APPENDIX C

Troubleshooting Cisco Switch Signaling

Revised: March 7, 2011, OL-0800-14

Deploy two Cisco switches in fault-tolerant, Cisco telephony solutions. Both switches are active. Virtual local-area networks (VLANs) are set up within these switches. System components use these VLANs to route message traffic to other system components.

Normally, at least two Cisco SS7 interfaces are connected to each switch for redundancy. SS7 call messages travel from the interfaces through the VLANs to the Cisco PGW 2200 Softswitches. Use these VLANs to link the Cisco PGW 2200 Softswitches to the media gateways.

This chapter includes the following sections:

VLANs

Configure VLANs on each switch to simplify management. All intrasystem Ethernet message traffic is partitioned and routed over VLANs according to component origination and destination. The active VLAN configuration is the same as the configuration of the standby VLANs.

Command Line Interface

Access the Command Line Interface (CLI) either locally through a console terminal that is connected to an EIA/TIA-232 port or remotely through a Telnet session. Telnet session access requires a previously set IP address for the switch. Telnet sessions are automatically disconnected after remaining idle for a configurable period.

There are two modes of operation, normal and privileged. Both modes are password protected. Normal-mode commands are used for everyday system monitoring. Privileged commands are used for system configuration and basic troubleshooting.

After you log in successfully, the system automatically enters normal mode, which gives you access to normal-mode commands only. Enter privileged mode by entering the **enable** command that requires a second password. The appearance of the word “enable” indicates privileged mode immediately after the system prompt. To return to normal mode, enter the disable command at the prompt.

Commands that are entered from the CLI can apply to the entire system or to a specific module, port, or VLAN. Modules (module slots), ports, and VLANs are numbered starting with 1.

To reference a specific port on a specific module, the command syntax is mod_num/port_num. For example, 3/1 denotes module 3, port 1. In some commands, such as set trunk, set cam, and set VLAN commands, you can enter lists of ports and VLANs. Designate ports by entering the module and port number. Separate the module and port number pairs with commas. To specify a range of ports, use a dash (-) between the module number and port number pairs. Dashes take precedence over commas.

The following examples show several ways to designate ports:

Example 1: `2/1,2/3 denotes module 2, port 1 and module 2, port 3`
Example 2: `2/1-12 denotes module 2, ports 1 through 12`
Example 3: `2/1-2/12 is the same as Example 2`

A single number designates each VLAN. You specify lists of VLANs in the same way that you do for ports. Separate individual VLANs with commas (,). Separate ranges with dashes (-). The following example specifies VLAN numbers 1 through 10:

```
1-10,1000
```

Some commands require a MAC address, IP address, or IP alias, which must be designated in a standard format. The MAC address format must be six hyphen-separated hexadecimal numbers, as shown in the following example:

```
00-00-0c-24-d2-fe
```

The IP address format is 32 bits, written as four octets, which are separated by periods (dotted decimal format). The address includes a network section, an optional subnet section, and a host section, as shown in the following example:

```
126.2.54.1
```

If the IP alias table is configured, you can use IP aliases in place of the dotted decimal IP address. This option is available for most commands that use an IP address, except commands that define the IP address or IP alias. For more information about the set interface and set IP alias commands, see the command reference for your switch.

Command Line Interface Local Access

To obtain local access to the CLI, complete the following steps:

Step 1 At the Console> prompt, press **Return** (or **Enter**).

Step 2 At the Enter Password: prompt, enter the system password. The Console> prompt indicates that you have successfully accessed the CLI in normal operation mode.

Step 3 Enter the necessary commands to complete the required task.

Step 4 Enter **quit** and press **Return** (or **Enter**) to exit the session.

Command Line Interface Remote Access

To get remote access to the CLI, complete the following steps:

Step 1 From the remote host, enter the Telnet command and designate the name or IP address of the switch you wish to access (Telnet hostname | IP address).

Step 2 At the Enter Password: prompt, enter the password for the CLI. There is no default password (press **Return** or **Enter**) unless a password was previously established using the set password command.

Step 3 Enter the necessary commands to complete the required task.

Step 4 Enter quit and press **Return** (or **Enter**) to exit the Telnet session.

Troubleshooting Virtual Pathways and ISLs

Use a recommended protocol analyzer (locally or remotely) equipped with a **ping** utility to perform Ethernet echo response tests to identify switch hardware, VLAN, and ISL connectivity problems. Use echo to see if another host is active on the network. The ping sender initializes the identifier and sequence number, which is used if multiple echo requests are sent. The ping sender adds some data to the data field, and sends the ICMP echo to the destination host. The ICMP header code field is zero. The recipient changes the type to Echo Reply and returns the datagram to the sender. Use this mechanism to determine if a destination host is reachable.

To use the **ping** command, complete the following steps:

Step 1 Log in to the CLI and enter the command:

```
Console> show port status
```

The command displays a response like the following:

```
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 1/1                     connected  523        normal   half   100 100BaseTX
 1/2                     notconnect 1          normal   half   100 100BaseTX
 2/1                     connected  trunk      normal   half   400 Route Switch
 3/1                     notconnect trunk      normal   full   155 OC3 MMF ATM
 5/1                     notconnect 1          normal   half   100 FDDI
 5/2                     notconnect 1          normal   half   100 FDDI
```

Step 2 Enter the CLI command **show vlan**.

```
Console> (enable) show vlan 998
```

The command displays a response like the following:

```
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- ------------------------
998  VLAN0998                         active    357


VLAN Type  SAID       MTU   Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ ------ ---- -------- ------ ------
998  trcrf 100998     4472  999    0xff   -      -    srb      0      0
```

```
VLAN AREHops STEHops Backup CRF
---- ------- ------- ----------
998  10      10      off
```

Step 3 Enter (for ISLs) the command **show trunk**.

```
Console> (enable) show trunk
```

The command displays a response like the following:

```
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/1      desirable    dot1q          trunking      1
 2/2      desirable    dot1q          trunking      1

Port      Vlans allowed on trunk
--------  ----------------------------------------------------
 2/1      1-1005
 2/2      1-1005

Port      Vlans allowed and active in management domain
--------  ----------------------------------------------------
 2/1      1,10,20,30,40,50,60
 2/2      1,10,20,30,40,50,60

Port      Vlans in spanning tree forwarding state and not pruned
--------  ----------------------------------------------------
 2/1      1,10,20,30,40,50,60
 2/2      1,10,20,30,40,50,60
```

Step 4 Use a **ping** utility to test the desired ports, VLANs, and ISLs.

Step 5 Check the switch equipment status, as described in the associated documentation. Replace suspected hardware, and then return to Step 1 to verify switch operation.