[Updated Constantly]

HERE

CCNA 4 (v5.0.3 + v6.0) Chapter 4 Exam Answers Full

1. **Which range represents all the IP addresses that are affected when network 10.120.160.0 with a wildcard mask of 0.0.7.255 is used in an ACE?**
   - 10.120.160.0 to 10.120.168.0
   - 10.120.160.0 to 10.127.255.255
   - 10.120.160.0 to 10.120.191.255
   - **10.120.160.0 to 10.120.167.255***

   A wildcard mask of 0.0.7.255 means that the first 5 bits of the 3rd octet must remain the same but the last 3 bits can have values from 000 to 111. The last octet has a value of 255, which means the last octet can have values from all zeros to all 1s.

2. **What two functions describe uses of an access control list? (Choose two.)**
   - ACLs assist the router in determining the best path to a destination.
   - Standard ACLs can restrict access to specific applications and ports.
   - **ACLs provide a basic level of security for network access.***
   - ACLs can permit or deny traffic based upon the MAC address originating on the router.
   - **ACLs can control which areas a host can access on a network.***
3. **Which two statements describe the effect of the access control list wildcard mask 0.0.0.15? (Choose two.)**
   - **The first 28 bits of a supplied IP address will be matched.***
   - The last four bits of a supplied IP address will be matched.
   - The first 28 bits of a supplied IP address will be ignored.
   - **The last four bits of a supplied IP address will be ignored.***
   - The last five bits of a supplied IP address will be ignored.
   - The first 32 bits of a supplied IP address will be matched.

   A wildcard mask uses 0s to indicate that bits must match. 0s in the first three octets represent 24 bits and four more zeros in the last octet, represent a total of 28 bits that must match. The four 1s represented by the decimal value of 15 represents the four bits to ignore.

4. **Refer to the exhibit. A network administrator is configuring an ACL to limit the connection to R1 vty lines to only the IT group workstations in the network 192.168.22.0/28. The administrator verifies the successful Telnet connections from a workstation with IP 192.168.22.5 to R1 before the ACL is applied. However, after the ACL is applied to the**

interface Fa0/0, Telnet connections are denied. What is the cause of the connection failure?

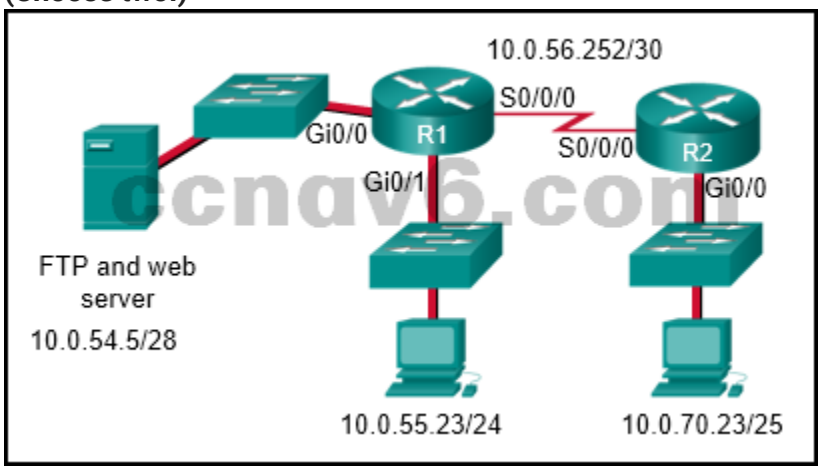
```
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# access-list 120 deny ip 192.168.20.0 0.0.3.255 10.0.10.0 0.0.0.255
R1(config)# access-list 120 permit tcp 192.168.22.0 0.0.0.15 10.0.10.0 0.0.0.15 eq 23
R1(config)# access-list 120 permit ip any any
R1(config)# line vty 0 4
R1(config-line)# password admin-in
R1(config-line)# access-class 120 in
R1(config-line)# exit
R1(config)# interface fastEthernet 0/0
R1(config-if)# ip address 10.0.10.1 255.255.255.252
R1(config-if)# no shutdown
R1(config-if)# ip access-group 120 in
R1(config-if)# end
R1#

R1# show access-lists
Extended IP access list 120
    deny ip 192.168.20.0 0.0.3.255 10.0.10.0 0.0.0.255 (16 match(es))
    permit tcp 192.168.22.0 0.0.0.15 10.0.10.0 0.0.0.15 eq telnet
    permit ip any any
R1#
```


- The enable secret password is not configured on R1.
- **The IT group network is included in the deny statement.***
- The permit ACE specifies a wrong port number.
- The permit ACE should specify protocol ip instead of tcp.
- The login command has not been entered for vty lines.

The source IP range in the deny ACE is 192.168.20.0 0.0.3.255, which covers IP addresses from 192.168.20.0 to 192.168.23.255. The IT group network 192.168.22.0/28 is included in the 192.168.20/22 network. Therefore, the connection is denied. To fix it, the order of the deny and permit ACE should be switched.

5. **Refer to the exhibit. The network administrator that has the IP address of 10.0.70.23/25 needs to have access to the corporate FTP server (10.0.54.5/28). The FTP server is also a web server that is accessible to all internal employees on networks within the 10.x.x.x address. No other traffic should be allowed to this server.**
Which extended ACL would be used to filter this traffic, and how would this ACL be applied? (Choose two.)



- R1(config)# interface s0/0/0
  R1(config-if)# ip access-group 105 outR2(config)# interface gi0/0
  R2(config-if)# ip access-group 105 in
- **access-list 105 permit tcp host 10.0.70.23 host 10.0.54.5 eq 20**
  access-list 105 permit tcp host 10.0.70.23 host 10.0.54.5 eq 21
  access-list 105 permit tcp 10.0.0.0 0.255.255.255 host 10.0.54.5 eq www
  access-list 105 deny ip any host 10.0.54.5
  access-list 105 permit ip any any*
- access-list 105 permit ip host 10.0.70.23 host 10.0.54.5
  access-list 105 permit tcp any host 10.0.54.5 eq www
  access-list 105 permit ip any any
- **R1(config)# interface gi0/0**
  R1(config-if)# ip access-group 105 out*
- access-list 105 permit tcp host 10.0.54.5 any eq www
  access-list 105 permit tcp host 10.0.70.23 host 10.0.54.5 eq 20
  access-list 105 permit tcp host 10.0.70.23 host 10.0.54.5 eq 21

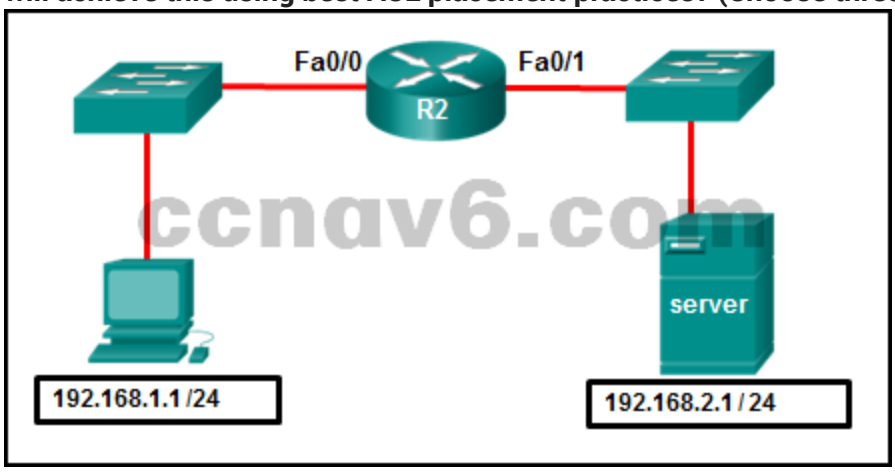
The first two lines of the ACL allow host 10.0.70.23 FTP access to the server that has the IP address of 10.0.54.5. The next line of the ACL allows HTTP access to the server from any host that has an IP address that starts with the number 10. The fourth line of the ACL denies any other type of traffic to the server from any source IP address. The last line of the ACL permits anything else in case there are other servers or devices added to the 10.0.54.0/28 network. Because traffic is being filtered from all other locations and for the 10.0.70.23 host device, the best place to put this ACL is closest to the server.

6. **A network administrator is designing an ACL. The networks 192.168.1.0/25, 192.168.0.0/25, 192.168.0.128/25, 192.168.1.128/26, and 192.168.1.192/26 are affected by the ACL. Which wildcard mask, if any, is the most efficient to use when specifying all of these networks in a single ACL permit entry?**
   - 0.0.0.127
   - 0.0.0.255
   - **0.0.1.255***
   - 0.0.255.255

   A single ACL command and wildcard mask should not be used to specify these particular networks or other traffic will be permitted or denied and present a security risk.
   Write all of the network numbers in binary and determine the binary digits that are identical in consecutive bit positions from left to right. In this example, 23 bits match perfectly. The wildcard mask of 0.0.1.255 designates that 25 bits must match.

7. **The exhibit shows router R2 connected through int fa0/0 to a switch which in turn is connected to host with an IP address 192.168.1.1 /24. R2 is connected to another switch through interface fa0/1 and the switch is connected to a server with the IP address 192.168.2.1 /24.Refer to the exhibit. A network administrator wants to permit only host 192.168.1.1 /24 to be able to access the server 192.168.2.1 /24. Which three commands**

will achieve this using best ACL placement practices? (Choose three.)



- R2(config-if)# ip access-group 101 out
- R2(config)# access-list 101 permit ip 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
- R2(config)# interface fastethernet 0/1
- **R2(config)# interface fastethernet 0/0***
- **R2(config)# access-list 101 permit ip host 192.168.1.1 host 192.168.2.1***
- **R2(config-if)# ip access-group 101 in***
- R2(config)# access-list 101 permit ip any any

An extended ACL is placed as close to the source of the traffic as possible. In this case.it is placed in an inbound direction on interface fa0/0 on R2 for traffic entering the router from host with the IP address192.168.1.1 bound for the server with the IP address192.168.2.1.

8. **Which two statements are correct about extended ACLs? (Choose two)**
   - **Extended ACLs evaluate the source and destination addresses.***
   - **Port numbers can be used to add greater definition to an ACL.***
   - Extended ACLs end with an implicit permit statement.
   - Extended ACLs use a number range from 1-99.
   - Multiple ACLs can be placed on the same interface as long as they are in the same direction.

   Extended ACLs can be used for precise traffic-filtering. Extended ACLs check for both source and destination addresses of packets. They also check the protocols and port numbers (or services), thus allowing for a greater range of criteria on which to base the ACL.

9. **Which three values or sets of values are included when creating an extended access control list entry? (Choose three.)**
   - **source address and wildcard mask***
   - **access list number between 100 and 199***
   - source subnet mask and wildcard mask
   - access list number between 1 and 99
   - **destination address and wildcard mask***
   - destination subnet mask and wildcard mask
   - default gateway address and wildcard mask
10. **Refer to the exhibit. This ACL is applied on traffic outbound from the router on the interface that directly connects to the 10.0.70.5 server. A request for information from a secure web**

page is sent from host 10.0.55.23 and is destined for the 10.0.70.5 server. Which line of the access list will cause the router to take action (forward the packet onward or drop the packet)?

```
1 - access-list 100 permit tcp host 10.0.55.23 host 10.0.70.55 eq 1719
2 - access-list 100 permit tcp host 10.0.55.23 host 10.0.70.55 eq 1720
3 - access-list 100 deny tcp any any eq 443
4 - access-list 100 deny tcp any any eq www
5 - access-list 100 permit ip any any
```


- 1
- **3***
- 2
- the deny ip any any that is at the end of every ACL
- 5
- 4

The first two lines of the ACL allow traffic from a particular application from the IP address 10.0.55.23 destined for 10.0.70.55. Because neither of these lines meets the criterion of request for information from a secure web page (port 443 is HTTPS) from 10.0.55.23 to the web server located at 10.0.70.5, no action is taken by the router. The third line is a match and because the “permission” is to deny the packet, the packet is dropped. No further examination is done by the router.

11. **Which set of access control entries would allow all users on the 192.168.10.0/24 network to access a web server that is located at 172.17.80.1, but would not allow them to use Telnet?**
    - access-list 103 deny tcp host 192.168.10.0 any eq 23
      access-list 103 permit tcp host 192.168.10.1 eq 80
    - **access-list 103 permit tcp 192.168.10.0 0.0.0.255 host 172.17.80.1 eq 80**
      access-list 103 deny tcp 192.168.10.0 0.0.0.255 any eq 23*
    - access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
      access-list 103 deny tcp 192.168.10.0 0.0.0.255 any eq 23
    - access-list 103 permit 192.168.10.0 0.0.0.255 host 172.17.80.1
      access-list 103 deny tcp 192.168.10.0 0.0.0.255 any eq telnet

    For an extended ACL to meet these requirements the following need to be included in the access control entries:
    identification number in the range 100-199 or 2000-2699
    permit or deny parameter
    protocol
    source address and wildcard
    destination address and wildcard
    port number or name

12. **Which two packet filters could a network administrator use on an IPv4 extended ACL? (Choose two.)**
    - **destination UDP port number***
    - source TCP hello address
    - **ICMP message type***
    - destination MAC address

- computer type

Extended access lists commonly filter on source and destination IPv4 addresses and TCP or UDP port numbers. Additional filtering can be provided for protocol types.

13. **Which two ACE commands will block traffic that is destined for a web server which is listening to default ports? (Choose two.)**
    - access-list 110 deny tcp any any lt 80
    - access-list 110 deny tcp any any eq 21
    - **access-list 110 deny tcp any any eq https***
    - **access-list 110 deny tcp any any gt 75***
    - access-list 110 deny tcp any any gt 443

    Traffic that is destined for a web server will use port 80 or 443. The keyword eq represents equal, gt represents greater than, and lt less than.

14. **Which feature is unique to IPv6 ACLs when compared to those of IPv4 ACLs?**
    - the use of wildcard masks
    - **an implicit permit of neighbor discovery packets***
    - an implicit deny any any ACE
    - the use of named ACL ACE

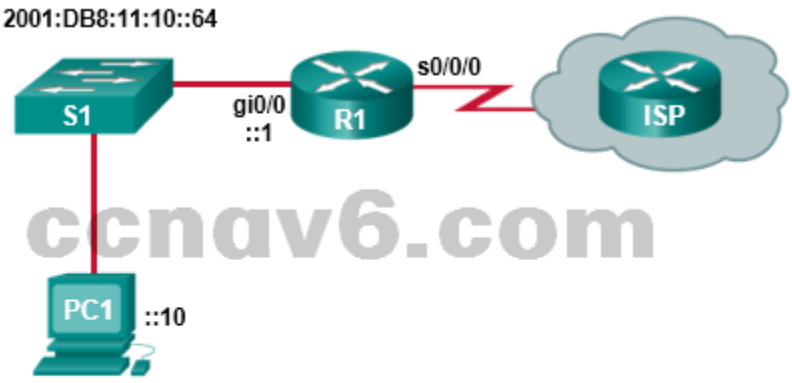
    One of the major differences between IPv6 and IPv4 ACLs are two implicit permit ACEs at the end of any IPv6 ACL. These two permit ACEs allow neighbor discovery operations to function on the router interface.

15. **What two ACEs could be used to deny IP traffic from a single source host 10.1.1.1 to the 192.168.0.0/16 network? (Choose two.)**
    - access-list 100 deny ip 10.1.1.1 255.255.255.255 192.168.0.0 0.0.255.255
    - **access-list 100 deny ip 10.1.1.1 0.0.0.0 192.168.0.0 0.0.255.255***
    - access-list 100 deny ip 192.168.0.0 0.0.255.255 host 10.1.1.1
    - **access-list 100 deny ip host 10.1.1.1 192.168.0.0 0.0.255.255***
    - access-list 100 deny ip 192.168.0.0 0.0.255.255 10.1.1.1 0.0.0.0
    - access-list 100 deny ip 192.168.0.0 0.0.255.255 10.1.1.1 255.255.255.255

    There are two ways to identify a single host in an access list entry. One, is to use the host keyword with the host IP address, the other is to use a wildcard mask of 0.0.0.0 with the host IP address. The source of the traffic to be inspected by the access list goes first in the syntax and the destination goes last.

16. **Refer to the exhibit. The IPv6 access list LIMITED_ACCESS is applied on the S0/0/0 interface of R1 in the inbound direction. Which IPv6 packets from the ISP will be dropped by**

the ACL on R1?




```
R1# show access-lists
IPv6 access list LIMITED_ACCESS
          permit tcp any host 2001:DB8:11:10::10 eq www sequence 10
          permit tcp any host 2001:DB8:11:10::10 eq 443 sequence 20
          deny ipv6 any 2001:DB8:11:10::/64 sequence 30
```

- **ICMPv6 packets that are destined to PC1***
- neighbor advertisements that are received from the ISP router
- HTTPS packets to PC1
- packets that are destined to PC1 on port 80

The access list LIMITED_ACCESS will block ICMPv6 packets from the ISP. Both port 80, HTTP traffic, and port 443, HTTPS traffic, are explicitly permitted by the ACL. The neighbor advertisements from the ISP router are implicitly permitted by the implicit permit icmp any any nd-na statement at the end of all IPv6 ACLs.

17. **Which command is used to activate an IPv6 ACL named ENG_ACL on an interface so that the router filters traffic prior to accessing the routing table?**
    - ipv6 access-class ENG_ACL in
    - ipv6 traffic-filter ENG_ACL out
    - **ipv6 traffic-filter ENG_ACL in***
    - ipv6 access-class ENG_ACL out

    For the purpose of applying an access list to a particular interface, the ipv6 traffic-filter IPv6 command is equivalent to the access-group IPv4 command. The direction in which the traffic is examined (in or out) is also required.

18. **What is the wildcard mask that is associated with the network 192.168.12.0/24?**
    - **0.0.0.255**
    - 0.0.255.255
    - 0.0.0.256
    - 255.255.255.0

    The wildcard mask can be found by subtracting the subnet mask from 255.255.255.255.

19. **Which IPv6 ACL command entry will permit traffic from any host to an SMTP server on network 2001:DB8:10:10::/64?**
    - permit tcp host 2001:DB8:10:10::100 any eq 23
    - **permit tcp any host 2001:DB8:10:10::100 eq 25***

- permit tcp any host 2001:DB8:10:10::100 eq 23
- permit tcp host 2001:DB8:10:10::100 any eq 25

The IPv6 access list statement, permit tcp any host 2001:DB8:10:10::100 eq 25, will allow IPv6 packets from any host to the SMTP server at 2001:DB8:10:10::100. The source of the packet is listed first in the ACL, which in this case is any source, and the destination is listed second, in this case the IPv6 address of the SMTP server. The port number is last in the statement, port 25, which is the well-known port for SMTP.

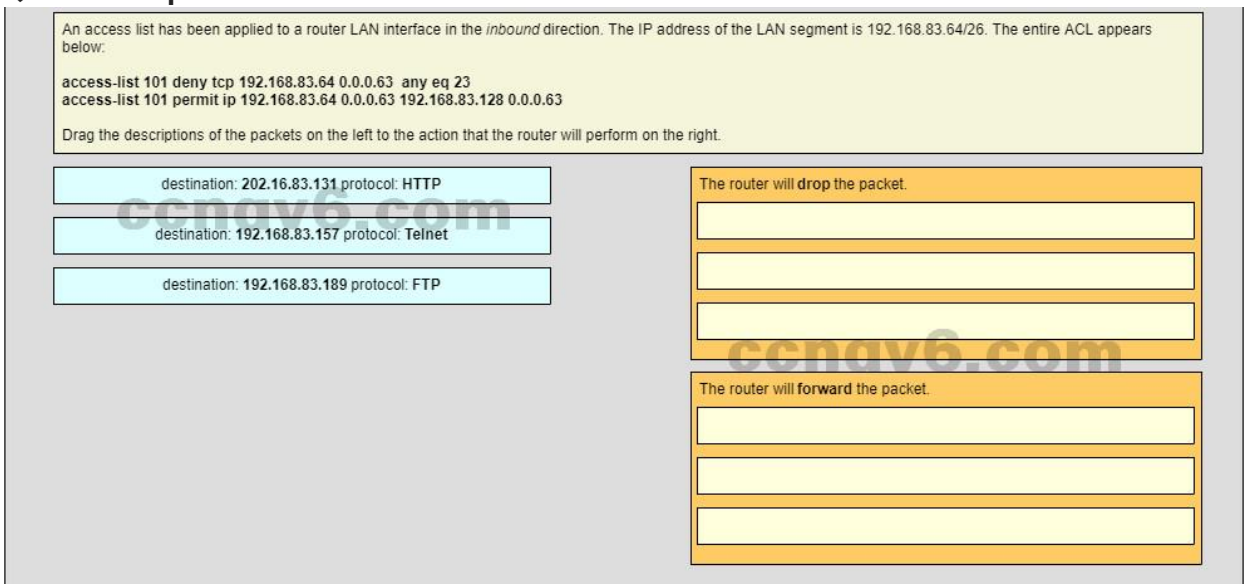
20. **In applying an ACL to a router interface, which traffic is designated as outbound?**
    - traffic for which the router can find no routing table entry
    - traffic that is going from the destination IP address into the router
    - **traffic that is leaving the router and going toward the destination host***
    - traffic that is coming from the source IP address into the router

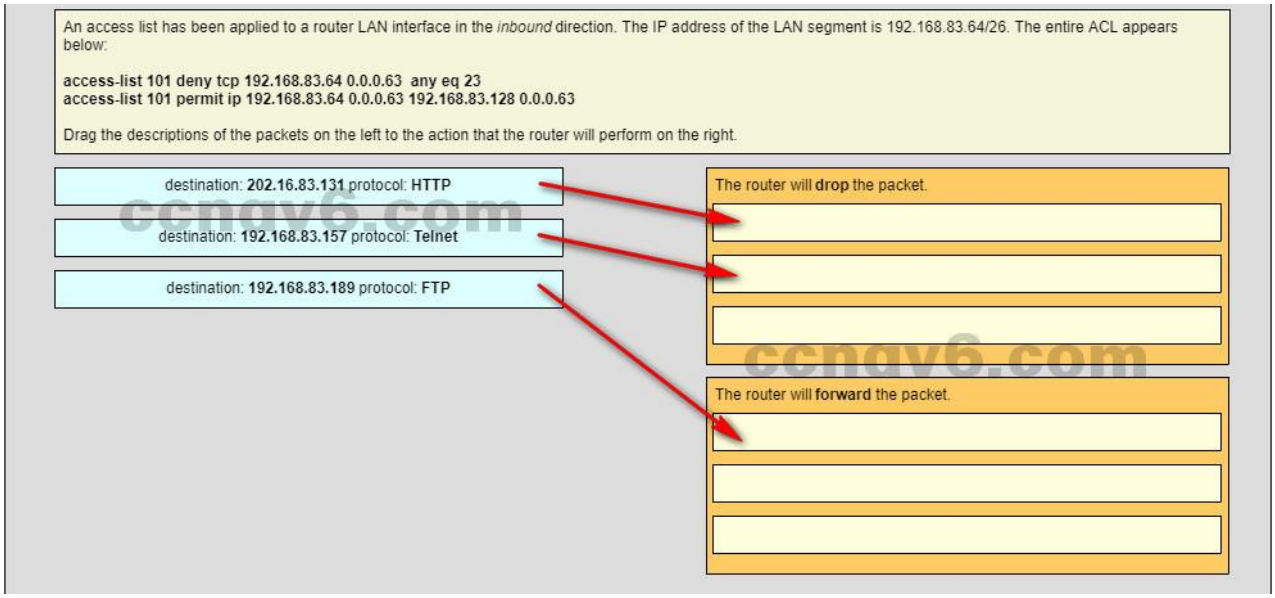
    Inbound and outbound are interpreted from the point of view of the router. Traffic that is designated in an inbound ACL will be denied or permitted when coming into that router interface from a source. Traffic that is designated in an outbound ACL will be denied or permitted when going out the interface to the destination.

21. **Fill in the blanks. Use dotted decimal format.**
    The wildcard mask that is associated with the network 192.168.12.0/24 is _____
    Correct Answer: 0.0.0.255*

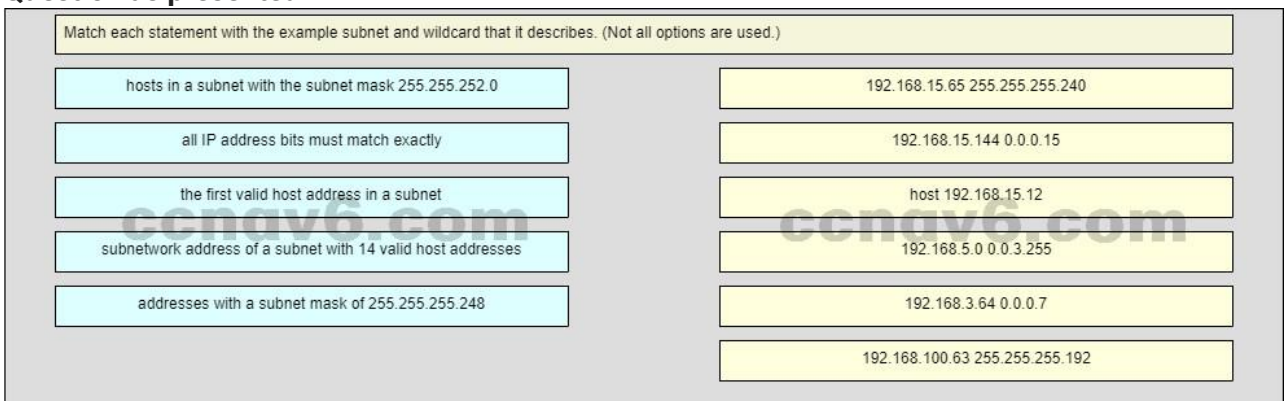
    The wildcard mask can be found by subtracting the subnet mask from 255.255.255.255.
    Mask 255.255.255.255
    Subnet mask – 255.255.255.0
    Wild card mask 0 . 0 . 0. 255

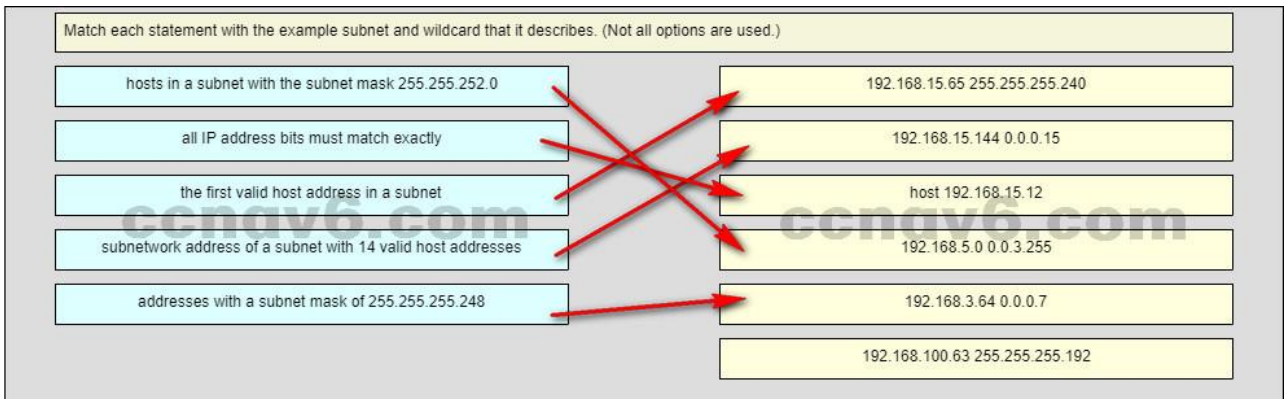
22. **Question as presented:**





23. **Question as presented:**





Converting the wildcard mask 0.0.3.255 to binary and subtracting it from 255.255.255.255 yields a subnet mask of 255.255.252.0.
Using the host parameter in a wildcard mask requires that all bits match the given address. 192.168.15.65 is the first valid host address in a subnetwork beginning with the subnetwork address 192.168.15.64. The subnet mask contains 4 host bits, yielding subnets with 16 addresses.
192.168.15.144 is a valid subnetwork address in a similar subnetwork. Change the wildcard

mask 0.0.0.15 to binary and subtract it from 255.255.255.255, and the resulting subnet mask is 255.255.255.240.
192.168.3.64 is a subnetwork address in a subnet with 8 addresses. Convert 0.0.0.7 to binary and subtract it from 255.255.255.255, and the resulting subnet mask is 255.255.255.248. That mask contains 3 host bits, and yields 8 addresses.

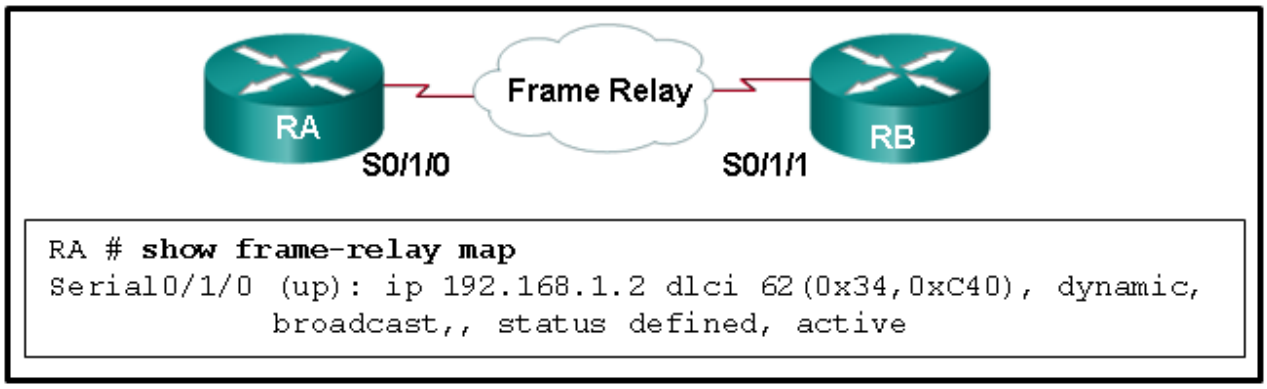
Older Version

24. **What is a characteristic of Frame Relay that provides more flexibility than a dedicated line?**
    - Dedicated physical circuits are installed between each site.
    - Customers use dedicated circuits in increments of 64 kb/s.
    - The Frame Relay cloud allocates as much bandwidth as required to active PVCs to maintain the connection.
    - **One router WAN port can be used to connect to multiple destinations.***
25. **What are the two major criteria that constitute the cost of a Frame Relay circuit? (Choose two.)**
    - circuit management fees
    - **local loop***
    - end-to-end connectivity
    - **required bandwidth***
    - QoS
26. **A router interface connects to a Frame Relay network over a preconfigured logical circuit that does not have a direct electrical connection from end to end. Which type of circuit is being used?**
    - SVC
    - full mesh
    - **PVC***
    - hub and spoke
    - dedicated leased line
27. **Which Frame Relay topology provides a connection from every site to every other site and maintains a high amount of reliability?**
    - partial mesh
    - **full mesh***
    - star
    - hub and spoke
28. **Which technology allows a Layer 3 IPv4 address to be dynamically obtained from a Layer 2 DLCI?**
    - **Inverse Address Resolution Protocol***
    - Inverse Neighbor Discovery
    - Address Resolution Protocol
    - Neighbor Discovery
29. **A network administrator has statically configured the LMI type on the interface of a Cisco router that is running Cisco IOS Release 11.2. If the service provider modifies its own LMI type in the future, what step must the network administrator take?**
    - The network administrator must modify the keepalive time interval to maintain connectivity with the LMI type of the service provider.

- The network administrator simply has to verify connectivity with the provider, because the router has an LMI autosensing feature that automatically detects the LMI type.
- **The network administrator must statically set the LMI type to be compatible with the service provider.***
- The network administrator does not have to do anything, because all LMI types are compatible with one another.

30. **Which two functions are provided by the Local Management Interface (LMI) that is used in Frame Relay networks? (Choose two.)**
    - **simple flow control***
    - error notification
    - congestion notification
    - mapping of DLCIs to network addresses
    - **exchange of information about the status of virtual circuits***
31. **Which parameter would be specified in a Frame Relay provider contract for a particular company?**
    - **CIR***
    - DE
    - Inverse ARP enabled/disabled
    - QoS
32. **Which three notification mechanisms are used when congestion is present in a Frame Relay network? (Choose three.)**
    - **BECN***
    - CIR
    - **DE***
    - DLCI
    - **FECN***
    - inverse ARP
33. **Why would a customer request a Frame Relay circuit with a CIR of zero?**
    - to have better QoS
    - to have a backup circuit for critical data transmissions
    - **to have a link with reduced costs***
    - to have a circuit used for voice traffic
    - to have a circuit used for network management traffic
34. **Which provider-negotiated parameter would allow a customer to send data above the rate of the bandwidth specified by the CIR?**
    - **Bc***
    - DE
    - Be
    - FECN
35. **What is the purpose of applying the command frame-relay map ip 10.10.1.2 110 broadcast?**
    - **to configure a device with a static Frame Relay map that also allows the forwarding of routing updates***
    - to allow Frame Relay frames to be broadcast on all Frame Relay interfaces
    - to allow Frame Relay frames to be broadcast toward host 10.10.1.2
    - to allow Frame Relay frames to be broadcast over DLCI 110
    - to support IPv6 traffic over the NBMA network by using DLCI 110

36. **Refer to the exhibit. Which two statements are correct? (Choose two.)**



- The Frame Relay map was set by using the command frame-relay map.
- The DLCI that is attached to the VC on RB to RA is 62.
- The IPv4 address of interface S0/1/0 on RA is 192.168.1.2.
- **The DLCI that is attached to the VC on RA to RB is 62. ***
- **The IPv4 address of interface S0/1/1 on RB is 192.168.1.2. ***

37. **Refer to the exhibit. Which statement is true about Frame Relay traffic on R1?**

```
R1# show frame-relay pvc 201
PVC Statistics for interface Serial0/0/0 (Frame Relay DTE)
DLCI = 201, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/0.102
  input pkts 21          output pkts 17          in bytes 1834
  out bytes 1698         dropped pkts 0          in pkts dropped 0
  out pkts dropped 0              out bytes dropped 0
  in FECN pkts 0         in BECN pkts 0          out FECN pkts 0
  out BECN pkts 0        in DE pkts 0            out DE pkts 0
  out bcast pkts 1       out bcast bytes 34
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 0 bits/sec, 1 packets/sec
  pvc create time 00:18:07, last time pvc status changed 00:01:20
```

- Traffic that is mapped to DLCI 201 will exit subinterface Serial 0/0/0.201.
- **Traffic that exits subinterface Serial 0/0/0.102 is marked with DLCI 201.***
- Traffic on Serial 0/0/0 is experiencing congestion between R1 and the Frame Switch.
- Frames that enter router R1 from a Frame Relay neighbor will have DLCI 201 in the frame header.

38. **Which three actions can be taken to solve Layer 3 routing protocol router reachability issues when using Frame Relay? (Choose three.)**

- **Use subinterfaces.***
- Disable Inverse ARP.
- **Disable split horizon.***
- **Use a full mesh topology.***
- Configure static DLCI mappings.
- Use the keyword cisco as the LMI type.

39. **When would the multipoint keyword be used in Frame Relay PVCs configuration?**

- when global DLCIs are in use

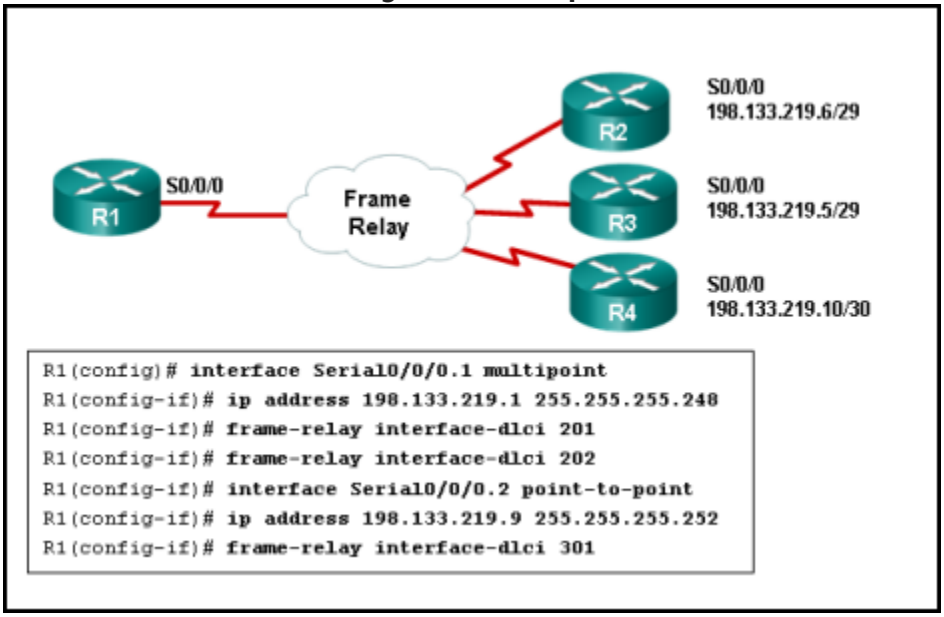
- when using physical interfaces
- when multicasts must be supported
- **when participating routers are in the same subnet***

40. **A network engineer has issued the interface serial 0/0/1.102 point-to-point command on a router that will be communicating with another router over a Frame Relay virtual circuit that is identified by the DLCI 102. Which two commands would be appropriate for the network engineer to issue next? (Choose two.)**
    - no ip address
    - no shutdown
    - encapsulation frame relay
    - **frame-relay interface-dlci 102 ***
    - **ip address 10.1.1.10 255.255.255.252***
41. **Which two Frame Relay router reachability issues are resolved by configuring logical subinterfaces? (Choose two.)**
    - Frame Relay is unable to map a remote IP address to a DLCI.
    - **Link-state routing protocols are unable to complete neighbor discovery.***
    - LMI status inquiry messages sent to the network are not received.
    - Inverse ARP fails to associate all IP addresses to the correct DLCIs.
    - **Distance vector routing protocols are unable to forward routing updates back out the incoming interface to other remote routers.***
42. **Refer to the exhibit. A network administrator has implemented the show interfaces serial 0/1/0 command. What can be verified from the displayed output?**

```
R1# show interfaces serial 0/1/0
Serial0/1/0 is up, line protocol is up
  Hardware is GT96K Serial
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  LMI enq sent  443, LMI stat recvd 444, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 0, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 1023  LMI type is CISCO  frame relay DTE
  FR SVC disabled, LAPF state down
  Broadcast queue 0/64, broadcasts sent/dropped 1723/0, interface broadcasts 1582
  Last input 00:00:01, output 00:00:01, output hang never
<output omitted>
```

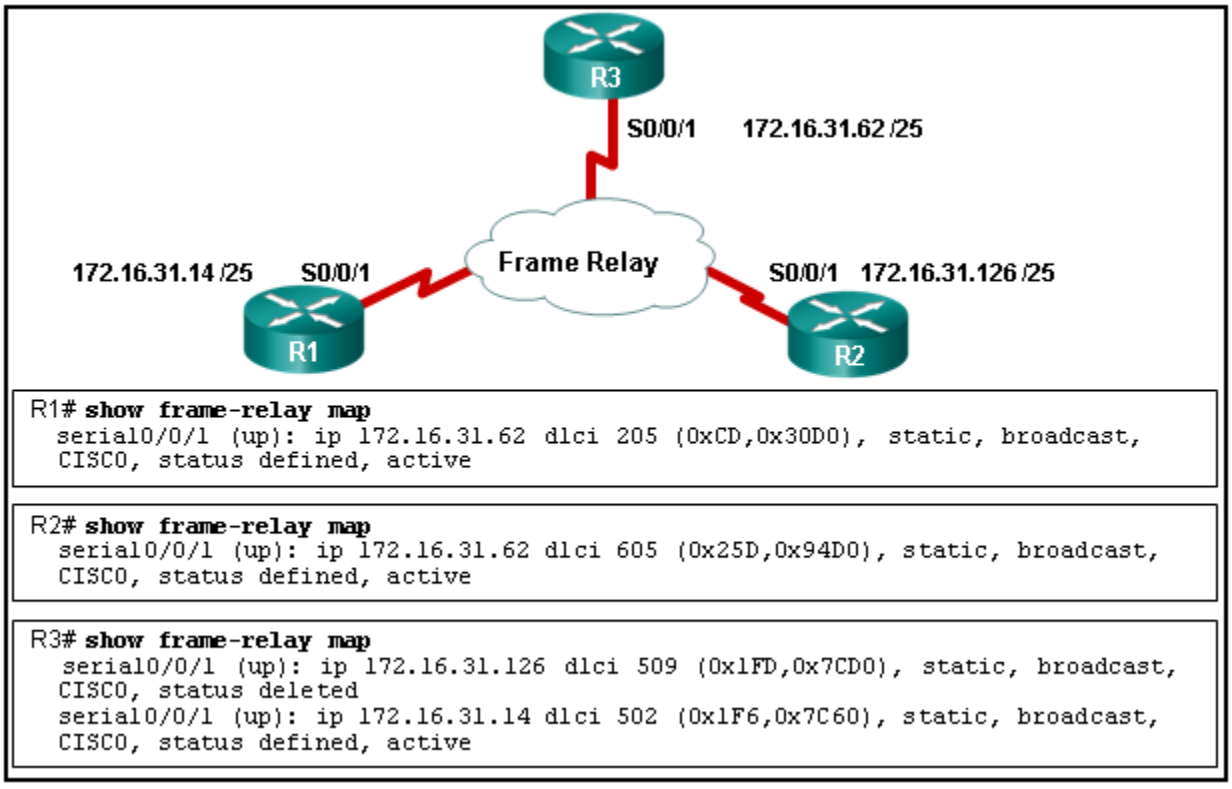
    - Router R1 connects to multiple sites through the serial 0/1/0 interface.
    - Router R1 is not using the default LMI type.
    - **Router R1 is forwarding traffic on interface serial 0/1/0 using the local DLCI 1023.***
    - Router R1 has been configured with Frame Relay via the ietf keyword.
43. **The show frame-relay pvc command is best utilized to display the number for which type of packets that are received by the router?**
    - LMI status messages
    - Inverse ARP messages
    - Inverse Neighbor Discovery messages
    - **FECN and BECN messages***
44. **Refer to the exhibit. A network administrator is configuring Frame Relay subinterfaces on R1. A distance vector routing protocol has also been configured. Data is routing**

successfully from R1 to networks that are connected to R2, R3, and R4, but routing updates between R2 and R3 are failing. What is the possible cause of this failure?



- Subinterfaces cannot be used on multipoint Frame Relay links.
- Two DLCI identifiers cannot be configured on one subinterface.
- Multipoint Frame Relay networks cannot be used with this IP addressing scheme.
- **Split horizon is preventing successful routing table updates on the multipoint link.***

45. **Refer to the exhibit. A network administrator issues the show frame-relay map command to troubleshoot the Frame Relay connection problem. Based on the output, what is the possible cause of the problem?**



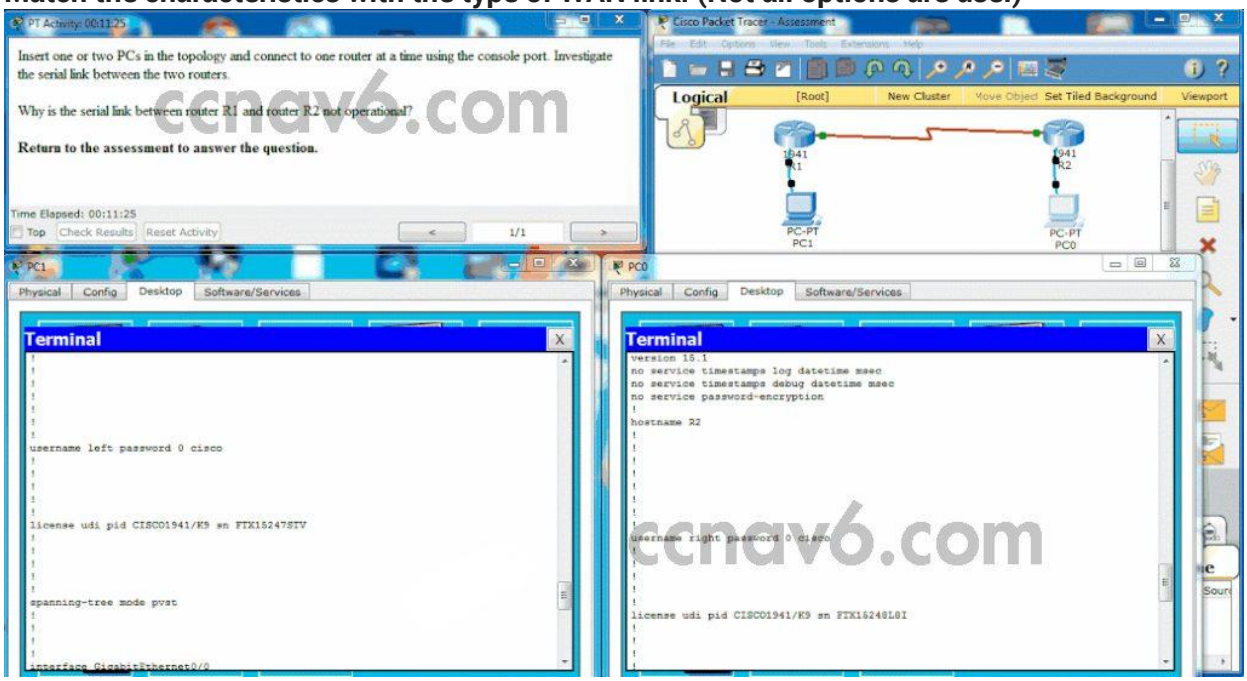
- The S0/0/1 interface of the R2 router is down.

- The IP address on S0/0/1 of R3 is configured incorrectly.
- Inverse ARP is providing false information to the R1 router.
- **The Frame Relay map statement on the R3 router for the PVC to R2 is configured with an incorrect DLCI number.***
- The S0/0/1 interface of the R2 router has been configured with the encapsulation frame relay ietf command.

46. **Fill in the blank. Use an acronym.**
The Frame Relay **DLCI** identifies a connection from one endpoint to a remote destination.

47. **Fill in the blank.**
The encapsulation frame-relay **ietf** command enables Frame Relay encapsulation and allows connection to a device from a different vendor.

48. **Match the characteristics with the type of WAN link. (Not all options are use.)**



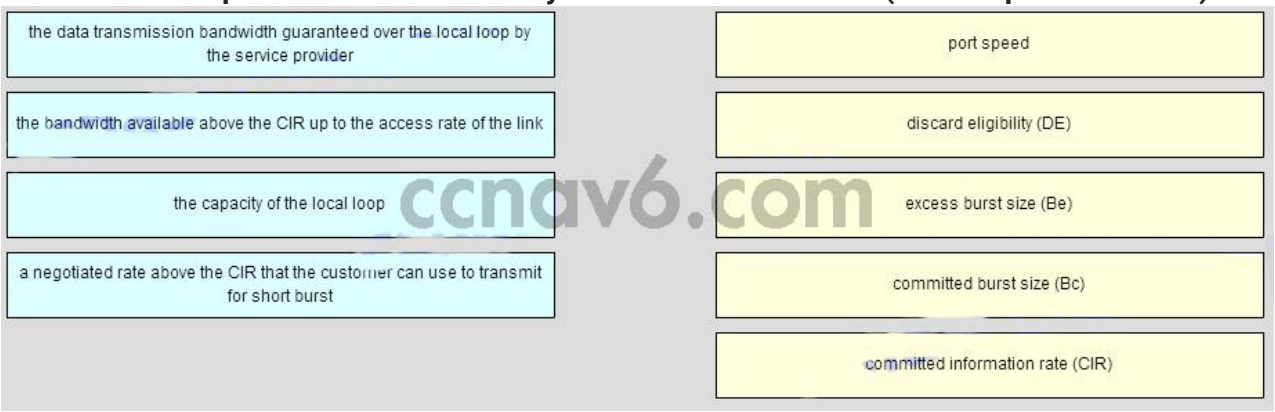
Place the options in the following order:
Leased line
[+] customers pay for an end-to-end connection
[+] customers do not share the line
[+] requires more equipment to purchase and maintain
[+] used in one-to-one network link only
Frame Relay
[#] used in one-to-many networks
[#] uses virtual circuits
[#] customers share bandwidth

49. **A network administrator uses the following command to configure a Frame Relay connection on a router towards the service provider:**
R1(config-if)# frame-relay map ip 209.165.200.225 102 broadcast
What is the purpose of using the broadcast keyword?

- to support IP address to MAC address resolution for the interface in the service provider site

- **to support dynamic routing protocol updates across the link***
- to enable VoIP packet transmission across the link
- to enable dynamic IP address-to-DLCI mapping

50. **What is an advantage of Frame Relay WAN technology compared with leased lines?**
    - **It uses one interface to connect to several remote sites.***
    - It offers a guaranteed direct electrical circuit from end to end.
    - It provides permanent dedicated capacity to the customers.
    - It supports both voice and data traffic.
51. **A network administrator of a large organization is designing a Frame Relay network. The organization needs redundancy between some key sites but not all. What WAN topology should the administrator choose to meet their needs?**
    - **partial mesh***
    - star
    - full mesh
    - extended star
52. **Match the descriptions to the Frame Relay transmission rate term. (Not all options are use.)**



Place the options in the following order:
port speed –> the capacity of the local loop
– not scored –
excess burst size (Be) –> the bandwidth available above the CIR up to the access rate of the link
committed burst size (Bc) –> a negotiated rate above the CIR that the customer can use to transmit for short burst
committed information rate (CIR) –> the data transmission bandwidth guaranteed over the local loop by the service provider