CHAPTER 7

Designing DDR Internetworks

Dial-on-demand routing (DDR) provides network connections across Public Switched Telephone Networks (PSTNs). Traditionally, PSTN connections have been dedicated leased lines. DDR provides low-volume, periodic network connections, allowing on-demand services and decreasing network costs. In traditional routing, a router examines packets for a destination address, looks up the address in its routing table, selects an interface through which the packets can be transmitted, and then sends the packets to the destination.

With Software Release 10.0, DDR is supported for IP, Novell IPX, and AppleTalk internetworks. DDR also supports single destination transparent bridging. DDR can be used over synchronous serial interfaces, Integrated Services Digital Network (ISDN) interfaces, or asynchronous serial interfaces. V.25bis and DTR dialing are used for Switched 56 CSU/DSUs, ISDN terminal adapters (TAs), or synchronous modems. Asynchronous serial lines are available on the auxiliary port on Cisco routers and on Cisco communication servers for connections to asynchronous modems. DDR is supported over ISDN using the Basic Rate Interface (BRI). Cisco routers that run Cisco Internetworking Operating System (Cisco IOS) 10.2, and have T1 channelized interfaces, support the ISDN Primary Rate Interface (PRI).

To establish a DDR connection, a router goes through the following steps:

1. Determines that there is a route to the destination.
2. Locates the DDR interface to that destination.
3. Checks the DDR interface to see if it is connected to the destination.
4. Determines if the packet is *interesting* (permitted by access list) or *uninteresting* (denied by access list). If the packet is uninteresting and there is no connection established, the packet is dropped. If the packet is uninteresting, but a connection is already established to the specified destination, the packet is sent across the connection. If the packet is interesting, it is sent and the idle timer is reset. If the packet is interesting and there is no connection, the router attempts to establish a connection.

Note This design guide assumes that the reader is familiar with DDR and terms associated with it. For an in-depth case study that contains several scenarios with detailed configuration examples illustrating DDR over IP internetworks, see Chapter 2, “Dial-on-Demand Routing” in the Cisco publication *Internetwork Case Studies*. This case study explains the flow of traffic through the router in a DDR environment in detail.

When designing DDR internetworks, ask the following questions:

- What topology is to be used?

  Three basic topologies are used with DDR networks: point-to-point, hub and spoke, and fully meshed. Addressing and security are two issues that affect your choice of topology.

- What media is to be used?

  Media choices include asynchronous serial, synchronous serial, and ISDN. This choice affects how packets are sent.

- Where are the packets going?

  To define where packets are sent, configure static routes, zones, and services. Static routes or zones are critical, because dynamic routing information is sent only after a DDR connection has been established. Static services ensure that only specified service advertisements will establish a DDR connection.

- How are the packets sent?

  To determine how packets reach their destination, configure dialer interfaces and map addresses to telephone numbers.

- When should the router connect?

  Interesting packets will establish DDR connections. To avoid unwanted DDR connections, configure packets to be uninteresting by denying packets through access lists. Packet types you may want to configure as uninteresting are regular routing updates, service advertisements, and serialization packets. You can also eliminate AppleTalk broadcasts and spoof IPX watchdog packets to avoid unwanted connections.

The guidelines and suggestions that follow can help you construct scalable, DDR internetworks that balance performance, fault tolerance, and cost.

DDR Topology Design

You can adopt one of three basic topologies for a DDR internetwork:

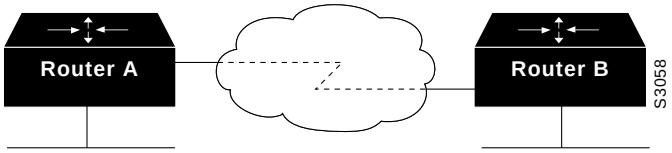
- Point-to-Point
- Hub and Spoke
- Fully Meshed

In each topology, consider whether the local or remote sites are set to answer calls, place calls, or both.

Point-to-Point

In a simple point-to-point topology, two sites are connected to each other. Each site has a dialer interface and maps the other site's address to a telephone number. If load sharing is desired, more than one interface can be configured for bandwidth on demand capability (see Figure 7-1).

Figure 7-1 Point-to-Point Topology

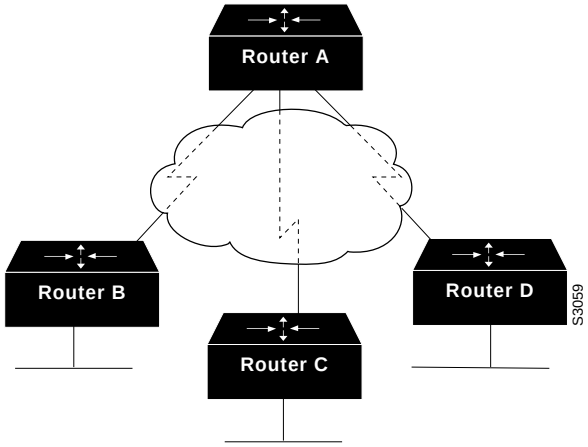


Hub and Spoke

In a hub and spoke topology, a central site is connected to several remote sites. The remote sites communicate with the central site directly; they do not call any of the other remote sites (see Figure 7-2). The central site has several interfaces that map to the remote sites. These interfaces are placed into a rotary group. A rotary group allows several sites to share several interfaces without dedicating an interface to each site. When a rotary is used for placing calls, a free interface is selected out of all of the physical interfaces in the rotary group. When used for incoming calls, the incoming call can be received by any of the physical interfaces, and packets will still be routed correctly. If an interface is already connected, incoming or outgoing calls can be received or placed by the next available interface in the rotary group. Hub and spoke topologies are easier to configure than fully meshed topologies (described in the next section) because remote site dialer interfaces are mapped only to the central site. A hub and spoke topology works well for communication servers (8 or 16 ports) or routers with multiple BRIs, multiple serial lines, or PRI interfaces.

If you want the spokes to communicate with each other in a hub and spoke topology for IP using RIP or IGRP, IP or IPX using Enhanced IGRP, or AppleTalk using Enhanced IGRP internetworks, you need to disable the split horizons feature. With split horizons enabled (the default), packets that are received by a particular interface are not sent out the same interface because it is assumed that all devices on that interface heard the packet that was received. In hub and spoke topologies, spokes learn about each other through the hub site to which they are connected by a single interface. In order for spokes to communicate with each other, split horizons must be disabled so that information can be sent and received over the same interface. If load sharing is desired, interfaces can be configured for bandwidth-on-demand capability.

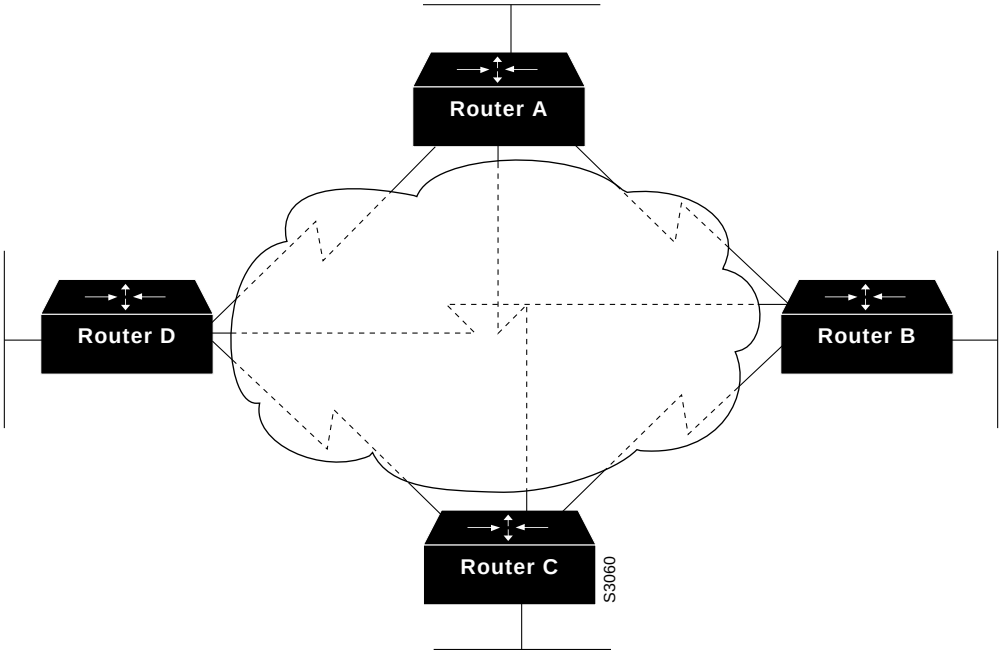
Figure 7-2 Hub and Spoke Topology



Fully Meshed

The fully meshed configuration is only recommended for very small DDR networks. Fully meshed topologies (see Figure 7-3) streamline the dialing process because each site can call any other site directly instead of having to call through a central site (as in the hub and spoke topology) which then places another call to the target site. However, the configuration for each site is more complex because each site must have mapping information for every other site. If load sharing is desired, interfaces can be configured for bandwidth-on-demand capability. In addition to the complexity of the configuration, either sufficient interfaces must be available on each device to deal with the possibility of all of the other devices calling in, or the possibility of contention for interfaces needs to be understood and dealt with.

Figure 7-3 Fully Meshed Topology



Addressing Considerations

There are normally two ways of viewing serial addressing requirements. The first is that each serial link is its own subnet. That subnet is a point-to-point connection. This is the common method used for leased lines using High-level Data Link Control (HDLC) and Point-to-Point Protocol (PPP) encapsulation. This approach tends to be used on point-to-point interfaces, or where interfaces are dedicated to specific destinations.The second addressing scheme is commonly used by Switched Multimegabit Data Service (SMDS)—each router is a different host number on the same subnet. This second approach is the method most widely used with dialer rotary groups and the hub and spoke topology. With the use of static routes pointing to the networks beyond the remote routers, the configuration is simple. This technique can be used for IP, IPX, and AppleTalk.

Security and Authentication

When choosing a topology, you need to consider where authentication is required. Authentication is used for two reasons. The first is for security, the second to identify who is calling in so that the called router can correctly forward packets to the correct interface. This is mostly required when using dialer rotary groups where multiple sites will be calling into a single router.

For security and authentication, Point-to-Point Protocol (PPP) with Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) can be used; or for ISDN interfaces, calling line identification (if available) can be used. CHAP and PAP, used with PPP encapsulation, allow routers to authenticate incoming calls.

CHAP

With CHAP, a remote device attempting to connect to the local router is requested, or challenged, to respond. When the local router receives the challenge response, it verifies the response by looking up the name of the remote device given in the response. The passwords must be identical on the remote device and the local router. The names and passwords are configured using the **username** command. In the following example, Router Macbeth will allow Router Macduff to call in using the password “bubble”:

```
hostname Macbeth
username Macduff password bubble
!
encapsulation ppp
ppp authentication chap
```

In the following example, Router Macduff will allow Router Macbeth to call in using the password “bubble”:

```
hostname Macduff
username Macbeth password bubble
!
encapsulation ppp
ppp authentication chap
```

PAP

Like CHAP, PAP is an authentication protocol used with PPP. However, PAP is less secure than CHAP. CHAP passes an encrypted version of the password on the physical link, but PAP passes the password and hostname or username in clear text.

On asynchronous lines when using interactive mode rather than dedicated mode, the **username** command allows a router to verify a username in an internal database before allowing the user to call in to the router. In the following example, user Joe Smith will be allowed to call in to the router if he uses the password “freedom”:

```
username JoeSmith password freedom
line 1
login
```

Calling Line Identification

You can configure BRI interfaces to use caller ID (identification). Incoming calls are screened to verify that the calling line ID is from an expected origin. Caller ID screening requires a local switch that can deliver the caller ID to the router.

DDR Media Considerations

The following are DDR internetwork media considerations:

- Encapsulation Methods
- Synchronous Serial Lines
- ISDN Connections
- Asynchronous Modem Connections

Encapsulation Methods

Cisco supports Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC), Serial Line Interface Protocol (SLIP), and X.25 data-link encapsulations for DDR.

PPP is the recommended encapsulation method because it supports multiple protocols and is used for synchronous, asynchronous, or ISDN connections. In addition, PPP performs address negotiation and authentication and is interoperable with different vendors.

HDLC is supported on synchronous serial lines and ISDN connections only. HDLC supports multiple protocols. However, HDLC does not provide authentication, which may be required if using dialer rotary groups.

SLIP works on asynchronous interfaces only and is supported by IP only. Addresses must be configured manually. SLIP does not provide authentication and is interoperable only with other vendors that use SLIP.

X.25 is supported on synchronous serial lines (IOS 10.0[5]), and a single ISDN B channel (Cisco IOS Software Release 10.2).

Synchronous Serial Lines

Dialing on synchronous serial lines can be initiated using V.25bis dialing or DTR dialing. V.25bis is an International Telecommunication Union Telecommunication Standardization Sector (ITU-T) standard for inband dialing. With inband dialing, dialing information is sent over the same connection that carries data. V.25bis is used with a variety of devices including synchronous modems, ISDN terminal adapters (TAs), and Switched 56 DSU/CSUs.

With DTR dialing, the DTR signal on the physical interface is activated, which causes some devices to dial a number configured into that device. When using DTR dialing, the interface cannot receive calls. But using DTR dialing allows lower cost devices to be used in cases where only a single number needs to be dialed.

Note The ITU-T carries out the functions of the former Consultative Committee for International Telegraph and Telephone (CCITT).

ISDN Connections

All ISDN devices subscribe to services provided by an ISDN service provider, usually a telephone company. Some service providers use Service Profile Identifiers (SPIDs) to define the services used by the ISDN device. The service provider assigns the ISDN device one or more SPIDs when you first subscribe to the service. If you are using a service provider that requires SPIDs, your ISDN device cannot place or receive calls until it sends a valid, assigned SPID to the service provider when accessing the switch to initialize the connection. Currently, only the DMS-100, NI-1, and 5ESS switch types require SPIDs. The 5ESS only requires SPIDs with multidrops. Other switches use subaddresses. In addition, SPIDs only have significance at the local access ISDN interface. SPIDs are never sent to the device being called.

ISDN calls are placed at 56 or 64 kbps. When dialing internationally, or making a DDR connection in the United States across more than one switch, ISDN lines may be available only at 56 kbps. ISDN supports caller ID (identification), providing security through authentication. For more information about ISDN, see Chapter 8, "Designing ISDN Internetworks."

Asynchronous Modem Connections

Asynchronous connections are used by communication servers or through the auxiliary port on a router. Asynchronous connections can be used by routers running TCP/IP, Novell IPX, and AppleTalk (IOS 10.2). Asynchronous connections support modems from 110 bps to 115 kbps—a real-world throughput is typically 2400 bps to 28.8 kbps.

When designing DDR internetworks over asynchronous connections, determine the type of connection you want users to make: interactive or dedicated. In interactive mode, the DDR line can be used for any type of connection, including Telnet, SLIP, or PPP encapsulation. In dedicated mode, the line is automatically placed into interface mode so that the user cannot change the encapsulation method, address, or other parameters.

If you rely on a dynamic routing protocol to receive routing information, you must enable asynchronous dynamic routing on the DDR interface so that the router will trust routes learned from that interface.

In order to dial out using asynchronous connections, chat scripts must be configured so that modem dialing and login commands are sent to remote systems. There are typically two scripts—modem (dialing) and system (login). Modem commands vary widely, depending upon modem and type and communication software. Several line commands are required to specify modem line characteristics, such as speed and parity setting. Login scripts request the network protocol and might include user name and password information for authentication purposes.

Creating Static Routes, Zones, and Service Updates

Typically, routers make decisions based on routing tables which they build from dynamic routing information. However, because routing updates are not sent over inactive DDR links, the administrator must configure static routes, services, and zones, so that routing can continue and so that hosts can still find services when the DDR link is not connected.

IP Static Routes

Use the **ip route command** to create static routes to specified destinations. To advertise static routes to other routers on the network, use the **redistribute** command with the **static** keyword.

For example, to redistribute the static route to other networks in IGRP autonomous system 109, use the following commands:

```
router igrp 109
network 131.108.0.0
redistribute static
```

IP Default Routes

Some routers may not be able to determine the routes to all other networks. It is common to configure these routers (using the **ip default-network** command) with default routes so that if the router cannot determine the destination for particular packets, it can forward the packets to the default address. The router at the default address will forward the packets to the intended destination.

Passive Interfaces

Interfaces that are tagged as *passive* will not send routing updates. To prevent routing updates from establishing DDR connections on dialer interfaces that do not rely on dynamic routing information, configure DDR interfaces with the **passive-interface** command or use access lists as described in the sections "IP Access Lists" and "IPX Access Lists" later in this chapter. Either the **passive-interface** command or an access list prevents routing updates from triggering a call. However, if you want routing updates to be passed when the link is active, use an access list instead of the **passive-interface** command.

Split Horizons

Routers connected to broadcast-type IP networks and routers that use distance-vector routing protocols use split horizons to reduce the possibility of routing loops. When split horizons is enabled, information about routes that comes in on an interface is not advertised out on that interface.

Note If remote sites need to communicate with each other, split horizons should be disabled for hub and spoke topologies. In hub and spoke topologies, spokes learn about each other through the hub site to which they are connected by a single interface. In order for spokes to send and receive information to each other, split horizons must be disabled so that information can be sent and received over the same interface.

IPX Static Routes and SAP Updates

With DDR, you need to configure static routes because routing updates are not received across inactive DDR connections. To create static routes to specified destinations, use the **ipx route** command. You can also configure static Service Advertisement Protocol (SAP) updates with the **ipx sap** command so that clients can always find a particular server. In this way, you can determine the areas on your internetwork where SAP updates will establish DDR connections.

In the following example, traffic to network 50 will always be sent to address 45.0000.0c07.00d3. Traffic to network 75 will always be sent to address 45.0000.0c07.00de. The router will respond to GNS queries with the server WALT if there are no dynamic SAPs available:

```
ipx route 50 45.0000.0c07.00d3
ipx route 75 45.0000.0c07.00de
ipx sap 4 WALT 451 75.0000.0000.0001 15
```

Configuring AppleTalk Static Zones

AppleTalk zones are by default dynamically updated with new AppleTalk addresses. To avoid unwanted DDR connections caused by dynamic zone updates, you can control the size and content of a zone statically instead. In the following example, the Marketing zone is configured to contain only addresses within a cable range of 110 to 110:

```
appletalk static cable-range 110-110 to 45.2 zone Marketing
```

Note For versions of Cisco IOS Release 10.0 that support snapshot routing, DDR dependence on static routes is minimized. Snapshot routing is a time-triggered technique optimized for remote sites with occasional access requirements, allowing a remote router to take a periodic snapshot of a central site routing table during a short *active* period. This information is then stored for a user-configurable period of inactivity until the next *active* period. If no routing updates are exchanged during the active period (because a DDR phone number or interface is unavailable), a user-configurable retry period is activated to ensure that a full inactive period does not pass before an attempt is made to exchange routing information again. Snapshot routing supports IP (RIP and IGRP), Novell IPX (RIP and SAP), and AppleTalk (RTMP) protocols.

Setting Up Dialer Maps

In addition to configuring static routes, you need to map network addresses to telephone numbers to design the DDR internetwork. Used with rotary groups, dialer maps can be configured to support multiple physical lines or multiple destinations on one interface. Dialer map statements map next hop addresses to telephone numbers. If a match is not found between a packet's next hop address and the dialer map statement defined for an interface, the packet is dropped. The next hop address for a packet is determined based on routing information. In the following example, packets received for a host on network 144.254.50.0 are routed to a next hop address of 144.254.45.2 and mapped to telephone number 555-1212:

```
ip route 144.254.50.0 255.255.255.0 144.254.45.2
interface dialer 1
dialer map IP 144.254.45.2 name HostA 5551212
```

Checks against dialer map statements for broadcasts will fail because a broadcast packet is transmitted with a next hop address of the broadcast address. If you want broadcast packets transmitted to telephone numbers defined by dialer map statements, use the **broadcast** keyword with the **dialer map** command.

To determine whether calls are placed at 56 or 64 kbps for ISDN calls, you can use the **speed** option with the **dialer map** command when configuring interfaces. See the "ISDN Connections" section earlier in this chapter for details on ISDN media. If you are calling a system that requires a login script and is running in interactive mode, use **the system-script** keyword with the **dialer map** command on asynchronous interfaces.

To take advantage of authenticated callers, use the **name** keyword with the **dialer map** command as illustrated in the following example:

```
dialer map ip 144.254.45.2 name localcall speed 64 5551212
dialer map ip 144.254.45.4 name longdistance speed 56 14155558888
```

For hub and spoke or fully meshed topologies that use multiple connections between single sites, configure rotary groups with the **interface dialer** and **dialer rotary-group** commands. A dialer interface is an entity that allows you to propagate an interface configuration to multiple interfaces. Physical interfaces assigned to the dialer rotary group inherit the interface dialer configuration parameters.

If one of the physical interfaces in a rotary group is busy, the next available interface can be used to place or receive a call. It is not necessary to configure rotary groups for BRI or PRI interfaces because ISDN channels are automatically placed into a rotary group, but multiple BRI or PRI interfaces may be placed in a rotary group to gain the advantages of rotary groups over a large number of B channels.

To load share so that additional bandwidth is provided as needed, use the **dialer load-threshold** command. In the following example, if the load to a particular destination on an interface in dialer rotary group 1 exceeds an interface load of 55% of the total bandwidth, the dialer will initiate another call to the destination. The load is displayed in a show interface as n/255. Load is calculated dynamically, based on the configured bandwidth of 9 kbps.

```
interface dialer 1
dialer load-threshold 55
bandwidth 9
```

Note On most of the hardware platforms supporting DDR, the packets are distributed among multiple links to the same destination based on the link with the shortest queue. If there are no packets queued on the device, the same link will always be used. With this technique, if a link is not being utilized to the point at which packets are backing up in the router, the extra link will be disconnected as a cost savings. The disadvantage of this technique is that if the dialer load-threshold is set too low, the second channel will be brought up, but it will never carry traffic and will be disconnected after the idle time. ISDN PRI currently does not use this approach, but instead employs a round-robin technique across all of the ports that are active to the same destination.

Determining Interesting and Uninteresting Packets

As described at the beginning of this chapter, if a packet is uninteresting and there is no connection established, the packet is dropped. If the packet is uninteresting, but a connection is already established to the specified destination, the packet is sent across the connection, but the idle timer is not reset. If the packet is interesting, and there is no connection on the available interface, the router attempts to establish a connection.

Once static routes are configured, you can apply access lists with the **access-list** command to DDR interfaces in order to control DDR connections by tagging packets as uninteresting and interesting. For example, RIP and IGRP routing update packets are sent across the internetwork periodically. These packets may need to be filtered with access lists to prevent unwanted DDR connections. Novell IPX SAP requests are sent periodically and will automatically activate any DDR link in their path. In the design of DDR internetworks, it is important to understand where updates and service requests are useful and where these packet types can be safely filtered. Use the **deny** option with access lists to tag packets as uninteresting. Use the **permit** option to configure interesting packets. You may also use the **passive-interface** command described earlier in the section “Passive Interfaces.”

On IP internetworks, it is important to consider filtering routing updates on DDR interfaces for the packet types listed in Table 7-1.

Table 7-1 IP Routing Update Packet Cycles

Packet Type	Periodic Update Cycle
Enhanced IGRP	5 seconds (Hello)
IGRP	90 seconds
RIP	60 seconds
OSPF	10 seconds (Hello)
IS-IS	10 seconds (Hello)

Note The routing protocols IS-IS, BGP, and OSPF are not recommended with DDR because they require an acknowledgment for routing updates. Because DDR lines are brought up as needed, DDR will not necessarily be active and available to send responses at the times the updates are sent.

On Novell IPX internetworks, it is important to consider filtering routing updates on DDR interfaces for the protocols listed in Table 7-2.

Table 7-2 Novell IPX Update Packet Cycles

Packet Type	Periodic Update Cycle
RIP	60 seconds
SAP	60 seconds
Serialization	66 seconds

Protocol-Specific Issues

Although the issues of topology and the configuration of dialer maps and filtering of interesting traffic are common to all DDR connections, there are specific issues for each of the following protocols:

- IP
- Novell IPX
- AppleTalk

IP

IP hosts use a variety of methods to access other IP hosts, including Telnet and the File Transfer Protocol (FTP). To initiate a DDR link, an IP host opens, for example, a Telnet session to the IP address of the destination.

IP Access Lists

Access lists determine whether packets are interesting or uninteresting. *Interesting* packets activate DDR connections automatically. *Uninteresting* packets do not trigger DDR connections, although if a DDR connection is already active, uninteresting packets will travel across the existing connection. You do not need to create a separate access list for each interface on a router. You can create several key access lists and apply them to as many interfaces as needed.

For example, you might apply access list 101 from the following example to several interfaces. Access list 101 prevents periodic IGRP routing updates from establishing an unwanted DDR connections, and allows all other IP packets to automatically trigger a DDR connection:

```
access-list 101 deny igrp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

Also refer to the section “Passive Interfaces” earlier in this chapter.

Novell IPX

Novell IPX hosts are attached to local Novell IPX servers and send a Get Nearest Server (GNS) packet to discover Novell servers on the internetwork. Novell IPX hosts find routers during NetWare shell loads.

IPX Access Lists

Access lists determine whether packets are interesting or uninteresting. *Interesting* packets activate DDR connections automatically. *Uninteresting* packets do not trigger DDR connections, although if a DDR connection is already active, uninteresting packets will travel across the existing connection.

Novell IPX internetworks use several types of update packets that may need to be filtered with access lists. Novell hosts broadcast serialization packets as a copy-protection precaution. Routing Information Protocol (RIP) routing table updates and SAP advertisements are broadcast every 60 seconds. Serialization packets are sent approximately every 66 seconds.

In the following example, access list 901 classifies SAP (452), RIP (453), and serialization (457) packets as uninteresting and classifies IPX packet types unknown/any (0), any or RIP (1), any or SAP (4), SPX (5), NCP (17), and NetBIOS (20) as interesting:

```
access-list 901 deny 0 FFFFFFFF 452
access-list 901 deny 4 FFFFFFFF 452
access-list 901 deny 0 FFFFFFFF 453
access-list 901 deny 1 FFFFFFFF 453
access-list 901 deny 0 FFFFFFFF 457
access-list 901 deny 0 FFFFFFFF 0 FFFFFFFF 452
access-list 901 deny 0 FFFFFFFF 0 FFFFFFFF 453
access-list 901 deny 0 FFFFFFFF 0 FFFFFFFF 457
access-list 901 permit 0
access-list 901 permit 1
access-list 901 permit 2
access-list 901 permit 4
access-list 901 permit 5
access-list 901 permit 17
```

You can permit any other type of IPX packet as needed.

With Cisco IOS 10.2, the configuration of Novell IPX access lists is improved with the support of wildcard (-1), so the previous example would be as follows:

```
access-list 901 deny -1 FFFFFFFF 452
access-list 901 deny -1 FFFFFFFF 453
access-list 901 deny -1 FFFFFFFF 457
access-list 901 deny -1 FFFFFFFF 0 FFFFFFFF 452
access-list 901 deny -1 FFFFFFFF 0 FFFFFFFF 453
access-list 901 deny -1 FFFFFFFF 0 FFFFFFFF 457
access-list 901 permit -1
```

IPX Watchdog Packets and Spoofing

Novell IPX watchdog packets are keepalive packets that are sent from servers to clients after a client session has been idle for approximately 5 minutes. Watchdog packets (keepalives) automatically establish connections over DDR links. To configure a router to ignore watchdog packets and thus prevent unwanted DDR connections from being established, use the **ipx watchdog-spoof** command.

AppleTalk

AppleTalk hosts use the Name Binding Protocol (NBP) to map network names to AppleTalk addresses. AppleTalk hosts access routers through the Chooser.

AppleTalk Broadcasts

While you cannot filter AppleTalk updates through access lists, you can eliminate broadcast traffic by not using the **broadcast** option with the **dialer map** command. For example, you may want to eliminate Zone Information Protocol (ZIP)—ZIP broadcasts are sent to track which networks are in which zone.

Eliminating Apple Filing Protocol Updates

AppleTalk servers use the Apple Filing Protocol (AFP) to send out *tickles* approximately every 10 seconds to hosts on the network.These tickles will establish connections when propagated across DDR interfaces. To avoid unwanted DDR connections, you must manually unmount AppleTalk servers or install software on the servers that will automatically disconnect idle users after a timeout period.

Summary

When designing DDR internetworks, consider topology type: point-to-point, hub and spoke, and fully meshed. With the topology type, consider the type of addressing scheme used and security issues. Keep in mind that media choice affects how packets are sent. Define where packets are sent by configuring static routes, zones, and services. Determine how packets reach their destination by configuring dialer interfaces and mapping addresses to telephone numbers. Finally, determine when the router should connect by configuring *interesting* versus *uninteresting* packets, eliminating unwanted AppleTalk broadcasts and spoofing IPX watchdog packets. Following these guidelines will help you construct scalable DDR internetworks that balance performance, fault tolerance, and cost.