Doc. No 78-1434-06

CDDI/FDDI Workgroup WS-C1100 Concentrator Release Note

Supplement to DOC-WGCONCUG2 (Document Number 78-1275-03)
Flashcode Version 3.4

Introduction

This release note describes modifications to the Copper Distributed Data Interface/Fiber Distributed Data Interface (CDDI/FDDI) Workgroup Concentrator. Refer to the *CDDI/FDDI Workgroup Concentrator User Guide* for detailed information about the CDDI/FDDI Workgroup Concentrator.

Product Overview

The CDDI/FDDI Workgroup Concentrator provides CDDI, multilevel transmission (MLT-3), and FDDI connectivity. Refer to the chapter "Product Overview" in the *CDDI/FDDI Workgroup Concentrator User Guide* for a detailed description of product features and functions.

This document covers the resolved issues and new features for Flashcode Version 3.4. Flashcode Version 3.4 is an upgrade to the previously released WS-C1100 Concentrator Flashcode Version 3.3.

Sections in this document include:

- Resolved Issues and New Features for Release 3.4
- Caveats of Release 3.4
- Resolved Issues for Release 3.3
- Caveats of Release 3.3
- Resolved Issues and New Features for Release 3.2
- Resolved Issues and New Features for Release 3.1
- Known Issue and Workaround

Resolved Issues and New Features for Release 3.4

This section describes the issues that were resolved and the features that were added during this release of the Workgroup WS-C1100 Concentrator software:

1. 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> set logout <timeout>
   ```

   Where <timeout> 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.

2. Traffic % is calculated 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 % was sometimes incorrect.

3. If a software exception occurs, the exception handler will store valuable register information in NVRAM and will reset the concentrator. The register information can be retrieved with the **show log** command. In previous releases, the exception handlers did not work correctly.

4. The system reports m port counts in SMT frames correctly. In previous releases, the m port count was always reported as 16, regardless of the actual number of m ports in the concentrator.

Caveats of Release 3.4

This section covers the caveats and known issues for Release 3.4:

- The system can respond slowly to Telnet and SNMP requests and pings in certain environments, such as a ring with over 200 stations or a ring with large amounts of broadcast traffic.

Resolved Issues for Release 3.3

The following issues were resolved for Release 3.3:

1. In the previous release, 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. As of this release, the memory buffers are released when the Telnet session is closed.

2. The default for all traps is disabled. To change the default of all the traps, use the following command:

   ```
   Console> set trap enable
   ```

   The linkUp and linkDown traps are generated by the concentrator when a physical connection to a port goes up or down. 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)
   ```

3 This release supports the following three link states:

— UP state LED is Green.

— DORMANT or STANDBY state LED is Orange.

— DOWN state LED is OFF.

The DORMANT state can be reached during the following two 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.

4 The concentrator generates a linkUp trap under the following conditions:

— When a port goes from a DOWN state to UP state.

— When a port goes from a DOWN state to DORMANT or STANDBY state.

5 The concentrator generates a linkDown trap under the following conditions:

— When a port goes from an UP state to a DOWN state.

— When a port goes from a DORMANT or STANDBY state to a DOWN state.

Note No trap is generated if a port goes from a DORMANT or STANDBY state to an UP state or vice versa.

Caveats of Release 3.3

This section covers the caveats and known issues for Release 3.3:

- During peak times of IP Broadcast use on the FDDI ring, the response time of the Telnet session to the concentrator might be slow.
- 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
  ```

  The linkUp and linkDown traps are generated by the concentrator when a physical connection to a port goes up or down. By default, this is enabled on all ports.
- Changing the subnet mask for an IP address dynamically might leave old entries in the routing table. To clear the old entries from the routing table, reset the concentrator, as in the following example:

  ```
  Console> set ipaddress 172.20.21.201 255.255.0.0 172.20.255.255
  ```

Resolved Issues and New Features for Release 3.2

This section describes the issues that were resolved and the features that were added during this revision of the Workgroup WS-C1100 Concentrator software:

1 This release supports RFC 1573. For more information, refer to the *Evolution of the Interfaces Group of MIB-II*.

2 You should update to the latest version of the Cisco-stack MIB.

You can obtain a copy of the Cisco MIB file in two ways:

— Use File Transfer Protocol (FTP) to access the cisco.com server.

— Use CIO to access the cisco.com server.

Using FTP to ACCESS the MIB File

You can obtain the file *cisco-stack.mib* describing the Cisco MIB with the following procedure:

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

Step 2 Log in with the username **anonymous**.

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

Step 4 At the `ftp>` prompt change directories to **/pub/MIBs/*xx*.** Where ***xx*** is **v1** for SNMPv1 MIBs, **v2** for SNMPv2 MIBs, **schema** for SNM schema files, **oid** for object ID files, and **traps** for trap files.

Step 5 Use the **get README** command to display the *readme* file containing a list of available files.

Step 6 Use the **get** *cisco-stack.mib.my* command to obtain a copy of the MIB file.

Using CIO to Access the MIB File

You can obtain the file *cisco-stack.mib* describing the Cisco MIB through CIO.

For information on using CIO, refer to the “Cisco Information Online” section in this document.

1 Passwords in the configuration file allow two-level password protection. The login and enable password modes are normal and privileged, respectively.

2 The **set unreachable <enable | disable>** command was added to support the ability of the concentrator to send ICMP unreachable messages. The default is disable.

To enable this command 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
```

3 The following is a list of the new traps added to this release.

```
enterprise 1.3.6.1.4.1.9.5
1 lerAlarmOn
2 lerAlarmOff
3 chassisAlarmOn
4 chassisAlarmOff
5 linkUp
6 linkDowm
```

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

Step 1 Configure an IP address to the concentrator using the following command:

```
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 Enable the trap on the concentrator using the following command:

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

Step 4 Set the trap receiver address with the proper community string using the following command:

```
Console> set trap <ip_addr> <community string>
SNMP trap receiver added

SNMP trap receiver added
```

To view the status of the SNMP configuration, use the following command:

```
Console> show snmp
```

The following is an example of the 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
```

4 The display for the **show port** command has changed to the following:

```
Port  Name                 Status     Req-Path  Cur-Path  Conn-State Type Neigh
----  -------------------- ---------- --------- --------- ---------- ---- -----
1                          notconnect secondary isolated  connecting  A    U
2                          connected  primary   concat    active      B    M
3                          notconnect primary   isolated  connecting  M    U
4                          notconnect primary   isolated  connecting  M    U
5                          notconnect primary   isolated  connecting  M    U
6                          notconnect primary   isolated  connecting  M    U
7                          notconnect primary   isolated  connecting  M    U
8                          notconnect primary   isolated  connecting  M    U
9                          notconnect primary   isolated  connecting  M    U
10                         notconnect primary   isolated  connecting  M    U
```

```
11                        notconnect primary   isolated  connecting  M    U
12                        notconnect primary   isolated  connecting  M    U
13                        notconnect primary   isolated  connecting  M    U
14                        notconnect primary   isolated  connecting  M    U
15                        notconnect primary   isolated  connecting  M    U
16                        notconnect primary   isolated  connecting  M    U
17                        notconnect primary   isolated  connecting  M    U
18                        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     false  16   8     7      0          0          286     mlt-3   enable
2     false  15   8     7      0          0          286     mlt-3   enable
3     false  16   8     7      0          0          286     cddi    enable
4     false  16   8     7      0          0          286     cddi    enable
5     false  16   8     7      0          0          286     cddi    enable
6     false  16   8     7      0          0          286     cddi    enable
7     false  16   8     7      0          0          286     cddi    enable
8     false  16   8     7      0          0          286     cddi    enable
9     false  16   8     7      0          0          286     cddi    enable
10    false  16   8     7      0          0          286     cddi    enable
11    false  16   8     7      0          0          286     fiber   enable
12    false  16   8     7      0          0          286     fiber   enable
13    false  16   8     7      0          0          286     fiber   enable
14    false  16   8     7      0          0          286     fiber   enable
15    false  16   8     7      0          0          286     fiber   enable
16    false  16   8     7      0          0          286     fiber   enable
17   false  16   8   7       0        0        286     fiber   enable
18    false  16   8     7      0          0          286     fiber   enable
```

5 The following commands are no longer available in the privileged mode:

```
show Pmac
show Smac
show Phy
```

Resolved Issues and New Features for Release 3.1

This section describes the issues that were resolved and the new features that were added to the Workgroup WS-C1100 Concentrator Release 3.1 software:

1 The **set enablepass** command was added and allows two-level password protection. The commands levels, or modes, are normal and privileged. Privileged mode commands are accessed using the **enable** command and entering the correct 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

Command	Description	Mode[1]
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 command 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
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 mode.

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 addresses	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
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 netwask	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
show help	Dislpys 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

2 Link Error Rate (LER) Estimate is cleared to 10^{-16} with the **clear port** and **clear counters** commands.

3 Single mode fiber A/B ports now report the correct media type when you use **show port** command.

4 When you use the **set attach** command, the appropriate paths (for example, primary or secondary) are requested for the ports of a null or single attachment concentrator during reset after you use the **set attach** command.

5 You can now use **set**, **show**, and **clear** for most commands.

6 The **write** and **show config** commands have been added for viewing and uploading the configuration.

7 The **upload** and **copy** commands have been added to upload the image file.

8 A **clear all** command can now be used to clear tables for the following **clear** commands:

- **clear arp**
- **clear coalias**
- **clear ipalias**
- **clear route**
- **clear trap**

9 The value you enter when using the following commands has been changed to case-insensitive:

- *coalias*
- *ipalias*
- *password*

10 The **history** command buffer has been increased from 8 to 20 commands.

11 The **connect** and **disconnect** commands have been changed to **connect fddi** and **disconnect fddi**.

12 The **set length** command hasbeen added so you can configure how the screen scrolls.

13 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 **show system** command

14 Maximum batch file size has been doubled from 4,608 to 9,216 bytes.

15 Confirmations and warning beeps that might affect your network connection were added to the following commands:

- **clear config**
- **configure**
- **copy flash tftp**
- **copy tftp flash**
- **disconnect fddi**
- **reset**
- **set port disable**

Known Issue and Workaround

Once 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. All 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 version of Flachcode, you must specifically request the no-signature option by adding the **nosig** argument to the download command. Following is an example:

```
Console> (enable) download cres c1100_10.net nosig
This command will disconnect your telnet session.
Download image c1100_10.net from host cres to flash (y/n) [n]? y
```

```
1st Pass
Initializing Flash...Erasing Flash....Done
Programing Flash...Base....Length....Time....Code....Done
2nd Pass
Programing Flash...Code....Done
3rd Pass
Programing Flash...Code....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, Internet e-mail, and fax download options, 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`.
- 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 Concentrator User Guide* publication.