

Deciding and Preparing to Configure DDR

This chapter presents the decisions and preparations leading to a DDR configuration and shows where some advanced features fit into the DDR configuration steps. It distinguishes between the topology decisions and the implementation of the decisions. In the implementation phase, it distinguishes the DDR-independent decisions from the DDR-dependent decisions.

For a complete description of the global dialer commands in this chapter, refer to the *Dial Solutions Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

This chapter provides the following information:

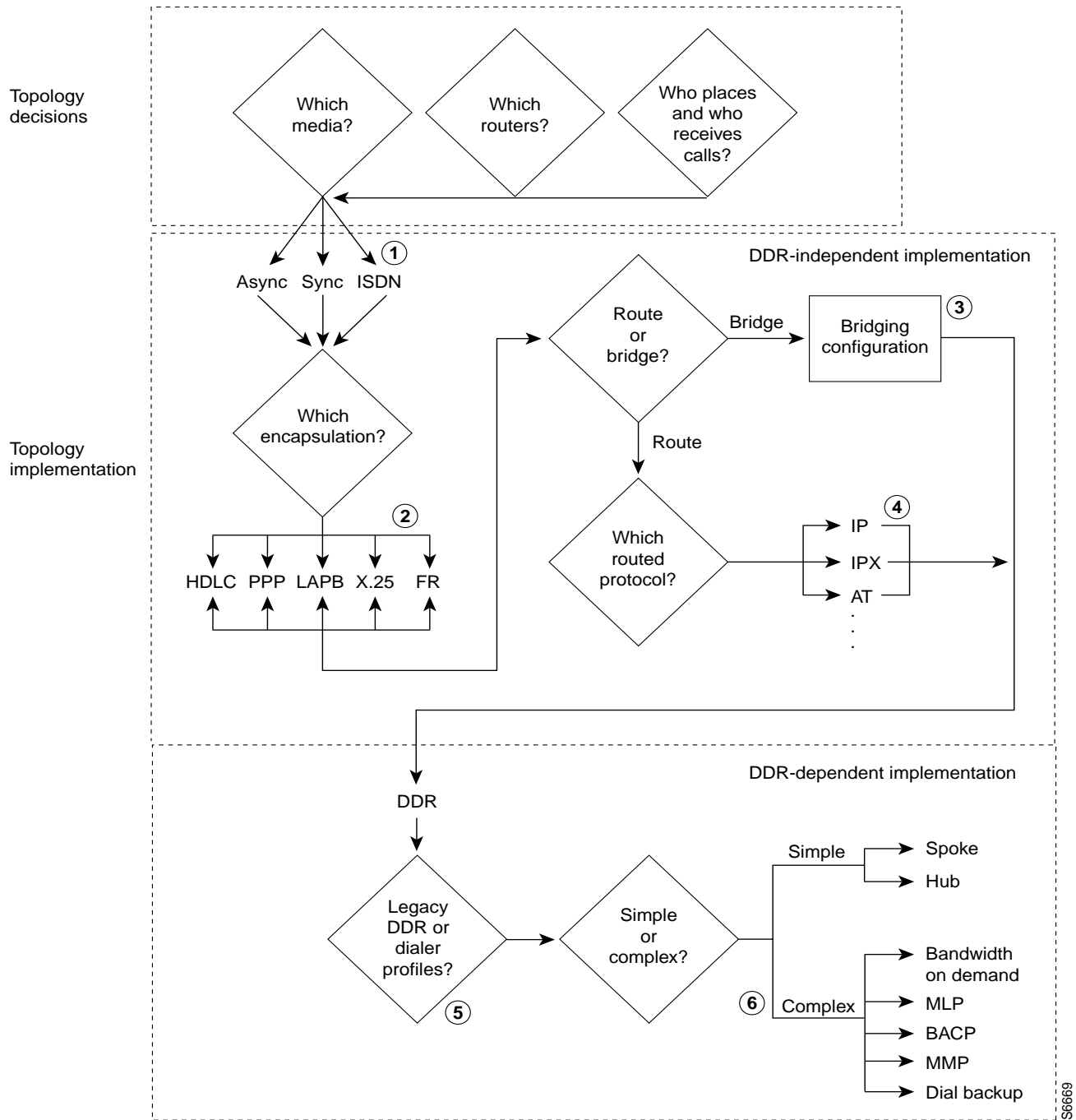
- **Decision Flowchart**
A flowchart of topology and implementation decisions you will need to make before you configure DDR
- **Topology Decisions, DDR-Independent Implementation Decisions, and DDR-Dependent Implementation Decisions**
References to sources of detailed information for the configuration steps associated with each decision
- **Global and Interface Preparations for DDR**
Brief description indicating which preparations are global and which are interface-specific.
- **Preparations for Routing or Bridging over DDR**
A description of the required steps to be completed for bridging or routing over DDR.

Decision Flowchart

This section provides a flowchart of the decisions to be made before and while you configure DDR and notes to the flowchart.

Figure 289 presents the entire decision flowchart. The decision phases are shown in separate boxes. Numbers in parentheses refer to notes, which are located on the next page.

Figure 289 Decisions and Implementation Flow to DDR



Notes to the Flowchart. The DDR chapters do not provide complete configuration information for most of the items in the following list. However, detailed information is available in other chapters and manuals. The numbers in this list correspond to the circled numbers in the flowchart.

- 1 Configuration of the dial port and interface. The port, line, and interface are expected to be configured and operational before you configure DDR. See the relevant chapters in the “Dial-In Port Setup” part of this manual.

- 2 Encapsulation; including encapsulation for other wide-area networks. See the “Configuring Media-Independent PPP and Multilink PPP” chapter of this manual for PPP encapsulation and see the *Wide-Area Networking Configuration Guide* for Frame Relay and X.25.
- 3 Bridging configurations. See the *Bridging and IBM Networking Configuration Guide*.
- 4 Routed protocols to be supported. See the protocol-specific chapters and manuals.
- 5 Dialer Profiles and Legacy DDR are described in different chapters of the “Dial-on-Demand Routing” part of this manual.
- 6 Complex DDR configurations. See the “Media-Independent PPP and Multilink PPP” chapter and the “Cost-Control Solutions” and the “Large-Scale Solutions” sections of this manual.

The DDR chapters provide complete configuration information about the simple spoke and hub DDR configurations, about the Dialer Profiles implementation of DDR, and about preparations required for configuring asynchronous interfaces for DDR.

Topology Decisions

Topology decisions determine which routers will use DDR, which media and interfaces each one will use for DDR, and how each interface will function when using DDR. For example, if you choose a hub-and-spoke topology, one router will communicate with multiple routers. You must decide whether that router will use one interface or multiple interfaces for DDR, and whether it will receive calls only (forcing the spokes to initiate and bear the cost of calls). If it will use multiple interfaces, you must decide whether they will be of different types or the same type.

DDR-Independent Implementation Decisions

DDR-independent implementation decisions include

- Using a specific interface or combination of interfaces for DDR.

For complete configuration steps for the various media and interfaces, see the chapters in the “Dial-In Port Setup” part of this manual.

- Using nondefault encapsulations.

The default encapsulation is HDLC. However, PPP is widely used for situations in which authentication is desired, especially situations in which an interface will receive calls from multiple sites. Detailed PPP encapsulation requirements are described in the “Configuring Media-Independent PPP and Multilink PPP” and “Configuring Asynchronous PPP and SLIP” chapters of this manual.

If you decide to send dial-on-demand traffic over Frame Relay, X.25, or LAPB networks, the interface must be configured with the appropriate encapsulation. For configuration details, see the related chapter in the *Wide-Area Networking Configuration Guide*.

- Routing or bridging the DDR traffic.

Legacy DDR supports bridging to only one destination, but Dialer Profiles supports bridging to multiple destinations.

If you decide to bridge traffic over a dial-on-demand connection, configure the interface for transparent bridging. For detailed information, see the “Configuring Transparent Bridging” chapter of the *Bridging and IBM Networking Configuration Guide*.

- Supporting one or more specific routed protocols, if you decide to route traffic.

Depending on the protocol, you do need to control access by entering access lists and decide how to support network addressing on an interface to be configured for DDR. You might also need to spoof keepalive or other packets. For configuration details, see the related network protocol chapters in the *Network Protocols Configuration Guide, Part 1* and *Network Protocols Configuration Guide, Part 2*, and *Network Protocols Configuration Guide, Part 3*.

DDR-Dependent Implementation Decisions

You must decide whether to implement Legacy DDR or the newer Dialer Profiles; both are documented in the “Dial-on-Demand Routing” part of this manual. You must also decide whether a simple DDR configuration meets your business needs or whether to add on other features.

Dialer Profiles

The Dialer Profiles implementation of DDR is based on a separation between logical and physical interface configuration. Dialer Profiles also allows the logical and physical configurations to be bound together dynamically on a per-call basis.

Dialer Profiles is advantageous when you want to share an interface (ISDN, asynchronous, or synchronous serial) to place or receive calls, when you want to change any configuration on a per-user basis (except encapsulation in the first phase of Dialer Profiles), when you want to bridge to many destinations, and for avoiding split horizon problem.

Most routed protocols are supported; however, Frame Relay, ISO CLNS, and LAPB are not supported.

If you decide to configure Dialer Profiles, you must disable validation of source addresses for the routed protocols you support.

For detailed Dialer Profiles information, see the “Configuring Peer-to-Peer DDR with Dialer Profiles” chapter.

Legacy DDR

Legacy DDR is powerful and comprehensive, but its limitations affect scaling and extensibility. Legacy DDR is based on a static binding between the per-destination call specification and the physical interface configuration.

However, Legacy DDR also has many strengths. It supports Frame Relay, ISO CLNS, LAPB, snapshot routing, and all routed protocols that are supported on Cisco routers. By default, Legacy DDR supports fast switching.

For information about simple Legacy DDR spoke configurations, see the “Configuring Legacy DDR Spokes” chapter. For information about simple Legacy DDR hub configurations, see the “Configuring Legacy DDR Hubs” chapter.

Simple or Complex DDR Configuration

You must also decide whether to implement a simple DDR configuration—whether it is a simple point-to-point (spoke-to-spoke) layout or a simple hub-and-spoke layout—or to add on features that make the implementation more complex. Add-on features include dial backup, bandwidth on demand, application of the Bandwidth Allocation Control Protocol (BACP), Multilink PPP, and many others.

For information about add-on features, see the chapters in the “Cost Control Solutions” and “Large-Scale Solutions” parts of this manual.

Global and Interface Preparations for DDR

Some preparations are global in nature and some depend on the type of interface you will configure for DDR.

Global Preparations

After you have made the required global decision whether to bridge or to route a specified protocol over a dial-on-demand link, you can make the following preparations:

- If you choose to bridge the protocol, decide whether to allow bridge packet access by Ethernet type codes or to permit all bridge packets across the link. Allowing access by Ethernet type codes requires you to define a bridging access list in global configuration mode.

Allowing all bridge packets to trigger calls across a dial-on-demand link to a single destination is a DDR-dependent task addressed in the “Configure Dialer Access Lists to Trigger Outgoing Calls” section of both the “Configuring Legacy DDR Spokes” and “Configuring Legacy DDR Hubs” chapters.

Bridging to multiple destinations requires Dialer Profiles.

- If you choose to route the protocol
 - Define one or more access lists for the selected routed protocol to determine which packets should be permitted or denied access to the dial-on-demand link.

Allowing those packets to trigger calls across a dial-on-demand link is a DDR-dependent task addressed in the “Configure Dialer Access Lists to Trigger Outgoing Calls” section of both the “Configuring Legacy DDR Spokes” and “Configuring Legacy DDR Hubs” chapters.
 - Define an appropriate dialer list for the protocol.
 - Disable validation of source addresses, if you decide to configure Dialer Profiles.

Preparations Depending on the Selected Interface Type

The steps shown in this chapter assume that you have also completed the required preparatory steps for the type of interface you will configure for DDR:

- The interface is installed, the cable is connected as needed, and operational.
- Chat scripts are ready, as needed, for any asynchronous interfaces and modem scripts have been assigned to the relevant asynchronous lines.
- Asynchronous lines and modems are configured and operational, as needed.
- Any ISDN line that will be used for DDR is properly provisioned and running.
- You have decided which interfaces and how many interfaces are to be configured for DDR, and what functions each interface will perform.

Preparations for Routing or Bridging over DDR

The following tasks are DDR-independent and can be completed before you configure DDR. Minimal tasks required for each item are presented in this chapter. For detailed information about bridging, routing, and wide-area networking configurations, refer to the appropriate chapters in other manuals of the Cisco IOS documentation set.

Complete the following minimal tasks for the global decisions you have made:

- Prepare for Transparent Bridging over DDR
- Prepare for Routing over DDR

Prepare for Transparent Bridging over DDR

To prepare for transparent bridging over DDR, complete the tasks in the following sections:

- Define the Protocols to Bridge
- Specify the Bridging Protocol
- Control Bridging Access

Define the Protocols to Bridge

IP packets are routed by default unless they are explicitly bridged; all others are bridged by default unless they are explicitly routed. To bridge IP packets, use the following command in global configuration mode:

Command	Purpose
no ip routing	Disable IP routing.

If you choose *not* to bridge another protocol supported on your network, use the relevant command to enable routing of that protocol. For more information about tasks and commands, refer to the relevant protocol chapter in either the *Network Protocols Configuration Guide, Part 1*, *Network Protocols Configuration Guide, Part 2*, and *Network Protocols Configuration Guide, Part 3*.

Specify the Bridging Protocol

You must specify the type of spanning tree bridging protocol to use and also identify a bridge group. To specify the spanning tree protocol and a bridge group number, use the following command in global configuration mode:

Command	Purpose
bridge <i>bridge-group</i> protocol {ieee dec}	Define the type of spanning tree protocol and identify a bridge group.

The bridge-group number is used when you configure the interface and assign it to a bridge group. Packets are bridged only among members of the same bridge group.

Control Bridging Access

You can control access by defining any transparent bridge packet as *interesting*, or you can use the finer granularity of controlling access by Ethernet type codes.

To control access by Ethernet type codes, use the following commands in global configuration mode:

Command	Purpose
access-list <i>access-list-number</i> { permit deny } <i>type-code</i> [<i>mask</i>]	Identify interesting packets by Ethernet type codes (access list numbers must be in the range 200–299).
dialer-list <i>dialer-group</i> protocol bridge list <i>access-list-number</i>	Define a dialer list for the specified access list.

Packets with a specified Ethernet type code can trigger outgoing calls. Spanning tree bridge protocol data units (BPDUs) are always treated as *uninteresting* and cannot trigger calls.

For a table of some common Ethernet types codes, see the “Ethernet Types Codes” appendix in the *Bridging and IBM Networking Command Reference*.

To identify all transparent bridge packets as interesting, use the following command in global configuration mode:

Command	Purpose
dialer-list <i>dialer-group</i> protocol bridge permit	Define a dialer list that treats all transparent bridge packets as interesting.

Prepare for Routing over DDR

DDR supports the following routed protocols: AppleTalk, Banyan VINES, DECnet, IP, Novell IPX, ISO CLNS, and XNS.

To prepare for routing a protocol over DDR, perform the tasks in the relevant section:

- Configure the Protocol for Routing and Access Control
- Associate the Protocol Access List with a Dialer Group

Configure the Protocol for Routing and Access Control

This section specifies the minimal steps required to configure a protocol for routing over DDR. For more options and more detailed descriptions, refer to the relevant protocol chapter.

Configure IP Routing

IP routing is enabled by default on Cisco routers; thus no preparation is required simply to enable it. You might, however, need to decide your addressing strategy and complete other global preparations for routing IP in your networks. To use dynamic routing where multiple remote sites communicate with each other through a central site, you might need to disable the IP split horizon feature. See the “Configuring IP Addressing” chapter in the *Network Protocols Configuration Guide, Part 1* for more information.

At a minimum, you must complete the following tasks.

- Disable validation of source addresses.
- Configure one or more IP access lists before you refer to the access lists in DDR **dialer-list** commands to specify which packets can trigger outgoing calls.

To disable validation of source addresses, use the following commands beginning in global configuration mode:

Command	Purpose
router rip	Specify the routing protocol; RIP, for example.
no validate-update-source	Disable validation of source addresses.
network number	Specify the IP address.

For more information about IP routing protocols, see the *Network Protocols Command Reference, Part 1*.

To configure IP access lists, use one of the following commands in global configuration mode:

Command	Purpose
access-list access-list-number {deny permit} source [source-mask]	Specify an IP standard access list.
or	
access-list access-list-number {deny permit} protocol source source-mask destination destination-mask [operator operand]	Specify an IP extended access list.

You can now also use simplified IP access lists that use the abbreviation *any* instead of the numeric forms of source and destination addresses and masks. Other forms of IP access lists are also available. For more information, see the “IP Services Commands” chapter in the *Network Protocols Command Reference, Part 1*.

For an example of configuring DDR for IP, see the “Configuring a Legacy DDR Spoke” or “Configuring a Legacy DDR Hub” chapter.

You can configure IP routing on DDR asynchronous, synchronous serial, and ISDN interfaces, as well as dialer rotary groups.

Configure Novell IPX Routing

To configure routing of IPX over DDR, you must complete both global and interface-specific tasks:

Step 1 Enable IPX routing globally.

Step 2 Enable IPX watchdog spoofing, or enable SPX keepalive spoofing on the interface.

To enable IPX routing, use the following command in global configuration mode:

Command	Purpose
ipx routing [node]	Enable IPX routing.

To enable IPX watchdog spoofing on the interface, use the following command in interface configuration mode:

Command	Purpose
ipx watchdog-spoof	Enable IPX watchdog spoofing.

To enable SPX keepalive spoofing, use the following commands in interface configuration mode:

Command	Purpose
ipx spx-spoof	Enable SPX keepalive spoofing.
ipx spx-idle-time <i>delay-in-seconds</i>	Set the idle time after which SPX spoofing begins.

You can configure IPX routing on DDR asynchronous, synchronous serial, and ISDN interfaces, as well as dialer rotary groups.

For detailed DDR for IPX configuration examples, see the “IPX over DDR Example” section in the “Configuring Novell IPX” chapter of the *Network Protocols Configuration Guide, Part 1*.

Configure AppleTalk Routing

You must enable AppleTalk routing and then specify AppleTalk access lists. After you specify AppleTalk access lists, define dialer lists. Use the **dialer-list protocol** command to define permit or deny conditions for the entire protocol; for a finer granularity, use the **dialer-list protocol** command with the **list** keyword.

You can configure AppleTalk routing on DDR asynchronous, synchronous serial, and ISDN interfaces, as well as dialer rotary groups.

See the “Configuring a Legacy DDR Spoke” chapter or “Configuring a Legacy DDR Hub” chapter for more information and examples.

Configure Banyan VINES Routing

To configure DDR for Banyan VINES, use one of the following commands in global configuration mode:

Command	Purpose
vines access-list <i>access-list-number</i> { permit deny } <i>source source-mask</i>	Specify a VINES standard access list.
or	
vines access-list <i>access-list-number</i> { permit deny } <i>source source-mask [destination] [destination-mask]</i>	Specify a VINES extended access list.

After you specify VINES standard or extended access lists, define DDR dialer lists. Use the **dialer-list protocol** command to define permit or deny conditions for the entire protocol; for a finer granularity, use the **dialer-list protocol** command with the **list** keyword. See the “Configuring a Legacy DDR Spoke” chapter or “Configuring a Legacy DDR Hub” chapter for more information and examples.

You can configure Banyan VINES on DDR asynchronous, synchronous serial, and ISDN interfaces, as well as dialer rotary groups.

Note The Banyan VINES “neighbor” command is not supported for LAPB and X.25 encapsulations.

Configure DECnet Routing

To configure DDR for DECnet, use one of the following commands in global configuration mode:

Command	Purpose
access-list <i>access-list-number</i> { permit deny } <i>source</i> <i>source-mask</i>	Specify a DECnet standard access list.
or	
access-list <i>access-list-number</i> { permit deny } <i>source</i> <i>source-mask</i> [<i>destination</i>] [<i>destination-mask</i>]	Specify a DECnet extended access list.

After you specify DECnet standard or extended access lists, define DDR dialer lists. Use the **dialer-list protocol** command to define permit or deny conditions for the entire protocol; for a finer granularity, use the **dialer-list protocol** command with the **list** keyword. See the “Configuring a Legacy DDR Spoke” chapter or “Configuring a Legacy DDR Hub” chapter for more information and examples.

You classify DECnet control packets, including hello packets and routing updates, using one or more of the following commands: **dialer-list protocol decnet_router-L1 permit**, **dialer-list protocol decnet_router-L2 permit**, and **dialer-list protocol decnet_node permit**.

You can configure DECnet on DDR asynchronous, synchronous serial, and ISDN interfaces, as well as dialer rotary groups.

Configure ISO CLNS Routing

To configure ISO CLNS for DDR, use the following commands, beginning in global configuration mode:

Step	Command	Purpose
1	cls filter-set <i>name</i> { permit deny } <i>template</i>	Specify one or more CLNS filters, repeating this command as needed to build the filter list associated with the filter name.
2	interface <i>type number</i>	Specify the interface to apply the filter to.
3	cls access-group <i>name out</i>	Filter CLNS traffic going out of the interface, on the basis of the filter specified and named in Step 1.

After you complete these CLNS-specific steps, define a dialer list for CLNS. Use the **dialer-list protocol** command to define permit or deny conditions for the entire protocol; for a finer granularity, use the **dialer-list protocol** command with the **list** keyword. Use the *access-group* argument with this command, because ISO CLNS uses access groups but does not use access lists. See the “Configuring a Legacy DDR Spoke” chapter or “Configuring a Legacy DDR Hub” chapter for more information and examples.

You classify CLNS control packets, including hello packets and routing updates, using the **dialer-list protocol cls_is permit** and/or **dialer-list protocol cls_es permit** command.

You can configure ISO CLNS on DDR asynchronous, synchronous serial, and ISDN interfaces, as well as dialer rotary groups.

Configure XNS Routing

You must enable XNS routing and then define an access list.

To define an XNS access list, use one of the following commands in global configuration mode:

Command	Purpose
access-list <i>access-list-number</i> { deny permit } <i>source-network</i> [. <i>source-address</i> [<i>source-address-mask</i>]] [<i>destination-network</i> [<i>destination-address</i> [<i>destination-address-mask</i>]]]	Specify a standard XNS access list.
or	
access-list <i>access-list-number</i> { deny permit } <i>protocol</i> [<i>source-network</i> [. <i>source-host</i> [<i>source-network-mask</i> .] <i>source-host-mask</i>] <i>source-socket</i> [<i>destination-network</i> [<i>destination-host</i> [<i>destination-network-mask</i> . <i>destination-host-mask</i>] <i>destination-socket</i> [/ pep]]]	Specify an extended XNS access list.

After you specify an XNS access list, define a DDR dialer list. Use the **dialer-list protocol** command to define permit or deny conditions for the entire protocol; for a finer granularity, use the **dialer-list protocol** command with the **list** keyword. See the “Configuring a Legacy DDR Spoke” chapter or “Configuring a Legacy DDR Hub” chapter for more information and examples.

You can configure XNS on DDR asynchronous, synchronous serial, and ISDN interfaces, as well as dialer rotary groups.

Associate the Protocol Access List with a Dialer Group

DDR supports the following routed protocols: AppleTalk, Banyan VINES, DECnet, IP, Novell IPX, ISO CLNS, and XNS.

You can permit or deny access by protocol, or you can specify an access list for more refined control. To associate a protocol or access list with a dialer group, use the following command in global configuration mode:

Command	Purpose
dialer-list <i>dialer-group</i> protocol <i>protocol-name</i> { permit deny list <i>access-list-number</i> <i>access-group</i> }	Associate a protocol access list number or access group name with the dialer group.

Note For a given protocol and a given dialer group, only one access list can be specified in the **dialer-list** command.

For the **dialer-list protocol list** command form, acceptable access list numbers are

- Banyan VINES, DECnet, IP, and XNS standard and extended access list numbers
- Novell IPX standard, extended, and SAP access list numbers
- AppleTalk access lists numbers
- Bridge type codes

