Doc. No. 78-1434-07

Release Notes for CDDI/FDDI Workgroup WS-C1100 Concentrator Release 3.5

November 27, 1996

Introduction

These release notes describe the features, caveats, and modifications for CDDI/FDDI Workgroup WS-C1100 Concentrator Release 3.5. Refer to the *CDDI/FDDI Workgroup WS-C1100 User Guide* for detailed information about the CDDI/FDDI Workgroup WS-C1100 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.

Sections in this document include:

- New Features in Release 3.5
- Release 3.5 Caveats
- Release 3.5 Modifications
- Release 3.4 Introduction
- Release 3.4 Caveats
- Release 3.4 Modifications
- Release 3.3 Introduction
- New Features in Release 3.3
- Release 3.3 Caveats

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

New Features in Release 3.5

The following enhancement has been added to Release 3.5:

The **set ringmap** [**enable | disable**] enables or disables the WS-C1100 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 3.5 Caveats

This section describes possibly unexpected behavior by Release 3.5.

- 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> (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> set ipaddress old_ipaddress old_ipaddress
  ```

Release 3.5 Modifications

The following caveats are resolved in Release 3.5:

- 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 3.4 Introduction

The following sections describe caveats and modifications for Release 3.4.

Release 3.4 Caveats

The following caveats describe possibly unexpected behavior by Release 3.4:

- 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]
- 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> set ipaddress old_ipaddress old_ipaddress
  ```

Release 3.4 Modifications

The following caveats are resolved in Release 3.4:

- The concentrator calculates the traffic percentage by counting the number of nonidle 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 3.3 Introduction

The following sections describe enhancements, caveats, and modifications for Release 3.3.

New Features in Release 3.3

The following enhancements have been added to Release 3.3:

- 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 A trap is not generated if a port transitions from a dormant or standby state to an up state or vice versa.

Release 3.3 Caveats

This section describes possibly unexpected behavior by Release 3.3:

- 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> set ipaddress new_ipaddress
  ```

Release 3.3 Modifications

The following caveats are resolved in Release 3.3:

- When a Telnet session was 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 3.2 Introduction

The following section describes enhancements and upgrade information for Release 3.2.

New Features in Release 3.2

The following enhancements have been added to Release 3.2:

- 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 a 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 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> 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> 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**

Release 3.2 Important Notes

Release 3.2 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 3.2 Caveats

The following caveats describe possibly unexpected behavior by Release 3.2:

- 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 3.1 Introduction

The following sections describe enhancements and important Flashcode information for Release 3.1.

New Features in Release 3.1

The following enhancements have been added to Release 3.1:

- The **set enablepass** command has been added, allowing two levels of password protection—privileged and users. The privileged level is accessed by using the **enable** command and then entering your password at the prompt.

  Table 1 lists the top-level commands and their modes.

Table 1 Top-Level Commands

Command	Description	Mode[1]
clear	Use **clear help** for information on **clear** commands.	P
configure	Configure from the terminal or the network.	P
connect fddi	Connect to the FDDI ring.	P
copy flash tftp	Upload the Flash memory image to a network host.	P
copy tftp flash	Copy files to and from Flash memory.	P
disable	Disable privileged mode.	P
disconnect fddi	Disconnect from the FDDI ring.	P
download	Download new code to Flash memory.	P
enable	Enable privileged mode.	N
help	Display top-level commands and a description of how the commands are used.	N
history	Show the contents of the history substitution buffer.	N
macreinit	Reinitialize all MACs[2].	P
ping	Send echo request packets to a node on the network.	N
quit	Exit from the console.	N
reset	Reset the system.	P
set	Use the **set help** command for information on the **set** commands.	N
show	Use the **show help** command for information on the **show** commands.	N
test	Use the **test help** command for information on the **test** commands.	P
traffic	Send continuous traffic on the ring.	P

Command	Description	Mode[1]
upload	Upload Flash memory code to the network.	P
write	Write configuration information to the terminal or to a file.	P

1. N = normal; P = privileged.
2. MAC = Media Access Control.

Table 2 lists the **clear** commands and their modes.

Table 2 clear Commands

Command	Description	Mode[1]
clear arp	Clears ARP[2] table entries.	P
clear coalias	Clears the MAC address alias.	P
clear config	Clears the configuration and reset the system.	P
clear counters	Clears MAC and port counters.	P
clear help	Displays **clear** commands and descriptions.	P
clear ipalias	Clears the alias of an IP address.	P
clear lem	Clears link error monitor counters.	P
clear log	Clears the system error log.	P
clear mac	Clears MAC counters.	P
clear port	Clears port counters.	P
clear route	Clears IP routing table entries.	P
clear trap	Clears the SNMP trap receiver address.	P

1. P = privileged.
2. ARP = Address Resolution Protocol.

Table 3 lists the **set** commands and their modes.

Table 3 set Commands

Command	Description	Mode[1]
set arp	Sets the ARP aging time.	P
set alarm	Sets the port line error rate alarm.	P
set arp	Sets the ARP table entry.	P
set attach	Sets the system attach type.	P
set baud	Sets the serial port baud rate.	P
set broadcast	Sets the SNMP broadcast address.	P
set coalias	Sets the alias for company MAC address.	P
set community	Sets the SNMP community string.	P
set cutoff	Sets the port line error rate cutoff.	P

Command	Description	Mode[1]
set defaultTTL	Sets the default TTL[2] for packets.	P
set echo	Sets echo mode (enable or disable).	P
set enablepass	Sets the enable password.	P
set help	Displays **set** commands and descriptions.	P
set insertmode	Sets the system insert mode.	P
set ipaddress	Sets SNMP IP, netmask, and broadcast addresses.	P
set ipalias	Sets the alias for an IP address.	P
set length	Sets the number of lines in terminal display.	N
set meter	Sets the system traffic meter path.	P
set netmask	Sets the SNMP netmask.	P
set password	Sets the console password.	P
set path	Sets the port requested path.	P
set port	Sets the port state (enable or disable).	P
set portname	Sets the port name.	P
set prompt	Sets the command-line prompt.	P
set redirect	Sets ICMP[3] redirects on or off.	P
set route	Sets an IP routing table entry.	P
set syscontact	Sets the system contact name.	P
set syslocation	Sets the system location.	P
set sysname	Sets the system name.	P
set time	Sets the system clock.	P
set tnotify	Sets SMT Time Notify.	P
set trap	Sets the SNMP trap receiver address.	P
set treq	Sets the token request value of the MAC.	P
set userdata	Sets SMT parameter user data.	P

1. N = normal; P = privileged.
2. TTL = time to live
3. ICMP = internet control message protocol.

Table 4 lists the **show** commands and their modes.

Table 4 show Commands

Command	Description	Mode[1]
show arp	Shows the ARP table entries.	N
show coalias	Shows company aliases.	N
show config	Shows the configuration of the concentrator.	P
show cspsig	Shows the CSP[2] signal history.	P
show driver	Shows the frame driver status or counts.	P

Command	Description	Mode[1]
show help	Displays information about the **show** commands.	N
show ipalias	Shows the IP aliases that have been assigned.	N
show log	Shows the system error log.	P
show mac	Shows MAC information.	N
show macdbg	Shows MAC debug information.	P
show macstatus	Shows the history of the MAC status register.	P
show mbuf	Shows mbuf[3] and malloc[4] statistics.	P
show phy	Shows PHY[5].	P
show pmac	Shows the primary MAC registers.	P
show port	Shows port information.	N
show portdbg	Shows port debug information.	P
show porthistory	Shows port events.	n/a
show remotemib	Shows a remote MIB[6].	N
show ringmap	Shows the ringmap for the primary MAC.	N
show route	Shows the IP routing table.	N
show smac	Shows the secondary MAC registers.	P
show snmp	Shows SNMP information.	N
show system	Shows the system information.	N
show test	Shows the results of diagnostic tests.	P
show time	Shows the time of day.	N

1. N = normal; P = privileged.
2. CSP = connection services process.
3. mbuf = memory buffer.
4. malloc = memory allocation.
5. PHY = physical memory registers.
6. MIB = management information base.

- The Link Error Rate (LER) estimate that is shown in the **show port** display is cleared to 10^{-16} with the **clear port** and **clear counters** commands.
- Single-mode fiber-optic A/B ports report the correct media type when you use the **show port** command.
- After you use the **set attach** command, the appropriate paths (primary or secondary) are requested for the ports of a null or single attachment concentrator during reset.
- The **set**, **show**, and **clear** commands have the same optional parameters.
- The **write** and **show config** commands are used for viewing and uploading the configuration.
- The **upload** and **copy** commands are used to upload the image file.
- The **clear all** command is used to clear tables for the following **clear** commands:
  - **clear arp**
  - **clear coalias**
  - **clear ipalias**

  - **clear route**
  - **clear trap**
- The values for the following commands have been changed to case insensitive:
  - **coalias**
  - **ipalias**
  - **password**
- The **history** command buffer has been increased from 8 to 20 commands.
- The **connect** and **disconnect** commands have been changed to **connect fddi** and **disconnect fddi**.
- The **set length** command has been added so that you can configure how the screen scrolls.
- The following system group commands have been added:
  - **set defaultTTL**—sets the default time-to-live command variable
  - **set syscontact**—sets the system-contact field in the **show system** command
  - **set syslocation**—sets the system-location field in the **show system** command
- The maximum batch file size has been increased from 4608 to 9216 bytes.
- Confirmation and warning messages were added to the following commands:
  - **clear config**
  - **configure**
  - **copy flash tftp**
  - **copy tftp flash**
  - **disconnect fddi**
  - **reset**
  - **set port disable**

Release 3.1 Important Notes

After the Workgroup WS-C1100 Concentrator Flashcode Version 3.1 is installed, future network downloads will allow only Flashcode with the WS-C1100 signature to be loaded. Version 3.1 and later versions of the Workgroup WS-C1100 Concentrator Flashcode will contain the WS-C1100 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. Following is an example of a download attempt without using the **nosig** argument:

```
Console> (enable) download 198.133.219.40 c1100_10.net
This command will disconnect your telnet session.
Download image c1100_10.net from host 198.133.219.40 to flash (y/n) [n]? y
\
Done.  Finished Network Download.  (453636 bytes)
ERROR: Downloaded code signature incorrect
```

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

```
Console> (enable) download 198.133.219.40 c1100_10.net nosig
This command will disconnect your telnet session.
Download image c1100_10.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), formerly Cisco Information Online (CIO), is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional content 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, 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 interfaces that are updated and enhanced simultaneously—a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as 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 baud rates up to 14.4 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 Workgroup WS-C1100 User Guide* publication.

969R