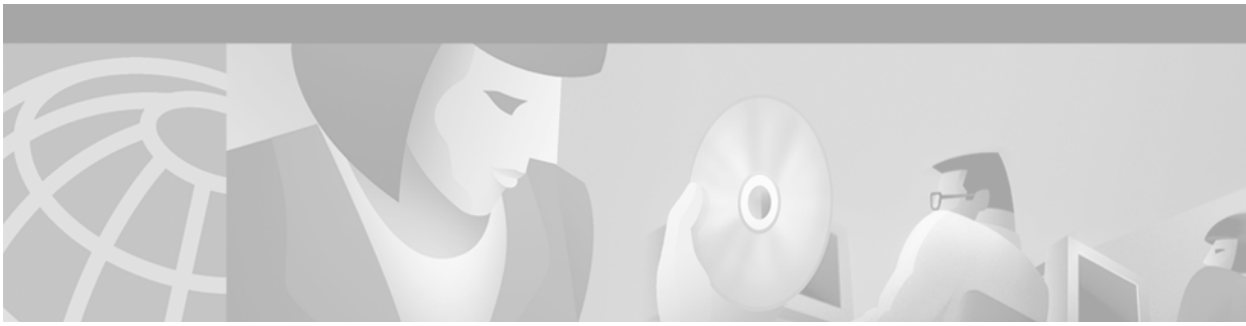

Release Notes for Cisco 800 Series Routers

This document describes new and changed information for the *Cisco 800 Series Routers Software Configuration Guide, Cisco 800 Series Routers Hardware Installation Guide, Quick Start Guide: Setting Up Cisco 800 Series Routers, Cisco 811 and Cisco 813 Routers Hardware Installation Guide,* and *Quick Start Guide: Setting Up Cisco 811 and Cisco 813 Routers*.

Remote CAPI Default Setting

The default setting for the Remote Common Application Programming Interface (CAPI) feature has been changed. By default, this feature is disabled. To enable this feature, use the IOS **rcapi server port** command in global configuration mode:

rcapi server port [*number***]**

no rcapi server port

where *number* is an optional parameter for the port number. If you do not enter a port number, the default port 2578 is used.

For more information, see the "Configuring Remote CAPI" chapter in the *Cisco 800 Series Software Configuration Guide.*

Supplementary Telephone Services for the Net3 Switch

The Cisco 800 series routers now support the following plain old telephone service (POTS) features for the European Telecommunications Standards Institute (ETSI) Net3 switch type:

- Caller ID presentation and restriction are available for Denmark and Finland. For more information, see "Configuring Caller ID for the Net3 Switch."
- Calling line identification restriction (CLIR) temporarily prevents your calling ID from being presented to the destination number for an outgoing call. You must configure CLIR before each call that you wish to restrict the calling party number from being presented at the destination.

CISCO SYSTEMS

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

78-5371-07

- Call forwarding is enabled by using IOS and dual tone multifrequency (DTMF) commands. For more information, see "Call Forwarding for the Net3 Switch."
- Call transfer enables you to connect two call destinations. The request for this service must originate from an active, outgoing call.

Requirements for Supplementary Telephone Services Support

You must subscribe to the following Net3 switch services for these supplementary telephone services to work:

- Calling line identification presentation (CLIP)
- CLIR in temporary mode
- Call holding
- Call transfer
- Call forwarding
- Call waiting

Configuring Caller ID for the Net3 Switch

To enable caller ID on the Net3 switch, configure the country type by using the IOS **pots country** command in global configuration mode:

pots country {dk|fi}

Note Caller ID for the Net3 switch is always enabled, provided that the POTS country type is correctly defined. Caller ID cannot be disabled using the IOS command-line interface (CLI).

To verify whether caller ID is enabled, use the **show pots status** command. The following is an example of the output from that command:

```
router# show pots status

POTS Global Configuration:

   Country:Denmark

   Dialing Method:Overlap, Tone Source:Local, CallerId Support:YES
----------------------
   Out Going Hunt:Disabled
```

Call Forwarding for the Net3 Switch

The following types of call forwarding services (for voice calls only) are supported on the Net3 switch:

- Call forward unconditional (CFU) redirects your calls without restrictions and takes precedence over other call forwarding types.
- Call forward busy (CFB) redirects your call to another number if your number is busy.
- Call forward no reply (CFNR) forwards your call to another number if your number does not answer within a specified period of time.

You can select one or more call forwarding services at a time. However, CFU has the highest precedence, CFB the next highest, and CFNR the lowest. The default setting is that no forwarding type is selected.

Note If you had configured call forwarding for a POTS port and the router finds that a dial peer is also configured for that port, call forwarding works only for the number defined in the **destination-pattern** dial-peer command and ignores all other numbers for that telephone. If the router does not find a dial peer or if the destination pattern is not defined, then call forwarding works for all numbers allocated to the ISDN line.

To enable and configure this feature, follow these steps:

Step 1 Enable and select the call forwarding method. See "Configuring the Call Forwarding Method."

Step 2 Configure your call forwarding service, depending on which method you previously selected:

- Functional method—Enter DTMF commands on the telephone keypad. For more information, see "Configuring the Call Forwarding Service."
- Keypad method—Follow the instructions in your Net3 switch documentation.

Configuring the Call Forwarding Method

You can select the method by which the call forwarding feature is controlled:

- Functional method gives control to the router. If you select this method, use the DTMF commands documented in "Configuring the Call Forwarding Service."
- Keypad method gives control to the Net3 switch.

To enable the call forwarding method, use the IOS **pots forwarding-method** command in global configuration mode:

pots forwarding-method {functional | keypad}

[no] pots forwarding-method

Note Use the **pots forwarding-method** command to configure only Net3 switch types. This command does not work for other switch types. This feature is disabled in the default setting.

The following example configures the call forwarding feature to give control to the router:

```
router# configure terminal
router(config)# pots forwarding-method functional
```

Configuring the Call Forwarding Service

Table 1 shows the DTMF keypad command sequence that you enter to configure the call forwarding service.

Table 1 Configuring the Call Forwarding Service

Task	DTMF Keypad Command
Activate CFU	****21***_number_**#** where *number* is the telephone number to which your calls are forwarded
Deactivate CFU	**#21#**
Activate CFNR	****61***_number_**#** where *number* is the telephone number to which your calls are forwarded
Deactivate CFNR	**#61#**
Activate CFB	****67***_number_**#** where *number* is the telephone number to which your calls are forwarded
Deactivate CFB	**#67#**

You should hear a dial tone after you enter the DTMF commands if the call forwarding service is successfully configured. If you hear a busy signal, either the command is invalid or the switch does not support that service.

Displaying POTS Status

Use the **show pots status** command to display details of the call forwarding type. This status is not stored when you reboot. The following is an example of the screen output:

```
router# show pots status

POTS Global Configuration:
Country:Denmark
Dialing Method:Overlap, Tone Source:Local, CallerId Support:YES
Out Going Hunt:Disabled
Forwarding Method:functional method
-------------------------------------

Call Forwarding status:

The Forwarding Method Enabled is CFU

The forwarded to Address is     :33236877
The served user Number(s) are   :33795742

The Forwarding Method Enabled is CFB

The forwarded to Address is     :33236877
The served user Number(s) are   :
    ALL -> Will work for all numbers allocated to the terminal.
```

Configuring CLIR

Configure CLIR by following these steps:

Step 1 Ensure that CLIR in temporary mode is enabled in the Net3 switch.

Step 2 Remove the handset and press ****31#** on the keypad.

Step 3 Listen for the dial tone, and then make your call.

Step 4 Repeat Steps 2 and 3 for each outgoing call for which you wish to restrict your calling identification.

Debug POTS Commands

Use the following commands to debug problems with caller ID configuration:

- **debug pots driver**
- **debug pots csm**

Use the following commands for problems configuring other supplementary telephone features:

- **debug pots csm**
- **debug isdn event**
- **debug isdn q931**

For more information about using debug commands, see the IOS documentation.

Prefix Dialing

Cisco 803 and Cisco 804 routers now support prefix dialing. You can add a telephone prefix and create a prefix filter to the dialed number for analog telephone calls. When a telephone number is dialed through the telephone port, the router checks for prefix filters. If the router finds a match, no prefix is added to the dialed number. If no filter match is found, the router adds the user-defined prefix to the called number.

Configuring a Prefix Number

To set a prefix to be added to a telephone number called, use the Cisco IOS **pots prefix number** command in global configuration mode:

pots prefix number *number*

no pots prefix number

where *number* is a prefix number from one to five digits in length. Only one prefix can be configured at a time, and configuring a new number will overwrite the existing one.

The following example sets the prefix number to *12345:*

```
router# configure terminal
router(config)# pots prefix number 12345
```

Configuring a Prefix Filter

You can configure a prefix filter that is compared to the digits that you dial. If a match occurs, the prefix number is not added to the called number. To create a prefix filter, use the **pots prefix filter** command in global configuration mode:

pots prefix filter *number*

no pots prefix filter *number*

where *number* is a prefix filter from one to eight digits in length. You can define up to ten filters for your router. If you have reached the maximum number of filters defined, no new filter configurations are accepted until you remove at least one existing filter number using the **no pots prefix filter** *number* command.

The following are examples of how to set prefix filters:

```
router# configure terminal
router(config)# pots prefix filter 192
router(config)# pots prefix filter 1
router(config)# pots prefix filter 9
router(config)# pots prefix filter 0800
router(config)# pots prefix filter 08456
```

Cisco 800 Series Router Enhancements

Cisco 800 series routers now support the following features:

- Hot Standby Routing Protocol (HSRP), which creates a Hot Standby router group with a lead router that services all packets sent to the Hot Standby address. The lead router is monitored by other routers in the group. If it fails, one of these standby routers inherits the lead position and the Hot Standby group address.
- Service Assurance Agent (SAA), which is both an enhancement to and a new name for the Response Time Reporter (RTR) feature that was introduced in Cisco IOS release 11.2. This feature allows you to monitor network performance by measuring key Service Level Agreement (SLA) metrics, such as response time, network resources, availability, jitter, connect time, packet loss, and application performance.
- Triple Data Encryption Standard (3DES), based on the standard cryptographic algorithm developed by the U.S. National Bureau of Standards.
- X.28, X.29, and X.3 emulation for Packet Assember/Disassembler (PAD), the standard user interface between the data terminal equipment and PAD.
- Frame Relay Inverse Address Resolution Protocol (ARP), which enables a station to request a protocol address corresponding to a given hardware address.
- Frame Relay support for a permanent virtual circuit (PVC) saves bandwidth associated with circuit establishment and tear down in situations where certain virtual circuits must exist all the time.

For more information about these features, see the Cisco IOS documentation set.

TinyROM Version 1.3(1) Enhancements

TinyROM performs the following functions for Cisco 800 series routers:

- Starts power-on self-test (POST) and makes minor configuration adjustments
- Loads and boots an IOS software image
- Uploads a new IOS software image

TinyROM has been enhanced to handle multiple Cisco IOS **boot system** commands, to ensure that your Cisco 800 series router boots with the IOS software.

The behavior of the IOS **boot system** command depends on which versions of TinyROM and IOS software you have installed on your router. The following section describes the behavior of various combinations of TinyROM and IOS software.

To view which versions of TinyROM and IOS are installed on your router, use the **show version** command in Exec mode.

Note For more information about Cisco IOS commands, see the IOS documentation set.

TinyROM and Cisco IOS Behavior

Table 2 summarizes the behavior of different versions of TinyROM and the IOS software.

Table 2 Summary of TinyROM and IOS Software Behavior

TinyROM Version	IOS Release	TinyROM and IOS Behavior
1.3(1)	12.1(2.2) and later	• TinyROM can handle multiple **boot system** commands in the order they were issued and will attempt to boot the valid images specified. • If none of the specified images boots, TinyROM boots any of the unspecified IOS images stored in Flash memory. • IOS will fail to boot only if there are no valid images, or if the router was configured to boot only from TinyROM.
1.2(3) and earlier	12.1(2.2) and later	• TinyROM cannot boot from more than one image. If the single image specified fails to boot, TinyROM boots from any valid image stored in Flash memory. TinyROM attempts to boot first from undeleted images, then to those marked for deletion. • IOS checks the validity of the single boot filename. If the filename is not valid, IOS will display warning messages to that effect.
1.2(1) and earlier	Any	TinyROM does not boot from an unspecified image in Flash memory. If the single IOS image that you specify fails to boot, the router remains at the boot# prompt without booting the IOS.
Any	12.1(2.1) and earlier	• IOS will modify the single boot image only if you use the IOS **boot system** command. Changes to the boot system by any other means (such as copying from TFTP or from Flash memory backup) are ignored. • Output from the **show startup** command does not show the correct boot filename unless you edit the boot system list to match the ROM boot filename.

Workaround for Earlier Versions of TinyROM

If you have TinyROM version 1.2(2) or later, you can rely on the boot fallback capability to ensure that IOS is booted, provided that you have at least one IOS image stored in Flash memory that is not marked for deletion.

Note If you have TinyROM version 1.2(1) or earlier installed on a remotely administered router, we strongly recommend that, at a minimum, you upgrade the IOS software. Using the workaround documented in this section will always boot IOS, but this procedure is susceptible to user error. Even a minor error could result in IOS not booting on your router.

If you have TinyROM version 1.2(1) or earlier, ensure that IOS will be booted by following these steps:

	Command	Description
Step 1	router# **configure terminal**	Enter the global configuration mode.
Step 2	router(config)# **no boot system flash** *old-c800-image0*	Clear all existing **boot system** commands from the configuration.
Step 3	router(config)# **boot system flash** *c800-nsy6-mw*	Specify the boot filename in the configuration. (See Note.)
Step 4	router(config)# **end**	End global configuration mode.
Step 5	router# **write memory**	Configure the boot order in IOS.

Note This step does not require the Flash file system designation (*flash:* preceding the filename).

You should have only one **boot system** command in your configuration that specifies which file to boot. To verify your configuration, use the **show running-config** command. To obtain a list of filenames, use the **dir** command. Files marked with **-r-x** are valid IOS boot file images. For more information, see the output example following these steps.

The following examples show the screen output for the **show run** and **dir** commands:

```
router# show run
 Building configuration...

 Current configuration:
 !
 version 12.1
 !
 boot config flash:backup-config
 boot system flash c800-nsy6-mw
 logging buffered 4096 debugging
 !
 ...
 router# dir
 Directory of flash:/

   0  ----       49088   Jan 20 2000 05:11:57  TinyROM-1.2(1)
   1  ----       49088   May 12 2000 04:43:56  TinyROM-1.3(1)
   2  -r-x     3664268   May 19 2000 22:07:32  c800-nsy6-mw
  58  -r--         750              <no date>  backup-config

 12582912 bytes total (8716288 bytes free)
 router#
```

Upgrading TinyROM and IOS Software

If you wish to upgrade TinyROM and IOS software, do the following:

- First upgrade TinyROM and then upgrade IOS. This is the recommended sequence.
- Use the Trivial File Transfer Protocol (TFTP) to upgrade IOS. It is faster and easier to do so by using TFTP.

- You need access to a console to upgrade TinyROM, because you cannot do so over the WAN. For more information, see Appendix D, "ROM Monitor and TinyROM," in the *Cisco 800 Series Routers Software Configuration Guide.*
- After upgrading IOS, enter the **write memory** command so that the new version of IOS will properly configure the boot order. If you are using the boot config feature, copy the full-config file from Flash memory to the running-config file, as in the following example:

```
boot# copy flash:full-config running-config
```

Note To obtain the name of the full-config file in Flash memory, review the boot config section of the output for the **show startup-config** command.

Correction to Modem Support Information

Cisco 803, 804, and 813 routers do not support the use of any modem that is connected to telephone ports. The sections describing the installation and troubleshooting of analog telephones, fax machines, and modems in the following documents apply only to analog telephones and fax machines:

- *Cisco 800 Series Routers Hardware Installation Guide*
- *Quick Start Guide: Setting Up Cisco 800 Series Routers*
- *Cisco 811 and Cisco 813 Routers Hardware Installation Guide*
- *Quick Start Guide: Setting Up Cisco 811 and Cisco 813 Routers*
- *Cisco 800 Series Routers Software Configuration Guide*

Caller ID on the Cisco 813 Router

The caller ID command syntax documented in "Configuring Caller ID Display" (page 8-3) in Chapter 8, "Configuring Enhanced Voice Features," of the *Cisco 800 Series Routers Software Configuration Guide* is incorrect. The correct information is as follows:

By default, the caller ID feature is disabled. To enable this feature, use the IOS **caller-id** command in the dial-peer configuration command mode.

caller-id

[no] caller-id

POTS Dial Feature

The Cisco 813 router supports the plain old telephone service (POTS) dial feature for Japanese telephones. This feature can be activated by a dial application on your workstation that dials a telephone number for the POTS port on the Cisco 813 router. The telephone connected to the port can be on- or off-hook when the dial command is issued. If the telephone is on-hook, the router rings the telephone, waits until the telephone is taken off hook, then dials the number requested. If the telephone is off-hook when the command is issued, the router dials the number requested, provided the telephone is receiving a dial tone.

Activating the POTS Dial Feature

Each time you wish to activate this feature using your dial application, enter the following IOS command in Exec mode:

test pots *port* **dial** *number***[#]**

where *port* is the port number 1 or 2, and *number* is the telephone number to dial.

Note The router does not turn off dual tone multifrequency (DTMF) detection from the telephone when you enter the POTS dial command. If you do not terminate the *number* variable with a pound (**#**) character, you can complete the call by using the telephone key pad.

The following example shows the POTS dial command:

```
router# test pots 1 dial 4085551234#
```

Displaying POTS Call State

To show the current state of POTS calls and the most recent event received by the call switching module (CSM), use the **show pots csm** command in Exec mode.

show pots csm *port*

where *port* is port number 1 or 2.

Output Example

The following is an example of the **show pots csm** command screen output:

```
router# show pots csm 1

POTS PORT: 1

   CSM Finite State Machine:
      Call 0 - State: idle, Call Id: 0x0
               Active: no
               Event: CSM_EVENT_NONE Cause: 0
      Call 1 - State: idle, Call Id: 0x0
               Active: no
               Event: CSM_EVENT_NONE Cause: 0
      Call 2 - State: idle, Call Id: 0x0
               Active: no
               Event: CSM_EVENT_NONE Cause: 0

router#
```

Disconnecting a POTS Call

To disconnect a telephone call for the POTS port on the router, use the **test pots** *port* **disconnect** command in Exec mode.

test pots *port* **disconnect**

where *port* is the port number 1 or 2.

The following example disconnects a telephone call from POTS port 1:

```
router# test pots 1 disconnect
router#
```

POTS Debug Command

To display the status of calls made to and from the POTS ports, enter the following command in Exec mode:

debug pots csm

Entering this command activates events by which your dial application can determine the progress of calls to and from the ports.

Debug Message Formats

Debug messages are displayed in one of two formats that are relevant to the POTS dial feature:

hh:mm:ss: CSM_STATE: CSM_EVENT, call id = ??, port = ?

or

hh:mm:ss: EVENT_FROM_ISDN:dchan_idb=0x???????, call_id=0x????, ces=? bchan=0x????????, event=0x?, cause=0x??

where:

- *hh:mm:ss* is a timestamp in hours, minutes, and seconds.
- *CSM_STATE* is one of the call switching module (CSM) states listed in Table 3.
- *call id* is a hexadecimal value from 0x00 to 0xFF.
- *port* is telephone port 1 or 2.
- *EVENT_FROM_ISDN* is a CSM event. Table 4 shows a list of CSM events.
- *dchan_idb* is an internal data structure address.
- *ces* is the connection end point suffix used by ISDN.
- *bchan* is the channel used by the call. A value of 0xFFFFFFFF indicates that a channel is not assigned.
- *event* is represented by a hexadecimal value that is translated into a CSM event. Table 5 shows a list of events and the corresponding CSM events.
- *cause* is represented by a hexadecimal value that is given to call-progressing events. Table 6 shows a list of cause values and definitions.

CSM States

The following table shows the values for CSM states.

Table 3 CSM States

CSM State	Description
CSM_IDLE_STATE	Telephone on hook
CSM_RINGING	Telephone ringing

Table 3 CSM States (continued)

CSM State	Description
CSM_SETUP	Setup for outgoing call in progress
CSM_DIALING	Dialing number of outgoing call
CSM_IVR_DIALING	Interactive voice response (IVR) for Japanese telephone dialing
CSM_CONNECTING	Waiting for carrier to connect the call
CSM_CONNECTED	Call connected
CSM_DISCONNECTING	Waiting for carrier to disconnect the call
CSM_NEAR_END_DISCONNECTING	Waiting for carrier to disconnect the call
CSM_HARD_HOLD	Call on hard hold
CSM_CONSULTATION_HOLD	Call on consultation hold
CSM_WAIT_FOR_HOLD	Waiting for carrier to put call on hard hold
CSM_WAIT_FOR_CONSULTATION_HOLD	Waiting for carrier to put call on consultation hold
CSM_CONFERENCE	Waiting for carrier to complete call conference
CSM_TRANSFER	Waiting for carrier to transfer call
CSM_APPLIC_DIALING	Call initiated from IOS command-line interface (CLI)

CSM Events

The following table shows the values for CSM events.

Table 4 CSM Events

CSM Events	Description
CSM_EVENT_INTER_DIGIT_TIMEOUT	Time waiting for dial digits has expired
CSM_EVENT_TIMEOUT	Near or far end disconnect timeout
CSM_EVENT_ISDN_CALL	Incoming call
CSM_EVENT_ISDN_CONNECTED	Call connected
CSM_EVENT_ISDN_DISCONNECT	Far end disconnected
CSM_EVENT_ISDN_DISCONNECTED	Call disconnected
CSM_EVENT_ISDN_SETUP	Outgoing call requested
CSM_EVENT_ISDN_SETUP_ACK	Outgoing call accepted
CSM_EVENT_ISDN_PROC	Call proceeding and dialing completed
CSM_EVENT_ISDN_CALL_PROGRESSING	Call being received in band tone
CSM_EVENT_ISDN_HARD_HOLD	Call on hard hold
CSM_EVENT_ISDN_HARD_HOLD_REJ	Hold attempt rejected
CSM_EVENT_ISDN_CHOLD	Call on consultation hold
CSM_EVENT_ISDN_CHOLD_REJ	Consultation hold attempt rejected

Table 4 CSM Events (continued)

CSM Events	Description
CSM_EVENT_ISDN_RETRIEVED	Call retrieved
CSM_EVENT_ISDN_RETRIEVE_REJ	Call retrieval attempt rejected
CSM_EVENT_ISDN_TRANSFERRED	Call transferred
CSM_EVENT_ISDN_TRANSFER_REJ	Call transfer attempt rejected
CSM_EVENT_ISDN_CONFERENCE	Call conference started
CSM_EVENT_ISDN_CONFERENCE_REJ	Call conference attempt rejected
CSM_EVENT_ISDN_IF_DOWN	ISDN interface down
CSM_EVENT_ISDN_INFORMATION	ISDN information element received (used by Nippon Telegraph and Telephone [NTT] IVR application)
CSM_EVENT_VDEV_OFFHOOK	Telephone off hook
CSM_EVENT_VDEV_ONHOOK	Telephone on hook
CSM_EVENT_VDEV_FLASHHOOK	Telephone hook switch has flashed
CSM_EVENT_VDEV_DIGIT	DTMF digit has been detected
CSM_EVENT_VDEV_APPLICATION_CALL	Call initiated from IOS command-line interface (CLI)

Events

The following table shows the values for events that are translated into CSM events.

Table 5 Event Values and Corresponding CSM Events

Hexadecimal Value	Event	CSM Event
0x0	DEV_IDLE	CSM_EVENT_ISDN_DISCONNECTED
0x1	DEV_INCALL	CSM_EVENT_ISDN_CALL
0x2	DEV_SETUP_ACK	CSM_EVENT_ISDN_SETUP_ACK
0x3	DEV_CALL_PROC	CSM_EVENT_ISDN_PROC
0x4	DEV_CONNECTED	CSM_EVENT_ISDN_CONNECTED
0x5	DEV_CALL_PROGRESSING	CSM_EVENT_ISDN_CALL_PROGRESSING
0x6	DEV_HOLD_ACK	CSM_EVENT_ISDN_HARD_HOLD
0x7	DEV_HOLD_REJECT	CSM_EVENT_ISDN_HARD_HOLD_REJ
0x8	DEV_CHOLD_ACK	CSM_EVENT_ISDN_CHOLD
0x9	DEV_CHOLD_REJECT	CSM_EVENT_ISDN_CHOLD_REJ
0xa	DEV_RETRIEVE_ACK	CSM_EVENT_ISDN_RETRIEVED
0xb	DEV_RETRIEVE_REJECT	CSM_EVENT_ISDN_RETRIEVE_REJ
0xc	DEV_CONFR_ACK	CSM_EVENT_ISDN_CONFERENCE
0xd	DEV_CONFR_REJECT	CSM_EVENT_ISDN_CONFERENCE_REJ

Table 5 Event Values and Corresponding CSM Events (continued)

Hexadecimal Value	Event	CSM Event
0xe	DEV_TRANS_ACK	CSM_EVENT_ISDN_TRANSFERRED
0xf	DEV_TRANS_REJECT	CSM_EVENT_ISDN_TRANSFER_REJ

Cause

This table shows cause values that are assigned only to call-progressing events.

Table 6 Cause Values and Definitions

Hexadecimal Value	Cause Definitions
0x01	UNASSIGNED_NUMBER
0x02	NO_ROUTE
0x03	NO_ROUTE_DEST
0x04	NO_PREFIX
0x06	CHANNEL_UNACCEPTABLE
0x07	CALL_AWARDED
0x08	CALL_PROC_OR_ERROR
0x09	PREFIX_DIALED_ERROR
0x0a	PREFIX_NOT_DIALED
0x0b	EXCESSIVE_DIGITS
0x0d	SERVICE_DENIED
0x10	NORMAL_CLEARING
0x11	USER_BUSY
0x12	NO_USER_RESPONDING
0x13	NO_USER_ANSWER
0x15	CALL_REJECTED
0x16	NUMBER_CHANGED
0x1a	NON_SELECTED_CLEARING
0x1b	DEST_OUT_OF_ORDER
0x1c	INVALID_NUMBER_FORMAT
0x1d	FACILITY_REJECTED
0x1e	RESP_TO_STAT_ENQ
0x1f	UNSPECIFIED_CAUSE
0x22	NO_CIRCUIT_AVAILABLE
0x26	NETWORK_OUT_OF_ORDER
0x29	TEMPORARY_FAILURE

Table 6 Cause Values and Definitions (continued)

Hexadecimal Value	Cause Definitions
0x2a	NETWORK_CONGESTION
0x2b	ACCESS_INFO_DISCARDED
0x2c	REQ_CHANNEL_NOT_AVAIL
0x2d	PRE_EMPTED
0x2f	RESOURCES_UNAVAILABLE
0x32	FACILITY_NOT_SUBSCRIBED
0x33	BEARER_CAP_INCOMPAT
0x34	OUTGOING_CALL_BARRED
0x36	INCOMING_CALL_BARRED
0x39	BEARER_CAP_NOT_AUTH
0x3a	BEAR_CAP_NOT_AVAIL
0x3b	CALL_RESTRICTION
0x3c	REJECTED_TERMINAL
0x3e	SERVICE_NOT_ALLOWED
0x3f	SERVICE_NOT_AVAIL
0x41	CAP_NOT_IMPLEMENTED
0x42	CHAN_NOT_IMPLEMENTED
0x45	FACILITY_NOT_IMPLEMENT
0x46	BEARER_CAP_RESTRICTED
0x4f	SERV_OPT_NOT_IMPLEMENT
0x51	INVALID_CALL_REF
0x52	CHAN_DOES_NOT_EXIST
0x53	SUSPENDED_CALL_EXISTS
0x54	NO_CALL_SUSPENDED
0x55	CALL_ID_IN_USE
0x56	CALL_ID_CLEARED
0x58	INCOMPATIBLE_DEST
0x5a	SEGMENTATION_ERROR
0x5b	INVALID_TRANSIT_NETWORK
0x5c	CS_PARAMETER_NOT_VALID
0x5f	INVALID_MSG_UNSPEC
0x60	MANDATORY_IE_MISSING
0x61	NONEXISTENT_MSG
0x62	WRONG_MESSAGE
0x63	BAD_INFO_ELEM

Table 6 Cause Values and Definitions (continued)

Hexadecimal Value	Cause Definitions
0x64	INVALID_ELEM_CONTENTS
0x65	WRONG_MSG_FOR_STATE
0x66	TIMER_EXPIRY
0x67	MANDATORY_IE_LEN_ERR
0x6f	PROTOCOL_ERROR
0x7f	INTERWORKING_UNSPEC

Call Scenarios for the POTS Dial Feature

This section describes three call scenarios and shows examples of the IOS command output for each scenario. The output examples for the **debug** and **disconnect** commands show the sequence of events that occur during a POTS dial call.

Call Scenario 1

In this call scenario, port 1 is on-hook, the application dial is set to call 4085552221, and the far end successfully connects. The following example shows the IOS command:

```
router# test pots 1 dial 4085552221#
router#
```

The following screen output shows an event indicating that port 1 is being used by the dial application:

```
01:58:27: CSM_PROC_IDLE: CSM_EVENT_VDEV_APPLICATION_CALL, call id = 0x0, port = 1
```

The following screen output shows events indicating that the CSM is receiving the application digits of the number to dial:

```
01:58:27: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:58:27: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:58:27: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:58:27: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:58:27: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:58:27: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:58:27: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:58:27: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:58:27: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:58:27: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
```

The following screen output shows that the telephone connected to port 1 is off hook:

```
01:58:39: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_OFFHOOK, call id = 0x0, port = 1
```

The following screen output shows a call-proceeding event pair indicating that the router ISDN software has sent the dialed digits to the ISDN switch:

```
01:58:40: EVENT_FROM_ISDN:dchan_idb=0x280AF38, call_id=0x8004, ces=0x1 bchan=0x0,
event=0x3, cause=0x0
01:58:40: CSM_PROC_ENBLOC_DIALING: CSM_EVENT_ISDN_PROC, call id =
0x8004, port = 1
```

The following screen output shows the call-progressing event pair indicating that the telephone at the far end is ringing:

```
01:58:40: EVENT_FROM_ISDN:dchan_idb=0x280AF38, call_id=0x8004, ces=0x1 bchan=0xFFFFFFFF,
event=0x5, cause=0x0
01:58:40: CSM_PROC_ENBLOC_DIALING: CSM_EVENT_ISDN_CALL_PROGRESSING, call id = 0x8004,
port = 1
```

The following screen output shows a call-connecting event pair indicating that the telephone at the far end has answered:

```
01:58:48: EVENT_FROM_ISDN:dchan_idb=0x280AF38, call_id=0x8004, ces=0x1 bchan=0xFFFFFFFF,
event=0x4, cause=0x0
01:58:48: CSM_PROC_CONNECTING: CSM_EVENT_ISDN_CONNECTED, call id = 0x8004, port = 1
```

The following screen output shows a call-progressing event pair indicating that the telephone at the far end has hung up, and the calling telephone is receiving an in-band tone from the ISDN switch:

```
01:58:55: EVENT_FROM_ISDN:dchan_idb=0x280AF38, call_id=0x8004, ces=0x1 bchan=0xFFFFFFFF,
event=0x5, cause=0x10
01:58:55: CSM_PROC_CONNECTED: CSM_EVENT_ISDN_CALL_PROGRESSING, call id = 0x8004, port = 1
```

The following screen output shows that the telephone connected to port 1 has hung up:

```
01:58:57: CSM_PROC_CONNECTED: CSM_EVENT_VDEV_ONHOOK, call id = 0x8004, port = 1
```

The following screen output shows an event pair indicating that the call has been terminated:

```
01:58:57: EVENT_FROM_ISDN:dchan_idb=0x280AF38, call_id=0x8004, ces=0x1 bchan=0xFFFFFFFF,
event=0x0, cause=0x0
01:58:57: CSM_PROC_NEAR_END_DISCONNECT: CSM_EVENT_ISDN_DISCONNECTED, call id = 0x8004,
port = 1
813_local#
```

Call Scenario 2

In this scenario, port 1 is on-hook, the application dial is set to call 4085552221, and the destination number is busy. The following example shows the IOS command:

```
router# test pots 1 dial 4085552221#
router#
```

The following screen output shows that your dial application is using port 1:

```
01:59:42: CSM_PROC_IDLE: CSM_EVENT_VDEV_APPLICATION_CALL, call id = 0x0, port = 1
```

The following screen output shows the events indicating that the CSM is receiving the application digits of the number to call:

```
01:59:42: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:59:42: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:59:42: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:59:42: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:59:42: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:59:42: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:59:42: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:59:42: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:59:42: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
01:59:42: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
```

The following screen output shows an event indicating that the telephone connected to port 1 is off-hook:

```
01:59:52: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_OFFHOOK, call id = 0x0, port = 1
```

The following screen output shows a call-proceeding event pair indicating that the telephone at the far end is busy:

```
01:59:52: EVENT_FROM_ISDN:dchan_idb=0x280AF38, call_id=0x8005, ces=0x1 bchan=0x0,
event=0x3, cause=0x11
01:59:52: CSM_PROC_ENBLOC_DIALING: CSM_EVENT_ISDN_PROC, call id = 0x8005, port = 1
```

The following screen output shows a call-progressing event pair indicating that the calling telephone is receiving an in-band busy tone from the ISDN switch:

```
01:59:58: EVENT_FROM_ISDN:dchan_idb=0x280AF38, call_id=0x8005, ces=0x1 bchan=0xFFFFFFFF,
event=0x5, cause=0x0
01:59:58: CSM_PROC_ENBLOC_DIALING: CSM_EVENT_ISDN_CALL_PROGRESSING, call id = 0x8005,
port = 1
```

The following screen output shows an event indicating that the calling telephone has hung up:

```
02:00:05: CSM_PROC_ENBLOC_DIALING: CSM_EVENT_VDEV_ONHOOK, call id = 0x8005, port = 1
```

The following screen output shows an event pair indicating that the call has terminated:

```
02:00:05: EVENT_FROM_ISDN:dchan_idb=0x280AF38, call_id=0x8005, ces=0x1 bchan=0xFFFFFFFF,
event=0x0, cause=0x0
02:00:05: CSM_PROC_NEAR_END_DISCONNECT: CSM_EVENT_ISDN_DISCONNECTED, call id = 0x8005,
port = 1
```

Call Scenario 3

In this call scenario, port 1 is on-hook, the application dial is set to call 4086661112, the far end successfully connects, and the command **test pots disconnect** terminates the call.

```
router# debug pots csm
router# test pots 1 dial 4086661112
router#
```

The following screen output follows the same sequence of events as shown in Call Scenario 1:

```
1d03h: CSM_PROC_IDLE: CSM_EVENT_VDEV_APPLICATION_CALL, call id = 0x0, port = 1
1d03h: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
1d03h: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
1d03h: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
1d03h: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
1d03h: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
1d03h: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
1d03h: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
1d03h: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
1d03h: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1
1d03h: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_DIGIT, call id = 0x0, port = 1

1d03h: CSM_PROC_APPLIC_DIALING: CSM_EVENT_VDEV_OFFHOOK, call id = 0x0, port = 1

1d03h: EVENT_FROM_ISDN:dchan_idb=0x2821F38, call_id=0x8039, ces=0x1
   bchan=0x0, event=0x3, cause=0x0
1d03h: CSM_PROC_ENBLOC_DIALING: CSM_EVENT_ISDN_PROC, call id = 0x8039, port = 1

1d03h: EVENT_FROM_ISDN:dchan_idb=0x2821F38, call_id=0x8039, ces=0x1
   bchan=0xFFFFFFFF, event=0x5, cause=0x0

1d03h: CSM_PROC_ENBLOC_DIALING: CSM_EVENT_ISDN_CALL_PROGRESSING, call id = 0x8039,
    port = 1

router# test pots 1 disconnect
```

The **test pots disconnect** command disconnects the call before you have to put the telephone back on hook.

```
1d03h: CSM_PROC_CONNECTING: CSM_EVENT_VDEV_APPLICATION_HANGUP_CALL, call id = 0x8039,
     port = 1
1d03h: EVENT_FROM_ISDN:dchan_idb=0x2821F38, call_id=0x8039, ces=0x1
   bchan=0xFFFFFFFF, event=0x0, cause=0x0

1d03h: CSM_PROC_DISCONNECTING: CSM_EVENT_ISDN_DISCONNECTED, call id = 0x8039,
    port = 1
1d03h: CSM_PROC_DISCONNECTING: CSM_EVENT_TIMEOUT, call id = 0x8039, port = 1
```

Restricting Access to Your Network

In Chapter 4, “Configuring Advanced Networks,” in the *Cisco 800 Series Routers Software Configuration Guide*, the configuration example for preventing IP spoofing in the “Restricting Access to Your Network” section is incorrect.

The correct configuration example shown in step 6 (on page 4-36) should be:

```
router(config)# access-list 100 deny ip 192.168.1.0 0.0.0.255 any
```

TACACS+ with AAA

Cisco 800 series routers now support the Terminal Access Controller Access Control System Plus (TACACS+) protocol through Telnet. TACACS+ is a Cisco proprietary authentication protocol that provides remote access authentication and related network security services, such as event logging. User passwords are administered in a central database, rather than in individual routers. TACACS+ also supports separate modular authentication, authorization, and accounting (AAA) facilities that are configured at individual routers.

For information on how to configure TACACS+, refer to the "Configuring TACACS+" chapter in the *Security Configuration Guide*. For information on TACACS+ commands, refer to the "TACACS, Extended TACACS, and TACACS+ Commands" chapter in the *Security Command Reference*.

Cisco 800 series routers do not support the following protocols:

- TACACS, an older access protocol now deprecated by Cisco, nor Extended TACACS, an extension to the TACACS protocol
- RADIUS or Kerberos protocols

PPP over Frame Relay Support (RFC-1973)

Cisco 800 series routers do not support PPP protocol over Frame Relay.

CiscoView Application Support

The CiscoView application supports the Cisco 800 series routers. The CiscoView application provides dynamic status, statistics, and comprehensive configuration information for Cisco switches, routers, concentrators, and adapters. It displays a graphical view of Cisco devices. This network management tool also provides configuring and monitoring functions and offers basic troubleshooting tips.

ROM Monitor set stop-bits Parameter

This release supports only the setting of 1 for the ROM monitor **set stop-bits** parameter. The display in the "Configuring Basic Configuration Parameters" section in Appendix D, "ROM Monitor," of the *Cisco 800 Series Routers Software Configuration Guide* incorrectly implies that you can set the console port stop bits to 1 or 2.

Obtaining Documentation

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly. Therefore, it is probably more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Registered CCO users can order the Documentation CD-ROM and other Cisco Product documentation through our online Subscription Services at http://www.cisco.com/cgi-bin/subcat/kaojump.cgi.

Nonregistered CCO users can order documentation through a local account representative by calling Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

Obtaining Technical Assistance

Cisco provides Cisco Connection Online (CCO) as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center. All customers can submit technical feedback on Cisco documentation using the Web, e-mail, a self-addressed stamped response card included in many printed docs, or by sending mail to Cisco.

Cisco Connection Online

Cisco continues to revolutionize how business is done on the Internet. Cisco Connection Online is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

CCO's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through CCO, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on CCO to obtain additional personalized information and services. Registered users may order products, check on the status of an order and view benefits specific to their relationships with Cisco.

You can access CCO in the following ways:

- WWW: www.cisco.com
- Telnet: cco.cisco.com
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
  - From North America, call 408 526-8070
  - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using CCO to cco-team@cisco.com.

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.

To display the TAC Web site that includes links to technical support information and software upgrades and for requesting TAC support, use www.cisco.com/techsupport.

To contact by e-mail, use one of the following:

Language	E-mail Address
English	tac@cisco.com
Hanzi (Chinese)	chinese-tac@cisco.com
Kanji (Japanese)	japan-tac@cisco.com
Hangul (Korean)	korea-tac@cisco.com
Spanish	tac@cisco.com
Thai	thai-tac@cisco.com

In North America, TAC can be reached at 800 553-2447 or 408 526-7209. For other telephone numbers and TAC e-mail addresses worldwide, consult the following Web site: http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml.

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate and value your comments.

This document is to be used with the following documents: *Cisco 800 Series Routers Software Configuration Guide, Cisco 800 Series Routers Hardware Installation Guide, Quick Start Guide: Setting Up Cisco 800 Series Routers, Cisco 811 and Cisco 813 Routers Hardware Installation Guide,* and *Quick Start Guide: Setting Up Cisco 811 and Cisco 813 Routers*.