Troubleshooting Novell IPX

This chapter presents protocol-related troubleshooting information for Novell Internet Packet Exchange (IPX) connectivity and performance problems.

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

- Novell IPX: Client Cannot Connect to Server on Same LAN
- Novell IPX: Client Cannot Connect to Server on Remote LAN
- Novell IPX: Clients Cannot Connect to Server over PSN
- Novell IPX: Client Cannot Connect to Server over ISDN
- Novell NetBIOS: Applications Cannot Connect to Server over Router
- IPX RIP: No Connectivity over IPX RIP Router
- IPX RIP: SAP Updates Not Propagated by Router
- IPX Enhanced IGRP: No Connectivity over IPX Enhanced IGRP Router
- IPX Enhanced IGRP: Routers Not Establishing Neighbors
- IPX Enhanced IGRP: SAP Updates Not Propagated by Router
- IPX Enhanced IGRP: Router Stuck in Active Mode
- Novell IPX: Intermittent Connectivity
- Novell IPX: Slow Performance

Novell IPX: Client Cannot Connect to Server on Same LAN

Symptom: Clients cannot make connections to servers located on the same LAN. Also, clients cannot connect to servers on remote networks.

Table 6-1 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 6-1 Novell IPX: Client Cannot Connect to Server on Same LAN

Possible Problem	Solution
Misconfigured client or server	**Step 1** Make sure that the software on both clients and servers is the current version, is configured correctly, and has loaded correctly. On clients, check the network drivers and the configuration specified in the *net.cfg* file. **Step 2** On servers, make certain that SAPs[1] are being generated properly and that any NLMs[2] are loaded properly. Use the **track on** command to monitor routing and SAP activity. **Step 3** Check the encapsulation on clients and servers to make sure they are not mismatched. For specific information on configuring your client or server, refer to the documentation provided with the device.
Not enough user licenses	Make sure there is a sufficient number of NetWare user licenses available. Use the Monitor utility screen on a NetWare server to see the total number of connections available and the number of connections in use.

Mismatched network numbers	All servers attached to the same cable must bind to the same external network number. If there are mismatched network numbers, packets will not be forwarded properly.
	Step 1 Watch for error messages on the system console similar to the following:
	`Router configuration error detected`
	`Node address claims network x`
	`should be y`
	These error messages indicate that a server on the LAN has a conflicting network number. The *Node address* is the node address of the network card from which the incorrect address came. *x* is the network number specified in packets received from the node. *y* is the network number configured on the server generating the error.
	Step 2 All servers on the same LAN must have the same external network number (if they use the same frame type). If the network numbers do not match, reconfigure the conflicting server with the correct external network number.

Client, server, or other hardware problem	Check all NIC[3] cards, transceivers, hub ports, switches, and other hardware. Check all appropriate LEDs to see if there are error indications. Replace any faulty or malfunctioning hardware. For information on troubleshooting a client, server, or other hardware problem not related to Cisco routers, refer to the documentation provided with the hardware.

Possible Problem	Solution
Media problem	**Step 1** Check all cabling and connections. Make sure cables are not damaged and that all connections are correct and make proper contact. **Step 2** Use the **show interfaces** EXEC command to check for input or output errors or other indications of problems on the media. **Step 3** If the command output shows excessive errors, use the **clear interface counter** privileged EXEC command to clear the interface counters. **Step 4** Check the output of the **show interfaces** command again. If the errors are incrementing rapidly, there is probably a problem with the media. For more detailed information on troubleshooting media problems, refer to the "Troubleshooting LAN Media Problems" chapter.

1. SAP=Service Advertisement Protocol
2. NLM=NetWare Loadable Module
3. NIC=Network Interface Card

Novell IPX: Client Cannot Connect to Server on Remote LAN

Symptom: Clients cannot make connections to servers on another network over one or more routers interconnected by LAN networks. Clients can connect to servers on their local network.

Note If clients cannot connect to servers on their local network, refer to the section "Novell IPX: Client Cannot Connect to Server on Same LAN" earlier in this chapter.

If there is a WAN network between the local and remote LANs, WAN problems must be considered as a source of problems as well. Refer to the IPX-specific WAN problems outlined later in this chapter, or to the general WAN problems outlined in other chapters in this publication.

Table 6-2 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 6-2 Novell IPX: Client Cannot Connect to Server on Remote LAN

Possible Problem	Solution
Router interface is down	**Step 1** Use the **show interfaces** EXEC command on the router to check the status of the router interfaces. Verify that the interface and line protocol are up. **Step 2** If the interface is administratively down, use the **no shutdown** interface configuration command to bring the interface back up. **Step 3** If the interface or line protocol is down, refer to the "Troubleshooting Hardware and Booting Problems" chapter, the "Troubleshooting LAN Media Problems" chapter, or the "Troubleshooting Serial Line Problems" chapter.
Mismatched Ethernet encapsulation methods	**Step 1** Use the **show ipx interface** privileged EXEC command to check the encapsulation type specified in the router configuration. By default, Cisco routers use Novell's Frame Type Ethernet_802.3 encapsulation. (Cisco refers to this as "novell-ether" encapsulation.) **Step 2** Compare the encapsulation type configured on router interfaces with the encapsulation type that is being used by clients and servers. **Step 3** If the router uses one encapsulation type but the clients and servers use a different type, then there is a mismatch. Change the encapsulation type used on either the clients and servers or the router, as appropriate, so that all devices use the same encapsulation method. On routers, specify the encapsulation type with the **ipx network** *network* **encapsulation** *encapsulation-type* interface configuration command. For information on changing the encapsulation type on clients and servers, consult the vendor documentation.
LIPX problem[1]	If you are using NetWare 3.12 or above and you have LIPX enabled, a client and server could conceivably negotiate a packet size larger than a router could support. This can cause intermediate routers to drop packets. For information on configuring LIPX, refer to the vendor documentation.

Possible Problem	Solution
Ring speed specification mismatch	In a Token Ring environment, all devices must agree on the configured ring speed (4 or 16 Mbps) or connectivity will fail. **Step 1** Use the **show interfaces token** EXEC command on the router. Look for the ring speed value in the output. Compare this value with the ring speed specification on Novell servers. **Step 2** If the ring speeds do not match, change the server or router configuration, as appropriate, so that all stations agree on the ring speed. On routers, use the **ring-speed** interface configuration command to change the ring speed. For information about configuring the ring speed on Novell servers, consult the vendor documentation.
Duplicate node numbers on routers	**Step 1** Use the **show running-config** privileged EXEC command to examine the current configuration of each router in the path. **Step 2** Check the node number specified in the **ipx routing** *node* global configuration command. The node number is either a user-specified node number or the MAC address of the first Ethernet, Token Ring, or FDDI interface card in the router. **Step 3** The node number configured on each router must be unique. If the number is the same on multiple routers, enter the **no ipx routing** global configuration command to disable IPX routing on the router. **Step 4** Reinitialize IPX routing by entering the **ipx routing** command (do not specify a node number). Use the **show running-config** command to verify that the rest of the IPX configuration is still correct.
Duplicate network numbers	Every network number must be unique throughout the entire Novell IPX internetwork. A duplicate network number will prevent packets from being forwarded properly. **Step 1** Use the **show ipx servers** and the **show ipx route** privileged EXEC commands. Check the output of these commands for server addresses that have been learned from the wrong interface. For example, if you know that you have a server on the local network with network number 3c.0000.0c01.2345 and the show command output shows that this server is located on a remote network, there is probably a server on the remote network using the same network number. **Step 2** If you suspect a duplicate network number, use a process of elimination to identify the misconfigured server. This can be difficult, particularly if you do not have access to every network device in the Novell IPX internetwork. When you have identified the misconfigured server, modify the server configuration to eliminate the duplicate network number.
Router hardware problem	Check all router ports, interface processors, and other router hardware. Make sure cards are seated properly and that no hardware is damaged. Replace faulty or malfunctioning hardware. For detailed information on troubleshooting router hardware problems, refer to the "Troubleshooting Hardware and Booting Problems" chapter.

Possible Problem	Solution
Backdoor bridge between segments	**Step 1** Use the **show ipx traffic** EXEC command on intermediate routers. Determine whether the "bad hop count" field is incrementing. **Step 2** If the counter is incrementing, use a network analyzer to look for packet loops on suspect segments. Look for RIP[2] and SAP updates as well. If a backdoor bridge exists, you are likely to see hop counts that increment to 16, at which time the route disappears and reappears unpredictably. **Step 3** Look for packets from known *remote* network numbers that appear on the *local* network. Look for packets whose source address is the MAC address of the remote node instead of the MAC address of the router. **Step 4** Examine packets on each segment. A back door is present on the segment if packets appear whose source address is the MAC address of a remote node instead of that of the router. **Step 5** Remove the backdoor bridge to close the loop.
Routing protocol problem	Misconfigurations and other routing protocol issues can cause connectivity and performance problems. For information on troubleshooting specific IPX routing protocols, see the appropriate section later in this chapter.

1. LIPX=Large Internet Packet Exchange
2. RIP=Routing Information Protocol

Novell IPX: Clients Cannot Connect to Server over PSN

Symptom: Clients cannot connect to servers over a packet-switched network (PSN), such as Frame Relay, X.25, or SMDS. Clients can connect to local servers.

Note Procedures for troubleshooting connectivity problems not specific to PSN environments are described in the section "Novell IPX: Client Cannot Connect to Server on Remote LAN" earlier in this chapter.

Table 6-3 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 6-3 Novell IPX: Client Cannot Connect to Server over PSN

Possible Problem	Solution
Address mapping error	**Step 1** Use the **show running-config** privileged EXEC command to view the configuration of the router. **Step 2** Depending on your PSN environment, look for any **x25 map ipx**, **frame-relay map ipx**[1], or **smds static-map ipx** interface configuration command entries in the router configuration. Make sure that the address mapping specified by these commands are correct. • For X.25, address mapping maps host protocol addresses to the host's X.121 address • For Frame Relay, address mapping maps a next hop protocol address and the DLCI used to connect to the address • For SMDS, address mapping defines static entries for SMDS remote peer routers For more information about configuring address maps, refer to the Cisco IOS *Wide Area Networking Configuration Guide* and *Wide Area Networking Command Reference*.

Encapsulation mismatch	**Step 1** Use the **show interfaces** privileged EXEC command to determine the encapsulation type being used (such as x25, frame-relay, or smds encapsulation). Look for output similar to the following:
	`Serial0 is up, line protocol is up`
	`Hardware is MCI Serial`
	`Internet address is 192.168.54.92 255.255.255.0`
	`MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255`
	`Encapsulation FRAME-RELAY, loopback not set, keepalive set (10 sec)`
	Step 2 If an **encapsulation** command is not present, the default is HDLC[2] encapsulation. For PSN interconnection, you must explicitly specify the proper encapsulation type (such as **encapsulation x25** for an X.25 connection).
	Configure the proper encapsulation type and use the **show interfaces** command to verify that the encapsulation type is correct.

Misconfigured DLCI assignments (Frame Relay only)	**Step 1** Use the **show frame-relay map** EXEC command on the hub router to see the Frame Relay map assignments currently configured. **Step 2** Check each Frame Relay map statement to ensure that the DLCI assignments are correctly configured. Make sure that you use the DLCIs obtained from your Frame Relay provider. Remember that DLCI values are locally significant.

Possible Problem	Solution
Misconfigured LMI type (Frame Relay only)	**Step 1** Use the **debug frame-relay lmi** privileged EXEC command to see the LMI type being used by the Frame Relay switch. **Step 2** The LMI type is determined by your Frame Relay provider. Make sure you use the LMI type specified by the provider.
Frame Relay broadcast queue full (Frame Relay only)	This problem is most likely to occur on the hub router in a Frame Relay hub-and-spoke topology. **Step 1** Use the **show interfaces** privileged EXEC command to check for dropped Frame Relay broadcast frames. **Step 2** If the number of drops on the broadcast queue is excessively high, increase the size of the queue using the **frame-relay broadcast-queue** *size byte-rate packet-rate* interface configuration command.
Hub router not forwarding SAPs (Frame Relay only)	In a Frame Relay hub-and-spoke topology, SAPs received on one of the hub router's interfaces will not be forwarded back out the same interface because of the split horizon rule. To allow SAPs to be forwarded appropriately, you must configure subinterfaces on the Frame Relay interface of the hub router. Assign a subinterface to each spoke site. The hub router will treat each subinterface as a physical interface, allowing it to advertise SAPs without violating the split horizon rule. For specific information on configuring subinterfaces, see the *Wide Area Networking Configuration Guide*. **Note:** There are other problems that can prevent a router from forwarding SAP packets. For more information, see the section "IPX RIP: SAP Updates Not Propagated by Router," later in this chapter.
Missing or misconfigured multicast address (SMDS only)	**Step 1** Use the **show running-config** privileged EXEC command to view the router configuration. Check for an **smds multicast ipx** interface configuration command entry. **Step 2** If the command is not present, add it to the configuration. If the command is present, confirm that the multicast address configured is correct. The SMDS multicast address is specified by your SMDS provider.

1. You can eliminate the need for Frame Relay address maps by using Inverse ARP instead. Use the **frame-relay interface-dlci** *dlci* **broadcast** interface configuration command to configure an interface to use Inverse ARP. For more information about the use of this command, refer to the Cisco IOS *Wide Area Networking Configuration Guide* and *Wide Area Networking Command Reference*.
2. HDLC=High-Level Data Link Control

Novell IPX: Client Cannot Connect to Server over ISDN

Symptom: Clients cannot connect to servers over an ISDN link. Clients can connect to local servers.

Note Procedures for troubleshooting connectivity problems not specific to ISDN environments are described in the section "Novell IPX: Client Cannot Connect to Server on Remote LAN," earlier in this chapter.

Procedures for troubleshooting ISDN connectivity problems not specific to IPX environments are described in the "Troubleshooting ISDN Connections" chapter.

Table 6-4 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 6-4 Novell IPX: Client Cannot Connect to Server over ISDN

Possible Problem	Solution
Static RIP and SAP statements missing or misconfigured	**Step 1** Use the **show running-config** privileged EXEC command to view the router configuration. Check for **ipx route** and **ipx sap** global configuration command entries. These commands, which specify static routes and static SAP entries, respectively, are required in an ISDN environment so that clients and servers on the local network are aware of clients and servers on the remote network. **Step 2** If you do not have static routes and static SAP entries configured, configure them using the **ipx route** and **ipx sap** commands. For detailed information on configuring static routes and SAP entries, refer to the Cisco IOS *Network Protocols Configuration Guide, Part 1* and *Network Protocols Command Reference, Part 1*.
Access lists specified in dialer lists misconfigured	**Step 1** Use the **show running-config** privileged EXEC command to view the router configuration. Check the access lists configured for use by dialer lists. **Step 2** Make sure that the access lists deny only RIP routing updates, SAP advertisements, and Novell serialization packets. If other packets are denied, connectivity problems can occur. **Step 3** Make sure access lists end with an **access-list** *access-list-number* **permit -1** statement, which permits all other IPX traffic to trigger the dialer.

Novell NetBIOS: Applications Cannot Connect to Server over Router

Symptom: Applications that use Novell NetBIOS (such as Windows 95) cannot connect to servers over a router. Clients cannot connect to servers on the same LAN.

Table 6-5 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 6-5 Novell NetBIOS: Applications Cannot Connect to Server over Router

Possible Problem	Solution
Missing **ipx type-20-propagation** commands	**Step 1** Use the **debug ipx packet** privileged EXEC command or a network analyzer to look for Novell packets with a specification of type 20. **Note:** Exercise caution when using the **debug ipx packet** command. This command can cause problems if used on a heavily loaded router. **Step 2** Use the **show running-config** privileged EXEC command to check for **ipx type-20-propagation** interface configuration command entries on routers in the path from client to server. **Step 3** If the **ipx type-20-propagation** command is not present, add it to the interface configuration for every router interface in the path from client to server.
Missing **ipx helper-address** command	**Step 1** Use the **debug ipx packet** privileged EXEC command or a network analyzer to look for Novell packets with a specification other than type 20 (such as type 0 or type 4). Sometimes applications do not conform to the Novell standard and use packet types other than type 20. **Note:** Exercise caution when using the **debug ipx packet** command. This command can cause problems on a heavily loaded router. **Step 2** If you see such packets, use the **show running-config** privileged EXEC command to view the router configuration. Check to see if the **ipx helper-address** interface configuration command is configured on the interface to which the client is attached. **Step 3** If the **ipx helper-address** command is not present, configure it on the router interfaces. Make sure that the helper address is the IPX protocol address of the NetBIOS server that the client needs to reach.
Workstation not running NetBIOS over IPX	Make sure that your workstation is running NetBIOS over IPX and not NetBIOS over another protocol, such as NetBEUI. For information about what protocols your workstation is running, refer to the vendor documentation.

IPX RIP: No Connectivity over IPX RIP Router

Symptom: IPX RIP routers are blocking connections. Clients cannot connect to servers over one or more routers running IPX RIP.

Note Procedures for troubleshooting connectivity problems not specific to IPX RIP routing are described in the section "Novell IPX: Client Cannot Connect to Server on Remote LAN," earlier in this chapter.

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

Table 6-6 IPX RIP: No Connectivity over IPX RIP Router

Possible Problem	Solution
IPX RIP routing not configured or misconfigured on the router	**Step 1** Use the **show running-config** privileged EXEC command to view the router configuration. **Step 2** Check the configuration to make sure there is an **ipx routing** global configuration command entry. If there is not, enter the **ipx routing** command to enable IPX routing. Issuing the **ipx routing** command on a router automatically enables IPX RIP routing on all interfaces that have a network number assigned to them.
Missing **ipx network** commands on interface	**Step 1** Use the **show ipx interface** privileged EXEC command to view the state of all IPX interfaces. **Step 2** If the output indicates that there are no interfaces running IPX, or if an interface that should be running IPX is not, you must configure the appropriate interfaces with an IPX address. To enable IPX protocol processing on an interface, enter the **ipx network** *number* interface configuration command.

RIP timer mismatch	You can change RIP timer values changed on servers running NetWare 4.x or later. Mismatches between routers and servers can cause connectivity problems.
	Step 1 Use the **show ipx interfaces** privileged EXEC command on the router to view the state of IPX interfaces. Look for output similar to the following:
	`C4500#show ipx interface`
	`[...]`
	`Updates each 60 seconds, aging multiples RIP: 3 SAP: 3`
	`[...]`
	Compare the timer value configured on the router with that configured on Novell servers.
	Step 2 The timer values configured on servers and routers should be the same across the whole IPX network.
	Reconfigure the router or the servers to bring the timer values into conformance. On the router, use the **ipx update-time** interface configuration command to change the RIP timer interval.
	For information on changing the timer value configured on Novell servers, consult your server documentation.

Possible Problem	Solution
Router not propagating RIP updates	**Step 1** Use the **debug ipx routing** activity privileged EXEC command on the router. Look for routing updates sent by the router out each interface. **Step 2** If you do not see RIP updates being sent out the interfaces, try disabling RIP routing using the **no ipx routing** global configuration command and then reenabling it using the **ipx routing** command. Use the **show running-config** command to verify that the rest of the IPX configuration is still correct. **Step 3** If disabling and reenabling IPX does not work, try restarting the router.
Misconfigured network filters	**Step 1** Use the **show access-lists** privileged EXEC command on suspect routers to see if there are Novell IPX access lists configured. **Step 2** Use the **show running-config** privileged EXEC command to view the router configuration. See if access lists are specified in an **ipx input-network-filter** or **ipx output-network-filter** interface configuration command. **Step 3** If access lists are used by one of these commands, disable the filters using the **no ipx input-network-filter** or **no ipx output-network-filter** command. **Step 4** Check whether the client can access the server normally. If the connection is successful, one or more access list needs modification. **Step 5** To isolate the problem access list, apply one IPX filter at a time until you can no longer create connections. **Step 6** When the problem access list is isolated, examine each **access-list** statement to see if it blocks traffic from desired networks. If it does, configure explicit **permit** statements for networks that you want to be advertised normally in updates. **Step 7** After altering the access list, reenable the filter to make sure connections between the client and the server still work. Continue testing access lists until all of your filters are enabled and the client can still connect to the server.
Routes not redistributed correctly	**Step 1** Use the **show ipx route** privileged EXEC command to see the IPX routing table. **Step 2** Examine the routing table and make sure that routes have been learned by the expected protocol and from the expected interface. **Step 3** Use the **show running-config** privileged EXEC command to view the router configuration. Check each **ipx router** global configuration command entry and the associated **redistribute** commands, if any. **Step 4** Make certain that redistribution is configured between IPX RIP and the desired protocols. Make sure that all of the desired networks are specified for redistribution. **Note:** Route redistribution is enabled automatically between IPX RIP and Enhanced IGRP[1] and between IPX RIP and NLSP.[2] For detailed information on configuring route redistribution, see the *Network Protocols Configuration Guide, Part 1*.
Router not propagating SAPs	For information on troubleshooting this problem, refer to the section "IPX RIP: SAP Updates Not Propagated by Router," later in this chapter.

1. Enhanced IGRP=Enhanced Interior Gateway Routing Protocol
2. NLSP=NetWare Link Services Protocol

IPX RIP: SAP Updates Not Propagated by Router

Symptom: Novell SAP packets are not forwarded through a router running IPX RIP. Clients might be unable to connect to servers over one or more routers, or they might intermittently be able to connect.

Note Procedures for troubleshooting IPX RIP problems not specific to SAPs are described in the section "IPX RIP: No Connectivity over IPX RIP Router," earlier in this chapter.

Additional problems relating to intermittent connectivity problems are described in the section "Novell IPX: Intermittent Connectivity," later in this chapter.

Table 6-7 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 6-7 IPX RIP: SAP Updates Not Propagated by Router

Possible Problem	Solution
SAP timer mismatch	**Step 1** Use the **show running-config** privileged EXEC command to view the router configuration. Look for **ipx sap-interval** interface configuration command entries. **Step 2** On LAN interfaces, it is recommended that you use the default SAP interval of 1 minute because the interval on servers cannot be changed. To restore the default value, use the **no ipx sap-interval** command. On serial interfaces, make sure that whatever interval you configure is the same on both sides of the serial link. Use the **ipx sap-interval** interface configuration command to change the SAP interval.
Misconfigured SAP filters	**Step 1** Use the **show access-lists** privileged EXEC command on suspect routers to see if there are Novell IPX access lists configured. Use the **show running-config** privileged EXEC command to see if there are SAP filters that use any of the configured access lists. **Step 2** If SAP filters are configured, disable them by removing **ipx input-sap-filter** and **ipx output-sap-filter** interface configuration commands as appropriate (using the **no** version of the command). **Step 3** Use the **debug ipx sap activity** privileged EXEC command to see if SAP traffic is forwarded normally. The debug command output shows the server name, network number, and MAC address of SAP packets. **Step 4** If SAP information is forwarded properly by the router, a SAP filter is causing SAP updates to be dropped by the router. **Step 5** To isolate the problem SAP filter, reenable filters one at a time until SAP packets are no longer forwarded by the router. **Step 6** Change the referenced access list to allow the SAP traffic you want to be forwarded to pass through the router. Make sure that all necessary ports are configured with an explicit **permit** statement. **Step 7** Continue enabling filters one at a time and checking to see that SAP traffic is still being forwarded properly until you have verified that all filters are configured properly.

Possible Problem	Solution
Novell server not sending SAP updates	**Step 1** Use the **debug ipx sap activity** privileged EXEC command or a protocol analyzer to look for SAP updates from servers. **Step 2** If a server is not sending SAP updates, make sure the server is attached to the network and is up and running. **Step 3** Make sure the server is properly configured to send SAPs. For information on configuring your server software properly, refer to your vendor documentation.
Novell servers not processing SAP updates as quickly as router is generating them	**Step 1** Use the **show interfaces** privileged EXEC command to check for output drops. **Step 1** If there are excessive drops, use the **show ipx servers** EXEC command on the router. Compare the output of this command with the output of the **display servers** system console command on Novell servers. **Step 2** If the **display servers** output for a Novell server shows only a partial listing of the SAP entries shown by the router, the Novell servers might not be able to process SAP updates as quickly as the router is generating them. **Step 3** Use the **ipx output-sap-delay** interface configuration command to configure the delay between packets in a multipacket SAP update. Novell specifies a delay of 55 ms.

IPX Enhanced IGRP: No Connectivity over IPX Enhanced IGRP Router

Symptom: IPX Enhanced IGRP routers are blocking connections. Clients cannot connect to servers over one or more routers running IPX Enhanced IGRP.

Note Procedures for troubleshooting connectivity problems not specific to IPX Enhanced IGRP routing are described in the section "Novell IPX: Client Cannot Connect to Server on Remote LAN," earlier in this chapter.

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

Table 6-8 IPX Enhanced IGRP: No Connectivity over IPX Enhanced IGRP Router

Possible Problem	Solution
IPX Enhanced IGRP not configured or is misconfigured on the router	Unlike IPX RIP, IPX Enhanced IGRP is *not* enabled by default on all interfaces when the **ipx routing** global configuration command is issued. **Step 1** Use the **show running-config** privileged EXEC command to view the router configuration. **Step 2** Check the configuration to make sure there is an **ipx routing** global configuration command entry. This command enables IPX routing globally. **Step 3** If the command is not present, use the **ipx routing** global configuration command to enable IPX routing. **Step 4** Check the router configuration for a **ipx router eigrp** *autonomous-system-number* global configuration command and associated **ipx network** interface configuration commands. **Step 5** If these commands are not present, configure the Enhanced IGRP process and then assign it to the appropriate interfaces with the **ipx network** commands.
Missing **ipx network** command on interface	**Step 1** Use the **show ipx interface** privileged EXEC command to view the state of all IPX interfaces. **Step 2** If the output indicates that there are no interfaces running IPX, or if an interface that should be running IPX is not, you must configure the appropriate interfaces with an IPX address. To enable IPX protocol processing on an interface, enter the **ipx network** *number* interface configuration command.
IPX RIP not enabled on network with connected Novell servers	Novell servers do not understand IPX Enhanced IGRP. You must ensure that IPX RIP is enabled on interfaces connected to LAN segments with attached Novell servers. Use the **show running-config** privileged EXEC command on suspect routers to view the router configuration. Make sure that any interfaces connected to a LAN segment with attached Novell servers have IPX RIP enabled. It is not necessary to disable the other routing protocol, but running IPX Enhanced IGRP and IPX RIP on the same interface can sometimes create performance problems.

Possible Problem	Solution
Misconfigured filters	**Step 1** Use the **show access-lists** privileged EXEC command on suspect routers to see if there are Novell IPX access lists configured. **Step 2** Use the **show running-config** privileged EXEC command to view the router configuration. See if access lists are specified in an **ipx input-network-filter** or **ipx output-network-filter** interface configuration command. **Step 3** If access lists are used by one of these commands, disable the filters using the **no ipx input-network-filter** or **no ipx output-network-filter** command. **Step 4** Check whether the client can access the server normally. If the connection is successful, one or more access lists need modification. **Step 5** To isolate the problem access list, apply one IPX filter at a time until you can no longer create connections. **Step 6** When the problem access list is isolated, examine each **access-list** statement to see if it is blocking traffic from desired networks. If it is, configure explicit **permit** statements for networks that you want to be advertised normally in updates. **Step 7** After altering the access list, reenable the filter to make sure connections between the client and the server still work. Continue testing access lists until all of your filters are enabled and the client can still connect to the server.
Routes not redistributed properly	Route redistribution between IPX Enhanced IGRP autonomous systems and between Enhanced IGRP and other routing protocols is not enabled by default. You must manually configure redistribution between different autonomous systems or routing protocols. **Step 1** Use the **show running-config** privileged EXEC command on any routers that border two Enhanced IGRP autonomous systems. Look for **redistribute** *protocol* IPX-router configuration command entries. **Step 2** If the command is not present, you must enter the appropriate **redistribute** *protocol* command to allow route redistribution between different autonomous systems or routing protocols. For detailed information on configuring route redistribution, see the *Network Protocols Configuration Guide, Part 1*.
Routers not establishing neighbors properly	For information on troubleshooting this problem, see the section "IPX Enhanced IGRP: Routers Not Establishing Neighbors," later in this chapter.
Router not propagating SAPs	For information on troubleshooting this problem, refer to the section "IPX Enhanced IGRP: SAP Updates Not Propagated by Router," later in this chapter.

IPX Enhanced IGRP: Routers Not Establishing Neighbors

Symptom: IPX Enhanced IGRP routers do not establish neighbors properly. Routers that are known to be connected do not appear in the neighbor table.

Note Procedures for troubleshooting IPX Enhanced IGRP problems not specific to establishing neighbors are described in the section "IPX Enhanced IGRP: No Connectivity over IPX Enhanced IGRP Router," earlier in this chapter.

Table 6-9 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 6-9 IPX Enhanced IGRP: Routers Not Establishing Neighbors

Possible Problem	Solution	
Routers are in different autonomous systems	**Step 1**	Neighbor relationships will not be established between routers in different autonomous systems. Make sure that the routers you want to be neighbors are in the same autonomous system.
	Step 2	Use the **show running-config** privileged EXEC command to view the router configuration. Check the **ipx router eigrp** command entries to see which autonomous systems the router belongs to.
Hello or hold-time timer mismatch	**Step 1**	Use the **show running-config** privileged EXEC command on each router in the network. Look for **ipx hello-interval eigrp** and **ipx hold-time eigrp** interface configuration command entries. The values configured by these commands should be the same for all IPX routers in the network.
	Step 2	If any router has a conflicting hello interval or hold-time value, reconfigure it to conform with the rest of the routers on the network. You can return these values to their defaults with the **no ipx hello-interval eigrp** and the **no ipx hold-time interval eigrp** interface configuration commands.
Link problem	**Step 1**	Use the **show interfaces** privileged EXEC command to check if the interface is up and functioning correctly.
	Step 2	Use the **show ipx eigrp neighbors** privileged EXEC command to make sure that all Enhanced IGRP neighbors are shown in the neighbor table.
	Step 3	If not all neighbors are in the neighbor table, there might be a link problem. Refer to other chapters in this publication for information on troubleshooting specific link types.

IPX Enhanced IGRP: SAP Updates Not Propagated by Router

Symptom: Novell SAP packets are not forwarded through a router running IPX Enhanced IGRP. Clients might be unable to connect to servers over one or more routers, or they might intermittently be able to connect.

Note Procedures for troubleshooting IPX Enhanced IGRP problems not specific to SAPs are described in the section "IPX Enhanced IGRP: No Connectivity over IPX Enhanced IGRP Router," earlier in this chapter.

Table 6-10 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 6-10 IPX Enhanced IGRP: SAP Updates Not Propagated by Router

Possible Problem	Solution
Misconfigured SAP filters	**Step 1** Use the **show access-lists** privileged EXEC command on suspect routers to see if there are Novell IPX access lists configured. Use the **show running-config** privileged EXEC command to see if there are SAP filters that use any of the configured access lists. **Step 2** If SAP filters are configured, disable them by removing **ipx input-sap-filter** and **ipx output-sap-filter** interface configuration commands as appropriate (using the **no** version of the command). **Step 3** Use the **debug ipx sap activity** privileged EXEC command to see if SAP traffic is being forwarded normally. The debug command output shows the server name, network number, and MAC address of SAP packets. **Step 4** If SAP information is being forwarded properly by the router, a SAP filter is causing SAP updates to be dropped by the router. **Step 5** To isolate the problem SAP filter, reenable filters one at a time until SAP packets are no longer forwarded by the router. **Step 6** Change the referenced access list to allow the SAP traffic you want to be forwarded to pass through the router. Make sure that all necessary ports are configured with an explicit **permit** statement. **Step 7** Continue enabling filters one at a time and checking to see that SAP traffic is being forwarded properly until you have verified that all filters are configured properly.
SAP updates are being sent incrementally rather than periodically	Connectivity problems can occur when LAN interfaces are configured to send incremental (not periodic) SAP updates on segments that have attached Novell clients or servers. Incremental SAP updates are sent only when there is a change in the SAP table. **Step 1** Use the **show running-config** privileged EXEC command to view the router configuration. Look for **ipx sap-incremental eigrp** interface configuration command entries on interfaces with attached Novell clients or servers. **Step 2** If the command is present and the interface in question has attached Novell clients or servers, you must disable the **ipx sap-incremental eigrp** command. This command should be configured on an interface only if all of the nodes out that interface are Enhanced IGRP peers.

Possible Problem	Solution
Link problem	**Step 1** Use the **show interfaces** privileged EXEC command and look for drops and interface resets. **Step 2** If you see many drops or interface resets, use the **debug ipx sap activity** privileged EXEC command and then the **clear ipx eigrp neighbor** privileged EXEC command. If there is a link problem, the **debug ipx sap activity** command will not produce any output. **Step 3** Refer to the appropriate chapter elsewhere in this publication for information on troubleshooting the particular link type. For example, for serial links, refer to the "Troubleshooting Serial Line Problems" chapter.

IPX Enhanced IGRP: Router Stuck in Active Mode

Symptom: An IPX Enhanced IGRP router is stuck in Active mode. The router repeatedly sends error messages similar to the following to the console:

```
%DUAL-3-SIA: Route 3c.0800.0c00.4321 Stuck-in-Active
```

Note Occasional messages of this type are *not* a cause for concern. This is how an Enhanced IGRP router recovers if it does not receive replies to its queries from all of its neighbors. However, if these error messages occur frequently, you should investigate the problem.

For a more detailed explanation of Enhanced IGRP Active mode, see the section "Enhanced IGRP and Active/Passive Modes" later in this chapter.

Table 6-11 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 6-11 IPX Enhanced IGRP: Router Stuck in Active Mode

Possible Problem	Solution
Active timer value is misconfigured	The active timer specifies the maximum period of time that an Enhanced IGRP router will wait for replies to its queries. If the active timer value is set too low, there might not be enough time for all of the neighboring routers to send their replies to the active router. **Step 1** Check the configuration of each Enhanced IGRP router using the **show running-config** privileged EXEC command. Look for a **timers active-time** router configuration command entry. **Step 2** The value set by the **timers active-time** command should be consistent among routers in the same autonomous system. A value of 3 (3 minutes, which is the default value) is strongly recommended to allow all Enhanced IGRP neighbors to reply to queries.
Interface or other hardware problem	**Step 1** Use the **show ipx eigrp neighbors** EXEC command and examine the Uptime and Q Cnt (queue count) fields in the output. If the uptime counter is continually resetting or if the queue count is consistently high, there might be a hardware problem. **Step 2** Check the output of the stuck in Active error message. The output will indicate the general direction of the problem node, but if there are multiple nodes in that direction the problem could be in any one of them. **Step 3** Make sure the suspect router still works. Check the interfaces on the suspect router. Make sure the interface and line protocol are up and determine whether the interface is dropping packets. For more information on troubleshooting hardware, see the "Troubleshooting Hardware and Booting Problems" chapter.
Flapping route	**Step 1** Check for a flapping serial route (caused by heavy traffic load) by using the **show interfaces** privileged EXEC command. You might have a flapping route if there are a high number of resets and carrier transitions. **Step 2** If there is a flapping route, queries and replies might not be forwarded reliably. Route flapping caused by heavy traffic on a serial link can cause queries and replies to be lost, resulting in the active timer timing out. Take steps to reduce traffic on the link, or increase the bandwidth of the link. For more information about troubleshooting serial lines, refer to the "Troubleshooting Serial Line Problems" chapter.

Enhanced IGRP and Active/Passive Modes

An Enhanced IGRP router can be in either Passive or Active mode. A router is said to be passive for a network when it has an established path to the network in its routing table.

If the Enhanced IGRP router loses the connection to a network, it becomes active for that network. The router sends out queries to all of its neighbors in order to find a new route. The router remains in active mode until it has either received replies from *all* of its neighbors or until the active timer, which determines the maximum period of time a router will stay active, has expired.

If the router receives a reply from each of its neighbors, it computes the new next hop to the network and becomes passive for that network. However, if the active timer expires, the router removes any neighbors that did not reply from its neighbor table, again enters Active mode, and issues a "Stuck-in-Active" message to the console.

Novell IPX: Intermittent Connectivity

Symptom: Connectivity between clients and servers is intermittent. Clients might be able to connect some of the time, while at other times no connectivity to certain servers or networks is possible.

Table 6-12 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 6-12 Novell IPX: Intermittent Connectivity

Possible Problem	Solution
SAP timer mismatch	**Step 1** Use the **show running-config** privileged EXEC command to view the router configuration. Look for **ipx sap-interval** interface configuration command entries. **Step 2** On LAN interfaces, it is recommended that you use the default SAP interval of 1 minute because the interval on servers cannot be changed. To restore the default value, you can use the **no ipx sap-interval** command. On serial interfaces, make sure that whatever interval you configure is the same on both sides of the serial link. Use the **ipx sap-interval** interface configuration command to change the SAP interval.

RIP timer mismatch	You can change RIP timer values on servers running NetWare 4.x or later. Mismatches between routers and servers can cause connectivity problems.
	Step 1 Use the **show ipx interfaces** privileged EXEC command on the router to view the state of IPX interfaces. Look for output similar to the following:
	`C4500#show ipx interface`
	`[...]`
	`Updates each 60 seconds, aging multiples RIP: 3 SAP: 3`
	`[...]`
	Compare the timer value configured on the router with that configured on Novell servers.
	Step 2 The timer values configured on servers and routers should be the same across the entire IPX network.
	Reconfigure the router or the servers to bring the timer values into conformance. On the router, use the **ipx update-time** interface configuration command to change the RIP timer interval.
	For information on changing the timer value configured on Novell servers, consult your server documentation.

SAP updates are sent incrementally rather than periodically	In IPX Enhanced IGRP environments, problems can occur when interfaces are configured to send incremental (not periodic) SAP updates on segments that have attached Novell servers. (Incremental SAP updates are sent only when there is a change in the SAP table.) **Step 1** Use the **show running-config** privileged EXEC command to view the router configuration. Check to see if there are **ipx sap-incremental eigrp** interface configuration command entries enabled on interfaces with attached Novell clients or servers. **Step 2** If the command is present and the interface in question has attached Novell clients or servers, you must disable the **ipx sap-incremental eigrp** command. This command should be configured on an interface only if all of the nodes out that interface are Enhanced IGRP peers.

Possible Problem	Solution
Novell servers not processing SAP updates as quickly as router is generating them	**Step 1** Use the **show interfaces** privileged EXEC command to check for output drops. **Step 1** If there are excessive drops, use the **show ipx servers** EXEC command on the router. Compare the output of this command with the output of the **display servers** system console command on Novell servers. **Step 2** If the **display servers** output for a Novell server shows only a partial listing of the SAP entries shown by the router, the Novell servers might be unable to process SAP updates as quickly as the router is generating them. **Step 3** Use the **ipx output-sap-delay** interface configuration command to configure the delay between packets in a multipacket SAP update. Novell specifies a delay of 55 ms.
SAP updates dropped from hub router's output queue	Slow serial lines can cause the router to drop SAP packets before they are transmitted. **Step 1** Use the **show interfaces serial** EXEC command and examine the output queue "drops" field. A large number of dropped packets might indicate that SAP updates are being dropped before they can be transmitted across the serial link. **Step 2** Use the **show ipx servers** EXEC command on the router. Compare the output of this command with the output of the **display servers** system console command on Novell servers. **Step 3** If the **display servers** output for a Novell server shows only a partial listing of the SAP entries shown by the router, the router might be dropping SAP packets from the output queue. **Step 4** Eliminate the forwarding of any SAP updates that are not absolutely necessary. Configure filters using the **ipx input-sap-filter**, **ipx output-sap-filter**, and **ipx router-sap-filter** interface configuration commands, as appropriate. **Step 5** Increasing the output hold queue on the serial interface might also improve performance. Use the **hold-queue** *length* **out** interface configuration command to increase the output hold queue length. **Step 6** If SAP filters and increased queue lengths do not solve the problem, increase the available bandwidth if possible. Add a second serial line or obtain a single link with more available bandwidth.[1]
Router is stuck in active mode (EIGRP only)	If you consistently receive stuck in active messages about a particular network, you probably have a flapping route (typically caused by heavy traffic load). Route flapping can cause routes to come and go in the routing table, resulting in intermittent connectivity to some networks. Take steps to reduce traffic on the link, or increase the bandwidth of the link. For more information about troubleshooting serial lines, refer to the "Troubleshooting Serial Line Problems" chapter.

1. If increasing the bandwidth is not possible, buffer management might help alleviate the problem. Contact the Cisco TAC for assistance in tuning buffers.

Novell IPX: Slow Performance

Symptom: Slow network performance is experienced in a Novell IPX network.

Table 6-13 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 6-13 Novell IPX: Slow Performance

Possible Problem	Solution
Novell servers not processing SAP updates as quickly as router is generating them	**Step 1** Use the **show interfaces** privileged EXEC command to check for output drops. **Step 2** If there are excessive drops, use the **show ipx servers** EXEC command on the router. Compare the output of this command with the output of the **display servers** system console command on Novell servers. **Step 3** If the **display servers** output for a Novell server shows only a partial listing of the SAP entries shown by the router, the Novell servers might be unable to process SAP updates as quickly as the router is generating them. **Step 4** Use the **ipx output-sap-delay** interface configuration command to configure the delay between packets in a multipacket SAP update. Novell specifies a delay of 55 ms.
Periodic SAP updates are using excessive bandwidth	In an non-IPX RIP environment (such as on a serial link running Enhanced IGRP), you can reduce SAP traffic by configuring routers to send incremental rather than periodic SAP updates. Incremental SAP updates are sent only when there is a change to the SAP table. You should have incremental SAP updates enabled only on interfaces that have *no* Novell clients or servers attached. Novell clients and servers require periodic SAP updates. Use the **ipx sap-incremental eigrp** interface configuration command to enable incremental SAP updates.
IPX RIP and IPX Enhanced IGRP are enabled on the same interface	Running both IPX Enhanced IGRP and IPX RIP on the same interface is sometimes desired or required in an IPX network. However, doing so can cause performance problems in some cases by creating excess traffic and processor overhead. **Step 1** Use the **show running-config** privileged EXEC command to view the router configuration. Check the **network** router configuration commands associated with **ipx router rip** and the **ipx router eigrp** global configuration commands to see if both routing protocols are enabled on the same interface. **Step 2** If both protocols are enabled, determine whether one or the other can be disabled without affecting the proper operation of the network. If there is no need for both protocols to be running on the same interface, remove the superfluous configuration commands as appropriate.
Router is stuck in active mode (EIGRP only)	If you consistently receive stuck in active messages about a particular network, you probably have a flapping route (typically caused by heavy traffic load). Route flapping can force routers to use a less preferred route, resulting in slower performance. Take steps to reduce traffic on the link, or increase the bandwidth of the link. For more information about troubleshooting serial lines, refer to the “Troubleshooting Serial Line Problems” chapter.