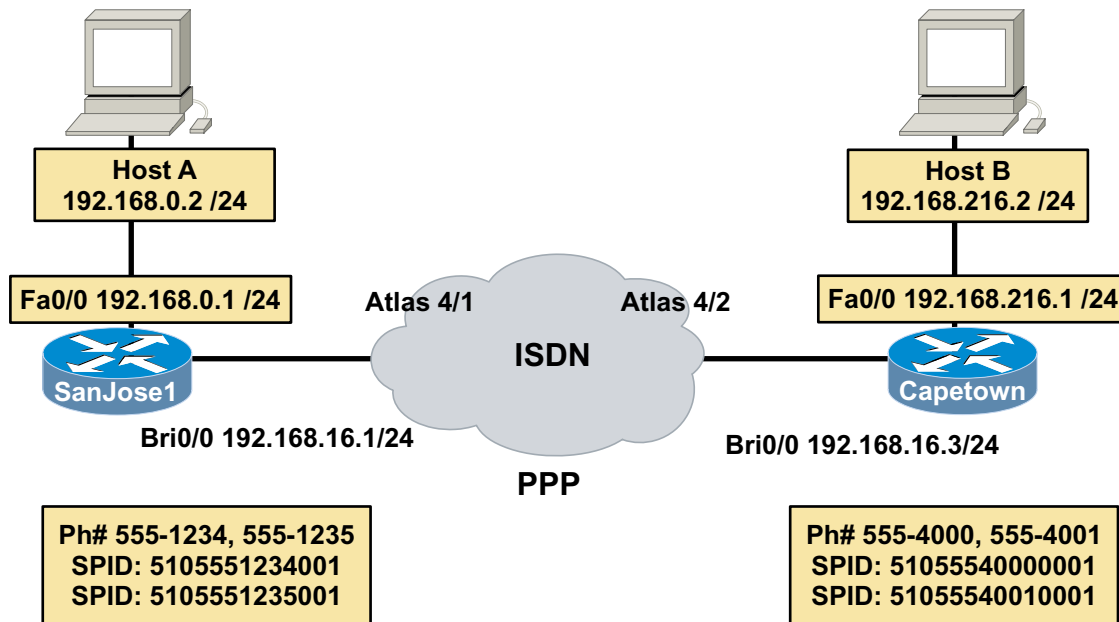


## 4.9.1: Configuring ISDN BRI



### Objective

In this lab, you will configure two Cisco routers for DDR using ISDN BRI.

### Scenario

The International Travel Agency wants you to configure an ISDN DDR connection between a remote office, Capetown, and its corporate network core router, SanJose1. They have asked that you configure PPP encapsulation and CHAP authentication over this link. You have been asked to configure DDR so that only the following mission-critical applications qualify as interesting traffic: web, DNS, FTP, Telnet, and mail.

### Step 1

Before beginning this lab, it is recommended that you reload the routers after erasing their startup configuration. This will prevent you from having problems caused by residual configurations. Build and configure the network according to the above diagram, but do not configure either router's BRI interfaces yet. Use the Adtran Atlas 550 or similar device to simulate the ISDN cloud. If you are using the Atlas 550, be sure to use straight-through cables and connect both routers to the respective BRI module ports of the Atlas 550 as labeled in the diagram. Be sure to configure both workstations with the correct IP address and default gateway (i.e., router Fa0/0 IP address). You should also read Appendix B before proceeding with Step 2.

### Step 2

Configure SanJose1 to use the appropriate ISDN switch type. Your ISP will provide you with this information and in this case, the International Travel Agency has been told their provider is using the National switch type. Enter the following command:

```
SanJose1(config)#isdn switch-type basic-ni
```

Since you will be using PPP encapsulation and CHAP on the B channels, enter username and password information for the remote router and an enable password for SanJose1. SanJose1 will use the enable password when responding to CHAP challenges.

```
SanJose1(config)#username Capetown password cisco
SanJose1(config)#enable password cisco
SanJose1(config)#line vty 0 4
SanJose1(config-line)#password cisco
SanJose1(config-line)#exit
```

**Note:** you could use the `enable secret password` here, but for the purposes of this lab, an `enable password` is all that is needed. The virtual terminal configuration is necessary because you will Telnet to SanJose1 in Step 7.

Next, set up a dialer list to use with DDR. This dialer list will be used to identify interesting traffic, that is, traffic for which the ISDN link should be established. The International Travel Agency wants you to restrict what constitutes “interesting” traffic, but for now, use the following command:

```
SanJose1(config)#dialer-list 1 protocol ip permit
```

This permissive command will establish the link for *any* IP traffic that needs to be routed out the BRI interface. In Step 7, you will reconfigure this dialer list to fulfill the client's requirements completely.

### Step 3

Configure the BRI on SanJose1.

```
SanJose1(config)#interface bri0/0
SanJose1(config-if)#ip address 192.168.16.1 255.255.255.0
SanJose1(config-if)#encapsulation ppp
SanJose1(config-if)#ppp authentication chap
SanJose1(config-if)#dialer-group 1
```

The `dialer-group 1` command associates this interface with dialer list 1. In order for this BRI to establish a connection with the ISP's ISDN switch, you must configure at least one SPID (service profile identifier). With two B channels, you will configure two SPIDs. Enter the following commands on SanJose1:

```
SanJose1(config-if)#isdn spid1 51055512340001 5551234
SanJose1(config-if)#isdn spid2 51055512350001 5551235
SanJose1(config-if)#no shutdown
```

After the SPIDs and ISDN switch type are configured, the router will send the SPID to the switch. If you have made a configuration error, you may receive the following output:

```
%ISDN-4-INVALID_SPID: Interface BR0/0, Spid1 was rejected
```

If you don't receive an error, use the **show isdn status** command to verify that SanJose1 has established communication with the ISDN switch. A sample output is shown below.

```
SanJose1#show isdn status
Global ISDN Switchtype = basic-ni
ISDN BRI0/0 interface
    dsl 0, interface ISDN Switchtype = basic-ni
Layer 1 Status:
    ACTIVE
Layer 2 Status:
    TEI = 64, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    TEI = 65, Ces = 2, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
Spid Status:
    TEI 64, ces = 1, state = 8(established)
        spid1 configured, spid1 sent, spid1 valid
        Endpoint ID Info: epsf = 0, usid = 70, tid = 1
    TEI 65, ces = 2, state = 8(established)
        spid2 configured, spid2 sent, spid2 valid
        Endpoint ID Info: epsf = 0, usid = 70, tid = 2
Layer 3 Status:
    0 Active Layer 3 Call(s)
Activated dsl 0 CCBs = 0
The Free Channel Mask: 0x80000003
Total Allocated ISDN CCBs = 0
```

Note that the highlighted lines of the above output show that the Layer 2 state between the switch and the router is “established” and that SPID1 and SPID2 were accepted. If the SPID status is not established or, if you change your router's SPID configuration, issue the command below to force the router to resend the SPID to the switch. Executing the command once, on a production network should be sufficient. However, when using the Atlas 550, it may be necessary to repeat the command a second or third time (refer to Appendix B):

```
SanJose1#clear interface bri0/0
```

You may also use the **debug isdn q921** command to troubleshoot Layer 2 issues between the router and the ISDN switch. Once you have verified connectivity to the ISDN switch, issue the **show interface bri0/0** command, as shown:

```
SanJose1#show interface bri0/0
BRI0/0 is up, line protocol is up (spoofing)
Hardware is PQUICC BRI with U interface
Internet address is 10.1.1.1/24
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set
<output omitted>
```

The highlighted portion of the above output shows that the BRI0/0 interface is up and the line protocol is up (spoofing).

1. Since no ISDN call has been made yet, why do you think the BRI shows “up and up (spoofing)”?

---

Now issue the **show ip interface brief** command, as shown:

```
SanJose1#show ip interface brief
```

Interface Protocol	IP-Address	OK?	Method	Status	
FastEthernet0/0	192.168.0.1	YES	manual	up	up
Serial0/0	unassigned	YES	unset	down	down
BRI0/0	192.168.16.1	YES	manual	up	up
BRI0/0:1	unassigned	YES	unset	down	down
BRI0/0:2	unassigned	YES	unset	down	down
Serial0/1	unassigned	YES	unset	down	down

2. What do BRI0/0:1 and BRI0/0:2 refer to?

- 
3. Why is BRI0/0 up, and BRI0/0:1 down?

---

Issue the **show dialer** command. A sample output is shown below.

```
SanJose1#show dialer
```

```
BRI0/0 - dialer type = ISDN
```

```
Dial String      Successes  Failures   Last DNIS   Last status
0 incoming call(s) have been screened.
0 incoming call(s) rejected for callback.
```

```
BRI0/0:1 - dialer type = ISDN
```

```
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle
```

```
BRI0/0:2 - dialer type = ISDN
```

```
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle
```

4. What is the idle timer set to for both BRI0/0:1 and BRI0/0:2?

---

Because organizations are typically charged by the minute when making a DDR call, it is very important that you consider the dialer idle timeout. If the connection is idle, the router will wait for this configurable period of time to elapse before closing the connection. The

International Travel Agency would like you to set an aggressive idle timeout in order to reduce costs. Use the following command to change the timer:

```
SanJose1(config)#interface bri0/0
SanJose1(config-if)#dialer idle-timeout 60
```

Finally, you must configure a dialer map for this interface, as shown:

```
SanJose1(config-if)#dialer map ip 192.168.16.3 name Capetown 5554000
```

Notice that this **dialer map** command is similar to the dialer maps you created in previous labs, but since a modem is not used, no modem-script is required.

#### Step 4

We will now configure the Capetown router. The steps to accomplish this are basically the same as Steps 2 - 4. Therefore, complete the following:

```
Capetown(config)#isdn switch-type basic-ni
Capetown(config)#username SanJose1 password cisco
Capetown(config)#enable password cisco
Capetown(config)#line vty 0 4
Capetown(config-line)#password cisco
Capetown(config-line)#exit
Capetown(config)#dialer-list 1 protocol ip permit
Capetown(config)#interface bri0/0
Capetown(config-if)#ip address 192.168.16.3 255.255.255.0
Capetown(config-if)#encapsulation ppp
Capetown(config-if)#ppp authentication chap
Capetown(config-if)#dialer-group 1
Capetown(config-if)#isdn spid1 51055540000001 5554000
Capetown(config-if)#isdn spid2 51055540010001 5554001
Capetown(config-if)#dialer idle-timeout 60
Capetown(config-if)#dialer map ip 192.168.16.1 name SanJose1 5551234
Capetown(config-if)#no shutdown
```

Issue a **show isdn status** to check that the Layer 2 and see if the SPIDs have been accepted. If not, execute a **clear interface bri0/0** command until the SPIDs are accepted.

#### Step 5

Configure a static route to 192.168.216.0/24 on SanJose1. Set up a static default route on Capetown.

```
SanJose1(config)#ip route 192.168.216.0 255.255.255.0 192.168.16.3
Capetown(config)#ip route 0.0.0.0 0.0.0.0 192.168.16.1
```

## Step 6

Test your ISDN connection. Before you bring up the ISDN link, you should enable debugging on **both** routers. This will allow you to troubleshoot more efficiently in the event you encounter problems. Issue the following command to view dialer information on both routers:

```
SanJose1#debug dialer
```

You may also wish to debug ISDN with this command:

```
SanJose1#debug isdn events
```

Finally, because you are using PPP with CHAP authentication, you should also debug PPP:

```
SanJose1#debug ppp authentication
```

```
SanJose1#debug ppp negotiation
```

Now, **ping** Host A from Host B. There will be a number of debug outputs--including a dialer debug on Capetown, that should report the following:

```
00:56:00: BRI0/0 DDR: Dialing cause ip (s=192.168.216.2, d=192.168.0.2)
```

```
00:56:00: BRI0/0 DDR: Attempting to dial 5551234
```

Also, Capetown should report that channel B1 is now up:

```
00:56:01:%LINEPROTO-5-UPDOWN:Line protocol on Interface BRI0/0:1,changed state to up
```

```
00:56:06: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to 5551234 SanJose1
```

Troubleshoot this connection as necessary. Use the debug output for clues. You may have to use the **clear interface bri0/0** command several times on both routers to reset the interfaces.

**Note:** To manually disconnect an ISDN call on BRI0/0, use the following command:

```
SanJose1#isdn disconnect interface bri0/0 [all, b1, b2]
```

Continue testing your ISDN connection, **ping** Host A from Host B and vice versa. You can also issue the **show isdn history** command to view all active and prior ISDN connections. The **show isdn active** command will output information about the current active connection. Below are sample outputs of both commands.

SanJose1#**show isdn history**

```
-----
                                ISDN CALL HISTORY
-----
History table has a maximum of 100 entries.
History table data is retained for a maximum of 15 Minutes.
-----
```

Call Type	Calling Number	Called Number	Remote Name	Seconds Used	Seconds Left	Seconds Idle	Charges Units/Currency
In							
Out +ilable----		5551234	Capetown	60			
Out +ilable----		5551234	Capetown	40	19	40	

```
-----
```

Capetown#**show isdn active**

```
-----
                                ISDN ACTIVE CALLS
-----
History table has a maximum of 100 entries.
History table data is retained for a maximum of 15 Minutes.
-----
```

Call Type	Calling Number	Called Number	Remote Name	Seconds Used	Seconds Left	Seconds Idle	Charges Units/Currency
Out		5551234	SanJose1	18	44	15	0

```
-----
```

## Step 7

Now that you have a working ISDN connection, you will return to your router configurations to configure a more restrictive dialer list on the Capetown remote router. The International Travel Agency has asked that only the following mission-critical applications be designated as interesting traffic: web, DNS, FTP, Telnet and mail. To do this, you must reconfigure dialer list 1 on Capetown (the remote router). The central site router, SanJose1, will continue to be allowed to establish DDR connections for any IP traffic.

Create an access list on Capetown that will permit the mission critical services:

```
Capetown(config)#access-list 101 permit tcp any any eq www
Capetown(config)#access-list 101 permit udp any any eq domain
Capetown(config)#access-list 101 permit tcp any any eq ftp
Capetown(config)#access-list 101 permit tcp any any eq telnet
Capetown(config)#access-list 101 permit tcp any any eq pop3
```

```
Capetown(config)#access-list 101 permit tcp any any eq smtp
```

Now enter a new **dialer-list** command that references this access list. The new **dialer-list** command will automatically replace the old one:

```
Capetown(config)#dialer-list 1 protocol ip list 101
```

Once you have configured the new dialer list, ping Host A from Host B.

1. The **ping** should fail, why?

---

Now **Telnet** from Host B to SanJose1.

2. The **Telnet** request should bring up the ISDN connection, why?

---

With the connection still up, **ping** Host A from Host B once again.

3. Instead of failing as before, this **ping** should work. Why?

---

You should also be able to **ping** Host B from Host A.

While connected, issue the **show dialer** command on both SanJose1 and Capetown.

4. According to the output of this command, what was SanJose1's time until disconnect?

---