Cisco AS5850 Universal Gateway Commissioning Guidelines

These guidelines detail Cisco AS5850 commissioning, from formal functional setup of the equipment, through systematic software configurations, to initial preparation of the system for data/voice call processing, using local-based authentication.

Use this guide in conjunction with these other Cisco AS5850 documents:

- *Cisco AS5850 Universal Gateway Hardware Installation Guide* at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5850/hw_inst/5850hig/
- *Cisco AS5850 Universal Gateway Card Guide* at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5850/hw_inst/5850cg/
- *Cisco AS5850 Operations, Administration, Maintenance, and Provisioning Guide* at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5850/sw_conf/5850oamp/

Contents

Information About Cisco AS5850 Universal Gateway Commissioning

To build a network using the Cisco AS5850, it is necessary to understand the following:

- The route-switch-controller (RSC) card
- Call-processing components

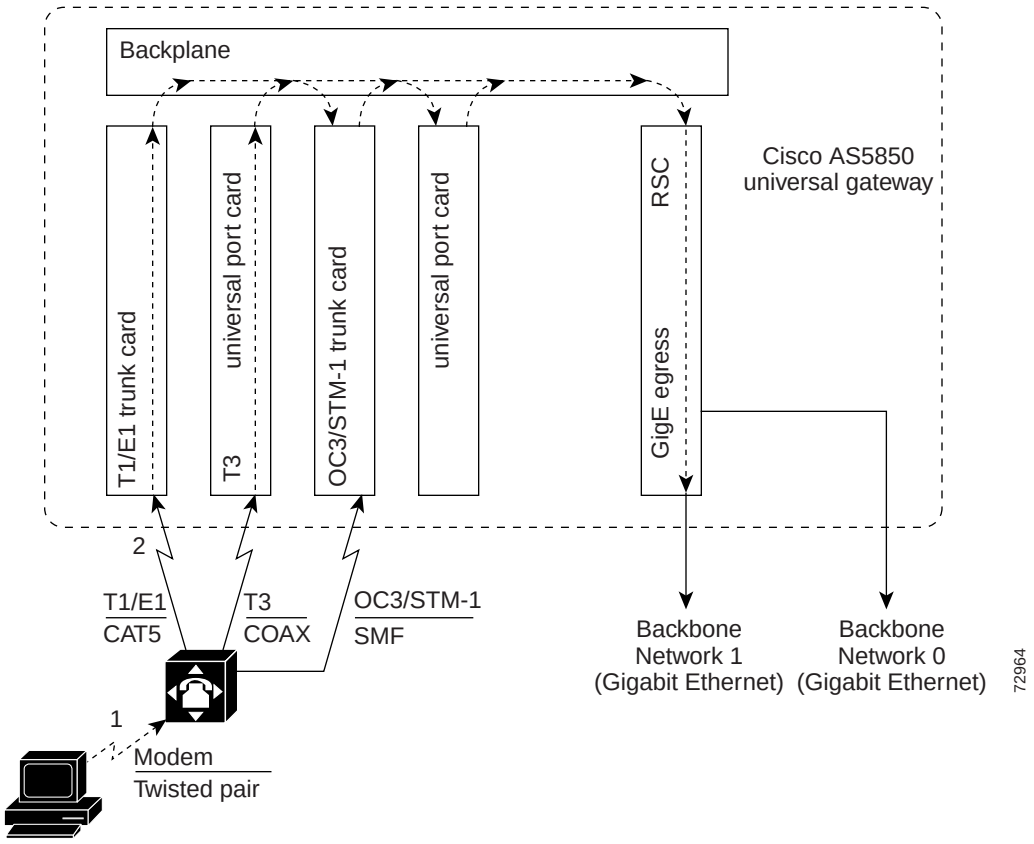
Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

The Cisco AS5850 universal gateway basic interfaces are as follows:

- Egress connects to the IP backbone
- Ingress connects from the PSTN

Figure 1 shows the Cisco AS5850 system architecture.

Figure 1 Cisco AS5850 System Architecture



Route-Switch-Controller Card

The route-switch-controller (RSC) card is the main processor card for the universal gateway. It installs in either slot 6 or slot 7 and plugs directly into the backplane, and performs the following functions:

- Transfers data as Fast Ethernet or Gigabit Ethernet packets encapsulated in proprietary protocol. This connection is also used for management.
- For egress, can connect to the IP backbone via two Gigabit Ethernet ports (in Figure 1, the RSC card uses GigabitEthernet6/0 or GigabitEthernet6/1 to connect to the IP backbone).
- Boots and reloads its own Cisco IOS software image.
- Provides source clocks for use by all feature cards and power supplies. Extracts an external reference clock from an external E1 or T1 signal through a BNC connector on the front panel.
- Can connect to an external alarm source through a DB-15 serial connector on the front panel.
- Provides a console port for initial configuration and maintenance.

- Supports SNMP for management information and enables retrieval of syslog information for troubleshooting.
- Provides high availability when configured in handover-split mode.

Note If there are two RSCs in the chassis, they can be configured in classic-split mode or handover-split mode. For more information on configuring the RSC, see the *Cisco AS5850 Operations, Administration, Maintenance, and Provisioning Guide* at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5850/sw_conf/5850oamp/index.htm.

The Dial Shelf Interconnect Protocol (DSIP) enables communication between RSC and feature cards:

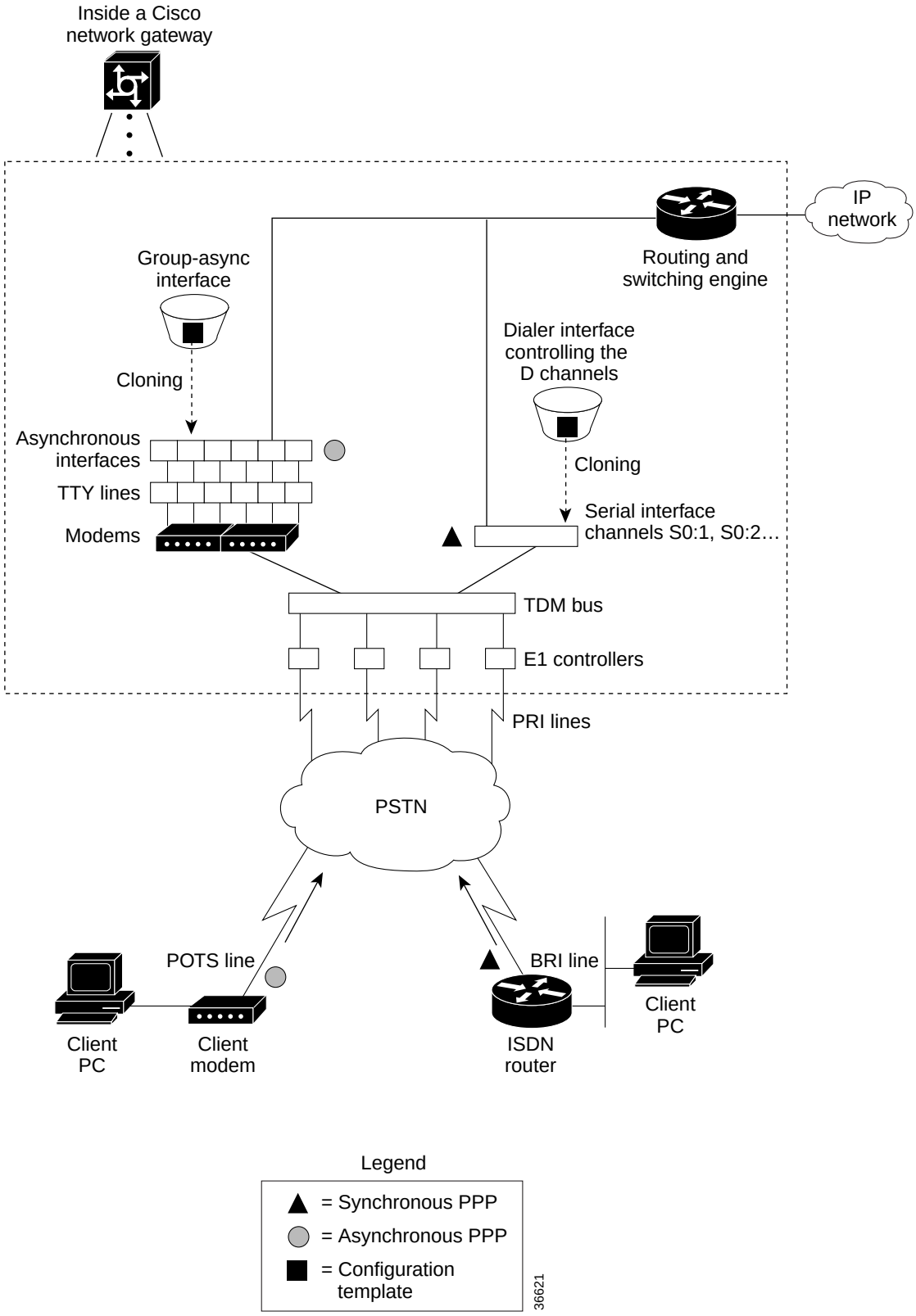
- Trunk cards connect to the public switched telephone network (PSTN) and fit in slots 0-5 and 8-13 only.
  - In classic-split mode, the RSC card in slot 6 controls slots 0-5; the RSC card in slot 7 controls slots 8-13.
  - In handover-split mode, each RSC can take over the feature cards of the other RSC if that RSC fails.
- Universal port cards also fit in slots 0-5 and slots 8-13, between the trunk cards and the RSC cards. The universal port card supports voice, modem, or fax connections. Each port can carry one DS0 of network traffic.

Call-Processing Components

As shown in Figure 2, the following components process a call:

- Client modems and ISDN routers dial in to the universal gateway through the PSTN.
- Asynchronous PPP calls (analog) connect to ports inside the universal gateway.
- Each port inside the universal gateway provides a corresponding TTY line and asynchronous interface for terminating character and packet mode services.
- Asynchronous interfaces clone their configurations from a group-async interface.
- Synchronous PPP calls (digital) connect to serial interface channels (for example, S0/0:1:23 and S2/0:2:23).
- Synchronous interfaces clone their configurations from a dialer interface.

Figure 2 Cisco AS5850 Call-Processing Components



One asynchronous PPP call requires the following:

- 1 DS0 channel
- 1 channel in a TDM bus
- 1 integrated modem
- 1 TTY line
- 1 asynchronous interface

One synchronous PPP call requires the following:

- 1 DS0 channel
- 1 serial interface channel

Note Synchronous PPP calls require HDLC resources. Each T3 trunk card supports 256 HDLC components and each STM1 card supports 512 HDLC components. E1 trunk cards do not have HDLC resource limitations.

How to Commission the Cisco AS5850 Universal Gateway

This section contains the following information:

Task 1. Verifying Basic Setup

To verify that basic system components are functioning, see the following sections:

- Verify Memory Usage, page 19
- Verify CPU Utilization, page 21

Analyze the System Boot Dialog

To view the boot sequence through a terminal session, you must have a console connection to the universal gateway before it powers up.

The following boot sequence occurs. Event numbers and comments are inserted in the example to describe the boot sequence.

In this segment, the universal gateway decompresses the system boot image, tests the NVRAM for validity, and decompresses the Cisco OS software image.

```
System Bootstrap, Version 12.2(2)T, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
5850-rsc platform with 524288 Kbytes of main memory

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

Sometimes boot images do not support hardware cards. Error messages look like this sample.

```
%OIR-3-SEATED: Insert/removal failed
```

Note Ignore these messages, but *do not* ignore error messages that appear after the Cisco IOS software image decompresses.

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

In this segment the following components are detected:

- Cisco IOS release
- Available memory
- Available interfaces

```
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) 5850 Software (C5850-P6-M), Version 12.2(20010828:201655)]
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Tue 28-Aug-01 16:20 by
Image text-base: 0x60008960, data-base: 0x6160E000

cisco c5850 (R7K) processor (revision 0.12) with 196608K/65536K bytes of memory.
```

```
R7000 CPU at 259Mhz, Implementation 39, Rev 2.1, 256KB L2, 2048KB L3 Cache
Last reset from Mbus reset
Channelized E1, Version 1.0.
X.25 software, Version 3.0.0.
Bridging software.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
Primary Rate ISDN software, Version 1.1.
1 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)
1404 terminal line(s)
24 Channelized T1/PRI port(s)
2 Channelized T3 port(s)
507K bytes of non-volatile configuration memory.

32768K bytes of Compact Flash card at slot 0 (Sector size 128K).
16384K bytes of Flash internal SIMM (Sector size 256K).
```

Note If a hardware card is not recognized, verify that you are running the optimum version of Cisco IOS software. See the hardware-software compatibility matrix, available online (logon required) at http://www.cisco.com/cgi-bin/front.x/Support/HWSWmatrix/hwswmatrix.cgi.

The following system message and prompt appears.

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

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

Because the universal gateway has never been configured, the Cisco IOS software cannot find a startup-config file, so abort the configuration dialog. In this example, the Cisco IOS software is configured manually; the automatic setup script is not used. The RSC card auto-detects the state of each card in the chassis.

```
00:00:09: %MBUS-3-UNKNOWN_REGISTER: Status change message for register 9 in slot 6,
value = 2
00:00:09: %MBUS-3-UNKNOWN_REGISTER: Status change message for register 0 in slot 6,
value = 88
00:00:09: %MBUS-3-UNKNOWN_REGISTER: Status change message for register 9 in slot 6,
value = 0
00:00:37: %SYS-7-NV_BLOCK_INIT: Initalized the geometry of nvram
00:00:42: %LINK-5-CHANGED: Interface FastEthernet6/0, changed state to initializing
00:00:42: %LINK-5-CHANGED: Interface GigabitEthernet6/1, changed state to initializing
00:00:42: %DSCREDCLK-5-BSWITCHT: Backup clock matched to the active clock reference,
slot 3 line 0
00:00:43: %DSCREDCLK-5-BNORMAL: Backup clock moving to NORMAL to phase lock to the
active clock
00:00:43: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet6/0, changed
state to down
00:00:43: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet6/1, changed
state to down
00:00:45: %LINK-5-CHANGED: Interface GigabitEthernet6/1, changed state to administratively
down
00:00:52: %LINK-3-UPDOWN: Interface FastEthernet6/0, changed state to up
00:00:53: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet6/0, changed
state to up
00:00:56: %SYS-5-CONFIG_I: Configured from memory by console
00:01:15: %LINK-3-UPDOWN: Interface GigabitEthernet6/0, changed state to up
00:01:17: %SYS-5-RESTART: System restarted --
Cisco Internetwork Operating System Software
IOS (tm) 5850 Software (C5850-P6-M), Version 12.1(20001120:130907)
[ssangiah-121_5_xv_build 100]
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Mon 20-Nov-00 05:09 by
```

```
00:01:17: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet6/0, changed
state to up
00:01:17: %SYS-6-BOOTTIME: Time taken to reboot after reload =  209 seconds
00:01:17: %OIR-6-REMCARD: Card removed from slot 11, interfaces disabled
00:01:17: %OIR-6-REMCARD: Card removed from slot 12, interfaces disabled

Press RETURN to get started!

Router>
```

Verify the Operating Environment

To verify the operating environment, perform the following steps as appropriate for your system.

Step 1 Power up the Cisco AS5850.

Step 2 Verify that there are no critical grounding, cooling, or power problems.

```
AS5850# show environment

Slot #  Exhaust Sensor  Inlet Sensor
         (deg C)          (deg C)

0          54.5            37.0
1          50.5            31.5
2          32.0            32.5
4          44.5            35.5
5          44.0            28.5
6          26.5            24.5
7          26.5            24.5
8          41.5            27.5
9          40.5            29.0
10         42.0            29.0
11         33.5            33.0
13         47.0            32.0

Slot #  3.3V    5V      MBUS 5V
        (mv)    (mv)    (mv)

0       3260    4968    5080
1       3260    4920    5072
2       3276    4976    5088
4       3268    4976    5080
5       3260    4976    5104
6       3284    5016    5128
7       3288    4984    5120
8       3276    4976    5080
9       3276    4968    5080
10      3256    4976    5088
11      3272    4944    5072
13      3264    4944    5096

Slot #  5.15V   MBUS 5V 48V     AMP_48  1.60V
        (mv)    (mv)    (Volt)  (Amp)   (mv)

24      5520    5136    49      13      1640
24 RAW  690     642     698     209     410
25      5536    5136    50      13      1808
25 RAW  692     642     712     218     452

PEMF slot 24: AC Shelf is normal
PEMF slot 24: Blower is normal. (MBUS Port2 returns 8E)
```

```
PEMF slot 25: AC Shelf is normal
PEMF slot 25: Blower is normal. (MBUS Port2 returns 8E)
```

Step 3 Check the Cisco IOS software image, uptime, and restart reason.

```
AS5850# show version

Cisco Internetwork Operating System Software
IOS (tm) 5850 Software (C5850-P6-M), Version 12.1(20000624:130156)]
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Thu 20-Jul-00 09:11 by
Image text-base: 0x60008908, data-base: 0x612B0000

ROM: System Bootstrap, Version 12.0(20000306:065252) [gclendon-rsc-rommon 104],E
ROM: 5850 Software (C5850-BOOT-M), Version 12.1(20000624:130156) []

AS5850 uptime is 18 hours, 30 minutes
System returned to ROM by reload
System image file is "disk0:c5850-p6-mz"

cisco c5850 (R7K) processor with 229376K/32768K bytes of memory.
R7000 CPU at 262Mhz, Implementation 39, Rev 1.0, 256KB L2, 2048KB L3 Cache
Last reset from unexpected value
Channelized E1, Version 1.0.
X.25 software, Version 3.0.0.
Bridging software.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
Primary Rate ISDN software, Version 1.1.
1 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)
756 terminal line(s)
24 Channelized T1/PRI port(s)
1 Channelized T3 port(s)
507K bytes of non-volatile configuration memory.
```

Inspect the Feature Cards

To inspect the feature cards, perform the following steps.

Step 1 Verify that feature cards are up.

```
AS5850# show chassis

System is in classic-split mode, RSC in slot 6.
  Slots owned: 0 1 2 3 4 5
  Slots configured: 0 1 2 3 4 5
  Slots owned by other: 8 9 10 11 12 13
Slot    Board     CPU       DRAM          I/O Memory   State         Elapsed
         Type     Util    Total (free)   Total (free)                Time
 0       24T1    0%/0%         0(  0%)        0(  0%)  Booting       00:00:23
 4  CT3_UP216    0%/0%         0(  0%)        0(  0%)  Booting       00:00:23
 5      UP324    0%/0%         0(  0%)        0(  0%)  Up            00:00:01
System set for auto boot
```

Possible feature-card states include *unknown*, *down*, *resetting*, *booting*, and *up*. The *Up* state means that a card can communicate with the RSC card.

Each universal port card contains its own DRAM memory and performs its own call processing. A normal CPU utilization range is 20-40%.

Step 2 If the feature card does not come up, perform the following troubleshooting steps.

a. Look for LED lights on the feature card. If the lights are off, try reseating the card.

Note More more information about the feature card LEDs, see the *Cisco AS5850 Universal Gateway Card Guide* that shipped with this system.

b. Verify that the RSC connection to the other cards is up.

```
AS5850# show dsi

6/0 is up, line protocol is up
  Hardware is AmdFE, address is 00b6.eaf4.2b00 (bia 00b6.eaf4.2b00)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Unknown duplex, Unknown Speed, 100BaseTX/FX
  ARP type:ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy:fifo
  Output queue 0/600, 0 drops; input queue 0/600, 0 drops
  1 minute input rate 0 bits/sec, 0 packets/sec
  1 minute output rate 0 bits/sec, 0 packets/sec
     45114 packets input, 3795862 bytes
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     22342 packets output, 15268108 bytes, 0 underruns(0/0/0)
     0 output errors, 0 collisions, 1 interface resets
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Interface 6/0
Hardware is AMD Laguna
ADDR:64FD7E24, FASTSEND:6001ED60, MCI_INDEX:0
DIST ROUTE ENABLED:0
Route Cache Flag:0
 LADRF=0x0000 0x0000 0x0000 0x0000
 CSR0  =0x00000072, CSR3  =0x00001044, CSR4  =0x0000491D, CSR15 =0x00008180
 CSR80 =0x00009900, CSR114=0x00000000, CRDA  =0x16462250, CXDA  =0x16465230
 BCR9 =0x00000001 (full-duplex)
 CSR5  =0x00000001, CSR7  =0x00000A20, CSR100=0x0000F000, CSR125=0x00005C3C
 BCR2  =0x00001000, BCR9  =0x00000001, BCR18 =0x000019E0, BCR22 =0x0000FF06
 BCR25 =0x00000017, BCR26 =0x0000000B, BCR27 =0x00000000, BCR32 =0x00004080
 BCR4 =0x000000C0, BCR7 =0x00000090, BCR20 =0x00000303, BCR39 =0x00000000
 BCR33 =0x00004800, BCR34 =0x0000FFFF
 HW filtering information:
  Promiscuous Mode Enabled, PHY Addr Enabled, Broadcast Addr Enabled
  PHY Addr=00B6.EAF4.2B00, Multicast Filter=0x0000 0x0000 0x0000 0x0000
 amdp2_instance=0x64FD9B70, registers=0x48000000, ib=0x6461D20
 rx ring entries=512, tx ring entries=512
 rxring=0x6461D80, rxr shadow=0x64FD9D2C, rx_head=77, rx_tail=0
 txring=0x6463DC0, txr shadow=0x64FDA558, tx_head=327, tx_tail=327, tx_count=0
 spurious_idon=0, throttled=0, enabled=0, disabled=0
 rx_framing_err=0, rx_overflow_err=0, rx_buffer_err=0, rx_bpe_err=0
 rx_soft_overflow_err=0, rx_no_enp=0, rx_discard=0, rx_miss_count=0
```

```
tx_one_col_err=0, tx_more_col_err=0, tx_no_enp=0, tx_deferred_err=0
tx_underrun_err=0, tx_late_collision_err=0, tx_loss_carrier_err=0
tx_exc_collision_err=0, tx_buff_err=0, fatal_tx_err=0 tx_limited=0(0)
```

Note Loss of DSIP keepalive messages indicates that there is no communication between the RSC card and the feature cards. After DSIP Hello messages succeed, the backplane Fast Ethernet connection changes its state to *Up*. Until the interfaces are up, the RSC card and feature cards cannot communicate.

Caution Verify that console logging is disabled. To do so, enter the **show logging** command and then, if needed, the **no logging console** command. If logging is enabled, the universal gateway might intermittently freeze up as soon as the console port gets overloaded with log messages.

Messages appear on the console terminal after the feature card is physically removed from slot 12 and reinserted. Approximately 120 seconds elapse before all these messages appear.

```
AS5850>
04:42:13: %ISDN-6-LAYER2DOWN: Layer 2 for Interface Se1/12/0:0:23, TEI 0 changed
to down
04:42:46: %DSIPPF-5-DS_KEEPALIVE_LOSS: DSIP Keepalive Loss from slot 12
04:42:53: %DSIPPF-5-DS_HELLO: DSIP Hello from slot 12 Succeeded
AS5850>
```

The following boot sequence occurs in the previous example:

- The feature card takes 15 seconds to boot up. Afterward, the card checks the system inventory.
- The RSC card loads the appropriate boot images onto the feature cards.
- More than one minute elapses before the RSC card detects the first DSIP Hello message from the first feature card (in slot 12).
- The RSC card gives the feature cards the appropriate images.

c. For advanced troubleshooting of the feature cards after the RSC card is up, open a virtual-console session to the feature card. To end the session, enter **Ctrl-C** three times.

```
AS5850# dsip console slave 12

Trying Dial shelf slot 12 ...
Entering CONSOLE for slot 12
Type "^C^C^C" to end this session


DA-Slot12>
DA-Slot12#
DA-Slot12#
DA-Slot12#
Terminate NIP IO session? [confirm]

[Connection to Dial shelf slot 12 closed by local host]
AS5850#
```

Note If the **show chassis** command reports that feature cards are booting for extended periods of time, start debugging from the RSC card by using the following commands:

- **debug dsip transport** shows the registered MAC address sent from each feature card.
- **debug dsip trace** displays detailed DSIP hello and keepalive messages.
- **debug dsip boot** shows whether the RSC card is sending the boot image to the feature cards.

To learn more about these and other Cisco IOS commands, start at http://www.cisco.com/univercd/cc/td/doc/product/software/ and click on your Cisco IOS release.

Use the DSIP Commands

The RSC card communicates with the feature cards using the following:

- Backplane MBUS
- Backplane packet bus
- Backplane Dial Shelf Interconnect Protocol (DSIP)

Note DSIP commands on the Cisco AS5850 function very much like the DSIP commands for the Cisco AS5800. For the DSIP command reference and other system management functions, see *Dial and System Management Commands for the Cisco AS5800* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113aa/113aa_2/58cfeats/c5800uas.htm.

To use the DSIP commands, perform the following steps.

Step 1 To understand how DSIP functions, enter commands from the following example.

Note Output from the **show dsi** command differs from that for the **show dsip** command.

```
AS5850# show dsip

DSIP transport statistics:
 IPC  : input msgs=595876, bytes=54824426; output msgs=80748, bytes=4884676
        total consumed ipc msgs=653;  total freed ipc msgs = 653
        transmit contexts in use = 10, free = 246, zombie = 0, invalid = 0
        ipc getmsg failures = 0, ipc timeouts=0
        core getbuffer failures=0, api getbuffer failures=0
        dsip test msgs rcvd = 0, sent = 0
 CNTL : input msgs=18800, bytes=1282416; output msgs=9585, bytes=5215320
        getbuffer failures=0
 DATA : input msgs=540, bytes=19440; output msgs=0, bytes=0

DSIP Private  Buffer Pool Hits  = 0

DSIP registered addresses:
 Shelf0 : Master: 0044.efbe.3d37, Status=local

DSIP Clients:
-------------
ID    Name
```

```
0   Console
1   Clock
2   Modem
3   Logger
4   TDM
5   Trunk
6   Async data
7   Unused
8   Dial shelf manager
9   Unused
10  Unused
11  RSC Red. UI
12  Unused
13  NextPort
14  Signalling
15  Unused
16  DSIP MIPC
17  Marvel Flow Manager
18  gigE
19  Unused
20  Egress Driver
21  DSIP Test

DSIP local ports:
----------------
Client:Portname             Portid    In-Msgs   Bytes     Last-i/p
Console:Master              10005     0         0         never
Clock:Master                10006     1058      245228    00:00:51
Modem:Master                10007     2         28        17:35:41
Logger:Master               10008     0         0         never
TDM:Master                  10009     2         48        17:35:41
Trunk:Master                1000A     51432     4319776   00:00:00
Async data:Master           1000B     0         0         never
Dial shelf manager:Master   1000D     0         0         never
RSC Red. UI:Master          1000E     0         0         never
NextPort:Master             1000F     737       30736     17:35:15
Signalling:Master           10010     0         0         never
DSIP MIPC:Master            10011     0         0         never
Marvel Flow Manager:Master  10012     2         8         17:35:40
gigE:Master                 10013     2         8         17:35:39
Egress Driver:Master        10014     25337     3445832   00:00:00
DSIP Test:Master            10015     0         0         never

DSIP remote ports:
-----------------
Client:Portname             Portid    Out-Msgs  Bytes     Last-o/p  Last-act
Modem:Slave1                1080007   326       8008      17:35:57  17:36:34
NextPort:Slave1             108000A   56        3904      17:35:58  17:36:33
Marvel Flow Manager:Slave1  108000D   2         2700      17:36:31  17:36:31
gigE:Slave1                 108000E   1         12        17:36:30  17:36:30
Clock:Slave13               1140006   1         28        17:35:43  17:35:43
Modem:Slave13               1140007   218       6280      17:35:15  17:35:43
Trunk:Slave13               1140009   8         4512      17:35:43  17:35:43
NextPort:Slave13            114000B   38        2608      17:35:16  17:35:42
Marvel Flow Manager:Slave1  114000E   2         2700      17:35:41  17:35:41
gigE:Slave13                114000F   1         12        17:35:39  17:35:39

DSIP ipc queue:
---------------
There are 0 IPC messages waiting for acknowledgement in the transmit queue.
There are 0 messages currently in use by the system.

DSIP ipc nodes:
---------------
```

```
There are 3 nodes in this IPC realm.
   ID     Type                Name                        Last  Last
                                                          Sent  Heard
   10000 Local      IPC Master                              0      0
 1080000 DSIP       Dial Shelf:Slave1                       33     33
 1140000 DSIP       Dial Shelf:Slave13                      40     40

DSIP version information:
------------------------
Local DSIP major version =  5,   minor version = 2

All feature boards are running DSIP versions compatible with router shelf

Local clients registered versions:
----------------------------------
Client Name      Major Version   Minor Version
Console          5               2
Clock            2               1
Modem            1               0
Logger           No version      No version
TDM              No version      No version
Trunk            No version      No version
Async data       No version      No version
VOICE            0               0
Dial shelf       No version      No version
RSC Red. UI      0               1
NextPort         0               0
Signalling       1               5
DSIP MIPC        No version      No version
Marvel Flow      No version      No version
gigE             No version      No version
Egress Driv      No version      No version
DSIP Test        No version      No version

Mismatched  remote client versions:
```

Step 2 Verify that each feature card's MAC address is registered by DSIP with the **show dsip transport** command. Unregistered cards cannot communicate with the system. Shelf 0 is the RSC card (master). Shelf 1 is the feature card (slave).

```
AS5850# show dsip transport

DSIP transport statistics:
 IPC  : input msgs=596027, bytes=54838680; output msgs=80772, bytes=4886020
        total consumed ipc msgs=653;  total freed ipc msgs = 653
        transmit contexts in use = 10, free = 246, zombie = 0, invalid = 0
        ipc getmsg failures = 0, ipc timeouts=0
        core getbuffer failures=0, api getbuffer failures=0
        dsip test msgs rcvd = 0, sent = 0
 CNTL : input msgs=18804, bytes=1282744; output msgs=9587, bytes=5215440
        getbuffer failures=0
 DATA : input msgs=540, bytes=19440; output msgs=0, bytes=0

DSIP Private  Buffer Pool Hits  = 0

DSIP registered addresses:
 Shelf0 : Master: 0044.efbe.3d37, Status=local

AS5850#
```

Step 3 Verify that all feature cards are running DSIP versions that are compatible with the RSC card.

```
AS5850# show dsip version
```

```
DSIP version information:
------------------------
Local DSIP major version =  5,   minor version = 2

All feature boards are running DSIP versions compatible with router shelf

Local clients registered versions:
-----------------------------------
Client Name      Major Version   Minor Version
Console          5               2
Clock            2               1
Modem            1               0
Logger           No version      No version
TDM              No version      No version
Trunk            No version      No version
Async data       No version      No version
VOICE            0               0
Dial shelf       No version      No version
RSC Red. UI      0               1
NextPort         0               0
Signalling       1               5
DSIP MIPC        No version      No version
Marvel Flow      No version      No version
gigE             No version      No version
Egress Driv      No version      No version
DSIP Test        No version      No version

Mismatched  remote client versions:
-----------------------------------
```

Note The **show dsip version** command also reports mismatched Cisco IOS software versions. No mismatches exist in this example.

Inspect the Initial Running Configuration

The Cisco IOS software creates an initial running configuration. To familiarize yourself with the default settings, inspect the software configuration on the RSC card as follows.

```
AS5850# show running-config

Building configuration...

Current configuration : 1495 bytes
!
version 12.2
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname AS5850
!
!
redundancy
 mode classic-split
no logging buffered
logging rate-limit console 10 except errors
```

```
!
!
resource-pool disable
spe link-info poll voice 5
!
!
ip subnet-zero
ip cef distributed
no ip finger
!
!
controller T3 0/0
 cablelength 224
!
controller T3 1/0
 cablelength 224
!
!
interface FastEthernet6/0
 no ip address
 ip route-cache distributed
 logging event link-status
 shutdown
!
interface GigabitEthernet6/0
 no ip address
 ip route-cache distributed
 logging event link-status
 shutdown
 no negotiation auto
!
interface GigabitEthernet6/1
 no ip address
 ip route-cache distributed
 logging event link-status
 shutdown
 no negotiation auto
!
interface Group-Async0
 no ip address
 ip route-cache distributed
 group-range 0/00 4/323
!
ip kerberos source-interface any
ip classless
no ip http server
!
!
line con 0
 logging synchronous
 transport input none
line aux 0
line vty 0 4
line 0/00 1/215
 activation-character 0
 disconnect-character 0
 modem InOut
 no modem status-poll
 no modem log rs232
 escape-character soft 0
 escape-character 0
 hold-character 0
line 2/00 4/323
 activation-character 0
```

```
 disconnect-character 0
 modem InOut
 no modem status-poll
 no modem log rs232
 escape-character soft 0
 escape-character 0
 hold-character 0
!
end
```

Explore the Cisco IOS File System

Familiarize yourself with the file system and memory storage areas. The Cisco IOS file system provides a consolidated interface to the following:

- Compact-flash memory file system
- Network file system (TFTP, rcp, and FTP)
- Any other endpoint for reading or writing data (such as NVRAM, SPE firmware, the running configuration, ROM, raw system memory, Xmodem, and flash load helper log)

Figure 3 shows the memory locations inside the Cisco AS5850.

Figure 3 Cisco AS5850 Memory Locations

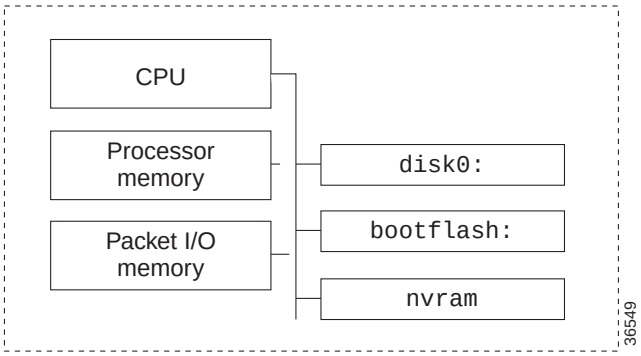


Table 1 describes the memory types on the Cisco AS5850.

Table 1 Memory Descriptions

Component	Description
CPU	Central processing unit.
Processor memory	The Cisco IOS software image is initially read out of compact-flash memory, decompressed, and loaded into processor memory (also known as main memory). Routing tables, call-control blocks, and other data structures are also stored here.
Packet I/O memory	Packets are temporarily stored in I/O memory.
disk0: or flash:	Compact-flash memory cards in the route-switching module. These cards store Cisco IOS software images, modem firmware/portware, and custom web pages.

Table 1 Memory Descriptions (continued)

Component	Description
bootflash:	Flash memory on the route-switching module.
nvram:	Nonvolatile configuration memory.

To inspect the file system, perform the following steps as appropriate for your system.

Step 1 View the different file storage areas and file management functions. Additionally, verify that you have everything you ordered from manufacturing, such as flash memory. The asterisk (*****) near the bottom of the output indicates the current directory.

```
AS5850# show file systems

File Systems:

     Size(b)     Free(b)      Type  Flags  Prefixes
    31916032    14307328     flash     rw   disk0:
           -           -   network     rw   rcp:
           -           -    opaque     rw   null:
           -           -    opaque     rw   system:
           -           -   network     rw   tftp:
      520184      481796     nvram     rw   nvram:
*   15990784    11484640     flash     rw   bootflash: flash:
           -           -   network     rw   ftp:
AS5850#
```

Step 2 Display the objects in the system memory directory:

```
AS5850# dir system:

Directory of system:/

  1  -rw-       51613              <no date>  running-config
  2  dr-x           0              <no date>  memory
 12  dr-x           0              <no date>  vfiles
No space information available
AS5850#
```

Note Remember to include the trailing colon (**:**) in the **dir** commands.

Step 3 Inspect the flash memory. As the chassis boots up, the image is copied, decompressed, and loaded into DRAM memory.

```
AS5850# pwd

disk0:
AS5850# dir
Directory of disk0:/

    3  -rw-      325539   Jan 01 2000 04:33:44  np_6_83_2.spe
   83  -rw-     8987568   Jan 02 2000 02:45:30  c5850-p6-mz.Aug23
 2278  -rw-     8617256   Jan 01 2000 00:17:16  c5850-p6-mz.Sep5
31916032 bytes total (13299712 bytes free)
```

Step 4 Inspect the boot flash.

```
AS5850# dir bootflash:

Directory of bootflash:/

    1  -rw-     1863976   Mar 01 1993 00:05:28  c5850-boot-mz.May26
15990784 bytes total (14100676 bytes free)
```

Note Keep a backup copy of the RSC Cisco IOS image in boot flash in case compact-flash memory cards are misplaced.

Step 5 Inspect the NVRAM memory on the RSC. Three files are present:

- The initial boot or startup-config.
- The private-config. This is a secure file that supports encryption technologies. It is not user accessible.
- The underlying-config. This is the version of the startup-config that is stored in NVRAM.

```
AS5850# dir nvram:

Directory of nvram:/
  1  -rw-         739              <no date>  startup-config
  2  ----          24              <no date>  private-config
  3  -rw-         739              <no date>  underlying-config
129016 bytes total (128277 bytes free)
AS5850#
```

Verify Memory Usage

Use the **show memory summary** command to do the following:

- Verify how memory is used for different processor and I/O memory processes.
- Identify memory leaks or fragmentation.
  - Memory leaks occur when memory is not released back to the processor. They are indicated by steady decreases of free memory. However, the preferred way to track memory leaks is to monitor the *FreeMem* variable in the OID MIB.
  - Memory fragmentation is indicated when the largest block of memory is unequal to the free block. Fragmentation increases as the numbers grow further apart.

To determine and calculate memory usage, perform the following steps.

Step 1 Display the memory status report. In the example, the largest memory block is close to the free-memory block. There is no fragmentation.

```
AS5850# show memory summary

           Head       Total(b)     Used(b)     Free(b)    Lowest(b)   Largest(b)
Processor   616CCD20   479408864    44937912   434470952   431866220   431896392
      I/O    E000000    33554432     2633464    30920968    30066928    30132444

          Processor memory

Alloc PC        Size     Blocks      Bytes    What
```

```
0x60009E3C        172          4        688    Init
0x6000F748        432       1080     466560    IDB: Serial Info
0x6000F748        436          1        436    IDB: Serial Info
0x6000F748        444          1        444    IDB: Serial Info
0x60017BE4       2048          1       2048    Init
0x60017C10       4096          1       4096    Init
0x6001B09C        184          1        184    Init
0x600265F0        128         25       3200    RIF Cache
0x6006CDFC        176       1086     191136    FIB: FIBIDB
0x6006D514      30000          1      30000    FIB: HWIDB MAP TABLE
0x6006D6A8        560       1086     608160    FIB: FIBHWIDB
0x6006D8CC      30000          1      30000    Init
0x6006EF08       1460          1       1460    RemoveReceiveHash Entries
0x60071274       1900          1       1900    FIB one path chunk
0x60071274      65496          1      65496    FIB one path chunk
0x6007CB74       1072          1       1072    FIB: Control Block
0x6007CBA0         32          1         32    Init
0x6007CE4C      30000          1      30000    FIB: Root-table
0x6007CE68      30000          1      30000    FIB: Cblk-table
0x6007CED8        144          1        144    FIB ndb
0x6007CEF4        384          1        384    FIB rdb
0x6007CF30         92          1         92    Init
```

Caution If you enter the **show memory summary** command with the **terminal length 0** command enabled, many output screens appear that might interrupt your session.

Table 2 describes the significant fields in the previous display.

Table 2 show memory summary Output Field Descriptions

Field	Description
Processor	Processor memory. The Cisco IOS software image is initially read out of flash memory, decompressed, and placed in main memory. Routing tables and call-control blocks are also stored in main memory.
I/O	Packets are temporarily stored in I/O memory.
Head	Hexadecimal address of the head of the memory-allocation chain.
Total(b)	Summary of used bytes plus free bytes.
Used(b)	Total number of bytes currently used for routing tables and call-processing components.
Free(b)	Total number of free bytes. Free-memory size should be close to the largest block available.
Lowest(b)	Smallest amount of free memory since last boot.
Largest(b)	Size of largest available free block. When the largest available block is equal to the free block, there is no fragmentation.

Step 2 Convert bytes to megabytes (MB):

- Total processor memory = 479,408,864 bytes = 457.2 MB
- Used processor memory = 44,937,912 bytes = 42.9 MB
- Free processor memory = 434,470,952 bytes = 414.3 MB

Total memory (457.2 MB) = Used memory (42.9 MB) + free memory (414.3 MB)

Step 3 Do some useful memory calculations:

Total Processor = Total RAM – Cisco IOS software (use the **show version** command to get the MB assigned for all of Cisco IOS software + processor)

```
cisco c5850 (R7K) processor (revision 0.12) with 491520K/32768K bytes of memory.
```

491520K = 480 MB

+ 32768K = 32 MB

Total = 512 MB (what you purchased)

Verify CPU Utilization

High utilization causes network performance problems. Knowing when the gateway is running at over 50% utilization is critical because the gateway might start dropping packets if an unexpected traffic burst comes through, or if OSPF gets recalculated. Fast switching reduces CPU utilization.

To verify CPU utilization, perform the following steps.

Step 1 Verify CPU utilization.

```
AS5850# show processes cpu

CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
 PID  Runtime(ms)  Invoked  uSecs    5Sec   1Min   5Min TTY Process
   1           0       88      0   0.00%  0.00%  0.00%   0 Load Meter
   2        1856    14859    124   0.00%  0.44%  0.28%   0 Exec
   3         384       63   6095   0.00%  0.09%  0.04%   0 Check heaps
   4           0        1      0   0.00%  0.00%  0.00%   0 Chunk Manager
   5           0        1      0   0.00%  0.00%  0.00%   0 Pool Manager
   6           0        2      0   0.00%  0.00%  0.00%   0 Timers
   7           0        2      0   0.00%  0.00%  0.00%   0 Serial Backgroun
   8          52        6   8666   0.00%  0.00%  0.00%   0 RSC Ucode Downlo
   9           0        2      0   0.00%  0.00%  0.00%   0 DS OIR Handler o
  10           0      469      0   0.00%  0.00%  0.00%   0 FB manager
  11          12     1873      6   0.00%  0.00%  0.00%   0 MBUS System
  12          64       31   2064   0.00%  0.00%  0.00%   0 ARP Input
  13           0      117      0   0.00%  0.00%  0.00%   0 HC Counter Timer
  14           0        2      0   0.00%  0.00%  0.00%   0 DDR Timers
  15           0        2      0   0.00%  0.00%  0.00%   0 Dialer event
  16           4        2   2000   0.00%  0.00%  0.00%   0 Entity MIB API
  17           0        1      0   0.00%  0.00%  0.00%   0 RM PROCESS
  18           0        1      0   0.00%  0.00%  0.00%   0 RM PROCESS
  19           0        1      0   0.00%  0.00%  0.00%   0 RM PROCESS
  20           0        1      0   0.00%  0.00%  0.00%   0 RM PROCESS
  21           0        2      0   0.00%  0.00%  0.00%   0 CAS Process
 PID  Runtime(ms)  Invoked  uSecs    5Sec   1Min   5Min TTY Process
  22           0        2      0   0.00%  0.00%  0.00%   0 IPC Zone Manager
  23           0      471      0   0.00%  0.00%  0.00%   0 IPC Periodic Tim
  24          28      275    101   0.00%  0.00%  0.00%   0 IPC Seat Manager
  25           0        1      0   0.00%  0.00%  0.00%   0 SERIAL A'detect
  26           0        1      0   0.00%  0.00%  0.00%   0 Critical Bkgnd
  27           8      496     16   0.00%  0.00%  0.00%   0 Net Background
  28           0       28      0   0.00%  0.00%  0.00%   0 Logger
  29           0      435      0   0.00%  0.00%  0.00%   0 TTY Background
  30           4      471      8   0.00%  0.00%  0.00%   0 Per-Second Jobs
  31           0        3      0   0.00%  0.00%  0.00%   0 rsc_sync_process
```

```
 32           0        59      0   0.00%  0.00%  0.00%   0 Net Input
 33         476        89   5348   0.08%  0.10%  0.08%   0 Compute load avg
 34          48         8   6000   0.00%  0.00%  0.00%   0 Per-minute Jobs
 35           0      7554      0   0.00%  0.00%  0.00%   0 RSC Redundancy
 36           4     16258      0   0.00%  0.00%  0.00%   0 MBUS monitoring
 37           0         2      0   0.00%  0.00%  0.00%   0 marker
 38           0       469      0   0.00%  0.00%  0.00%   0 MIPC Periodic Ti
 39           0       331      0   0.00%  0.00%  0.00%   0 MIPC Server Proc
 40           0         1      0   0.00%  0.00%  0.00%   0 FDM TCAM Daemon
 41         428      3457    123   0.00%  0.00%  0.00%   0 NIP Boot Daemon
 42          72      3548     20   0.00%  0.00%  0.00%   0 DSIP Daemon
 43           0         1      0   0.00%  0.00%  0.00%   0 DSIP INTRAPI Dae
PID  Runtime(ms)  Invoked  uSecs    5Sec   1Min   5Min TTY Process
 44           0       571      0   0.00%  0.00%  0.00%   0 DS RSC Clock Dae
 45           0       107      0   0.00%  0.00%  0.00%   0 Env Mon
 46           0         2      0   0.00%  0.00%  0.00%   0 CSM Periodic
 47           0         1      0   0.00%  0.00%  0.00%   0 Portware Downloa
 48           0         1      0   0.00%  0.00%  0.00%   0 COT Timer proces
 49           0         1      0   0.00%  0.00%  0.00%   0 COT Queue proces
 50           4        13    307   0.00%  0.00%  0.00%   0 PM SPE SM Proces
 52           0         2      0   0.00%  0.00%  0.00%   0 PM FW Process
 53           0         2      0   0.00%  0.00%  0.00%   0 PM DOWNLOAD MAIN
 54          12        70    171   0.00%  0.00%  0.00%   0 EST msg processi
 55           0         8      0   0.00%  0.00%  0.00%   0 VRM reset proces
 56           0         1      0   0.00%  0.00%  0.00%   0 VRM
 57           0         1      0   0.00%  0.00%  0.00%   0 PM CSM Event Bac
 58           4        36    111   0.00%  0.00%  0.00%   0 RSC PIF Interfac
 59           0       471      0   0.00%  0.00%  0.00%   0 DSBIC Periodic
 60          24       314     76   0.00%  0.00%  0.00%   0 IP Input
 61          48       122    393   0.00%  0.00%  0.00%   0 CDP Protocol
 62           0        74      0   0.00%  0.00%  0.00%   0 IP Background
 63           0         1      0   0.00%  0.00%  0.00%   0 PPP IP Add Route
 64           0         9      0   0.00%  0.00%  0.00%   0 Adj Manager
 65           0         1      0   0.00%  0.00%  0.00%   0 TCP Timer
 66           0         1      0   0.00%  0.00%  0.00%   0 TCP Protocols
 67           0         1      0   0.00%  0.00%  0.00%   0 Probe Input
 68           0         1      0   0.00%  0.00%  0.00%   0 RARP Input
 69           0         1      0   0.00%  0.00%  0.00%   0 HTTP Timer
 70           0         1      0   0.00%  0.00%  0.00%   0 Socket Timers
 71           0         2      0   0.00%  0.00%  0.00%   0 DHCPD Receive
 72           0         8      0   0.00%  0.00%  0.00%   0 IP Cache Ager
 73           0         1      0   0.00%  0.00%  0.00%   0 COPS
 74           0         1      0   0.00%  0.00%  0.00%   0 PAD InCall
 75           0         2      0   0.00%  0.00%  0.00%   0 X.25 Background
 76           0         2      0   0.00%  0.00%  0.00%   0 Emulator
 77           0         8      0   0.00%  0.00%  0.00%   0 TCP Intercept Ti
 78           0         1      0   0.00%  0.00%  0.00%   0 Time Range Proce
 80           0         1      0   0.00%  0.00%  0.00%   0 ISDN Timer
 81           0         1      0   0.00%  0.00%  0.00%   0 sssapp
 82           0         2      0   0.00%  0.00%  0.00%   0 tcl ivr app
 83           0         2      0   0.00%  0.00%  0.00%   0 tcl ivr app
 84           0         2      0   0.00%  0.00%  0.00%   0 tcl ivr app
 85           0         2      0   0.00%  0.00%  0.00%   0 tcl ivr app
 86           0         2      0   0.00%  0.00%  0.00%   0 tcl ivr app
 87           0         2      0   0.00%  0.00%  0.00%   0 tcl ivr app
 88           0         2      0   0.00%  0.00%  0.00%   0 tcl ivr app
 89           4         2   2000   0.00%  0.00%  0.00%   0 tcl ivr app
PID  Runtime(ms)  Invoked  uSecs    5Sec   1Min   5Min TTY Process
 90           0         1      0   0.00%  0.00%  0.00%   0 CallMIB Backgrou
 91           0         1      0   0.00%  0.00%  0.00%   0 ISDNMIB Backgrou
 92           0         1      0   0.00%  0.00%  0.00%   0 SNMP ConfCopyPro
 93           0         1      0   0.00%  0.00%  0.00%   0 Syslog Traps
 94           0         3      0   0.00%  0.00%  0.00%   0 AAA Accounting
 96           0         4      0   0.00%  0.00%  0.00%   0 DHCPD Timer
```

```
 97           0       121       0   0.00%  0.00%  0.00%   0 DHCPD Database
```

Step 2 Look at the top line of the output. If you see utilization over 50%, inspect the columns *5Sec*, *1Min*, and *5Min*. Find the process that uses the most CPU power. For an idle chassis, numbers larger than 2% indicate a problem.

Table 3 describes the significant output fields in the previous example.

Table 3 CPU Utilization Display Fields

Field	Description
`CPU utilization for five seconds: 2%/0%;`	The first % number is the CPU utilization for the last 5 seconds. The second % number is the percentage of CPU time spent at the packet-based interrupt level.
`one minute: 1%;`	CPU utilization for the last 1 minute.
`five minutes: 14%`	CPU utilization for the last 5 minutes.

Whenever memory cannot be allocated to a process request (a memory leak), a console error message appears. To identify the problem, inspect the first few output lines of the **show memory summary** command and **show processor memory** command.

Task 2. Configuring Basic Cisco IOS Software

To apply a basic running configuration to the universal gateway, see the following sections:

- Configure Host Name, Enable-Secret Password, and Time Stamps, page 23
- Configure Local AAA Security, page 24
- Set Up a Login Banner, page 26
- Configure Basic IP, page 27

Tip Save the configuration often by using the **copy running-config startup-config** command.

Configure Host Name, Enable-Secret Password, and Time Stamps

You assign a host name to the universal gateway, specify an *enable-secret* password, and turn on time stamps.

- A host name allows you to distinguish between different network devices.
- A secret enable password allows you to prevent unauthorized configuration changes.
- Encrypted passwords in the configuration file add greater security to the universal gateway.
- Time stamps help you trace debug output for testing connections. If you do not know exactly when an event occurs, you are not able to trace debug output for testing conditions.

To configure a hostname, enable-secret passwords, and time stamps, perform the following steps.

Step 1 Enter the following commands in global configuration mode.

```
ip hostname Gateway
enable secret yourpasswordhere
service password-encryption
service timestamps debug datetime msec
service timestamps log datetime msec
```

Note Do not use the obsolete **enable password** command.

Step 2 Log in with the *enable secret* password. Use the **show privilege** command to show the current security privilege level.

```
Gateway# disable
Gateway> enable
Password:

Gateway# show privilege
Current privilege level is 15
Gateway#
```

Configure Local AAA Security

Configure AAA to perform login authentication by using the local username database. The **login** keyword authenticates EXEC-shell users. Additionally, configure PPP authentication to use the local database if the session was not already authenticated by **login**.

AAA is the Cisco IOS software security model used on all Cisco devices. AAA provides the primary framework through which you set up access control on the universal gateway.

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

Note We recommend using a AAA RADIUS server. For more information on the AAA RADIUS server, see Chapter 4 "Cisco AS5850 Administration," under "RADIUS Management" of the *Cisco AS5850 Operations, Administration, Maintenance, and Provisioning Guide* at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5850/sw_conf/5850oamp/index.htm.

To configure local security, perform the following steps.

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

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

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

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

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

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

Step 4 Return to privileged EXEC mode.

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

Step 5 Log in with your username and password:

Caution After you configure AAA security, all access will require a username and password. Make sure your login name and password are working before you exit or reboot. If you are unable to get back into your universal gateway, see the password-recovery instructions at http://www.cisco.com/warp/public/474/pswdrec_as5300.shtml.

```
Gateway# login

User Access Verification

Username: admin
Password:

Gateway#
```

A successful login means your local username works on any TTY or VTY line. Do not disconnect your session until you can log in.

Tip To save the gateway configuration, save it to NVRAM.

Note For comprehensive information about how to implement a Cisco AAA-based security environment, see the relevant Cisco security features documents at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/newsecf/.

Table 4 describes the configuration line-item commands.

Table 4 Local AAA Commands

Command	Purpose
aaa new-model	Initiates the AAA access control system and immediately locks down **login** and PPP authentication.
aaa authentication login default local	Configures AAA to perform login authentication by using the local username database. The **login** keyword authenticates EXEC-shell users.
aaa authentication ppp default if-needed local	Configures PPP authentication to use the local database if the session was not already authenticated by **login**.

Set Up a Login Banner

Create a login banner. However, do not tell users what device they are connecting to until after they log on. Providing device-sensitive information can tempt unauthorized users to hack into the system.

To set up a login banner, perform the following steps.

Step 1 Create the banner.

```
Gateway(config)# banner login |

Enter TEXT message.  End with the character '|'.
This is a secured device.
Unauthorized use is prohibited by law.
|
Gateway(config)#^Z
Gateway#
```

Step 2 Test the banner.

```
Gateway#
Gateway# login

This is a secured device.
Unauthorized use is prohibited by law.

User Access Verification

Username: admin
Password:

Gateway#
```

Configure Basic IP

To configure a basic dial-access service of two loopback interfaces, bring up one Fast Ethernet interface, and add an IP route to the default gateway, perform the following steps.

Step 1 Assign the IP addresses and create an IP route to the default gateway.

```
!
interface Loopback0
 ip address 172.22.99.1 255.255.255.0
!
interface Loopback1
 ip address 172.22.90.1 255.255.255.0
!
interface FastEthernet0/1/0
 ip address 172.22.66.23 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 172.22.66.1
!
```

The advantage of assigning a gateway's IP address to a loopback rather than a physical interface is that a loopback interface never goes down. The roles of the two loopback interfaces is as follows:

- **interface Loopback0** identifies the gateway with a unique and stable IP address for network-management purposes. Assigning one IP address from a common address block to each network device enables the network operations center to more easily perform security filtering.
- **interface Loopback1** hosts a pool of IP addresses for the remote nodes. Thus, one route is summarized and propagated to the backbone instead of 254 host routes.

Step 2 Verify that the Fast Ethernet interface is up by pinging the default gateway.

```
Gateway# ping 172.22.66.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.22.66.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

Gateway#
```

This step verifies that you have IP connectivity with another device on the subnet. If the ping succeeds to the default gateway, try pinging the DNS server in your backbone. Make sure the backbone is configured to get to the universal gateway; otherwise, the ping does not work. Configure the backbone gateways to support the routes to the networks that you are using.

Note An 80% ping-success rate is normal the first time you ping an external device. The universal gateway does not yet have an address-resolution-protocol (ARP) entry for the external device. A 100% success rate should result the next time you ping the device.

Task 3. Configuring Channelized T1 or E1

This section shows how to configure channelized T1 or E1. You can allocate the available channels for channelized E1 and T1 in the following ways:

- All channels can be configured to support ISDN PRI.
- If you are not running ISDN PRI, all channels can be configured to support robbed-bit signaling (also known as channel-associated signaling).
- All channels can be configured in a single channel group.
- Mix and match channels supporting ISDN PRI, channel grouping, and channel-associated signaling.
- Mix and match channels supporting ISDN PRI, channel grouping, and robbed-bit signaling across the same T1 line.

To configure a basic T1 or E1 controller, perform the following steps.

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

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

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

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

Step 3 Enter controller configuration mode to configure your controller slot and port. Slot values range from 0 to 5 and 8 to 13. Port values range from 0 to 23 for T1 and E1.

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

for the Sonet controller:

```
Router(config)# controller E1 slot/port.path:E1 contoller
Router(config-controller)#
```

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

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

or enter the framing type for the CE1 controller.

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

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

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

or define the line code as high-density bipolar 3 (HDB3) for the CE1 controller.

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

Step 6 Return to privileged EXEC mode.

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

Tip To save the gateway configuration, save it to NVRAM.

Verify

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

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

```
Gateway# show controller t1 1/7

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

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

Tip If you are having trouble, do or note the following:

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

Task 4. Configuring Channelized T3

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

To configure channelized T3, perform the following steps.

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

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

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

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

Step 3 Enter controller configuration mode to configure your T3 controller slot and port. Slot values range from 0 to 5 and 8 to 13. Port number is always 0.

```
Gateway(config)# controller t3 slot/port
Gateway(config-controller)#
```

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

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

Step 5 Enter your clock source: **internal** or **line**.

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

Step 6 Enter your cablelength: values range from **0** to **450** feet.

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

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

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

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

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

Step 8 Return to privileged EXEC mode.

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

Tip To save the gateway configuration, save it to NVRAM.

Verify

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

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

```
Gateway# show controller t3 1/0

T3 1/0 is up.
  Applique type is Channelized T3
```

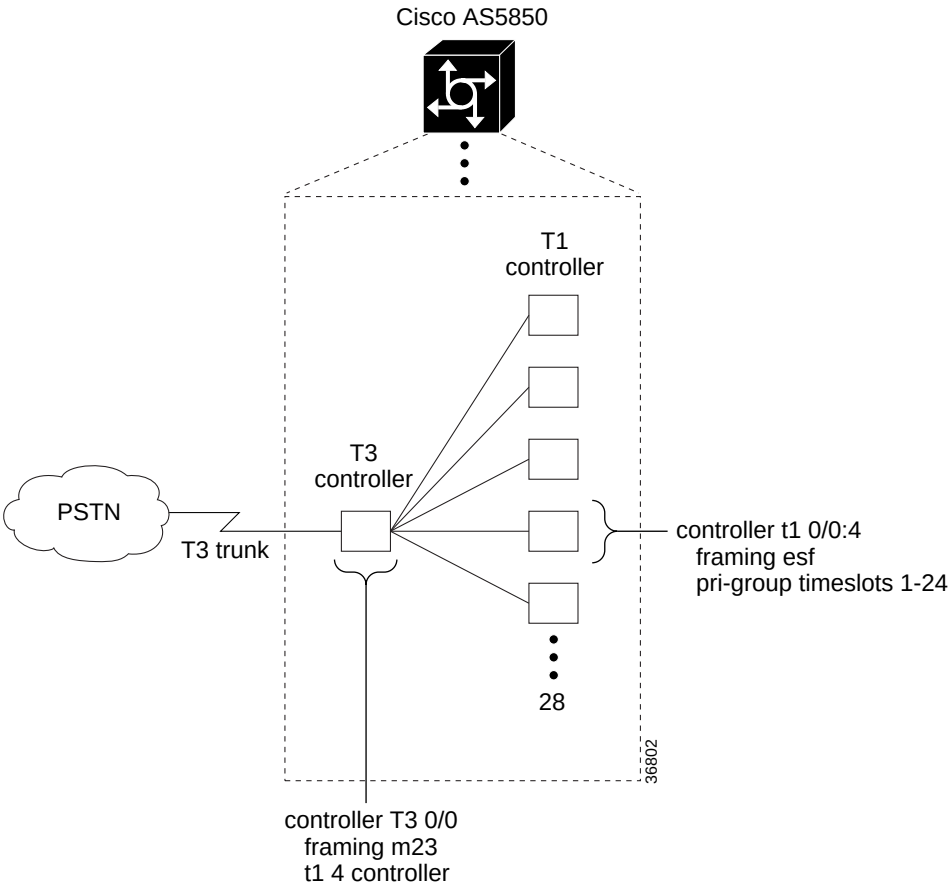
```
No alarms detected.
MDL transmission is disabled

FEAC code received:No code is being received
Framing is C-BIT Parity, Line Code is B3ZS, Clock Source is Internal
Data in current interval (270 seconds elapsed):
   0 Line Code Violations, 0 P-bit Coding Violation
   0 C-bit Coding Violation, 0 P-bit Err Secs
   0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
   0 Unavailable Secs, 0 Line Errored Secs
   0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
Total Data (last 32 15 minute intervals):
   0 Line Code Violations, 0 P-bit Coding Violation,
   0 C-bit Coding Violation, 0 P-bit Err Secs,
   0 P-bit Severely Err Secs, 0 Severely Err Framing Secs,
   0 Unavailable Secs, 0 Line Errored Secs,
   0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
```

Task 5. Configuring ISDN PRI

Figure 4 displays the logical controller components inside a Cisco AS5850. The figure demonstrates that a T3 trunk card requires T1 and T3 controller configuration settings. In the figure, only the fourth controller is configured. There are a total of 28 T1 controllers to configure.

Figure 4 Matching Controller Settings



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

Note

- For more information on dial services, see the *Dial Solutions Command Reference* for your Cisco IOS software release.
- Before configuring ISDN PRI on your Cisco universal gateway, order a correctly provisioned ISDN PRI line from your telecommunications service provider.

To configure ISDN PRI, perform the following steps.

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

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

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

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

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

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

Note Under the individual serial-D channels, a different switch type can be defined for each PRI trunk. See "Task 6. Configuring the Serial Interfaces" section on page 36.

Note For T1 CAS trunks, no ISDN switch type is configured.

Table 5 ISDN Switch Types

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

Table 5 ISDN Switch Types (continued)

Area	Keyword	Switch Type
	primary-5ess	AT&T 5ESS switch type for the United States
	primary-dms100	NT DMS-100 switch type for the United States
	primary-ni	National ISDN switch type

Step 4 Specify the T1 controller you want to configure.

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

or

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

or

Specify the E1 controller you want to configure.

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

or, for Sonet controller

```
Router(config)# controller E1 slot/port.path:E1 contoller
```

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

Step 5 Specify the PRI channels.

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

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

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

Step 6 Return to privileged EXEC mode.

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

Step 7 Verify that the controllers are up and no alarms or errors are detected. Error counters are recorded over a 24-hour period in 15-minute intervals. In the display output, focus on the data in the current interval.

```
Gateway# show controller t3

T3 0/0 is up.
  Applique type is Channelized T3
  No alarms detected.
  FEAC code received: No code is being received
```

```
  Framing is M23, Line Code is B3ZS, Clock Source is Internal
  Data in current interval (201 seconds elapsed):
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     0 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
  Total Data (last 1 15 minute intervals):
     30664 Line Code Violations, 49191 P-bit Coding Violation,
     47967 C-bit Coding Violation, 0 P-bit Err Secs,
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs,
     2 Unavailable Secs, 0 Line Errored Secs,
     10 C-bit Errored Secs, 10 C-bit Severely Errored Secs
Gateway#

Gateway# show controller T1 0/0:4

T1 0/0:4 is up.
  Applique type is Channelized T1
  Cablelength is short
  No alarms detected.
  Framing is ESF, Line Code is AMI, Clock Source is Line.
  Data in current interval (240 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, 8 Path Code Violations
     11 Slip Secs, 26 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 26 Unavail Secs
  Total Data (last 1 15 minute intervals):
     0 Line Code Violations, 8 Path Code Violations,
     11 Slip Secs, 26 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 26 Unavail Secs#
```

Step 8 After each controller is correctly set up, clear the counters and look for ongoing line violations and errors. To do this, enter the **clear counter** command followed by the **show controller** command.

```
Gateway# clear counter t3
Gateway# show controller t3
```

In the display output, focus on the data in the current interval. Error counters stop increasing when the controller is configured correctly.

From the reference point of the universal gateway, Table 6 provides a list of E1 alarm conditions and descriptions.

Table 6 Alarm Conditions

Alarm	Description
CRC Errors	Occur only in ESF format when a CRC bit has an error.
Excessive CRC Error Indication (ECRCEI)	Reported in ESF format when 32 of any 33 consecutive CRCs are in error.
Out of Frame (OOF)	Occurs when the framing pattern for a T1 line has been lost, and data cannot be extracted. This is a red alarm. In SF and ESF formats, OOF occurs when any two of four consecutive frame-synchronization bits are in error.

Table 6 Alarm Conditions (continued)

Alarm	Description
Loss of Signal (LOS)	Occurs when 175 consecutive 0s are detected in the MC. This is a red alarm. The signal is recovered if the density of 1s reaches 12.5%. Recovery happens when four 1s are received within a 32-bit period.
Remote Frame Alarm (RHEA)	Indicates that an OOF framing pattern occurred at the remote end. This is a yellow alarm.
Alarm Indication Signal (AIS)	Indicates to the remote end a loss of the received signal. This is a blue alarm. AIS occurs when a stream of 1s is received.
Loopback	Indicates that a remotely initiated loopback (from the network) is in progress.
Errored Seconds	Depending on the framing format, indicates OOF conditions, frame slip conditions, or error events. For SF, errored seconds reports the number of seconds the frame was in the OOF or slip condition. For ESF, errored seconds reports error events in seconds.
Bursty Errored Seconds	Reports CRC error conditions in seconds (ESF format only).
Severely Errored Seconds	Reports error events or frame slip conditions in seconds.

Note For more information about controllers, see *Channelized E1 and Channelized T1 Setup Commands* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/dial_r/drprt1/index.htm.

Step 9 Verify that individual serial D channels are created. B channels S0/0:4:0 through S0/0:4:22 are rotary members (dialers) of the signaling D channel S0/0:4:23.

```
Gateway# show ip interface brief | inc :23

Serial0/0:4:23           unassigned      YES NVRAM  up       up

Gateway#
```

Step 10 Enter the **show interface S0/0:4:23** command.

```
Gateway# show interface s0/0:4:23
```

Tip To save the gateway configuration, save it to NVRAM.

Task 6. Configuring the Serial Interfaces

Configure the serial D channels to route incoming voice calls from the PSTN to the integrated modems. The behavior of the B channels is controlled by the D-channel configuration instructions. The D channel is the signaling channel.

Table 7 describes the relationship between T1 controllers and serial interfaces.

- After timeslots are assigned by the **pri-group** command, D-channel serial interfaces are automatically created in the configuration file (for example, S0/0:0:23, S0/0:1:23, and so on).
- Individual B-channel serial interfaces are created as rotary members (dialers) of their signaling D channels (for example, S0/0:0:0 through S0/0:0:22). The D-channel interface functions like a dialer for all the 23 B channels using the controller.
- An ISDN switch type defined on the global level is automatically propagated to the serial D-channel interface level. However, a switch type defined on the serial-interface level overrides a switch type defined on the global level.

Table 7 Controller-to-Channel Relationships

T1 Controllers	D Channels	B Channels
Controller T1 0/0	Interface serial 0/0:23	S0/0:0 through S0/0:22
Controller T1 0/1	Interface serial 0/1:23	S0/1:0 through S0/1:22
Controller T1 0/2	Interface serial 0/2:23	S0/2:0 through S0/2:22
Controller T1 0/3	Interface serial 0/3:23	S0/3:0 through S0/3:22
Controller T1 0/4	Interface serial 0/4:23	S0/4:0 through S0/4:22
...	...	...

To configure the serial interfaces, perform the following steps.

Step 1 Apply the **isdn incoming-voice modem** command to each D-channel serial interface. In this example, one interface is configured.

```
Gateway(config)# interface serial 1/0/0:4:23
Gateway(config-if)# isdn incoming-voice modem
```

Step 2 Verify that ISDN is functioning properly, and that the serial channels are up.

a. Check the ISDN status. Confirm that Layer 1 reports ACTIVE, and the display field MULTIPLE_FRAME_ESTABLISHED appears at Layer 2. For PRI lines, the terminal endpoint identifier (TEI) is always 0. The Layer 3 status reports no active calls.

```
Gateway# show isdn status

Global ISDN Switchtype = primary-ni
ISDN Serial0/0:4:23 interface
        dsl 0, interface ISDN Switchtype = primary-5ess
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 0 CCBs = 0
    The Free Channel Mask:  0x807FFFFF
```

```
Total Allocated ISDN CCBs = 0
```

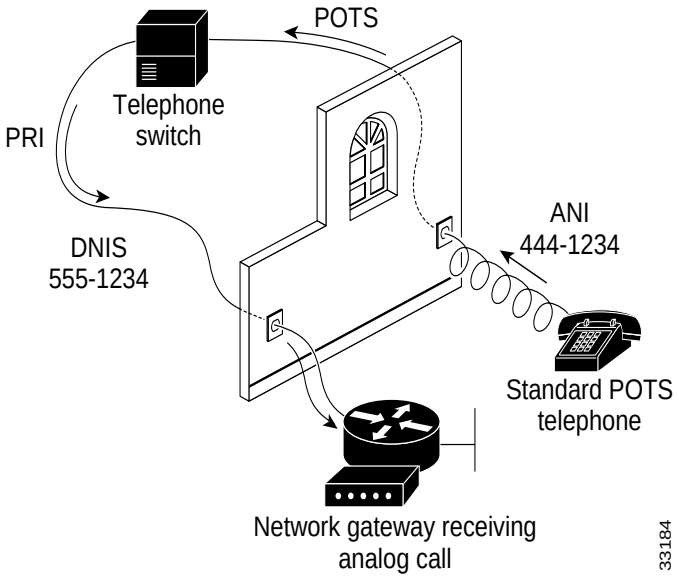
b. Look at the status of the DS0 channels. In this example, 23 DS0s are idle. The 24th channel is reserved for PRI D-channel signaling.

```
Gateway# show isdn service

PRI Channel Statistics:
ISDN Se0/0:4:23, Channel [1-24]
  Configured Isdn Interface (dsl) 0
  Channel State (0=Idle 1=Propose 2=Busy 3=Reserved 4=Restart 5=Maint_Pend)
  0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 3
  Service State (0=Inservice 1=Maint 2=Outofservice)
  0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
```

Step 3 Test the configuration by sending a plain old telephone service (POTS) call into the Cisco AS5850 universal gateway. If the modem answers (you hear modem squelch), the configuration works. In Figure 5 a different telephone number is associated with each end of the connection.

Figure 5 Sending a POTS Telephone Call to a Network Gateway



Note To display incoming call information on the monitor, use the **debug ISDN q931** command with the **logging console** command enabled.

- The called-party number is delivered by the dial number identification service (DNIS). It identifies the directory number assigned to the Cisco AS5850's PRI trunks. In Figure 5, the telephone dialed 555-1234.
- The calling-party number is delivered by the automatic number identification (ANI) service. It identifies the directory number assigned to the device that initiates the call. In this example, the telephone line is assigned 444-1234.

Task 7. Configuring Ports and Lines

Ports and lines are configured after the following occur:

- The serial channels are operational.
- POTS telephone calls are successfully routed to the modems.

Each modem is mapped to a dedicated asynchronous line inside the universal gateway. After the **modem inout** command is applied to the lines, the gateway is ready to accept modem calls.

AAA security is applied to the lines by the **aaa new-model** command and **aaa authentication login default local** command. AAA performs logon authentication by using the local username database. The **login** keyword authenticates EXEC-shell users.

Note Defaults for integrated modems are modem speed 115200 bps and hardware flow control.

To configure ports and lines, perform the following steps.

Step 1 Configure modem control (DCD/DTR) for incoming and outgoing modem calls.

```
Gateway(config)# line 2/00 10/323
Gateway(config-line)# modem InOut
```

Note The **no modem log rs232** command limits the size of the **show modem log** command output.

Step 2 Familiarize yourself with the modem-numbering scheme for the Cisco AS5850. Modems use the *slot*/*port* notation.

```
Gateway# show spe
```

Step 3 Choose a specific modem and inspect the modem-to-TTY line association. TTY lines are simulated EIA/TIA-232 ports. In this example, TTY 648 is associated with modem 1/00.

TTY line numbers map to specific slots. Each slot is hard-coded with 324 TTY lines. In the example, the first modem card is in slot 1.

```
Gateway# show SPE modem 1/00
```

Task 8. Enabling IP Basic Setup

To tune IP routing behavior and domain-name services for EXEC-shell users, perform the following steps.

Step 1 Optimize IP routing functions. Enter the following commands in global configuration mode:

```
Gateway(config)# ip subnet-zero
Gateway(config)# no ip source-route
Gateway(config)# ip classless
```

Table 8 describes the previous commands.

Table 8 IP Routing Commands

Command	Purpose
`ip subnet-zero`	Specifies that 172.22.0.0 is a valid subnet.
`no ip source-route`	Tightens security by ensuring that IP-header packets cannot define their own paths through the universal gateway.
`ip classless`	Turns off traditional IP network class distinctions in the gateway (Class-A, Class-B, Class-C).

Step 2 Enter domain-name service global configuration commands to support EXEC-shell users.

```
ip domain-lookup
ip host aurora 172.22.100.9
ip domain-name the.doc
ip name-server 172.22.11.10
ip name-server 172.22.12.10
```

Table 9 describes the previous commands.

Table 9 Domain-Name Commands

Command	Purpose
`ip domain-lookup`	Enables IP domain-name lookups.
`ip host aurora 172.22.100.9`	Creates a local name-to-address map. This map is useful when the gateway is not entered in a DNS server.
`ip domain-name the.doc`	Tells the gateway how to qualify DNS look ups. In this example, the.doc is appended to the end of each name that is looked up.
`ip name-server 172.22.11.10` `ip name-server 172.22.12.10`	Specifies the primary and secondary name servers. They are used for mapping names to IP addresses.

Task 9. Testing Asynchronous EXEC-Shell Connections

This task verifies that the following components are working:

- Physical asynchronous data path
- Basic modem links
- Basic IP functionality to support EXEC-shell sessions

The Cisco IOS software provides a command-line interface (CLI) called the EXEC. The EXEC has the following properties:

- Can be accessed by dialing in with a modem
- Provides access to terminal EXEC-shell services (no PPP) to do the following:
  - Modify configuration files
  - Change passwords
  - Troubleshoot possible problems including modem connections
  - Access other network resources through use of Telnet

While performing this task, some administrators try to make complex services function, such as PPP-based web browsing. However, many other elements still need to be configured (for example, PPP and IPCP) before these services may be configured.

The asynchronous-shell test ensures that the EXEC log-in prompt can be accessed by a client modem. Taking a layered approach to building a network isolates problems and saves time.

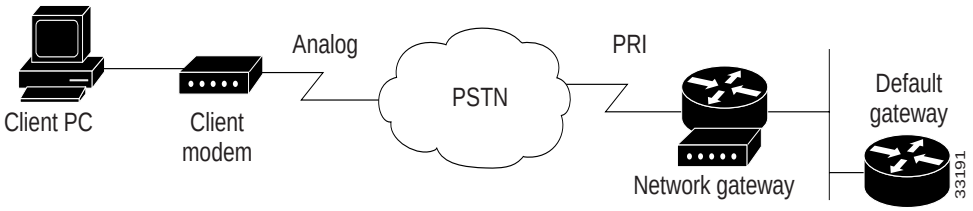
Note

- The Cisco AS5850 is designed to process primarily PPP sessions. If you need to support high levels of EXEC-shell users or V.120 users compared to PPP sessions, ask your support team to advise you on optimal system configuration.
- Many modems support the **a/** command, which recalls the last AT command. The **ath** command hangs up a modem call. The **atdl** command dials the last telephone number.

To test asynchronous EXEC-shell connections, perform the following steps.

Step 1 Locate a client PC, client modem, and analog line. From the client PC, open a terminal-emulation program (such as Hyper Terminal, not Dial-Up Networking) and connect to the client modem. Figure 6 shows the network environment for this test.

Figure 6 Network Test Environment



Step 2 From a terminal-emulation program, test the EIA/TIA-232 connection to the client modem. Enter the **at** command. The modem sends an OK return message.

```
at
OK
```

Step 3 Dial the PRI telephone number assigned to the universal gateway. After the modem successfully connects, a connect message appears.

```
atdt5551234
CONNECT 28800 V42bis
```

Step 4 Log on to the EXEC session.

```
This is a secured device.
Unauthorized use is prohibited by law.

User Access Verification

Username: theuser
Password:

Gateway>
```

Step 5 Determine upon which line the call landed. The following example shows that TTY line 436 accepted the call. The call has been up and active for 20 seconds.

```
Gateway# show caller
                                                Active    Idle
  Line         User               Service       Time      Time
  con 0        admin              TTY           00:13:43  00:00:00
  tty 648    theuserTTY           00:00:20  00:00:08

Gateway# show caller user theuser

  User: theuser, line tty 436, service TTY
        Active time 00:00:34, Idle time 00:00:09
  Timeouts:            Absolute  Idle      Idle
                                 Session   Exec
      Limits:          -         -         00:10:00
      Disconnect in:   -         -         00:09:50
  TTY: Line 1/00
  DS0: (slot/unit/channel)=0/4/2
  Status: Ready, Active, No Exit Banner
  Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out
                Modem Callout, Modem RI is CD
  Modem State: Ready

Gateway#
```

Step 6 Test the IP functionality to support shell sessions. From the universal gateway, Telnet to another device in your network.

```
Gateway# telnet 172.22.66.26
Trying 172.22.66.26 ... Open

User Access Verification

Username: admin
Password:
Gateway#
```

Task 10. Configuring GigE Egress

To commission Gigabit Ethernet service, perform the following steps.

Note See Table 10 for additional Gigabit Ethernet interface commands and descriptions.

Step 1 Assign IP addresses.

```
Gateway# config t
Gateway(config)# interface GigabitEthernet6/1
Gateway(config-if)# ip address 172.21.101.50 255.255.255.0
```

Configure additional IP addresses as required.

Step 2 Bring the interface online (up).

```
Gateway(config-if)# no shutdown
```

Step 3 Verify that the Gigabit Ethernet interface is up.

```
Gateway# show interface gigabitethernet6/1
GigabitEthernet6/1 is up, line protocol is up
```

Step 4 Verify network connectivity between the interface and a device on the network using the ping utility. This step verifies that you have IP connectivity with another device on the subnet.

```
Gateway# ping 172.22.66.1

Sending 5, 100-byte ICMP Echos to 172.22.66.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

Gateway#
```

Table 10 Summary of Optional Gigabit Ethernet Interface Commands

Command	Purpose
`[no] ip redirects`	Sends an ICMP Redirect message to the originator of any datagram that the gateway is forced to resend through the same interface on which it was received, since the originating host could presumably have sent that datagram to the ultimate destination without involving the gateway at all. The gateway ignores *Redirect* messages that have been sent to it by other gateways. Use the **ip redirects interface** subcommand to enable or disable the sending of these messages.
`[no] ip route-cache`	Enables/disables the use of high-speed switching caches for IP routing.

Table 10 Summary of Optional Gigabit Ethernet Interface Commands (continued)

Command	Purpose
[**no**] **ip route-cache distributed**	Enables/disables VIP distributed switching on the interface. If both **ip route-cache flow** and **ip route-cache distributed** are configured, the VIP does distributed flow switching. If only **ip route-cache distributed** is configured, the VIP does distributed switching.
[**no**] **ip mroute-cache**	Enables/disables fast switching on the interface.
logging event link-status	Logs *link-status* events to the syslog server or other management server.
negotiation auto	Auto-negotiates the link speed for the line (100mbps, 1000mpbs for GigE).
[**no**] **cdp enable**	Enables/disables Cisco Discovery Protocol on the interface. This is on by default.

Task 11. Confirming the Final Running Configuration

After you complete the tasks in this section, your final running configuration looks like this.

```
Gateway# show running-config

Building configuration...
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Gateway
!
resource-pool disable
!
modem-pool Default
 pool-range 0/0-0/215,1/0-1/323,13/0-13/215
!
ip subnet-zero
ip host aurora 172.21.100.100
ip domain-name the.doc
ip name-server 172.22.11.10
ip name-server 172.22.12.11
!
redundancy
 mode classic-split
isdn switch-type primary-5ess
!
controller T3 0/0
 framing m23
 cablelength 0
 t1 1-2 controller
!
controller T1 0/0:1
 framing esf
 pri-group timeslots 1-24
```

```
!
controller T1 0/0:2
 framing esf
 pri-group timeslots 1-24
!
interface Serial0/0:1:23
 no ip address
 ip mroute-cache
 isdn switch-type primary-5ess
 isdn incoming-voice modem
!
interface Serial0/0:2:23
 no ip address
 ip mroute-cache
 isdn switch-type primary-5ess
 isdn incoming-voice modem
!
interface FastEthernet6/0
 no ip address
 ip route-cache distributed
 logging event link-status
 shutdown
!

interface GigabitEthernet6/0
 no ip address
 ip route-cache distributed
 logging event link-status
 shutdown
 no negotiation auto
!
interface GigabitEthernet6/1
 no ip address
 ip route-cache distributed
 logging event link-status
 shutdown
 no negotiation auto
!
interface Async0/00
 no ip address
 ip route-cache distributed
!
interface Async0/01
 no ip address
 ip route-cache distributed
!
interface Async0/02
 no ip address
 ip route-cache distributed
!
interface Async0/03
 no ip address
 ip route-cache distributed
!
interface Group-Async0
 no ip address
 ip route-cache distributed
 no group-range
!
ip classless
no ip http server
ip pim ssm
!
line con 0
```

```
 transport input none
line aux 0
line vty 0 4
line 0/00 0/215
 modem InOut
 no modem ibc
 no modem status-poll
 no modem log rs232
line 1/00 1/323
 modem InOut
 no modem ibc
 no modem status-poll
 no modem log rs232
line 13/00 13/215
 modem InOut
 no modem ibc
 no modem status-poll
 no modem log rs232
end
```

If your configuration is close to the above, your Cisco AS5850 is now configured for basic dial-up services. If your configuration differs significantly, retrace your steps to make sure no sections were skipped.

Note To configure AAA and other advanced services, see *Cisco AS5850 Operations, Administration, Maintenance, and Provisioning Guide*, available online at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5850/sw_conf/5850oamp/index.htm.

Additional References

This section contains the following information:

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

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

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

http://www.cisco.com/go/marketplace/

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

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

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

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

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

- Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

- Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.
- Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

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

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

This document is to be used in conjunction with the *Cisco AS5850 Universal Gateway Hardware Installation Guide*, *Cisco AS5850 Universal Gateway Card Guide*, and *Cisco AS5850 Operations, Administration, Maintenance, and Provisioning Guide*.