



Configuring the Cisco 766 Router

This chapter describes how to configure the Cisco 766 Router to dial out to the Cisco AS5300 as described in Chapter 1, “Dial Case Study Overview”.

Network Topology, Hardware, and Software Selections

Figure 4-1 Case Study Scenario Network Topology from the Perspective of the Cisco 766

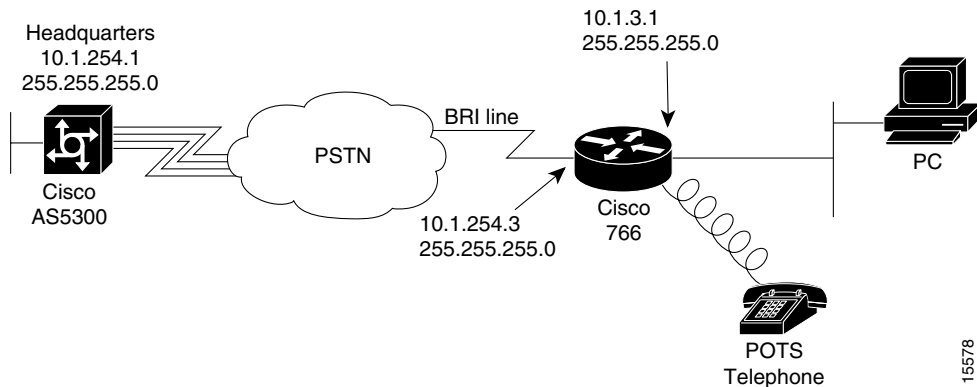


Table 4-1 provides detailed information about each end of the connection as illustrated in Figure 4-1. This is the network administrator’s top-level design table. The Cisco 766’s default route is 10.1.254.1, which is the Cisco AS5300’s configured dialer interface IP address and is the next-hop IP address.

Table 4-1 Network Device Characteristics

Site Hardware	WAN IP Address	Ethernet IP Address	Assigned Phone Number	Host Name/ User Name	Username Password
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 AS5300	10.1.254.1 255.255.255.0 Dialer Interface	10.1.1.10 255.255.255.0	4085551234	hq-sanjose	hq-sanjose-pw

Overview of Steps

Follow these steps to configure your Cisco 766 router for connection to the network:

- Step 1—Configuring System Level Settings
- Step 2—Configuring the LAN Profile
- Step 3—Configuring the Site Profile hq-sanjose
- Step 4—Testing the Cisco 766's Connection to the Cisco AS5300
- Step 5—Confirming the Final Cisco 766 Running Configuration
- Step 6—Saving the Configuration

Step 1—Configuring System Level Settings

System level settings include system name, security, ISDN setup, and PPP setup. To configure the system level settings, enter the following commands in system mode:

-
- Step 1** Enter the host name for this Cisco 766.
- ```
> set system soho-tahoe
```
- Step 2** Specify the ISDN switch type that the local phone company uses.
- ```
soho-tahoe> set switch nil
```
- Step 3** Enter the directory numbers for the BRI port's two B channels.
- ```
soho-tahoe> set 1 directorynumber 5558084
soho-tahoe> set 2 directorynumber 5558085
```
- Step 4** Configure your SPIDs, which are required by many switch types. The SPID number is a derivative of the directory number.
- ```
soho-tahoe> set 1 spid 53055580840101
soho-tahoe> set 2 spid 53055580850101
```
- Step 5** Enable calls to route to the phone 1 and phone 2 POTS jacks.
- ```
soho-tahoe> set phone1 5558084
soho-tahoe> set phone2 5558085
```
- Step 6** Set the incoming and outgoing voice priority mode that determines whether the system will disconnect a B channel assigned to a data call to allow a voice call.
- ```
soho-tahoe> set voicepriority out conditional
soho-tahoe> set voicepriority in conditional
```
- Step 7** Turn on multilink PPP.
- ```
soho-tahoe> set ppp multilink on
```
- Step 8** Authenticate incoming callers by using CHAP
- ```
soho-tahoe> set ppp authentication incoming chap
```

- Step 9** Specify the CHAP password for authenticating PPP peers. You must enter it twice for verification. Use your own secret password. Do not use “tahoe-pw” or “admin-pw”.

```
soho-tahoe> set ppp secret host
Enter new password: tahoe-pw
Re-Type new password: tahoe-pw
```

- Step 10** Protect the Cisco 766 terminal service shell with a password. Again, be sure to use your own secret password instead of “tahoe-pw” or “admin-pw”. You can access the system configuration mode through the console port or a Telnet session. To modify what is protected by the password, enter the **set local access** command.

```
soho-tahoe> set password system
Enter new password: admin-pw
Re-Type new password: admin-pw
```

Verifying System Level Setting Configuration

To verify the Cisco 766’s system-level setting configuration:

- Step 1** Enter the **show configuration** command to see 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           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         Link 1          Link 2
  Auto                   ON             ON
  Called Number
  Backup Number
  Ringback Number
  CLI Validate Number
CLICallback             OFF
CLIAuthentication       OFF

```

Step 2 Enter the **show security** command to see 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

```

Step 3 Enter the **show status** command to see the Cisco 766's line and port status:

```

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

```

Step 2—Configuring the LAN Profile

The LAN profile contains the Cisco 766's Ethernet IP address and routing characteristics.

The Cisco 766's operating system uses a profile model as its configuration scheme. The LAN and remote site parameters are configured inside profiles. When you use the command-line interface for configuring the Cisco 766, 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 (change directories), enter 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

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, note that the output of the **show security** command is different for each configuration mode or profile:

```
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

```

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

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

Verifying the LAN Profile Parameters

To verify the LAN profile parameters:

- Step 1** Enter the **show configuration** command to see 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           Link 1           Link 2
    Auto                     ON             ON
    Called Number
    Backup Number
    Ringback Number
    CLI Validate Number
  CLICallback               OFF
  CLIAuthentication         OFF
```

- Step 2** Enter the **show lan packets** command to see 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 is used for configuring the dialing characteristics for connecting to the Cisco AS5300 (hq-sanjose).

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

- Step 1** Set a profile name that matches the PPP name sent by the NAS during CHAP authentication to create the profile for the headquarters NAS. On Cisco IOS devices the PPP name is defined by using one of the following commands: **hostname**, **sgbp group**, **ppp pap sent-username**, or **ppp chap hostname**.

```
soho-tahoe:LAN> set user hq-sanjose
soho-tahoe> New user hq-sanjose being created
```

- Step 2** Ensure that the profile is currently active and active at reboot.

```
soho-tahoe:hq-sanjose> set prof power=activate user=hq-sanjose
soho-tahoe:hq-sanjose> set active
```

- Step 3** Enable PPP encapsulation.
- ```
soho-tahoe:hq-sanjose> set encap ppp
```
- Step 4** Turn on IP routing.
- ```
soho-tahoe:hq-sanjose> set ip routing on
```
- Step 5** Set IP framing for PPP encapsulation.
- ```
soho-tahoe:hq-sanjose> set ip framing none
```
- Step 6** Set the IP address to be used on the WAN port when using this profile. See Table 4-1.
- ```
soho-tahoe:hq-sanjose> set ip address 10.1.254.3
```
- Step 7** Set the IP netmask address for the dialer cloud.
- ```
soho-tahoe:hq-sanjose> set ip netmask 255.255.255.0
```
- Step 8** 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.
- ```
soho-tahoe:hq-sanjose> set ip route destination 0.0.0.0 gateway 10.1.254.1
```
- Step 9** Turn off bridging.
- ```
soho-tahoe:hq-sanjose> set bridging off
```
- Step 10** Turn off IP RIP updates.
- ```
soho-tahoe:hq-sanjose> set ip rip update off
```
- Step 11** Enter the hq-sanjose telephone number.
- ```
soho-tahoe:hq-sanjose> set number 14085551234
```
- Step 12** Start your connection testing with 56K, which is often a more dependable connect speed than 64K. After the connection is up and running, try to upgrade the speed to 64K. However, call blocking is more common at 64K. If you are blocked, try again at 56K.
- ```
soho-tahoe:hq-sanjose> set speed 56k
```
- Step 13** Set the Cisco 766 such that when soho-tahoe dials out, it will not authenticate hq-sanjose.
- ```
soho-tahoe:hq-sanjose> set ppp authentication outgoing none
```
- Step 14** Authenticate all incoming PPP callers with CHAP.
- ```
soho-tahoe:hq-sanjose> set ppp authentication incoming chap
```
- Step 15** Specify the secret password to use when soho-tahoe is logging in to hq-sanjose. 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."
- ```
soho-tahoe:hq-sanjose> set ppp secret client
soho-tahoe:hq-sanjose> Enter new Password: tahoe-pw
soho-tahoe:hq-sanjose> Re-Type new Password: tahoe-pw
```
-

# Verifying the Site Profile Configuration

To verify the Cisco 766's site profile configuration:

- Step 1** Enter the **show security** command to see the security parameters associated with the hq-sanjose profile. Note 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
```

- Step 2** Enter the **show configuration** command to view the configuration settings for the hq-sanjose profile. Note that bridging is turned off, and IP routing is on. The dialed number (shown as "Called Number" in the example below) for each channel will be displayed. Hq-sanjose's phone number is 4085551234.

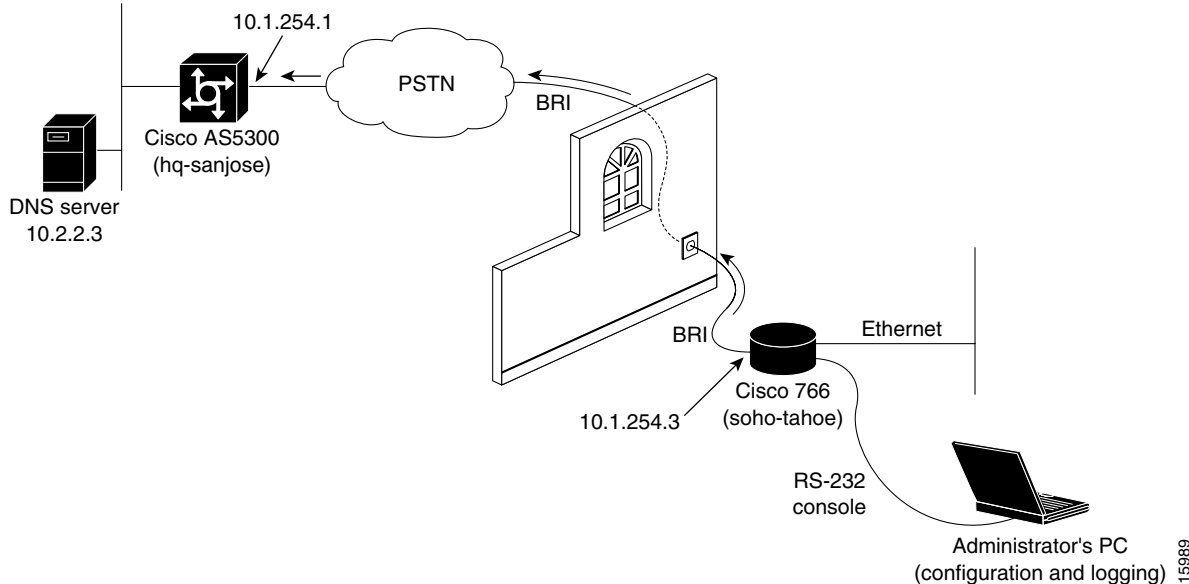
```
soho-tahoe:hq-sanjose> show configuration
```

```
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
 Ringback Number
 CLI Validate Number
 CLICallback OFF
 CLIAuthentication OFF
```

## Step 4—Testing the Cisco 766's Connection to the Cisco AS5300

The test strategy is to ping the Cisco AS5300's WAN port; then, ping the backbone behind the Cisco AS5300 network access server. Ping the domain name server (DNS) on the backbone since this device should always be running.

Figure 4-2 Case Study Lab Environment for Testing the Cisco 766's Connection to the Cisco AS5300



**Step 1** Enter the **show ip route** command to verify that the correct routes are set up. Compare the information displayed with the routing table. Before you try to use IP, verify that it works.

Examine the 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. Note 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 this ping fails, move back and 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 to see whether or not the call is connected and in progress:

```
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** Ping the DNS server from a test PC on the local Ethernet LAN by opening the DOS application and entering 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
```



### 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. Wait for the call to go through.
- If problems persist, have the local administrator connect to the command-line interface (CLI) of the Cisco 766 by using telnet or a directly attached console to enter various **show** commands:
- Enter **log** commands to enhance the output to the CLI.

For example, entering the **log calls verbose** command shows call information on the terminal screen. If calls connect (channel LED on steady) then quickly disconnect, and 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.

## Step 5—Confirming the Final Cisco 766 Running Configuration

You can see a file of the final configuration running on the Cisco 766 by entering the **show running** command. Use this file as a basic template for adding more remote sites. Entries in **bold** are site specific; customize them for each site.



### Timesaver

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

The following output was produced by entering the **show running** command at the CLI prompt:

```

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
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

```

## Step 6—Saving the Configuration

- Step 1** After you verify that the configuration works, use your terminal emulation program to send the current configuration to the console port for display on your terminal.
- Step 2** Use the **upload** command at the command line prompt to display the setting of every configuration parameter on the Cisco 766. Do not press Return after you enter the command:
- Step 3** From the Transfer menu, select Receive Text File.
- Step 4** In the Receive Text dialog box, specify a filename to save the configuration in, and select the directory where you want to save the file.
- Step 5** Click OK.
- Step 6** Return to the terminal emulation program, and press Return to execute the command. The configuration is saved to the file specified in Step 4.

```

soho-tahoe> upload
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
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 BUTTTON Standard
LOGOUT
```

---

