Dial-on-Demand Routing (DDR) provides network connections across Public Switched Telephone Networks (PSTNs). Dedicated wide-area networks are typically implemented on leased lines or more modern service provider options such as Frame Relay, SMDS, or ATM. Dial-on-Demand Routing provides session control for wide-area connectivity over circuit switched networks, which in turn provides on-demand services and decreased network costs.

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 BRI and PRI interfaces.

Guide Contents
Internetworking Design Basics Designing various internetworks Network Enhancements IP Routing Concepts UDP Broadcast Flooding Large-Scale H.323 Network Design for Service Providers LAN Switching Subnetting an IP Address Space IBM Serial Link Implementation Notes References and Recommended Reading

Contents

- 1 Introduction to DDR
  - 1.1 DDR Design Stack
    - 1.1.1 Figure: DDR design stack
  - 1.2 Dialer Clouds
- 2 Traffic and Topology of DDR
  - 2.1 Topologies
    - 2.1.1 Point-to-Point Topology
      - 2.1.1.1 Figure: Point-to-point topology
  - 2.2 Fully Meshed Topology
    - 2.2.1 Figure: Fully meshed topology
    - 2.2.2 Hub-and-Spoke DDR Solutions
      - 2.2.2.1 Figure: Hub-and-spoke topology
  - 2.3 Traffic Analysis
    - 2.3.1 Table: DDR Protocol Connectivity Requirements for KDT
- 3 Dialer Interfaces
  - 3.1 Supported Physical Interfaces
    - 3.1.1 Synchronous Serial Interfaces
    - 3.1.2 ISDN Interfaces
    - 3.1.3 Asynchronous Modem Connections
  - 3.2 Dialer Rotary Groups
  - 3.3 Dialer Profiles
  - 3.4 Encapsulation Methods

- 3.5 Addressing Dialer Clouds
- 3.6 Dialer Maps
  - 3.6.1 Table: DDR Address Mapping Table for KDT
- 4 Routing Strategies
  - 4.1 Static Routing
  - 4.2 Dynamic Routing
    - 4.2.1 Selecting a Dynamic Routing Protocol
    - 4.2.2 Passive Interfaces
    - 4.2.3 Split Horizons
    - 4.2.4 Dynamic Connected Routes
  - 4.3 Snapshot Routing
    - 4.3.1 Snapshot Model
      - 4.3.1.1 Figure: Snapshot routers in action
  - 4.4 Enabling Snapshot Routing
    - 4.4.1 Figure: AppleTalk snapshot routing
  - 4.5 Dial Backup for Leased Lines
    - 4.5.1 Backup Interfaces
      - 4.5.1.1 Figure: Example of dial backup over ISDN
    - 4.5.2 Floating Static Routes
    - 4.5.3 IPX Static Routes and SAP Updates
    - 4.5.4 Configuring AppleTalk Static Zones
- 5 Dialer Filtering
  - 5.1 Figure: Dialer filtering
  - 5.2 Defining Interesting Packets Using ACLs
    - 5.2.1 SNMP
  - 5.3 IPX Packets
    - 5.3.1 Table: Novell IPX Update Packet Cycles
    - 5.3.2 Controlling IPX Watchdog Packets
    - 5.3.3 Controlling SPX Keepalive Packets
    - 5.3.4 Time Server and NDS Replica Packets
    - 5.3.5 AppleTalk Filtering
    - 5.3.6 Banyan VINES, DECnet IV, and OSI Packets
- 6 Authentication
  - 6.1 PPP Authentication
    - 6.1.1 CHAP
    - 6.1.2 PAP
    - 6.1.3 ISDN Security
    - 6.1.4 DDR Callback
    - 6.1.5 IPX Access Lists
- 7 Summary

Introduction to DDR

Cisco IOS Dial-on-Demand Routing (DDR) provides several functions. First DDR spoofs routing tables to provide the image of full-time connectivity using Dialer interfaces. When the routing table forwards a packet to a Dialer interface, DDR then filters out the interesting packets for establishing, maintaining, and releasing switched connections. Internetworking is achieved over the DDR maintained connection using PPP or other WAN encapsulation techniques (such as HDLC, X.25, SLIP). Internetwork engineers can use the model presented in this article to construct scalable, DDR internetworks that balance performance, fault tolerance, and cost.

DDR Design Stack

Similar to the model provided by the OSI for understanding and designing internetworking, a stacked approach, shown in Figure: DDR design stack, can be used to design DDR networks.

Figure: DDR design stack

Dialer Clouds

The network formed by the interconnected DDR devices can generically be labeled the dialer media or dialer cloud. The scope of the dialer cloud includes only the intended interconnected devices and does not include the entire switched media (the entire ISDN spans the globe and is beyond the scope of the dialer cloud). The exposure to the ISDN must be considered when designing security.

The fundamental characteristics of dialer clouds are as follows:

- Dialer clouds are collective bundles of potential and active point-to-point connections.
- On active connections, dialer clouds form an NBMA (non-broadcast multiaccess) media similar to Frame Relay.
- For outbound dialing on switched circuits (such as ISDN) network protocol address to directory number mapping must be configured.
- Inactive DDR connections are spoofed to appear as active to routing tables.
- Unwanted broadcast or other traffic causing unneeded connections can be prohibitively expensive. Potential costs on Tariffed media (such as ISDN) should be closely analyzed and monitored to prevent such loss.

The characteristics of dialer clouds affect every stage of DDR internetworking design. A solid understanding of network protocol addressing, routing, and filtering strategies can result in very robust and cost-effective internetworks.

Traffic and Topology of DDR

To determine the optimum topology, the DDR designer should perform a traffic analysis of internetworking applications that must be supported. This includes answering the following questions:

- How often does data traffic need to move between the DDR sites?
- What side of the DDR connection can establish the connection? How many remote sites?
- Is this a point-to-point solution or a multipoint solution?

Topologies

The most important factor in selecting the topology is the number of sites that will be supported. If only two sites will be involved, the point-to-point topology is used. If more than two sites are to be supported, the hub-and-spoke topology is typically used. For small numbers of sites with very low traffic volumes, the fully meshed topology may be the most appropriate solution.

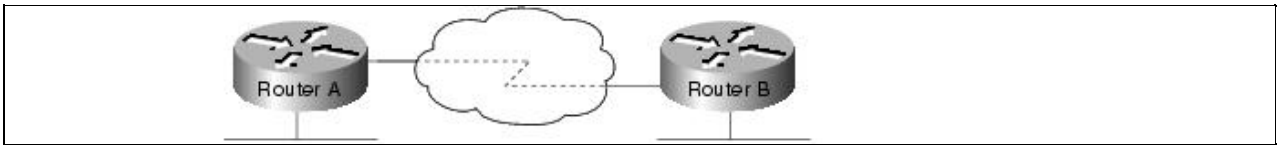
Topologies for DDR covered in this section include:

- Point-to-point
- Fully meshed
- Hub-and-spoke

Point-to-Point Topology

In a simple point-to-point topology (see Figure: 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 additional bandwidth is required, multiple links can be aggregated using Multilink PPP.

Figure: Point-to-point topology

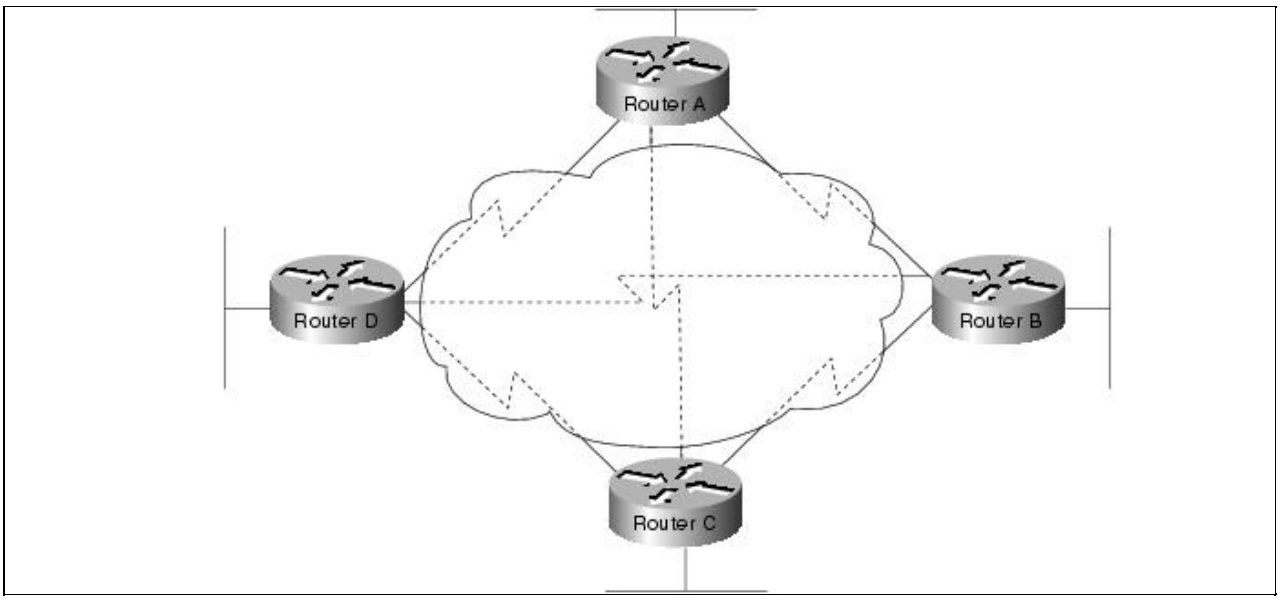


Fully Meshed Topology

The fully meshed configuration (see Figure: Fully meshed topology) is recommended only for very small DDR networks. Fully meshed topologies can streamline the dialing process for any-to-any connectivity as each site can call any other site directly, rather than having to call through a central site, 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 MultiLink PPP 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.

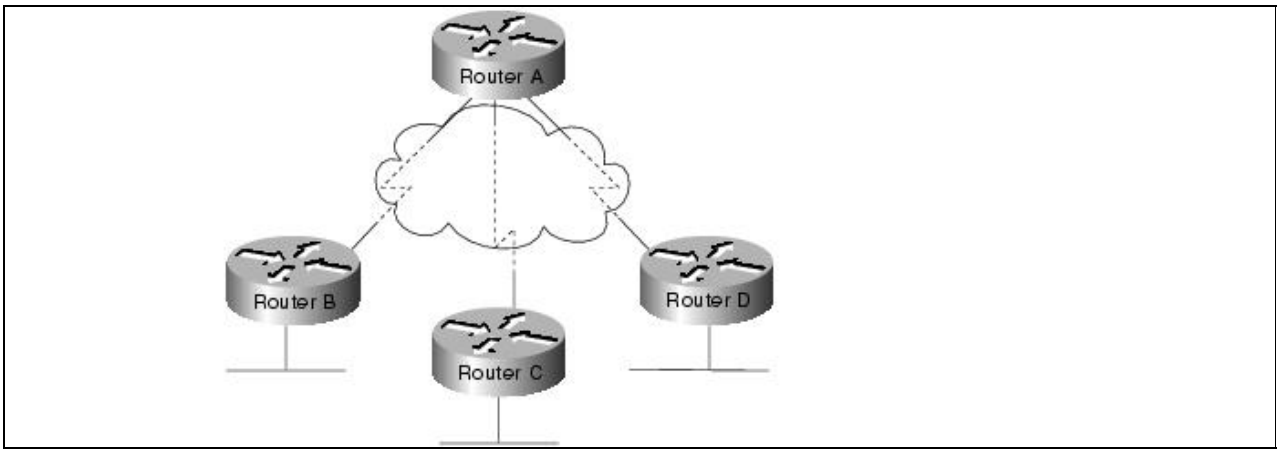
Figure: Fully meshed topology



Hub-and-Spoke DDR Solutions

In a hub-and-spoke topology (see Figure: 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. This topology works very well for scaling large solutions.

Figure: Hub-and-spoke topology



Hub-and-spoke topologies are easier to configure than fully meshed topologies when multipoint topologies are required because remote site dialer interfaces are mapped only to the central site. This allows most of the design complexity (such as addressing, routing, and authentication) to be managed on the DDR Hub. Configuration support of the remote sites can be greatly simplified (similar to one end of a point-to-point topology).

If any-to-any connectivity initiation is required between remote sites, routing behavior may need to be modified depending on dialer interface behavior (that is, it may be necessary to disable split-horizon on distance vector routing protocols).

Multiple hubs can be used to provide further scaling of hub-and-spoke technologies. When using MultiLink PPP, as is very common in ISDN solutions, designers can implement Cisco IOS MultiChassis MultiLink PPP to scale the dial-in rotary group between multiple Network Access Servers.

Traffic Analysis

For traffic analysis, develop a chart of which protocols need to be able to support DDR-based dialing from which devices. This will form the basis of the rest of the DDR design.

For example, Company KDT has selected a hub-and-spoke topology (to provide for scaling) and has developed the needs shown in Table: DDR Protocol Connectivity Requirements for KDT for its DDR cloud requirements.

Table: DDR Protocol Connectivity Requirements for KDT

Remote Site	Dial-In Protocols	Dial-Out Protocols	Notes
c700A	IP, IPX	None	
c700B	IP	None	
c1600A	IP, AppleTalk	IP	
c2500A	IP, IPX, AppleTalk	IP, IPX, AppleTalk	
c2500B	IP, IPX	IP	
NAS3600A	IP, IPX, AppleTalk	IP, IPX, AppleTalk	

The purpose of Table: DDR Protocol Connectivity Requirements for KDT is to identify which sites and protocols require the capability to initiate the DDR connections. Once connectivity is established, each protocol requires two-way connectivity via routing tables and dialer cloud address mapping. Dial-in versus dial-out is from the perspective of the hub.

Often a primary goal of a DDR network is to offer a cost improvement over WAN charges associated with dedicated connections. Additional traffic analysis must be performed for each protocol at this or the Dialer Filtering design stage. Network applications use the infrastructure provided by the internetwork in many different and often unexpected ways. It is critical to perform a thorough analysis of real-world network traffic that will transit the dialer media in order to determine whether a DDR network can operate in a feasible manner. Packet capture and analysis tools provide the most valuable tool for this analysis.

Dialer Interfaces

Access to the dialer media is via Cisco ISO Dialer interfaces. ISDN B channels, Synchronous Serial interfaces, and Asynchronous interfaces can all be converted to dialer interfaces using dialer interface configuration commands. To understand dialer interfaces, the following concepts are covered:

- Supported physical interfaces
- Dialer rotary groups
- Dialer profiles
- Dialer addressing
- Dialer mapping

Dialer Interfaces also provide the basis for support of routing table spoofing and dialer filtering. This section focuses on lower-layer characteristics of dialer interfaces.

Supported Physical Interfaces

Several types of physical interfaces can be enabled as dialer interfaces.

Synchronous Serial Interfaces

Dialing on synchronous serial lines can be initiated using V.25bis dialing or DTR dialing. V.25bis is the ITU standard for in-band dialing. With in-band dialing, dialing information is sent over the same connection that carries the 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. Synchronous Serial Lines support PPP, HDLC, and X.25 datagram encapsulation.

To convert a synchronous serial interface into a dialer interface, use the Cisco IOS command **dialer in-band** or **dialer dtr**.

ISDN Interfaces

All ISDN devices subscribe to services provided by an ISDN service provider, usually a telephone company. ISDN DDR connections are made on B channels at 56 or 64 Kbps depending on the bearer capabilities of the end-to-end ISDN switching fabric. MultiLink PPP is often used to allow BRI devices to aggregate both B channels for great bandwidth and throughput.

ISDN BRI and PRI interfaces are automatically configured as dialer in-band interfaces. ISDN can support PPP, HDLC, X.25, and V.120 encapsulation. Typically, PPP will be used for DDR solutions. ISDN interfaces are automatically configured as dialer in-band interfaces.

For example, when examining a BRI interface on a Cisco IOS router, you can see that it is in the spoofing (pretending to be up/up so the routing table can point to this interface):

```
c1600A# sh int bri 0

BRI0 is up, line protocol is up (spoofing)
```

However, the physical interfaces are the individual B (BRI0:1 and BRI0:2) channels being managed by the dialer interface (BRI0).

```
c1600A# sh int bri 0 1

 BRI0:1 is down, line protocol is down
Hardware is BRI
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
LCP Closed, multilink Closed
Closed: IPCP, CDPCP
```

Asynchronous Modem Connections

Asynchronous connections are used by communication servers or through the auxiliary port on a router. Asynchronous DDR connections can be used to support multiple network layer protocols. When considering asynchronous DDR solutions, designers should consider if the internetworking applications can tolerate the longer call setup time and lower throughput of analog modems (in comparison with ISDN). For some design applications, DDR over asynchronous modem connections may provide a very cost-effective option.

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. For design flexibility, multiple chat scripts can be configured on dialer maps. Modem scripts can be used to configure modems for outbound calls. Login scripts are intended to deal with logging onto remote systems and preparing the link for establishment of PPP. Chat scripts are configured with expect-send pairs and keywords to modify settings, as follows:

```
chat-script dialnum "" "atdt\T" TIMEOUT 60 CONNECT \c
```

If you are using asynchronous DDR and calling a system that requires a character-mode login, use the **system-script** keyword with the **dialer map** command.

Chat scripts often encounter problems with timing due to the fact that they are run with much greater precision than when a human is controlling the connection. For example, sometimes when a modem sends the CONNECT message, it is not actually ready to send data, and may even disconnect if any data is received on the TX circuitry. To avoid such failure modes, pauses are added at the head of some send strings.

Each send string is terminated with a carriage return, even when it's a null string ("""). Often the chat script will be set up without the final "send" string. This may produce unexpected results. Ensure that all chat scripts have complete expect-send pairs. If the final element in the chat script logic turns out to be an expect (as in the previous example), use the \c as the final send to suppress unwanted output.

Use the **debug chat** commands to troubleshoot chat script problems. Line-specific debugging can provide additional details when expect-send logic is failing.

Dialer Rotary Groups

For hub-and-spoke or fully meshed topologies that support multiple connections between sites, physical interfaces can be grouped into rotary groups with the **dialer rotary-group** command. Physical interfaces assigned to the dialer rotary-group inherit their configuration from the corresponding interface dialer.

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 as ISDN B channels are automatically placed into a **rotary-group**, however multiple BRI or PRI interfaces can be grouped using **dialer rotary-group**.

Dialer Profiles

Dialer profiles introduced in Cisco IOS 11.2 offer additional design flexibility such as multisite bridging over ISDN. Dialer profiles provide an alternative methodology for designing DDR networks by removing the logical definition of dialer sites from the physical dialer interfaces.

Encapsulation Methods

When a clear DataLink is established between two DDR peers, internetworking datagrams must be encapsulated and framed for transport across the Dialer media. The encapsulation methods available depend on the physical interface being used. 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 and a single ISDN B channel.

Addressing Dialer Clouds

There are two ways of setting up addressing on dialer clouds, as follows:

- Applying a subnet to the dialer cloud

  Each site connected to the dialer cloud is given a unique node address on a shared subnet for use on its dialer interface. This method is similar to numbering a LAN or multipoint WAN and simplifies the addressing scheme and creation of static routes.

- Using unnumbered interfaces

  Similar to using unnumbered addressing on leased line point-to-point interfaces, the address of another interface on the router is borrowed for use on the dialer interface. Unnumbered addressing takes advantage of the fact that there are only two devices on the point-to-point link. The routing table points to an interface (the dialer interface) and a next-hop address (which must match a dialer map: static or dynamic).
  Building static routes for unnumbered interfaces can be a little more complex because the router must be configured with the interface that finds the next-hop out.

Dialer Maps

Similar to the function provided by an ARP table, **dialer map** statements translate next-hop protocol addresses to telephone numbers. Without statically configured dialer maps, DDR call initiation cannot occur. When the routing table points at a dialer interface, and the next-hop address is not found in a dialer map, the packet is dropped.

In the following example, packets received for a host on network 172.20.0.0 are routed to a next-hop address of 172.20.1.2, which is statically mapped to telephone number 555-1212:

```
interface dialer 1
ip address 172.20.1.1 255.255.255.0
dialer map ip 172.20.1.2 name c700A 5551212
!
ip route 172.20.0.0 255.255.255.0 172.20.1.2
```

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 remote sites defined by **dialer map** statements, use the **broadcast** keyword with the **dialer map** command.

To configure 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.

When setting up DDR between more than two sites, it is necessary to use PPP authentication and to use the **name** keyword with the **dialer map** command, as dialer maps for inbound calls are maps between protocol addresses and authenticated user names.

To facilitate building of dialer maps, the internetwork designer should build an Address Mapping Table as an aid for configuration. In Table: DDR Address Mapping Table for KDT, the dialer cloud has been assigned IP subnet 172.20.1.0/24, IPX network 100, and AppleTalk cable-range 20-20. Table: DDR Address Mapping Table for KDT forms the basis for building proper dialer maps for each site.

Table: DDR Address Mapping Table for KDT

Remote Site	Dial-In Protocols	Directory#	Notes
c700A	IP: 172.20.1.2 IPX: 100.0000.0c00.0002	4085551212	
c700B	IP:172.20.1.3	4155558888	56K
c1600A	IP: 172.20.1.4 AT: 20.4	5305551000	
c2500A	IP: 172.20.1.5 IPX: 100.0000.0c00.0005 AT: 20.5	5125558085	
c2500B	IP: 172.20.1.6 IPX: 100.0000.0c00.0006	2105552020	
NAS3600A	IP: 172.20.1.1 IPX: 100.0000.0c00.0001	8355558661	Hub

As NAS3600A forms the hub in the hub-and-spoke topology, each remote site is configured with the dialer maps to get to the central site. For example, the dialer map configuration for c1600A would be as follows:

```
interface dialer1
encapsulation ppp
ip address 172.20.1.4 255.255.255.0
appletalk cable-range 20-20 20.4
appletalk zone ZZ DDR
dialer in-band
dialer map ip 172.20.1.1 name nas3600A speed 56 18355558661
dialer map appletalk 20.1 name nas3600A speed 56 18355558661
dialer-group 5
ppp authentication chap callin
```

The dialer map configuration for NAS3600A would be as follows:

```
interface dialer1
encapsulation ppp
ip address 172.20.1.1 255.255.255.0
appletalk cable-range 20-20 20.1
appletalk zone ZZ DDR
ipx network 100
dialer in-band
```

```
dialer map ip 172.20.1.2 name c700A
dialer map ipx 100.0000.0c00.0002 c700A
dialer map ip 172.20.1.3 name c700B
dialer map ip 172.20.1.4 name speed 56 c1600A 15305551000
dialer map appletalk 20.4 name c1600A
dialer map ip 172.20.1.5 name c2500A 15125558085
dialer map ipx 100.0000.0c00.0005 name c2500A 15125558085
dialer map appletalk 20.5 name c2500A 15125558085
dialer map ip 172.20.1.6 name c2500B 12105552020
dialer map ipx 100.0000.0c00.0006 name c2500B
dialer-group 5
ppp authentication chap callin
```

Note that dialer maps provide mapping between remote site protocol addresses, remote site names, and remote site directory numbers. For dial-in only sites, directory numbers are not required and can be left off to avoid inadvertent dialing. [[Internetwork Design Guide -- Designing DDR Internetworks#Table was used to determine which sites do not require dial-out support. For dial-in sites, the ppp authentication name is mapped to the protocol address to ensure outbound packets are placed on the correct PPP connection.

Recent Cisco IOS releases can build dynamic dialer maps using for IP (using IPCP address negotiation) and IPX (using IPXCP address negotiation), eliminating the need for dialer maps for dial-in only sites.

The DDR designer should familiarize themselves with the use of the Cisco IOS exec commands **show dialer** and **show dialer map** to examine the state of the DDR sites, the physical interfaces, and the dialer map table. Use **debug dialer** to troubleshoot DDR connection problems.

`c1600A#` **sh dialer**

```
 BRI0 - dialer type = ISDN
Dial String      Successes   Failures    Last called   Last status
1835558661 0          0    never                   -
0 incoming call(s) have been screened.
BRI0:1 - dialer type = ISDN
Idle timer (60 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (5 secs)
Dialer state is idle
BRI0:2 - dialer type = ISDN
Idle timer (60 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (5 secs)
Dialer state is idle
```

`c1600A#` **sh dialer map**

```
Static dialer map ip 172.20.1.4 name nas (8355558661) on BRI0
```

Routing Strategies

The nature of DDR networks is that routing and some directory services tables must be maintained over idle connections. DDR designers may use a combination of static, dynamic, and snapshot routing techniques to meet design needs. Default routing and remote node spoofing techniques (such as Cisco 700 Series PAT and Cisco IOS EZIP) can be used to greatly simplify routing design.

Often the backbone at the NAS site will use a fast-converging routing protocol such as OSPF or EIGRP; however, these protocols do not operate easily on the dialer media due to their broadcast and link-state nature. Typically, static routing and/or distance vector routing protocols are selected for the DDR connections. Routing redistribution may be required to support propagation of routing information between the different routing protocols.

A complete discussion of routing redistribution techniques is beyond the scope of this article; however, DDR designers do need to develop and verify their routing strategy for each network protocol.

Static Routing

With static routes, network protocol routes are entered manually, eliminating the need for a routing protocol to broadcast routing updates across the DDR connection. Static routes can be effective in small networks that do not change often. Routing protocols can generate traffic that causes connections to be made unnecessarily.

When designing with IP unnumbered environments, older versions of Cisco IOS required multiple static routes for each site: one route to define the next-hop IP address and a second to define the interface on which to find the next-hop (and dialer map). The following code:

```
interface Dialer1
ip unnumbered Ethernet0/0
dialer in-band
dialer map ip 172.17.1.100 name kdt-NAS speed 56 5558660
dialer-group 5
!
ip classless
'''ip route 0.0.0.0 0.0.0.0 172.17.1.100 200'''
ip route 172.17.1.100 255.255.255.255 Dialer1 200
dialer-list 5 protocol ip permit
```

creates the following routing table:

```
kdt-3640#sh ip route
...<snip>...
Gateway of last resort is 172.17.1.100 to network 0.0.0.0
172.17.0.0/32 is subnetted, 1 subnets
S       172.17.1.100 is directly connected, Dialer1
     172.20.0.0/24 is subnetted, 1 subnets
S*   0.0.0.0/0 [200/0] via 172.17.1.100
```

Recent Cisco IOS versions allow configuration of this as one route. For example, the example configuration here:

ip route 0.0.0.0 0.0.0.0 Dialer1 172.17.1.100 200 permanent

results in a simplified routing table, as follows:

```
kdt-3640#sh ip route
...<snip>...
Gateway of last resort is 172.17.1.100 to network 0.0.0.0
172.20.0.0/24 is subnetted, 1 subnets
C       172.20.1.0 is directly connected, Ethernet0/0
S*   0.0.0.0/0 [200/0] via 172.17.1.100, Dialer1
```

It is typically necessary to configure redistribution of static routes into the backbone dynamic routing protocol to ensure end-to-end connectivity. For example, to redistribute the static route to other networks in IGRP autonomous system 20, use the following configuration commands:

```
router igrp 20
network 172.20.0.0
redistribute static
```

Dynamic Routing

Dynamic routing can be used in DDR network design in a number of ways. Dynamic routing can be used with snapshot routing (as described in the Snapshot Routing section later in this article) to cache routes learned by dynamic routing protocols, thus allowing the automation of static routing maintenance. Dynamic routing can be used as a trigger for routing convergence in large and complex DDR designs.

When the DDR link is connected, routing updates will flow to the peer, allowing redundant designs to converge on the physical connection by redistribution of trigger routing updates.

Selecting a Dynamic Routing Protocol

The routing protocol selected for DDR link is typical of a Distance Vector protocol such as RIP, RIP II, EIGRP, IGRP, or RTMP. Selecting the simplest protocol that meets the needs of the internetwork design and that is supported by the DDR routers is recommended.

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 section IPX Access Lists later in this article. Using 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 rather than 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 are enabled, information about routes that comes in on an interface is not advertised out on that same interface.

Note: If remote sites need to communicate with one another, split horizons should be disabled for hub-and-spoke topologies. In hub-and-spoke topologies, spokes learn about one another through the hub site to which they are connected by a single interface. In order for spokes to send and receive information to one another, split horizons may need to be disabled so that full routing tables are built at each site.

Dynamic Connected Routes

Dynamic connected routes include the two following:

- **Per-user AAA Installed Routes**-AAA servers can install routes associated with users by using AAA authorization to download and install routes as remote sites connect.
- **PPP Peer Routes**-IPCP address negotiation installs host-routes (/32 subnet mask) for the remote peer. This host-route can be propagated to backbone routers to provide robust routing convergence. In most applications, the peer host-route will be beneficial (or innocuous) to the internetwork design. If PPP peer host-routes interact poorly with existing routing strategies, they can be turned off with the interface configuration command **no peer neighbor-route**.

Snapshot Routing

With snapshot routing, the router is configured for dynamic routing. Snapshot routing controls the update interval of the routing protocols. Snapshot routing works with the following distance vector protocols:

- Routing Information Protocol (RIP) for IP
- Interior Gateway Routing Protocol (IGRP) for IP
- Routing Information Protocol (RIP) and Service Advertisement Protocol (SAP) for Novell Internet Packet Exchange (IPX)
- Routing Table Maintenance Protocol (RTMP) for AppleTalk
- Routing Table Protocol (RTP) for Banyan VINES

Under normal circumstances, these routing protocols broadcast updates every 10 to 60 seconds, so an ISDN link would be made every 10 to 60 seconds simply to exchange routing information. From a cost perspective, this frequency is prohibitive. Snapshot routing solves this problem.

Note: Snapshot routing is available in Cisco IOS Software Release 10.2 or later.

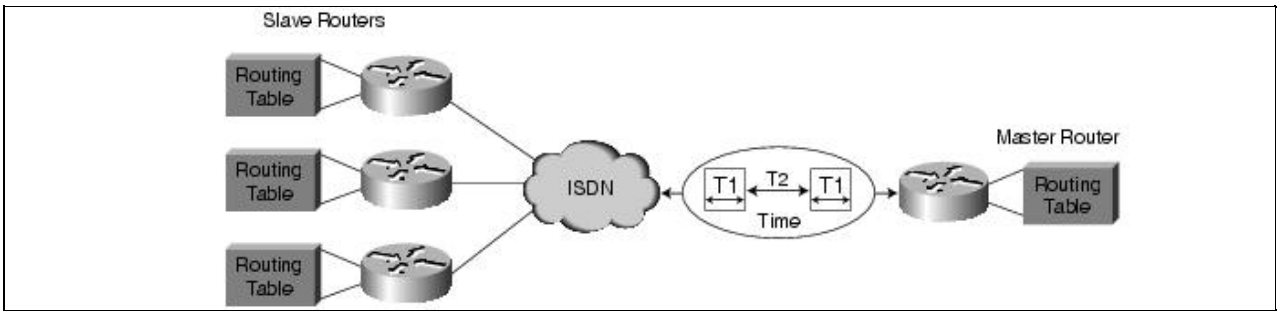
Snapshot Model

Snapshot routing uses the client-server design model. When snapshot routing is configured, one router is designated as the snapshot server and one or more routers are designated as snapshot clients. The server and clients exchange routing information during an active period. At the beginning of the active period, the client router dials the server router to exchange routing information. At the end of the active period, each router takes a snapshot of the entries in its routing table. These entries remain frozen during a quiet period. At the end of the quiet period, another active period begins, and the client router dials the server router to obtain the latest routing information. The client router determines the frequency at which it calls the server router. The quiet period can be as long as 100,000 minutes (approximately 69 days).

When the client router transitions from the quiet period to the active period, the line might be down or busy. If this happens, the router would have to wait through another entire quiet period before it could update its routing table, which might severely affect connectivity if the quiet period is very long. To avoid having to wait through the quiet period, snapshot routing supports a retry period. If the line is not available when the quiet period ends, the router waits for the amount of time specified by the retry period and then transitions to an active period once again.

The retry period is also useful in dial-up environments in which there are more remote sites than interface lines. For example, the central site might have one PRI (with 23 B channels available) but might dial more than 23 remote sites. In this situation, there are more dialer map commands than available lines. The router tries the **dialer map** commands in order and uses the retry time for the lines that it cannot immediately access (see Figure: Snapshot routers in action).

Figure: Snapshot routers in action



Enabling Snapshot Routing

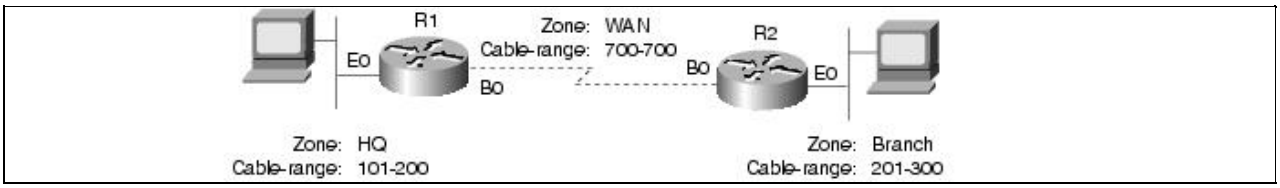
Snapshot routing is enabled through interface configuration commands (see Figure: AppleTalk snapshot routing). The central router is configured for snapshot routing by applying the **snapshot server** interface configuration command to its ISDN interfaces. The **snapshot server** command specifies the length of the active period and whether the router is allowed to dial remote sites to exchange routing updates in the absence of regular traffic.

The remote routers are configured for snapshot routing by applying the **snapshot client** command to each ISDN interface. The **snapshot client** interface configuration command specifies the following variables:

- The length of the active period (which must match the length specified on the central router)
- The length of the quiet period
- Whether the router can dial the central router to exchange routing updates in the absence of regular traffic
- Whether connections that are established to exchange user data can be used to exchange routing updates

When the backbone routing protocol is not supported by snapshot routing (for example, OSPF or EIGRP), standard routing redistribution techniques can be used to ensure that routing updates are propagated between routing protocols, as required. Care should be taken to ensure redistribution of subnets if needed and to avoid routing loops.

Figure: AppleTalk snapshot routing



- R1 configuration is as follows:

```
username R2 password SECRET
appletalk routing
isdn switch-type basic-5ess
!
interface BRI0
 encapsulation ppp
 appletalk cable-range 700-700 700.1
 appletalk zone WAN
 dialer map appletalk 700.2 name R2 speed 56 broadcast 5552222
 dialer map snapshot 2 name R2 speed 56 broadcast 5552222
 dialer-group 1
 snapshot client 5 60 dialer
 isdn spid1 5550066
```

```
 ppp authentication chap
!
dialer-list 1 protocol appletalk permit
```

- R2 configuration is as follows:

```
username R1 password SECRET
appletalk routing
isdn switch-type basic-5ess
interface BRI0
 encapsulation ppp
 appletalk cable-range 700-700 700.2
 appletalk zone WAN
 dialer wait-for-carrier-time 60
 dialer map appletalk 700.1 name R1 speed 56 broadcast 5550066
 dialer-group 1
  snapshot server 5 dialer
isdn spid1 5552222
ppp authentication chap
!
dialer-list 1 protocol appletalk permit
```

For a further examination of snapshot routing, see Using ISDN Effectively in Multiprotocol Networks.

Dial Backup for Leased Lines

Dial backup protects against wide-area network (WAN) downtime by allowing a dedicated serial connection to be backed up by a circuit-switched connection. Dial backup can be performed in several ways: either with floating static routes or with backup interfaces.

Dial backup challenges the designer with different traffic patterns than DDR-supported SOHO and ROBO sites. When designing Dial backup port densities, consider how many links might fail concurrently in a mass-failure scenario, as well as how many ports will be required on the central site in a worst-case scenario. Typical design involves selecting only dial-in or dial-out to avoid contention when both sides are trying to re-establish connectivity.

Backup Interfaces

A primary/dedicated serial line is configured to have a backup interface in the event of link failure or exceeded load thresholds. If the interface line or line protocol state goes down, the backup interface is used to establish a connection to the remote site.

Once configured, the dial backup interface remains inactive until one of the following conditions is met:

1. Line Protocol on the primary link goes down. The backup line is then activated, re-establishing the connection between the two sites.
2. The traffic load on the primary line exceeds a defined limit-The traffic load is monitored and a five-minute moving average is computed. If the average exceeds the user-defined value for the line, the backup line is activated. Depending on how the backup line is configured, some or all of the traffic flows onto it.

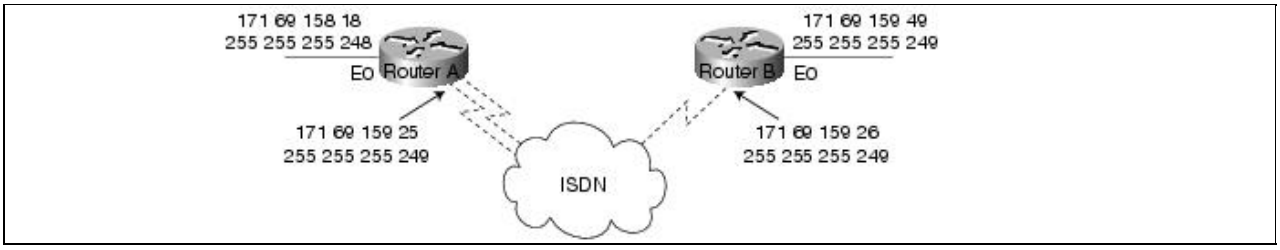
A Cisco IOS interface is placed into backup mode by applying the **backup interface** command:

- The **backup interface** interface configuration command specifies the interface that is to act as the backup.

- The **backup load** command specifies the traffic threshold at which the backup interface is to be activated and deactivated.
- The **backup delay** command specifies the amount of time that is to elapse before the backup interface is activated or deactivated after a transition on the primary interface.

Backup interfaces traditionally lock the backup interface into BACKUP state so it is unavailable for other use. Dialer Profiles eliminates this lock and allows the physical interface to be used for multiple purposes. Floating Static Route DDR design also eliminates this lock on the dialer interface. In Figure: Example of dial backup over ISDN, a leased line connects Router A to Router B, and BRI 0 on Router B is used as a backup line.

Figure: Example of dial backup over ISDN



Using the configuration that follows, BRI 0 is activated only when serial interface 1/0 (the primary line) goes down. The **backup delay** command configures the backup connection to activate 30 seconds after serial interface 0 goes down and to remain activated for 60 seconds after the serial interface 1/0 comes up:

```
interface serial 1/0
ip address 172.20.1.4 255.255.255.0
backup interface bri 2/0
backup delay 30 60
```

Using the configuration that follows, BRI 2/0 is activated only when the load on serial 0 (the primary line) exceeds 75 percent of its bandwidth. The backup line is deactivated when the aggregate load between the primary and backup lines is within five percent of the primary line's bandwidth:

```
interface serial 1/0
ip address 172.20.1.4 255.255.255.0
backup interface bri 2/0
backup load 75 5
```

Using the following configuration, BRI 2/0 is activated only when serial interface 1/00 goes down or when traffic exceeds 25 percent. If serial interface 1/0 goes down, 10 seconds will elapse before BRI 0 becomes active. When serial interface 1/0 comes up, BRI 2/0 will remain active for 60 seconds. If BRI 2/0 is activated by the load-threshold on serial interface 1/0, BRI 2/0 is deactivated when the aggregate load of serial interface 1/0 and BRI 2/0 returns to within five percent of the bandwidth of serial interface 1/0:

```
interface serial 1/0
ip address 172.20.1.4 255.255.255.0
backup interface bri 2/0
backup load 25 5
backup delay 10 60
```

Floating Static Routes

Backup interface operation is determined by the state of the line and line protocol on the primary link. It is possible that end-to-end connectivity is lost, but line protocol stays up. For example, line protocol on a

FrameRelay link is determined by the status of ILMI messages between the FrameRelay DCE (switch). Connectivity to the Frame Relay DCE does not guarantee end-to-end connectivity.

Designing Dial Backup with floating static routes utilizes Cisco IOS routing table maintenance and dynamic routing protocols. See Dial-on-Demand Routing, for examples of using Floating Static Routes to provide backup to leased lines.

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

Static AppleTalk routes and zones are created using the **appletalk static** command as in the following example:

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

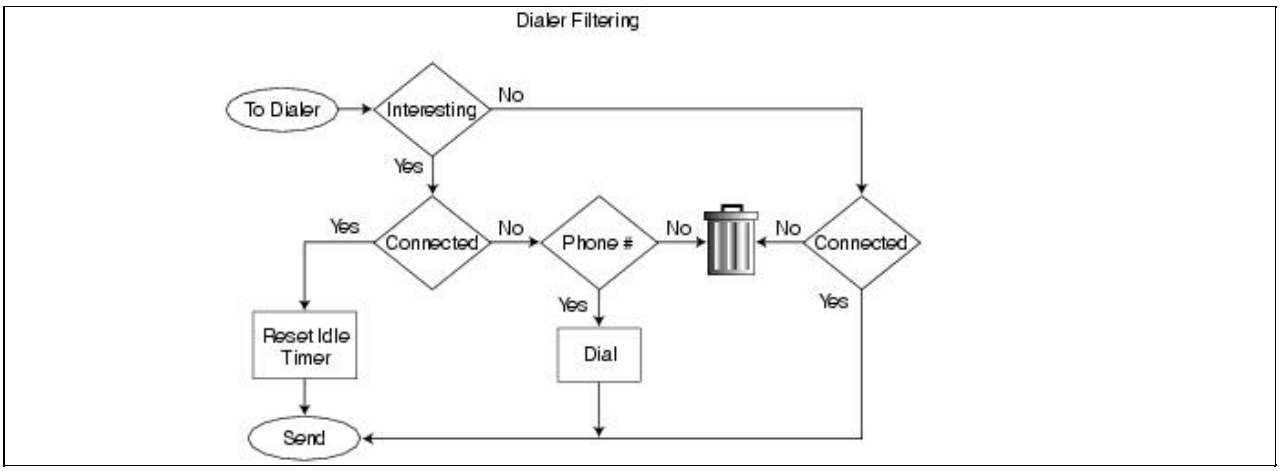
In many cases, manual configuration of static appletalk cable-ranges and zones will prove to be onerous. Snapshot routing should be investigated to provide automated route caching.

Dialer Filtering

Dialer filtering (see Figure: Dialer filtering) is used to classify all packets traversing the DDR connection as either interesting or uninteresting using Access Control Lists (ACLs). Only interesting packets can bring up and keep up DDR connections. It is the task of the DDR designer to determine which kinds of packets are to be deemed uninteresting and develop ACLs to prevent these uninteresting packets from causing unnecessary DDR connections.

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.

Figure: Dialer filtering



Each packet arriving at a dialer interface is filtered and determined to be interesting or uninteresting based on **dialer-group** and **dialer-list** configuration. The following Cisco IOS configuration interface dialer 1 uses dialer-group 5 to determine interesting packets, as defined by the dialer-list 5 commands. Dialer-group 5 is defined by dialer-list 5 commands which in this case deems all IP, IPX, and AppleTalk packets to be interesting.

```
interface Dialer1
dialer-group 5
!
dialer-list 5 protocol ip permit
dialer-list 5 protocol ipx permit
dialer-list 5 protocol appletalk permit
!
```

Cisco IOS now supports many dialer-filtering protocols, as seen by the dialer-list online help:

```
kdt-3640(config)#dialer-list 5 protocol ?
appletalk         AppleTalk
bridge            Bridging
clns              OSI Connectionless Network Service
clns_es           CLNS End System
clns_is           CLNS Intermediate System
decnet            DECnet
decnet_node       DECnet node
decnet_router-L1  DECnet router L1
decnet_router-L2  DECnet router L2
ip                IP
ipx               Novell IPX
llc2              LLC2
vines             Banyan Vines
xns               XNS
```

Defining Interesting Packets Using ACLs

Further dialer-filtering granularity is provided for each protocol by definition of Cisco IOS Access Control Lists (ACLs). For example, the following configuration defines SNMP traffic as not interesting using dialer-list 3 and extended IP ACLs:

```
dialer-list protocol ip 3 list 101
!
access-list 101 deny udp any any eq snmp
access-list 101 permit ip any any
```

Figure: Dialer filtering

Routing updates and directory services effects on Dialer interfaces can be managed by several techniques: static and default routing, passive-interfaces, or non-broadcast dialer maps. For solutions that require dynamic routing and cannot use SnapShot, routing can still be supported on the ISDN link, and then deemed uninteresting by the dialer filtering.

For example, if the internetwork design requires IGRP routing update packets, the IGRP packets can be filtered with access lists to prevent unwanted DDR connections as follows:

```
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
```

You can use one of the following two access lists to classify Enhanced IGRP traffic as uninteresting:

```
access-list 101 deny eigrp any any
access-list 101 deny ip any 224.0.0.10 0.0.0.0
```

The first access list denies all Enhanced IGRP traffic and the second access list denies the multicast address (224.0.0.10) that Enhanced IGRP uses for its updates. When you use access lists to control Enhanced IGRP traffic, you need to configure static routes to create routes across the ISDN link. When the DDR link is connected, routing updates will be able to flow across the line. In the design of DDR filtering, it is important to understand where updates and service requests are useful and where these packet types can be safely filtered.

It is important to consider closely the directory service protocols and the internetworking applications that need to be supported at each site. Numerous protocols and applications can cause DDR connections to be established and maintained, and may result in extraordinary WAN charges if not properly monitored and filtered. Don't wait until you get a phone bill surprise to perform careful traffic and costing analysis for your network. If you are concerned about WAN costs, implement network monitoring tools to provide quick feedback on connection frequency and duration.

SNMP

Although SNMP can provide useful information about ISDN connections and how they are used, using SNMP can result in excessive uptime for ISDN links. For example, HP OpenView gathers information by regularly polling the network for SNMP events. These polls can cause the ISDN connections to be made frequently in order to check that the remote routers are there, which results in higher ISDN usage charges. To control ISDN charges, the central site should filter SNMP packets destined for remote sites over ISDN. Incoming SNMP packets from remote sites can still be permitted, which allows SNMP traps to flow to the SNMP management platform. That way, if an SNMP device fails at the remote site, the alarm will reach the SNMP management platform at the central site.

To control SNMP traffic, create an access list that denies SNMP packets.The following is an example of SNMP filtering:

```
access-list 101 deny tcp any any eq 161
access-list 101 deny udp any any eq snmp
access-list 101 permit ip any any
!
dialer-list 1 list 101
```

IPX Packets

On Novell IPX internetworks, it is important to consider filtering routing updates on DDR interfaces for the protocols listed in Table: Novell IPX Update Packet Cycles.

Table: Novell IPX Update Packet Cycles

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

You can use access lists to declare as uninteresting packets intended for the Novell serialization socket (protocol number 0, socket number 457), RIP packets (protocol number 1, socket number 453), SAP packets (protocol number 4, socket number 452), and diagnostic packets generated by the autodiscovery feature (protocol number 4, socket number 456). Uninteresting packets are dropped and do not cause connections to be initiated. For a sample IPX access list, see Using ISDN Effectively in Multiprotocol Networks.

IPX sends out several types of packets that, if not controlled, cause unnecessary connections: IPX watchdog packets and SPX keepalive packets. In addition, NetWare includes a time synchronization protocol that, if not controlled, causes unnecessary connections.

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
```

Controlling IPX Watchdog Packets

NetWare servers send watchdog packets to clients and disconnect any clients that do not respond. When IPX watchdog spoofing is enabled, the router local to the NetWare server responds to watchdog packets on behalf of the server's clients. IPX watchdog spoofing allows clients to remain attached to servers without having to

constantly send packets across the ISDN link to do so. This feature is particularly important when trying to control ISDN link uptime. The interface configuration command for enabling IPX watchdog spoofing is **ipx watchdog-spoof**.

Controlling SPX Keepalive Packets

Some Sequenced Packet Exchange (SPX)-based services in the Novell environment use SPX keepalive packets. These packets are used to verify the integrity of end-to-end communications when guaranteed and sequenced packet transmission is required. The keepalive packets are generated at a rate that can be adjusted by the user from a default of one every five seconds to a minimum of one every 15 minutes. SPX spoofing as implemented in the Cisco IOS software receives, recognizes, and successfully acknowledges keepalive packets both at the server end and the client end.

Time Server and NDS Replica Packets

NetWare 4.x includes a time synchronization protocol that causes NetWare 4.x time servers to send an update every 10 minutes. To prevent the time server from generating update packets that would cause unwanted connections, you need to load a NetWare-loadable module (NLM) named TIMESYNC.NLM that allows you to increase the update interval for these packets to several days.

A similar problem is caused by efforts to synchronize NDS replicas. NetWare 4.1 includes two NLMs: DSFILTER.NLM and PINGFILT.NLM. They work together to control NDS synchronization updates. Use these two modules to ensure that NDS synchronization traffic is sent to specified servers only at the specified times.

AppleTalk Filtering

AppleTalk's user-friendly directory services are based on Zone names and the Name Binding Protocol (NBP). Applications (such as the MacOS Chooser) use NBP Lookups to look for services (such as AppleShare and Printing) by zone names. Some applications may abuse NBP services assuming that DDR networks do not exist and send broadcasts to all zones. This in turn can cause excessive dial-on-demand triggers. Applications such as QuarkXpress and 4D use all zone NBP broadcasts to periodically probe the network either for licensing purposes or to provide links to other networked resources.The **test appletalk:nbp lookup** command combined with the **debug dialer** command monitors NBP traffic and can help you determine the kinds of packets that cause connections to be made.

Beginning with Cisco IOS 11.0, you can filter NBP packets based on the name, type, and zone of the entity that originated the packet. AppleTalk NBP filtering allows Cisco routers to build firewalls, dial-on-demand triggers, and queuing options based on any NBP type or object. For a configuration example, see Using ISDN Effectively in Multiprotocol Networks. Ultimately, if the applications that use NBP have been isolated, consult the individual vendors and ask for their advice on how to control or eliminate NBP traffic.

Some Macintosh applications periodically send out NBP Lookup to all zones for numerous reasons; checking same serial number for copy protection, automatic search of other servers, and so on. As a result, the ISDN link will get brought up frequently and waste usages. In 11.0(2.1) or later, Cisco routers allow the user to configure NBP Filtering for dialer-list to prevent this problem. To do this, you should replace this line on both routers:

```
dialer-list 1 protocol appletalk permit
```

with these lines:

```
dialer-list 1 list 600
access-list 600 permit nbp 1 type AFPServer
access-list 600 permit nbp 2 type LaserWriter
access-list 600 deny other-nbps
access-list 600 permit other-access broadcast-deny
```

The previous example indicates you want to permit only two kinds of service for NBP Lookup to bring up the ISDN line. If you want to permit additional types, add to the example before the **denyother-nbps** statement. Make sure you have a different sequence number or it will overwrite the previous one. For example, if you want to also permit NBP Lookup for DeskWriter to bring up the line, the list will look like this:

```
dialer-list 1 list 600
access-list 600 permit nbp 1 type AFPServer
access-list 600 permit nbp 2 type LaserWriter
access-list 600 permit nbp 3 type DeskWriter
access-list 600 deny other-nbps
access-list 600 permit other-access broadcast-deny
```

Note: AppleShare servers use the Apple Filing Protocol (AFP) to send out tickles approximately every 30 seconds to connected AppleShare clients. These tickles will cause DDR connections to stay up. To avoid unwanted DDR connections, you must manually unmount AppleTalk servers or install software on the servers that automatically disconnects idle users after a timeout period.

Banyan VINES, DECnet IV, and OSI Packets

Cisco IOS 10.3 introduced access lists for Banyan VINES, DECnet IV, and the Open Systems Integration (OSI) protocol. When a dialer map is configured for these protocols, access lists can be used to define interesting packets (that is, packets that will trigger the DDR link).

Authentication

Authentication in DDR network design provides two functions: security and dialer state. As most DDR networks connect to the Public Switched Telephone Network, it is imperative that a strong security model be implemented to prevent unauthorized access to sensitive resources. Authentication also allows the DDR code to keep track of what sites are currently connected and provides for building of MultiLink PPP bundles. The following issues are addressed:

- PPP Authentication
- CHAP
- PAP
- ISDN Security
- DDR Callback
- IPX Access Lists

PPP Authentication

PPP Authentication via CHAP or PAP (as described in RFC 1334) should be used to provide security on DDR connections. PPP authentication occurs after LCP is negotiated on the DDR connection, but before any network protocols are allowed to flow. PPP Authentication is negotiated as an LCP option, and is bidirectional, meaning each side can authenticate the other. In some environments, it may be necessary to enable PPP authentication on the call-in side only (meaning the calling side does not authenticate the called side).

CHAP

With CHAP, a remote device attempting to connect to the local router is presented with a CHAP challenge containing the host name and a challenge seed. When the remote router receives the challenge, it looks up the hostname received in the challenge and replies with the hostname and a CHAP response derived from the challenge seed and the password for that hostname. 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 nas3600A will allow Router c1600A to call in using the password "bubble":

```
hostname nas3600A
username c1600A password bubble
!
interface dialer 1
ppp authentication chap callin
```

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

```
hostname c1600A
username nas3600A password bubble
!
interface dialer 1 encapsulation ppp
dialer in-band
dialer-group 5
dialer map ip 172.20.1.1 name nas3600A 18355558661
ppp authentication chap callin
```

The following steps illustrate the CHAP process:

1. c1600A calls nas3600A and LCP is negotiated.
2. nas3600A challenges c1600A with: <nas3600A/challenge_string>.
3. c1600A looks up the password for username nas3600A and generates response_string.
4. c1600A sends response to c3600A: <nas1600A/response_string>.
5. c3600A looks up the password for username c1600A and generates the expected response_string. If the response_string received matches the response string expected, PPP authorization passes, and the PPP can negotiate the network control protocols (such as IPCP). If it fails, the remote site is disconnected.

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 in clear text, which makes it susceptible to sniffer attack.

When being authenticated with PAP, the router looks up the username that matches the dialer map used to initiate the call. When being authenticated with PAP on a receiving call, PAP looks up the username associated with its hostname (because no dialer map was used to initiate the connection).

In the following configuration, the NAS router will authenticate the peer with PAP when answering the DDR call, and compare the result to the local database:

```
hostname nas3600A
aaa new-model
aaa authentication ppp default local
username c2500A password freedom
username nas3600A password texas
!
```

```
interface Dialer1
encapsualtion ppp
ppp authentication pap
```

ISDN Security

ISDN DDR can use caller-ID for enhanced security by configuring ISDN caller on the incoming ISDN interfaces. Incoming calls are screened to verify that the calling line ID is from an expected origin. However, caller-ID screening requires an end-to-end ISDN connection that can deliver the caller-ID to the router.

DDR Callback

DDR environments can be configured for callback operations. When a remote site dials into a central site (or the opposite), the central site can be configured to disconnect and initiate an outbound DDR connection to the remote site.

DDR callback provides enhanced security by ensuring that the remote site can connect only from a single location as defined by the callback number. DDR callback can also enhance administration by centralizing billing for remote DDR connections.

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.

Summary

When designing DDR internetworks, consider the 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.

For further guidance on building DDR networks, including protocol-specific examples, see Scaling Dial-on-Demand Routing, and Using ISDN Effectively in Multiprotocol Networks.