



Doc. No. 78-1815-09

Release Notes for CDDI/FDDI Workgroup WS-C1400 Concentrator Release 1.8

These release notes describe the features and caveats for CDDI/FDDI Workgroup WS-C1400 Concentrator software Release 1.8. Refer to the *CDDI/FDDI C1400 Concentrator Installation and Configuration Guide* for detailed information about the CDDI/FDDI Workgroup WS-C1400 Concentrator.

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more up to date than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

This document is divided into the following sections:

- Release 1.8 Introduction
 - New Features in Release 1.8
 - Release 1.8 Caveat Corrections
 - Release 1.8 Caveats
- Release 1.7 Introduction
 - Release 1.7 Caveat Corrections
 - Release 1.7 Caveats
- Release 1.6 Introduction
 - Release 1.6 Caveat Corrections
 - Release 1.6 Caveats

Corporate Headquarters

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

Copyright © 1997-1998
Cisco Systems, Inc.
All rights reserved.

- Release 1.5 Introduction
 - New Features in Release 1.5
 - Release 1.5 Caveat Corrections
 - Release 1.5 Caveats
- Release 1.4 Introduction
 - New Features in Release 1.4
 - Release 1.4 Caveat Corrections
 - Release 1.4 Caveats
- Release 1.3 Introduction
 - New Features in Release 1.3
 - Release 1.3 Important Notes
 - Using FTP to Obtain the MIB File
 - Release 1.3 Caveats
- Release 1.2 Introduction
 - New Features in Release 1.2
 - Release 1.2 Important Notes
- Cisco Connection Online

Release 1.8 Introduction

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

New Features in 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.

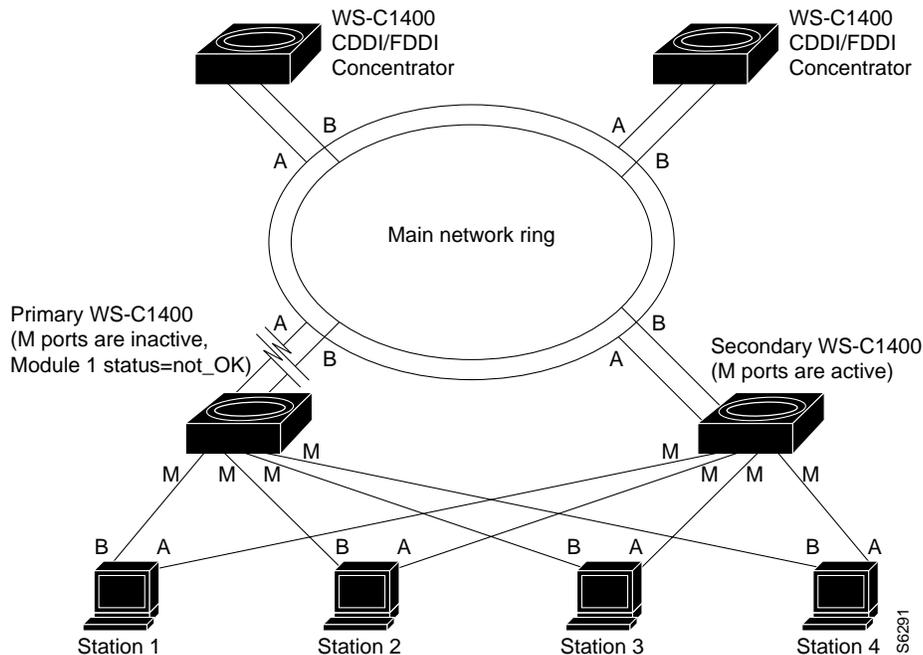
A WS-C1400 concentrator in module-priority attachment mode functions like a concentrator that is in dual-attachment mode, except that Module 1 must be present, enabled, and functional before any master (M) port can connect. If Module 1 experiences a major or minor hardware failure or is disabled or removed, 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 “Cisco Connection Online” 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   1/1                    notconnect secondary  isolated  A     U
1/2   1/2                    notconnect primary    isolated  B     U
1/3   1/3                    inactive   primary    isolated  M     U
1/4   1/4                    inactive   primary    isolated  M     U
:
:
1/16  1/16                  disabled   primary    isolated  M     U
2/1   2/1                    inactive   primary    isolated  M     U
:
:
2/8   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.

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]

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 IP address by using the following command:

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

- 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_ipaddress
```

- 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]

Release 1.7 Introduction

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

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]

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 IP address by using the following command:

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

- 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_ipaddress
```

- 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]

Release 1.6 Introduction

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

New Features in 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

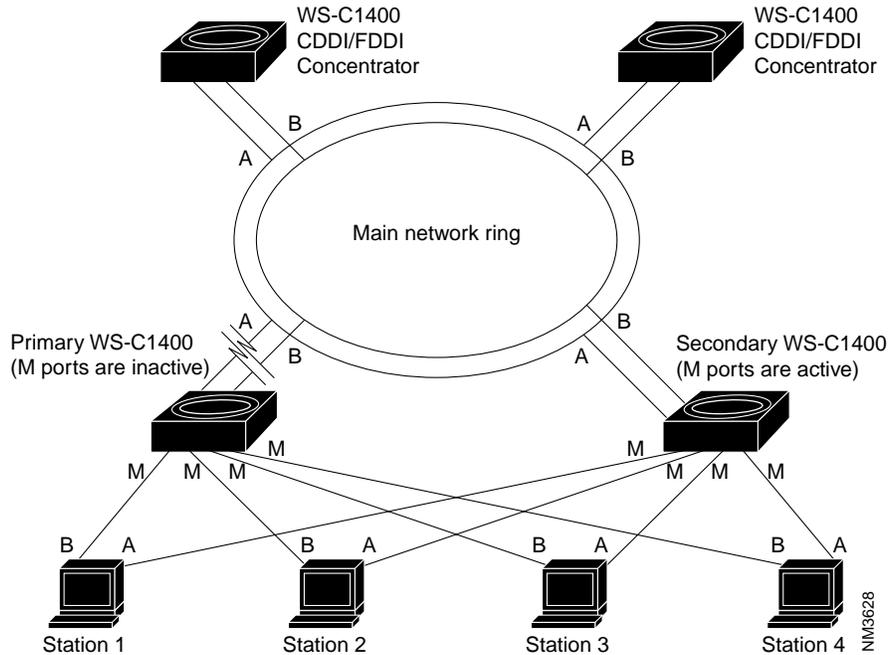
A WS-C1400 concentrator in dual-priority attachment mode functions like a concentrator that is in dual-attachment mode, except that the A or B ports must be active before any master (M) port can connect. If the A or B ports are not active, the M ports will report as inactive and are disabled until either 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 “Cisco Connection Online” 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    1/1              notconnect secondary isolated  A     U
1/2    1/2              notconnect primary   isolated  B     U
1/3    1/3              inactive   primary   isolated  M     U
1/4    1/4              inactive   primary   isolated  M     U
:
:
1/16   1/16            disabled   primary   isolated  M     U
2/1    2/1              inactive   primary   isolated  M     U
:
:
2/8    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.

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]

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 IP address by using the following command:

```
Console> set ipaddress new_ipaddress
```

- 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> set ipaddress old_ipaddress old_ipaddress
```

Release 1.5 Introduction

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

New Features in 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.

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.

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]

Release 1.4 Introduction

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

New Features in 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.

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)
```

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 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_ipaddress
```

- 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 IP address by using the following command:

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

Release 1.3 Introduction

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

New Features in 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

Port	Ler Cond	Ler Est	Ler Alarm	Ler 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**

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 “Cisco Connection Online” 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.

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.

Release 1.2 Introduction

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

New Features in 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)
```

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.
```

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two World Wide Web (WWW) interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version. The character-based version of CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The multimedia version of CCO provides richly formatted documents with photographs, figures, graphics, and video. Both versions provide hyperlinks to related information.

You can access CCO in the following ways:

- WWW: <http://www.cisco.com>
- WWW: <http://www-europe.cisco.com>
- WWW: <http://www-china.cisco.com>
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

This document is to be used in conjunction with the *CDDI/FDDI C1400 Concentrator Installation and Configuration Guide* publication.

AtmDirector, AutoConnect, AutoRoute, AXIS, BPX, Catalyst, CD-PAC, CiscoAdvantage, CiscoFusion, Cisco IOS, the Cisco IOS logo, *CiscoLink*, CiscoPro, the CiscoPro logo, CiscoRemote, the CiscoRemote logo, CiscoSecure, Cisco Systems, CiscoView, CiscoVision, CiscoWorks, ClickStart, ControlStream, EdgeConnect, EtherChannel, FairShare, FastCell, FastForward, FastManager, FastMate, FastPADImp, FastPADmicro, FastPADmp, FragmentFree, FrameClass, Fulcrum INS, IGX, Impact, Internet Junction, JumpStart, LAN²LAN Enterprise, LAN²LAN Remote Office, LightSwitch, MICA, NetBeyond, NetFlow, Newport Systems Solutions, *Packet*, PIX, Point and Click Internetworking, RouteStream, Secure/IP, SMARTnet, StrataSphere, StrataSphere BILLder, StrataSphere Connection Manager, StrataSphere Modeler, StrataSphere Optimizer, Stratm, StrataView Plus, StreamView, SwitchProbe, SwitchVision, SwitchWare, SynchroniCD, *The Cell*, The FastPacket Company, TokenSwitch, TrafficDirector, Virtual EtherSwitch, VirtualStream, VlanDirector, Web Clusters, WNIC, Workgroup Director, Workgroup Stack, and XCI are trademarks; Access by Cisco, Bringing the Power of Internetworking to Everyone, Enter the Net with MultiNet, and The Network Works. No Excuses. are service marks; and Cisco, the Cisco Systems logo, CollisionFree, Combinet, EtherSwitch, FastHub, FastLink, FastNIC, FastPacket, FastPAD, FastSwitch, ForeSight, Grand, Grand Junction, Grand Junction Networks, the Grand Junction Networks logo, HSSI, IGRP, IPX, Kalpana, the Kalpana logo, LightStream, MultiNet, MultiWare, OptiClass, Personal Ethernet, Phase/IP, RPS, StrataCom, TGV, the TGV logo, and UniverCD are registered trademarks of Cisco Systems, Inc. All other trademarks, service marks, registered trademarks, or registered service marks mentioned in this document are the property of their respective owners.

Copyright © 1996-1998, Cisco Systems, Inc.
All rights reserved. Printed in USA.
9801R