString

Syntax

```
SETDefault -SYS WelcomeString = “<string>”
SHow -SYS WelcomeString
```

Default “Welcome to the 3Com NETBuilder”

Description The WelcomeString parameter specifies the string that the bridge/router displays on the local device after login or when the console is activated. The string can be up to 80 characters. If you set the prompt for greater than 80 characters, it is truncated to 80 characters, and the message “String truncated” appears.

59

TCP SERVICE PARAMETERS

This chapter describes the Transmission Control Protocol (TCP) Service parameters. The TCP Service is related to the ARP, IP, RIPIP, and OSPF Services. Table 59-1 lists the TCP Service parameters and commands.

Table 59-1 TCP Service Parameters and Commands

Parameters	Commands
CONFiguration	SHow
CONNections	DELete, SHow
CONTrol	SETDefault, SHow
DelayedAckTime	SETDefault, SHow
KeepAliveLimit	SETDefault, SHow
KeepAliveTime	SETDefault, SHow
MaxSegmentSize	SETDefault, SHow
RetransmitLimit	SETDefault, SHow
SYNRetrys	SETDefault, SHow
WINdow	SETDefault, SHow

CONFiguration

Syntax

```
SHow -TCP CONFiguration
```

Default No default

Description The CONFiguration parameter displays all the modifiable TCP parameters and the number of connections on the router.

CONNections

Syntax

```
DELete -TCP CONNections <Connection ID>
SHow -TCP CONNections
```

Default No default

Description The CONNections parameter displays all TCP connections originated from or received by the router. The display includes the local and remote Internet addresses, the local and remote TCP port numbers, the connection state, and the connection ID.

TCP connections are used for Telnet access to 3Com bridge/routers only. To abort a TCP session, use the DELete command. The DELete -TCP CONNections command can also be used to delete a TCP connection that has become inoperable.

The bridge/router can have up to four TCP Telnet connections.

Example The following command displays the TCP Connection Table:

```
SHow -TCP CONNEctions
```

The following display indicates that this bridge/router (local IP address 129.213.48.98) has a connection to its TCP port 23 (Telnet) from the system with IP address 129.213.48.34 using TCP port 1240. The connection is established. The ID is an internal identifier tied to this connection, which means that the DELete -TCP CONNections command could reference it.

```
------------------------TCP Connection Table--------------------
Loc IP        Loc Port   Rem IP        Rem Port State   Conn ID
129.213.48.98 Telnet(23) 129.213.48.34 1240     estab   1441796
Total Connections: 1
```

CONTrol

Syntax

```
SETDefault -TCP CONTrol = [KeepAlive | NoKeepAlive]
SHow -TCP CONTrol
```

Default NoKeepAlive

Description The CONTrol parameter enables or disables transmission of keepalive packets, which are used to determine whether a connection is still alive.

Values

KeepAlive	Enables transmission of keepalive packets.
NoKeepAlive	Disables transmission of keepalive packets.

DelayedAckTime

Syntax

```
SETDefault -TCP DelayedAckTime = <milliseconds> (1–1000)
SHow -TCP DelayedAckTime
```

Default 200

Description On each TCP connection, the transmission of acknowledgment packets for the data received is delayed. The DelayedAckTime parameter specifies the length of the delay, which can range from 1 to 1,000 milliseconds.

KeepAliveLimit

Syntax

```
SETDefault -TCP KeepAliveLimit = <retrys> (0–15)
SHow -TCP KeepAliveLimit
```

Default 0

Description The KeepAliveLimit parameter determines the number of keepalive packets to be transmitted. After these packets are transmitted, if there is no response from the peer TCP, a connection is reset.

The default is 0, which means that a connection is never dropped because of the lack of response to keepalive packets.

When KeepAliveLimit is set to 0, the router does not drop the connection even if the peer fails. This situation can cause the router to be inaccessible through Telnet until it is reset or until the TCP connection is terminated with the DELete

-TCP CONNections command. The DELete -TCP CONNections command must be issued through a terminal directly attached to the console port or through the REMote command.

KeepAliveTime

Syntax

```
SETDefault -TCP KeepAliveTime = <seconds> (1–16000)
SHow -TCP KeepAliveTime
```

Default 45

Description The KeepAliveTime parameter specifies the time-out value for the transmission of keepalive packets. This parameter is used to determine the time interval between the transmissions of two keepalive packets.

MaxSegmentSize

Syntax

```
SETDefault -TCP MaxSegmentSize = <bytes> (1–4096)
SHow -TCP MaxSegmentSize
```

Default 1024

Description The MaxSegmentSize parameter specifies the maximum segment size that the TCP layer of the router can receive. This is the value advertised in the TCP MaxSegmentSize option when a connection is made to the router.

RetransmitLimit

Syntax

```
SETDefault -TCP RetransmitLimit = <retrys> (0–128)
SHow -TCP RetransmitLimit
```

Default 17

Description The RetransmitLimit parameter specifies the number of times a data segment can be transmitted without response before a connection is aborted. When RetransmitLimit is 0, the data segment is retransmitted continuously until a response is detected.

SYNRetrys

Syntax

```
SETDefault -TCP SYNRetrys = <number> (1–128)
SHow -TCP SYNRetrys
```

Default 4

Description The SYNRetrys parameter specifies the number of times a connection request is transmitted before the connection attempt is aborted. This parameter is used only if the connection originates from the router.

WINdow

Syntax

```
SETDefault -TCP WINdow = <bytes> (1–32767)
SHow -TCP WINdow
```

Default 2048

Description The WINdow parameter specifies the maximum window size to advertise.

60 TCPAPPL SERVICE PARAMETERS

This chapter describes the parameters in the Transmission Control Protocol Applications (TCPAPPL) Service. Table 60-1 lists the TCPAPPL Service parameters and commands.

Table 60-1 TCPAPPL Service Parameters and Commands

Parameters	Commands
LIStenerPorts	ADD, DELete, SHow
RLogSendName	SETDefault, SHow

LIStenerPorts

Syntax

```
ADD -TCPAPPL LIStenerPorts <Port number> (1–9999)
DELete -TCPAPPL LIStenerPorts <Port number> (1–9999)
SHow -TCPAPPL LIStenerPorts
```

Default No default

Description The LIStenerPorts parameter adds, deletes, and displays user-defined service ports. User-defined service ports are ports that name the ends of logical connections and provide a contact point for unknown callers. If a contact point other than a well known port (such as 23 for Telnet and 513 for Rlogin) is needed, the port must be explicitly assigned using LIStenerPorts.

The ADD command adds a user-defined service port to the Transmission Control Protocol/Internet Protocol (TCP/IP) interface. The assigned service listener ports can be found in the Assigned Numbers (RFC 1010). Up to 16 services can be added. The service ports can be used to export the TCP interface to a serial line. The host can bind a process to that line to accept incoming data units from the active side of the particular service and generate appropriate responses for the service protocol.

If the Rlogin port (513) is configured as a listener port, the server accepts connections for TCP port 513 and sends an initial NUL byte. The use of TCP port 513 is intended to allow Rlogin connections to serial ports on the communications server, even though the communications server does not implement an Rlogin server. The Rlogin client expects a NUL byte.

The DELete commands removes services from the list of listener ports.

RLogSendName

Syntax

```
SETDefault -TCPAPPL RLogSendName = [Yes | No]
SHow -TCPAPPL RLogSendName
```

Default Yes

Description The RLogSendName parameter determines whether the gateway sends the actual client username or an empty string to the Rlogin server during connection setup. If an empty string is sent, automatic login can be prevented.

Values

Yes	When this value is set to Yes, the gateway sends the client username to the server when an Rlogin connection is made. The username used to log in during network login (local access control) is used as the value for the client username. If access control is disabled, then an empty string is sent for this field. The client username is also sent as the server username, unless overridden by the -l option (the letter "l") in the RLOGin command. The Rlogin server uses this information, along with other configuration information, to determine if an automatic login can be performed.
No	When this value is set to No, automatic login is prevented during Rlogin connections. The value for the server username is not affected, but the client username is sent as an empty string. This action causes the Rlogin server to prompt the user for a password.

61

TERM SERVICE PARAMETERS

This chapter describes the parameters in the TERM Service. Some parameters in the TERM Service depend on the requirements of the originating data terminal equipment (DTE) and remain constant for the duration of the X.25 call. Other parameters may vary from session to session depending on the host. If you change a value with the SETDefault command and then immediately use the SHow command, the change is not reflected. The SHow command reflects only current values when an active session is occurring.

Table 61-1 lists the TERM Service parameters and commands.

Table 61-1 TERM Service Parameters and Commands

Parameters	Commands
AllSessions	SHow
AUToDisconnect	SET, SETDefault, SHow
AUToListen	SETDefault, SHow
BAud	SET, SETDefault, SHow
BReakAction	SET, SETDefault, SHow
BReakChar	SET, SETDefault, SHow
BUffersize	SET, SETDefault, SHow
COLumns	SET, SETDefault, SHow
CRPad	SET, SETDefault, SHOw
DataForward	SET, SETDefault, SHow
DefaultParams	SHow
DeVice	SETDefault, SHow
ECHOData	SET, SETDefault, SHow
ECHOMask	SET, SETDefault, SHow
ECMChar	SET, SETDefault, SHow
ERAse	SET, SETDefault, SHow
FlowCtrlFrom	SET, SETDefault, SHow
FlowCtrlTo	SET, SETDefault, SHow
FlushVC	SHow
FunctionalUnit	SET, SETDefault, SHow
IdleTimer	SET, SETDefault, SHow
InitMacro	SETDefault, SHow
InterActTerm	SET, SETDefault, SHow
LFInsertion	SET, SETDefault, SHow
LFPad	SET, SETDefault, SHow

(continued)

Table 61-1 TERM Service Parameters and Commands (continued)

Parameters	Commands
LineERase	SET, SETDefault, SHow
LocalEDit	SET, SETDefault, SHow
MaxSessions	SET, SETDefault, SHow
NetAScii	SET, SETDefault, SHow
PARAmeters	SHow
PARIty	SET, SETDefault, SHow
PROFile	SETDefault, SHow
ReprintLine	SET, SETDefault, SHow
ROWs	SET, SETDefault, SHow
SavedParams	SHow
SESsions	SHow
TERMType	SET, SETDefault, SHow
VERBatim	SET, SETDefault, SHow
WordERAse	SET, SETDefault, SHow
XmitBinary	SET, SETDefault, SHow
XOFF	SET, SETDefault, SHow
XON	SET, SETDefault, SHow

The gateway uses configuration files to initialize a port and session with a host. Configuration file !2 is used as the default for outgoing connections, and configuration file !1 is used as the default for incoming connections. In most cases, you can use these two configuration files without modification; the default settings of the TERM Service parameters are acceptable for most incoming and outgoing connections.

If you require different settings than the defaults already provided, use the SETDefault command with a configuration file number. If you change the defaults of configuration file 1 or 2, the changes will affect all defaulted sessions. Configuration file 1 is the default for incoming connections and must not be used for outgoing connections. Also, configuration file 2 is the default for outgoing connections and must not be used for incoming connections.

While the help string in the software may display [!<config file>] with the SET command, the configuration file cannot be used with this command in the TERM Service. The help string in the software also may not display [!<port>] with the SHow command, but a port number can be used with the TERM Service parameters in most cases. Valid port numbers range from 0 to 127 on the NETBuilder II system.

When setting parameters for configuration files 3–32, make sure the DeVice parameter is properly configured for the type of connection desired; for example, DeVice should be set to Terminal for incoming connections and to Host for outgoing connections.

During incoming and outgoing connections, the gateway selects a port through which the connection is established. These ports are not physical ports, but virtual ports, and range in number from 0 to 127 on a NETBuilder II system. During startup and during connection establishment, the gateway initializes the port with a configuration file containing default values copied from the diskette into gateway memory. After the port is initialized and a session with the host begins, the default values in the configuration file are copied within memory and become active port-related and session-related values. During the active port and session period, changing the default values with the SETDefault command has no effect on the active values but will affect new sessions; changing the active values with the SET command has no effect on the default values. The SET command operates on active ports and sessions while the SETDefault command operates on default port and session parameters. Figure 61-1 shows the relationship between SET and SETDefault.

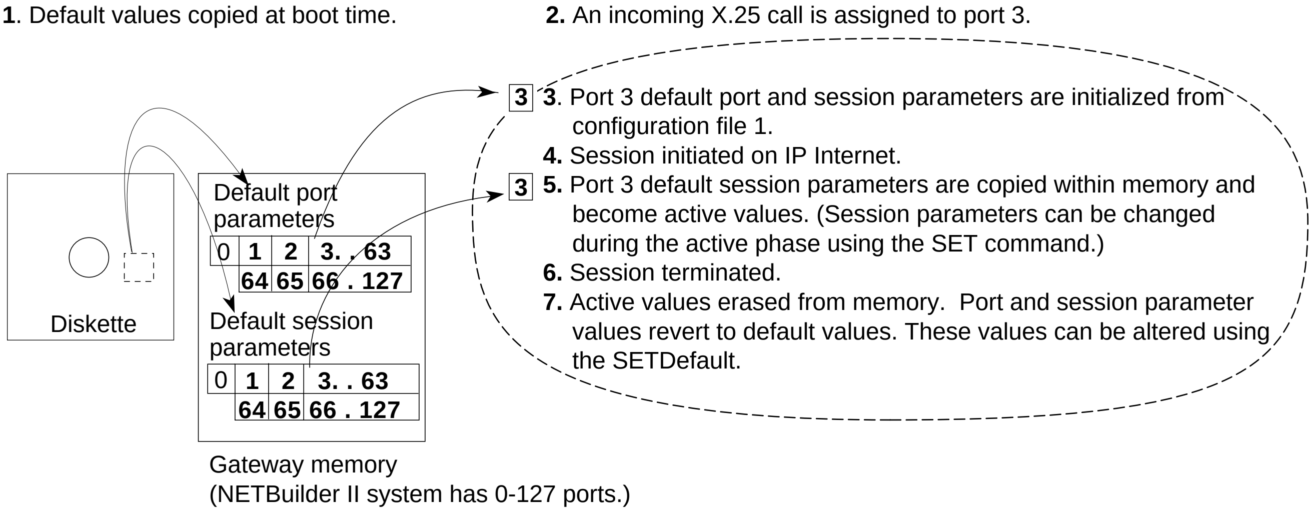

1. Default values copied at boot time.
2. An incoming X.25 call is assigned to port 3.
3
3. Port 3 default port and session parameters are initialized from configuration file 1.
4. Session initiated on IP Internet.
3
5. Port 3 default session parameters are copied within memory and become active values. (Session parameters can be changed during the active phase using the SET command.)
6. Session terminated.
7. Active values erased from memory. Port and session parameter values revert to default values. These values can be altered using the SETDefault.
Diskette
Default port parameters
0 1 2 3. . 63
64 65 66 . 127
Default session parameters
0 1 2 3. . 63
64 65 66 . 127
Gateway memory
(NETBuilder II system has 0-127 ports.)

Figure 61-1 Altering Port and Session Parameters with the SET and SETDefault Commands

The network manager can alter the default or active parameters by using the SETDefault command with a a configuration file number, but cannot display port or session parameters unless there is an active port and session. The network manager can SHow both active and default values. (If the port is not active, both default and active parameters are displayed the same.) The user can alter active values by using the SET command on the current port; however, the user cannot SHow or SET port or session parameters unless there is an active port and session.

The TERM Service can be divided into global, general, and session-related for incoming and outgoing connections, and per-port-related for incoming and outgoing connections as shown in Table 61-2. This table can help you configure TERM Service parameters.

Table 61-2 Classification of TERM Service Parameters

Classification Type	Subcategory	TERM Service Parameter
Global parameters		AllSessions, SavedParams
General parameters		DefaultParams, PARAmeters, SESsions
Incoming connections	Session-related*	BReakAction, BReakChar, DataForward, ECHOData, ECHOMask, ECMChar, ERAse, FlowCtrlFrom, FlowCtrlTo, FlushVC, IdleTimer, LFInsertion, LineERase, LocalEDit, NetAScii, ReprintLine, VERBatim, WordERAse, XmitBinary, XON, XOFF

(continued)

Table 61-2 Classification of TERM Service Parameters (continued)

Classification Type	Subcategory	TERM Service Parameter
	Port-related†	AUToListen, BAud, BUffersize, COLumns, DeVice, InitMacro, InterActTerm, MaxSessions, ROWs, PARIty, TERMType‡
Outgoing connections	Session-related	BReakAction, ECHOData, FlowCtrlFrom, FlowCtrlTo, FlushVC, IdleTimer, LFInsertion, XOFF, XON
	Port-related	AUToDisconnect, BAud, BUffersize, DeVice, PARIty

* Users can use the SET command to configure their session parameters; these session parameters can be different per session.

† These parameters can be used with the SET command to change their active values; the change applies to all sessions

‡ The TERMType parameter is not maintained per session but has a per-session effect. This parameter is used at the start of a session; if it is changed, there is no corresponding change for existing sessions.

AllSessions

Syntax

```
SHow -TERM AllSessions
```

Default No default

Description The AllSessions parameter displays all the sessions on a port on the LAN side of the gateway. To display sessions on the X.25 side of the connection, use the SHow -Gateway PadSession command. For more information, refer to Chapter 26.

The display indicates whether the port is connected or in command or listen mode. Up to 128 ports can be displayed on a NETBuilder II system.

AUToDisconnect

Syntax

```
SET -TERM AUToDisconnect = [Disabled | <number> (1–16000 minutes)]
SETDefault [!<config file>] -TERM AUToDisconnect = [Disabled |
  <number> (1–16000 minutes)]
SHow [!<port>] -TERM AUToDisconnect
```

Default 60

Description The AUToDisconnect parameter specifies the number of minutes the current session remains connected if no activity occurs during the specified time. If there is no activity, the current session is disconnected. Setting a value other than Disabled is appropriate only for outgoing connection ports. If you enter the SHow -TERM AUToDisconnect command on an incoming connection port, an error message appears.

AUToListen

Syntax

```
SETDefault [!<config file>] -TERM AUToListen = [Disabled | <number>
  (1–100) minutes]
SHow [!<port>] -TERM AUToListen
```

Default Disabled

Description The AUToListen parameter determines the amount of time in minutes that a port can remain idle in command mode with no sessions. After the timer expires, the port is placed automatically into listen mode. AUToListen can be configured or disabled on a per-port basis.

AUToListen applies only to incoming connections.

AUToListen cannot be applied to an idle user interface on an incoming Telnet session to the network management port.

Values

Disabled	The AUToListen parameter is disabled.
1–100	The length of time a port can remain idle in command mode with no sessions is from 1 to 100 minutes. The time selected can take up to a minute longer than the specified time.

BAud

Syntax

```
SET -TERM BAud = [50 | 75 | 110 | 134.5 | 150 | 200 | 300 | 600
  | 1200 | 1800 | 2400 | 3600 | 4800 | 7200 | 9600 | 19.2k |
  38.4k | 56k | 64k]
SETDefault [!<config file>] -TERM BAud = [50 | 75 | 110 | 134.5 |
  150 | 200 | 300 | 600 | 1200 | 1800 | 2400 | 3600 | 4800 |
  7200 | 9600 | 19.2k | 38.4k | 56k | 64k]
SHow [!<port>] -TERM BAud
```

Default 9600

Description The BAud parameter specifies the terminal device baud rate.

During incoming connections, BAud is initialized by an X.29 READ command from the originating DTE. During outgoing connections, BAud is initialized to the value in the port parameters, and the gateway responds to an X.29 READ with that value.

To find the X.3 parameter equivalent to BAud, refer to Appendix L in *Using NETBuilder Family Software.*

BReakAction

Syntax

```
SET -TERM BReakAction = [IGnore | (OutofBand, InBand, FlushVC,
  EscDTM)]
SETDefault [!<config file>] -TERM BReakAction = [IGnore |
  (OutofBand, InBand, FlushVC, EscDTM)]
SHow [!<port>] -TERM BReakAction
```

Default OutOfBand (for incoming connections)
IGnore (for outgoing connections)

Description During an incoming call, the BReakAction parameter specifies the action the gateway takes when a break (or the alternative character specified by BReakChar) is received from the packet assembler/dissembler (PAD) device on the X.25 network, and how that break condition is signaled to the server Telnet of an Internet Protocol (IP) Internet-attached host. With Rlogin connections, there is no way to communicate a break; therefore, it is ignored. Only the EscDTM value applies to Rlogin connections.

During an outgoing call, the BReakAction parameter specifies the action the gateway takes when either a Telnet BREAK or Telnet IP command is received from the client Telnet of an IP Internet-attached host. In this PAD mode, the gateway considers these Telnet commands to be the same as a break signal from a PAD device, and so follows the procedures documented in the CCITT X.29 Recommendation for various possible combinations of actions.

To find the X.3 parameter equivalent to the BReakAction parameter, refer to Appendix L in *Using NETBuilder Family Software.*

Values You can select incoming and outgoing values listed in Table 61-3 and Table 61-4 with the SET and SETDefault commands.

Table 61-3 Incoming Call Values

Value	Action
IGnore	No action. (This value cannot be used with any other value; more than one of the remaining values can be specified.)
OutofBand	Sends Telnet BREAK command.
InBand	Sends Telnet IP command.
FlushVC*	Sends DO TIMING MARK. Discard data until a receive response (either WILL or WONT TIMING MARK).
EscDTM†	Enters command mode at the gateway user interface.

* Some hosts may not respond to the DO TIMING MARK. Do not select this action for use with such a host.
† For incoming Rlogin connections, EscDTM is the only value that applies.

Table 61-4 Outgoing Call Values

Value	Action
IGnore	No action. (This value cannot be used with any other value; more than one of the remaining values can be specified.
OutofBand	Sends an interrupt packet with user data field set to 0.
InBand	Sends an indication of break PAD message.
OutofBand AND InBand	Sends an interrupt packet with user data field set to 1. Sends an indication of break PAD message.
OutofBand AND InBand AND FlushVC	Sends an interrupt packet with user data field set to 1. Sends an indication of break PAD message with the parameter 8 set to 1. Discards data until receive PAD command to set parameter 8 to 0.
EscDTM	Enters command mode at gateway PAD emulator.

BReakChar

Syntax

```
SET -TERM BReakChar = [Disabled | <char>]
SETDefault [!<config file>] -TERM BReakChar = [Disabled | <char>]
SHow [!<port>] -TERM BReakChar
```

Default Disabled

Description The BReakChar parameter specifies the character that the gateway interprets as a break signal. This parameter is useful for terminals that do not have Break keys. Because most terminals have Break keys, the default is Disabled.

BReakChar applies only to incoming connections.

Do not use [Ctrl]+P as the break character for incoming connections. Most PADs use [Ctrl]+P as its own break into command mode from data transfer mode.

Values

Disabled	This value disables the Break key function.
<char>	This value assigns the <char> key as the Break key.

BUffersize

Syntax

```
SET -TERM BUffersize = <number> (1–512 bytes)
SETDefault [!<config file>] -TERM BUffersize = <number>
  (1–512 bytes)
SHow [!<port>] -TERM BUffersize
```

Default 82

Description The BUffersize parameter determines the size of the gateway's internal buffer. BUffersize is used in both incoming and outgoing connections.

Data accumulates in the gateway's internal buffer until it becomes full (as determined by the BUffersize setting) or until the interval specified by the -TERM IdleTimer parameter elapses; then the data is packetized and forwarded. Depending on the value of the -TERM DataForward parameter, data can also be forwarded when a data-forwarding character is entered. Setting BUffersize to a smaller value than the gateway's internal buffer size may be useful for PC-to-host file transfer applications, since the gateway more quickly packets and forwards the data.

COLumns

Syntax

```
SET -TERM COLumns = <number> (1–255)
SETDefault [!<config file>] -TERM COLumns = <number> (1–255)
SHow [!<port>] -TERM COLumns
```

Default 80 (for incoming connections; parameter is inappropriate for outgoing connections)

Description The COLumns parameter displays and sets the number of characters in a single line on the terminal. If requested by the Rlogin server, the COLumns information is transmitted by the Rlogin client when a connection is established or whenever the value is changed using the SETDefault command. This parameter is valid only for incoming Rlogin connections.

CRPad

Syntax

```
SET -TERM CRPad = [None | <number> (1–127 nulls of padding)]
SETDefault [!<port>] -TERM CRPad = [None | <number>
  (1–127 nulls of padding)]
SHow -TERM CRPad
```

Default None

Description The CRPad parameter specifies the number of nulls inserted between the carriage return (CR) character and the next character. The BS, CR, FF, LF, and tab characters all have delay and pad parameter options.

Values

None	No nulls are inserted.
<1–127>	From 1 to 127 nulls of padding are inserted.

DataForward

Syntax

```
SET -TERM DataForward = [None | (AlphaNum, CR, ESC, EDiting,
  Term, FormEf, COntrol, Punct)]
SETDefault [!<config file>] -TERM DataForward = [None | (AlphaNum,
  CR, ESC, EDiting, Term, FormEf, COntrol, Punct)]
SHow [!<port>] -TERM DataForward
```

Default None

Description The DataForward parameter specifies the kinds of key stroke events that cause data to be packetized and forwarded in data transfer mode. Some events are predetermined conditions, such as the elapsing of the -TERM IdleTimer parameter (if enabled), the filling of the data buffer, and the occurrence of the ATTN or break signal. This parameter applies to incoming connections only.

To find the X.3 parameter equivalent to the DataForward parameter, refer to Appendix L in *Using NETBuilder Family Software*.

Values

None — Specifies that data is forwarded if the predetermined conditions above occur.

AlphaNum — Specifies that a packet is created and forwarded as soon as any upper- or lowercase alphabetic character or numeric character is detected.

CR — Specifies that a packet is created and forwarded as soon as a carriage return is detected.

The CR value also causes data forwarding on a linefeed for sessions in local edit mode.

ESC — Specifies that a packet is created and forwarded as soon as an escape (ASCII codes ESC, BEL, ENQ, or ACK) is detected.

EDiting — Specifies that a packet is created and forwarded as soon as any editing character is detected. Editing characters consist of ^R, ^X, Delete, DC2, CAN, and DEL.

Term — Specifies that a packet is created and forwarded as soon as any terminator (ETX or EOT) is detected.

FormEf — Specifies that a packet is created and forwarded as soon as any form effector character is detected. Form effectors are the linefeed, horizontal tab (^I, ASCII 9), vertical tab (^K, ASCII 11), and formfeed characters.

COntrol — Specifies that a packet is created and forwarded as soon as any control character is detected. These control characters include all ASCII characters 0 through 31 (decimal) except for ENQ, ACK, and BEL (5, 6, 7).

Punct — Specifies that a packet is created and forwarded as soon as any punctuation character is detected. Punctuation characters include all the nonalphanumeric graphics characters shown here:
! @ # $ % ^ & * ( ) _ - + = ~ ` | \ [ ] { } : ; “ ’ < > , . ? / and space.

DefaultParams

Syntax

```
SHow [!<port>] -TERM DefaultParams [<param-name>] ...
```

Default No default

Description The DefaultParams parameter displays the default values of the port- and session-related parameters for the port, as shown in the examples. Only active ports can be displayed. If the specified port is not active, an error message is displayed when the SHow !<port> -TERM DefaultParams command is executed.

On a NETBuilder II system, valid port numbers are 0–127.

DeVice

Syntax

```
SETDefault [!<config file>] -TERM DeVice = ([Host | Terminal],
  [Paper | Glass])
SHow [!<port>] -TERM DeVice
```

Default Terminal, Glass (for odd-numbered configuration files)
Host, Glass (for even-numbered configuration files)

Description The DeVice parameter specifies the type of device that is attached to the port. For outgoing connections, set the DeVice parameter to Host on the specified port. For incoming connections, set the DeVice parameter to Terminal on the specified port.

If the device type is specified as terminal, the port provides a user interface. Terminal ports are usually the initiation point of connections but also can be connection destinations. If the device type is specified as host, no user interface is provided. Host ports are primarily used for connection destinations. The device setting can change the availability of other parameters; host ports do not use -TERM InitMacro.

Values Host | Terminal Specifies whether the device to be attached to the port is a host or a terminal. Setting DeVice to Host automatically sets these parameters:

Parameter	**Setting**
AUToDisconnect	60
BReakAction	IGnore
LFInsertion	None

Setting DeVice to Terminal automatically sets these parameters:

Parameter	**Setting**
BReakAction	InBand
ECMChar	^^(0x1E)
InterActTerm	(Verbose, NoMacroEcho, MacroBreak, BroadcastON)
NetAScii	UseLF
XmitBinary	OFF

If DeVice is set to Terminal, one of the following secondary characteristics can be specified:

Paper | Glass Determines whether the terminal is a video display unit (Glass, the default) or a hardcopy printer (Paper). The setting affects how backspacing is handled during local editing; for instance, when you erase a character or a word using the backspace key or the local editing characters. If DeVice is set to Glass, the server moves the terminal cursor to the left one column for each character erased. If DeVice is set to Paper, the server prints a pound sign (#) for each character erased instead of attempting to move the print mechanism.

ECHOData

Syntax

```
SET -TERM ECHOData = [OFF | ON]
SETDefault [!<config file>] -TERM ECHOData = [OFF | ON]
SHow [!<port>] -TERM ECHOData
```

Default OFF

Description The ECHOData parameter specifies whether the gateway tells the PAD to echo input data back to the device. This parameter applies to both incoming and outgoing connections.

This parameter may be automatically set for Telnet sessions according to the results of the Telnet option negotiation (Echo option).

To find the X.3 parameter equivalent to the ECHOData parameter, refer to Appendix L in *Using NETBuilder Family Software.*

Values

OFF	Disables echoing of input data back to the device.
ON	Enables echoing of input data back to the device.

ECHOMask

Syntax

```
SET -TERM ECHOMask = [None | (AlphaNum, CR, ESC, EDiting, Term,
  FormEf, COntrol, Punct)]
SETDefault [!<config file>] -TERM ECHOMask = [None | (AlphaNum, CR,
  ESC,EDiting, Term, FormEf, COntrol, Punct)]
SHow [!<port>] -TERM ECHOMask
```

Default AlphaNum, CR, Term, PunctDescription

The ECHOMask parameter specifies which characters are echoed if ECHOData is enabled. The character classes are the same as those listed for the -TERM DataForward parameter. If ECHOData is enabled, all characters that fit the ECHOMask descriptions are echoed when typed. This parameter applies to incoming connections.

To find the X.3 parameter equivalent to the ECHOMask parameter, refer to Appendix L in *Using NETBuilder Family Software.*

ECMChar

Syntax

```
SET -TERM ECMChar = [Disabled | <char>]
SETDefault [!<config file>] -TERM ECMChar = [Disabled | <char>]
SHow [!<port>] -TERM ECMChar
```

Default ^^ ([Ctrl] + ^)

Description The ECMChar parameter specifies a character that is interpreted by the gateway as a request to change from data transfer mode to command mode. The defined character cannot be transmitted as data by using the TRansmit command. This parameter is useful when the application requires that a break signal be transmitted as data (that is, the BReakAction parameter is set to InBand or OutofBand). This parameter applies to incoming connections.

To find the X.3 parameter equivalent to ECMChar, refer to Appendix L in *Using NETBuilder Family Software*.

ERAse

Syntax

```
SET -TERM ERAse = [Disabled | <char>]
SETDefault [!<config file>] -TERM ERAse = [Disabled | <char>]
SHow [!<port>] -TERM ERAse
```

Default ^H ([Ctrl] + H)

Description The ERAse parameter specifies the character that the gateway tells the PAD to interpret as an erase character. Entered before the current line is terminated by the Return key, the erase character deletes the most recently typed character. This parameter applies to incoming connections.

To find the X.3 parameter equivalent to the ERAse parameter, refer to Appendix L in *Using NETBuilder Family Software*.

Values

Disabled	This value disables the ERAse parameter.
<char>	This value assigns a key or key combination as the erase character.

FlowCtrlFrom and FlowCtrlTo

Syntax

```
SET -TERM FlowCtrlFrom = [None | Xon_Xoff]
SETDefault [!<config file>] -TERM FlowCtrlFrom = [None | Xon_Xoff]
SHow [!<port>] -TERM FlowCtrlFrom
SET -TERM FlowCtrlTo = [None | Xon_Xoff]
SETDefault [!<config file>] -TERM FlowCtrlTo = [None | Xon_Xoff]
SHow [!<port>] -TERM FlowCtrlTo
```

Default Xon_Xoff

Description The FlowCtrlFrom parameter specifies the flow control mechanism from the gateway to the LAN-attached device (that is, the gateway can turn transmission from the IP Internet-attached device on or off). These parameters apply to both incoming and outgoing connections.

The FlowCtrlTo parameter specifies the flow control mechanism from the LAN-attached device to the gateway (that is, the IP Internet-attached device can turn transmission from the gateway on or off).

The remote device can use different flow control than the local device, since flow control across the network is handled by the servers at either end of the circuit independently of local flow control. Flow control during Rlogin connections takes precedence over the settings of the FlowCtrlTo/From parameters, and the Xon (^Q) or Xoff (^S) characters can be added or removed.

Local FlowCtrlFrom/To can affect the transparency of the connections if Xon and Xoff are used locally. These characters may not be considered to be normal data for purposes of forwarding across the network.

To find the X.3 parameter equivalent of the FlowCtrlTo parameters, refer to Appendix L in *Using NETBuilder Family Software.*

Values

None	Specifies that no flow control is used.
Xon_Xoff	Specifies that the characters defined by the Xon (transmit on) and Xoff (transmit off) parameters are used.

FlushVC

Syntax

```
SHow [!<port>] -TERM FlushVC
```

Default OFF

Description The FlushVC parameter specifies whether packets for a session are being flushed (discarded) or transmitted. FlushVC applies only if the -TERM BReakAction parameter is set to FlushVC. This parameter applies to both incoming and outgoing connections.

To find the X.3 parameter equivalent to the FlushVC parameter, refer to Appendix L in *Using NETBuilder Family Software.*

FunctionalUnit

Syntax

```
SET -TERM FunctionalUnit = [(None, UrgentData, VtBreak)]
SETDefault [!<port>] -TERM FunctionalUnit = [(None, UrgentData,
  VtBreak)]
SHow -TERM FunctionalUnit
```

Default UrgentData, VtBreak

Description The FunctionalUnit parameter enables or disables some Virtual Terminal Protocol (VTP) services. You can set this parameter to more than one of the following values. If you change the value of this parameter, current sessions are not affected.

Values

None	No functional units.
UrgentData	Enables the Urgent Information Exchange Functional Unit, which allows urgent information to pass between users. If necessary, normal data flow control is bypassed.
VtBreak	Enables the Break Functional Unit, which allows a user to destructively interrupt and discard current data and resynchronize both ends of a connections.

IdleTimer

Syntax

```
SET -TERM IdleTimer = [Disabled | <number>
  (1–255 sixtieths of a second)]
SETDefault [!<config file>] -TERM IdleTimer = [Disabled | <number>
  (1–255 sixtieths of a second)]
SHow [!<port>] -TERM IdleTimer
```

Default 1 (outgoing connections)
2 (incoming connections)

Description The IdleTimer parameter specifies the interval after which, if no further characters are entered from the PAD, all accumulated characters are packetized and forwarded. In data transfer mode, characters are accumulated in a data buffer until an event specified by -TERM DataForward occurs, the buffer fills, or the IdleTimer interval elapses.

To find the X.3 parameter equivalent to the IdleTimer parameter, refer to Appendix L in *Using NETBuilder Family Software.*

Values	Disabled	This value disables the IdleTimer.
	<1–255>	This value sets the IdleTimer from 1 to 255 sixtieths of a second.

InitMacro

Syntax

```
SETDefault [!<config file>] -TERM InitMacro = “<string>”
SHow [!<port>] -TERM InitMacro
```

Default No default

Description The InitMacro parameter specifies the name of a port initialization macro (“*string*”) to be executed automatically each time the device makes a transition from listen mode to command mode. The macro itself is defined with the DEFine command. Port modes are described in Chapter 52 in *Using NETBuilder Family Software*. This parameter applies to incoming connections.

Example This command sets “menu2” as the macro to be executed automatically each time the PAD-attached terminal user makes an incoming automatic connection and specifies configuration file 3. The menu2 macro could be a custom-designed menu that includes choices for connecting to a Transmission Control Protocol/Internet Protocol (TCP/IP) host. The menu2 macro is created with the DEFine command.

```
SETDefault !3 -TERM InitMacro = “menu2”
```

InterActTerm

Syntax

```
SET -TERM InterActTerm = ([Verbose | Brief], [MacroEcho |
  NoMacroEcho], [MacroBreak | NoMacroBreak], [BroadcastON |
  BroadcastOFF])
SETDefault [!<config file>] -TERM InterActTerm = ([Verbose |
  Brief], [MacroEcho | NoMacroEcho], [MacroBreak | NoMacroBreak],
  [BroadcastON | BroadcastOFF])
SHow [!<port>] -TERM InterActTerm
```

Default Verbose, NoMacroEcho, MacroBreak, BroadcastON

Description The InterActTerm parameter controls the interaction environment between you and the gateway. This parameter applies to incoming connections.

To find the X.3 parameter equivalent to the InterActTerm parameter, refer to Appendix L in *Using NETBuilder Family Software.*

Values	Verbose | Brief	Determines whether broadcast messages are preceded by a header indicating the port number of the message sender. The value Brief is appropriate for a host or a terminal emulator program; Verbose is appropriate for a terminal.
	MacroEcho | NoMacroEcho	Determines whether macros are echoed on the screen as they are executed.
	MacroBreak | NoMacroBreak	Determines whether the break signal can be used to stop execution of a macro. In macros that raise the privilege level to Network Manager, setting NoMacroBreak prevents the user from breaking out of the macro and, as a result, remaining in network manager privilege level.

BroadcastON | BroadcastOFF	Determines whether the port receives messages sent with the Broadcast command when the port is in command or data transfer mode. The default is BroadcastON.

LFInsertion

Syntax

```
SET -TERM LFInsertion = [None | (OutputCrlf, EchoCrlf)]
SETDefault [!<config file>] -TERM LFInsertion = [None |
  (OutputCrlf, EchoCrlf)]
SHow [!<port>] -TERM LFInsertion
```

Default None

Description The LFInsertion parameter specifies whether linefeeds are transmitted (or echoed) following a Return. This parameter applies to both incoming and outgoing connections.

To find the X.3 parameter equivalent to LFInsertion, refer to Appendix L in *Using NETBuilder Family Software*.

Values

None	Specifies that no linefeed is echoed or transmitted with a Return. This value cannot be used with the other values.
OutputCrlf	Specifies that if a Return is received from the LAN-attached device, a Return and a linefeed are sent to the device attached to the PAD.
EchoCrlf	Specifies that if a Return is received from the device attached to the PAD, a Return and a linefeed are echoed by the PAD.

LFPad

Syntax

```
SET -TERM LFPad = [None | <number> (1–127 nulls of padding)]
SETDefault [!<port>] -TERM LFPad = [None | <number>
  (1–127 nulls of padding)]
SHow -TERM LFPad
```

Default None

Description The LFPad parameter specifies the number of nulls the server inserts between the linefeed (LF) character and the next character. The BS, CR, FF, LF, and tab characters all have delay and pad parameter options.

To find the X.3 parameter equivalent to the LFPad parameter, refer to Appendix L in *Using NETBuilder Family Software*.

Values

None	No nulls are inserted.
<1–127>	From 1 to 127 nulls of padding are inserted.

LineERase

Syntax

```
SET -TERM LineERase = [Disabled | <char>]
SETDefault [!<config file>] -TERM LineERase = [Disabled | <char>]
SHow [!<port>] -TERM LineERase
```

Default ^U ([Ctrl] + U)

Description The LineERase parameter specifies the character that the gateway tells the PAD to interpret as a line-erase character. Entered before the current line is terminated by the Return key, the line-erase character deletes the entire line. This parameter applies to incoming connections.

To find the X.3 parameter equivalent to LineERase, refer to Appendix L in *Using NETBuilder Family Software.*

Values

Disabled	This value disables the LineERase parameter.
<char>	This value assigns a key or key combination as the line-erase character.

LocalEDit

Syntax

```
SET -TERM LocalEDit = [OFF | ON]
SETDefault [!<config file>] -TERM LocalEDit = [OFF | ON]
SHow [!<port>] -TERM LocalEDit
```

Default OFF

Description The LocalEDit parameter specifies whether local editing is used during a session (that is, when the port is in data transfer mode). When this parameter is enabled, the local editing characters can be used to edit a line during a session with a host. The port does not send these characters to the host as data. In conjunction with the appropriate DataForward, ECHOData, and IdleTimer settings, this parameter provides the mode. The LocalEDit parameter can be changed (automatically set) through, for example, Telnet option negotiation. This parameter applies to incoming connections.

To find the X.3 parameter equivalent to LocalEDit, refer to Appendix L in *Using NETBuilder Family Software*.

MaxSessions

Syntax

```
SET -TERM MaxSessions = <number> (1–8 sessions)
SETDefault [!<config file>] -TERM MaxSessions = <number>
  (1–8 sessions)
SHow [!<port>] -TERM MaxSessions
```

Default 2

Description The MaxSessions parameter specifies the maximum number of open sessions permitted on a single port. This parameter establishes an administrative limit; the actual number of sessions depends on the number of sessions available. This parameter applies to incoming connections.

NetAScii

Syntax

```
SET -TERM NetAScii = [UseLF | UseNUL]
SETDefault [!<config file>] -TERM NetAScii = [UseLF | UseNUL]
SHow [!<port>] -TERM NetAScii
```

Default UseLF

Description The NetAScii parameter specifies the character sequence transmitted by the Telnet protocol on the gateway when you press the Return key at the terminal. This parameter is used only by the terminal (active) port for Telnet sessions in netascii mode; it has no effect on a host (passive) port or when the Telnet session is in binary mode. NetAScii can be modified using the SETDefault command. The new value takes effect at the next session. This parameter applies to incoming connections.

Values	UseLF	Specifies a Return + LF character sequence. This value should be set for a host that neglects to strip a NUL following a Return.
	UseNUL	Specifies a Return + NUL character sequence. This value should be set for a host that correctly recognizes the Return + LF and Return + NUL as encoded network functions.

PARAmeters

Syntax

```
SHow [!<port>] -TERM PARAmeters
```

Default No default

Description The PARAmeters parameter displays the active values of the port- and session-related parameters for the current session if a session exists on a port. If there are no sessions but an active port, it displays the active values of the port parameters.

On a NETBuilder II system, valid port numbers are 0–128.

PARIty

Syntax

```
SET -TERM PARIty = ([None | Odd | Even | 1 | 0 | DoNotFold])
SETDefault [!<config file>] -TERM PARIty = ([None | Odd | Even | 1
  | 0 | DoNotFold])
SHow [!<port>] -TERM PARIty
```

Default None

Description The PARIty parameter specifies the local device parity. This parameter applies to both incoming and outgoing connections.

To find the X3 parameter equivalent to the PARIty parameter, refer to Appendix L in *Using NETBuilder Family Software*.

Values	None	Specifies no parity is in effect.
	Odd	Specifies odd parity is in effect.
	Even	Specifies even parity is in effect.
	DoNotFold	Used in conjunction with None, Odd, or Even parity. Allows the use of single eight-bit ASCII characters for control characters such as XON and XOFF.

PROFile

Syntax

```
SETDefault [!<port>] -TERM PROFile = [TELnet | TRansparent | X3 |
  Default]
SHow -TERM PROFile
```

Default TELnet

Description The PROFile parameter selects a virtual terminal profile for outgoing connections. If you change the value of this parameter, current sessions are not affected. The new value establishes the profile for the virtual terminal association (VTA) in subsequent sessions. Other ISO VTA-dependent parameters may be affected by the value of this parameter.

Values

TELnet	Provides service similar to the service provided by the Telnet protocol used in TCP/IP implementations.
TRansparent	Provides basic, asynchronous-mode, virtual "wire" communication.
X3	Enables functionality of 22 parameters according to the CCITT X.3 recommendations. For more information on X3 parameters, refer to Appendix L in *Using NETBuilder Family Software.*
Default	Enables the A-mode default virtual terminal profile.

ReprintLine

Syntax

```
SET -TERM ReprintLine = [Disabled | <char>]
SETDefault [!<config file>] -TERM ReprintLine = [Disabled |
  <char>]
SHow [!<port>] -TERM ReprintLine
```

Default ^R ([Ctrl] + R)

Description The ReprintLine parameter specifies the character that the gateway tells the PAD to interpret as a reprint-line character. This character is used to reprint all pending input on the current line before the line is terminated by the Return key. This parameter applies to incoming connections.

To find the X.3 parameter equivalent to the ReprintLine parameter, refer to Appendix L in *Using NETBuilder Family Software*.

Values

Disabled	Disables the ReprintLine parameter.
<char>	Assigns a key or key combination as the reprint-line character.

ROWs

Syntax

```
SET -TERM ROWs = <number> (1–255)
SETDefault [!<config file>] -TERM ROWs = <number> (1–255)
SHow [!<port>] -TERM ROWs
```

Default 24 (for incoming connections; parameter is inappropriate for outgoing connections)

Description The ROWs parameter sets and displays the number of lines in the terminal. If ROWs is requested by the Rlogin server, the information is transmitted by the Rlogin client during connection establishment or whenever the ROWs value is changed with the SETDefault command. This parameter is valid only for incoming Rlogin connections.

SavedParams

Syntax

```
SHow -TERM SavedParams [<filename>]
```

Default No default

Description The SavedParams parameter displays a list of all configuration tables saved on the disk. The list of tables includes both default tables (tables with filenames consisting of port numbers) and alternate tables (with filenames consisting of alphanumeric characters).

Because no tables exist initially, the message "Directory empty" appears after execution of the SHow -TERM SavedParams command. If numbers 1 through 32 are specified as a filename after the "Directory empty" message, the compiled-in default port- and session-related values are displayed even though these files do not initially exist on the disk.

You can also display the contents of configuration files by substituting a configuration file number for <filename>.

SESsions

Syntax

```
SHow [!<port>] -TERM SESsions
```

Default No default

Description The SESsions parameter displays a list of all current connections between the specified virtual port and other destinations.

Valid port numbers are 0–127 on a NETBuilder II system.

TERMType

Syntax

```
SET -TERM TERMType = "<string>"
SETDefault [!<config file>] -TERM TERMType = "<string>"
SHow [!<port>] -TERM TERMType
```

Default "network" (for incoming connections; parameter inappropriate for outgoing connections)

Description The TERMType parameter sets and displays the terminal type. The TERMType "<string>" is transmitted to the Rlogin server during incoming Rlogin connections. The TERMType "<string>" is sent by Telnet in response to a request from the host using the terminal type option (refer to RFC 1091). The string is sent as specified, not as one of the strings in the RFC.

The "<string>" has a maximum of 40 characters. This parameter also is used by the TELnet command.

VERBatim

Syntax

```
SET -TERM VERBatim = [Disabled | <char>]
SETDefault [!<config file>] -TERM VERBatim = [Disabled | <char>]
SHow [!<port>] -TERM VERBatim
```

Default ^V ([Ctrl] + V)

Description The VERBatim parameter specifies the character that the gateway interprets as a verbatim character. The next character following a verbatim character is to be used verbatim instead of interpreted by the gateway as a special character. The verbatim character has no effect if the next character entered is a Return. This parameter applies to incoming connections only.

Values

Disabled	Disables the VERBatim parameter.
<char>	Assigns a key or key combination as the verbatim character.

WordERAse

Syntax

```
SET -TERM WordERAse = [Disabled | <char>]
SETDefault [!<config file>] -TERM WordERAse = [Disabled | <char>]
SHow [!<port>] -TERM WordERAse
```

Default ^W ([Ctrl] + W)

Description The WordERAse parameter specifies the character that the gateway interprets as a word-erase character. Entered before the current line is terminated, (line termination occurs by pressing the Return key), the word-erase character deletes the word most recently typed. This parameter applies to incoming connections only.

Values

Disabled	Disables the WordERAse parameter.
<char>	Assigns a key or key combination as the word-erase character.

XmitBinary

Syntax

```
SET -TERM XmitBinary = [OFF | ON]
SETDefault [!<config file>] -TERM XmitBinary = [OFF | ON]
SHow [!<port>] -TERM XmitBinary
```

Default OFF

Description The XmitBinary parameter enables or disables a binary transmission request to the host. This parameter applies to incoming Telnet connections only; it affects the Telnet BINARY mode option negotiation.

A new value set by the network manager with the SETDefault command takes effect at the next session.

The XmitBinary parameter turns the binary transmission request to the host on or off; the host may refuse the request at any time. The current value of this parameter does not indicate the status of the session. Also, because the transmit and receive channels are independent, the session does not guarantee that both channels have the same options simultaneously.

Values

OFF	The gateway transmits 7-bit ASCII data while the session is in progress and pads the <CR> character with a <NUL> or <LF> character depending on the setting of the -TERM NetAScii parameter. If Telnet is not in BINARY mode and the XmitBinary is set to off, the gateway initiates negotiation for WONT BINARY and DONT BINARY.
ON	The gateway provides an 8-bit data path with the host, where the data packet retains the parity bit (some applications may require this). If Telnet is in BINARY mode and the XmitBinary is set to on, the gateway initiates negotiation for WILL BINARY and DO BINARY.

XON and XOFF

Syntax

```
SET -TERM XON = [Disabled | <char>]
SETDefault [!<config file>] -TERM XON = [Disabled | <char>]
SHow [!<port>] -TERM XON
SET -TERM XOFF = [Disabled | <char>]
SETDefault [!<config file>] -TERM XOFF = [Disabled | <char>]
SHow [!<port>] -TERM XOFF
```

Default ^Q ([Ctrl] + Q for XON)
^S ([Ctrl] + S for XOFF)

Description The XOFF and XON parameters specify characters that are recognized by the gateway (which tells the PAD) as Xoff/Xon flow control characters. These parameters apply to both incoming and outgoing connections.

The FlowCtrlTo and FlowCtrlFrom parameters must be configured to Xon_Xoff and not None in order for the key character assignment of the XON and XOFF parameters to be effective.

To find the X.3 parameter equivalent to XOFF and XON, refer to Appendix L in *Using NETBuilder Family Software*.

Values

Disabled This value disables the XON and XOFF parameters.

<char> This value assigns a key or key combination as the Xon or Xoff character.

62 UDPHELP Service Parameters

This chapter describes the UDPHELP Service parameters for the User Datagram Protocol (UDP) Broadcast Helper feature. Table 62-1 lists the UDPHELP Service parameters and commands.

Table 62-1 UDPHELP Service Parameters and Commands

Parameters	Commands
ActivePorts	ADD, DELete, SHow, SHowDefault
AuthDHCPServer	ADD, DELete, SHow, SHowDefault
BootpMaxHops	SETDefault, SHow, SHowDefault
BootpThreshold	SETDefault, SHow, SHowDefault
CONFiguration	SHow, SHowDefault
CONTrol	SETDefault, SHow, SHowDefault
ForwardAddress	ADD, DELete, SHow, SHowDefault
Name	ADD, DELete, SHow, SHowDefault
TTLOverride	SETDefault, SHow, SHowDefault

A UDP port is part of an entity address and not related to an interface (port) on the bridge/router. In the command syntax, the UDP port does not need to be preceded by an exclamation point (!).

ActivePorts

Syntax

```
ADD -UDPHELP ActivePorts {<UDP port> | <name>}
DELete -UDPHELP ActivePorts {{<UDP port> | <name>} | ALL}
SHow -UDPHELP ActivePorts [<UDP port> | <name>]
SHowDefault -UDPHELP ActivePorts [<UDP port> | <name>]
```

Default No default

Description The ActivePorts parameter adds or deletes a UDP port to or from the active port list. You can add up to 32 active ports to the list. You can also display a list of UDP ports on which UDP Broadcast Helper is enabled.

Values <UDP port> The value must be a decimal number in the range of 1 to 65,535. Because the UDP port is not related to a physical interface (port) on the bridge/router, you do not need to precede the UDP port number with an exclamation point (!).

UDP port numbers 77, 161, and 520 are reserved for the 3Com REMote command, Simple Network Management Protocol (SNMP), and Internet Protocol-Routing Information Protocol (IP-RIP), respectively. Do not add these UDP port numbers to the active ports list.

<name> The maximum length of a name string is eight characters; the leading character must be an English character. The name is not case-sensitive. You can specify a built-in name or a name you define. (For more information on built-in names, refer to Chapter 20 in *Using NETBuilder Family Software*.) If you define a name, you must define and map the name to a UDP port number using the -UDPHELP Name parameter. For more information, refer to "Name" on page 62-5.

ALL This option can be used to delete all entries from the active ports list.

AuthDHCPServer

Syntax

```
ADD -UDPHELP AuthDHCPServer <IP address>
DELete -UDPHELP AuthDHCPServer {<IP address> | ALL}
SHow -UDPHELP AuthDHCPServer [<IP address>]
SHowDefault -UDPHELP AuthDHCPServer [<IP address>]
```

Default No default

Description The AuthDHCPServer parameter adds or deletes an authorized Dynamic Host Configuration Protocol (DHCP) or BOOTP server to or from the server list. You can add up to 32 servers to the list. Any BOOTPREPLY or DHCP OFFER packet received with an IP source address that does not match any server's IP address on the list is discarded, a system message is entered, and an SNMP trap is sent. The trap object is defined as follows:

```
a3sysBogusDhcpSvr OBJECT-TYPE
SYNTAX IpAddress
STATUS mandatory
DESCRIPTION
“This object has the IP address of the last seen bogus DHCP or
 BOOTP server.”
:: = {a3ComSysMisc 11}
a3BogusDhcpSvr TRAP-TYPE
ENTERPRISE a3Com
VARIABLES {a3sysBogusDhcpSvr}
DESCRIPTION
“A a3BogusDhcpSvr trap signifies that an unauthorized DHCP or
 BOOTP server has been detected on the network.”
::=100
```

If the list is empty, the packet is forwarded to the client.

BootpMaxHops

Syntax

```
SETDefault !<port> -UDPHELP BootpMaxHops = <value>(1–16)
SHow [!<port> | !*] -UDPHELP BootpMaxHops
SHowDefault [!<port> | !*] -UDPHELP BootpMaxHops
```

Default 4

Description The BootpMaxHops parameter controls how far (across how many hops) a BOOTPREQUEST packet can travel on a network. You can set the appropriate values on a bridge/router so that clients in a given area of the network can only boot from a specific server or servers. If a bridge/router on the network receives a BOOTPREQUEST packet whose hop value is greater than or equal to its BootpMaxHops value, the packet is discarded. If the hop value is less than the bridge/router's BootpMaxHops value, the packet is forwarded. You can also display the setting of this parameter.

BootpThreshold

Syntax

```
SETDefault !<port> -UDPHELP BootpThreshold = <seconds>(0–300)
SHow [!<port> | !*] -UDPHELP BootpThreshold
SHowDefault [!<port> | !*] -UDPHELP BootpThreshold
```

Default 4

Description The BootpThreshold parameter configures your network so that BOOTPREQUEST packets initiated by clients across a gateway are prioritized and forwarded to a server according to a predetermined plan. Each bridge/router port can be set with a different BootpThreshold value (in seconds) depending upon which BOOTPREQUEST packets you want forwarded first by that port. The lower the BootpThreshold value, the sooner the BOOTPREQUEST is forwarded and processed.

Clients initially send out BOOTPREQUEST packets with the Seconds Elapsed Field set to 0. The client increments this field with each retry. The bridge/router compares the value of the BootpThreshold parameter to the Seconds Elapsed Field of the BOOTPREQUEST packet and forwards the request if the Seconds Elapsed Field is equal to or greater than the threshold value. Setting the threshold value to 0 causes the packet to be immediately forwarded by the bridge/router; you can use this setting for clients that do not increment the Seconds Elapsed Field only if there are no local BOOTP servers servicing requests.

CONFiguration

Syntax

```
SHow -UDPHELP CONFiguration
SHowDefault -UDPHELP CONFiguration
```

Default No default

Description The CONFiguration parameter displays all of the configuration values associated with the UDPHELP Service.

CONTrol

Syntax

```
SETDefault -UDPHELP CONTrol = [Enable | Disable]
SHow -UDPHELP CONTrol
SHowDefault -UDPHELP CONTrol
```

Default Disable

Description The CONTrol parameter specifies whether or not UDP Broadcast Helper is in service. You can also display the current value of this parameter.

ForwardAddress

Syntax

```
ADD -UDPHELP ForwardAddress {<UDP port> | <Name>} {{<IP address>
 <subnet mask> [Ones | Zeroes]]} | <list of interfaces>}
DELete -UDPHELP ForwardAddress {{{<UDP port> | <Name>} [<IP address>
 | <list_of_interfaces>]} | ALL}
SHow -UDPHELP ForwardAddress [<UDP port> | <name>]
SHowDefault -UDPHELP ForwardAddress [<UDP port> | <name>]
```

Variations:

```
ADD -UDPHELP ForwardAddress <UDP port or name> <IP address>
ADD -UDPHELP ForwardAddress <UDP port or name> <IP address>
 <subnet mask>
ADD -UDPHELP ForwardAddress <UDP port or name> <IP address>
 <subnet mask> Ones | Zeroes
ADD -UDPHELP ForwardAddress <UDP port or name> <list of
 interfaces>
```

Variations:

```
DELete -UDPHELP ForwardAddress <UDP port or name>
DELete -UDPHELP ForwardAddress <UDP port or name> <IP address>
DELete -UDPHELP ForwardAddress <UDP port or name>
 <list of interfaces>
DELete -UDPHELP ForwardAddress ALL
```

Default No default

Description The ForwardAddress parameter sets up for each UDP port added to the active port list by the ADD -UDPHELP ActivePorts command a list of networks or servers that should receive the UDP broadcast packets. If you add a network or server to the list, UDP Broadcast Helper sends a directed broadcast packet to each added network IP address and a packet directly to each added server IP address. A valid IP address can be added to the ForwardAddress list even if it cannot be reached at the time it is added. The maximum number of addresses that can be added is 32.

If your bridge/router is configured to boot from a server that must be accessed through an X.25, Frame Relay, or Switched Multimegabit Data Service (SMDS) interface, you must use this parameter to set up a list of networks or servers. The bridge/router does not rebroadcast BOOTPREQUEST packets over X.25, Frame Relay, or SMDS interfaces. For all other applications, 3Com recommends setting up a list for each UDP port to avoid broadcast loops. If you do not set up a list for each UDP port, network packets are rebroadcast to all links on the network.

You can also delete a UDP port and display the list of networks or server for a particular UDP port.

Values		
	<UDP port or name>	For a UDP port, the value must be a decimal number in the range of 1 to 65,535. Because the UDP port is not related to a physical interface (port) on the bridge/router, you do not need to precede the UDP port number with an exclamation point (!). For a UDP name, you can specify a built-in name or a name you define. (For more information on built-in names, refer to Chapter 20 in *Using NETBuilder Family Software*.) If you define a name, you must define and map the name to a UDP port number using the -UDPHELP Name parameter. For more information, refer to “Name.”
	<IP address>	This value must be in dotted decimal format.
	<subnet mask>	This value, if specified, must be in dotted decimal format, and must be formatted as a contiguous string of left-justified one bits. The default subnet mask is the same as the network mask.

Ones | Zeroes	This option configures the IP broadcast address. The value Ones indicates that the host portion of the IP address contains all one bits. The value Zeroes indicates that the host portion is all zero bits. The default value is all one bits.
ALL	This option can be used to delete all entries from the list.
<list of interfaces>	This option specifies a list of port numbers. The port numbers must be preceded by an exclamation point (!), and each port number must be separated by a comma, for example, !1, !2, !3.

Name

Syntax

```
ADD -UDPHELP Name <name string> <UDP port>
DELete -UDPHELP Name {{<name string> | <UDP port>} | ALL}
SHow -UDPHELP Name [<UDP port> | <name strings>]
SHowDefault -UDPHELP Name [<UDP port> | <name strings>]
```

Default No default

Description The Name parameter defines a name for a UDP port, maps it to a UDP port number, and adds it to a name list.

The following scenarios determine if you need to define a name for a UDP port and map the name to a UDP port number using SETDefault -UDPHELP Name command:

- If you added a UDP port using ADD -UDPHELP ActivePorts and specified it by port number, you can optionally define a name for the UDP port and map the name to a UDP port.
- If you added a UDP port using ADD -UDPHELP ActivePorts and specified it by a built-in name, you do not need to define a name. For more information on built-in names, refer to Chapter 20 in *Using NETBuilder Family Software*.
- If you added a UDP port using ADD -UDPHELP ActivePorts and specified it by a name you created, you must define the name and map it to a UDP port number.

You can configure up to 18 names. A one-to-one mapping between a name and a UDP port number exists; that is, no two names can have the same corresponding UDP port number or vice versa. You can also unmap one or all user-defined names bound to UDP ports.

You can display the current name mapped to UDP ports.

Values

<name string>	The maximum length of a name string is 8 characters; the leading character must be an English character. The name is not case-sensitive.
<UDP port>	The value must be in the range of 1 to 65,535. Because the UDP port is not related to a physical interface (port) on the bridge/router, you do not need to precede the UDP port number with an exclamation point (!).
ALL	Allows you to delete all user-defined names bound to UDP ports.

TTLOverride

Syntax

```
SETDefault -UDPHELP TTLOverride = <seconds>(1–255)
SHow -UDPHELP TTLOverride
SHowDefault -UDPHELP TTLOverride
```

Default 10

Description The TTLOverride parameter limits the reach of a broadcast packet and the potential duration of broadcast storms by specifying the default number of seconds that pass before a broadcast packet is discarded. The number of seconds is approximately equal to the number of hops.

Upon receiving a client's request packet, the bridge/router assigns the packet a time-to-live (TTL) value. The bridge/router assigns the lowest TTL value among the following possible sources:

- The TTL value of the incoming request packet minus one
- The TTL value configured by the -UDPHELP TTLOverride parameter
- The TTL value configured by the -IP DefaultTTL parameter

If the TTL value configured by -UDPHELP TTLOverride is the lowest, the bridge/router forwards the packet with the TTL value configured by this parameter, which overrides the other TTL values. For more information on the -IP DefaultTTL parameter, refer to Chapter 29.

You can also display the setting of this parameter.

63 VIP SERVICE PARAMETERS

This chapter describes all the parameters that are related to Banyan VINES Internet Protocol (VIP) routing. These parameters are found in the VIP Service. Table 63-1 lists the VIP Service parameters and commands.

Table 63-1 VIP Service Parameters and Commands

Parameters	Commands
ADDRess	SHow
AllRoutes	FLush, SHow
CONFiguration	SHow, SHowDefault
CONTrol	SETDefault, SHow, SHowDefault
HeaderFormat	SETDefault, SHow, SHowDefault
Metric	SETDefault, SHow, SHowDefault
Neighbor	FLush, SHow
RtrName	SETDefault, SHow, SHowDefault
SMDSGroupAddr	SETDefault, SHow, SHowDefault
STATUS	SHow
SymbolicNames	ADD, DELete, SHow, SHowDefault
UpdateTime	SETDefault, SHow, SHowDefault
WideAreaNbr	ADD, DELete, SHow, SHowDefault
X25PROFileid	SETDefault, SHow
X25ProtID	SETDefault, SHow, SHowDefault

ADDRess

Syntax

```
SHow -VIP ADDRess
```

Default No default

Description The ADDRess parameter displays the 48-bit VIP address of your router. The address consists of network number (32 bits) and the subnetwork number of 16 bits.

The 32-bit network number consists of the 11-bit vendor ID and the 21-bit serial number. The vendor ID for 3Com is 601 (octal), which is reserved by the Banyan Systems, Inc. The serial number is the 21 least-significant bits of Ethernet address of the 3Com router. The concatenation of the vendor ID and the serial number gives a unique network number for the 3Com routers. The subnetwork number for a service node or a router is always 0x0001.

AllRoutes

Syntax

```
FLush [!<port>] -VIP AllRoutes
SHow [!<port> | !*] -VIP AllRoutes [Dec | Hex | Sym]
```

Default Decimal display

Description The AllRoutes parameter displays all known VIP routes if a port number is not provided. The port number is optional. You can also delete all dynamic routes from the VINES Routing Table by using the FLush command; this command simultaneously removes all entries from the VINES Neighbor Table so that the two tables remain consistent.

Values The routing table can be displayed in three different formats: decimal, hexadecimal, and symbolic. To conform with the VINES server display, decimal format is the default display option. If symbolic is selected, those entries that have symbolic names assigned will be displayed in character strings. The difference between decimal and hexadecimal is how NETnumber and Gateway addresses are presented in the display. Hexadecimal format displays route status information while decimal format does not. The following is the list of possible route status:

Up Route is up and usable.

Dn Route is down and soon to be purged.

Ch Entry has been recently updated and must be included in the next RTP updates across permanent links.

Hd1 Route is in the first hold down period and identifies a network whose unreachable state was recently updated, but not verified.

Hd2 Route is in the second hold down period and indicates the unreachable state has been confirmed and it can be now advertised.

CONFiguration

Syntax

```
SHow [!<port> | !*] -VIP CONFiguration
SHowDefault [!<port> | !*] -VIP CONFiguration
```

Default No default

Description The CONFiguration parameter displays the current VIP configuration for the router.

CONTrol

Syntax

```
SETDefault !<port> -VIP CONTrol = ([Route | NoRoute], [Checksum
   | NoChecksum], [Arp | NoArp], [PktChrge | NoPktChrge], [Server
   | NoServer])
SHow [!<port> | !*] -VIP CONTrol
SHowDefault [!<port> | !*] -VIP CONTrol
```

Default NoRoute, NoChecksum, NoArp, NoPktChrge, Server

Description The CONTrol parameter tunes the behavior of the VIP router as described in the next section.

Values

Route | NoRoute — If Route is selected, the router routes VIP packets. If NoRoute is selected, the router stops routing VIP packets.

Checksum | NoChecksum — If Checksum is selected, error checking is performed to detect data corruption on the packets received. NoChecksum does not provide this service, but increases network performance.

Verification of checksums for Internet packets is performed at their final destinations, not at the intermediate routers.

Arp | NoArp — If Arp is selected, the router responds to both Address Resolution Protocol (ARP) Assignment Request Query and ARP requests and assigns VIP addresses to clients on the port chosen. NoArp ignores any ARP Queries and Requests on the port selected.

PktChrge | NoPktChrge — The class subfield in the VINES broadcast packets affects the way the router propagates broadcast packets. When the VINES router receives broadcast packets for all reachable nodes or servers except those on media that impose a packet charge, it forwards them to only those ports that have no charge; that is, those with NoPktChrge set. PktChrge prevents them from being forwarded on those ports.

Server | NoServer — NoServer must be selected on the interface where no VINES server exists, except WAN interfaces. This allows VINES to have all net broadcasts with a hop count of zero propagated. To locate VINES servers, clients generate VINES File Service and Security Service, which use all net broadcasts with a hop count of zero. This type of broadcast packet is not forwarded unless NoServer is configured. The NoServer option is not required if a server is located one hop away from a client since the client node tries at least twice, with the hop count set to 1 the second time.

HeaderFormat

Syntax

```
SETDefault !<port> -VIP HeaderFormat = Ethernet | Ieee | Snap
SHow [!<port> | !*] -VIP HeaderFormat
SHowDefault [!<port> | !*] -VIP HeaderFormat
```

Default

Ethernet for Ethernet interface
Ieee for token ring interface
Snap for FDDI interface

Description

The HeaderFormat parameter configures a preferred packet encapsulation type on Ethernet, fiber distributed data interface (FDDI), or token ring interfaces. The same header format should be used by both VINES servers and clients.

To display the current options for this parameter, use SHow -VIP HeaderFormat.

Values

Ethernet — Provides Ethernet encapsulation for all packets going out of the port.

Ieee — Provides IEEE encapsulation for all packets going out of the port. Effective on token ring interfaces only.

Snap — Provides Snap encapsulation for all packets going out of the port. Effective on Ethernet and FDDI Interfaces only.

Metric

Syntax

```
SETDefault !<port> -VIP Metric = <number> (1–512) | Default
SHow [!<port> | !*] -VIP Metric
SHowDefault [!<port> | !*] -VIP Metric
```

Default See "Values."

Description The Metric parameter displays the cost involved for a specific port, which is automatically calculated (200-millisecond intervals) based on the baud rate. Permissible values range from 1 to 512 milliseconds.

Values The recommended metric value depends on the medium and speed. Table 63-2 lists recommended metric values for specific interface types.

Table 63-2 Recommended Metric Values

Type of Interface	Metric (in 200 millisecond units)
10 Mbps Ethernet	2
16 Mbps Token Ring	2
4 Mbps Token Ring	4
>= 56 kbps	45
>= 9600 baud (X.25)	90
>= 4800 baud (HDLC/ASYNC)	90
>= 4800 baud (X.25)	150
>= 2400 baud (HDLC/ASYNC)	150
>= 1200 baud	450
>= 45 kbps	43
>= 128 kbps	42
>= 192 kbps	39
>= 256 kbps	36
>= 320 kbps	34
>= 384 kbps	32
>= 448 kbps	30
>= 512 kbps	28
>= 576 kbps	26
>= 640 kbps	24
704 kbps– 832 kbps	20
896 kbps–1024 Mbps	14
088–1.280 Mbps	10
1.344–1.535 Mbps	8
Tunneling through TCP/IP	25

Neighbor

Syntax

```
FLush [!<port>] -VIP Neighbor
SHow [!<port> | !*] -VIP Neighbor [Dec | Hex | Sym]
```

Default Decimal display. No default if nothing is available.

Description The Neighbor parameter displays a list of neighbor addresses that VIP Routing Update Protocol (RTP) uses to maintain the network table and the neighbor table to learn network topology. VIP uses the network table and the neighbor table to determine paths when routing packets.

The FLush command removes neighbor addresses for the specified port or removes all neighbor addresses in the table if no port number is specified.

The SHow command displays all neighbors currently known if no port number is provided. It also displays all neighbors learned from that port, providing the port is specified, including the NETnumber, subnet header format, media address, metric, and node type.

The neighbor table can be displayed in three different formats: decimal, hexadecimal, and symbolic. To conform with the VINES server display, decimal format is the default display option. The difference between decimal and hexadecimal is how the NETnumber is presented in the display. Symbolic format shows any symbolic names assigned to neighbors using the ADD -VIP SymbolicNames command.

The following is the list of possible Neighbor status:

Svr	Neighbor is a server or a router.
Clnt	Neighbor is a client.
Perm	Neighbor is permanent and will not age out. Any neighbor learned over a serial line is considered permanent.
IP	Neighbor is learned through IP.
Redir	Neighbor is in the process of RTP redirect.

RtrName

Syntax

```
SETDefault -VIP RtrName = “<string>”
SHow -VIP RtrName
SHowDefault -VIP RtrName
```

Default The concatenation of the prefix “3Com-” and the last 4 bytes (in hexadecimal) of the bridge/router Ethernet address.

Description The RtrName parameter assigns a unique system ID to a 3Com VINES router. It can be renamed to any string of 15 characters, but it must be unique in a given VINES network. Upon any server/router name request from neighbors, the VINES router responds with this name.

SMDSGroupAddr

Syntax

```
SETDefault !<port> -VIP SMDSGroupAddr = $<E0-E999999999999999> | None
SHow [!<port> | !*] -VIP SMDSGroupAddr
SHowDefault [!<port> | !*] -VIP SMDSGroupAddr
```

Default No default

Description The SMDSGroupAddr parameter configures an SMDS group address that is used as the VINES multicast address on the specified port. The port must be configured with the -PORT OWNer set to SMDS and the -VIP SMDSGroupAddr configured with a valid group address for VINES routing to occur over SMDS.

Values <E0–E999999999999999> The format for an SMDS group, or multicast, address. The group address type is used to route data to all routers 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, it is padded on the right with Fs.

None Removes a group address previously assigned to a port.

STATUS

Syntax

```
SHow [!<port> | !*] -VIP STATUS
```

Default Down

Description The STATUS parameter displays the VIP interface port status when routing has been enabled. Port status is either Up or Down.

SymbolicNames

Syntax

```
ADD -VIP SymbolicNames <number> (1-FFFFFFFE) “<string>”
DELete -VIP SymbolicNames <number> (1-FFFFFFFE) | ALL
SHow -VIP SymbolicNames
SHowDefault -VIP SymbolicNames
```

Default No default

Description The SymbolicNames parameter assigns symbolic names to VINES networks. When examining the VINES Routing Table and VINES Neighbor Table, these names can help identify specific networks or neighbors. Use the “Sym” option to display the routing and neighbors tables in symbolic format.

Three display options (decimal, hexadecimal, and symbolic) currently are available for the routing and neighbor tables. These names have no relationship with VINES StreetTalk names, are for internal use only, and are not advertised. Up to 128 symbolic names can be added and each name can be 15 characters long. If a symbolic name is longer than 15 characters, it is truncated. The network number must be entered as a decimal number. Symbolic names can be deleted per network, or the whole table can be displayed by using the ALL option. The “<string>” value must be entered inside double quotation marks.

UpdateTime

Syntax

```
SETDefault -VIP UpdateTime = <seconds> (5–65535)
SHow -VIP UpdateTime
SHowDefault -VIP UpdateTime
```

Default 90 seconds

Description The UpdateTime parameter specifies how often the router sends broadcast packets to let other routers know about its routing table.

WideAreaNbr

Syntax

```
ADD !<port> -VIP WideAreaNbr #<X.25 addr> | @<DLCI>
DELete !<port> -VIP WideAreaNbr #<X.25 addr> | @<DLCI>
SHow [!<port> | !*] WideAreaNbr
SHowDefault [!<port> | !*] WideAreaNbr
```

Default No default

Description The WideAreaNbr parameter modifies and displays the list of neighbor addresses that VIP RTP uses to determine to which neighbors it should send update packets over X.25 or Frame Relay interfaces. It is a port-dependent parameter. The port number is mandatory in the ADD and DELete command; it is optional in the SHow command. Up to 16 neighbors can be configured per port.

You must configure WideAreaNbr if you want VIP RTP to pass routing information over X.25 or Frame Relay. When no neighbors are configured, VIP RTP traffic is not passed over X.25 or Frame Relay.

Values

<X.25 addr>	Use this type of address to add neighbors if the media type of a selected port is X.25. You can prefix the address with the uppercase letters DTE or use the pound sign (#).
<DLCI >	Use this type of address to add neighbors if the media type of a selected port is Frame Relay. You can prefix the address with the uppercase letters DLCI or use the at sign (@).

X25PROFileid

Syntax

```
SETDefault !<port> -VIP X25PROFileid = <number> (0–255)
SHow [!<port> | !*] -VIP 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 VIP packets. A value of 0 indicates that no specific X.25 user profile is configured for VIP packets.

X25ProtID

Syntax

```
SETDefault !<port> -VIP X25ProtID = <protocol id> (1 octet)
SHow [!<port> | !*] -VIP X25ProtID
SHowDefault [!<port> | !*] -VIP X25ProtID
```

Default 0xBC

Description The X25ProtID parameter applies to routing VIP over an X.25 public data network. It specifies a protocol identifier to be included in all outgoing packets. Enter a value between 1 and FF.

When a packet reaches its destination, the destination router verifies this protocol identifier against its own protocol ID. If they match, the incoming packet is accepted. If they do not match, the packet is discarded. The chosen value must not conflict with that used by other protocols.

64

WE SERVICE PARAMETERS

This chapter describes the WE Service parameters, which relate to the WAN Extender system. For a description of the WAN Extender and instructions on how to configure a NETBuilder II to use a WAN Extender, refer to Chapter 36 in *Using NETBuilder Family Software.* For a description of ports and paths, and virtual paths, which apply to the WAN Extender, refer to Chapter 1 in *Using NETBuilder Family Software.*

Table 64-1 lists the WE Service parameters and commands.

Table 64-1 WE Service Parameters and Commands

Parameters	Commands
CONFiguration	SHow
DevCONTrol	SET
DevSTATistics	SHow
DialPathLimit	SETDefault, SHow, SHowDefault
ErrorThreshold	SETDefault, SHow, SHowDefault
FullStatusFreq	SETDefault, SHow, SHowDefault
KeepAliveInt	SETDefault, SHow, SHowDefault
ProFiles	SHow

CONFiguration

Syntax

```
SHow [!<port>] -WE CONFiguration
```

Default No default

Description The CONFiguration parameter displays the current WAN Extender system and network configuration settings for the specified port as well as its local management interface (LMI) parameters and their settings. If no port is specified, then the configuration information for all ports (and their owners) are displayed in ascending order.

Refer to Chapter 36 in *Using NETBuilder Family Software* for a sample display generated with the CONFiguration parameter.

DevCONTrol

Syntax

```
SET !<port> -WE DevCONTrol = ReBoot [<sec_delay>]
```

Default No default

Description The DevCONTrol parameter reboots the WAN Extender device that is connected to the specified port.

Values

<port>	Specifies the port that is connected to the device that is to be rebooted.
<sec_delay>	Specifies the amount of delay in seconds before the reboot occurs.

DevSTATistics

Syntax

```
SHow [!<port>] -WE DevSTATistics
Flush !<port> -WE DevSTATistics
```

Default No default

Description The DevSTATistics parameter displays the connection and data packet statistics for the specified NETBuilder II port entered, for the WAN Extender connected to the port, and for the WAN Extender network ports. The statistics displayed are maintained by the WAN Extender.

Refer to Chapter 36 in *Using NETBuilder Family Software* for a sample display generated with the DevSTATistics parameter.

This parameter can only be entered as a UI command at a local console. This parameter is not available through the Scheduler or Remote commands.

DialPathLimit

Syntax

```
SETDefault !<port> -WE DialPathLimit = <64/56kbps path count>[<384kbps
H0 path count>]
```

Default 64/56 kbps path count = 60
H0 path count = 0

The default varies depending on how many channels a WAN Extender unit combined with a particular networking service can support (see Table 64-2).

The range of paths for the 64 kbps path is 0–60, and for the H0 path (384 kbps) the range is 0–3.

Description The DialPathLimit parameter limits the number of virtual paths that are available in the dial pool from the WAN Extender connected to the specified port. Settings for 64 kbps and H0 virtual paths can be entered for the same port.

If you have multiple WAN Extenders connected to the same NETBuilder II and some ports are set up for dial-up virtual paths and others for channelized virtual paths, the DialPathLimit parameter must be set to a dial-up path count that considers the following:

- The overall limit of 75 virtual paths that can supported by the NETBuilder II
- The number of virtual paths that are already registered for dial-up
- The number of virtual paths that are already designated for channelized data connections
- The type of WAN Extender and the networking service being used, which in turn determines how many channels can be supported per WAN Extender port. Because channels and virtual paths have a one-to-one relationship, the number of channels supported determines how many virtual paths can be used.

- If the DialPathLimit setting is greater than the number of virtual paths that can be supported by the WAN Extender port, the number of virtual paths created will be the number of virtual paths supported, which is the smaller amount.

Table 64-2 shows how many channels per port each WAN Extender model can support combined with different networking services.

Table 64-2 Channels Supported by WAN Extender Models for Different Services

	Network Services and Channels Supported per Port			
WAN Extender Models	**Channelized T1**	**Channelized E1**	**ISDN PRI**	**Switch 56**
WAN Extender 2T	24 channels		23 B-channels 1 D-channel	24 channels
WAN Extender 2E		31 channels	30 B-channels 1 D-channel	

Example You have two WAN Extender 2T models (two ports each) connected to the same NETBuilder II. You configured one port of the first WAN Extender for channelized data connections using 20 virtual paths, and another 20 (64 kbps) virtual paths are set for dial-up for the other port of the first WAN Extender. You will have a total of 35 virtual paths to add for the ports of the second WAN Extender.

The following calculations show how many virtual paths are left to be added to the second WAN Extender ports:

> Seventy-five virtual paths supported by the NETBuilder II bridge/router, minus 20 virtual paths for channelized connections, minus 20 virtual paths for dial-up equals 35 virtual paths that can be added by a second WAN Extender without running out.

ErrorThreshold

Syntax

```
SETDefault !<port> -WE ErrorThreshold = (1 – 10)
SHowDefault !<port> -WE ErrorThreshold
```

Default 3

Description The ErrorThreshold parameter sets the maximum number of unanswered Status Enquiry messages sent by the NETBuilder II bridge/router before shutting down the physical path associated with the port and removing all related virtual paths.

FullStatusFreq

Syntax

```
SETDefault !<port> -WE FullStatusFreq = (1 – 255)
SHow !<port> -WE FullStatusFreq
SHowDefault !<port> -WE FullStatusFreq
```

Default 6

Description The FullStatusFreq parameter sets the number of KeepAlive intervals that pass before a Full Status Enquiry message is sent to the WAN Extender. Refer to “KeepAliveInt”for a description of KeepAlive intervals.

KeepAliveInt

Syntax

```
SETDefault !<port> -WE KeepAliveInt = (5 – 30)
SHow !<port> -WE KeepAliveInt
SHowDefault !<port> -WE KeepAliveInt
```

Default 10

Description The KeepAliveInt parameter sets the amount of time (in seconds) between successive transmissions of Status Enquiry messages to the WAN Extender.

ProFiles

Syntax

```
SHow [!<port>] -WE ProFiles [<first PID> | <first PID> <last PID>]
[STATistics | DETail]
```

Default SUMMary (neither STATistics or DETail are selected)

Description The ProFiles parameter retrieves information from the WAN Extender that is connected to the NETBuilder II bridge/router port. The information describes the configuration and the incoming and outgoing calls made through the port.

Refer to Chapter 36 in *Using NETBuilder Family Software* for a sample display generated with the ProFiles parameter.

This parameter can only be entered as a UI parameter at a local console. This parameter is not available through the Scheduler or Remote commands.

Values

<port>	Specifies the NETBuilder II bridge/router port for which you want the profile information. If no port is specified, the profiles for all the NETBuilder II bridge/router ports connected to the WAN Extender are displayed in ascending port order.
<first PID>	Specifies that the first profile ID is to be displayed for the port entered.
<first PID> <last PID>	Specifies a range from a first profile ID to a last profile ID, of profiles generated that you want displayed. For example, if you enter 5 for the first value and 10 for the last value, the system displays profiles 5 through 10 for the port entered. If the last profile is not entered, only the first profile is displayed.
STATistics	Specifies that statistics information be displayed for the associated profile.
DETail	Specifies that detailed information be displayed for the associated profile.
SUMMary	Specifies that if neither STATistics or DETail is selected, summary information associated with the profile is displayed. SUMMary is the default value.

65

X25 Service Parameters

This chapter describes the parameters for configuring serial lines on your bridge/router for communication with an X.25 public or private data network. Table 65-1 lists the X25 Service parameters and commands.

Table 65-1 X25 Service Parameters and Commands

Parameters	Commands
CONFiguration	SHow
CONTrol	SETDefault, SHow, SHowDefault
IncomingSVCs	SETDefault, SHow, SHowDefault
NbrPROFile	ADD, DELete, SHow
OutgoingSVCs	SETDefault, SHow, SHowDefault
PDNetworkType	SETDefault, SHow, SHowDefault
PVC	ADD, DELete, SHow
STATUS	SHow
Trace	SET, SETDefault, SHow, SHowDefault
TwowaySVCs	SETDefault, SHow, SHowDefault
X25Address	SETDefault, SHow, SHowDefault
X25PROFileid	SETDefault, SHow, SHowDefault
X25STATistics	FLush, SHow, SHowDefault

CONFiguration

Syntax

```
SHow [!<port>| !*] -X25 CONFiguration
```

Default No default

Description The CONFiguration parameter displays the values of the X25 Service parameters for all the serial ports. If you want to display the configuration for a specific port, specify the port number.

CONTrol

Syntax

```
SETDefault !<port> -X25 CONTrol = [ExtendedPacketSeq|
  NoExtendedPacketSeq]
SHow [!<port>|!*] -X25 CONTrol
SHowDefault [!<port>|!*] -X25 CONTrol
```

Default NoExtendedPacketSeq

Description The CONTrol parameter configures extended packed sequence numbering for a specified port.

Values

ExtendedPacketSequence	Indicates that packet sequencing is performed modulo 128.
NoExtendedPacketSequence	Indicates that packet sequencing is performed modulo 8.

IncomingSVCs

Syntax

```
SETDefault !<port> -X25 IncomingSVCs = NONE | <1–4095> {,<1–4095>}
SHow [!<port> | !*] -X25 IncomingSVCs
SHowDefault [!<port> | !*] -X25 IncomingSVCs
```

Default NONE

Description The IncomingSVCs parameter specifies the circuits or logical channel numbers (LCNs) on each port allocated exclusively for incoming calls. The X.25 standard specifies a range of 1 through 4095 LCNs, which can be used for permanent incoming, outgoing, or two-way (both incoming and outgoing) calls. The IncomingSVCs parameter specifies the number of LCNs allocated exclusively for incoming calls.

Values

NONE	Indicates no circuits are allocated exclusively for incoming calls.
<min>, <max>	Specifies a value or range of values between 1 and 4095 to indicate LCNs allocated exclusively for incoming calls.

NbrPROFile

Syntax

```
ADD -X25 NbrPROFile <dte_addr(1..14 digits)> <profile id>
DELete -X25 NbrPROFile <dte_addr(1..14 digits)> <profile id>
SHow -X25 NbrPROFile
```

Default No default

Description The NbrPROFile parameter configures a profile ID for each neighboring data terminal equipment (DTE). This profile ID overrides the X.25 profile ID configured for a specified port when establishing a call to or from a DTE. If the profile ID is not assigned to a neighboring DTE, the X25PROFileid parameter value is used. The DELete command removes the association between the X.25 DTE address and the X.25 DTE profile.

For more information on configuring a profile ID, refer to “X25PROFileid” on page 65-4.

OutgoingSVCs

Syntax

```
SETDefault !<port> -X25 OutgoingSVCs = NONE | <1–4095> {,<1–4095>}
SHow [!<port> | !*] -X25 OutgoingSVCs
SHowDefault [!<port> | !*] -X25 OutgoingSVCs
```

Default NONE

Description The OutgoingSVCs parameter specifies the number of LCNs allocated exclusively for outgoing calls. The X.25 standard specifies a range from 1 through 4095 LCNs to be distributed for permanent incoming, outgoing, or two-way (both incoming and outgoing) traffic. You can distribute the LCNs according to the requirements of your installation.

Values

NONE	Specifies that no LCNs are allocated exclusively for outbound calls.
<min>, <max>	Specifies one or a range of numbers between 1 and 4095 to indicate the LCNs to be used exclusively for outbound calls.

PDNetworkType

Syntax

```
SETDefault !<port> -X25 PDNetworkType = PRIVATE | TELENET | TYMNET
 | PSS | DDN | BFE | NET2 | DATEX | TRANSPAC | LAPOSTE
SHow [!<port> | !*] -X25 PDNetworkType
SHowDefault [!<port> | !*] -X25 PDNetworkType
```

Default PRIVATE

Description The PDNetworkType parameter configures a port for communication with a particular type of public data network. For example, if you subscribe to the Telenet public data network (PDN), you need to set this parameter to TELENET.

PVC

Syntax

```
ADD !<port> -X25 PVC <lcn1> [,lcn2] <destination dte address>
 <protocol ID> [<user profID>]
DELete -X25 PVC <lcn1>, <lcn2>
SHow -X25 PVC
```

Default No default

Description The PVC parameter configures a permanent virtual circuit on the specified logical channel numbers (LCNs) to and from the specified DTE address.

Values

<lcn1> ,lcn2	Indicates the logical channel number. This can be a single (lcn1) value or a range of values as needed (lcn2, lcn3).
<destination dte address>	Specifies the address of the destination DTE.
<protocol ID>	Specifies the protocol ID of the network protocol to be used on the PVC.
<user profID>	Specifies the user profile identification number.

STATUS

Syntax

```
SHow [!<port> | !*] -X25 STATUS
```

Default No default

Description The STATUS parameter provides information about the status of the X.25 line, including the virtual circuit number, the virtual circuit state, the packet size, the window size used by the virtual circuit, the user and DTE profile IDs, compression type, and the DTE address to or from which the virtual circuit was originated.

Trace

Syntax

```
SET !<port> -X25 Trace = ([Data | NoData], [Control | NoControl])
SETDefault !<port> -X25 Trace = ([Data | NoData], [Control |
 NoControl])
SHow [!<port> | !*] -X25 Trace
SHowDefault [!<port> | !*] -X25 Trace
```

Default NoData, NoControl

Description The Trace parameter displays information for the specified X.25 port at the network layer (level 3) for debugging purposes. This parameter can be set to display both packet contents and header contents or header only.

Values

Data | NoData	Indicates whether the data displays complete packet content information including header. NoData does not display packet content information.
Control | NoControl	Specifies whether control displays only packet header information. NoControl does not display packet header information.

TwowaySVCs

Syntax

```
SETDefault !<port> -X25 TwowaySVCs = NONE | <1–4095> {,<1–4095>}
SHow [!<port> | !*] -X25 TwowaySVCs
SHowDefault [!<port> | !*] -X25 TwowaySVCs
```

Default 1, 4095

Description The TwowaySVCs parameter specifies the number of circuits to be used for two-way calls. The X.25 standard specifies a range of from 1 through 4,095 logical channel numbers (LCNs) to be used for permanent incoming, outgoing, or two-way (both incoming and outgoing) traffic. TwowaySVCs specifies the number of LCNs allocated exclusively for two-way (both outgoing and incoming) traffic. The default assigns all switched virtual circuits (SVCs) with LCN numbers from 1 through 4,095 as two-way SVCs.

Values

NONE	Specifies that no circuits are used for two-way calls.
<min>, <max>	Specifies one or more numbers between 1 and 4095 to indicate the circuits to be used exclusively for two-way calls.

X25Address

Syntax

```
SETDefault !<port> -X25 X25Address = NONE | <0–99999999999999>(1–15
 digits)>
SHow [!<port> | !*] -X25 X25Address
SHowDefault [!<port> | !*] -X25 X25Address
```

Default NONE

Description The X25Address parameter assigns the local DTE address for each port used for X.25 routing. A DTE address must be configured for each port used for X25 Service in all data networks except a PDN. To remove an address, use the NONE value.

Do not specify this parameter for a virtual port; specify it for a nonvirtual port only.

X25PROFileid

Syntax

```
SETDefault !<port> -X25 X25PROFileid = <profile ID (0–255)>
SHow [!<port> | !*] -X25 X25PROFileid
SHowDefault [!<port> | !*] -X25 X25PROFileid
```

Default 0

Description The X25PROFileid parameter creates an X.25 profile. When you specify a profile ID, X.25 uses the specified DTE profile to establish a call request for that port. A profile ID of 0 means the default DTE profile will be used.

X25STATistics

Syntax

```
FLush [!<port>] -X25 X25STATistics
SHow [!<port> | !*] -X25 X25STATistics
SHowDefault [!<port> | !*] -X25 X25STATistics
```

Default No default

Description The X25STATistics parameter displays the statistics for the specified port. If no port is specified, statistics for all ports are displayed.

The FLush command clears the X.25 statistics.

66 XSWITCH SERVICE PARAMETERS

This chapter describes XSWitch Service parameters for configuring X.25 local and global switching on the bridge/router. Table 66-1 lists the XSWitch Service parameters and commands.

Table 66-1 XSWitch Service Parameters and Commands

Parameters	**Commands**
CONFiguration	SHow
CONTrol	SETDefault, SHow
SWitchedVC	DELete, SHow
TUNnelPassWord	SETDefault, SHow
TUNnelPort	SETDefault, SHow
X25Prefix	ADD, DELete, SHow
XSWPVC	ADD, DELete, SHow

CONFiguration

Syntax

```
SHow -XSWitch CONFiguration
```

Default No default

Description The CONFiguration parameter displays the current XSWitch configuration.

CONTrol

Syntax

```
SETDefault -XSWitch CONTrol = ([LoclSW | NoLoclSW], [GlobSW |
  NoGlobSW])
SHow -XSWitch CONTrol
```

Default LoclSW, GlobSW

Description The CONTrol parameter enables and disables local and global switching.

Values

LoclSW | NoLoclSW	LoclSW enables local switching for the entire bridge/router. NoLoclSW disables local switching.
GlobSW | NoGlobSW	GlobSW enables global switching for the entire bridge/router. NoGlobSW disables global switching.

SWitchedVC

Syntax

```
DELete -XSWitch SWitchedVC <SW#> | ALL
SHow -XSWitch SWitchedVC
```

Default No default

Description The SWitchedVC parameter deletes one or all switched circuits and displays current switched circuit information. The display includes switched circuit number, X25 source address, destination address, input-requested high-speed serial (HSS port) or Internet Protocol (IP) address, switched-output HSS port or IP address, status, and number of bytes transferred.

Switched virtual circuits are numbered from 0 to 63 on the NETBuilder bridge/router and from 0 to 127 on the NETBuilder II bridge/router.

You can disconnect a virtual circuit at any time using the DELete SWitchedVC command.

The display of virtual circuit information reports the state of each virtual circuit, using the following three abbreviations:

ACT	Active (connected) state in which a virtual circuit has been established and communication is taking place.
WFC	Waiting For Connection state in which a virtual circuit has not yet been established to the destination.
WFD	Waiting For Disconnect state in which communication is complete and the virtual circuit is about to be disconnected.

Deleting a virtual circuit disconnects the virtual circuit.

TUNnelPassWord

Syntax

```
SETDefault -XSWitch TUNnelPassWord = "<string>"
SHow -XSWitch TUNnelPassWord
```

Default No default

Description The TUNnelPassWord parameter configures a password for the tunnel. It is used for limited-security authentication of incoming requests. If a bridge/router is configured with a password, each time it issues an encapsulated X.25 call request the global switch service attaches the password. When the remote bridge/router receives this encapsulated X.25 call request through the tunnel, a limited-security authentication is executed.

If the remote bridge/router is also configured with a password, its local TUNnelPassWord and the password in the encapsulated X.25 call request must match before the remote bridge/router accepts the tunnel session. If the remote bridge/router is not configured with any password, it accepts any incoming request, bypassing the verification sequence and directly processing the encapsulated X.25 call request. To initiate a tunnel to a peer that has TUNnelPassWord configured, the local bridge/router must be configured with the same password.

TUNnelPort

Syntax

```
SETDefault -XSWitch TUNnelPort = <0h-7FFFh>
SHow -XSWitch TUNnelPort
```

Default 357h

Description The TUNnelPort parameter defines a user-configurable Transmission Control Protocol (TCP) port number on which the tunnel can listen. The bridge/router provides a default port for the tunnel if there is no user-defined port.

X25Prefix

Syntax

```
ADD !<ip addr> | !<x.25 port> -XSWitch X25Prefix <x25prefix>
  [, <x25prefix> [,…]]
DELete !<ipaddr> | !<x.25 port> -XSWitch X25Prefix <x25prefix>
  [, <x25prefix>| ALL | Default}
SHow [!<ip addr> | !<x.25 port>] -XSWitch X25Prefix
```

Default No default.

The Default value can only be used with the DELete command.

Description The X25Prefix parameter allows the XSWitch Service to maintain a table of X.25 prefix address mappings. The mapping between X.25 prefix and target can be one of two forms: X.25 prefix to HSS port for local switching or X.25 prefix to IP address for global switching.

The ADD command adds static HSS ports and IP addresses to the X25Prefix table. The DELete command deletes a single entry, a group of entries, or all entries from the address prefix table.

Values

<ip addr>	Specifies target IP address for global switching.
<x.25 port>	Specifies target HSS port for local switching.
<x25prefix>	Specifies X.25 prefix. Switching occurs when the destination call field of an incoming X.25 call matches a configured data terminal equipment (DTE) address (X.25 prefix).
Default	Identifies an X25Prefix default HSS port. When the bridge/router receives an incoming call with a called address that does not match an entry in the prefix table, the call is switched to the default port. The default value applies to local switching as well as to outgoing X.25 service. The Default value can only be used with the DELete command syntax.

XSWPVC

Syntax

```
ADD !<ip addr> | !<x.25 port> -XSwitch XSWPVC <SDTE (1...14
  digits)> <SLCN> <dest ipa> | !<dest x.25 port> <DDTE (1...14
  digits)> <DLCN>
DELete !<ip addr> | !<x.25 port> -XSwitch XSWPVC <SDTE (1...14
  digits)> <SLCN> | ALL
SHow -XSWitch XSWPVC
```

Default No default

Description The XSWPVC parameter defines the configuration for both local and global switches. This parameter maintains a permanent virtual circuit (PVC) mapping table locally for local switching and source-to-destination DTE mapping for global switching and tunneling.

A tunnel is established between two NETBuilder bridge/routers with one bridge/router acting as the local end and the other acting as the remote end. Multiple cirtuits can be supported between two NETBuilder bridge/routers where each circuit is set up independenty.

The local end (source) and remote end (destination) addresses can be an IP address or HSS port. For tunnel mapping, one address must be an HSS port and the other must be an IP address. When the local end (source) is an HSS port and the remote end (destination) is an IP address, the circuit is called the local end of the tunnel. WHen the local end (source) is an IP address and the remote end is an HSS port, the circuit is called the remote end of the tunnel. The NETBuilder bridge/router can support both local and remote end tunnels at the same time as long as each circuit is properly configured on both NETBuilder bridge/routers.

Using X25 PVC support for tunneling, the circuit remains up at all times regardless of the state of the HSS or LAN tunnel. When the PVC is properly configured and the NETBuilder is booted, or when the HSS or LAN (IP) state is bounced, tunnel setup continuously attempts to connect the local end to the remote end until a tunnel circuit is established and running. The PVC tunnel is in the down state only when the HSS or LAN interface is in the down state.

Values

<ip addr> Specifies local end (source) IP address for global switching.

<x.25 port> Specifies local end (source) HSS port for local switching.

<SDTE> Specifies local end (source) X25 address (X25 prefix). This address can consist of 1 to 14 digits.

<SCLN> Indicates the local end (source) logical channel number.

<dest x.25> Indicates the remote end (destination) IP address for global switching.

<DDTE> Specifies remote end (destination) X25 address (X25 prefix). This address can consist of 1 to 14 digits.

<DLCN> Indicates the remote end (destination) logical channel number.

A

SysconF Command Menus

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

This appendix describes each menu option of the SysconF command for the following NETBuilder platforms:

- NETBuilder II with DPE module
- NETBuilder II with CEC module (refer to page A-9)
- SuperStack II NETBuilder and OfficeConnect NETBuilder bridge/routers (refer to page A-21)

NETBuilder II with DPE

This section describes the System Configuration menu for the NETBuilder II bridge/router with DPE module installed.

Syntax

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

Minimum Privilege

“Root” user with Network Manager privilege

Description

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.

Normal Response

A menu appears that allows you to configure the firmware parameters for your system.

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

The following sections describe each menu option and suboption.

Serial Ports

The Serial Ports parameter sets the baud rate for the CONSOLE port. This port is located on the connector/LED panel of the DPE module.

Possible baud rate settings are:

```
1. 110 bps
2. 300 bps
3. 1200 bps
4. 2400 bps
5. 4800 bps
6. 9600 bps
7. 19200 bps
8. 38400 bps
9. 57600 bps
10. 115200 bps
```

Databits are always set at 8 and parity at none.

Default The default baud rate is 9600 bps.

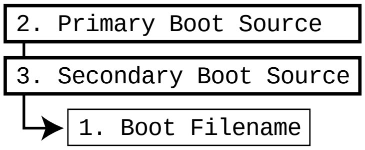
Primary Boot Source and Secondary Boot Source

The Primary Boot Source parameter allows you to set the path for your primary boot source. The Secondary Boot Source parameter allows you to set the path for the alternative boot source if the primary boot source fails. Both of these parameters work in conjunction with the Boot Sources parameter. For more information, refer to “Boot Sources” on page A-5.

The following options are available:

```
1. Boot Filename
2. Config File Source
3. IP Addresses
4. FTP login parameters
```

Boot Filename



You are prompted for the drive, path, and filename. Use:

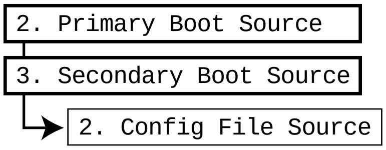
```
[<drive>:][/<path>]<filename>
```

Enter the entire path of the boot file. If you do not specify a drive, the path will be for drive A.

The configuration files must reside on the same drive as the boot source. If the drive you specify is different from the Config File Source drive, you receive a message asking whether you want to change the Config File Source to the same drive.

If the boot drive you specify conflicts with the one set in the Dump Destination parameter on page A-5, you are prompted for a different drive.

Config File Source



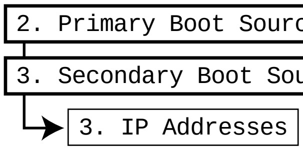
Specifies where the boot device accesses the configuration files during the boot sequence. You are prompted for the default directory. Use:

```
[<drive>:]/<path>
```

The configuration files must reside on the same drive as the boot source. If the drive you specify is different from the Boot Filename drive, you receive a message asking whether you want to change the Boot Filename to the same drive.

If the drive you specify conflicts with the one set in the Dump Destination parameter on page A-5, you are prompted for a different drive.

IP Addresses



Specifies IP addresses for the following:

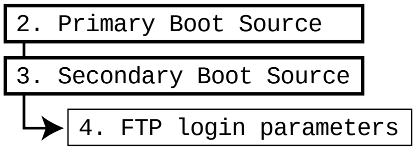
```
1. Client
2. Server
3. Gateway
4. Remote File Server (not applicable)
5. Subnet Mask
```

Default The default setting is 0.0.0.0.

To specify an address, enter an IP address in the dotted decimal notation (for example, 129.213.24.31), then press the Return key.

To delete an IP address, enter 0.0.0.0 or press the space bar once, then press the Return key.

FTP login parameters



The following options are available:

```
  1. Username
  2. Password
  3. Account
```

Each option can be up to 20 characters long.

Test Boot Source

The Test Boot Source parameter does the following tasks:

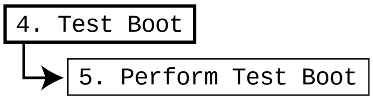
- Initiates the system reboot directly from the test boot source menu
- Clears the test boot timer when the test boot succeeds

The following options are available:

```
1. Boot Filename
2. Default File Source
3. IP Addresses
4. FTP login parameter
5. Perform Test Boot
6. Clear Test Boot Timer
```

Refer to "Primary Boot Source and Secondary Boot Source" on page A-2 for information about the first four options. Options 5 and 6 are specific to the Test Boot Source parameter.

Perform Test Boot



4. Test Boot

5. Perform Test Boot

If you are updating software from a remote device, you must perform a test boot of the new software to determine its reliability.

The following prompt is displayed:

```
Enter number of seconds until automatic reboot after test boot
  (CR = 0):
```

3Com recommends entering 300 seconds, which should allow the system enough time to initialize.

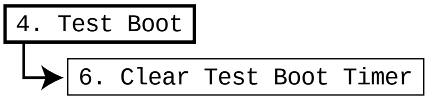
The following prompt is displayed:

```
Press Y to test boot now (any other key to cancel):
```

Type Y to initiate the test boot.

If the test boot is successful, you will access the new software. If the test boot fails, the bridge/router waits the number of seconds specified earlier, and then attempts to reboot using the primary boot source.

Clear Test Boot Timer



4. Test Boot

6. Clear Test Boot Timer

If your test boot fails and you do not want to wait the number of seconds you specified until automatic reboot, you can clear the timer by entering this parameter.

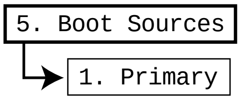
Boot Sources The Boot Sources parameter determines which boot source will be used.

The following options are available:

```
1. Primary
2. Primary and Secondary
3. Secondary
```

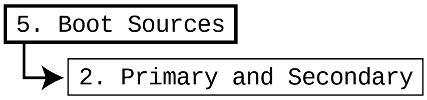
Default The default is Primary and Secondary.

Primary



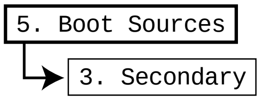
The primary option causes the system to boot from the primary boot source only.

Primary and Secondary



The primary and secondary option causes the system to boot from the primary boot source first, and if this boot source fails, then boot from the secondary boot source.

Secondary



The secondary option causes the system to boot from the secondary boot source only.

For complete information on the Secondary Boot Source parameter, refer to "Primary Boot Source and Secondary Boot Source" on page A-2.

Dump Destination The Dump Destination parameter selects where the contents of bridge/router memory will be stored in case of a crash (fatal error). (The Recovery Procedure parameter allows you to decide whether to store this memory and which module contents to store.)

You must configure the Recovery Procedure parameter for the dump destination to take effect.

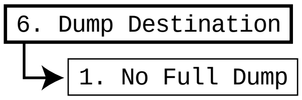
The following options are available:

```
1. No Full Dump
2. Single PC Card Full Dump to Drive A
3. Single PC Card Full Dump to Drive B
4. Multiple PC Card Full Dump to Drive A
5. Multiple PC Card Full Dump to Drive B
```

Default The default is No Full Dump.

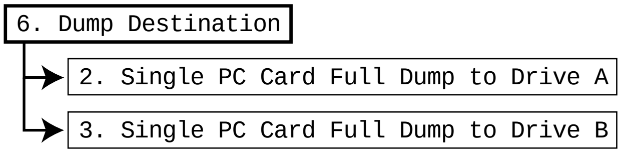
A partial dump is stored on the internal FPROM every time there is a fatal error or crash, regardless of the Dump Destination and Recovery Procedure settings.

No Full Dump



No full dump type or destination is configured. A full dump will not occur even if the Recovery Procedure parameter is set to dump.

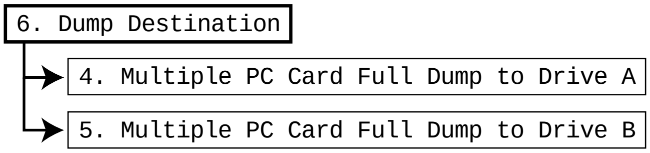
Single PC Card Full Dump to Drive A or B


6. Dump Destination
2. Single PC Card Full Dump to Drive A
3. Single PC Card Full Dump to Drive B

The system dumps as much as will fit on a single flash memory card. A single card, depending on the size, may be large enough for the entire dump.

You cannot set the dump destination to the same drive as your primary, secondary, or test boot source. If drives A and B are configured for boot sources, you must select No Full Dump.

Multiple PC Card Full Dump to Drive A or B


6. Dump Destination
4. Multiple PC Card Full Dump to Drive A
5. Multiple PC Card Full Dump to Drive B

The system dumps onto as many flash memory cards as needed. A single card, depending on the size, may be large enough for the entire dump, but if your dump is larger than one card, you can use extra flash memory cards as prompted.

You cannot set the dump destination to the same drive as your primary, secondary, or test boot source. If drives A and B are configured for boot sources, you must select No Full Dump.

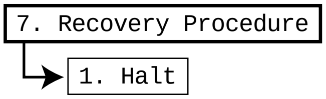
Recovery Procedure

The Recovery Procedure parameter configures the behavior and recovery in case of a crash (fatal error) of the NETBuilder II system and each MP module.

The DPE module slot and each slot with an MP module can each be set to one of the following options:

```
1. Halt
2. Halt System
3. Reboot
4. Reboot System
5. Dump and Reboot
6. Selective Dump and Reboot
```

Halt



If the DPE module fails, the system halts and enters the boot monitor.

If an MP module fails, the module stops operating, but the system continues to run.

Halt System

```
7. Recovery Procedure
  └─> 2. Halt System
```

If the DPE or an MP module fails, the system halts and enters the boot monitor.

Reboot

```
7. Recovery Procedure
  └─> 3. Reboot
```

If the DPE module fails, the system reboots.

If an MP module fails, the MP module reboots.

Reboot System

```
7. Recovery Procedure
  └─> 4. Reboot System
```

If the DPE or MP module fails, the system reboots.

Dump and Reboot

```
7. Recovery Procedure
  └─> 5. Dump and Reboot
```

If the DPE module fails, the system dumps the memory of the DPE module (refer to “Dump Destination” on page A-5) and reboots.

If an MP module fails, the system dumps the memory of the MP module and the DPE module and reboots.

The All option sets each MP module to dump itself and the DPE module and reboot.

Selective Dump and Reboot

```
7. Recovery Procedure
  └─> 6. Selective Dump and Reboot
```

This option allows you to dump the failing MP module as well as any other specified MP module. The DPE module will always dump.

After the dump occurs, the system reboots.

The All option sets each module to dump all modules. If you enter no at the prompt to dump and reboot all, all modules will cause a dump, but only the DPE module will be dumped.

MP Boot Source

The MP Boot Source parameter specifies the software image each MP module uses as a boot source. The boot source image location is kept in a configuration file, not in FPROM. This configuration file must be kept with the other configuration files in the primary, secondary, or test directories for standard boot or upgrade. If the boot source image location configuration file is not found, the default values are used for the MP module image names.

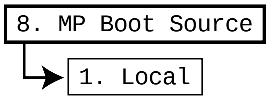
If you want to access the MP boot file from a location other than the default configuration file directory, use the MP Boot Source parameter.

The following options are available:

```
1. Local
2. Default File Source
```

Default The default is Default File Source.

Local



The following options are displayed:

```
1. Drive A
2. Drive B
```

Default The default is Drive A.

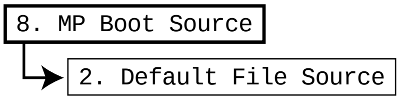
The following prompt is displayed:

```
Enter MP Boot Filename:
```

Enter the name of the MP boot filename, including the path:

```
[<drive>:][/<path>]/<filename>
```

Default File Source



The following prompt is displayed:

```
Enter MP Boot Filename:
```

Enter the name of the MP boot filename.

Default The default drive and path are the same as the configuration file location.

Boot Statistics

The Boot Statistics parameter displays the following information:

- Number of boots, including the date and time of last successful boot
- Number of exceptions, including date and time of last exception (unsuccessful boot)
- Boot source used for last successful boot
- Last error during boot attempt

When you have the information you need, you can clear the boot statistics by typing Y.

NETBuilder II with CEC

This section describes the System Configuration menu for the NETBuilder II bridge/router with CEC module installed.

Syntax

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

Minimum Privilege

“Root” user with Network Manager privilege

Description

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.

You can also configure the firmware parameters by entering the MONitor command to use the monitor.

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.

```
1.  Serial Ports            See page A-9
2.  Self-Test               See page A-10
3.  Start-Up Action         See page A-10
4.  Primary Boot Source     See page A-11
5.  Secondary Boot Source   See page A-11
6.  Test Boot Source        See page A-16
7.  Boot Sources            See page A-17
8.  Dump Destination        See page A-18
9.  Recovery Procedure      See page A-19
10.  MP Boot Source         See page A-20
11.  Boot Statistics        See page A-20
```

The following sections describe each menu option and suboption.

Serial Ports

The Serial Ports parameter sets the baud rate for the CONSOLE and AUXILIARY ports. These ports are located on the connector/LED panel of the CEC module.

The following options are available:

```
1. Console
2. Auxiliary
```

Possible baud rate settings for both parameters are:

```
1. 110 bps
2. 300 bps
3. 1200 bps
4. 2400 bps
5. 4800 bps
6. 9600 bps
7. 19200 bps
```

Databits are always set at 8 and parity at none.

Default

The default baud rate is 9600 bps.

Self-Test

The Self-Test parameter determines how your system handles self-tests when you turn the power on or reset.

The following options are available:

```
1. Skip self-test
2. Run self-test
```

Default The default is Skip self-test.

Start-Up Action

The Start-Up Action parameter determines the boot action when you turn the power on or reset.

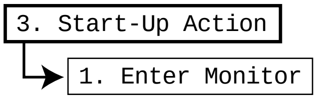
The following options are available:

```
1. Enter monitor
2. Local
3. Try boot once
4. Try boot forever
```

The bridge/router goes through self-tests, if configured, before booting.

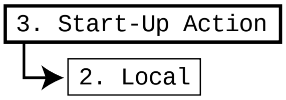
Default The default is Try boot forever.

Enter Monitor



The system enters the monitor utility.

Local



The system boots from the local drive even if it is not specified as the primary or secondary boot source.

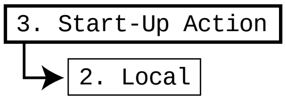
The following options are available:

```
1. Drive A
2. Drive B
```

After entering the drive number, you are prompted for the filename:

```
Enter Boot Filename (CR = no change):
```

Try Boot Once



The system attempts to boot from the source specified in the Primary Boot Source parameter. If unsuccessful, the system attempts to boot from the source specified in Secondary Boot Source parameter. If booting is still unsuccessful, the system enters the monitor utility.

Try Boot Forever

```
3. Start-Up Action
  └► 4. Try Boot Forever
```

The system attempts to boot from the source specified in the Primary Boot Source parameter. If unsuccessful, the system attempts to boot from the source specified in the Secondary Boot Source parameter. The system keeps trying to boot until it is successful.

Primary Boot Source and Secondary Boot Source

The Primary Boot Source parameter allows you to set the path for your primary boot source. The Secondary Boot Source parameter allows you to set the path for the alternative boot source if the primary boot source fails. Both of these parameters work in conjunction with the Boot Sources parameter. For more information, refer to "Boot Sources" on page A-17.

The following options are available:

```
1. Boot Device
2. Default File Source
3. Maximum Retries
4. I/O Module Parameters
5. Boot Protocol
6. IP Addresses
7. MAC Address
8. ARP Format
9. FTP login parameter
```

Boot Device

```
4. Primary Boot Source
5. Secondary Boot Source
  └► 1. Boot Device
```

You can specify the following boot device options:

```
1. Local
2. Network
```

Default The default primary boot device is local. The default secondary boot device is network.

Local The system attempts to boot from the local flash memory drive. If it cannot, it displays a diagnostic message, such as "Please insert boot floppy in drive." The system also asks if you want to access the monitor.

The following options are available:

```
1. Drive A
2. Drive B
```

After entering the drive number, you are prompted for the filename:

```
Enter Boot Filename (CR = no change):
```

The configuration files must reside on the same drive as the boot source. If the drive you specify is different from the Default File Source drive, you receive a message asking whether you want to change the Default File Source to the same drive.

Network The system boots from the network path specified in the Primary Boot Source parameter. If unsuccessful, the system boots from the source specified in the Secondary Boot Source parameter. If booting is still unsuccessful, the system asks if you want to access the monitor.

You are prompted for the physical slot where the I/O module that will be booted from is installed:

```
Slot number [1 to 8] (CR = 1):
```

Figure A-1 shows the numbering scheme of slots in the three types of chassis.

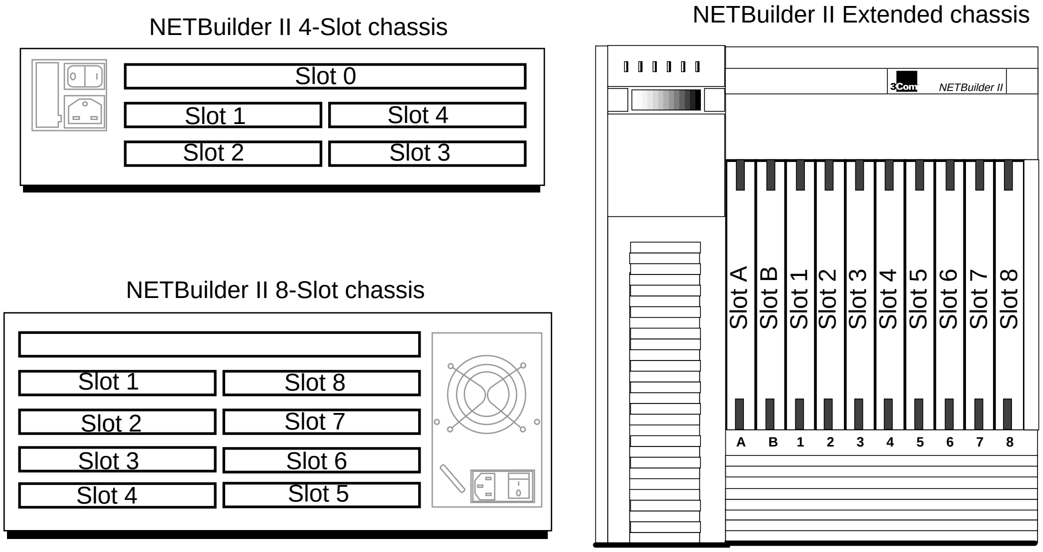


Figure A-1 Slot Numbering for NETBuilder II Chassis

If you have a multiport module, you are prompted for the port number:

XXX

A specifies the first port on the module. Subsequent interface options are numbered B, C, and so forth.

You are then prompted for the filename:

```
Enter Boot Filename:
```

3Com recommends specifying both the pathname and filename. If the pathname is not specified, the file is accessed from the root directory.

If you select network as your boot device, you need to configure the following additional parameters:

- *Default File Source on page A-13*
- *I/O Module Parameters on page A-13*
- *Boot Protocol on page A-14*
- *IP Addresses on page A-14*
- *MAC Address on page A-15*
- *ARP Format on page A-15*

You may also want to increase the default setting of the Maximum Retries parameter.

Default File Source

```
4. Primary Boot Source
5. Secondary Boot Source
   2. Default File Source
```

Specifies where the boot device accesses the configuration files during the boot sequence. The following options are available:

```
1. Boot device
2. Local
3. Network
```

Default The default is Boot device.

Maximum Retries

```
4. Primary Boot Source
5. Secondary Boot Source
   3. Maximum Retries
```

Specifies the number of times to retry the boot source specified in the Boot Device parameter if the initial try fails. Options are 0 to 254.

Default The default is 0.

I/O Module Parameters

```
4. Primary Boot Source
5. Secondary Boot Source
   4. I/O Module Parameters
```

You need to configure this parameter only if you are booting over an HSS port running PPP or a token ring port.

The options available depend on which interface you are booting over.

HSS port running PPP If you are booting over an HSS port running PPP, you are prompted to configure the following options:

```
1. HSS Baud Rate
2. HSS Clock Source
3. HSS Connector Type
4. HSS Protocol
5. HSS WAN Password
```

HSS Baud Rate This setting must correspond to your serial line setting.

HSS Clock Source Set this parameter appropriately.

Default: The default is external.

HSS Connector Type Set this parameter to the connector that the server is reachable through.

Default: The default is V.35.

HSS Protocol Select PPP.

HSS WAN Password Leave this field empty.

Token ring port If you are booting over a token ring port, you are prompted to configure the following options:

```
1. Token ring speed
2. Token ring baud rate
```

Token Ring Speed Determines the speed of the token ring line. The following options are available:

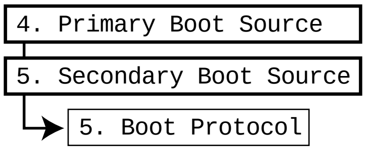
```
1. 4 Mbps
2. 16 Mbps
```

Default: The default is 4 Mbps.

Baud Rate Determines the baud rate of the token ring. Make sure the setting of this field corresponds to that of your token ring line.

Default: There is no default unless the firmware is set at 3Com, instead of upgraded; if it is set at 3Com, the default is 64 kbps.

Boot Protocol



```
4. Primary Boot Source
5. Secondary Boot Source
5. Boot Protocol
```

Specifies the boot and address discovery protocols that are used when the bridge/router boots from a network boot source.

The boot protocol option is:

```
2. TFTP
```

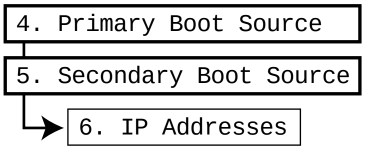
TFTP The following options are available for TFTP Address Discovery:

```
1. local configured addresses
2. BOOTP
```

Default: The default is BOOTP.

If you specify local configured addresses, the IP addresses configured in the IP Addresses parameter are used. For complete information, refer to “IP Addresses” next.

IP Addresses



```
4. Primary Boot Source
5. Secondary Boot Source
6. IP Addresses
```

Specifies IP addresses for the following:

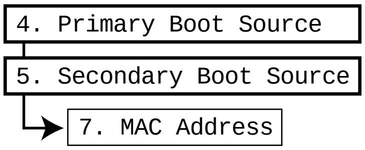
```
1. Client
2. Server
3. Gateway
4. Remote File Server
5. Subnet Mask
```

Default The default settings are 0.0.0.0.

To specify an address, enter an IP address in the dotted decimal notation (for example, 129.213.24.31), then press the Return key.

To delete an IP address, enter 0.0.0.0 or press the space bar once, then press the Return key.

MAC Address



```
4. Primary Boot Source
5. Secondary Boot Source
    7. MAC Address
```

Determines the MAC address to be used for booting over the network.

The following options are available:

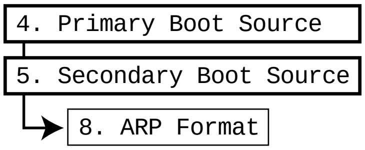
```
1. System
2. Slot
```

Default The default is System. The default setting of this parameter can be used if your boot source is a TFTP server. 3Com recommends reconfiguring this parameter to slot X (I/O module MAC address) when your boot source is over the network.

System The MAC address is assigned to the CEC module.

Slot The MAC address is assigned to an I/O module over which the system is booted. The slot number is 1 through 4 if you have a 4-Slot chassis or 1 through 8 if you have an 8-Slot chassis. Figure A-1 on page A-12 displays the numbering scheme for all chassis.

ARP Format



```
4. Primary Boot Source
5. Secondary Boot Source
    8. ARP Format
```

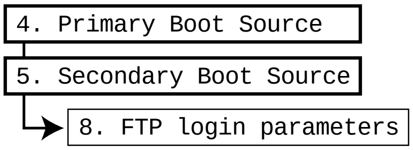
Reconfigure this parameter only if you are booting over a token ring port. This parameter determines whether canonical or noncanonical addressing is used for the Address Resolution Protocol (ARP). Token ring networks use noncanonical addressing.

The following options are available:

```
1. Canonical
2. Noncanonical
```

Default The default is canonical.

FTP login parameters



4. Primary Boot Source

5. Secondary Boot Source

8. FTP login parameters

The following options are available:

```
1. Username
2. Password
3. Account
```

Each option can be up to 20 characters long.

Test Boot Source

The Test Boot Source parameter does the following tasks:

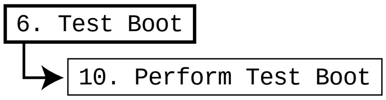
- Initiates the system reboot directly from the test boot source menu
- Clears the test boot timer when the test boot succeeds

The following options are available:

```
1. Boot Device
2. Default File Source
3. Maximum Retries
4. I/O Module Parameters
5. Boot Protocol
6. IP Addresses
7. MAC Address
8. ARP Format
9. FTP login parameter
10. Perform Test Boot
11. Clear Test Boot Timer
```

Refer to “Primary Boot Source and Secondary Boot Source” on page A-11 for information about the above options. Options 5 and 6 are specific to the Test Boot Source parameter.

Perform Test Boot



6. Test Boot

10. Perform Test Boot

If you are upgrading software from a remote device, you must perform a test boot of the new software to determine its reliability.

The following prompt is displayed:

```
Enter number of seconds until automatic reboot after test boot
  (CR = 0):
```

3Com recommends entering 300 seconds, which should allow the system enough time to initialize.

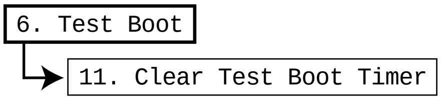
The following prompt is displayed:

```
Press Y to test boot now (any other key to cancel):
```

Type Y to initiate the test boot.

If the test boot is successful, you will access the new software. If the test boot fails, the bridge/router waits the number of seconds specified earlier, and then attempts to reboot using the primary boot source.

Clear Test Boot Timer



If your test boot fails and you do not want to wait the number of seconds you specified until automatic reboot, you can clear the timer by entering this parameter.

Boot Sources

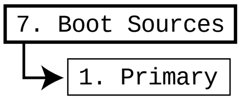
The Boot Sources parameter determines which boot source is used.

The following options are available:

```
1. Primary
2. Primary and Secondary
3. Secondary
```

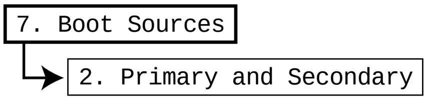
Default The default is Primary.

Primary



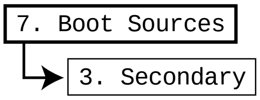
The primary option causes the system to boot from the primary boot source only.

Primary and Secondary



The primary and secondary option causes the system to boot from the primary boot source first, and if this boot source fails, then boot from the secondary boot source.

Secondary



The secondary option causes the system to boot from the secondary boot source only.

For complete information on the Secondary Boot Source parameter, refer to “Primary Boot Source and Secondary Boot Source” on page A-11.

Dump Destination

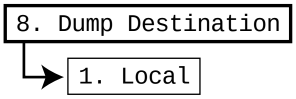
The Dump Destination parameter selects where the contents of bridge/router memory are stored in case of a crash. (The Recovery Procedure parameter allows you to decide whether to store this memory and which module contents to store.)

The following options are available:

```
1. Local
2. Network
```

If you select Local, both CEC and multiprocessor (MP) module images can be dumped. If you select Network, only the CEC module can be dumped. A local dump can be performed only to a floppy disk drive, not to a flash memory drive.

Local



8. Dump Destination

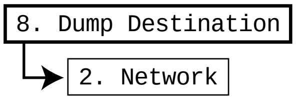
1. Local

Dumps memory to the local floppy drive.

Insert the first blank floppy diskette into the floppy disk drive. When a diskette is filled, you are prompted to insert another until the entire memory is dumped. To indicate a new diskette is in place, press Return.

Have a supply of formatted diskettes available. A dump may require up to four 4 MB diskettes for a CEC 12 or six 4 MB diskettes for a CEC 20, plus two 4 MB diskettes for each MP module. You must be present to remove filled diskettes and insert blank diskettes until the memory is fully dumped.

Network



8. Dump Destination

2. Network

Uploads memory to the source you specify. MP modules cannot be dumped to the network.

The following options are available:

1. `Dump Device`
2. `Maximum Retries` (See page A-13)
3. `IP Addresses` (See page A-14)
4. `MAC Address` (See page A-15)
5. `ARP Format` (See page A-15)

If the dump is unsuccessful, type Y to access the monitor and perform the dump manually or N to retry the dump to the network.

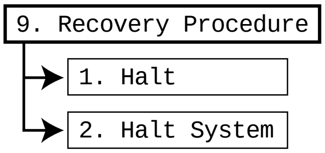
Recovery Procedure

The Recovery Procedure parameter configures the behavior and recovery in case of a crash (fatal error) of the NETBuilder II system and each MP module.

The following options are available:

```
1. Halt
2. Halt System
3. Reboot
4. Reboot System
5. Dump and Reboot
6. Selective Dump and Reboot
```

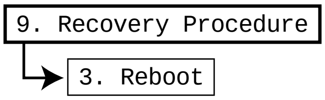
Halt and Halt System



9. Recovery Procedure
1. Halt
2. Halt System

Halt and Halt System are for internal 3Com use and should not be selected.

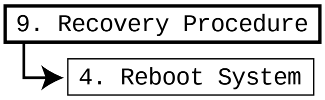
Reboot



9. Recovery Procedure
3. Reboot

Resets the selected module.

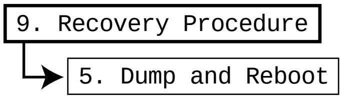
Reboot System



9. Recovery Procedure
4. Reboot System

Resets all modules.

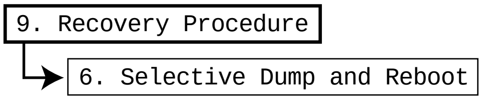
Dump and Reboot



9. Recovery Procedure
5. Dump and Reboot

Saves the memory of the CEC and all MP modules (if the dump destination is Local) or the CEC module only (if the dump destination is Network). The bridge/router then reboots. 3Com can examine this saved memory to help determine the cause of the crash.

Selective Dump and Reboot



9. Recovery Procedure
6. Selective Dump and Reboot

Dumps only selected modules.

MP Boot Source The MP Boot Source parameter specifies the software image each MP module uses as a boot source. The boot source image location is kept in a configuration file, not in EEPROM. This configuration file must be kept with the other configuration files in the primary, secondary, or test directories for standard boot or upgrade. If the boot source image location configuration file is not found, the default values are used for the MP module image names.

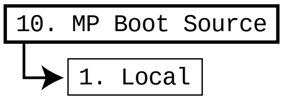
If you want to access the MP boot file from a location other than the default configuration file directory, use this parameter.

The following options are available:

```
1. Local
2. Default File Source
```

Default The default is Default File Source.

Local



The following options are displayed:

```
1. Drive A
2. Drive B
```
(Shown if present)

Default The default is Drive A.

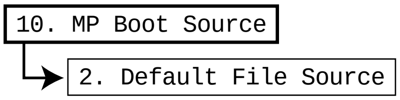
The following prompt is displayed:

```
Enter MP Boot Filename:
```

Enter the name of the MP boot filename, including the path:

```
[<drive>:][/<path>]/<filename>
```

Default File Source



The following prompt is displayed:

```
Enter MP Boot Filename:
```

Enter the name of the MP boot filename.

Default The default drive and path are the same as the configuration file location.

Boot Statistics The Boot Statistics parameter displays the following information:

- Number of boots, including the date and time of last successful boot
- Number of exceptions, including date and time of last exception (unsuccessful boot)
- Boot source used for last successful boot
- Last error during boot attempt

When you have the information you need, you can clear the boot statistics by typing Y.

SuperStack II NETBuilder and OfficeConnect NETBuilder

This section describes the System Configuration menu for the SuperStack II NETBuilder bridge/router and the OfficeConnect NETBuilder bridge/router.

Syntax

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

Minimum Privilege “Root” user with Network Manager privilege

Description 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.

You can also configure the firmware parameters by entering the MONitor command to use the monitor.

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.

`1. Upgrade Menu`	*See* page A-21
`2. Console Port`	*See* page A-21
`3. Self-Test`	*See* page A-22
`4. Primary Boot Source`	*See* page A-22
`5. Secondary Boot Source`	*See* page A-22
`6. Test Boot Source`	*See* page A-23
`7. Boot Sources`	*See* page A-24
`8. Dump Destination`	*See* page A-25
`9. Boot Statistics`	*See* page A-26

The following sections describe each menu option and suboption.

Upgrade Menu

The Upgrade Menu allows you to restore your MAC address if the EEPROM has been reinitialized for software restoration.

Console Port

The Console Port parameter sets the baud rate for the Console port.

Possible baud rate settings are:

```
1. 110 bps
2. 300 bps
3. 1200 bps
4. 2400 bps
5. 9600 bps
6. 19200 bps
7. 38400 bps
```

Databits are always set at 8 and parity at none.

Default The default baud rate is 9600 bps.

Self-Test The Self-Test parameter determines whether your system runs all self-tests or a subset when you turn the power on or reset.

The following options are available:

```
1. Quick
2. Full
```

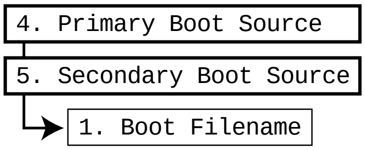
Default The default is Full.

Primary Boot Source and Secondary Boot Source The Primary Boot Source parameter allows you to set the path for your primary boot source. The Secondary Boot Source parameter allows you to set the path for the alternative boot source if the primary boot source fails. Both of these parameters work in conjunction with the Boot Sources parameter. For more information, refer to "Boot Sources" on page A-24.

The following options are available:

```
1. Boot Filename
2. Default File Source
3. IP Addresses
4. FTP login parameters
```

Boot Filename



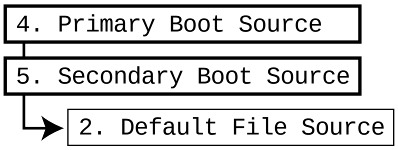
You can specify the boot filename. Enter the full path:

```
/<directory>/<filename>
```

Do not include a drive letter in the boot path.

Default The default boot file is /primary/boot.68k for Primary Boot Source and /secondar/boot.68k for Secondary Boot Source.

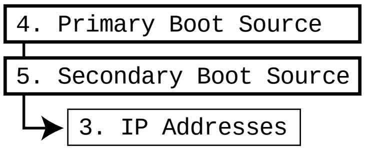
Default File Source



You can specify the configuration file directory.

Default The default directory is /primary for Primary Boot Source and /secondar for Secondary Boot Source.

IP Addresses



Specifies IP addresses for the following:

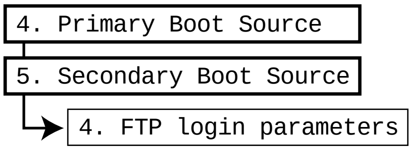
```
1. Client
2. Server
3. Gateway
4. Remote File Server (not applicable)
5. Subnet Mask
```

Default The default setting is 0.0.0.0.

To specify an address, enter an IP address in the dotted decimal notation (for example, 129.213.24.31), then press the Return key.

To delete an IP address, enter 0.0.0.0 or press the space bar once, then press the Return key.

FTP login parameters



The following options are available:

```
1. Username
2. Password
3. Account
```

Each option can be up to 20 characters long.

Test Boot Source

The Test Boot Source parameter does the following:

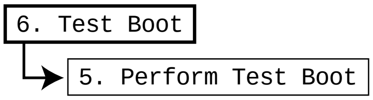
- Initiates the system reboot directly from the test boot source menu.
- Clears the test boot timer when the test boot succeeds.

The following options are available:

```
1. Boot Source
2. Default File Source
3. IP Addresses
4. FTP login parameters
5. Perform Test Boot
6. Clear Test Boot Timer
```

Refer to “Primary Boot Source and Secondary Boot Source” on page A-22 for information about options 1 through 4. Options 5 and 6 are specific to the Test Boot Source parameter.

Perform Test Boot



If you are upgrading software from a remote device, you must perform a test boot of the new software to determine its reliability.

The following prompt is displayed:

```
Enter number of seconds until automatic reboot after test boot
 (CR = 0):
```

3Com recommends entering 300 seconds, which should allow the system enough time to initialize.

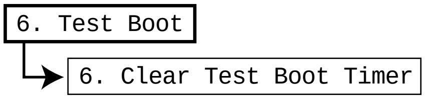
The following prompt is displayed:

```
Press Y to test boot now (any other key to cancel):
```

Type Y to initiate the test boot.

If the test boot is successful, you can access the new software. If the test boot fails, the bridge/router waits the number of seconds specified earlier, and then attempts to reboot using the primary boot source.

Clear Test Boot Timer



If your test boot fails and you do not want to wait the number of seconds you specified until automatic reboot, you can clear the timer by entering this parameter.

Boot Sources

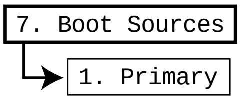
The Boot Sources parameter determines which boot source is used.

The following options are available:

```
1. Primary
2. Primary and Secondary
3. Secondary
```

Default The default is Primary.

Primary



The primary option causes the system to boot from the primary boot source only.

Primary and Secondary

```
7. Boot Sources
  → 2. Primary and Secondary
```

The primary and secondary option causes the system to boot from the primary boot source first, and if this boot source fails, then boot from the secondary boot source.

Secondary

```
7. Boot Sources
  → 3. Secondary
```

The secondary option causes the system to boot from the secondary boot source only.

For complete information on the Secondary Boot Source parameter, refer to “Primary Boot Source and Secondary Boot Source” on page A-22.

Dump Destination

The Dump Destination parameter selects where the contents of bridge/router memory are stored in case of a crash.

The following options are available:

```
1. Do not dump
2. Network
```

Do not dump

```
8. Dump Destination
  → 1. Do not dump
```

If your system crashes, the bridge/router reboots.

Network

```
8. Dump Destination
  → 2. Network
```

The system uploads memory to the source you specify.

The following options are available:

```
1. Client
2. Server
3. Gateway
4. Remote File Server (not applicable)
5. Subnet Mask
6. Dump Destination Directory
```

Set the dump destination directory on the server specified in option 2.

Default The default dump destination directory is /dump.

Boot Statistics

The Boot Statistics parameter displays the following information:

- Number of boots, including the date and time of last successful boot
- Number of exceptions, including date and time of last exception (unsuccessful boot)
- Boot source used for last successful boot
- Last error during boot attempt

When you have the information you need, you can clear the boot statistics by typing Y.

B

FIRMWARE COMMANDS

This appendix describes the firmware Boot Monitor commands available on the NETBuilder II DPE module.

The boot monitor is a utility accessible only during startup. It provides several commands including commands for overriding the boot process, displaying filenames, and setting dump parameters.

Entering the Boot Monitor

To enter the boot monitor during startup, watch your console for a message similar to the following:

```
3Com Corporation NETBuilder II
32 MB instruction/data memory, 8 MB shared memory
Do you want to enter the boot monitor? (y/n):
```

Enter Y within five seconds to enter the boot monitor. If you enter N or enter nothing, the NETBuilder II system begins booting the software.

Commands

The following commands are available from the boot monitor.

Boot

Syntax

```
BT [<drive>:]/<path>/<filename>
```

Description

The BT command allows you to reboot or to override the default boot path configured in the firmware by the boot monitor or by the SysconF command in the software. This command is useful if the boot path has a typing error or if you have a malfunctioning flash memory drive. If you enter a new boot path, the firmware parameter is updated to reflect the new path.

If you do not enter the drive, drive A is used. If you do not enter a filename, you will see a set of prompts similar to the following:

```
>BT
File name? (CR=a:/93/boot.29k):
Configuration path? (CR=a:/93):
Loading brouter software...decompressing...done
>
```

After you have responded to the second prompt, the system attempts to boot from the specified image file. If there is an error, a message is sent to the console and you are returned to the boot monitor.

Errors include:

- The file does not exist.
- The file has the wrong format.
- The file has a bad checksum.
- The path points at the slot configured for a full dump.

Boot Utility

Syntax

```
BU [<drive>:]/<path>/<filename>
```

Description

The BU command allows you to boot a utility file. The command will not boot the boot image or other bundled images.

If you do not enter the drive, drive A is used. If you do not enter a filename, you will see a prompt similar to the following:

```
>BU
Filename of utility to boot? (CR=none):
>
```

After you have responded to the second prompt, the system attempts to boot from the specified utility file. If there is an error, a message is sent to the console and you are returned to the boot monitor.

Display Files

Syntax

```
DF [<drive>:]/<path>/
```

Description

The DF command displays information about files on a file system or in a specified directory. It also displays the available free space in the file system.

If you do not specify a drive, drive A is used. If you do not enter a path, you will see a set of prompts similar to the following:

```
>DF
Path?:
PC card slot A
Directory of PC card slot A:
BRIDGE            61         06-28-1995   18:57
BOOT.29k          1480418    06-27-1995   10:51
SYS               15         06-27-1995   10:51
CCSMACRO          6053       06-28-1995   21:33
MANIFEST          118        06-27-1995   10:51
BROUTES           26         06-28-1995   21:11
PPM               1079       06-29-1995   0:30
V3T2              131072     06-28-1995   18:31

                  8 file(s)  1618842 bytes
                             1307648 writable bytes free

>
```

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

Help

Syntax

```
H
```

or

```
?
```

Description

The Help command lists all available commands in the boot monitor along with syntax parameters.

Recovery Action

Syntax RA

Description The RA command allows you to configure the recovery action and memory dump parameters if your system crashes.

After entering RA, you will see a set of prompts similar to the following:

```
>RA
Recovery action? (r=reboot, d=dump and reboot, h=halt, CR=r):
Full dump type? (n=none, s=single card, m=multi-card, CR=n):
Full dump PC card slot? (a=a:, b=b:, CR=b:)
>
```

After completing the dialogue, if the recovery action is to dump and reboot, the system checks that the dump type is not none and the dump slot is not the same as the boot or configuration path. If there is a conflict, an error message is shown and the parameters are not changed. Refer to "Recovery Procedure" on page A-6 for more complete recovery procedure parameters.

Prompt Options

Recovery Action

If the system crashes, you can configure one of the following actions:

r=reboot	The system automatically reboots.
d=dump and reboot	The system downloads the contents of its memory at the time of the crash and then reboots. The memory dump can then be analyzed by 3Com technical support.
h=halt	The system halts operation and enters the debug monitor. From the debug monitor, you can display memory, initiate a dump, and reboot. Refer to "Debug Monitor (DPE Only)" on page 1-34 for more information about the MONitor command.

Full Dump Type

If you have specified a dump and reboot, you can configure the following dump types:

n=none	No dump occurs.
s=single card	The memory dump is written to a single flash memory card. If the dump is larger than a single card, it is truncated when the card is full. However, the dump can run unattended, and the card may be large enough for the full dump.
m=multi-card	If the dump is larger than one card, you are prompted on the console to insert another card to continue the dump.

The target flash memory card must be in the flash memory drive at the time of the dump, or the dump will be aborted.

Full Dump PC Card Slot

Specify the flash memory drive where the dump is written:

a=a:	The dump is written to drive A.
b=b:	The dump is written to drive B.

The target flash memory card must be in the flash memory drive at the time of the dump, or the dump is aborted. You cannot specify a drive that is the same as the boot or configuration path.

Reboot

Syntax RB

Description The RB command reboots the NETBuilder II system.

Show Version

Syntax SV

Description The SV command shows the firmware versions running on your DPE module.

```
> sv
NETBuilder II boot1 version:FW/DPE-BOOT1,1.0.0.09I
NETBuilder II boot2 version:FW/DPE/BOOT2,1.0.0.34I
NETBuilder II PID version:PID_UTIL,1.0.0.07I
```

INDEX

3Com Corporation LIMITED WARRANTY

HARDWARE

3Com warrants its hardware products to be free from defects in workmanship and materials, under normal use and service, for the following lengths of time from the date of purchase from 3Com or its Authorized Reseller:

Network adapters	Lifetime
Other hardware products (unless specified above)	1 year
Spare parts and spares kits	90 days

If a product does not operate as warranted above during the applicable warranty period, 3Com shall, at its option and expense, repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of 3Com. Replacement products may be new or reconditioned. Any replaced or repaired product or part has a ninety (90) day warranty or the remainder of the initial warranty period, whichever is longer.

3Com shall not be responsible for any software, firmware, information, or memory data of Customer contained in, stored on, or integrated with any products returned to 3Com for repair, whether under warranty or not.

SOFTWARE

3Com warrants that the software programs licensed from it will perform in substantial conformance to the program specifications therefor for a period of ninety (90) days from the date of purchase from 3Com or its Authorized Reseller. 3Com warrants the media containing software against failure during the warranty period. No updates are provided. 3Com's sole obligation with respect to this express warranty shall be (at 3Com's discretion) to refund the purchase price paid by Customer for any defective software products, or to replace any defective media with software which substantially conforms to 3Com's applicable published specifications. Customer assumes responsibility for the selection of the appropriate applications program and associated reference materials. 3Com makes no warranty or representation that its software products will work in combination with any hardware or applications software products provided by third-parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the software products will be corrected. For any third-party products listed in the 3Com software product documentation or specifications as being compatible, 3Com will make reasonable efforts to provide compatibility, except where the noncompatibility is caused by a "bug" or defect in the third-party's product.

STANDARD WARRANTY SERVICE

Standard warranty service for *hardware* products may be obtained by delivering the defective product, accompanied by a copy of the dated proof of purchase, to 3Com's Corporate Service Center or to an Authorized 3Com Service Center during the applicable warranty period. Standard warranty service for *software* products may be obtained by telephoning 3Com's Corporate Service Center or an Authorized 3Com Service Center, within the warranty period. Products returned to 3Com's Corporate Service Center must be pre-authorized by 3Com with a Return Material Authorization (RMA) number marked on the outside of the package, and sent prepaid, insured, and packaged appropriately for safe shipment. The repaired or replaced item will be shipped to Customer, at 3Com's expense, not later than thirty (30) days after receipt of the defective product by 3Com.

WARRANTIES EXCLUSIVE

IF A 3COM PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY FOR BREACH OF THAT WARRANTY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND SATISFACTORY QUALITY. 3COM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, OR USE OF ITS PRODUCTS.

3COM SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY

TO THE FULL EXTENT ALLOWED BY LAW, 3COM ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF 3COM OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers or the limitation for personal injury, so the above limitations and exclusions may be limited in their application to you. This warranty gives you specific legal rights which may vary depending on local law.

GOVERNING LAW

This Limited Warranty shall be governed by the laws of the state of California.

3Com Corporation, 5400 Bayfront Plaza, Santa Clara, CA 95052-8145 (408) 764-5000

9/1/96