

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

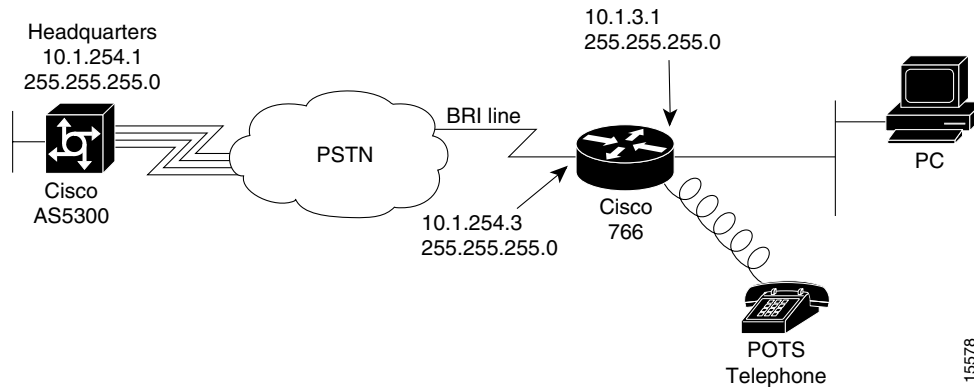


Table 4-1 provides detailed information about each end of the connection. This is the network administrator’s top-level design table.

Table 4-1 Site Characteristics

Host Name/ Username	Username Password	WAN IP Address ¹	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	> set system soho-tahoe	Enter the host name for this Cisco 766.
2	soho-tahoe> set switch nil	Specify the ISDN switch type that your phone company uses.
3	soho-tahoe> set 1 directorynumber 5558084 soho-tahoe> set 2 directorynumber 5558085	Enter the directory numbers for the BRI port’s two B channels.
4	soho-tahoe> set 1 spid 53055580840101 soho-tahoe> set 2 spid 53055580850101	Configure your SPIDs, which are required by many switches types. The SPID number is a derivative of the directory number.
5	soho-tahoe> set phone1 5558084 soho-tahoe> set phone2 5558085	Enable calls to route to the phone 1 and phone 2 POTS jacks.
6	soho-tahoe> set voicepriority out conditional soho-tahoe> set voicepriority in conditional	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> set ppp multilink on	Turn on multilink PPP.
8	soho-tahoe> set ppp authentication incoming chap	Authenticate incoming callers using CHAP.
9	soho-tahoe> set ppp secret host Enter new password: tahoe-pw Re-Type new password: tahoe-pw	Specify the CHAP password for authenticating PPP peers. You must enter it twice for verification ¹ .

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

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
```

Step 2—Configuring the LAN Profile

```
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> cd lan	Enter LAN profile mode.
2	soho-tahoe:LAN> set ip address 10.1.3.1	Enter the IP address.
3	soho-tahoe:LAN> set netmask 255.255.255.0	Configure the subnet mask.
4	soho-tahoe:LAN> set bridging off	Turn bridging off.
5	soho-tahoe:LAN> set ip routing on	Turn on IP routing.
6	soho-tahoe:LAN> set ip rip update off	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 2
                             ON           ON
    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> set user hq-sanjose 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 ¹ .
2	soho-tahoe:hq-sanjose> set prof power=activate user=hq-sanjose soho-tahoe:hq-sanjose> set active	Ensure that the profile is currently active and active at reboot.
3	soho-tahoe:hq-sanjose> set encaps ppp	Enable PPP encapsulation.
4	soho-tahoe:hq-sanjose> set ip routing on	Turn on IP routing.
5	soho-tahoe:hq-sanjose> set ip framing none	Set IP framing for PPP encapsulation.
6	soho-tahoe:hq-sanjose> set ip address 10.1.254.3	Set the IP address to be used on the WAN port when using this profile. See Table 4-1.
7	soho-tahoe:hq-sanjose> set ip netmask 255.255.255.0	Set the IP netmask address for the dialer cloud.
8	soho-tahoe:hq-sanjose> set ip route destination 0.0.0.0 gateway 10.1.254.1	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 ² .
9	soho-tahoe:hq-sanjose> set bridging off	Turn off bridging.
10	soho-tahoe:hq-sanjose> set ip rip update off	Turn off IP RIP updates.
11	soho-tahoe:hq-sanjose> set number 14085551234	Enter the hq-sanjose telephone number.
12	soho-tahoe:hq-sanjose> set speed 56k	Start your connection testing with 56K, which is often a more dependable connect speed ³ .
13	soho-tahoe:hq-sanjose> set ppp authentication outgoing none	When soho-tahoe dials out, it will not authenticate hq-sanjose.
14	soho-tahoe:hq-sanjose> set ppp authentication incoming chap	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> set ppp secret client soho-tahoe:hq-sanjose> Enter new Password: tahoe-pw soho-tahoe:hq-sanjose> Re-Type new Password: tahoe-pw</pre>	Specify the secret password to use when soho-tahoe is logging into hq-sanjose ⁴ .

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
```

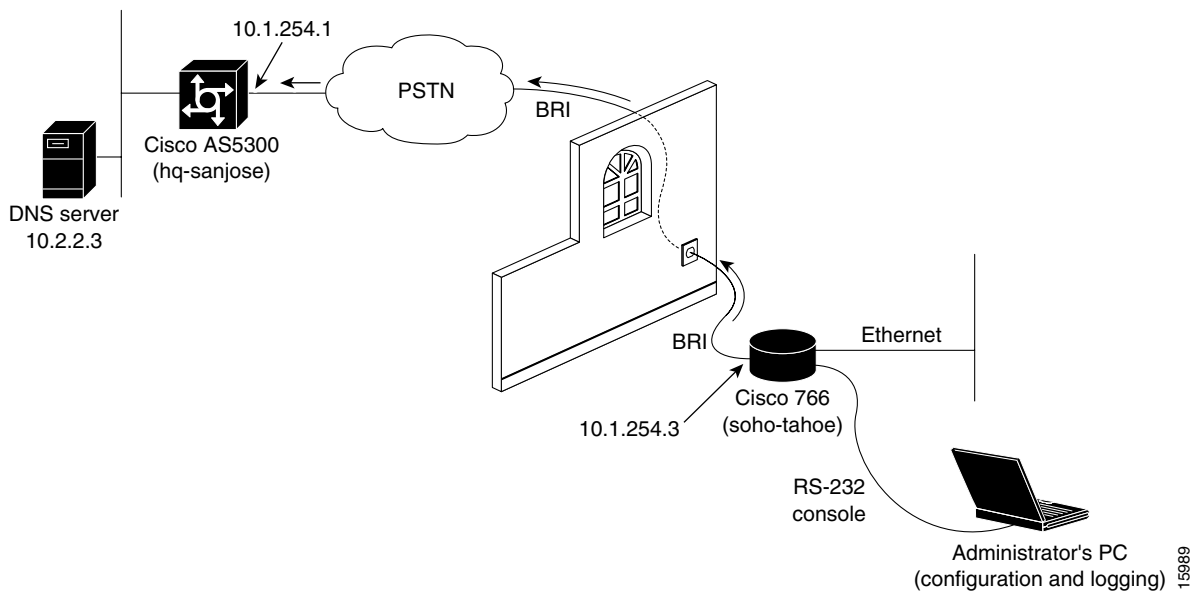
```

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
```