



Doc. No. 78-1434-08

## Release Notes for CDDI/FDDI Workgroup WS-C1100 Concentrator Release 3.6

---

These release notes describe the features, notes, caveats, and caveat corrections for CDDI/FDDI Workgroup WS-C1100 Concentrator Release 3.6. 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>.

This document is divided into the following sections:

- Release 3.6 Introduction
  - Release 3.6 Caveat Corrections
  - Release 3.6 Caveats
- Release 3.5 Introduction
  - New Features in Release 3.5
  - Release 3.5 Caveat Corrections
  - Release 3.5 Caveats
- Release 3.4 Introduction
  - Release 3.4 Caveat Corrections
  - Release 3.4 Caveats

---

### Corporate Headquarters

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

Copyright © 1996-1998  
Cisco Systems, Inc.  
All rights reserved.

- Release 3.3 Introduction
  - New Features in Release 3.3
  - Release 3.3 Caveat Corrections
  - Release 3.3 Caveats
- Release 3.2 Introduction
  - New Features in Release 3.2
  - Release 3.2 Important Notes
  - Release 3.2 Caveats
- Release 3.1 Introduction
  - New Features in Release 3.1
  - Release 3.1 Important Notes

## Release 3.6 Introduction

The following sections describe the caveats and corrected caveats in Release 3.6.

### Release 3.6 Caveat Corrections

This section describes caveats that have been corrected in the 3.6 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 3.6 Caveats

This section describes the caveats for Release 3.6.

- 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
```

## Release 3.5 Introduction

The following sections describe the features, caveats, and corrected caveats in Release 3.5.

### 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 Caveat Corrections

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 3.5 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> (enable) set ipaddress old_ipaddress old_ipaddress
```

## Release 3.4 Introduction

The following sections describe caveats and caveat corrections for Release 3.4.

### Release 3.4 Caveat Corrections

The following caveats have been 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 3.4 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 3.3 Introduction

The following sections describe features, caveats, and caveat corrections 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 Caveat Corrections

The following caveats have been 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 3.3 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 3.2 Introduction

The following sections describe new features, important information, and caveats 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

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

1. N = normal; P = privileged. 2.

2. MAC = Media Access Control.

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

**Table 2 clear Commands**

Command	Description	Mode <sup>1</sup>
<b>clear arp</b>	Clears ARP <sup>2</sup> table entries.	P
<b>clear coalias</b>	Clears the MAC address alias.	P
<b>clear config</b>	Clears the configuration and reset the system.	P
<b>clear counters</b>	Clears MAC and port counters.	P
<b>clear help</b>	Displays <b>clear</b> commands and descriptions.	P
<b>clear ipalias</b>	Clears the alias of an IP address.	P
<b>clear lem</b>	Clears link error monitor counters.	P
<b>clear log</b>	Clears the system error log.	P
<b>clear mac</b>	Clears MAC counters.	P
<b>clear port</b>	Clears port counters.	P
<b>clear route</b>	Clears IP routing table entries.	P
<b>clear trap</b>	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 <sup>1</sup>
<b>set arp</b>	Sets the ARP aging time.	P
<b>set alarm</b>	Sets the port line error rate alarm.	P
<b>set arp</b>	Sets the ARP table entry.	P
<b>set attach</b>	Sets the system attach type.	P
<b>set baud</b>	Sets the serial port baud rate.	P
<b>set broadcast</b>	Sets the SNMP broadcast address.	P
<b>set coalias</b>	Sets the alias for company MAC address.	P
<b>set community</b>	Sets the SNMP community string.	P
<b>set cutoff</b>	Sets the port line error rate cutoff.	P
<b>set default TTL</b>	Sets the default TTL <sup>2</sup> for packets.	P
<b>set echo</b>	Sets echo mode (enable or disable).	P
<b>set enablepass</b>	Sets the enable password.	P
<b>set help</b>	Displays <b>set</b> commands and descriptions.	P
<b>set insertmode</b>	Sets the system insert mode.	P
<b>set ipaddress</b>	Sets SNMP IP, netmask, and broadcast addresses.	P

Command	Description	Mode <sup>1</sup>
<b>set ipalias</b>	Sets the alias for an IP address.	P
<b>set length</b>	Sets the number of lines in terminal display.	N
<b>set meter</b>	Sets the system traffic meter path.	P
<b>set netmask</b>	Sets the SNMP netmask.	P
<b>set password</b>	Sets the console password.	P
<b>set path</b>	Sets the port requested path.	P
<b>set port</b>	Sets the port state (enable or disable).	P
<b>set portname</b>	Sets the port name.	P
<b>set prompt</b>	Sets the command-line prompt.	P
<b>set redirect</b>	Sets ICMP <sup>3</sup> redirects on or off.	P
<b>set route</b>	Sets an IP routing table entry.	P
<b>set syscontact</b>	Sets the system contact name.	P
<b>set syslocation</b>	Sets the system location.	P
<b>set sysname</b>	Sets the system name.	P
<b>set time</b>	Sets the system clock.	P
<b>set tnotify</b>	Sets SMT Time Notify.	P
<b>set trap</b>	Sets the SNMP trap receiver address.	P
<b>set treq</b>	Sets the token request value of the MAC.	P
<b>set userdata</b>	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 <sup>1</sup>
<b>show arp</b>	Shows the ARP table entries.	N
<b>show coalias</b>	Shows company aliases.	N
<b>show config</b>	Shows the configuration of the concentrator.	P
<b>show cspsig</b>	Shows the CSP <sup>2</sup> signal history.	P
<b>show driver</b>	Shows the frame driver status or counts.	P
<b>show help</b>	Displays information about the <b>show</b> commands.	N
<b>show ipalias</b>	Shows the IP aliases that have been assigned.	N
<b>show log</b>	Shows the system error log.	P
<b>show mac</b>	Shows MAC information.	N
<b>show macdbg</b>	Shows MAC debug information.	P
<b>show macstatus</b>	Shows the history of the MAC status register.	P

Command	Description	Mode <sup>1</sup>
<b>show mbuf</b>	Shows mbuf <sup>3</sup> and malloc <sup>4</sup> statistics.	P
<b>show phy</b>	Shows PHY <sup>5</sup> .	P
<b>show pmac</b>	Shows the primary MAC registers.	P
<b>show port</b>	Shows port information.	N
<b>show portdbg</b>	Shows port debug information.	P
<b>show porthistory</b>	Shows port events.	n/a
<b>show remotemib</b>	Shows a remote MIB <sup>6</sup> .	N
<b>show ringmap</b>	Shows the ringmap for the primary MAC.	N
<b>show route</b>	Shows the IP routing table.	N
<b>show smac</b>	Shows the secondary MAC registers.	P
<b>show snmp</b>	Shows SNMP information.	N
<b>show system</b>	Shows the system information.	N
<b>show test</b>	Shows the results of diagnostic tests.	P
<b>show time</b>	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<sup>-16</sup> 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](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](mailto:cco-help@cisco.com). For additional information, contact [cco-team@cisco.com](mailto: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](mailto: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](mailto:cs-rep@cisco.com).

---

---

This document is to be used in conjunction with the *CDDI/FDDI Workgroup WS-C1100 User 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, LAN<sup>2</sup>LAN Enterprise, LAN<sup>2</sup>LAN Remote Office, LightSwitch, 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

