Release Notes
IBM Nways Multiprotocol Switched Services (MSS) Server Operational Code Version 1 Release 1.1

IBM Corporation (Part Number 86H2884, EC E48799)

These release notes contain information available after January 1997 about the IBM Nways Multiprotocol Switched Services (MSS) Server product and supplements information formally published in the Version 1, Release 1.1 manuals.

These release notes contain the following sections:

Chapter 1, “General Changes, Procedures, and Restrictions” on page 1-1
Chapter 2, “Command Line and Web Configuration Interface” on page 2-1
Chapter 3, “Configuration Program Restriction” on page 3-1
Chapter 4, “Changes for the MSS Command Line Interface Vol. 1 - SC30-3818” on page 4-1
Chapter 5, “Changes for the MSS Command Line Interface Vol. 2 - SC30-3819” on page 5-1
Chapter 6, “Changes for the MSS Server Service Manual - GY27-0354” on page 6-1

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

AIX IBM OS/2

Other company, product, and service names, which may be denoted by a double asterisk (**), may be trademarks or service marks of others.

Chapter 1. General Changes, Procedures, and Restrictions

Latest Information and Quick Guide

You can get the latest MSS information and the MSS Quick Guide on the World Wide Web at URL: `http://www.networking.ibm.com/nes/nesswitc.htm`

Hardware

Slot Restriction

You cannot place a FDDI card in slot 1 of the 8210; slot 1 is currently reserved for ATM cards only.

Available Adapters

There are other adapters that can be used with the 8210 besides the ATM and FDDI adapters that ship with the 8210. For information about the available adapters, contact your IBM representative or call IBM for a “Request for Price Quotation” (RPQ).

Obtaining the MAC Address of a FDDI Adapter

To obtain the MAC address for a FDDI adapter in the 8210:

1. Make sure the 8210 is configured.
2. Do one of the following:

   a. Enter **talk 5**
   b. Enter **net intf#**, where **intf#** is the number that the 8210 assigned to the FDDI adapter.
   c. Enter **list**. The list command will display the MAC address of the adapter.

   a. Enter **talk 5**
   b. Enter **interface intf#**, where **intf#** is the number that the 8210 assigned to the FDDI adapter. This command provides you with the MAC address of the FDDI adapter, the upstream and downstream MAC addresses for the neighboring adapters, and other parameters such as frame counts, port states and error counts.

Using MSS Release 1.1 with 8260 Hubs

If you plan to use MSS release 1.1 with an 8260 Hub, you must upgrade the 8260 to version 2.5 or later for LAN emulation clients to obtain the LECS address from the 8260 through ILMI.

ILMI LECS address retrieval from the 8260 by the MSS R1.1 requires the 8260 CPSW code to be at 2.5 or later.

Notes:

1. MSS Release 1.0 is compatible with 8260 versions 2.4.3 and earlier.
2. The MSS does not support non-zero VPI connections. If you are using VPI connections between an MSS and an 8260 Hub, make sure the Hub is configured correctly for the MSS.
3. 8260 CPSW version 2.5.1 corrects ILMI LECS address retrieval compatibility problems with all versions of the MSS.

Software

ATM ARP Configuration Restriction

Important

Before configuring an ATM ARP Client on an ATM adapter in the 8210, make sure that the ATM adapter is installed in the 8210. Configuring an ATM ARP Client to an adapter that is not installed can cause the 8210 to halt.

IP Host Support

All IP clients that use IPHOST to communicate with the MSS must use the lowest numbered bridge port that is configured for source route bridging.

Bridging Considerations

The current manuals have incorrect statements about bridging and RFC 1483 bridging. The following are the corrections:

1. Bridging and routing a single protocol over a single interface using RFC 1483 bridging does not currently work. This will be corrected at a later date.
2. Protocols are automatically bridged on a MSS/8210 interface, if bridging is configured for that interface. However, if a protocol address is defined on the bridge port interface, then that protocol will only be routed on that interface.
3. If you want to perform RFC 1483 bridging and routing of the same protocol on an ATM interface, do the following:
   a. Configure RFC 1483 bridging on the physical ATM Interface.
   b. Add a virtual ATM interface on the Physical ATM Interface.
   c. Add a protocol address on the virtual ATM interface in order to enable RFC 1483 routing.

IBM LAN Emulation Client (ILEC) Restrictions

If you experience a problem with an IBM LEC joining an IBM ELAN, it might be due to a mismatch between the IBM LES frame size and the MSS 8210 ATM interface frame size. To correct this problem, ensure that the IBM LEC's Physical ATM interface has a SDU size that is greater than or equal to the IBM LES's Max Frame Size. Also note:

- The default for the IBM LES's Max Frame size is 18200.

- Any value set for the Max SDU size for the ATM Interface sets an upper bound on the maximum frame size of the ELANs defined on the interface.
- A setting of 18200 for the ATM frame size might adversely impact MSS 8210 buffer sizes as well as their availability.
- Forward and backward peak cell rates on the IBM LEC's might also have to be adjusted should you change the system defaults.

Chapter 2. Command Line and Web Configuration Interface

Deleting Interfaces

If interfaces are deleted using the command line or web configuration interface, you **must** save that configuration and reboot the MSS 8210 before you execute any on-line informational or status commands, such as *list* or *interface*.

Note: Failure to follow this procedure will cause problems ranging from erroneous information being displayed to a disruption of network traffic.

Configuring ELS

You can only configure ELS from either the command-line or web configuration interfaces. If you use the configuration program to retreive a configuration, the program will preserve any ELS settings that were configured in the device at the time of retrieval. If you make changes with the command-line or web interface before you send the configuration in the configuration program to the device, the configuration program's ELS settings will overlay the settings in the device.

If you begin a configuration with the configuration program for a device, you should not allow any configuration updates to that device through the command-line or web configuration interfaces.

Using an AIX Workstation With a Redundant ARP Server

To use an AIX workstation with a redundant ARP server in an 8210 network:

1. Make sure that the filesets for the ATM adapter on the AIX workstation are at AIX version 4.1.5. If the workstation is not running AIX 4.1.5 or the filesets are not at level 4.1.5, install APAR number IX64179 and proceed with the next step.
2. Install APAR IX65006. This will bring the filesets to 4.1.5.2 from 4.1.5.

TFTP Web Interface Restriction

You cannot use TFTP functions from the HTML Interface. However, you can still use TFTP from the command line interface.

Chapter 3. Configuration Program Restriction

Attention

The configuration program you use to configure an Nways device must match the software that resides on the device you are configuring.

Note: The configuration program for Release 1 PTF 1 can be used to configure operational code for Release 1 PTF2 and Release 1 PTF 3.

Incompatability

The configuration program is not supported on OS/2 Version 4.

Note: To obtain the best performance from the configuration program, limit the number of concurrent processes running on the workstation.

Chapter 4. Changes for the MSS Command Line Interface Vol. 1 - SC30-3818

Changes to the Config Process Chapter

Added Information

Add the following information to the chapter, “The Config Process and Commands”.

CONFIG Commands

This section describes each of the CONFIG commands. Each command includes a description, syntax requirements, and an example. The CONFIG commands are summarized in Table 4-1.

After accessing the CONFIG environment, enter the configuration commands at the `Config>` prompt.

Table 4-1 (Page 1 of 2). CONFIG Command Summary

Command	Function
? (Help)	Lists the CONFIG commands or lists the options associated with specific commands.
Add	Adds an interface to the router configuration, or a user to the router.
Boot	Enters Boot CONFIG command mode.
Change	Changes a user’s password or a user's parameter values associated with this interface. Also changes a slot/port of an interface.
Clear	Clears configuration information.
Delete	Deletes an interface from the router configuration or deletes a configured user.
Disable	Disables login from a remote console, system memory dumping and rebooting, or a specified interface.
Enable	Enables login from a remote console, enables modem use, enables system memory dumping and rebooting, or enables a specified interface.
Event	Enters the Event Logging System configuration environment.
Feature	Provides access to configuration commands for independent router features outside the usual protocol and network interface configuration processes.
List	Displays system parameters, hardware configuration, a complete user list.
Network	Enters the configuration environment of the specified network.
Patch	Modifies the router’s global configuration.
Protocol	Enters the command environment of the specified protocol.
Qconfig	Initiates the Quick Config process.

Table 4-1 (Page 2 of 2). CONFIG Command Summary

Command	Function
Set	Sets system-wide parameters for buffers, host name, inactivity timer, packet size, prompt level, location, and contact-person.
System	Retrieves dumps.
Time	Keeps track of system time and displays it on the console.
Unpatch	Restores patch variables to default values.
Update	Updates the current version of the configuration.
Write	Writes the current configuration information to the non-volatile memory.

? (Help)

Use the **?** (**help**) command to list the commands that are available from the current prompt level. You can also enter a **?** after a specific command name to list its options.

Syntax: ?

Example:

```
?
ADD
BOOT
CHANGE
CLEAR
DELETE
DISABLE
ENABLE
EVENT
FEATURE
LIST
NETWORK
PATCH
PROTOCOL
QCONFIG
SET
SYSTEM
TIME OF DAY PARAMS
UNPATCH
UPDATE
WRITE
```

Example:

```
list ?
devices
configuration
patches
users
v25-bis-address
```

Set

Use the **set** command to configure various system-wide parameters.

Syntax: set
- contact-person . . .
- data-link . . .
- down-notify . . .
- global-buffers
- hostname
- inactivity-timer
- input-low-water
- location . . .
- packet-size
- prompt
- receive-buffers

contact-person *sysContact*

Sets the name or identification of the contact person for this managed SNMP node. There is a limit of 80 characters for the *sysContact* name length.

This variable is for information purposes only and has no effect on router operation. It is useful for SNMP management identification of the system.

Example: `set contact-person nautilus`

Select the data link type for a serial interface.

down-notify *interface# # of seconds*

Allows the user to specify the number of seconds before declaring an interface as being down. The normal maintenance packet interval is 3 seconds, and it takes four maintenance failures to declare the interface as down.

The **set down-notify** command is used primarily when tunneling LLC traffic over an IP network using OSPF. If an interface goes down, OSPF cannot detect it fast enough because of the length of time that it takes for an interface to be declared down. Therefore, LLC sessions would begin to timeout. You can set the down-notify timer to a lower value, allowing OSPF to sense that an interface is down quicker. This enables an alternate route to be chosen more quickly, which will prevent the LLC sessions from timing out.

Note: If the **set down-notify** command is executed on one end of a serial link, the same command must be performed at the other end of the link or the link may not come up and stay up.

Interface#

The number of the interface you are configuring.

# of seconds

The down notification time value that specifies the maximum time that will elapse before a down interface is marked as such. Large values will cause the router to ignore transient connection problems, and smaller values will cause the router to react more quickly. The range of values is 1 to 300 seconds and the default is 0, which sets the 3-second period. Setting the down notification time to 0 will restore the default time for that interface.

The **list devices** command will show the down notification time setting for any interface that has the default value overridden.

Example: `set down-notify 4 3`

global-buffers *max#*

Sets the maximum number of global packet buffers, which are the packet buffers used for locally originated packets. The default is to autoconfigure for the maximum number of buffers (up to 1000). To restore the default, set the value to 0. To display the setting for global-buffers, use the **list configuration** command.

Example: `set global-buffers 30`

hostname

Adds or changes the router name. The router name is for identification only; it does not affect any router addresses. The name must be:

- Less than 78 characters and is case sensitive

Example: `set hostname sales`

inactivity-timer *# of min*

Changes the setting of the Inactivity Timer. The Inactivity Timer logs out a user if the remote or physical console is inactive for the period of time specified in this command. This command affect only consoles that require login. The default setting of 0 turns the inactivity timer off, indicating that no logoff is performed, no matter how long a console remains inactive.

Example: `set inactivity-timer 3`

input-low-water *interface # low # of receive buffers*

Allows you to configure the value of the low number of receive buffers, or packets, on a per-interface basis, thus overriding the default values.

The memory allocation strategy changes to conserve buffers when the number of free buffers is equal or less than the low or low-water mark value. When a packet is received, and the current value of the interface is less than the low water value, then that packet is eligible for flow control (dropping).

The range of values is 1 to 255. The default is both platform and device specific. Setting the value to 0 restores the autoconfigured default.

Interface # is the number of the interface you are configuring. *Low # of receive buffers* is the low water value.

Lowering the value will make it less likely that packets from this interface will be dropped when sent on congested networks. However, lowering the value may negatively affect performance if it drops packets to the extent that the receive queue is frequently empty. Raising the value has the opposite effect.

Type the **QUEUE** or **BUFFER** command at the GWCON prompt (**+**) to show the low setting.

Example: `set input-low-water 4 7`

location *sysLocation*

Sets the physical location of an SNMP node. There is a limit of 80 characters for the *sysLocation* name length. This variable is for information purposes only and has no effect on router operation. It is useful for SNMP management identification of the system.

Example: `set location atlanta`

packet-size *max packet size in bytes*

Establishes or changes the maximum size of a packet buffer.

Attention: Use this command only under direct instructions from your service representative. ***Never*** use it to reduce packet size – ***only*** to increase it.

Example:

```
set packet-size
```

prompt *user-defined-name*

Adds a user-defined name as a prefix to all operator prompts, replacing the hostname.

The user-defined-name can be any combination of characters, numbers, and spaces up to 80 characters. Special characters may be used to request additional functions as described in Table 4-2.

Example:

```
set prompt
What is the new MOS prompt [ ]? AnyHost 99
AnyHost 99 Config>
```

Table 4-2. Additional Functions Provided by the Set Prompt Command

Special Characters	Function Provided by the Set Prompt Command

$n	Displays the hostname. This is useful when you want the hostname included in the prompt. For example:
	`Config> set prompt`
	`What is the new MOS prompt [ ]? $n`
	`hostname:: Config>`

$t	Displays the time. For example:
	`Config> set prompt.`
	`What is the new MOS prompt [ ]? $t`
	`02:51:08[GMT-300] Config>`

$d	Displays the current date-month-year. For example:
	`Config> set prompt.`
	`What is the new MOS prompt [ ]? $d`
	`26-Feb-1997 Config>`

$v	Displays the software VPD information in the following format: `program-product-number Feature xxxx Vx Rx.x PTFx RPQx`
$e	Erases one character *after* this combination within the user-defined prompt.
$h	Erases one character *before* this combination within the user-defined prompt.
$_	Adds a carriage return to the user-defined prompt.
$$	Displays the $.

Note: You can combine these commands. For example:

```
Config> set prompt.
What is the new MOS prompt [ ]? $n::$d
hostname::26-Feb-1997 Config>
```

receive-buffers *interface # max #*

Adjusts the number of private receive buffers for most interfaces. The range is 5 to 255.

Note: This command is not applicable for ISDN Primary Rate Interfaces. For ISDN PRI, the interface handler determines the value based on the number of dial circuits configured.

To restore the default, set the value to 0. The **set receive-buffers** command can be used to increase the receive performance of an interface. In addition, this command can be used to reduce flow control drops when the router is forwarding many packets from a fast interface to a slow interface. The effect of this command is visible on the GWCON **buffer** command.

Attention: Use this command only under direct instructions from your service representative.

Example: **`set receive-buffers 4 30`**

System

Use the **system** command to retrieve system dumps.

This command uses TFTP to send the memory image to a remote location, with a destination TFTP file address, path, and file name supplied by the user.

If memory dumping is disabled, the function is aborted and the following message is displayed:

```
Image file transfer aborted:  function disabled
```

If the memory file is not present on the hard disk, or if the hard disk has been removed, the function is aborted and the following message is displayed.

```
Image file transfer aborted:  image file not found
```

Syntax: system retrieve

Example: **`system retrieve`**

```
Config> system retrieve
Destination IP address [0.0.0.0] ?
Fully qualified destination path/file name [/tmp/dump.cmp] ?
The memory image file is 11.2 Mb long
Proceed? [No] :
```

Write

Use the **write** command to save a configuration to the router before reloading. If you fail to issue the write command and try to reload the router, you will be asked if you want to save the configuration. The configuration is saved in the next CONFIG on the hard disk in the bank you are currently using. If you are using FLASH, the configuration is saved in the next CONFIG in bank F.

Syntax: write

Example: **`write`**

```
Config> write
```

Changes to Configuring and Monitoring ELS Chapters

Added Information

Add the following into the chapter titled “Configuring ELS”.

Set

Use the **set** command to set the maximum number of traps per second, to set the timestamp feature, or to set tracing options for ATM devices.

Syntax: set pin . . .
timestamp . . .
trace . . .

pin *max_traps*

Use the **set pin** command to set the pin parameter to the maximum number of traps that can be sent on a per-second basis. Internally, the pin resets every tenth of a second. (One tenth of the number (*max_traps*) is sent every tenth of a second.)

Example: `set pin 100`

timestamp timeofday OR uptime OR off

Allows you to turn on message timestamping so that either the time of day or uptime (number of hours, minutes, and seconds, but no date, since the router was last initialized) appears next to each message. Set timestamp can also be turned off.

Use the **set timestamp** command to enable one of the following timestamp options.

Example: `set timestamp timeofday`

timeofday

Adds an HH:MM:SS prefix to each ELS message indicating the time of the occurrence during a 24-hour day.

uptime

Adds an HH:MM:SS prefix to each ELS message indicating the time of the occurrence during a 100-hour cycle. After 100 hours of uptime, the uptime counter returns to zero to begin another 100-hour cycle.

off

Turns off the ELS timestamp prefix.

trace

Use the **set trace** command to configure tracing options for ATM devices. When tracing options are configured from the monitoring console, the changes take effect immediately, and return to their previously configured settings when the device is rebooted.

Note: Only set tracing and disk shadowing on when instructed by service personnel.

Syntax: set trace decode
default-bytes-per-port
disk-shadowing
max-bytes-per-port

memory-trace-buffer-size
off
on
reset
stop-event
wrap-mode

decode *off/on*

Turns packet decoding on or off. Packet decoding is not supported by all components.

default-bytes-per-pkt *bytes*

Sets the default number of bytes traced. This value is used if a value is not specified by the component doing the tracing.

disk-shadowing *off / on* OR *record-size* OR *time-limit*

Turns disk shadowing on or off, sets the maximum trace file size, or sets the maximum time for disk-shadowing traces.

off / on Turns disk shadowing on or off. If disk shadowing is enabled, trace records are copied to the hard disk. The trace records are written as follows:

Note: Using disk shadowing with tracing will slow down your server in proportion to the number of events you are tracing. You should not trace a large number of events in a critical, operational network.

- If the active bank is Bank A, then the trace file is written to the /hd0/sys0/ subdirectory
- If the active bank is Bank B, then the trace file is written to the /hd0/sys1/ subdirectory
- If the device is booting from the network (from a remote server), then the trace file is written to the /hd0/network/ subdirectory.
- If active bank is Bank-F (flash memory), then the configuration program will display the message: "Active Bank is Flash Memory - Active Bank must be hard disk or network in order to disk-shadow." when you enable disk-shadowing.

Once a traced record is copied to the hard disk, it can no longer be viewed from the console.

Note: Disk shadowing should be set to OFF whenever the WRITE, TFTP software, RETRIEVE system dump, or COPY software commands are issued.

Example: `set trace off`

record-size Sets the record size for trace file records:

Valid Values 1024, 2048, or 4096 bytes
Default 2048 bytes

Notes:

1. If a trace file already exists, “Cannot change Record Size without first deleting the existing Trace File” is displayed and record size is not changed.
2. If you configure a record size and a trace file already exists, the trace will use the record size of the existing file.

Example: `set trace record-size 4096`

time-limit Sets the maximum time for disk-shadowing of traces:

Valid Values 1 - 72 hours
Default 24 hours

Note: Disk shadowing stops (tracing continues) after this time has elapsed. The actual time is reset to 0 when disk shadowing is turned on again.

Example: `set trace disk-shadowing time 36`

max-bytes-per-pkt *bytes*

Sets the maximum number of bytes traced for each packet.

memory-trace-buffer-size *bytes*

Sets the maximum size, in bytes, of the RAM trace buffer.

There is no default for this parameter.

Note: If you specify a size larger than the memory available in the device, you will receive an error message and be prompted to respecify this parameter.

off Disables packet tracing.
on Enables packet tracing.
reset Clears the trace buffer and resets all associated counters.

stop-event *event id*

Stops tracing when an event (event id) occurs. Enter either an ELS event id (for example: TCP.013) or “None.” “None” is the default. Tracing stops only if the display of the particular ELS event is enabled.

When a stop-event occurs, an entry is written to the trace buffer. The **view** command for this trace entry will display “Tracing stopped due to ELS Event Id: TCP.013.”

After tracing stops due to a stop-event, you must re-enable tracing with the **set trace on** command. (A restart will also re-enable tracing if enabled from the `ELS Config>` prompt.)

Example: `set trace stop-event TCP.013`

wrap-mode *off/on*

Turns the trace buffer wrap mode on or off. If wrap mode is on and the trace buffer is full, previous trace records will be overwritten by new trace records as necessary to continue tracing.

Notes:

1. To preserve the oldest trace records, set wrap mode off. This action causes the device to discard trace records after the memory buffer fills. The device increments the “Trace Errors” field for each trace record discarded.
2. To ensure the latest trace records, set wrap mode on. This action causes the device to overwrite the oldest records in the memory buffer with the newer records when the memory buffer fills. The device increments the “Trace Errors” field for each trace record overwritten.

Example 1: `set trace decode on`

Example 2: `set trace default-bytes-per-packet 64`

Example 3: `set trace off`

Added Information

Add the following into the chapter titled “Monitoring ELS”.

Files Trace TFTP

Deleted Information

Note: This command is not supported. Ignore any documentation in the base publications on this command.

Set

Use the **set** command to set the maximum number of traps per second, to set the timestamp feature, or to set the tracing options.

pin

Use the **set pin** command to set the pin parameter to the maximum number of traps that can be sent on a per-second basis. Internally, the pin resets every tenth of a second. (One tenth of the number *max_traps* is sent every tenth of a second.)

Syntax: set *pin max_traps*

Example: `set pin 100`

timestamp

Allows you to turn on message timestamping so that either the time of day or uptime (number of hours, minutes, and seconds, but no date, since the router was last initialized) appears next to each message, or to turn off message timestamping.

Note: If you turn on timestamping, you must remember to go back into the CONFIG process and set the router's date and time using the time command. Otherwise, all messages will come out with 00:00:00, or negative numbers in the hours, minutes, and/or seconds, for example 00:-4:-5.

Use the **set timestamp** command to enable one of the following timestamp options:

timeofday Adds an HH:MM:SS prefix to each ELS message indicating the time of the occurrence during a 24-hour day.

uptime Adds an HH:MM:SS prefix to each ELS message indicating the time of the occurrence during a 100-hour cycle of uptime for the router. After 100 hours of uptime, the uptime counter returns to zero to begin another 100-hour cycle.

off Turns off the ELS timestamp prefix.

Syntax: set timestamp timeofday OR uptime OR off

Example: `set timestamp timeofday`

trace

Use the **set trace** command to configure tracing options. When tracing options are configured from the monitoring console, the changes take effect immediately, and return to their previously configured settings when the device is rebooted.

Note: Only set tracing and disk shadowing on when instructed by service personnel.

Syntax: set trace

- decode . . .
- default-bytes-per-port . . .
- disk-shadowing . . .
- max-bytes-per-port . . .
- memory-trace-buffer-size . . .
- off
- on
- reset
- stop-event . . .
- wrap-mode . . .

decode *off* / *on*

Turns packet decoding on or off. Packet decoding is not supported by all components.

default-bytes-per-pkt *bytes*

Sets the default number of bytes traced. This value is used if a value is not specified by the component doing the tracing.

disk-shadowing *off* / *on* OR *record-size* OR *time-limit*

Turns disk shadowing on or off, sets the maximum trace file size, or sets the maximum time for disk-shadowing traces.

Note: Using disk shadowing with tracing will slow down your server in proportion to the number of events you are tracing. You should not trace a large number of events in a critical, operational network.

off / on

Turns disk shadowing on or off. If disk shadowing is enabled, trace records are copied to the hard disk. The trace records are written as follows:

- If the active bank is Bank A, then the trace file is written to the /hd0/sys0/ subdirectory
- If the active bank is Bank B, then the trace file is written to the /hd0/sys1/ subdirectory
- If the device is booting from the network (from a remote server), then the trace file is written to the /hd0/network/ subdirectory.
- If active bank is Bank-F (flash memory), then the configuration program will display the message: “Active Bank is Flash Memory - Active Bank must be hard disk or network in order to disk-shadow.” when you enable disk-shadowing.

Once a traced record is copied to the hard disk, it can no longer be viewed from the console.

Note: Disk shadowing should be set to OFF whenever the WRITE, TFTP software, RETRIEVE system dump, or COPY software commands are issued.

Example: `set trace off`

Turns disk shadowing on or off and sets the maximum trace file size. If disk shadowing is enabled, trace records

are copied to the hard disk. Once a traced record is copied to the hard disk, it is no longer viewable through the console.

record-size — Sets the record size for trace file records:

Valid Values: 1024, 2048, or 4096 bytes
Default: 2048 bytes

Notes:

1. If a trace file already exists, “Cannot change Record Size without first deleting the existing Trace File” is displayed and record size is not changed.
2. If you configure a record size and a trace file already exists, the trace will use the record size of the existing file.

Example: `set trace record-size 4096`

delete-file — Deletes the trace file (in the subdirectory associated with the active bank only).

Note: If disk shadowing is ON when the command is issued, “ Disk-shadowing must be set to OFF before trace file can be deleted” is displayed and the file is not deleted.

time-limit — Sets the maximum time for disk-shadowing of traces:

Valid Values: 1 - 72 hours:
Default 24 hours

Note: Disk shadowing stops (tracing continues) after this time has elapsed. The actual time is reset to 0 when disk shadowing is turned on again.

Example: `set trace disk-shadowing time 36`

max-bytes-per-pkt *bytes*
Sets the maximum number of bytes traced for each packet.

memory-trace-buffer-size *bytes*
Sets the maximum size, in bytes, of the RAM trace buffer. p.There is no default for this parameter.

Note: If you specify a size larger than the memory available in the device, you will receive an error message and be prompted to respecify this parameter.

off
Disables packet tracing.

on
Enables packet tracing.

reset
Clears the trace buffer and resets all associated counters.

stop-event *event id*
Stops tracing when an event (event id) occurs. Enter either an ELS event id (for example: TCP.013) or “None.” “None” is the default. Tracing stops only if the display of the particular ELS event is enabled.

When a stop-event occurs, an entry is written to the trace buffer. The **view** command for this trace entry will display “Tracing stopped due to ELS Event Id: TCP.013.”

After tracing stops due to a stop-event, you must re-enable tracing with the **set trace on** command. (A restart will also re-enable tracing if enabled from the `ELS Config>` prompt.)

Example: **`set trace stop-event TCP.013`**

wrap-mode *off/on*

Turns the trace buffer wrap mode on or off. When wrap mode is enabled and the trace buffer is full, previous trace records will be overwritten by new trace records as necessary to continue tracing.

Notes:

1. To preserve the oldest trace records, set wrap mode off. This action causes the device to discard trace records after the memory buffer fills. The device increments the “Trace Errors” field for each trace record discarded.
2. To ensure the latest trace records, set wrap mode on. This action causes the device to overwrite the oldest records in the memory buffer with the newer records when the memory buffer fills. The device increments the “Trace Errors” field for each trace record overwritten.

Example 1: **`set trace decode on`**

Example 2: **`set trace default-bytes-per-packet 64`**

Example 3: **`set trace off`**

Changes to Chapter 24. Monitoring LAN Emulation Services

New Information

Add the following to the section titled “LECS Policies Console Commands”

ELANS

Use the **ELANS** command to create, delete, list, and select ELAN parameters for the LECS.

These commands modify the current LE services and take effect immediately. These commands do not modify the static memory of the router and are lost on the next reload of the MSS Server.

Use the **Help** option to display **ELANS** help information.

Use the **Create** option to create an ELAN for the LECS from the ELAN configuration data. The configuration data must already exist in static memory. Creating the ELAN results in the creation of all LESs, TLVs, and policy values for that ELAN.

Use the **Delete** option to delete an ELAN from the LECS. The LESs, TLVs, and policy values of that ELAN are also deleted.

Use the **List** option to list an ELAN configuration for the LECS.

Use the **Select ELAN** option to enter into the LECS ELAN Details Console environment. In this environment, you work more closely with a particular ELAN.

You can:

- Use the **LES Create** option to create LES ATM address information from the configuration. Note that configuration data must already exist.

  Creation of the LES also creates all policy value information associated with that LES.
- Use the **LES Delete** option to delete a LES ATM address from the LECS. The policy value information associated with that LES is also deleted.
- Use the **LES Set Backup LES Address** option to change the ATM address of a backup LES.
- Use the **LES Set Primary LES Address** option to change the ATM address of a primary LES.

Use the **Statistics** option to display statistics for an ELAN for the LECS.

Example

```
LECS console+ policies
LECS policies console
LECS policies+ elans
LECS policies+ ?
     ?
     create
     delete
     list
     select elan
     statistics
LECS policies+ select elan
LECS policies select ELAN console
LECS policies select elan+ ?
     LES Create
     LES Delete
     LES set backup LES address
     LES set primary LES address
```

Chapter 5. Changes for the MSS Command Line Interface Vol. 2 - SC30-3819

Changes to Dynamic Protocol Filtering (VLAN)

The following changes occurred since the books were published.

Default Aging Timers

The defaults for the VLAN aging timers have changed to better match the different protocol characteristics. The new timer defaults are:

IP subnet 10 000 minutes

IPX network 10 minutes

NetBIOS 5 000 minutes

Required Static Configurations

You must statically configure VLAN ports in the following situations:

- Ports with devices with low network utilization.

  Devices such as printers, servers or routers on a port could lose connectivity because of low network utilization. To prevent "aging-out" of a port that defines a VLAN to such a device, configure the port statically; specify **always** when prompted to configure the VLAN on the port. For example:

  ```
  add ip
  IP address: [0.0.0.0]? 9.37.15.24
  Subnet Mask: [255.0.0.0]?
  Configure Specific Ports? [No]: yes
  Configure VLAN on port 1 (Include, Exclude, or Auto-detect) [A]? I
  Age (expiration in minutes, 0=infinity) [10000]
  Enable IP-Cut-Through from this VLAN? [Yes]:
  Enable IP-Cut-Through to this VLAN? [Yes]:
  Enable this filter? [Yes]:
  VLAN Name (32 chars max) []? Finance
  VLAN 'Finance' (IP subnet 9.0.0.0) successfully added
  ```

- An 8210 bridge port connected to IPX clients only.

  IPX clients do not know their network numbers. This prevents a VLAN from learning the association between the network number and the port number. Specify "always" when prompted to configure the VLAN for a bridge port connected to IPX clients only.

IP-Cut-Through Considerations

IP Cut-Through allows the establishment of data direct VCCs between stations on different IP subnets. IP Cut-Through is applicable in subnetted IP networks only. If stations are on different IP "nets", then data-direct VCCs cannot be established between them and a router must be used to forward traffic between those stations.

To use IP Cut-Through, the subnet mask in end-stations (typically just servers) should be shortened. That is, a 255.255.255.255 subnet mask is shortened to

255.255.255.0 to imply a 3-byte subnet and a 255.255.0.0 subnet mask implies a 2-byte subnet. Shortening the subnet mask will cause the end-station to ARP for the destination and establish a direct connection (VCC) to the destination (or intermediate LAN switch), maximizing network throughput. However, this configuration can produce the following side effects:

1. A large number of ARP entries can be created in end-stations with a shortened mask which in turn can increase their CPU utilization. If these end-stations are ATM-attached, the number of ATM connections (data-direct VCCs) will also increase.

   Therefore, the need for faster network throughput must be balanced against increased CPU utilization in the end-stations and increased VCC utilization in the ATM switches.

2. An end-station with a shortened mask could ARP for a destination that is not directly connected. For example, this can happen if the destination is on a different type of LAN or behind a router firewall. The only way to reach this destination is through a router but routers normally do not propagate ARPs between networks. To allow this scenario to work, the Proxy ARP function must be enabled in the router. This will cause the router to respond to the ARP and subsequent traffic will be sent to the router.

   To enable proxy ARP in the MSS, the following must be done in IP configuration. See *MSS Server Command Line Interface Volume 2*, Chapter 14, “Enabling ARP Subnet Routing” on page 14-6 for additional information.

   ```
   Config> protocol ip
   Internet protocol user configuration
   IP Config>enable arp-subnet-routing
   ```

   Proxy ARP is also known as Transparent Subnetting or ARP-Subnet routing. Refer to IETF RFC 1027 for a complete description of Transparent Subnetting.

Answering “Yes” to the `Enable IP-Cut-Through from this VLAN? [Yes]:` question will allow forwarding of IP traffic from devices on this VLAN to devices on other VLANs that have IP-Cut-Through reception enabled.

Information about SNMP MIBs

Added Information

Add the following to the the chapter titled “Configuring SNMP”.

SNMP Management of the MSS Server

The MSS Server provides a Simple Network Management Protocol (SNMP) interface to network management platforms and applications, such as IBM NetView for AIX and the Nways Campus Manager products.

SNMP is used for monitoring and managing IP hosts in an IP network and uses software called an SNMP agent to enable network hosts to read and modify some of the MSS Server's operational parameters. In this way, SNMP establishes network management for the IP community.

You need to consider the following aspects of SNMP when you configure SNMP for your MSS Server:

Community The community allows you to define the IP address of the SNMP management station that is allowed to access the information in the SNMP agent's Management Information Base (MIB). You define a community name for use in accessing the MIB.

Authentication The community name is used as an authentication scheme to prevent unauthorized users from learning information about an SNMP agent or modifying its characteristics.

This scheme involves defining one or more sets of MIB data (referred to as MIB views) and associating an access privilege (read-only, read-write), an IP mask, and a community name with each MIB view. The IP mask establishes which IP addresses can originate access requests for a given MIB view and the community name serves as a password that must be matched by the SNMP requests. The community name is included in each SNMP message and verified by the MSS Server SNMP agent. An SNMP request will be rejected if it does not provide the correct community name, does not match the IP mask, or attempts an access that is inconsistent with the assigned access privilege.

MIB Support A Management Information Base (MIB) defines operational variables.

A MIB is a virtual information store that provides access to management information. This information is defined as MIB objects which can be accessed and, in some cases, be modified using network management tools.

MSS Server provides a comprehensive set of standard and enterprise-specific MIBs for monitoring and managing resources

You can access readme files documenting MSS Server MIB support using the World Wide Web at URL:

ftp://ftp.nways.raleigh.ibm.com/

in the appropriate release level directory under /pub/netmgmt/MSS/

Trap Messages Trap messages are unsolicited messages sent from the SNMP agent in the server to an SNMP manager in response to a server or network condition, such as a server reload or network down.

Changes to Using, Configuring, and Monitoring NetBIOS

Added Information

Add the following to the chapter “Using, Configuring, and Monitoring NetBIOS”

Test (Monitoring only)

Allows testing of real NetBIOS names against the NetBIOS name list.

Syntax: test name-list

test name-list

Displays a list of NetBIOS name list entries (local or remote) that match the given NetBIOS name.

Example: `test name-list`

```
Enter up to 15 characters of NetBIOS name (no wild cards).
  Enter NetBIOS name []? LA_SERV01
Enter last character of NetBIOS name in hex [0]?

Name Qualifier    Type        IP Address
----------------  ----------  ---------------
LA_SERV*          INDIVIDUAL  20.2.1.3
```

Changes to NHRP

Using NHRP with LAN Emulation

If you want to use NHRP on the IBM 8210, you must configure all LECs with a unique locally administered MAC address (LAA). If you do not configure the LECs with unique LAAs, the NHRP shortcut capability to the corresponding switch or device will not work because:

- Traffic sent over an NHRP LANE shortcut VCC will contain the MSS Universally Administered (burned-in) MAC address as the source MAC address.
- Some network devices learn the association between the MAC address and the VCC from traffic the device has received. These devices then use the NHRP VCC to transmit data.
- If the MSS detects incoming traffic on an NHRP VCC, it will assume that an error condition has occurred and will shut down that VCC thus preventing any further shortcuts to that network device.

Note: By default, the MSS Server enables IBM LAN Emulation Extensions on NHRP, so you must either disable the extensions or configure the unique locally administered MAC address for each LEC.

Output of the NHRP LIST

Changed Information

The output of the NHRP LIST command has changed as follows:

List

Use the **list** command to list the NHRP configuration.

Syntax: list
Example: list

```
Box level NHRP enabled
   Explicit interface definitions override box level setting

Interfaces explicitly defined for NHRP
--------------------------------------
  Interface 0: ATM
    NHRP enabled

NHRP LANE Shortcut Interface:
-----------------------------------------------------
  Interface: 1  ESI: burned-in          Sel: auto
  Use Best Effort: no   (Data)
  Cell Rate(kbps):  Peak: 155000    Sustained: 155000
  ATM adapter's burned-in MAC address is used as source address

General Parameters
------------------
  Holding time:                           20 minutes
  Protocol Access Controls:               Use source and destination address
  When should NHC attempt shortcuts?:     Based on datarate
     Data-rate threshold:                 10 packets/second
  NHS allows shortcuts to ATMARP clients?: Yes

Cache Sizes
-----------
  Resolution cache:           512 entries
  Server purge cache:         512 entries
  Server registrations cache: 512 entries

Extension Usage
---------------
  Use NHRP Forward transit NHS record client extension: No
  Use NHRP Reverse transit NHS record client extension: No
  Use Responder Address client extension:               No
  Use LANE shortcuts extension:                         Yes

List of NHRP IP exclude records
-------------------------------
  # Address         Mask
  1 6.6.6.6         255.255.255.255
  2 5.5.5.0         255.255.255.0

Disallowed router-to-router shortcuts for IP
--------------------------------------------
    None
```

Chapter 6. Changes for the MSS Server Service Manual - GY27-0354

Chapter 6. Removal and Replacement Procedures

Changed Information

Change steps 4 through 9 in the section “Installing Operational Software on the Hard Drive” as follows:

4. Select the Utilities Menu from the System Management Services menu.

5. Select the Prepare Hard Disk option.

Respond **yes** to the prompts that initiate the hard disk formatting process.

6. The hard disk will be formatted and the system will restart.

7. The CORE (dump) file will be created, followed by the necessary directory structure. Do not abort this process or you will have to restart the Prepare Hard Disk process.

8. Choose Copy Remote Files from the Utilties menu. Download (via TFTP or XMODEM) a copy of the firmware to a file called PRECOVER.IMG.

9. Use Change Management to download the operational code images and associated config files to Banks A and B.

Appendix D. Firmware Error Codes

Changed Information

Add the following codes to the error code table.

Error Code	Physical Location	Software Subsystem	Explanation
00015504	System Board	Interrupts	Error occurred during dead-man timer tests
80000000	System Board	8260 Interface	Echo Response Test with 8260 failed

Appendix G. MSS Server Module LED Status Indicators

Changed Information

Change Appendix G as follows:

Table G-1 (page (G-2)

Change “Explanation” for “Adapter Ports 1 or 2, Green, On” to read:

An adapter is in the port, configured, enabled, and operational (Note 1).

Add a note at the end of the table to read:

Notes:

1. If there is an FDDI adapter in Port 2 (top slot), check the condition of the green and yellow LEDs on the FDDI adapter:

LED	Color	State	Explanation
FDDI adapter	Green	ON	If both green LEDs are ON, both ports are connected correctly to the FDDI hub or port in the network, there is a primary and redundant data path to the next FDDI hop, and data can be transmitted. If one green LED is ON (in either position), there is only one primary data path, and only one port is correctly connected to the next hop in the FDDI network. The other port could be faulty because: a. It is not connected or has a bad cable connection to the next FDDI port b. The next FDDI port in the network is faulty. When only one green LED is ON, the yellow LED is always OFF.
		OFF	There is no data path to the next hop in the FDDI network, or the adapter is not configured, enabled, or operational. When one (or two) FDDI adapter green LEDs is OFF, the yellow LED is ON.
	Yellow	ON	No data path is available. Neither port is connected to another valid FDDI port. This could be because: a. There is no cable connected. b. Incorrect cables are being used. c. The cables are placed in the wrong order to complete the correct data path needed for FDDI. d. The connecting FDDI port is faulty. e. Code is loaded but the adapter interface is not enabled. Perform the following wrap test procedure on the FDDI adapter ports to check the adapter before removing and replacing it.

Add a heading and procedure after the LED table to read:

FDDI Adapter Wrap Test

Perform the following steps to ensure that the FDDI adapter is OK before removing and replacing the adapter.

1. Insert and completely seat the ends of a small piece of optical fiber cable into the cable connectors on the FDDI adapter.
2. Observe the yellow LED.
   a. If it goes OFF, the adapter is functionally OK, and the problem is as indicated Table G-1. Contact your network administrator.
   b. If it remains ON, the adapter is faulty. Contact your network administrator or your service representative to remove and replace the faulty FDDI adapter (See “Removing the Adapter in Port 2 (Top Slot)”).