8371 Networking Multilayer Ethernet Switch

Enhancements to Release 1.0 of the IBM 8371

8371 Networking Multilayer Ethernet Switch

Enhancements to Release 1.0 of the IBM 8371

Contents

© Copyright IBM Corp. 1996, 1999

Figures

© Copyright IBM Corp. 1996, 1999

Tables

© Copyright IBM Corp. 1996, 1999

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering the subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or program(s) described in this publication at any time without notice.

© Copyright IBM Corp. 1996, 1999

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, or other countries, or both:

Advanced Peer-to-Peer Networking
APPN
eNetwork
IBM
OS/2

VTAM

Microsoft, Windows, Windows NT, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

NetView is a trademark of Tivoli Systems, Inc. in the United States or other countries or both.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

© Copyright IBM Corp. 1996, 1999

Chapter 1.

This document describes three enhancements that have been made to Release 1.0 of the IBM 8371 Multilayer Ethernet Switch.

- Multiple Bridge Instances, see “Chapter 2. Multiple Bridge Instances” on page 3.
- LEC Persistence, see “Chapter 5. LEC Persistence” on page 53.
- Port Security, on page 22.

© Copyright IBM Corp. 1996, 1999

Chapter 2. Multiple Bridge Instances

Support for multiple bridge instances allows the IBM 8371 to be partitioned into multiple, independent layer-2 switches. Up to 24 bridge instances may be configured. Each bridge instance maintains its own layer-2 database and has an independent instance of the spanning tree protocol.

Figure 1 depicts an example network design that uses the multiple bridge instance capability. In this example, each IBM 8371 is partitioned into two bridge domains. Each bridge domain is made up of a set of Ethernet ports and an Ethernet LEC. The LECs are members of ELANs that connect the 8371 switches.

Since each bridge has an independent instance of the spanning tree protocol, the parallel ELANs do not create a layer-2 loop. Therefore, all of the LECs can be forwarding traffic simultaneously, which is advantageous to ATM throughput.

The ports assigned to Bridge 1 effectively form a port-based VLAN and the 8371's other VLAN functions may be used to further refine the scope of broadcast/multicast traffic within the port-based domain.

While ports on different bridge instances are isolated at layer-2, stations of these ports may still communicate at layer 3. Release 1.0 of the IBM 8371 supports layer-3 switching using the MPOA client and Self-learning IP. Both of these layer-3 functions can switch traffic directly between ports that are members of different bridge instances. The 8371's local shortcut capability in the MPOA client enables layer-3 traffic to be switched directly between two Ethernet ports without traversing the ATM backbone.

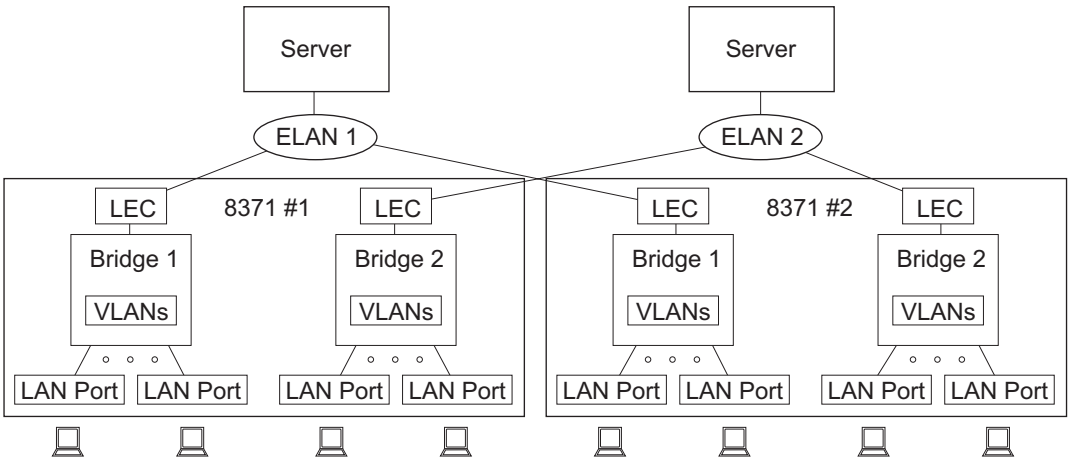

Figure 1. Example Network Design with Multiple Bridge Instances

The multiple bridge instance support also assists MPOA load balancing. Figure 2 on page 5 illustrates one way that multiple bridge instances can be used in conjunction with MPOA. In this example, traffic for ports assigned to Bridge 1 is shortcutted over ATM interface 1, while traffic to and from ports assigned to Bridge 2 is shortcutted over ATM interface 2. The stations assigned to Bridge 1 may be on the same subnet as the stations assigned to Bridge 2, or on different subnets.

© Copyright IBM Corp. 1996, 1999

Multiple Bridge Instances

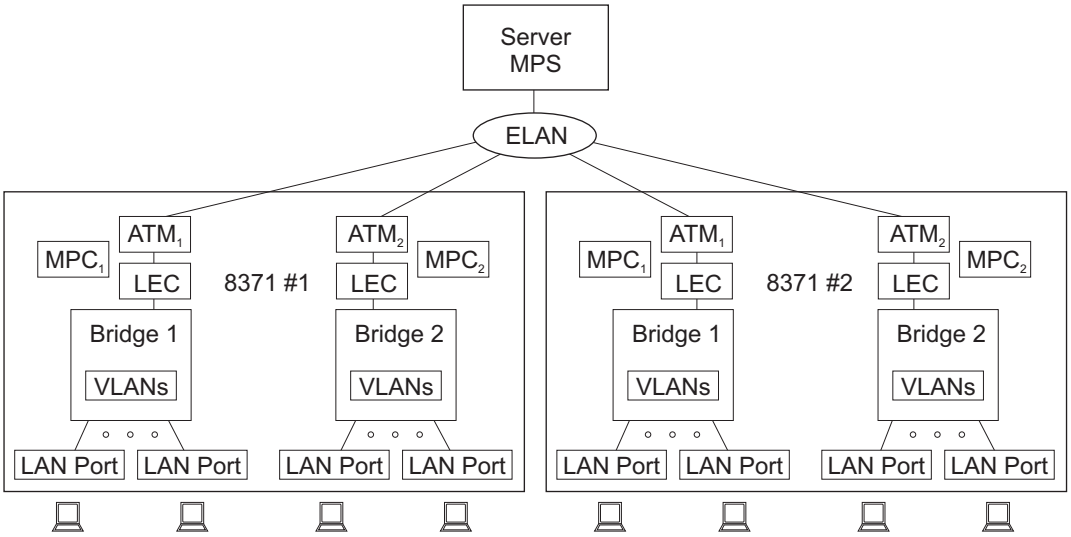

Figure 2. MPOA Load Balancing

Chapter 3. Configuring and Monitoring Bridging

This chapter is presented here in its entirety with a | used in the left margin to mark changes for the 8371 Release 1.0 enhancements. You can use this document to replace the "Configuring and Monitoring Bridging" chapter of *IBM 8371 Networking Multilayer Ethernet Switch Software User's Guide and Configuration Reference*, GC30-9688-00.

This chapter describes how to configure the adaptive source routing transparent (ASRT) bridge protocol and how to use the ASRT configuration commands. The chapter includes the following sections:

Accessing the ASRT Configuration Environment

To access the ASRT configuration environment, enter the **protocol asrt** command at the `Config>` prompt:

```
Config>protocol asrt
Transparent Bridge user configuration
ASRT config>
```

ASRT Configuration Commands

The ASRT configuration commands allow you to create multiple bridge instances. You must adhere to the following criteria in order to configure multiple bridge instances:

© Copyright IBM Corp. 1996, 1999

ASRT Configuration Commands

- Any existing 8371 Release 1.0 configuration MUST be deleted after installing the enhancements to Release 1.0. The 8371 must then be restarted before reconfiguring. Failure to delete the existing Release 1.0 configuration before reconfiguring the 8371 with the Release 1.0 enhancements may cause unpredictable results.
- The device must be restarted for the new configuration to take effect.

Enter the ASRT configuration commands at the `ASRT config>` prompt. Access the commands as follows:

Table 1 shows the ASRT configuration commands.

Table 1. ASRT Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available).
Add *n*	Adds one or more bridge instances. The parameter *n* specifies the number of bridge instances to be added. Up to 24 bridge instances may be configured.
Bridge *i*	Accesses the detailed configuration menus for a particular bridge instance. The parameter *i* specifies the bridge instance to be configured. See Table 2 for a list of commands available for detailed configuration.
Delete *i*	Deletes a specific bridge instance. The parameter *i* specifies the bridge instance to be deleted.
List	Displays configuration information for all configured bridges or for a specific bridge instance.
Netbios	Accesses the detailed configuration menus for NetBIOS filtering parameters that are applicable to all bridge instances in the switch. See “NetBIOS Configuration Commands” on page 25 for a discussion of commands available at the NetBIOS command prompt.
Exit	Returns you to the previous command level.

Detailed Configuration Commands for a Particular Bridge

The detailed bridge configuration commands allow you to specify network parameters for a specific ASRT bridge and its network interfaces.

Note: The device must be restarted for the new configuration to take effect.

Enter the detailed bridge configuration commands at the `ASRT config>` prompt.

Table 2 shows the detailed bridge configuration commands.

Table 2. Detailed Configuration Command for a Particular Bridge Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available).
Add	Adds a LAN/WAN port.
Delete	Deletes a LAN/WAN port.
Disable	Disables the following functions: • Bridging • Transparent (spanning tree) bridging function on a given port

Table 2. Detailed Configuration Command for a Particular Bridge Summary (continued)

Command	Function
Enable	Enables the following functions: • Bridging • Transparent (spanning tree) bridging function on a given port
List	Displays information about the complete bridge configuration or about selected configuration parameters.
Netbios	Displays the NetBIOS configuration prompt. See “NetBIOS” on page 12.
Set	Sets the following parameters: • Aging time for dynamic address entries • Bridge address • Maximum frame size • Spanning tree protocol bridge and port parameters • Filtering database size • IPX Conversion Mode • Ethernet Preference
vlans	Allows the user to configure dynamic protocol filtering.
Exit	Returns you to the previous command level.

Add

Use the **add** command to add the following information to your bridging configuration:
- Specific address mapping for a given protocol
- LAN/WAN ports

Syntax:

add port . . .

port *interface# port#*

Adds a LAN/WAN port to the bridging configuration. This command associates a port number with the interface number and enables that port’s participation in transparent bridging.

Port Number Valid Values: 1 to 254

Port Number Default Value: none

Example: add a port

```
ASRT config> add port
Interface Number [0]?
Port Number [5]?
```

Delete

Use the **delete** command to delete the following information from your bridging configuration:
- Specific address mapping for a given protocol
- LAN/WAN ports

Syntax:

delete port . . .

port *port#*

Removes a port from a bridging configuration. Because the **enable bridge** command by default configures all LAN devices to participate in bridging,

this command allows you to customize which devices should or should not participate in the bridging. The port number value normally is one greater than the interface number.

Example: `delete port 2`

Disable

Use the **disable** command to disable the following bridge functions:
- Bridging
- Transparent (spanning tree) bridging function on a given port

Syntax:

disable bridge | stp | transparent . . . | tree

bridge
Disables bridging function entirely. This command does not remove previously configured bridging values, however.

Example: `disable bridge`

stp Disables the Spanning Tree Protocol on the bridge. The default is enabled.

Example: `disable stp`

transparent *port#*
Disables transparent bridging function on the given port.

Example: `disable transparent 2`

tree *port#*
Disables STP participation for the bridge on a per-port basis.

Example: `disable tree 1`

Note: Disabling STP on a per-port basis can produce network loops because of the existence of parallel bridges.

Enable

Use the **enable** command to enable the following bridging functions:
- Bridging
- Transparent (Spanning Tree) bridging function on a given port

Syntax:

enable bridge . . . | stp | transparent . . . | tree

bridge
Enables transparent bridging function on all the LAN devices (interfaces) configured in the bridging device. The port numbers are assigned to each

interface as the previous interface number plus 1. For example, if interface 0 is a LAN device its port number will be 1.

Example: `enable bridge`

stp Enables the spanning tree protocol on the bridge. This is the default.

Example: `enable stp`

transparent *port#*
Enables transparent bridging function on the given port. Under normal circumstances, this command is not necessary.

Example: `enable transparent`

```
Port Number [1]?
```

tree *port#*
Enables STP participation for the bridge on a per-port basis.

Example: `enable tree 1`

List

Use the **list** command to display information about the complete bridge configuration or to display information about selected configuration parameters.

Syntax:

list bridge
filtering . . .
port . . .
prot-filter . . .
protocol
range . . .

bridge
Lists all general information regarding the bridge.

filtering *datagroup-option*
The following general data groups can be displayed under the **list filtering** command:

All Displays all filtering database entries.

Ethertype
Displays Ethernet protocol type filter database entries.

SAP Displays SAP protocol filter database entries.

SNAP Displays SNAP protocol identifier filter database entries.

The following examples illustrate each of the **list filtering** display options.

Example 1: `list filtering all`

```
Ethernet type 0800 is routed on ports 1
IEEE 802.2 destination SAP 42 is routed on ports 1
IEEE 802 SNAP PID 00-00-00-08-00 is routed on ports 2-3
```

Descriptors used in explaining how packets are communicated include:

Routed
Describes packets passed to routing forwarder to be forwarded.

Filtered
Describes packets that are administratively filtered setting protocol filters that you set.

Bridged and routed
This describes a protocol identifier for which there is a protocol entity within the system that is not a forwarder. For example a link level echo protocol. Unicast packets from this protocol are bridged or locally processed if being sent to a registered address. Multicast packets are forwarded and locally processed for a registered multicast address.

All of these descriptors also apply to ARP packets with this Ethertype.

Example 2:

```
list filtering ethertype

Ethernet type (in hexadecimal), 0 for all [0]? 0800
Ethernet type 0800 is routed on ports 1
```

Example 3:

```
list filtering sap

SAP (in hexadecimal), 100 for all [100]? 42
IEEE 802.2 destination SAP 42 is routed on ports 1
```

Example 4:

```
list filtering snap

SNAP Protocol ID, return for all [00-00-00-00-00]?
IEEE 802 SNAP PID 00-00-00-08-00 is routed on ports 2-3
```

port *port#*
Displays port information related to ports that are already configured. Port# selects the port you want to list. Specifying no number selects all ports.

Example: `list port`

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Port ID (dec)    : 128: 2, (hex): 80-02
Port State       : Enabled
STP Participation: Enabled
Port Supports    : Transparent Bridging Only
Assoc Interface  : 0  VPI  0  VCI:    78
Path Cost        : 0
```

Port ID
The ID consists of two parts: the port priority and the port number. In the example, 128 is the priority, and 1, 2, and 3 are the port numbers. In hexadecimal format, the low-order byte denotes the port number and the high-order byte denotes the priority.

Port state
Displays current state of the specified port or ports. This can be either ENABLED or DISABLED.

Port supports
Displays bridging method supported by that port (for example, transparent bridging).

Assoc interface
Displays interface number associated with the displayed port. Also displays the VPI/VCI or the destination ATM address if the port exists on an ATM interface.

Path Cost
Cost associated with the port which is used for possible root path cost. The range is 1 to 65535.

prot-filter *port#*

Reads a current list of the filter protocol types. Filters can be listed selectively by port or all ports can be displayed at once. Port# selects the bridge port that you want to list.

Example: **`list prot-filter 1`**

```
PORT 1
Protocol Class   :  DSAP
Protocol Type    :  01
Protocol State:  :  Filtered
Port Map         :  1, 2, 3
```

Port Number

Port number is displayed for each port if all ports are selected to be displayed.

Protocol Class

Displays protocol class (SNAP, Ether, or DSAP).

Protocol Type

Displays protocol ID in hexadecimal format.

Protocol State

Denotes that protocol is being filtered for selected port.

Port Map

Displays the numbers of the ports where this type of protocol filter is present.

protocol

Displays bridge information related to the spanning tree protocol.

Note: Each of these bridge-related parameters is also described in detail in the previous chapter.

Bridge Identifier

8-byte value in ASCII format. If you did not set the bridge address prior to displaying this information, the low order 6 bytes will be displayed as zero, denoting that the default MAC address of a port is being used. When a bridge has been selected as the root bridge, the bridge max age and bridge hello time are transmitted by it to all the bridges in the network via the HELLO BPDUs.

Bridge-Max-Age

Maximum age (period of time) that should be used to time out spanning tree protocol-related information.

Bridge-Hello-Timer

Time interval between HELLO BPDUs.

Bridge-Forward-Delay

Time interval used before changing to another state (should this bridge become the root).

range *start-index stop-index*

Reads a range of address entries from the permanent database. To specify this, first determine the size of the database by using the **list permanent** command. From this value you can then determine a “start index” value for your entry range. The start index is in the range from 1 to the size of the database. You can then choose a “stop index” for displaying a limited number of entries. This input is optional. If you do not specify the stop index, the default value is the size of the database.

Bridge Detailed Configuration Commands

Address entries contain the following information:

Example: `list range`

```
Start-Index [1]? 1
Stop-index [17]? 6
ADDRESS                 ENTRY TYPE      PORT MAP

=======                 ==========      ========
01-80-C2-00-00-00       REGISTERED      Input Port:  ALL PORTS
                                        Output ports:

01-80-C2-00-00-01       RESERVED        NONE/DAF
01-80-C2-00-00-02       RESERVED        NONE/DAF
01-80-C2-00-00-03       RESERVED        NONE/DAF
01-80-C2-00-00-04       RESERVED        NONE/DAF
01-80-C2-00-00-05       RESERVED        NONE/DAF
```

Address
6-byte MAC address of the entry.

Type of Entry
Specifies one of the following types:

- Reserved - entries reserved by the IEEE 802.1d committee
- Registered - entries consist of unicast addresses belonging to proprietary communications hardware attached to the box or multicast addresses enabled by protocol forwarders
- Dynamic - entries “learned” by the bridge “dynamically” that do not survive power on/offs or system resets and that have an “age” associated with the entry
- Free - locations in database that are free to be filled by address entries

Port Map
Displays outgoing port map for all incoming ports.

NetBIOS

Enter **netbios** at the `Bridge x config>` prompt to display the NetBIOS filtering configuration prompt. For example:

```
Bridge 2 Config> netbios
NetBIOS Filtering Configuration
NetBIOS Bridge 2 Filter config>
```

NetBIOS Filtering Configuration Commands

Note: The NetBIOS filtering configuration commands are not effective immediately. You must restart or reload the device before they become effective.

Table 3. NetBIOS Filtering Configuration Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available).
Create	Creates byte filter and host-name filter lists for NetBIOS filtering.
Delete	Deletes byte filter and host-name filter lists for NetBIOS filtering.
Disable	Disables NetBIOS filtering on the bridging router.
Enable	Enables NetBIOS filtering on the bridging router.
Filter-on	Assigns a created filter to a specific port. This filter can then be applied to all NetBIOS packets input ***or*** output on the specified port.
List	Displays all information concerning created filters.
Update	Adds information to or deletes information from a host-name or byte filter list.
Exit	Returns you to the previous command level.

Response to NetBIOS Configuration Commands: The NetBIOS configuration (Talk 6) commands are not effective immediately. They remain pending until you issue the **reload** command.

Create: Use the **create** command to create a byte filter-list or host-name filter list.

Syntax:

create byte-filter-list *filter-list*
name-filter-list *filter-list*

byte-filter-list *filter-list*

Creates a byte filter-list name for NetBIOS filtering. You can use up to 16 characters to identify the list being built. *Filter-list* must be a unique name that has not been used previously with the **create byte-filter-list** or **create name-filter-list** command.

Example: `create byte-filter-list newyork`

name-filter-list *filter-list*

Creates a host-name filter-list name for NetBIOS filtering. You can use up to 16 characters to identify the name filter-list being built. *Filter-list* must be a unique name that has not been used previously with the **create byte-filter-list** or **create name-filter-list** command.

Example: `create name-filter-list atlanta`

Delete: Use the **delete** command to delete byte filter lists, host-name filter lists, and filters created using the **filter-on input** or **filter-on output** command. The command removes all information associated with byte and host-name filter lists. It also frees the user-defined string as a name for a new filter list.

Syntax:

delete byte-filter-list *filter-list*
name-filter-list *filter-list*
filter input *port#*
filter output *port#*

byte-filter-list *filter-list*

Deletes a byte filter-list created for NetBIOS filtering. *Filter-list* is the user-defined string being used to identify the byte filter-list being deleted.

Example: `delete byte-filter-list newyork`

name-filter-list *filter-list*

Deletes a host-name filter-list created for NetBIOS filtering. *Filter-list* is the user-defined string that is used to identify the name-filter-list being deleted.

Example: `delete name-filter-list atlanta`

filter input *port#*

Deletes a filter that was created using the **filter-on input** command. The command removes all information associated with the filter and fills any resulting gap in filter numbers.

Example: `delete filter input 2`

filter output *port#*

Deletes a filter that was created using the **filter-on output** command. The command removes all information associated with the filter and fills any resulting gap in filter numbers.

Example: `delete filter output 2`

NetBIOS Filtering Configuration Commands

Disable: Use the **disable** command to globally disable NetBIOS name and byte filtering on the router.

Syntax:

disable netbios-filtering

Example: `disable netbios-filtering`

Enable: Use the **enable** command to globally enable NetBIOS name and byte filtering on the router.

Syntax:

enable netbios-filtering

Example: `enable netbios-filtering`

Filter-on: This command assigns one or more previously configured filter lists to the input or output of a specific port.

Syntax:

filter-on input *port# filter-list <operator filter-list . . . >*
output *port# filter-list <operator filter-list . . . >*

input *port# filter-list <operator filter-list . . . >*

This command assigns one or more filter lists to incoming packets on a specific port. The resulting filter is then applied to all NetBIOS packets input on the specified port.

Port# is a configured bridge port number on the router. The port number identifies this filter. Enter **list** to see a list of port numbers. Filter-list is a string previously entered using the **create** command. To add additional filter lists to this port, enter AND or OR in all capital letters followed by the filter list name.

Note: Multiple operators can be used to create a complex filter. If you enter multiple operators, they must all be entered at the same time on the same command line.

The filter created by this command is applied to all incoming NetBIOS packets on the specified port. Each filter list on the command line is evaluated left to right along with any operators that are present. An Inclusive evaluation of a filter list is equivalent to a True condition and an Exclusive evaluation is equivalent to a False condition. If the result of the evaluation of the filter-lists is True, the packet is bridged. Otherwise, the packet is filtered (dropped).

If the packet is not one of the types supported by NetBIOS filtering then all host-name filter lists for this filter are designated “Inclusive” (True). If an input filter already exists for specified port number, an error message is displayed.

Example: `filter-on input 2 newyork AND boston`

output *port# filter-list <operator filter-list . . . >*

This command assigns one or more filters to outgoing packets on a port. This filter is then applied to all NetBIOS packets output on that port.

Port# is a configured bridge port number on the router. The port number identifies this filter. Enter **list** to see a list of port numbers. Filter-list is a string previously entered using the create command. Enter an optional operator as either AND or OR in all capital letters. If an operator is present, it must be followed by a filter-list name. The port number is used to identify this filter.

Note: Multiple operators can be used. This creates a complex filter. If one or more operators are present, they must all be entered at the same time on the same command line.

The filter created by this command is applied to all NetBIOS packets output on the specified port number. Each filter list on the command line is evaluated left to right along with any operators that are present. An Inclusive evaluation of a filter list is equivalent to a True condition and an Exclusive evaluation is equivalent to a False condition. If the result of the evaluation of the filter-lists is True, the packet is bridged. Otherwise, the packet is filtered (dropped).

If the packet is not one of the types supported by NetBIOS filtering then all host-name filter lists for this filter are designated “Inclusive” (True). If an output filter already exists for specified port number, an error message is displayed.

Example: `filter-on output 2 newyork OR boston`

List: Use the **list** NetBIOS Filtering command to display all information concerning created filters.

Syntax:

list

Example: `list`

```
NetBIOS Filtering: Disabled

NetBIOS Filter Lists
--------------------

Handle           Type

nlist            Name
newyork          Byte

NetBIOS Filters
---------------

Port #      Direction      Filter List Handle(s)

3           Output         nlist
```

NetBIOS Filtering:
Displays whether NetBIOS filtering is enabled or disabled.

NetBIOS Filter Lists
Displays the user-defined name (handle) of the configured filter lists. For type, “Name” indicates a host-name filter list and “Byte” indicates a byte filter list.

NetBIOS Filtering Configuration Commands

NetBIOS Filters

Displays the assigned port number and direction (input or output) of each filter. Filter List Handles displays the names of the filter lists making up the filter.

Update: Use the **update** command to add or delete information from host-name or byte filter lists. The filter-list is a string previously entered using the create byte (or name) filter-list prompt. This command brings you to the `NetBIOS Byte (or Name) filter-list Config>` prompt, which lets you perform update tasks to the specified filter list. At this prompt you can add, delete, list, or move filter-items from byte and host-name filter lists. At this prompt you can also set the default value of each filter list to Inclusive or Exclusive.

Using the add subcommand creates a filter item within the filter list. The first filter item created is assigned number 1, the next one is assigned number 2, and so on. After you enter a successful add subcommand, the router displays the number of the filter item just added.

Note: Adding more filter items to filter lists adds to processing time (due to the time it takes to evaluate each filter item in the list) and can affect performance in heavy NetBIOS traffic.

The order in which filter items are specified for a given filter list is important as this determines the way in which the filter items are applied to a packet. The first match that occurs stops the application of filter items, and the filter list is evaluated as either Inclusive or Exclusive (depending on the Inclusive or Exclusive designation of the matched filter item). If none of the filter items of a filter list produces a match, then the default condition (Inclusive or Exclusive) of the filter list is returned.

The delete subcommand specifies the number of a filter item to be deleted from the filter list. When a delete subcommand is given, any hole created in the list is filled in. For example, if filter items 1, 2, 3, and 4 exist and filter item 3 is deleted, then filter item 4 will be renumbered to 3.

The default subcommand lets you change the default setting of the filter list to either Inclusive or Exclusive. If a filter list evaluates as Inclusive, then the packet is bridged. Otherwise, the packet is filtered.

The move subcommand is available to renumber filter items within a filter list. The first argument to the move subcommand is the number of the filter list to be moved. The second argument to the move subcommand is the number of the filter list after which the first filter list should be moved.

Syntax:

update byte-filter-list . . .
name-filter-list . . .

byte-filter-list *filter-list*

Updates information belonging to a byte filter-list. The filter-list parameter is a string previously entered via the **create byte-filter-list** command. This command brings you to the next `NetBIOS BYTE filter-list Config>` command level (see example). At this level you can perform update tasks to the spe

Example: **`update byte-filter-list newyork`**

```
NetBIOS Byte newyork Config>
```

At this prompt level you can execute several commands. Each available command is listed under "**Update Byte-Filter** Command Options".

name-filter-list *filter-list*

Updates information belonging to a name-filter list. This command is identical to the byte-filter-list command, except that it specifies a name-filter list rather than a byte-filter list. The filter-list parameter is a string previously entered using the create name-filter-list prompt. This command brings you to the next `NetBIOS Name filter-list Config>` command level (see example). At this level you can perform update tasks to the specified filter-list.

Example: `update name-filter-list accounting`

```
NetBIOS Name accounting Config>
```

At this prompt level you can execute several commands. Each available command is listed under "**Update Name-Filter** (Command Options)".

Update Byte-Filter-List (Command Options): This section lists the command options available for the **update byte-filter-list** command:

add inclusive *byte-offset hex-pattern <hex mask>*

Adds a filter item to the byte filter list. If the byte filter item that is added produces a match with a NetBIOS packet, the filter list it belongs to will evaluate to Inclusive (True).

- Byte-offset specifies the number of bytes (in decimal) to offset into the packet being filtered. This starts at the NetBIOS header of the packet.
- Hex-pattern is a hexadecimal number used to compare with the bytes starting at the byte-offset of the NetBIOS header. Syntax rules for hex-pattern include no 0x in front, a maximum of 32 numbers, and an even number of hex digits.
- Hex-mask, if present, must be the same length as hex-pattern and is logically ANDed with the bytes in the packet starting at byte-offset before the result is compared for equality with hex-pattern. If the hex-mask argument is omitted, it is considered to be all binary 1s.

If the offset and pattern of a byte filter item represent bytes that do not exist in a NetBIOS packet (that is, if the packet is shorter than was intended when setting up a byte-filter list), then the filter item will not be applied to the packet and the packet will not be filtered. If a series of byte filter items is used to set up a single NetBIOS filter list, then a packet will not be tested for filtering if any of the byte filter items within the NetBIOS filter list represent bytes that do not exist in the NetBIOS packet.

Example: `add inclusive`

```
Byte Offset  [0] ?
Hex Pattern  [] ?
Hex Mask (<CR> for no mask)  [] ?
```

add exclusive *byte-offset hex-pattern <hex mask>*

Adds a filter item to the byte filter list. This command is identical to the add inclusive command, except that if the result of the comparison between the filter item and a NetBIOS packet results in a match, then the filter list evaluates to Exclusive (False). Datagram Broadcast Packets can be specified to be discarded by using this command with a byte offset of 4 and a byte pattern of 09.

- Byte-offset specifies the number of bytes (in decimal) to offset into the packet being filtered. This starts at the NetBIOS header of the packet.
- Hex-pattern is a hexadecimal number that is compared with the bytes starting at the byte-offset offset of the NetBIOS header. Syntax rules for hex-pattern include no 0x in front, a maximum of 32 numbers, and an even number of hex digits.
- Hex-mask, if present, must be the same length as hex-pattern and is logically ANDed with the bytes in the packet starting at byte-offset before the result is compared for equality with hex-pattern. If the hex-mask argument is omitted, it is considered to be all binary 1's.

If the offset and pattern of a byte filter item represent bytes that do not exist in a NetBIOS packet (that is, if the packet is shorter than was intended when setting up a byte-filter list), then the filter item will not be applied to the packet and the packet will not be filtered. If a series of byte filter items is used to set up a single NetBIOS filter list, then a packet will not be tested for filtering if any of the byte filter items within the NetBIOS filter list represent bytes that do not exist in the NetBIOS packet.

Example: `add exclusive`

```
Byte Offset  [0] ?
Hex Pattern  [] ?
Hex Mask  (<CR> for no mask)  [] ?
```

default include
Changes the default setting of the filter list to "inclusive." This command indicates that if no filter items of the filter list match the contents of the packet being considered for filtering, the filter list will be evaluated as Inclusive. This is the default setting.

default exclude
Changes the default setting of the filter list to "exclusive." This command indicates that, if no filter items of the filter list match the contents of the packet being considered for filtering, the filter list will be evaluated as Exclusive.

delete *filter-item*
Deletes a filter item from the filter list.

Filter-item is a decimal number representing a filter item that was previously created by the add command.

list Displays information related to filter items in the specified filter list.

```
BYTE Filter List Name:     Engineering
BYTE Filter List Default:  Exclusive
Filter Item # Inc/Ex       Byte Offset    Pattern          Mask
1          Inclusive        14         0x123456         0xFFFF00
2          Exclusive         0         0x9876           0xFFFF
3          Exclusive        28         0x1000000        0xFF00FF00
```

move *filter-item1 filter-item2*
Reorders filter items within the filter list. The filter item whose number is specified by filter-item1 is moved and renumbered to be just after filter item2.

exit Exits to the previous command prompt level.

Update Name-Filter-List (Command Options): The following section lists the command options available for the update name-filter-list command:

add inclusive *ASCII host-name <LAST-hex number>*
Adds a filter item to the host-name filter list. With this command, the host

name fields of the NetBIOS packets are compared with the host-name given in this command. The following list shows how these comparisons are made:

- ADD_GROUP_NAME_QUERY: Source NetBIOS name field is examined
- ADD_NAME_QUERY: Source NetBIOS name field is examined
- DATAGRAM: Destination NetBIOS name field is examined
- NAME_QUERY: Destination NetBIOS name field is examined

If there is a match (taking into account wildcard designations in this command), then the filter list evaluates to Inclusive. If not, the next filter item of the filter list (if any) of the filter is applied to the packet. If the packet is not one of the four types supported by NetBIOS Name filtering, then the packet is bridged.

- Host-name is an ASCII string up to 16 characters long. A question mark (?) can be used in host-name to indicate a single character wildcard. An asterisk (*) can be used as the final character of host-name to indicate a wildcard for the remainder of the host-name. If host-name contains fewer than 15 characters, it is padded to the 15th character with ASCII spaces. Host-name can contain any character except the following:

  . / \ [ ] : | < > + = ; , <space>

  Note: Host-name is case sensitive.
- LAST-hex-number can be used if host-name contains fewer than 16 characters. It is a hexadecimal number (with no 0x in front of it) which indicates the value to be used for the last character. If the LAST argument is not specified on a hostname less than 16 characters, then a “?” wildcard is supplied for the 16th character.

add inclusive HEX *hexstring*

Adds a filter item to the host-name filter list. This command is functionally the same as the add inclusive ASCII command. However, the representation of hostname is different. This command supplies the hostname as a series of hexadecimal numbers (with no 0x in front).

- Hexstring must consist of an even number of hexadecimal numbers. If you do not supply a full 32 hexadecimal numbers, ASCII blanks are padded to the 29th and 30th numbers and a wildcard is supplied as the 31st and 32nd (16th byte) numbers. A wildcard for a single byte can be specified by **??**.

add exclusive ASCII *host-name <LAST-hex-number>*

Adds a filter item to the host-name filter list. This command is identical to the add inclusive ASCII command, except that packets that are matched against this filter item produce an Exclusive result for the filter list.

- Host-name is an ASCII string up to 16 characters long. A question mark (?) can be used in host-name to indicate a single character wildcard. An asterisk (*) can be used as the final character of host-name to indicate a wildcard for the remainder of the host-name. If host-name contains fewer than 15 characters, it is padded to the 15th character with ASCII spaces. Host-name can contain any character except the following:

  . / \ [ ] : | < > + = ; , <space>
- LAST-hex-number can be used if host-name contains fewer than 16 characters. It is a hexadecimal number (with no 0x in front of it) that indicates the value to be used for the last character. If the LAST argument is not specified on a host-name less than 16 characters, then a **?** wildcard is supplied for the 16th character.

NetBIOS Filtering Configuration Commands

add exclusive HEX *hexstring*

Adds a filter item to the name filter list. This command is functionally the same as the add inclusive hex command, except that packets that are matched against this filter item produce an Exclusive result for the filter list.

- Hexstring must consist of an even number of hexadecimal numbers. If you do not supply a full 32 hexadecimal numbers, ASCII blanks are padded to the 29th and 30th numbers and a wildcard is supplied as the 31st and 32nd (16th byte) numbers. A wildcard for a single byte can be specified by **??**.

default include

Changes the default setting of the filter list to "inclusive." This command indicates that, if no filter items of the filter list match the contents of the packet being considered for filtering, the filter list will evaluate to Inclusive. This is the default setting.

default exclude

Changes the default setting of the filter list to "exclusive." This command indicates that, if no filter items of the filter list match the contents of the packet being considered for filtering, the filter list is evaluated as Exclusive.

delete *filter-item*

Deletes a filter item from the filter list.

- Filter-item is a decimal number representing a filter item that was previously created by the add command.

list Displays information related to filter items in the specified filter-list.

```
NAME Filter List Name: nlist
NAME Filter List Default: Exclusive

Filter Item #   Type    Inc/Ex        Hostname       Last Char

      1         ASCII   Inclusive     EROS
      2         ASCII   Inclusive     ATHENA
      3         ASCII   Exclusive     FOOBAR
```

move *filter-item1 filter-item2*

Reorders filter items within the filter list. The filter item whose number is specified by filter-item1 is moved and renumbered to be just after filter-item2.

exit Exits to the previous command prompt level.

Set

Use the **set** command to set certain values, functions, and parameters associated with the bridge configuration. These include:

- Aging time for dynamic address entries in the filtering database
- Bridge address
- MAC service data unit (MSDU) size
- Spanning tree protocol bridge and port parameters
- Size of the bridge filtering database
- Protection against unauthorized access to the switched network using port security.

Syntax:

set age

bridge

filtering

maximum-packet-size . . .

port

port security

protocol bridge

protocol port . . .

age *seconds resolution*

Sets the time for aging out dynamic entries in the filtering database when the port with the entry is in the forwarding state. This age is also used for aging RIF entries in the adaptive database in the case of an SR-TB bridge personality.

Enter the required value after each prompt and press **Return**.

Aging Time Valid Values: 10 to 1000000

Aging Time Default Value: 30

The resolution value specifies how often dynamic entries in the filtering database should be scanned to determine if they have exceeded their age limit as set by the aging timer.

Resolution Valid Values: 1 to 60 seconds

Resolution Default Value: 5 seconds

Example: `set age`

```
seconds [300]  ?  400
resolution [5] ?  6
```

bridge *bridge-address*

Sets the bridge address. This is the low-order 6-octet bridge address found in the bridge identifier. By default, the bridge-addr-value is set to the medium access control (MAC) address of the lowest-numbered port at initialization time. You can use this command to override default address and enter your own unique address.

Note: Each bridge in the network must have a unique address for the spanning tree protocol to operate correctly.

Attention: In cases where a serial line interface is the lowest numbered port, it is mandatory to use this command so that the bridge will have a unique address when restarted. This process is necessary because serial lines do not have their own MAC address.

At the prompt, enter the bridge address in 12-digit hexadecimal format and press **Return**.

If you enter the address in the wrong format you will receive the message `Illegal Address`. If you enter no address at the prompt you will receive the message `Zero length`

Valid Values: 12 hexadecimal digits

Do not use dashes or colons to separate each octet. Each bridge in the network must have a unique address for the spanning tree protocol to operate correctly.

Default Value: 000000000000

Example: `set bridge`

```
Bridge Address (in 12-digit hex)[]?
```

filtering *database-size*

Sets the number of entries that can be held in the bridge filtering database.

Default Value: 1024 times the number of bridge ports.

For more information, see the **list filtering** command on page 9.

Example: `set filtering`

```
database-size [2048]?
```

maximum-packet-size *port# msdu-size*

Sets the largest MAC service data unit (MSDU) size for the port, if source routing is enabled on this port. The MSDU value setting has no implication on traditionally transparent media. An MSDU value greater than the packet size configured in the device will be treated as an error.

If this parameter is not set, the default value used is the size configured as the packet size for that interface.

Valid Values: Specify an integer in the range 16 to 65535

Default Value: packet size set for the port

Example: `set maximum-packet-size 1 4399`

port *block* **or** *disable*

Begins the port's participation in the spanning tree protocol. This is done by entering a status value of "block." This places the port in the "blocked" status as a starting point. The actual state of the port will later be determined by the spanning tree protocol as it determines its topology. Entering a status value of "disable" removes the port from participating in the spanning tree.

Example: `set port block`

```
Port Number [1]?
```

port security *enable* **or** *disable*

Specifies whether port security is enabled or disabled. Port security provides protection against unauthorized access to the switched network and is available only on Ethernet interfaces.

When enabled, an Ethernet port will learn the source MAC address of the first frame that it receives. If a frame with a different source MAC address is subsequently received, the Ethernet interface will be disabled. The disabling of the interface causes *link down* and *bridge topology change* SNMP traps to be sent to alert the network manager of the situation.

Once a source MAC address has been learned on a secure port, the MAC address is inserted into the bridging database as a static entry, preventing the entry from being aged out due to inactivity. You can use the `talk 5 ASRT>` **list database static** command to display these MAC addresses. See page 38 for more information about the **list database static** command.

Learned MAC addresses are not retained if the IBM 8371 is rebooted.

protocol *bridge* **or** *port*

Modifies the spanning tree protocol bridge or port parameters for a new configuration, or tunes the configuration parameters to suit a specific topology.

Enter “bridge” as the option to modify bridge parameters. The bridge-related parameters that can be modified with this command are described below.

When setting these values, make sure that the following relationships exist between the parameters or the input will be rejected:

2 X (Bridge Forward Delay - 1 second) ≥ Bridge Maximum Age
Bridge Maximum Age ≥ 2 X (Bridge Hello Time + 1 second)

Example: `set protocol bridge tb`

```
Bridge Max-Age [20]  25
Bridge Hello Time [2]   3
Bridge Forward Delay [15] 20
Bridge Priority [32768]    1
```

Bridge Maximum Age

Maximum age (period of time) that should be used to time out spanning tree protocol-related information.

When this bridging device is selected as the root bridge in a spanning tree, the value of this parameter specifies how long other active bridges are to store the configuration bridge protocol data units (BPDUs) they receive. When a BPDU reaches its maximum age limit without being replaced, the active bridges in the network discard it and assume that the root bridge has failed. A new root bridge is then selected.

Dependencies

The setting of this parameter may be affected by the setting of the Bridge Hello Time parameter. In addition, the setting of this parameter may affect the setting of the Bridge Forward Delay parameter.

Valid Values: 6 to 40 seconds

Default Value: 20 seconds

Bridge Hello Timer

Time interval between HELLO BPDUs.

When this bridging device is selected as the root bridge in a spanning tree, this parameter specifies how often this bridge transmits configuration bridge protocol data units (BPDUs). BPDUs contain information about the topology of the spanning tree and reflect changes to the topology.

Dependencies

The setting of this parameter may affect the setting of the Max age parameter.

Valid Values: 1 to 10 seconds

Default Value: 2

Bridge Forward Delay

Time interval used before changing to another state (should this bridge become the root).

When this bridging device is selected as the root bridge in a spanning tree, the value of this parameter specifies how long active ports in all bridges remain in a *listening state*. When the forward delay time expires, ports in the listening state go into the *forwarding*

state. State changes occur as a result of changes in the topology of the spanning tree, such as when an active bridge fails or is shut down.

The root bridge conveys this value to all bridges. This process ensures that all bridges are consistent between changes.

Valid Values: 4 to 30 seconds

Default Value: 15

Bridge Priority

A high-order 2-octet bridge address found in the Bridge Identifier - either the MAC address obtained from the lowest-numbered port or the address set by the **Set Bridge** command.

The bridge priority indicates the chances that this bridge will become the root bridge of the spanning tree. The lower the numerical value of the bridge priority parameter, the higher the priority of the bridge and the more likely it is to be chosen. The spanning tree algorithm chooses the bridge with the lowest numerical value of this parameter to be the root bridge.

Valid Values: 0 to 65535

Default Value: 32768

Enter **port** as the option to modify the spanning tree protocol port parameters. Enter the desired value at each prompt and press **Return**.

Example: **`set protocol port`**

```
Port Number [1] ?
Port Path-Cost (0 for default) [0] ?   1
Port Priority [128] ?   1
```

Port Number

Bridge port number; selects the port for which the path cost and port priority will be changed.

Path Cost

Cost associated with the port, which is used for possible root path cost.

Each port interface has an associated path cost, which is the relative value of using the port to reach the root bridge in a bridged network. The spanning tree algorithm uses the path cost to compute a path that minimizes the cost from the root bridge to all other bridges in the network topology.

This parameter specifies the cost associated with passing frames through this port interface, should this bridging device become the root bridge. Factor this value in when determining spanning tree routes between any two stations. A value of 0 instructs the bridging device to automatically calculate a path cost for this port using its own formula.

Valid Values: 1 to 65535

Default Value: 0 (means the cost will be calculated automatically)

Port Priority

Identifies port priority for the specified port. This is used by the spanning tree algorithm in making comparisons for port

selection (which port offers the lowest cost path to the root bridge) and blocking decisions.

Valid Values: 0 to 255

Default Value: 128

VLANS

Use the **vlans** command to access the VLAN configuration prompt. VLAN configuration commands are entered at this prompt. See “Dynamic Protocol Filtering (VLANS) Configuration Commands” on page 29 for an explanation of each of these commands.

Syntax:

vlans

Example:

```
Bridge 2 Config> vlans
Bridge 2 VLAN config>
```

NetBIOS Configuration Commands

Use these NetBIOS configuration commands to access the `NetBIOS config>` command prompt from which you can access detailed configuration menus for NetBIOS filtering parameters that are applicable to all the bridge instances in the switch.

Example:

```
ASRT Config> netbios
NetBIOS Support User Configuration
NetBIOS config>
```

Table 4. NetBIOS Configuration Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available).
Disable	Disables duplicate frame filtering and route caching.
Enable	Enables duplicate frame filtering and route caching.
List	Displays various NetBIOS filters and general configuration information.
Set	Configures parameters for name caching, duplicate frame filtering, and frame type filtering.
Exit	Returns you to the previous command level.

Response to NetBIOS Configuration Commands

The NetBIOS configuration (Talk 6) commands are not effective immediately. They remain pending until you issue the **reload** command.

Disable

Disables duplicate frame filtering or route caching.

Syntax:

disable duplicate-filtering

route-caching

duplicate-filtering

Disables duplicate frame filtering for bridging. You cannot disable duplicate frame filtering for DLSw traffic.

Example: `disable duplicate-filtering`

```
Duplicate frame filtering is          OFF
```

route-caching

Disables route caching for bridging and DLSw. Route caching is the process of converting broadcast frames to specifically routed frames (SRFs) using the entries in the NetBIOS name cache.

Example: `disable route-caching`

```
Route caching is                      OFF
```

Enable

Enables duplicate frame filtering, use of NetBIOS name lists, or route caching.

Syntax:

enable duplicate-filtering
route-caching

duplicate-filtering

Enables duplicate frame filtering for bridging. Duplicate frame filtering is always enabled for DLSw. You cannot enable and disable it.

Example: `enable duplicate-filtering`

```
Duplicate frame filtering is          ON
```

route-caching

Enables route caching for bridging and DLSw. Route caching is the process of converting broadcast to specifically routed frames (SRFs) using the NetBIOS name cache.

Example: `enable route-caching`

```
Route caching is                      ON
```

List (Configuration)

Displays all cache entries or displays cache entries by type of entry. Displays filter configuration information or general configuration information. Displays local NetBIOS name list entries.

Syntax:

list filters
general

filters Displays whether frame type filtering is on or off for bridging. Use the **set filters** to turn these filters on or off.

Example: `list filters`

```
Bridge name conflict filtering is     OFF
Bridge general bcast filtering is     OFF
Bridge trace control filtering is     OFF
```

general

Displays the current NetBIOS caching and filtering configuration.

Example:

```
list general
Bridge-only Information:

Bridge duplicate filtering is          OFF
Bridge duplicate frame filter t/o      1.5 seconds
```

Set

Sets name caching parameters, turns frame type filtering on or off for bridging, adjusts duplicate frame filtering timers and frame retry timers, and sets NetBIOS name list parameters. Also displays the NetBIOS name and byte filtering prompt.

Syntax:

set cache-parms
filters
general

cache-parms

Sets name caching parameters that apply to bridging or switching.

Example: `set cache-parms`

```
Significant characters in name [15]?
Best path aging timeout value in seconds [60.0]?
Reduced search timeout value in seconds [1.5]?
Unreferenced entry timeout value in minutes [5000]?
Max nbr local name cache entries [500]?
Max nbr remote name cache entries [100]?

Cache parameters set
```

Significant characters in name

Determines whether the router considers 15 or 16 characters when it looks up the NetBIOS name. If you enter 15, the router ignores the 16th character. If you select 16, the router includes the 16th character when it looks up cache entries.

The default is 15.

Best path aging timeout

Amount of time the router considers the address and route for a name cache entry to be the best path to that station. When this timer expires, the router deletes the name cache entry and attempts to discover a new best path for the NetBIOS name.

To determine the best path, the router considers transmission time between nodes on all possible routes connecting those nodes, as well as largest frame size. The router does not consider a path suitable if it cannot accommodate the largest NetBIOS frame that could be transmitted over the path.

The default is 60 seconds. The range is 1.0 to 100000.0 seconds.

Reduced search timeout

When the router receives a Name-Query, Status-Query, or Datagram during the timeout period, it carries out a search based on current NetBIOS name cache information.

If the router receives a duplicate frame after this timer expires, it assumes the previous route is not longer valid and it widens its search. The router forwards the duplicate frame to both bridges and DLS. DLS broadcasts the corresponding SSP message to all possible DLS partners.

The default is 1.5 seconds. The range is 1.0 to 100.0 seconds.

Unreferenced entry timeout
The router keeps a name that is not referenced in its cache for this length of time before deleting it. If the cache fills up, the router removes entries sooner.

The default is 5000 minutes. The range is 1 to 100 000 minutes.

Max nbr local name cache entries
Maximum number of locally-learned entries the router saves in the name cache.

The default is 500. The range is 100 to 30 000. You can lower this value to save router memory. To optimize memory usage, processor usage, and the amount of broadcast traffic, set the number of local name cache entries as close as possible to the total number of NetBIOS stations (servers and clients) that are active on this router's local bridge network.

Max nbr remote name cache entries
Maximum number of remotely-learned entries, group name entries, and unknown entries that the router saves in the name cache.

The default is 100. The range is 100 to 30 000. You can lower this value to save router memory. To optimize memory usage, processor usage, and the amount of broadcast traffic, set the number of remote name cache entries to the number of remote NetBIOS servers that are to be accessed by NetBIOS clients on this router's local bridge network, plus about 25%.

filters Turns frame-type filtering for bridging on or off.

Example: `set filters`

```
Filter Name Conflict frames? [No]: y
Name conflict filtering is            ON
Filter General Broadcast frames? [No]:
General broadcast filtering is        OFF
Filter Trace Control frames? [No]:
Trace control filtering is            OFF
```

general
Sets the duplicate frame timeout, duplicate frame-detect timeout, and the command frame retry count and timeout.

Example: `set general`

```
ATTENTION! Setting Duplicate Frame Filter Timeout to zero...
disables duplicate frame checking!
Duplicate frame filter timeout value in seconds [1.5]?
Duplicate frame detect timeout value in seconds [5.0]?
General parameters set
```

Duplicate frame filter timeout
Applies only to bridged traffic if duplicate filtering is enabled. During this timeout period, the router filters all duplicate frames it receives.

The range is 0.0 to 100.0 seconds. Zero disables duplicate frame checking. The default is 1.5 seconds.

Duplicate frame-detect timeout
Applies to both bridged and DLSw traffic. Amount of time during which the router saves entries in its duplicate frame filter database. When this timer expires, the router creates new entries for new frames that it receives.

The range is 0.0 to 100.0 seconds. The default is 5 seconds.

—

Dynamic Protocol Filtering (VLANS) Configuration Commands

This section explains all of the VLAN configuration commands. These commands let you configure protocol and IP multicast VLANs.

Configuration commands for the ASRT bridge are entered at the `ASRT VLAN config>` prompt. This prompt is accessed by entering the **vlans** command at the `ASRT confi`

Table 5. VLAN Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available).
Add	Adds the definition of a new VLAN filter
Change	Changes VLAN filtering parameters for an indicated VLAN
Delete	Deletes the selected VLAN filters
Disable	Disables VLAN filtering on the selected VLANs
Enable	Enables VLAN filtering on the selected VLANs
List	Displays all information associated with the selected VLAN filters
Exit	Returns you to the previous command level.

Add

Use the **Add** command to define a new VLAN filter. Refer to the chapter entitle “Bridging Features” in the *8371 Networking Multilayer Ethernet Switch Software User’s Guide and Configuration Reference*, GC30-9688-00 for a discussion of VLANs concepts.

Syntax:

add ip

ip-multicast

ipx

netbios

sliding-window

Example 1: add ip

```
IP Address [0.0.0.0]? 9.2.3.4
Subnet Mask [255.0.0.0]?
Configure this VLAN on Specific Ports? [No]:
Age (expiration in minutes,0=infinity) [10000]? 0
Enable IP-Cut-Through from this VLAN? [Yes]:
Enable IP-Cut-Through to this VLAN? [Yes]:
Track Active MAC Addresses on this VLAN? [No]:
Enable This Filter? [Yes]:
VLAN Name (32 chars max) []? IP 9.x.x.x
VLAN 'IP 9.x.x.x' (IP subnet 9.0.0.0) successfully added
```

If some ports should not be configured as Auto-Detect and Include, then the port can be manually configured.

Example 2: add ip-multicast

```
IP Multicast Address [0.0.0.0]? 230.1.1.1
Configure Specific Ports? [No]:
Age (expiration in minutes,0=infinity) [10]? 0
Track Active MAC Addresses on this VLAN? [No]:
Enable This Filter? [Yes]:
VLAN Name (32 chars max) []? IPmcast01
VLAN 'IPmcast01' (IP Multicast 230.1.1.1) successfully added
```

Example 3: add ipx

```
Network Number (in 8-digit hex) (1 - FFFFFFFE) [1]? 2FF
Configure this VLAN on Specific Ports? [No] y
Configure VLAN on port 1 (Include, Exclude, or Auto-Detect) [A]?
Configure VLAN on port 2 (Include, Exclude, or Auto-Detect) [A]? e
Age (expiration in minutes,0=infinity) [5000]?
Track Active MAC Addresses on this VLAN? [No]:
Enable This Filter? [Yes]:
VLAN Name (32 chars max) []? IPX 2FF
VLAN 'IPX 2FF' (IPX network 0x2FF) successfully added
```

A description of each parameter follows:

IP Address

This prompt allows you to enter the IP address of the IP subnet whose traffic will be dynamically filtered to create this VLAN. This value, after the subnet mask is applied, is what will be saved and referenced in other VLAN commands.

Subnet Mask

This is the subnet mask that will be applied to the input IP Address to create the IP subnet value used to detect traffic for this VLAN.

IP Multicast address

This is the IP group address whose multicast traffic will be filtered to create this VLAN.

Note: A VLAN for 224.0.0.1 (the all IP hosts address) is created during initialization and is used to configure IP multicast VLANs that are auto-created when an IGMP report frame is detected and the 224.0.0.1 VLAN is enabled. See

Valid Values: 224.0.1.0 - 239.255.255.255

Default Value: none

Network Number

This prompt allows you to enter the IPX network ID number whose traffic will be dynamically filtered to create this VLAN.

Sliding Window Filter Base

Determines whether the base for the offset is the first byte of the destination MAC address or the first byte of the frame's information field.

Valid Values: mac or info

Default Value: mac

Sliding Window Filter Offset

Sets the byte offset into the frame where the comparison with the mask and value begins.

Valid Values: 0 - 255

Default Value: 0

Sliding Window Filter Value

The value used for comparing the sliding window filter.

A frame "matches" a sliding window filter if the octet pattern (whose start is determined by the *Sliding Window Filter Base* and *Sliding Window Filter Offset*) ANDED with the *Sliding Window Filter Mask* equals this *Sliding Window Filter Value* ANDED with the *Sliding Window Filter Mask*.

Valid Values: Any octet string of length 1 - 10

Default Value: None

Sliding Window Filter Mask
The mask used for comparing the sliding window filter.

Valid Values: Any octet string of length 1 - 10

Default Value: None

Configure

Answering “No” to this prompt causes all bridge ports to be set to the default value of Auto-Detect and Include. Answering *yes* to this prompt causes further prompting to select the desired port inclusion mode for each bridge port.

The modes are:
- Auto-Detect and Include (the default mode that requires that traffic from this vlan be received on the port before being included in the VLAN forwarding domain).
- Include Always (to always include this port in the forwarding domain regardless of received traffic)
- Exclude Always (to always exclude this port from the forwarding domain regardless of received traffic).

Age The amount of time, in minutes, that an Auto-Detect port will remain in the forwarding state in the absence of traffic received from that port for this VLAN. Entering a value of zero means that ports auto-detected will never expire and be removed from the forwarding domain.

If MAC address tracking is enabled for a VLAN, the aging time also determines when a MAC address is no longer considered a member of the VLAN in the absence of traffic received from that MAC address.

Valid Values: 0 to 4 294 967 295

Default Value

IP subnet
10 000 minutes

IP multicast
10 minutes

IPX Network
10 minutes

NetBIOS
5000 minutes

Sliding Window
5000 minutes

Enable IP-Cut-Through Transmission Status
Answering *yes* will allow forwarding of IP traffic from devices on this VLAN to devices on other VLANs that have IP-Cut-Through reception enabled.

Enable IP-Cut-Through Reception Status
Answering *yes* will allow IP traffic to be forwarded to devices on this VLAN from devices on other VLANs that have IP-Cut-Through transmission enabled.

Track Active MAC Addresses
Answering *yes* causes source MAC addresses from transmissions on this

VLAN to be saved. These learned addresses can be displayed with the **show-members** command. Learned addresses will be aged out with the aging timer for this VLAN.

VLAN Filter Status
Answering *yes* will enable dynamic filtering for this VLAN. Answering “No” means that no filtering will be done on traffic from members of this VLAN.

VLAN Name
This prompt lets you define a name for this VLAN that can be used with all VLAN commands. A VLAN name is required for MAC address, port-based, and sliding window VLANs.

This name must be unique among all VLANs of all types within the ASRT bridge. This name consists of up to 32 characters and can include spaces.

Change

Use the change command to change the configuration parameters associated with a particular VLAN. The VLAN to change can be chosen by explicitly specifying the subnet or by selecting the VLAN from a list with the *by-name* option. This command invokes the same prompts used with the add command. The current parameter values will be displayed as the default and can be maintained by simply pressing **Return**.

Syntax:

change by-name
ip subnet address
ip-multicast
ipx network number
netbios
sliding-window

Example: change ip

```
IP Address [9.0.0.0]?
Configure Specific Ports? [No]:
Age (expiration in minutes,0=infinity) [0]? 300
Enable IP-Cut-Through from this VLAN? [Yes]:
Enable IP-Cut-Through to this VLAN? [Yes]:
Track Active MAC Addresses on this VLAN? [No]:
Enable This Filter? [Yes]:
VLAN Name (32 chars max) [IP 9.x.x.x]?
VLAN 'IP 9.x.x.x' (IP subnet 9.0.0.0) successfully changed
```

Delete

Use the **delete** command to delete a particular VLAN filter, all VLAN filters of a particular type, or all defined VLAN filters. If you are deleting a single filter, you can choose the VLAN to be deleted by selecting the VLAN from a list using the *by-name* option.

Syntax:

delete by-name
ip all
ip subnet *subnet address*
ip-multicast all

ip-multicast by-name

ipx all

ipx network *network-number*

netbios

sliding-window all

sliding-window by-name

all

Example 1: del ip subnet 9.0.0.0

```
VLAN 'IP 9.x.x.x' (IP subnet 9.0.0.0) deleted
```

Example 2: del ipx all

```
Are you sure you want to delete ALL IPX VLANS? [No]: y
All IPX VLANS deleted
```

Disable

Use the **disable** command to disable a particular VLAN filter, all VLAN filters of a particular type, or all defined VLAN filters. If disabling a single filter, the VLAN to be disabled can be chosen by selecting the VLAN from a list using the *by-name* option.

Syntax:

disable

by-name

ip all

ip subnet *subnet-address*

ip-multicast all

ip-multicast by-name

ipx all

ipx network *network-number*

netbios

sliding-window all

sliding-window by-name

all

Example: disable ip subnet 220.5.3.0

```
VLAN 'Building #4' (IP subnet 220.5.3.0) now disabled
```

Enable

Use the **enable** command to enable a particular VLAN filter, all VLAN filters of a particular type, or all defined VLAN filters. If you are enabling a single filter, you can choose the VLAN to be enabled by selecting the VLAN from a list using the *by-name* option.

Syntax:

enable

by-name

ip all

ip subnet *subnet-address*

ip-multicast all

ip-multicast by-name

ipx all

ipx network *network-number*

netbios

sliding-window all

sliding-window by-name

all

Example: enable by-name

```
 Choice of VLAN:
       VLAN type    Identifier         VLAN Name
       =========    ==========         =========
    (1) IP           9.0.0.0            IP 9.x.x.x
    (2) IP           220.5.3.0          Building #4
    (3) IPX          0x2FF              Ethernet A
    (4) IPX          0x3FF              Ethernet B
Enter Selection [1]? 3
VLAN 'Ethernet A' (IPX Network 0x2FF) now enabled
```

List

Use the **list** command to list the configuration information about a particular VLAN filter, all VLAN filters of a particular type, or all defined VLAN filters. If you are listing a single filter, you can choose the VLAN to be listed can be chosen by selecting the VLAN from a list using the *by-name* option.

Syntax:

list

by-name

ip all

ip subnet *subnet-address*

ip-multicast all

ip-multicast by-name

ipx all

ipx network *network-number*

netbios

sliding-window all

sliding-window by-name

all

Example 1: list ip subnet 9.0.0.0

```
Subnet Address              = 9.0.0.0
Subnet Mask                 = 255.0.0.0
Bridge Port 1 (Interface 0) = Auto-Detect and Include
Bridge Port 2 (Interface 1) = Always Exclude
Age (expiration in minutes) = 300
IP-Cut-Through Status:
   Transmit From This VLAN  = Enabled
   Reception By This VLAN   = Enabled
```

```
Tracking of MAC Addresses   = Disabled
VLAN Filter State           = Enabled
VLAN Name                   = IP 9.x.x.x
```

Example 2: list ipx all

```
----------- IPX VLANS -------------------------------
IPX Network Number          = 0x2FF
Bridge Port 1 (Interface 0) = Auto-Detect and Include
Bridge Port 2 (Interface 1) = Always Exclude
Age (expiration in minutes) = Never Expires
IP-Cut-Through Status:
   Transmit From This VLAN  = Enabled
   Reception By This VLAN   = Disabled
Tracking of MAC Addresses   = Disabled
VLAN Filter State           = Enabled
VLAN Name                   = Ethernet A
+++++++++++++++++++++++++++++++++++++++++++++++++++++++
IPX Network Number          = 0x3FF
Bridge Port 1 (Interface 0) = Auto-Detect and Include
Bridge Port 2 (Interface 1) = Auto-Detect and Include
Age (expiration in minutes) = 5000
IP-Cut-Through Status:
   Transmit From This VLAN  = Enabled
   Reception By This VLAN   = Enabled
Tracking of MAC Addresses   = Disabled
VLAN Filter State           = Disabled
VLAN Name                   = Ethernet B
```

Accessing the ASRT Monitoring Environment

To access the ASRT monitoring environment, enter the **protocol asrt** command at the + (GWCON) prompt:

```
+protocol asrt
ASRT>
```

ASRT Monitoring Commands

Enter the ASRT monitoring commands at the ASRT+> prompt. Access the commands as follows:

Table 6 shows the ASRT configuration commands. Use these commands to access a particular bridge instance or to display information about all bridge instances in the switch.

Table 6. ASRT Multiple Bridge Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available).
Bridge *i*	Accesses a particular bridge instance for which more detailed information is desired. The parameter *i* specifies the particular bridge instance. See “Detailed Monitoring Commands for a Particular Bridge Instance” on page 36 for a list of detailed monitoring commands available.
List	Displays status information for all configured bridges or for a specific bridge instance.
Netbios	Accesses the commands available to work with NetBIOS filtering parameters that are applicable to all bridge instances in the switch. See “NetBIOS Monitoring Commands” on page 46 for a discussion of commands available at the NetBIOS command prompt.
Exit	Returns you to the previous command level.

Detailed Monitoring Commands for a Particular Bridge Instance

This section describes the ASRT monitoring commands. These commands allow you to view and modify parameters from the active monitoring. Information you modify with the monitoring commands is reset to the SRAM configuration when you restart the bridging device.

You can use these commands to temporarily modify the configuration without losing configuration information in the bridge memory. The `ASRT>` prompt is displayed for all ASRT monitoring commands.

Monitoring and dynamic reconfiguration VLANS commands are entered at the `VLAN>` monitoring prompt. The `VLAN>` command is accessed by entering the **VLANS** command explained later in this chapter.

Note: For commands requiring you to enter MAC Addresses, the addresses can be entered in the following formats:

IEEE 802 canonical bit order

00-00-00-12-34-56

IEEE 802 canonical bit order (shorthand format)

000000123456

Table 7 shows the ASRT monitoring commands.

Table 7. Detailed Monitoring Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available).
Cache	Displays cache entries for a specified port.
Delete	Deletes MAC addresses entries from the bridging device database.
List	Displays information about the complete bridge configuration or about selected configuration options.
NetBIOS	Displays the NetBIOS monitoring prompt. See “NetBIOS” on page 41.
VLANS	Displays the VLAN monitoring prompt.
Exit	Returns you to the previous command level.

Cache

Use the **cache** command to display the contents of a selected bridging-port routing cache. If the port does not possess a cache you will see the message `Port X does not have a cache.`

Syntax:

cache *port#*

Example: **`cache`**

```
Port number [1]? 3

MAC Address    MC*          Age  Port(s)

00-00-93-00-C0-D0             0  3 (TKR/1)
00-00-00-11-22-33             0  3 (TKR/1)
```

MAC Address

6-byte MAC address of the entry.

Entry Type

Specifies one of the following address entry types:

Reserved - entries reserved by the IEEE 802.1d Standard.

Registered - entries consist of unicast addresses belonging to proprietary communications hardware attached to the box or multicast addresses enabled by protocol forwarders.

Dynamic - entries “learned” by the bridge “dynamically” which do not survive power on/offs or system resets and which have an “age” associated with the entry.

Free - locations in database that are free to be filled by address entries.

Unknown - entry types unknown to the bridge. May be possible bugs and/or illegal addresses.

Age Age in seconds of each dynamic entry. Age is decremented at each resolution intervals.

port(s)

Specifies the port number associated with that entry and displays the interface name (this will always be that of the interface having the cache).

Delete

Use the **delete** command to delete station (including MAC) address entries from the device’s permanent database.

Syntax:

delete mac-address

Example: `delete 00-00-93-10-04-15`

List

Use the **list** command to display information about the bridging device configuration or to display information about selected configuration or bridging options.

Syntax:

list

bridge . . .

database . . .

filtering . . .

port

spanning-tree-protocol . . .

transparent . . .

bridge

Lists all general information regarding the bridge device configuration.

Example: `list bridge`

Bridge ID

Unique ID used by the spanning tree algorithm in determining the spanning tree. Each bridge in the network is assigned a unique bridge identifier. The bridge priority is displayed in decimal followed by the hex address.

Bridge State
Indicates whether bridging is enabled or disabled.

Bridge Type
Displays the configured bridge type. This is displayed as NONE, TB, or ASRT.

Number of Ports
Displays the number of ports configured for that bridge.

Port Specifies a user defined number assigned to an interface by the Add Port command.

Interface
Identifies devices connected to a network segment through the bridge.

State Indicates the current state of the port. This is displayed as UP or DOWN.

MAC address
Displays the MAC address associated with that port in canonical bit order.

Modes
Displays the bridging mode for that port. T indicates transparent bridging. SR indicates source routing. A indicates adaptive bridging.

MSDU Specifies the maximum frame (data unit) size (including the MAC header but not the FCS field) the bridge can transmit and receive on this interface.

database *datagroup-option*
Lists the contents of transparent filtering databases. There are a number of datagroups which can be chosen to be displayed under the list database command. These include the following:

- All - Displays the entire transparent bridging database.
- Dynamic - Displays all dynamic (learned) address database entries.
- Local - Displays all local (reserved) address database entries.
- Port - Displays address entries for a specific port.
- Range - Displays a range of database entries from the total transparent bridging filtering address database. A starting and ending MAC address is given to define the range. All entries falling within this range will be displayed.

The following examples break down the list database command options. The first example also shows the related output.

Example: `list database all`

Note: The following fields are displayed for all of the **list database** command options.

MAC Address
Specifies the address entry in 12-digit hex format (canonical bit order).

MC* An asterisk following an address entry indicates that the entry has been flagged as a multicast address.

Entry Type

Specifies one of the following types:

Reserved
Entries reserved by the IEEE 802.1d standard.

Registered
Entries consist of unicast addresses belonging to interfaces participating in the bridge or multicast addresses enabled by protocol forwarders

Dynamic
Entries “learned” by the bridge “dynamically” which do not survive power on/offs or system resets and which have an “age” associated with the entry

Free This type is not used and should not be normally be seen except in occasional “race” conditions between the monitoring and the bridge.

Unknown
Unknown entry type. May indicate a software bug. Report the hex entry type to Customer Service.

Age Refers to the age (in seconds) of each dynamic entry. Age is decremented at each resolution interval.

Port(s)
Specifies the outgoing port number(s) for that entry. Device type is also listed for single port entries.

Example: `list database dynamic`

Example: `list database local`

```
MAC Address    MC*  Entry Type       Age  Port(s)

00-00-93-B8-00-48   Registered            1 (TKR/1)
01-80-C2-00-00-00*  Registered            1
03-00-02-00-00-00*  Registered            1
ASRT>
```

Example: `list database permanent`

Example: `list database port` *port#*

Example: `list database static`

Example: `list database range`

```
First MAC address [00-00-00-00-00-00]? 00-00-93-00-C0-D0
Last MAC address [FF-FF-FF-FF-FF-FF]? 01-80-C2-00-00-00

MAC Address    MC*  Entry Type       Age  Port(s)
00-00-93-10-04-15   Registered            1 (Eth/2)
01-80-C2-00-00-00   Registered            1,3
```

filtering *datagroup-option*

Displays general information about the bridge’s protocol filtering databases. There are a number of general datagroups which may be displayed under the **list filtering** command. These include the following:

- All - Displays all filtering database entries.
- Ethertype - Displays Ethernet protocol type filter database entries.
- SAP - Displays SAP protocol filter database entries.
- SNAP - Displays SNAP protocol identifier filter database entries.

The following examples break down each of the list filtering display options.

Example: list filtering all

```
Ethernet type 0800 is routed on ports 1
IEEE 802.2 destination SAP 42 is routed on ports 1
IEEE 802 SNAP PID 00-00-00-08-00 is routed on ports 2-3
```

Descriptors used in explaining how packets are communicated include the following:

- Routed - Describes packets which are passed to routing forwarder to be forwarded
- Filtered- Describes packets which are administratively filtered by the user setting protocol filters
- Bridged and routed - This describes a protocol identifier for which there is a protocol entity within the system which is not a forwarder. An example of this would be a link level echo protocol. Unicast packets from this protocol are bridged or locally processed if being sent to a registered address. Multicast packets are forwarded and locally processed for a registered multicast address.

All of the descriptors just explained also apply to ARP packets with this Ethertype.

Example: list filtering ethertype

```
Ethernet type (in hexadecimal), 0 for all [0]? 0800
Ethernet type 0800 is routed on ports 1
```

Example: list filtering SAP

```
SAP (in hexadecimal), 100 for all [100]? 42
IEEE 802.2 destination SAP 42 is routed on ports 1
```

Example: list filtering SNAP

```
SNAP Protocol ID, return for all [00-00-00-00-00]?
IEEE 802 SNAP PID 00-00-00-08-00 is routed on ports 2-3
```

port *port#*

Displays port information.

Example: list port

```
Port Id (dec)    : 128: 3, (hex): 80-03
Port State       : Forwarding
STP Participation: Enabled
Port Supports    : Transparent Bridging Only
Assoc Interface #/name : 5/Eth/1
```

Port Specifies a user defined number assigned to an interface by the Add Port command.

Interface
Identifies devices connected to a network segment through the bridge.

State Indicates the current state of the port. This is displayed as UP or DOWN.

MAC address
Displays the MAC address associated with that port in canonical bit order.

Modes
Displays the bridging mode for that port. T indicates transparent bridging. SR indicates source routing. A indicates adaptive bridging.

MSDU Specifies the maximum frame (data unit) size (including the MAC header but not the FCS field) the bridge can transmit and receive on this interface.

spanning-tree protocol *datagroup-option*

- Displays spanning tree protocol information. The spanning tree protocol is used by the transparent bridge to form a loop-free topology. There are a number of general datagroup options which may be displayed under the **list spanning-tree-protocol** command. These include the following:
  - Configuration - Displays information concerning the spanning tree protocol.
  - Counters - Displays the spanning tree protocol counters.
  - State - Displays the current spanning tree protocol state information.
  - Tree - Displays the current spanning tree information including port, interface, and cost information.

  The following examples illustrate each of the list spanning-tree-protocol display options.

Example: `list spanning-tree-protocol configuration`

```
Bridge ID (prio/add):  32768/0000-93-00-84-EA
Bridge state:          Enabled
Maximum age:           20 seconds
Hello time:            2 seconds
Forward delay:         15 seconds
Hold time:             1 seconds
Filtering age:         320 seconds
Filtering resolution:  5 seconds

Port  Interface  Priority  Cost   State
  4   Eth/1      128    100     Enabled
128   Tunnel     128    65535   Enabled
```

Example: `list spanning-tree-protocol counters`

```
  Time since topology change (seconds)         0
  Topology changes:                            1
  BPDUs received:                              0
  BPDUs sent:                              14170

Port  Interface  BPDUs received  BDPU input overflow  Forward transitions

  1  TKR/1             0              0               1
```

Example: `list spanning-tree-protocol state`

```
Designated root (prio/add):    32768/00-00-93-00-84-EA
Root cost:                     0
Root port:                     Self
Current (root) maximum age:    20 seconds
Current (root) hello time:     2 seconds
Current (root) Forward delay:  15 seconds
Topology change detected:      FALSE
Topology change:               FALSE

Port  Interface   State
  4  Eth/1       Forwarding
```

Example: `list spanning-tree-protocol tree`

```
Port                Designated   Desig.         Designated   Des.
No.  Interface           Root     Cost             Bridge   Port

 2  ATM/0:0:48  0/00-00-00-00-00-00    0     0/00-00-23-45-00-00 80-00
```

NetBIOS

Use the **netbios** command to access the NetBIOS> prompt. NetBIOS monitoring commands may be entered at the NetBIOS> prompt.

Syntax:

netbios

NetBIOS Filtering Monitoring Commands

Enter **netbios** at the `Bridge x console>` prompt to display the NetBIOS filtering monitoring prompt. For example:

```
Bridge 2 Console> netbios
NetBIOS Support User Console for Bridge 2
NetBIOS Bridge 2>
```

Table 8. NetBIOS Filtering Monitoring Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available).
List	Displays all information concerning cache or statistics.
Set	Adds information to or deletes information from a host-name or byte filter list.
Exit	Returns you to the previous command level.

List: Use the **list** NetBIOS Filtering command to display all information concerning created name-byte filters.

Syntax:

list cache

statistics

Set: Use the **set** command to display byte filter lists. The filter-list is a string previously entered using the create byte (or name) filter-list prompt. This command brings you to the `NetBIOS Byte (or Name) filter-list+` prompt. At this prompt you can list byte filter lists.

Syntax:

set filters name-byte

You can issue the **list** command to display information about lists or filters.

Syntax:

list byte-filter-lists

Example:

```
BYTE Filter List Name:     Engineering
BYTE Filter List Default:  Exclusive
Filter Item # Inc/Ex       Byte Offset    Pattern          Mask
1          Inclusive        14         0x123456         0xFFFF00
2          Exclusive         0         0x9876           0xFFFF
3          Exclusive        28         0x1000000        0xFF00FF00
```

name-filter-lists *filter-list*

Example:

```
NAME Filter List Name: nlist
NAME Filter List Default: Exclusive

Filter Item #   Type    Inc/Ex        Hostname       Last Char

      1         ASCII   Inclusive     EROS
      2         ASCII   Inclusive     ATHENA
      3         ASCII   Exclusive     FOOBAR
```

Dynamic Protocol Filtering (VLANS)

The VLAN monitoring commands are a superset of the VLAN configuration commands. However, instead of updating the SRAM configuration records immediately, they change the behavior of VLANs in real-time. Changes made

through the monitoring can be optionally saved to SRAM. Also, the configuration in SRAM can be loaded and used without requiring a reboot.

Monitoring commands for the ASRT bridge are entered at the ASRT VLAN> prompt. This prompt is accessed by entering the **vlans** command at the ASRT> prompt. The following table shows the VLAN monitoring commands.

Table 9. VLAN Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available).
Add	Adds the definition of a new VLAN filter
Change	Changes VLAN filtering parameters for an indicated VLAN
Delete	Deletes the selected VLAN filters
Disable	Disables VLAN filtering on the selected VLANs
Enable	Enables VLAN filtering on the selected VLANs
List	Displays all information associated with the selected VLAN filters
Load	Loads and uses the VLAN configuration currently in SRAM
Reset-Counters	Resets all counters associated with the selected VLAN filters
Save	Saves the current runtime configuration to SRAM
Show-members	Displays learned MAC addresses for a selected VLAN
Show-vlans	Lists the enabled VLANs of which a particular MAC address is a member
Exit	Returns you to the previous command level.

For a description of the **Add**, **Change**, **Delete**, **Disable**, and **Enable** commands, see “Dynamic Protocol Filtering (VLANS) Configuration Commands” on page 29.

List Use the list command to list the current real-time configuration for a particular VLAN filter, all VLAN filters of a particular type, or all defined VLAN filters. If listing a single filter, the VLAN to list can be chosen by selecting the VLAN from a list with the *by-name* option. The resulting output includes both configuration parameters and VLAN counters.

Syntax:

list by-name

ip all

ip subnet *subnet address*

ip-multicast all

ip-multicast by-name

ipx all

ipx network *network number*

netbios

sliding-window all

sliding-window by-name

all

Example:

```
vlans config>list ip subnet 9.0.0.0

   Subnet Address              = 9.0.0.0
   Subnet Mask                 = 255.0.0.0
```

```
Port 1 (Interface 0) = Auto-Detect and Include, Forwarding
Port 2 (Interface 1) = Always Exclude,          Not Forwarding
Age (expiration in minutes) = 300
IP-Cut-Through Status:
   Tx From This VLAN    = Enabled  Reception By This VLAN = Disabled
   Packets Transmitted  = 25       Packets Received       = 0
   Tx Packets Discarded = 0        Rx Packets Discarded   = 14
Tracking of MAC Addresses  = Disabled
VLAN Status                = Enabled
Packets Processed          = 43
Discards Due To Exclusion  = 13
VLAN Name                   = IP 9.x.x.x
```

A description of the VLAN counters follows:

Packets Transmitted
Total number of IP packets successfully cut through from this VLAN.

Packets Received
Total number of IP packets successfully cut through to this VLAN.

Tx Packets Discarded
Number of IP packets that were intended to be cut through from this VLAN, but were discarded due to IP-Cut-Through transmission being disabled. Packets from ports configured as Always Exclude are not included in this count.

Rx Packets Discarded
Number of IP packets that were intended to be cut-through to this VLAN, but were discarded due to IP-Cut-Through reception being disabled.

Packets Processed
Total number of packets processed by this VLAN's forwarding logic. This includes all packets forwarded and discarded. For IP Multicast VLANs, this number includes IGMP Reports and matching IP Multicast frames. For the IP Multicast auto-creation VLAN (group 224.0.0.1), this counter indicates the number of received IGMP Query packets from multicast devices.

Discards Due To Exclusion
Number of packets received matching this VLAN on ports configured as Always Exclude for this VLAN.

Load Use the load command to load and immediately use the VLAN configuration stored in SRAM. This will overwrite any configuration changes that may have been made via monitoring since the last save. All timers and counters associated with VLANs will be reset.

Syntax: load

Example: load

```
Warning: This process will overwrite your current configuration.
Are you sure you want to load the VLAN configuration from SRAM? [No] y
VLAN configuration loaded
```

Reset-Counters
Use the reset-counters command to set all counters to zero for a particular VLAN filter, all VLAN filters for a particular protocol, or all defined VLAN filters. If you are resetting the counters in a single filter, you can choose the VLAN by specifying the subnet or by selecting the VLAN from a list with the by-name option.

Syntax:
reset-counters
by-name

ip all
ip subnet *subnet address*
ip-multicast all
ip-multicast by-name
ipx all
ipx network *network number*
netbios
sliding-window all
sliding-window by-name
all

Example: reset ipx network 3ff

```
VLAN 'Ethernet B' (IPX Network 0x3FF) counters reset
```

Save Use the **save** command to store the current runtime VLAN configuration into SRAM. This will overwrite the current SRAM configuration. This command does not affect the runtime behavior of VLANs or reset the timers or counters associated with VLANs.

Syntax: save

Example: save

```
Are you sure you want to save the VLAN configuration to SRAM? [No] y
VLAN configuration saved
```

Show-members

Use the **show-members** command to display all the learned MAC addresses for a particular VLAN that has MAC Address Tracking enabled. Addresses in this list have all transmitted broadcast frames within the configured aging time. The MAC addresses will be displayed along with the associated bridge port and interface and can be sorted by bridge port or increasing MAC address.

Syntax:
show-members
by-name
ip *subnet-address*
ip-multicast
ipx *network-number*
netbios
sliding-window

Example: show-members ip

```
Subnet Address [9.0.0.0]?

        Sort VLAN Members by Port (P) or Mac Address (M) [P]?
        Port Number to Show Membership (0=All) [0]?

        Current Members of Runtime VLAN 'IP 9.x.x.x' (IP Subnet 9.0.0.0):

           Port  1 (Interface  0),  Mac Address: 10.00.5A.00.64.00
           Port  2 (Interface  1),  Mac Address: 10.00.5A.00.65.00
```

Show-vlans

Use the **show-vlans** command to display all the enabled VLANs in which traffic from a particular MAC address has been observed since the last aging timer expiration.

Syntax:

Example: show-vlans

```
Enter Mac Address in Hex: []? 10005A006400

        List of VLANS with Mac Address 10.00.5A.00.64.00:
```

```
                VLAN Type    Identifier            VLAN Name
                =========    ==========            =========
           (1)  IP           9.0.0.0               IP 9.x.x.x
```

NetBIOS Monitoring Commands

Enter **netbios** at the ASRT> prompt to display the NetBIOS monitoring prompt. For example:

```
ASRT> netbios
NetBIOS Support User Console
NetBIOS>
```

Use these NetBIOS monitoring commands to access the detailed monitoring menus for NetBIOS filtering parameters that are applicable to all the bridge instances in the switch.

Table 10. NetBIOS Monitoring Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available).
Disable	Disables duplicate frame filtering and route caching.
Enable	Enables duplicate frame filtering and route caching.
List	Displays various NetBIOS name cache configuration information.
Set	Configures parameters for name caching, duplicate frame filtering and frame type filtering.
Exit	Returns you to the previous command level.

Disable

Disables duplicate frame filtering or route caching.

Syntax:

disable duplicate-filtering

route-caching

duplicate-filtering

Disables duplicate frame filtering for bridging. You cannot disable duplicate frame filtering for DLSw traffic.

Example: `disable duplicate-filtering`

```
Duplicate frame filtering is          OFF
```

route-caching

Disables route caching for bridging and DLSw. Route caching is the process of converting broadcast frames to specifically routed frames (SRFs) using the entries in the NetBIOS name cache.

Example: `disable route-caching`

```
Route caching is                      OFF
```

Enable

Enables duplicate frame filtering or route caching.

Syntax:

enable duplicate-filtering

route-caching

duplicate-filtering

Enables duplicate frame filtering for bridging. Duplicate frame filtering is always enabled for DLSw. You cannot enable and disable it.

Example: `enable duplicate-filtering`

```
Duplicate frame filtering is          ON
```

route-caching

Enables route caching for bridging and DLSw. Route caching is the process of converting broadcast to specifically routed frames (SRFs) using the NetBIOS name cache.

Example: `enable route-caching`

```
Route caching is                      ON
```

List

Displays various types of cache entries, filter configuration, general configuration information, or statistics on other things.

Syntax:

list filters

general

filters Displays whether or not frame type filtering is on or off for bridging. Use the **set filters** command to turn these filters on or off.

Example: `list filters`

```
Bridge name conflict filtering is      OFF
Bridge general bcast filtering is      OFF
Bridge trace control filtering is      OFF
```

general

Displays the current NetBIOS caching and filtering configuration.

Example: `list general`

```
Bridge-only Information:

Bridge duplicate filtering is         OFF
Bridge duplicate frame filter t/o     1.5 seconds

Route caching is                      OFF
Significant characters in name         15
Max local name cache entries          500
Duplicate frame detect timeout        5.0 seconds
Best path aging timeout              60.0 seconds
Reduced search timeout                1.5 seconds
Unreferenced entry timeout           5000 minutes
```

Set

Sets name caching parameters, turns frame type filtering on or off for bridging, adjusts duplicate frame filtering timers and frame retry timers.

Syntax:

set cache-parms

filters

general

cache-parms

Sets name caching parameters that apply to bridging or switching.

Example: `set cache-parms`

```
Significant characters in name [15]?
Best path aging timeout value in seconds [60.0]?
Reduced search timeout value in seconds [1.5]?
Unreferenced entry timeout value in minutes [5000]?
Max nbr local name cache entries [500]?
Max nbr remote name cache entries [100]?

Cache parameters set
```

Significant characters in name

Determines whether the router considers 15 or 16 characters when it looks up the NetBIOS name. If you enter 15, the router ignores the 16th character. If you select 16, the router includes the 16th character when it looks up cache entries.

The default is 15.

Best path aging timeout

Amount of time the router considers the address and route for a name cache entry to be the best path to that station. When this timer expires, the router deletes the name cache entry and attempts to discover a new best path for the NetBIOS name.

To determine the best path, the router considers transmission time between nodes on all possible routes connecting those nodes, as well as largest frame size. The router does not consider a path suitable if it cannot accommodate the largest NetBIOS frame that could be transmitted over the path.

The default is 60 seconds. The range is 1.0 to 100000.0 seconds.

Reduced search timeout

When the router receives a Name-Query, Status-Query, or Datagram during the timeout period, it carries out a search based on current NetBIOS name cache information.

If the router receives a duplicate frame after this timer expires, it assumes the previous route is not longer valid and it widens its search. The router forwards the duplicate frame to both bridges and DLS. DLS broadcasts the corresponding SSP message to all possible DLS partners.

The default is 1.5 seconds. The range is 1.0 to 100.0 seconds.

Unreferenced entry timeout

The router keeps a name that is not referenced in its cache for this length of time before deleting it. If the cache fills up, the router removes entries sooner.

The default is 5000 minutes. The range is 1 to 100 000 minutes.

Max nbr local name cache entries

Maximum number of locally-learned entries the router saves in the name cache.

The default is 500. The range is 100 to 30 000. You can lower this value to save router memory. To optimize memory usage, processor usage, and the amount of broadcast traffic, set the number of local name cache entries as close as possible to the total number of NetBIOS stations (servers and clients) that are active on this router's local bridge network.

Max nbr remote name cache entries

Maximum number of remotely-learned entries, group name entries, and unknown entries that the router saves in the name cache.

The default is 100. The range is 100 to 30 000. You can lower this value to save router memory. To optimize memory usage, processor usage, and the amount of broadcast traffic, set the number of remote name cache entries to the number of remote NetBIOS servers that are to be accessed by NetBIOS clients on this router's local bridge network, plus about 25%.

filters Turns frame-type filtering for bridging on or off.

Example: `set filters`

```
Filter Name Conflict frames? [No]: y
Name conflict filtering is             ON
Filter General Broadcast frames? [No]:
General broadcast filtering is         OFF
Filter Trace Control frames? [No]:
Trace control filtering is             OFF
```

general

Sets the duplicate frame timeout, duplicate frame-detect timeout, and the command frame retry count and timeout.

Example: `set general`

```
ATTENTION! Setting Duplicate Frame Filter Timeout to zero...
disables duplicate frame checking!
Duplicate frame filter timeout value in seconds [1.5]?
Duplicate frame detect timeout value in seconds [5.0]?
General parameters set
```

Duplicate frame filter timeout

Applies only to bridged traffic if duplicate filtering is enabled. During this timeout period, the router filters all duplicate frames it receives.

The range is 0.0 to 100.0 seconds. Zero disables duplicate frame checking. The default is 1.5 seconds.

Duplicate frame-detect timeout

Applies to both bridged and DLSw traffic. Amount of time during which the router saves entries in its duplicate frame filter database. When this timer expires, the router creates new entries for new frames that it receives.

The range is 0.0 to 100.0 seconds. The default is 5 seconds.

Command frame retry count

Applies only to DLSw traffic.

Number of duplicate NetBIOS UI frames the target DLSw router sends to its locally attached LAN. These frames are sent at intervals specified by the command frame retry timeout.

The range is 0 to 10. The default is 5.

Command frame retry timeout

Applies only to DLSw traffic. This is the interval at which a neighbor DLSw router retries sending duplicate NetBIOS UI frames to its local bridge network.

The range is 0.0 to 10.0 seconds. The default is 0.5 seconds.

NetBIOS Monitoring Commands

Chapter 4. Network Management Support for Multiple Bridge Instances

When you are defining SNMP community names, use the **add community** command at the `SNMP Config>` command prompt. Specify an alphanumeric character string from 1 to 31 characters in length as the community name.

When you are performing a MIB query with a MIB browser and you want to obtain MIB information related to a specific bridge instance, specify the community name with a two-digit numeric designation added. The numeric designation identifies the bridge instance with which you are working. For example:

- If your community name is *public*, then bridge instance 1 can be accessed using *public*, or *public01*.
- Other bridge instances can be accessed using *public* with a two-digit numeric designation in the range of [02 to 24].

You should note that this numeric designation will limit the SNMP agent community name to a maximum of 29 characters if you want SNMP access to multiple bridge instances.

Also, using a community name with the numeric designation added to reference any MIB other than the bridge MIB will have no affect.

© Copyright IBM Corp. 1996, 1999

Chapter 5. LEC Persistence

LEC Persistence allows a LEC to immediately rejoin its ELAN over a backup interface in the event of the failure of the primary ATM interface to which it is bound. The LEC connects to the same LES it was connected to over the primary ATM interface and uses the same MAC address it had been using. These values are not altered based on the configuration. For example, the LEC will not recontact the LECS to find its LES or use the burned-in address on the backup ATM interface, if those were the configured actions. The LEC's configuration information is otherwise preserved. The LE_ARP cache is also preserved, and if the addresses in it can be re-verified, the associated Data Direct VCCs are automatically re-established.

Configuring a Backup ATM Interface for a LEC

Use the **config** command at the `LE Client Config>` prompt to access the appropriate Ethernet LEC interface number, or use the **network** cor

Table 11. LAN Emulation Client Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available).
ARP-Configuration	Allows you to configure the LE-ARP configuration for the ATM Forum-compliant client
IP-Encapsulation	Sets the IP encapsulation as Ethernet (type X'0800') or IEEE (802.3 with SNAP). Applies only to Ethernet LECs.
List	Lists the LAN Emulation Client configuration.
QoS-Configuration	Gets you to the `LEC QoS Config` prompt from which you can configure Quality of Service.
1 Set 1	Sets the LAN Emulation Client parameters, including backup interface and automatic switchback.
Exit	Returns you to the previous command level.

Only a discussion of the **set** command is included here. Refer to *8371 Networking Multilayer Ethernet Switch Software User's Guide and Configuration Reference*, GC30-9688-00 for a description of all LEC commands.

Set

Use the **set** command to set LE Client parameters.

Syntax:

set
- arp-aging-time
- arp-cache-size
- arp-queue-depth
- arp-response-time
- auto-config
- 1 backup *atm-net#*
- best-effort-peakrate
- bus-connect-retries
- conn-completion-time

© Copyright IBM Corp. 1996, 1999

control-timeout
data-direct-timeout
data-direct-vcc-mode
elan-name
esi-address
flush-timeout
forward-delay
forward-disconnect-timeout
frame-size
initial-control-timeout
lecs-atm-address
les-atm-address
mac-address
multicast-send-avg
multicast-send-peak
multicast-send-type
multiplier-control-timeout
path-switch-delay
reconfig-delay-min
reconfig-delay-max
retry-count
1 selector
1 switchback
trace
unknown-count
unknown-time
vcc-timeout

arp-aging-time

Sets ARP aging time. This is the maximum time that a LEC will maintain an entry in its LE_ARP cache in the absence of a verification of that relationship. A larger aging time may result in a faster session setup time, but may also use more memory and reacts slower to changes in network configuration.

Valid Values:

An integer number of seconds in the range of 10 to 300.

Default Value:

300

Example:

```
LEC Config> set arp-aging-time 200
```

arp-cache-size

Sets the number of entries in the ARP cache. The size of the ARP cache limits the number of simultaneous data direct VCCs. Larger ARP caches require more memory, but permit the client to simultaneously converse with a larger number of destinations.

Valid Values:

An integer number in the range of 10 to 65535.

Default Value:

5000

Example:

```
LEC Config> set arp-cache-size 10
```

arp-queue-depth

Sets the maximum number of queued frames per ARP cache entry. The LEC queues frames when switching the data path from the Multicast Send VCC to a Data Direct VCC. Frames passed to the LEC for transmission will be discarded if the queue is full. A larger queue requires more memory, but results in fewer discarded frames during the data path switch.

Valid Values:

An integer number in the range of 0 to 10.

Default Value:

5

Example:

```
LEC Config> set arp-queue-depth 10
```

arp-response-time

Sets expected ARP response time. This value controls how frequently an unanswered LE ARP request is retried. Larger values result in fewer LE ARPs, which causes less traffic and possibly increase the amount of time before a Data Direct VCC is established.

Valid Values:

An integer number of seconds in the range of 1 to 30.

Default Value:

1 second

Example:

```
LEC Config> set arp-response-time 20
```

auto-config

Specifies whether this LEC uses LECS auto-config mode. Specify YES or NO. The LEC may contact the LECS to obtain the address of its LES and various other configuration parameters.

Valid Values:

If YES, then you do not have to configure the ATM address of the LES.

If NO, then you *must* configure the ATM address of the LES using the **set les-atm-address** command as described on page 59.

Default Value:

NO

Example:

```
LEC Config> set auto-config yes
```

backup *atm-net#*
Sets the ATM net number of the backup ATM interface to be used as the ATM interface for the LEC in case of the primary ATM interface failure. This backup ATM interface can be concurrently functioning as the primary ATM interface for other LECs.

best-effort-peakrate
Sets the Best Effort Peak Rate. Used when establishing best effort multicast send connections.

The maximum peak rate depends on the maximum data rate of the ATM device.

Specify an integer from 1 to the maximum peak rate in Kbps (the definition is the maximum data rate) as follows:

- If ATM maximum data rate is 25 Mbps, the maximum peak rate is 25,000 Kbps.
- If ATM maximum data rate is 155 Mbps, the maximum peak rate is 155,000 Kbps.

Valid Values:
An integer number in the range of 1 - device maximum data rate.

Default Value:
155000

Example:

```
LEC Config> set best-effort-peakrate 24000
```

bus-connect-retries
This parameter sets the maximum number of times that the LEC will attempt to reconnect to the BUS before returning to the initial state.

Valid Values:
0 - 2

Default Value:
1

connection-completion-time
Sets the connection completion time. This is the time interval in which data or a READY_IND message is expected from a calling party.

When a Data Direct VCC is established to the client, the LEC expects data or a READY_IND message within this time period. The LEC will not transmit frames over a Data Direct VCC established to it until receiving data or a READY_IND. This parameter value controls the amount of time which passes before the LEC issues a READY QUERY (in hopes of receiving a READY_IND). Smaller values lead to faster response times, but also to unnecessary transmissions.

Valid Values:
An integer number of seconds in the range of 1 to 10.

Default Value:
4

Example:

```
LEC Config> set connection-completion-time 5
```

control-timeout

This parameter sets the maximum cumulative control timeout of a request.

A current timeout value is initialized to the value of ***initial-control-timeout***. If a response to a request is not received within the current timeout value, the current timeout is multiplied by the value of the ***multiplier-control-timeout*** and the request is reissued. Each time the current timeout value expires, this process is repeated until the current timeout value exceeds the value of ***control-timeout***.

Valid Values:

An integer number of seconds in the range of 10 to 300.

Default Value:

30

Example:

```
LEC Config> set control-timeout 100
```

data-direct-timeout

Specifies the timeout value for the data direct VCC. This parameter limits the time the Data Direct VCCs are left up without the LEC having a connection to the LES/BUS.

Valid Values:

10 - 300 seconds

Default Value:

30

data-direct-vcc-mode

Specifies whether persistent Data Direct VCC mode is enabled or disabled. When the Data Direct VCC mode is enabled, if the LEC loses its connection to the LES/BUS, the Data Direct VCCs are not dropped and the reconnect timeout timer is started.

Valid Values:

yes or no

Default Value:

no

elan-name

Specifies name of the ELAN that the LEC wishes to join. This is the ELAN name sent to the LECS in the configure request (if the LEC autoconfigures) or to the LES in the join request. The LECS or LES may return a different ELAN name in the response.

Valid Values:

Any character string length of 0 - 32 bytes.

Default Value:

Blank

Note: A blank name (0 length string) is valid.

Example:

```
LEC Config> set elan-name FUZZY
```

esi-address

Sets the ESI portion of the LEC's ATM address.

Specify the ESI portion (octets 13 through 19) of the LEC's ATM address. The ESI and selector combination of the LEC must be unique among all LAN emulation components on the device.

Valid Values:

Any 12 hexadecimal digits.

Default Value:

Burned-in ESI

Example:

```
set esi
Select ESI
   (1) Use burned in ESI
   (2) 11.22.33.44.55.66

Enter selection [1]?
```

flush-timeout

Sets the flush timeout. This is the time limit to wait to receive the LE_FLUSH_RESPONSE after the LE_FLUSH_REQUEST has been sent before taking recovery action. During recovery, any queued frames are dropped and a new flush request is sent.

When switching from the multicast send to a data direct data path, the client sends a flush request over the multicast send VCC. Until a flush response is received, or until the path switch delay expires, frames are queued for the destination.

Valid Values:

An integer number of seconds in the range of 1 to 4.

Default Value:

4

Example:

```
LEC Config> set flush-timeout 3
```

forward-delay

Sets the forward delay. Entries in the LE ARP cache must be periodically re-verified. The forward delay time is the maximum amount of time a remote entry may remain in the cache during a network topology change. Larger aging times may result in stale (invalid) entries, but also cause less re-verification traffic.

Valid Values:

An integer number of seconds in the range of 4 to 30.

Default Value:

15

Example:

```
LEC Config> set forward-delay 10
```

forward-disconnect-timeout

This parameter sets the amount of time that a LEC will wait after losing its last Multicast Forward VCC from the BUS before returning to the initial state. This delay permits the BUS to attempt to reconnect to the client without returning to the initial state.

Valid Values:

10 - 300 seconds

Default Value:
60

frame-size
Sets the frame size.

The value specified for frame-size must be equal to or less than the value specified for ATM max-frame using the ATM INTERFACE> **set max-frame** command.

Valid Values:
1516

4544

9234

18190

Default Value:
If the ELAN type is token ring, the default is 4544. If the ELAN type is Ethernet, the default is 1516.

Example:

```
LEC Config> set frame-size 4544
```

initial-control-timeout
This parameter sets the value of the initial control timeout used in the control timeout algorithm described o n page 57.

Valid Values:
1 - 10

Default Value:
5

Example:

```
LEC Config> set initial-control-timeout 10
```

lecs-atm-address
Specifies the ATM address of the LECS.

If the client is set to auto configure, it attempts to connect to a LECS. If it is unable to connect to a LECS, then it may try another LECS ATM address. The LECS ATM addresses that are tried, in order, are:
1. This configured LECS address
2. Any LECS address obtained through ILMI
3. The well-known LECS address defined by the ATM Forum.

No default is provided.

Note: This command should be entered on one command line. It is shown here on two lines because of spacing.

Example:

```
LEC Config> set lecs-atm-address
39.84.0F.00.00.00.00.00.00.00.00.00.01.10.00.5A.00.DE.AD.01
```

les-atm-address
Sets the LES ATM address. This command may be optional or required depending upon the setting of lecs-auto-config as described in the **set auto-config** command on page 55.
- If auto-config is YES, the les-atm-address is not configurable.

- If auto-config is NO, then the les-atm-address is required.

Specify the ATM address of the LES. No default is provided.

Note: This command should be entered on one command line. It is shown here on two lines because of spacing.

Example:

```
LEC Config> set les-atm-address
      39.84.0F.00.00.00.00.00.00.00.00.00.01.10.00.5A.00.DE.AD.02
```

mac-address

Sets the MAC address for this LE client. You *may* specify that the client use the burned-in MAC address of the ATM interface, or you may specify a different MAC address. If you have two clients that are bridged together, they should use different MAC addresses.

This MAC address is registered with the LES when the client joins the ELAN.

Valid Values:

Any valid MAC address.

Default Value:

none

Example:

```
LEC Config> set mac-address
  Use adapter address for MAC? [No]
  MAC address []: 10.00.5a.00.00.01
```

multicast-send-avg

Sets the multicast send VCC average rate in Kbps. Used by the LEC for reserving bandwidth on the VCC to the BUS. It specifies the forward and backward sustained cell rate used when setting up a reserved bandwidth multicast send VCC.

This parameter is only applicable when the multicast-send-type is reserved bandwidth. If multicast-send-avg equals multicast-send-peak, then a constant bit rate (CBR) multicast send is signalled. Otherwise, a variable bit rate (VBR) multicast send is signalled. Multicast-send-avg must be less than or equal to multicast-send peak.

A reserved bandwidth multicast send VCC may improve data transfer rates in congested networks, but reserving bandwidth and not using it wastes network resources.

When the multicast-send-type is reserved, then multicast-send-avg and multicast-send-peak must be specified.

Example:

```
LEC Config> set multicast-send-avg 4000
```

multicast-send-peak

Sets the multicast send peak rate in Kbps. Used by LEC for reserving bandwidth on the VCC to the BUS. It specifies the forward and backward peak cell rate used when establishing a reserved bandwidth multicast send VCC.

This parameter is only applicable when the multicast-send-type is reserved bandwidth. If multicast-send-avg equals multicast-send-peak, then a

constant bit rate (CBR) multicast send is signalled. Otherwise, a variable bit rate (VBR) multicast send is signalled. Multicast-send-avg must be less than or equal to multicast-send peak.

A reserved bandwidth multicast send VCC may improve data transfer rates in congested networks, but reserving bandwidth and not using it wastes network resources.

When the multicast-send-type is reserved, then multicast-send-avg and multicast-send-peak must be specified.

Example:

```
LEC Config> set multicast-send-peak 155
```

multicast-send-type

Sets the multicast send type. Specifies the method used by the LEC when establishing the multicast send VCC.

If multicast-send-avg equals multicast-send-peak, then a constant bit rate (CBR) multicast send is signalled. Otherwise, a variable bit rate (VBR) multicast send is signalled. Multicast-send-avg must at least equal multicast-send peak.

A reserved bandwidth multicast send VCC may improve data transfer rates in congested networks, but reserving bandwidth and not using it wastes network resources.

When the multicast-send-type is reserved, then multicast-send-no and multicast-send-peak must be specified.

Valid Values:

Best Effort or Reserved

Default Value:

Best Effort

Example:

```
LEC Config> set multicast-send-type best-effort
```

multiplier-control-timeout

This parameter sets the value of the control timeout multiplier used in the control timeout algorithm described on page 57.

Valid Values:

2 - 5

Default Value:

2

Example:

```
LEC Config> set multiplier-control-timeout 5
```

path-switch-delay

Sets the path switch delay.

The LEC must ensure that all frames sent through the BUS to a destination have arrived at the destination before it can start using a Data Direct VCC. This is accomplished using the flush protocol, or by waiting path-switch-delay seconds after sending the last packet to the BUS. Smaller values improve performance, but may result in out-of-order packets in a heavily congested network.

Valid Values:

An integer number of seconds in the range of 1 to 8.

Default Value:

6

Example:

```
LEC Config> set path-switch-delay 5
```

reconfig-delay-min

This parameter sets the minimum delay time when LEC returns to the initial state. This value must be ≤ ***reconfig-delay-max***.

Valid Values:

1 - the value of ***reconfig-delay-max***

Default Value:

1

Example:

```
LEC Config> set reconfig-delay-min  5
```

reconfig-delay-max

This parameter sets the maximum delay time when LEC returns to the initial state. This value must be ≥ ***reconfig-delay-min***.

Valid Values:

1 - 10

Default Value:

5

Example:

```
LEC Config> set reconfig-delay-max 9
```

retry-count

Sets the retry count. This is maximum number of times that the LEC retries an LE_ARP_REQUEST for a specific frame's LAN destination. If no ARP response is received after the specified number of retries, then the entry is purged from the LE ARP cache.

Valid Values:

0, 1, or 2

Default Value:

1

Example:

```
LEC Config> set retry-count 2
```

selector

Specifies the selector portion of the client's ATM address. The combination of ESI and selector must be unique among all LANE components on the device. By default, a unique selector is selected for the configured ESI.

Valid Values:

Any octet, in hexadecimal, that is not in use by another LANE component with the same ESI.

Example:

```
LEC Config> set selector 01
```

switchback
Specifies whether automatic switchback is enabled or disabled.

If enabled (*yes*), the LEC will automatically switch back to the primary ATM if the primary interface becomes available while the LEC is operating over the backup ATM interface.

If disabled (*no*), the LEC will continue to operate over the backup ATM interface even if the primary ATM interface becomes available. You can force the LEC to switch back to the primary ATM interface by issuing the **switchback** command from the `talk 5 LEC+` command prompt.

Also if disabled (*no*), the LEC will switch back to the primary ATM interface is the primary interface is available and the backup interface fails while the LEC is operating over the backup interface.

If both the primary and backup ATM interfaces fail, the LEC will begin operating over the interface which becomes available first.

Valid Values:
yes or no

Default Value:
no

trace Enables tracing for the LEC. To perform packet tracing, three steps are required:
1. Enable packet tracing system (under ELS)
2. Enable tracing on the LEC subsystem (under ELS)
3. Enable packet tracing on the desired LECs (using this command).

Valid Values:
Yes or No

Default Value:
No

unknown-count
Sets the unknown frame count. This is the maximum number of frames for a specific unicast MAC address or route descriptor that may be sent to the BUS within the time specified by the unknown-time parameter. Larger values decrease the number of discarded frames while increasing the load on the BUS.

Valid Values:
An integer number of frames in the range of 1 to 255.

Default Value:
10

unknown-time
Sets the unknown frame time. This is the time interval during which the maximum number of frames for a specific unicast MAC address or route descriptor (specified by the unknown-count parameter) may be sent to the BUS. Larger values increase the number of discarded frames while decreasing the load on the BUS.

Valid Values:
An integer number of seconds in the range of 1 to 60.

Default Value:
1

Example:

```
LEC Config> set unknown-time 5
```

vcc-timeout

Sets the VCC timeout. Data direct VCCs over which no traffic has been sent for this period of time should be released.

Valid Values: 0 to 31536000 seconds (1 year).

Default Value: 1200

Note: This parameter is meaningful only for SVC connections.

Example:

```
LEC Config> set vcc-timeout 1000
```

Index

© Copyright IBM Corp. 1996, 1999

P

S

U

V

Readers' Comments — We'd Like to Hear from You

8371 Networking Multilayer Ethernet Switch
Enhancements to Release 1.0 of the IBM 8371

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	☐	☐	☐	☐	☐

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	☐	☐	☐	☐	☐
Complete	☐	☐	☐	☐	☐
Easy to find	☐	☐	☐	☐	☐
Easy to understand	☐	☐	☐	☐	☐
Well organized	☐	☐	☐	☐	☐
Applicable to your tasks	☐	☐	☐	☐	☐

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? ☐ Yes ☐ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name _____ Address _____

Company or Organization _____

Phone No. _____

Readers' Comments — We'd Like to Hear from You

Cut or Fold
Along Line

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape

IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Design & Information Development
Department CGF/Bldg. 656
PO Box 12195
Research Triangle Park, NC 27709-9990

NO POSTAGE
NECESSARY

IBM®

Fold and
Tape **Please do not staple** Fold
and Tape

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

Spine information:

8371 Networking Multilayer
Ethernet Switch

8371 Release 1.0 Enhancements