



8239 Release Notes

Operational Code Version 1.1 8/03/98

These release notes contain information related to the 8239 Token-Ring Stackable Hub. The major sections are:

- Enhancements
- Fixes
- Known Problems
- Current MIB Information
- Where to Go for Information
- Questions
- Using the Terminal Interface
- Operating Considerations
- Updating 8239 Operational Code
- Documentation Changes

For the latest product and documentation updates, check our website at <http://www.networking.ibm.com/support>.

Enhancements

None with this code release.

Fixes

Updating Operational Code

When 8239 Model 1 code is updated using the LOAD OPERATIONAL_CODE or REPLICATE OPERATIONAL_CODE terminal interface command and there are three or more Model 1s in the stack, the Model 1 initiating the update resets. This problem has been corrected. For more information about updating V1.0 operational code in a stack with three or more Model 1s, see "Loading New 8239 Operational Code" on page 16.

Private Traps

Some 8239-specific traps contained an incorrect trap type or specific trap type. This problem has been corrected.

Known Problems

Changing the Default Gateway

When the default gateway is set up or changed (using the SET IP terminal interface command or via BOOTP), a message is displayed on the terminal interface giving the IP address of the router that was added or deleted. At the end of this message, text enclosed in parentheses appears. **Action:** This text should be ignored. The default gateway **was** successfully added or deleted.

Loading the MIB

For information about problems loading the MIB, see "MIB Fails to Load" under "Current MIB Information."

Sending MIB II Traps via SNMP

In order to send MIB II traps to a trap receiver via SNMP, the community name for the trap receiver must be traps. To set the community name, enter the following terminal command: **set trap_community rmon/mib2 traps ip_address**

Current MIB Information

CD-ROM Contents

Under "Verifying the Shipment" in the *Setup and User's Guide*, it is stated that the 8239 MIB is contained on the CD. The MIB is no longer included on the CD. Download it from our website: <http://www.networking.ibm.com/support>.

IBM Private MIBs Supported by the 8239

The latest IBM 8239 MIB may be obtained from our website at <http://www.networking.ibm.com/support>.

MIB Fails to Load

The 8239 V1.0 MIB file (mib/ibm8239.mib) on the CD-ROM dated June, 1998, cannot be loaded by some MIB browsers. **Action:** The MIB file is no longer included on the CD-ROM. Download the current 8239 MIB from our website: <http://www.networking.ibm.com/support>.

MIB Version

Be sure you use the 8239 MIB V1.1 with operational code V1.1.

Where to Go for Information

Use this section for information about where to find:

- Code updates
- Product information
- Network management applications

Code Updates

The latest 8239 operational code may be obtained using either of these methods:

- Retrieve it from our website at <http://www.networking.ibm.com/support>.
- If the 8239 is under warranty, contact your reseller or call IBM. In the United States, call IBM at **1-800-772-2227**; in Canada, call IBM at **1-800-IBM-SERV (1-800-426-7378)**.
If the 8239 is not under warranty, call IBM at **1-800-IBM-SERV (1-800-426-7378)**.

Product Information

The latest versions of the following documentation may be obtained from our website at <http://www.networking.ibm.com/support>.

- *8239 Token-Ring Stackable Hub Setup and User's Guide*
- *8239 Token-Ring Stackable Hub Command Reference*
- *8239 Token-Ring Stackable Hub Quick Reference*
- *8239 Release Notes* (this document)

Network Management Applications

Network management for the 8239 is provided by the following Nways Network Management products:

For graphical device (element) management

- IBM Nways Workgroup Manager for Windows NT Version 1.1.2 or later
- IBM Nways Manager for AIX Version 1.2.2 or later - Campus Manager LAN component
- IBM Nways Manager for HP-UX Version 1.2 or later - Element Manager component

For remote network monitoring (RMON/RMON2/ECAM)

- IBM Nways Workgroup Remote Monitor for Windows NT Version 1.1 or later
- IBM Nways Manager for AIX Version 1.2 or later - Remote Monitor and Traffic Monitor components
- IBM Nways Manager for HP-UX Version 1.2 or later - Remote Monitor component

For media management using the IBM Token Ring Surrogate MIB

- IBM Nways Manager for AIX Version 1.2.2 or later - Campus Manager LAN component

The 8239 fully supports RMON, RMON 2 and ECAM. However, the versions of remote network monitoring applications mentioned above have varying levels of RMON, RMON 2, or ECAM support.

The latest information about these products can be obtained from our website at <http://www.networking.ibm.com/netmgt>.

Questions

To report problems or ask questions:

- If the 8239 is under warranty, contact your reseller or call IBM. In the United States, call IBM at **1-800-772-2227**; in Canada, call IBM at **1-800-IBM-SERV (1-800-426-7378)**.
- For warranty upgrade or post-warranty maintenance service, call IBM at **1-800-IBM-SERV (1-800-426-7378)**.

Using the Terminal Interface

This section contains information about logging on to the terminal interface and about configuration settings for the terminal emulation sessions. For more information, see the *8239 Setup and User's Guide*.

Login Name and Password

To use the terminal interface via Telnet or the EIA-232 port, you must enter a login name and password. The default administrator access login name is "admin" with no password. You should change the 8239 login password to a more secure password. If you forget your passwords associated with login names that have administrator access, contact IBM using the telephone numbers listed in "Questions."

Using the 8239 EIA-232 Port

To connect a workstation directly to the 8239's EIA-232 port, a null-modem cable is required. To connect a modem to the 8239's EIA-232 port, use a standard EIA-232 cable. Configure your terminal emulation application with:

- 9600 bps
- No parity
- 8 data bits
- 1 stop bit
- No flow control
- VT100 emulation
- The communications port

Operating Considerations

This section contains information about these topics:

- Address-to-port mapping
- Configuration Report Server
- Ring in/ring out
- RMON
- Soft errors

Address-to-Port Mapping

When known external stations are not appearing in `network_map` (for example, in the `DISPLAY NETWORK_MAP ALL_STATIONS` command), the 8239's RMON ring station table may be full. To clear the RMON ring station table, issue the `CLEAR RMON RINGSTATION_ALL` terminal interface command to the 8239 Model 1. Once the Token Ring Neighbor Notification Process completes successfully, subsequent displays of the `network_map` will include all currently active stations.

Configuration Report Server

When the Configuration Report Server (CRS) surrogate agent on the 8239 Model 1 is active, it sends CRS Request MAC frames to all stations participating in the token-ring Neighbor Notification Process every 10 minutes and after NAUN changes occur. If a station does not respond to the CRS Request frame, the 8239 sends out the CRS Request MAC frames every minute; if this situation occurs, the `DISPLAY TR_SURROGATE CRS_STATION ALL` command identifies the MAC address that did not respond so that you can take further action.

Ring In/Ring Out

Be sure that both ends of the RI/RO cables are connected before enabling the RI and RO interfaces. Any of these interfaces that are not going to be used should be administratively disabled. The default administrative mode value for RI/RO is disabled.

RMON

RMON Tables

When an RMON table becomes full, new entries will not be added to the table. The RMON table must be deleted or cleared in order for the table to be automatically rebuilt based on current traffic data. RMON tables can be cleared through SNMP or the terminal interface. RMON 2 tables can only be cleared using SNMP.

Depending on your network configuration and network traffic characteristics, you may want to periodically delete or clear the RMON and RMON 2 tables. RMON events and alarms can be used to indicate when a table is full.

When deleting large RMON or RMON 2 tables, in-band connectivity to the 8239 Model 1 Management Interface may be lost temporarily. However, in-band connectivity to the Management Interface automatically resumes once the table deletion processing is completed. Other hub operations are not affected.

Table 1, Table 2 on page 6, and Table 3 on page 6 show the maximum number of entries for each RMON, RMON 2, and ECAM table.

Host Data Table	30 000
Host Top N Control Table	10
Matrix Data Table	18 000
History Data Table	1 164
History Control Table	10
Filter Entries	60
Channel Entries	40
Alarm Entries	60
Log Table	2 800
Event Table	150
Capture Buffer Packets	8 000
Capture Buffer Total Octets	1 048 576
Buffer Control Entries	16
Ring Station Table	300
Mac-Layer Statistics Table	1
Promiscuous Statistics Table	1
Source Routing Statistics Table	1

<i>Table 2. Maximum Number of Entries in Each RMON 2 Table</i>	
protocolDirTable	1 300
protocolDistControlTable	1
protocolDistTable	1 000
addressMapControlTable	3
addressMapTable	40 000
nlHostControlTable	3
nlHostTable	10 000
alHostTable	10 000
hlMatrixControlTable	3
hlMatrixSDTable	40 000
hlMatrixDSTable	40 000
hlMatrixTopNControlTable	4
hlMatrixTOPNTable	25 000
alMatrixSDTable	40 000
alMatrixDSTable	40 000
alMatrixTopNControlTable	4
alMatrixTopNTable	25 000
userHistoryControlTable	10
userHistoryObjectTable	16 per bucket
userHistoryTable	1 164
netConfigTable	1
trapDestTable	300

<i>Table 3. Maximum Number of Entries in Each ECAM Table</i>	
hlStatsTable	2 048
hlHostTable	200
hlMatrixTable	256
protocolDirectoryTable	256
atTable	1 024

RMON Protocols

This section lists the protocols supported by operational code version 1.0 or later. It contains these sub-sections:

- Protocol overview
- Predefined protocols
- User-defined protocols

Protocol Overview: Each entry in the protocol directory table on a device represents a protocol that the device can decode and count. These protocols can be standard or custom.

The entries within the table are indexed by each data-link layer protocol: first, by MAC-layer protocol and then, by each level of encapsulated protocol. For example:

- llc** Denotes the LLC (802.2) protocol
- llc.ip** Denotes IP running over LLC protocol
- llc.ip.udp** Denotes UDP running over IP over LLC
- llc.ip.udp.snmp** Identifies the application-level protocol SNMP operating over LLC

The MAC-layer protocols consist of:

- ether2** Ethernet II
- llc** LLC (802.2) protocol
- snap** Subnetwork access protocol
- vsnap** Pseudo-protocol associated with snap
- ianaAssigned** Those protocols that do not conform to the format of the other link-layer branches
- anyLink** A wildcard protocol, identified by the prefix "*", that aggregates all link-layer protocols by their layer 2 encapsulated protocol. For example, if IPX is the layer 2 encapsulated protocol, the denotation is:

**.ipx ~ ether2.ipx + llc.ipx + snap.ipx + ianaAssigned.ipx, where ~ indicates equivalence.*

The anyLink protocol is enabled as a default for operational code version 1.0 or later.

Predefined Protocols: This section gives predefined protocols supported by operational code version 1.0 or later. Encapsulated protocols are listed alphabetically and the MAC-layer protocols over which they run are marked. For example, the 802.1-bridge protocol appears as both

*.802.1-bridge

llc.802.1-bridge

<i>Table 4 (Page 1 of 3). Protocol Names</i>	
Protocols	Protocol Name
802.1-bridge	802.1D Bridge Spanning Tree
aarp	AppleTalk Address Resolution Protocol
adsp	AppleTalk Data Stream Protocol
aep	AppleTalk Echo Protocol
arp	Address Resolution Protocol
atalk	AppleTalk Datagram Delivery (short and long headers)
atp	AppleTalk Transaction Protocol
bootpc	Bootstrap Protocol Client
bootps	Bootstrap Protocol Server
ccmail	Lotus cc-Mail
dec-diag	DEC Diagnostic
dns	Domain Name Service
drp	DECnet (Phase IV) Routing Protocol

Table 4 (Page 2 of 3). Protocol Names

Protocols	Protocol Name
ftp	File Transfer Protocol Control Port
ftp-data	File Transfer Protocol Data Port
gopher	Internet Document Search and Retrieval
icmp	Internet Control Message Protocol
idp	XNS Internet Datagram Protocol
igrp	Inter-Gateway Routing Protocol
ip	Internet Protocol
ipx	Internet Packet Exchange
nbp	AppleTalk Name Binding Protocol
lat	DECnet Local Area Transport
lavc	Local Area Vax Cluster
mop	DECnet Maintenance Operations Protocol
nbt_data	NetBIOS Datagram Support
nbt_name	NetBIOS Name Support
nbt_session	NetBIOS Session Support
netbeui	LAN Manager Netbeui
netbios-3com	3Com NetBIOS
news	Network Window Service
nfs	Network File Service
nntp	Network News Transfer Protocol
notes	Lotus Notes
nov-bcast	Novell Broadcast
nov-diag	Novell Diagnostic
nov-echo	Novell Echo
nov-error	Novell Error-Handler
nov-ncp	Novell Netware Core Protocol
nov-netbios	Novell NetBIOS
nov-pep	Novell Packet Exchange Protocol
nov-rip	Novell Routing Information Protocol
nov-sap	Novell Service Advertising Protocol
nov-sec	Novell Security
nov-spx	Novell Sequenced Packet Exchange
nov-watchdog	Novell Watchdog
nsp	DECnet Network Services Protocol
ntp	Network Time Protocol
ospf	Open Shortest Path First
pop3	Post Office Protocol Version 3
printer	Printer

Table 4 (Page 3 of 3). Protocol Names

Protocols	Protocol Name
rcmd	Remote Command
rexec	Remote Process Execution
rlogin	Remote Login
router	Local Routing Processes (520/upd)
rtmp	AppleTalk Routing Table Maintenance Protocol
rwho	Remote Who
smb	Microsoft Server Message Block
smtp	Simple Mail Transfer Protocol
sna	Systems Network Architecture
snmp	Simple Network Management Protocol
snmptrap	Simple Network Management Protocol TRAPS
sunrpc	SUN Remote Procedure Call
tcp	Transmission Control Protocol
telnet	Network Virtual Terminal
tftp	Trivial File Transfer Protocol
udp	User Datagram Protocol
varp	Banyan VINES Address Resolution Protocol
vecho	Banyan VINES Data Link Level Echo
vicp	Banyan VINES Internet Control Protocol
vip	Banyan VINES Internet Protocol
vipc	Banyan VINES InterProcess Communications
vipc-dgp	Banyan VINES Unreliable Datagram Protocol
vipc-rdp	Banyan VINES Reliable Datagram Protocol
vrtp	Banyan VINES Routing Update Protocol
vspp	Banyan VINES Sequenced Packet Protocol
www-http	World Wide Web HTTP
X	X Windows
xns-echo	XNS Echo
xns-error	XNS Error-Handler
xns-pep	XNS Packet Exchange Protocol
xns-rip	XNS Routing Information Protocol
xns-spp	XNS Sequenced Packet Protocol
zip	Zone Information Protocol

Table 5 (Page 1 of 5). Predefined Protocols

MAC-Layer Protocol					
*	llc.	snap.	vsnap_ether2.	ianaAssigned.	Encapsulated Protocols
√	√				802.1-bridge
√		√			aarp
√		√			arp
√		√	√		atalk
√		√	√		atalk.adsp
√		√	√		atalk.aep
√		√	√		atalk.atp
√		√	√		atalk.atp.zip
√		√	√		atalk.nbp
√		√	√		atalk.rtmp
√		√	√		atalk.snmp
√		√	√		atalk.snmptrap
√		√	√		atalk.zip
√		√			dec-diag
√		√			drp
√		√			drp.nsp
√		√			idp
√		√			idp.xns-echo
√		√			idp.xns-error
√		√			idp.xns-pep
√		√			idp.xns-rip
√		√			ipd.xns-spp
√	√	√			ip
√	√	√			ip.icmp
√	√	√			ip.igrp
√	√	√			ip.ip
√	√	√			ip.ip.icmp
√	√	√			ip.ip.igrp
√	√	√			ip.ip.opsf
√	√	√			ip.ip.tcp
√	√	√			ip.ip.tcp.ccmil
√	√	√			ip.ip.tcp.dns
√	√	√			ip.ip.tcp.ftp
√	√	√			ip.ip.tcp.ftp-data
√	√	√			ip.ip.tcp.gopher
√	√	√			ip.ip.tcp.nbt_data
√	√	√			ip.ip.tcp.nbt_data.smb

Table 5 (Page 2 of 5). Predefined Protocols

MAC-Layer Protocol					
*	llc.	snap.	vsnap_ether2.	ianaAssigned.	Encapsulated Protocols
√	√	√			ip.ip.tcp.nbt_name
√	√	√			ip.ip.tcp.nbt_session
√	√	√			ip.ip.tcp.nbt_session.smb
√	√	√			ip.ip.tcp.news
√	√	√			ip.ip.tcp.nntp
√	√	√			ip.ip.tcp.notes
√	√	√			ip.ip.tcp.pop3
√	√	√			ip.ip.tcp.printer
√	√	√			ip.ip.tcp.rcmd
√	√	√			ip.ip.tcp.rexec
√	√	√			ip.ip.tcp.rlogin
√	√	√			ip.ip.tcp.smtp
√	√	√			ip.ip.tcp.snmp
√	√	√			ip.ip.tcp.snmptrap
√	√	√			ip.ip.tcp.telnet
√	√	√			ip.ip.tcp.www-http
√	√	√			ip.ip.tcp.X
√	√	√			ip.ip.udp
√	√	√			ip.ip.udp.bootpc
√	√	√			ip.ip.udp.bootps
√	√	√			ip.ip.udp.ccmil
√	√	√			ip.ip.udp.dns
√	√	√			ip.ip.udp.nbt_data
√	√	√			ip.ip.udp.nbt_data.smp
√	√	√			ip.ip.udp.nbt_name
√	√	√			ip.ip.udp.nbt_session
√	√	√			ip.ip.udp.nbt_session.smp
√	√	√			ip.ip.udp.notes
√	√	√			ip.ip.udp.ntp
√	√	√			ip.ip.udp.printer
√	√	√			ip.ip.udp.router
√	√	√			ip.ip.udp.rwho
√	√	√			ip.ip.udp.snmp
√	√	√			ip.ip.udp.snmptrap
√	√	√			ip.ip.udp.sunrpc
√	√	√			ip.ip.udp.sunrpc.nfs
√	√	√			ip.ip.udp.ftp

Table 5 (Page 3 of 5). Predefined Protocols

MAC-Layer Protocol					
*	llc.	snap.	vsnap_ether2.	ianaAssigned.	Encapsulated Protocols
√	√	√			ip.ip.udp.X
√	√	√			ip.ospf
√	√	√			ip.tcp
√	√	√			ip.tcp.ccmil
√	√	√			ip.tcp.dns
√	√	√			ip.tcp.ftp
√	√	√			ip.tcp.ftp-data
√	√	√			ip.tcp.gopher
√	√	√			ip.tcp.nbt_data
√	√	√			ip.tcp.nbt_data.smb
√	√	√			ip.tcp.nbt_name
√	√	√			ip.tcp.nbt_session
√	√	√			ip.tcp.nbt_session.smb
√	√	√			ip.tcp.news
√	√	√			ip.tcp.nntp
√	√	√			ip.tcp.notes
√	√	√			ip.tcp.pop3
√	√	√			ip.tcp.printer
√	√	√			ip.tcp.rcmd
√	√	√			ip.tcp.rexec
√	√	√			ip.tcp.rlogin
√	√	√			ip.tcp.smtp
√	√	√			ip.tcp.snmp
√	√	√			ip.tcp.snmptrap
√	√	√			ip.tcp.telnet
√	√	√			ip.tcp.www-http
√	√	√			ip.tcp.X
√	√	√			ip.udp
√	√	√			ip.udp.bootpc
√	√	√			ip.udp.bootps
√	√	√			ip.udp.ccmil
√	√	√			ip.udp.dns
√	√	√			ip.udp.nbt_data
√	√	√			ip.udp.nbt_data.smb
√	√	√			ip.udp.nbt_name
√	√	√			ip.udp.nbt_session
√	√	√			ip.udp.nbt_session.smb

Table 5 (Page 4 of 5). Predefined Protocols

MAC-Layer Protocol					
*	llc.	snap.	vsnap_ether2.	ianaAssigned.	Encapsulated Protocols
√	√	√			ip.udp.notes
√	√	√			ip.udp.ntp
√	√	√			ip.udp.printer
√	√	√			ip.udp.router
√	√	√			ip.udp.rwho
√	√	√			ip.udp.snmp
√	√	√			ip.udp.snmptrap
√	√	√			ip.udp.sunrpc
√	√	√			ip.udp.sunrpc.nfs
√	√	√			ip.udp.tftp
√	√	√			ip.udp.X
√	√	√		√	ipx
√	√	√		√	ipx.nov-echo
√	√	√		√	ipx.nov-error
√	√	√		√	ipx.nov-netbios
√	√	√		√	ipx.nov-netbios.notes
√	√	√		√	ipx.nov-netbios.smb
√	√	√		√	ipx.nov-pep
√	√	√		√	ipx.nov-pep.nov-bcast
√	√	√		√	ipx.nov-pep.nov-diag
√	√	√		√	ipx.nov-pep.nov-netbios
√	√	√		√	ipx.nov-pep.nov-netbios.notes
√	√	√		√	ipx.nov-pep.nov-netbios.smb
√	√	√		√	ipx.nov-pep.nov-rip
√	√	√		√	ipx.nov-pep.nov-sap
√	√	√		√	ipx.nov-pep.nov-sap.notes
√	√	√		√	ipx.nov-pep.nov-sap.nov-ncp
√	√	√		√	ipx.nov-pep.nov-sec
√	√	√		√	ipx.nov-pep.nov-watchdog
√	√	√		√	ipx.nov-pep.smb
√	√	√		√	ipx.nov-pep.snmp
√	√	√		√	ipx.nov-pep.snmptrap
√	√	√		√	ipx.nov-rip
√	√	√		√	ipx.nov-spx
√		√			lat
√		√			lavc
√		√			mop

Table 5 (Page 5 of 5). Predefined Protocols					
MAC-Layer Protocol					
*	llc.	snap.	vsnap_ether2.	ianaAssigned.	Encapsulated Protocols
√	√				netbeui
√	√				netbeui.notes
√	√				netbeui.smb
√					netbios-3com
√	√				sna
√	√	√			vecho
√	√*	√			vip
√	√*	√			vip.varp
√	√*	√			vip.vicp
√	√*	√			vip.vipc
√	√*	√			vip.vipc.vipc-dgp
√	√*	√			vip.vipc.vipc-rdp
√	√*	√			vip.vrtp
√	√*	√			vip.vsp

Note: * These protocols running over LLC are displayed as *llc.vtr.vecho* and so on, where *vtr* is an additional protocol layer.

User-Defined Protocols: If you are using customized protocols or protocol encapsulations on your network, you may want to add these to your protocol directory using a management application such as IBM Nways Manager or IBM Nways Workgroup Remote Monitor.

With operational code version 1.0 or later installed on the 8239, you can specify at least 64 wildcard protocols or 256 non-wildcard protocols; see "Protocol Overview" on page 7 for a description of the anyLink or wildcard protocol.

Operational code version 1.0 or later supports a number of extensible protocols, as shown in Table 6, with the following exceptions:

- ipx is not extensible by either values 0 or 17
- llc is not extensible by odd-numbered children
- nov-sap, nsp, sunrpc, vip, vipc, and vsnap are not extensible

The maxchildren value shows the total number of child protocols that may be defined. This value is calculated irrespective of the encapsulation used. For example, *ether2.ip.upd* and *llc.ip.upd* would be counted as one child only.

Table 6 (Page 1 of 2). Extensible Protocols and maxChildren Values			
Protocol	maxChildren		
	Total	Pre-Defined	User-Defined
atalk	16	9	7
idp	8	5	3
ip	256	7	249
ip.ip	16	7	9

<i>Table 6 (Page 2 of 2). Extensible Protocols and maxChildren Values</i>			
Protocol	maxChildren		
	Total	Pre-Defined	User-Defined
ipx	256	5	249*
llc	256	8	120†
nov-pep	16	11	5
nov-spx	16	0	16
snap	32	14	18
tcp	64	22	42
udp	64	17	47
vipc-dgp	4	0	4
vipc-rdp	4	0	4
vspp	4	0	4
xns-pep	4	0	4
xns-spp	4	0	4
Notes:			
* ipx is not extensible by either values 0 or 17			
† llc is not extensible by odd-numbered children			

Soft Errors

The 8239 automatically detects and isolates faults that result in hard errors (beaconing) on the network. The 8239 cannot automatically resolve soft errors (such as ring purges, burst errors, and token errors) on the network. When configured, you can use the 8239 network management features like RMON or REM to detect or identify the occurrence of soft errors on the data network. Refer to the *Token-Ring Problem Determination Guide (SX27-3710)* for information about isolating soft errors.

Some faults in the Stack In/Out cable can cause soft errors on the control ring, resulting in connectivity problems between the hubs and unexpected Hub Up/Down traps. If you are experiencing unexpected Hub Up/Down traps, consider replacing the SI/SO cable.

Updating 8239 Operational Code

This section contains the following information:

- Obtaining 8239 operational code
- Loading 8239 operational code using XMODEM or TFTP
- Updating 8239 V1.0 to a later version with three or more Model 1s in the stack

Obtaining New 8239 Operational Code

The 8239 operational code is contained in a binary file. The files used for the 8239 Model 1 and the 8239 Model 2 are unique files. The Model 1 and Model 2 filenames have a format of m1r x y.opr and m2r x y.opr, respectively, where x is the release number and y is the version number.

The Model 1 operational code file, which contains both the Model 1 and Model 2 operational code, is loaded on a Model 1; all of the Model 1s and Model 2s in the stack will be updated with the code. The

Model 2 operational code file, which contains only the Model 2 operational code, is loaded on a Model 2; all of the Model 2s in the stack will be updated with the code. All 8239s in the same stack should run the same code level.

The most recent 8239 operational code can be obtained by either of these methods.

- Retrieving it from our website at <http://www.networking.ibm.com/support>.
- If the 8239 is under warranty, contact your reseller or call IBM. In the United States, call IBM at **1-800-772-2227**; in Canada, call IBM at **1-800-IBM-SERV (1-800-426-7378)**.

For warranty upgrade or post-warranty maintenance service, call IBM at **1-800-IBM-SERV (1-800-426-7378)**.

If you have a Model 1 in the stack, obtain the Model 1 operational code file; this file contains both the Model 1 and Model 2 operational code. If you have only Model 2s in the stack, obtain the Model 2 operational code file.

Loading New 8239 Operational Code

The Model 1 will update all Model 1s and Model 2s in the stack. The Model 1 operational code file is loaded on the Model 1 using either XMODEM or TFTP. After the code is loaded, the appropriate code is automatically copied to all of the other 8239 Model 1s and Model 2s in the stack. To start executing the new code, all of the 8239s in the stack must be reset.

The Model 2 will update only Model 2s in the stack. Load the Model 2 operational code file on the Model 2 using XMODEM. After the code is loaded, the code is automatically copied to all of the other 8239 Model 2s in the stack. To start executing the new code, all of the 8239 Model 2s in the stack must be reset.

Updating Using XMODEM

To load new code onto your Model 1 or Model 2 using XMODEM:

1. Put the file containing the new code on the workstation that connects to the 8239 EIA-232 port.
2. Log onto the 8239 using your terminal emulation software.
3. If your terminal baud rate has not been changed from the default value of 9600 bits per second, you may want to configure both the 8239 and the terminal emulation software for a higher baud rate so that the file transfer goes faster.
4. Issue the `LOAD OPERATIONAL_CODE XMODEM` command.
5. When the message *Ready to RECEIVE File in binary mode* appears, indicate to your terminal emulation software that the file transfer should start. Specify:
 - XMODEM or 1K-XMODEM for the protocol. 1K-XMODEM causes the file transfer to occur faster.
 - The filename of the file to be transferred.
6. After the file transfer is completed, the 8239 will automatically update the code on the appropriate hubs in the stack. Once the message *Code load complete* appears, the hubs can be reset at any time to execute the new code; for example, you can issue the `RESET_HUB ALL` command.

Updating Using TFTP

Code can be updated using TFTP on Model 1s only. The code transfer can be triggered through a terminal interface command or SNMP. Only the instructions for updating code using the terminal interface are described here.

1. Put the file containing the new code on your TFTP server. Make sure that the permission code for the file allows read-access for "others". For example, on AIX or UNIX systems, specify *chmod o+r FILE*, where *FILE* is the name of the file to be transferred.
2. Log onto the 8239 using either your terminal emulation software or Telnet.
3. Issue the `LOAD OPERATIONAL_CODE` TFTP command, specifying the TFTP server's IP address and the filename of the file to be transferred.
4. After the file transfer is done, the 8239 will automatically update the code on all other hubs in the stack. Once the message *Code load complete* appears, the hubs can be reset at any time to execute new code; for example, you can issue the `RESET_HUB ALL` command.

Updating 8239 V1.0 with Three or More Model 1s in the Stack

When there are three or more 8239 Model 1s in a stack running V1.0 operational code and a code update is performed, the Model 1 initiating the update may reset. This problem does not exist in V1.1, or later, operational code. To update the Model 1 from V1.0 to a later version, follow these steps:

1. Load the V1.1 or later code onto one of the Model 1s running V1.0.
2. If the Model 1 resets, issue the `REPLICATE OPERATIONAL_CODE` command on the Model 1 after it becomes operational; the rest of the Model 1s will then be updated with the new code.

Documentation Changes

This section contains additions or changes to the latest versions of the 8239 publications.

Documentation Corrections

8239 Setup and User's Guide

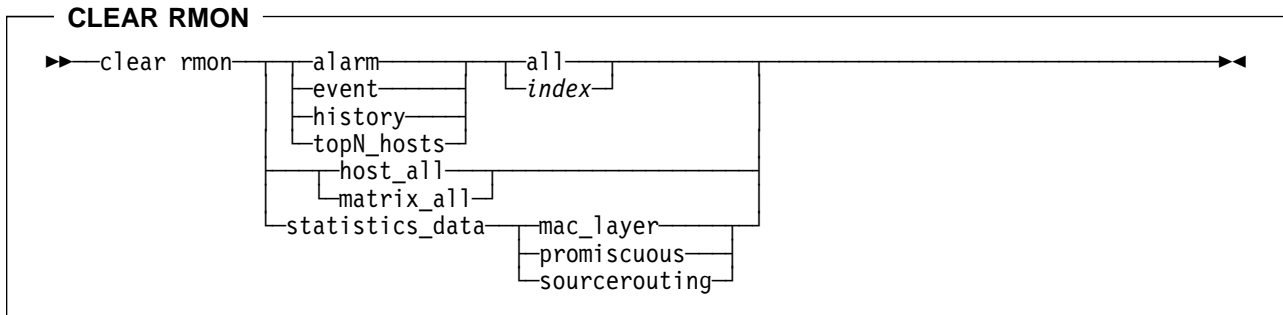
Configuration Parameters: Under "Configuration Parameters", the default values for "Ring In administrative mode" and "Ring Out administrative mode" are DISABLED, not UNWRAPPED.

Phone Number for Warranty Service: Under "Warranty Information", the phone number for warranty service in Canada should be **1-800-IBM-SERV (1-800-4426-7378)**.

SI/SO LEDs: Under "SI/SO LEDs", the green LED blinking on the SI/SO connector indicates a status of administratively wrapped, not unwrapped.

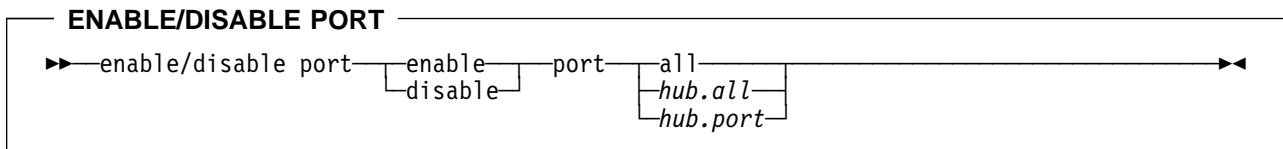
8239 Command Reference

CLEAR RMON command: Under "CLEAR RMON", the name of the **counter** parameter has been changed to **statistics_data**. Use this new documentation for the CLEAR RMON command:



- alarm** Specifies an RMON table.
- event** Specifies an RMON table.
- history** Specifies an RMON table.
- topN_hosts** Specifies an RMON table.
- host_all** Specifies an RMON table.
- matrix_all** Specifies an RMON table.
- ringstation_all** Specifies an RMON table.
- statistics_data** Specifies an RMON counter.
- mac_layer** Identifies the specific RMON statistic counter for this operation
- promiscuous** Identifies the specific RMON statistic counter for this operation.
- sourcerouting** Identifies the specific RMON statistic counter for this operation.
- all** Clears all entries from the specified RMON table.
- index* Is the RMON table entry. Use one of the DISPLAY RMON commands (ALARM_DATA, EVENT_DATA, CONTROL HISTORY, or CONTROL TOPN_HOSTS) to view table entry numbers.

ENABLE/DISABLE PORT command: The parameter **mode** listed in the *Command Reference* is not a valid parameter. Use this new documentation for the ENABLE/DISABLE PORT command.

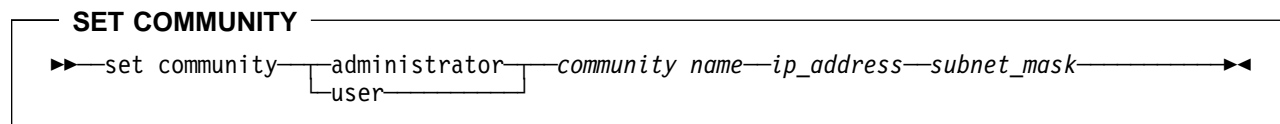


- all** Identifies this operation to be for all ports on all hubs in this stack.
- hub.all** Identifies all of the ports on the specified hub, where *hub* is a number from 1 to 8.
- hub.port** Identifies the port for this operation, where *hub* is a number from 1 to 8 and *port* is a number from 1 to 32.

ENABLE/DISABLE PORT_SETTING command: Under “ENABLE/DISABLE PORT_SETTING”, the default value of the **traps** parameter is enabled.

SCRIPT command: The **copy_to m** parameter makes a copy of commands but not the name.

SET COMMUNITY command: Under “SET COMMUNITY”, there are two additional parameters: **ip_address** and **subnet_mask**. Use this new documentation for the SET COMMUNITY command:



administrator Specifies that the community can issue any administrator-level commands.

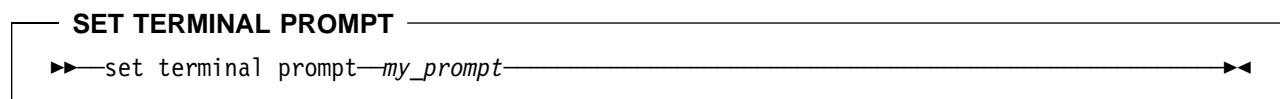
user Specifies that the community can issue any user-level commands.

community name Specifies the name (case sensitive) of the community to which this operation applies.

ip_address An IP address (or portion thereof) from which this device will accept SNMP packets with the associated community. The requesting entity’s IP address is ANDed with the specified **subnet_mask** before being compared to the specified **ip_address**. Note that if **subnet_mask** is set to 0.0.0.0, an **ip_address** of 0.0.0.0 matches all IP addresses. The format of **ip_address** is a series of 4 decimal bytes separated by periods, for example, 0.67.75.3. The default value is 0.0.0.0.

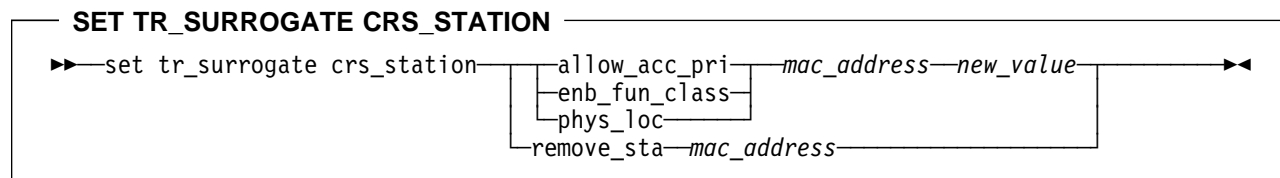
subnet_mask A mask to be ANDed with the requesting entity’s IP address before comparison with **ip_address** in the community table. If the result matches the **ip_address** in the community table, then the address is authenticated. The format is a series of 4 decimal bytes separated by periods, for example, 255.255.255.255. The default value is 0.0.0.0.

SET TERMINAL PROMPT command: The syntax diagram in the *Command Reference* does not show the variable **new_prompt**. Use this new documentation for the SET TERMINAL PROMPT command:



new_prompt Represents the prompt that appears during a terminal session, where **prompt** can be up to 15 characters. The default setting is **?=Help>**.

SET TR_SURROGATE CRS_STATION command: The **remove_sta** parameter does not accept a **new_value** parameter. Use this new documentation for the SET TR_SURROGATE CRS_STATION command:



Documentation Additions

The following sections contain information pertinent to the *8239 Token-Ring Stackable Hub Setup and User's Guide*.

Modem Connection

This section contains:

- General suggestions about using modems with the 8239
- Setting information for several specific modems

Modem Hints

- It is helpful to consider the modem as an extension of the EIA-232 terminal, rather than as a controller of the 8239. There are no *smart* requirements for interaction between the modem and the 8239. Such features can actually cause problems during the connection handshaking.
- Be sure to disable both software and hardware flow control. The 8239 will not try to communicate with the modem using any EIA-232 control lines, DTR, DSR, and so on; the modem should ignore these. Turning off all flow control is a one-step command with some modems, but with other modems, you may have to execute several commands to completely disable flow control.

Settings for Specific Modems

Sportster 14.4: Note that external switch settings take precedence over stored values after resetting the modem. Set the switches in this fashion, where *Down* = on:

1	Down
4	Down
8	Down
All others	Up

Use the following command string to set up the modem:

```
ATE0F1Q1&H0&R1S0=1
```

Be sure to save the results.

28.8 FaxModem V.34/V.32 bis: Note that external switch settings take precedence over stored values after resetting the modem.

Set the switches in this fashion, where *Down* = on:

1	Down
2	Down
4	Down
6	Down
8	Down
All others	Up

Use the following command string to set up the modem:

```
ATF1Q1&H0&R1S0=1
```

Be sure to save the results.

IBM 7855: Using the factory default settings, set up the modem with the following command:

```
ATE0Q1&D0\Q0\R0&S0S0=1
```

Be sure to save the results.

IBM 7858: Using the factory default settings, set up the modem with the following command:

```
ATE0Q1&D0&K0&U0S0=1
```

Be sure to save the results.

Terminal Interface

When a terminal interface command is issued, the command is displayed on the command line until execution of the command is completed. Be aware that traps may appear on the terminal while execution of a command is in process.

Up to 10 previously entered commands that have completed execution can be recalled, edited, if necessary, and then executed. To retrieve commands, simultaneously press:

- **Ctrl** and **R** to recall the last entered command
- **Ctrl** and **F** to go forward in the command history
- **Ctrl** and **B** to go backward in the command history

To edit a recalled command, press **Backspace** until you reach what needs changing, type the new information and press **Enter**.

Note: Commands can be recalled only if the command has completed execution. For example, if you enter `DISPLAY NETWORK_MAP ALL_STATIONS` and press **Esc** before the last entry is displayed, then the `DISPLAY NETWORK_MAP ALL_STATIONS` command will not be in the recall list.