

Cisco AS5350 and Cisco AS5400 Universal Gateways

- 1** Documents, Equipment, and Tools
- 2** Install Chassis
- 3** Install Modules
- 4** Connect Cables
- 5** Power Up the Universal Gateway
- 6** Perform Initial Configuration
- 7** Slot Numbering
- 8** Obtaining Documentation
- 9** Obtaining Technical Assistance
- 10** Obtaining Additional Publications and Information



1 Documents, Equipment, and Tools

User Documentation

All of the documents described here are available on line and on the documentation CD-ROM that you received with your universal gateway. To be sure of obtaining the latest information, you should access the online documentation.



Note The information in this document applies to the Cisco AS5350, Cisco AS5400, and Cisco AS5400HPX universal gateways.

To access online user documentation:

From Cisco.com at <http://www.cisco.com>, under **Service & Support**, select **Technical Documents** and select **Cisco Product Documentation**.

To access user documentation on the Documentation CD-ROM:

On the Documentation CD-ROM, select **Cisco Product Documentation**.

Paths to specific documents are provided below, starting at **Cisco Product Documentation**.



Tip To navigate up to the next higher level in the documentation hierarchy, click on **CONTENTS** in the navigation bar at the top of each page.

Cisco AS5350 and Cisco AS5400 Universal Gateway Documentation

Regulatory Compliance and Safety Information

The *Regulatory Compliance and Safety Information* document provides essential safety information applicable to your universal gateway. A printed copy of this document is shipped with this device.

You can access this document at **Cisco Product Documentation > Access Servers and Routers > Access Servers> Cisco AS5350 or Cisco AS5400> Regulatory Compliance and Safety Info for the Cisco AS5350 or Cisco AS5400**.

Hardware Installation

The hardware installation guide provides additional detailed description, installation, and cabling information.

You can access this document at **Cisco Product Documentation > Access Servers and Routers > Access Servers > Cisco AS5350 or Cisco AS5400 > Hardware Installation Documents for Cisco AS5350 or Cisco AS5400**.

Software Configuration

The software configuration guide provides additional detailed configuration information.

You can access this document at **Cisco Product Documentation > Access Servers and Routers > Access Servers> Cisco AS5350 or Cisco AS5400 > Software Configuration Documents for Cisco AS5350 or Cisco AS5400**.

Release Notes

Cisco IOS release notes for the Cisco AS5350 and Cisco AS5400 universal gateways provide up-to-date information about specific Cisco IOS software releases and new hardware used on these universal gateways.

You can access these documents at **Cisco Product Documentation > Access Servers and Routers > Access Servers> Cisco AS5350 or Cisco AS5400 > Cisco IOS Release Notes for Cisco AS5350 or Cisco AS5400**.

Related Hardware Documentation

Replacing the Power Supply in the Cisco AS5300 Series and Cisco AS5400 has instructions about replacing the power supply. You can access this document at [Cisco Product Documentation > Access Servers and Routers > Access Servers > Cisco AS5350 or Cisco AS5400 > Hardware installation documents for Cisco AS5350](#).

Cisco IOS Software Documentation

Master Index to Software Documentation

The master index provides links to topics and commands for specific Cisco IOS software releases.

You can access these documents at [Cisco Product Documentation > Cisco IOS Software > Cisco IOS Software Release you are using > Master index for Cisco IOS software release you are using](#).

Configuration Guides

The Cisco IOS software configuration guides provide detailed configuration procedures and examples.

You can access these documents at [Cisco Product Documentation > Cisco IOS Software > Cisco IOS Software Release you are using > Configuration Guides and Command References > Configuration guide for your application](#).

Command References

The Cisco IOS software command references provide detailed information about each command.

You can access these documents at [Cisco Product Documentation > Cisco IOS Software > Cisco IOS Software Release you are using > Configuration Guides and Command References > Command reference for your application](#).

New Feature Documentation

New Feature Documentation contains detailed information about new features introduced in specific Cisco IOS releases.

You can access these documents at [Cisco Product Documentation > Cisco IOS Software > Cisco IOS Software Release you are using > New Feature Documentation](#).

If you have an account on Cisco.com, you can get updated information about platform support for features by accessing Feature Navigator at the following URL:

<http://www.cisco.com/go/fn>

Release Notes

Cisco IOS release notes for all platforms provide up-to-date information about specific Cisco IOS software releases.

You can access these documents at [Cisco Product Documentation > Cisco IOS Software > Cisco IOS Software Release you are using > Release Notes > Release Notes for the Cisco IOS software release you are using](#).

Supporting Documents and Related Documentation

These documents contain additional information, including debug commands and error messages, about specific Cisco IOS software releases.

You can access these documents at [Cisco Product Documentation > Cisco IOS Software > Cisco IOS Software Release you are using > Supporting Documents or Related Documentation](#).

Additional documents of this type are located at [Cisco Product Documentation > Access Servers and Access Routers > Access Servers > Cisco AS5350 or Cisco AS5400](#).

Items Included with Cisco AS5350 and Cisco AS5400 Universal Gateways

- 19- and 24-inch rack-mount kits
- Rubber feet for desktop installation
- RJ-45-to-DB-9 female DTE adapter (labeled TERMINAL)
- RJ-45-to-DB-25 female DTE adapter (labeled TERMINAL)
- RJ-45-to-DB-25 male DCE adapter (labeled MODEM)
- RJ-45-to-RJ-45 rollover console cable
- ESD-preventive wrist strap
- Nylon cable ties
- Cable tie holder
- Grounding lug
- Cisco Information and CD-ROM Package

Items Not Included

Individual items in this list may be required for your particular application:

- Straight-through RJ-45-to-RJ-45 cable for an Ethernet connection
- Straight-through RJ-45-to-RJ-45 cables for T1 connections
- E1 cables for E1 connections
- Ethernet hub or PC with a network interface card for Ethernet LAN connections
- PC running terminal emulation software for local administrative access
- Modem for remote administrative access
- One breakout cable consisting of a 36-pin connector connected to eight RJ-45 adapters for CT1/CE1 connections
- 75-ohm coaxial cable for a CT3 connection

2 Install Chassis



Note The information in this document applies to the Cisco AS5350, Cisco AS5400, and Cisco AS5400HPX universal gateways.



Note Unless specifically noted, all references to the Cisco AS5400 also apply to the Cisco AS5400HPX.

Safety Information



Warning For safety information you need to know before working on your Cisco universal gateway, see the *Regulatory Compliance and Safety Information* document that accompanied this device.

Setting Up the Chassis

You can install the chassis in a rack or set it on a desktop. Select the procedure that best meets the needs of your network:

- Rack-Mounting the Chassis, page 5
- Desktop Installation, page 7



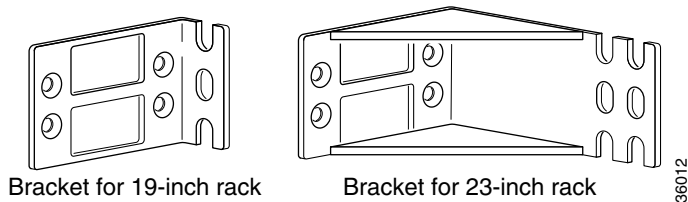
Warning

This unit is intended for installation in restricted access areas. A restricted access area is where access can only be gained by service personnel through the use of a special tool, lock and key, or other means of security, and is controlled by the authority responsible for the location. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.

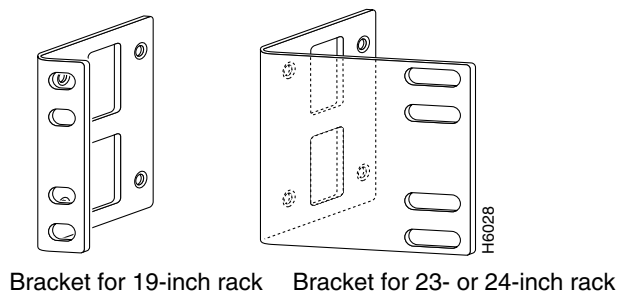
Rack-Mounting the Chassis

This section describes how to rack-mount the chassis. The universal gateway arrives with 19-inch rack-mount brackets and larger brackets for use with a 23- or 24-inch rack.

Cisco AS5350 Rack-Mount Brackets



Cisco AS5400 Rack-Mount Brackets



The following information will help you plan your equipment rack configuration:

- Enclosed racks must have adequate ventilation. Ensure that the rack is not congested, because each unit generates heat. An enclosed rack should have louvered sides and a fan to provide cooling air. Heat generated by equipment near the bottom of the rack can be drawn upward into the intake ports of the equipment above.
- When mounting a chassis in an open rack, ensure that the rack frame does not block the intake or exhaust ports. If the chassis is installed on slides, check the position of the chassis when it is seated in the rack.
- Baffles can isolate exhaust air from intake air, which also helps to draw cooling air through the chassis. The best placement of the baffles depends on the airflow patterns in the rack, which can be found by experimenting with different configurations.
- When equipment installed in a rack (particularly in an enclosed rack) fails, try operating the equipment by itself, if possible. Power off other equipment in the rack (and in adjacent racks) to allow the unit under test a maximum of cooling air and clean power.
- Install the chassis and external devices to which it will connect in a contiguous stack.

Required Tools and Equipment

You need the following tools and equipment to rack-mount the chassis:

- Number 2 Phillips screwdriver (not included)
- Medium flat-blade screwdriver (not included)
- Screws for attaching the chassis to the rack (not included)
- Standard rack-mount brackets (included)
- Screws for attaching the brackets to the chassis (included)

Attaching Brackets

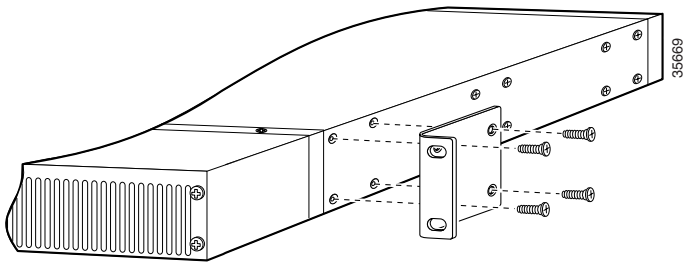
Attach the mounting brackets to the chassis as shown, using the screws provided. Attach the second bracket to the opposite side of the chassis.



Note

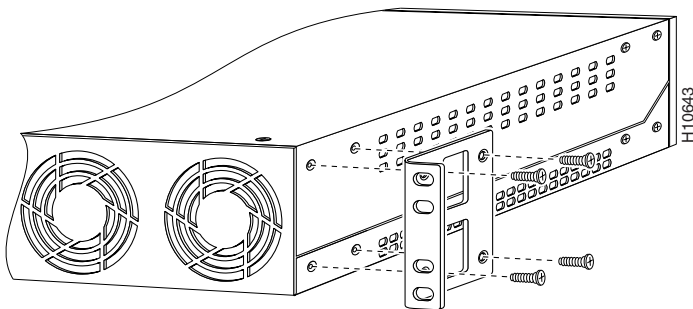
The chassis may be installed with either the front or rear panel facing forward.

Cisco AS5350 Bracket Installation—Front Panel Forward (19-Inch Rack)



Note: The second bracket attaches to the other side of the chassis.
The chassis can also be installed with the rear panel forward.

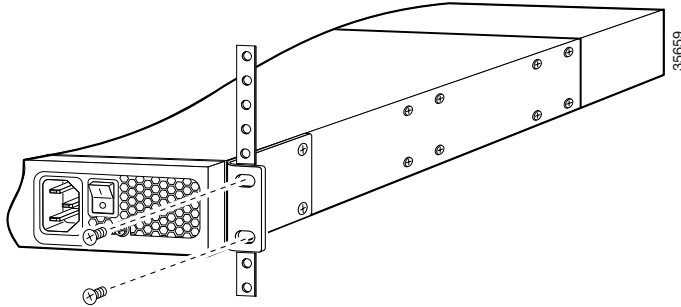
Cisco AS5400 Bracket Installation—Front Panel Forward (19-Inch Rack)



Installation in a Rack

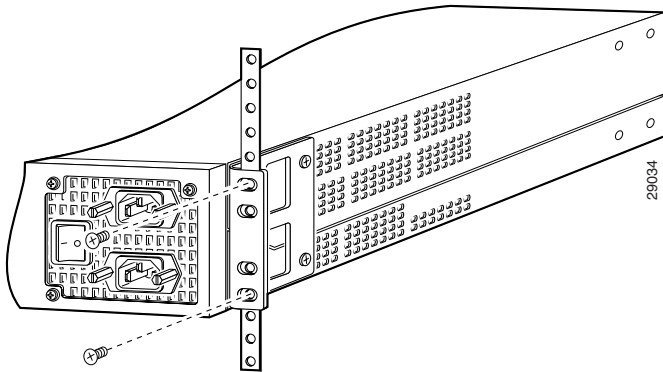
Install the chassis in the rack. Rack-mounting screws are not provided. Use two screws for each side (supplied with the rack).

Installing the Cisco AS5350 in a Rack (19-Inch Rack)



Note: The second bracket attaches to the rack at the other side of the chassis. The chassis can also be installed with the front panel forward.

Installing the Cisco AS5400 in a Rack (19-Inch Rack)



Note: The second bracket attaches to the rack at the other side of the chassis. The brackets can also be installed with the front panel forward.

Desktop Installation

For desktop or shelf mounting, use the rubber “feet” shipped on a black adhesive strip with the chassis. They protect the chassis and provide a nonskid surface.

The location of the chassis is extremely important for proper operation. Equipment placed too close together, inadequate ventilation, and inaccessible panels can cause malfunctions and shutdowns, and can make maintenance difficult. The following information will help you to plan the location of the chassis:

- Plan for access to both front and rear panels of the chassis.
- Ensure that the room where the chassis operates has adequate ventilation. Remember that electrical equipment generates heat. Ambient air temperature may not cool equipment to acceptable operating temperatures without adequate ventilation

To attach the rubber feet, take the following steps:

-
- Step 1** Locate the rubber feet that shipped with the chassis.
 - Step 2** Place the universal gateway upside-down on a smooth, flat surface.

Step 3 Peel the rubber feet off the black adhesive strip and place them adhesive-side down at each corner of the underside of the chassis.

Step 4 Place the universal gateway top-side up on a flat, smooth, secure surface.



Caution

Do not place anything on top of the universal gateway that weighs more than 10 lb (4.5 kg). Excessive weight on top could damage the chassis.

Chassis Ground Connection

You must connect the chassis to a reliable earth ground using the ground lug (provided) and size AWG 6 (13 mm²) wire.

To attach the chassis ground, take the following steps:

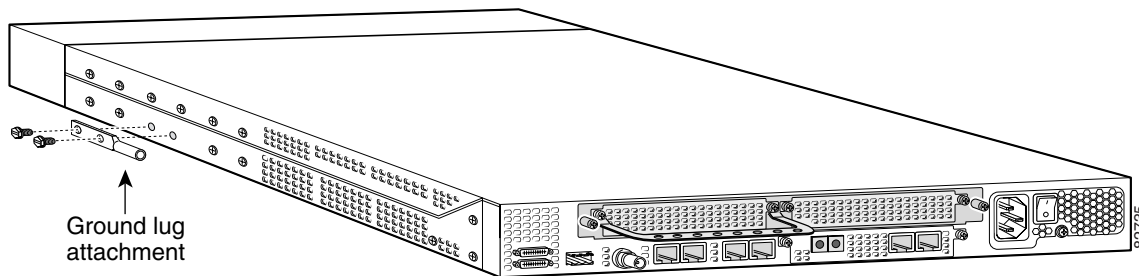
Step 1 Strip one end of the ground wire to expose approximately 0.75 in. (20 mm) of conductor.

Step 2 Crimp the ground wire to the ground lug, using a crimp tool of the appropriate size.

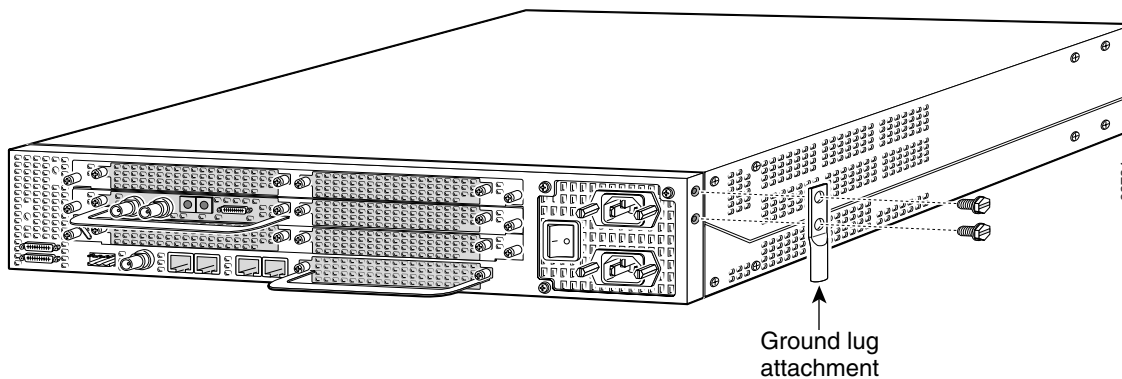
Step 3 Attach the ground lug to the chassis. Use a medium flat-blade screwdriver and the screws supplied with the ground lug. Tighten the screws to a torque of 8 to 10 in-lb (0.9 to 1.1 N-m).

Step 4 Connect the other end of the ground wire to a suitable grounding point at your site.

Cisco AS5350 Ground Lug Attachment



Cisco AS5400 Ground Lug Attachment



3 Install Modules



Note The information in this document applies to the Cisco AS5350, Cisco AS5400, and Cisco AS5400HPX universal gateways.



Note Unless specifically noted, all references to the Cisco AS5400 also apply to the Cisco AS5400HPX.



Note Cisco AS5350 and Cisco AS5400 come with carrier cards and DFCs already installed. If the required dial feature cards are already installed, proceed to the “Connect Cables” section on page 14.

For additional information about installing carrier cards and dial feature cards, refer to the *Cisco AS5350 and Cisco AS5400 Universal Gateway Card Installation Guide*.

You can access this document at [Cisco Product Documentation > Access Servers and Access Routers > Access Servers > Cisco AS5350 or Cisco AS5400 > Hardware Installation Documents for Cisco AS5350 or Cisco AS5400](#).

Installing Carrier Cards



Caution The carrier cards that carry the DFCs are not hot swappable. Removing a carrier card while the system is still powered on may cause permanent damage to electronic circuits on the card.



Warning **Before opening the chassis, disconnect the telephone-network cables to avoid contact with telephone-network voltages. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**



Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

Installing a Carrier Card

If you need to install a carrier card, follow this procedure:

Step 1 Make sure the chassis is powered off.

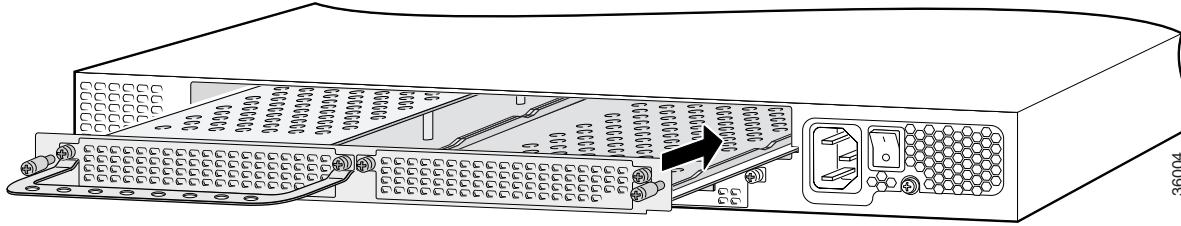


Warning **Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

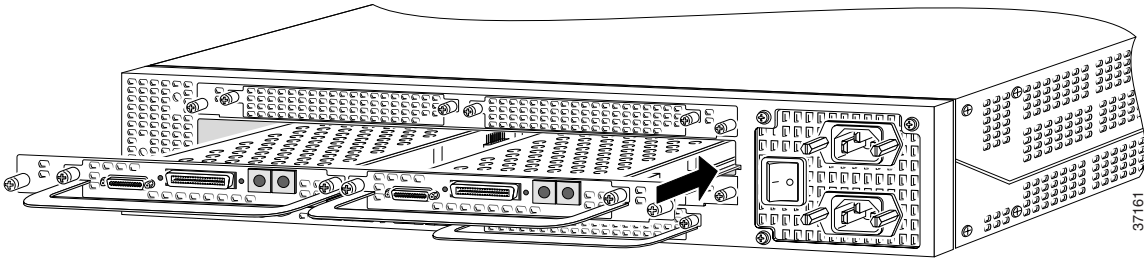
Step 2 Attach an ESD-preventive wrist strap.

Step 3 Slide the carrier card into the slot until it touches the backplane connector.

Install the Carrier Card in the Cisco AS5350



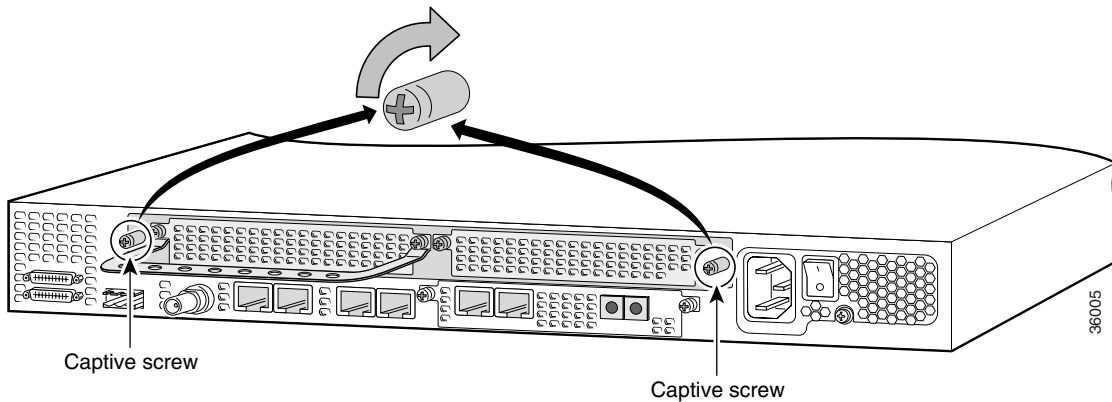
Install the Carrier Card in the Cisco AS5400



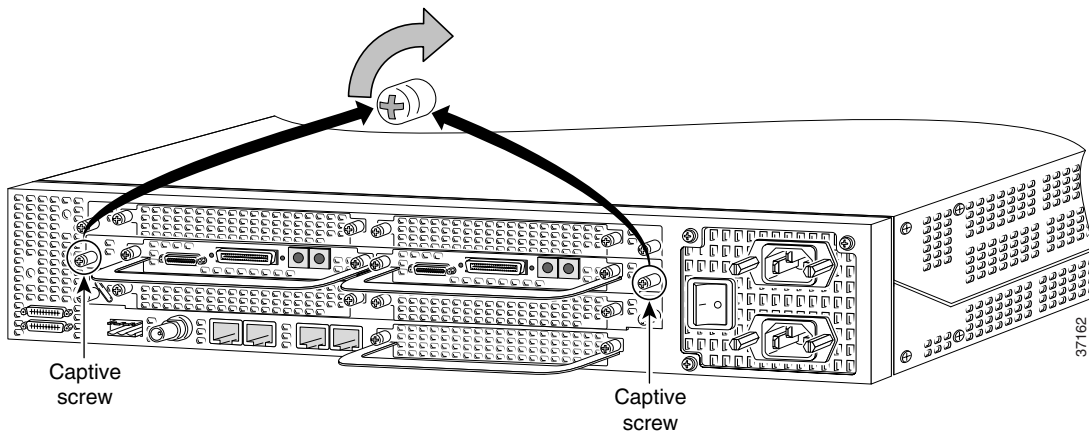
Step 4 Align the captive screws with their holes, and seat the card completely.

Step 5 Tighten the two captive screws to secure the carrier card to the chassis.

Tighten the Captive Screws on the Cisco AS5350

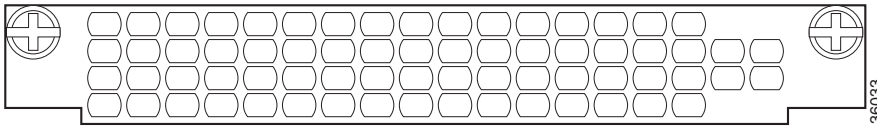


Tighten the Captive Screws on the Cisco AS5400



Step 6 If the carrier card has a blank DFC slot, install a blank cover over the open DFC slot to ensure proper airflow inside the chassis.

Blank DFC Cover




Step 7 For AC powered units, reconnect the AC power cord. For DC powered units, reinstate power at the circuit breaker. For more information on the AC and DC power supplies, refer to the chassis installation guide. To access the chassis guide see the “Documents, Equipment, and Tools” section on page 2.


Step 8 Reconnect all interface cables.


Installing DFCs

For detailed information on installing and connecting DFCs, refer to the *Cisco AS5350 and Cisco AS5400 Universal Gateway Card Installation Guide*. You can access this document at [Cisco Product Documentation > Access Servers and Access Routers > Access Servers > Cisco AS5350 or Cisco AS5400 > Hardware Installation Documents for Cisco AS5350 or Cisco AS5400](#).

 **Warning** Do not work on the system or connect or disconnect cables during periods of lightning activity. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.

 **Warning** The telecommunications lines must be disconnected 1) before unplugging the main power connector and/or 2) while the housing is open. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.

 **Note** When you replace a DFC with a new DFC of the same type in the same slot, the system software recognizes the new trunk interfaces and brings them up automatically. If you replace the existing DFC with a new DFC of a different type, you must reconfigure the system. For configuration details, refer to the *Cisco AS5350 and Cisco AS5400 Universal Gateway Software Configuration Guide*.

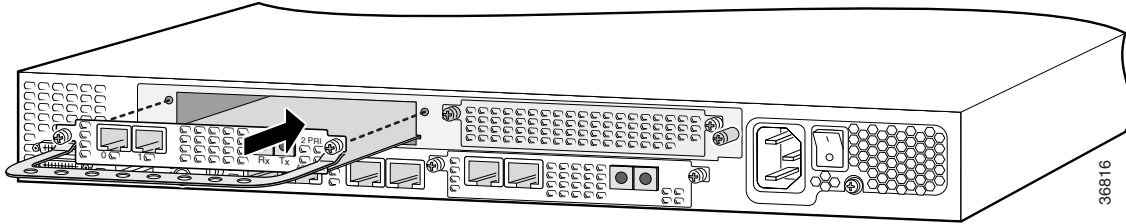
 **Note** The Cisco AS5350 and Cisco AS5400 support one type of WAN DFC at a time. For more information about mixing WAN DFCs, see the *Cisco AS5350 and Cisco AS5400 Universal Gateway Card Installation Guide*.

To install a DFC, follow these steps:

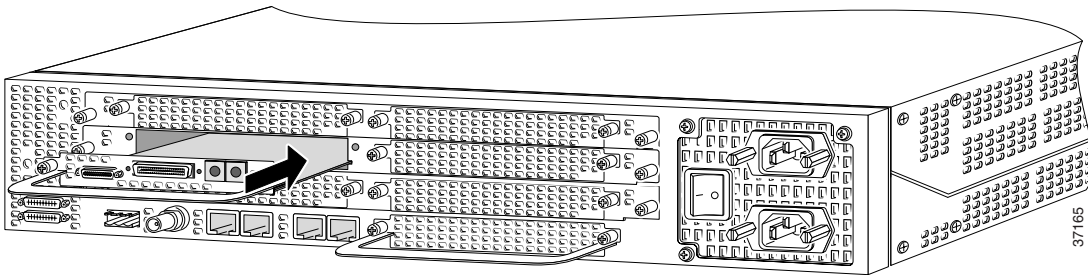
Step 1 Attach an ESD-preventive wrist strap.

Step 2 Slide the DFC into the slot until the connector pins make contact with the carrier card backplane connector.

Installing a DFC in a Cisco AS5350



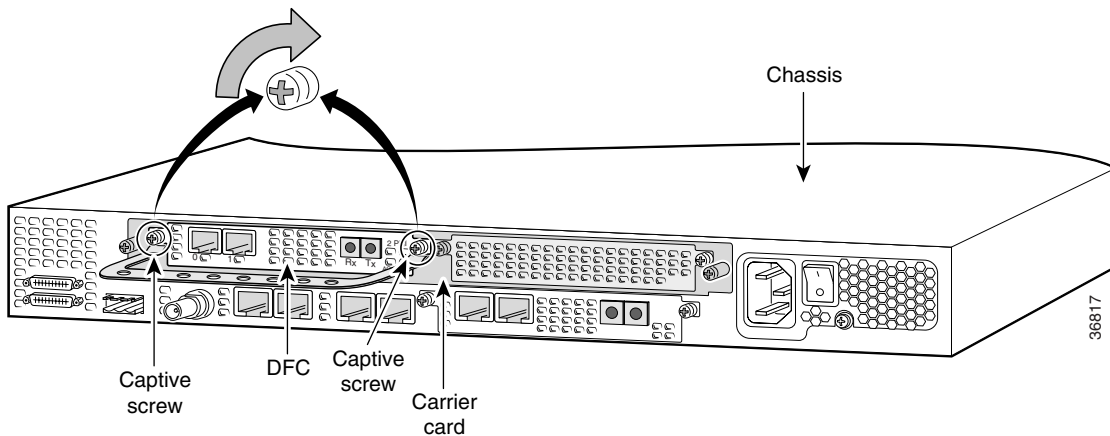
Installing a DFC in a Cisco AS5400



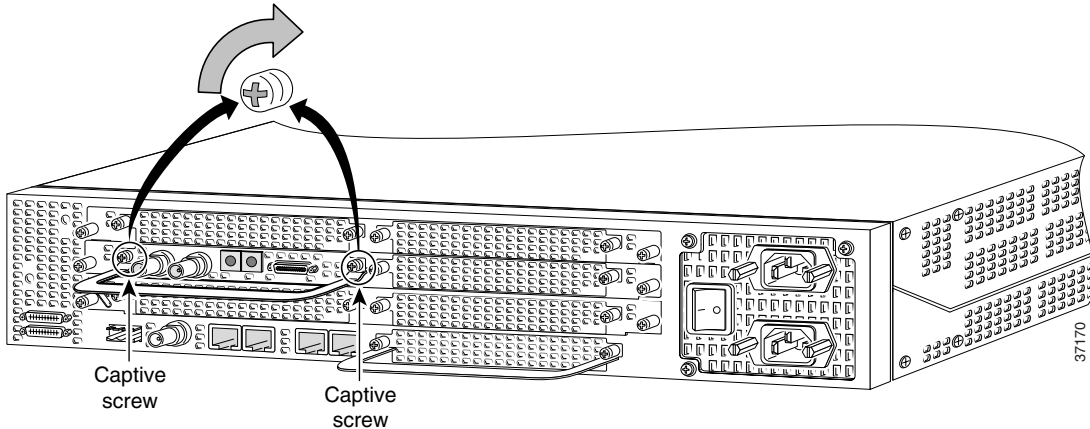
Step 3 Align the captive screws with their holes, and seat the card completely.

Step 4 Tighten the screws to secure the DFC to the chassis.

Tighten the Captive Screws on the Cisco AS5350



Tighten the Captive Screws on the Cisco AS5400



Step 5 Check the card LEDs to verify that the card is working properly. The following table summarizes the LED function for the trunk and port DFCs.

Dial Feature Card LEDs

DFC	LED	State	Description
T1 or E1 DFC	ACTIVITY (ACT)	Fast flicker (Green)	Indicates DFC is up and running.
		Slow flicker (Green)	Indicates DFC is not yet fully functional.
	OK/MAINT	Green	The T1 or E1 DFC has passed initial power-up diagnostics tests and is operating normally.
		Yellow	The T1 or E1 DFC is not functioning. See the console for messages.
		Off	Indicates that all calls associated with the card are shut down and it is safe to remove the card with the system powered on.
	Remote alarm (RA), local alarm (LA), or loopback (LB)	On (Yellow)	One LED below each T1/E1 port indicates one of the following: <ul style="list-style-type: none"> A local or remote loopback diagnostic test is running on the associated T1 port. An alarm is received on the associated T1/E1 port, indicating loss of signal (LOS) or loss of multiframe alignment (LOF) at the local or remote node.

Dial Feature Card LEDs (continued)

DFC	LED	State	Description
T3 DFC	ACTIVITY (ACT)	Fast flicker	Indicates DFC is up and running.
		Slow flicker	Indicates DFC is not yet fully functional.
	OK/MAINT	On (Green)	The CT3 DFC passed initial power-up diagnostics tests and is operating normally.
		Yellow	The CT3 DFC is not functioning. See the console for messages.
		Off	Indicates that all calls associated with the DFC are shut down and it is safe to remove the card with the system powered on.
	M13 alarm (MA)	On	Indicates the presence of one of the following on the CT3 line: received alarm indication signal (RAIS), loss of signal (LOS), receive red alarm (RRED), or a far-end receive failure (RFERF). ¹
		Off	Remains off when operating condition is normal.
	Remote alarm (RA)	On	Indicates a T1 alarm condition encountered by software.
		Off	Remains off when operating condition is normal.
	Local alarm (LA)	On	Indicates a T1 alarm condition encountered by software for a specific port.
		Off	Remains off when operating condition is normal.
	T3 EN/DIS	Green	Indicates a CT3 card line connection enabling normal operation.
		Yellow	Normal operation is disabled.
	Low signal (LOS)	On	Indicates the CT3 LIU is experiencing a loss of signal.
Off		Remains off when operating condition is normal.	
Network loop (LOOP)	On	Indicates that at least one T1 is unavailable.	
	Off	Remains off when operating condition is normal.	
Universal port DFC	ACTIVITY (ACT)	Flickering	There is call activity on the DFC.
	OK/MAINT	On	The DFC passed the initial power-up diagnostic tests and is operating normally.
		Off	Indicates that all calls associated with the card are shut down and it is safe to remove the card with the system powered on.

1. To display information about an M13 alarm, use the `show CT3 EXEC` command.

4 Connect Cables



Note The information in this document applies to the Cisco AS5350, Cisco AS5400, and Cisco AS5400HPX universal gateways.



Note Unless specifically noted, all references to the Cisco AS5400 also apply to the Cisco AS5400HPX.

System Management and Power Connections

The connections described here provide electrical power and management access. For cable pinouts, see the chassis and card installation guides for the Cisco AS5350 and Cisco AS5400. You can access these documents at [Cisco Product Documentation > Access Servers and Access Routers > Access Servers > Cisco AS5350 or Cisco AS5400 > Hardware Installation Documents for Cisco AS5350 or Cisco AS5400](#).

Power and Management Cable Connections

Port or Connection	Color or Type	Connected to:	Cable
Console	Light blue	PC or ASCII terminal communication port (usually labeled COM)	RJ-45-to-RJ-45 rollover cable (included) and terminal adapter (included).
Auxiliary	Black	Modem for remote access	RJ-45-to-RJ-45 rollover cable and a modem adapter (included).
Power (AC)	Power cable	100-240 VAC, 50-60 Hz	Grounding power cord (included).
Power (DC)	Refer to the "Connect DC Power" section on page 27 for instructions about the DC power connections.		
Bantam jack		Test device	
Alarm		Alarm device	12 or 14 AWG copper wire
BITS port		Signal generator	Coax cable

WAN, LAN, and Voice Connections

The following table summarizes the WAN, LAN, and voice connections.

WAN, LAN and Voice Connections

Port or Connection	Port type, color	Connected to:	Cable
Ethernet	RJ-45, Yellow	Ethernet hub	Straight-through Ethernet
T1/E1 WAN	RJ-45	T1 or E1 network	RJ-45 to DB-15
			RJ-45 to BNC interface cable for unbalanced connections
			RJ-45 to Twinax interface cable for balanced connections
			RJ-45 to RJ-45
			RJ-45 to bare wire
	36-pin serial		8-port interface cable
T3 WAN	BNC	T3 network	BNC to BNC

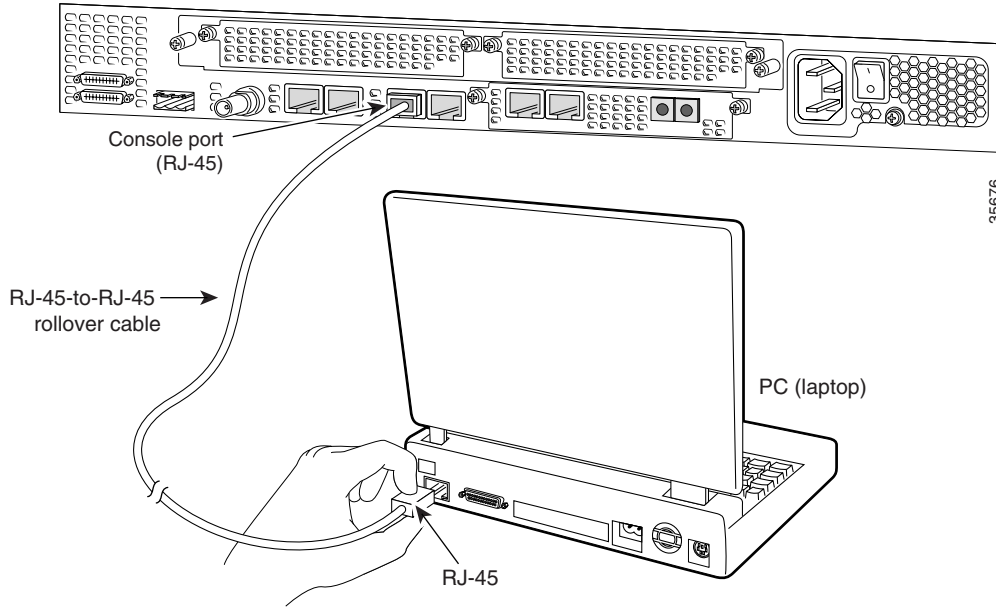
Connect a Console Terminal

Use the console terminal for local administrative access to the universal gateway. You can only connect a terminal to the console port. You can use the auxiliary port to connect a terminal or a modem for remote access to the universal gateway.

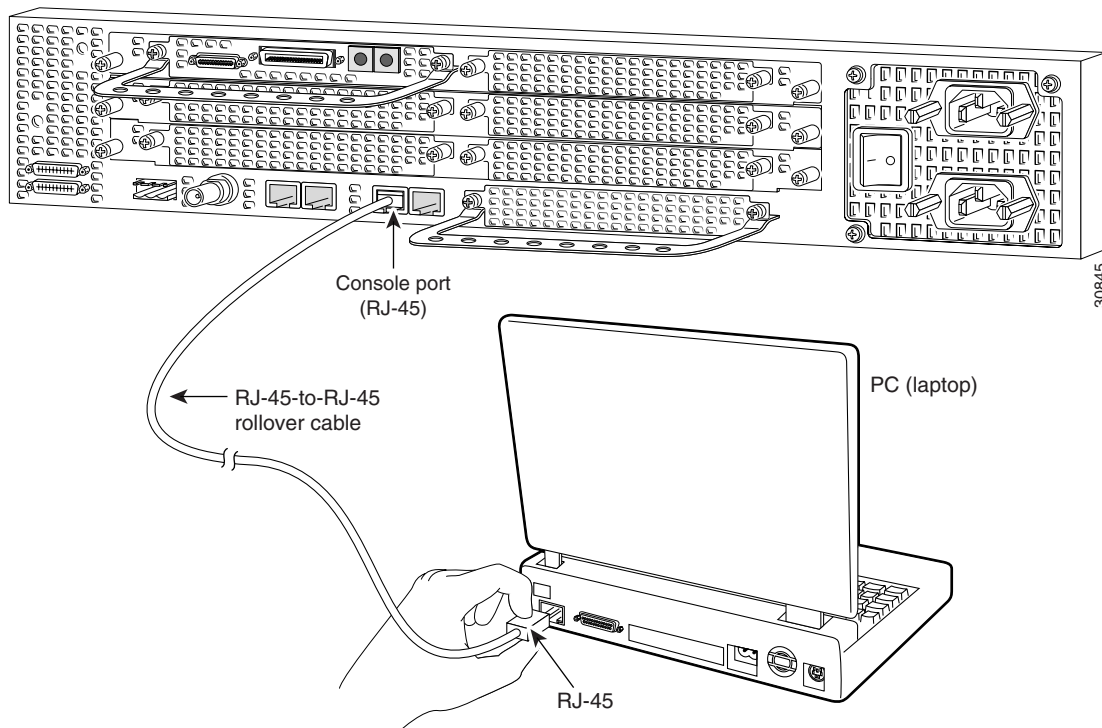
To connect a terminal (an ASCII terminal or a PC running terminal emulation software) to the console port on the Cisco AS5350 or Cisco AS5400, follow this procedure.

Step 1 Connect the terminal to the console port using an RJ-45 rollover cable and an RJ-45-to-DB-25 or RJ-45-to-DB-9 adapter. The adapters provided are labeled **TERMINAL**. The adapters and the rollover cable are included in the accessory kit that ships with the universal gateway.

Connecting Cisco AS5350 to Console Terminal



Connecting Cisco AS5400 to Console Terminal

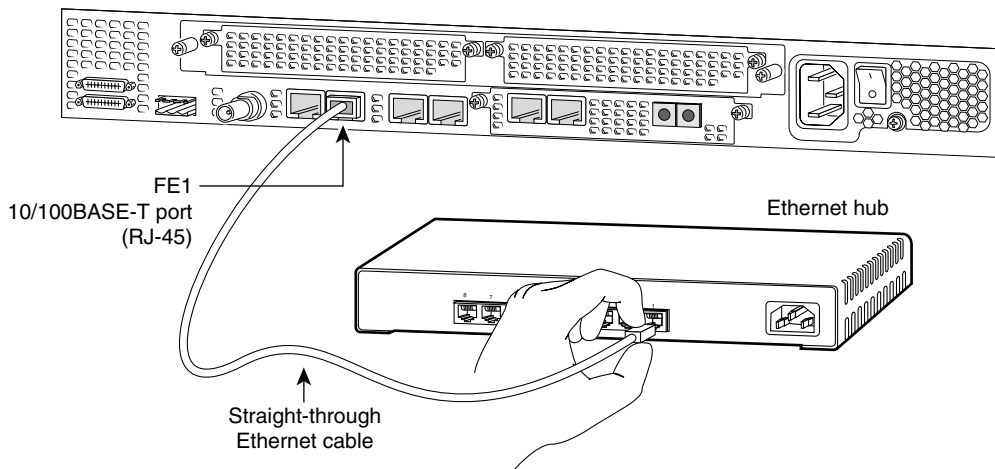


Step 2 Configure your terminal or PC terminal emulation software for 9600 baud, 8 data bits, no parity, and 2 stop bits. To configure the console port, refer to the *Cisco AS5350 and Cisco AS5400 Universal Gateway Software Configuration Guide*.

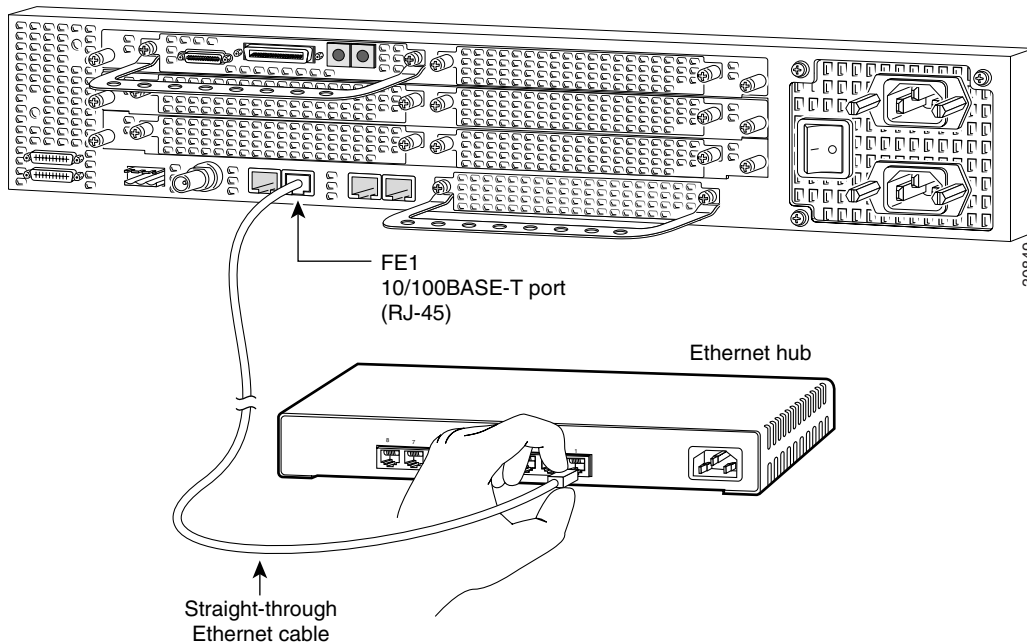
Connect to Ethernet Network

- Connect the universal gateway to an Ethernet network by using a straight-through RJ-45-to-RJ-45 Ethernet cable to connect the Fast Ethernet port to an Ethernet hub.

Connecting Cisco AS5350 to Ethernet Hub



Connecting Cisco AS5400 to Ethernet Hub



Connect to a WAN



Warning

The telecommunications lines must be disconnected 1) before unplugging the main power connector and/or 2) while the housing is open. To see translations of the warnings that appear in the publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.



Warning

Hazardous network voltages are present in WAN ports regardless of whether power to the router is OFF or ON. To avoid electric shock, use caution when working near WAN ports. When detaching cables, detach the end away from the router first. To see translations of the warnings that appear in the publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.



Warning

This equipment is to be installed and maintained by service personnel only as defined by AS/NZS 3260 Clause 1.2.14.3 Service Personnel. To see translations of the warnings that appear in the publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.



Warning

To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord. To see translations of the warnings that appear in the publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.



Warning

The ISDN connection is regarded as a source of voltage that should be inaccessible to user contact. Do not attempt to tamper with or open any public telephone operator (PTO)-provided equipment or connection hardware. Any hardwired connection (other than by a nonremovable, connect-one-time-only plug) must be made only by PTO staff or suitably trained engineers. To see translations of the warnings that appear in the publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.



Warning

To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables. To see translations of the warnings that appear in the publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.



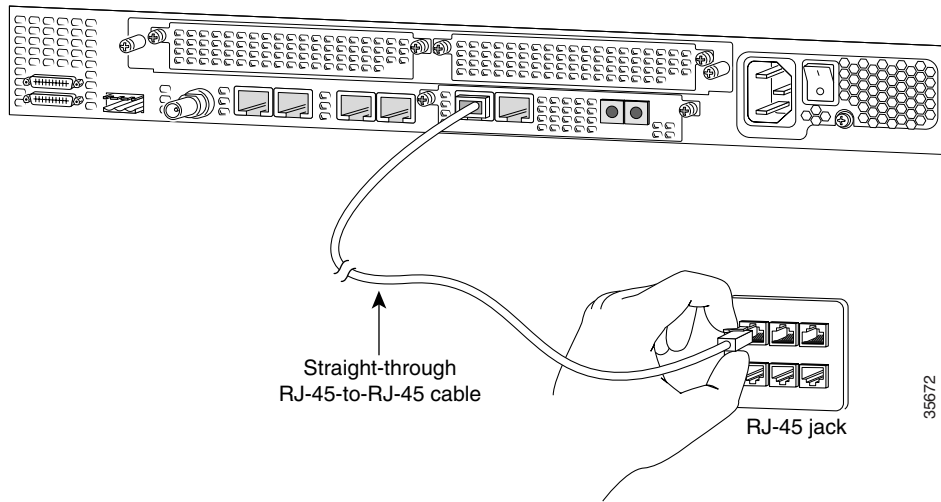
Warning

Incorrect connection of this or connected equipment to a general purpose outlet could result in a hazardous situation. To see translations of the warnings that appear in the publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.

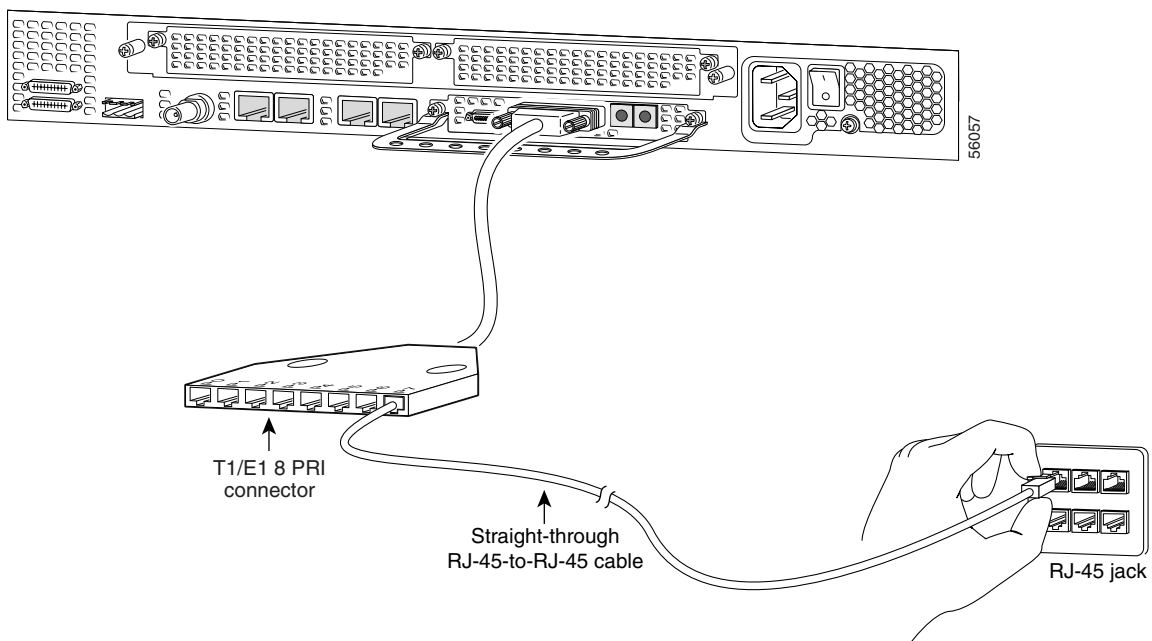
You can connect the Cisco AS5350 and Cisco AS5400 to a WAN in the following ways:

- Connect each T1/PRI port to an RJ-45 jack with a straight-through RJ-45 to RJ-45 cable.

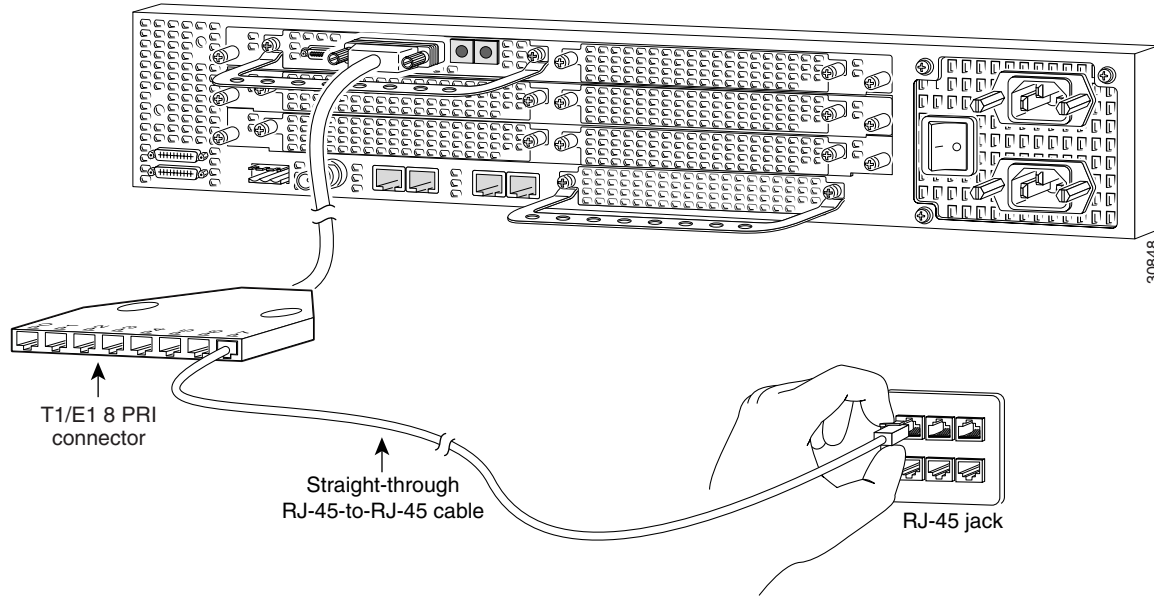
Connecting 2-Port or 4-Port DFC on Cisco AS5350 to RJ-45 Jack



Connecting 8-Port DFC on Cisco AS5350 to RJ-45 Jack



Connecting 8-Port DFC on Cisco AS5400 to RJ-45 Jack



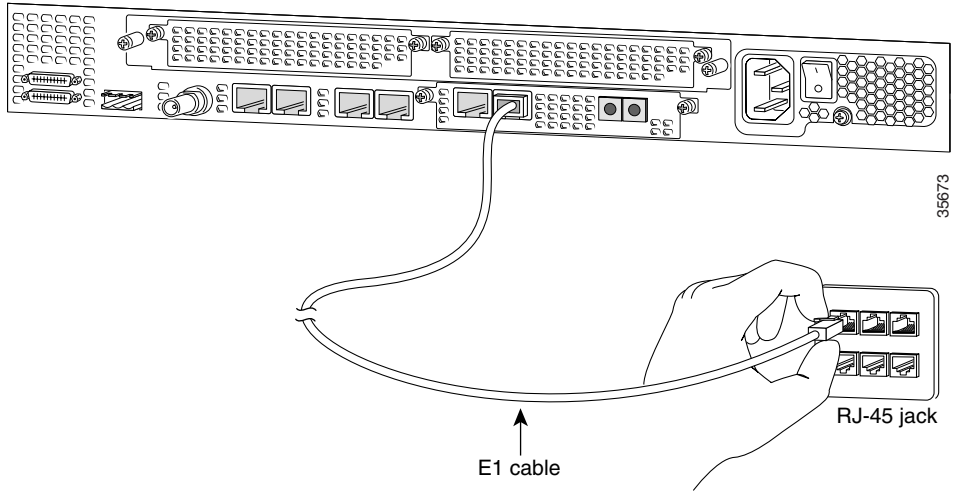
Note For other T1 cabling options, see the card installation guide for the Cisco AS5350 and Cisco AS5400. You can access this document at [Cisco Product Documentation > Access Servers and Access Routers > Access Servers > Cisco AS5350 or Cisco AS5400 > Hardware Installation Documents for Cisco AS5350 or Cisco AS5400](#).

- Connect each E1/PRI port to an RJ-45 jack with a straight-through RJ-45 to RJ-45 cable.

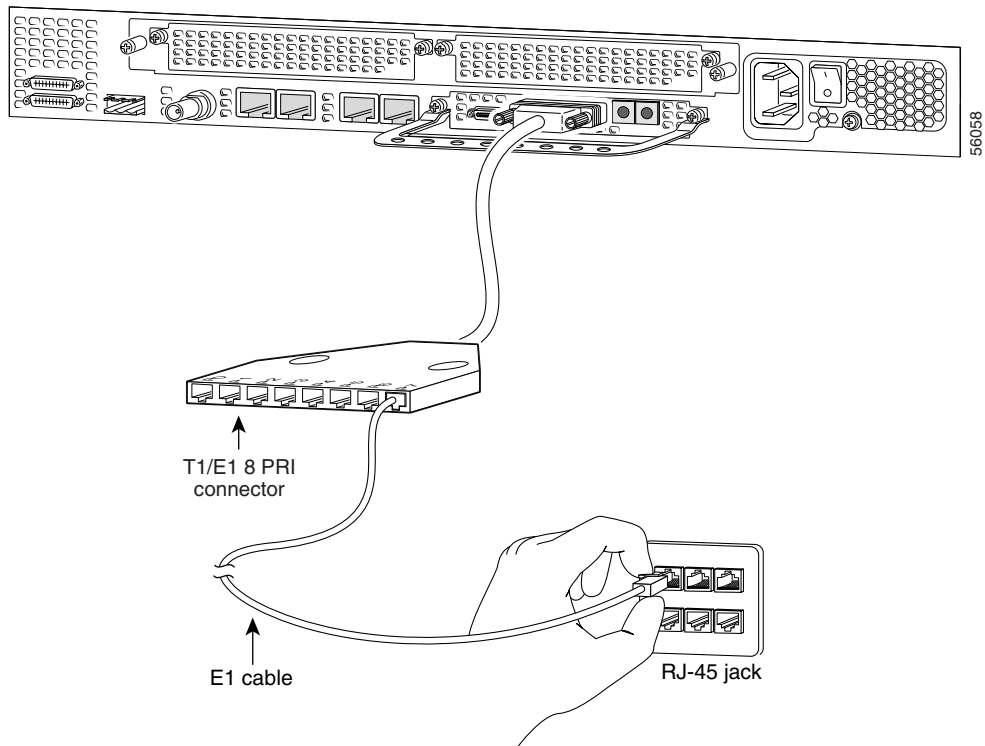
Note If you choose a port with 75-ohm input impedance, use an RJ-45-to-75-ohm coaxial cable adapter and plug it into that port. Use software commands to choose a particular port and the line termination on that port. For information on software commands, see the *Cisco AS5350 and Cisco AS5400 Universal Gateway Software Configuration Guide*.

Warning **The E1 interface card may only be installed in an ACA-permitted customer equipment or a Data Terminal Equipment (DTE) that is exempted from ACA's permit requirements. The customer equipment must only be housed in a cabinet that has screw-down lids to stop user access to overvoltages on the customer equipment. The customer equipment has circuitry that may have telecommunications network voltages on them. To see translations of the warnings that appear in the publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

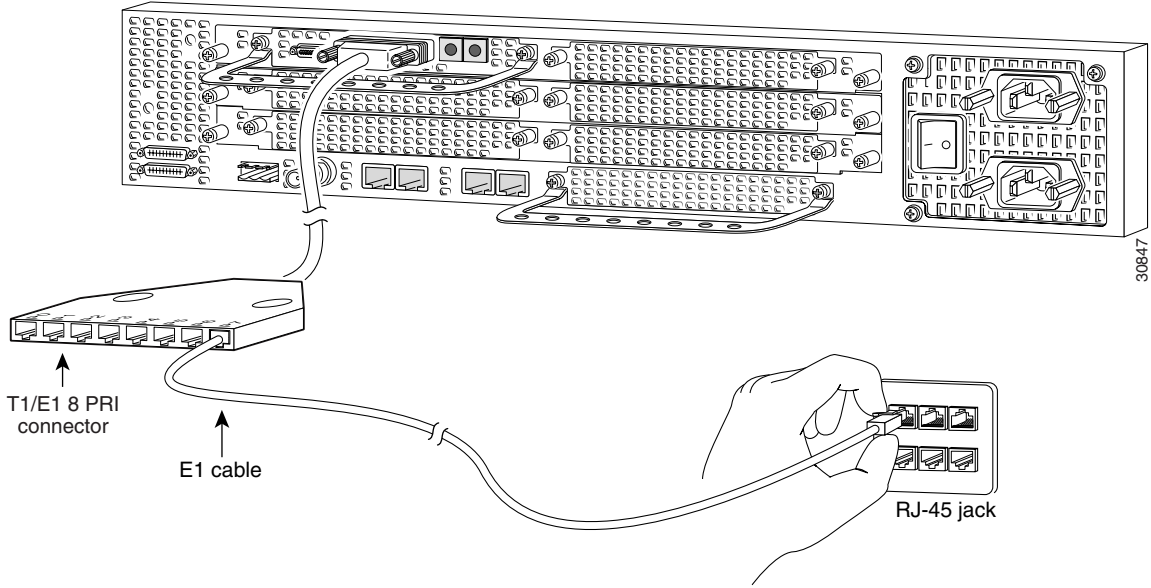
Connecting 2-Port or 4-Port DFC on Cisco AS5350 to RJ-45 Jack



Connecting 8-Port DFC on Cisco AS5350 to RJ-45 Jack

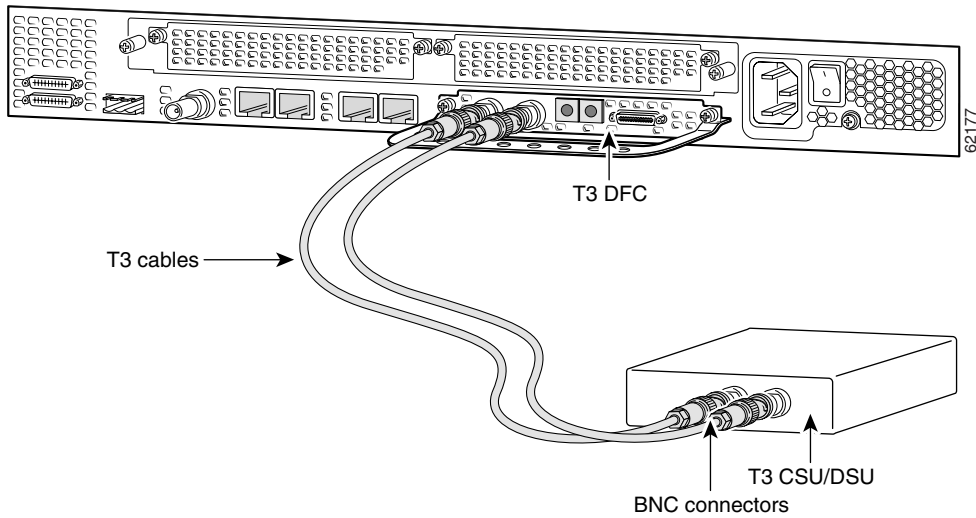


Connecting 8-Port DFC on Cisco AS5400 to RJ-45 Jack

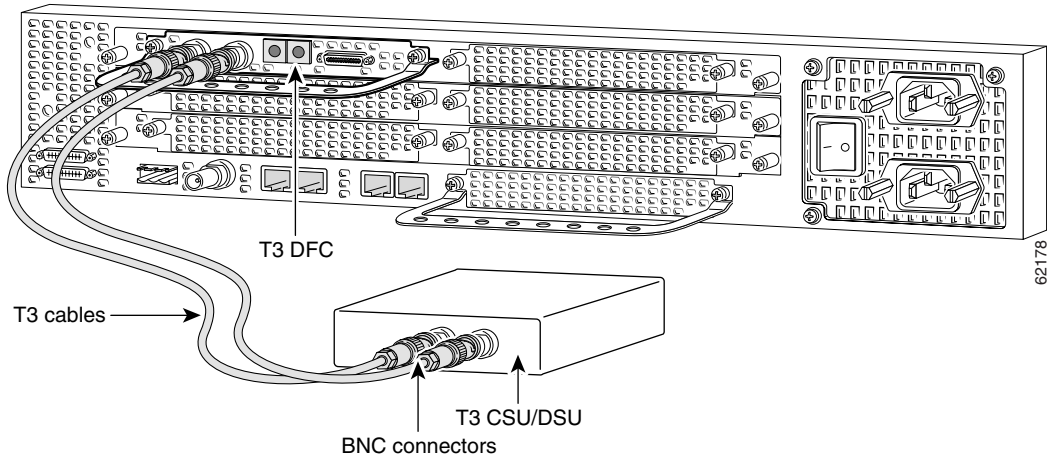


- Connect each T3 DFC to a T3 CSU/DSU with two 75-ohm BNC cables

Connecting T3 DFC on Cisco AS5350 to T3 CSU/DSU

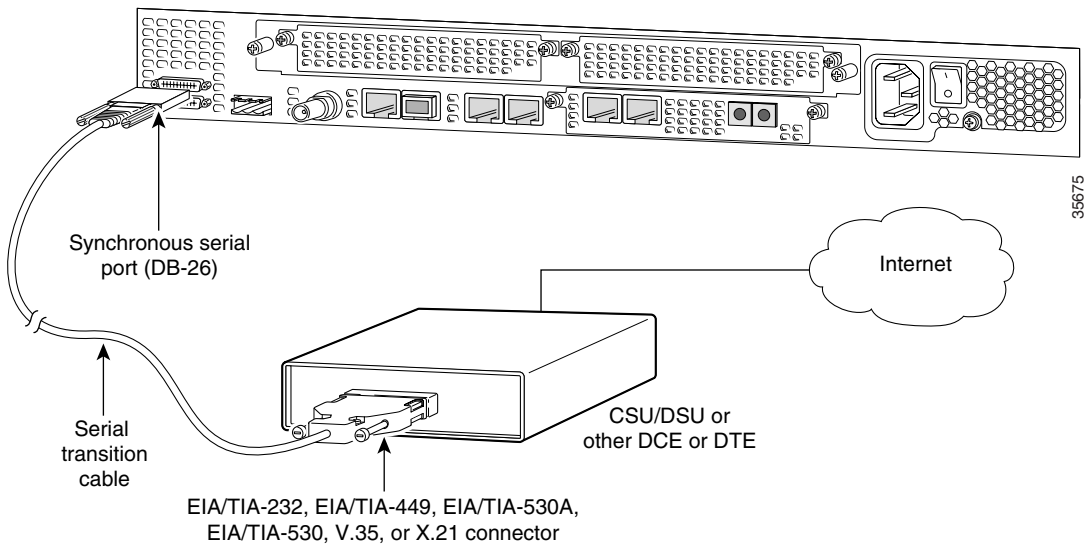


Connecting T3 DFC on Cisco AS5400 to T3 CSU/DSU

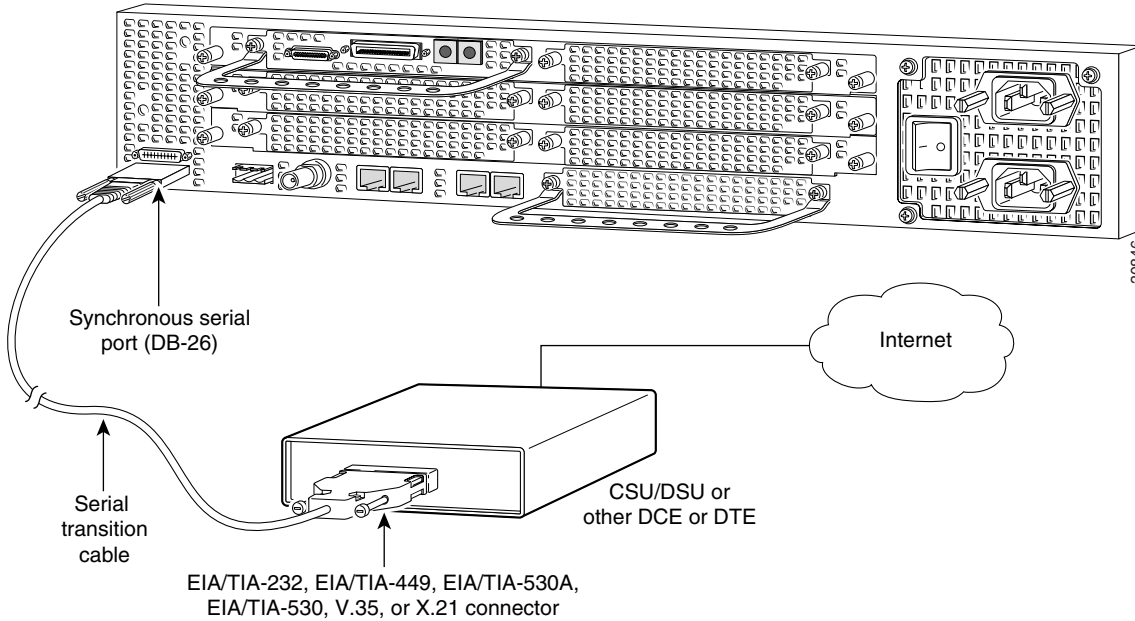


- Connect a synchronous serial port to a modem or a CSU/DSU with a serial transition cable.

Connecting Serial Port on Cisco AS5350 to CSU/DSU

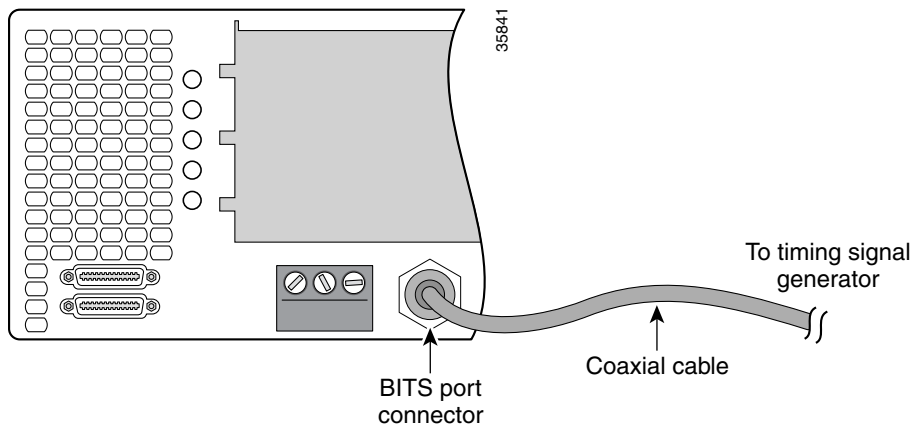


Connecting Serial Port on Cisco AS5400 to CSU/DSU



- Use a coaxial cable to connect a timing signal generator (TSG) to the BITS port. The BITS port is used for external clocking.

Connecting Cisco AS5350 and Cisco AS5400 to BITS Port



- Use a copper wire cable to connect to the alarm port.

Warning

The plug-socket combination must be accessible at all times because it serves as the main disconnecting device. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.

Warning

Incorrect connection of this or connected equipment to a general purpose outlet could result in a hazardous situation. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.

To connect an alarm device to the alarm port, follow this procedure:

Note The alarm connector is a 3-wire connector that plugs into a receptacle in the rear of the chassis. The connector is provided in the accessory kit that ships with the universal gateway.

Step 1 Insert the three-pin alarm port connector (included in the accessory kit) into the alarm port terminal block.

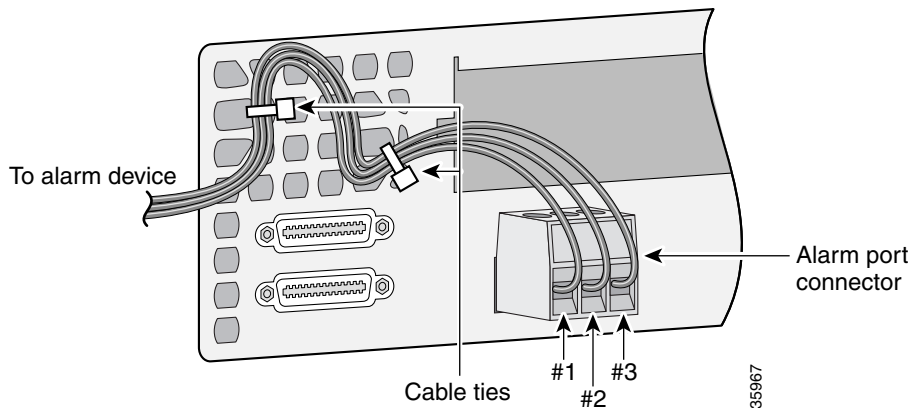
Step 2 Strip a minimum 1/4 in. (0.625 cm) off the wire insulation to connect the stranded wires to the alarm connector. The maximum insulation strip length is 0.31 in. (0.78 cm).

Note Use stranded Number 12 or 14 AWG copper wires to connect an alarm device to the alarm port connector.

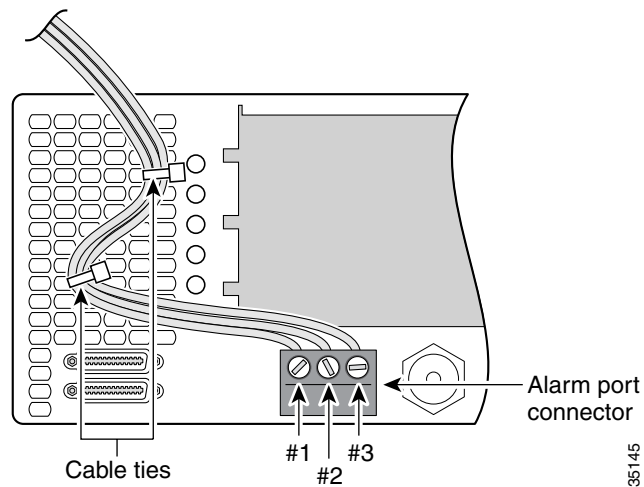
Step 3 Secure the wires to the alarm connector with the screws on the connector.

Caution The maximum tightening torque on the screws is 7 in.-lb (0.79 N-m).

Connecting Alarm Device to Cisco AS5350



Connecting Alarm Device to Cisco AS5400



Step 4 Attach two cable ties to the chassis and connect the wires to the cable ties.

Step 5 Attach the alarm wires to the alarm device.

Alarm Pinouts

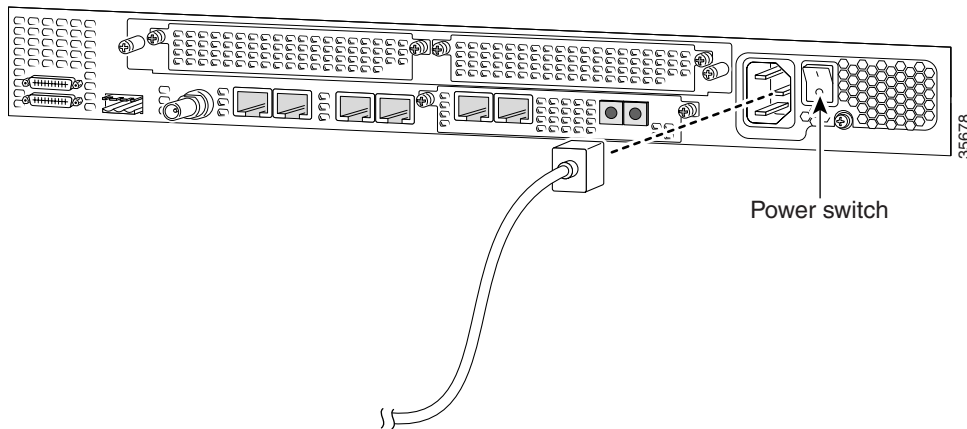
Pin ¹	Description
1	Normally open
2	Pole
3	Normally closed

1. The pins are numbered from left to right (facing the back of the chassis), starting with pin 1.

Connect AC Power

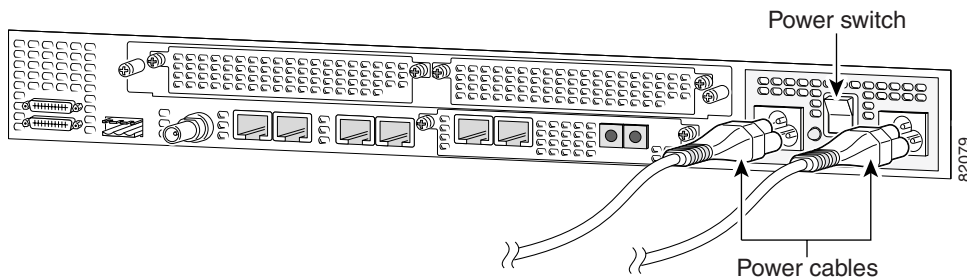
Step 1 Connect the black power cord to the receptacle on the power supply at the rear of the universal gateway.

Connecting AC Power Cord to Cisco AS5350 Single Power Supply



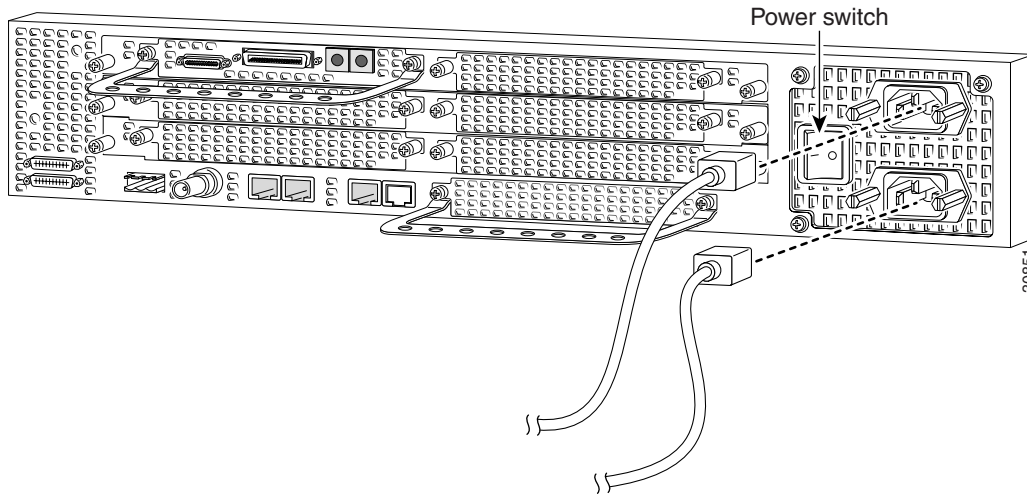
Note For the Cisco AS5350 redundant power supply, use the special power cable that came with your universal gateway.

Connecting AC Power Cord to Cisco AS5350 Redundant Power Supply



Note The Cisco AS5350 redundant power supply is supported in Cisco IOS Release 12.2(2)XB5 or later releases.

Connecting AC Power Cord to Cisco AS5400



Step 2 Connect the other end of the power cord to the electrical outlet.

Step 3 If your universal gateway has a second power supply installed, repeat Step 1 and Step 2 for the second power supply.

Connect DC Power

Warning

A readily accessible two-poled disconnect device must be incorporated in the fixed wiring. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.

Warning

This product relies on the building's installation or power supply for short circuit (overcurrent) protection. Ensure that a listed and certified fuse or circuit breaker no larger than 60 VDC, 15A U.S. is used on all current-carrying conductors. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.

If you ordered the universal gateway with a DC-input power supply, follow the directions in this section for proper wiring.

Note

The Cisco AS5350 redundant power supply is supported in Cisco IOS Release 12.2(2)XB5 or later releases.

Caution

In a DC power supply installation, do not connect the 48 VDC Return to chassis ground at the universal gateway. A single-point ground is recommended at the power distribution rack.

Note

This product is intended for installation in restricted access areas and is approved for connection using 12 or 14 AWG copper conductors only. The installation must comply with all applicable codes.

Step 1 Remove power from the DC circuit.


Warning

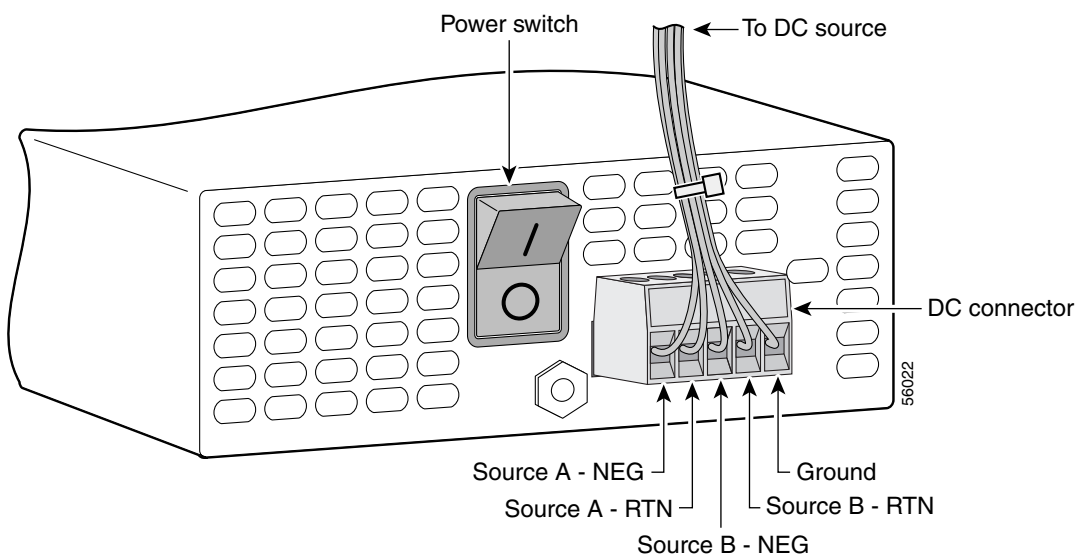
Before performing any of the following procedures, ensure that power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.

Step 2 Note the orientation of the DC power supply. The power supply cord should have three wires: 48 VDC Return, -48 VDC, and a safety ground (green wire).

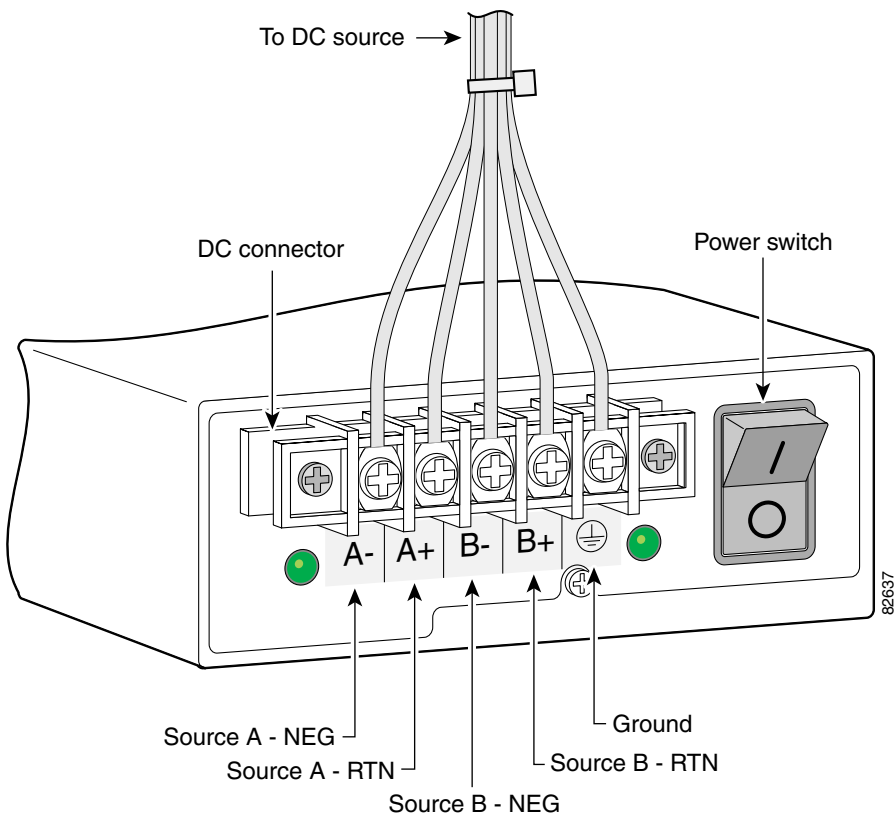

Warning

The illustration shows the DC power supply terminal block. Wire the DC power supply using the appropriate wire terminations at the wiring end, as illustrated. The proper wiring sequence is ground to ground, return to return, and negative to negative. Note that the ground wire should always be connected first and disconnected last. To see translations of the warnings that appear in the publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.

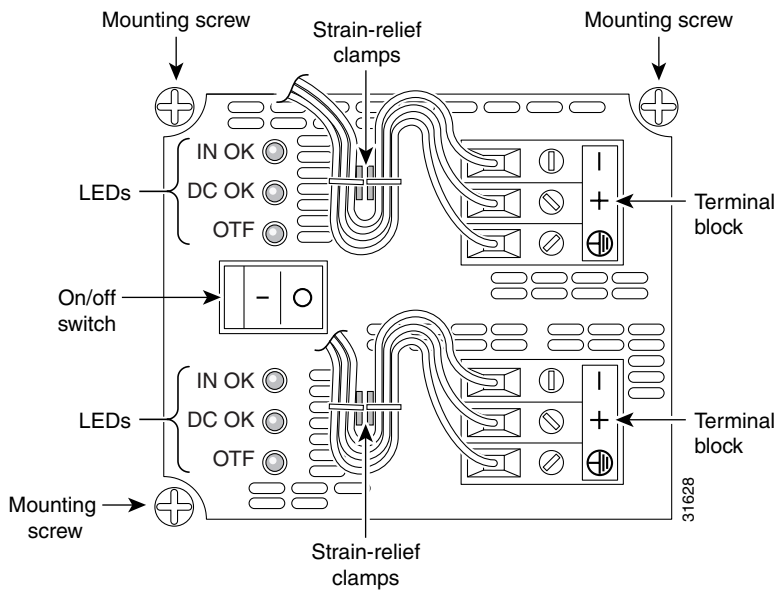
Cisco AS5350 DC Power Supply Connections—Single Power Supply



Cisco AS5350 DC Power Supply Connections—Redundant Power Supply



Cisco AS5400 DC Power Supply Connections



Step 3 Strip off a quarter of an inch (1/4 in. [0.625 cm]) of insulation on the safety ground, 48 VDC Return, and -48 VDC input wires.



Note If you are installing a redundant power supply in the Cisco AS5350, you should attach appropriate sized spade terminals to the stripped ends of the ground and input wires.

Step 4 Install the safety grounds (green wire) into the terminal block ground connectors and tighten the locking screws. Ensure that no bare wire is exposed.



Note For central office installations, we recommend using a copper 6 AWG green ground wire with one end connected to reliable earth. The other end of the wire should be crimped onto the double-hole lug provided in the installation pack. The lug should be secured to the mating holes on either side of the chassis with the two screws included in the accessory pack.

Step 5 Insert the 48 VDC Return wires into the terminal block positive connectors (+) and tighten the locking screws. Ensure that no bare wire is exposed.



Caution Do not overtorque the terminal block contact screws. The recommended torque is 5.0 in.-lb (0.56 N-m).

Step 6 Insert the -48 VDC wires into the terminal block negative connectors (-) and tighten the locking screws. Ensure that no bare wire is exposed.

Step 7 Make sure that the power supply wires are secured to cable strain-relief clamps with cable ties.



Warning **After wiring the DC power supply, remove the tape from the circuit breaker switch handle and reinstate power by moving the handle of the circuit breaker to the ON position. To see translations of the warnings that appear in the publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

Step 8 Power up the universal gateway. The internal power supply fan should power on.

5 Power Up the Universal Gateway



Note The information in this document applies to the Cisco AS5350, Cisco AS5400, and Cisco AS5400HPX universal gateways.



Note Unless specifically noted, all references to the Cisco AS5400 also apply to the Cisco AS5400HPX.

Checklist for Power Up

You are ready to power up the Cisco universal gateway if the following steps are completed:

- Chassis is securely mounted.
- Power and interface cables are connected.
- Your PC terminal emulation program is configured for 9600 baud, 8 data bits, 1 stop bit, and no parity.
- You have selected passwords for access control.
- You have determined the IP addresses for the Ethernet and serial interfaces.

Power-Up Procedure

Perform this procedure to power up your Cisco universal gateway and verify that it goes through its initialization and self-test. When this is finished, the Cisco universal gateway is ready to configure.



Note To view the boot sequence through a terminal session, you must have a console connection to the Cisco universal gateway before it powers on. To connect to the console, refer to the “Connect a Console Terminal” section on page 15.

Move the power switch to the ON position. The system board OK LED should come on and messages will begin to appear in your terminal emulation program window.



Caution *Do not press any keys on the keyboard until the messages stop.* Any keys pressed during this time are interpreted as the first command typed when the messages stop, which might cause the universal gateway to power off and start over. It takes a few minutes for the messages to stop.



Note The displayed messages depend on the Cisco IOS software release and cards installed in your system. The screen displays in this section are for reference only and might not exactly reflect the messages on your console.

The messages look similar to the following:

```
System Bootstrap, Version 12.1(2r)XD1, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
AS5350 platform with 131072 Kbytes of main memory
```

```
Self decompressing the image : ##### [OK]
Self decompressing the image : ##### [OK]
```

Restricted Rights Legend


```
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
```

```
cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
```

```
Cisco Internetwork Operating System Software
IOS (tm) 5350 Software (C5350-IS-M), Version 12.2(2)XA, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)
TAC:Home:SW:IOS:Specials for info
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Tue 26-Jun-01 23:47 by hwcheng
Image text-base: 0x600089C8, data-base: 0x61000000
```

```
cisco AS5350 (R7K) processor (revision O) with 131072K/65536K bytes of memory.
Processor board ID JAB0430086M
R7000 CPU at 250Mhz, Implementation 39, Rev 1.0, 256KB L2, 2048KB L3 Cache
Last reset from IOS reload
Bridging software.
X.25 software, Version 3.0.0.
Primary Rate ISDN software, Version 1.1.
Manufacture Cookie Info:
EEPROM Type 0x0001, EEPROM Version 0x01, Board ID 0x32,
Board Hardware Version 3.27, Item Number 800-5171-01,
Board Revision B0, Serial Number JAB0430086M,
```

PLD/ISP Version 1.0, Manufacture Date 20-Jul-2000.
Processor 0x14, MAC Address 0x0142B35F36
Backplane HW Revision 1.0, Flash Type 5V
2 FastEthernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
60 terminal line(s)
2 Channelized T1/PRI port(s)
512K bytes of non-volatile configuration memory.
32768K bytes of processor board System flash (Read/Write)
8192K bytes of processor board Boot flash (Read/Write)




Note If the `rommon 1>` prompt appears, your system has booted in ROM monitor mode. For information on the ROM monitor, see the universal gateway ROM monitor information in the *Cisco IOS Configuration Fundamentals Configuration Guide* for your Cisco IOS software release.

6 Perform Initial Configuration



Note The information in this document applies to the Cisco AS5350, Cisco AS5400, and Cisco AS5400HPX universal gateways.




Note Unless specifically noted, all references to the Cisco AS5400 also apply to the Cisco AS5400HPX.

At this point you can continue, using the setup command facility, or you can configure the universal gateway manually using the CLI.


- The following section describes the procedure for the setup command facility for the initial configuration.
- See the “Initial Configuration Using CLI (Manual Configuration)” section on page 35 for information about manual configuration using CLI.

Initial Configuration Using the Setup Command Facility

This section shows how to prepare the system to perform basic communication functions through its Ethernet and WAN interfaces.



Note The displayed messages depend on the Cisco IOS software release and cards installed in your system. The screen displays in this section are for reference only and might not exactly reflect the messages on your console.




Note If you make a mistake while using the **setup** command facility, you can exit and run the facility again. Press **Ctrl-c**, and type **setup** at the enable mode prompt (`Router#`).

Step 1 To proceed using the setup command facility, enter **yes**:

```
Would you like to enter the initial configuration dialog? [yes/no]: yes
```

At any point you may enter a question mark '?' for help.
Use **ctrl-c** to abort configuration dialog at any prompt.
Default settings are in square brackets '['].

Step 2 When the following message appears, enter **no** to configure all interfaces:



Note Note that, if you enter **yes**, your system will not be configured correctly.

Basic management setup configures only enough connectivity for management of the system. Extended setup will ask you to configure each interface on the system.

Would you like to enter basic management setup? [yes/no]: **no**

Step 3 When the following message appears, press **Return** to see the current interface summary:

First, would you like to see the current interface summary? [yes]:

Any interface listed with OK? value "NO" does not have a valid configuration

Interface	IP-Address	OK?	Method	Status	Protocol
Async1/00	unassigned	NO	unset	up	up
Async1/01	unassigned	NO	unset	up	up
.					
.					
FastEthernet0/0	unassigned	NO	unset	up	up
FastEthernet0/1	unassigned	NO	unset	up	up
Group-Async0	unassigned	NO	unset	up	up
Serial0/0	unassigned	NO	unset	up	down
Serial0/1	unassigned	NO	unset	up	down

Step 4 Enter a host name for the gateway:

Configuring global parameters:

Enter host name [Router]: **Gateway**

Step 5 Enter an enable secret password. This password is encrypted (more secure) and cannot be seen when viewing the configuration.

The enable secret is a password used to protect access to privileged EXEC and configuration modes. This password, after entered, becomes encrypted in the configuration.

Enter enable secret: **xxxxx**

Step 6 Enter an enable password that is different from the enable secret password. This password is *not* encrypted (less secure) and can be seen when viewing the configuration.

The enable password is used when you do not specify an enable secret password, with some older software versions, and some boot images.

Enter enable password: **guessme**

Step 7 Enter the virtual terminal password, which prevents unauthenticated access to the universal gateway through ports other than the console port:

The virtual terminal password is used to protect access to the router over a network interface.

Enter virtual terminal password: **guessagain**

Step 8 Respond to the following prompts as appropriate for your network:

Configure System Management [yes/no] **no**

Configure SNMP Network Management? [yes]:

Community string [public]:

Configure LAT? [yes]: **no**

Configure AppleTalk? [no]:

Configure DECnet? [no]:

Configure IP? [no]: **yes**

Configure IGRP routing? [yes]:

Your IGRP autonomous system number [1]:

Configure CLNS? [no]:

Configure IPX? [no]:

Configure Vines? [no]:

Configure XNS? [no]:

Configure Apollo? [no]:

Configure bridging? [no]:

Async lines accept incoming modems calls. If you will have users dialing in via modems, configure these lines.

```
Configure Async lines? [yes]:
Async line speed [115200]:
Will you be using the modems for inbound dialing? [yes]:
  Would you like to put all async interfaces in a group and configure
  them all at one time ? [yes]:
  Allow dial-in users to choose a static IP address? [no]:
  Configure for TCP header compression? [yes]:
  Configure for routing updates on async links? [no]:
  Enter the starting address of IP local pool? [X.X.X.X]: 10.1.2.1
  Enter the ending address of IP local pool? [X.X.X.X]: 10.1.2.59

  You can configure a test user to verify that
  your dial-up service is working properly
  Would you like to create a test user? [no]:
  Will you be using the modems for outbound dialing? [no]:
```

Step 9 Enter the letter corresponding to the ISDN switch type that matches your telco switch type, or press **Enter** to accept the default:

```
Do you want to configure ISDN switch type? [yes]:
The following ISDN switch types are available:
[a] primary-4ess
[b] primary-5ess
[c] primary-dms100
[d] primary-net5
[e] primary-ntt
[f] primary-ts014
Enter the switch type [b]:
```

Next, you will be prompted to configure controllers.
These controllers enable users to dial in via ISDN or analog modems.

Step 10 Enter **yes** to allow users to dial in via ISDN or analog modems:

```
Do you intend to allow users to dial in? [yes]:

There are 2 controllers on this access server. If you want to use
the full capacity of the access server configure all controllers.

Controller T3 0,1...etc in software corresponds to Port 0,1...etc
on the back of the access server.

PRI configuration can be configured to controllers all at once
based on your PRI controllers selection. Where as CAS configuration
will be configured individually for each controller.
```

Step 11 Enter the number of controllers you will be using for the PRI configuration or press **Enter** to configure all controllers:

```
Enter # of controllers, you will be using for PRI configuration [2]:

Configuring controller parameters:
```

Step 12 Press **Enter** for every slot, port, and channel:

```
Configuring controller t1 3/0:
  Configuring PRI on this controller.

Configuring controller t1 3/1:
  Configuring PRI on this controller.
```

Step 13 Enter **yes** to configure the FastEthernet0/0 interface to connect the gateway to a LAN, then respond to the remaining questions to configure the FastEthernet port:

```
Do you want to configure FastEthernet0/0 interface? [yes]:
  Use the 100 Base-TX (RJ-45) connector? [yes]:
```

```
Operate in full-duplex mode? [no]:
Operate at 100 Mbps speed? [yes]:
Configure IP on this interface? [yes]:
  IP address for this interface [X.X.X.X]: 172.22.50.10
  Subnet mask for this interface [255.255.0.0] : 255.255.255.128
  Class B network is 172.22.0.0, 25 subnet bits; mask is /25
```

```
Do you want to configure FastEthernet0/0 interface? [yes]: no
```

Step 14 Configure your serial interfaces by responding to the following prompts:

```
Do you want to configure Serial0/0 interface? [no]: yes
Configure IP on this interface? [no]: yes
Configure IP unnumbered on this interface? [no]:
  IP address for this interface interface: 172.22.50.11
  Subnet mask for this interface: 255.255.0.0
```

```
Do you want to configure Serial0/1 interface? [yes]: no
```

```
Configuring interface Group-Async1:
```

Step 15 After you complete the configuration script, the setup script displays the configuration command script. Review your new configuration and then make the appropriate selection below:

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
```

```
Enter your selection [2]:
```

Initial Configuration Using CLI (Manual Configuration)

This section shows how to perform basic configuration using the command line interface (CLI).

Step 1 To proceed with manual configuration using CLI, enter **no**.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

Step 2 To terminate autoinstall and continue with manual configuration, press **Return**:

```
Would you like to terminate autoinstall? [yes] Return
```

Step 3 To bring up the `Router>` prompt, press **Return**:

```
...
Router>
```

Step 4 Enter privileged EXEC mode.

```
Router> enable
Router#
```

Step 5 Enter global configuration mode. You are in global configuration mode when the prompt changes to `Router(config)#`.

```
Router# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Step 6 Changes the name of the gateway to a meaningful name:

```
Router(config)# hostname Gateway
Gateway(config)#
```

Step 7 Create a secret password. This password provides access to privileged EXEC mode. Substitute your enable secret password for **guessme**.

```
Gateway(config)# enable secret guessme
```

Step 8 Enable password encryption. When password encryption is enabled, the encrypted form of the password is displayed when a **show configuration** command is entered. You cannot recover a lost encrypted password.

```
Gateway(config)# service password-encryption
```

Step 9 Configure debugging messages to include milliseconds in the date and time stamp:

```
Gateway(config)# service timestamps debug datetime msec
```

Step 10 Configure logging messages to include milliseconds in the date and time stamp:

```
Gateway(config)# service timestamps log datetime msec
```

Step 11 Enter line configuration mode to configure the console port. You are in line configuration mode when the prompt changes to **Gateway(config-line)#**.

```
Gateway(config)# line con 0
```

Step 12 Prevent the gateway's EXEC facility from timing out if you do not type any information on the console screen for an extended period:

```
Gateway(config-line)# exec-timeout 0 0
```

Step 13 Exit line configuration mode:

```
Gateway(config-line)# exit
Gateway(config)#
```

Step 14 Return to privileged EXEC mode:

```
Gateway(config)# Ctrl-Z
Gateway#
```

Step 15 Save the configuration:

```
Gateway# write memory

Building configuration ...
[OK]
Gateway#
```

Verify

To verify that you configured the right host name and passwords:

- Enter the **show configuration** command:

```
Gateway# show configuration

Using 1888 out of 512000 bytes
!
version XX.X
.
.
!
hostname Gateway
!
enable secret 5 $1$60L4$X2JY0woDc0.kqa1lo0/w8/
.
```

- Exit privileged EXEC mode and attempt to log in using the new enable secret password. The **show privilege** command shows the current security privilege level.

```
Gateway# exit
```

```
Gateway con0 is now available
Press RETURN to get started.
Gateway> enable
Password:
Gateway# show privilege
Current privilege level is 15
Gateway#
```

Configuring Local AAA Security

Configure authentication, authorization, and accounting (AAA) to perform log in authentication by using the local username database. The **login** keyword authenticates EXEC shell users. Additionally, configure PPP authentication to use the local database if the session was not already authenticated by **login**.

AAA (called triple A) is the Cisco IOS security model used on all Cisco devices. AAA provides the primary framework through which you set up access control on the Cisco AS5350 or Cisco AS5400.

The same authentication method is used on all interfaces. AAA is set up to use the local database configured on the gateway. This local database is created with the **username** configuration commands.

Step 1 Enter global configuration mode. You are in global configuration mode when your prompt changes to Gateway(config)#.

```
Gateway# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.
Gateway(config)#

Step 2 Create a local login username database in global configuration mode. In this example, the administrator's username is *admin*. The remote client's login username is *Harry*.

```
Gateway(config)# username admin password adminpasshere
Gateway(config)# username Harry password Harrypasshere
```

Step 3 Configure local AAA security in global configuration mode. You *must* enter the **aaa new-model** command before the other two authentication commands.

```
Gateway(config)# aaa new-model
Gateway(config)# aaa authentication login default local
Gateway(config)# aaa authentication ppp default if-needed local
```

Step 4 Return to privileged EXEC mode:

```
Gateway(config)# Ctrl-Z
Gateway#
```

Step 5 Log in with your username and password:



Caution

After you have configured AAA security, all access will require a username and password. Make sure that your login name and password are working before you exit or reboot. If you are unable to get back into your universal gateway, refer to the password recovery instructions at the following URL:

http://www.cisco.com/warp/public/474/pswdrec_as5300.shtml

```
Gateway# login
```

User Access Verification

```
Username: admin
Password:
Gateway#
```



Tip To save the gateway configuration, save it to NVRAM. Refer to the “Saving Configuration Changes” section on page 57.



Note For comprehensive information about how to implement a Cisco AAA-based security environment, see the relevant documents at [Cisco Product Documentation > Network Security > Cisco IOS Technology-Specific Security Features](#).

Configure Basic Dial Access

To commission a basic dial access service perform the following tasks:

- Create two loopback interfaces.
- Bring up the Fast Ethernet interface.
- Add an IP route to the default gateway.

Step 1 Enter global configuration mode. You are in global configuration mode when your prompt changes to Gateway(config)#.

```
Gateway# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Gateway(config)#
```

Step 2 Assign the IP addresses as in the following example, and create an IP route to the default gateway:

```
Gateway(config)# interface loopback 0  
Gateway(config-if)# ip address 172.22.99.1 255.255.255.255  
Gateway(config-if)# exit  
Gateway(config)# interface loopback 1  
Gateway(config-if)# ip address 172.22.90.1 255.255.255.0  
Gateway(config-if)# exit  
Gateway(config)# interface FastEthernet 0/0  
Gateway(config-if)# ip address 172.28.186.55 255.255.255.240  
Gateway(config-if)# no shutdown  
Gateway(config-if)# exit  
Gateway(config)# ip route 0.0.0.0 0.0.0.0 172.28.186.49
```

In this example:

- Interface loopback 0—Identifies with a unique and stable IP address. One unique IP address from a common block of addresses is assigned to each device in the IP network. This technique makes security-filtering easy for the Network Operations Center (NOC). One class C subnet used for device identification can support 254 distinct devices with unique loopback addresses.
- Interface loopback 1—Hosts a pool of IP addresses for the remote nodes. In this way, one route, instead of 254 routes, is summarized and propagated to the backbone. Pick the IP address for loopback 1 from the range of addresses that you will assign to the local address pool.

Step 3 Return to privileged EXEC mode:

```
Gateway(config)# Ctrl-Z
```

```
Gateway#
```

Step 4 Verify that the Fast Ethernet interface is up. Ping the default gateway to verify this.

```
Gateway# ping 172.28.186.49
```

Type escape sequence to abort.

```
Sending 5, 100-byte ICMP Echos to 172.28.186.49, timeout is 2 seconds:
```

```
.!!!!
```

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/4 ms
```



Tip To save the gateway configuration, save it to NVRAM. Refer to the “Saving Configuration Changes” section on page 57



Note An 80 percent ping-success rate is normal for the first time you ping an external device. The universal gateway does not have an Address Resolution Protocol (ARP) entry for the external device. A 100 percent success rate is achieved the next time you ping the device.

Configuring the Asynchronous Group Interface

This section shows how to configure asynchronous interfaces. Asynchronous group interfaces allow administrators to easily configure a large number of asynchronous interfaces by allowing them to clone from one managed copy. This can also reduce the number of lines in the configuration, because each individual asynchronous interface configuration can be replaced by at least one group-async. To assign the asynchronous interfaces to a group-async interface, first determine the number of asynchronous lines that need to be aggregated. This can be determined from the running configuration.

Step 1 Enter the **enable** command and password to go to privileged EXEC mode. You are in privileged EXEC mode when the prompt changes to `Gateway#`.

```
Gateway> enable
```

```
Password: password
```

```
Gateway#
```

Step 2 Enter global configuration mode. You are in global configuration mode when the prompt changes to `Gateway(config)#`.

```
Gateway# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Gateway(config)#
```

Step 3 Place all asynchronous interfaces in a single group, so that you configure the same parameters quickly on all interfaces at one time:

```
Gateway(config)# interface group-async 1
```

```
Gateway(config-if)#
```

Step 4 Define the slot/port group range of the interface. The range that you specify depends on the number of asynchronous interfaces you have on your gateway. If your gateway has 108 asynchronous interfaces, you can specify **group-range 1/1 1/107**.

```
Gateway(config-if)# group-range slot/port slot/port
```

```
Building configuration...
```

```
Gateway(config-if)#
```

Step 5 Return to privileged EXEC mode:

```
Gateway(config-if)# Ctrl-Z
Gateway#
```



Tip To save the gateway configuration, save it to NVRAM. Refer to the “Saving Configuration Changes” section on page 57.

Verify

- To verify your group interface configuration, enter the **show interface async** command in privileged EXEC mode:

```
Gateway# show interface async 4/0

Async4/00 is down, line protocol is down
modem(slot/port)=4/0, state=IDLE
dsxl(slot/unit/channel)=NONE, status=VDEV_STATUS_UNLOCKED
Hardware is Async Serial
MTU 1500 bytes, BW 115 Kbit, DLY 100000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation SLIP, loopback not set
DTR is pulsed for 5 seconds on reset
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/10/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
    Conversations 0/1/32 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
    Available Bandwidth 86 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
```

If you are having trouble:

- To check for errors and local and remote addresses, enter the **show async status** command in privileged EXEC mode:

```
Gateway# show async status

Async protocol statistics:

Int    Local          Remote    Qd      InPack  OutPac  Inerr   Drops   MTU
1/00   42.1.1.1       None      0       0       0       0       0       1500
1/01   192.168.10.100 None      0       0       0       0       0       1500
1/02   192.168.10.100 None      0       0       0       0       0       1500
1/03   192.168.10.100 None      0       0       0       0       0       1500
1/04   192.168.10.100 None      0       0       0       0       0       1500
1/05   192.168.10.100 None      0       0       0       0       0       1500
.
Rcvd: 25762 packets, 1052214 bytes
    0 format errors, 891 checksum errors, 0 overrun
Sent: 8891 packets, 222264 bytes, 0 dropped
```


Configuring a Channelized T1 or E1 DFC

This section shows how to configure channelized T1 or E1. On a Cisco AS5350 or Cisco AS5400, you can allocate the available channels for channelized E1 and T1 in the following ways:

- All channels can be configured to support ISDN PRI.
- If you are not running ISDN PRI, all channels can be configured to support robbed-bit signaling (also known as channel-associated signaling).
- All channels can be configured in a single channel group.
- Mix and match channels supporting ISDN PRI, channel grouping, and channel-associated signaling (CAS).
- Mix and match channels supporting ISDN PRI, channel grouping, and robbed-bit signaling across the same T1 line. For example, on the same channelized T1 you can configure the **pri-group timeslots 1-10,24** command, **channel-group 11 timeslots 11-16** command, and **ds0-group 17 timeslots 17-23 type e&m-fgb** command. This is an unusual configuration because it requires you to align the correct range of time slots on both ends of the connection.



Note For configuration information about leased-line or nondial use, see the *Configuration Fundamentals Configuration Guide*, available online. You can access this document at [Cisco Product Documentation > Cisco IOS Software > Cisco IOS Software Release you are using > Configuration Guides and Command References > Configuration guide for your application](#).



Note The CT1/E1 controller numbering convention is *dfc-slot/port* in CLI commands. DFC slot numbering starts from the motherboard and works up from left to right. Slot 0 is reserved for the motherboard. The CT1/E1 DFC slots are numbered sequentially from 1 to 7. Port numbering is from 0 to 7.

Step 1 Use the **enable** command and password to enter privileged EXEC mode. You are in privileged EXEC mode when the prompt changes to Gateway#.

```
Gateway> enable
Password: password
Gateway#
```

Step 2 Enter global configuration mode. You are in global configuration mode when the prompt changes to Gateway(config)#.

```
Gateway# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(config)#
```

Step 3 Enter controller configuration mode to configure your controller slot and port. Slot values range from 1 to 7. Port values range from 0 to 7 for T1 and E1.

```
Gateway(config)# controller [t1 | e1] slot/port
Gateway(config-controller)#
```

Step 4 Enter your telco's framing type for the CT1 controller, either **esf** or **sf**:

```
Gateway(config-controller)# framing esf
or
```

Enter the framing type for the CE1 controller:

```
Gateway(config-controller)# framing crc4
```

Step 5 Define the line code as binary 8 zero substitution (B8ZS) for the CT1 controller:

```
Gateway(config-controller)# linecode b8zs
or
```

Define the line code as high-density bipolar 3 (HDB3) for the CE1 controller:

```
Gateway(config-controller)# linecode hdb3
```

Step 6 Return to privileged EXEC mode:

```
Gateway(config-controller)# Ctrl-Z
Gateway#
```



Tip To save the gateway configuration, save it to NVRAM. Refer to the “Saving Configuration Changes” section on page 57.

Verify

To verify that your controller is up and running and that no alarms have been reported:

- Enter the **show controller** command and specify the controller type, slot, and port numbers:

```
Gateway# show controller t1 1/7
```

```
T1 1/7 is up.
No alarms detected.
Framing is ESF, Line Code is B8ZS, Clock Source is Line Primary.
Version info of slot 2: HW: 2, Firmware: 14, NEAT PLD: 13, NR Bus PLD: 19
Data in current interval (476 seconds elapsed):
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Total Data (last 24 hours)
  0 Line Code Violations, 0 Path Code Violations,
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

- Note the following:
 - The controller must report being up.
 - No errors should be reported.

If you are having trouble:

- First decide if the problem is because of the T1 or E1 line or with a particular channel group. If the problem is with a single channel group, you have a potential interface problem. If the problem is with the T1 or E1 line, or with all channel groups, you have a potential controller problem.
- To troubleshoot your E1 or T1 controllers, first check that the configuration is correct. The framing type and line code should match to what the service provider has specified. Then check channel group and PRI-group configurations, especially to verify that the time slots and speeds are what the service provider has specified. At this point, the **show controller t1** or **show controller e1** commands should be used to check for T1 or E1 errors. Use the command several times to determine if error counters are increasing, or if the line status is continually changing. If this is occurring, you need to work with the service provider.
- Another common reason for failure is the **dial-tdm-clock priority** setting. The default setting is a free-running clock that causes clock slip problems if not set properly.

Configuring a Channelized T3 DFC

Your CT3 card offers 28 individual T1 channels (bundled in the T3) for serial transmission of voice and data. The CT3 link supports the maintenance data link channel in C-bit parity mode and also payload and network loopbacks. The T1s multiplexed in the CT3 link support facilities data link (FDL) in extended super frame (ESF) framing.



Note The CT3 controller numbering convention is *dfc-slot/port* in CLI commands. DFC slot numbering starts from the motherboard and works up from left to right. Slot 0 is reserved for the motherboard. The DFC slots are numbered sequentially from 1 to 7. Port number value is always 0. Under the CT3, the CT1 controller numbering convention is *dfc-slot/port:channel* in CLI commands. Port numbering values range from 1 to 28.

Step 1 Use the **enable** command and password to enter privileged EXEC mode. You are in privileged EXEC mode when the prompt changes to Gateway#.

```
Gateway> enable
Password: password
Gateway#
```

Step 2 Enter global configuration mode. You are in global configuration mode when the prompt changes to Gateway(config)#.

```
Gateway# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(config)#
```

Step 3 Enter controller configuration mode to configure your T3 controller for slot 1 port 0. Slot values range from 1 to 7. Port number is always 0.

```
Gateway(config)# controller t3 1/0
Gateway(config-controller)#
```

Step 4 Enter your telco's framing type, either **c-bit** or **m23**:

```
Gateway(config-controller)# framing c-bit
```

Step 5 Enter your clock source, either **internal** or **line**:

```
Gateway(config-controller)# clock source line
```

Step 6 Enter your cable length. Values range from 0 to 450 feet.

```
Gateway(config-controller)# cablelength 450
```

Step 7 Configure your T1 controllers. Range is 1 to 28. In this instance, all 28 T1s are configured at once.

```
Gateway(config-controller)# t1 1-28 controller
```

or

Omit specified T1 controllers while configuring others. In this instance, T1 controllers 11-14, 21, 22, and 24-28 are not configured.

```
Gateway(config-controller)# t1 1-10,15-20,23 controller
```

Step 8 Return to privileged EXEC mode:

```
Gateway(config-controller)# Ctrl-Z
Gateway#
```



Tip To save the gateway configuration, save it to NVRAM. Refer to the "Saving Configuration Changes" section on page 57.

Verify

To verify that your controller is up and running and that no alarms have been reported:

- Enter the **show controller** command and specify the controller type, slot, and port numbers:

```
Gateway# show controller t3 1/0
```

```
T3 1/0 is up.
  Applique type is Channelized T3
  No alarms detected.
  MDL transmission is disabled
```

```
FEAC code received:No code is being received
Framing is C-BIT Parity, Line Code is B3ZS, Clock Source is Internal
Data in current interval (270 seconds elapsed):
```

```
0 Line Code Violations, 0 P-bit Coding Violation
0 C-bit Coding Violation, 0 P-bit Err Secs
0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
0 Unavailable Secs, 0 Line Errored Secs
0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
Total Data (last 32 15 minute intervals):
0 Line Code Violations, 0 P-bit Coding Violation,
0 C-bit Coding Violation, 0 P-bit Err Secs,
0 P-bit Severely Err Secs, 0 Severely Err Framing Secs,
0 Unavailable Secs, 0 Line Errored Secs,
0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
```

Configuring ISDN PRI

Channelized T1 ISDN PRI offers 23 B channels and 1 D channel. Channelized E1 ISDN PRI offers 30 B channels and 1 D channel. Channel 24 is the D channel for T1, and channel 16 is the D channel for E1. ISDN provides out-of-band signaling using the D channel for signaling and the B channels for user data.

For a complete description of the commands mentioned in this chapter, refer to the *Dial Solutions Command Reference*.

You can access this document at [Cisco Product Documentation > Cisco IOS Software > Cisco IOS Software Release you are using > Configuration Guides and Command References > Command reference for your application](#).

Request PRI Line and Switch Configuration from a Telco Service Provider

Before configuring ISDN PRI on your Cisco universal gateway, you must order a correctly provisioned ISDN PRI line from your telecommunications service provider.

This process varies from provider to provider on a national and international basis. However, some general guidelines follow:

- Determine if the outgoing B channel calls are made in ascending or descending order. The Cisco IOS software default is descending order; however, if the switch from the service provider is configured for outgoing calls made in ascending order, the universal gateway can be configured to match the switch configuration of the service provider.
- Ask for delivery of calling line identification. Providers sometimes call this CLI or automatic number identification (ANI).
- If the gateway will be attached to an ISDN bus (to which other ISDN devices might be attached), ask for point-to-multipoint service (subaddressing is required) and a voice-and-data line.

Configure ISDN PRI by executing the following steps:

Step 1 Use the **enable** command and password to enter privileged EXEC mode. You are in privileged EXEC mode when the prompt changes to Gateway#.

```
Gateway> enable
Password: password
Gateway#
```

Step 2 Enter global configuration mode. You are in global configuration mode when the prompt changes to Gateway(config)#.

```
Gateway# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Gateway(config)#
```

Step 3 Select a service provider switch type that matches your service provider switch:

```
Gateway(config)# isdn switch-type switch-type
```

ISDN Switch Types

Area	Keyword	Switch Type
Australia	primary-ts014	Australia PRI switches
Europe	primary-net5	European, New Zealand, and Asia ISDN PRI switches (covers the Euro-ISDN E-DSS1 signaling system and is European Telecommunication Standards Institute or ETSI-compliant)
Japan	primary-ntt	Japanese ISDN PRI switches
None	none	No switch defined
North America	primary-4ess	AT&T 4ESS switch type for the United States
	primary-5ess	AT&T 5ESS switch type for the United States
	primary-dms100	NT DMS-100 switch type for the United States
	primary-ni	National ISDN switch type

Step 4 Specify the T1 controller you want to configure.



Note The CT1/E1 controller numbering convention is *dfc-slot/port* in CLI commands. DFC slot numbering starts from the motherboard and works up from left to right. Slot 0 is reserved for the motherboard. The DFC slots are numbered sequentially from 1 to 3 for the Cisco AS5350 and 1 to 7 for the Cisco AS5400. Port numbering is from 0 to 7, depending on the trunk DFC installed.

The CT3 controller numbering convention is *dfc-slot/port* in CLI commands. DFC slot numbering starts from the motherboard and works up from left to right. Slot 0 is reserved for the motherboard. The DFC slots are numbered sequentially from 1 to 3 for the Cisco AS5350 and 1 to 7 for the Cisco AS5400. Port number value is always 0. Under the CT3, the CT1 controller numbering convention is *dfc-slot/port:channel* in CLI commands. Channel values range from 1 to 28. For illustrations showing the slot locations, see the “Slot Numbering” section on page 59

```
Gateway(config)# controller t1 1/0
```

or

```
Gateway(config)# controller t3 7/0:16
```

or

Specify the E1 controller you want to configure.

```
Gateway(config)# controller e1 1/0
```



Note When you configure the CT1 or CE1 controller, a corresponding D-channel serial interface is created automatically.

Step 5 Specify the PRI channels:

```
Gateway(config-controller)# pri-group [timeslots range]
```



Note For CT1 ISDN PRI—If you do not specify the time slots, the specified controller is configured for 23 B channels and 1 D channel. B channel numbers range from 1 to 23; channel 24 is the D channel for T1. Corresponding serial interface numbers range from 0 to 23. In commands, the D channel is `interface serial slot/port:23`—for example, `interface serial 1/0:23`.



Note For CE1 ISDN PRI—If you do not specify the time slots, the specified controller is configured for 30 B channels and 1 D channel. B channel numbers range 1 to 31; channel 16 is the D channel for E1. Corresponding serial interface numbers range 0 to 30. In commands, the D channel is **interface serial slot/port:15**—for example, **interface serial 1/0:15**.

Step 6 Return to privileged EXEC mode:

```
Gateway(config-controller)# Ctrl-Z
Gateway#
```



Tip To save the gateway configuration, save it to NVRAM. Refer to the “Saving Configuration Changes” section on page 57.

Verify

To verify that you have configured the interfaces correctly:

- Enter the **show controller t3** command and specify the slot and port numbers. Verify that the controller is up and that you do not have excessive errors; otherwise, your controller might go down frequently. This could indicate switch problems.

```
Gateway# show controller t3 1/0

T3 1/0 is up.
  Applique type is Channelized T3
  No alarms detected.
  MDL transmission is disabled
  FEAC code received:No code is being received
  Framing is C-BIT Parity, Line Code is B3ZS, Clock Source is Internal
  Data in current interval (270 seconds elapsed):
    0 Line Code Violations, 0 P-bit Coding Violation
    0 C-bit Coding Violation, 0 P-bit Err Secs
    0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
    0 Unavailable Secs, 0 Line Errored Secs
    0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
  Total Data (last 32 15 minute intervals):
    0 Line Code Violations, 0 P-bit Coding Violation,
    0 C-bit Coding Violation, 0 P-bit Err Secs,
    0 P-bit Severely Err Secs, 0 Severely Err Framing Secs,
    0 Unavailable Secs, 0 Line Errored Secs,
    0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
```

- Enter the **show controller t1** command and specify the slot and port numbers:

```
Gateway# show controller t1 1/0

T1 1/0 is up.
  Applique type is Channelized T1
  Cablelength is long gain36 0db
  No alarms detected.
  alarm-trigger is not set
  Version info of slot 1: HW:768, PLD Rev:4
  Framers Version:0x8

Manufacture Cookie Info:
  EEPROM Type 0x0001, EEPROM Version 0x01, Board ID 0x041,
  Board Hardware Version 3.0, Item Number 73-4089-03,
  Board Revision 05, Serial Number JAB99432626,
  PLD/ISP Version 0.1, Manufacture Date 11-Nov-1999.
```

```

Framing is ESF, Line Code is B8ZS, Clock Source is Line.
Data in current interval (264 seconds elapsed):
  3 Line Code Violations, 1 Path Code Violations
  5 Slip Secs, 0 Fr Loss Secs, 1 Line Err Secs, 1 Degraded Mins
  5 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs

```

- Enter the **show isdn status** command to view layer status information:

```

Gateway# show isdn status

Global ISDN Switchtype = primary-5ess
ISDN Serial1/0:1:23 interface
  dsl 0, interface ISDN Switchtype = primary-5ess
  Layer 1 Status:
    ACTIVE
  Layer 2 Status:
    TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
  Layer 3 Status:
    0 Active Layer 3 Call(s)
  Activated dsl 0 CCBS = 0
  The Free Channel Mask: 0x807FFFFF

```

- Monitor ISDN channels and service by entering the **show isdn service** command:

```

Gateway# show isdn service

PRI Channel Statistics:
ISDN Se3/0:23, Channel [1-24]
  Configured Isdn Interface (dsl) 0
  Channel State (0=Idle 1=Proposed 2=Busy 3=Reserved 4=Restart 5=Maint_Pend)
  Channel : 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4
  State   : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 3
  Service State (0=Inservice 1=Maint 2=Outofservice)
  Channel : 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4
  State   : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 2
.
.

```



Note Your Cisco AS5350 or Cisco AS5400 supports a total of 248 ISDN channels per ingress DFC. If you are configuring individual T1 channels of your CT3 for backup links or serial backhaul connections, the CT1s must be configured into channel-groups—each channel-group using 24 time slots or channels. For example, to configure 6 CT1s (6x24), 144 ISDN channels are in use, leaving a remainder of 104 (248–144) channels for ISDN use.

In the following **show running-config** example, five CT1s are configured into channel-groups:

```

Gateway# show running-config

Building configuration...

Current configuration:
!
! Last configuration change at 15:49:30 UTC Mon Apr 3 2000 by admin
! NVRAM config last updated at 01:35:05 UTC Fri Mar 17 2000 by admin
!
version 12.0
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
---text omitted---
!
controller T3 1/0
  framing m23
  clock source line
  t1 1-28 controller
!

```

```

controller T1 1/0:11
  framing esf
  channel-group 20 timeslots 1-24 speed 64
!
controller T1 1/0:12
  framing esf
  channel-group 20 timeslots 1-24 speed 64
!
controller T1 1/0:13
  framing esf
  channel-group 20 timeslots 1-24 speed 64
!
controller T1 1/0:14
  framing esf
  channel-group 20 timeslots 1-24 speed 64
!
controller T1 1/0:15
  framing esf
  channel-group 20 timeslots 1-24 speed 64

```

If you are having trouble:

- If the Layer 1 Status is “Deactivated,” make sure that the cable connection is not loose or disconnected. This status message indicates a problem at the physical layer.
- There may be a problem with your telco, or the framing and line code types you entered may not match your telco’s. A Layer 2 error indicates that the universal gateway cannot communicate with the telco. There is a problem at the data link layer.

Configuring the D Channels for ISDN Signaling

The ISDN D channels carry the control and signaling information for your ISDN calls—for both circuit-switched data calls, and analog modem calls.

The D channel notifies the central office switch to send the incoming call to particular time slots on the Cisco universal gateway. Each one of the B channels carries data or voice. The D channel carries signaling for the B channels. The D channel identifies if the call is a circuit-switched digital call or an analog modem call. Analog modem calls are decoded and then sent off to the onboard modems. Circuit-switched digital calls are directly relayed to the ISDN processor in the gateway.

When you configured your ISDN PRI on the CT1 or CE1 controller, you automatically created a serial interface that corresponds to the PRI group time slots. This interface is a logical entity that is associated with the specific controller. After the serial interface is created, you must configure the D channel serial interface that carries signaling. The configuration applies to all the PRI B channels (time slots) for that PRI group.

The following table shows the logical contents of a ISDN PRI interface used in a T1 network configuration. The logical contents includes 23 B channels, one D channel, 24 time slots, and 24 virtual serial interfaces (total number of Bs + D).

Relationship of ISDN PRI Components for T1

Channel type	Time slot number	Virtual serial interface number
B (data channel)	1	S0:0
B (data channel)	2	S0:1
B (data channel)	3	S0:2
B (data channel)	4	S0:3
•	•	•
•	•	•
•	•	•
•	•	•
•	•	•
B (data channel)	21	S0:20
B (data channel)	22	S0:21
B (data channel)	23	S0:22
Ⓚ (signaling channel)	24	S0:23

35765

Logical contents of a PRI interface



Note When you configure your CT1 controller for an Non-Facility Associated Signaling (NFAS) backup D channel, a serial interface is automatically created only when your primary D channel fails.

To configure ISDN signaling, follow these steps:

Step 1 Enter the **enable** command and password to go to privileged EXEC mode. You are in privileged EXEC mode when the prompt changes to `Gateway#`.

```
Gateway> enable
Password: password
Gateway#
```

Step 2 Enter global configuration mode. You are in global configuration mode when the prompt changes to `Gateway(config)#`.

```
Gateway# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(config)#
```

Step 3 Enter serial interface configuration mode. After configuring the CT1 controller, a corresponding D-channel serial interface is automatically created. For example, serial interface `1/0:23` is the D channel for CT1 controller 1. You must configure each serial interface to receive incoming signaling and send outgoing signaling.



Note On a CE1 PRI line, the serial interface for the D channel is `1/0:15`.

```
Gateway(config)# interface serial 1/0:23
Gateway(config-if)#
```

Step 4 Assign an IP address and subnet mask to the interface:

```
Gateway(config-if)# ip address 172.16.254.254 255.255.255.0
```

Step 5 Configure all incoming voice calls.



Note This command has two possible keywords: **data** and **modem**. You must use the **modem** keyword to enable both modem and voice calls. The **modem** keyword represents bearer capabilities of speech.

```
Gateway(config-if)# isdn incoming-voice modem
```

Step 6 Return to privileged EXEC mode:

```
Gateway(config-if)# ctrl-z  
Gateway#
```



Tip To save the gateway configuration, save it to NVRAM. Refer to the “Saving Configuration Changes” section on page 57.

Verify

To verify your D channel configuration:

- Enter the **show interface serial** command and make sure that the line protocol is up and that you are using the correct IP interface. Also, make sure that excessive errors are not being reported.

```
Gateway# show interface serial 1/0:23
```

```
Serial1/0:23 is up, line protocol is up (spoofing)  
Hardware is DSX1  
Internet address is 172.16.254.254/16  
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Encapsulation PPP, loopback not set  
Last input 00:00:03, output never, output hang never  
Last clearing of "show interface" counters 00:00:01  
Queueing strategy:fifo  
Output queue 0/40, 0 drops; input queue 0/75, 0 drops  
1 minute input rate 0 bits/sec, 0 packets/sec  
1 minute output rate 0 bits/sec, 0 packets/sec  
0 packets input, 0 bytes, 0 no buffer  
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort  
0 packets output, 0 bytes, 0 underruns  
0 output errors, 0 collisions, 0 interface resets  
0 output buffer failures, 0 output buffers swapped out  
0 carrier transitions  
Timeslot(s) Used:24, Transmitter delay is 0 flags
```

Configuring the Universal Port Dial Feature Card and Lines

Rather than the more traditional line/modem one-to-one correspondence, lines are mapped to a service process element (SPE) that resides on the universal port DFC. Associated SPE firmware serves a function similar to modem code on a MICA modem. One SPE provides services for six ports, with additional ports per SPE. Busyout and shutdown can be configured at the SPE or port level.

The universal port DFC performs the following functions:

- Converts pulse code modulation (PCM) bitstreams to digital packet data.
- Forwards converted and packetized data to the main processor, which examines the data and forwards it to the backhaul egress interface.
- Supports all modem standards (such as V.34 and V.42bis) and features, including dial-in and dial-out.



Note For detailed information about the universal port DFC CLI commands, refer to *Monitoring Voice and Fax Services on the Cisco AS5350 and Cisco AS5400 Universal Gateway*, available online at the following URL:

```
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121x/121xm/121xm\_5/ftupspe.htm
```

SPE Firmware

SPE firmware is automatically downloaded to a universal port DFC from the Cisco AS5350 or Cisco AS5400 when you boot the system for the first time or when you insert a universal port DFC while the system is operating. When you insert DFCs while the system is operating, the Cisco IOS image recognizes the cards and downloads the required firmware to the cards.

The SPE firmware image is bundled with the universal gateway Cisco IOS image. The SPE firmware image uses an *auto detect* mechanism, which enables the universal port DFC to service multiple call types. An SPE detects the call type and automatically configures itself for that operation. The firmware is upgradable independent of Cisco IOS upgrades, and different firmware versions can be configured to run on SPEs in the same DFC.

The universal port DFC supports the modem standards and features listed in the following table.

Modem Standards and Supported Features

Feature	Description
Carrier protocols	ITU V.23 at 75/1200 bps Telcordia Technologies (formerly Bellcore) 103 at 300 bps ITU V.21 at 300 bps ITU V.22 at 1200 bps Telcordia Technologies (formerly Bellcore) 212A at 1200 bps ITU V.22bis at 2400 bps ITU V.32 up to 9600 bps ITU V.32bis up to 14,400 bps V.32 turbo up to 19,200 bps V.FC up to 28,800 bps V.34 up to 28,800 bps V.34+ up to 33.6 bps TIA/ITU V.90 K56flex
Error-correcting link-access protocols	V.42 LAPM, MNP 2-4
Compression protocols	V.42bis (includes MNP 5)
Command interface	Superset of the AT command set
In-band signaling/tone generation and detection	DTMF generation DTMF detection MF generation MF detection
Other	Out-of-band access for management PPP and SLIP framing



Note The modem speed 115200 bps and hardware flow control are the default settings for integrated modems.

To configure the lines and ports to allow users to dial in to your network, follow these steps:

Step 1 Use the **enable** command and password to enter privileged EXEC mode. You are in privileged EXEC mode when the prompt changes to Gateway#.

```
Gateway> enable
Password: password
Gateway#
```

Step 2 Enter global configuration mode. You are in global configuration mode when the prompt changes to `Gateway(config)#`.

```
Gateway# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Gateway(config)#
```

Step 3 Specify the country to set the DFC parameters (including country code and encoding). This setting is applied at the system level. All DFCs use the same country code. The default is `usa` if the gateway is configured with T1 interfaces and `e1-default` if the gateway is configured with E1 interfaces. Use the `no` form of this command to set the country code to the default of domestic.



Note All sessions on all DFCs in all slots must be idle for this command to run.

```
Gateway(config)# spe country country name
```

Step 4 Enter the numbers of the ports to configure. If you want to configure 108 ports on slot 3, enter `line 3/00 3/107`. If you want to configure 324 ports on slots 3-5, enter `line 3/00 5/107`.

```
Gateway(config)# line slot/port slot/port
```

```
Gateway(config-line)#
```

Step 5 Allow all protocols to be used when connecting to the line:

```
Gateway(config-line)# transport input all
```

Step 6 Enable remote IP users running a PPP application to dial in, bypass the EXEC facility, and connect directly to the network:

```
Gateway(config-line)# autoselect ppp
```

Step 7 Enable incoming and outgoing calls:

```
Gateway(config-line)# modem inout
```

Step 8 Return to privileged EXEC mode:

```
Gateway(config-line)# Ctrl-Z
```

```
Gateway#
```



Tip To save the gateway configuration, save it to NVRAM. Refer to the “Saving Configuration Changes” section on page 57.

Verify

To verify your SPE configuration:

- To display a summary for all the lines, enter the `show spe` command:

```
Gateway# show spe
```

```
SPE settings:
=====
Country code configuration: default T1 (u Law)
Polling interval: 8 secs.
History log events: 50(per port)
Port legends:
=====
Port state: (s)shutdown (t)test (r)recovery (d)download
            (b)busiedout (p)busyout pending, (B)bad (a)active call
Call type: (m)modem (d)digital (f)fax-relay (v)voice (_)not in use
System resources summary:
=====
```

Total ports: 108, in use ports: 0, disabled ports: 0, free ports: 108
 Total active calls: modem 0, voice 0, digital 0, fax-relay 0

SPE#	Port #	SPE State	SPE Busyout	SPE Shut	SPE Crash	Port State	Call Type
4/00	0000-0005	ACTIVE	0	0	0	_____	_____
4/01	0006-0011	ACTIVE	0	0	0	_____	_____
4/02	0012-0017	ACTIVE	0	0	0	_____	_____
4/03	0018-0023	ACTIVE	0	0	0	_____	_____
4/04	0024-0029	ACTIVE	0	0	0	_____	_____

- To display a summary for a single line, enter the **show line number** command:

Gateway# **show line 1**

```
Tty Typ Tx/Rx A Modem Roty AccO AccI Uses Noise Overruns Int
1 AUX 9600/9600 - - - - - 0 0 0/0 -
Ready
```

```
Line 1, Location: "", Type: ""
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 9600/9600, no parity, 2 stopbits, 8 databits
Status: Ready
Capabilities: none
Modem state: Ready
Group codes: 0
Modem hardware state: noCTS noDSR DTR RTS
TTY NUMBER 1
Parity Error = 0 Framing Error = 0 Receive Error = 0 Overrun = 0
Outcount = 0 totalout = 39 incount = 0 totalin = 0
```

```
Special Chars: Escape Hold Stop Start Disconnect Activation
                ^^x none - - none
Timeouts:      Idle EXEC Idle Session Modem Answer Session Dispatch
                00:10:00 never none none not set
                Idle Session Disconnect Warning
                never
                Login-sequence User Response
```



Tip If you are having trouble, make sure that you turned on the protocols for connecting to the lines (**transport input all**) and configured for incoming and outgoing calls (**modem inout**).

Configure Clocking

The time-division multiplexing (TDM) bus on the Cisco AS5350 and Cisco AS5400 backplane can receive an input clock from one of four basic sources on the universal gateway:

- A CT1/CE1 card
- A CT3 card
- An external T1/E1 clock source feed directly through the building integrated timing supply (BITS) interface port on the motherboard



Note Building integrated timing supply (BITS) is a single building master timing supply. BITS generally supplies DS1- and DS0-level timing throughout an office. In North America, BITS are the clocks that provide and distribute timing to a wireline network's lower levels.

- Free-running clock provides clock from an oscillator

Dial Feature Card Ports

The TDM bus can be synchronized with any DFC cards. On the CT1/CE1 DFCs, each port receives the clock from the T1/E1 line. The CT3 DFC uses an M13 multiplexer to receive the DS1 clock. Each port on each DFC trunk slot has a default clock priority. Also, clock priority is configurable through the `dial-tdm-clock priority` CLI command.

External Clock

The TDM bus can be synchronized with an external clock source that can be used as an additional network reference. If no clocks are configured, the system uses a primary clock through a software-controlled default algorithm. If you want the external T1/E1 clock (via the BITS interface) as the primary clock source, you must configure it using the `dial-tdm-clock priority` CLI command; the external clock is never selected by default.

The BITS interface requires a T1 line composite clock reference set at 1.544 MHz and an E1 line composite clock reference set at 2.048 MHz.

Free-Running Clock

If there is no good clocking source from a DFC card or an external clock source, then select the free-running clock from the local oscillator using the `dial-tdm-clock priority` CLI command.

To configure the clock source and clock source priority used by the TDM bus, follow these steps:

Step 1 Use the `enable` command and password to enter privileged EXEC mode. You are in privileged EXEC mode when the prompt changes to `Gateway#`.

```
Gateway> enable
Password: password
Gateway#
```

Step 2 Enter global configuration mode. You are in global configuration mode when the prompt changes to `Gateway(config)#`.

```
Gateway# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.
Gateway(config)#

Step 3 Perform Step a or Step b, depending on your configuration:

- a. Step a configures the CT1/CE DFC clock priority, trunk slot, and port that is providing the clocking source. Priority range is defined as a value from 1 to 99. DFC slot is defined as a value from 1 to 7. DS1 port number controller is defined as a value from 0 to 7.



Note DS1 port specifies T1 port.

```
Gateway(config)# dial-tdm-clock priority priority# {external | freerun | slot/ds1 port}
```

- b. Step b configures the CT3 DFC clock priority, trunk slot, and port that is providing the clocking source. Priority range is defined as a value from 1 to 99.
DFC slot is defined as a value from 1 to 7. DS3 port specifies the T3 port. DS1 port number controller is defined as a value between 1 and 28.

```
Gateway(config)# dial-tdm-clock priority priority# {external | freerun | slot/ds3 port:ds1 port}
```

Step 4 Return to privileged EXEC mode:

```
Gateway(config)# Ctrl-Z
Gateway#
```



Tip To save the gateway configuration, save it to NVRAM. Refer to the “Saving Configuration Changes” section on page 57.

Clocking Configuration Examples

In the following example, a BITS clock is set at priority 1:

```
Gateway(config)# dial-tdm-clock priority 1 external
Gateway(config)# exit
Gateway#
```

In the following example, a trunk clock from an 8 PRI CT1 DFC is set at priority 2 and uses slot 4 and ds1 port (controller) 6:

```
Gateway(config)# dial-tdm-clock priority 2 4/6
Gateway(config)# exit
```

In the following example, a trunk clock from a CT3 DFC is set at priority 2 and uses slot 1, ds3 port 0, and ds1 port 19:

```
Gateway(config)# dial-tdm-clock priority 2 1/0:19
Gateway(config)# exit
```

In the following example, free-running clock is set at priority 3:

```
Gateway(config)# dial-tdm-clock priority 3 free
Gateway(config)# exit
```

Verify

You can verify the system primary and backup clocks, the status of all trunk DFC controller clocks, and information about and the history of the last 20 TDM clock changes and the events that caused them.

- Verify your default system clocks and clock history by using the **show tdm clocks** command (this example is for T1/E1):

```
Gateway# show tdm clocks

Primary Clock:
-----
TDM Bus Master Clock Generator State = HOLDOVER

Backup clocks for primary:
Source Slot Port DS3-Port Priority Status State
-----

Trunk cards controllers clock health information
-----
Slot Type 7 6 5 4 3 2 1 0
1 T1 B B B B B B B

CLOCK CHANGE HISTORY
-----

CLOCK      Event                               Time
-----
1/1      Loss Of Signal (LOS)                00:00:22 UTC Tue Nov 30 1999
1/2      Loss Of Signal (LOS)                00:00:22 UTC Tue Nov 30 1999
1/3      Alarm Indication Signal (AIS)        00:00:22 UTC Tue Nov 30 1999
1/4      Alarm Indication Signal (AIS)        00:00:22 UTC Tue Nov 30 1999
1/5      Alarm Indication Signal (AIS)        00:00:22 UTC Tue Nov 30 1999
1/6      Alarm Indication Signal (AIS)        00:00:22 UTC Tue Nov 30 1999
1/7      Alarm Indication Signal (AIS)        00:00:22 UTC Tue Nov 30 1999
Gateway#
```

- Verify your TDM clock history by using the **show tdm clocks** command (this example is for CT3):

```

Gateway# show tdm clocks

Primary Clock:
-----
System primary is slot 7 ds3_port 0 dsl_port 1 of priority 1
TDM Bus Master Clock Generator State = NORMAL

Backup clocks for primary:
Source Slot Port DS3-Port Priority Status State
-----
Trunk 7 8 YES 214 Good Default
Trunk 7 9 YES 215 Good Default

Trunk cards controllers clock health information
-----
CT3 2 2 2 2 2 2 2 2 2 1 1 1 1 1 1 1 1 1 1 1 1
Slot Port Type 8 7 6 5 4 3 2 1 0 9 8 7 6 5 4 3 2 1 0 9 8 7 6 5 4 3 2 1
7 0 T3 G G G G G G G G G G G G G G G G G G G G G G G G G G G G
CLOCK CHANGE HISTORY
-----

CLOCK Event Time
----
7/1 Signal recovered from LOS 00:03:29 UTC Sat Jan 1 2000
7/8 Alarm Indication Signal (AIS) 11:27:48 UTC Fri Feb 25 2000
7/1 Signal recovered from LOS 11:30:22 UTC Fri Feb 25 2000
Gateway#

```

- Verify your user-configured trunk clock selection by using the **show tdm clocks** command:

```

Gateway# show tdm clocks

Primary Clock:
-----
System primary is slot 2 port 0 of priority 15
TDM Bus Master Clock Generator State = NORMAL

Backup clocks for primary:
Source Slot Port DS3-Port Priority Status State
-----
Trunk 2 1 NO 205 Good Default

Trunk cards controllers clock health information
-----
Slot Type 7 6 5 4 3 2 1 0
2 T1 B B B B G G G G

CLOCK CHANGE HISTORY
-----

CLOCK Event Time
----
2/1 Controller shutdown 23:23:06 UTC Tue Nov 30 1999
2/0 Change in CLI configuration 23:27:25 UTC Tue Nov 30 1999
Gateway#

```

- Verify your free-running clock selection by using the **show tdm clocks** command:

```

Gateway# show tdm clocks

Primary Clock:
-----
System primary is FREE RUNNING with priority 2
TDM Bus Master Clock Generator State = FREERUN
Backup clocks for primary:
Source Slot Port DS3-Port Priority Status State
-----
Trunk 2 0 NO 204 Good Default
Trunk 2 1 NO 205 Good Default

Trunk cards controllers clock health information
-----

```



```
Slot Type 7 6 5 4 3 2 1 0
2      T1  B B B B G G G G
CLOCK CHANGE HISTORY
```

```
CLOCK      Event_                               Time
Freerun Change in CLI configuration           23:27:25 UTC Tue Nov 30 1999
Gateway#
```

- Verify your BITS clock selection by using the **show tdm clocks** command:

```
Gateway# show tdm clocks

Primary Clock:
System primary is external with priority 1
TDM Bus Master Clock Generator State = NORMAL
Backup clocks for primary:
Source Slot Port DS3-Port Priority Status State
Trunk 2 0 NO 204 Good Default
Trunk 2 1 NO 205 Good Default
Trunk cards controllers clock health information
Slot Type 7 6 5 4 3 2 1 0
2      T1  B B B B G G G G
CLOCK CHANGE HISTORY
```

```
CLOCK      Event_                               Time
External Change in CLI configuration         23:27:25 UTC Tue Nov 30 1999
Gateway#
```



Tip

The most common reason for clock slip problems is that the **dial-tdm-clock priority** parameter is set improperly. Change the default setting for **dial-tdm-clock priority** from free-running clock to a setting that matches your system requirements.

Saving Configuration Changes

To prevent the loss of the gateway configuration, save it to NVRAM, by following these steps:

- Step 1** Enter the **enable** command and password to go to privileged EXEC mode. You are in privileged EXEC mode when the prompt changes to Gateway#.

```
Gateway> enable
Password: password
Gateway#
```

- Step 2** Save the configuration changes to NVRAM so that they are not lost during resets, power cycles, or power outages:

```
Gateway# copy running-config startup-config
```

- Step 3** Return to privileged EXEC mode:

```
Gateway(config-if)# Ctrl-Z
Gateway#
```

Voice over IP

Prerequisites

Before you can configure your universal gateway to use Voice over IP, you must first do the following:

- Establish a working IP network. For more information about configuring IP, refer to the appropriate release of the *Cisco IOS IP Configuration Guide*. You can access this document at [Cisco Product Documentation > Cisco IOS Software Configuration > Cisco IOS Software Release you are using > Configuration Guides and Command References](#).
- Complete basic configuration for the universal gateway, which includes, as a minimum, the following tasks:
 - Complete your company’s dial plan.
 - Establish a working telephony network based on your company’s dial plan.
- Integrate your dial plan and telephony network into your existing IP network topology. Merging your IP and telephony networks depends on your particular IP and telephony network topology. In general, Cisco recommends the following suggestions:
 - Use canonical numbers wherever possible. It is important to avoid situations in which numbering systems are significantly different on different routers or universal gateways in your network.
 - Make routing and dialing transparent to the user—for example, avoid secondary dial tones from secondary switches, where possible.

Configuration Tasks

- Configure your IP network for real-time voice traffic

You need to have a well-engineered network end-to-end when running delay-sensitive applications such as VoIP. Fine-tuning your network to adequately support VoIP involves a series of protocols and features geared toward quality of service (QoS). It is beyond the scope of this quick start guide to explain the specific details relating to wide-scale QoS deployment. To configure your IP network for real-time voice traffic, you must consider the entire scope of your network, then select the appropriate QoS tool or tools.

It is important to remember that QoS must be configured throughout your network—not just on the universal gateway devices running VoIP—to improve voice network performance. Not all QoS techniques are appropriate for all network routers. Edge routers and backbone routers in your network do not necessarily perform the same operations; the QoS tasks they perform might also differ. To configure your IP network for real-time voice traffic, you must consider the functions of both edge and backbone routers in your network, then select the appropriate QoS tool or tools.

To configure QoS, refer to the relevant chapters of the *Cisco IOS Quality of Service Solutions Configuration Guide*. You can access this document at [Cisco Product Documentation > Cisco IOS Software Configuration > Cisco IOS Software Release you are using > Configuration Guides and Command References](#).

- Configure dial peers

Configuring dial peers is the key to setting up dial plans and implementing voice over a packet network. Dial peers are used to identify call source and destination endpoints and to define the characteristics applied to each call leg in the call connection.

For more information about VoIP, refer to the *Cisco IOS Multiservice Applications Configuration Guide*. You can access this document at [Cisco Product Documentation > Cisco IOS Software > Cisco IOS Software Release you are using > Configuration Guides and Command References](#).

Where to Go Next

For additional specialized configuration procedures, refer to the appropriate Cisco IOS software configuration documentation on the Documentation CD-ROM and on Cisco.com:

For detailed configuration information specific to the Cisco AS5350 and Cisco AS5400 Universal Gateway:

Cisco AS5350 and Cisco AS5400 Software Configuration Guide.

You can access this document at [Cisco Product Documentation > Access Servers and Access Routers > Access Servers > Cisco AS5350 or Cisco AS5400](#).

For detailed configuration information for specific features:

Configuration Guides and Command References for the Cisco IOS software release installed on your Cisco gateway.

You can access these documents at [Cisco Product Documentation > Cisco IOS Software Configuration > Cisco IOS Software Release you are using > Configuration Guides and Command References](#).

For new features associated with a software release:

New feature documentation for the Cisco IOS software release installed on your Cisco gateway.

You can access these documents at [Cisco Product Documentation > Cisco IOS Software Configuration > Cisco IOS Software Release you are using > New Feature Documentation](#).

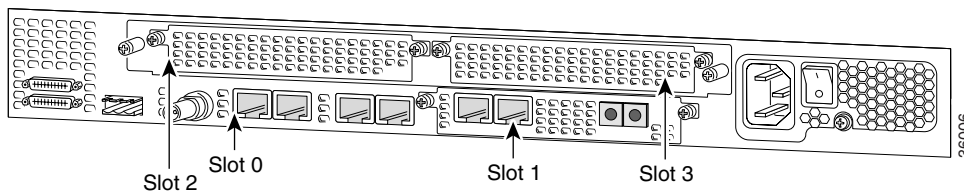
7 Slot Numbering

DFC slot numbering starts from the system board and works up from left to right. Slot 0 is reserved for the system board. The DFC slots are numbered sequentially.

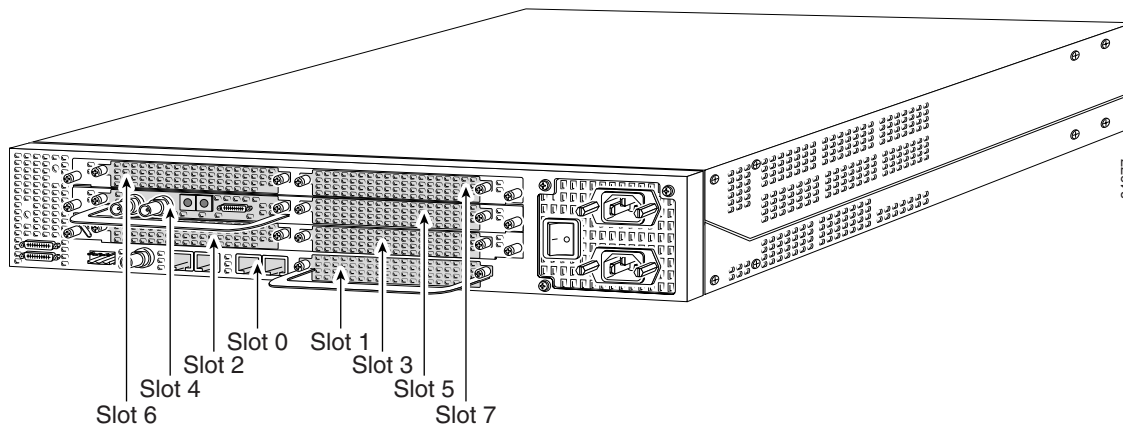


Note Unless specifically noted, all references to the Cisco AS5400 also apply to the Cisco AS5400HPX.

Cisco AS5350 Slot Numbers



Cisco AS5400 Slot Numbers



8 Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

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

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco web sites can be accessed from this URL:

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

Documentation CD-ROM

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

Registered Cisco.com users can order the Documentation CD-ROM (product number DOC-CONDOCCD=) through the online Subscription Store:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Registered Cisco.com users can order the Documentation CD-ROM (Customer Order Number DOC-CONDOCCD=) through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

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

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

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

We appreciate your comments.

9 Obtaining Technical Assistance

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

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

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

To obtain customized information and service, you can self-register on Cisco.com at this URL:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Cisco TAC Website

You can use the Cisco TAC website to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC website, go to this URL:

<http://www.cisco.com/tac>

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

<http://tools.cisco.com/RPF/register/register.do>

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

<http://www.cisco.com/en/US/support/index.html>

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words and attach any necessary files.

Cisco TAC Escalation Center

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

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

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

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

10 Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco monthly periodical that provides industry professionals with the latest information about the field of networking. You can access *Packet* magazine at this URL:

http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html

- *iQ Magazine* is the Cisco monthly periodical that provides business leaders and decision makers with the latest information about the networking industry. You can access *iQ Magazine* at this URL:

http://business.cisco.com/prod/tree.taf%3fasset_id=44699&public_view=true&kbns=1.html

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in the design, development, and operation of public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training, with current offerings in network training listed at this URL:

http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico
The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia
Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSF, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

© 2001-2003 Cisco Systems, Inc. All rights reserved.

♻️ Printed in the USA on recycled paper containing 10% postconsumer waste.
78-13590-04

Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>