Advanced Cisco Router Configuration Exam Study Guide

1. **Describe the key requirements of scalable internetwork?**
   Core – responsible for reliable transport, typically includes LAN and WAN backbones. Need to be highly reliable, because outages affects routing on a large scale.
   Distribution – responsible for providing quality of service (QOS) for various types of protocols by using policy based traffic control. Need to be able to select the best path to different locations in order to make the best use of bandwidth.
   Access – localizes broadcasts, provides authentication and encryption services for the network.

2. **Select a Cisco IOS feature as a solution for a given internetwork requirement.**
   Reliable and available:
   - Reachability – Scalable routing protocols such as OSPF, EIGRP, and NLSP use metrics that expand the reachability potential for routing updates because they use cost, rather than hop count, as a metric.
   - Fast convergence time – Scalable protocols can converge quickly because of the router's ability to detect failure rapidly and because it only sends changes not the entire routing table.
   - Alternate Paths – Scalable protocols, such as EIGRP and OSPF keep record of alternate routes in case the preferred route is not available.
   - Load balancing – Because scalable protocols maintain entire network topology, they are able to transport data across multiple paths to a given location simultaneously.
   - Tunnels – ability to transport various protocols within IP
   - Dial backup – Use the backup link when the primary fails or when the primary is congested.

   Responsive:
   - Weighted fair queuing – An automated method that provides fair bandwidth allocation to all network traffic. It ensures that high-bandwidth conversations do not consume all bandwidth.
   - Priority queuing – A particular traffic type is prioritized higher than all other traffic types.
   - Custom queuing – Each traffic type gets a minimum of the share bandwidth at all times.

   Efficient:
   - Access lists – Can be used to permit or drop protocol update traffic, data traffic, and broadcast traffic.
   - Snapshot routing – Allows peer routers to exchange full distance vector routing information upon initial connection, then on a predefined interval.
   - Compression over WANs – Cisco supports TCP/IP header compression and data (payload) compression.
   - Dial-on-demand routing – Active links are created only after the router detects interesting traffic.
   - Switched access – Packet-switched networks (X.25 or Frame Relay)
   - Route summarization – Supported by RIP 2, EIGRP, OSFP
   - Incremental updates – Sends only the topology changes when the changes occur rather than the entire routing table contents at fixed intervals.

   Adaptable:
   - Network must support routable and nonroutable traffic

   Accessible but secure:
   - Dedicated access – T1/E1
   - Switched access – Frame Relay, X.25, SMDS, and ATM
   - Exterior protocol support – Exterior Gateway Protocol (EGP) and Border Gateway Protocol (BGP)
   - Access lists – Can be used to permit or drop protocol update traffic, data traffic, and broadcast traffic.
   - Authentication protocols – WAN connections using PPP, we can use PAP or CHAP.

3. Describe causes of network congestion.

4. List solutions for controlling network congestion.

Congestion occurs when the data traffic exceeds the data-carrying capacity of the link

Traffic in an IP Network (Sources of data and overhead traffic):

- User applications
- Routing protocol updates
- Domain name server (DNS) requests
- Encapsulated protocol transport

Traffic in an IPX Network (Sources of data and overhead traffic):

- User services
- Routing protocol updates
- Service Advertising Protocol (SAP) announcements
- Client/Server keepalive updates

Datalink layer Traffic concerns

- Address Resolution Protocol (ARP) to resolve logical-to-physical addressing issues
- Keepalives to maintain connectivity
- Tokens for accessibility
- Time to Live updates

Control network congestion by:

- Filtering user and application traffic.
- Filtering broadcast traffic
- Adjusting timers on periodic announcements
- Providing static entries in tables
- Prioritizing traffic

5. Configure IP standard access lists.

Permit or deny packets based only on the source IP address of the packet.
Access list range: 1 – 99

Define a standard access list (numbered 1-99):
Router(config)# *access-list ## {permit | deny} {source [source-wildcard] | any}*

Apply an access list to a specific interface:
Router(config-if)# *ip access-group ## {in | out}*

Implicit deny any – unless you end your access list with an explicit permit any, it will deny by default all traffic that fails to match any of the access list lines.

6. Limit virtual terminal access.

There are five virtual terminal lines, numbered vty 0 through 4. You must set identical restrictions on all virtual terminal lines because you cannot control on which virtual terminal line a user will connect.

Enter configuration mode for a terminal line or a range of lines:
Router(config)# *line {vty-# | vty-range}*

Apply a standard access list to restrict incoming and outgoing connections
Router(config-line)# *access-class access-list-number {in | out}*

Example:

```
Access-list 12 permit 192.89.55.0  0.0.0.255
!
line vty 0 4
access-class 12 in
```

Permits only hosts in network 192.89.55.0 to connect to the virtual terminal ports on the router.

7. Configure IP extended access lists

Enables filtering based on the session-layer protocol, destination address, and application port number.
Access list range: 100 – 199

Syntax:

Access-list access-list-number {permit | deny} {protocol|protocol-keyword} {source source-wildcard | any} {destination destination-wildcard | any} [protocol-specific options] [log]

8. Verify access list operation.

show access-list (*Displays access lists from all protocols*)

show ip access-list [access-list-number] (*Displays a specific IP access list*)

clear access-list counters [access-list-number] (*Clears packet counts*)

show line (*Displays line configuration*)

9. Configure an alternative to using access lists.

Null Interface

It is a software-only interface which saves CPU cycles by using a static route to drop packets.

Syntax:

Ip route address mask null 0

10. Configure an IP helper address to manage broadcasts.

- Routers do not forward broadcasts, by default.
- Helper address provides selective connectivity by forwarding these broadcasts directly to the target server or target network.
- Helper command change broadcasts addresses to unicast or directed broadcast addresses so that the broadcast message can be routed to a specific destination.

Syntax:

Router(config-if)# *ip helper-address {address}*

Router(config)# *ip forward-protocol {udp [port]* | *nd* | *snds}* specific protocols

11. Describe IPX/SPX traffic management issues.

As IPX internetworks grow, slower and more expensive WAN links are incorporated into the internetwork. Netware broadcast traffic can use a significant portion of the available WAN bandwidth.

IOS tools to manage IPX traffic

- Traffic filtering - access lists can be used to filter source and destination network address or socket.
- IPX broadcast filtering – access lists can be used to restrict SAP and RIP broadcasts.
- WAN connectivity – you can tunnel IPX traffic through an IP network.
- Spoofing – Periodic update spoofing for WAN links
- GNS filtering – access list can be used to configure GNS replies from the router.

12. Filter IPX traffic using IPX access lists.
13. Manage IPX traffic over WAN connections.

IPX standard access-lists (800-899)

Syntax:

Router(config)# access-list ### {permit | deny} source-network or node destination-network or node

Router(config-if)# ipx access-group ### [in | out]

IPX extended access-lists (900-999) – uses source and destination sockets in addition to above.

SAP Filter Configuration (1000-1099)

Syntax:

Create a SAP access-list
Router(config)# access-list #### {deny | permit} network [service-typ [server-name]]

Apply SAP filter to the interface
Router(config-if)# ipx {input-sap-filer | output-sap-filer} access-list-number

Service Type (SAP) Example:

File server 4
Print server 7

Filtering RIP Traffic

Use **ipx input-network-filter** and **ipx output-network-filter** commands to control which networks are added to the router's routing table. The ipx output-network-filter command applies to IPX RIP only. Use the distribute-list out command to control advertising of EIGRP routes.

SAP/GNS Operations

The ipx output-gns-filter command is used with the access-list command to control which servers are included in GNS responses.

Use the ipx sap-interval command to configure less frequent SAP updates.

14. Verify IPX/SPX filter operations.

Show ipx interface – Displays the status of the IPX interfaces
Show ipx route – Lists the entries of the IPX routing table
Show ipx servers – Lists the servers discovered through SAP advertisements
Show ipx traffic – Shows ipx packet information.

Ethernet	novell-ether (default) arpa sap snap	Ethernet_802.3 Ethernet_II Ethernet_802.2 Ethernet_Snap
Token Ring	sap (default) snap	Token-Ring Token-Ring_Snap
FDDI	Snap (default) Sap	Fddi_Snap Fddi_802.2

15. Describe the need for queuing in a large network.
16. 17. 18. Describe 3 types of queuing in Cisco.

First-in, first-out (FIFO) queuing has been the classic algorithm for routers.

Cisco IOS offers 3 queuing options as an alternative to FIFO queuing:

- Weighted fair queuing(WFQ) prioritizes interactive traffic over file transfers in order to enduser satisfactory response time for common users applications. WFQ is default for serial interfaces at E1 speed (2.048 Mbs) and below.
- Priority queuing ensures timely delivery of a specific protocol or type of traffic because that traffic is transmitted before all others.

Configuration:

Set priority by protocol type
Router(config)# **priority-list** ## **protocol** protocol-name {high,medium,normal,low}

Set priority by imcoming interface type
Router(config)# **priority-list** ## **interface** interface-type {high,medium,normal,low}

Assign a default queue
Router(config)# **priority-list** ## default {high,medium,normal,low}

Specifie the queue size
Router(config)# **priority-list** ## queue-limit high-limit medium-limit normal-limit low-limit

Links priority list to an interface
Router(config-if)# **priority-group** ##

- Custom queuing establishes bandwidth allocations for each different type of traffic.

  Queues handled in round-robin fashion. With custom queuing you reserve a certain percentage of bandwidth for each specified class of traffic. You can use custome queuing to allocate bandwidth based on a protocol or source interface. Possible queues (1 to 16)

  Configuration:

  Set queue priority by protocol type
  Router(config)# **queue-list** ## **protocol** protocol-name queue-number

  Set priority by interface type
  Router(config)# **queue-list** ## **interface** interface-type interface-number queue-number

  Assign a priority queue for all other packets
  Router(config)# **queue-list** ## **default** queue-number

  Change the capacity of a queue
  Router(config)# **queue-list** ## **queue** queue-number **limit** limit-number

  Assign threshold byte count per queue per transfer
  Router(config)# **queue-list** ## **queue** queue-number **byte-count** byte-count number

  Assign a queue list to an interface
  Router(config-if)# **custom-queue-list** ##

19. List the key information routers need to route data.

To be able to route anything, a router needs to know the following key information.

- The destination, or address of the item that needs to be routed.
- From which source it can learn the paths to given destination.
- Possible routes, or paths, to intended destination.
- The best path(s) to the intended destination.
- A way of verifying that the known paths to destination are the most current.

20. Compare distance vector and link-state protocol operation.

Protocol Categories	**Distance Vector**	**Link State**
Characteristics	Older, for small networks	Newer, for large networks
Supported Protocols	RIP, IGRP, RTMP	OSPF, NLSP, IS-IS

21. Given an IP address, use VLSMs to extend the use of the IP address.
22. Given a network plan that includes IP addressing, explain if route summarization is or is not possible.

Two addressing issues have resulted from internet growth.

- IP address exhaustion
- Routing table growth and manageability.

Benefits of Hierarchical Addressing

- Effcient allocation of addresses – continues address assignment.
- Reduce the number of route table entries using summaries.

VLSMs can be used when the routing protocol sends a subnet mask along with each network address. The protocols that support this are RIP2, OSPF, EIGRP, BGP, and ISIS.

Route Summarization – Routing protocols can summarize addresses of several networks into one address. Route summarization is supported by RIP2, OSPF, and EIGRP based on subnet addresses, including VLSM addressing.

23. Define private addressing and determine when it can be used.

Following IP address ranges are considered private:

- Class A – 10.0.0.0
- Class B – 172.16.0.0 to 172.31.255.255
- Class C – 192.168.0.0 to 192.168.255.255

Implementation Considerations:

- Identify the hosts that do not need external access.
- Filter private addresses.
- Changing IP addresses from private to public requires time.

24. Define network address translation and determine when it can be used.

Network Address Translator (NAT) is used to access the internet using private addresses.

25. Explain why OSPF is better than RIP in a large internetwork.

Reasons:

- Has fast convergence
- Supports VLSM
- Has no hop count limitation
- Processes updates efficiently
- Selects paths based on bandwidth

26. Explain how OSPF discovers, chooses, and maintains routes.

Establishing Adjacencies:

OSPF routing is depended on the status of a link between two routers. Adjacency between neighboring routers are established using hello protocol.

Discovering Routes:

Exstart state – when the DR and BDR have been elected. Master/slave relation is created between each router and its adjacent DR/BDR.

Exchange state – the process used to discover the network routes. The master/slave exchange one or more database description packet (DBDs or DDPs).

Full state – when all the routes are discovered. The router has to be in Full state before it can route any packets. At this point, the routers all have identical link-state databases.

Choosing Routes:

Link-state protocols (ie. OSPF) uses a cost metric to determine the best path to a destination. *It uses a algorithm, which adds up the total costs between the local router (the root) and each destination network*. OSPF keeps up to 6 equal cost route entries in the routing table for load balancing. To minimize some serial

link flapping, Cisco routers use **spf holdtime** command to wait for a period of time before recalculating its routing table.

Maintaining Routing Information:

When there is a change in a link-state, the routers use a *flooding process* to notify the other routers in the network of the change.

1. If a router notices a change in link state, it multicasts an LSU (link state update) packet to all OSPF DR/BDRs.
2. DR acknowledges the receipt and floods the LSU to others on the network. After receiving the LSU, each router responds to the DR with an LSAck.
3. If a router is connected to another network, it floods the LSU to other networks by forwarding the LSU to respective DR or adjacent router if in a point-to-point network.
4. When a router receives the LSU that includes the changed LSU, the router updates its link-state database.

27 Configure OSPF for proper operation.

To configure OSPF, do the following:

Enable OSPF on the router.
Router(config)# **router ospf** *process-id*

Identify which IP networks on the router are part of the OSPF network.
Router(config-router)# **network** *address wildcard-mask* **area** *area-id*

28. Verify OSPF operation.

Verifies OSPF is configured
Router# **show ip protocol**

Displays all the routes learned by the router
Rotuer# **show ip route**

Displays area ID and adjacency information
Router# **show ip ospf interface**

Displays OSPF timers
Router# **show ip ospf**

Displays information about DR/BDR and neighbors
Router# **show ip ospf neighbor detail**

Displays the link-stat database
Router# **show ip ospf database**

29. Describe the issues with interconnecting multiple areas and how OSPF addresses each.

Issues with Maintaining a Large Single-Area Network

- Frequent SPF calculations
- Large routing table
- Large link-state table

OSPF Hierarchical Routing – separate a large internetwork into multiple areas

Advantages of OSPF hierarchical topology

- Reduced frequency of SPF calculations.
- Smaller routing tables
- Reduced LSU overhead

30. Explain the differences between the possible types of areas, routers, and LSAs

OSPF Multiarea Components

- Internal Router (LSA Type 1 or 2) – Routers that have all interfaces in the same area. They have identical link-state database and run single copy of routing algorithm.
- Backbone Routers (LSA Type 1 or 2) – Routers that have at least one interface connected to area 0.

- Area Border Router (LSA Type 3 or 4) – Routers that have interfaces attached to multiple areas. They maintain separate link-state database for each area.
- Autonomous System Boundary Router (LSA Type 5) – Routers that have at least one interface into an external internetwork (another autonomous system), such as a non-OSPF network. These routers can redistribute non-OSPF network information to and from OSPF network.

Types of Areas

- Standard area – Can accept link updates and route summaries.
- Backbone area (transit area) – This area is always labeled "0". All other areas must connect to this area in order to exchange and route information.
- Stub area – This area does not accept information about redistributed routes (LSA Type 5)
- Totally stubby area – This area does not accept information about redistributed routes and route summary.

31. Configure a multiarea OSPF network.

Configuring OSPF area border routers

There are no special commands to make a router an ABR or ASBR. The router takes on this role by virtue of the areas to which it is connected. As a reminder, the basic OSPF configuration steps are as follows and you would simply add another network statement for ABR or ASBR to another area.

To configure OSPF, do the following:

Enable OSPF on the router.
Router(config)# **router ospf** *process-id*

Identify which IP networks on the router are part of the OSPF network.
Router(config-router)# **network** *address wildcard-mask* **area** *area-id*

Configuring Route Summarization

Consolidate IA (intra-area) routes on an ABR
Router(config-router)# **area area-id** range address mask

Consolidates external routes (interarea) on an ASBR
Router(config-router)# **summary-address** address mask

Configuring Stub and Totally Stubby Areas

Creates a stub network
Router(config-router)# **area area-id stub**

Creates a totally stub network
Router(config-router)# **area area-id stub no-summary**

32. Verify OSPF operation.

Lists the ABRs in the autonomous system
Router# **show ip ospf border-routers**

Displays the status of the virtual link
Router# **show ip ospf virtual-link**

Displays statistics about each area to which the router is connected
Router# **show ip ospf process-id**

Displays the contents of the OSPF tables
Router# **show ip ospf database**

33. Describe EIGRP features and operation.

EIGRP supports:

- Rapid convergence
- Reduced bandwidth usage
- Multiple network-layer support (AppleTalk, IP, and Novell Netware)

EIGRP Terminology:

- Neighbor table – maintains a neighbor table that lists adjacent routers.
- Topology table – this table includes entries for all destinations that the router has learned.
- Routing table – EIGRP chooses the best (successor) routes to a destination from the topology table and places these routes in the routing table.
- Successor – A route selected as the primary route to use to reach a destination. Successors are the entries kept in the routing table.
- Feasible successor – A backup route. Multiple feasible successors for a destination can be retained, kept in topology table.

34. Configure EIGRP.

Configuring EIGRP for IP

Enable EIGRP and define the autonomous system
Router(config)# **router eigrp** *autonomous-system-number*

Indicate which networks are part of the EIGRP autonomous system
Router(config-router)# **network** network-number

Define bandwidth of a link for the purposes of sending routing update traffic on the link
Router(config-if)# **bandwidth** kilobits

Configuring EIGRP for IPX

Enable IPX routing
Router(config)# **ipx routing**

Define EIGRP as the IPX routing protocol
Router(config-ipx-router)# **ipx router {eigrp** *autonomous-system-number* **| rip}**

EIGRP	Specifies IPX EIGRP as the routing protocol
RIP	Specifies RIP as the routing protocol (RIP is on by default)

Indicate which networks are part of the EIGRP autonomous system
Router(config-router)# **network** network-number

Configuring EIGRP for IPX SAP Updates

1. Enable EIGRP for IPX routing
2. Select the interface which you want the SAP updates to be sent incrementally.
3. Instruct the router to issue SAP updates only when a change occurs in the network, instead of the periodic update interval:

Router(config-if)# **ipx sap-incremental eigrp** *autonomous-system-number*

35. Verify EIGRP operation.

Verifying EIGRP for IP Operation

Displays the neighbors discovered by IP EIGRP
Router# **show ip eigrp neighbors**

Displays EIGRP topology table
Router# **show ip eigrp topology**

Displays eigrp routing table
Router# **show ip route eigrp**

Displays the parameters and current state of the active routing protocol process
Router# **show ip protocols**

Displays the number of IP EIGRP packets sent and received
Router# **show ip eigrp traffic**

Verifying EIGRP for IPX Operation

Displays the contents of the IPX routing table
Router# **show ipx route**

Displays the neighbors discovered by IPX EIGRP
Rotuer# **show ipx eigrp neighbors**

Displays the IPX EIGRP topology
Router# **show ipx eigrp topology**

36. Select and configure the different ways to control route update traffic.

Controlling Routing Update Traffic

Using and Configuring **passive-interface**

The **passive-interface** command prevents all routing updates for a given routing protocol from being sent into a network, but does not prevent the specified interface from receiving updates.

1. Select the router that requires the passive interface.
2. Determine what interface(s) you do not want routing update traffic to be sent through.
3. Configure the passive interface.

Router(config-router)# **passive-interface** *type number*

Using and Configuring Default Routes

1. Determine what network(s) you want as the default network
2. Select the router(s) that need to have a default route defined
3. Configure the selected network as default:

   For IP:
   Router(config)# **ip default-network** network-number

   For IPX:
   Router(config)# **ipx advertised-default-route-only** network

Using and Configuring Static Routes

Defines a path using a next hop address. Use if you have a route to the defined address. Requires redistribution.

Router(config)# **ip route** network mask {next hop address} [administrative distance]

Defines a path using an interface. Use if you do not have a route to the next hop address. Automatically redistributed.

Router(config)# **ip route** network mask {out interface} [administrative distance]

Using and Configuring Route Filters

You can filter routing update traffic for any protocol by defining an access list and applying it to specific routing protocol. To configure a filter, do the following:

1. Identify the network addresses you want to filter and create an access list.
2. Determine if you want to filter them on an incoming or outgoing interface.
3. Assign the access list to filter outgoing routing updates:

   Router(config-router)# **distribute-list** *access-list-number* **out** [interface-name]

4. Assign the access list to filter incoming routing updates, use the following

   Router(config-router)# **distribute-list** *access-list-number* **in** [interface-name]

37. Configure route redistribution in a network that does not have redundant paths between dissimilar routing process.

1. Determine core or backbone routing protocol (usually EIGRP or OSPF)
2. Locate the ASBR where redistribution needs to be configured on.

3. Determine which routing protocol is the edge or short-term protocol.
4. Access the routing process into which you want routes redistributed. (ie OSPF do..)

   Router(config)# **router ospf** *process-id*

5. Configure the router to redistribute routing updates from the short-term protocol into the backbone protocol. This command will vary depending upon the protocol type.

   Router(config-router)# **redistribute** *protocol [*process-id] **metric** [metric-value]

   Router(config-router)# **default-metric** *bandwidth delay reliability loading mtu*
   - Used for IGRP and EIGRP redistribution

   Router(config-router)# **default-metric** *number*
   - Used for OSPF, RIP, EGP, and BGP redistribution

38. Configure route redistribution in a network that has redundant paths between dissimilar routing process.

- Use default-network statement or Route filtering

39. Resolve path selection problems that result in a redistributed network.

- Use administrative distance
- Use default metric

40. Verify route redistribution.

Router# **show ip | ipx | appletalk route**

Router# **trace**

41. Describe when to use BGP to connect to an ISP.

- When you connect to 2 different ISPs, it is frequently necessary to use BGP. Redundancy, load sharing, and lower tariffs at particular times of the day or night are some reasons why you would use 2 different ISPs.

- Also if you different policy requirements than the ISP.

42. Describe methods to connect to an ISP using static and default routes, and BGP.

- Self-explanatory.

43. Compare the differences between WAN connection types: dedicated, asynchronous dial-in, dial-on-demand, and packet switched services. (encapsulation type)

44. Determine when to use PPP, HDLC, LAPB, and IETF encapsulation type.

- Dedicated Connectivity – Also called leased lines, provides full-time synchronous connection. (Cisco HDLC, PPP, LAPB)
- Asynchronous Dial-In Connectivity – Modem connection (PPP)
- Dial-on-Demand Routing – Connections are made only when traffic dictates a need. (PPP)
- Packet-Switched Services – Use virtual circuits that provide end-to-end connectivity. (X.25-LAPB; Frame Relay-IETF)

45. List at least four common issues to be considered when evaluating a WAN service.

- Availability - Not all WAN services are available in all areas of the world.
- Application traffic – Categorize the type of application traffic that will cross the link.
- Bandwidth – WAN bandwidth is expensive.
- Ease of management – Degree of difficulty associated with managing connections.
- Routing protocol characteristics – broadcasts and routing update traffic.

46. Describe the components that make up ISDN connectivity.

ISDN access options – 2 standard access methods

- Primary Rate Interface (PRI) – In North America and Japan, 23 (B) channels and 1 64 kbps D channel.
- Basic Rate Interface (BRI) – Two 64 kbps (2B) and one 16 kbps data channel service.

ISDN encapsulation options
- Defaults to HDLC
- PPP with CHAP
- LAPD

ISDN functions
- TA Converts from RS-232, V.35 and other signals to BRI signals
- TE1 Device having a native ISDN interface.
- TE2 Device requiring a TA for its BRI signals
- NT1 Converts BRI signals into a form used by the ISDN digital lines
- NT2 Point where al ISDN lines at customer site are aggregated and switched

ISDN reference points
- R – Connection between a non-ISDN compatible device and TA
- S – Connection between ISD compatible device and NT2 (customer switching device)
- T – Outbound connection from the NT2 to the ISDN network.
- U – References the connection between the NT1 and the ISDN network.

ISDN switch types
- United States AT&T 5ess and 4ess

47. Configure ISDN BRI

Specify the type of ISDN switch with which the router communicates

Router(config)# **isdn switch-type** *switch-type*

48. Configure Legacy dial-on-demand routing (DDR)

Legacy DDR – The ability to enable a PSTN connection only when there is traffic to send.

Generic DDR Operation
1. Interesting packets dictate DDR call
2. Route to destination is determined
3. Dialer information is looked up
4. Traffic is transmitted
5. Call is terminated

Configuring Legacy DDR

1. Specify interesting traffic-What traffic enables the link?

   Router(config)# **dialer-list** *dialer-group* **protocol** *protocol-name* [**permit | deny | list**] *access-list-number*

2. Define a static route to the destination – What route do I use?

3. Configure the dialer information – What number do I call?

   1. Select the physical interface that you want to be your dialup line.
   2. Configure the network address for the interface. (i.e.)
      Router(config-if)# **ip address** *ip-address mask*

   3. Configure the encapsulation type. (i.e.)
      Router(config-if)# **encapsulation ppp**

   4. If you do not have native ISDN BRI and are using sync or async interfaces
      Router(config-if)# **dialer in-band**

5. Bind the traffic definition to an interface
   Router(config-if)# **dialer-group** *group-number*

6. Define destination(s)
   Router(config-if)# **dialer map** *protocol next-hop-address* [**name** *next-hop-address*] [**speed** 56/64] [**broadcast**] *dialer-string*

4. Legacy DDR Optional Commands

   Establishes the amount of traffic on link before a second link is enabled
   Router(config-if)# **dialer load-threshold** *load* [**outbound | inbound | either**]
   load = 1-255 (255 being 100%)

   Establishes the idle time before disconnect
   Router(config-if)# **dialer idle-timeout** *seconds* *(default is 120 seconds)*

5. Verifying Legacy DDR Operation

   Triggers a link
   Router# **ping or telnet**

   Displays current status of link
   Router# **show dialer**

   When using ISDN, displays call status while call is in progress
   Router# **show isdn active**

   Displays the status of an ISDN connection
   Router# **show isdn status**

   Displays all routes, including static routes
   Router# **show ip route**

49. Configure dialer profiles.

Legacy DDR – Same interface uses same dialer specifications for all calls
Dialer profiles – Same interface can use different dialer specifications for each call. With dialer profiles, the physical interfaces become members of a dialer pool.

1. Specify interesting traffic – What traffic enables the link?

2. Define static routes – What route do I use?

3. Create the dialer interface – What logical interface do I use?

   1. Create a dialer interface and enter dialer interface configuration mode.
      Router(config)# **interface dialer** *number*

   2. Specify the dialing information to use to call the destination.
      Router(config-if)# **dialer-string** *string* **class** *class-name*

      Dialer-string – The phone number to be dialed
      Class-name – The map class that should be applied to the call
   3. Specify the dialer pool to associate with this dialer interface.
      Router(config-if)# **dialer pool** *member*

   4. Assign the interesting traffic definition to the dialer interface.
      Router(config-if)# **dialer-group** *number*

   5. Specify the dialer map class
      Router(config)# map-class dialer class-name

4. Make the physical interface a dial pool member – What physical interface do I use?

   1. Select the physical interface that you want to be part of the dialer profile.
      Router(config)# **interface bri0**

2. Assign the interface to one or more dialer pools
   Router(config-if)# **dialer pool-member** *number* **[priority** *priority***]**

50. Verify DDR operation.

Triggers a link
Router# **ping or telnet**

Displays current status of link
Router# **show dialer**

When using ISDN, displays call status while call is in progress
Router# **show isdn active**

Displays all routes, including static routes
Router# **show ip route**

Clears currently established connections
Router# **clear [dialer | interface]**

51. Configure dial backup.

Configuring Dial Backup for Primary Links

1. Select the primary interface and go into interface configuration mode.
2. Indicated the backup interface to use in case of primary link failure or if a load threshold is exceeded.

   Router(config-if)# **backup interface** *interface-name*

   Interface-name - specify the interface or dialer interface to use for backup.

3. Define the number of seconds to wait before enabling the backup link when the primary link fails.

   Router(config-if)# **backup delay** {*enable-delay* | **never**} {*disable-delay* | **never**}

   Enable-delay | ***never*** - Number of seconds to wait after the primary link has failed to bring up to backup.
   Disable-delay | ***never*** – Number of seconds to wait after the primary link is available to drop the backup.

Configuring Dial Backup for Excessive Traffic Load

1. Select the primary interface and go into interface configuration mode.
2. Indicated the backup interface to use in case of primary link failure or if a load threshold is exceeded.

   Router(config-if)# **backup interface** *interface-name*

   Interface-name - specify the interface or dialer interface to use for backup.

3. Set the traffic load thresholds for dial backup service

   Router(config-if)# **backup load** {*enable-threshold* | **never**} {*disable-load* | **never**}

   Enable-threshold | ***never*** - Primary link bandwidth % which must be reached to bring up the backup.
   Disable-load | ***never*** – Primary link bandwidth % which must be reached to bring down the backup.

52. Verify dial backup operation.

53. Configure Multilink PPP

Multilink PPP – Interfaces are grouped into a bundle to increase the available bandwidth for the connection.

1. Configure either dialer profiles or dialer rotary groups on selected interfaces or select single BRI.
2. Configure the dialer interface

   Router(config-if)# **ppp multilink**

3. Specify the load threshold that the interface should reach before enabling one or more additional links.

Router(config-if)# **dialer load-threshold** load **[outbound | inbound | either]**

54. Verify Multilink PPP operation.

Displays information about existing bundles
Router# **show dialer**

Displays event information
Router# **debug ppp multilink**

55. Configure snapshot routing.

Snapshot Routing – allows dynamic distance vector routing protocols to run over DDR. Reduces overhead or routing updates.

1. Specify an ISDN interface
2. Configure the client/server router
3. Define a dialer map

Configure the client router

1. Select and get into interface configuration mode for a physical or dialer interface.
2. Enable snapshot routing on the client router
   Router(config-if)# **snapshot client** *active-time quite-time*

3. Define a dialer map that includes the server router(s) to call for routing updates.
   Router(config-if)# **dialer map snapshot** *sequence-number* **name** *name dial-string*

Configure the Server router

1. Select and get into interface configuration mode for a physical or dialer interface.
2. Enable snapshot routing on the server router
   Router(config-if)# **snapshot server** *active-time*

3. Define a dialer map that includes the client router(s) to call for routing updates.
   Router(config-if)# **dialer map snapshot** *sequence-number* **name** *name dial-string*

56. Configure IPX spoofing.

IPX spoofing – spoofing allows the router to respond while the DDR interface is idle.

Configuring IPX Spoofing

1. Turn off route caching
   Router(config-if)# **no ipx route-cache**

2. Enable SPX spoofing of the idle DDR link.
   Router(config-if)# **ipx spx-spoof**

3. Enable IPX watchdog spoofing.
   Router(config-if)# **ipx watchdog-spoof**

4. Set SPX idle time.
   Router(config-if)# **ipx spx-idle-time**

57. Define routable and nonroutable protocols and give an example of each.

Routing is based on logical addresses contained in the network layer.
Examples or routable protocols – IP, IPX, Appletalk

Bridging is based on the MAC address contained in the data link layer.
Examples of nonroutable protocols – LAT, NetBIOS

58. Define various bridging types and describe when to use each type.

Transparent bridging – used to connect two or more physical networks into one LAN.

Encapsulated bridging – is used to connect LAN via an independent transport connection, normally FDDI or serial. It consists of encapsulating the bridged frame inside another data link layer protocol (such as HDLC) and de-encapsulating it on the other side of the link.

Integrated routing and bridging (IRB) – used to route a given protocol between routed interfaces and bridged interfaces within a single router.

Source-route bridging (SRB) – the entire route to a destination is predetermined, in real time, prior to the sending of data. The source places the complete source-to-destination route in the frame header of all inter-LAN frames.

Source-route transparent bridging (SRT) – employs both SRB and transparent bridging in one device.

Source-route Translational bridging (SR/TLB) – provides the functionality to connect the two hosts on different topology (i.e. Ethernet to Token Ring).

59. Configure transparent bridging.

- Select the spanning tree protocol

  Router(config)# **bridge** *bridge-group* **protocol** { **ieee | dec** }

- Assigns an interface to a bridge group

  Router(config-if)# **bridge-group** *bridge-group*

60. Configure Integrated Routing and Bridging (IRB)

What is IRB?

- Packets received on bridged interface can be routed through routed interface.
- Packets received on routed interface can be routed through bridged interface.

1. Enable IRB

   Router(config)# **bridge irb**

2. Configure the BVI (Bridge-group virtual interface)

   Router(config-if)# **interface bvi** *bridge-group*

3. Enable the BVI to accept routed packets

   Router(config)# **bridge** *bridge-group* **route** *protocol*

4. Enable routing on the BVI for desired protocols

   Router(config)# **interface bvi 1**
   Router(config-if)# **ip address** *ip-address mask*

61. Describe basic functions of source-route bridging (SRB)

SRB determines the entire route to a destination, in real time, prior to the sending of data.

62. Configure SRB

Specify the local bridge connection

Router(config-if)# **source-bridge** *local-ring bridge-number target-ring*

Activates manual spanning for an interface.

Router(config-if)# **source-bridge spanning**

Activates automatic spanning for an interface

Router(config-if)# **bridge** *bridge-group* **protocol** *ibm*

63. Configure source-route transparent bridging (SRT)

SRT handles transparent bridging and source-route bridging traffic handled appropriately

To configure SRT, enable transparent and SRB bridging on interfaces used for SRT bridging. Traffic without RIF information is transparently bridged, and traffic with RIF information is source-route bridged.

64. Configure source-route Translational bridging (SR/TLB)

SR/TLB translates between transparent and SRB bridging.

- Enables bridging between the transparent bridge configuration and the source-route bridge configuration.

Router(config)# **source-bridge transparent** *ring-group pseudo-ring bridge-number tb-group [oui]*

Ring-group	The virtual ring group that was create by the **source-bridge ring-group** command
Pseudo-ring	The ring number used to represent the transparent bridging domain to the source-route bridged domain.
Bridge-number	The SRB number assigned to the router
Tb-group	The number of the transparent bridge group that you want to tie into your source-route bridged domain.

65. Verify SRB operation.

Router# **show source-bridge**

Router# **show rif**