



Troubleshooting Novell IPX

NetWare is a network operating system (NOS) and related support services environment created by Novell, Inc., and introduced to the market in the early 1980s. Then, networks were small and predominantly homogeneous, local-area network (LAN) workgroup communication was new, and the idea of a personal computer (PC) was just becoming popular.

Much of NetWare's networking technology was derived from Xerox Network Systems (XNS), a networking system created by Xerox Corporation in the late 1970s.

By the early 1990s, NetWare's NOS market share had risen to between 50 percent and 75 percent. With more than 500,000 NetWare networks installed worldwide and an accelerating movement to connect networks to other networks, NetWare and its supporting protocols often coexisted on the same physical channel with many other popular protocols, including TCP/IP, DECnet, and AppleTalk. Although networks today are predominately IP, there are some legacy Novel IPX traffic.

Novell Technology Basics

As an NOS environment, NetWare specifies the upper five layers of the OSI reference model. The parts of NetWare that occupy the upper five layers of the OSI model are as follows:

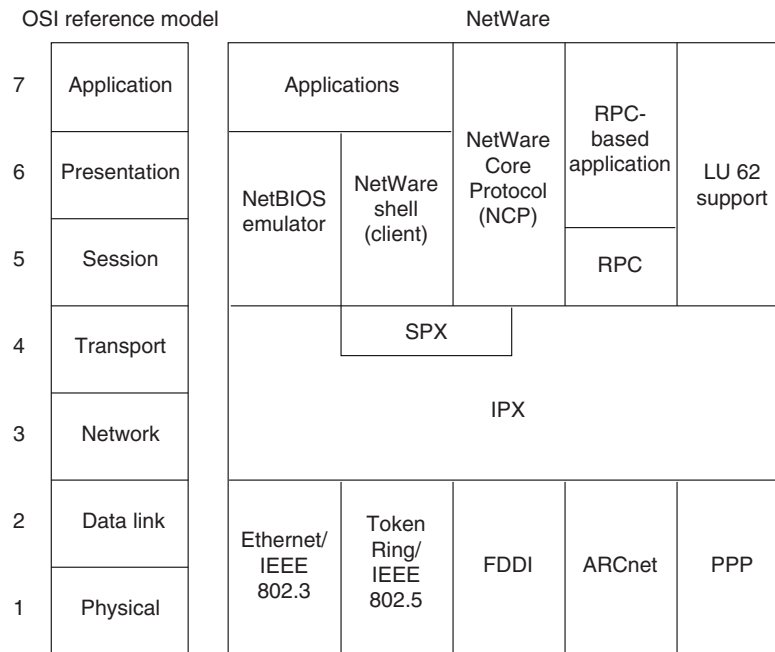
- NetWare Core Protocol (NCP)
- Service Advertisement Protocol (SAP)
- Routing Information Protocol (RIP)

NetWare provides file and printer sharing, support for various applications such as electronic mail transfer and database access, and other services. Like other NOSs, such as the network file system (NFS) from Sun Microsystems, Inc., and Windows NT from Microsoft Corporation, NetWare is based on a client/server architecture. In such architectures, clients (sometimes called workstations) request certain services such as file and printer access from servers.

Originally, NetWare clients were small PCs, whereas servers were slightly more powerful PCs. As NetWare became more popular, it was ported to other computing platforms. Currently, NetWare clients and servers can be represented by virtually any kind of computer system, from PCs to mainframes.

A primary characteristic of the client/server system is that remote access is transparent to the user. This is accomplished through remote procedure calls, a process by which a local computer program running on a client sends a procedure call to a remote server. The server executes the remote procedure call and returns the requested information to the local computer client.

Figure 8-1 illustrates a simplified view of NetWare's best-known protocols and their relationship to the OSI reference model. With appropriate drivers, NetWare can run on any media-access protocol. The figure lists those media-access protocols currently supported with NetWare drivers.

Figure 8-1 NetWare and the OSI Reference Model

Media Access

NetWare runs on Ethernet/IEEE 802.3, Token Ring/IEEE 802.5, Fiber Distributed Data Interface (FDDI), Copper Distributed Data Interface (CDDI), and ARCnet. NetWare also works over synchronous wide-area network (WAN) links using the Point-to-Point Protocol (PPP).

The Network Layer

Internetwork Packet Exchange (IPX) is Novell's original network layer protocol. When a device to be communicated with is located on a different network, IPX routes the information to the destination through any intermediate networks. Figure 8-2 shows the IPX packet format.

Figure 8-2 IPX Packet Format

Checksum	
Packet length	
Transport control	Packet type
Destination network	
Destination node	
Destination socket	
Source network	
Source node	
Source socket	
Upper-layer data	

The fields of the IPX packet are as follows:

- **Checksum**—A 16-bit field that is set to ones.
- **Packet length**—A 16-bit field that specifies the length, in bytes, of the complete IPX datagram. IPX packets can be any length, up to the media maximum transmission unit (MTU) size. There is no packet fragmentation.
- **Transport control**—An 8-bit field that indicates the number of routers that the packet has passed through. When the value of this field reaches 15, the packet is discarded under the assumption that a routing loop might be occurring. With the use of NetWare Links State Protocol (NLSP), an IPX packet can travel up to 127 hops to reach a destination.
- **Packet type**—An 8-bit field that specifies the upper-layer protocol to receive the packet's information. Two common values for this field are 5, which specifies Sequenced Packet Exchange (SPX), and 17, which specifies the NetWare Core Protocol (NCP).
- **Destination network (32-bit field), Destination node (48-bit field), and Destination socket (16-bit field)**—Fields that specify destination information.
- **Source network (32-bit field), Source node (48-bit field), and Source socket (16-bit field)**—Fields that specify source information.
- **Upper-layer data**—Information for upper-layer processes. This section of the packet is also referred to as the Higher Level Protocol Headers headers of the higher level NetWare protocols such as NCP or SPX. These headers occupy the data position of the IPX packet.

Although IPX was derived from XNS, it has several unique features. From the standpoint of routing, the encapsulation mechanisms of these two protocols represent the most important difference.

Encapsulation is the process of packaging upper-layer protocol information and data into a frame. For Ethernet, XNS uses standard Ethernet encapsulation, whereas IPX packets are encapsulated in Ethernet Version 2.0 or IEEE 802.3, without the IEEE 802.2 information that typically accompanies these frames. Figure 8-3 illustrates Ethernet, standard IEEE 802.3, and IPX encapsulation.


Note

NetWare 4.0 supports encapsulation of IPX packets in standard IEEE 802.3 frames. It also supports Subnetwork Access Protocol (SNAP) encapsulation, which extends the IEEE 802.2 headers by providing a type code similar to that defined in the Ethernet specification.

Figure 8-3 Ethernet, IEEE 802.3, and IPX Encapsulation Formats

Ethernet	Standard IEEE 802.3	IPX
Destination address	Destination address	Destination address
Source address	Source address	Source address
Type	Length	Length
Upper-layer data	802.2 header	IPX data
	802.2 data	
CRC	CRC	CRC

To route packets in an internetwork, IPX uses a dynamic routing protocol called the Routing Information Protocol (RIP). Like XNS, RIP was derived from work done at Xerox for the XNS protocol family.

In addition to the difference in encapsulation mechanisms, Novell added a protocol called the Service Advertising Protocol (SAP) to its IPX protocol family. SAP allows nodes that provide services (such as file servers and print servers) to advertise their addresses and the services that they provide.

Novell also supports IBM logical unit (LU) 6.2 network addressable units (NAUs). LU 6.2 allows peer-to-peer connectivity across IBM communication environments. Using NetWare's LU 6.2 capability, NetWare nodes can exchange information across an IBM network. NetWare packets are encapsulated within LU 6.2 packets for transit across the IBM network.

The Transport Layer

Sequenced Packet Exchange (SPX) is the most commonly used NetWare transport protocol. Novell derived this protocol from the XNS Sequenced Packet Protocol (SPP). As with the Transmission Control Protocol (TCP) and many other transport protocols, SPX is a reliable, connection-oriented protocol that supplements the datagram service provided by Layer 3 protocols.

SPX is noted by Novell's documentation as follows: "SPX (Sequenced Packet Exchange) is a protocol within IPXODI. SPX is derived from Novell's IPX using the Xerox Sequenced Packet Protocol. It enhances the IPX protocol by supervising data sent out across the network."

Novell also offers Internet Protocol (IP) support in the form of User Datagram Protocol (UDP)/IP encapsulation of other Novell packets, such as SPX/IPX packets. IPX datagrams are encapsulated inside UDP/IP headers for transport across an IP-based internetwork. NetWare 5.0 runs native IP, but the previous versions can run IP in the form mentioned previously or NetWare/IP.

Upper-Layer Protocols

NetWare supports a wide variety of upper-layer protocols, but several are somewhat more popular than others. The NetWare shell runs in clients (often called workstations in the NetWare community) and intercepts application I/O calls to determine whether they require network access for satisfaction. If they do, the NetWare shell packages the requests and sends them to lower-layer software for processing and network transmission. If they do not require network access, they are simply passed to local I/O resources. Client applications are unaware of any network access required for completion of application calls. NetWare remote procedure call (NetWare RPC) is another more general redirection mechanism supported by Novell.

NCP is a series of server routines designed to satisfy application requests coming from, for example, the NetWare shell. Services provided by NCP include file access, printer access, name management, accounting, security, and file synchronization.

NetWare also supports the Network Basic Input/Output System (NetBIOS) session layer interface specification from IBM and Microsoft. NetWare's NetBIOS emulation software allows programs written to the industry-standard NetBIOS interface to run within the NetWare system.

NetWare application layer services include NetWare Message Handling Service (NetWare MHS), Btrieve, NetWare-loadable modules (NLMs), and various IBM connectivity features. NetWare MHS is a message delivery system that provides electronic mail transport. Btrieve is Novell's implementation of the binary tree (btree) database access mechanism. NLMs are implemented as add-on modules that attach into the NetWare system. NLMs for alternate protocol stacks, communication services, database services, and many other services are currently available from Novell and third parties.

Troubleshooting Novell IPX

This section presents protocol-related troubleshooting information for Novell IPX connectivity and performance problems. It describes specific Novell IPX symptoms, the problems that are likely to cause each symptom, and the solutions to those problems.

The following sections outline the most common issues in Novell IPX networks:

- 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 Public Switched Network (PSN)
- Novell IPX: Client Cannot Connect to Server over Integrated Services Digital Network (ISDN)
- Novell NetBIOS: Applications Cannot Connect to Server over Router
- IPX RIP: No Connectivity over IPX Routing Information Protocol (RIP) Router
- IPX RIP: Service Advertisement Protocol Updates Not Propagated by Router
- IPX Enhanced IGRP: No Connectivity over IPX Enhanced Interior Gateway Routing Protocol 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 8-1 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 8-1 Novell IPX: Client Cannot Connect to Server on Same LAN

Possible Problem	Solution
Misconfigured client or server	<p>Verify 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.</p> <p>(On servers, make certain that SAPs¹ are being generated properly and that any NLMs² are loaded properly. Use the track on command to monitor routing and SAP activity.</p> <p>Check the encapsulation on clients and servers to make sure that they are not mismatched.</p> <p>For specific information on configuring your client or server, refer to the documentation provided with the device.</p>
Not enough user licenses	<p>Make sure that 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.</p>
Mismatched network numbers	<p>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.</p> <p>Watch for error messages on the system console similar to the following:</p> <ul style="list-style-type: none"> • “Router configuration error detected” • “Node address claims network x should be y” <p>These error messages indicate that a server on the LAN has a conflicting network number. <i>Node address</i> is the node address of the network card from which the incorrect address came. <i>x</i> is the network number specified in packets received from the node. <i>y</i> is the network number configured on the server generating the error.</p> <p>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.</p>

Table 8-1 Novell IPX: Client Cannot Connect to Server on Same LAN (continued)

Possible Problem	Solution
Client, server, or other hardware problem	<p>Check all NIC³ 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.</p> <p>For information on troubleshooting a client, server, or other hardware problem not related to Cisco routers, refer to the documentation provided with the hardware.</p>
Media problem	<ol style="list-style-type: none"> 1. Check all cabling and connections. Make sure that cables are not damaged and that all connections are correct and make proper contact. 2. Use the show interfaces exec command to check for input or output errors, or other indications of problems on the media. 3. If the command output shows excessive errors, use the clear interface counter privileged exec command to clear the interface counters. 4. Check the output of the show interfaces command again. If the errors are incrementing rapidly, there is probably a problem with the media. <p>For more detailed information on troubleshooting media problems, refer to the media troubleshooting chapter that covers the media type used in your network.</p>

1. SAP = Service Advertising 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. Table 8-2 outlines the problems that might cause this symptom and describes solutions to those problems.



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 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 book.

Table 8-2 Novell IPX: Client Cannot Connect to Server on Remote LAN

Possible Problem	Solution
Router interface is down.	<ol style="list-style-type: none"> 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. 2. If the interface is administratively down, use the no shutdown interface configuration command to bring the interface back up. (Q14) 3. If the interface or line protocol is down, refer to the media troubleshooting chapter that covers the media type used in your network.
Ethernet encapsulation methods are mismatched.	<ol style="list-style-type: none"> 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.) 2. Compare the encapsulation type configured on router interfaces with the encapsulation type that is being used by clients and servers. 3. If the router uses one encapsulation type but the clients and servers use a different type, then there is a mismatch. <p>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.</p>
LIPX ¹ problem has occurred.	<p>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. Without LIPX, the server checks the network number for the buffer size request packet from the client, and if the network number is different than the server’s (which means that the packet is from another network over a router), it orders clients to use 512 bytes (hard-coded) instead.</p> <p>For information on configuring LIPX, refer to the vendor documentation.</p>

Table 8-2 Novell IPX: Client Cannot Connect to Server on Remote LAN (continued)

Possible Problem	Solution
Ring speed specification mismatch has occurred.	<p>In a Token Ring environment, all devices must agree on the configured ring speed (4 or 16 Mbps), or connectivity will fail.</p> <ol style="list-style-type: none"> 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. 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 are present.	<ol style="list-style-type: none"> 1. Use the show running-config privileged exec command to examine the current configuration of each router in the path. 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 FDDI² interface card in the router. 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. 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 are present.	<p>Every network number must be unique throughout the entire Novell IPX internetwork. A duplicate network number will prevent packets from being forwarded properly.</p> <ol style="list-style-type: none"> 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. <p>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 that's using the same network number.</p> <ol style="list-style-type: none"> 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.

Table 8-2 Novell IPX: Client Cannot Connect to Server on Remote LAN (continued)

Possible Problem	Solution
Router hardware problem has occurred.	<p>Check all router ports, interface processors, and other router hardware. Make sure that cards are seated properly and that no hardware is damaged. Replace faulty or malfunctioning hardware.</p> <p>For detailed information on troubleshooting router hardware problems, refer to Chapter 3, “Troubleshooting Hardware and Booting.”</p>
Back-door bridge between segments exists.	<ol style="list-style-type: none"> 1. Use the show ipx traffic exec command on intermediate routers. Determine whether the bad hop count field is incrementing. 2. If the bad hop count counter is incrementing, use a network analyzer to look for packet loops on suspect segments. Look for RIP³ and SAP updates as well. If a back-door bridge exists, you are likely to see hop counts that increment to 16, at which time the route disappears and reappears unpredictably. 3. Look for packets from known <i>remote</i> network numbers that appear on the <i>local</i> network. Look for packets whose source address is the MAC⁴ address of the remote node instead of the MAC address of the router. 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. 5. Remove the back-door bridge to close the loop.
Routing protocol problem has occurred.	Misconfigurations and other routing protocol issues can cause connectivity and performance problems.

1. LIPX = Large Internet Packet Exchange
2. FDDI = Fiber Distributed Data Interface
3. RIP = Routing Information Protocol
4. MAC = Media Access Control

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.

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

Table 8-3 Novell IPX: Client Cannot Connect to Server over PSN

Possible Problem	Solution
Address mapping error	<ol style="list-style-type: none"> 1. Use the show running-config privileged exec command to view the configuration of the router. 2. Depending on your PSN environment, look for any x25 map ipx, frame-relay map ipx,¹ or smds static-map ipx² interface configuration command entries in the router configuration. <ul style="list-style-type: none"> • Make sure that the address mapping specified by these commands is 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 DLCI³ used to connect to the address. • For SMDS, address mapping defines static entries for SMDS remote peer routers. <p>For more information about configuring address maps, refer to the <i>Cisco IOS Wide Area Networking Configuration Guide and Wide Area Networking Command Reference</i>.</p>
Encapsulation mismatch	<ol style="list-style-type: none"> 1. Use the show interfaces privileged exec command to determine the encapsulation type being used (such as X.25, Frame Relay, or SMDS encapsulation). Look for output similar to the following: <pre>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)</pre> 2. If an encapsulation command is not present, the default is HDLC⁴ encapsulation. For PSN interconnection, you must explicitly specify the proper encapsulation type (such as encapsulation x25 for an X.25 connection). <p>Configure the proper encapsulation type, and use the show interfaces command to verify that the encapsulation type is correct.</p>
Misconfigured DLCI assignments (Frame Relay only)	<ol style="list-style-type: none"> 1. Use the show frame-relay map exec command on the hub router to see the Frame Relay map assignments currently configured. 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.

Table 8-3 Novell IPX: Client Cannot Connect to Server over PSN (continued)

Possible Problem	Solution
Misconfigured LMI ⁵ type (Frame Relay only)	<ol style="list-style-type: none"> 1. Use the debug frame-relay lmi privileged exec command to see the LMI type being used by the Frame Relay switch. 2. The LMI type is determined by your Frame Relay provider. Make sure that you use the LMI type specified by the provider.
Full Frame Relay broadcast queue (Frame Relay only)	<p>This problem is most likely to occur on the hub router in a Frame Relay hub-and-spoke topology.</p> <ol style="list-style-type: none"> 1. Use the show interfaces privileged exec command to check for dropped Frame Relay broadcast frames. 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. <p>Command syntax:</p> <p>frame-relay broadcast-queue <i>size byte-rate packet-rate</i></p> <p>Command syntax:</p> <p><i>size</i>—Number of packets to be held in the broadcast queue. The default is 64 packets.</p> <p><i>byte-rate</i>—Maximum number of bytes to be transmitted per second. The default is 256,000 bytes per second.</p> <p><i>packet-rate</i>—Maximum number of packets to be transmitted per second. The default is 36 packets per second.</p>

Table 8-3 Novell IPX: Client Cannot Connect to Server over PSN (continued)

Possible Problem	Solution
Hub router not forwarding SAPs (Frame Relay only)	<p>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, which states that an incoming packet cannot be placed on the same network interface from which it originated, preventing an infinite routing loop if a link fails.</p> <p>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 <i>Wide Area Networking Configuration Guide</i>.</p> <p>Note: Other problems 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.</p>
Missing or misconfigured multicast address (SMDS only)	<ol style="list-style-type: none"> 1. Use the show running-config privileged exec command to view the router configuration. Check for an smds multicast ipx interface configuration command entry. 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. DLCI = data-link connection identifier
3. SMDS = Switched Multimegabit Data Service
4. HDLC = High-Level Data Link Control
5. LMI = Local Management Interface

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.

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 Chapter 17, "Troubleshooting ISDN Connections."

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

Table 8-4 Novell IPX: Client Cannot Connect to Server over ISDN

Possible Problem	Solution
Static RIP and SAP statements are missing or have been misconfigured.	<ol style="list-style-type: none"> 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. <p>Both 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.</p> <ol style="list-style-type: none"> 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 <i>Cisco IOS Network Protocols Configuration Guide, Part 1</i> and <i>Network Protocols Command Reference, Part 1</i>.
Access lists specified in dialer lists have been misconfigured.	<ol style="list-style-type: none"> 1. Use the show running-config privileged exec command to view the router configuration. Check the access lists configured for use by dialer lists. 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. 3. Make sure that 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 8-5 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 8-5 Novell NetBIOS: Applications Cannot Connect to Server over Router

Possible Problem	Solution
Missing ipx type-20-propagation commands	<ol style="list-style-type: none"> 1. Use the debug ipx packet privileged exec command or a network analyzer to look for Novell packets with a specification of type 20.
Missing ipx type-20-propagation commands (continued)	<p>Caution: Exercise caution when using the debug ipx packet command. Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.</p> <ol style="list-style-type: none"> 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. 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.

Table 8-5 Novell NetBIOS: Applications Cannot Connect to Server over Router (continued)

Possible Problem	Solution
Missing ipx helper-address command	<ol style="list-style-type: none"> 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. <p>Caution: Exercise caution when using the debug ipx packet command. Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.</p> <ol style="list-style-type: none"> 2. If you see packets other than type 20, use the show running-config privileged exec command to view the router configuration. Check to see whether the ipx helper-address interface configuration command is configured on the interface to which the client is attached. 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. The following is the syntax for the ipx helper-address command: <p>ipx helper-address <i>network.node</i></p>
Missing ipx helper-address command (continued)	<p>Syntax Description:</p> <p><i>network</i>—Network on which the target IPX server resides. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of –1 indicates all-nets flooding. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter just AA.</p> <p><i>node</i>—Node number of the target Novell server. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (xxxx.xxxx.xxxx). A node number of FFFF.FFFF.FFFF matches all servers.</p>
Workstation not running NetBIOS over IPX	Make sure that your workstation is running NetBIOS over IPX, 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 8-6 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 8-6 *IPX RIP: No Connectivity over IPX RIP Router*

Possible Problem	Solution
IPX RIP routing not configured or misconfigured on the router	<ol style="list-style-type: none">1. Use the show running-config privileged exec command to view the router configuration.2. Check the configuration to make sure that there is an ipx routing global configuration command entry. If there is not, enter the ipx routing command to enable IPX routing. <p>Issuing the ipx routing command on a router automatically enables IPX RIP routing on all interfaces that have a network number assigned to them.</p>

Table 8-6 IPX RIP: No Connectivity over IPX RIP Router (continued)

Possible Problem	Solution
Missing ipx network commands on interface	<ol style="list-style-type: none"> 1. Use the show ipx interface privileged exec command to view the state of all IPX interfaces. 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. The Novell server administrator can provide the IPX network number for the segment to which your router is attached. <p>To enable IPX protocol processing on an interface, enter the ipx network number interface configuration command:</p> <pre>ipx network network [encapsulation encapsulation-type [secondary]]</pre> <p>Syntax description:</p> <ul style="list-style-type: none"> • network—Network number. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter just AA. • encapsulation encapsulation-type—(Optional) Type of encapsulation. It can be one of the following values: <ul style="list-style-type: none"> – arpa—(For Ethernet interfaces only.) Use Novell's Ethernet II encapsulation. This encapsulation is recommended for networks that handle both TCP/IP and IPX traffic. – hdlc—(For serial interfaces only.) Use HDLC encapsulation. – novell-ether—(For Ethernet interfaces only.) Use Novell's Ethernet 802.3 encapsulation. This encapsulation consists of a standard 802.3 MAC header followed directly by the IPX header with a checksum of FFFF. It is the default encapsulation used by NetWare Version 3.11. – sap—<i>For Ethernet interfaces:</i> Use Novell's Ethernet 802.2 encapsulation. This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 LLC header. This is the default encapsulation used by NetWare Version 4.0. <i>For Token Ring interfaces:</i> This encapsulation consists of a standard 802.5 MAC header followed by an 802.2 LLC header. <i>For FDDI interfaces:</i> This encapsulation consists of a standard FDDI MAC header followed by an 802.2 LLC header.

Table 8-6 IPX RIP: No Connectivity over IPX RIP Router (continued)

Possible Problem	Solution
Missing ipx network commands on interface (continued)	<ul style="list-style-type: none"> – snap—<i>For Ethernet interfaces:</i> Use Novell Ethernet Snap encapsulation. This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 SNAP LLC header. <i>For Token Ring and FDDI interfaces:</i> This encapsulation consists of a standard 802.5 or FDDI MAC header followed by an 802.2 SNAP LLC header. – secondary—(Optional) Indicates an additional network configured after the first (primary) network.
RIP timer mismatch	<p>You can change RIP timer values changed on servers running NetWare 4.x or later. Mismatches between routers and servers can cause connectivity problems.</p> <ol style="list-style-type: none"> 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: <pre>C4500#show ipx interface [...] Updates each 60 seconds, aging multiples RIP: 3 SAP: 3 [...]</pre> <p>Compare the timer value configured on the router with that configured on Novell servers.</p> <ol style="list-style-type: none"> 2. The timer values configured on servers and routers should be the same across the whole IPX network. <p>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.</p> <p>For information on changing the timer value configured on Novell servers, consult your server documentation.</p>
Router not propagating RIP updates	<ol style="list-style-type: none"> 1. Use the debug ipx routing activity privileged exec command on the router. Look for routing updates sent by the router out each interface. 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 re-enabling it using the ipx routing command. <p>Use the show running-config command to verify that the rest of the IPX configuration is still correct.</p> <ol style="list-style-type: none"> 3. If disabling and re-enabling IPX does not work, try restarting the router.

Table 8-6 IPX RIP: No Connectivity over IPX RIP Router (continued)

Possible Problem	Solution
Misconfigured network filters	<ol style="list-style-type: none"> 1. Use the show access-lists privileged exec command on suspect routers to see whether there are Novell IPX access lists configured. 2. Use the show running-config privileged exec command to view the router configuration. You can see whether access lists are specified in an ipx input-network-filter or ipx output-network-filter interface configuration command. <p>Examples:</p> <p>In the following example, access list 876 controls which networks are added to the routing table when IPX routing updates are received on Ethernet interface 1:</p> <pre>access-list 876 permit 1b interface ethernet 1 ipx input-network-filter 876</pre> <p>Routing updates for network 1b will be accepted. Routing updates for all other networks are implicitly denied and are not added to the routing table.</p> <p>The following example is a variation of the preceding that explicitly denies network 1a and explicitly allows updates for all other networks:</p> <pre>access-list 876 deny 1a access-list 876 permit -1</pre> <ol style="list-style-type: none"> 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 commands. 4. Check whether the client can access the server normally. If the connection is successful, one or more access list needs modification. 5. To isolate the problem access list, apply one IPX filter at a time until you can no longer create connections. 6. When the problem access list is isolated, examine each access-list statement to see whether it blocks traffic from desired networks. If it does, configure explicit permit statements for networks that you want to be advertised normally in updates. 7. After altering the access list, re-enable the filter to make sure that connections between the client and the server still work. Continue testing access lists until all your filters are enabled and the client can still connect to the server.

Table 8-6 IPX RIP: No Connectivity over IPX RIP Router (continued)

Possible Problem	Solution
Routes not redistributed correctly Routes not redistributed correctly	<ol style="list-style-type: none"> 1. Use the show ipx route privileged exec command to see the IPX routing table. 2. Examine the routing table and make sure that routes have been learned by the expected protocol and from the expected interface. 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. 4. Make certain that redistribution is configured between IPX RIP and the desired protocols. Make sure that all the desired networks are specified for redistribution. <p>Note: Route redistribution is enabled automatically between IPX RIP and Enhanced IGRP,¹ and between IPX RIP and NLSP.²</p> <p>For detailed information on configuring route redistribution, see the <i>Network Protocols Configuration Guide, Part 1</i>.</p>
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 incapable of connecting to servers over one or more routers, or they might intermittently be capable of connecting.



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

Table 8-7 IPX RIP: SAP Updates Not Propagated by Router

Possible Problem	Solution
SAP timer mismatch has occurred.	<ol style="list-style-type: none"> 1. Use the show running-config privileged exec command to view the router configuration. Look for ipx sap-interval interface configuration command entries. Example: In the following example, SAP updates are sent (and expected) on serial interface 0 every 5 minutes: <pre>interface serial 0 ipx sap-interval 5</pre> 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. The following is the syntax for the ipx sap-interval command: ipx sap-interval <i>minutes</i> no ipx sap-interval Syntax description: <i>minutes</i>—Interval, in minutes, between SAP updates sent by the communication server. The default value is 1 minute. If minutes is 0, periodic updates are never sent. 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.
SAP filters have been misconfigured.	<ol style="list-style-type: none"> 1. Use the show access-lists privileged exec command on suspect routers to see whether there are Novell IPX access lists configured. Use the show running-config privileged exec command to see whether there are SAP filters that use any of the configured access lists. At the end of this chapter is a list of Novell SAPs that includes the SAP description and hex and decimal values. 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). 3. Use the debug ipx sap activity privileged exec command to see whether SAP traffic is forwarded normally. The debug command output shows the server name, network number, and MAC address of SAP packets.

Table 8-7 IPX RIP: SAP Updates Not Propagated by Router (continued)

Possible Problem	Solution
SAP filters have been misconfigured. (continued)	<p>Caution: Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.</p> <ol style="list-style-type: none"> 4. If SAP information is forwarded properly by the router, a SAP filter is causing SAP updates to be dropped by the router. 5. To isolate the problem SAP filter, re-enable filters one at a time until SAP packets are no longer forwarded by the router. 6. Change the referenced access list to allow the SAP traffic that you want to be forwarded to pass through the router. Make sure that all necessary ports are configured with an explicit permit statement. 7. Continue enabling filters one at a time, checking to see that SAP traffic is still being forwarded properly until you have verified that all filters are configured properly.

Table 8-7 IPX RIP: SAP Updates Not Propagated by Router (continued)

Possible Problem	Solution
Novell server is not sending SAP updates.	<ol style="list-style-type: none"> 1. Use the debug ipx sap activity privileged exec command or a protocol analyzer to look for SAP updates from servers. <p>Caution: Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.</p> <ol style="list-style-type: none"> 2. If a server is not sending SAP updates, make sure that the server is attached to the network and is up and running. 3. Make sure that the server is properly configured to send SAPs. For information on configuring your server software properly, refer to your vendor documentation.
Novell servers are not processing SAP updates as quickly as the router is generating them.	<ol style="list-style-type: none"> 1. Use the show interfaces privileged exec command to check for output drops. 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. 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 not be capable of processing SAP updates as quickly as the router is generating them. 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. <p>The following is the syntax for the ipx output-sap-delay command:</p> <p>ipx output-sap-delay <i>delay</i></p> <p>Syntax description:</p> <ul style="list-style-type: none"> • <i>delay</i>—Delay, in milliseconds, between packets in a multiple-packet SAP update.

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

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

Possible Problem	Solution
IPX Enhanced IGRP is not configured or is misconfigured on the router.	<p>Unlike IPX RIP, IPX Enhanced IGRP is <i>not</i> enabled by default on all interfaces when the ipx routing global configuration command is issued.</p> <ol style="list-style-type: none"> 1. Use the show running-config privileged exec command to view the router configuration. 2. Check the configuration to make sure that there is an ipx routing global configuration command entry. This command enables IPX routing globally. 3. If the command is not present, use the ipx routing global configuration command to enable IPX routing. The following is the syntax for the ipx routing command: ipx routing [node] Syntax description: <ul style="list-style-type: none"> • <i>node</i>—(Optional) Node number of the router. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (xxxx.xxxx.xxxx). It must not be a multicast address. <p>If you omit <i>node</i>, the router uses the hardware MAC address currently assigned to it as its node address. This is the MAC address of the first Ethernet, Token Ring, or FDDI interface card. If no satisfactory interfaces are present in the router (for example, there are only serial interfaces), you must specify <i>node</i>.</p> 4. Check the router configuration for an ipx router eigrp autonomous-system-number global configuration command and associated ipx network interface configuration commands. 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. <p>The following example enables RIP on networks 1 and 2, and Enhanced IGRP on network 1:</p> <pre> ipx routing ! interface ethernet 0 ipx network 1 ! interface ethernet 1 ipx network 2 ! ipx router eigrp 100 network 1 </pre>

continues

Table 8-8 IPX Enhanced IGRP: No Connectivity over IPX Enhanced IGRP Router (continued)

Possible Problem	Solution
The ipx network command is missing on the interface.	<ol style="list-style-type: none"> 1. Use the show ipx interface privileged exec command to view the state of all IPX interfaces. 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. <p>To enable IPX protocol processing on an interface, enter the ipx network number interface configuration command.</p>
IPX RIP is not enabled on the network with connected Novell servers.	<p>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.</p> <p>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.</p> <p>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.</p>
Filters have been misconfigured.	<ol style="list-style-type: none"> 1. Use the show access-lists privileged exec command on suspect routers to see whether there are Novell IPX access lists configured. 2. Use the show running-config privileged exec command to view the router configuration. See whether access lists are specified in an ipx input-network-filter or ipx output-network-filter interface configuration command. 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 commands. 4. Check whether the client can access the server normally. If the connection is successful, one or more access lists need modification. 5. To isolate the problem access list, apply one IPX filter at a time until you can no longer create connections.
Filters have been misconfigured. (continued)	<ol style="list-style-type: none"> 6. When the problem access list is isolated, examine each access-list statement to see whether 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. 7. After altering the access list, re-enable the filter to make sure that connections between the client and the server still work. Continue testing access lists until all your filters are enabled and the client can still connect to the server.

Table 8-8 IPX Enhanced IGRP: No Connectivity over IPX Enhanced IGRP Router (continued)

Possible Problem	Solution
Routes are not redistributed properly.	<p>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.</p> <ol style="list-style-type: none"> 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. 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. <p>For detailed information on configuring route redistribution, see the <i>Network Protocols Configuration Guide, Part 1</i>.</p>
Routers are not establishing neighbors properly.	For information on troubleshooting this problem, see the section “IPX Enhanced IGRP: Routers Not Establishing Neighbors,” next.
Router are 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 8-9 outlines the problems that might cause this symptom and describes solutions to those problems.

Table 8-9 IPX Enhanced IGRP: Routers Not Establishing Neighbors

Possible Problem	Solution
Routers are in different autonomous systems.	<ol style="list-style-type: none"> 1. Neighbor relationships will not be established between routers in different autonomous systems. Make sure that the routers that you want to be neighbors are in the same autonomous system. 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 has occurred.	<ol style="list-style-type: none"> 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. 2. If any router has a conflicting hello interval or hold-time value, reconfigure it to conform to the rest of the routers on the network. You can return these values to their defaults with the no ipx hello-interval eigrp and no ipx hold-time interval eigrp interface configuration commands.
Link problem has occurred.	<ol style="list-style-type: none"> 1. Use the show interfaces privileged exec command to check whether the interface is up and functioning correctly. The following is sample output from the show interfaces command: <pre>Router#show interface fastethernet1/0 FastEthernet1/0 is up, line protocol is up Hardware is cyBus FastEthernet Interface, address is 0010.5498.d020 (bia 0010.5498.d020) Internet address is 210.84.3.33/24 MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 230/255, load 1/255 Encapsulation ARPA, loopback not set, keepalive set (10 sec), hdx, 100BaseTX/FX</pre> 2. Use the show ipx eigrp neighbors privileged exec command to make sure that all Enhanced IGRP neighbors are shown in the neighbor table. 3. If not all neighbors are in the neighbor table, there might be a link problem. Refer to other chapters in this book 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 incapable of connecting to servers over one or more routers, or they might connect only intermittently.

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

Table 8-10 IPX Enhanced IGRP: SAP Updates Not Propagated by Router

Possible Problem	Solution
SAP filters have been misconfigured.	<ol style="list-style-type: none"> 1. Use the show access-lists privileged exec command on suspect routers to see whether there are Novell IPX access lists configured. Use the show running-config privileged exec command to see whether there are SAP filters that use any of the configured access lists. At the end of this chapter is a list of Novell SAPs that includes the SAP description and hex and decimal values. 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). 3. Use the debug ipx sap activity privileged exec command to see whether SAP traffic is being forwarded normally. The debug command output shows the server name, network number, and MAC address of SAP packets. <p>Caution: Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.</p> <ol style="list-style-type: none"> 4. If SAP information is being forwarded properly by the router, a SAP filter is causing SAP updates to be dropped by the router.
SAP filters have been misconfigured. (continued)	<ol style="list-style-type: none"> 5. To isolate the problem SAP filter, re-enable filters one at a time until SAP packets are no longer forwarded by the router. 6. Change the referenced access list to allow the SAP traffic that you want to be forwarded to pass through the router. Make sure that all necessary ports are configured with an explicit permit statement. 7. Continue enabling filters one at a time, checking to see that SAP traffic is being forwarded properly until you have verified that all filters are configured properly.

Table 8-10 IPX Enhanced IGRP: SAP Updates Not Propagated by Router (continued)

Possible Problem	Solution
SAP updates are being sent incrementally rather than periodically.	<p>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.</p> <ol style="list-style-type: none">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.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 the nodes attached to that interface are Enhanced IGRP peers.

Table 8-10 IPX Enhanced IGRP: SAP Updates Not Propagated by Router (continued)

Possible Problem	Solution
Link problem has occurred.	<p>1. Use the show interfaces privileged exec command, and look for drops and interface resets.</p> <p>The following is sample output from the show interfaces command:</p> <pre>Router#show interface fastethernet 1/0 FastEthernet1/0 is up, line protocol is up Hardware is cyBus FastEthernet Interface, address is 0010.5498.d020 (bia 0010. 5498.d020) Internet address is 208.84.3.33/24 MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255 Encapsulation ARPA, loopback not set, keepalive set (10 sec), hdx, 100BaseTX/FX ARP type: ARPA, ARP Timeout 04:00:00 Last input 00:00:07, output 00:00:07, output hang never Last clearing of "show interface" counters never Queueing strategy: fifo Output queue 0/40, 0 drops; input queue 0/75, 0 drops</pre>
Link problem has occurred. (continued)	<p>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.</p> <p>Caution: Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.</p> <p>If there is a link problem, the debug ipx sap activity command will not produce any output.</p> <p>3. Refer to the appropriate chapter elsewhere in this book for information on troubleshooting the particular link type. For example, for serial links, refer to Chapter 15, "Troubleshooting Serial Lines."</p>

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

Table 8-11 IPX Enhanced IGRP: Router Stuck in Active Mode

Possible Problem	Solution
Active timer value is misconfigured.	<ol style="list-style-type: none">1. 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 the neighboring routers to send their replies to the active router. A value of 3 (3 minutes, which is the default value) is strongly recommended to allow all Enhanced IGRP neighbors to reply to queries.2. 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.3. 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.

Table 8-11 IPX Enhanced IGRP: Router Stuck in Active Mode (continued)

Possible Problem	Solution
Interface or other hardware problem has occurred.	<ol style="list-style-type: none"> Use the show ipx eigrp neighbors exec command, and examine the Uptime and Q Cnt (queue count) fields in the output. The following is sample output from the show ipx eigrp neighbors command: <pre>Router# show ipx eigrp neighbors IPX EIGRP Neighbors for process 200 H Address Interface Hold Uptime Q Seq SRTT RTO (secs) (h:m:s) Cnt Num (ms) (ms) 6 90.0000.0c02.096e Tunnel44444 13 0:30:57 0 21 9 20 5 80.0000.0c02.34f2 Fddi0 12 0:31:17 0 62 14 28 4 83.5500.2000.a83c TokenRing2 13 0:32:36 0 626 16 32 3 98.0000.3040.a6b0 TokenRing1 12 0:32:37 0 43 9 20 2 80.0000.0c08.cbf9 Fddi0 12 0:32:37 0 624 19 38 1 85.aa00.0400.153c Ethernet2 12 0:32:37 0 627 15 30 0 82.0000.0c03.4d4b Hssi0 12 0:32:38 0 629 12 24</pre> <p>If the uptime counter is continually resetting, or if the queue count is consistently high, there might be a hardware problem.</p> Check the output of the “Stuck-in-Active” error message. The output indicates 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. Make sure that the suspect router still works. Check the interfaces on the suspect router. Make sure that the interface and line protocol are up, and determine whether the interface is dropping packets. For more information on troubleshooting hardware, see Chapter 3.

Table 8-11 IPX Enhanced IGRP: Router Stuck in Active Mode (continued)

Possible Problem	Solution
Flapping route has occurred.	<ol style="list-style-type: none"> 1. Check for a flapping serial route (caused by heavy traffic load) by using the show interfaces privileged exec command. Flapping is a routing problem in which an advertised route between two nodes alternates (flaps) back and forth between two paths due to a network problem that causes intermittent interface failures. You might have a flapping route if there are large numbers of resets and carrier transitions. 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. <p>Take steps to reduce traffic on the link, or increase the bandwidth of the link.</p> <p>For more information about troubleshooting serial lines, refer to Chapter 15.</p>

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. The route is in an active state when a router is undergoing a route recomputation. If there are always feasible successors, a route never has to go into active state and avoids a route recomputation.

If the Enhanced IGRP router loses the connection to a network, it becomes active for that network. The router sends out queries to all its neighbors to find a new route. The router remains in active mode until either it has received replies from all its neighbors or 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 capable of connecting some of the time, but at other times no connectivity to certain servers or networks is possible.

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

Table 8-12 Novell IPX: Intermittent Connectivity

Possible Problem	Solution
SAP timer mismatch has occurred.	<ol style="list-style-type: none"> 1. Use the show running-config privileged exec command to view the router configuration. Look for ipx sap-interval interface configuration command entries. 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. <p>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.</p>
RIP timer mismatch has occurred.	<p>You can change RIP timer values on servers running NetWare 4.x or later. Mismatches between routers and servers can cause connectivity problems.</p> <ol style="list-style-type: none"> 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: <pre> C4500#show ipx interface [...] Updates each 60 seconds, aging multiples RIP: 3 SAP: 3 [...] </pre> <p>Compare the timer value configured on the router with that configured on Novell servers.</p> <ol style="list-style-type: none"> 2. The timer values configured on servers and routers should be the same across the entire IPX network. <p>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.</p> <p>For information on changing the timer value configured on Novell servers, consult your server documentation.</p>

Table 8-12 Novell IPX: Intermittent Connectivity (continued)

Possible Problem	Solution
SAP updates are sent incrementally rather than periodically.	<p>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.)</p> <ol style="list-style-type: none"> 1. Use the show running-config privileged exec command to view the router configuration. Check to see whether there are ipx sap-incremental eigrp interface configuration command entries enabled on interfaces with attached Novell clients or servers. 2. If the incremental command is present and the interface in question has attached Novell clients or servers, you must disable the ipx sap-incremental eigrp command by using the no version of the command. This command should be configured on an interface only if all the nodes attached to that interface are Enhanced IGRP peers.
Novell servers not processing SAP updates as quickly as the router is generating them.	<ol style="list-style-type: none"> 1. Use the show interfaces privileged exec command to check for output drops. 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. 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 incapable of processing SAP updates as quickly as the router is generating them. 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.

continues

Table 8-12 Novell IPX: Intermittent Connectivity (continued)

Possible Problem	Solution
SAP updates are dropped from the hub router's output queue.	<p>Slow serial lines can cause the router to drop SAP packets before they are transmitted.</p> <ol style="list-style-type: none"> 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. 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. 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. 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. 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. The default output hold-queue limit is 100 packets. The general rule when using the hold-queue command is to use a small output hold-queue limit for slow links. This approach prevents storing packets at a rate that exceeds the transmission capability of the link. For fast links, use a large output hold-queue limit. A fast link may be busy for a short time (and thus require the hold queue), but it can empty the output hold queue quickly when capacity returns. 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

Table 8-12 Novell IPX: Intermittent Connectivity (continued)

Possible Problem	Solution
Router is stuck in active mode (EIGRP only).	<p>If you consistently receive “Stuck-in-Active” messages about a particular network, you probably have a flapping route (typically caused by heavy traffic load).</p> <p>Route flapping can cause routes to come and go in the routing table, resulting in intermittent connectivity to some networks.</p> <p>Take steps to reduce traffic on the link, or increase the bandwidth of the link.</p> <p>For more information about troubleshooting serial lines, refer to Chapter 15.</p>

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

Novell IPX: Slow Performance

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

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

Table 8-13 Novell IPX: Slow Performance

Possible Problem	Solution
Novell servers are not processing SAP updates as quickly as the router is generating them.	<ol style="list-style-type: none"> 1. Use the show interfaces privileged exec command to check for output drops. 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. 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 incapable of processing SAP updates as quickly as the router is generating them. 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.	<p>In a 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.</p> <p>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.</p> <p>Use the ipx sap-incremental eigrp interface configuration command to enable incremental SAP updates.</p>

Table 8-13 Novell IPX: Slow Performance (continued)

Possible Problem	Solution
IPX RIP and IPX Enhanced IGRP are enabled on the same interface.	<p>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.</p> <ol style="list-style-type: none"> 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 whether both routing protocols are enabled on the same interface. 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).	<p>If you consistently receive “Stuck-in-Active” messages about a particular network, you probably have a flapping route (typically caused by heavy traffic load).</p> <p>Route flapping can force routers to use a less preferred route, resulting in slower performance.</p> <p>Take steps to reduce traffic on the link, or increase the bandwidth of the link.</p> <p>For more information about troubleshooting serial lines, refer to Chapter 15.</p>

Novell SAPs

The list of Novell SAPs in Table 8-14 is contributed unverified information from various sources. Novell, in an official capacity, does not and has not provided any of this information.

Table 8-14 Novell SAPs, Their Descriptions, and Their Decimal and Hex Values

Decimal	Hex	SAP Description
0	0000	Unknown
1	0001	User
2	0002	User Group
3	0003	Print Queue or Print Group
4	0004	File Server (SLIST source)
5	0005	Job Server
6	0006	Gateway

Table 8-14 Novell SAPs, Their Descriptions, and Their Decimal and Hex Values (continued)

Decimal	Hex	SAP Description
7	0007	Print Server or Silent Print Server
8	0008	Archive Queue
9	0009	Archive Server
10	000a	Job Queue
11	000b	Administration
15	000F	Novell TI-RPC
23	0017	Diagnostics
32	0020	NetBIOS
33	0021	NAS SNA Gateway
35	0023	NACS Async Gateway or Asynchronous Gateway
36	0024	Remote Bridge or Routing Service
38	0026	Bridge Server or Asynchronous Bridge Server
39	0027	TCP/IP Gateway Server
40	0028	Point to Point (Eicon) X.25 Bridge Server
41	0029	Eicon 3270 Gateway
42	002a	CHI Corp
44	002c	PC Chalkboard
45	002d	Time Synchronization Server or Asynchronous Timer
46	002e	ARCserve 5.0/Palindrome Backup Director 4.x (PDB4)
69	0045	DI3270 Gateway
71	0047	Advertising Print Server
74	004a	NetBlazer Modems
75	004b	Btrieve VAP/NLM 5.0
76	004c	Netware SQL VAP/NLM Server
77	004d	Xtree Network Version Netware XTree
80	0050	Btrieve VAP 4.11
82	0052	QuickLink (Cubix)
83	0053	Print Queue User
88	0058	Multipoint X.25 Eicon Router
96	0060	STLB/NLM
100	0064	ARCserve
102	0066	ARCserve 3.0
114	0072	WAN Copy Utility
122	007a	TES-Netware for VMS
146	0092	WATCOM Debugger or Emerald Tape Backup Server
149	0095	DDA OBGYN

Table 8-14 Novell SAPs, Their Descriptions, and Their Decimal and Hex Values (continued)

Decimal	Hex	SAP Description
152	0098	Netware Access Server (Asynchronous gateway)
154	009a	Netware for VMS II or Named Pipe Server
155	009b	Netware Access Server
158	009e	Portable Netware Server or SunLink NVT
161	00a1	Powerchute APC UPS NLM
170	00aa	LAWserve
172	00ac	Compaq IDA Status Monitor
256	0100	PIPE STAIL
258	0102	LAN Protect Bindery
259	0103	Oracle DataBase Server
263	0107	Netware 386 or RSPX Remote Console
271	010f	Novell SNA Gateway
273	0111	Test Server
274	0112	Print Server (HP)
276	0114	CSA MUX (f/Communications Executive)
277	0115	CSA LCA (f/Communications Executive)
278	0116	CSA CM (f/Communications Executive)
279	0117	CSA SMA (f/Communications Executive)
280	0118	CSA DBA (f/Communications Executive)
281	0119	CSA NMA (f/Communications Executive)
282	011a	CSA SSA (f/Communications Executive)
283	011b	CSA STATUS (f/Communications Executive)
286	011e	CSA APPC (f/Communications Executive)
294	0126	SNA TEST SSA Profile
298	012a	CSA TRACE (f/Communications Executive)
299	012b	Netware for SAA
301	012e	IKARUS virus scan utility
304	0130	Communications Executive
307	0133	NNS Domain Server or Netware Naming Services Domain
309	0135	Netware Naming Services Profile
311	0137	Netware 386 Print Queue or NNS Print Queue
321	0141	LAN Spool Server (Vap, Intel)
338	0152	IRMALAN Gateway
340	0154	Named Pipe Server
358	0166	NetWare Management
360	0168	Intel PICKIT Comm Server or Intel CAS Talk Server

Table 8-14 Novell SAPs, Their Descriptions, and Their Decimal and Hex Values (continued)

Decimal	Hex	SAP Description
369	0171	Unknown
371	0173	Compaq
372	0174	Compaq SNMP Agent
373	0175	Compaq
384	0180	XTree Server or XTree Tools
394	018A	Unknown Running on a Novell Server
432	01b0	GARP Gateway (net research)
433	01b1	Binfview (Lan Support Group)
447	01bf	Intel LanDesk Manager
458	01ca	AXTEC
459	01cb	Shiva NetModem/E
460	01cc	Shiva LanRover/E
461	01cd	Shiva LanRover/T
472	01d8	Castelle FAXPress Server
474	01da	Castelle LANPress Print Server
476	01dc	Castille FAX/Xerox 7033 Fax Server/Excel Lan Fax
496	01f0	LEGATO
501	01f5	LEGATO
563	0233	NMS Agent or Netware Management Agent
567	0237	NMS IPX Discovery or LANtern Read/Write Channel
568	0238	NMS IP Discovery or LANtern Trap/Alarm Channel
570	023a	LABtern
572	023c	MAVERICK
574	023e	Unknown Running on a Novell Server
575	023f	Used by 11 various Novell Servers/Novell SMDR
590	024e	NetWare connect
618	026a	Network Management Service (NMS) Console
619	026b	Time Synchronization Server (Netware 4.x)
632	0278	Directory Server (Netware 4.x)
989	03dd	Banyan ENS for Netware Client NLM
772	0304	Novell SAA Gateway
776	0308	COM or VERMED 1
778	030a	Galacticomm's Worldgroup Server
780	030c	Intel Netport 2 or HP JetDirect or HP Quicksilver

Table 8-14 Novell SAPs, Their Descriptions, and Their Decimal and Hex Values (continued)

Decimal	Hex	SAP Description
800	0320	Attachmate Gateway
807	0327	Microsoft Diagnostics
808	0328	WATCOM SQL server
821	0335	MultiTech Systems Multisynch Comm Server
835	2101	Performance Technology Instant Internet
853	0355	Arcada Backup Exec
858	0358	MSLCD1
865	0361	NETINELO
894	037e	Twelve Novell file servers in the PC3M family
895	037f	Virusafe Notify
902	0386	HP Bridge
903	0387	HP Hub
916	0394	NetWare SAA Gateway
923	039b	Lotus Notes
951	03b7	Certus Anti Virus NLM
964	03c4	ARCserve 4.0 (Cheyenne)
967	03c7	LANspool 3.5 (Intel)
983	03d7	Lexmark printer server (type 4033-011)
984	03d8	Lexmark XLE printer server (type 4033-301)
990	03de	Gupta Sequel Base Server or NetWare SQL
993	03e1	Univel Unixware
996	03e4	Univel Unixware
1020	03fc	Intel Netport
1021	03fd	Print Server Queue
1196	04ac	On-Time Scheduler NLM
1034	040A	ipnServer Running on a Novell Server
1035	040B	Unknown
1037	040D	LVERRMAN Running on a Novell Server
1038	040E	LVLIC Running on a Novell Server
1040	0410	Unknown <i>continues</i> Running on a Novell Server
1044	0414	Kyocera
1065	0429	Site Lock Virus (Brightworks)

Table 8-14 Novell SAPs, Their Descriptions, and Their Decimal and Hex Values (continued)

Decimal	Hex	SAP Description
1074	0432	UFHELP R
1075	0433	Synoptics 281x Advanced SNMP Agent
1092	0444	Microsoft NT SNA Server
1096	0448	Oracle
1100	044c	ARCserve 5.01
1111	0457	Canon GP55 Running on a Canon GP55 network printer
1114	045a	QMS Printers
1115	045b	Dell SCSI Array (DSA) Monitor
1169	0491	NetBlazer Modems
1200	04b0	CD-Net (Meridian)
1217	04C1	Unknown
1299	0513	Emulux NQA Something from Emulex
1312	0520	Site lock checks
1321	0529	Site Lock Checks (Brightworks)
1325	052d	Citrix OS/2 App Server
1343	0535	Tektronix
1344	0536	Milan
1387	056b	IBM 8235 modem server
1388	056c	Shiva LanRover/E PLUS
1389	056d	Shiva LanRover/T PLUS
1408	0580	McAfee's NetShield anti-virus
1466	05B A	Compatible Systems Routers
1569	0621	IBM AntiVirus NLM
1571	0623	Unknown Running on a Novell Server
1900	076C	Xerox
1947	079b	Shiva LanRover/E 115
1958	079c	Shiva LanRover/T 115
2154	086a	ISSC collector NLMs
2175	087f	ISSC DAS agent for AIX
2857	0b29	Site Lock
3113	0c29	Site Lock Applications
3116	0c2c	Licensing Server

Table 8-14 Novell SAPs, Their Descriptions, and Their Decimal and Hex Values (continued)

Decimal	Hex	SAP Description
9088	2380	LAI Site Lock
9100	238c	Meeting Maker
18440	4808	Site Lock Server or Site Lock Metering VAP/NLM
21845	5555	Site Lock User
25362	6312	Tapeware
28416	6f00	Rabbit Gateway (3270)
30467	7703	MODEM
32770	8002	NetPort Printers (Intel) or LANport
32776	8008	WordPerfect Network Version
34238	85BE	Cisco Enhanced Interior Routing Protocol (EIGRP)
34952	8888	WordPerfect Network Version or Quick Network Management
36864	9000	McAfee's NetShield antivirus
38404	9604	CSA-NT_MON
46760	b6a8	Ocean Isle Reachout Remote Control
61727	f11f	Site Lock Metering VAP/NLM
61951	f1ff	Site Lock
62723	F503	SCA-NT
64507	fbfb	TopCall III fax server
65535	ffff	Any Service or Wildcard

