Troubleshooting IBM

This chapter focuses on connectivity and performance problems associated with bridging and routing in IBM-based networks.

The sections in this chapter describe specific IBM-related symptoms, the problems that are likely to cause each symptom, and the solutions to those problems.

- Local SRB: Host Cannot Connect to Server

- Local SRB: Routing Does Not Function

- RSRB: Host Cannot Connect to Server (Peers Not Open)

- RSRB: Host Cannot Connect to Server (Peers Open)

- RSRB: Periodic Communication Failures

- RSRB: NetBIOS Client Cannot Connect to Server

- Translational Bridging: Client Cannot Connect to Server

- SRT Bridging: Client Cannot Connect to Server

- SDLC: Router Cannot Communicate with SDLC Device

- SDLC: Intermittent Connectivity

- SDLC: Client Cannot Connect to Host over Router Running SDLLC

- SDLC: Sessions Fail over Router Running STUN

- CIP: CLAW Connection Does Not Come Up

- CIP: No Enabled LED On

- CIP: CIP Will Not Come Online to Host

- CIP: Router Cannot ping Host or Host Cannot ping Router

- CIP: Host Cannot Reach Remote Networks

- CIP: Host Running Routed Has No Routes

Local SRB: Host Cannot Connect to Server

Symptom: Connections fail over a router configured as a source-route bridge (SRB) connecting two or more Token Rings.

Table 8-1 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 8-1   **Local SRB: Host Cannot Connect to Server**

Possible Problem	Solution
Ring number mismatch	A router interface configured for bridging will fail to insert into a ring when it detects a ring number mismatch, and will post an error message to the console.
	Step 1 Get the ring number (specified in hexadecimal) from IBM SRBs (either by examining the configuration of other SRBs, or from the system administrator).
	Step 2 Use the **show running-config** privileged EXEC command to view the configuration of routers configured as SRBs. Look for **source-bridge** interface configuration command entries that assign ring numbers (displayed in decimal) to the rings that are connected to the router's interfaces.[1]
	For example, the following configuration entry shows the entry for local ring 10, bridge number 500, and remote ring 20:
	`source-bridge 10 500 20`
	Note: Parallel bridges situated between the same two rings must have different bridge numbers.
	Step 3 Convert IBM SRB ring numbers to decimal and verify that the ring numbers configured on all internetworking nodes agree.
	Step 4 If the ring numbers do not agree, reconfigure the router interface or IBM SRBs so that the ring numbers match.
End system does not support RIF	**Step 1** Place a network analyzer on the same ring to which the end system is connected.
	Step 2 Look for RIF frames sent from the end system (RIF frames have the high-order bit of the source MAC address set to 1).
	Step 3 If no RIF frames are found, the end system does not support RIF and cannot participate in source routing.
	If the protocol is routable, you can route the protocol or configure transparent bridging. If you do use transparent bridging, be careful not to create loops between the SRB and the transparent bridging domains.
	Step 4 If your environment requires SRB, contact your workstation or server vendor for SRB drivers or for information about setting up your workstation or server to support SRB.

Possible Problem	Solution
Hop count exceeded	Use the **show** *protocol* **route** command to check the hop count values on routers and bridges in the path. Packets that exceed the hop count are dropped.
	Alternatively, you can enable the **debug source event** privileged EXEC command to see whether packets are being dropped because the hop count has been exceeded.
	Increase the hop count if it is less than the default value of 7. Otherwise, the network must be redesigned so that no destination is greater than 7 hops away.
Router is not configured to forward spanning explorers	Spanning explorer packets are equivalent to a single-route broadcast. Routers must therefore be configured to route them.
	Step 1 Use the **show source-bridge** EXEC command to determine whether the spanning explorer count is incrementing.
	Step 2 If the spanning explorer count is not incrementing, use the **show running-config** privileged EXEC command on routers to see whether the **source-bridge spanning** interface configuration command is configured. This command configures the router to forward spanning explorers.
	Step 3 If the command entry is not present in the configuration, add it to any router that is required to pass spanning explorers.
	Step 4 Use the **show source-bridge** EXEC command to determine whether explorers are being sent.
	Step 5 If explorers are not being sent, place a network analyzer on the same ring to which the end system is connected.
	Step 6 If you find spanning all-ring frames, use the **show running-config** privileged EXEC command to make sure the router is properly configured. If sessions still cannot be established over the SRB, contact your technical support representative for more assistance.

1. Although you can enter the ring number in hexadecimal or decimal, it always appears in the configuration as a decimal number.

Local SRB: Routing Does Not Function

Symptom: Routed protocols are not forwarded properly by routers in a local SRB environment. SRBs bridge traffic normally.

Table 8-2 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 8-2 **Local SRB: Routing Does Not Function**

Possible Problem	Solution
Routing problem	For detailed information on troubleshooting routing problems, refer to the chapters in this publication that cover the routing protocols in question. For example, if you are running Novell IPX, see the chapter "Troubleshooting Novell IPX."
Missing **multiring** command	**Step 1** Use the **show running-config** privileged EXEC command on the router. Look for a **multiring** interface configuration command entry. This command enables the collection and use of RIF information on router interfaces.
	Step 2 If the **multiring** command is not present, add the command to the configuration using the following command: `C4000(config-if)#`**`multiring all`**
Incomplete ARP[1] table	**Step 1** Determine whether you can **ping** hosts.
	Step 2 If the host does not respond, use the **show arp** EXEC command to determine whether an entry for the host exists in the ARP table.
	Step 3 If an entry exists, there is probably a routing problem. Determine if you have a source-route path to the destination hardware (MAC) address. Use the **show rif** EXEC command to match the RIF with the hardware address of the host.
	Step 4 If no entry exists, use a network analyzer to see if ARP requests are getting through to the remote ring and to see if replies come back.

1. ARP=Address Resolution Protocol

RSRB: Host Cannot Connect to Server (Peers Not Open)

Symptom: Hosts cannot make connections to servers across a router configured as an RSRB. The output of the **show source-bridge** privileged EXEC command shows that SRB peers are not open.

Note If you succeed in getting peers to open but hosts are still unable to communicate with servers, refer to the section "RSRB: Host Cannot Connect to Server (Peers Open)," later in this chapter.

Table 8-3 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 8-3   RSRB: Host Cannot Connect to Server (Peers Not Open)

Possible Problem	Solution	
Missing or misconfigured **source-bridge remote-peer** command on the router	**Step 1**	Use the **show source-bridge** EXEC command to check for remote peers.
		If the output shows that peers are open, refer to the section "RSRB: Host Cannot Connect to Server (Peers Open)," later in this chapter.
	Step 2	If the output shows that peers are not open, use the **show running-config** privileged EXEC command to view the router configuration. Verify that there are two **source-bridge remote-peer** global configuration command entries present—one should point to the IP address of the local router and the other should point to the IP address of the remote router.
	Step 3	If either or both of the commands are missing or point to the wrong address, add or modify the commands as required.
		For detailed information about configuring routers for RSRB, see the Cisco IOS *Bridging and IBM Networking Configuration Guide* and *Bridging and IBM Networking Command Reference*.
No route to the remote peer	If you are using TCP or FST encapsulation between the local and remote SRB:	
	Step 1	Test IP connectivity using the extended **ping** privileged EXEC command. Use the local peer ID as the source address and the remote peer ID as the destination address.
	Step 2	If the ping fails, use the **show ip route** EXEC command to view the IP routing table.
	Step 3	If the **show ip route** output does not show a route to the intended remote peer, there is probably an IP routing problem or a problem with the hardware or cabling in the path from the local to the remote SRB.
		For information on troubleshooting IP routing, refer to the "Troubleshooting TCP/IP" chapter. For information about troubleshooting hardware problems, see the "Troubleshooting Hardware and Booting Problems" chapter.
Serial link problem	If there is a direct connection between the local and remote SRB (that is, you are not using FST or TCP encapsulation):	
	Step 1	Check to make sure that the next hop router is directly adjacent.
	Step 2	If it is adjacent, perform other tests to ensure that the link is functioning properly. For more information, refer to the "Troubleshooting Serial Line Problems" chapter.
	Step 3	If the next hop is not directly adjacent, redesign your network so that it is.

Possible Problem	Solution	
End system not generating explorer traffic	**Step 1**	Use the **show source-bridge** privileged EXEC command to see if the explorer count is incrementing.
	Step 2	If the explorer count is not incrementing, use the **show running-config** privileged EXEC command to view the router configuration. Check for a **source-bridge spanning** interface configuration command on the local and remote routers.
	Step 3	If the **source-bridge spanning** command is not configured on the routers, configure it on the interfaces connecting the local and remote SRBs. This command is required if the end system is using single-route explorers.
Encapsulation mismatch	**Step 1**	Use the **show interfaces** EXEC command to verify that the interface and line protocol are up. If the status line indicates any other state, refer to the "Troubleshooting Serial Line Problems" chapter.
	Step 2	Verify that the configured encapsulation type matches the requirements of the network to which the serial interface is attached.
		For example, if the serial interface is attached to a leased line but the configured encapsulation type is Frame Relay, there is an encapsulation mismatch.
	Step 3	To resolve the mismatch, change the encapsulation type on the serial interface to the type appropriate for the attached network.
Hop count exceeded	**Step 1**	Use the **show** *protocol* **route** command to check the hop count values on routers and bridges in the path. Packets that exceed the hop count are dropped.
		Alternatively, you can enable the **debug source event** privileged EXEC command to see whether packets are being dropped because the hop count has been exceeded.
	Step 2	Increase the hop count if it is less than the default value of 7. Otherwise, the network must be redesigned so that no destination is greater than 7 hops away.

RSRB: Host Cannot Connect to Server (Peers Open)

Symptom: Hosts cannot make connections to servers across a router configured as an RSRB. The output of the **show source-bridge** privileged EXEC command shows that SRB peers are open.

```
ionesco#show source-bridge
[...]
Peers:                  state   lv  pkts_rx  pkts_tx  expl_gn    drops TCP
   TCP 150.136.92.92     -       2      0        0          0      0    0
   TCP 150.136.93.93     open    2*    18       18          3      0    0
[...]
```

Table 8-4 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 8-4   **RSRB: Host Cannot Connect to Server (Peers Open)**

Possible Problem		Solution
End system misconfiguration	Step 1	If the end system is on the ring local to the router, use the **show lnm station** privileged EXEC command on the local router. This command lists the stations on the local ring.
	Step 2	Check the command output for the MAC address of the workstation or server. If the MAC address is not present in the output, check the configuration of the end system.
	Step 3	If the problem persists, use a network analyzer to check network traffic generated by the end system. If you do not have a network analyzer, use the **debug token-ring** and the **debug source-bridge** commands.
		Caution: Using the **debug token-ring** and the **debug source-bridge** commands on a heavily loaded router is not advised. These commands can cause further network degredation or complete network failure if not used judiciously.
	Step 4	Check the output of the debug commands to see if the end system is sending traffic to the correct MAC addresses or destination names (in the case of NetBIOS).
End system does not support RIF	Step 1	Place a network analyzer on the same ring to which the end system is connected.
	Step 2	Look for RIF frames sent from the end system (RIF frames have the high-order bit of the source MAC address set to 1).
	Step 3	If no RIF frames are seen, the end system does not support RIF and cannot participate in source routing.
		If the protocol is routable, you can route the protocol or configure transparent bridging. If you do use transparent bridging, be careful not to create loops between the SRB and the transparent bridging domains.
	Step 4	If your environment requires SRB, contact your workstation or server vendor for SRB drivers or for information about setting up your workstation or server to support SRB.

Possible Problem	Solution	
Explorer traffic not reaching remote ring	**Step 1**	Using a network analyzer or the **debug source-bridge** command, watch network traffic to see if explorers from the end system reach the remote ring.
	Step 2	If traffic reaches the remote ring successfully, check the configuration of the destination end system (for example, a server) to see why that station does not reply to the explorer traffic from the source.
		If traffic does not reach the remote ring, use the **show source-bridge** command to check ring lists. If information about the ring has not been learned, check router configurations.
	Step 3	If you are using NetBIOS, use the **show netbios name-cache** EXEC command to see if traffic is passing through the network properly. If it is not, check router configurations.
	For detailed information about configuring routers for RSRB, refer to the Cisco IOS *Bridging and IBM Networking Configuration Guide* and *Bridging and IBM Networking Command Reference*.	

RSRB: Periodic Communication Failures

Symptom: Communication failures occur periodically over a router configured as an RSRB.

Table 8-5 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 8-5   **RSRB: Periodic Communication Failures**

Possible Problem	Solution
Misconfigured T1 timers	If you are not using local acknowledgment, misconfigured T1 timers can cause periodic timeouts.
	Step 1 Use a network analyzer to see how long it takes for packets to travel from one end of the network to the other.
	Step 2 Use a **ping** test to the remote router and note the round trip delay. Compare this value with the configured T1 timer values on end systems.
	Step 3 If the round trip delay is close to or exceeds the T1 timer value, acknowledgments are probably being delayed or dropped by the WAN. For delays, increase the T1 configuration on end systems. For drops, check buffers and interface queues.
	Step 4 Enable local acknowledgment to see if that solves the problem.
WAN link problem	For information on troubleshooting serial line problems, refer to the "Troubleshooting Serial Line Problems" chapter. For information on troubleshooting different WAN environments, refer to the appropriate chapter elsewhere in this publication.

RSRB: NetBIOS Client Cannot Connect to Server

Symptom: NetBIOS clients cannot connect to NetBIOS servers over a router configured as an RSRB.

Table 8-6 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 8-6   RSRB: NetBIOS Client Cannot Connect to Server

Possible Problem	Solution

Incorrect mapping of NetBIOS name cache server-to-client mapping	**Step 1** For each router on which NetBIOS name caching is enabled, use the **show rif** EXEC command to determine whether the RIF entry shows the correct path from the router to *both* the client and the server.
	
	```cantatrice#show rif```
	`Codes: * interface, - static, + remote`
	`Hardware Addr  How    Idle (min)   Routing Information Field`
	`5C02.0001.4322 rg5           -     0630.0053.00B0`
	`5A00.0000.2333 TR0           3     08B0.0101.2201.0FF0`
	`5B01.0000.4444 -             -     -`
	`0000.1403.4800 TR1           0     -`
	`0000.2805.4C00 TR0           *     -`
	`0000.2807.4C00 TR1           *     -`
	`0000.28A8.4800 TR0           0     -`
	`0077.2201.0001 rg5          10     0830.0052.2201.0FF0`
	
	Step 2 Use the **show running-config** privileged EXEC command to view the router configuration. Make sure that the **source-bridge proxy-explorer** interface configuration command is included in the Token Ring configuration. Proxy explorers must be enabled on any interface that uses NetBIOS name caching.
	
	Step 3 Use the **show netbios-cache** EXEC command to see if the NetBIOS cache entry shows the correct mappings of server and client names to MAC addresses.
	
	```cantatrice#show netbios-cache```
	`  HW Addr          Name           How      Idle     NetBIOS Packet Savings`
	`1000.5a89.449a    IC6W06_B       TR1       6          0`
	`1000.5a8b.14e5    IC_9Q07A       TR1       2          0`
	`1000.5a25.1b12    IC9Q19_A       TR1       7          0`
	`1000.5a25.1b12    IC9Q19_A       TR1      10          0`
	`1000.5a8c.7bb1    BKELSA1        TR1       4          0`
	`1000.5a8b.6c7c    ICELSB1        TR1       -          0`
	`1000.5a31.df39    ICASC_01       TR1       -          0`
	`1000.5ada.47af    BKELSA2        TR1      10          0`
	`1000.5a8f.018a    ICELSC1        TR1       1          0`
	
	Step 4 Use the **show running-config** privileged EXEC command at each router to examine the mapping of addresses specified in **netbios name-cache** global configuration command entries.
	
	The following example shows a configuration in which the NetBIOS server is accessed remotely:
	
	`source-bridge ring-group 2`
	`rif 0110.2222.3333 0630.021.0030 ring group 2`
	`netbios name-cache 0110.2222.3333 DEF ring-group 2`
	
	Change any mappings that are not correct.
	
	For detailed information about configuring NetBIOS name caching, refer to the Cisco IOS *Bridging and IBM Networking Configuration Guide* and *Bridging and IBM Networking Command Reference*.

Possible Problem	Solution	
Misconfigured **source-bridge** command	**Step 1**	For each router on which NetBIOS name caching is enabled, use the **show source-bridge** command to obtain the version of the remote connection. The value specified should be 2 or 3. If the value is 1, connections will not get through, and you must modify your configuration.
	Step 2	If the router is running a software release prior to Cisco Internetwork Operating System (Cisco IOS) Release 10.0, specify either **version 2** or **version 3** in the **source-bridge remote-peer** interface configuration command.
		If the router is running Cisco IOS Release 10.0 or later, the specification of a version is ignored.
		For more information, refer to the Cisco IOS *Bridging and IBM Networking Configuration Guide* and *Bridging and IBM Networking Command Reference*.

Translational Bridging: Client Cannot Connect to Server

Symptom: Clients cannot communicate over a router configured as a translational bridge.

⚠️ **Caution** In certain situations, replacing existing translational bridges with Cisco translational bridges can cause interoperability problems. Some translational bridge implementations map functional addresses between media (such as LAT functional address 0900.2B00.00FA on Ethernet) to a broadcast address on the Token Ring side (such as C000.FFFF.FFFF). Cisco does not support this functionality. Furthermore, you cannot use translational bridging with any protocol that embeds the MAC address of a station inside the Information field of the MAC frames (examples include IP ARP and Novell IPX).

Table 8-7 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 8-7   Translational Bridging: Client Cannot Connect to Server

Possible Problem	Solution
Media problem	Verify the line using the **show interfaces** EXEC command. If the interface or line protocol is down, troubleshoot the media. For LAN media, refer to the chapter "Troubleshooting LAN Media Problems." For serial lines, refer to the chapter "Troubleshooting Serial Line Problems."
Ethernet-to-Token Ring address mapping is misconfigured	**Step 1** Use the **show bridge** EXEC command to verify the existence of the Ethernet station. Ethernet and Token Ring addresses use opposite bit ordering schemes. The Token Ring address 0110.2222.3333 is equivalent to the Ethernet address 8008.4444.cccc. **Step 2** Use the **show spanning** EXEC command to determine whether the Ethernet port is in forwarding mode. **Step 3** Use the **show rif** EXEC command to determine whether the target Token Ring station is visible on the internetwork. When configured for translational bridging, the router extracts the RIF of a packet received from the Token Ring network and saves it in a table. The router then transmits the packet on the Ethernet network. Later, the router reinserts the RIF when it receives a packet destined for the originating node on the Token Ring side. **Step 4** If Ethernet and Token Ring end systems are visible, statically configure any relevant server MAC addresses in the client configurations so that clients can listen to the server advertisements directly. One case in which static mapping is required is when bridging DEC LAT traffic over a translational bridge. LAT services on Ethernet are advertised on a multicast address that is mapped by some translational bridges to a broadcast address on the Token Ring side. Routers do not support this mapping.
Vendor code mismatch	Older Token Ring implementations require that the vendor code (OUI[1] field) of the SNAP[2] header be 000000. Cisco routers modify this field to be 0000F8 to specify that the frame was translated from Ethernet Version 2 to Token Ring. This can cause problems on older Token Ring networks. Specify the **ethernet-transit-oui** interface configuration command to force the router to make the vendor code field 000000. This change is frequently required when there are IBM 8209s (IBM Token Ring-to-Ethernet translating bridges) in the network.

Possible Problem	Solution	
Cisco and non-Cisco translational bridges in parallel	**Step 1**	Check for translational bridges in parallel with the Cisco translational bridge. If there are any parallel non-Cisco translational bridges, loops will probably be created.
	Step 2	Because implementing translational bridging defeats the spanning-tree mechanism of both transparent bridging and SRB environments, you must eliminate all loops caused by inserting the translational bridge. A transparent spanning tree and a source-bridge spanning tree cannot communicate with one another.
Trying to bridge protocols that embed MAC addresses in the Information field of the MAC frame (such as IP ARP, Novell IPX, or AARP[3])	If MAC addresses are embedded in the Information field of the MAC frame, bridges will be unable to read the address. Bridges will therefore be unable to forward the traffic.	
	Step 1	If you are attempting to bridge this type of protocol, route the protocol instead.
	Step 2	If you still cannot communicate over the router, contact your technical support representative.

1. OUI=Organizational Unique Identifier
2. SNAP=Subnetwork Access Protocol
3. AARP=AppleTalk Address Resolution Protocol

SRT Bridging: Client Cannot Connect to Server

Symptom: Clients cannot communicate over a router configured to perform source-route transparent (SRT) bridging. Packets are not forwarded by the SRT bridge.

Note SRT bridging allows you to implement transparent bridging in Token Ring environments. It is *not* a means of translating between SRB on a Token Ring and transparent bridging on Ethernet (or other) media.

Table 8-8 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 8-8   SRT Bridging: Client Cannot Connect to Server

Possible Problem	Solution
Trying to bridge frames containing RIF from Token Ring network to Ethernet network over an SRT bridge	Use translational bridging instead of SRT bridging to allow SRB-to-transparent bridging translation.
	Because SRT bridging works only between Ethernet and Token Ring, any packet containing a RIF is dropped when SRT bridging is used.
Attempting to transfer large frame sizes	Problems will occur if Token Ring devices transmit frames exceeding the Ethernet MTU of 1500 bytes. Configure hosts on the Token Ring to generate frame sizes less than or equal to the Ethernet MTU.
Trying to bridge protocols that embed the MAC address in the Information field of the MAC frame (such as IP ARP, Novell IPX, or AARP)	If MAC addresses are embedded in the Information field of the MAC frame, bridges will be unable to read the address. Bridges will therefore be unable to forward the traffic.
	Step 1 If you are attempting to bridge this type of protocol, route the protocol instead.
	Step 2 If you still cannot communicate over the router, contact your technical support representative.
Media problem	Verify the line using the **show interfaces** EXEC command. If the interface or line protocol is down, troubleshoot the media. For LAN media, refer to the chapter "Troubleshooting LAN Media Problems." For serial lines, refer to the chapter "Troubleshooting Serial Line Problems."

SDLC: Router Cannot Communicate with SDLC Device

Symptom: Router cannot communicate with an IBM Synchronous Data Link Control (SDLC) device.

Table 8-9 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 8-9   SDLC: Router Cannot Communicate with SDLC Device

Possible Problem	Solution	
Physical layer problem	**Step 1**	Use the **show interfaces** EXEC command to determine whether the interface and line protocol are up.
	Step 2	If the interface and line protocol are both up, troubleshoot link layer problems as described later in this table.
	Step 3	If the output does not indicate up/up, make sure the device is powered on. Make sure all cabling is correct, securely connected, and undamaged. Make sure that the cabling does not exceed the recommended length for the speed of the connection.
	Step 4	If the interface or line protocol is still down, use a breakout box to check the signals on the line.
		Note: On some Cisco platforms, such as the Cisco 7000 running a recent Cisco IOS release, the output of the **show interfaces** command will indicate the state of line signals.
		• If the router is full-duplex DCE, check for DTR and RTS. If these signals are not high, proceed to Step 5. If these signals are high, the interface should be up. If it is not, contact your technical support representative.
		On a Cisco 7000, if the breakout box shows these signals are high but the **show interfaces** command shows they are not, check the router cabling. In particular, make sure that the 60-pin high-density cable is not plugged into the router upside down.
		• If the router is half-duplex DCE, check for DTR. If DTR is not high, proceed to Step 5. If DTR is high, the interface should be up. If it is not, contact your technical support representative.
		Note: Half-duplex is not supported on Cisco 7000 series routers.
		• If the router is full- or half-duplex DTE, check for CD. If CD is not high, proceed to Step 5. If CD is high, the interface should be up. If it is not, contact your technical support representative.
	Step 5	If the router is full-duplex DCE, make sure the device is configured for permanent RTS high. If the device does not allow you to configure permanent RTS, set the signal high by strapping DTR from the device side to RTS on the router side (see Figure 8-1).
	Step 6	If the router is DCE, it is typically required to provide clock to the device. Make sure the **clock rate** interface configuration command is present in the router configuration.
		If the router is DTE, it should get clock from an external device. Make sure that a device is providing clock properly. Make sure that the clocking source is the same for all devices.

Possible Problem	Solution	
Link layer problem (router is primary)	**Step 1**	Use the **debug sdlc** privileged EXEC command[1] to see if the router is sending SNRMs.[2]
	Step 2	If the router is not sending SNRMs, check the physical layer (see the preceding problem in this table). If the router is sending SNRMs, the device should send UAs[3] in reply.
	Step 3	If the device is not sending UAs, make sure the addresses of the router and device are correct.
	Step 4	If you are using a V.35 connection, make sure that the SCT/SCTE[4] setting is correct on the interface. The router should use SCTE if the router is DCE and SCT if the router is DTE.
		This setting might be changed with a jumper or with the software configuration command **dce-terminal-timing enable**, depending on the platform. Some platforms do not allow you to change this setting.
	Step 5	Make sure that the device and the router are using the same signal coding (NRZ[5] or NRZI[6]). NRZ is enabled by default on the router. To enable NRZI encoding, use the **nrzi-encoding** interface configuration command.
	Step 6	Try reducing the line speed to 9600 bps using the **clock rate** interface configuration command.
	Step 7	Make sure that cabling is correct, is securely attached, and is undamaged.
Link layer problem (router is secondary)	**Step 1**	Use the **debug sdlc** privileged EXEC command to see if the router is receiving SNRMs.
	Step 2	If the router is not receiving SNRMs, check the primary device. Make sure the physical layer is operational (see the first problem in this table). If the router is receiving SNRMs, it should send UAs in reply.
	Step 3	If the router is not sending UAs, make sure the addresses of the router and device are correct.
	Step 4	If you are using a V.35 connection, make sure that the SCT/SCTE setting is correct on the interface. The router should use SCTE if the router is DCE and SCT if the router is DTE.
		This setting might be changed with a jumper or with the software configuration command **dce-terminal-timing enable**, depending on the platform. Some platforms do not allow you to change this setting.
	Step 5	Use a breakout box to check for CTS high on the line.
	Step 6	Make sure that both the device and the router are using the same signal coding (NRZ or NRZI). NRZ is enabled by default on the router. To enable NRZI encoding, use the **nrzi-encoding** interface configuration command.
	Step 7	Try reducing the line speed to 9600 bps using the **clock rate** interface configuration command.
	Step 8	Make sure that cabling is correct, is securely attached, and is undamaged.

1. To reduce the amount of screen output produced by the **debug sdlc** command, configure the **sdlc poll-pause-timer 1000** command to reduce the frequency at which the router sends poll frames. Remember to return this command to its original value (the default is 10 milliseconds).
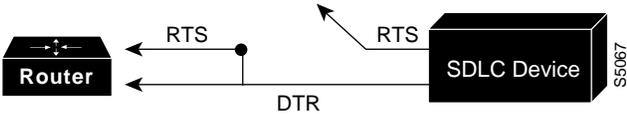2. SNRM=send normal response mode
3. UA=unnumbered acknowledgment
4. SCT/SCTE=serial clock transmit/serial clock transmit external
5. NRZ=nonreturn to zero
6. NRZI=nonreturn to zero inverted

Figure 8-1   Strapping DTR to RTS

SDLC: Intermittent Connectivity

Symptom: User connections to hosts time out over a router configured to perform SDLC Transport.

Table 8-10 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 8-10   SDLC: Intermittent Connectivity

Possible Problem	Solution	
SDLC timing problems	**Step 1**	Place a serial analyzer on the serial line attached to the source station and monitor packets.
	Step 2	If duplicates appear, check the router configuration using the **show running-config** privileged EXEC command. Check to see if the **local-ack** keyword is present in the configuration.
	Step 3	If the keyword is missing, add it to the router configuration for SDLC interfaces.
	Step 4	Local acknowledgment parameters can be adjusted in the router, the attached device, or both. Adjust SDLC protocol parameters as appropriate. These parameters are used to customize SDLC Transport over various network configurations. In particular, you might need to tune various LLC2 timer values.
	For more information about configuring SDLC, refer to the Cisco IOS *Bridging and IBM Networking Configuration Guide* and *Bridging and IBM Networking Command Reference*.	

SDLC: Client Cannot Connect to Host over Router Running SDLLC

Symptom: Users cannot open connections to hosts on the other side of a router configured to support SDLLC.

Table 8-11 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 8-11   SDLC: Client Cannot Connect to Host over Router Running SDLLC

Possible Problem	Solution	
SDLC physical or data link layer problem	Step 1	Use the **show interface** *slot/port* EXEC command to check the state of the connection with the SDLC device.
	Step 2	Look for USBUSY in the output, which indicates that the router is attempting to establish an LLC connection. If the router is not USBUSY, make sure that the physical and link layer are working properly. For more information, refer to the section "SDLC: Router Cannot Communicate with SDLC Device" earlier in this chapter.
	Step 3	If the router is USBUSY, proceed to the next problem in this table.
Router not sending test frames to FEP[1]	Step 1	With the **debug sdllc** and **debug llc2 packet** privileged EXEC commands enabled on the router, check to see if the router is sending test frames to the FEP.
	Step 2	If the router is sending test frames to the FEP, proceed to the next problem in this table.
	Step 3	If the router is not sending test frames to the FEP, use the **show running-config** privileged EXEC command to view the router configuration. Make sure that the **sdllc partner** interface configuration command is present.
	Step 4	If the command is not present, add it to the configuration. Make sure that it points to the hardware address of the FEP on the Token Ring
FEP on Token Ring not replying to test frames	Step 1	With the **debug sdllc** and **debug llc2 packet** privileged EXEC commands enabled on the router, check to see if the FEP is replying to test frames sent by the router.
	Step 2	If the FEP is responding, proceed to the next problem in this table.
	Step 3	If the FEP is not responding, check the MAC address of the router's partner (the FEP). Make sure that the address is correctly specified in the **sdllc partner** command entry on the router.
	Step 4	Check to see if RSRB peers are up. If the peers are not open, refer to the section "RSRB: Host Cannot Connect to Server (Peers Not Open)" earlier in this chapter.
	Step 5	If the RSRB peers are up, attach a network analyzer to the Token Ring with the FEP attached and make sure that the router's test frames are arriving on the ring and that the FEP is replying.
XID not sent by router	Step 1	With the **debug sdllc** and **debug llc2 packet** privileged EXEC commands enabled on the router, check to see if the router is sending XID frames to the FEP.
	Step 2	If the router is sending XID frames to the FEP, proceed to the next problem in this table.
	Step 3	If the router is not sending XID frames, use the **show running-config** privileged EXEC command to view the router configuration. Make sure there is an **sdllc xid** interface configuration command entry present.
	Step 4	If the **sdllc xid** command is not configured on the router, add it to the configuration.

Possible Problem	Solution	
FEP not replying to XID	**Step 1**	With the **debug sdllc** and **debug llc2 packet** privileged EXEC commands enabled on the router, check to see if the FEP is replying to XID frames from the router.
	Step 2	If the FEP is responding, proceed to the next problem in this table.
	Step 3	If the FEP is not responding, check the XID values configured by the **sdllc xid** command on the router. The values for IDBLK and IDNUM on the router must match the values in VTAM on the FEP.
	Step 4	Make sure that the XID information on the hosts is properly defined. If a 317X device is a channel-attached gateway, the XID must be 0000000 for IDBLK and IDNUM.
Host problem	Check for activation, application problems, VTAM and NCP misconfigurations, configuration mismatches, and other problems on the IBM host.	

1. FEP=front end processor

Virtual Token Ring Addresses and SDLLC

The **sdllc traddr** command specifies a virtual Token Ring MAC address for an SDLC-attached device (the device you are spoofing to look like a Token Ring device). The last two hexadecimal digits of the virtual MAC address *must* be 00. The router then reserves any virtual ring address that falls into the range xxxx.xxxx.xx00 to xxxx.xxxx.xxff for the SDLLC serial interface.

As a result, other IBM devices on an internetwork might have an LAA that falls in the same range. This can cause problems if you are using local acknowledgment because routers examine only the first 10 digits of the LAA address of a packet (not the last two, which are considered wildcards).

If the router sees an address that matches an assigned SDLLC LAA address, it automatically forwards that packet to the SDLLC process. This can result in packets being incorrectly forwarded to the SDLLC process and sessions never being established.

Note To avoid assigning conflicting addresses, be certain you know the LAA naming convention used in the internetwork before assigning a virtual ring address for any SDLLC implementation.

SDLC: Sessions Fail over Router Running STUN

Symptom: SDLC sessions between two nodes fail when they are attempted over a router that is running serial tunnel (STUN).

Note   This section discusses troubleshooting procedures for STUN without local acknowledgment (LACK). For STUN with LACK, the procedures are essentially the same, but remember that there are two sessions, one from the Primary to the router, and one from the Secondary to the router.

Table 8-12 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 8-12   **SDLC: Sessions Fail over Router Running STUN**

Possible Problem	Solution	
Peers are not open	**Step 1**	Use the **show stun** EXEC command to see if the peers are open. If the peers are open, one of the other problems in this table is probably the cause.
	Step 2	If the peers are not open, use the **debug stun** command on the core router to see if the peers are trying to open. Peers will not open if there is no traffic on the link.
		Caution: Do not enable **debug** commands on a heavily loaded router. Doing so can cause performance and connectivity problems. Use a protocol analyzer or **show** commands instead.
	Step 3	If you do not see the peers trying to open, use the **show interface** EXEC command to make sure the interface and line protocol are both up. If they are not both up, there could be a link problem. Proceed to the problem "SDLC physical or link layer problem" later in this table.
	Step 4	If the peers are trying to open, use the **show running-config** privileged EXEC command to make sure that the **stun route** and other STUN configuration commands are configured correctly. Reconfigure the router if necessary.
	Step 5	Use the **debug stun packet** privileged EXEC command on the core router. Look for SNRMs or XIDs being sent.
	Step 6	If you do not see SNRMs or XIDs, there is probably a basic link problem. See the problem "SDLC physical or link layer problem" later in this table.
	Step 7	Check to make sure that there are not other network problems occurring, such as interface drops, buffer misses, overloaded Frame Relay switches, IP routing problems and so forth.

Possible Problem	Solution	
SNRMs or XIDs not sent	Step 1	Use the **show stun** command to see if the peers are open. If the peers are not open, see the preceding problem in this table.
	Step 2	If the peers are open, use the **debug stun packet** privileged EXEC command on the remote end. Check for SNRMS or XIDs from the Primary arriving as NDI packets.
	Step 3	If SNRMs or XIDs are arriving, proceed to the next problem in this table.
	Step 4	If SNRMS or XIDs are not arriving, use the **debug stun packet** command on the core router to see if SNRMs or XIDs are being sent.
	Step 5	If the core router is not sending SNRMs or XIDs, make sure that the physical and link layers are operating properly. See the problem "SDLC physical or link layer problem" later in this table.
	Step 6	If the core router is sending SNRMs or XIDs, use the **show running-config** privileged EXEC command to make sure the **stun route** command is properly configured on the router.
	Step 7	Check to make sure that there are not other network problems occurring, such as interface drops, buffer misses, overloaded Frame Relay switches, IP routing problems and so forth.
No reply to SNRMs or XIDs	Step 1	Use the **show stun** command to see if the peers are open. If the peers are not open, see the first problem in this table.
	Step 2	If the peers are open, use the **debug stun packet** privileged EXEC command on the remote end. Check for SNRMS or XIDs from the Primary arriving as NDI packets.
	Step 3	If SNRMs or XIDs are not arriving, refer to the preceding problem in this table.
	Step 4	If SNRMs or XIDs are arriving, make sure that the core router is sending UA or XID responses as SDI packets.
	Step 5	If the router is not sending responses, there might be a link problem. Refer to the problem "SDLC physical or link layer problem" later in this table.
	Step 6	If the router is sending responses, use the **debug stun packet** command to see if the UA or XID responses are getting back to the Primary as SDI packets.
	Step 7	If the responses are not getting back to the Primary, use the **show running-config** privileged EXEC command to make sure that the **stun route** and other STUN configuration command are properly configured on the remote router.
	Step 8	Check to make sure that there are not other network problems occurring, such as interface drops, buffer misses, overloaded Frame Relay switches, IP routing problems and so forth.
	Step 9	If packets are passed end-to-end in both directions, check end station configurations, duplex settings, configurations, and so forth.
SDLC physical or link layer problem	Step 1	Use the **show interfaces** EXEC command on the link connecting to the Primary device. Make sure that the interface and line protocol are both up.
	Step 2	If the interface or line protocol is not up, make sure the devices are powered up and connected correctly. Check the line to make sure it is active. Check for clocking, address misconfigurations, correct NRZ or NRZI specifications and so forth.
	Step 3	Try slowing the clock rate of the connection.
	For more information about troubleshooting SDLC physical and link layer problems, see the section "SDLC: Router Cannot Communicate with SDLC Device" earlier in this chapter.	

CIP: CLAW Connection Does Not Come Up

Symptom: Common Link Access for Workstations (CLAW) connections do not come up properly over a Channel Interface Processor (CIP). The output of the **show extended channel** *slot/port* **statistics** EXEC command shows "N" for CLAW connections, indicating that they are down.

Table 8-13 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 8-13 **CIP: CLAW Connection Does Not Come Up**

Possible Problem	Solution	
TCP/IP not running on host	**Step 1**	Check to see if TCP/IP is running on the host.
	Step 2	If TCP/IP is not running, start it.
CIP devices not online to host	**Step 1**	Check the mainframe to see if the CIP devices are online to the host.
	Step 2	If the CIP devices are not online, vary them online. If devices do not come online, see the section "CIP: CIP Will Not Come Online to Host" later in this chapter.
	Step 3	Check to see if the TCP/IP device has been started.
	Step 4	If the device has not been started, start it.
		Note: It might be necessary to stop and start the TCP/IP application to start the device. If you are using obey files this might not be necessary.
	Step 5	Check the configuration for the CIP in the TCP/IP Profile on the host, and the router configuration for the CIP device.
	Step 6	Use the **moretrace claw** command on the host, either from an obey file or in the TCP/IP Profile. This command traces the establishment of CLAW connections and can provide information useful for determining causes of connection problems.

CIP: No Enabled LED On

Symptom: The Enabled LED on the CIP card does not come on.

Table 8-14 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 8-14   CIP: No Enabled LED On

Possible Problem	Solution	
Hardware problem	**Step 1**	Check to make sure that the router is plugged in and is turned on.
	Step 2	Use the **show version** EXEC command and see if the CIP card appears in the output.
	Step 3	If the CIP card appears in the output, the Enabled LED might be faulty.
		If the CIP card does not appear in the output, reseat the CIP card, reboot the router, and check the output of the **show version** command again.
Old Cisco IOS release	**Step 1**	Use the **show version** EXEC command to find out what version of the Cisco IOS software you are running.
	Step 2	If you are using Cisco IOS software prior to Release 10.2(6), you should upgrade to a more recent version.

CIP: CIP Will Not Come Online to Host

Symptom: The CIP card will not come online to the host.

Table 8-15 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 8-15　　**CIP: CIP Will Not Come Online to Host**

Possible Problem	Solution	
CHPID[1] not online to host	**Step 1**	Make sure the Enabled LED on the CIP card is on. If it is not on, refer to the section "CIP: No Enabled LED On" earlier in this chapter.
	Step 2	Use the **show extended channel** *slot/port* **subchannel** command and check for the SIGNAL flag in the output.
	Step 3	If the SIGNAL flag is not present, check to see if the CHPID is online to the host. If it is not, configure it to come online.
		Note: On a bus and tag channel, the SIGNAL flag is turned on by OP_OUT being high from the host. On an ESCON channel, the SIGNAL flag is turned on by the presence of light on the channel.
	Step 4	If the CHPID does not come online to the host, check the physical cabling.
	Step 5	If the CIP still does not come online, check the IOCP[2] definitions for the CIP device, and the router configuration.

1. CHPID=channel path identifier
2. IOCP=input/output control program

CIP: Router Cannot ping Host or Host Cannot ping Router

Symptom: Attempts to **ping** are unsuccessful, either from the CIP card in a router to a host or from a host to the CIP card in a router.

Table 8-16 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 8-16   **CIP: Router Cannot ping Host or Host Cannot ping Router**

Possible Problem	Solution	
Addressing problem between CIP and host	Step 1	Verify that the CLAW connection is up by checking the output of the **show extended channel** *slot/port* **statistics** EXEC command on the router.
	Step 2	If the output shows CLAW connections are not up (indicated by a "N"), refer to the section "CIP: CLAW Connection Does Not Come Up" earlier in this chapter.
	Step 3	If the CLAW connections are up (indicated by a "Y") issue the **clear counters** privileged EXEC command. Then attempt a basic **ping** to the host from the router or to the router from the host.
	Step 4	When the ping is completed, use the **show extended channel** *slot/port* **statistics** EXEC command on the router.
		If you issued the ping from the router to the host, the host should have read 5 100-byte ICMP echos from the router. The Total Blocks field in the **show** command output should indicate 5 blocks read. If the host replied, the output should indicate 5 blocks written.
		If you issued the ping from the host to the router, the host should have sent one 276 byte ICMP echo to the router. The Write field should indicate 1 block written. If the router replied, the output should indicate 1 block in the Read field.
	Step 5	If this is not the case, there could be an addressing problem between the CIP and the host. Check all IP addresses on the router and in the host TCP/IP Profile and make sure they are correct.

CIP: Host Cannot Reach Remote Networks

Symptom: Mainframe host cannot access networks across a router.

Table 8-17 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 8-17   CIP: Host Cannot Reach Remote Networks

Possible Problem	Solution	
Missing or misconfigured IP routes	**Step 1**	If the mainframe host is unable to communicate with networks on the other side of the router, try to **ping** the remote network from the router.
		If the ping succeeds, proceed to Step 4.
	Step 2	If the **ping** fails, use the **show ip route** privileged EXEC command to verify that the network is accessible by the router.
	Step 3	If there is no route to the network, check the network and router configuration for problems.
	Step 4	Verify that the host connection is active by pinging the host IP address from the router. If the **ping** is unsuccessful, see the section "CIP: Router Cannot ping Host or Host Cannot ping Router" earlier in this chapter.
	Step 5	Issue the **netstat gate** command on the host and check for a route to the network.
	Step 6	If a route does not exist, make sure the host is using the address of the CIP in the router as the default route. If it is not, add a GATEWAY statement in the TCP/IP Profile that points to the network, or set the CIP in the router as the default route using a DEFAULTNET statement in the TCP/IP Profile.

CIP: Host Running Routed Has No Routes

Symptom: A host running *routed* has no routes to remote networks.

Table 8-18 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 8-18   CIP: Host Running Routed Has No Routes

Possible Problem	Solution	
RIP not properly configured on the router	Step 1	Use the **show running-config** privileged EXEC command to view the router configuration. Make sure that RIP is configured on the router. If RIP is not configured, configure it.
	Step 2	Check the configuration to see if there are **network** statements for each of the networks that should be advertised in RIP updates. If they are missing, add them to the configuration.
	Step 3	Make sure that the **passive-interface** command is not configured on the channel interface.
	Step 4	If the command is present, remove it using the **no passive-interface** router configuration command.
	Step 5	Make sure that there are no **distribute-list** statements filtering RIP routing updates.
	Step 6	Check the router configuration to be sure that the **broadcast** keyword has been specified in the **claw** interface configuration command.
	Step 7	If there is no **broadcast** keyword specified, add it to the configuration.
Host misconfiguration	Step 1	Use the **netstat gate** command on the host. Check to see if there are routes learned from RIP updates.
	Step 2	If you do not see RIP routes, verify that the host connection is active by pinging the host IP address from the router.
	Step 3	If the ping is unsuccessful, see the section "CIP: Router Cannot ping Host or Host Cannot ping Router" earlier in this chapter.
	Step 4	Verify that the *routed* daemon is running on the host.
	Step 5	Use the **show extended channel** *slot/port* **stat** EXEC command to see if RIP routing updates are incrementing the counters.
	Step 6	Check the TCP/IP Profile on the host to be sure that there are BSDROUTINGPARMS instead of GATEWAY statements.