Configuring ISDN Special Signaling

This chapter describes features that either depend on special signaling services offered by an ISDN network service provider or overcome an inability to deliver certain signals. It describes these features in the following main sections:

- How to Configure ISDN Special Signaling
- Troubleshooting ISDN Special Signaling
- Configuration Examples for ISDN Special Signaling

For an overview of ISDN PRI, see the section "ISDN Service" in the "Overview of Dial Interfaces, Controllers, and Lines" chapter, and the section "ISDN Overview" in the *Configuring ISDN BRI* chapter.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the "Identifying Supported Platforms" section in the "Using Cisco IOS Software" chapter.

For a complete description of the ISDN signaling commands in this chapter, refer to the *Cisco IOS Dial Technologies Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

How to Configure ISDN Special Signaling

To configure special signaling features of ISDN, perform the tasks in the following sections; all tasks are optional:

- Configuring ISDN AOC (Optional)
- Configuring NFAS on PRI Groups (Optional)
- Enabling an ISDN PRI to Take PIAFS Calls on MICA Modems (Optional)
- Configuring Automatic Detection of Encapsulation Type (Optional)
- Configuring Encapsulation for Combinet Compatibility (Optional)

See the section "Configuration Examples for ISDN Special Signaling" at the end of this chapter for examples of these signaling features. See the "Troubleshooting ISDN Special Signaling" section later in this chapter for help in troubleshooting ISDN signaling features.

Configuring ISDN AOC

ISDN Advice of Charge (AOC) allows users to obtain charging information for all calls during the call (AOC-D) or at the end of the call (AOC-E) or both.

Users must have subscribed through their local ISDN network to receive the AOC information from the switch. No router configuration changes are required to retrieve this call charging information.

The ISDN AOC feature also supports, for the AOC-D service, an optional configurable short-hold mode that provides a dynamic idle timeout by measuring the call charging period, based on the frequency of the AOC-D or the AOC-E message from the network. The short-hold mode allows users to track call costs and to control and possibly reduce tariff charges. The short-hold mode idle time will do the following:

- Disconnect a call just before the beginning of a new charging period if the call has been idle for at least the configured minimum idle time.
- Maintain the call to the end of the current charging period past the configured idle timeout if the time left in the charging period is longer.

Incoming calls are disconnected using the static dialer idle timeout value.

The AOC-D and AOC-E messages are part of the Facility Information Element (IE) message. Its contents can be verified with the **debug q931** command. Call accounting information from AOC-D and AOC-E messages is stored in Simple Network Management Protocol (SNMP) MIB objects.

ISDN AOC is provided for ISDN PRI NET5 and ISDN BRI NET3 switch types only. AOC information at call setup is not supported.

Configuring Short-Hold Mode

No configuration is required to enable ISDN AOC. However, you can configure the optional short-hold minimum idle timeout period for outgoing calls; the default minimum idle timeout is 120 seconds. If the short-hold option is not configured, the router default is to use the static dialer idle timeout. If the short-hold idle timeout has been configured but no charging information is available from the network, the static dialer idle timeout applies.

To configure an ISDN interface and provide the AOC short-hold mode option on an ISDN interface, perform the following steps:

Step 1 Configure the ISDN BRI or PRI interface, as described in the chapter *Configuring ISDN BRI* or the section "How to Configure ISDN PRI" in the chapter "Configuring ISDN PRI" later in this publication, using the relevant keyword in the **isdn switch-type** command:

- BRI interface—**basic-net3**
- PRI interface—**primary-net5**

Step 2 Configure dialer profiles or legacy dial-on-demand routing (DDR) for outgoing calls, as described in the chapters in the "Dial-on-Demand Routing" part of this publication, making sure to do the following:

- Configure the static line-idle timeout to be used for incoming calls.
- For each destination, use the **dialer map** command with the **class** keyword (legacy DDR) or a **dialer string class** command (dialer profiles) to identify the dialer map class to be used for outgoing calls to the destination.

Step 3 Configure each specified dialer map class, providing a dialer idle timeout, or ISDN short-hold timeout, or both for outgoing calls, as described in this chapter.

To configure a dialer map class with timers, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# **map-class dialer** *classname*	Specifies the dialer map class and begins map class configuration mode.
Step 2	`Router(config-map-class)#` **dialer idle-timeout** *seconds*	(Optional) Specifies a static idle timeout for the map class to override the static line-idle timeout configured on the BRI interface.
Step 3	`Router(config-map-class)#` **dialer isdn short-hold** *seconds*	Specifies a dialer ISDN short-hold timeout for the map class.

Monitoring ISDN AOC Call Information

To monitor ISDN AOC call information, use the following command in EXEC mode:

Command	Purpose
`Router>` **show isdn** {**active** [**dsl** | **serial-number**] | **history** [**dsl** | **serial-number**] | **memory** | **nfas group** *group-number* | **service** [**dsl** | **serial-number**] | **status** [**dsl** | **serial-number**] | **timers** [**dsl** | **serial-number**]}	Displays information about active calls, call history, memory, nfas group, service or status of PRI channels, or Layer 2 or Layer 3 timers. The **history** keyword displays AOC charging time units used during the call and indicates whether the AOC information is provided during calls or at the end of calls. (The **service** keyword is available for PRI only.)

Configuring NFAS on PRI Groups

ISDN Non-Facility Associated Signaling (NFAS) allows a single D channel to control multiple PRI interfaces. A backup D channel can also be configured for use when the primary NFAS D channel fails.

Use of a single D channel to control multiple PRI interfaces can free one B channel on each interface to carry other traffic.

Any hard failure causes a switchover to the backup D channel and currently connected calls remain connected.

Once the channelized T1 controllers are configured for ISDN PRI, only the NFAS primary D channel must be configured; its configuration is distributed to all the members of the associated NFAS group.

ISDN NFAS Prerequisites

NFAS is only supported with a channelized T1 controller. Table 1 shows the Cisco IOS keywords for the ISDN switch types and lists whether NFAS is supported.

Table 1 ISDN Switch Types and NFAS Support

Switch Type	Keyword	NFAS Support
Lucent 4ESS Custom NFAS	**primary-4ess**	Yes
Lucent 5ESS Custom NFAS	**primary-5ess**	No (use National)
Nortel DMS Custom NFAS	**primary-dms**	Yes
NTT Custom NFAS	**primary-ntt**	Yes
National	**primary-ni**	Yes
Other switch types	—	No (use National)

Note On the Nortel (Northern Telecom) DMS-100 switch, when a single D channel is shared, multiple PRI interfaces may be configured in a single trunk group. The additional use of alternate route indexing, which is a feature of the DMS-100 switch, provides a rotary from one trunk group to another. This feature enables the capability of building large trunk groups in a public switched network.

The ISDN switch must be provisioned for NFAS. The primary and backup D channels should be configured on separate T1 controllers. The primary, backup, and B-channel members on the respective controllers should be the same as that configured on the router and ISDN switch. The interface ID assigned to the controllers must match that of the ISDN switch.

ISDN NFAS Configuration Task List

To configure NFAS on channelized T1 controllers configured for ISDN, perform the tasks in the following section: Configuring NFAS on PRI Groups (required).

You can also disable a channel or interface, if necessary, and monitor NFAS groups and ISDN service. To do so, perform the tasks in the following sections:

- Configuring NTT PRI NFAS (Optional)
- Disabling a Channel or Interface (Optional)
- Monitoring NFAS Groups (Optional)
- Monitoring ISDN Service (Optional)

See the section "NFAS Primary and Backup D Channels" later in this chapter for ISDN, NFAS, and DDR configuration examples.

Configuring NFAS on PRI Groups

This section documents tasks used to configure NFAS with D channel backup. When configuring NFAS, you use an extended version of the ISDN **pri-group** command to specify the following values for the associated channelized T1 controllers configured for ISDN:

- The range of PRI time slots to be under the control of the D channel (time slot 24).

- The function to be performed by time slot 24 (primary D channel, backup, or none); the latter specifies its use as a B channel.
- The group identifier number for the interface under control of the D channel.

To configure ISDN NFAS, use the following commands in controller configuration mode:

	Command	Purpose
Step 1	`Router(config-controller)# pri-group timeslots 1-24 nfas_d primary nfas_interface` *number* `nfas_group` *number*	On one channelized T1 controller, configures the NFAS primary D channel.
Step 2	`Router(config-controller)# pri-group timeslots 1-24 nfas_d backup nfas_interface` *number* `nfas_group` *number*	On a different channelized T1 controller, configures the NFAS backup D channel to be used if the primary D channel fails.
Step 3	`Router(config-controller)# pri-group timeslots 1-24 nfas_d none nfas_interface` *number* `nfas_group` *number*	(Optional) On other channelized T1 controllers, configures a 24-B-channel interface, if desired.

For an example of configuring three T1 controllers for the NFAS primary D channel, the backup D channel, and 24 B channels, along with the DDR configuration for the PRI interface, see the section "NFAS Primary and Backup D Channels" at the end of this chapter.

When a backup NFAS D channel is configured and the primary NFAS D channel fails, rollover to the backup D channel is automatic and all connected calls stay connected.

If the primary NFAS D channel recovers, the backup NFAS D channel remains active and does not switch over again unless the backup NFAS D channel fails.

Configuring NTT PRI NFAS

Addition of the NTT switch type to the NFAS feature allows its use in geographic areas where NTT switches are available. This feature provides use of a single D channel to control multiple PRI interfaces, and can free one B channel on each interface to carry other traffic.

To configure NTT PRI NFAS, use the procedure described in the "Configuring NFAS on PRI Groups" section. Specify a **primary-ntt** switch type.

Note You cannot configure a backup D channel for the NTT PRI NFAS feature; it does not support D channel backup.

Verifying NTT PRI NFAS

Step 1 Enter the **show isdn status** command to learn whether the ISDN PRI switch type was configured correctly:

```
Router# show isdn status serial 0:23

Global ISDN Switchtype = primary-ntt
ISDN Serial0:23 interface
```

Step 2 Enter the **show isdn nfas group** command to display information about members of an NFAS group:

```
Router# show isdn nfas group 1

ISDN NFAS GROUP 1 ENTRIES:
```

```
The primary D is Serial1/0:23.
The NFAS member is Serial2/0:23.

There are 3 total nfas members.
There are 93 total available B channels.
The primary D-channel is DSL 0 in state INITIALIZED.
The current active layer 2 DSL is 0.
```

Step 3 Enter the **show isdn service** command to display information about ISDN channels and the service states:

```
Router# show isdn service

PRI Channel Statistics:

ISDN Se1/0:23, Channel (1-24)
  Configured Isdn Interface (dsl) 0
  State (0=Idle 1=Propose 2=Busy 3=Reserved 4=Restart 5=Maint)
  0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 3
  Channel (1-24) Service (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 0 0

ISDN Se1/1:23, Channel (1-24)
  Configured Isdn Interface (dsl) 1
  State (0=Idle 1=Propose 2=Busy 3=Reserved 4=Restart 5=Maint)
  0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
  Channel (1-24) Service (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 0 0

ISDN Se2/0:23, Channel (1-24)
  Configured Isdn Interface (dsl) 2
  State (0=Idle 1=Propose 2=Busy 3=Reserved 4=Restart 5=Maint)
  0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
  Channel (1-24) Service (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 0 0
```

Disabling a Channel or Interface

You can disable a specified channel or an entire PRI interface, thus taking it out of service or placing it into one of the other states that is passed in to the switch. To disable a specific channel or PRI interface, use one of the following commands in interface configuration mode as appropriate for your network:

Command	Purpose
`Router(config-if)# isdn service dsl` *number* `b_channel` *number* `state` *state-value*	Takes an individual B channel out of service or sets it to a different state.
`Router(config-if)# isdn service dsl` *number* `b_channel 0 state` *state-value*	Sets the entire PRI to the specified state.

The supported *state-values* are as follows:

- 0—In service
- 1—Maintenance
- 2—Out of service

When the T1 Controller Is Shut Down

In the event that a controller belonging to an NFAS group is shut down, all active B-channel calls on the controller that is shut down will be cleared (regardless of whether the controller is set to be primary, backup, or none), and one of the following events will occur:

- If the controller that is shut down is configured as the primary and no backup is configured, all active calls on the group are cleared.
- If the controller that is shut down is configured as the primary, and the active (In service) D channel is the primary and a backup is configured, then the active D channel changes to the backup controller.
- If the controller that is shut down is configured as the primary, and the active D channel is the backup, then the active D channel remains as backup controller.
- If the controller that is shut down is configured as the backup, and the active D channel is the backup, then the active D channel changes to the primary controller.

Note The active D channel changeover between primary and backup controllers happens only when one of the link fails and not when the link comes up. The T309 timer is triggered when the changeover takes place.

Monitoring NFAS Groups

To monitor NFAS groups, use the following command in EXEC mode:

Command	Purpose
`Router> show isdn nfas group number`	Displays information about members of an NFAS group.

Monitoring ISDN Service

To display information about ISDN channel service states, use the following command in EXEC mode:

Command	Purpose
`Router> show isdn service`	Displays information about ISDN channels and the service states.

Enabling an ISDN PRI to Take PIAFS Calls on MICA Modems

The Personal-Handyphone-System Internet Access Forum Standard (PIAFS) specifications describe a transmission system that uses the PHS 64000 bps/32000 bps unrestricted digital bearer on the Cisco AS5300 universal access server platform.

The PIAFS TA (terminal adapter) module is like a modem or a V.110 module in the following ways:

- Ports will be a pool of resources.
- Calls will use the same call setup Q.931 message.
- Module supports a subset of common AT commands.
- Call setup and teardown are similar.

However, the rate negotiation information will be part of the bearer cap and not the lower-layer compatibility. PIAFS calls will have the user rate as 32000 and 64000; this will be used to distinguish a PIAFS call from a V.110 call. Also, PIAFS will use only up to octets 5a in a call setup message. The data format will default to 8N1 for PIAFS calls.

To configure ISDN PRI to take PIAFS call on MICA modems, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface serial` *controller:channel*	Enters interface configuration mode for a D-channel serial interface.
Step 2	`Router(config-if)# isdn piafs-enabled`	Enables the PRI to take PIAFS calls on MICA modems.
Step 3	`Router(config-if)# exit`	Exits interface configuration mode.

Verifying PIAFS

Step 1 Enter the **show modem operational-status** *slot/port* command to view PIAFS call information.

```
Router# show modem op 1/32

Mdm Typ Status Tx/Rx G Duration RTS CTS DCD DTR
1/32 ISDN Conn 64000/64000 0 1d01h x x x x

Modem 1/32, Mica Hex Modem (Managed), Async33, tty33
Firmware Rev: 8.2.0.c
Modem config: Incoming and Outgoing
→ Protocol: PIAFS, Compression: V.42bis both

Management config: Status polling
RX signals: 0 dBm

Last clearing of "show modem" counters never
2 incoming completes, 0 incoming failures
0 outgoing completes, 0 outgoing failures
0 failed dial attempts, 0 ring no answers, 0 busied outs
0 no dial tones, 0 dial timeouts, 0 watchdog timeouts
0 no carriers, 0 link failures, 0 resets, 0 recover oob
0 recover modem, 0 current fail count
0 protocol timeouts, 0 protocol errors, 0 lost events
0 ready poll timeouts
```

Configuring Automatic Detection of Encapsulation Type

You can enable a serial or ISDN interface to accept calls and dynamically change the encapsulation in effect on the interface when the remote device does not signal the call type. For example, if an ISDN call does not identify the call type in the lower-layer compatibility fields and is using an encapsulation that is different from the one configured on the interface, the interface can change its encapsulation type dynamically.

This feature enables interoperation with ISDN terminal adapters that use V.120 encapsulation but do not signal V.120 in the call setup message. An ISDN interface that by default answers a call as synchronous serial with PPP encapsulation can change its encapsulation and answer such calls.

Automatic detection is attempted for the first 10 seconds after the link is established or the first 5 packets exchanged over the link, whichever is first.

To enable automatic detection of encapsulation type, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# autodetect encapsulation` *encapsulation-type*	Enables automatic detection of encapsulation type on the specified interface.

You can specify one or more encapsulations to detect. Cisco IOS software currently supports automatic detection of PPP and V.120 encapsulations.

Configuring Encapsulation for Combinet Compatibility

Historically, Combinet devices supported only the Combinet Proprietary Protocol (CPP) for negotiating connections over ISDN B channels. To enable Cisco routers to communicate with those Combinet bridges, the Cisco IOS supports a the CPP encapsulation type.

To enable routers to communicate over ISDN interfaces with Combinet bridges that support only CPP, use the following commands in interface configuration mode:

	Command	Purpose
Step 1	`Router(config-if)# encapsulation cpp`	Specifies CPP encapsulation.
Step 2	`Router(config-if)# cpp callback accept`	Enables CPP callback acceptance.
Step 3	`Router(config-if)# cpp authentication`	Enables CPP authentication.

Most Combinet devices support PPP. Cisco routers can communicate over ISDN with these devices by using PPP encapsulation, which supports both routing and fast switching.

Cisco 700 and 800 series routers and bridges (formerly Combinet devices) support only IP, Internet Protocol Exchange (IPX), and bridging. For AppleTalk, Cisco routers automatically perform half-bridging with Combinet devices. For more information about half-bridging, see the section "Configuring PPP Half-Bridging" in the chapter "Configuring Media-Independent PPP and Multilink PPP" later in this publication.

Cisco routers can also half-bridge IP and IPX with Combinet devices that support only CPP. To configure this feature, you only need to set up the addressing with the ISDN interface as part of the remote subnet; no additional commands are required.

Troubleshooting ISDN Special Signaling

To troubleshoot ISDN, use the following commands in EXEC mode as needed:

Command	Purpose
`Router# debug dialer`	Displays the values of timers.

`Router# debug isdn q921 [interface bri number]`
 	
or
 	
`Router# debug isdn q921 interface serial slot/controller-number:23`
	Displays link layer information for all interfaces or, optionally, for a single BRI interface.
	
	Displays link layer information for a single PRI interface.

`Router# debug isdn q931 [interface bri number]`
 	
or
 	
`Router# debug isdn q931 interface serial slot/controller-number:23`
	Displays the content of call control messages and information elements, in particular the Facility IE message for all interfaces or, optionally, for a single BRI interface.
	
	Displays the content of call control messages and information elements, in particular the Facility IE message for a single PRI interface.

Configuration Examples for ISDN Special Signaling

This section provides the following configuration examples:

- ISDN AOC Configuration Examples
- ISDN NFAS Configuration Examples

ISDN AOC Configuration Examples

This section provides the following ISDN AOC configuration examples:

- Using Legacy DDR for ISDN PRI AOC Configuration
- Using Dialer Profiles for ISDN BRI AOC Configuration

Using Legacy DDR for ISDN PRI AOC Configuration

This example shows ISDN PRI configured on an E1 controller. Legacy DDR is configured on the ISDN D channel (serial interface 0:15) and propagates to all ISDN B channels. A static dialer idle-timeout is configured for all incoming calls on the B channels, but the map classes are configured independently of it. Map classes Kappa and Beta use AOC charging unit duration to calculate the timeout for the call. A short-hold idle timer is set so that if the line is idle for 10 or more seconds, the call is disconnected when the current charging period ends. Map class Iota uses a static idle timeout.

```
version 11.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname A
!
username c2503isdn password 7 1511021F0725
username B password 7 110A1016141D29
username C password 7 1511021F072508
isdn switch-type primary-net5
!
controller E1 0
```

```
 pri-group timeslots 1-31
!
interface Serial 0:15
 ip address 10.0.0.35 255.0.0.0
 encapsulation ppp
 dialer idle-timeout 150
 dialer map ip 10.0.0.33 name c2503isdn class Iota 06966600050
 dialer map ip 10.0.0.40 name B class Beta 778578
 dialer map ip 10.0.0.45 name C class Kappa 778579
 dialer-group 1
 ppp authentication chap
!
map-class dialer Kappa
 dialer idle-timeout 300
 dialer isdn short-hold 120
!
map-class dialer Iota
 dialer idle-timeout 300
!
map-class dialer Beta
 dialer idle-timeout 300
 dialer isdn short-hold 90
!
dialer-list 1 protocol ip permit
```

Using Dialer Profiles for ISDN BRI AOC Configuration

This example shows ISDN BRI configured as a member of two dialer pools for dialer profiles.

```
version 11.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname delorean
!
username spanky password 7 0705344245
username delorean password 7 1511021F0725
isdn switch-type basic-net3
!
interface BRI0
 description Connected to NTT 81012345678901
 no ip address
 dialer pool-member 1 max-link 1
 dialer pool-member 2 max-link
 encapsulation ppp
 no fair-queue
!
interface Dialer1
 ip address 10.1.1.8 255.255.255.0
 encapsulation ppp
 dialer remote-name spanky
 dialer string 81012345678902 class Omega
 dialer pool 1
 dialer-group 1
 ppp authentication chap
!
interface Dialer2
 ip address 10.1.1.8 255.255.255.0
 encapsulation ppp
 dialer remote-name dmsisdn
 dialer string 81012345678902 class Omega
 dialer string 14153909503 class Gamma
 dialer pool 2
```

```
 dialer-group 1
 ppp authentication chap
!
map-class dialer Omega
 dialer idle-timeout 60
 dialer isdn short-hold 150
!
map-class dialer Gamma
 dialer isdn short-hold 60
!
dialer-list 1 protocol ip permit
```

ISDN NFAS Configuration Examples

This section provides the following configuration examples:

- NFAS Primary and Backup D Channels
- PRI Interface Service State
- NTT PRI NFAS Primary D Channel Example

NFAS Primary and Backup D Channels

The following example configures ISDN PRI and NFAS on three T1 controllers of a Cisco 7500 series router. The NFAS primary D channel is configured on the 1/0 controller, and the NFAS backup D channel is configured on the 1/1 controller. No NFAS D channel is configured on the 2/0 controller; it is configured for 24 B channels. Once the NFAS primary D channel is configured, it is the only interface you see and need to configure; DDR configuration for the primary D channel—which is distributed to all B channels—is also included in this example.

```
isdn switch-type primary-4ess
!
! NFAS primary D channel on the channelized T1 controller in 1/0.
controller t1 1/0
 framing esf
linecode b8zs
 pri-group timeslots 1-24 nfas_d primary nfas_interface 0 nfas_group 1
!
! NFAS backup D channel on the channelized T1 controller in 1/1.
controller t1 1/1
 framing esf
linecode b8zs
 pri-group timeslots 1-24 nfas_d backup nfas_interface 1 nfas_group 1
!
! NFAS 24 B channels on the channelized T1 controller in 2/0.
controller t1 2/0
 framing esf
linecode b8zs
 pri-group timeslots 1-24 nfas_d none nfas_interface 2 nfas_group 1
!
! NFAS primary D channel interface configuration for PPP and DDR. This
! configuration is distributed to all the B channels in NFAS group 1 on the
! three channelized T1 controllers.
!
interface Serial 1/0:23
 ip address 10.1.1.2 255.255.255.0
 no ip mroute-cache
 encapsulation ppp
 dialer map ip 10.1.1.1 name flyboy 567898
```

```
 dialer map ip 10.1.1.3 name flyboy 101112345678
 dialer map ip 10.1.1.4 name flyboy 01112345678
 dialer-group 1
 no fair-queue
 no cdp enable
 ppp authentication chap
```

PRI Interface Service State

The following example puts the entire PRI interface back in service after it previously had been taken out of service:

```
isdn service dsl 0 b-channel 0 state 0
```

NTT PRI NFAS Primary D Channel Example

The following example configures ISDN PRI and NFAS on three T1 controllers of a Cisco 7500 series router. The NFAS primary D channel is configured on the 1/0 controller. No NFAS D channel is configured on the 1/1 and 2/0 controllers; they are configured for 24 B channels. Once the NFAS primary D channel is configured, it is the only interface you see and need to configure. DDR configuration for the primary D channel—which is distributed to all B channels—is also included in this example.

```
isdn switch-type primary-ntt
!
! NFAS primary D channel on the channelized T1 controller in 1/0.
controller t1 1/0
 framing esf
linecode b8zs
 pri-group timeslots 1-24 nfas_d primary nfas_interface 0 nfas_group 1
!
! NFAS backup D channel on the channelized T1 controller in 1/1.
controller t1 1/1
 framing esf
linecode b8zs
 pri-group timeslots 1-24 nfas_d none nfas_interface 1 nfas_group 1
!
! NFAS 24 B channels on the channelized T1 controller in 2/0.
controller t1 2/0
 framing esf
linecode b8zs
 pri-group timeslots 1-24 nfas_d none nfas_interface 2 nfas_group 1
!
! NFAS primary D channel interface configuration for PPP and DDR. This
! configuration is distributed to all the B channels in NFAS group 1 on the
! three channelized T1 controllers.
!
interface Serial 1/0:23
 ip address 10.1.1.2 255.255.255.0
 no ip mroute-cache
 encapsulation ppp
 dialer map ip 10.1.1.1 name flyboy 567898
 dialer map ip 10.1.1.3 name flyboy 101112345678
 dialer map ip 10.1.1.4 name flyboy 01112345678
 dialer-group 1
 no fair-queue
 no cdp enable
 ppp authentication chap
```