IBM 8260 Nways Multiprotocol Switching Hub DMM and EC-DMM v5.25, RCTL v1.15, A/DMM v5.25/v1.15, E-MAC v3.0, HEMAC v2.10, T-MAC v4.00, HTMAC v2.10, and T-MAC v4.00 Release Note

IBM Corporation • (Part Number 42L2467) • February 1999

This release note summarizes management-related issues for IBM® products DMM, EC-DMM, E-MAC, HEMAC, T-MAC, HTMAC, Advanced/DMM Controller (A/DMM), and Fault-Tolerant Controller Module for the Distributed Management Module (DMM) Version v5.25.

Note: A/DMM Version v5.25 software includes all DMM Version v5.25 software functionality. Unless otherwise noted, references in this document to DMM Version v5.25 software also apply to the A/DMM Version v5.25 software.

This release note includes the following sections:

- Important Download Information
- Required DMM Memory Upgrade
- A/DMM Installation Issues
- New Features
- Corrected Problems
- Known Problems
- 8260 Switching Module Information
- New Command Support
- Important Network Management Application Consideration
- Operating Considerations
- Token Ring MAC Address-to-Port Security Issues
- Controller Module (8000-RCTL) Issues
- 8260 Module Code Versions.

Store this release note in the release note section of your 8260 Reference Library.

Important Download Information

This section describes important download information and includes the following topics:

- Recommended Download Procedure
- Downloading New Software
- Download Operating Considerations.

Recommended Download Procedure

Warning: You must upgrade the DMM memory (for Version v2.3 or earlier, you must upgrade to Version v3.01 or later) before you complete this procedure.

Before you upgrade the A/DMM, determine which controller is installed in the same hub and download the correct operating and boot code for that controller. If it is an 8260 Redundant Controller (RCTL), download RCTL operating code Version v1.15 and boot code Version v1.03. If it is an 8260 Advanced RCTL (ARCTL), download operating code Version v1.15 and boot code Version v1.04. RCTL operating code Version v1.15 allows the A/DMM to be elected master, and ensures consistent power management.

When you upgrade the DMM, EC-DMM, RCTL, or A/DMM and MAC Cards from earlier versions, download modules in the following order:

1. Download T-MAC or E-MAC code (boot code then operational, if applicable).
2. Download RCTL code (boot code then operational code, if applicable).
3. Download DMM code (boot code then operational code, if applicable).
4. Download HEMAC, if applicable. The DMM does not recognize the HEMAC card until the DMM has been upgraded to Version v3.01 or later.
5. Download HTMAC code (boot code then operational code, if applicable). The DMM does not recognize the HTMAC card until the DMM has been upgraded to Version v4.11 or later.
6. Download T-MAC TRchipset and/or HTMAC TRchipset, if applicable.

Warning: Modules may not function properly if you do not use the specified download order.

Note: Refer to the Installation Instructions that are shipped with the code upgrade kit, and follow the carefully detailed download instructions (for Out-of-Band Download).

Downloading New Software

Consider the following issues when you download new software to 8260 modules:

Note: Instructions for performing software downloads are contained in the 8260 *Distributed Management Module User's Guide* (Document Number SA33-0259). Follow these instructions carefully.

Warning: You must upgrade 8260 modules in a particular order. Refer to the section titled Recommended Download Procedure on page 2 of this document for more information.

1. Before you begin the download, remove 8350 Fiber Distributed Data Interface (FDDI) media modules with firmware prior to Version v3.00 from the hub. If there are FDDI media modules (running software versions prior to Version v3.00) in the hub, the DMM initiates a mastership election during downloads. This causes the download to fail and the module stays in Download mode.

   To remedy this situation:

   a. Remove any installed FDDI modules before you begin the download.

   b. Retry the download procedure.

   If the download failure causes you to lose in-band connectivity, repeat the download out-of-band.

   In general:

   a. When the DMM download mode fails repeatedly, retry the download.

   b. If the in-band download fails, try an out-of-band download. If the download still fails, call your service representative.

2. Before you download code to a TRMM prior to Version v3.3, set the TRMM to master. If you inadvertently download a TRMM without setting the TRMM to master, and the TRMM and DMM fail, reset both modules to correct the problem.

Download Operating Considerations

Consider the following issues when you download software:

1. After a hub reset, if you want the DMM to be assigned as master in a hub that contains an A/DMM, set the mastership priority of the A/DMM (by issuing the SET MODULE <*slot*>.<*subslot*> MASTERSHIP_PRIORITY command) to at least 2 less than the DMM mastership priority. This ensures that the DMM becomes the master module.

2. Upgrade boot code *before* operational code. Before you upgrade the operational code for any DMM or A/DMM, download the latest boot version of boot code. (This is required because versions of operational code may be too large to be supported by older boot codes.)

Required DMM Memory Upgrade

This section contains the following upgrade information:

- DMM and EC-DMM Memory Upgrade
- Checking for DMM RAM Upgrade
- Checking for DMM EEPROM Upgrade.

DMM and EC-DMM Memory Upgrade

If you are not running Distributed Management Module software Version v3.01 or later, the DMM (Feature Code 1000 only) and the EC-DMM (Feature Code 1100 only) require a memory upgrade.

Note: If you do not have a memory upgrade kit and are running DMM Version v2.3 or earlier, contact your IBM representative to order Feature Code 8932.

Checking for DMM RAM Upgrade

If you are running DMM Version v3.01, determine if you have the required amount of installed RAM by issuing the SHOW MODULE <*slot*>.1 VERBOSE command (where slot is the DMM slot). If the displayed CPU RAM Size (MB) is 5, then the RAM upgrade is already installed.

Note: For A/DMM Version v4.12 and later, the 'CPU RAM Size (Mb):' field displays '8'.

If you are running DMM Version v2.3 or earlier, to see if the RAM upgrade has been installed, remove the DMM from the hub and place it on an antistatic surface. Locate JP5 on the DMM. The installed RAM is located at this jumper. For detailed RAM installation instructions, refer to the document *IBM 8260 Distributed Management Module Memory Upgrade* (Part Number 29H4293) that is shipped with Feature Code 8932.

Checking for DMM EEPROM Upgrade

If you are running DMM Version v3.01, determine if you have the required amount of installed EEPROM by issuing the SHOW MODULE <*slot*>.1 VERBOSE command (where slot is the DMM slot). If the 'FLASH Memory (MB):' field displays 3, then the EEPROM upgrade is already installed.

Note: For A/DMM Version v4.12 and later, the 'FLASH Memory (Mb):' field displays 4 (or greater).

If you are running DMM Version v2.3 or earlier, determine if the memory upgrade kit has been installed on your DMM. To see if the EEPROMs have been installed, remove the DMM from the hub and check socket positions U4 and U11 on your module. If the sockets are empty, then install the EEPROMs so that the small dot on the edge of the chip lines up with the arrow on the inside of the socket. For detailed information on installed EEPROMs, refer to the document *IBM 8260 Distributed Management Module Memory Upgrade* (Part Number 29H4293) that is shipped with Feature Code 8932.

A/DMM Installation Issues

This section describes installation issues specific to the A/DMM/ (Feature Code 1700):

- Before you upgrade the operational code for any DMM or A/DMM, download the latest version of boot code. (This is required because versions of operational code may be too large to be supported by older boot codes.)

  After the new boot code is successfully downloaded, download the operational code.

Note: You can find the latest versions of operational codes and boot codes listed in Table 1 on page 37 of this release note.

Note: Before you install the A/DMM, ensure that you have installed the 4 MB DRAM card that is included with A/DMM package. For installation instructions, refer to the *8260 A/DMM Quick Start Guide* (Part Number 29H4324).

- The A/DMM cannot be used with an 8250 FDDI Management Module (FMM) if the FMM is required to become the master management module. If you need to use an FMM as a master module, remove the A/DMM from the hub.

  IBM recommends that you install RCTL operating code Version v1.15 to support this functionality.

New Features

The following new features have been added to the DMM at Version v5.25:

- New functionality prioritizes the selection of which Switching Module bridge port becomes the IP relay master of the interface for a vbridge network. If the default selection of LOW_TO_HIGH is used, the priority scheme searches for the bridge port with the lowest slot and port numbering on an -A module on that vbridge. If no such bridge port is found, the priority scheme searches for a bridge port with the lowest slot and port numbering on a non -A module on that vbridge.

  If the HIGH_TO_LOW selection is used, then the priority scheme searches for the bridge port with the highest slot and port numbering on an -A module on that vbridge. if no such bridge port is found, the priority scheme searches for a bridge port with the highest slot and port numbering on a non -A module on that vbridge.

  Regardless of the setting, the -A modules always have priority over non -A modules when determining the IP relay port. This setting is saved to NVRAM as part of the IP group. The following commands implement the new functions:

  – SET IP ELECTION_PRIORITY <LOW_TO_HIGH, HIGH_TO_LOW>
  – SHOW IP ELECTION_PRIORITY
  – SHOW IP ALL
  – SHOW IP
  – SAVE IP
  – REVERT IP

- Support has been added for patch versions of code for all 8260 Switching Modules. Support for Alpha versions has been dropped. Existing Alpha ("a") versions now appear as "p".

Corrected Problems

This section describes problems that have been fixed in DMM and A/DMM operating code for the indicated versions and the RCTL and ARCTL operating code at Version v1.15.

Corrected Problems for Version v5.25

This section describes problems that have been fixed in DMM and A/DMM operating code for Version v5.25.

- When a new Switching Module bridge port was added to an existing vbridge, no election was performed and the current master retained mastership. Now a new election is performed. This fixes problems that occurred in previous releases when the IP master went down and then came back up. Also see the New Features section for information about the IP Relay election priority command.
- Traps that appeared at the console used type 107 for -A Switching Modules. All Switching Modules now use type 96.
- Previous download of code, and download and upload of configuration, did not check for unsaved configuration. The new fix now searches for unsaved configuration changes at a higher level in the menu.
- When the IP relay master of a vbridge network was changed, sometimes the previous entry was not removed from the Address Forwarding Table (AFT). Now the previous entry is deleted from the AFT before adding a new one.
- If an SNMP getnext was issued to the A/DMM with the ocPort OID and the instance was incomplete, the wrong default value was returned. Now the correct default value is returned.
- When you entered a SHOW VBRIDGE X AFT MAC XX-XX-XX-XX-XX-XX command and the MAC address did not exist in the AFT, the console displayed an error message. Now, the console displays a NO SUCH ENTRY message.
- When you use the DOWNLOAD IN_BAND ALL XXXXXX <OPERATIONAL BOOT> command from a Telnet session, the output no longer prints dots (".") while the code transfers from the A/DMM to the Switching Module. Also, during the time that the Switching Modules that have the connection or the IP interface are downloading and rebooting, the connection is temporarily inactive.
- The Packet Channel/ATM Switching Module (FC 7302) BPORT_LEC ELAN_NAME parameter previously did not support non-alphanumeric characters. The command line for entering the parameter, SET BPORT_LEC XX.YY ELAN_NAME ABCDEFG, has been changed to use the same format as the SET TFTP FILENAME command:

  ENTER BPORT_LEC 6.1 ELAN_NAME <CR> (INPUT)

  ENTER BPORT_LEC 6.1 ELAN_NAME (OUTPUT)

  >(PROMPT OUTPUT) ABC_DEF_123_!@#$%^ (ANY CHARACTER INPUT)

- The A/DMM previously supported fragmentation of packets for ICMP (pings). Now any ICMP packets that have the fragmentation bit set are discarded and no reply is generated.
- The SHOW RING_MAP TOKEN_RING MAC_ADDRESS X command, where X is the address of an external station of the ring, previously showed X as being on the slot of the module to which it is connected with an extremely large port number. This has been corrected to show X as an external station of the ring.
- The CLEAR IP X command line previously did not correctly clear IP table entries for standby and non-assigned interfaces. The code now clears IP table entries for standby and non-assigned interfaces. This problem occurred when the A/DMM was reset and the table entries reappeared.
- The SHOW VBRIDGE X AFT BRIDGE_PORT ALL ALL command previously did not display entries above logical port 255. Now all bridge ports are displayed.
- The SHOW VBRIDGE X AFT MAC ALL ALL command in v5.20 did not work correctly with Switching Module v2.10 or earlier code that did not support rate limiting. The command now requests the proper information from the Switching Module and displays it correctly.
- The UPLOAD IN_BAND DEVICE CONFIGURATION command did not work from PC Telnet sessions. This command now works with PC Telnet sessions.
- The HEMAC (A-ENMC) was not synchronized to the EC-DMM sysUptime clock. This has been corrected.
- The DOWNLOAD IN_BAND DEVICE CONFIGURATION command previously executed without any prompt for the user. The command now prompts the user with the following message:
  - This operation will overwrite the current device configuration
  - Do you wish to continue? (y/n)
- When you previously reset the Ethernet Security daughter card, the MIB variable ocModStatus was returned as 38, notOperational and was not enumerated on the A/DMM. The A/DMM now uses this value.
- The SET BPORT_LEC XX.YY TIME.MAX_UNKNOWN_FRAME_TIME variable maximum has changed from 1 through 60 to the new range of 1 through 10.
- Previously, some Switching Module-related commands did not execute properly from scripts. The code has been corrected to allow all Switching Module-related commands to execute properly from scripts.
- The Packet Channel/ATM Switching Module supports 512 virtual connections that can be split between VPI and VCI channels. Previously, the SET_ATM <*slot*> VPI_VCI_BITS X/Y command only checked for VPI and VCI limits of 0-to-3 and 6-to-9, respectively. This command has been changed to also check that the combination of VPI and VCI bit settings does not exceed 9. The legal combinations of VPI/VCI are:
  - 0/9
  - 1/8
  - 2/7
  - 3/6

Corrected Problems for Version v5.22

This section describes problems that have been fixed in DMM and A/DMM operating code for Version v5.22, and the RCTL and ARCTL operating code, Version v1.15.

- The output that is displayed when you download modules via a Telnet session has been reformatted. This resolves a previous problem that was caused by downloading the module(s) that provide the IP connection between the Telnet host and the A/DMM. When this occurs, the output is buffered internally on the A/DMM until the connection is reestablished, which causes a delay in downloading. The following is an example of a module download during a Telnet session:

>**set tftp file_name**
Enter tftp file name:
>**speed2_v2.11.op**
TFTP file name changed.
>**save tftp**
Saving download parameters.
>**download in_band all 66nnM_XX_A operational**

Please stand by for download:
(Target will reset upon successful download completion)
(Hub IP connectivity may be lost or interrupted during this download)
(This could result in delayed or no terminal output)

Opening file speed2_v2.11.op on XXX.XXX.XXX.XXX . . .
Connected to XXX.XXX.XXX.XXX.

Receiving TFTP Packets

File transfer into device complete.

Downloading module(s).

1.01 done

2.01 done

3.01 done

5.01 done

6.01 done

14.01 done

15.01 d0ne

Download completed successfully.

>

- RCTL /ARCTL operating code for Version v1.15 corrects a problem that occurred when a power supply failed or was turned off by the user while the hub was in power non-fault-tolerant mode.

  This problem occurred when two or more power supplies were loaded to near full capacity, ARCTL was Active, and RCTL was in Standby. If one of the power supplies failed or was shut off, the results were as follows:

  — Controller switchover occurred and the new Active controller was not providing any slots with power.

  — The new Standby controller provided slots with power but not to the correct slots.

  — A SHOW POWER ALL showed that slots had insufficient power and the power budget indicated that there was power available relative to the number of power supplies that were indicated as OK.

  This potential problem is alleviated when both RCTLs/ARCTLs are running Version v1.15 operational code.

- ARCTL boot Version v1.04 resolves a download problem with the Advanced Fault-Tolerant Controller Module. In a single ARCTL configuration (when no Standby ARCTL or RCTL is present), the download of the ARCTL by a DMM located in one of the payload slots resulted in all payload slots becoming power-disabled, thereby halting the download of the ARCTL. This occurred because the slot containing the DMM became power-disabled.

  The boot code fix verifies that the ARCTL is not undergoing a command download before disabling power to all slots during boot-up initialization. The A/DMM can download the ARCTL because the controller bay slots can never be power-disabled.

- You can now set the last octet of the IP address to 255.

- Previously, erroneous multiple 00-00-00-00-00-00- addresses were displayed in a Token Ring map for the same slot and port. This no longer occurs.

- For the Active Per Module Media Module (Model Number T18MSA) and the Passive Per Module Media Module (Model Number T20MS), changing mismatched resolution from disable to enable now automatically causes the ring map to be re-mapped. T18MSA Version v1.50 or T20MS Version v1.50 are required for this fix.

- The poll range in the menu prompt of the SET ATM QSAAL command has been fixed. The valid range is 100 to 10000.

- A problem occurred when the vbridge master did not recognize that a port on a Switching Module was assigned to the master's vbridge. The DMM no longer prints a menu_bport error message.

- The DMM Script Scheduling feature is now functioning properly. Previously, if you created a SHOW MODULE ALL script through scheduling, the script ran, but there was no output.

- Security features are now available at the hub level with a single command, in addition to the current commands on a per-module basis.

- There was a problem with clearing an IP address on a Switching Module. Now when the IP that is assigned to a vbridge is cleared, the address is also cleared on the Switching Module.
- There was a problem with hello traps being sent continuously when a Version v1.1 Switching Module was installed in the hub. This has been corrected. The hello traps go out every 15 minutes instead of the previous 1-minute intervals.
- Previously, Ethernet ports on the Integrated Bridge were reported as ATM ports in the SNMP agent and not as Ethernet ports. This created a problem when managing these ports. This problem has been fixed.
- Previously, the DMM did not recognize the correct port status forwarding on a Switching Module. The DMM now recognizes the correct port status forwarding.

Known Problems

This section describes known problems that occur in the following software:

- DMM Version v5.25
- DMM Version v5.21
- E-MAC Software Version v3.0
- HTMAC Software Version v2.10 and T-MAC Version v4.00
- FDDI Switching Module Known Problem.

DMM Version v5.25

This section describes known problems that occur on the DMM and A/DMM at release v5.25.

Caution: If you have two or more management modules installed in your 8260 hub, you must wait at least one minute after you initialize the hub before you can configure the other modules. Not waiting results in an improper hub configuration because the management modules are in the process of communicating redundancy information.

- Network management applications do not work when you use the A/DMM's SLIP feature for in-band connections.
- The DOWNLOAD OUT_OF_BAND DEVICE <BOOT OPERATIONAL> command does not work for the boot option, and does not support the ALL option.
- When you generate command line interface input through the console port from a PC or similar external piece of equipment, some characters that generated at a rate of 10 ms are lost due to buffer overrun in the port drivers.

- Because of memory limitations, the older style DMMs and EC-DMM do not operate if too many RMON entries (between 3000 and 4000) are created.
- The PING command does not always function correctly when the number of times to PING is given. The actual PING process does work but the display of the number of times to PING by the A/DMM is incorrect.
- If you remove Switching Modules from the hub with interfaces that were listed in the A/DMM's interface table (SHOW INTERFACE command) and you attempt to assign the parameters that were assigned to another interface, such as IP address or network, problems may arise because the interface table is not cleared. If this happens, enter the RESET DEVICE command to clear unused entries in the interface table.
- When an IP relay master for a vbridge network is changed, the ARP cache is not flushed and results in inaccurate displays when you enter the SHOW IP ARP_CACHE command.
- RMON alarms are not retained after resets because the RMON alarm parameters are not saved to NVRAM.
- When the A/DMM attempts a download of a corrupted binary image, the A/DMM loops during download retry. When this occurs, reset the A/DMM and enter the DOWNLOAD OUT_OF_BAND command. Before you download copies of code files, ensure that the file is complete and not corrupted.
- There is no option for the CLEAR COUNTER <BRIDGE_PORT ETHERNET INTERFACE REPEATER RMON TOKEN RING> command line for PACKET_CHANNEL. The only way to reset these counters is to reset the module.
- For the SET PROTOCOLS <*slot.subslot*>FORWARDING<DSAP ENET SNAP_TO_DEFAULTS UNKNOWN> (FILTER) <HIGH_PRIORITY NORMAL_PRIORITY> 123... XNAME (NAME)... command line, there is a limitation of 12 ports per command line.
- If you enter a SHOW PROTOCOLS <*slot.subslot*> command for a Switching Module that has been removed from the chassis, the A/DMM hangs, and you cannot access it either through the console or through a Telnet session.

DMM Version v5.21

This section lists problems that occur in the following software:

- DMM v5.21
- Ethernet Network Monitor Card (ENMC) v3.00
- RCTL-ARCTL Controllers v1.15.

Warning: If you have two DMMs or one DMM and one A/DMM installed in your 8260 hub, you must wait at least one minute after you initialize the hub before you can configure the other modules. Not waiting will result in an improper hub configuration.

- When two or more network monitor cards are assigned to the same network, and the IP address, subnet mask, or default gateway for that network is either set or cleared and then saved after resetting the device or hub, the original settings may reappear. To work around this, reenter the new settings, save them, and reset the network monitor cards.

- If you have an 8250 Token Ring Per-Module Switching Module in a hub with a TRMM, the 8250 T18MSA module may cause the ring map to fail on the DMM. As a result, beacon recovery does not function properly on the TRMM.

- If you perform a SHOW TFTP command and the TFTP filename is too long, the DMM may stop functioning. To avoid this condition, do not use 50 or more characters for the filenames.

- The DMM might not log out when you exit from a UNIX **tip** utility session. That is, when you restart the **tip** session, you may still have the same access rights that you had when you exited the previous session.

- If a DMM is installed in the same hub as an FDDI Management Module, you must set the mastership priority of the DMM higher than 5. If an election occurs with the value set to less than 6, the management modules become stuck in the election process.

- Occasionally, IBM 8260 may experience the following ring mapping problems when displaying an address-to-port map (for example, when you use the SHOW RING_MAP TOKEN RING LOGICAL command):

  — MAC-less devices do not appear in the ocTRnetMapSummary MIB table when a T-MAC is on the same ring and the T-MAC has rmon_group and rmon_ring_stats enabled.

  — Occasionally, when stations from one ring, with a T-MAC and with rmon_group and rmon_ring_station_stats enabled, are moved to another ring, some of the stations that were moved to the new ring may be incorrectly reported in the original ring map as well as correctly reported in the new ring map. This occurs only when the T-MAC becomes the only station on the ring.

  To remove the entries from the original ring map, disable and then reenable rmon_ring_station_stats on the T-MAC.

- The DMM may display debugging messages (for example, FILE = ...). If one of these messages appears, contact your service representative.

- You cannot globally set certain port parameters (auto_polarity, link_integrity, squelch) on the E04M-MOD module using the SET PORT <*slot*>.ALL command.

- The DMM allows you to create up to 10 RMON topn Hosts in the control table for the E-MAC. The maximum number allowed is 6. Hence, any entry greater than 6 but less than 10 is invalid.

- If a hub has multiple Token Ring segments that are trunked together with MACless devices connected to the segments, the modules that have the trunks must be in the highest number slot for that network segment.

  For example, if modules are in slots 1, 2, and 3 on Token_Ring_1 and there are modules in slots 4, 5, and 6 on Token_Ring_2, and there are MACless devices connected in either Token Ring network, the modules with the trunks must be in slots 3 and 6. This prevents the DMM from taking too much time to display the logical ring map.

- If you force a manual switchover of a redundant Switching Module port using the SET BPORT_MAU MODE command, the port status (whether it is active or standby) may not always be reported correctly in the SHOW BPORT_MAU VERBOSE command screen.

- When a redundant Switching Module port pair is configured to be non-redundant and you reset the module, the following conditions occur:

  — The RESET MODE for the port that displays a mode of disable is incorrect.

  — The reset mode displayed in the show bport_mau verbose field is enabled, even though the correct reset mode for this port is disabled.

  — The port comes up in the correct operational state (disabled) upon reset, but the status still displays enabled (the incorrect state) on the screen.

E-MAC Software Version v3.0

The following problems can occur in E-MAC Version v3.0 software *only* when 'probe mode' is disabled and 'host statistics' is enabled:

- Alignment or CRC errors *are not* reflected in the RMON Host Table.

- If you toggle the RMON hostControlStatus object for an E-MAC interface from *valid* to *under Creation* and then back to *valid*, statistics for that interface ***do not clear***. Instead the host statistics feature becomes disabled on the E-MAC. To resolve this, reenable host statistics on the E-MAC.

- Currently, when you issue a DMM command to gather RMON statistics, there is a difference in statistical values between an E-MAC and an HEMAC. This is a hardware issue. The HEMAC supports advanced capabilities that the E-MAC does not support.

HTMAC Software Version v2.10 and T-MAC Version v4.00

The following problems can occur in HTMAC Version v2.10 and T-MAC Version v4.00 in the areas listed:

- Connectivity
- RMON Support
- ECAM (Enterprise Communication Analysis Module)
- IEEE 802.5 Token Ring MIB Support
- IBM Token Ring Surrogate Function.

Connectivity

- When the same HTMAC is being used for DMM connectivity and as an RMON probe, the DMM is unable to Ping the probe's IP address.
- After you configure the HTMAC to go from using a locally administered MAC address to the burned-in MAC address (universally administered MAC address) or vice-versa, connectivity to the probe's IP address is lost.

  After you change the HTMAC's MAC address type (for example, SET MODULE <*slot*>.2 MAC_ADDRESS_TYPE LOCALLY_ADMINISTERED), do the following:

  a. Save the configuration parameters (for example, SAVE MODULE_PORT)

  b. Reset the HTMAC (for example, RESET MODULE 4.2).

- When HTMAC arp_resolve_method is set to non_source_route, DMM connectivity works properly, but probe connectivity may not work if the HTMAC probe is the one that sends the ARP request.

RMON Support

If the ring segment number changes after the HTMAC has initially inserted into the network, the source routing statistics do not increment properly until after the HTMAC is reset.

ECAM

A problem exists on the HTMAC with invalid address translation entries. When using an Nways® Remote Monitor application to access Address Translation information, the Duplicate Net Address Report may list entries where a given NetAddress appears only once in the report.

These single entries are likely to be erroneous in the report and may also contain incorrect information for the NetAddress. The corresponding entries in the Network Layer Address Report may also contain incorrect information for the NetAddress and IsDuplicate fields.

IEEE 802.5 Token Ring MIB Support

When you access IEEE 802.5 MIB statistics (for example, SHOW COUNTER TOKEN_RING network), the functional address value provided does not reflect when the T-MAC or HTMAC is the Active Monitor. The Configuration Report Server (CRS) may be used to get the correct functional address information from a T-MAC or HTMAC. To use CRS for this purpose:

1. Ensure that CRS is enabled on the T-MAC or HTMAC.
2. Issue the following DMM command:

   SHOW TR_SURROGATE <*slot*>.2 CRS_STATION MAC_ADDRESS <*mac_address*>

   where *mac_address* is the HTMAC or T-MAC's address.

IBM Token Ring Surrogate Function

If REM and/or CRS are still enabled when the Surrogate function is disabled, the REM or CRS functionality is not performed; but the REM or CRS functional address is still enabled. To work around this, ensure that REM and CRS are disabled *before* disabling the Surrogate function. For example, use the following sequence of commands:

1. SET TR_SURROGATE <*slot*>.2 SURR_STATUS REM_ADMIN DISABLED
2. SET TR_SURROGATE <*slot*>.2 SURR_STATUS CRS_ADMIN DISABLED
3. SET TR_SURROGATE <*slot*>.2 SURR_STATUS SURR_ADMIN DISABLED

FDDI Switching Module Known Problem

Occasionally, the SHOW BRIDGE_PORT VERBOSE command may display bogus FDDI upstream and downstream neighbor MAC addresses.

8260 Switching Module Information

This section contains the following topics about Switching Module Version v2.11 running with DMM Version v5.21:

- New Features
- Software Support
- General Switching Module Issue
- New Switching Module Commands.

New Features

The following 8260 Switching Modules and software features are introduced for Version v2.10.

New Switching Modules

- 18-port Fast Ethernet 100BASE-TX Switching Module (Model Number SWE18-TX-A)

  The maximum achievable port density for 100BASE-TX in a 8260 hub is increased by the introduction of the SWE18-TX-A. The 18-port Fast Ethernet card uses front-end repeaters to provide group switched capability and uses the same main logic board as the existing 4-port Fast Ethernet Switching modules (Model Numbers SWE4-TX-A and SWE4-FX-A). It supports many, but not all, of the same features as existing Fast Ethernet Switching Modules.

- 20-Port Ethernet 10BASE-T Switching Module (Model Number SWE20-TP-A)

  The 20-port Ethernet 10BASE-T Switching Module increases the 8260 hub port density for switched 10BASE-T with RJ-45 connectors. The 20-port Switching Module supports the same features as existing Ethernet Switching Modules.

Software Features

The following new software features are provided in Version v2.11:

- Support for traffic from multiple Vbridges to be transmitted and received between two Switching Module ports via a single link through the use of Frame Tagging.
  - Frame tagging is supported only on Switching Modules SWE4-TX-B (top level assembly number 02L3848 or higher) and SWE4-FX-B (top level assembly number 02L3849 or higher). To determine the top level assembly number, inspect the shipping label on the outside of the shipping box.
  - If the Switching Module is already installed in the hub, see Chapter 8 in the *8260 Switching Module User's Guide* for more detailed information
- Information relating to transmit buffer overflows (Model Number SWEXX-A Switching Modules only)

- Peak rate statistics for the following:
  - — Transmit and receive frame rates
  - — Transmit and receive byte rates
  - — Maximum number of addresses held in the address forwarding table (AFT)
- Reduction in the time it takes for the network to recover from resilient link switchover
- Switching Module time of day
- Ability to set port up and port down alerts on a per-port basis
- Ability to configure packet rate limiting for any multicast MAC address
- Maximum and latest CPU utilization parameters for Switching Modules (not supported on Model Number SWE2-MOD PacketChannel/ATM Switching Modules)

PacketChannel/ATM Switching Module

- Selectable Vbridge ILMI MIB object `atmfmyIpNmAddress` via the following command:

  > **set atm <*slot*> ilmi vbridge <*vbridge*>**

- Support for a variable Loss of Signal Detection, which affects the PHY switchover timing. The Loss of Signal Detection can be configured from 0 (default) through 60 seconds via the following command:

  > **set atm <*slot*> loss of signal detection <*value*>**

- The MAX size of the MTU has increased to support the MAX size FDDI packets.
- Peak Cell rates for ddVCCs now include 2 & 8 Mbps. Also, the range of acceptability has increased from 5 percent to 10 percent.

Software Support

Note: To manage and configure IBM 8260 Switching Modules, you must use DMM software Version v4.11 or later. You can manage 8260 Switching Modules using the DMM command line interface or a supported graphical network management program.

The following versions of controller software on the A/DMM (Feature Code 1700) software are required to manage Switching Modules:

— Operational code Version v5.21

— Boot code Version v1.03.

If a Switching Module is running software Version v2.00 or later with a DMM or A/DMM running Version v5.10 or earlier, set VBRIDGE to INVALID.

DMM Version v5.21 provides the following new software support:

- Switching Modules SNMP Connectivity — DMM software commands support Switching Modules configuration (Virtual Bridges and Spanning Tree Protocol).
- Support for the following new commands to manage the Switching Modules:
  - SET BRIDGE_PORT (and SHOW BRIDGE_PORT)
  - SET BPORT_MAU (and SHOW BPORT_MAU)
  - SET VBRIDGE (and SHOW VBRIDGE).
- Additional IBM Nways LAN ReMON Features
  - DLM support for Traffic Generator
  - Address Translation Capability.
- HEMAC — The 8260 High-end Ethernet Medium Access Control Card Version v2.1 supports:
  - Ethernet Port Security — You enable Port Security through the SET SECURITY PORT MODE command. A network map of source addresses accumulates. After the number of these accumulated addresses is greater than the maximum number of allowable addresses, the port becomes disabled. The maximum number is eight.
  - Port/Address Correlation MIB (PACMIB) — RMON etherStatsExtTable and portStatsTable support. Information is reported on a per-port basis.
  - The option *quick_forward*, which decreases the time a port takes to enter the Forwarding state
  - A new command that displays the current roving analysis configuration:

    >SHOW ROVING_ANALYSIS_PORT <hub_info> <system_analyzer_info>

General Switching Module Issue

The SHOW IP ROUTE_TABLE command does not display an interface's information correctly unless the subnet mask's last byte is 00 (for example, ff.ff.ff.00).

New Switching Module Commands

DMM Version v5.21 provides the following new commands for the 8260 Switching Modules at Version v1.01. These commands are not listed in the Switching Module documentation:

- SHOW LOG MODULE <*slot*> EVENT_LOG
- CLEAR LOG MODULE <*slot*> EVENT_LOG.

After you download DMM Version v4.11 and later code, enter the CLEAR LOG command for all Switching Modules in the hub. This command removes the download-related information from the Switching Module NVRAM so that, in the event of a Switching Module crash, the SHOW LOG command displays only pertinent troubleshooting information (register and stack information) about the Switching Module.

New Command Support

The SET NETWORK TOKEN_RING PURGE_ON_INSERT command for Token Ring media modules is in 8260 DMM software Version v4.11 and later. This command is invalid until it is supported by 8260 Token Ring media module software.

Important Network Management Application Consideration

To discover an 8260 hub with a master DMM v4.11 or later agent into the hub topology map, you must obtain the PTF UR46637 through your IBM support organization. The PTF UR46637 will upgrade the Nways Campus Manager LAN for AIX® program to Version v3.11.

If your Nways Campus Manager LAN program is only at Version v3.10, you may not discover your 8260 hub containing a master DMM Version v4.11 or later. You may only get a network symbol icon in the hub topology map and you will not get a realistic view of your hub.

Operating Considerations

This section describes the following *operating considerations* for:

- DMM
- RMON
- Traps
- SNMP
- Power Management
- Statistics
- T-MAC
- HTMAC.

DMM Operating Considerations

Consider the following issues when you use the DMM Version v5.10 and later terminal command interface:

1. The A/DMM only supports Ethernet2 MAC frame encapsulation for its IP interfaces.
2. Before you install an A/DMM in the same hub with an 8260 Redundant Controller Module, download RCTL Version v1.15 and boot code Version v1.04 software to the 8260 Redundant Controller Module. RCTL Version v1.15 software allows the A/DMM to be elected master, and ensures consistent power management.
3. Moving Management Modules

   When you insert a management module into a hub that is up and running, redundancy is achieved by the following:

   — When RESET_MASTERSHIP is enabled, it causes an election, and the configuration of all management modules is set to that of the elected master.

   — When RESET_MASTERSHIP is disabled, the inserted module is updated to the configuration of the current master. The factory default setting is disabled.

Caution: Be careful care when you move management modules from hub to hub to ensure the desired outcome.

4. An E-MAC on a master or slave EC-DMM has a redundancy limitation. For example, your network hardware configuration has the master DMM containing the active E-MACs and the slave DMM containing a standby E-MAC. If you remove the master DMM with the active E-MAC, the slave DMM becomes the master. However, the standby E-MAC does not become the active E-MAC and you experience a loss of SNMP connectivity.

To set up redundancy on the daughter cards and avoid this condition:

a. Place the active interface E-MAC on the slave DMM.

b. Place the standby interface E-MAC on the master DMM.

By setting up this configuration, you should not lose SNMP or Telnet connectivity if either DMM fails or if you place the daughter cards on media modules.

5. After a hub reset, if you want the DMM to be assigned as master in a hub that contains an A/DMM, set the mastership priority of the A/DMM (by issuing the SET MODULE <*slot*>.<*subslot*> MASTERSHIP_ PRIORITY command) to at least 2 less than the DMM mastership priority. This ensures that the DMM becomes the master module.

6. If you perform a hub reset or a fast reset (fast reset is when a new controller module takes over), a new DMM or A/DMM can become the master. In this situation, configuration data may be lost.

   To avoid losing data, use the mastership priority capability provided to ensure that the original DMM or A/DMM becomes the master. Issue a RESET MASTERSHIP to allow the standby DMM or A/DMM to become master. Then issue a SAVE ALL on the new master to ensure configuration integrity.

7. If you have both the DMM and A/DMM and you are upgrading both to the latest version of code, you must make the DMM master to download the new code.

8. If you use the n + 1 redundancy feature and you back up an HEMAC with an E-MAC card, some features from the HEMAC are not supported (for example, the security feature) after the E-MAC takes over. If you want the full feature functionality of an HEMAC, use another HEMAC for your n + 1 redundancy feature.

9. Ethernet MAC Card's probe mode feature is not redundant under n + 1 redundancy, which means full capability is not provided. There are two solutions to this situation:

   a. Before you set the module to standby mode, enable probe mode on the E-MAC (probe mode does not apply to the HEMAC).

   b. If a standby module becomes active, enable probe mode manually.

10. The following versions of DMM software are used as follows:

    — DMM Version v2.3 or later can be used with T-MAC Version v3.0 or E-MAC Version v3.0 and later.

    — DMM Version v3.01 can be used with HEMAC Version v1.0.

    — DMM Version v4.11 or later can be used with HEMAC Version v2.1 or later.

    — DMM Version v4.11 or later can be used with HTMAC Version v1.0 or later.

    — DMM Version v4.12 or later can be used with HTMAC Version v1.1 or v2.0.

    — DMM Version v5.10 or later can be used with HTMAC Version v2.1 or later.

    If you do not have the correct versions, contact your IBM Representative for an upgrade. Current code versions are listed in the 8260 Module Code Versions section later in this release note.

11. To ensure reliable network connectivity, always set an active default gateway for the DMM.

12. If you define more than one default gateway, duplicate hubs might appear when you use the Nways Campus LAN Manager for AIX program.

13. If you issue the DMM TELNET command using an invalid IP address, there is no escape sequence to exit. Wait 60 seconds for the session to time out.

14. When a standby DMM becomes hub master, the new master may not have a default gateway assigned. Use the SET IP ACTIVE_DEFAULT_GATEWAY command to set a default gateway.

15. If you remove an enabled MAC Card from the hub, and a standby MAC Card becomes active, the newly active card remains active even if the removed card is reinserted into the hub. This feature prevents unnecessary switchover when the modules are removed or reset. Issuing the REVERT command does not cause the previously active card to become active again.

16. If you use a modem to initiate a Serial Line Internet Protocol (SLIP) connection, noise on the communication lines is sometimes interpreted as a break character. When this occurs, the connection breaks. To correct this situation:

    a. Reestablish the connection.

    b. Issue the SET LOGIN ACCESS command to regain super-user privileges.

17. Before the DMM configures all of the modules in the hub, the DMM displays RDY (ready) and the Login prompt appears on the DMM console. Allow a few minutes for the DMM to learn the hub configuration before you enter SET or SHOW commands.

18. When a standby MAC assumes the role of active MAC, stations may be unable to communicate with the DMM until the stations clear their ARP (Address Resolution Protocol) caches. This happens because the standby MAC assumes the IP parameters of the card it replaced, although the MAC maintains a different MAC address. The communication problem corrects itself when either of the following occurs:

    — The station's ARP cache times out.

    — The station receives a message (and therefore clears its ARP cache).

19. After you reset a MAC Card (either individually or as part of a larger reset), Link Down and Link Up traps occur.

20. To map MAC addresses that are external to the 8260 module domain (stations connected to 8250 modules or third-party equipment using 8260 fiber or copper trunks), you must enable rmon_groups and rmon_ring_station_stats on the T-MAC. All indirectly connected stations are mapped to "external" in the logical map.

21. If you enable the rmon_ring_station group on a T-MAC in an 8260 hub that is connected to another 8260 hub using 8260 fiber optic or copper trunks, MAC-less stations disappear from the ring map.

22. If the HTMAC or T-MAC is being managed by a remote station, and the router on the same network as the HTMAC or T-MAC does not support source routing for ARP, use the SET MODULE <*slot*>.2 ARP_RESOLVE_METHOD NON_SOURCE_ROUTE command to prevent the HTMAC or T-MAC from including an RI-field in the ARP request. If you do not do this, you cannot perform IP communications across the router boundary.

23. If you have previously configured modules (8260 24-Port 10BASE-T and 10BASE-FB Version v1.00 only) in an unmanaged 8260 hub, adding a DMM to the hub overwrites the module's current configuration. To avoid this problem in the future, upgrade the media module software to the latest version.

24. You must have TRMM Version v3.00 or later software to ensure proper Token Ring beacon recovery for 8250 modules from a slave TRMM in an 8260 hub. If you have an earlier TRMM version, the TRMM must be the master management module to ensure proper beacon recovery for 8250 modules.

25. Although the DMM supports multiple IP addresses, enable the interface for only one address per DMM (on the network attached to your default gateway). Enabling multiple IP address on the same DMM may cause connectivity problems.

26. IBM recommends using the same version of DMM code for all management modules in the *same* hub.

27. When using DMM software with the IBM 8260 Ethernet Flexible Concentration Module (Model Number E04M-MOD), occasionally, the SHOW COUNTER and MONITOR REPEATER commands display invalid data. This condition occurs when all counters and source addresses display a value of 0 on a screen but then resume counting again.

28. If a hub has multiple Token Ring segments that are trunked together with MAC-less devices connected to the segments, the modules that have the trunks must be in the highest number slot for that network segment.

    For example, if the following conditions exist:

    — Modules in slots 1, 2, and 3 are on Token_Ring_1

    — Modules in slots 4, 5, and 6 are on Token_Ring_2

    — There are MAC-less devices connected in either Token Ring network.

    Then the modules with the trunks must be in slots 3 and 6. This prevents the DMM from taking too much time to display the logical ring map.

29. You cannot disable beacon recovery on an isolated network.

30. Hot insertion of an 8250 MAU TR Media Module (Model Number 3820T) into the hub causes a DMM mastership election.

31. You may not be able to view 8260 module repeater statistics on some Ethernet networks unless they have an E-MAC assigned to them.

RMON Operating Considerations

Consider the following issues when you use the DMM Version v4.12 RMON feature:

1. According to the RMON specification, the MAC should create certain default entries when you enable host statistics on the MAC. MACs may not automatically create RMON host table entries when enabled, or delete RMON host table entries when disabled.

2. If you have difficulty obtaining RMON statistics from the DMM, ensure that you have enabled the RMON function and the appropriate RMON statistics, either using the command line or using SNMP. An RMON manager cannot dynamically allocate any RMON group unless the data source and index match the T-MAC or E-MAC interface index.

3. If a station inserts into the ring and becomes the Active Monitor's NAUN, then de-inserts from the ring before participating in at least two ring poll cycles, the station may be incorrectly listed in the RMON ring station table as Active and be included in the number of Active Ring Stations listed in the Ring Station Control Table. This applies only to the T-MAC.

4. The RMON Host and Ring Station Tables do not contain any entries for a station with an address of 00-00-00-00-00-00. This applies to T-MAC only.

5. When you locate an Ethernet MAC Card (E-MAC or HEMAC) on a 20-port 10BASE-T module, the DMM may display RMON data on networks that are not being monitored currently.

6. If you enter an RMON event description with too many characters, the DMM forces a carriage return. To change the text, re-create the event.

7. After a hub reset command is issued, RMON statistics may display on interfaces with no incoming traffic.

Trap Operating Considerations

Consider the following issues when you analyze trap messages that are sent by DMM Version v4.12:

1. If an IBM 8250 FDDI Management Module (FMM) is installed in the hub and you remove any module from hub slot 1, the FMM displays module down traps continuously until you remove the FMM.

2. Traps are not displayed on Telnet-connected DMM sessions.

3. When you manage FDDI media modules that are running a code version before Version v3.00, the DMM may generate false port disable/off traps when you make changes to module or port parameters.

4. The DMM does not support rptrHealthTraps.

5. If you set up a SLIP connection using the SET TERMINAL AUXILIARY MODE SLIP command, the trap contains the correct information. However, if you then issue the REVERT ALL command (effectively closing the SLIP connection), traps may not be reported as expected.

SNMP Operating Considerations

Consider the following issues when you use SNMP to manage DMM Version v4.12:

1. If you configure a subnet mask for an inappropriate class (using the terminal interface), the DMM displays a warning. The terminal interface displays the incorrect setting, but the ipAdEntNetMask MIB object returns a subnet mask that is appropriate for the class.

2. A MAC address obtained using SNMP may appear as ASCII characters instead of hexadecimal digits. This error is caused by certain SNMP tools, not the DMM.

3. The valid values for the MIB etherStatsOwner object are 0 through 127. The terminal interface prints only 78 characters in response to this object.

Power Management Operating Considerations

Consider the following issues when you use the DMM Version v4.12 power management feature:

1. Configured power management settings will be lost for all installed 8260 modules when you perform any of the following actions after powering off the hub:
   - Swap an 8260 module for an 8250 module
   - Swap an 8250 module for an 8260 module
   - Remove a module and leave the slot empty
   - Install an 8250 or 8260 module in a previously empty slot.

2. If the hub exceeds its power budget because of newly inserted 8250 modules, 8260 modules do not power down automatically, but the controller module *does* send a power threshold trap warning of a power utilization problem.

   The hub remains in power deficit until it power cycles, or until you reset the hub. When you reset the hub, installed controller modules use the remaining power not consumed by 8250 modules to power-enable 8260 modules according to their power class settings. The 8260 modules are power-enabled only after all 8250 modules have powered up.

3. Double-fault scenarios in a mixed environment (8260 and 8250 modules) may cause all 8260 modules to be powered down. (Example of a double-fault scenario: when a controller switchover occurs and a power supply failure follows within 30 seconds of the switchover.)

   To recover from a double-fault scenario:

   a. Power down the hub

   b. Remove an 8250 module.

   Upon power-up, the controller reassesses the power budget. When the 8260 modules power up, all power values revert to their default values.

4. When the power required by installed 8250 modules is greater than the capacity of the first power supply you switch on, switch on all installed power supplies at the same time to avoid the possible shutdown of one or more power supplies.

   For example, if you switch on one power supply at a time, the first power supply you switch on may become overloaded and shut down before a second power supply can power up and share the load. If a power supply shuts down due to an overload, wait at least 10 seconds before you attempt to switch on that power supply again.

Statistics Operating Considerations

Consider the following issues when you use DMM Version v4.12 to monitor network statistics:

1. The 8260 24-port 10BASE-T module repeater MIB statistics are not 100 percent accurate at high error rates. DMM statistics are sufficient for general network diagnostic analysis.

2. The 8260 Token Ring RMON statistics are not 100 percent accurate at high network traffic rates. DMM statistics are sufficient for general network diagnostic analysis.

3. Significant reconfiguration of the 8260 24-Port 10BASE-T module (such as removing or powering down the module) causes statistics counters to reset.

4. If you have assigned an 8260 36-Port 10BASE-T module and an 8260 24-Port 10BASE-T module to the same backplane network, the 24-Port module may not record repeater collision statistics. Issue the RESET DEVICE command to correct this problem.

5. When an E-MAC is monitoring Ethernet network 1, 2, or 3, and a collision occurs between two ports on a media module (one port receiving, followed by another starting to receive), the event is logged in the Runts field (displayed by the SHOW COUNTER REPEATER ETHERNET_(1,2,3) command). The error should be logged in the Transmit Collisions field. When an E-MAC is monitoring Ethernet networks 4 to 8, the DMM records transmit collisions properly.

6. If you request counter statistics on a port or network that is not currently being monitored, the DMM may report counters set to all zeros (rather than issuing a warning message).

T-MAC Operating Considerations

Consider the following issues when you use the T-MAC:

1. RMON events and alarms for the T-MAC using SNMP are now supported. However, no terminal configuration capability is available at this time.

2. The T-MAC does not support group addresses.

3. When you access 802.5 Token Ring Statistics to obtain the T-MAC functional address, the functional address value does not reflect when the T-MAC is the Active Monitor. Use the SHOW TR_SURROGATE <*slot*>.2 CRS_STATION command to view the T-MAC Active Monitor Status. To ensure correct functional address information from a T-MAC, use the SHOW TR_SURROGATE <*slot*>.2 CRS_STATION MAC_ADDRESS <*mac_address*> command, where *mac_address* is the address of the T-MAC.

4. When you enable a T-MAC and start a statistics-collection task, then disable the T-MAC, your SNMP application may still show statistics for the disabled interface. These statistics are not valid.

5. To determine what version of trchipset code is on the T-MAC, perform a SHOW MODULE <*slot*>.2 VERBOSE command for the T-MAC and look at Adapter Microcode Version. The Adapter Microcode Version for T-MAC trchipset v4.0 shows up as:
   00 00 01 c1 e3 f1 c1 c4 f0 40.

6. When the T-MAC is unable to communicate to the DMM, the following message appears:

   ```
   WARNING - Module is not communicating. Failed or Initializing.
   ```

   If this condition persists and is not due to the T-MAC experiencing receive congestion, perform the following steps to recover the T-MAC from this state:

   a. Reset the host media module that is carrying the T-MAC.

   b. If the T-MAC does not initialize within 30 seconds of being reset, call your service representative. The T-MAC may need to be replaced.

HTMAC Operating Considerations

Consider the following ioperating issues when you use the HTMAC for these areas:

- Configuration
- Connectivity
- RMON
- ECAM
- Trchipset microcode version.

Note: If you need information about the 8260 High-end Token Ring Medium Access Control Card (HTMAC) at Version v1.01, refer to the specific HTMAC Release Note (Part Number 38H5148).

Configuration

If your network management application does not support the HTMAC, use one of the following methods to configure the HTMAC's probe information:

- The DMM terminal interface (SET MODULE <*slot*>.2 PROBE_*)
- Use SNMP to set the SpecMods Table for the HTMAC in the IBM 8260 MIB.

Connectivity

Consider the following issues when you use the HTMAC for DMM connectivity or as an RMON probe:

1. The IP address assigned for DMM connectivity or for the probe must be unique.
2. When a different MAC address is used for the same IP address (for example, a standby HTMAC takes over as the active MAC), connectivity problems may occur with the DMM or the HTMAC probe. This communication problem corrects itself when either of the following occurs:
   - The station's ARP cache times out.
   - The station's ARP cache entry is cleared.

RMON

Consider the following issues when you use the HTMAC as an RMON probe:

1. When the Host table is full, no additional entries are allowed. To clear all entries from the table, perform either of the following:
   - Reset the HTMAC (for example, RESET MODULE <*slot*>.2).
   - Disable then re-enable the HTMAC's interface mode:

     > **SET MODULE <*slot*>.2 INTERFACE DISABLE**

     > **SET MODULE <*slot*>.2 INTERFACE ENABLE**
2. To ensure that RMON control information (for example, alarms) is saved after being configured, cause the HTMAC to do a warm start by performing either one of the following:
   - Use the DMM to reset the HTMAC (for example, RESET MODULE <*slot*>.2).
   - Issue a warm start using the Aspen Config MIB.
3. Filter/Capture is supported only for the first 1500 bytes of the frame.
4. HostTopN is not available in the Nways Remote Monitor Summary Window.

   If the HostTopN graphs are not available in the Summary Window, then the HostTopN tables may be too full.

   To resolve this condition, you must delete one or more of the HostTopN tables on the HTMAC. The way to delete a HostTopN table depends on the IBM Nways Remote Monitor application.

The following is an example of how to delete the HostTopN table using IBM Nways Campus Manager - Remote Monitor. Follow these steps:

a. From the **Summary** Window, click [**Config**] to display a **Config Dialog**.

b. From the **Config Dialog**, click [**Tables**] to display the **Table Editor**.

c. From the **Table Editor**, click [**Delete Host Top N tables**].

d. Select an entry in the **Delete Table Entry** list.

e. Click [**Delete**].

f. Repeat steps d and e until you have deleted the desired number of entries.

g. From the **Delete Table Entry** list, click [**Cancel**].

h. From the **Editor Dialog**, click [**Close**].

In Nways Workgroup Remote Monitor for Windows, a pop-up window appears when the HostTopN tables are full, which allows you to choose the entries that you want to delete.

ECAM

This section contains the following topics:

- Overview
- Starting ECAM on the HTMAC
- Stopping ECAM on the HTMAC
- Considerations.

Overview — ECAM (Enterprise Communication Analysis Module) is an application that provides RMON value-added extensions in the areas of network protocol distribution and address translation. ECAM is IBM's pre-RMON2 standard. Protocol distribution provides information on what network protocols are being used on a given network (for example, what amount of your network traffic consists of which protocols, which stations have conversations with each other using which protocols).

Address translation provides a mapping between MAC address and network addresses (IP addresses or host names). Address translation also contains the ability to identify duplicate addresses.

To use ECAM, you must be running:

- An RMON probe (for example, the 8260 HTMAC operational code v2.0 or later)
- An Nways Remote Monitor application that supports ECAM.

The HTMAC collects the data and provides it to an Nways Remote Monitor application, which then presents the information to the user.

ECAM is considered a Dynamically Loadable Module (DLM) that is loaded onto an RMON probe when you launch ECAM from your Nways Remote Monitor application. The HTMAC ECAM support is part of the HTMAC operational code, so it is not dynamically loaded. To use ECAM on the HTMAC, you must still load ECAM from an Nways Remote Monitor application, which then automatically triggers the HTMAC to perform the ECAM function. The only difference is that you do not have an ECAM file to put on your TFTP server and it does not matter what address is specified in the TFTP Server Address on the SmartAgent Maintenance dialog window.

The HTMAC can dynamically start and stop running ECAM by selecting the appropriate option on the SmartAgent Maintenance dialog window.

Note: For more information about ECAM, refer to the *IBM Nways Campus Manager – Remote Monitor Enterprise Communications Analysis Module User's Guide* (Document Number SA33-068.)

Starting ECAM on the HTMAC — This section contains an example for loading (starting) ECAM on the HTMAC using IBM Nways Campus Manager — Remote Monitor. This example assumes that you already have ECAM up and running on your network management workstation. For detailed installation information, refer to the *IBM Nways Campus Manager – Remote Monitor Enterprise Communications Analysis Module User's Guide* (Document Number SA33-068).

To load ECAM on your HTMAC:

1. To open the **Config Dialog** window, click [**Config**] from the **Summary** window.
2. In the **Config Dialog**, select the probe that you want to start ECAM from the **Select Probe** list. To open the **SmartAgent Maintenance** dialog, click [**SmartAgents**].
3. In the **SmartAgent Maintenance** dialog, select any one of the applications that indicate ECAM from the **Available SmartAgent Applications** list.

   Depending on the Nways Remote Monitor platform and version of code being used, there may be up to three applications associated with ECAM. For example, when you use Nways Campus Manage Remote Monitor for AIX v2.0, choosing any one of the following ECAM applications results in starting ECAM on the HTMAC:

   — Protocol Distribution: ecam [Not Loaded]

   — Address Translation: ecam [Not Loaded]

   — ECAM: ecam [Not Loaded].
4. The TFTP Server Address is not required to load ECAM on to the HTMAC, so that parameter may be left as is. Click [**Load**].

When ECAM is running on the HTMAC, all ECAM-based applications change from the [Not Loaded] to the [Loaded] state. Sometimes, to see the status change, you may need to exit the **SmartAgent Maintenance** dialog and then open it again.

The Reference value for each ECAM application listed under the **Available SmartAgent Applications** list increments each time that you load an ECAM application.

Stopping ECAM on the HTMAC — This section contains an example for unloading (stopping) ECAM on the HTMAC using IBM Nways Campus Manager — Remote Monitor. For detailed installation information, refer to the *IBM Nways Campus Manager – Remote Monitor Enterprise Communications Analysis Module User's Guide* (Document Number SA33-068).

To unload ECAM on your HTMAC:

1. To open the **Config Dialog**, click [**Config**] from the **Summary** window.
2. In the **Config Dialog**, select the probe that you want to stop ECAM from the **Select Probe** list. To open the **SmartAgent Maintenance** dialog, click [**SmartAgents**].
3. In the **SmartAgent Maintenance** dialog, select any one of the applications that indicate ECAM from the **Available SmartAgent Applications** list. The TFTP Server Address is not required to unload ECAM from the HTMAC, so that parameter may be left as is. Click [**Unload**].

The Reference value for each ECAM application listed under the **Available SmartAgent Applications** list decrements each time that you unload an ECAM application. ECAM is unloaded when [**Unload**] is selected and when the reference value is **1**.

When ECAM is unloaded from the HTMAC, all ECAM-based applications change status from [**Loaded**] to [**Not Loaded**]. Sometimes, to see the status change, you may need to exit the **SmartAgent Maintenance** dialog and then open it again.

Considerations — This section describes additional ECAM operating considerations.

1. ECAM Data Sources not defined after changing HTMAC state — When you use ECAM, the Data Sources defined in Nways Remote Monitor may need to be reconfigured after the HTMAC has some type of state change. Examples of HTMAC state changes are:
   - — After the HTMAC is reset
   - — After HTMAC interface mode is changed
   - — After the HTMAC is assigned to a different network
   - — After ECAM is loaded.
2. **NetAddress** 0.0.0.0 entries appear in the **Duplicate Net Address Report** and **Network Layer Address Report** — Stations that use BootP to learn their IP address may appear in the **Duplicate Net Address Report** and **Network Layer Address Report** of 0.0.0.0. This is normal operation because multiple stations may specify an IP address of 0.0.0.0 when issuing a request to the BootP server.
3. Different data is reported when you use different Nways Remote Monitor Applications — Some Nways Remote Monitor applications may report different data other Nways Remote Monitor applications because of the level of support that each application provides.

   For example, Nways Campus Manager Remote Monitor for AIX Version 2.0 lists '5', '6', and '7' under **NetAddrType** for AppleTalk, Vines, and SNA, respectively: whereas Nways Workgroup Remote Monitor for Windows Version 1.0 lists 'AppleTalk', 'VINES', and 'SNA' under **NetAddrType**.

Trchipset Microcode Version

To determine the version of trchipset code in the HTMAC, perform a SHOW MODULE <*slot*>.2 VERBOSE command for the HTMAC and look at the **Adapter Microcode Version**. The adapter microcode version of the HTMAC trchipset v1.0 appears as:

00 00 01 c1 e3 f1 c1 c4 f0 40

Token Ring MAC Address-to-Port Security Issues

Consider the following issues when you use the MAC-Address-to-Port Security feature with 8260 Token Ring modules:

1. When the neighbor notification process cannot complete three consecutive ring polls or more, the ring map may be invalid. Examples of network problems that prevent the ring poll process from completing are persistent soft errors on the ring that result in ring purges or claim frames. When the network is unstable and there are MAC-less stations or fanout devices inserted in the network, the network's port-to-address mapping may be skewed and the MAC Address-to-Port Security feature may report erroneous security violations.

   Because security violations may be reported erroneously, you should *not* set security to disable ports upon detecting a violation. Instead, set the SET SECURITY PORT ACTION_ON_INTRUSION value to trap_only.

2. You can use the SET SECURITY AUTOLEARN command to instruct the DMM to automatically learn MAC-Address-to-Port correlations. Issuing the command frequently helps to ensure that the DMM's list of valid MAC addresses is up-to-date.

3. To remove all old MAC addresses from the Autolearning database, you must clear both the Autolearn Address table using the CLEAR SECURITY AUTOLEARN <*slot*>.ALL MAC_ADDRESS ALL command and then clear the Security Address database using the CLEAR SECURITY PORT <*slot*>.ALL MAC_ADDRESS ALL command.

Controller Module (8000-RCTL) Issues

This section applies to the IBM Controller Module and contains the following topics:

- RCTL New Features
- Corrected Problems
- Operating Considerations
- Power Management Issues.

Note: This section also applies to the Controller software portion of the A/DMM (Feature Code 1700).

RCTL New Features

This section describes new features for RCTL Versions v1.14 and v1.13.

- RCTL and ARCTL (Fault-Tolerant Controller Module) Version v1.14 support Mastership Priority as a purely priority-driven event. Prior to Version v1.14, any 8260 management took precedence over any 8250 management. Now all management is elected based only on the Mastership Priority settings. However, when an A/DMM is in the same hub as any 8250 management module, the ADMM always wins the Mastership election (this has always been normal operation).

- Fault-Tolerant Controller Module (Feature Code 8000) Version v1.13 provides the following changes to support the A/DMM:

  — Power management initial power budget accounts for the power requirements of the A/DMM.

  — Redundant Controller Boot code Version v1.03 normalizes the power-on arbitration process between an 8260 A/DMM and the 8260 Redundant Controller. This allows the A/DMM to become the active controller when the Advanced Controller Module is installed in the left slot and the Redundant Controller is installed in the right slot of the controller bay.

Corrected Problems

This section describes problems that are fixed in Fault-Tolerant Controller software Version v1.14.

1. Version v1.14 now allows for an 8250 FDDI Management Module to be elected with or without a DMM in the hub. However, no 8250 management module can become master when an A/DMM is in the hub.

2. Version v1.14 corrects mailbox issues with the 8250 carrier modules that were introduced with RCTL and ARCTL Version v1.11 operational code. The problem was with losing configuration settings on the various components that are on this carrier. For example, carrier configurations are 5101M-(EDEK), (SDEK), 5201M-SDEK AB5000.

Note: To prevent configuration loss (on the modules listed previously) when using the DMM-CTLR as the master management module, set the Device Diagnostics to disabled.

3. RCTL Version v1.11 caused an extended election time, which caused a problem with the FMM8250 FDDI Management Module. The FMM never got elected and it also issued a break at the end of 6 seconds, which then caused an infinite election to occur when there was no 8260 management module installed in the hub. Version v1.14 corrects this problem. Beta Version b1.13.7 is no longer required to get an FMM elected.

Operating Considerations

This section describes operating considerations for the controller module at Version v1.14.

1. Version v1.13 is not backward-compatible with earlier versions of controller module software (for example, Versions v1.00, v1.01, v1.02, v1.10, v1.11, or v1.12). Therefore, ensure that all controller modules in the same hub are operating at *Version v1.13 and later*.

2. When updating standby and active controllers, update the standby controller first.

3. When RCTL and ARCTL Version v1.11 was released, this code added support in the election routine to allow for an A/DMM to be elected as master management. This added time to the process, which caused compatibility issues with 8250 management modules.

   Version v1.14 has changed this election process to a single pass operation, which takes less time overall and, therefore, corrects the timing deficiencies for 8250 management use.

Note: Changing to a single pass election scheme has made Management Election a purely priority-driven event. Therefore, there is no priority given to 8260 management over 8250 and the setting of Mastership Priority governs the Mastership Election, except when an 8260 A/DMM is used in conjunction with an 8250 management module. In this case, the A/DMM always becomes the master management module.

Power Management Issues

Consider the following issues when you use the DMM power management feature in Fault-Tolerant Controller software:

1. Configured power management settings *will be* lost for all installed 8260 modules when you perform any of the following actions after powering off the hub:
   - Swap an 8260 module for an 8250 module
   - Swap an 8250 module for an 8260 module
   - Remove a module and leave the slot empty
   - Install an 8250 or 8260 module in a previously empty slot.

2. If the hub exceeds its power budget because of newly inserted 8250 modules, 8260 modules are not powered off automatically. However, the DMM sends a power threshold trap warning of a power utilization problem.

   The hub remains in power deficit until it power cycles, or until a hub reset is performed. At this time, installed controller modules use the remaining power not consumed by 8250 modules to power-enable 8260 modules according to their power class settings. 8260 modules are power-enabled only after all 8250 modules have powered on.

3. Double-fault scenarios in a mixed environment (8260 and 8250 modules) may cause all 8260 modules to power off (for example, when a controller module switchover occurs, followed by a power supply failure within 30 seconds of the switchover).

   To recover from a double-fault scenario:

   a. Power off the hub.

   b. Remove any installed module.

   Upon power-on, installed controller modules assess the power budget. When the 8260 modules previously powered off are powered on again, power configuration values are configured to factory defaults.

4. When the power required by installed 8250 modules is greater than the capacity of the first power supply that you switch on, switch on all installed power supplies at the same time to avoid the possible shutdown of one or more power supplies.

   For example, if you switch on one power supply at a time, the first power supply you switch on may become overloaded and shut down before a second power supply can power on and share the load. If a power supply shuts down due to an overload, wait at least 10 seconds before you attempt to switch on that power supply again.

Caution: If a power supply shuts down due to an overload, wait at least 10 seconds before you attempt to switch on that power supply again.

8260 Module Code Versions

Table 1 lists the most recently released code versions (except for modules that still use Version v1.00 code) for 8260 non-ATM modules. If you need to upgrade to any of these versions, contact your IBM Representative or get the latest microcode upgrades from the Internet at URL http://www.networking.ibm.com.

Table 1. Latest 8260 Module Code Versions

Version	Module Feature Code
TR Active Per Module card operational v1.50	3118
TR Active Per Port card operational v1.50	3018
TR Dual Fiber Repeater card operational v1.50	3010
TR Passive Per Module card operational v1.50	3020
T-MAC Card boot v2.00	8913
T-MAC Card operational v4.00	8913
T-MAC Card trchipset v4.00	8913
High-end Token Ring Medium Access Control Card boot v1.01	8925
High-end Token Ring Medium Access Control Card operational v2.10	8925
10BASE-FB Media card operational v1.05	1110, 1210, 1310
24-Port 10BASE-T Module boot v1.02	1024
24-Port 10BASE-T Module operational v1.04	1024
36-Port 10BASE-T Module operational v1.01	1036
Ethernet Flexible Concentration Module operational v1.01	1004
Ethernet MAC Card boot v1.01	8918
Ethernet MAC Card operational v3.00	8918
High-end Ethernet Medium Access Control Card operational v2.10	8924
Ethernet Security Card (E-SEC) operational v1.01	8915
DMM boot v1.01	1000, 1100
DMM operational v2.30	1000, 1100
DMM boot v1.03	1200 and 1300
DMM operational v5.25	1200, 1300
A/DMM boot v1.03	1700
A/DMM operational v5.25	1700
Redundant Controller boot v1.03	8000
Redundant Controller operational v1.15	8000
Advanced Redundant Controller (ARCTL) boot v1.04	1700
Advanced Redundant Controller (ARCTL) operational v1.15	1700

Table 1. Latest 8260 Module Code Versions (Continued)

Version	Module Feature Code
PacketChannel/ATM Switching Module boot v2.05	7302
PacketChannel/ATM Switching Module operational v2.11	7302
Switching Modules boot v1.12	7304, 7310, 7312, 7314, 7320, 7324, 7404, 7412, 7504
Switching Modules operational v2.15	7304, 7310, 7312, 7314, 7320, 7324, 7404, 7412, 7504
Switching Modules boot v1.04	7304-A, 7310-A, 7312-A, 7314-A, 7320-A, 7324-A, 7404-A, 7412-A, 7504-A, 7016-A, 7524-A, 7620-A, and 7618-A
Switching Modules operational v2.15	7304-A, 7310-A, 7312-A, 7314-A, 7320-A, 7324-A, 7404-A, 7412-A, 7504-A, 7016-A, 7524-A, 7620-A, and 7618-A
TR Active Per Module card operational v1.50	3118