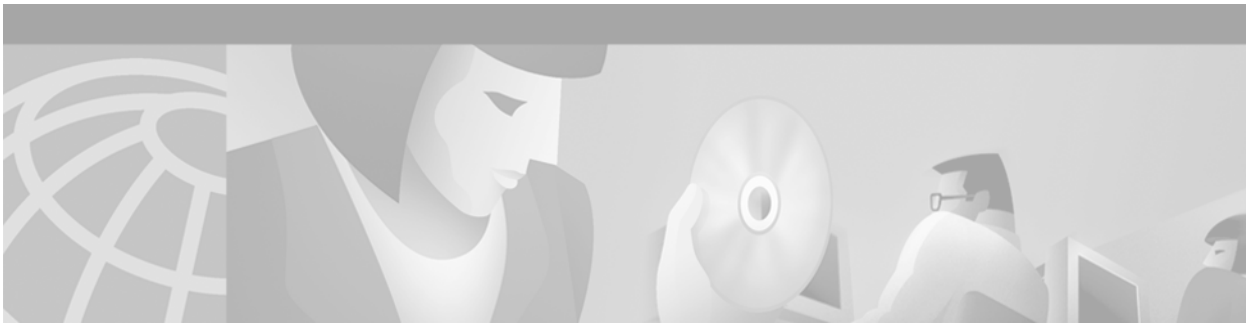


Release Notes for CDDI/FDDI Workgroup WS-C1400 Concentrator Release 1.10

Release 1.10
May 13, 2002

These release notes describe the features and caveats for CDDI/FDDI Workgroup WS-C1400 Concentrator Software Release 1.10. Refer to the *CDDI/FDDI C1400 Concentrator Installation and Configuration Guide* for detailed information about the CDDI/FDDI Workgroup WS-C1400 Concentrator.

This document is divided into the following sections:

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Software Release 1.10 Introduction

The following sections describe the caveats and corrected caveats in Software Release 1.9.

Software Release 1.10 Caveat Corrections

This section describes caveats that have been corrected in Software Release 1.10 .

- Under rare circumstances, resetting a FDDI attached ags+ on the same ring as a C1400 may cause the C1400 to leave the ring permanently.

  To resolve this problem, configure an automatic system reboot when this fault condition occurs using this new CLI command:

  set reset {**none**| **onringoff** | **test**}

  none—default

  onringoff —resets the system when the fault condition is detected

  test—resets the system now

  The configuration is stored in NVRAM.

  [CSCdw45943]

Software Release 1.10 Caveats

This section describes the caveats for Software Release 1.9.

- When the IP address of a concentrator is changed from one class to another, the old IP broadcast address is retained. You must explicitly set the new broadcast address by using the following command:

```
Console> (enable) set ipaddress new_ipaddress new_netmask new_broadcastaddress
```

- When dynamically changing the subnet mask for an IP address, old entries might exist in the routing table. To clear the old entries from the routing table, reset the concentrator, identifying the old IP addresses, as follows:

```
Console> (enable) set ipaddress old_ipaddress old_netmask
```

- When setting port path from Primary to Secondary, the change is evident in show port, but not in show config. This may cause a conflict after a concentrator is power cycled. [CSCdj15942]
- When continuously polling the MIB variable fddimibPORTConnectState, the WS-C1400 will occasionally return an incorrect value of disabled for a port that is not disabled. [CSCdj64908]
- In a 32-port configuration, with all ports connected, the last port (port 2/16) retains an Ler Est of 16 after a system reset instead of changing to 15 like all the other ports. The problem occurs because the Link Error Monitor is not started on the last port. In order to correct the problem manually, you can issue a **clear lem** command or a **clear port** command. Both of these commands will start the LEM on all ports. [CSCdi29983]
- After hot swapping a module in a C1400 running software version 1.213, the **show mac** command displays only the primary MAC address and not the secondary MAC address. [CSCdi31272]

Software Release 1.9 Introduction

The following sections describe the caveats and corrected caveats in Software Release 1.9.

Software Release 1.9 Caveat Corrections

This section describes caveats that have been corrected in Software Release 1.9 .

- Under some circumstances the C1400 will lose IP connectivity to the network (data is still switched normally), crash, or hang the system console. This caveat is fixed in this release of the concentrator software. [CSCdj02108]
- Under some circumstances, the C1400 concentrator with the WS-X1450 module installed resets without logging stack information. This caveat is fixed in this release of the concentrator software. [CSCdj12458]
- The C1400 concentrator sends SNMP traps incorrectly using an IP address tag, which causes some NMS systems to ignore these traps. This caveat is fixed in this release of the concentrator software. [CSCdm44214]
- If the interrupt level shows an “interrupt level not zero count,” the system could hang. This caveat is fixed in this release of the concentrator software.

Software Release 1.9 Caveats

This section describes the caveats for Software Release 1.9.

- When the IP address of a concentrator is changed from one class to another, the old IP broadcast address is retained. You must explicitly set the new broadcast address by using the following command:

```
Console> (enable) set ipaddress new_ipaddress new_netmask new_broadcastaddress
```

- When dynamically changing the subnet mask for an IP address, old entries might exist in the routing table. To clear the old entries from the routing table, reset the concentrator, identifying the old IP addresses, as follows:

```
Console> (enable) set ipaddress old_ipaddress old_netmask
```

- When setting port path from Primary to Secondary, the change is evident in show port, but not in show config. This may cause a conflict after a concentrator is power cycled. [CSCdj15942]
- When continuously polling the MIB variable fddimibPORTConnectState, the WS-C1400 will occasionally return an incorrect value of disabled for a port that is not disabled. [CSCdj64908]
- In a 32-port configuration, with all ports connected, the last port (port 2/16) retains an Ler Est of 16 after a system reset instead of changing to 15 like all the other ports. The problem occurs because the Link Error Monitor is not started on the last port. In order to correct the problem manually, you can issue a **clear lem** command or a **clear port** command. Both of these commands will start the LEM on all ports. [CSCdi29983]
- After hot swapping a module in a C1400 running software version 1.213, the **show mac** command displays only the primary MAC address and not the secondary MAC address. [CSCdi31272]

Software Release 1.8 Introduction

The following sections describe the features, caveats, and corrected caveats in Software Release 1.8.

New Features in Software Release 1.8

This section describes the Module-Priority Attachment Mode, a new feature in CDDI/FDDI Workgroup WS-C1400 Concentrator Software Release 1.8.

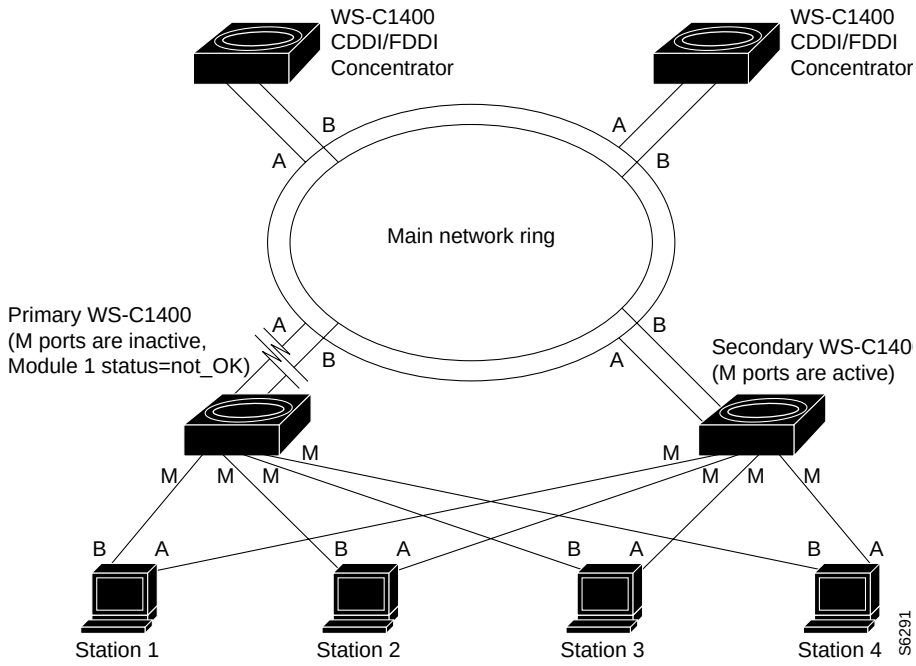
A WS-C1400 concentrator in module-priority attachment mode functions like a concentrator that is in dual-attachment mode, except that Module 1 must be present, enabled, and functional before any master (M) port can connect. If Module 1 experiences a major or minor hardware failure or is disabled or removed, the M ports report as inactive and are disabled.

Module-priority attachment mode can be used to switch a primary WS-C1400 to a secondary WS-C1400 if the primary concentrator loses the main network ring connection due to the removal, disabling, or failure of Module 1. Figure 1 shows an example of a primary and secondary WS-C1400 configuration during a failover.

Note If you are using SNMP to manage the WS-C1400 while in module-priority attachment mode, you must update the *CISCO-STACK-MIB.my* file. You can obtain the latest version of the *CISCO-STACK-MIB.my* file from the Cisco Systems FTP site. Refer to the "Using FTP to Obtain the MIB File" section later in this document.

You can also obtain the *CISCO-STACK-MIB.my* file from Cisco Connection Online (CCO). Refer to the "Obtaining Documentation" section later in this document for information about using CCO.

Figure 1 WS-C1400 Configuration During a Failover



To enable module-priority attachment mode, enter the following command from the command-line interface (CLI):

```
Console> (enable) set attach modpri
```

Once the **set attach modpri** command is executed, the following message is displayed:

```
Attachment type changed to module-priority attach.
```

The following applies to module-priority attachment:

- When the primary WS-C1400 detects that Module 1 is inactive—a condition that can cause a failover—approximately 2 seconds elapse before the concentrator deactivates the active master (M) ports. Use the **show port** command to display the primary concentrator current M-port status, as follows:

```
Console> (enable) show port
Port  Name                 Status      Req-Path   Cur-Path   Type  Neigh
----  -------------------- ----------  ---------  ---------  ----  -----
1/1                        notconnect  secondary  isolated    A     U
1/2                        notconnect  primary    isolated    B     U
1/3                        inactive    primary    isolated    M     U
1/4                        inactive    primary    isolated    M     U
:
:
1/16                       disabled    primary    isolated    M     U
2/1                        inactive    primary    isolated    M     U
:
:
```

```
2/8                          inactive    primary    isolated    M     U
```

Note Module-priority attachment mode does not affect ports that you disable. All ports that you disable remain disabled until configured otherwise. All disabled ports are identified as **disabled** in the **show port** command display.

- When changing the attachment mode from module-priority to dual-priority after a failover, the M ports are activated if Module 1 is enabled.
- When using the **set port** command during a failover, the following message is displayed:

```
Console> (enable) set port 2/9 enable
Port 2/9 inactive due to dual priority attachment mode in effect.
```

  In this case, the port is enabled in NVRAM. However, it is set to inactive during the failover. When the main network ring connection is restored, the port is activated. Use the **show port** command to display the current M-port status.

- When disabling an M-port during a failover, the port is disabled in NVRAM.
- When enabling Module 1 during a failover, the M-port state remains inactive until Module 1 is online. The following message is displayed:

```
Console> (enable) set module 1 enable
Module 1 M-ports may be inactive due to module priority attach mode in effect.
```

- When enabling Module 2, the ports remain inactive if Module 1 is not functional. The following message is displayed:

```
Console> (enable) set module 2 enable
Module 2 ports inactive due to module priority attach mode in effect.
```

- When setting the WS-C1400 to module-priority attachment mode from either null- or single-attachment mode, the following message is displayed:

```
Attachment type changed to module-priority attach.
Must reset concentrator for this to take effect!
```

  At this point, you must reset the WS-C1400 before module-priority attachment takes effect. There is no need to reset the concentrator when you switch between module-priority, dual-priority, and dual-attachment modes.

Software Release 1.8 Caveat Corrections

This section describes caveats that have been corrected in the 1.8 release.

- It is possible to set an invalid date, such as February 29th, on a year that is not a leap year. This caveat is fixed in this release of the concentrator software. [CSCdj20518]
  For reference, see also CSCdj20509 and CSCdj20543.
- The concentrators are vulnerable to the LAND.C Denial of Service Attack program. This caveat is fixed in this release of the concentrator software. [CSCdj62723]

Software Release 1.8 Caveats

This section describes the caveats for Release 1.8.

- When the IP address of a concentrator is changed from one class to another, the old IP broadcast address is retained. You must explicitly set the new broadcast address by using the following command:

```
Console> (enable) set ipaddress new_ipaddress new_netmask new_broadcastaddress
```

- When dynamically changing the subnet mask for an IP address, old entries might exist in the routing table. To clear the old entries from the routing table, reset the concentrator, identifying the old IP addresses, as follows:

```
Console> (enable) set ipaddress old_ipaddress old_netmask
```

- When setting port path from Primary to Secondary, the change is evident in show port, but not in show config. This may cause a conflict after a concentrator is power cycled. [CSCdj15942]
- When continuously polling the MIB variable fddimibPORTConnectState, the WS-C1400 will occasionally return an incorrect value of disabled for a port that is not disabled. [CSCdj64908]

Software Release 1.7 Introduction

The following section describes caveats and caveats that have been corrected for Release 1.7.

Software Release 1.7 Caveat Corrections

The following caveat is resolved in Release 1.7: When a standby PHY-A port transitions up and down due to normal standby port activity, the dual-homed concentrator no longer sends SNMP trap messages. [CSCdi66807]

Software Release 1.7 Caveats

This section describes the caveats for Release 1.7.

- When the IP address of a concentrator is changed from one class to another, the old IP broadcast address is retained. You must explicitly set the new broadcast address by using the following command:

```
Console> (enable) set ipaddress new_ipaddress new_netmask new_broadcastaddress
```

- When dynamically changing the subnet mask for an IP address, old entries might exist in the routing table. To clear the old entries from the routing table, reset the concentrator, identifying the old IP addresses, as follows:

```
Console> (enable) set ipaddress old_ipaddress old_netmask
```

- When setting port path from Primary to Secondary, the change is evident in show port but not in show config. This may cause a conflict after a concentrator is power cycled. [CSCdj15942]
- When continuously polling the MIB variable fddimibPORTConnectState, the WS-C1400 will occasionally return an incorrect value of disabled for a port that is not disabled. [CSCdj64908]

Software Release 1.6 Introduction

The following sections describe features, caveats, and caveat corrections for Release 1.6.

New Features in Software Release 1.6

The following enhancements added to Release 1.6 are described in the following sections:

- Dual-Priority Attachment Mode
- Ring-Map Enable/Disable

Dual-Priority Attachment Mode

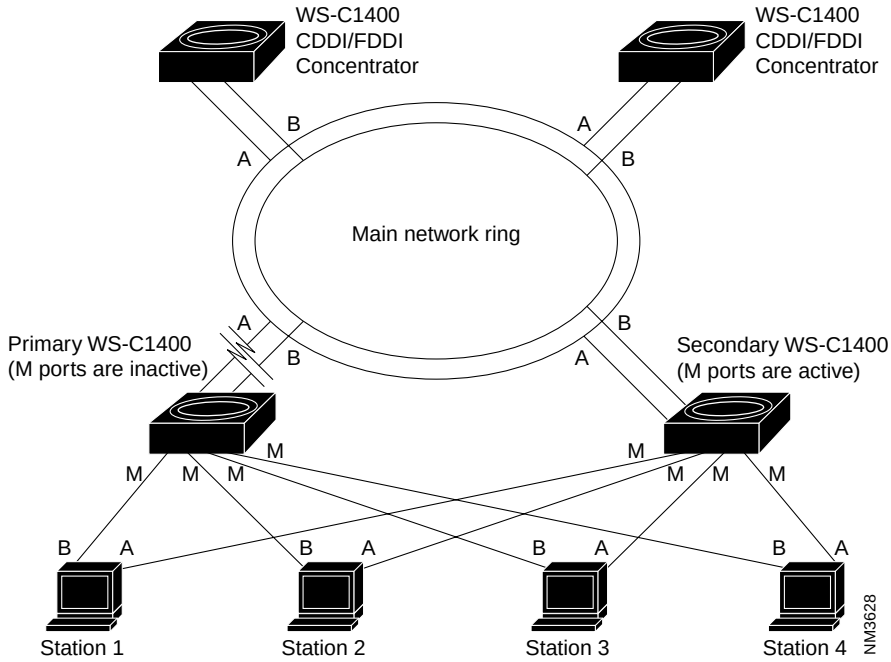
A WS-C1400 concentrator in dual-priority attachment mode functions like a concentrator that is in dual-attachment mode, except that the A or B ports must be active before any master (M) port can connect. If the A or B ports are not active, the M ports will report as inactive and are disabled until either the A or B port becomes active.

Dual-priority attachment mode can be used to switch a primary WS-C1400 to a secondary WS-C1400 if the primary loses the main network ring connection via the A and B ports. Figure 2 shows an example of a primary and secondary WS-C1400 configuration during a main network ring disconnect.

Note If you are using SNMP to manage the WS-C1400 while in dual-priority attachment mode, you must update the *CISCO-STACK-MIB.my* file. You can obtain the latest version of the *CISCO-STACK-MIB.my* file from the Cisco Systems FTP site. Refer to the "Using FTP to Obtain the MIB File" section later in this document.

You can also obtain the *CISCO-STACK-MIB.my* file from Cisco Connection Online (CCO). Refer to the "Obtaining Documentation" section later in this document for information about using CCO.

Figure 2 WS-C1400 Configuration During a Main Network Ring Disconnect



Note It is recommended that you set the primary WS-C1400 to dual-priority attachment mode and set the secondary WS-C1400 to dual-attachment mode when only two concentrators are connected to the main network ring or when two concentrators are connected back-to-back.

To enable dual-priority attachment mode, enter the following command from the command-line interface (CLI):

```
Console> (enable) set attach dualpri
```

Once the **set attach dualpri** command is executed, the following message is displayed:

```
Attachment type changed to dual-priority attach.
```

The following applies to dual-priority attachment:

- When the primary WS-C1400 detects a main network ring disconnect, approximately 2 seconds elapse before the concentrator disables the active master (M) ports. Use the **show port** command to display the primary concentrator current M-port status:

```
Console> (enable) show port
Port  Name                 Status      Req-Path   Cur-Path   Type  Neigh
----  -------------------  ----------  ---------  ---------  ----  -----
1/1                        notconnect  secondary  isolated    A     U
1/2                        notconnect  primary    isolated    B     U
1/3                        inactive    primary    isolated    M     U
1/4                        inactive    primary    isolated    M     U
:
:
1/16                       disabled    primary    isolated    M     U
2/1                        inactive    primary    isolated    M     U
:
:
2/8                        inactive    primary    isolated    M     U
```

Note Dual-priority attachment mode does not affect ports that you disable. All ports that you disable remain disabled until configured otherwise. All disabled ports are identified as **disabled** in the **show port** command display.

- When changing the attachment mode from dual-priority to dual after a main network ring disconnect, the M ports are active.
- When using the **set port** command during a main network ring disconnect, the following message is displayed:

```
Console> (enable) set port 1/9 enable
Port 1/9 inactive due to dualpriority attachment mode in effect.
```

  The port is enabled in NVRAM. However, it is set to inactive during the disconnect. When the main network ring connection is restored, the port is active. Use the **show port** command to display the current M-port status.

- When disabling an M-port during a main network ring disconnect, the port is disabled in NVRAM.
- When enabling module 1 during a main network ring disconnect, the M-port state remains inactive until the A or B port is reconnected to the ring. The following message is displayed:

```
Console> (enable) set module 1 enable
Module 1 M-ports may be inactive due to dual attach priority mode in effect.
```

- When enabling module 2, the ports remain inactive if the main network ring connection is not restored. The following message is displayed:

```
Console> (enable) set module 2 enable
Module 2 ports inactive due to dual attach priority mode in effect.
```

- When setting the WS-C1400 to dual-priority attachment mode from either null- or single-attachment mode, the following message is displayed:

```
Attachment type changed to dual-priority attach.
Must reset concentrator for this to take effect!
```

  At this point, you must reset the WS-C1400 before dual-priority attachment takes effect. There is no need to reset the concentrator when you switch between dual-priority attachment and dual-attachment modes.

Ring-Map Enable/Disable

The **set ringmap** [**enable** | **disable**] command enables or disables the WS-C1400 ring-mapping feature and saves the state to NVRAM. The default is **enable**.

To enable ring-mapping, enter the following command:

```
Console> (enable) set ringmap enable
Ring mapping enabled
```

To disable ring-mapping, enter the following command:

```
Console> (enable) set ringmap disable
Ring mapping disabled
```

To verify the ring map status, use the **show ringmap** command.

Software Release 1.6 Caveat Corrections

The following caveats are resolved in Release 1.6:

- When in a ring with over 200 stations, the concentrator no longer responds slowly to telnet or SNMP requests or pings. [CSCdi50341]
- When the concentrator gets IPX/VINES broadcast frames, it no longer increments the **unknown protocol errors** counter and does not distort the SNMP reports that are received. [CSCdi62339]
- When the concentrator receives an all-zero broadcast (0.0.0.0) frame, it no longer responds erroneously with the following message: `tftp error: access denied`. [CSCdi66808]

Software Release 1.6 Caveats

This section describes the caveats for Release 1.6.

- During peaks of IP broadcast use on the FDDI ring, the telnet session response time to the concentrator might be slow. [CSCdi38842]
- When a standby PHY-A port transitions up and down, a dual-homed concentrator sometimes sends SNMP trap messages. [CSCdi66807]

  As a workaround, disable the trap by using the following command:

```
Console> (enable) set port trap 1 disable
```

- When the IP address of a concentrator is changed from one class to another, the old IP broadcast address is retained. You must explicitly set the new broadcast address by using the following command:

```
Console> (enable) set ipaddress new_ipaddress new_netmask new_broadcastaddress
```

- When dynamically changing the subnet mask for an IP address, old entries might exist in the routing table. To clear the old entries from the routing table, reset the concentrator, identifying the old IP addresses, as follows:

```
Console> (enable) set ipaddress old_ipaddress old_netmask
```

Software Release 1.5 Introduction

The following sections describe enhancements, caveats, and caveat corrections for Release 1.5.

New Features in Software Release 1.5

The following enhancement has been added to Release 1.5:

This release supports a timeout feature that is configured from the console. It lets you change the time interval until the system disconnects an idle session after a period of non-activity. Use the following command:

```
Console> (enable) set logout timeout
```

The **timeout** variable is the number of minutes, from 0 to 10,000, until the system disconnects an idle session. The default is 20 minutes, and 0 disables the feature.

Software Release 1.5 Caveat Corrections

The following caveats are resolved in Release 1.5:

- The concentrator calculates the traffic percentage by counting the number of non-idle symbols received during a specific time interval. SMT and LLC frames and tokens are included as traffic in the calculation. In previous releases, the traffic percentage was sometimes incorrect. [CSCdi39662]
- The exception handler stores register information in NVRAM and resets the concentrator when a software exception occurs. The register information can be retrieved with the **show log** command. In previous releases, the exception handlers did not work correctly.

Software Release 1.5 Caveats

This section describes possibly unexpected behavior by Release 1.5.

- When in a ring with over 200 stations, the concentrator responds slowly to telnet or SNMP requests or pings. [CSCdi50341]
- When the concentrator gets IPX/VINES broadcast frames, it increments the **unknown protocol errors** counter, which distorts the SNMP reports that are received. [CSCdi62339]
- When the concentrator receives an all-zero broadcast (0.0.0.0) frame, it responds erroneously with the following message: `tftp error: access denied`. [CSCdi66808]

Software Release 1.4 Introduction

The following sections describe enhancements, caveats, and corrections for Release 1.4.

New Features in Software Release 1.4

The following enhancements have been added to Release 1.4:

- The **set trap enable** command changes the default from disabled to enabled for all traps.
- The following link states are supported:
  - Up state—LED is green.
  - Dormant or standby state—LED is orange.
  - Down state—LED is off.
- The dormant state occurs during the following conditions:
  - When you are dual-homing the concentrator or when you are dual-homing an end station.
  - When there is a bad FDDI or CDDI cable connected to a port or the cable is not plugged in completely.
- The concentrator generates a linkUp trap under the following conditions:
  - When a port transitions from a down state to an up state.
  - When a port transitions from a down state to a dormant or a standby state.

- The concentrator generates a linkDown trap under the following conditions:
  - When a port transitions from an up state to a down state.
  - When a port transitions from a dormant or a standby state to a down state.

Note No trap is generated if a port transitions from a dormant or standby state to an up state or vice versa.

Software Release 1.4 Caveat Corrections

The following caveats are resolved for Release 1.4:

- When a telnet session is opened and closed to the concentrator, some of the numbered buffers were not released. This caused an exception when the system ran out of resources. The memory buffers are now released when the telnet session is closed.
- When a physical connection to a port transitions up or down, the concentrator generates the linkUp and linkDown traps. By default, this is enabled on all ports.

  To change the default for the linkUp or linkDown trap for a specific port, use the following command:

```
Console> (enable) set porttrap
Usage: set porttrap <mod_num/port_num> <enable|disable>
Console> (enable)
Console> (enable) set porttrap 2/1 disable
Port 2/1 up/down trap disabled.
Console> (enable)
```

Software Release 1.4 Caveats

This section describes possibly unexpected behavior by Release 1.4.

- During peaks of IP broadcast use on the FDDI ring, the response time of the telnet session to the concentrator might be slow. [CSCdi38842]
- When the concentrator calculates the traffic percentage, the percentage is sometimes incorrect. [CSCdi39662]
- When the concentrator gets IPX/VINES broadcast frames, it increments the **unknown protocol errors** counter, which distorts the SNMP reports that are received. [CSCdi62339]
- When a software exception occurs, the concentrator does not reset, and the exception handler does not store register information in NVRAM.
- When the IP address of a concentrator is changed from one class to another, the old IP broadcast address is retained. You must explicitly set the new broadcast address by using the following command:

```
Console> (enable) set ipaddress new_ipaddress new_netmask new_broadcastaddress
```

- When dynamically changing the subnet mask for an IP address, old entries might exist in the routing table. To clear the old entries from the routing table, reset the concentrator, identifying the old IP addresses, as follows:

```
Console> (enable) set ipaddress old_ipaddress old_netmask
```

Software Release 1.3 Introduction

The following sections describe new features, important information, and caveats for Release 1.3.

New Features in Software Release 1.3

The following enhancements have been added to Release 1.3:

- The login and enable passwords in the concentrator provide two levels of password protection: normal and privileged.
- The **set unreachable** [**enable** | **disable**] command enables or disables the concentrator so that it sends ICMP unreachable messages. The default is **disable**.

  To enable the concentrator, use the following command:

```
Console> (enable) set unreachable enable
ICMP Unreachables enabled
```

  To view the status of the ICMP unreachables, use the following command:

```
Console> (enable) show snmp
```

- The following new traps have been added to this release:
  - enterprise 1.3.6.1.4.1.9.5
  - 1 lerAlarmOn
  - 2 lerAlarmOff
  - 3 moduleUp
  - 4 moduleDown
  - 5 chassisAlarmOn
  - 6 chassisAlarmOff
  - 7 linkUp
  - 8 linkDown

  To receive traps on an SNMP management station, follow these steps:

Step 1 Use the following command to configure an IP address to the concentrator:

```
Console> (enable) set ipaddress
Usage: set ipaddress <ip_addr> [net_mask [broadcast_addr]]
(all values given in IP dot notation: a.b.c.d)
```

Step 2 Use the ping utility to verify that you can reach the SNMP management station. If the SNMP management station is on a different network, set a default gateway for the concentrator by using the following command:

```
Console> (enable) set route default ip_addr
```

Step 3 Use the following command to enable the trap on the concentrator:

```
Console> (enable) set trap enable
SNMP authentication traps enabled
```

Step 4 Use the following command to set the trap receiver address with the proper community string:

```
Console> (enable) set trap 172.20.21.201 public
SNMP trap receiver added
```

Step 5 Use the following command to view the status of the SNMP configuration:

```
Console> (enable) show snmp
```

The following is an example of the **show snmp** output:

```
Console (enable) show snmp

IP_Address          IP-Netmask          IP-Broadcast
------------------  ------------------  ---------------
199.133.219.163     255.255.255.0       199.133.219.255

ICMP-Redirects      ICMP-Unreachables   DefaultTTL       Traps Enabled
------------------  ------------------  ---------------  -------------
enabled             enabled             60               None

Community-Access    Community-String
------------------  ------------------
none
read-only           public
read-write          private
read-write-all      secret

Trap-Rec-Address    Trap-Rec-Community
------------------  -------------------
199.133.219.161     Public
```

- The **show port** command has changed to report the following information:

```
Port  Name                 Status     Req-Path  Cur-Path  Conn-State Type Neigh
----  -------------------- ---------- --------- --------- ---------- ---- -----
1/1                        notconnect secondary isolated  standby     A    M
1/2                        connected  primary   concat    active      B    M
1/3                        notconnect primary   isolated  connecting  M    U
1/4                        notconnect primary   isolated  connecting  M    U
1/5                        notconnect primary   isolated  connecting  M    U
1/6                        notconnect primary   isolated  connecting  M    U
1/7                        notconnect primary   isolated  connecting  M    U
1/8                        notconnect primary   isolated  connecting  M    U
1/9                        notconnect primary   isolated  connecting  M    U
1/10                       notconnect primary   isolated  connecting  M    U
1/11                       notconnect primary   isolated  connecting  M    U
1/12                       notconnect primary   isolated  connecting  M    U
1/13                       notconnect primary   isolated  connecting  M    U
1/14                       notconnect primary   isolated  connecting  M    U
1/15                       notconnect primary   isolated  connecting  M    U
1/16                       notconnect primary   isolated  connecting  M    U
      Ler    Ler  Ler   Ler
Port  Cond   Est  Alarm Cutoff Lem-Ct     Lem-Rej-Ct tl-min  Media   Link-Trap
----  -----  ---- ----- ------ ---------- ---------- ------- ------  ---------
1/1   false  16   8     7      0          0          286     tp-pmd  enable
1/2   false  15   8     7      0          0          286     tp-pmd  enable
1/3   false  16   8     7      0          0          286     tp-pmd  enable
1/4   false  16   8     7      0          0          286     tp-pmd  enable
1/5   false  16   8     7      0          0          286     tp-pmd  enable
1/6   false  16   8     7      0          0          286     tp-pmd  enable
1/7   false  16   8     7      0          0          286     tp-pmd  enable
1/8   false  16   8     7      0          0          286     tp-pmd  enable
1/9   false  16   8     7      0          0          286     tp-pmd  enable
1/10  false  16   8     7      0          0          286     tp-pmd  enable
1/11  false  16   8     7      0          0          286     tp-pmd  enable
1/12  false  16   8     7      0          0          286     tp-pmd  enable
```

```
1/13  false  16   8     7      0          0          286     tp-pmd  enable
1/14  false  16   8     7      0          0          286     tp-pmd  enable
1/15  false  16   8     7      0          0          286     tp-pmd  enable
1/16  false  16   8     7      0          0          286     tp-pmd  enable
```

- The following commands are no longer available in privileged mode:
  - **show Pmac**
  - **show Smac**
  - **show Phy**

Software Release 1.3 Important Notes

Release 1.3 supports RFC 1572. For more information, refer to the *Evolution of the Interfaces Group of MIB-II*.

The latest version of the *CISCO-STACK-MIB.my* file can be obtained from the Cisco Systems FTP site. Refer to the "Using FTP to Obtain the MIB File" section.

You can also obtain the *CISCO-STACK-MIB.my* file from Cisco Connection Online (CCO). Refer to the "Obtaining Documentation" section later in this document for information about using CCO.

Using FTP to Obtain the MIB File

You can obtain the *CISCO-STACK-MIB.my file* that describes the Cisco MIB by following these steps:

Step 1 Use FTP to access the ftp.cisco.com server.

Step 2 Use the **anonymous** username to log into the server.

Step 3 Enter your e-mail name when prompted for the password.

Step 4 At the `ftp>` prompt, change directories to **/pub/mibs/**.

Step 5 Change directories to one of the following:

- **v1** for SNMPv1.
- **v2** for SNMPv2.
- **schema** for SNM schema files.
- **oid** for object files.
- **traps** for trap files.

Step 6 Use the **get README** command to display the file that has the list of available files.

Step 7 Use the **get CISCO-STACK-MIB.my** command to obtain a copy of the MIB file.

Software Release 1.3 Caveats

The following caveats describe possibly unexpected behavior by Release 1.3:

- When the concentrator calculates the traffic percentage, the percentage is sometimes incorrect. [CSCdi39662]
- When a telnet session is opened and closed to the concentrator, some of the numbered buffers are not released. This causes an exception when the system runs out of resources.
- When a physical connection to a port transitions up or down, the concentrator does not generate the linkUp and linkDown traps.

Software Release 1.2 Introduction

The following sections describe new features and important Flashcode information for Release 1.2.

New Features in Software Release 1.2

The following enhancement has been added to Release 1.2:

The **set tlmin** command sets the time required for 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 *mod_num* is 1 or 2, and the *port_num* is 1 through 16, depending on the card. The *hexvalue* is 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 MIB structure in nonvolatile memory and is used for initializing the PHY hardware setting each time the concentrator is rebooted.

```
Console> (enable) set tlmin ?
Usage: set tlmin <mod_num/port_num> <hexvalue>
       (hexvalue is in 2's complement)
Console> (enable) set tlmin 2/5 fdfd
Port 2/5 tlmin set to 0xfdfd.
Console> (enable)
```

Software Release 1.2 Important Notes

After the Workgroup WS-C1400 Concentrator firmware Version 1.2 is installed, future network downloads will allow only Flashcode with the WS-C1400 signature to be loaded. Version 1.2 and later versions of the Workgroup WS-C1400 Concentrator Flashcode will contain the WS-C1400 signature.

To download or copy an earlier Flashcode version, you must specifically request the no-signature option by adding the **nosig** argument to the **download** command. The following is an example of a download attempt without using the **nosig** argument:

```
Console> (enable) download 198.133.219.40 c1400_11.net
This command will disconnect your telnet session.
Download image c1400_11.net from host 198.133.219.40 to flash (y/n) [n]? y
\
Done.  Finished Network Download.  (453636 bytes)
ERROR: Downloaded code signature incorrect
```

The following is an example of a successful download using the **nosig** argument:

```
Console> (enable) download 198.133.219.40 c1400_11.net nosig
This command will disconnect your telnet session.
Download image c1400_11.net from host 198.133.219.40 to flash (y/n) [n]? y
\
Done. Finished Network Download. (453636 bytes)
Initializing flash...Erasing Flash...Done
```

```
Programming flash
Base....Code....Length....Time....Done
Disconnected from FDDI ring.
Connection closed by foreign host.
```

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

http://www.cisco.com

Translated documentation is available at the following URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click the **Fax** or **Email** option under the “Leave Feedback” at the bottom of the Cisco Documentation home page.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.

- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

http://www.cisco.com/register/

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.