Advanced Cisco Router Configuration

Objective Overview

1. Describe the Key requirements of a scalable internetwork.

- **Reliability and Available** –
  - Scalable protocols – Reachability, Fast convergence time, Congestion control
  - Alternate paths
  - Load balancing
  - Tunnels
  - Dial backup
- **Responsiveness**
  - Queueing - Weighted fair queuing, Priority queuing, Custom queuing
  - Frame relay traffic shaping
  - Generic traffic shaping
  - Random early detection
- **Efficiency**
  - Access lists
  - Snapshot routing
  - Compression over WANs
  - Dial on demand routing
  - Switched access
  - Reduce the number of routing table entries - Route summarization, Incremental updates
- **Adaptability**
  - Mixing routable and non routable protocols
  - Integrating “islands” of networks
  - Meet the varying requirements for each protocol in the internetwork
  - EIGRP – supports IP, IPX, and Appletalk
  - Redistribution
  - Bridging mechanisms
- **Accessible but secure**
  - Dedicated and switched WAN support
  - Exterior protocol support
  - Access lists
  - Authentication protocols
  - Lock and key security
  - Network layer encryption

2. Select a Cisco IOS feature as a solution for a given internetwork requirement

NETWORK PROBLEM	KEY	CISCO IOS FEATURES

	REQUIREMENT	
Connectivity restrictions	Accessible but secure	Dedicated and switched access technologies BGP support
Single paths available to all networks	Reliable and available	Scalable protocols Dial backup
Too much broadcast traffic	Efficient	Access lists Scalable protocols
Application sensitivity to traffic delays	Responsive	Weighted fair queuing Priority queuing Custom queuing
Convergence problems with metric limitations	Reliable and available	Scalable protocols
Competition for bandwidth	Efficient, responsive	Access lists Snapshot routing Compression over WANs Queueing Generic traffic shaping
Illegal access to services on the internetwork	Accessible but secure	Access lists Authentication Lock and key security
Single WAN links available to each remote site	Reliable and available	Dial backup
Expensive tariffs on WAN links that do not get much use	Efficient	Switched access technologies
Very large routing tables	Efficient	Route summarization Incremental updates
Integrate networks using legacy protocols	Adaptable	Bridging mechanisms

3. Describe causes of Network Congestion

Chapter 2.

4. List Solutions for controlling network congestion

- Filtering traffic
- Adjusting timers
- Using static entries
- Prioritizing traffic

5. Configure IP standard access lists

Standard access lists filter based on source address only and should be placed as close to the destination as possible.
Make sure that you list the entries in order from specific to general.

IP standard access list commands

- **ip access-group {in | out} -** to apply the access list to an interface.
- **no access-list** *access-list-number* - to eliminate the entire list
- **no ip access-group** *access-list-number* - .to unapply the access list
- **access-list** *access-list-number* {**permit** | **deny**} source [source-wildcard] **any**

Access-list command	Description
Access-list-number	Identifies the list to which the entry belongs; a number from 1 to 99
Permit | **deny**	Indicates whether this entry allows or blocks traffic form the specified address
Source	Identifies the source IP address
Source-wildcard	(optional) identifies which bits in the address field are matched.
Any	Uses address 0.0.0.0 and source wildcard 255.255.255.255 to match any address

Steps:

```
1.  enter global config mode
2.  generate the access list
3.  enter interface specific mode
4.  apply the access list
```

Ex:

```
router>enable
router#config terminal
router(config)#access-list 1 permit 172.16.0.0  0.0.255.255
router(config)#interface ethernet 0
router(config-if)#ip access-group 1 in
```

6. Limit virtual terminal access

Line – use the line command to place the router in line configuration mode
Access-class – link an existing access list to a terminal line or range of lines.

line { *vty-number* | *vty-range* }

access-class *access-list-number* { **in | out** }

Steps:

```
1.  enter global config mode
2.  generate the access list
3.  enter line configuration mode
4.  apply the access list
```

Ex:

```
router>enable
router#config terminal
router(config)#access-list 12 permit 192.89.55.0  0.0.0.255
router(config)#line vty 0 4
router(config-line)#access-class 12 in
```

7. Configure IP extended access lists

(refer to pages 50 –63)

Extended access lists filter on source address, destination address, or protocol characteristics.

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

Access-list command	Description
Access-list-number	A number from 100 to 199
Permit | deny	Whether this entry is used to allow or block the specified address
Protocol	**Ip, tcp, udp, icmp, igmp, gre, igrp, eigrp, ospf, nos**, or a number in the range of 0 through 255. To match any internet protocol, use the keyword **ip.**
Source and destination	Ip addresses
Source wildcard and destination wildcard	Wildcard masks of address bits that must match. 0's indicate must match. 1's indicate don't care
Any	Use this keyword as an abbreviation for a source and source-wildcard, and/or a destination and destination-wildcard of 0.0.0.0 255.255.255.255
Log	(optional) causes information logging messages about the packet that matches the entry to be sent to the console. Consumes CPU cycles.

Steps:

```
1.  enter global config mode
2.  generate the access list
3.  enter line configuration mode
4.  apply the access list
```

Ex:

```
router>enable
router#config terminal
router(config)#access-list 104 permit tcp any 128.88.0.0 0.0.255.255
established
router(config)#access-list 104 permit tcp any host 128.88.1.2 eq smtp
router(config)#access-list 104 permit udp any eq domain any
router(config)#access-list 104 permit icmp any any echo
router(config)#access-list 104 permit icmp any any echo-reply
router(config)#interface ethernet 0
router(config-if)#ip access-group 104 in
```

8. Verify access list operation

- **show access-list –** display access lists from all protocols
- **show ip access-list [** ***access-list-number*** **] –** display IP access lists
- **clear access-list counters [** ***access-list-number*** **] –** clear the counters of an access list

- **show line –** display information about terminal lines.

9. Configure an alternative to using access lists (pg. 66)

There is an alternative to using access lists if the policy is for unwanted traffic to a certain destination to be discarded every time.
The null interface is a software only interface. Message traffic that is not required is directed to the null interface using a static route, where it is effectively "dropped".

ip route *address mask* **null 0**

Steps:
```
1. enter global configuration mode
2. assign the static route
```

Ex:
```
router>enable
router#config terminal
router(config)#ip route 172.16.1.0 255.255.255.0 null 0
```

10. Configure an IP helper address to manage broadcasts. (pg. 68-74)

Helpers change broadcasts to unicasts.

- ip helper-address – used to configure an interface where broadcasts are expected. If an ip helper-address is defined, forwarding for 8 UDP ports is enabled automatically. TFTP (69), DNS (53), Time (37), NetBIOS name service (137), NetBIOS datagram service (138), BOOTP/DHCP server (67), BOOTP/DHCP client (68), and TACACS (49).
- ip forward-protocol – to specify which type of broadcast packet is forwarded. Used for individual ports as opposed to **ip helper-address** which does all 8. You must use **ip forward-protocol udp** [port] for the ports you want to forward and then specify **no ip forward-protocol udp** [port] for the default ports you do not want forwarded.

Steps:
```
1. enable global configuration mode
2. enable specific interface mode
3. use the commands
```

Ex 1:
```
router>enable
router#config terminal
router(config)#interface ethernet 0
router(config-if)#ip helper-address 144.253.2.2
```

Ex 2:
```
router>enable
router#config terminal
```

```
router(config)#interface ethernet 0
router(config-if)#ip address 144.253.1.100 255.255.255.0
router(config-if)#ip helper-address 144.253.2.2
router(config-if)#ip forward-protocol udp 3000
router(config-if)#no ip forward-protocol udp 69
```

11. Describe IPX/SPX traffic management issues (ch. 4 pg 83 –114)

12. Filter IPX traffic using IPX access list

Commands:

- **access-list** *access-list-number* **{permit | deny }** *source-network [.source-node [source-node-mask]]* [*destination-network [.destination-node [destination-node-mask]]]*
- **ipx access-group** *access-list-number* **{ in | out }**
- **ipx input-network-filter** *access-list-number* **:** used to filter rip traffic
- **ipx output-network-filter** *access-list-number* **: used to filter rip traffic**
- **ipx sap-interval** *number* : number in minutes to delay sap update: default 1;

Parameters:

access-list-number : identifies the list to which the entry belongs: 800 to 899
permit | deny : indicates whether this entry permits or blocks traffic
source-network : the source network number, 8 digit hex
.source-node : node number on the source network.
source-node-mask : mask
destination-network : network number to which the packet is being sent
.destination-node : node on the destination network the packet is being sent
destination-node-mask : mask

Steps:

1. enter global config mode
2. enable ipx routing
3. generate the access list
4. enter interface specific mode
5. apply the access list
6. set the sap interval (optional - used for wan)

Ex:

```
router>enable
router#config terminal
router(config)#ipx routing
router(config)#access-list 800 permit 2b 4d
router(config)#interface ethernet 0
router(config-if)#ipx access-group 800 in
router(config-if)#ipx sap-interval 10
```

Ex:

```
router>enable
router#config terminal
router(config)#ipx routing
router(config)#access-list 800 permit 4d
router(config)#interface ethernet 0
router(config-if)#ipx input-network-filter 800
```

Configure SAP Access Lists

Commands:

- **access-list** *access-list-number* {**permit | deny** } *network[.node] [network-mask node-mask] [service-type [server-name*]]
- **ipx input-sap-filter** *access-list-number*
- **ipx output-sap-filter** *access-list-number*

Parameters:

```
access-list-number : list to which the entry belongs: 1000 to 1099
permit | deny : indicates whether this entry permits or blocks traffic
network.node : the source network number, -1 means all
network-mask node-mask : mask, place 1's in all positions to be masked
service-type : 4-file server, 7-print server, 24-router
server-name : name of server providing service
```

Steps:

```
1. enter global config mode
2. enable ipx routing
3. generate the access list
4. enter interface specific mode
5. specify the ipx networks
6. apply the access list
```

Ex:

```
router>enable
router#config terminal
router(config)#access-list 1000 permit -1 4
router(config)#interface ethernet 0
router(config)#ipx network 9e
router(config-if)#ipx output-sap-filter 1000
```

13. Manage IPX/SPX traffic over WAN connections

14. Verify IPX/SPX filter operation

- **show ipx interface** – verify the status of the interfaces that are routing ipx traffic, displays information on the ipx address of the interface, ipxwan status, ipx helper information, and sap and access list filtering
- **show ipx route** – view the ipx routing table, displays information on the following types of routers: connected primary network, internal network, static, floating static, ipxwan, rip, eigrp, nlsp, and external, and aggregate.
- **show ipx cache** – verify the ipx fast switching cache

- **show ipx servers** – display the available ipx servers, displays the type of service, the name of the servers, the network address of the server, and the distance in hops and ticks to the server. Displays the routers sap table
- **show ipx traffic** – verify ipx traffic, shows the number of packets transmitted and received. Includes boradcast, sap, routing, and watchdog information.

15. Describe the need for queuing in a large network

Queuing is the process of allowing certain traffic to be delivered before others, controls traffic congestion. Is especially critical on low bandwidth serial links when some multi-protocol traffic, such as video/audio traffic, is more time critical than other types of traffic.

The need for queuing stems from the need to prioritize traffic. This is due to the diverse mixture of protocols and their associated behaviors. Prioritization is most effective on WAN links where the combination of **bursty traffic** and **relatively lower data rates** can **cause temporary congestion**. Most effectively when applied to links at T1/E1 speeds. If there is no congestion on the WAN link, there is no reason to implement traffic prioritization because traffic prioritization adds overhead to the router's operation. If a WAN link is constantly congested, traffic prioritization may resolved the problem, add more bandwidth.

16. Describe weighted fair queuing operation (pg. 124).

Router is allowed to decide which packets are dropped.
WFQ prioritizes interactive traffic over file transfers in order to ensure satisfactory response time for common user applications.

Small, low volume packets are given priority over large, high volume conversation packets.
Automatically runs on all low speed serial interfaces.

17. Configure priority queuing (pg. 126 – 135).

Network manager decides which packets are dropped.

- **priority-list protocol** – define a priority list for a protocol
  - **priority-list** *list-number* **protocol** *protocol-name* { **high** |**medium** |**normal** |**low** } *queue-keyword keyword-value*
- **priority-list interface –** to set queuing priorities for all traffic.
  - **Priority-list** *list-number* **interface** *interface-type interface-number* { **high** |**medium** |**normal** |**low** }
- priority-list default – assign packets to a queue if no other priority list conditions are met
  - **priority-list** *list-number* **default** { **high** |**medium** |**normal** |**low** }
- **priority-list queue-limit** – changes the default maximum number of packets in each queue
- **priority group –** command to link a priority list to an interface.
  - **Priority-group** *list*

Steps:

```
1. enable global configuration mode
2. create the list
3. enable interface configuration mode
4. apply list to the interface
```

Ex 1:

```
router>enable
router#config terminal
router(config)#priority-list 1 protocol ip high tcp 23
router(config)#priority-list 1 protocol appletalk medium
router(config)#priority-list 1 protocol ipx medium
```

```
router(config)#priority-list 1 protocol ip normal
router(config)#priority-list 1 default low
router(config)#interface serial 0
router(config-if)#priority-group 1
```

Ex 2:

```
router>enable
router#config terminal
router(config)#access-list 1 permit 131.108.0.0  0.0.255.255
router(config)#priority-list 2 protocol ip high tcp 23
router(config)#priority-list 2 ip high list 1
router(config)#priority-list 2 interface ethernet 0 medium
router(config)#priority-list 2 protocol ip normal
router(config)#priority-list 2 default low
router(config)#priority-list 2 queue-limit 15 20 20 30
router(config)#interface serial 0
router(config-if)#priority-group 1
```

18. Configure custom queuing (pg. 137 – 145)

Network manager decides which packets are dropped. Lets you guarantee bandwidth for traffic by assigning queue space to each protocol. With custom queuing, you reserve a certain percentage of bandwidth for each specified class of traffic, can be based on protocol or source interface.

- **Queue-list protocol** – specify inclusion of a protocol in a particular queue.
- **Queue-list interface** – establish queuing priorities on incoming interfaces
- **Queue-list default** – assign packets to a queue if no other queue list conditions are met
- **Queue-list queue limit** – limit the length of a particular queue
- **Queue-list queue byte-count** – set the minimum byte count transferred from a given queue at a time.
- **Custom-queue-list** – link a queue list to an interface

Steps:

1. enable global config mode
2. create a queue list
3. enable interface specific mode
4. apply the queue list

Ex:

```
router>enable
router#config terminal
router(config)#queue-list 1 protocol ip 1 tcp 20
router(config)#queue-list 1 interface ethernet 0 2
router(config)#queue-list 1 protocol ip 3
router(config)#queue-list 1 protocol ipx 4
router(config)#queue-list 1 protocol appletalk 5
router(config)#queue-list 1 default 6
router(config)#queue-list 1 queue 1 byte-count 4500
router(config)#interface serial 0
router(config-if)#custom-queue-list 1
```

19. List the key information routers need to route data

- the destination of the packet that needs to be routed
- a routing entry for that destination.

- Destination network address
- Identify neighbors
- Discover routes
- Select routes
- Maintain routing information

20. Compare distance vector and link state protocol operation

Category	Routing Protocol
Distance Vector Routing Protocols	IP RIP, IPX RIP, AppleTalk RTMP, IGRP
Link-State routing Protocols	IP OSPF, IPX NLSP, IS-IS

DISTANCE VECTOR	**LINK_STATE**
IDENTIFY NEIGHBORS	
Does not have a formal way of learning about neighbors	Establishes a formal connection with each directly connected neighbor. This is done using the hello protocol.
Detects when a network is unavailable only when the routing update is missing for a specific period of time (usually 3 times the update interval)	Detects when a neighbor is unavailable when 3 hellos in a row are not received (the dead interval)
DISCOVERING ROUTES	
Each router creates a routing table that includes its directly connected networks and sends the routing table to its directly connected neighbors. The routing table sent out by distance vector routers follows the split horizon algorithm	Each router creates a link-state table that includes entries about the entire network
The neighbor incorporates all received routing tables into its own routing table and sends the updated routing table to its neighbors	Each router floods the entire internetwork with information about the links it knows about in update packets. Each neighboring router receives the update packet, copies the contents, and continues sending it. Note that the router does not recalculate its routing table before sending the entry to its neighbors.
SELECTING A ROUTE	
The typical metric used is to count the number of routers (hops) on the path to the destination. IPX RIP also uses a time value called a tick ($1/18^{th}$ of a second).	The metric used is a numerical value based on the bandwidth of the link. The value is called cost.
The path with the lowest number of hops is the best path. The maximum number of hops is typically 15.	The path with the lowest total cost is the best path. The maximum possible cost is almost unlimited.
To determine the shortest path, the bellman-ford algorithm is used	The algorithm used to determine the lowest cost is the shortest path first (SPF) algorithm
The routing table can include multiple equal cost routes to a given destination. These can be used for load balancing or redundancy	The routing table can include multiple equal cost routes to a given destination. These can be used for load balancing or redundancy.

MAINTAINING ROUTING INFORMATION	
When a router learns about a change in the internetwork, the router updates its routing table with the change. this change is propagated when the router broadcasts its periodic update.	When a router learns about a change in the internetwork, it updates its link-state table and sends an update only about changed entries to all routers in the internetwork
Neighboring routers incorporate the received routing information into their routing table. When their next update process occurs, they broadcast this new information along with the other entries in their tables	Each router receives the update and adds it to the link-state table
This process continues until all routers converge	The routes then run the SPF algorithm to select the best paths
If there is no change in the internetwork at a periodic interval, each router sends out its routing table to its neighbors.	If no change occurs in the internetwork, the routes will sned updates only for those route entries that have not been updated periodically.

21. Given an IP address, use VLSMs to extend the use of IP address

22. Given a network plan that includes IP addressing, explain if route summarization is or is not possible. (chapter 7).

The protocols that support subnet mask information include RIP2, OSPF, Enhanced IGRP, BGP, and IS-IS.

Requirements for route summarization

- multiple IP addresses must share the same high order bits
- routing tables and protocols must base their routing decisions on a 32 bit IP address and prefix length that can be up to 32 bits
- routing protocols must carry the prefix length (subnet mask) with the 32 bit IP address.

Ex: pg. 182

172.16.1.192/28 = 172.16.1.11000000 = 172.16.1.192/26
172.16.1.208/28 = 172.16.1.11010000 = 172.16.1.192/26
172.16.1.64/28 = 172.16.1.01000000 = 172.16.1.64/26
172.16.1.80/28 = 172.16.1.01010000
172.16.1.96/28 = 172.16.1.01100000
172.16.1.112/28 = 172.16.1.01110000

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

- Class A – 10.0.0.0 to 10.255.255.255
- Class B – 172.16.0.0 to 172.31.255.255
- Class C – 192.168.0.0 to 192.168.255.255

Private addressing are addresses that are not allowed on the public internet because they are either reserved addresses or previously assigned.

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

Network address translation is the process of substituting 1 network address (normally private) for another network address (public – internet capable).

The NAT router translates the internal local addresses into globally unique IP addresses before sending packets to the outside world. Normally placed on a stub network connecting to the internet.

NAT can also be used when you need to modify your internal addresses because you change ISP's.

One disadvantage of using NAT is with network management. In order to track NAT activity, you need two network management hosts on either side of the NAT router because the SNMP IP address table does not go through the NAT router correctly.

NAT can be used when you need hosts that use private addresses to be able to periodically access the Internet without having to redo their IP addresses.

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

- **Speed of convergence** – in large networks, RIP convergence can take several minutes as the routing algorithm goes through a holddown and route-aging period. With OSPF, convergence is faster because routing changes are flooded immediately and computed in parallel.
- **Support for Variable-Length Subnet Masks** – RIP1 does not support VLSMs. OSPF supports subnet masking and VLSMs.
- **Network reachability** – a RIP network that spans more than 15 hops is considered unreachable. OSPF has virtually no reachability limitations.
- **Use of bandwidth** – RIP broadcasts full routing tables to all neighbors every 30 seconds, which is especially problematical over slow WAN links. OSPF multicasts link-state updates and sends the updates only when there is a change in the network.
- **Method for path selection** – RIP has no concept of network delays and link costs. Routing decisions are based purely on hop count, which could lead to suboptimal path selection in cases where a longer path has a higher aggregate link bandwidth and shorter delays.

OSPF protocol benefits: No hop count limitation, The capability to multicast routing updates, Faster convergence rates, and Better path selection

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

The process used to discover the network routes is called the exchange protocol, and is performed to get the routers to a full state of communication.

1. In the exstart state, the DR and BDR establish adjacencies with each router in the network. During this process, a master slave relationship is created between each router and its DR/BDR. The router that has the higher router ID acts as the master.
2. The master and slave routers exchange one or more database description packets (DBD). A DBD includes the LSA (link state advertisement) entries that appear in the master router's link state database. Each LSA entry includes such things as a link state type, the address of the advertising router, the cost of the link, and the sequence number.
3. When the slave router receives the DBD, it does the following
    a. acknowledges the receipt of the DBD by echoing the link-state entry sequence numbers in a link-state ack packet.
    b. Compares the information it received with the information it has. Remember that the initial entries put into the link-state database are from the adjacencies database. If the DBD has a more up to date link-state entry, then the slave router sends a link state request (LSR) to the master router.
    c. The master router responds with the complete information about the requested entry in a link state update (LSU) packet.
4. All routers add the new link-state entries into their link state database
5. After all LSR's have been satisfied for a given router, the adjacent routers are considered synchronized and in full state. The routers must be in full state before they can route traffic.

CHOOSING ROUTES

Link-state protocols use a cost metric to determine the best path to a destination. To calculate the lowest cost to a destination, OSPF uses the Dijkstra algorithm. The algorithm adds up the total costs between the local router and each destination network. If there are multiple paths to a destination, the lowest cost path is preferred. But OSPF can keep up to 6 equal cost route entries for load balancing.

The Dijkstra algorithm simply "walks" the tree from the root (local router) to the distant branches (remote networks), adding the costs associated with traversing each link. Paths are compared to ensure the least-cost paths are considered most favorable.

MAINTAINING ROUTING INFORMATION

When there is a change in a link-state, the router uses a flooding process to notify the other routers in the network of change. The flooding process is as follows:

1. a router notices a change in a link-state and multicasts an LSU packet that includes the updated LSA entry to 224.0.0.6, the "all OSPF DRs" (and BDR) address.
2. The DR acknowledges the receipt of the change and floods the LSU to others on the network using the OSPF multicast address 224.0.0.5. after receiving the LSU, each router responds to the DR with an LSAck.
3. If a router is connected to another network, if floods the LSU to other networks by forwarding the LSU to the DR of the multi access network, or adjacent router if in a point to point network. The DR, in turn, multicasts the LSU to the other routers in the network.
4. When a router receives the LSU that includes the changed LSU, the router updates its link-state database. It then computes the SPF algorithm with the new database to generate a new routing table. After a shorrt delay, it switches over to the new routing table.

27. Configure OSPF for proper operation

enabling OSPF requires that you create an OSPF routing process, specify the range of IP addresses to be associated with the routing process, and assign area IDs to be associated with that range of IP addresses.

Perform the following tasks, starting in global configuration mode:

Step 1 Enable OSPF routing, which places you in router configuration mode.

Step 2 Define an interface on which OSPF runs and define the area ID for that interface.

```
router>enable
router#config terminal
router(config)#router ospf 1
router(config-router)#network 10.2.0.0 0.255.255.255 area 0
router(config-router)#network 10.64.0.0 0.255.255.255 area 0
```

28. Verify OSPF operation (pg. 203)

- **show ip protocol** – displays parameters about timers, filers, metrics, networks, and other information for the entire router.
- **Show ip route** – displays the routes known to the router and how they were learned.
- **Show ip ospf interface** – verifies that interfaces have been configured in the intended areas. It also gives the timer intervals including the hello interval and shows the neighbor adjacencies.
- **Show ip osfp** – displays the number of times the SPF algorithm has been executed. It also shows the link-state update interval.
- **Show ip ospf neighbor detail** – displays details list of neighbors, their priorities, and their state (init, exstart, full)
- **Show ip ospf database** – displays the contents of the topological database maintained by the router. Also shows the router ID and the OSPF process ID.

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

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

Hierarchical routing – OSPF's capability to separate large internetworks into multiple areas.

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

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

- **Types of Areas**
  - Standard area – this area can accept link updates and route summaries.
  - Backbone area (transit area) – when interconnecting multiple areas, the backbone area is the central entity to which all other areas connect. The backbone area is always labeled 0. All other areas must connect to this area in order to exchange and router information.
  - Stub area – refers to an area that does not accept information about routes external to the autonomous system (that is, the OSPF internetwork). If routers need to route to networks outside the autonomous system, they use a default route. A default route is noted as 0.0.0.0
  - Totally stubby area – an area that does not accept external autonomous system routes and summary routes from other areas internal to the autonomous system. If the router needs to send a packet to a network external to the area, it sends it using a default route.
- **Types of Routers** – a router can be more than 1 router type.
  - Internal router – routers that have all interfaces in the same area. Internal routers within the same area have identical link state databases and run a single copy of the routing algorithm
  - Backbone Router – routers that sit on the perimeter of the backbone area. They have at least on interface connected to area 0. These routers maintain OSPF routing information using the same procedures and algorithms as internal routers.
  - Area Border Router – routers that have interfaces attached to multiple areas. These routers maintain separate link state databases for each area to which they are connected. ABR's are exit points for the area. ABRs summarize information from their link state databases of their attached areas and distribute the information into the backbone. An area can have more than 1 ABR
  - Autonomous System Boundary Router (ASBR) – routers that have at least one interface into an external internetwork (another autonomous system), such as a non OSPF network. These routers can import (referred to as redistribution) non OSPF network information to the OSPF network and visa versa.

- **Types of Link State Advertisements** (LSAs)

LSA type	Name	Description
1	Router link entry	*Generated by each router for each area to which it belongs. It describes the states of the router's link to the area*. These are only flooded within a particular area. The link status and cost are two of the descriptors provided.
2	Network link entry	*Generated by the designated driver in multiaccess networks. They describe the set of routers attached to a particular network*. Flooded within the area that contains the network only
3 or 4	Summary link entry	*Originated by ABRs. Describes the links between the ABR and the internal routers of a local area*. These entries are flooded throughout the backbone area to the other ABRs. Type-3 describes routes to networks within the local area and are sent to the backbone area. Type-4 describes reachability to ASBRs. These link entries are not flooded through totally stubby areas.

5	Autonomous system external link entry External type 1 External type 2	*Originated by the ASBR. Describes routes to destinations external to the autonomous system.* Flooded throughout an OSPF autonomous system except for stub and totally stubby areas.

31. Configure a multi-area OSPF network (pg 216 – 236)

Route summarization ABR
Router(config-router)#**area** *area-id* **range** *address mask*
Area 1 range 172.16.32.0 255.255.224.0
Route summarization ASBR
Router(config-router)#**summary-address** *address mask*
Summary-address 172.16.32.0 255.255.224.0

Define an area as a stub – use no-summary to make it totally stubby.
Router(config-router)#area area-id stub [no-summary]

Configuring virtual links
Router(config-router)#**area** *area-id* **virtual-link** *router-id*

Commands:

- **router ospf** *process-id*
- **network** *address wildcard-mask* **area** *area-id*
- **area** *area-id* **range** *address mask* : used for summarization on a ABR
- **summary-address** *summary mask* : used for summarization on ASBR
- **area** *area-id* **stud [no-summary]** : used for stub, use no summary for totally stubby

Steps:

1. enable global configuration mode
2. enable ospf on the ABR or ASBR router
3. identify the ip networks and their areas.
1. Optional (configure summarization)

Ex of ABR: drawing on page 225

```
router>enable
router#config terminal
router(config)#router ospf 1
router(config-router)#network 172.16.32.1 0.0.0.0 area 1
router(config-router)#network 172.16.96.1 0.0.0.0 area 0
router(config-router)#area 0 range 172.16.96.0 255.255.224.0
router(config-router)#area 1 range 172.16.32.0 255.255.224.0
```

Ex of ABR: drawing on page 231

```
Router3>enable
router3#config terminal
router3(config)#router ospf 1
router3(config-router)#network 192.168.14.0 0.0.0.255 area 0
router3(config-router)#network 192.168.15.0 0.0.0.255 area 2
router3(config-router)#area 2 stub no-summary

router4>enable
router4#config terminal
router4(config)#router ospf 1
router4(config-router)#network 192.168.15.0 0.0.0.255 area 2
router4(config-router)#area 2 stub
```

32. Verify OSPF operation.

- Show ip ospf border-routers – displays the internal OSPF routing table entries to an ABR
- Show ip ospf virtual-links – displays parameters about the current state of OSPF virtual links
- Show ip ospf process-id – displays information about each area to which the router is connected, and indicates whether the router is an ABR, ASBR, or both.
- Show ip ospf database – displays the contents of the topological database maintained by the router.
    - Show ip ospf [process-id area-id] database [network] – displays network link stae information. The area ID is the area number associated with the OSPF address range defined in the network router configuration command when defining a particular area.
    - Show ip ospf [process-id area-id] database [asbr-summary] – displays information about asbr link states
    - Show ip ospf [process-id area-id] database [external] – displays information about autonomous system external link states
    - Show ip ospf [process-id area-id] database [database-summary] – displays database summary information and totals.

33. Describe Enhanced IGRP features and operation. (ch. 10)

EIGRP is a cisco proprietary protocol that combines the advantages of link state and distance vector routing protocols. Supports automatic route summarization and vlsm addressing.

- Rapid convergence – uses DUAL. Guarantees loop free operation at every instant throughout a route computation and allows all routers involved in a topology change to synchronize at the same time. Routers that are not affected by topology changes are not involved in recomputations.
- Reduced bandwidth usage – does not make periodic updates. It sends partial updates about a route when the path changes or when the metric for that route changes. The information is sent only to the routers that need it, in contrast to link state protocol operation, which sends a change update to all routers in the area.
- Multiple network layer support – supports appletalk, ip and novell.

EIGRP support for Novell IPX RIP and SAP –IPX RIP and SAP send updates every 60 seconds regardless of whether a network topology change has occurred.

- EIGRP supports incremental RIP and SAP updates. EIGRP sends out RIP and SAP updates only when changes occur, and only sends out the changed information.
- EIGRP IPX networks have a diameter of 224 hops instead of 15.
- EIGRP for Novell IPX provides optimal path selection. Unlike IPX which uses ticks and hop count to determine best route. EIGRP uses bandwidth and delay.

Enhanced IGRP Operation

- **Building the neighbor table** – a neighbor table is maintained by the EIGRP router and lists adjacent routers. Its purpose is to ensure bidirectional communication between each of the directly connected routers. EIGRP routers multicast hello packets to discover neighbor routers and to exchange route updates. The neighbor table includes the following key elements: *neighbor address, queue, smooth round trip timer, hold time.*
- **Discovering routes** –
  1. a new router (router A) comes up on the link and sends out a hello through all interfaces.
  2. Routers receiving the hello reply with update packets that contain all the routes they have in their topology tables, except those learned through that interface (split horizon). These update packets have the init bit set, indicating that this is the initialization process. An update packet includes information about the routes a neighbor is aware of, including the metric that the neighbor is advertising for each destination.
  3. Router A replies to each neighbor with an Ack packet, indicating that it received the update information.
  4. Router A puts all update packets in its topology table. The topology table includes all destinations advertised by neighboring routers. It is organized such that each destination is listed, along with all the neighbors that can get to the destination and their associated metrics.
  5. Router A then exchanges update packets with each of its neighbors.
  6. Upon receiving the update packets, each router sends and Ack packet to router A. when all updates are received, the router is ready to choose the primary and backup routes to keep in the topology table.
- **Choosing routes –**
  - EIGRP selects primary and backup routes that are kept in the topology table (up to 6). The primary routes are then moved to a routing table. EIGRP supports several types of routes: internal, external, and summary routes.
  - EIGRP uses the same composite metric as IGRP to determine the best path. The default criteria used are:
    - Bandwidth – the smallest bandwidth between source and destination
    - Delay – cumulative interface delay along the path.

    Following is additional criteria that can be used. These criteria are not recommended for use because they typically result in frequent recalculation of the topology table.
    - Reliability – worst reliability between source and destination based on keepalives
    - Loading – worst load on a link between source and destination based on bits per second
    - MTU – the smallest MTU.

  - EIGRP uses the DUAL algorithm to calculate the best route to a destination. DUAL selects routes based on the composite metric and ensures that the selected routes are loop free.

  <u>EIGRP uses the following process to determine which routes to keep in the topology and route tables</u>.
  1. DUAL is run on the topology table to determine the best and loop free primary and backup routes to each destination. (pg. 248-250)
     - "best" is the lowest cost route that is calculated by adding the cost between the next hop router and the destination (advertised distance) to the cost between the local router and the next hop router (feasible distance).
     - The next hop router(s) selected as the best path is referred to as the successor.

- The next hop router(s) for the backup path is referred to as the feasible successor.

2. The successors and feasible successors are kept in the topology table, along with all other routers, and referred to as possible successors. The only routes removed are those that have a metric of infinity.

- **Maintaining routes –** when there is a change in the network, the router that learned about the change advertises it to its neighbors by multicasting an update packet with the change.

34. Configure Enhanced IGRP (pg 253-258)

Configuring EIGRP for IP:

1. enable EIGRP and define the autonomous system number
   router(config)#**router eigrp** *autonomous-system-number*
2. indicate which networks are part of the EIGRP autonomous system.
   router(config)#**network** *network-number*
3. when using serial links, configure bandwidth, default is T1. For generic serial interfaces (PPP or HDLC), set the bandwidth to the line speed. For frame relay or point to point, set it to the CIR, or for multipoint connections set it to the sum of the all CIRs.
   Router(config-if)# **bandwidth** kilobits

Configuring EIGRP for IPX:

1. enable IPX routing
   router(config)#ipx routing
2. define EIGRP as the IPX routing protocol
   router(config-ipx-router)#**ipx router** {**eigrp** *autonomous-system-number* | **rip** }
3. indicate which networks are part of the EIGRP autonomous system.
   Router(config-router)#**network** *network-number*
4. Optional – if IPX RIP is also operating on the router, remove RIP form the networks using EIGRP
   Router(config-router)# **no network** *network-number*

Configuring EIGRP for IPX SAP Updates:

1. enable EIGRP for IPX
   router(config)#ipx routing
2. select the interface on which you want the SAP updates to be sent incrementally
3. instruct the router is issue SAP updates only when a change occurs.
   Router(config-if)#**ipx sap-incremental eigrp** *autonomous-system-number* [**rsup-only**]
   Use [rsup-only] is you are using rip instead of EIGRP to carry routing updates.

35. Verify Enhanced IGRP operation

- **show ip eigrp neighbors** – desplays neighbors discovered by EIGRP
- **show ip eigrp topology**– displays the eigrp topology table. This command shows the topology table, the active/passive state of routes, the number of successors, and the feasible distance to the destination.
- **Show ip route eigrp** – displays the current eigrp entries in the routing table
- **Show ip protocols** – displays the parameters and current state of the active routing protocol process. This command shows the eigrp autonomous system number, displays filtering and redistribution numbers as well as neighbors and distance information.
- **Show ip eigrp traffic** – displays the number of eigrp packets sent and received. Displays statistics on hello, updates, queries, replies, and acks.
- **Show ipx route** – displays the contents of the IPX routing table.

- **Show ipx eigrp neighbors** – displays the ipx neighbors discovered by eigrp.
- **Show ipx eigrp topology** – displays the topology table, the active/passive state of routes, the number of successors, and the feasible distance to the destination.

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

The capabilities covered include passive interfaces, default routes, static routes, route filtering, and redistributing routes between different protocols.

- **Using and configuring the passive-interface command** - The passive-interface command prevents all routing updates for a given routing protocol from being sent to or received from a network via a specific interface.
  1. select the router that requires the passive interface.
  2. Determine which 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*
     Type refers to the type of interface, such at serial or ethernet.
     Number refers to the interface number. Ethernet 0.

- **Using and configuring default routes** –
  Router(config)#**ip default-network** *network-number*
  Router(config)#**ipx advertised-default-route-only** *network*
  For IGRP or RIP also enable classless behavior
  Router(config)#**ip classless**

- **Using and configuring static routes**
  Router(config)#**ip route** *prefix mask* {*address* | *interface*} [*distance*] [**permanent**]
  Router (config)#**ipx route** {*network* | **default**} {*network.node* | *interface*} [**floating-static**]
- **Using and configuring route filters**
  Router(config-router)# **distribute-list** *access-list-number* | *name* **out** [*interface-name* | *routing-process* | *autonomous-system-number*].
  Router(config-router)# **distribute-list** *{access-list-number* | *name }* **in** *{type number}*

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

Chapter 11. review big time

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

Chapter 11 review big time

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

Chapter 11 review big time

40. Verify route redistribution.

- Know your network topology, particularly where redundant routes exist.
- Show the routing table of the appropriate routing protocol on a variety of routers in the internetwork using the show command.

- Perform a trace on some of the routes that go across the autonomous systems to verify that the shortest path is being used for routing, especially run traces to networks for which redundant routes exist.
- Use trace and debug commands to observe the routing update traffic on the ASBRs and internal routers.

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 day or night.

If you have a backup link for redundancy, you can use a combination of static and default routes. If both of these are active at the same time, BFP is required.

Any time your policy requirements differ from the policy of your ISP, BGP is required.

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

Use the **ip route** command to define a static route entry in the IP routing table.
The route 0.0.0.0 is a default route in the IP routing table.
Default static route ex:
Ip route 0.0.0.0 0.0.0.0 Serial 0

Use router bgp command to activate the BGP protocol and identify the local AS. The AS is assigned to you by the InterNIC.
Use the network command to permit BGP to advertise a network when it is present in the IP routing table.

BGP ex: (pg. 309)

Config for router A
Router bgp 100
Network 19.0.0.0
Neighbor 15.1.1.2 remote-as 200

Config for router B
Router bpg 200
Network 15.0.0.0
Neighbor 15.1.1.1 remote-as 100

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

- Dedicated – leased line, provides full-time synchronous connections.
- Asynchronous dial-in connectivity – can make temporary connections using PSTN.
- Dial-on-demand – connection is enabled only when a specific type of traffic initiates the call, or when you need a backup link. Uses PSTN or ISDN.
- Packet switched services – frame relay, x.25, smds, atm.

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

Dialup/Dedicated – PPP, SLIP, ARAP, CLIP
Dedicated Point to Point – HDLC, PPP, LAPB

Packet Switched – X.25-Lapb, Frame relay – ieft
Circuit switched – ISDN, X.25, frame relay

- PPP – common for dial up single user to lan or lan to lan (router to router) access. It supports the encapsulation of multiple upper layer protocols including ip and ipx, and user authentication. It is a standard
- HDLC – Cisco encapsulation type. It is used typically when communicating with another cisco device.
- LAPB – for packet switched networks, used to encapsulate x.25 packets. It can also be used over point to point links.
- Cisco/IETF – used to encapsulate frame relay traffic. 4 byte header, 2 for the DLCI and 2 for the packet type.

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

- Availability of services
- Application traffic
- Bandwidth
- Ease of management
- Routing protocol characteristics
- Cost

46. Describe the components that make up ISDN connectivity

ISDN is a collection of standards that define a digital architecture that provides an integrated void data capability utilizing the public switched network.

E-series – recommend telephone network standards
I-series – deals with concepts, terminology, and general methods.
Q-series – switching and signaling.

PUT DRAWING HERE PG. 336

ACRONYM	Device Type	Device Function
TE1	Terminal Endpoint 1	Designates a router as a device have a native ISDN interface
NT2	Network termination 2	The point at which all ISDN lines at the customer site are aggregated and switched using a customer switching device
NT1	Network termination 1	Converts BRI signals into a form used by the ISDN digital line
TE2	Terminal endpoint 2	Designates a router as a device requiring a TA for its BRI signals
TA	Terminal adapter	Converts 232, v.35 and other

		signals into BRI signals
LT	Line termination	Portion of the local exchange that terminates the local loop
ET	End termination	Portion of the exchange that communicates with other ISDN components in the ISDN cloud.

Reference Points
R – between a non ISDN compatible device and a terminal adapter
S – connect into the NT2, or customer switching device
T – references the outbound connection from the NT2 to the ISDN network
U – references the connection between the NT1 and the ISDN network

47. Configure ISDN BRI

See isdn stuff at end

1. define the switch type
2. set the SPIDs. Depends on switch type. Pg 341.
3. Set the encapsulation type

48. Configure Legacy dial-on-demand routing (DDR) chapter 14.

The redistribute command will make the router advertise the static route.

1. specify interesting traffic.
2. Define static routes.
   Router(config)#**ip config** prefix mask {address | interface } [distance] [permanent]
3. Configure the dialer information.

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

Ex:
Dialer-list 1 protocol ip permit
Dialer-list 1 protocol ipx permit

49. Configure dialer profiles

Chapter 14 pg. 360 – 364.

1. specify interesting traffic
2. define static routes
3. create the dialer interface
4. make a physical interface a dialer pool member
5. define the map class.

50. Verify DDR operation

- ping/telnet
- show dialer – general diagnostic information about an interface
- show isdn active – it shows that a call is in progress and lists the number called
- show ip route – displays the routes known to the router
- clear [dialer | interface] – clear a call that is in progress.

51. Configure dial backup

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

EX:
Int s 0
Backup interface serial 1
Backup load 60 5

52. Verify dial backup operation

??????

53. Configure Multilink PPP\

1. configure either dialer profiles or dialer rotary groups on selected interfaces, or select a 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

- show dialer
- debug ppp multilink

55. Configure snapshot routing

Snapshot routing – involves building a routing table based on a snapshot of routing information exchanged during an active time on the network. Can be applied to IP RIP, IGRP, IPX RIP, AND RTMP. Can't be used with Link state routing protocols including EIGRP due to periodic hellos.

Snapshot routing is a routing update mechanism that provides the following two key benefits:
1. it eliminates the need for configuring and maintaining large static tables by allowing dynamic routing protocols to be used on DDR lines.
2. It enables the exchange of routing updates across the DDR link only when you specify it to.

Snapshot routing is designed for hub and spoke environments where remote sites dial into the same central router, ISDN is a primary target for snapshot routing. Not recommended for mesh networks.

ON THE CLIENT SIDE:
1. enter the interface configuration mode for the interface.
2. Enable snapshot routing on the client router
   Router(config-if)# **snapshot client** *active-time quiet-time* [**suppress-statechange-updates**] **dialer**
3. define a dialer map the includes the server router to call
   router(config-if)# **dialer map snapshot** *sequence-number* **name** *name dial-string*

ON THE SERVER SIDE:
1. select the physical interface and enable snapshot routing
   router(config-if)# **snapshot server** *active-timer* [**dialer**]
2. define a dialer map the includes the client routers
   router(config-if)# **dialer map snapshot** *sequence-number* **name** *name dial-string*

Client router Ex:
Interface BRI 0
Snapshot client 5 720 dialer
Dialer map snapshot 1 name server-router 14155551212

Server-rouer Ex:
Interface dialer 1
Snapshot server 5 dialer
Dialer map snapshot 1 name client-router 17605551111

56. Configure IPX spoofing

IPX spoofing is the process of pretending that the WAN link is up and keepalive traffic is being answered across it on a regular basis.

IPX spoofing refers to the process of replying on behalf of another device that is being polled in order to avoid bringing up a DDR link for overhead traffic.

1. turn off route caching on the interface that is spoofing. This is a requirement because the router needs to look inside the packet to determine its contents (it needs to know what to spoof)
   router(config)#**no ipx route-cache**
2. enable SPX spoofing of the idle DDR link.
   Router(config)#**ipx spx-spoof**
3. Enable IPX watchdog spoofing
   Router(config)#**ipx watchdog-spoof**
4. Set the time in seconds that must elapse before SPX spoofing of keepalive packets can occur
   Router(config)#**ipx spx-idle-time** *time*

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

A routable protocol has a layer 3 address. IPX, IP
A non routable protocol does not have a layer 3 address. LAT, SNA, NetBIOS, MOP,

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

- **Transparent Bridging** – used to connect 2 or more physical networks into one LAN. Most often found in ethernet networks in which bridges pass frames along one hop at a time based on tables associating end nodes with bridge ports. It does not alter the data frame, is never a source or destination for frames, and makes the attached segments look like one cable.
- **Encapsulated Bridging** – is used to connect LANs via an independent transport connection, normally FDDI or serial. 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 – allows combinations of routing and bridging functionality to be selectively provided.
- **Source-Route Bridging** – method of bridging developed by IBM for use in token ring networks. With SRB, the entire route to a destination is predetermined, in real-time, prior to the sending of data (contrast this with transparent bridging, where bridging occurs on a hop by hop basis). With SRB, the source places the complete source to destination route in the frame header of all inter-LAN frames.

- **Source-Route Transparent Bridging** – employ both SRB and transparent bridging technologies in 1 device. SRT is used for Token Ring networks where some stations are performing source routing and some are not. An SRT bridge does not translate between the two bridging domains, nor does it convert frames from ethernet to token ring. Traffic with routing information will be handled using SRB configuration, and traffic without routing information will be handled using the transparent bridging configuration.
- **Source-Route Translational Bridging** (SR/TLB) – allows LANs of ethernet and token ring to be connected together. It translates from back and forth between the 2.

59. Configure transparent bridging chapter 17

1. select a spanning tree protocol in global config mode.
   Router(config)# **bridge** bridge-group **protocol** {**ieee** | **dec** }
2. assign a priority to the bridge in global config mode. Helps determine root bridge.
   Router(config-if)# **bridge-group** bridge-group number
3. assign the interface to a spanning tree group in interface config mode
   router(config-if)# **bridge** bridge-group number **priority** number
4. assign a cost to the outgoing interface in interface config mode.
   Router(config-if)# **bridge-group** bridge-group **path-cost** cost

EX:

Bridge 1 protocol ieee
Bridge 1 priority 100

Interface ethernet 0
Bridge-group 1
Bridge-group 1 path-cost 10

Show bridge
Show span

60. Configure integrated routing and bridging (IRB)

Example on page 447

1. enable IRB.
   Router(config)# **bridge irb**
2. Configure the BVI
   Router(config-if)# **interface bvi** bridge-group
3. Enable the BVI to accept and route routable packets
   Router(config)# **bridge** bridge-group **route** protocol
4. Enable routing on the BVI for the protocols that you want to route
   Router(config)# **interface bvi** number
   Router(config)# **ip address** ip-address mask

DRAW EX HERE pg. 453

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

- SRB is a bridging method in which one end host locates another end host by discovering available source to destination paths. SRB determines the entire route to a destination, in real time, prior to the sending of data.
- Connects multiple physical TR's into one logical network segment

3 types of explorer packets:
- local ring test frame – checks the local ring for the destination end station.
- All routes explorer - SNA
- Single route explorer – NetBIOS

62. Configure SRB

Router(config-if)#**source-bridge** *local-ring bridge-number target-ring*
Router(config-if)#**source-bridge spanning** **:** used to pass single route explorer packets
Router(config)#**bridge** *bridge-group* **protocol ibm** **:** used to enable automatic spanning tree

EX of dual port:
No ip routing
!
interface TokenRing 0
ip address 131.108.129.2 255.255.255.0
source-bridge 129 1 130
source-bridge spanning
!
interface tokenring 1
ip address 131.108.129.2 255.255.255.0
source-bridge 130 1 129
source-bridge spanning

Ex of Multiring
Rings 1000, 1001, 1002, 1003 are all source-route bridged to each other across ring group 7

!
source-bridge ring-group 7
!
interface tokenring 0
source-bridge 1000 1 7
source-bridge spanning
!
interface tokenring 1
source-bridge 1001 1 7
source-bridge spanning
!
interface tokenring 2
source-bridge 1002 1 7
source-bridge spanning

!
interface tokenring 3
source-bridge 1003 1 7
source-bridge spanning

63. Configure source route transparent bridging (SRT)

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. A frame contains RIF information if the RII bit is set. The RII bit is bit 1 of byte 0 of the source address.

64. Configure source route translational bridging (SR/TLB)

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

EX on page 473

Bridge 4 protocol ieee
Source-bridge ring-group 10
Source-bridge tranparent 10 13 1 4

Interface ethernet 0
Bridge-group 4
Interface ethernet 1
Bridge-group 4
Interface tokenring 0
Source-bridge 500 1 10
Source-bridge spanning
Interface tokenring 1
Source-bridge 501 1 10
Source-bridge spanning

65. Verify SRB operation

- Show source-bridge – maximum route descriptor length in hops, number of frames and bytes received on the interface for SRB, number of frames and bytes transmitted on interface for SRB, ring number of this token ring, bridge number of this router, group in which the interface is configured, describes the ring groups, describes the explorer packets, interface on which explorers

were received, number of spanning tree explorers, number of all routes explored, total number of spanning and all routes explorers.

- Show rif – how: means through which the RIF was learned; Idle: number of minutes since the last response was received directly from this node. RIF

ISDN STUFF

ISDN Configuration Tasks

- **Global configuration**
- **Select switch type**
- **Specify traffic to trigger DDR call**

- **Interface configuration**
- **Select interface specifications**
- **Configure ISDN addressing**

Selecting the ISDN Switch Type

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

- **Specifies the type of ISDN switch with which the router communicates**

- **Other line configuration requirements vary for specific providers**

Use the isdn switch-type global command to specify the CO switch to which the router connects. For BRI ISDN service, the switch type can be one of the following:

Switch Type	Description
basic-5ess	AT&T basic rate switches (USA)
basic-dms100	NT DMS-100 (North America)
basic-ni1	National ISDN-1 (North America)
basic-1tr6	German 1TR6 ISDN switches
basic-nwnet3	Norwegian Net3 switches
basic-nznet3	New Zealand Net3 switches
basic-ts013	Australian TS013 switches

basic-net3	Switch type for NET3 in United Kingdom and Europe
nnt	NTT ISDN switch (Japan)
nn3	French VN3 ISDN switches
none	No specific switch specified

Specifying Traffic to Trigger Call

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

Router (config) # dialer-group *group-number*

Router (config) # dialer map *protocol next-hop-address* [name *hostname*] [speed 56|64] [broadcast] [dialer string *dial-string*]

These commands are used to configure dial-on-demand calls that will initiate a connection.

Selecting Interface Specifications

Router (config) # interface bri *interface-number*

- **Selects the interface for ISDN BRI operation**

Router (config) # encapsulation [*ppp* | *hdlc*]

- **Selects framing for ISDN BRI**

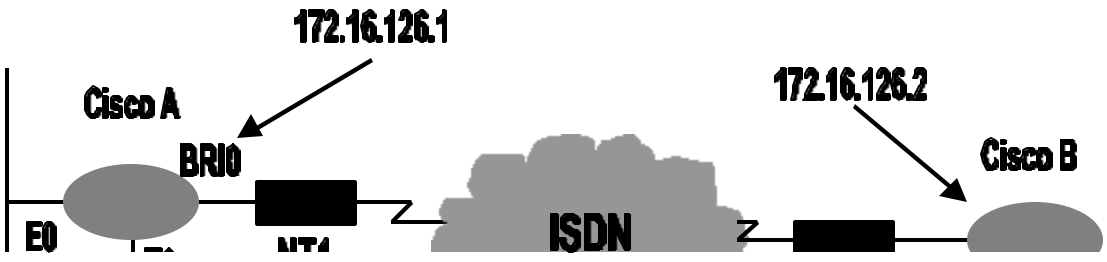
The interface bri interface-number command designates the interface used for ISDN on a router acting as a TE1

If the router does not have a native BRI (is a TE2 device), it must use an external ISDN terminal adapter. On the TE2 router, use the command **interface serial** *interface-number*.

Use the encapsulation ppp command if you want PPP encapsulation for your ISDN interface. This is the case if you want any of the rich LCP options that PPP offers (for example, CHAP authentication). You must use PPP PAP or CHAP if you will receive calls from more than one dial-up source.

To revert from PPP encapsulation to the default, use the **encapsulation hdlc** command.

Configuring for a Simple ISDN Call



DDR is configured to connect Cisco A to Cisco B. The network between the serial interfaces of the two routers uses 8 bits of subnetting. Static route statements define the IP route to the Cisco B LAN interfaces over 172.16.126.0

IP packets will initiate a call, but not IGRP routing updates. Interesting traffic to DDR must be defined in an access list.

The number dialled is for the remote ISDN device. This number is provided by the Regional Bell Operating Company (RBOC) offering the ISDN service. Cisco B (the next-hop router to the destination networks) has subnets 126 and 29 directly connected.

BRI Simple Configuration Example

```
! set up switch type, static route and dialer for ISDN on Cisco A
isdn switch-type basic-5ess
ip route 172.16.29.0 255.255.255.0 172.16.126.2
dialer-list 1 protocol ip permit
!
! configure BRI interface for PPP; set address and mask
interface bri 0
encapsulation ppp
ip address 172.16.126.1 255.255.255.0
!
! refer to protocols in dialer-list to identify interesting packets dialer-group 1
!
! select call start, stop, and other ISDN provider details
dialer wait-for-carrier-time 15
dialer idle-timeout 300
isdn spid1 0145678912
! call setup details for router
dialer map ip 172.16.126.2 name cisco-b 445
```

In the example:

Command	Description
isdn switch-type	Selects the AT&T switch as the CO ISDN switch on this interface.
dialer-list 1 protocol ip permit	Associates permitted IP traffic with the dialer group 1. The router will not start an ISDN call for any other packet traffic with dialer group 1.
interface bri 0	Selects the interface with TA and other ISDN functions on the router.
encapsulation ppp	Use PPP encapsulation on the selected interface.
dialer-group 1	Associates the serial 0 interface with dialling access group 1.
dialer wait-for-carrier-time	Specifies a 15 –second maximum time for the provider to respond once the call initiates.
dialer idle-timeout 300	Number of seconds of idle time before the router drops the ISDN call. Note that a long duration is configured to delay termination.

dialer map command	Description
ip	Name of protocol.
172.16.126.2	Destination address.
name	An identification for the remote side router. Refers to called router.
445	ISDN connection number used to reach this DDR destination.

This is was designed by a person who took the ACRC course from a Cisco Authorized Training Center Page numbers and diagram numbers are found throughout this document, reference the actual ACRC course book. Unfortunately Cisco makes you take a very expensive class to buy this book, so we hope the summary will be useful. If you have taken the ACRC course you will find this an excellent review prior to taking the exam.