

# Dial Case Study Overview

---

This case study builds a dial-up network environment using one Cisco AS5300. The access server supports remote users and remote LANs connecting with modems and ISDN routers. The remote routers in this case study are a Cisco 1604 and Cisco 766. Only IP and basic security are used.

This exercise gives you a basic foundation from which you can scale to support larger dial implementations.

The following sections are provided:

- “Scenario Description” on page 1
- “Design Architecture” on page 4
- “Overview of Tasks” on page 9
- “Related Documents and Web Tools” on page 10

## Scenario Description

The case study is structured around the following three figures.

Figure 1-1 shows a headquarters network providing dial-up services to one small office/home office (SOHO), one remote office/branch office (ROBO), and remote modem users.

**Figure 1-1 Business Scenario**

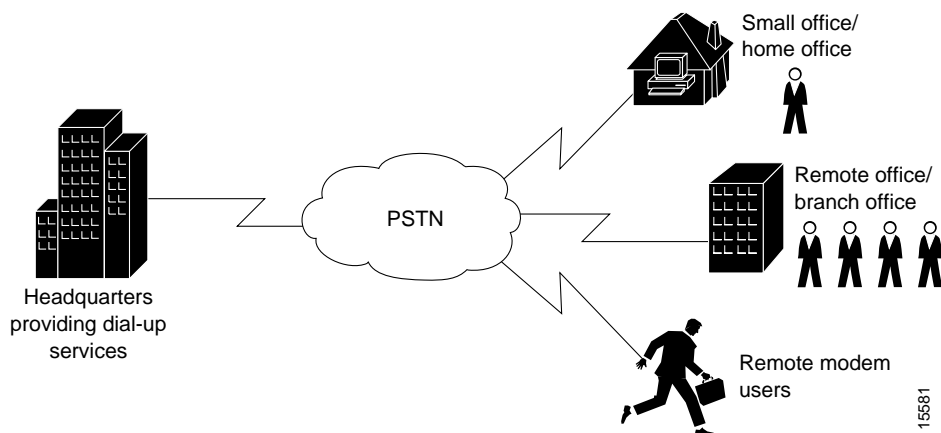
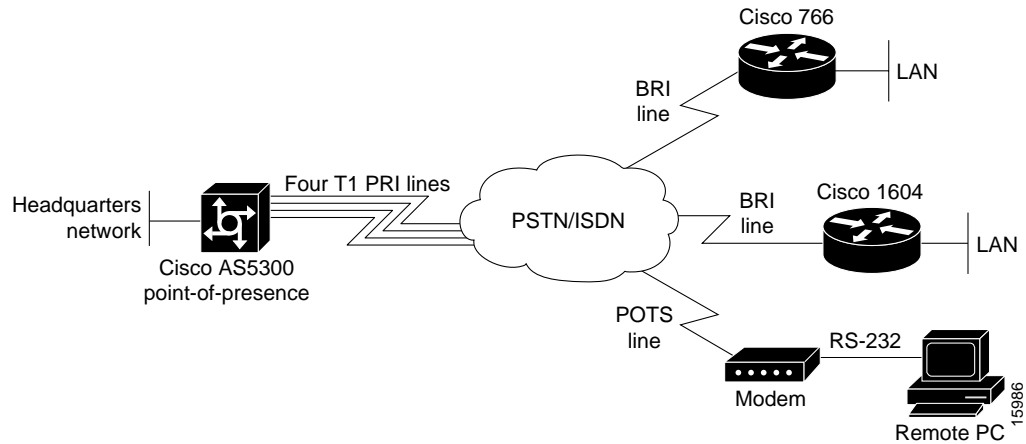


Figure 1-2 shows some of the physical elements present at layer 1 of the Open System Interconnection (OSI) reference model. The public switched telephone network (PSTN) provides the core interconnecting fabric between devices.

**Figure 1-2 OSI Layer 1 Elements**



In this scenario, a single Cisco AS5300 supports 96 concurrent modem and ISDN connections using four T1 PRI lines and 96 integrated modems. Modem connections are established via the Cisco IOS lines and corresponding asynchronous interfaces. Digital ISDN connections are established via the Cisco IOS channelized serial interfaces.

Figure 1-3 shows the layer 2 and layer 3 elements. The links going across the PSTN use the Point-to-Point Protocol (PPP). In this case study scenario PPP negotiates the link control protocol (LCP), CHAP or PAP authentication, and IP Control Protocol (IPCP) to bring up IP over PPP. IPCP is the network control protocol (NCP) used in this case study. IPCP is the mechanism that opens the links and negotiates the IP parameters.

Figure 1-3 OSI Layer 2 and Layer 3 Elements

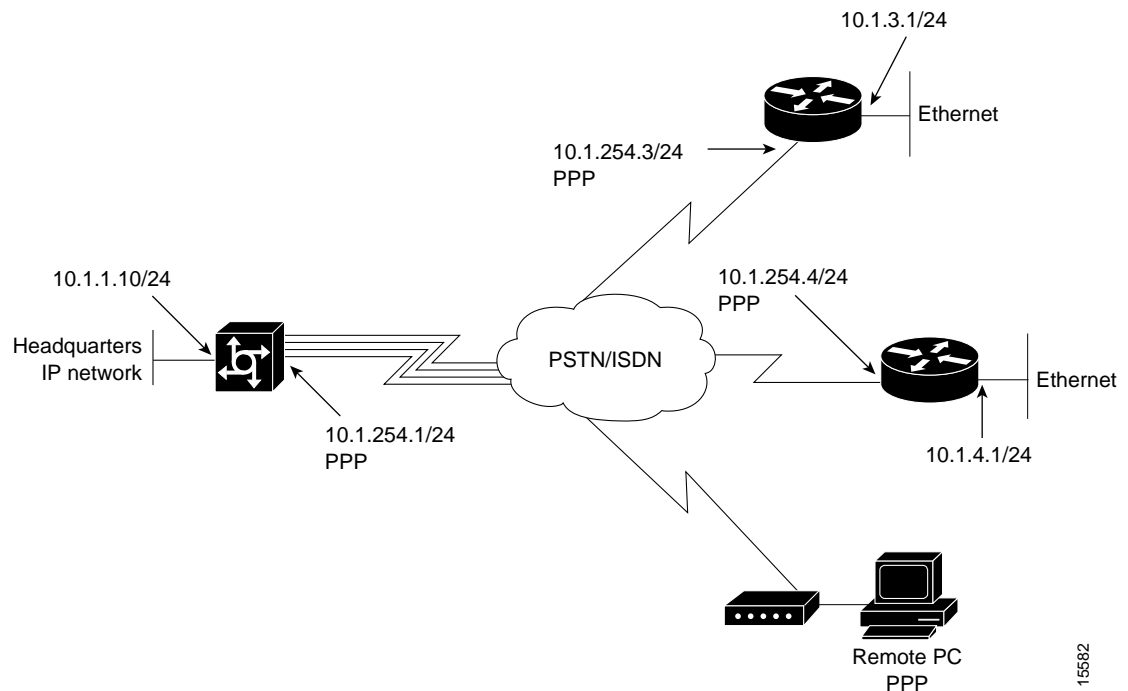


Table 1-1 summarizes the types of services provided by the headquarters POP to the remote nodes and sites. For more information, see Table 1-2 on page 4.

Table 1-1 Scenarios and Site Characteristics Provided by Headquarters

Scenario	Remote Hardware <sup>1</sup>	Services Required	Notes
Remote node modem	Modem	Asynchronous shell <sup>2</sup> (async shell) Asynchronous PPP (async PPP)	Dial in only <sup>4</sup> . Remote devices are assigned an IP address from a central pool.
Remote node ISDN	ISDN routers using port address translation (PAT) <sup>3</sup> , PC-based ISDN terminal adapters	Synchronous PPP (sync PPP)	Dial in only <sup>4</sup> . PAT enabled. Connecting devices are assigned an IP address from a central pool.
Remote office LAN	Cisco 1604	Synchronous PPP	Dial in and dial out <sup>4</sup> . Distinct IP subnet. PAT not used.
Small office LAN	Cisco 766	Synchronous PPP	Dial in and dial out <sup>4</sup> . Distinct IP subnet. PAT not used.

1. This is the typical hardware required at the remote site.
2. Cisco IOS shell terminal services can be used for low-level troubleshooting on asynchronous connectivity. The shell is the service you use to access the command line interface. The shell provides you with a terminal screen.
3. PAT = Port address translation. Easy IP is an implementation of PAT. PAT vastly simplifies IP addressing design when supporting remote sites. This case study does not describe how to configure PAT. For more information, see the *Dial Solutions Configuration Guide*. PAT is mentioned in this table to show you how the technology is positioned in the remote access paradigm.
4. Unless otherwise stated, the terms “dial-in” and “dial-out” are from the perspective of the Cisco AS5300.

## Design Architecture

The following sections provide the framework for this case study:

- Service Definitions
- Layer 3 IP Design
- IP Subnet Rationale
- Call Processing Components

## Service Definitions

In this case study, the Cisco AS5300 offers three basic services: async shell, async PPP, and sync PPP. See Table 1-2.

These services are based on real needs as requested by the remote sites. To access these services, remote devices connect to the Cisco AS5300 via the PSTN.

**Table 1-2 Services Provided by Headquarters**

Service Term	Purpose	Physical Data Path <sup>1</sup>	Security Method Used
Async shell	Provides access to Cisco IOS terminal services (no PPP) to do the following: <sup>2</sup> <ul style="list-style-type: none"> <li>• Change passwords</li> <li>• Access menus</li> <li>• Troubleshoot modem connections using a simple environment</li> <li>• Access other network resources via telnet</li> </ul>	Client modems, POTS <sup>3</sup> , Cisco IOS integrated modems, lines, and asynchronous interfaces	Login
Async PPP	<ul style="list-style-type: none"> <li>• Provides IP (and multi-protocol) connectivity for remote node modem users</li> <li>• Supports any Internet application available using IP such as e-mail, web browsing, FTP, and Telnet.</li> </ul>	Client modems, POTS <sup>3</sup> , Cisco IOS integrated modems, lines, and asynchronous interfaces	PPP (CHAP, PAP, or login)
Sync PPP	<ul style="list-style-type: none"> <li>• Provides IP (and multi-protocol) connectivity for BRI or PRI attached remote sites.</li> <li>• Supports any Internet application available using IP such as e-mail, web browsing, FTP, and Telnet<sup>4</sup>.</li> </ul>	End-to-end ISDN using B channels over a digital synchronous path, calls use interface serial channels (for example, S0:1, S0:2, and so forth)	PPP (CHAP or PAP)

1. This is the equipment and interface path used to deliver calls into the Cisco AS5300. See Figure 1-5.

2. Terminal services provided by the Cisco AS5300's integrated modems are terminated on TTY and VTY lines. The Cisco IOS shell is called the EXEC, which you can reach via a modem. The Cisco IOS shell is secured using "login" security. Authentication security associated with the EXEC is referred to as login. Sites offering terminal services can use menus to improve the user friendliness of the environment. For tips on how to create menus, see the *Configuration Fundamentals Configuration Guide*.

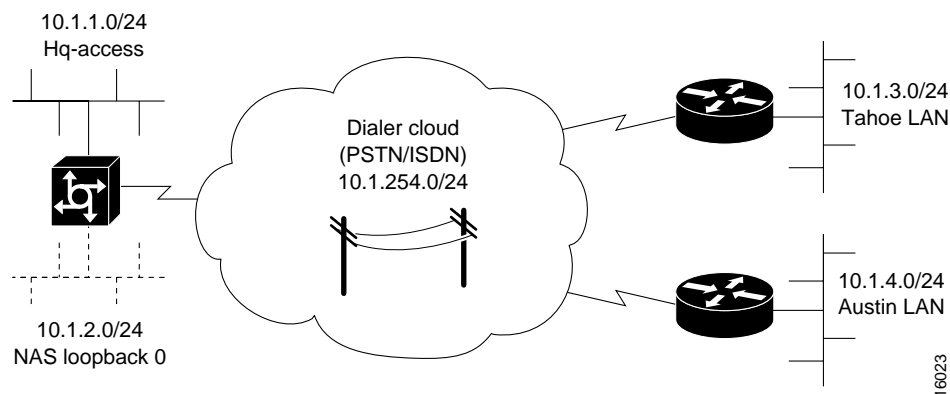
3. POTS = Plain old telephone service.

4. Terminal services via a shell are not available to synchronous link users (for example, ISDN routers and terminal adapters via a BRI channel). Only an asynchronous shell is available.

## Layer 3 IP Design

This case study uses PPP to transport IP packets across the PSTN and into the end-user devices (remote LAN or remote node). IPCP is the specific service enabled over the PPP links. To deliver this service, the case study uses address space from 10.1.0.0/16. See the following figures and tables for the IP subnetting plan.

**Figure 1-4 IP Subnetting Diagram**



**Table 1-3 IP Subnetting Plan**

Subnet Name	Assigned Subnet	Location
Hq-access	10.1.1.0 /24	Hq-access Ethernet
NAS loopback 0 <sup>1</sup>	10.1.2.0 /24	Loopback interface inside the Cisco AS5300
Dialer cloud	10.1.254.0 /24	Public switched telephone network
Tahoe LAN	10.1.3.0 /24	Tahoe Ethernet
Austin LAN	10.1.4.0 /24	Austin Ethernet
... <sup>2</sup>	...	...
...	...	...

1. NAS = network access server. The loopback subnet supports the remote node devices.
2. These dots mean that you can add additional subnets and remote LANs to this solution. This case study gives you a basic foundation from which you can scale to support larger dial implementations.

Using the subnetting plan and topologies shown in the previous tables and figures, a router naming and addressing plan is created in Table 1-4. Notice that the IP addresses are derived directly from the subnet plan.

**Table 1-4 Router IP Addressing Plan**

Router Name <sup>1</sup>	WAN IP Address	Ethernet IP Address
hq-sanjose	10.1.254.1 255.255.255.0	10.1.1.10 255.255.255.0
soho-tahoe	10.1.254.3 255.255.255.0	10.1.3.1 255.255.255.0
robo-austin	10.1.254.4 255.255.255.0	10.1.4.1 255.255.255.0
... <sup>2</sup>	...	...
...	...	...

1. Using the subnetting plan and topologies shown in the previous tables and figures, a router naming and addressing plan is created in are now assigned host names.
2. These dots mean that you can add additional subnets and remote LANs to this solution. This case study gives you a basic foundation from which you can scale to support larger dial implementations.

## IP Subnet Rationale

This section describes each IP subnet and its design criteria. IP route summarization occurs at the gateway that connects the NAS to the IP backbone. IP range 10.1.0.0/16 is propagated to the backbone.

### Hq-access Subnet

IP subnet 10.1.1.0/24 is assigned to the Ethernet connected to the Cisco AS5300. If additional access servers and POP management devices are needed, they are assigned to this IP subnet. Using one subnet for the entire headquarters dial access POP simplifies network design.

### NAS Loopback 0 Subnet

IP subnet 10.1.2.0/24 is assigned to the loopback interface on the Cisco AS5300. This is the subnet used to host the remote node IP addresses. The access server has an IP pool range of 10.1.2.2 through 10.1.2.97.

Remote nodes dialing in request addresses from the Cisco AS5300's local IP address pool. This IP pool behaves like an address server handing out IP addresses to remote nodes during IPCP negotiation (a component of PPP).

## Dialer Cloud Subnet

IP subnet 10.1.254.0/24 is assigned to the PSTN/ISDN. The static IP addresses are described in Table 1-4. See the column “WAN IP Address.” The PSTN/ISDN becomes a “dialer cloud” from the Cisco IOS perspective. Dialer interfaces are used to connect to this dialer cloud. BRI and PRI interfaces are also dialer interfaces and use the same dial-on-demand routing (DDR) mechanisms to open and close circuit-switched connections.

A key design decision in this case study is to number the dialer cloud subnet. (That is, IP unnumbered is not used on these interfaces.) Numbering the dialer cloud ports to match the remote LAN supported by the same remote device is part of our design strategy to simplify administration. For example, remote subnet 10.1.3.0/24 is connected to the same remote site as dialer cloud node 10.1.254.3. IP node 10.1.254.4 supports IP subnet 10.1.4.0/24.

On the Cisco AS5300, all the individual serial channel interfaces are grouped together under one master dialer interface. As the individual remote sites connect, their configurations must coordinate with the configuration of the master dialer interface.

## Tahoe and Austin LAN Subnets

IP subnet 10.1.3.0/24 is assigned to the Ethernet connected to the Cisco 766 (soho-tahoe). IP subnet 10.1.4.0/24 is assigned to the Cisco 1604 (robo-austin) Ethernet. Each site that supports a distinct IP subnet must be assigned its own distinct IP subnet address space. Routers with LANs behind them must have their own distinct IP subnets when not using PAT.

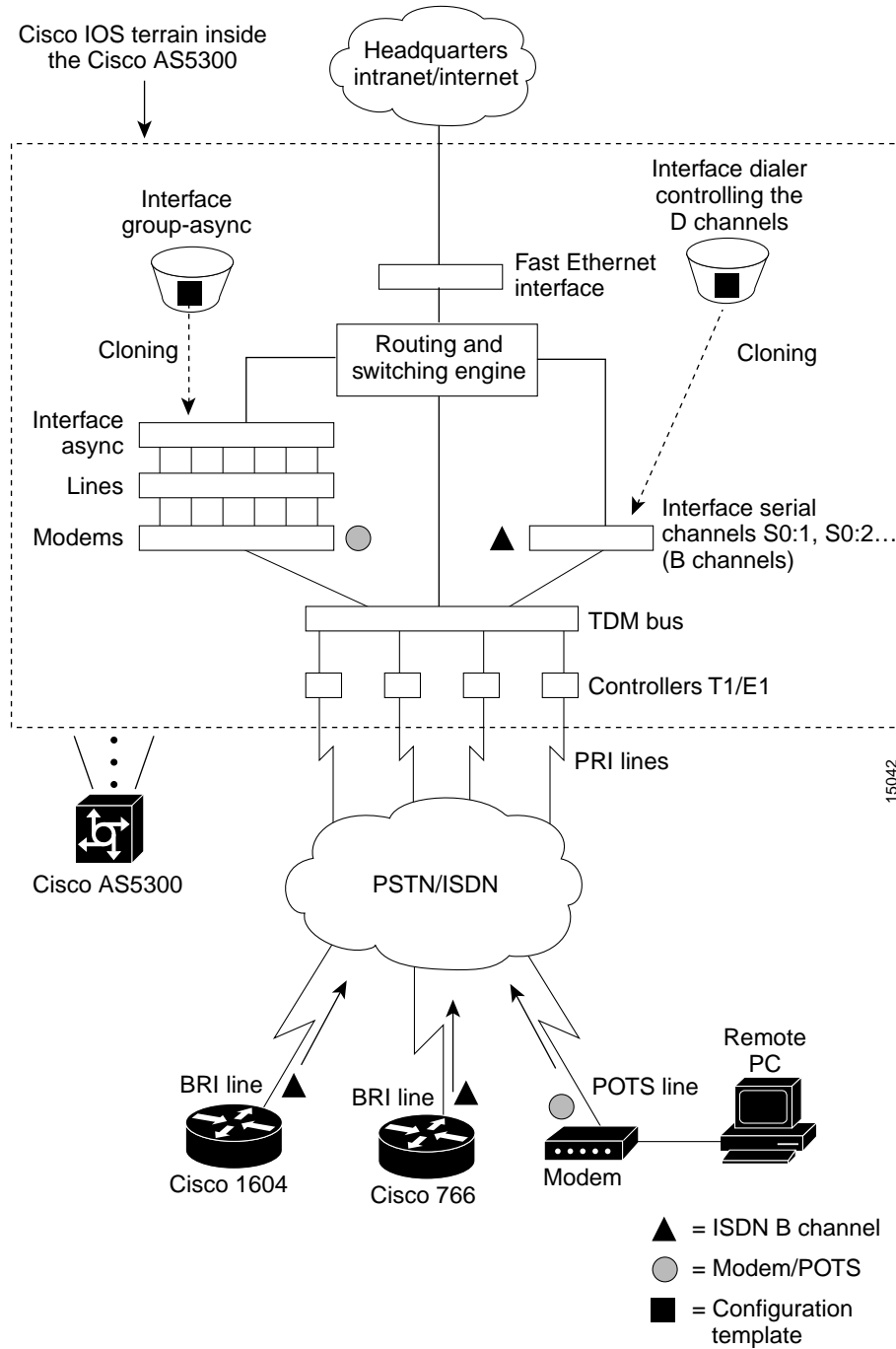
These remote LAN routers point to the central site as the default route. The hq-sanjose NAS is configured with static routes to the remote IP subnets.

## Call Processing Components

Figure 1-5 illustrates the connectivity path as calls come into the Cisco AS5300. The contents inside the dotted square box are the internal components of the Cisco AS5300. Both analog modem and digital calls enter the Cisco AS5300 via the E1/T1 controllers. Incoming modem calls are connected with the integrated modems and routed to the asynchronous interfaces. Incoming sync PPP calls are connected to the individual serial channels (for example, S0:1 and S0:2).

As shown in Figure 1-5, one PPP/modem user consumes resources from one channel, one integrated modem, one line, and one asynchronous interface. An ISDN B-channel user connects directly via a channel of the T1 and a serial B-channel. The group-async and dialer interfaces are used to control the interfaces' behavior and configuration of async and serial channels.

Figure 1-5 Call Processing Components



## Overview of Tasks

The network devices in this case study are manually configured using Cisco IOS software. The automatic Cisco IOS setup script is not used. This setup script usually runs when no startup configuration is found in NVRAM (for example, when powering up a new router).

Here is the action plan to build the network. For step-by-step configuration tasks, refer to the device-specific configuration chapters that follow.

- Step 1** Set up async shell services on the Cisco AS5300. See chapter 2 “Cisco AS5300 Configuration.”
- Configuring the Host Name, Password, and Time Stamps
  - Configuring Local AAA Security
  - Configuring the Fast Ethernet 100BaseT Interface
  - Commissioning the T1 Controllers
  - Configuring the Serial Channels to Let Modem Calls Come in
  - Configuring the Modems and Lines
  - Testing Async Shell Connections
- Step 2** Set up async PPP services on the Cisco AS5300. See chapter 2 “Cisco AS5300 Configuration.”
- Setting Up IP Address Pools
  - Configuring the Group-Async Interface
  - Testing Async PPP Connections
- Step 3** Set up synchronous PPP services on the Cisco AS5300. See chapter 2 “Cisco AS5300 Configuration.”
- Configuring DDR
  - Configuring Definitions for Remote LAN Sites
  - Configuring a Backhaul Routing Protocol
  - Confirming the Final Running Configuration
  - Saving the Configuration
  - Testing Sync PPP Connections to Remote LANs
  - Adding More Remote LAN Sites as Needed
- Step 4** Configure the Cisco 1604 to dial into the Cisco AS5300. See chapter 3 “Cisco 1604 Configuration.”
- Configuring the Host Name, Password, and Time Stamps
  - Configuring Local AAA Security
  - Configuring the Ethernet Interface
  - Configuring BRI
  - Configuring DDR
  - Testing Connections to the Cisco AS5300

- Confirming the Final Running Configuration
- Saving the Configuration
- Step 5** Configure the Cisco 766 to dial into the Cisco AS5300. See chapter 4 “Cisco 766 Configuration.”
  - Configuring System Level Settings
  - Configuring the LAN Profile
  - Configuring the Site Profile hq-sanjose
  - Testing Connections to the Cisco AS5300
  - Confirming the Final Running Configuration

## Related Documents and Web Tools

Refer to the following online resources for more information:

- *Internetworking Case Studies*—Provides practical examples of how to implement Cisco IOS software features. Case studies address implementation concerns and show how to apply features to their best advantage. Detailed configuration file examples and network diagrams are included.  
<http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/index.htm>
- *Cisco Access Dial Configuration Cookbook*—Contains common configurations or recipes to configure various access routers and dial technologies. It covers common configurations for async, dial-on-demand routing (DDR), integrated services digital network (ISDN), and other access dial concepts including basic security. It also provides configurations for the Cisco 700, AS5200, and AS5300. You must be a registered Cisco Connection Online (CCO) user to gain access to this publication.  
[http://www.cisco.com/warp/customer/793/access\\_dial/](http://www.cisco.com/warp/customer/793/access_dial/)
- *Dial Solutions Configuration Guide and Command Reference*—Provides a comprehensive library of Cisco’s dial software features, which are configured using the command line interface.  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed\\_cr/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/index.htm)
- *Internetworking Technology Overview, Point-to-Point Protocol*—Describes the background and general operation of PPP.  
[http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/55168.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/55168.htm)

- *Troubleshooting Engine*—Helps you solve common problems involving hardware, configuration, and performance.  
<http://te.cisco.com/cgi-bin/webcgi.exe?New,KB=TE>
- *Cisco AS5x00 Access Server Documentation*—Includes software and hardware configuration guides for Cisco's access server product line.  
[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/index.htm)

---

**Note** These URLs can change without notice.

---



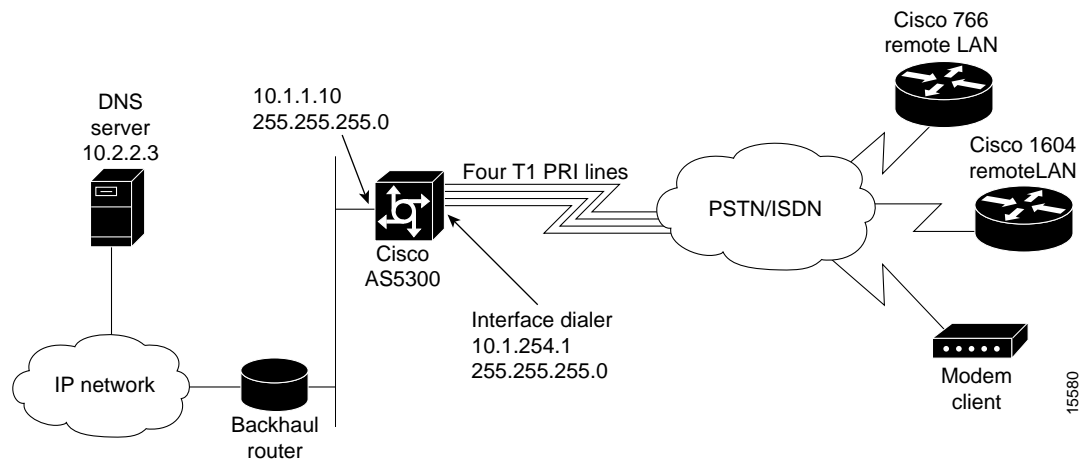
# Cisco AS5300 Configuration

This chapter describes how to configure the Cisco AS5300 to receive calls from the Cisco 1604, Cisco 766, and remote modem users.

## Site Profile Characteristics

Figure 2-1 shows the network topology from the Cisco AS5300's perspective.

**Figure 2-1 Network Topology**



**Note** Before you perform the configuration tasks in this chapter, be sure you understand the overall dial case action plan described in the previous chapter “Dial Case Study Overview.”

Table 2-1 provides detailed information about each end of the connection. This is the network administrator’s top-level design table.

**Table 2-1 Site Characteristics**

Site Hardware	WAN IP Address	Ethernet IP Address	Assigned Phone Number	Host Name/Username <sup>1</sup>	Username Password <sup>1</sup>
Cisco AS5300 <sup>2</sup>	10.1.254.1 255.255.255.0 <sup>3</sup>	10.1.1.10 255.255.255.0	4085551234 <sup>4</sup>	hq-sanjose	hq-sanjose-pw
Cisco 766	10.1.254.3 255.255.255.0	10.1.3.1 255.255.255.0	Directory number = 5305558084	soho-tahoe	tahoe-pw
Cisco 1604	10.1.254.4 255.255.255.0	10.1.4.1 255.255.255.0	Directory number = 5125554433	robo-austin	austin-pw

1. Make sure to use your own host names and passwords. For example *soho-tahoe* and *tahoe-pw* are for this case study’s purpose only.
2. The subnet 10.1.2.0 255.255.255.0 is used for the loopback interface and the local IP address pools.
3. This address is configured on the Cisco AS5300’s dialer interface.
4. This is the PRI telephone number assigned to the central site (hq-sanjose). This number is often called the hunt group number, which distributes calls among the available B channels. All four PRI trunks on the Cisco AS5300 should be assigned to this number by the PRI provider.

Cisco IOS Release 12.0 is running inside the access server. If the startup configuration is blank, the following screen is displayed at bootup. The automatic setup script is engaged. Enter **no** when you are asked the question, “Would you like to enter the initial configuration dialog? [yes]: **no**.”

In this case study, the Cisco AS5300 is manually configured using the Cisco IOS software. The automatic setup script is not used.

**Note** To enhance readability throughout this chapter, the most important output fields are highlighted with **bold** font. The commands you enter are also **bold** but are preceded by a router prompt.

```
Copyright (c) 1994-1995 by cisco Systems, Inc.
AS5300 processor with 32768 Kbytes of main memory
program load complete, entry point: 0x80008000, size: 0xf4b10
```

```
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) 5300 Software (C5300-JS-M), Version 12.0(x)
Copyright (c) 1986-1998 by cisco Systems, Inc.
Compiled Tue 07-Jul-98 15:26 by xxxx
Image text-base: 0x600088E8, data-base: 0x608F4000
cisco AS5300 (R4K) processor (revision A.04) with 32768K/8192K bytes of memory.
Processor board ID 04614948
R4700 processor, Implementation 33, Revision 1.0 (512KB Level 2 Cache)
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
Primary Rate ISDN software, Version 1.1.
Backplane revision 1
Manufacture Cookie is not programmed.
1 Ethernet/IEEE 802.3 interface(s)
1 FastEthernet/IEEE 802.3 interface(s)
96 terminal line(s)
4 Channelized T1/PRI port(s)
128K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)
4096K bytes of processor board Boot flash (Read/Write)
Cisco Internetwork Operating System Software
IOS (tm) 5300 Software (C5300-JS-M), Version 12.0(x),
Copyright (c) 1986-1998 by cisco Systems, Inc.
Compiled Tue 07-Jul-98 15:26 by xxx
00:00:50: %MICA-5-BOARDWARE_RUNNING: Slot 2 is running boardware version 2.5.0.8
--- System Configuration Dialog ---

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 '['].

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

Press RETURN to get started!

Router>
```

---

**Note** Use the **show version** command to determine if the access server is recognizing all of its modems cards. For example, the output field “96 terminal line(s)” tells you that the chassis can find all 96 integrated modems.

---

## Overview of Tasks

Perform the following steps to configure the access server:

- Set up asynchronous shell services:
  - “Step 1—Configuring the Host Name, Password, and Time Stamps” on page 5
  - “Step 2—Configuring Local AAA Security” on page 6
  - “Step 3—Configuring the Fast Ethernet 100BaseT Interface” on page 8
  - “Step 4—Commissioning the T1 Controllers” on page 10
  - “Step 5—Configuring the Serial Channels to Let Modem Calls Come in” on page 14
  - “Step 6—Configuring the Modems and Lines” on page 18
  - “Step 7—Testing Async Shell Connections” on page 19
- Set up asynchronous PPP services:
  - “Step 8—Setting Up IP Address Pools” on page 27
  - “Step 9—Configuring the Group-Async Interface” on page 28
  - “Step 10—Testing Async PPP Connections” on page 31
- Set up synchronous PPP services:
  - “Step 11—Configuring DDR” on page 36
  - “Step 12—Configuring Definitions for Remote LAN Sites” on page 39
  - “Step 13—Configuring a Backhaul Routing Protocol” on page 41
  - “Step 14—Confirming the Final Running Configuration” on page 42
  - “Step 15—Saving the Configuration” on page 44
  - “Step 16—Testing Sync PPP Connections to Remote LANs” on page 44
  - “Step 17—Adding More Remote LAN Sites as Needed” on page 44

## Step 1—Configuring the Host Name, Password, and Time Stamps

Assign a host name to the Cisco AS5300, enable basic security, and turn on time stamping. Configuring a host name allows you to distinguish between different network devices. Enable passwords allow you to prevent unauthorized configuration changes. Time stamps help you trace debug output for testing connections. Not knowing exactly when an event occurs hinders you from examining background processes.

### Configure

To configure the host name, enable password, and time stamps use the following commands beginning in user EXEC mode:

Step	Command	Purpose
1	Router> <b>enable</b>	Enter privileged EXEC mode.
2	Router# <b>configure terminal</b> Enter configuration commands, one per line. End with CNTL/Z.	Enter global configuration mode <sup>1</sup> .
3	Router(config)# <b>hostname hq-sanjose</b>	Assign a host name to the access server <sup>2</sup> . This host name is typically used during authentication with PPP peers.
4	hq-sanjose(config)# <b>enable secret letmein</b>	Enter a secret enable password, which secures privileged EXEC mode <sup>3</sup> .
5	hq-sanjose(config)# <b>service password-encryption</b>	Encrypt passwords in the configuration file for greater security <sup>4</sup> .
6	hq-sanjose(config)# <b>service timestamps debug datetime msec</b> hq-sanjose(config)# <b>service timestamps log datetime msec</b>	Enable millisecond time stamping on debug and logging output. Time stamps are useful for detailed access troubleshooting.

1. If the logging output generated by the access server interferes with your terminal screen, redisplay your current command line using the **Tab** key.
2. The step is verified by the router prompt changing from Router(config)# to hq-sanjose(config)#.
3. Make sure to change "letmein" to your own secret password.
4. Additional measures should be used, as the passwords are not strongly encrypted by today's standards.

### Verify

To verify the configuration:

- Try logging in with your new enable password. Exit out of enable mode using the **disable** command. The prompt changes from hq-sanjose# to hq-sanjose>. Enter the **enable** command followed by your password. The **show privilege** command shows the current security privilege level.

```
hq-sanjose# disable
hq-sanjose> enable
Password: letmein
hq-sanjose# show privilege
Current privilege level is 15
hq-sanjose#
```

- Enter the **show running** command:

```
hq-sanjose# show running
Building configuration...
Current configuration:
!
version 12.0
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname hq-sanjose
!
enable secret 5 $1$.voA$9/8.Zo1l3jeWJMP6hEE6U0
!
----- snip -----
```

### Tips

If you have trouble:

- Make sure **Caps Lock** is off.
- Make sure you entered the correct passwords. Passwords are case sensitive.
- Password protection is very important. Cisco highly recommends that you use the **show tech-support** command to report system configuration information to Cisco TAC:

```
hq-sanjose# show tech-support ?
ipmulticast  IP multicast related information
page         Page through output
password     Include passwords
rsvp        IP RSVP related information
<cr>
```

## Step 2—Configuring Local AAA Security

The Cisco IOS security model to use on all Cisco devices is authentication, authorization, and accounting (AAA). AAA provides the primary framework through which you set up access control on the access server.

- Authentication—Who are you?
- Authorization—What can you do?
- Accounting—What did you do?

In this case study, the same authentication method is used on all interfaces. AAA is set up to use the local database configured on the router. This local database is created with the **username** configuration commands.

---

**Note** After you finish setting up basic security, you can enhance the security solution by extending it to an external TACACS+ or RADIUS server. This case study describes local AAA security only.

---

## Configure

To configure local AAA security, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	hq-sanjose(config)# <b>username joe-admin password joe-password</b>	Create a local login database and username for yourself <sup>1</sup> .  This step also prevents you from getting locked out of the access server.
2	hq-sanjose(config)# <b>aaa new-model</b>	Initiate the AAA access control system.  This step immediately locks down login and PPP authentication.
3	hq-sanjose(config)# <b>aaa authentication login default local</b>	Configure AAA to perform login authentication using the local username database.  The <b>login</b> keyword authenticates shell/EXEC users.
4	hq-sanjose(config)# <b>aaa authentication ppp default if-needed local</b>	Configure PPP authentication to use the local database if the session was not already authenticated by <b>login</b> .

1. Make sure to change “joe-admin” to your own username and “joe-password” to your own password.

## Verify

To verify the configuration:

- Try to log in with your username:password. Enter the **login** command at the EXEC shell prompt. If you get in, the login authentication is working with your local username. Do not disconnect your access server session until you can log in successfully. (If you get locked out, you will need to perform password recovery by rebooting the access server.)

```
hq-sanjose# login

User Access Verification

Username: joe-admin
Password: joe-password

hq-sanjose#
```

- Enter the **show running** command:

```
hq-sanjose# show running
Building configuration...
Current configuration:
!
version 12.0
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname hq-sanjose
```

```

!
aaa new-model
aaa authentication login default local
aaa authentication ppp default if-needed local
enable secret 5 $1$.voA$9/8.Zoil3jeWJMP6hEE6U0
!
username joe-admin password 7 <removed>
!
----- snip -----

```

## Step 3—Configuring the Fast Ethernet 100BaseT Interface

Assign an IP address, line speed, and duplex mode to the Fast Ethernet interface. The Fast Ethernet interface supports 10- and 100-Mbps speeds.

The default priority search order for auto negotiating the line speed is as follows:

- 1 100Base-TX full duplex
- 2 100Base-TX half duplex
- 3 10Base-T full duplex
- 4 10Base-T half duplex

## Configure

To configure the Fast ethernet 100BaseT interface, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	hq-sanjose(config)# <b>interface fastethernet 0</b> hq-sanjose(config-if)# <b>ip address 10.1.1.10 255.255.255.0</b>	Configure the IP address and subnet mask on the Fast Ethernet interface.
2	hq-sanjose(config-if)# <b>speed auto</b>	Auto negotiate the line speed based on the peer routers, hubs, and switch media.
3	hq-sanjose(config-if)# <b>duplex auto</b>	Auto negotiate duplex mode.
4	hq-sanjose(config-if)# <b>no shutdown</b> %LINK-3-UPDOWN: Interface FastEthernet0, changed state to up	Bring up the interface <sup>1</sup> .

1. This command changes the state of the interface from administratively down to up.

## Verify

To verify the configuration:

- Enter the **show ip interface brief** command to view the interface’s status. The “up” display field should appear under the Status and Protocol columns. The display fields “down” or “administratively down” signify a connection problem.

```

hq-sanjose# show ip interface brief fastethernet 0
Interface          IP-Address      OK?    Method    Status    Protocol
FastEthernet0     10.1.1.10      YES    manual    up        up

```

- Try pinging a device in your network, such as a backhaul router or the backbone gateway:

```
hq-sanjose# ping 10.1.1.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
```

- Enter the **show interface fastethernet 0** command to see detailed interface information. Look for the display field “FastEthernet 0 is up, line protocol is up.” This means that the access server sees its own sent and received keepalives.

```
hq-sanjose# show interface fastethernet 0
```

```
FastEthernet0 is up, line protocol is up
```

```
Hardware is DEC21140AE, address is 00e0.1e6b.2ffb (bia 00e0.1e6b.2ffb)
```

```
Internet address is 10.1.1.10 /24
```

```
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
```

```
Encapsulation ARPA, loopback not set, keepalive set (10 sec), auto duplex,  
100BaseTX/FX, auto speed
```

```
ARP type: ARPA, ARP Timeout 04:00:00
```

```
Last input 00:00:05, output 00:00:05, output hang never
```

```
Last clearing of "show interface" counters never
```

```
Queueing strategy: fifo
```

```
Output queue 0/40, 0 drops; input queue 0/120, 0 drops
```

```
5 minute input rate 0 bits/sec, 0 packets/sec
```

```
5 minute output rate 0 bits/sec, 0 packets/sec
```

```
282 packets input, 68476 bytes, 0 no buffer
```

```
Received 282 broadcasts, 0 runts, 0 giants, 0 throttles
```

```
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
0 watchdog, 0 multicast
```

```
0 input packets with dribble condition detected
```

```
176 packets output, 16936 bytes, 0 underruns
```

```
0 output errors, 0 collisions, 0 interface resets
```

```
0 babbles, 0 late collision, 0 deferred
```

```
0 lost carrier, 0 no carrier
```

```
0 output buffer failures, 0 output buffers swapped out
```

- Enter the **show running** command:

```
hq-sanjose# show running
```

```
Building configuration...
```

```
Current configuration:
```

```
!
```

```
----- snip -----
```

```
!
```

```
interface FastEthernet0
```

```
ip address 10.1.1.10 255.255.255.0
```

```
no ip directed-broadcast
```

```
no ip route-cache
```

```
no ip mroute-cache
```

```
duplex auto
```

```
speed auto
```

```
!
```

```
----- snip -----
```

## Tips

If you have trouble:

- Make sure the cable connections are not loose or disconnected.
- Make sure you are using the correct IP address.

## Step 4—Commissioning the T1 Controllers

Configure the T1 controllers to allow calls to come into the access server. You must specify the following information for each controller: framing type, line code type, clock source, and timeslot assignments.

### Configure

To configure the controllers, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	<code>hq-sanjose(config)# isdn switch-type primary-ni</code>	Enter your telco's switch type. This example uses primary national ISDN 1.
2	<code>hq-sanjose(config)# controller t1 0</code>	Enter controller configuration mode for the first T1 controller, which is 0. The controller ports are labeled 0 through 3 on the quad T1/PRI card.
3	<code>hq-sanjose(config-controller)# framing esf</code>	Enter the T1 framing type. This example uses extended super frame.
4	<code>hq-sanjose(config-controller)# linecode b8zs</code>	Enter the T1 line code type. This example uses B8ZS.
5	<code>hq-sanjose(config-controller)# clock source line primary</code>	Configure the access server to get its primary clocking from the T1 line assigned to controller 0. Line clocking comes from the remote switch.
6	<code>hq-sanjose(config-controller)# pri-group timeslots 1-24</code>	Assign all 24 T1 timeslots as ISDN PRI channels <sup>1</sup> .
7	<code>hq-sanjose(config-controller)# exit</code>	Exit back to global configuration mode.
8	<code>hq-sanjose(config)# controller t1 1</code> <code>hq-sanjose(config-controller)# framing esf</code> <code>hq-sanjose(config-controller)# linecode b8zs</code> <code>hq-sanjose(config-controller)# clock source line secondary</code> <code>hq-sanjose(config-controller)# pri-group timeslots 1-24</code> <code>hq-sanjose(config-controller)# exit</code>	Configure the second controller, controller T1 1. Set the clocking to <b>secondary</b> . If the line clocking from controller T1 0 fails, the access server will receive its clocking from controller T1 1.
9	<code>hq-sanjose(config)# controller t1 2</code> <code>hq-sanjose(config-controller)# framing esf</code> <code>hq-sanjose(config-controller)# linecode b8zs</code> <code>hq-sanjose(config-controller)# clock source internal</code> <code>hq-sanjose(config-controller)# pri-group timeslots 1-24</code> <code>hq-sanjose(config-controller)# exit</code> <code>hq-sanjose(config)# controller t1 3</code> <code>hq-sanjose(config-controller)# framing esf</code> <code>hq-sanjose(config-controller)# linecode b8zs</code> <code>hq-sanjose(config-controller)# clock source internal</code> <code>hq-sanjose(config-controller)# pri-group timeslots 1-24</code> <code>hq-sanjose(config-controller)# exit</code> <code>hq-sanjose(config)#</code>	Configure the remaining two controllers. Set both clocking entries to <b>internal</b> . The primary and secondary clock sources have already been assigned.

1. After you enter this command, a D-channel serial interface is instantly created (for example S0:23, S1:23, and so on) in the configuration file as well as the individual B-channel serial interfaces (for example S0:0, S0:1, ...). The D-channel interface functions like a dialer for all the 23 B channels using the controller.

## Verify

To verify the configuration:

- Use the **show controller t1** command. The output from this command enables you to determine when and where errors occur. See the display field “Data in current interval.”

```

hq-sanjose# show controller t1
T1 0 is up.
  No alarms detected.
  Version info of slot 0: HW: 2, Firmware: 16, PLD Rev: 0
  Manufacture Cookie Info:
  EEPROM Type 0x0001, EEPROM Version 0x01, Board ID 0x42,
  Board Hardware Version 1.0, Item Number 73-2217-4,
  Board Revision A0, Serial Number 07557185,
  PLD/ISP Version 0.0, Manufacture Date 17-Dec-1997.
  Framing is ESF, Line Code is B8ZS, Clock Source is Line Primary.
  Data in current interval (25 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
T1 1 is up.
  No alarms detected.
  Version info of slot 0: HW: 2, Firmware: 16, PLD Rev: 0
  Manufacture Cookie Info:
  EEPROM Type 0x0001, EEPROM Version 0x01, Board ID 0x42,
  Board Hardware Version 1.0, Item Number 73-2217-4,
  Board Revision A0, Serial Number 07557185,
  PLD/ISP Version 0.0, Manufacture Date 17-Dec-1997.
  Framing is ESF, Line Code is B8ZS, Clock Source is Line Secondary.
  Data in current interval (827 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
T1 2 is administratively down.
  Transmitter is sending remote alarm.
  Receiver has loss of signal.
  Version info of slot 0: HW: 2, Firmware: 16, PLD Rev: 0
  Manufacture Cookie Info:
  EEPROM Type 0x0001, EEPROM Version 0x01, Board ID 0x42,
  Board Hardware Version 1.0, Item Number 73-2217-4,
  Board Revision A0, Serial Number 07557185,
  PLD/ISP Version 0.0, Manufacture Date 17-Dec-1997.
  Framing is ESF, Line Code is B8ZS, Clock Source is Internal.
  Data in current interval (868 seconds elapsed):
    3 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 868 Fr Loss Secs, 2 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 868 Unavail Secs
  Total Data (last 24 hours)
    182 Line Code Violations, 0 Path Code Violations,
    1 Slip Secs, 86400 Fr Loss Secs, 125 Line Err Secs, 0 Degraded Mins,
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 86400 Unavail Secs
T1 3 is administratively down.
  Transmitter is sending remote alarm.
  Receiver has loss of signal.
  Version info of slot 0: HW: 2, Firmware: 16, PLD Rev: 0
  Manufacture Cookie Info:

```

```
EEPROM Type 0x0001, EEPROM Version 0x01, Board ID 0x42,
Board Hardware Version 1.0, Item Number 73-2217-4,
Board Revision A0, Serial Number 07557185,
PLD/ISP Version 0.0, Manufacture Date 17-Dec-1997.
Framing is ESF, Line Code is B8ZS, Clock Source is Internal.
Data in current interval (142 seconds elapsed):
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 142 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 142 Unavail Secs
Total Data (last 24 hours)
  12 Line Code Violations, 0 Path Code Violations,
  0 Slip Secs, 86400 Fr Loss Secs, 8 Line Err Secs, 0 Degraded Mins,
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 86400 Unavail Secs
```

- Enter the **show controller t1 number** command. If counters are increasing on a specific T1 controller, look more closely at the error statistics. Error counters are recorded for a 24-hour period in 15-minute intervals. You must specify a specific controller number to see this detailed information. Focus on the current interval.

In the following example, notice that the frame loss and line errors present in data intervals 1 through 4 were eventually cleared up in the current data interval.

---

**Note** Errors are reported to the controller's counters each time an error is encountered. Therefore, clear the counters using the **clear controller t1 number** command before you look for current error statistics. Error counters stop increasing when the controller is configured correctly.

---

```
hq-sanjose# show controller t1 0
T1 0 is up.
  No alarms detected.
  Version info of slot 0: HW: 2, Firmware: 16, PLD Rev: 0
Manufacture Cookie Info:
EEPROM Type 0x0001, EEPROM Version 0x01, Board ID 0x42,
Board Hardware Version 1.0, Item Number 73-2217-4,
Board Revision A0, Serial Number 07557185,
PLD/ISP Version 0.0, Manufacture Date 17-Dec-1997.
Framing is ESF, Line Code is B8ZS, Clock Source is Line Primary.
Data in current interval (72 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
Data in Interval 1:
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 405 Fr Loss Secs, 14 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 405 Unavail Secs
Data in Interval 2:
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 450 Fr Loss Secs, 1 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 450 Unavail Secs
Data in Interval 3:
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 450 Fr Loss Secs, 1 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 450 Unavail Secs
Data in Interval 4:
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 450 Fr Loss Secs, 2 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 450 Unavail Secs
----- snip -----
```

- Enter the **show running** command:

```
hq-sanjose# show running
Building configuration...
Current configuration:
!
----- snip -----
!
isdn switch-type primary-ni
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 1
 framing esf
 clock source line secondary
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 2
 framing esf
 clock source internal
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 3
 framing esf
 clock source internal
 linecode b8zs
 pri-group timeslots 1-24
!
----- snip -----
```

## Tips

If you have trouble:

- Make sure the controller reports “up.”
- No errors should be reported in the current interval.

## Step 5—Configuring the Serial Channels to Let Modem Calls Come in

The async shell service is the first service to enable. Configure the D channels to allow incoming voice calls to be routed to the integrated modems.

In the section “Configuration DDR,” the D channel configuration is expanded to also accept ISDN synchronous PPP calls from the remote offices. Cisco recommends getting modem users up first.

### Configure

To configure the serial channels, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	hq-sanjose(config)# <b>interface serial 0:23</b>	Enter configuration mode for the D-channel serial interface that corresponds to controller T1 0 <sup>1</sup> .  The behavior of S0:0 through S0:22 is controlled by the configuration instructions provided for S0:23. This concept is also true for the other remaining D channel configurations.
2	hq-sanjose(config-if)# <b>isdn incoming-voice modem</b> hq-sanjose(config-if)# <b>no shutdown</b>	Enable analog modem voice calls coming in over the B channels to be connected to the integrated modems.
3	hq-sanjose(config-if)# <b>exit</b>	Exit back to global configuration mode.
4	hq-sanjose(config)# <b>interface serial 1:23</b> hq-sanjose(config-if)# <b>isdn incoming-voice modem</b> hq-sanjose(config-if)# <b>no shutdown</b> hq-sanjose(config-if)# <b>exit</b> hq-sanjose(config)# <b>interface serial 2:23</b> hq-sanjose(config-if)# <b>isdn incoming-voice modem</b> hq-sanjose(config-if)# <b>no shutdown</b> hq-sanjose(config-if)# <b>exit</b> hq-sanjose(config)# <b>interface serial 3:23</b> hq-sanjose(config-if)# <b>isdn incoming-voice modem</b> hq-sanjose(config-if)# <b>no shutdown</b> hq-sanjose(config-if)# <b>exit</b> hq-sanjose(config)#	Configure the three remaining D channels with the same settings.

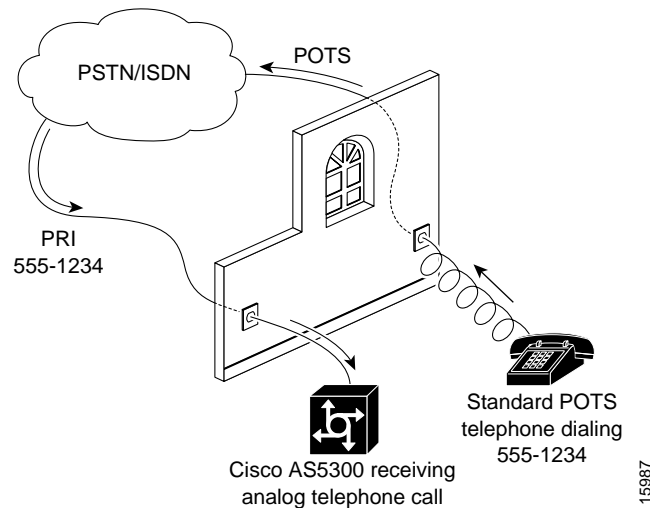
1. The D channel is the signaling channel.

## Verify

To verify the configuration:

- Launch a voice call into the access server using a standard POTS telephone. If you hear modem squelch (tone) from the access server's internal modem, the configuration works. See Figure 2-2.

**Figure 2-2 Voice Test Call**



- Enter the **show interface serial 0:23** command. The term “spoofing” means that the interface is presenting itself to the Cisco IOS software as up and operational. This interface can now receive routes. There are 23 more channels behind this interface that you do not see (for example, S0:0, S0:1, and so on). The D channel decides which serial channel to assign to an incoming call.

```

hq-sanjose# show interface serial 0:23
Serial0:23 is up, line protocol is up (spoofing)
  Hardware is DSX1
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set
  DTR is pulsed for 1 seconds on reset
  Last input 00:00:12, output 00:00:12, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
    Conversations 0/1/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
    937 packets input, 19612 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 2 giants, 0 throttles
    2 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    945 packets output, 4263 bytes, 0 underruns
    0 output errors, 0 collisions, 4 interface resets
    0 output buffer failures, 0 output buffers swapped out
    3 carrier transitions
  Timeslot(s) Used:24, Transmitter delay is 0 flags
  
```

---

**Note** The packet counters shown by the **interface serial 0:23** command are for signaling traffic only. Data traffic passes through S0:0 through S0:22.

---





```

!
interface Serial1:23
  no ip address
  no ip directed-broadcast
  isdn incoming-voice modem
!
interface Serial2:23
  no ip address
  no ip directed-broadcast
  isdn incoming-voice modem
!
interface Serial3:23
  no ip address
  no ip directed-broadcast
  isdn incoming-voice modem
!
---- snip ----

```

### Tips

If you have trouble:

- Be sure you have the correct ISDN switch type configured.
- Make sure no wires or cables are loose.
- The framing or line code types you entered might not match your telco’s settings. A Layer 2 error indicates that the access server cannot communicate with the telco.
- Make sure the **show controller t1** command’s current output shows no errors occurring.

## Step 6—Configuring the Modems and Lines

Modems and lines are configured after the ISDN channels are operational, and voice calls are successfully routed to the modems. Each modem is directly mapped to a dedicated async line in the access server. After this configuration is set up, the access server is ready to take modem calls.

The modem speed 115200 bps and hardware flow control are the defaults for integrated modems.

### Configure

To configure the modems and asynchronous lines, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	hq-sanjose(config)# <b>line 1 96</b>	Enter the range of modem lines to configure. In this example, the access server has 96 integrate modems.
2	hq-sanjose(config-line)# <b>autoselect ppp</b> hq-sanjose(config-line)# <b>autoselect during-login</b>	Enable remote PPP users to dial in, bypass the EXEC facility, and automatically launch PPP on the line. <sup>1</sup> Enter the <b>autoselect during-login</b> command to display the username:password prompt after modems connect.
3	hq-sanjose(config-line)# <b>modem inout</b>	Support incoming and outgoing modem calls.

1. These two autoselect commands provide for transparent launching of shell and PPP services on the same lines.

## Verify

Enter the **show running** command to verify the configuration:

```
hq-sanjose# show running
Building configuration...
Current configuration:

---- snip ----
!
line 1 96
  autoselect during-login
  autoselect ppp
  modem InOut
---- snip ----
```

## Step 7—Testing Async Shell Connections

Now you are ready to send the first modem call into the Cisco AS5300. This step shows you how to perform the test and track the async data path taken by a single modem call.

Conduct this test using a shell service, which verifies that the physical async data path is working. This is the most efficient way to get quick test results in a simple test environment.

At this step, many administrators try to make complex services work such as PPP-based Web browsing. Do not jump ahead. Many other elements still need to be configured. This step is provided to ensure that the basic modem link is functioning and that the shell/EXEC prompt can be accessed from a remote location. To avoid problems, take a layered approach to building a network.

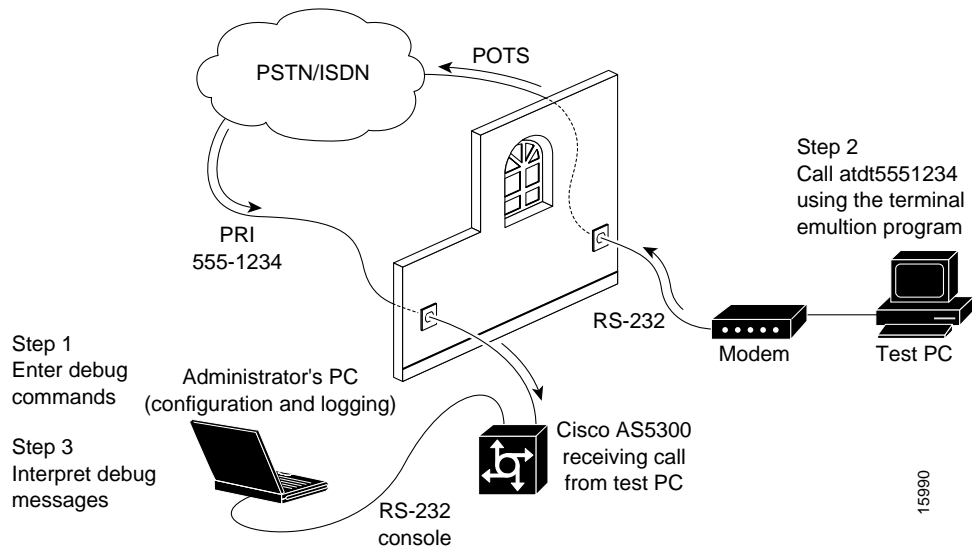
---

**Note** To enhance readability of debug output messages, the significant display output fields are highlighted with **bold** font.

---

Figure 2-3 shows the test lab environment used for this test case. The test PC is running a terminal emulation program, such as Hyper Terminal. This program enables the test PC to make a modem-to-modem connection with the Cisco AS5300 via the PSTN/ISDN network.

Figure 2-3 Test Lab Environment



**Step 1** Enter the following debug commands on the Cisco AS5300 to debug calls landing on the integrated modems. These commands capture the call-switching module and ISDN connection messages. After you are finished with the test, turn off all debugging with the **undebg all** command.

```

hq-sanjose# debug modem csm
Modem Management Call Switching Module debugging is on
hq-sanjose# debug isdn q931
ISDN Q931 packets debugging is on
hq-sanjose# terminal monitor
% Console already monitors
    
```

---

**Note** The ISDN Q.931 messages display call information coming into the access server. The modem call switching module captures the calls getting routed to the internal modems. The terminal monitor ensures that your EXEC session is receiving the logging and debug output.

---

**Step 2** From a terminal emulation program running on the test PC, enter **atdt** followed by the primary rate interface (PRI) phone number assigned to the Cisco AS5300. In this case test, 5551234 is used.

If the modem successfully connects, you will see a connect message followed by the terminal service EXEC login prompt. This is displayed on the test PC.

```

atdt5551234
CONNECT 24000/REL - MNP

User Access Verification
Username: joe-admin
Password: joe-password

hq-sanjose>
    
```

---

**Note** The modem attached to the test PC sends out “CONNECT 24000/REL - MNP” The Cisco AS5300 sends out “User Access Verification,” “Username:,” and “Password:.” These messages are confirmation that you have end-to-end async shell connectivity.

---

**Step 3** For educational purposes, look at and interpret the debug messages that appear on the administrator’s terminal screen as a result of Step 2. As the modem call came into the access server, this debug output was created.

The following comments apply to the debug output example:

- (a) See 20:43:35.906 through 20:43:35.918.  
The setup message is received. The bearer capability is a voice call as indicated by 0x8090A2. The calling party number is 5551111, the test PC’s phone number. The called party number is 5551234, the access server’s dialed hunt group number.
- (b) See 20:43:35.938.  
Modem 1/1 is assigned to the incoming voice call.
- (c) See 20:43:36.754 and 20:43:36.782.  
The call successfully connects as indicated by the fields “TX -> CONNECT” and “RX <- CONNECT\_ACK.”
- (d) See 20:43:36.806.  
The integrated modem waits to negotiate carrier with the remote modem.

```
*Mar 1 20:43:35.906: ISDN Se0:23: RX <- SETUP pd = 8 callref = 0x0001
*Mar 1 20:43:35.906: Bearer Capability i = 0x8090A2
*Mar 1 20:43:35.910: Channel ID i = 0xA98381
*Mar 1 20:43:35.914: Calling Party Number i = '!', 0x80, '5551111'
*Mar 1 20:43:35.918: Called Party Number i = 0xA1, '5551234'
*Mar 1 20:43:35.934: EVENT_FROM_ISDN:dchan_idb=0x27C878, call_id=0xB, ces=0x1
    bchan=0x0, event=0x1, cause=0x0
*Mar 1 20:43:35.938: VDEV_ALLOCATE: slot 1 and port 1 is allocated.
*Mar 1 20:43:35.938: EVENT_FROM_ISDN:(000B): DEV_INCALL at slot 1 and port 1
*Mar 1 20:43:35.942: CSM_PROC_IDLE: CSM_EVENT_ISDN_CALL at slot 1, port 1
*Mar 1 20:43:35.946: Fast Ringing On at modem slot 1, port 1
*Mar 1 20:43:35.966: ISDN Se0:23: TX -> CALL_PROC pd = 8 callref = 0x8001
*Mar 1 20:43:35.970: Channel ID i = 0xA98381
*Mar 1 20:43:35.978: ISDN Se0:23: TX -> ALERTING pd = 8 callref = 0x8001
*Mar 1 20:43:36.742: Fast Ringing Off at modem slot 1, port 1
*Mar 1 20:43:36.742: CSM_PROC_IC1_RING: CSM_EVENT_MODEM_OFFHOOK at slot 1, port
1
*Mar 1 20:43:36.754: ISDN Se0:23: TX -> CONNECT pd = 8 callref = 0x8001
*Mar 1 20:43:36.782: ISDN Se0:23: RX <- CONNECT_ACK pd = 8 callref = 0x0001
*Mar 1 20:43:36.798: EVENT_FROM_ISDN:dchan_idb=0x27C878, call_id=0xB, ces=0x1
    bchan=0x0, event=0x4, cause=0x0
*Mar 1 20:43:36.802: EVENT_FROM_ISDN:(000B): DEV_CONNECTED at slot 1 and port 1
*Mar 1 20:43:36.806: CSM_PROC_IC4_WAIT_FOR_CARRIER: CSM_EVENT_ISDN_CONNECTED at
slot 1, port 1
```

Every Q.931 message indicates whether the message was transmitted by the access server (TX ->) or received by the access server (RX <-). Table 2-2 shows the most common message types used for opening and closing connections. Information elements exist within each message type, as described in Table 2-3.

**Table 2-2 Debug Q.931 ISDN Messages**

Message Type	Description
SETUP	Indicates that a SETUP message has been received to initiate call establishment between PSTN end devices.  A key element to observe within the call setup message is the bearer capability.
CALL_PROC	Call proceeding. The network attempts to service the call. The switch is attempting to set up a call through the ISDN network backbone.
CONNECT	The called side transmits "CONNECT" when the connection is made. The side that transmits "CONNECT" is usually the side that receives the call, which is the called party.
CONNECT_ACK	Connect acknowledgment. Transmitted by the calling side to indicate that the "CONNECT" message was received.
DISCONNECT	Indicates that the transmitting side is ending the call. This messages indicates who dropped the call.
RELEASE	Indicates that the sending equipment is releasing the call and the associated channel.
RELEASE_COMP	Release complete. Indicates that the ISDN network has received the "RELEASE" message.

ISDN setup messages contain different information elements. See Table 2-3.

**Table 2-3 Information Elements within an ISDN Setup Message**

Message	Description
Bearer Capability	Indicates what kind of service the caller is requesting. For example, a 64K data call is indicated by the bearer capability of 0x8890. An analog voice call is indicated by the value 0x8090A2.
pd	Indicates the protocol discriminator number, which is 8 for Q.931 messages.
callref	A number used by the access server and the switch to reference the call. Indicates the call reference number in hexadecimal format. The field value indicates the number of calls made from the router (outgoing calls) or the network (incoming calls). Note that the originator of the SETUP message sets the high-order bit of the call reference number to 0.  The destination of the connection sets the high-order bit to 1 in subsequent call control messages, such as the CONNECT message. For example, callref = 0x04 in the request becomes callref = 0x84 in the response.
Cause i	Indicates the Information Element Identifier. The value depends on the field with which it is associated. Refer to the ITU-T Q.931 specification for details about the possible values associated with each field for which this identifier is relevant.
Channel ID	Indicates the Channel Identifier. The value 83 indicates any channel, 89 indicates the B1 channel, and 8A indicates the B2 channel. For more information about the Channel Identifier, refer to ITU-T Recommendation Q.931.
Calling Party Number	Identifies the phone number of the device that initiated the call.  In this case study, 5551111 is the directory number assigned to the telephone line used by the test PC.

**Table 2-3 Information Elements within an ISDN Setup Message (Continued)**

Message	Description
Called Party Number	Identifies the called phone number that is used to reach another device. In this case study, 5551234 is the directory number assigned to the Cisco AS5300. The test PC dialed this number to make a modem connection.

**Step 4** To determine the status of the modem call connected to the Cisco AS5300, use the following modem management commands.

- Enter the **show user** command to see which TTY line the call landed on:

```
hq-sanjose# show user
  Line      User      Host(s)      Idle Location
*  0 con 0   joe-admin   idle         0
  2 tty 2   joe-admin   Async interface 1
```

- Enter the **show line 2** command. Note that TTY 2 is associated with modem 1/1. The state is currently idle because this command was entered after the user disconnected.

```
hq-sanjose# show line 2
Tty Typ      Tx/Rx      A Modem  Roty AccO AccI  Uses   Noise  Overruns
  2 TTY 115200/115200 - inout   - - -    0      0      0/0

Line 2, Location: "", Type: ""
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 115200/115200, no parity, 1 stopbits, 8 databits
Status: No Exit Banner
Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out
Modem Callout, Modem RI is CD
Modem state: Idle
modem(slot/port)=1/1, state=IDLE
dsxl(slot/unit/channel)=NONE, status=VDEV_STATUS_UNLOCKED
Group codes: 0
Modem hardware state: CTS noDSR DTR RTS
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
                00:00:30
                Autoselect Initial Wait
Tty Typ      Tx/Rx      A Modem  Roty AccO AccI  Uses   Noise  Overruns
                not set

Modem type is unknown.
Session limit is not set.
Time since activation: never
Editing is enabled.
History is enabled, history size is 10.
DNS resolution in show commands is enabled
Full user help is disabled
Allowed transports are lat pad telnet rlogin v120. Preferred is lat.
No output characters are padded
No special data dispatching characters
```

- Enter the **show modem log 1/1** command to view the information logged for modem 1/1. The time stamps show when the event occurred. The most current events begin at the bottom of the output.

```

hq-sanjose# show modem log 1/1
Modem 1/1 Events Log:
 20:40:45: Startup Response: Microcom (Managed)
           Modem (boot) firmware = 2.2(8) (1.0(5))
---- snip ----
00:02:19: ISDN incoming calling number: 5551111
00:02:19: ISDN incoming called number: 5551234
00:02:13: Modem State event: Dialing/Answering
00:02:13: Modem State event: Incoming ring
00:02:13: Modem State event: Waiting for Carrier
00:02:13: RS232 event: RTS DTR CTS DSR noDCD noRI* noTST
00:02:01: Modem State event: Connected
00:02:01: Connection event: TX/RX Speed = 33600/33600, Modulation = V34
           Direction = Answer, Protocol = reliable/LAPM, Compression = V42bis
00:02:02: RS232 event: RTS DTR CTS DSR DCD* noRI noTST
00:01:50: Modem Analog signal event: TX = -21, RX = -18, Signal to noise = 43
00:00:15: DTR event: DTR Off
00:00:15: Modem State event: Connected
00:00:15: End connection event: Retransmits for EC block (TX/RX) = 0/0
           Duration = 0:01:43, Number of TX/RX char = 159/0
           Local Disc Reason = DTR Drop
           Remote Disc Reason = Unknown
00:00:15: Modem State event: Disconnecting
00:00:15: DTR event: DTR On
00:00:15: RS232 event: RTS DTR* CTS* DSR* noDCD* noRI* noTST*

```

- Enter the **show modem** command. In the following example, the current active call is on modem 1/1, which is functioning properly at 100%. An active call is indicated by an asterisk (\*).

```

hq-sanjose# show modem

```

Mdm	Usage	Inc calls		Out calls		Busied Out	Failed Dial	No Answer	Succ Pct.
		Succ	Fail	Succ	Fail				
1/0	0%	0	0	0	0	0	0	0	0%
* 1/1	0%	1	0	0	0	0	0	0	100%
1/2	0%	0	0	0	0	0	0	0	0%
1/3	0%	0	0	0	0	0	0	0	0%
1/4	0%	0	0	0	0	0	0	0	0%
1/5	0%	0	0	0	0	0	0	0	0%
1/6	0%	0	0	0	0	0	0	0	0%
1/7	0%	0	0	0	0	0	0	0	0%
1/8	0%	0	0	0	0	0	0	0	0%
1/9	0%	0	0	0	0	0	0	0	0%
1/10	0%	0	0	0	0	0	0	0	0%
1/11	0%	0	0	0	0	0	0	0	0%

```

---- snip -----

```

- Enter the **show controller t1 0 call-counters** command, which shows you the DS0 timeslot used to carry the modem call. This example shows that timeslot 1 has accepted one call for a total duration of 1 minute 30 seconds.

```
hq-sanjose# show controller t1 0 call-counters
T1 0:
DS0's Active: 0
DS0's Active High Water Mark: 0
TimeSlot  Type  TotalCalls  TotalDuration
  1         pri         1         00:01:30
  2         pri         0         00:00:00
  3         pri         0         00:00:00
  4         pri         0         00:00:00
  5         pri         0         00:00:00
  6         pri         0         00:00:00
  7         pri         0         00:00:00
  8         pri         0         00:00:00
  9         pri         0         00:00:00
 10        pri         0         00:00:00
 11        pri         0         00:00:00
 12        pri         0         00:00:00
 13        pri         0         00:00:00
 14        pri         0         00:00:00
 15        pri         0         00:00:00
 16        pri         0         00:00:00
 17        pri         0         00:00:00
 18        pri         0         00:00:00
 19        pri         0         00:00:00
 20        pri         0         00:00:00
 21        pri         0         00:00:00
 22        pri         0         00:00:00
 23        pri         0         00:00:00
Total DS0's Active High Water Mark: 0
```

- To further troubleshoot modem problems, connect to a modem’s out-of-band management port. For Microcom modems, use the **modem at-mode slot/port** command. For MICA modems, use the **show modem operational-status slot/port** command and the **show modem configuration slot/port** command.

```

hq-sanjose# modem at-mode 2/15
You are now entering AT command mode on modem (slot 2 / port 15).
Please type CTRL-C to exit AT command mode.
at@e1
    
```

```

MNP Class 10 K56flex Modem
MODEM HW: OEM 2W United States
Firmware Rev 3.3.20/85
Bootstrap Rev 3.0.4
DSP C36 Part/Rev          3635 4241
DSP C58 Part/Rev          3635 2041
DSP Controller Rev      42
DSP Data Pump Rev         4.2
NET ADDR:      FFFFFFFF
Connect Time          000:06:41
4 RTS 5 CTS 6 DSR 8 CD 20 DTR - RI
Disconnect Remote - Local -

Mod Type                V.34
TX/RX Spd              24000 26400 BPS
TX/RX Spd Mask          NA BFFF Hex
Symbol Rate             3200 Hz
TX/RX Carrier Freq      1829 1829 Hz
TX/RX States            16 16
TX/RX NLE               ON ON
TX/RX Precoding         ON ON
TX/RX Shaping           ON ON
TX Preemphasis Index    0

TX Lvl REG              - 13 dBm
TX Lvl RAM              - 0 dB
TX Lvl Reduct           1 dB
TX Lvl                  - 14 dBm
RX Lvl                  - 19 dBm
S/NR                    42
S/DR                    0
EQM                     1C00 Hex
AVG EQM                 19BE Hex
Lower/Upper Edge        150 3675 Hz
Phase Jitter Freq       139 Hz
Phase Jitter Amp        0.0 deg
Far Echo Lvl            138 N
Round Trip Delay         0 msec
Dropouts > 5dB         0
RTRNs Init/Accept       0 0
RRENs Init/Accept       0 0
BLER                    0000 Hex
RBS Counter              0000 Hex
Digital Pad Detected     0 dB
Max SECRXB              67
Max SECTXB              67
V8BIS STATUS            NAK
    
```

OK

## Step 8—Setting Up IP Address Pools

Create a pool of IP address to support remote nodes dialing in. As remote node devices connect, they request an IP address from the central site.

It is important to determine how your intranet/Internet backbone will route packets to the addresses in this pool. There are several ways to do this, such as using addresses off a subnet defined on the access server (for example, on the loopback or Ethernet interface).

---

**Note** Administrators commonly create a loopback interface and new subnet if their existing Ethernet subnet has all its IP addresses already consumed. Loopback interfaces are very stable and do not go up and down as LAN interfaces may.

---

## Configure

To set up the address pool, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	hq-sanjose(config)# <b>interface loopback 0</b>	Create loopback interface 0.
2	hq-sanjose(config-if)# <b>ip address 10.1.2.1 255.255.255.0</b>	Assign an IP subnet and address to loopback 0. This subnet is used for the creation of your IP address pool <sup>1</sup> .
3	hq-sanjose(config-if)# <b>exit</b>	Exit back to global configuration mode.
4	hq-sanjose(config)# <b>ip local pool dialin_pool 10.1.2.2 10.1.2.97</b>	Create a pool of IP addresses for assigning to the remote nodes <sup>2</sup> .
5	hq-sanjose(config)# <b>async-bootp dns-server 10.2.2.3 10.2.3.1</b>	Specify the domain name servers on the network, which can be used for clients dialing in with PPP.

1. This subnet is now dedicated to this Cisco AS5300 for remote node support. This subnet cannot be used in other places in your network.
2. A remote LAN is typically a router that has a next hop address and its own IP subnet. It also requires IP routing support from the backbone, which is commonly accomplished with a static IP route. A remote node gets an IP address out of a central pool of IP addresses. Remote LANs and remote nodes are primarily differentiated by this IP addressing scheme. Remote LANs can appear as remote nodes by using PAT.

## Verify

Enter the **show ip local pool** command to verify the configuration:

```
hq-sanjose# show ip local pool
Pool          Begin          End            Free   In use   Cache Size
dialin_pool   10.1.2.2      10.1.2.97     96     0       20
```

## Step 9—Configuring the Group-Async Interface

The group-async interface is a template, which is used to control the configuration of all the async interfaces on the access server. Async interfaces are lines that are running in PPP mode. An async interface uses the same number as its corresponding line. Configuring the asynchronous interfaces as a group-async saves you time and configuration file size.

### Configure

To configure the group-async interface, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	hq-sanjose(config)# <b>interface group-async 1</b>	Create the group-async interface.
2	hq-sanjose(config-if)# <b>ip unnumbered loopback 0</b>	To conserve IP address space, configure the asynchronous interfaces as unnumbered.
3	hq-sanjose(config-if)# <b>encapsulation ppp</b>	Enable PPP.
4	hq-sanjose(config-if)# <b>async mode interactive</b>	Configure interactive mode on the asynchronous interfaces. Interactive means that users can dial in and get to a shell or PPP session on that line.
5	hq-sanjose(config-if)# <b>ppp authentication chap pap</b>	Enable CHAP and PAP authentication on the interface during LCP negotiation.  The access server first requests to authenticate with CHAP. If CHAP is rejected by the remote client (modem), then PAP authentication is requested.
6	hq-sanjose(config-if)# <b>peer default ip address pool dialin_pool</b>	Assign dial-in clients IP addresses from the pool named dialin_pool.
7	hq-sanjose(config-if)# <b>no cdp enable</b>	Disable the Cisco discovery protocol.
8	hq-sanjose(config-if)# <b>group-range 1 96</b>	Specify the range of asynchronous interfaces to include in the group, which is usually equal to the number of modems you have in the access server.

### Verify

Enter the **show running** command. After completing Steps 1 through 9, the configuration looks like this:

```
hq-sanjose# show running
Building configuration...
Current configuration:
!
version 12.0
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname hq-sanjose
!
aaa new-model
aaa authentication login default local
```

```
aaa authentication ppp default if-needed local
enable secret 5 $1$.voA$9/8.Zo1l3jeWJMP6hEE6U0
!
username joe-admin password 7 <removed>
!
async-bootp dns-server 10.2.2.3 10.2.3.1
isdn switch-type primary-ni
!
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 1
 framing esf
 clock source line secondary
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 2
 framing esf
 clock source internal
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 3
 framing esf
 clock source internal
 linecode b8zs
 pri-group timeslots 1-24
!
interface Loopback0
 ip address 10.1.2.1 255.255.255.0
 no ip directed-broadcast
!
interface Ethernet0
 no ip address
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 shutdown
!
interface Serial0:23
 no ip address
 no ip directed-broadcast
 isdn incoming-voice modem
 no fair-queue
 no cdp enable
!
interface Serial1:23
 no ip address
 no ip directed-broadcast
 isdn incoming-voice modem
 no fair-queue
 no cdp enable
!
interface Serial2:23
 no ip address
 no ip directed-broadcast
 isdn incoming-voice modem
 no fair-queue
 no cdp enable
```

## Step 9—Configuring the Group-Async Interface

---

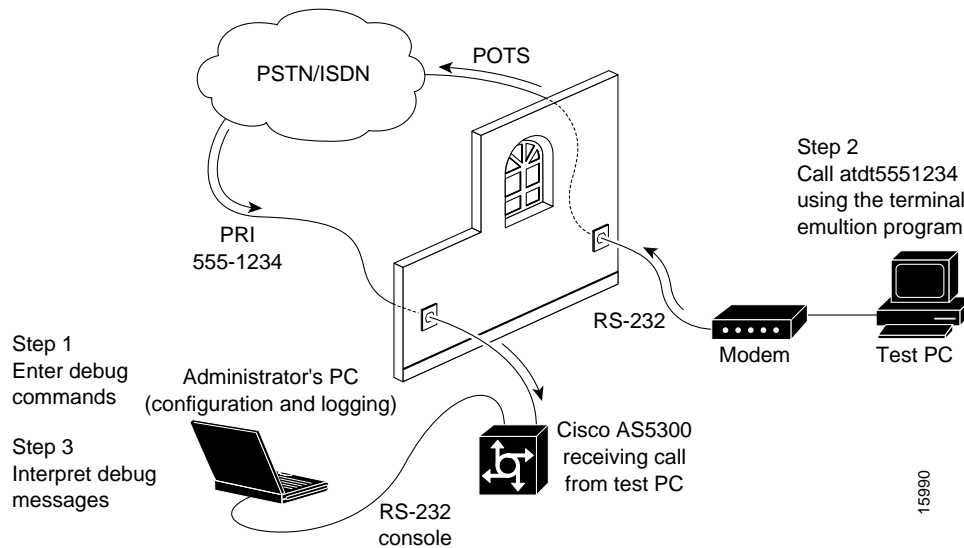
```
!  
interface Serial3:23  
  no ip address  
  no ip directed-broadcast  
  isdn incoming-voice modem  
  no fair-queue  
  no cdp enable  
!  
interface FastEthernet0  
  ip address 10.1.1.10 255.255.255.0  
  no ip directed-broadcast  
  no ip route-cache  
  no ip mroute-cache  
  duplex auto  
  speed auto  
!  
interface Group-Async1  
  ip unnumbered Loopback0  
  no ip directed-broadcast  
  encapsulation ppp  
  async mode interactive  
  peer default ip address pool dialin_pool  
  no cdp enable  
  ppp authentication chap pap  
  group-range 1 96  
!  
ip local pool dialin_pool 10.1.2.2 10.1.2.97  
!  
!  
line con 0  
line 1 96  
  autoselect during-login  
  autoselect ppp  
  modem InOut  
line aux 0  
line vty 0 4  
!  
end
```

## Step 10—Testing Async PPP Connections

Now you are ready to send the first async PPP modem call into the Cisco AS5300. This step provides you with a picture of the test lab followed by debug output for a successful connection.

Figure 2-3 shows the test lab environment used for this test. A test PC makes a PPP modem-to-modem connection with the Cisco AS5300 via the PSTN/ISDN network.

**Figure 2-4 Test Lab Environment**



**Step 1** Enter the following debugging commands on the Cisco AS5300:

```

hq-sanjose# debug ppp negotiation
PPP protocol negotiation debugging is on
hq-sanjose# debug ppp authentication
PPP authentication debugging is on
hq-sanjose# debug modem
Modem control/process activation debugging is on
hq-sanjose# debug ip peer
IP peer address activity debugging is on

hq-sanjose# show debug
General OS:
  Modem control/process activation debugging is on
Generic IP:
  IP peer address activity debugging is on
PPP:
  PPP authentication debugging is on
  PPP protocol negotiation debugging is on

hq-sanjose# terminal monitor

```

- Step 2** From a terminal emulation program running on the test PC, enter **atdt** followed by the telephone number assigned to the Cisco AS5300. In this case test, 5551234 is used.

```
atdt5551234
CONNECT 24000/REL - MNP

User Access Verification
Username: joe-admin
Password: joe-password

hq-sanjose>
```

- Step 3** Interpret the debug messages that appear on the administrator's terminal screen as a result of Step 2. As the modem call comes into the access server, debug output is created.

---

**Note** When examining PPP between two remote peers, first check to see if both sides get through LCP negotiation. If they do, move on to check authentication. After authentication is successful, check IPCP negotiation.

---

The following comments apply to the debug output example, which spans over the next few pages. Locate the time stamps in the debug output then interpret the call behavior.

- (a) See 21:34:56.958.  
A modem call comes into the access server on TTY line 4.
- (b) See 21:34:59.722 through 21:34:59.734.  
An incoming PPP frame is recognized, so PPP is launched on TTY line 4.
- (c) See 21:34:59.790.  
The test PC gets assigned an IP address from the address pool set up on the access server. The address is 10.1.2.2.
- (d) See 21:35:01.798.  
Interface async 4 comes up. After PPP launches, TTY line 4 becomes async interface 4.
- (e) See 21:35:02.718.  
Incoming config request (I CONFREQ). The remote test PC requests a set of options to be negotiated. The PC asks the Cisco AS5300 to support the callback option.
- (f) See 21:35:02.738.  
Outgoing config reject (O CONFREJ). The Cisco AS5300 rejects this option, because the access server is not configured to support Microsoft Callback in this case study.
- (g) See 21:35:02.850.  
Incoming config request (I CONFREQ). The test PC requests a new set of options.
- (h) See 21:35:02.862.  
Outgoing config acknowledgment (O CONFACK). The Cisco AS5300 accepts the new set of options.
- (i) See 21:35:03.978.  
LCP is now open (LCP: State is Open). Both sides have acknowledged (CONFACK) the other side's configuration request (CONFREQ).

- (j) See 21:35:03.978.  
After LCP negotiates, authentication starts. Authentication must happen before any network protocols, such as IP, are delivered. Both sides authenticate with the method negotiated during LCP. The Cisco AS5300 is authenticating the test PC using CHAP. The test PC is not authenticating the access server in this test case.
- (k) See 21:35:03.982.  
Outgoing challenge from hq-sanjose.
- (l) See 21:35:04.162.  
Incoming CHAP response from the test PC, which shows the username joe-admin.
- (m) See 21:35:04.182.  
An outgoing success is sent from the NAS—authentication is successful.
- (n) See 21:35:04.186.  
PPP is up. The Cisco AS5300 PPP link is now open and available to negotiate any network protocols supported by both peers.
- (o) See 21:35:04.314 through 21:35:04.322.  
The test PC requests support for Microsoft Point-to-Point Compression (MPPC). The Cisco AS5300 rejects this request. The access server's integrated modems already support hardware compression, and the Cisco IOS is not configured to support software compression.
- (p) See 21:35:07.274 through 21:35:07.478.  
The primary and secondary DNS addresses are negotiated. At first, the test PC asks for 0.0.0.0 addresses. The access server sends out a CONFNAK and supplies the correct values. Values include an IP address from the pool, the primary DNS address, and the backup DNS address.
- (q) See 21:35:07.426.  
The test PC sends an incoming request saying that the new values are accepted. Whenever the access server sends out a CONFNAK that includes values, the test PC still needs to come back and report acceptance of the new values.
- (r) See 21:35:07.458 through 21:35:07.490.  
An outgoing CONFACK is sent for IPCP. The state is open for IPCP. A route is negotiated for the IPCP peer, which is 10.1.2.2.

---

**Note** To enhance readability of debug output messages, significant display output fields are highlighted with **bold font**.

---

```

hq-sanjose#
*Mar 1 21:34:56.958: TTY4: DSR came up
*Mar 1 21:34:56.962: TTY4: Modem: IDLE->READY
*Mar 1 21:34:56.970: TTY4: EXEC creation
*Mar 1 21:34:56.978: TTY4: set timer type 10, 30 seconds
*Mar 1 21:34:59.722: TTY4: Autoselect(2) sample 7E
*Mar 1 21:34:59.726: TTY4: Autoselect(2) sample 7EFF
*Mar 1 21:34:59.730: TTY4: Autoselect(2) sample 7EFF7D
*Mar 1 21:34:59.730: TTY4: Autoselect(2) sample 7EFF7D23
*Mar 1 21:34:59.734: TTY4 Autoselect cmd: ppp negotiate
*Mar 1 21:34:59.746: TTY4: EXEC creation
*Mar 1 21:34:59.746: TTY4: create timer type 1, 600 seconds
*Mar 1 21:34:59.786: ip_get_pool: As4: using pool default
*Mar 1 21:34:59.790: ip_get_pool: As4: returning address = 10.1.2.2
*Mar 1 21:34:59.794: TTY4: destroy timer type 1 (OK)
*Mar 1 21:34:59.794: TTY4: destroy timer type 0
*Mar 1 21:35:01.798: %LINK-3-UPDOWN: Interface Async4, changed state to up
*Mar 1 21:35:01.834: As4 PPP: Treating connection as a dedicated line
*Mar 1 21:35:01.838: As4 PPP: Phase is ESTABLISHING, Active Open
*Mar 1 21:35:01.842: As4 LCP: O CONFREQ [Closed] id 1 len 25
*Mar 1 21:35:01.846: As4 LCP: ACCM 0x000A0000 (0x0206000A0000)
*Mar 1 21:35:01.850: As4 LCP: AuthProto CHAP (0x0305C22305)
*Mar 1 21:35:01.854: As4 LCP: MagicNumber 0x64E923A8 (0x050664E923A8)
*Mar 1 21:35:01.854: As4 LCP: PFC (0x0702)
*Mar 1 21:35:01.858: As4 LCP: ACFC (0x0802)
*Mar 1 21:35:02.718: As4 LCP: I CONFREQ [REQsent] id 3 len 23
*Mar 1 21:35:02.722: As4 LCP: ACCM 0x000A0000 (0x0206000A0000)
*Mar 1 21:35:02.726: As4 LCP: MagicNumber 0x00472467 (0x050600472467)
*Mar 1 21:35:02.726: As4 LCP: PFC (0x0702)
*Mar 1 21:35:02.730: As4 LCP: ACFC (0x0802)
*Mar 1 21:35:02.730: As4 LCP: Callback 6 (0x0D0306)
*Mar 1 21:35:02.738: As4 LCP: O CONFREQ [REQsent] id 3 len 7
*Mar 1 21:35:02.738: As4 LCP: Callback 6 (0x0D0306)
*Mar 1 21:35:02.850: As4 LCP: I CONFREQ [REQsent] id 4 len 20
*Mar 1 21:35:02.854: As4 LCP: ACCM 0x000A0000 (0x0206000A0000)
*Mar 1 21:35:02.854: As4 LCP: MagicNumber 0x00472467 (0x050600472467)
*Mar 1 21:35:02.858: As4 LCP: PFC (0x0702)
*Mar 1 21:35:02.858: As4 LCP: ACFC (0x0802)
*Mar 1 21:35:02.862: As4 LCP: O CONFACK [REQsent] id 4 len 20
*Mar 1 21:35:02.866: As4 LCP: ACCM 0x000A0000 (0x0206000A0000)
*Mar 1 21:35:02.870: As4 LCP: MagicNumber 0x00472467 (0x050600472467)
*Mar 1 21:35:02.870: As4 LCP: PFC (0x0702)
*Mar 1 21:35:02.874: As4 LCP: ACFC (0x0802)
*Mar 1 21:35:03.842: As4 LCP: TIMEout: State ACKsent
*Mar 1 21:35:03.842: As4 LCP: O CONFREQ [ACKsent] id 2 len 25
*Mar 1 21:35:03.846: As4 LCP: ACCM 0x000A0000 (0x0206000A0000)
*Mar 1 21:35:03.850: As4 LCP: AuthProto CHAP (0x0305C22305)
*Mar 1 21:35:03.854: As4 LCP: MagicNumber 0x64E923A8 (0x050664E923A8)
*Mar 1 21:35:03.854: As4 LCP: PFC (0x0702)
*Mar 1 21:35:03.858: As4 LCP: ACFC (0x0802)
*Mar 1 21:35:03.962: As4 LCP: I CONFACK [ACKsent] id 2 len 25
*Mar 1 21:35:03.966: As4 LCP: ACCM 0x000A0000 (0x0206000A0000)
*Mar 1 21:35:03.966: As4 LCP: AuthProto CHAP (0x0305C22305)
*Mar 1 21:35:03.970: As4 LCP: MagicNumber 0x64E923A8 (0x050664E923A8)
*Mar 1 21:35:03.974: As4 LCP: PFC (0x0702)
*Mar 1 21:35:03.974: As4 LCP: ACFC (0x0802)
*Mar 1 21:35:03.978: As4 LCP: State is Open
*Mar 1 21:35:03.978: As4 PPP: Phase is AUTHENTICATING, by this end
*Mar 1 21:35:03.982: As4 CHAP: O CHALLENGE id 1 len 26 from "hq-sanjose"

```

```

*Mar 1 21:35:04.162: As4 CHAP: I RESPONSE id 1 len 26 from "joe-admin"
*Mar 1 21:35:04.170: As4 AUTH: Started process 0 pid 47
*Mar 1 21:35:04.182: As4 CHAP: O SUCCESS id 1 len 4
*Mar 1 21:35:04.186: As4 PPP: Phase is UP
*Mar 1 21:35:04.190: As4 IPCP: O CONFREQ [Not negotiated] id 1 len 10
*Mar 1 21:35:04.194: As4 IPCP: Address 10.1.2.1 (0x03060A010201)
*Mar 1 21:35:04.282: As4 IPCP: I CONFREQ [REQsent] id 1 len 28
*Mar 1 21:35:04.282: As4 IPCP: CompressType VJ 15 slots CompressSlotID (0x02
06002D0F01)
*Mar 1 21:35:04.286: As4 IPCP: Address 0.0.0.0 (0x030600000000)
*Mar 1 21:35:04.290: As4 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar 1 21:35:04.298: As4 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar 1 21:35:04.306: As4 IPCP: O CONFREQ [REQsent] id 1 len 10
*Mar 1 21:35:04.310: As4 IPCP: CompressType VJ 15 slots CompressSlotID (0x02
06002D0F01)
*Mar 1 21:35:04.314: As4 CCP: I CONFREQ [Not negotiated] id 1 len 15
*Mar 1 21:35:04.318: As4 CCP: MS-PPC supported bits 0x00000001 (0x1206000000
01)
*Mar 1 21:35:04.318: As4 CCP: Stacker history 1 check mode EXTENDED (0x11050
00104)
*Mar 1 21:35:04.322: As4 LCP: O PROTREQ [Open] id 3 len 21 protocol CCP
*Mar 1 21:35:04.326: As4 LCP: (0x80FD0101000F120600000000111050001)
*Mar 1 21:35:04.330: As4 LCP: (0x04)
*Mar 1 21:35:04.334: As4 IPCP: I CONFACK [REQsent] id 1 len 10
*Mar 1 21:35:04.338: As4 IPCP: Address 10.1.2.1 (0x03060A010201)
*Mar 1 21:35:05.186: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async4, ch
anged state to up
*Mar 1 21:35:07.274: As4 IPCP: I CONFREQ [ACKrcvd] id 2 len 22
*Mar 1 21:35:07.278: As4 IPCP: Address 0.0.0.0 (0x030600000000)
*Mar 1 21:35:07.282: As4 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar 1 21:35:07.286: As4 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar 1 21:35:07.294: As4 IPCP: O CONFNAK [ACKrcvd] id 2 len 22
*Mar 1 21:35:07.298: As4 IPCP: Address 10.1.2.2 (0x03060A010202)
*Mar 1 21:35:07.302: As4 IPCP: PrimaryDNS 10.2.2.3 (0x81060A020203)
*Mar 1 21:35:07.310: As4 IPCP: SecondaryDNS 10.2.3.1 (0x83060A020301)
*Mar 1 21:35:07.426: As4 IPCP: I CONFREQ [ACKrcvd] id 3 len 22
*Mar 1 21:35:07.430: As4 IPCP: Address 10.1.2.2 (0x03060A010202)
*Mar 1 21:35:07.434: As4 IPCP: PrimaryDNS 10.2.2.3 (0x81060A020203)
*Mar 1 21:35:07.442: As4 IPCP: SecondaryDNS 10.2.3.1 (0x83060A020301)
*Mar 1 21:35:07.446: ip_get_pool: As4: validate address = 10.1.2.2
*Mar 1 21:35:07.450: ip_get_pool: As4: using pool default
*Mar 1 21:35:07.450: ip_get_pool: As4: returning address = 10.1.2.2
*Mar 1 21:35:07.454: set_ip_peer_addr: As4: address = 10.1.2.2 (3) is redundant
*Mar 1 21:35:07.458: As4 IPCP: O CONFACK [ACKrcvd] id 3 len 22
*Mar 1 21:35:07.462: As4 IPCP: Address 10.1.2.2 (0x03060A010202)
*Mar 1 21:35:07.466: As4 IPCP: PrimaryDNS 10.2.2.3 (0x81060A020203)
*Mar 1 21:35:07.474: As4 IPCP: SecondaryDNS 10.2.3.1 (0x83060A020301)
*Mar 1 21:35:07.478: As4 IPCP: State is Open
*Mar 1 21:35:07.490: As4 IPCP: Install route to 10.1.2.2

hq-sanjose# undebug all
All possible debugging has been turned off

```

---

**Note** After you finish testing, turn off all debugging with the **undebug all** command. Isolating the display of debug output helps you efficiently build a network. Debug only at the components that you have built so far.

---

## Step 11—Configuring DDR

Dial-on-demand routing (DDR) provides a mechanism to establish and maintain connectivity over a circuit switched network, such as the PSTN. DDR also supports remote LANs by maintaining IP routes to the remote sites when they are not connected.

### Configure

To configure the dialer interfaces, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	hq-sanjose(config)# <b>interface dialer 1</b> hq-sanjose(config-if)# <b>ip address 10.1.254.1 255.255.255.0</b>	Create interface dialer 1 and enable IP routing.
2	hq-sanjose(config-if)# <b>exit</b>	Exit back to global configuration mode.
3	hq-sanjose(config)# <b>interface serial 0:23</b> hq-sanjose(config-if)# <b>dialer rotary-group 1</b> hq-sanjose(config-if)# <b>exit</b>	Group serial 0's channels into dialer 1.
4	hq-sanjose(config)# <b>interface serial 1:23</b> hq-sanjose(config-if)# <b>dialer rotary-group 1</b> hq-sanjose(config-if)# <b>exit</b> hq-sanjose(config)# <b>interface serial 2:23</b> hq-sanjose(config-if)# <b>dialer rotary-group 1</b> hq-sanjose(config-if)# <b>exit</b> hq-sanjose(config)# <b>interface serial 3:23</b> hq-sanjose(config-if)# <b>dialer rotary-group 1</b> hq-sanjose(config-if)# <b>exit</b>	Group the remaining serial channels into dialer 1.
5	hq-sanjose(config)# <b>interface dialer 1</b>	Now with all the D channels grouped together, return to dialer 1.
6	hq-sanjose(config-if)# <b>encapsulation ppp</b>	Encapsulate the packets with PPP.
7	hq-sanjose(config-if)# <b>peer default ip address pool dialin_pool</b>	Assign an address pool to interface dialer 1. This step supports remote node ISDN devices, such as those running Easy IP and PAT <sup>1</sup> .
8	hq-sanjose(config-if)# <b>dialer in-band</b>	Specify that this is an in-band dialer interface, which enables passing the phone number across the D channel.
9	hq-sanjose(config-if)# <b>dialer idle-timeout 1800</b>	Configure the idle timeout, which is set to 1800 seconds (30 minutes) in this example <sup>2</sup> .
10	hq-sanjose(config-if)# <b>dialer-group 2</b>	Define the interesting packets, which are packets that reset the idle timer or trigger calls. This dialer filter is defined by the <b>dialer-list 2</b> command. See Step 17 <sup>3</sup> .
11	hq-sanjose(config-if)# <b>ppp multilink</b>	Enable PPP multilink, which fragments and reassembles packets among bundled B channels.
12	hq-sanjose(config-if)# <b>ppp authentication chap pap</b>	Enable CHAP and PAP authentication. CHAP is used first. PAP is the second choice.
13	hq-sanjose(config-if)# <b>no fair-queue</b>	Disable fair queuing.
14	hq-sanjose(config-if)# <b>no cdp enable</b>	Disable the Cisco discovery protocol, unless you are using it for a specific purpose.
15	hq-sanjose(config-if)# <b>no ip mroute-cache</b>	Turn off multicast route caching.

Step	Command	Purpose
16	hq-sanjose(config-if)# <b>exit</b>	Return to global configuration mode.
17	hq-sanjose(config)# <b>dialer-list 2 protocol ip permit</b>	Define a DDR dialer-list to allow any IP traffic to maintain the connection. Any IP packet will maintain the DDR session.  Minor or extensive tuning of your dialer list might be required to control costs in your environment. <sup>3</sup>

1. These users will also need a username and password.
2. Other environments might require shorter timeouts. The default is 120 seconds.
3. The **dialer-group** command and **dialer-list** command must use the same number. To monitor the idle timer value and the packets that reset it, use the **debug dialer packet** command and **show dialer** command.

## Verify

To verify the configuration:

- Enter the **show dialer** command. This command shows you the state associated with each IP interface. Notice that each individual serial channel is actually a dialer interface.

```
hq-sanjose# show dialer

Dialer1 - dialer type = IN-BAND SYNC NO-PARITY
Idle timer (1800 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)

Dial String      Successes   Failures    Last called   Last status

Serial0:0 - dialer type = ISDN
Idle timer (1800 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

Serial0:1 - dialer type = ISDN
Idle timer (1800 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

Serial0:2 - dialer type = ISDN
Idle timer (1800 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

----- snip -----
```

- Enter the **show running** command:

```
hq-sanjose# show running
Building configuration...
Current configuration:
!
----- snip -----
!
interface Serial0:23
 no ip address
 no ip directed-broadcast
 dialer rotary-group 1
 isdn incoming-voice modem
!
interface Serial1:23
```

```
no ip address
no ip directed-broadcast
dialer rotary-group 1
isdn incoming-voice modem
!
interface Serial2:23
no ip address
no ip directed-broadcast
dialer rotary-group 1
isdn incoming-voice modem
!
interface Serial3:23
no ip address
no ip directed-broadcast
dialer rotary-group 1
isdn incoming-voice modem
!
---- snip ----
!
interface Dialer1
ip address 10.1.254.1 255.255.255.0
no ip directed-broadcast
encapsulation ppp
no ip mroute-cache
dialer in-band
dialer idle-timeout 1800
dialer-group 2
peer default ip address pool dialin_pool
no fair-queue
no cdp enable
ppp authentication chap pap
ppp multilink
!
dialer-list 2 protocol ip permit
!
---- snip ----
```

## Step 12—Configuring Definitions for Remote LAN Sites

You must configure additional parameters to enable synchronous PPP services for the remote sites. Each remote site must have the following three entries configured on the Cisco AS5300:

- Username and password
- Static route
- Dialer map to support IP connectivity with the remote peer

Table 2-4 summarizes the critical parameters used by DDR, which works primarily at the addressing layer. These routes are stored in the routing table when the sites are not connected.

**Table 2-4 Site Characteristics**

Router Name	Password	WAN IP Address	Ethernet IP Address	Assigned Phone Number	Site Hardware
hq-sanjose	hq-sanjose-pw	10.1.254.1 255.255.255.0	10.1.1.10 255.255.255.0	4085551234	Cisco AS5300
soho-tahoe	tahoe-pw	10.1.254.3 255.255.255.0	10.1.3.1 255.255.255.0	5305558084	Cisco 766
robo-austin	austin-pw	10.1.254.4 255.255.255.0	10.1.4.1 255.255.255.0	5125554433	Cisco 1604

## Configure

To enable the remote LANs to dial into the Cisco AS5300, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	hq-sanjose(config)# <b>username robo-austin password austin-pw</b>	Specify the robo-austin username and password <sup>1</sup> .
2	hq-sanjose(config)# <b>ip route 10.1.4.0 255.255.255.0 10.1.254.4 permanent</b>	Enable IP routing for the robo-austin subnet.
3	hq-sanjose(config)# <b>username soho-tahoe password tahoe-pw</b>	Specify the soho-tahoe username and password <sup>1</sup> .
4	hq-sanjose(config)# <b>ip route 10.1.3.0 255.255.255.0 10.1.254.3 permanent</b>	Enable IP routing for the soho-tahoe subnet.
5	hq-sanjose(config)# <b>interface dialer 1</b>	Enter interface dialer 1.
6	hq-sanjose(config-if)# <b>dialer map ip 10.1.254.4 name robo-austin #</b>	Create a dialer map entry to the robo-austin router <sup>2</sup> .
7	hq-sanjose(config-if)# <b>dialer map ip 10.1.254.3 name soho-tahoe #</b>	Create a dialer map entry to the soho-tahoe router <sup>2</sup> .

1. Make sure to use your own usernames and passwords for the remote sites.

2. In this case study, hq-sanjose does not dial out to the remote sites. The pound sign (#) is used to map the remote site's name to the IP address.

### Verify

Enter the **show running** command:

```
hq-sanjose# show running
Building configuration...
Current configuration:
!
---- snip ----
!
username joe-admin password 7 <removed>
username robo-austin password 7 <removed>
username soho-tahoe password 7 <removed>
!
---- snip ----
!
interface Dialer1
 ip address 10.1.254.1 255.255.255.0
 no ip directed-broadcast
 encapsulation ppp
 no ip mroute-cache
 dialer in-band
 dialer idle-timeout 1800
 dialer map ip 10.1.254.3 name soho-tahoe #
 dialer map ip 10.1.254.4 name robo-austin #
 dialer-group 2
 peer default ip address pool dialin_pool
 no fair-queue
 no cdp enable
 ppp authentication chap pap
 ppp multilink
!
---- snip ----
!
ip local pool dialin_pool 10.1.2.2 10.1.2.97
ip route 10.1.3.0 255.255.255.0 10.1.254.3 permanent
ip route 10.1.4.0 255.255.255.0 10.1.254.4 permanent
!
dialer-list 2 protocol ip permit
!
---- snip ----
```

### Tips

- Dialer mapping provides layer 3 to layer 2 address resolution for a telephone network. This is done by mapping a host name and IP address to a telephone number.
- To display the static and dynamic dialer maps, enter the **show dialer map** command on the Cisco AS5300.

---

**Note** If you want the Cisco AS5300 to initiate calls to the remote sites, you must define a dialer map phone number. This case study does not cover this option. See the *Dial Solutions Configuration Guide* for more information.

---

## Step 13—Configuring a Backhaul Routing Protocol

Assign a routing protocol and configure its related configuration parameters to integrate with the IP backbone. The dialer network uses static routing.

### Configure

To configure the routing protocol, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	<pre> hq-sanjose(config)# router eigrp 10 hq-sanjose(config-router)# network 10.0.0.0 hq-sanjose(config-router)# passive-interface dialer 1 hq-sanjose(config-router)# redistribute static hq-sanjose(config-router)# no auto-summary hq-sanjose(config-router)# exit </pre>	Configure the Enhanced IGRP routing protocol, enable IP routing, turn off routing updates on the dialer interface, and advertise remote LAN static routes.
2	<pre> hq-sanjose(config)# interface fastethernet 0 hq-sanjose(config-if)# ip summary-address eigrp 10 10.1.2.0 255.255.255.0 </pre>	Configure a summary aggregate address on the Fast Ethernet interface 0.  This step summarizes the IP addresses that are advertised to the backbone.

### Verify

To verify the configuration:

- Enter the **show ip eigrp topology** command:

```

hq-sanjose# show ip eigrp topology
IP-EIGRP Topology Table for process 10
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status
P 10.1.3.0/24, 1 successors, FD is 46226176
   via Redistributed (46226176/0)
P 10.1.2.0/24, 1 successors, FD is 128256
   via Connected, Loopback0
P 10.1.4.0/24, 1 successors, FD is 46226176
   via Redistributed (46226176/0)
P 10.1.254.0/24, 1 successors, FD is 46226176
   via Connected, Dialer1

```

- Enter the **show running** command:

```

hq-sanjose# show running
Building configuration...

Current configuration:
!
---- snip ----
!
router eigrp 10
 redistribute static
 passive-interface Dialer1
 network 10.0.0.0
 no auto-summary
!
---- snip ----

```

## Step 14—Confirming the Final Running Configuration

Here is the final running configuration:

```
hq-sanjose# show running
Building configuration...
Current configuration:
!
version 12.0
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname hq-sanjose
!
aaa new-model
aaa authentication login default local
aaa authentication ppp default if-needed local
enable secret 5 $1$.voA$9/8.Zo1l3jeWJMP6hEE6U0
!
username joe-admin password 7 <removed>
username robo-austin password 7 <removed>
username soho-tahoe password 7 <removed>
!
async-bootp dns-server 10.2.2.3 10.2.3.1
isdn switch-type primary-ni
!
!
controller T1 0
framing esf
clock source line primary
linecode b8zs
pri-group timeslots 1-24
!
controller T1 1
framing esf
clock source line secondary
linecode b8zs
pri-group timeslots 1-24
!
controller T1 2
framing esf
clock source internal
linecode b8zs
pri-group timeslots 1-24
!
controller T1 3
framing esf
clock source internal
linecode b8zs
pri-group timeslots 1-24
!
interface Loopback0
ip address 10.1.2.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet0
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
```

```
!  
interface Serial0:23  
  no ip address  
  no ip directed-broadcast  
  dialer rotary-group 1  
  isdn incoming-voice modem  
!  
interface Serial1:23  
  no ip address  
  no ip directed-broadcast  
  dialer rotary-group 1  
  isdn incoming-voice modem  
!  
interface Serial2:23  
  no ip address  
  no ip directed-broadcast  
  dialer rotary-group 1  
  isdn incoming-voice modem  
!  
interface Serial3:23  
  no ip address  
  no ip directed-broadcast  
  dialer rotary-group 1  
  isdn incoming-voice modem  
!  
interface FastEthernet0  
  ip address 10.1.1.10 255.255.255.0  
  no ip directed-broadcast  
  ip summary-address eigrp 10 10.1.2.0 255.255.255.0  
  no ip route-cache  
  no ip mroute-cache  
  duplex auto  
  speed auto  
!  
interface Group-Async1  
  ip unnumbered Loopback0  
  no ip directed-broadcast  
  encapsulation ppp  
  async mode interactive  
  peer default ip address pool dialin_pool  
  no cdp enable  
  ppp authentication chap pap  
  group-range 1 96  
!  
interface Dialer1  
  ip address 10.1.254.1 255.255.255.0  
  no ip directed-broadcast  
  encapsulation ppp  
  no ip mroute-cache  
  dialer in-band  
  dialer idle-timeout 1800  
  dialer map ip 10.1.254.3 name soho-tahoe #  
  dialer map ip 10.1.254.4 name robo-austin #  
  dialer-group 2  
  peer default ip address pool dialin_pool  
  no fair-queue  
  no cdp enable  
  ppp authentication chap pap  
  ppp multilink  
!  
router eigrp 10  
  redistribute static  
  passive-interface Dialer1  
  network 10.0.0.0  
  no auto-summary
```

## Step 15—Saving the Configuration

---

```
!  
ip local pool dialin_pool 10.1.2.2 10.1.2.97  
ip route 10.1.3.0 255.255.255.0 10.1.254.3 permanent  
ip route 10.1.4.0 255.255.255.0 10.1.254.4 permanent  
!  
dialer-list 2 protocol ip permit  
!  
!  
line con 0  
line 1 96  
  autoselect during-login  
  autoselect ppp  
  modem InOut  
line aux 0  
line vty 0 4  
!  
end
```



**Caution** Do not expect your final configuration to look exactly like this one. You must localize for your own network environment. Additionally, most Cisco IOS software versions have different default settings. However, this final configuration provides a good basis for comparison.

## Step 15—Saving the Configuration

Save the configuration to NVRAM by entering the **copy running-config startup-config** command.

## Step 16—Testing Sync PPP Connections to Remote LANs

You must configure the remote ISDN routers before you can test DDR connections. For configuration tasks and end-to-end test examples, see the following chapters:

- Chapter 4, “Cisco 1604 Configuration”
- Chapter 5, “Cisco 766 Configuration”

## Step 17—Adding More Remote LAN Sites as Needed

After you bring up your remote LANs and remote nodes, you might decide to expand the solution to a larger dial implementation. The following key items must be configured on the Cisco AS5300 to support each additional remote LAN router:

- One dialer map
- One IP route
- One username:password

---

**Note** The *italic* variables in Table 2-5 must be replaced with the actual WAN IP address, host name, IP subnet address, subnet mask, and password for each additional remote LAN router.

---

**Table 2-5 Required Commands for Each Additional Site**

Command	Purpose
<code>dialer map ip peer-wan-addr name hostname #</code>	A dialer map. Create a user entity in the security database for the remote site, which is appended to a dialer map <sup>1</sup> .
<code>ip route subnet mask wan-addr</code>	A static route that points to the dialer map IP address.
<code>username hostname password password</code>	A username and password that matches the name on the dialer map.

1. If no phone number is used in the dialer map, this will prevent the central site from dialing out to the remote site.



# Cisco 1604 Configuration

This chapter describes how to configure the Cisco 1604 to dial out to the Cisco AS5300.

## Site Profile Characteristics

Figure 3-1 shows the network topology from the Cisco 1604’s perspective.

**Figure 3-1 Network Topology**

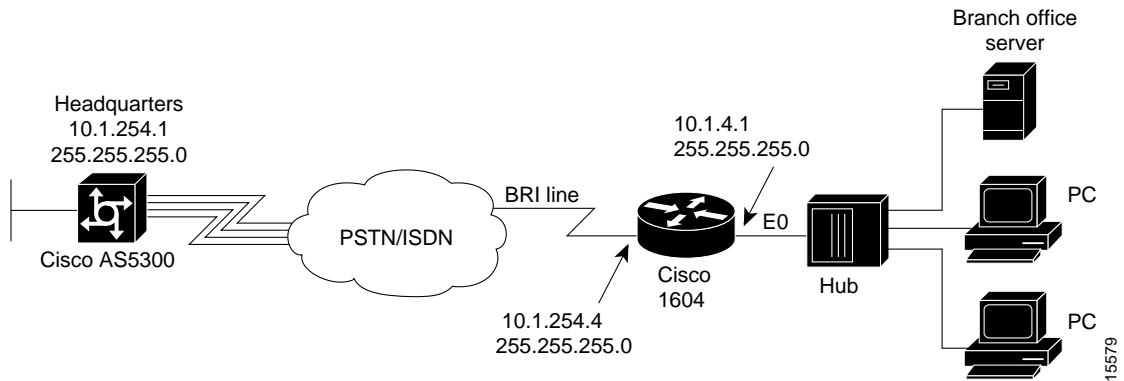


Table 3-1 provides detailed information about the end-to-end connection. This is the network administrator’s top-level design table.

**Table 3-1 Site Characteristics**

Host Name/ Username	Username Password	WAN IP Address <sup>1</sup>	Ethernet IP Address	Assigned Phone Number	Site Hardware
robo-austin	austin-pw	10.1.254.4 255.255.255.0	10.1.4.1 255.255.255.0	Directory number = 5125554433	Cisco 1604
hq-sanjose	hq-sanjose-pw	10.1.254.1 255.255.255.0	10.1.1.10 255.255.255.0	4085551234	Cisco AS5300

1. The Cisco 1604’s WAN default gateway is 10.1.254.1, which is the Cisco AS5300’s dialer interface address.

Cisco IOS Release 12.0 is running inside the router. If the startup configuration is blank, the following screen is displayed at bootup. The automatic setup script is engaged. Enter **no** when you are asked the question, "Would you like to enter the initial configuration dialog? [yes]: **no**."

In this case study, the Cisco 1604 is manually configured. The automatic setup script is not used.

---

**Note** To enhance readability throughout this chapter, the most important output fields are highlighted with **bold** font. The commands you enter are also **bold** but are preceded by a router prompt.

---

```
System Bootstrap, Version 11.1(7)AX [kuong (7)AX], RELEASE SOFTWARE (fc1)
Copyright (c) 1994-1996 by cisco Systems, Inc.
C1600 processor with 2048 Kbytes of main memory
```

```
program load complete, entry point: 0x4018060, size: 0x1da928
```

```
Notice: NVRAM invalid, possibly due to write erase.
```

```
%QUICC_ETHER-1-LOSTCARR: Unit 0, lost carrier. Transceiver problem?program load
complete, entry point: 0x8000060, size: 0x3f5f2c
```

#### 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) 1600 Software (C1600-SY-L), Version 12.0(x)
Copyright (c) 1986-1998 by cisco Systems, Inc.
Compiled Tue 25-Aug-98 01:45 by xxxx
Image text-base: 0x0802DA90, data-base: 0x02005000
```

```
ROM: System Bootstrap, Version 11.1(10)AA, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
```

```
Router uptime is 10 minutes
System restarted by reload
System image file is "flash:c1600-sy-1.120-x"
```

```
cisco 1604 (68360) processor (revision C) with 17920K/512K bytes of memory.
Processor board ID 08823977, with hardware revision 00972006
Bridging software.
X.25 software, Version 3.0.0.
Basic Rate ISDN software, Version 1.1.
1 Ethernet/IEEE 802.3 interface(s)
1 ISDN Basic Rate interface(s)
System/IO memory with parity disabled
2048K bytes of DRAM onboard 16384K bytes of DRAM on SIMM
System running from FLASH
8K bytes of non-volatile configuration memory.
12288K bytes of processor board PCMCIA flash (Read ONLY)
```

```
--- System Configuration Dialog ---

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

Would you like to terminate autoinstall? [yes]: yes

Press RETURN to get started!

00:00:17: %QUICC_ETHER-1-LOSTCARR: Unit 0, lost carrier. Transceiver problem?
00:00:17: %LINK-3-UPDOWN: Interface Ethernet0, changed state to up
00:00:17: %LINK-3-UPDOWN: Interface Serial0, changed state to down
00:00:17: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0, changed state to down
00:00:17: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:1, changed state to down
00:00:17: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:2, changed state to down
00:00:17: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0, changed state to
down
00:00:17: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed stat to down
00:00:44: %LINK-5-CHANGED: Interface BRI0, changed state to administratively down
00:00:46: %LINK-5-CHANGED: Interface Serial0, changed state to administratively down
00:00:46: %LINK-5-CHANGED: Interface Ethernet0, changed state to administratively down
00:00:47: %IP-5-WEBINST_KILL: Terminating DNS process

Router>
```

## Overview of Tasks

Perform the following steps to configure the router:

- “Step 1—Configuring the Host Name, Password, and Time Stamps” on page 4
- “Step 2—Configuring Local AAA Security” on page 5
- “Step 3—Configuring the Ethernet Interface” on page 7
- “Step 4—Configuring BRI” on page 9
- “Step 5—Configuring DDR” on page 11
- “Step 6—Testing Connections to the Cisco AS5300” on page 14
- “Step 7—Confirming the Final Running Configuration” on page 21
- “Step 8—Saving the Configuration” on page 21

---

**Note** Before you perform the configuration tasks in this chapter, be sure you understand the overall dial case action plan. See the chapter “Dial Case Study Overview.”

---

## Step 1—Configuring the Host Name, Password, and Time Stamps

Assign a host name to the Cisco 1604, enable basic security, and turn on time stamping. Configuring a host name allows you to distinguish between different network devices. Enable passwords allow you to prevent unauthorized configuration changes. Time stamps help you trace debug output for testing connections. Not knowing exactly when an event occurs hinders you from examining background processes.

### Configure

To configure the host name, enable password, and time stamps, use the following commands beginning in user EXEC mode:

Step	Command	Purpose
1	Router> <b>enable</b>	Enter privileged EXEC mode.
2	Router# <b>configure terminal</b> Enter configuration commands, one per line. End with CNTL/Z.	Enter global configuration mode <sup>1</sup> .
3	Router(config)# <b>hostname robo-austin</b>	Assign a host name to the router. This host name is typically used during authentication with the central site.
4	robo-austin(config)# <b>enable secret guessme</b>	Enter a secret enable password, which secures privileged EXEC mode <sup>2</sup> .
5	hq-sanjose(config)# <b>service password-encryption</b>	Encrypt passwords in the configuration file for greater security <sup>3</sup> .
6	hq-sanjose(config)# <b>service timestamps debug datetime msec</b> hq-sanjose(config)# <b>service timestamps log datetime msec</b>	Enable millisecond time stamping on debug and logging output. Time stamps are useful for detailed access tracing.

1. As you are configuring the software, make sure that all logging dialog generated by the router is displayed on your terminal screen. If it is not, enter the **terminal monitor** EXEC command. If you are configuring the router via the console port, logging is automatically displayed.
2. Make sure to change “guessme” to your own secret password.
3. Additional measures should be used, as the passwords are not strongly encrypted by today’s standards.

### Verify

To verify the configuration:

- Enter the **show running** command:

```

robo-austin# show running
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname robo-austin
!
enable secret 5 $1$og7B$nSwMZM0NBKTPHv09KVgx11
!
interface Ethernet0
no ip address
    
```

```

    shutdown
    !
interface Serial0
    no ip address
    shutdown
    !
interface BRI0
    no ip address
    shutdown
    !
ip classless
    !
    !
line con 0
line vty 0 4
    login
    !

```

- Try logging in with your new enable password. Exit out of enable mode using the **disable** command. The prompt changes from `robo-austin#` to `robo-austin>`. Enter the **enable** command followed by your password. The **show privilege** command shows the current security privilege level, which is level 15.

```

robo-austin# disable
robo-austin> enable
Password: letmein
robo-austin# show privilege
Current privilege level is 15
robo-austin#

```

### Tips

If you have trouble:

- Make sure **Caps Lock** is off.
- Make sure you entered the correct password. Passwords are case sensitive.

## Step 2—Configuring Local AAA Security

The Cisco IOS security model to use on all Cisco devices is authentication, authorization, and accounting (AAA). AAA provides the primary framework through which you set up access control on the access server.

- Authentication—Who are you?
- Authorization—What can you do?
- Accounting—What did you do?

In this case study, the same authentication method is used on all interfaces. AAA is set up to use the local database configured on the router. This local database is created with the **username** configuration commands.

---

**Note** After you finish setting up basic security, you can enhance the security solution by extending it to an external TACACS+ or RADIUS server. This case study describes local AAA security only.

---

## Configure

To configure local AAA security, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	<code>robo-austin(config)# username joe-admin password joe-password</code>	Create a local username for yourself <sup>1</sup> . This step prevents you from getting locked out of the router when you enable AAA.
2	<code>robo-austin(config)# aaa new-model</code>	Enable AAA access control. This step immediately enables login and PPP authentication.
3	<code>robo-austin(config)# aaa authentication login default local</code>	Configure AAA to perform login authentication using the local username database. The <b>login</b> keyword indicates authentication of EXEC (shell) users.
4	<code>robo-austin(config)# aaa authentication ppp default if-needed local</code>	Configure PPP authentication to use the local database if the session was not already authenticated by <b>login</b> .

1. Make sure to change “joe-admin” to your own username and “joe-password” to your own password.

## Verify

To verify the configuration:

- Try to log in with your username:password. Enter the **login** command at the EXEC (shell) prompt. Do not disconnect your EXEC session until you can log in successfully. (If you get locked out, you will need to perform password recovery by rebooting the router.)

```
robo-austin# login

User Access Verification

Username: joe-admin
Password: joe-password

robo-austin#
```

- Enter the **show running** command:

```
robo-austin# show running
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname robo-austin
!
aaa new-model
aaa authentication login default local
aaa authentication ppp default if-needed local
enable secret 5 $1$og7B$nSwMZM0NBKTPHV09KVgx11
```

```

!
username joe-admin password 7 <removed>
!
interface Ethernet0
  no ip address
  shutdown
!
interface Serial0
  no ip address
  shutdown
!
interface BRI0
  no ip address
  shutdown
!
ip classless
!
!
line con 0
line vty 0 4
!

```

## Step 3—Configuring the Ethernet Interface

Assign an IP address to the Ethernet interface. Test the interface by pinging it from a PC on the LAN.

### Configure

To configure the Ethernet interface, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	<pre> robo-austin(config)# <b>interface ethernet 0</b> robo-austin(config-if)# <b>ip address 10.1.4.1 255.255.255.0</b> </pre>	Configure the IP address and subnet mask on the Ethernet interface.
2	<pre> robo-austin(config-if)# <b>no shutdown</b> </pre>	Bring up the interface <sup>1</sup> .

1. This command changes the state of the interface from administratively down to up.

### Verify

To verify the configuration:

- Enter the **show ip interface brief** command, which allows you to quickly check the status of all router interfaces.

The field “administratively down” means that the interface is configured with the **shutdown** command. To bring the interface up, you must enter the **no shutdown** command. The Status column refers to the ability to physically connect the network at layer 1 (needed for getting clocks and carrier signals). The Protocol column refers to the ability to see traffic flow, which typically occurs at the data link layer. For example, the Ethernet interface sends a loopback Ethernet packet out to itself via the Ethernet LAN.

```

robo-austin# show ip interface brief
Interface                IP-Address      OK? Method Status                Protocol
BRI0                     unassigned     YES unset  administratively down down
BRI0:1                   unassigned     YES unset  administratively down down
BRI0:2                   unassigned     YES unset  administratively down down

```

```

Ethernet0          10.1.4.1          YES manual up          up
Serial0           unassigned        YES unset  administratively down down
  
```

In the next example, notice that the status is up but the protocol is down. The following logging message appears at 00:40:20: “Unit 0, lost carrier. Transceiver problem?.” After the administrator plugs the Ethernet cable into the Ethernet port, the interface comes up. See 00:40:25.

```

robo-austin# show ip interface brief
Interface          IP-Address          OK? Method Status          Protocol
BRI0               unassigned         YES unset  administratively down down
BRI0:1             unassigned         YES unset  administratively down down
BRI0:2             unassigned         YES unset  administratively down down
Ethernet0          10.1.4.1           YES manual up          down
Serial0            unassigned         YES unset  administratively down down
robo-austin#
00:40:20: %QUICC_ETHER-1-LOSTCARR: Unit 0, lost carrier. Transceiver problem?
00:40:25: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0, changed state to up
robo-austin#
  
```

- Establish connectivity with an Ethernet-based device. In this example, IP address 10.1.4.2 is assigned to the first external PC on this LAN to test for router-to-PC connectivity. The PC’s DOS prompt application is opened and the **ping 10.1.4.1** command is issued.

```

Microsoft(R) Windows 95
(C)Copyright Microsoft Corp 1981-1996.

C:\WINDOWS> ping 10.1.4.1
Pinging 10.1.4.1 with 32 bytes of data:

Reply from 10.1.4.1: bytes=32 time=3ms TTL=236
Reply from 10.1.4.1: bytes=32 time=2ms TTL=236
Reply from 10.1.4.1: bytes=32 time=3ms TTL=236
Reply from 10.1.4.1: bytes=32 time=2ms TTL=236
  
```

- Try pinging the PC from the Cisco 1604. If the PC has not yet used any IP services or drivers, you might get a failure. The preferred method is to ping the router from a PC on the LAN first.

```

robo-austin# ping 10.1.4.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.4.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
  
```

- If you know that the Ethernet interface is up but not performing correctly, enter the **show interface ethernet 0** command. This example shows errors in the counters, because the Ethernet cable was not plugged in.

```

robo-austin# show interface ethernet 0
Ethernet0 is up, line protocol is up
Hardware is QUICC Ethernet, address is 0060.834f.6626 (bia 0060.834f.6626)
Internet address is 10.1.4.1/24
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 234/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:08, output 00:00:04, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  2 packets input, 644 bytes, 0 no buffer
  
```

```

Received 2 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
28 packets output, 2905 bytes, 0 underruns
25 output errors, 0 collisions, 2 interface resets
0 babbles, 0 late collision, 0 deferred
3 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out

```

## Step 4—Configuring BRI

Enable BRI connectivity with the central office switch. PPP framing is used on the B channels. Dial-on-demand routing (DDR) is configured in the next section “Step 5—Configuring DDR.”

---

**Note** The **dialer in-band** command does not need to be configured on the BRI interface. A BRI interface is a dialer in-band interface by default. Interface BRI0:1 and BRI0:2 are controlled by the dialer interface “**interface bri 0**.”

---

## Configure

To configure BRI, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	robo-austin(config)# <b>isdn switch-type basic-ni1</b>	Configure the ISDN switch type, which is <b>basic-ni1</b> in this example.
2	robo-austin(config)# <b>interface bri 0</b> robo-austin(config-if)# <b>ip address 10.1.254.4 255.255.255.0</b>	Configure the IP address and subnet mask on the BRI interface.
3 8	robo-austin(config-if)# <b>isdn spid1 51255544330101</b> robo-austin(config-if)# <b>isdn spid2 51255544340101</b>	Configure your SPIDs, which are required by many switch types.
4	robo-austin(config-if)# <b>encapsulation ppp</b>	Enable PPP.
5	robo-austin(config-if)# <b>no fair-queue</b>	Disable fair queuing.
6	robo-austin(config-if)# <b>ppp multilink</b>	Enable PPP multilink.
7	robo-austin(config-if)# <b>ppp authentication chap pap callin</b>	Enable CHAP and PAP authentication on the interface during LCP negotiation.  The access server will first authenticate with CHAP. If CHAP is not used by the remote client, then PAP is tried. CHAP is requested first. <sup>1</sup>
8	robo-austin(config-if)# <b>no shutdown</b>	Bring up the interface. <sup>2</sup>

1. You have the choice to authenticate the remote side on any connection. The **callin** keyword means that all outbound connection attempts made by the Cisco 1604 will not authenticate the remote peer. The remote peer is the device at the other end of the PPP link (Cisco AS5300). Only the calls that come into the Cisco 1604 will be authenticated.

2. The **no shutdown** command changes the state of the interface from administratively down to up.

## Verify

- You should see the following output messages after you enter the **no shutdown** command.

This example shows the BRI0:1 and BRI0:2 states change to “down,” because the previous state was “administratively down.” The BRI0 D channel changes to “up” as it spoofs for the two B channels. After the D channel finds the B channels, the B channels change state to “up.” The Cisco 1604 communicates with the telephone switch and receives its TEI numbers for its two B channels.

```
robo-austin(config-if)# no shutdown
robo-austin#
00:45:01: %LINK-3-UPDOWN: Interface BRI0:1, changed state to down
00:45:01: %LINK-3-UPDOWN: Interface BRI0:2, changed state to down
00:45:01: %LINK-3-UPDOWN: Interface BRI0, changed state to up
robo-austin#
00:45:02: %ISDN-6-LAYER2UP: Layer 2 for Interface BR0, TEI 100 changed to up
00:45:02: %ISDN-6-LAYER2UP: Layer 2 for Interface BR0, TEI 101 changed to up
robo-austin(config-if)#
```

- Check the ISDN status by entering the **show isdn status** command:

```
robo-austin# show isdn status
Global ISDN Switchtype = basic-ni
ISDN BRI0 interface
    dsl 0, interface ISDN Switchtype = basic-ni
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 100, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
        TEI = 101, Ces = 2, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Spid Status:
        TEI 100, ces = 1, state = 5(init)
            spid1 configured, no LDN, spid1 sent, spid1 valid
            Endpoint ID Info: epsf = 0, usid = 2, tid = 1
        TEI 101, ces = 2, state = 5(init)
            spid2 configured, no LDN, spid2 sent, spid2 valid
            Endpoint ID Info: epsf = 0, usid = 4, tid = 1
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 0 CCBs = 0
    Total Allocated ISDN CCBs = 0
```

---

**Note** Here are some defined terms from the output. DSL = Digital Subscriber Loop. CCBs = Call Control Blocks. TEI = Terminal Equipment Identifier. LDN = Local Directory Number. The BRI 0 interface corresponds to dsl 0, which has three channels (2B + D). The CCB counter increases by 1 for each active call on the Cisco 1604. The CCB counter for one call gets destroyed upon disconnect.

---

- Enter the **show ip interface brief** command to check the current state of the interface.

```
robo-austin# show ip interface brief
Interface          IP-Address      OK? Method Status          Protocol
BRI0               10.1.254.4     YES manual up              up
BRI0:1            unassigned     YES unset  down            down
BRI0:2            unassigned     YES unset  down            down
Ethernet0         10.1.4.1       YES manual up              up
Serial0           unassigned     YES unset  administratively down down
```

---

**Note** Notice that the status and protocol for BRI 0 and Ethernet 0 are both up/up, which is what we expect to see. The term manual means that you manually configured the interface since the last reboot. The two B channels (BRI0:1 and BRI0:2) are down because there are no active calls on the BRI interface at this time.

---

### Tips

If you have trouble:

- Make sure the correct ISDN switch type and SPIDs are configured.
- Make sure your BRI line is connected to the correct port.

## Step 5—Configuring DDR

Set up the DDR routing components. In most cases, a remote site with a single LAN will require a simple DDR configuration. DDR is the mechanism that supports the routing table and call control in a circuit switched environment.

DDR in this case study takes the standard dialer map approach. You must configure specific parameters to establish connectivity with the Cisco AS5300 using sync PPP. Parameters include a static route, username:password, and a dialer map.

## Configure

To configure DDR, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	robo-austin(config)# <b>interface bri 0</b>	Enter configuration mode for the BRI interface.
2	robo-austin(config-if)# <b>dialer-group 2</b>	Define the interesting packets that activate the ISDN connection. Interesting packets reset the idle timer and trigger dialing.  This dialer filter is defined by the <b>dialer-list 2</b> command. See Step 7.
3	robo-austin(config-if)# <b>no fair-queue</b>	Disable fair queuing.
4	robo-austin(config-if)# <b>no cdp enable</b>	Disable the Cisco discovery protocol, unless you are using it for a specific purpose.
5	robo-austin(config-if)# <b>dialer load-threshold 60 either</b>	Configure the interface to bring up the second B channel when the bandwidth load exceeds 60/255.
6	robo-austin(config-if)# <b>dialer map ip 10.1.254.1 name hq-sanjose 14085551234</b> robo-austin(config-if)# <b>exit</b>	Build a dialer map that maps to the Cisco AS5300's IP address, host name, and directory number.  The static route in Step 8 points to this dialer map.
7	robo-austin(config)# <b>dialer-list 2 protocol ip permit</b>	Define a DDR's dialer-list to allow any IP packets to establish and maintain calls.

Step	Command	Purpose
8	robo-austin(config) <b>ip route 0.0.0.0 0.0.0.0 10.1.254.1 permanent</b>	Create a static route for the next hop, which is the Cisco AS5300's WAN port. IP address 10.1.254.1 is used on the Cisco AS5300's dialer interface.  This static route points at the dialer map on the access server's dialer interface.
9	robo-austin(config)# <b>username hq-sanjose password austin-pw</b>	When the Cisco AS5300 (hq-sanjose) authenticates the Cisco 1604 using CHAP, this password will be used by the Cisco 1604 <sup>1</sup> .
10	robo-austin(config)# <b>ip classless</b>	Ensure that all unknown subnets use the default route.

1. On Cisco IOS devices the PPP name is determined by one of the following commands: **hostname**, **sgbp group**, **ppp pap sent-username**, or **ppp chap hostname**.

## Verify

To verify the configuration:

- Enter the **show ip route** command to confirm that the static route is installed and pointing at your dialer map address. The static IP default route must first be configured before you enter this command.

```
robo-austin# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
```

```
Gateway of last resort is 10.1.254.1 to network 0.0.0.0
```

```
      10.0.0.0/24 is subnetted, 2 subnets
C       10.1.4.0 is directly connected, Ethernet0
C       10.1.254.0 is directly connected, BRI0
S*    0.0.0.0/0 [1/0] via 10.1.254.1
```

**Note** The static route is the first software building block (design crux) that receives the packet routed to the dialer map. The route must direct the packets to at the dialer map before the DDR features can establish connectivity.

- Enter the **show dialer** command. The following example shows that the Cisco 1604 has not placed any calls yet, and there have been no failures. An ISDN interface is a dialer interface. Key statistics are shown for each B channel.

```
robo-austin# show dialer

BRI0 - dialer type = ISDN

Dial String      Successes  Failures  Last called  Last status
14085551234      0          0         never        -
0 incoming call(s) have been screened.
```

0 incoming call(s) rejected for callback.

```
BRI0:1 - dialer type = ISDN
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle
```

```
BRI0:2 - dialer type = ISDN
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle
```

- Enter the **show dialer map** command to view the static dialer map that was built to the Cisco AS5300. This map is built using the phone number and WAN IP address of the access server.

```
robo-austin# show dialer map
Static dialer map ip 10.1.254.1 name hq-sanjose (14085551234) on BRI0
```

- Enter the **show running** command:

```
robo-austin# show running
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname robo-austin
!
aaa new-model
aaa authentication login default local
aaa authentication ppp default if-needed local
enable secret 5 $1$aZ1D$wNO71EpS6y5zRYuW9qFEr.
!
username joe-admin password 0 6y5zRYuW9qFEr$wNO71EpS6$aZ1
username hq-sanjose password 0 $wNO71EpS6y5zy5zRYuW9aZ1D$w
isdn switch-type basic-ni
!
interface Ethernet0
 ip address 10.1.4.1 255.255.255.0
!
interface Serial0
 no ip address
 shutdown
!
interface BRI0
 ip address 10.1.254.4 255.255.255.0
 encapsulation ppp
 dialer map ip 10.1.254.1 name hq-sanjose 14085551234
 dialer load-threshold 60 either
 dialer-group 2
 isdn switch-type basic-ni
 isdn spid1 51255544330101
 isdn spid2 51255544340101
 no cdp enable
 ppp authentication chap pap callin
 ppp multilink
 hold-queue 75 in
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.254.1 permanent
```

```
!  
dialer-list 2 protocol ip permit  
!  
line con 0  
line vty 0 4  
!  
end
```

### Tips

- To display the actual load currently assigned to the interface, enter the **show interface bri 0:1** command. Search for the output field “load x/255.” SNMP can be used to monitor the load on an interface. How you set the threshold depends on each site’s characteristics, such as traffic patterns and WAN costs. If you are in an environment where all calls are local, then you might nail up the connections full time.
- Large ISDN phone bills arise due to failure to appropriately tune filters and load thresholds. Filters are dialer lists, which are applied with dialer groups. The **dialer-list** command and **dialer-group** command control the first B channel. The **dialer load-threshold** command controls the behavior when additional B channels are connected.
- In this case study, the Cisco AS5300 does not dial out to the remote sites. Therefore, you do not need to tune the central site’s dialer threshold setting. Only the remote side is in charge of opening and closing channels based on the settings of the dialer commands.
- Make sure you configured the correct SPID numbers on the BRI interface.

## Step 6—Testing Connections to the Cisco AS5300

The test strategy is to ping the Cisco AS5300’s WAN port then ping the backbone behind the access server. Cisco recommends you ping the domain name server (DNS) on the backbone, since this device should always be up and operational.

Pinging a next hop IP address can have complications in an IP-unnumbered environment. For example, complications arise when WAN interfaces are configured with IP unnumbered.

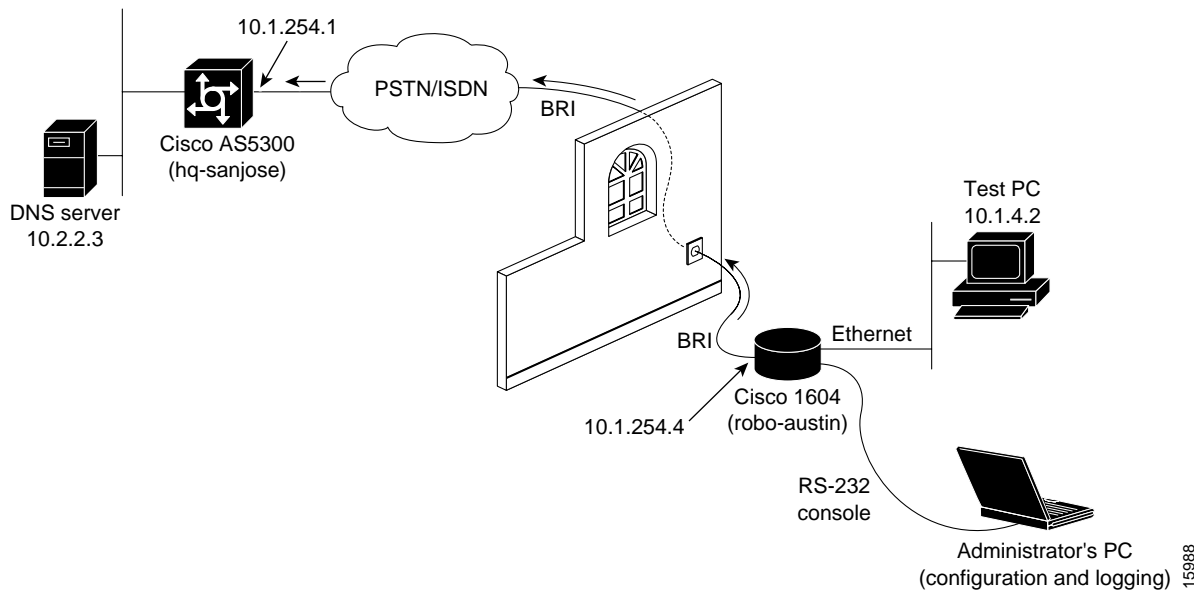
---

**Note** The typical low-level test to verify connectivity in a sync PPP environment is to ping a device on the other end of the WAN link. In a modem environment (async PPP), the low-level test is to get an EXEC shell established on the router.

---

Figure 3-2 shows the actual test lab environment used in this test case.

Figure 3-2 Test Lab Environment



- Step 1** Turn on the appropriate debugging. Examining the background processes is essential for effective troubleshooting.

```

robo-austin# undebug all
All possible debugging has been turned off
robo-austin# terminal monitor
robo-austin# debug dialer
Dial on demand events debugging is on
robo-austin# debug isdn q931
ISDN Q931 packets debugging is on
robo-austin# debug ppp negotiation
PPP protocol negotiation debugging is on
robo-austin# debug ppp authentication
PPP authentication debugging is on
robo-austin# debug ip peer
IP peer address activity debugging is on

```

- Step 2** Verify that your routing table points to the hq-sanjose network access server (NAS):

```

robo-austin# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
Gateway of last resort is 10.1.254.1 to network 0.0.0.0
 10.0.0.0/24 is subnetted, 2 subnets
 C    10.1.4.0 is directly connected, Ethernet0
 C    10.1.254.0 is directly connected, BRI0
 S*   0.0.0.0/0 [1/0] via 10.1.254.1

```

**Step 3** Verify that the correct dialer map exists:

```
robo-austin# show dialer map
Static dialer map ip 10.1.254.1 name hq-sanjose (14085551234) on BRI0
```

**Step 4** Ping the IP address assigned to the Cisco AS5300's dialer interface. Notice that the Cisco 1604 (robo-austin) quickly gets 4 of 5 pings back from the Cisco AS5300 (hq-sanjose). After the ping is sent, examine the background processes as displayed by the debug output.

```
robo-austin# ping 10.1.254.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.254.1, timeout is 2 seconds:
..!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 116/182/372ms
robo-austin#
```

**Step 5** Look at the debug output. The following comments apply to the debug output example on the next page:

- (a) See 08:03:55.  
The source and destination IP address of the DDR dial cause are displayed.  
(s=10.1.254.4, d=10.1.254.1)
- (b) See 08:03:55.  
Hq-sanjose's hunt group number is dialed.  
(Attempting to dial 14085551234)
- (c) See 08:03:55.  
ISDN Setup is transmitted.  
(TX -> SETUP pd = 8 callref = 0x2F)
- (d) See 08:03:55.  
A synchronous data bearer capability is displayed.  
(Bearer Capability i = 0x8890)
- (e) See 08:03:55.  
The outgoing LCP configuration request is made.  
(BR0:1 LCP: 0 CONFREQ [Closed] id 42 len 28)
- (f) See 08:03:55.  
The incoming LCP configuration request wants to authenticate with CHAP.  
(AuthProto CHAP (0x0305C22305))
- (g) See 08:03:55.  
The outgoing acknowledgment says this peer will do CHAP.  
(LCP: 0 CONFACK [REQsent])
- (h) See 08:03:55.  
Both PPP peers have received LCP CONFACK. LCP is now open.  
(BR0:1 LCP: State is Open)
- (i) See 08:03:55.  
Authentication phase is initiated by robo-austin.  
(BR0:1 PPP: Phase is AUTHENTICATING, by the peer)
- (j) See 08:03:55.  
Robo-austin accepts a CHAP challenge initiated by hq-sanjose. The device robo-austin is not authenticating hq-sanjose, which is the desired behavior for this

scenario.

```
(BR0:1 CHAP: I CHALLENGE id 5 len 31 from "hq-sanjose")
```

```
(BR0:1 CHAP: O RESPONSE id 5 len 32 from "robo-austin")
```

(k) See 08:03:55.

The robo-austin PPP peer is successfully authenticated by the hq-sanjose peer.

```
(BR0:1 CHAP: I SUCCESS id 5 len 4)
```

(l) See 08:03:55.

MultiLink PPP uses a virtual-access interface to host the bundle.

```
(BR0:1 PPP: Phase is VIRTUALIZED)
```

(m) See 08:03:56.

LCP on Virtual-Access2 is forced up as it was already negotiated on the physical interface. For more information, use the **show interface virtual-access2 conf** command and **debug vtemp** command.

```
(%LINK-3-UPDOWN: Interface Virtual-Access2, changed state to up)
```

```
(Vi2 PPP: Phase is UP)
```

(n) See 08:03:56.

IPCP negotiation begins.

```
(Vi2 IPCP: O CONFREQ [Closed] id 1 len 10)
```

```
(Vi2 IPCP: Address 10.1.254.4 (0x03060A01FE04))
```

(o) See 08:03:56.

IP can now be used across this PPP connection.

```
(Vi2 IPCP: I CONFACK [ACKsent] id 1 len 10)
```

```
(Vi2 IPCP: State is Open)
```

(p) See 08:03:57.

A route is installed to 10.1.254.1 to match the IP address negotiated by the peer.

```
(BR0 IPCP: Install route to 10.1.254.1)
```

(q) See 08:03:57 and 08:04:01.

The connection is made to hq-sanjose.

```
(Line protocol on Interface Virtual-Access2, changed state to up)
```

```
(Interface BRI0:1 is now connected to 14085551234 hq-sanjose)
```

```
robo-austin# ping 10.1.254.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.254.1, timeout is 2 seconds:
..!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 116/182/372ms
robo-austin#
```

```
08:03:55: BRI0: Dialing cause ip (s=10.1.254.4, d=10.1.254.1)
08:03:55: BRI0: Attempting to dial 14085551234
08:03:55: ISDN BR0: TX -> SETUP pd = 8 callref = 0x2F
08:03:55: Bearer Capability i = 0x8890
08:03:55: Channel ID i = 0x83
08:03:55: Keypad Facility i = '14085551234'
08:03:55: ISDN BR0: RX <- CALL_PROC pd = 8 callref = 0xAF
08:03:55: Channel ID i = 0x89
08:03:55: ISDN BR0: RX <- CONNECT pd = 8 callref = 0xAF
08:03:55: ISDN BR0: TX -> CONNECT_ACK pd = 8 callref = 0x2F
08:03:55: %LINK-3-UPDOWN: Interface BRI0:1, changed state to up
08:03:55: BR0:1 PPP: Treating connection as a callout
08:03:55: BR0:1 PPP: Phase is ESTABLISHING, Active Open
08:03:55: BR0:1 PPP: No remote authentication for call-out
08:03:55: BR0:1 LCP: O CONFREQ [Closed] id 42 len 28
08:03:55: BR0:1 LCP: MagicNumber 0x623E5C69 (0x0506623E5C69)
08:03:55: BR0:1 LCP: MRRU 1524 (0x110405F4)
```

## Step 6—Testing Connections to the Cisco AS5300

```
08:03:55: BR0:1 LCP: EndpointDisc 1 Local
(0x130E01726F626F2D61757374696E)
08:03:55: BR0:1 LCP: I CONFREQ [REQsent] id 7 len 32
08:03:55: BR0:1 LCP: AuthProto CHAP (0x0305C22305)
08:03:55: BR0:1 LCP: MagicNumber 0xE16A73E6 (0x0506E16A73E6)
08:03:55: BR0:1 LCP: MRRU 1524 (0x110405F4)
08:03:55: BR0:1 LCP: EndpointDisc 1 Local
(0x130D0168712D73616E6A6F7365)
08:03:55: BR0:1 LCP: O CONFACK [REQsent] id 7 len 32
08:03:55: BR0:1 LCP: AuthProto CHAP (0x0305C22305)
08:03:55: BR0:1 LCP: MagicNumber 0xE16A73E6 (0x0506E16A73E6)
08:03:55: BR0:1 LCP: MRRU 1524 (0x110405F4)
08:03:55: BR0:1 LCP: EndpointDisc 1 Local
(0x130D0168712D73616E6A6F7365)
08:03:55: BR0:1 LCP: I CONFACK [ACKsent] id 42 len 28
08:03:55: BR0:1 LCP: MagicNumber 0x623E5C69 (0x0506623E5C69)
08:03:55: BR0:1 LCP: MRRU 1524 (0x110405F4)
08:03:55: BR0:1 LCP: EndpointDisc 1 Local
(0x130E01726F626F2D61757374696E).
08:03:55: BR0:1 LCP: State is Open
08:03:55: BR0:1 PPP: Phase is AUTHENTICATING, by the peer
08:03:55: BR0:1 CHAP: I CHALLENGE id 5 len 31 from "hq-sanjose"
08:03:55: BR0:1 CHAP: O RESPONSE id 5 len 32 from "robo-austin"
08:03:55: BR0:1 CHAP: I SUCCESS id 5 len 4
08:03:55: BR0:1 PPP: Phase is VIRTUALIZED
08:03:55: BR0:1 IPCP: Packet buffered while building MLP bundle
interface
08:03:56: Vi2 PPP: Phase is DOWN, Setup
08:03:56: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:1,
changed state to up
08:03:56: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to up
08:03:56: Vi2 PPP: Treating connection as a callout
08:03:56: Vi2 PPP: Phase is ESTABLISHING, Active Open
08:03:56: Vi2 PPP: No remote authentication for call-out
08:03:56: Vi2 LCP: O CONFREQ [Closed] id 1 len 28
08:03:56: Vi2 LCP: MagicNumber 0x623E60D6 (0x0506623E60D6)
08:03:56: Vi2 LCP: MRRU 1524 (0x110405F4)
08:03:56: Vi2 LCP: EndpointDisc 1 Local
(0x130E01726F626F2D61757374696E)
08:03:56: Vi2 PPP: Phase is UP
08:03:56: Vi2 IPCP: O CONFREQ [Closed] id 1 len 10
08:03:56: Vi2 IPCP: Address 10.1.254.4 (0x03060A01FE04)
08:03:56: Vi2 PPP: Pending ncpQ size is 1
08:03:56: BR0:1 IPCP: Redirect packet to Vi2
08:03:56: Vi2 IPCP: I CONFREQ [REQsent] id 1 len 10
08:03:56: Vi2 IPCP: Address 10.1.254.1 (0x03060A01FE01)
08:03:56: set_ip_peer_addr: Vi2: address = 10.1.254.1 (7)
08:03:56: Vi2 IPCP: O CONFACK [REQsent] id 1 len 10
08:03:56: Vi2 IPCP: Address 10.1.254.1 (0x03060A01FE01)
08:03:57: Vi2 IPCP: I CONFACK [ACKsent] id 1 len 10
08:03:57: Vi2 IPCP: Address 10.1.254.4 (0x03060A01FE04)
08:03:57: Vi2 IPCP: State is Open
08:03:57: dialer Protocol up for Vi2
08:03:57: BR0 IPCP: Install route to 10.1.254.1
08:03:57: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access2, changed state to up
08:04:01: %ISDN-6-CONNECT: Interface BRI0:1 is now connected to
14085551234 hq-sanjose
```

**Step 6** Ping the DNS server behind hq-sanjose. The DNS server is the first backbone device that Cisco 1604 will try to use. The DNS server in this case study uses 10.2.2.3.

```
robo-austin# ping 10.2.2.3
```

Type escape sequence to abort.

```

Sending 5, 100-byte ICMP Echos to 10.2.2.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/12 ms

```

**Step 7** Use additional commands to verify robo-austin's connection with hq-sanjose:

```

robo-austin# show dialer map
Static dialer map ip 10.1.254.1 name hq-sanjose (14085551234) on BRI0

robo-austin# show dialer

BRI0 - dialer type = ISDN

Dial String      Successes  Failures  Last called  Last status
14085551234      1          0         00:00:30    successful
0 incoming call(s) have been screened.
0 incoming call(s) rejected for callback.

BRI0:1 - dialer type = ISDN
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is multilink member
Dial reason: ip (s=10.1.254.4, d=10.1.254.1)
Connected to 14085551234 (hq-sanjose)

BRI0:2 - dialer type = ISDN
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

Virtual-Access1 - dialer type = IN-BAND SYNC NO-PARITY
Rotary group 0, priority 0
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is data link layer up
Time until disconnect 105 secs
Connected to 14085551234 (hq-sanjose)

robo-austin# show ppp multilink

Bundle hq-sanjose, 1 member, Master link is Virtual-Access1
Dialer Interface is BRI0
  0 lost fragments, 0 reordered, 0 unassigned, sequence 0x0/0x0 rcvd/sent
  0 discarded, 0 lost received, 1/255 load

Member Link: 1 (max not set, min not set)
BRI0:1

robo-austin# show interface bri 0:1
BRI0:1 is up, line protocol is up
  Hardware is BRI
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive set (10 sec)
  LCP Open, multilink Open
  Last input 00:00:07, output 00:00:07, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    472 packets input, 13496 bytes, 0 no buffer
    Received 469 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    504 packets output, 18013 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets

```

## Step 6—Testing Connections to the Cisco AS5300

---

```
0 output buffer failures, 0 output buffers swapped out
104 carrier transitions
```

```
robo-austin# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
BRI0	10.1.254.4	YES	manual	up	up
BRI0:1	unassigned	YES	unset	up	up
BRI0:2	unassigned	YES	unset	down	down
Ethernet0	10.1.3.1	YES	manual	up	up
Serial0	unassigned	YES	unset	administratively down	down
Virtual-Access1	unassigned	YES	unset	up	up

```
robo-austin# show interface bri 0 1 2
```

```
BRI0:1 is up, line protocol is up
```

```
Hardware is BRI
```

```
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

```
Encapsulation PPP, loopback not set, keepalive set (10 sec)
```

```
LCP Open, multilink Open
```

```
Last input 00:00:00, output 00:00:00, output hang never
```

```
Last clearing of "show interface" counters never
```

```
Queueing strategy: fifo
```

```
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
```

```
5 minute input rate 0 bits/sec, 0 packets/sec
```

```
5 minute output rate 0 bits/sec, 0 packets/sec
```

```
478 packets input, 13592 bytes, 0 no buffer
```

```
Received 474 broadcasts, 0 runts, 0 giants, 0 throttles
```

```
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
509 packets output, 18093 bytes, 0 underruns
```

```
0 output errors, 0 collisions, 0 interface resets
```

```
0 output buffer failures, 0 output buffers swapped out
```

```
104 carrier transitions
```

```
BRI0:2 is down, line protocol is down
```

```
Hardware is BRI
```

```
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

```
Encapsulation PPP, loopback not set, keepalive set (10 sec)
```

```
LCP Closed, multilink Closed
```

```
Closed: IPCP
```

```
Last input 00:09:36, output 00:09:36, output hang never
```

```
Last clearing of "show interface" counters never
```

```
Queueing strategy: fifo
```

```
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
```

```
5 minute input rate 0 bits/sec, 0 packets/sec
```

```
5 minute output rate 0 bits/sec, 0 packets/sec
```

```
23 packets input, 722 bytes, 0 no buffer
```

```
Received 23 broadcasts, 0 runts, 0 giants, 0 throttles
```

```
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
22 packets output, 727 bytes, 0 underruns
```

```
0 output errors, 0 collisions, 0 interface resets
```

```
0 output buffer failures, 0 output buffers swapped out
```

```
2 carrier transitions
```

```
robo-austin# show user
```

Line	User	Host(s)	Idle	Location
* 0 con 0	admin	idle	0	
BR0:1	hq-sanjoe	Sync PPP	00:00:38	

## Step 7—Confirming the Final Running Configuration

Here is the final running configuration for the Cisco 1604:

```

robo-austin# show running
Building configuration...
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname robo-austin
!
aaa new-model
aaa authentication login default local
aaa authentication ppp default if-needed local
enable secret 5 $1$aZlD$wNO7lEpS6y5zRYuW9qFEr.
!
username joe-admin password 7 <removed>
username hq-sanjose password 7 <removed>
isdn switch-type basic-ni!
!
interface Ethernet0
 ip address 10.1.4.1 255.255.255.0
!
interface BRI0
 ip address 10.1.254.4 255.255.255.0
 encapsulation ppp
 no ip route-cache
 dialer map ip 10.1.254.1 name hq-sanjose 14085551234
 dialer load-threshold 60 either
 dialer-group 2
 isdn switch-type basic-ni
 isdn spid1 51255544330101
 isdn spid2 51255544340101
 no cdp enable
 ppp authentication chap callin
 ppp multilink
 hold-queue 75 in
!
ip classless
ip route 0.0.0.0 255.0.0.0 10.1.254.1 permanent
!
!
dialer-list 2 protocol ip permit
!
line con 0
line vty 0 4
!
end

```

## Step 8—Saving the Configuration

Save the configuration to NVRAM by entering the **copy running-config startup-config** command.



# Cisco 766 Configuration

This chapter describes how to configure the Cisco 766 to dial out to the Cisco AS5300.

## Site Profile Characteristics

Figure 4-1 shows the network topology from the Cisco 766's perspective.

**Figure 4-1 Network Topology**

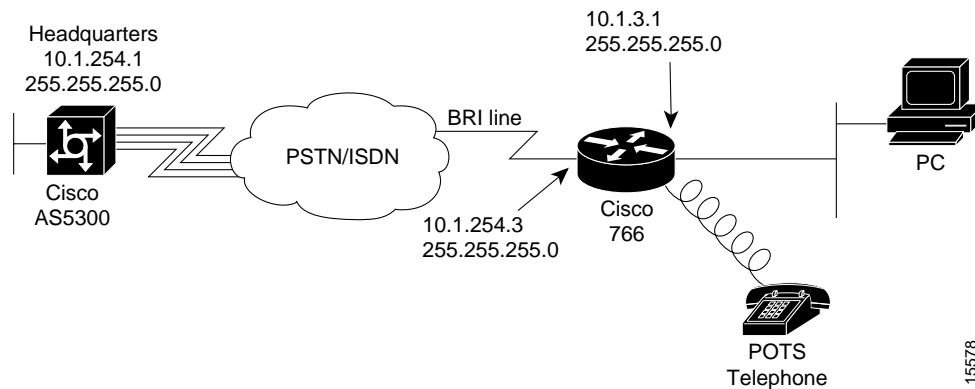


Table 4-1 provides detailed information about each end of the connection. This is the network administrator's top-level design table.

**Table 4-1 Site Characteristics**

Host Name/ Username	Username Password	WAN IP Address <sup>1</sup>	Ethernet IP Address	Assigned Phone Number	Site Hardware
soho-tahoe	tahoe-pw	10.1.254.3 255.255.255.0	10.1.3.1 255.255.255.0	Directory numbers = 5558084 5558085	Cisco 766
hq-sanjose	hq-sanjose-pw	10.1.254.1 255.255.255.0	10.1.1.10 255.255.255.0	4085551234	Cisco AS5300

1. The Cisco 766's default route is 10.1.254.1, which is the Cisco AS5300's dialer interface IP address. This is the next hop IP address.

---

**Note** To enhance readability throughout this chapter, the most important output fields are highlighted with **bold** font. The commands you enter are also **bold** but are preceded by a router prompt.

---

## Overview of Tasks

Perform the following steps:

- “Step 1—Configuring System Level Settings” on page 2
- “Step 2—Configuring the LAN Profile” on page 5
- “Step 3—Configuring the Site Profile hq-sanjose” on page 7
- “Step 4—Testing Connections to the Cisco AS5300” on page 9
- “Step 5—Confirming the Final Running Configuration” on page 11

---

**Note** Before you perform the configuration tasks in this chapter, be sure you understand the overall software configuration action plan. See the chapter “Dial Case Study Overview.”

---

## Step 1—Configuring System Level Settings

System level settings include system name, security, ISDN setup, and PPP setup.

### Configure

To configure the system level settings, use the following commands in system mode:

Step	Command	Purpose
1	> <b>set system soho-tahoe</b>	Enter the host name for this Cisco 766.
2	soho-tahoe> <b>set switch nil</b>	Specify the ISDN switch type that your phone company uses.
3	soho-tahoe> <b>set 1 directorynumber 5558084</b> soho-tahoe> <b>set 2 directorynumber 5558085</b>	Enter the directory numbers for the BRI port’s two B channels.
4	soho-tahoe> <b>set 1 spid 53055580840101</b> soho-tahoe> <b>set 2 spid 53055580850101</b>	Configure your SPIDs, which are required by many switches types. The SPID number is a derivative of the directory number.
5	soho-tahoe> <b>set phone1 5558084</b> soho-tahoe> <b>set phone2 5558085</b>	Enable calls to route to the phone 1 and phone 2 POTS jacks.
6	soho-tahoe> <b>set voicepriority out conditional</b> soho-tahoe> <b>set voicepriority in conditional</b>	Set the incoming and outgoing voice priority mode. It determines whether the system will disconnect a B channel assigned to a data call to allow a voice call.
7	soho-tahoe> <b>set ppp multilink on</b>	Turn on multilink PPP.
8	soho-tahoe> <b>set ppp authentication incoming chap</b>	Authenticate incoming callers using CHAP.
9	soho-tahoe> <b>set ppp secret host</b> Enter new password: <b>tahoe-pw</b> Re-Type new password: <b>tahoe-pw</b>	Specify the CHAP password for authenticating PPP peers. You must enter it twice for verification <sup>1</sup> .

Step	Command	Purpose
10	soho-tahoe> <b>set password system</b> Enter new password: <b>admin-pw</b> Re-Type new password: <b>admin-pw</b>	Protect your Cisco 766 terminal service shell with a password <sup>1</sup> . The system configuration mode can be accessed through the console port or a telnet session <sup>2</sup> .

1. Make sure to use your own secret password. Do not use “tahoe-pw” or “admin-pw.”
2. To modify what is protected by the password, use the **set local access** command.

## Verify

To verify the configuration:

- Enter the **show configuration** command to display a subset of the current configuration parameters:

---

**Note** This case study configures IP routing on the LAN and access profile. The internal profile is not used. See the display field “Profile Parameters.”

---

```
soho-tahoe> show configuration
System Parameters
  Environment
    Screen Length          20
    Echo Mode              ON
    CountryGroup           1
  Bridging Parameters
    LAN Forward Mode      ANY
    WAN Forward Mode      ONLY
    Address Age Time      OFF
  Call Startup Parameters
    Multidestination      OFF
  Line Parameters
    Switch Type           NI-1
    Svc Profile ID 1      53055580840101
    Directory Number(s)   5558084
    Svc Profile ID 2      53055580850101
    Directory Number(s)   5558085
    Auto SPID and Switch Detection  OFF
    Conference access code 60
Transfer access code 61
  Call Parameters
    Retry Delay           Link 1      Link 2
                        30           30
    Button                Standard
Profile Parameters
  Bridging Parameters
    Bridging              ON
    Routed Protocols      NONE
    Learn Mode            ON
    Passthru              OFF
  Call Startup Parameters
  Line Parameters
    Line Speed            AUTO
    Numbering Plan        NORMAL
  Call Parameters
    Auto                  Link 1      Link 2
                        ON           ON
    Called Number
    Backup Number
    Ringback Number
```

```

CLI Validate Number
CLICallback          OFF
CLIAuthentication    OFF
    
```

- Enter the **show security** command to display the current system security configuration:

```

soho-tahoe> show security
System Parameters
Security
  Access Status      ON
  System Password    EXISTS
  Remote Configuration PROTECTED
  Local Configuration ON
  ClickStart         ON
  Logout Timeout     5
  Caller ID Security OFF
  Caller Id Numbers

PPP Security
  PPP Authentication IN  CHAP
  CHAP REFUSE          NONE

Profile Parameters
PPP Security
  PPP Authentication OUT NONE
  PPP Authentication ACCEPT EITHER
  Token Authentication Support
  TAS Client          0.0.0.0
  Use Local CHAP Secret ON
  Client
  User Name           soho-tahoe
  PAP Password        NONE
  CHAP Secret         NONE
  Host
  PAP Password        NONE
  CHAP Secret         EXISTS
  Callback
  Request             OFF
  Reply               OFF
    
```

- Enter the **show status** command:

```

soho-tahoe> show status
Status      01/01/1998 00:01:08
Line Status
  Line Activated
  Terminal Identifier Assigned  SPID Accepted
  Terminal Identifier Assigned  SPID Accepted
Port Status
Connection Link
Ch: 1      Waiting for Call
Ch: 2      Waiting for Call
Interface
    
```

## Step 2—Configuring the LAN Profile

The LAN profile contains the Cisco 766's Ethernet IP address and routing characteristics. Before you configure the LAN profile, you should understand how profiles work.

The Cisco 766's operating system uses a profile model. The LAN and remote site parameters are configured inside profiles. When using the command line interface for configuring the device, the current mode determines the effect and display output of each command. The current mode is indicated by the router prompt. To move between modes, use the **cd** command.

```
soho-tahoe>          <----- This is system mode.
soho-tahoe> cd lan   <----- Change to the LAN profile.
soho-tahoe:LAN> cd hq-sanjose <----- Change to the hq-sanjose profile.
soho-tahoe:hq-sanjose> cd <----- Go back to system mode.
soho-tahoe>
```

---

**Note** For illustrative purposes, the hq-sanjose profile is included in this example. The actual hq-sanjose profile is configured later in the next section “Step 3—Configuring the Site Profile hq-sanjose.”

---

In the following example, notice that the output of the **show security** command is different for each configuration mode.

```
soho-tahoe> show security
System Parameters
  Security
    Access Status           ON
    System Password         EXISTS
    Remote Configuration    PROTECTED
    Local Configuration     ON
    ClickStart              ON
    Logout Timeout          5
    Caller ID Security      OFF
    Caller Id Numbers

  PPP Security
    PPP Authentication IN   CHAP
    CHAP REFUSE             NONE

Profile Parameters
  PPP Security
    PPP Authentication OUT  NONE
    PPP Authentication ACCEPT EITHER
  Token Authentication Support
    TAS Client              0.0.0.0
    Use Local CHAP Secret  ON
  Client
    User Name               soho-tahoe
    PAP Password            NONE
    CHAP Secret             NONE
  Host
    PAP Password            NONE
    CHAP Secret             EXISTS
  Callback
    Request                 OFF
    Reply                   OFF
```

```
soho-tahoe> cd hq-sanjose
soho-tahoe:hq-sanjose> show security

Profile Parameters
  PPP Security
    PPP Authentication OUT      NONE<*>
    PPP Authentication ACCEPT  EITHER
  Token Authentication Support
    TAS Mode                   OFF
    TAS Client                  0.0.0.0
    Use Local CHAP Secret      ON
  Client
    User Name                  soho-tahoe
    PAP Password               NONE
    CHAP Secret                EXISTS
  Host
    PAP Password               NONE
    CHAP Secret                EXISTS
  Callback
    Request                    OFF
    Reply                      OFF
```

## Configure

To configure the LAN profile parameters, use the following commands beginning in system configuration mode:

Step	Command	Purpose
1	soho-tahoe> <b>cd lan</b>	Enter LAN profile mode.
2	soho-tahoe:LAN> <b>set ip address 10.1.3.1</b>	Enter the IP address.
3	soho-tahoe:LAN> <b>set netmask 255.255.255.0</b>	Configure the subnet mask.
4	soho-tahoe:LAN> <b>set bridging off</b>	Turn bridging off.
5	soho-tahoe:LAN> <b>set ip routing on</b>	Turn on IP routing.
6	soho-tahoe:LAN> <b>set ip rip update off</b>	Turn off IP RIP updates.

## Verify

To verify the configuration:

- Enter the **show configuration** command to display the current LAN configuration:

```
soho-tahoe:LAN> show configuration

Profile Parameters
  Bridging Parameters
    Bridging                OFF<*>
    Routed Protocols        IP <*>
    Learn Mode              ON
    Passthru                 OFF
  Call Startup Parameters
  Line Parameters
    Line Speed              AUTO
    Numbering Plan          NORMAL
  Call Parameters
    Auto                    ON                Link 1          Link 2
    Called Number
    Backup Number
```

```

Ringback Number
CLI Validate Number
CLICallback          OFF
CLIAuthentication    OFF

```

- Enter the **show lan packets** command to display packeting statistics associated with the LAN interface:

```

soho-tahoe:LAN> show lan packets
Packet Statistics for LAN
Filtered: 120 Forwarded: 1 Received: 124
Dropped: 0 Lost: 0 Corrupted: 0 Misordered: 0
Ethernet Type: 0800 Count: 15
Ethernet Type: 0806 Count: 7

```

## Step 3—Configuring the Site Profile hq-sanjose

The hq-sanjose profile provides the dialing characteristics for connecting to the Cisco AS5300 (hq-sanjose).

### Configure

To configure the site profile, use the following commands beginning in LAN profile mode:

Step	Command	Purpose
1	soho-tahoe:LAN> <b>set user hq-sanjose</b> soho-tahoe> New user hq-sanjose being created	Create the profile for the headquarters NAS. This profile name must match the PPP name sent by the NAS during CHAP authentication <sup>1</sup> .
2	soho-tahoe:hq-sanjose> <b>set prof power=activate user=hq-sanjose</b> soho-tahoe:hq-sanjose> <b>set active</b>	Ensure that the profile is currently active and active at reboot.
3	soho-tahoe:hq-sanjose> <b>set encaps ppp</b>	Enable PPP encapsulation.
4	soho-tahoe:hq-sanjose> <b>set ip routing on</b>	Turn on IP routing.
5	soho-tahoe:hq-sanjose> <b>set ip framing none</b>	Set IP framing for PPP encapsulation.
6	soho-tahoe:hq-sanjose> <b>set ip address 10.1.254.3</b>	Set the IP address to be used on the WAN port when using this profile. See Table 4-1.
7	soho-tahoe:hq-sanjose> <b>set ip netmask 255.255.255.0</b>	Set the IP netmask address for the dialer cloud.
8	soho-tahoe:hq-sanjose> <b>set ip route destination 0.0.0.0 gateway 10.1.254.1</b>	Create a static route for the next hop, which is the Cisco AS5300's WAN port. IP address 10.1.254.1 is used on the Cisco AS5300's dialer interface <sup>2</sup> .
9	soho-tahoe:hq-sanjose> <b>set bridging off</b>	Turn off bridging.
10	soho-tahoe:hq-sanjose> <b>set ip rip update off</b>	Turn off IP RIP updates.
11	soho-tahoe:hq-sanjose> <b>set number 14085551234</b>	Enter the hq-sanjose telephone number.
12	soho-tahoe:hq-sanjose> <b>set speed 56k</b>	Start your connection testing with 56K, which is often a more dependable connect speed <sup>3</sup> .
13	soho-tahoe:hq-sanjose> <b>set ppp authentication outgoing none</b>	When soho-tahoe dials out, it will not authenticate hq-sanjose.
14	soho-tahoe:hq-sanjose> <b>set ppp authentication incoming chap</b>	All incoming PPP callers are authenticated with CHAP.

### Step 3—Configuring the Site Profile hq-sanjose

Step	Command	Purpose
15	<pre>soho-tahoe:hq-sanjose&gt; set ppp secret client soho-tahoe:hq-sanjose&gt; Enter new Password: tahoe-pw soho-tahoe:hq-sanjose&gt; Re-Type new Password: tahoe-pw</pre>	Specify the secret password to use when soho-tahoe is logging into hq-sanjose <sup>4</sup> .

1. On Cisco IOS devices the PPP name is defined by one of the following commands: **hostname**, **sgbp group**, **ppp pap sent-username**, or **ppp chap hostname**.
2. By definition IP address 10.1.254.1 is connected to the Cisco 766's BRI interface, because the dialer's subnet contains address 10.1.254.1.
3. You are less likely to run into a problem by using 56K. After the connection is up and operational, try to upgrade the speed to 64K. Call blocking is more common at 64K than 56K. During the experiment, check to see if you have any reliability issues. The **set speed auto** command tells the router to try 64K. However, only a 64K end-to-end data path will work. If you are blocked, try again at 56K.
4. This secret client password must match the password configured on hq-sanjose. For example, the password "tahoe-pw" is in the central site's **username soho-tahoe password tahoe-pw** command. See the section "Configuring Site Definitions" in the chapter "Cisco AS5300 Configuration."

## Verify

To verify the configuration:

- Enter the **show security** command to view the security parameters associated with the hq-sanjose profile. Notice that the Cisco 766 is not configured to support PAP.

```
soho-tahoe:hq-sanjose> show security

Profile Parameters
  PPP Security
    PPP Authentication OUT      NONE<*>
    PPP Authentication ACCEPT  EITHER
  Token Authentication Support
    TAS Mode                   OFF
    TAS Client                  0.0.0.0
    Use Local CHAP Secret      ON
  Client
    User Name                  soho-tahoe
    PAP Password               NONE
    CHAP Secret                EXISTS
  Host
    PAP Password               NONE
    CHAP Secret                EXISTS
  Callback
    Request                    OFF
    Reply                      OFF
```

- Enter the **show configuration** command to view the configuration settings for the hq-sanjose profile. Notice that bridging is turned off and IP routing is on. The dialed number for each channel is displayed. Hq-sanjose's phone number is 4085551234.

```
soho-tahoe:hq-sanjose> show configuration

Profile Parameters
  Bridging Parameters
    Bridging                   OFF<*>
    Routed Protocols           IP <*>
    Learn Mode                 ON
    Passthru                   OFF
  Call Startup Parameters
  Line Parameters
    Line Speed                 AUTO
    Numbering Plan             NORMAL
  Call Parameters
    Auto                       ON
    Called Number              14085551234<*>
    Backup Number              14085551234<*>
    Link 1                      Link 2
    Auto                       ON
```

```

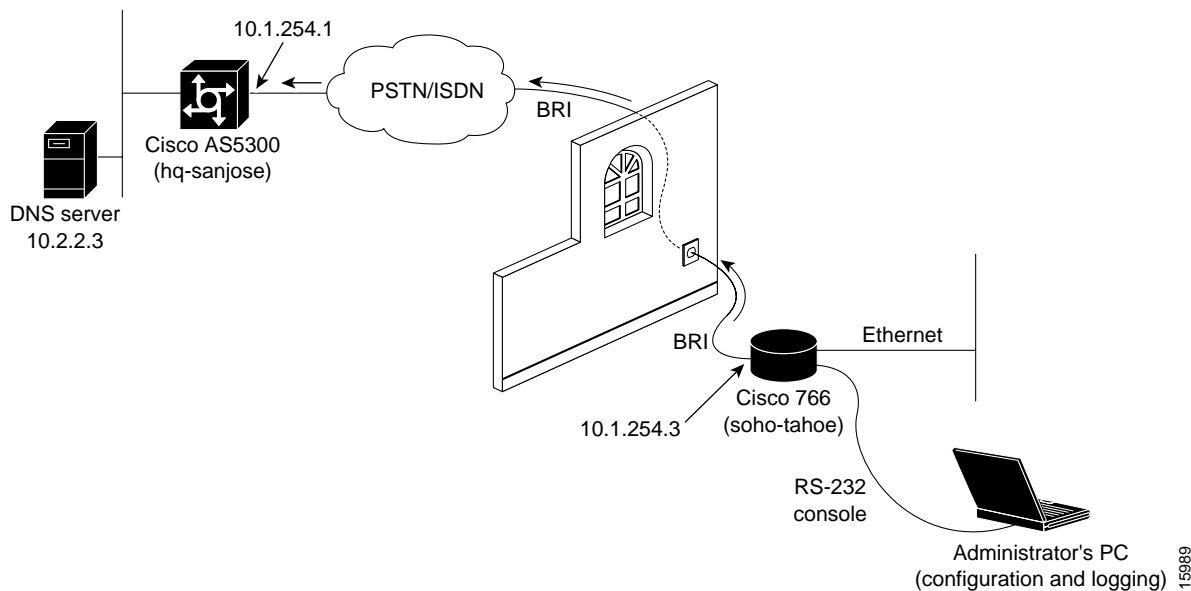
Ringback Number
CLI Validate Number
CLICallback          OFF
CLIAuthentication    OFF

```

## Step 4—Testing Connections to the Cisco AS5300

This section describes how to perform the test. Figure 4-2 shows the actual test lab environment used in this test case.

Figure 4-2 Test Lab Environment



**Step 1** Look at the routing table. Enter the **show ip route** command to verify that the correct routes are set up. Before you try to use IP, you should verify that IP will work.

View this information in the hq-sanjose profile and at the system level. If the profile is shut down, you will not see the route at the system level.

```

soho-tahoe:hq-sanjose> show ip route
Profile          Type Destination      Bits Gateway          Prop Cost Source Age
-----
hq-sanjose      NET  10.1.254.0         24  DIRECT            ON  1  DIRECT  0

soho-tahoe:hq-sanjose> cd
soho-tahoe> show ip route
Profile          Type Destination      Bits Gateway          Prop Cost Source Age
-----
LAN              NET  10.1.3.0           24  DIRECT            ON  1  DIRECT  0
hq-sanjose      NET  10.1.254.0         24  DIRECT            ON  1  DIRECT  0

```

**Step 2** Change to the hq-sanjose profile. Enter the **show connection** command. Verify that no calls are currently connected:

```
soho-tahoe> cd hq-sanjose
soho-tahoe:hq-sanjose> show connection
Connections      01/01/1998 00:04:47
  Start Date & Time # Name                               # Ethernet
  1 01/01/1998 00:00:00 #                               # 00 00 00 00 00 00
  2 01/01/1998 00:02:36 #                               # 00 00 00 00 00 00
```

**Step 3** Call hq-sanjose manually by entering the **call ch2** command. Notice that the call must be initiated from within the hq-sanjose profile:

```
soho-tahoe:hq-sanjose> call ch2
01/01/1998 00:04:50 L05 0 14085551234 Outgoing Call Initiated
01/01/1998 00:04:53 L08 2 14085551234 Call Connected
01/01/1998 00:04:53 Connection 2 Add      Link 1 Channel 2
```

**Step 4** Ping the DNS server, which is behind hq-sanjose and might be several hops away. If it fails, move back and try to ping the closest router (10.1.254.1).

```
soho-tahoe:hq-sanjose> ping 10.2.2.3
Start sending: round trip time is 100 msec.
```

**Step 5** Enter the **show connection** command to verify that the second connection is up:

```
soho-tahoe:hq-sanjose> show connection
Connections      01/01/1998 00:05:42
  Start Date & Time # Name                               # Ethernet
  1 01/01/1998 00:00:00 #                               # 00 00 00 00 00 00
  2 01/01/1998 00:02:36 # hq-sanjose                          #
                               Link: 1 Channel: 2 Phone: 14085551234
```

**Step 6** Enter the **show status** command:

```
soho-tahoe> show status
Status      01/01/1998 00:47:50
Line Status
  Line Activated
  Terminal Identifier Assigned  SPID Accepted
  Terminal Identifier Assigned  SPID Accepted
Port Status
  Ch: 1 56K Call In Progress 14085551234 DATA 2 1
  Ch: 2 Waiting for Call
```

**Step 7** Try pinging the DNS server from a test PC on the local Ethernet LAN. Open the DOS application and enter the **ping** command.

```
Microsoft(R) Windows 95
(C)Copyright Microsoft Corp 1981-1996.

C:\WINDOWS> ping 10.2.2.3
Pinging 10.1.3.2 with 32 bytes of data:

Reply from 10.1.3.2: bytes=32 time=3ms TTL=236
Reply from 10.1.3.2: bytes=32 time=2ms TTL=236
Reply from 10.1.3.2: bytes=32 time=3ms TTL=236
Reply from 10.1.3.2: bytes=32 time=2ms TTL=236
```

### Troubleshooting and Debugging Tips

- Sometimes calls fail because the public phone network is blocking the call, which is beyond your control. Look at the B channel LEDs on the router. If the CH1 light is flashing, it means that the router is trying to place a call. Be patient and wait for the call to go through.
- If problems persist, have the local administrator connect to the command line interface (CLI) of the Cisco700 using telnet or a directly attached console to use various **show** commands, as described in the next bullet.
- Use **log** commands to enhance the output to the CLI. For example, the **log calls verbose** command displays call information on the terminal screen. If calls connect (channel LED on steady) then quickly disconnect, plus you are having serious connection problems, turn on PPP debugging by entering the **diag ppp on | off** command. Be sure to set **diag ppp off** when the function is not in use by an administrator.

## Step 5—Confirming the Final Running Configuration

Here is the final configuration running on the Cisco 766. This configuration file can be used as a basic template for turning up additional remote sites. The **bold** entries are site specific. They should be customized for each site.



**Timesaver** You can save time configuring a Cisco 766 by pasting a configuration file directly into a router. To do this, first return the router to its default state using the **set default** command. The router has no running configuration after this command is entered. Next, paste in the configuration file.

```

set system soho-tahoe
set switch nil
set 1 spid 53055580840101
set 2 spid 53055580850101
set 1 directorynumber 5558084
set 2 directorynumber 5558085
set phone1 5558084
set phone2 5558085
set voice out conditional
set voice in conditional
set ppp multilink on
set ppp authentication incoming chap
set ppp secret host
tahoe-pw
tahoe-pw
set password system
admin-pw
admin-pw
cd lan
set ip address 10.1.3.1
set ip netmask 255.255.255.0
set ip routing on
set ip rip update off
set bridging off
cd
set user hq-sanjose
set prof power=activate user=hq-sanjose
cd hq-sanjose
set active
set encaps ppp
set ip routing on
set ip framing none
set ip address 10.1.254.3

```

## Step 5—Confirming the Final Running Configuration

---

```
set ip netmask 255.255.0.0
set ip pat off
set ip rip update off
set ip route destination 0.0.0.0 gateway 10.1.254.1
set bridging off
set number 14085551234
set speed 56
set ppp authentication outgoing none
set ppp authentication incoming chap
set ppp secret client
tahoe-pw
tahoe-pw
cd
reboot
```

After you verify that the configuration works, initiate an upload at the end of the session and save it. An upload displays the setting of every configuration parameter on the Cisco 766.

```
soho-tahoe> upl
CD
SET SCREENLENGTH 20
SET COUNTRYGROUP 1
SET LAN MODE ANY
SET WAN MODE ONLY
SET AGE OFF
SET MULTIDESTINATION OFF
SET SWITCH NI-1
SET 1 SPID 53055580840101
SET 1 DIRECTORYNUMBER 5558084
SET PHONE1 = 5558084
SET 2 SPID 53055580850101
SET 2 DIRECTORYNUMBER 5558085
SET PHONE2 = 5558085
SET AUTODETECTION OFF
SET CONFERENCE 60
SET TRANSFER 61
SET 1 DELAY 30
SET 2 DELAY 30
SET BRIDGING ON
SET LEARN ON
SET PASSTHRU OFF
SET SPEED AUTO
SET PLAN NORMAL
SET 1 AUTO ON
SET 2 AUTO ON
SET 1 NUMBER
SET 2 NUMBER
SET 1 BACKUPNUMBER
SET 2 BACKUPNUMBER
SET 1 RINGBACK
SET 2 RINGBACK
SET 1 CLIVALIDATENUMBER
SET 2 CLIVALIDATENUMBER
SET CLICALLBACK OFF
SET CLIAUTHENTICATION OFF
SET SYSTEMNAME SOHO-TAHOE
LOG CALLS TIME VERBOSE
SET UNICASTFILTER OFF
DEMAND 1 THRESHOLD 0
DEMAND 2 THRESHOLD 48
DEMAND 1 DURATION 1
DEMAND 2 DURATION 1
DEMAND 1 SOURCE LAN
DEMAND 2 SOURCE BOTH
TIMEOUT 1 THRESHOLD 0
```

```
TIMEOUT 2 THRESHOLD 48
TIMEOUT 1 DURATION 0
TIMEOUT 2 DURATION 0
TIMEOUT 1 SOURCE LAN
TIMEOUT 2 SOURCE BOTH
SET PASSWORD SYSTEM ENCRYPTED 0500120632484048
SET REMOTEACCESS PROTECTED
SET LOCALACCESS ON
SET CLICKSTART ON
SET LOGOUT 5
SET CALLERID OFF
SET PPP AUTHENTICATION IN CHAP
SET PPP CHAPREFUSE NONE
SET PPP AUTHENTICATION OUT NONE
SET PPP AUTHENTICATION ACCEPT EITHER
SET PPP TAS CLIENT 0.0.0.0
SET PPP TAS CHAPSECRET LOCAL ON
SET PPP SECRET HOST ENCRYPTED 10471a1d0b43191f4d45
SET PPP CALLBACK REQUEST OFF
SET PPP CALLBACK REPLY OFF
SET PPP NEGOTIATION INTEGRITY 10
SET PPP NEGOTIATION COUNT 10
SET PPP NEGOTIATION RETRY 3000
SET PPP TERMREQ COUNT 2
SET PPP MULTILINK ON
SET COMPRESSION STAC
SET PPP BACP ON
SET PPP ADDRESS NEGOTIATION LOCAL OFF
SET PPP IP NETMASK LOCAL OFF
SET IP PAT UDPTIMEOUT 5
SET IP PAT TCPTIMEOUT 30
SET IP RIP TIME 30
SET CALLDURATION 0
SET SNMP CONTACT ""
SET SNMP LOCATION ""
SET SNMP TRAP COLDSTART OFF
SET SNMP TRAP WARMSTART OFF
SET SNMP TRAP LINKDOWN OFF
SET SNMP TRAP LINKUP OFF
SET SNMP TRAP AUTHENTICATIONFAIL OFF
SET DHCP OFF
SET DHCP DOMAIN
SET DHCP NETBIOS_SCOPE
SET VOICEPRIORITY INCOMING INTERFACE PHONE1 CONDITIONAL
SET VOICEPRIORITY OUTGOING INTERFACE PHONE1 CONDITIONAL
SET CALLWAITING INTERFACE PHONE1 ON
SET VOICEPRIORITY INCOMING INTERFACE PHONE2 CONDITIONAL
SET VOICEPRIORITY OUTGOING INTERFACE PHONE2 CONDITIONAL
SET CALLWAITING INTERFACE PHONE2 ON
SET CALLTIME VOICE INCOMING OFF
SET CALLTIME VOICE OUTGOING OFF
SET CALLTIME DATA INCOMING OFF
SET CALLTIME DATA OUTGOING OFF
SET USER LAN
SET BRIDGING OFF
SET IP ROUTING ON
SET IP ADDRESS 10.1.3.1
SET IP NETMASK 255.255.255.0
SET IP FRAMING ETHERNET_II
SET IP PROPAGATE ON
SET IP COST 1
SET IP RIP RECEIVE V1
SET IP RIP UPDATE OFF
SET IP RIP VERSION 1
SET USER Internal
```

## Step 5—Confirming the Final Running Configuration

---

```
SET IP FRAMING ETHERNET_II
SET USER Standard
SET PROFILE ID 000000000000
SET PROFILE POWERUP ACTIVATE
SET PROFILE DISCONNECT KEEP
SET IP ROUTING ON
SET IP ADDRESS 0.0.0.0
SET IP NETMASK 0.0.0.0
SET IP FRAMING NONE
SET IP RIP RECEIVE V1
SET IP RIP UPDATE OFF
SET IP RIP VERSION 1
SET USER HQ-SANJOSE
SET PROFILE ID 000000000000
SET PROFILE POWERUP ACTIVATE
SET PROFILE DISCONNECT KEEP
SET BRIDGING OFF
SET SPEED 56K
SET 1 NUMBER 14085551234
SET 2 NUMBER 14085551234
SET PPP AUTHENTICATION OUT NONE
SET PPP SECRET CLIENT ENCRYPTED 020f175f055204350d0f
SET IP ROUTING ON
SET IP ADDRESS 10.1.254.3
SET IP NETMASK 255.255.0.0
SET IP FRAMING NONE
SET IP PROPAGATE ON
SET IP COST 1
SET IP RIP RECEIVE V1
SET IP RIP UPDATE OFF
SET IP RIP VERSION 1
SET IP PAT OFF
SET IP ROUTE DEST 0.0.0.0/0 GATEWAY 10.1.254.1 PROPAGATE OFF COST 1
CD
SET BUTTON Standard
LOGOUT
```