Software Release Summary

This appendix describes the changes made to previously released versions of the Catalyst Switch software.

Initial Release

Known Issues and Workarounds

1 When you set the Internet Protocol (IP) address using the **ifconfig** command, you must explicitly set the netmask and broadcast addresses to the desired values. If this is not done, network management applications do not recognize those values.

> **Caution**   If the Catalyst 1200 switch is reset, the netmask changes to the default netmask for the assigned class address. You must then use the **ifconfig** command to reset the netmask and broadcast addresses to the desired values.

2 Giant packet counters are not incremented in the **display mac** command. The **display mac** command displays parameters for the Media Access Control (MAC) layer for each port of the switch.

DMP Version 1.4, NMP Version 1.3

Known Issues and Workarounds

1 When you set the IP address using the **ifconfig** command, you must explicitly set the netmask and broadcast addresses to the desired values. If this is not done, network management applications do not recognize those values.

Caution   If the Catalyst 1200 switch is reset, the netmask changes to the default netmask for the assigned class address. You must then use the **ifconfig** command to reset the netmask and broadcast addresses to the desired values.

2 Giant packet counters are not incremented in the **display mac** command. The **display mac** command displays parameters for the MAC layer for each port of the switch.

3 Data frames on FDDI networks *less than* 25 bytes long may be discarded. This may cause network connection loss on FDDI-attached stations using protocols that use *less than* 25 byte frames, such as NETBIOS and NetBEUI.

Note   This does not affect Ethernet-to-Ethernet through FDDI connections.

DMP Version 1.6, NMP Version 1.3

Known Issues and Workarounds

1 If the netmask is not set using the **ifconfig** command, the Catalyst 1200 switch is unable to communicate through the IP network using, for example, the **ping**, **download**, and other commands.

2 Enabling a disabled port when spanning tree is active causes that port to change to a permanent blocked state. To eliminate the blocked state after enabling the port, disable then enable spanning tree.

DMP Version 2.3, NMP Version 2.3

Resolved Issues

The following issues were resolved during this revision of the Catalyst Series software:

1 Subnet mask changes set using commands other than **ifconfig** would not allow communication through the IP network.

Known Issues and Workarounds

1 DMP and NMP Versions 2.3—If a port is disabled, the **show port** command displays the status of the disabled port as ok instead of the correct status of disabled.

Workaround:

The **show port** command displays the actual hardware status of all the ports in the switch. The **disable port** command available through the admin. interface does not change the hardware status of the ports and all the ports are still shown as ok. However, to get the software status of the ports, use the **show bridge** command.

2 DMP and NMP Versions 2.3—When an FDDI or Ethernet port is physically disconnected or when the **disconnect** command is used to disconnect a switch port from the ring, spanning tree still considers the port to be in forwarding state. Therefore the **show bridge** command displays the port to be in forwarding state.

Workaround:

The **disconnect** command temporarily disconnects a switch from the FDDI ring. Therefore, this information is not passed to the spanning tree and the **show bridge** command shows that the port is still in forwarding state. Spanning tree is informed that the port is being disabled only when the user uses the **disable port** command.

3 DMP and NMP Versions 2.3—When the switch receives fragmented ping packets destined to itself on an FDDI interface, the terminal admin. interface session stops. However, the switch still responds to any ping and Telnet requests.

Workaround:

This problem can be eliminated by not sending fragmented ping packets to the switch on the FDDI ring. Reset the switch to clear the terminal stop situation.

4   DMP and NMP Versions 2.3—When the IP address of the switch is changed from one class to another, you may not be able to delete the static routes defined for the previous class.

Workaround:

The only way to delete those entries is to reboot the switch.

5   DMP and NMP Versions 2.3—When the switch Content Addressable Memory (CAM) table has many MAC entries and the switch is very busy bridging, the **show cam** command displays the CAM entries on the screen at a slower rate. This is because the admin. interface receives a lower priority and the screen display can become slower as a result.

Workaround:

If your CAM table has many entries, you should use the **cam lookup** command to track any of the MAC addresses in the CAM table. You should not use the **show cam** command under very busy switch conditions.

6   DMP and NMP Versions 2.3—This release of the switch software allows users to control the display screen scrolling by using the **set length** command. However, if the screen length is set to a finite value, the switch CAM table is full, and the user issues the **show cam** command the switch might truncate the display on the screen because of its limited buffer allocation for the screen display.

Workaround:

You should use the **cam lookup** command to look up for any MAC entries in the cam table instead of using the **show cam** command which dumps all the MAC entries on the screen. If you use the **show cam** command, you should set the length to zero using the **set length** command.

Caveat

1 Giant Packets—When any Ethernet or FDDI port receives a giant packet (greater than 1,714 bytes), the switch resets. To eliminate this problem perform, set the **encheck** parameter to on.

Note The largest valid frame is a 1514-byte + 4 byte cyclic redundancy check (CRC). If your network does not use frames larger than 1714 bytes, you do not need to modify this parameter.

By default, the **encheck** parameter is turned off. To turn the **encheck** parameter on, perform the following steps:

Note Be sure that you set up a terminal session into the switch by connecting a terminal to the EIA/TIA-232 port of the switch. Do not use a Telnet session to the switch to modify this parameter.

Step 1 At the Catalyst user prompt, change to privileged mode by entering **enable**.

Step 2 At the prompt, enter **show optimization** and press **Return**.

The system displays the following:

```
Console> (enable) show optimization
encheck = off
enrx = 0x20
entx = 0x10
fddirx = 0x100
fdditx = 0x10
Console> (enable)
```

Step 3 Check the **encheck** parameter. If the parameter is set to on, the system handles giant packets efficiently without resetting the switch. If the **encheck** parameter is set to off, proceed to the next step.

Step 4   At the prompt, enter **set optimization encheck on** and press **Return** to change the **encheck** parameter. Following is an example:

```
Console> (enable) set optimization ?
Usage: set optimization encheck <on|off>
       set optimization enrx <value>
       set optimization entx <value>
       set optimization fddirx <value>
       set optimization fdditx <value>
       set optimization default
Console> (enable) set optimization encheck on
```

The system responds with the following confirmation message:

```
This command will reset and restart the system for Ethernet
re-configuration.
Do you want to continue (y/n) [n]?
```

Step 5   Enter **y** to continue.

This enables the **encheck** parameter and the switch reboots itself to make the change in the system configuration. This change prevents the switch from resetting when it receives a giant packet in the future.

DMP Version 2.5

Resolved Issues

The following issues were resolved during this revision of the Catalyst 1200 switch software:

1   Under certain circumstances the Catalyst switch would report a large number of giant packets on a port causing that port to reinitialize frequently. This problem occurred due to a race condition between the DMP RISC processor and the SONIC processor while processing the received packets on that port.

2   When a Catalyst switch received FDDI subnetwork access protocol (SNAP) frames other than IP, Internet Protocol Exchange (IPX), or AppleTalk, the switch was converting them into an incorrect format.

Known Issues and Workarounds

1   When using the **set cam** command to enter static entries into the CAM table, any MAC address with the 00 as the last byte is treated as an invalid address.

2   When using the **set route** command to add routing table entries with a metric value 1 the Catalyst switch defaults to a metric value 0 although the default is 1.

   Workaround:

   When entering a metric value 1, always enter the desired metric value.

3   If a port is disabled, the **show port** command displays the status of the disabled port as ok instead of the correct status of disabled.

   Workaround:

   The **show port** command displays the actual hardware status of all the ports in the switch. The **disable port** command available through the admin. interface does not change the hardware status of the ports, and all the ports are still shown as ok. However, to get the software status of the ports, use the **show bridge** command.

4   When an FDDI or Ethernet port is physically disconnected, or when the **disconnect** command is used to disconnect a switch port from the ring, the spanning tree still considers the port to be in the forwarding state. Therefore the **show bridge** command displays the port as in the forwarding state.

   Workaround:

   The **disconnect** command temporarily disconnects a switch from the FDDI ring. Therefore, this information is not passed to the spanning tree and the **show bridge** command still shows that the port is in forwarding state. Spanning tree is informed that the port is being disabled only when you use the **disable port** command.

5   When the switch receives fragmented ping packets destined to itself on an FDDI interface, the terminal admin. interface session stops. However, the switch still responds to any ping and Telnet requests.

   Workaround:

   This problem can be eliminated by not sending fragmented ping packets to the switch on the FDDI ring. Reset the switch must to clear the terminal stop situation.

6 When the IP address of the switch is changed from one class to another, you may not be able to delete the static routes defined for the previous class.

Workaround:

The only way to delete those entries is to reboot the switch.

7 When the switch CAM table has many MAC entries and the switch is very busy bridging, the **show cam** command displays the CAM entries on the screen at a slower rate. This is because the admin. interface receives a lower priority and the screen display can become slower as a result.

Workaround:

If your CAM table has many entries, you should use the **cam lookup** command to track any of the MAC addresses in the CAM table. You should not use the **show cam** command under very busy switch conditions.

8 This release of the switch software allows users to control the display screen scrolling by using the **set length** command. However, if the screen length is set to a finite value, the switch CAM table is full, and the user issues the command **show cam**, the switch might truncate the display on the screen because of its limited buffer allocation for the screen display.

Workaround:

You should use the **cam lookup** command to look up any MAC entries in the CAM table instead of using the **show cam** command which dumps all the MAC entries on the screen. If you choose to use the **show cam** command, you should set the length to zero using the **set length** command.

Caveat

1 Giant Packets—When any Ethernet port receives a giant packet (greater than 1,714 bytes), the switch resets. To eliminate this problem, set the **encheck** parameter to on.

Note   The largest valid frame is a 1,514-byte + 4-byte cyclic redundancy check (CRC). If your network does not use frames larger than 1,714 bytes, you do not need to modify this parameter.

By default the **encheck** parameter is turned off. To turn the **encheck** parameter on, perform the following steps:

Note   Be sure that you set up a terminal session into the switch by connecting a terminal to the EIA/TIA-232 port of the switch. Do not use a Telnet session to the switch to modify this parameter.

Step 1   At the Catalyst user prompt, change to privileged mode by entering **enable**.

Step 2   At the prompt, enter **show optimization** and press **Return**.

The system displays the following:

```
Console> (enable) show optimization
encheck = off
enrx = 0x20
entx = 0x10
fddirx = 0x80
fdditx = 0x80
```

Step 3   Check the **encheck** parameter. If the parameter is set to on, the system handles giant packets efficiently without resetting the switch. If the **encheck** parameter is set to off, proceed to the next step.

Step 4 At the prompt, enter **set optimization encheck on** and press **Return** to change the **encheck** parameter. Following is an example:

```
Console> (enable) set optimization ?
Usage: set optimization encheck <on|off>
       set optimization enrx <value>
       set optimization entx <value>
       set optimization fddirx <value>
       set optimization fdditx <value>
       set optimization default
Console> (enable) set optimization encheck on
```

The system responds with the following confirmation message:

```
This command will reset and restart the system for Ethernet
re-configuration.
Do you want to continue (y/n) [n]?
```

Step 5 Enter **y** to continue.

This enables the **encheck** parameter and the switch reboots itself to make the change in the system configuration. This change prevents the switch from resetting when it receives a giant packet in the future.

DMP Version 3.1, NMP Version 3.1

Modifications

The following modifications have been made since the previous release:

1 When the **set optimization** command variable **encheck** was set to on, false giant packets were being reported, causing poor switch performance. With this version of Flash code, if giant packets are received, the **encheck** parameter is automatically set to on, eliminating the problem.

2 The **set tlmin** command has been added to set the time required for Physical Layer Protocol (PHY) hardware to transmit a given line state before advancing to the next physical connection management (PCM) state at the station management (SMT) level. The *port_num* should be 1 or 2, and the *hexvalue* should be between 0 and 0xffff. The *tl_min* setting is stored in the TL_MIN register (also known as the LS_MAX register) as part of the SMT management information base (MIB) structure in nonvolatile memory, and is used for initializing the PHY hardware setting each time the switch is rebooted.

```
Console> (enable) set tlmin ?
Usage: set tlmin <port_num> <hexvalue>
       (hexvalue is in 2's complement)
Console> (enable) set tlmin 1 fdfd
Port 1 tlmin set to 0xfdfd.
Console> (enable)
```

3 Some FDDI SNAP frames with the proprietary organizationally unique identifier (OUI) field were not being translated correctly. This version of Flash code corrects this problem.

4 Performance enhancements have been made to boost the Catalyst switch performance significantly while handling broadcast frames at wire speed.

5 All non-ODI (open data-link interface) IPX drivers and some other LAN drivers that were sensitive to 802.3 frame length were experiencing connectivity problems with the Catalyst switch. This version of Flash code corrects this problem.

6 Static CAM entries were not allowed with the last byte set to 00. This version of Flash code corrects this problem.

7 Static CAM entries were not being handled correctly. This version of Flash code corrects this problem.

Caveats

The following caveats have been identified and workarounds provided:

1 The SUM port (sc0) IP address scheme has changed with Catalyst Switch Software Release 3.1. The switch IP address previously assigned to the SUM port will now, by default, be assigned to route group 1. Route group 1 will include all ports of the switch including the FDDI port. The SUM port (sc0) will be set to IP address 0.0.0.0. The SUM port will not be part of the default route group 1, and will not be able to communicate with the switch.

Workaround:

The SUM port must be assigned a unique IP address to allow communication with the switch.

2 Aborting serial download will cause an NMP exception error when you enter the **show interface** command at the admin port.

Workaround:

Do not abort a serial download. Let the serial download complete. If you do abort a serial download, reset the switch and reinitiate the serial download.

3 The Catalyst switch may continue to learn routes using the router interface protocol (RIP), but cannot route packets on interfaces that are administratively set to down using the **set interface** *port#* **down** command.

Note The switch can still bridge data on interfaces administratively configured as down.

Workaround:

To stop learning RIP updates on an interface, disable the port using the **set port** *port#* **disable** command.

4 The **show bridge** command displays an FDDI port to be forwarding even though it is disconnected physically or disconnected using the **disconnect fddi** command. The erroneous status is displayed because the bridge still considers the FDDI port to be in the forwarding state. This is because the **disconnect fddi** command only *temporarily* disconnects the switch from the FDDI ring.

Workaround:

The spanning tree is informed that the FDDI port is disabled only when you use the **disable port 1** command.

5 Use the **connect fddi** and **disconnect fddi** commands carefully while the switch is bridging and routing traffic. If you use the **connect fddi** command, the connect state LED may change to orange, indicating a minor alarm.

Workaround:

Reissue the **disconnect fddi** command and then reconnect the port using the **connect fddi** command until the connect state LED changes to GREEN, indicating no alarms.

6 Terminal sessions may freeze if the switch receives fragmented Internet Control Message Protocol (ICMP) packets destined to itself on the FDDI ring. The switch will still respond to any ping and Telnet requests destined to it, and bridge or route any packets.

Workaround:

Reset the switch to eliminate the frozen terminal session.

7 The switch does not automatically delete the default route if the routing group configuration is changed using the **set routegroup** command. For example:

- A switch has a default route set to 199.133.219.42, which is part of a route group 199.133.219.161.

- The user deletes or reconfigures the route group 199.133.219.161 to be part of 194.133.216.219.

- The default route is still set as 199.133.219.42 and is *not* deleted.

- The switch will not allow a new default route to be configured until you manually delete the default route group 199.133.219.42.

Workaround:

If you remove an IP network from your routing group, delete the corresponding default route using the **clear route default** command.

NetScout RMON Caveats

1 The Resource Manager, Remote Login, and Token Ring Main screen icons are not supported by the NetScout Manager software and should not be used.

2 If the screen appears frozen or unresponsive, this may be due to a series of unintentional actions by the user. For example, if both the Main screen and the Add Agent submenu screen are opened at the same time and you click on an inappropriate button (for example, **cancel**) the Main screen will move to the front, obscuring the Add Agent submenu. However, the Add Agent submenu screen will remain active in the background, making the Main screen inaccessible.

You must complete all submenu actions items before you can activate other Main menu items.

Workaround:

Reduce the frozen screen(s) to icons to find the active submenu screen hidden behind them. You must close the active submenu screen before you can make another Main menu selection.

3 From the Main screen menu, all other submenus require only one click of the mouse to activate. If you click twice on a selection, two instances of the same selection will be activated, causing multiple instances of the same function with overlapping screens. Multiple instances of the same submenu are a drain on the Client and Agent resources, and should be closed when not in use.

> **Note**   The submenus of the Main Screen are independent and can be activated from the Main menu screen with a single click of the mouse button.

4   The Client may run out of resources because you have too many processes open at the same time for the amount of RAM and swap space configured in the Client workstation. The agent may also run out of resources due to limited memory availability.

The Catalyst Switch will attempt to install all possible resources using the available memory. If the switch cannot successfully install all of the enabled groups for the chosen domain, it will install as many as possible and display the following error messages:

```
no resources...
could not install
```

5   If the system appears slow to respond to a command, the possible causes are:

- The network is very busy, causing the Client to retransmit the messages to the agent for proper responses.

- The screens that generate graphic displays, for example, pie charts and bar graphs may be compiling data needed to generate the graphic display. Initial screen updates may take up to a minute or longer while the system command is sent to the probe, and an initial period of 15 seconds is required for the agent to wait for updated information before returning a screen update.

6   If you use the Config option from the Main screen to configure RMON, the system does not respond when the configuration has been completed.

> **Note**   RMON configuration may take up to two minutes to complete.

Workaround:

Use the Domain Management menu to confirm the completion of the RMON configuration, or use the Domain Manager submenu from the Main menu screen to install logical agents.

7 While communicating with an agent, an error message similar to the following may appear:

```
-- Error accessing agent < agent name >
   While retrieving Domains
   Error: cannot communicate with agent
```

This error message does not indicate that the Catalyst switch is down. This error message may be caused by one or more of the following conditions:

- Busy network
- Two clients are accessing the same agent at the same time
- Not enough socket resources in the TCP/IP stack

Workaround:

To verify the Catalyst switch state, ping the switch or refer to the console window to determine the exact nature of the problem.

8 You should not modify the sample configuration files with the file extension .cfg, stored in the *usr/nohome/samples* directory. These files should be copied to the user's working directory and modified to create user-specific configuration files.

> **Caution**   If the sample configuration files become corrupted, you must reinstall the RMON to create new sample configuration files.

9 The two terms *segment* and *domain* have different meanings in the NetScout Manager context:

- Domain means an aggregate of protocol filters supported by the NetScout Manager.

- Segment means the network itself, or the subnet, which is fully connected.

Note For a subnet of nodes to form a segment, the nodes do not have to be separated by bridges, routers, or gateways.

To specify segments, a drawing of all nodes including bridges, routers, and gateways, should be made. This facilitates interpretation of the collected data and the comparison of the various segments in terms of various data collection activities and remote monitoring of the MIBs.

10 When creating logical agents using the Edit window, any of the following entries will generate an SNMP error code 3:

- Incorrect interface number

- Incorrect Read community name

- Incorrect Write community name

Workaround:

Correct the mistakes by editing the configuration file associated with that agent and then reinstalling the file.

Note The correct interface number range is 3 through 10.