CCNA 3 v7.0 Final Exam Answers Full – Enterprise Networking, Security, and Automation

itexamanswers.net/ccna-3-v7-0-final-exam-answers-full-enterprise-networking-security-and-automation.html

December 22, 2019

How to find: Press **"Ctrl + F"** in the browser and fill in whatever wording is in the question to find that questio **are two types of attacks used on DNS open resolvers? (Choose** n/answer.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

CCNA 3 Final Exam Answers

1. Which design feature will limit the size of a failure domain in an enterprise network?

- the purchase of enterprise equipment that is designed for large traffic volume
- the installation of redundant power supplies
- the use of a collapsed core design
- **the use of the building switch block approach**

2. Which two things should a network administrator modify on a router to perform password recovery? (Choose two.)

- the system image file
- the NVRAM file system
- **the configuration register value**
- **the startup configuration file**
- system ROM

3. What type of network uses one common infrastructure to carry voice, data, and video signals?

- borderless
- **converged**
- managed
- switched

4. What are three advantages of using private IP addresses and NAT? (Choose three.)

- **hides private LAN addressing from outside devices that are connected to the Internet**
- **permits LAN expansion without additional public IP addresses**
- reduces CPU usage on customer routers
- creates multiple public IP addresses
- improves the performance of the router that is connected to the Internet
- **conserves registered public IP addresses**

5. Which two scenarios are examples of remote access VPNs? (Choose two.)

- All users at a large branch office can access company resources through a single VPN connection.
- A small branch office with three employees has a Cisco ASA that is used to create a VPN connection to the HQ.
- A toy manufacturer has a permanent VPN connection to one of its parts suppliers.
- **A mobile sales agent is connecting to the company network via the Internet connection at a hotel.**
- **An employee who is working from home uses VPN client software on a laptop in order to connect to the company network.**

6. What are three benefits of cloud computing? (Choose three.)

- It utilizes end-user clients to do a substantial amount of data preprocessing and storage.
- It uses open-source software for distributed processing of large datasets.
- **It streamlines the IT operations of an organization by subscribing only to needed services.**
- **It enables access to organizational data anywhere and at any time.**
- It turns raw data into meaningful information by discovering patterns and relationships.
- **It eliminates or reduces the need for onsite IT equipment, maintenance, and management.**

7. What is a characteristic of a single-area OSPF network?

- All routers share a common forwarding database.
- All routers have the same neighbor table.
- **All routers are in the backbone area.**
- All routers have the same routing table.

8. What is a WAN?

- a network infrastructure that spans a limited physical area such as a city

- **a network infrastructure that provides access to other networks over a large geographic area**
- a network infrastructure that provides access in a small geographic area
- a network infrastructure designed to provide data storage, retrieval, and replication

9. A network administrator has been tasked with creating a disaster recovery plan. As part of this plan, the administrator is looking for a backup site for all of the data on the company servers. What service or technology would support this requirement?

- **data center**
- virtualization
- dedicated servers
- software defined networking

10. Which type of OSPF packet is used by a router to discover neighbor routers and establish neighbor adjacency?

- link-state update
- **hello**
- database description
- link-state request

11. Which two statements are characteristics of a virus? (Choose two.)

- A virus has an enabling vulnerability, a propagation mechanism, and a payload.
- **A virus can be dormant and then activate at a specific time or date.**
- A virus provides the attacker with sensitive data, such as passwords.
- A virus replicates itself by independently exploiting vulnerabilities in networks.
- **A virus typically requires end-user activation.**

Explanation: The type of end user interaction required to launch a virus is typically opening an application, opening a web page, or powering on the computer. Once activated, a virus may infect other files located on the computer or other computers on the same network.

12. Which public WAN access technology utilizes copper telephone lines to provide access to subscribers that are multiplexed into a single T3 link connection?

- ISDN
- **DSL**
- cable
- dialup

13. A customer needs a metropolitan area WAN connection that provides high-speed, dedicated bandwidth between two sites. Which type of WAN connection would best fulfill this need?

- packet-switched network
- **Ethernet WAN**
- circuit-switched network
- MPLS

14. A company has contracted with a network security firm to help identify the vulnerabilities of the corporate network. The firm sends a team to perform penetration tests to the company network. Why would the team use debuggers?

- to detect installed tools within files and directories that provide threat actors remote access and control over a computer or network
- **to reverse engineer binary files when writing exploits and when analyzing malware**
- to obtain specially designed operating systems preloaded with tools optimized for hacking
- to detect any evidence of a hack or malware in a computer or network

15. Consider the following output for an ACL that has been applied to a router via the access-class in command. What can a network administrator determine from the output that is shown?

```
R1#
Standard IP access list 2
10 permit 192.168.10.0, wildcard bits 0.0.0.255 (2 matches)
20 deny any (1 match)
```

- Two devices connected to the router have IP addresses of 192.168.10. x .
- **Two devices were able to use SSH or Telnet to gain access to the router.**
- Traffic from one device was not allowed to come into one router port and be routed outbound a different router port.
- Traffic from two devices was allowed to enter one router port and be routed outbound to a different router port.

Explanation: The access-class command is used only on VTY ports. VTY ports support Telnet and/or SSH traffic. The match permit ACE is how many attempts were allowed using the VTY ports. The match deny ACE shows that a device from a network other than 192.168.10.0 was not allowed to access the router through the VTY ports.

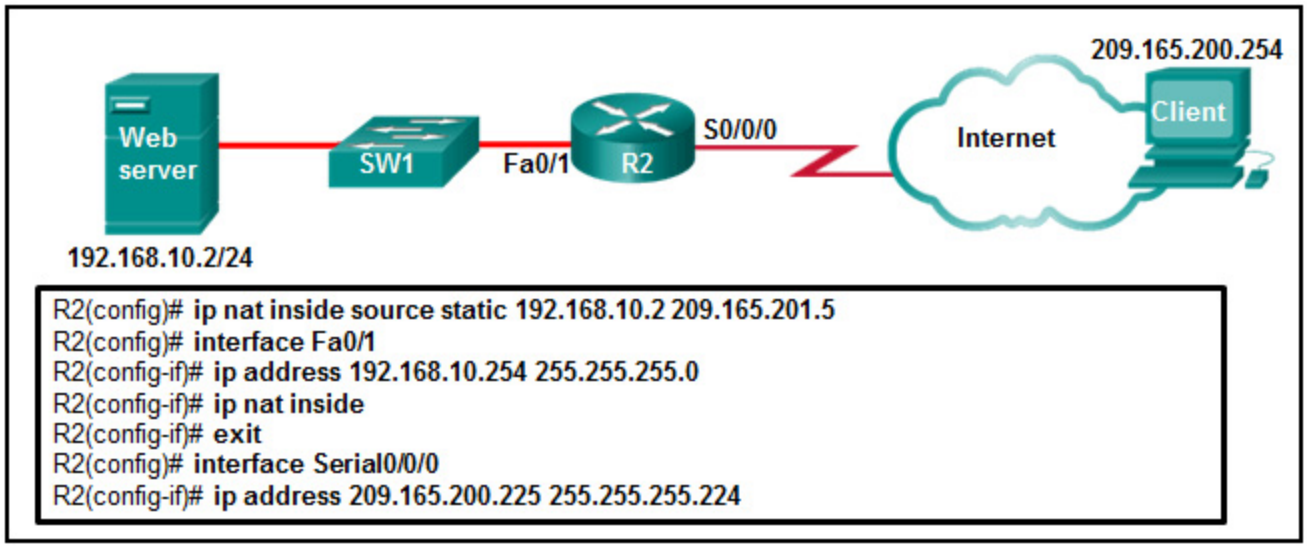
16. What command would be used as part of configuring NAT or PAT to clear dynamic entries before the timeout has expired?

- clear ip dhcp
- **clear ip nat translation**
- clear access-list counters
- clear ip pat statistics

17. What are two characteristics of video traffic? (Choose two.)

- Video traffic consumes less network resources than voice traffic consumes.
- **Video traffic latency should not exceed 400 ms.**
- Video traffic is more resilient to loss than voice traffic is.
- Video traffic requires a minimum of 30 kbs of bandwidth.
- **Video traffic is unpredictable and inconsistent.**

18. Refer to the exhibit. A technician is configuring R2 for static NAT to allow the client to access the web server. What is a possible reason that the client PC cannot access the web server?



- The IP NAT statement is incorrect.
- Interface Fa0/1 should be identified as the outside NAT interface.
- **Interface S0/0/0 should be identified as the outside NAT interface.**
- The configuration is missing a valid access control list.

Explanation: Interface S0/0/0 should be identified as the outside NAT interface. The command to do this would be R2(config-if)# ip nat outside.

19. In setting up a small office network, the network administrator decides to assign private IP addresses dynamically to workstations and mobile devices. Which feature must be enabled on the company router in order for office devices to access the internet?

- UPnP

- MAC filtering
- **NAT**
- QoS

Explanation: Network Address Translation (NAT) is the process used to convert private addresses to internet-routable addresses that allow office devices to access the internet.

20. A data center has recently updated a physical server to host multiple operating systems on a single CPU. The data center can now provide each customer with a separate web server without having to allocate an actual discrete server for each customer. What is the networking trend that is being implemented by the data center in this situation?

- online collaboration
- BYOD
- **virtualization**
- maintaining communication integrity

21. Refer to the exhibit. Which address or addresses represent the inside global address?

```
Router1 (config)# ip nat inside source static 192.168.0.100 209.165.20.25
Router1 (config)# interface serial0/0/0
Router1 (config-if)# ip nat inside
Router1 (config-if)# ip address 10.1.1.2 255.255.255.0
Router1 (config)# interface serial 0/0/2
Router1 (config-if)# ip address 209.165.20.25  255.255.255.0
Router1 (config-if)# ip nat outside
```

- 192.168.0.100
- 10.1.1.2
- any address in the 10.1.1.0 network
- **209.165.20.25**

22. Which two IPsec protocols are used to provide data integrity?

- **MD5**
- DH
- AES
- **SHA**
- RSA

Explanation: The IPsec framework uses various protocols and algorithms to provide data confidentiality, data integrity, authentication, and secure key exchange. Two popular algorithms used to ensure that data is not intercepted and modified (data integrity) are MD5 and SHA. AES is an encryption protocol and provides data confidentiality. DH (Diffie-Hellman) is an algorithm used for key exchange. RSA is an algorithm used for authentication.

23. If an outside host does not have the Cisco AnyConnect client preinstalled, how would the host gain access to the client image?

- The Cisco AnyConnect client is installed by default on most major operating systems.
- **The host initiates a clientless VPN connection using a compliant web browser to download the client.**
- The host initiates a clientless connection to a TFTP server to download the client.
- The host initiates a clientless connection to an FTP server to download the client.

Explanation: If an outside host does not have the Cisco AnyConnect client preinstalled, the remote user must initiate a clientless SSL VPN connection via a compliant web browser, and then download and install the AnyConnect client on the remote host.

24. A company is considering updating the campus WAN connection. Which two WAN options are examples of the private WAN architecture? (Choose two.)

- **leased line**
- cable
- digital subscriber line
- **Ethernet WAN**
- municipal Wi-Fi

Explanation: An organization can connect to a WAN through basic two options:

- **Private WAN infrastructure** – such as dedicated point-to-point leased lines, PSTN, ISDN, Ethernet WAN, ATM, or Frame Relay
- **Public WAN infrastructure** – such as digital subscriber line (DSL), cable, satellite access, municipal Wi-Fi, WiMAX, or wireless cellular including 3G/4G

25. Which type of QoS marking is applied to Ethernet frames?

- IP precedence
- DSCP
- ToS
- **CoS**

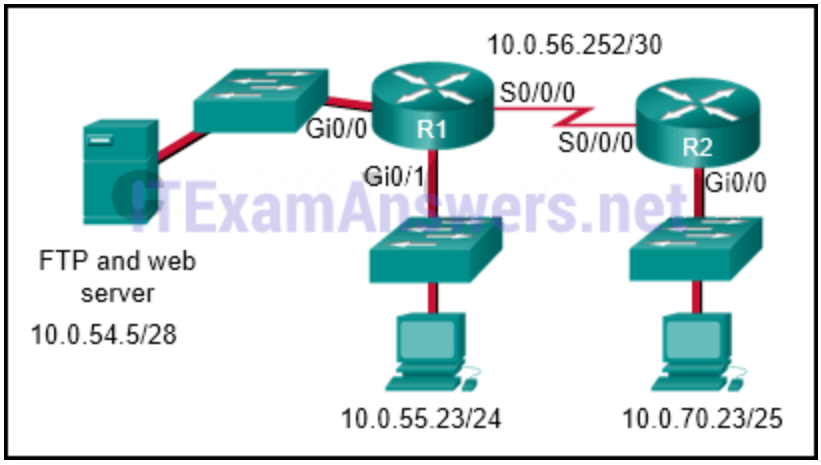
26. Refer to the exhibit. Routers R1 and R2 are connected via a serial link. One router is configured as the NTP master, and the other is an NTP client. Which two pieces of information can be obtained from the partial output of the show ntp associations detail command on R2? (Choose two.)

```
R2# show ntp associations detail
192.168.1.2 configured, authenticated, our_master, sane, valid,
stratum 3
<output omitted>
```

- Both routers are configured to use NTPv2.
- **Router R1 is the master, and R2 is the client**
- The IP address of R2 is 192 168.1.2.
- Router R2 is the master, and R1 is the client
- **The IP address of R1 is 192.168.1.2**

Explanation: With the show NTP associations command, the IP address of the NTP master is given.

27. 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 out
R2(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

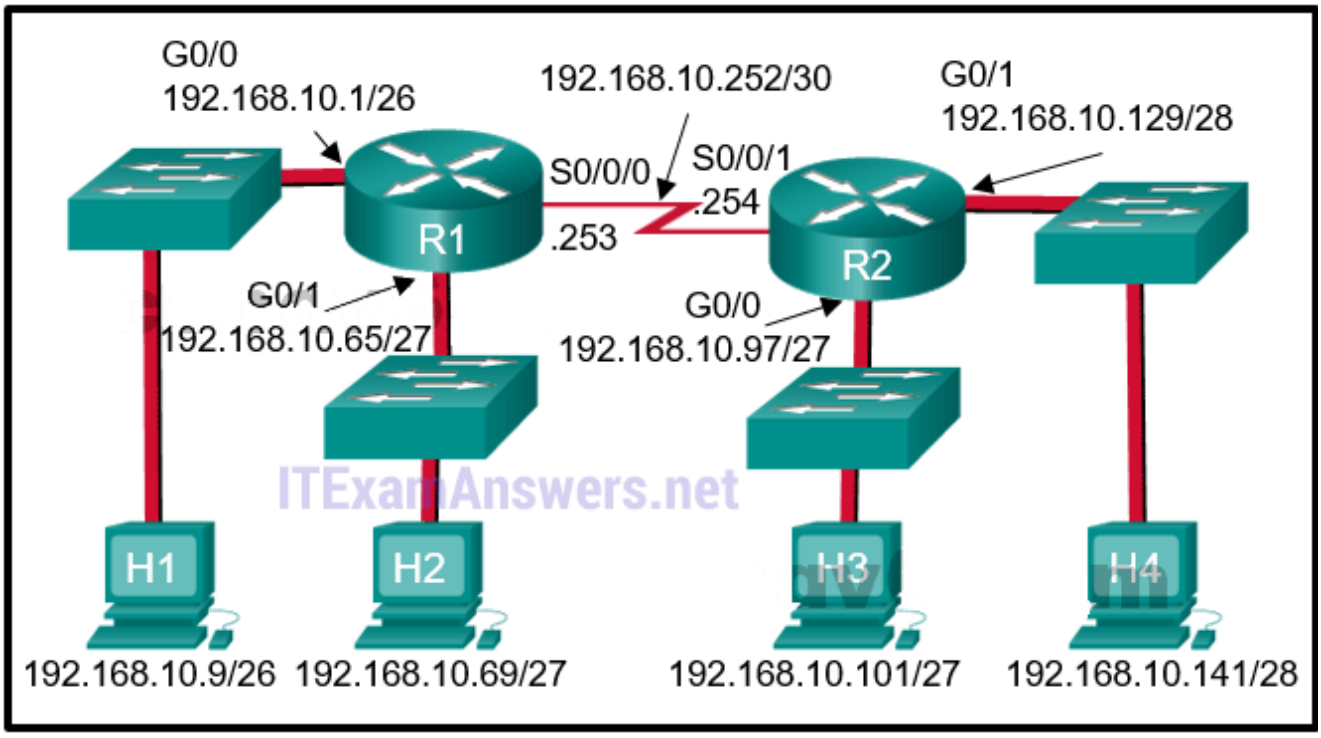
access-list 105 permit ip host 10.0.70.23 host 10.0.54.5
access-list 105 permit tcp any host 10.0.54.5 eq www
access-list 105 permit ip any any

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

Explanation: 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.

28. Refer to the exhibit. If the network administrator created a standard ACL that allows only devices that connect to the R2 G0/0 network access to the devices on the R1 G0/1 interface, how should the ACL be applied?



- inbound on the R2 G0/0 interface
- **outbound on the R1 G0/1 interface**
- inbound on the R1 G0/1 interface
- outbound on the R2 S0/0/1 interface

Explanation: Because standard access lists only filter on the source IP address, they are commonly placed closest to the destination network. In this example, the source packets will be coming from the R2 G0/0 network. The destination is the R1 G0/1 network. The proper ACL placement is outbound on the R1 G0/1 interface.

29. Which is a characteristic of a Type 2 hypervisor?

- **does not require management console software**
- has direct access to server hardware resources
- best suited for enterprise environments
- installs directly on hardware

30. What are the two types of VPN connections? (Choose two.)

- PPPoE
- Frame Relay
- **site-to-site**
- **remote access**
- leased line

Explanation: PPPoE, leased lines, and Frame Relay are types of WAN technology, not types of VPN connections.

31. Refer to the exhibit. What three conclusions can be drawn from the displayed output? (Choose three.)

```
R3# show ip ospf interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.3/28, Area 0, Attached via Network Statement
  Process ID 10, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1          no          no            Base
  Transmit Delay is 1 sec, State DROTHER, Priority 0
  Designated Router (ID) 1.1.1.1, Interface address 192.168.1.1
  Backup Designated router (ID) 2.2.2.2, Interface address 192.168.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:01

<output omitted>
```


- **The DR can be reached through the GigabitEthernet 0/0 interface.**
- **There have been 9 seconds since the last hello packet sent.**
- This interface is using the default priority.
- **The router ID values were not the criteria used to select the DR and the BDR.**
- The router ID on the DR router is 3.3.3.3
- The BDR has three neighbors.

32. 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.

Explanation: 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.

33. What functionality does mGRE provide to the DMVPN technology?

- **It allows the creation of dynamically allocated tunnels through a permanent tunnel source at the hub and dynamically allocated tunnel destinations at the spokes.**
- It provides secure transport of private information over public networks, such as the Internet.
- It is a Cisco software solution for building multiple VPNs in an easy, dynamic, and scalable manner.
- It creates a distributed mapping database of public IP addresses for all VPN tunnel spokes.

Explanation: DMVPN is built on three protocols, NHRP, IPsec, and mGRE. NHRP is the distributed address mapping protocol for VPN tunnels. IPsec encrypts communications on VPN tunnels. The mGRE protocol allows the dynamic creation of multiple spoke tunnels from one permanent VPN hub.

34. What is used to pre-populate the adjacency table on Cisco devices that use CEF to process packets?

- the FIB
- the routing table
- **the ARP table**
- the DSP

35. What command would be used as part of configuring NAT or PAT to display information about NAT configuration parameters and the number of addresses in the pool?

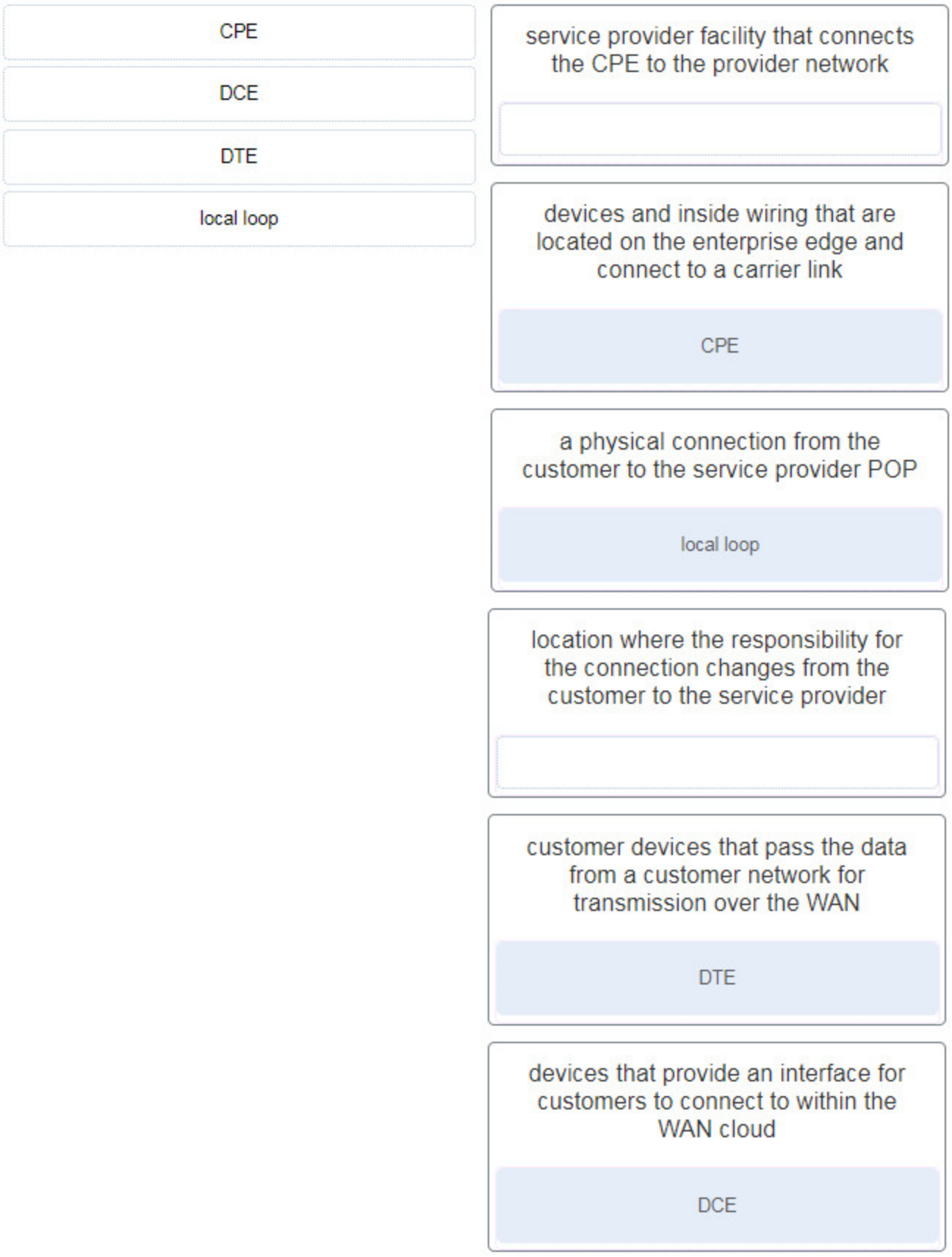
- show running-config
- **show ip nat statistics**
- show ip cache
- show version

36. What is a purpose of establishing a network baseline?

- It provides a statistical average for network performance.
- **It creates a point of reference for future network evaluations.**
- It manages the performance of network devices.
- It checks the security configuration of network devices.

Explanation: A baseline is used to establish normal network or system performance. It can be used to compare with future network or system performances in order to detect abnormal situations.

37. Match the type of WAN device or service to the description. (Not all options are used.)



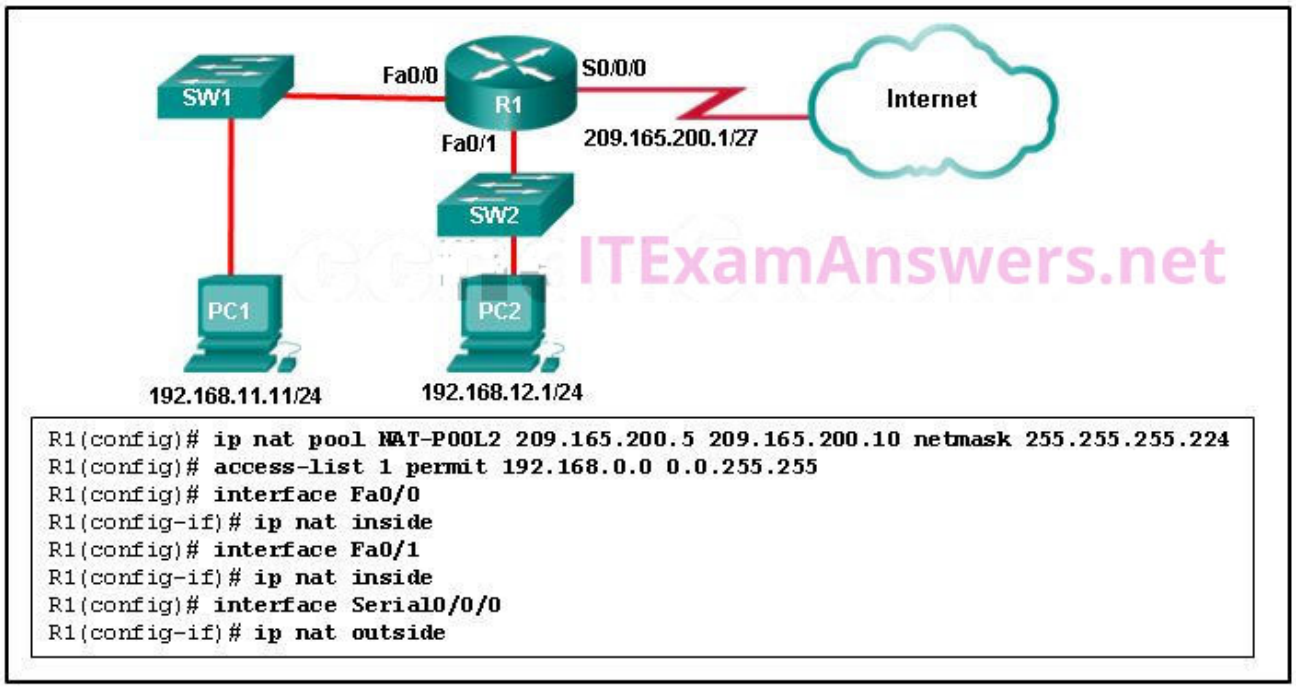
CPE —> devices and inside wiring that are located on the enterprise edge and connect to a carrier link
DCE —> devices that provide an interface for customers to connect to within the WAN cloud

DTE —> customer devices that pass the data from a customer network for transmission over the WAN
local loop —> a physical connection from the customer to the service provider POP

38. Which statement describes a characteristic of standard IPv4 ACLs?

- **They filter traffic based on source IP addresses only.**
- They can be created with a number but not with a name.
- They are configured in the interface configuration mode.
- They can be configured to filter traffic based on both source IP addresses and source ports.

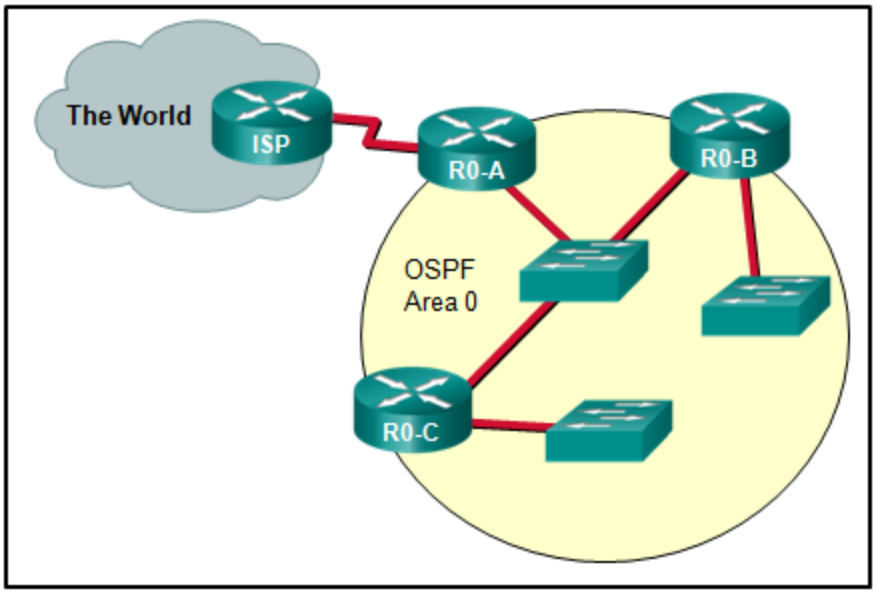
39. Refer to the exhibit. R1 is configured for NAT as displayed. What is wrong with the configuration?



- **NAT-POOL2 is not bound to ACL 1.**
- Interface Fa0/0 should be identified as an outside NAT interface.
- The NAT pool is incorrect.
- Access-list 1 is misconfigured.

Explanation: R1 has to have NAT-POOL2 bound to ACL 1. This is accomplished with the command R1(config)#ip nat inside source list 1 pool NAT-POOL2. This would enable the router to check for all interesting traffic and if it matches ACL 1 it would be translated by use of the addresses in NAT-POOL2.

40. Refer to the exhibit. What method can be used to enable an OSPF router to advertise a default route to neighboring OSPF routers?



- Use a static route pointing to the ISP and redistribute it.
- Use the redistribute static command on R0-A.
- Use the default-information originate command on ISP.
- **Use the default-information originate command on R0-A.**

41. A company has contracted with a network security firm to help identify the vulnerabilities of the corporate network. The firm sends a team to perform penetration tests to the company network. Why would the team use applications such as John the Ripper,THC Hydra, RainbowCrack, and Medusa?

- to capture and analyze packets within traditional Ethernet LANs or WLANs
- to probe and test the robustness of a firewall by using specially created forged packets
- **to make repeated guesses in order to crack a password**

42. What are two syntax rules for writing a JSON array? (Choose two.)

- **Each value in the array is separated by a comma.**
- The array can include only one value type.
- A space must separate each value in the array.
- A semicolon separates the key and list of values.
- **Values are enclosed in square brackets.**

43. What is a characteristic of a Trojan horse as it relates to network security?

- An electronic dictionary is used to obtain a password to be used to infiltrate a key network device.
- **Malware is contained in a seemingly legitimate executable program.**
- Extreme quantities of data are sent to a particular network device interface.

- Too much information is destined for a particular memory block, causing additional memory areas to be affecte

Explanation: A Trojan horse carries out malicious operations under the guise of a legitimate program. Denial of service attacks send extreme quantities of data to a particular host or network device interface. Password attacks use electronic dictionaries in an attempt to learn passwords. Buffer overflow attacks exploit memory buffers by sending too much information to a host to render the system inoperable.

44. An attacker is redirecting traffic to a false default gateway in an attempt to intercept the data traffic of a switched network. What type of attack could achieve this?

- TCP SYN flood
- DNS tunneling
- **DHCP spoofing**
- ARP cache poisoning

Explanation: In DHCP spoofing attacks, an attacker configures a fake DHCP server on the network to issue DHCP addresses to clients with the aim of forcing the clients to use a false default gateway, and other false services. DHCP snooping is a Cisco switch feature that can mitigate DHCP attacks. MAC address starvation and MAC address snooping are not recognized security attacks. MAC address spoofing is a network security threat.

45. A company is developing a security policy for secure communication. In the exchange of critical messages between a headquarters office and a branch office, a hash value should only be recalculated with a predetermined code, thus ensuring the validity of data source. Which aspect of secure communications is addressed?

- data integrity
- non-repudiation
- **origin authentication**
- data confidentiality

Explanation: Secure communications consists of four elements:
Data confidentiality – guarantees that only authorized users can read the message
Data integrity – guarantees that the message was not altered
Origin authentication – guarantees that the message is not a forgery and does actually come from whom it states
Data nonrepudiation – guarantees that the sender cannot repudiate, or refute, the validity of a message sent

46. A company has contracted with a network security firm to help identify the vulnerabilities of the corporate network. The firm sends a team to perform penetration tests to the company network. Why would the team use packet sniffers?

- to detect installed tools within files and directories that provide threat actors remote access and control over a computer or network
- to detect any evidence of a hack or malware in a computer or network
- to probe and test the robustness of a firewall by using specially created forged packets
- **to capture and analyze packets within traditional Ethernet LANs or WLANs**

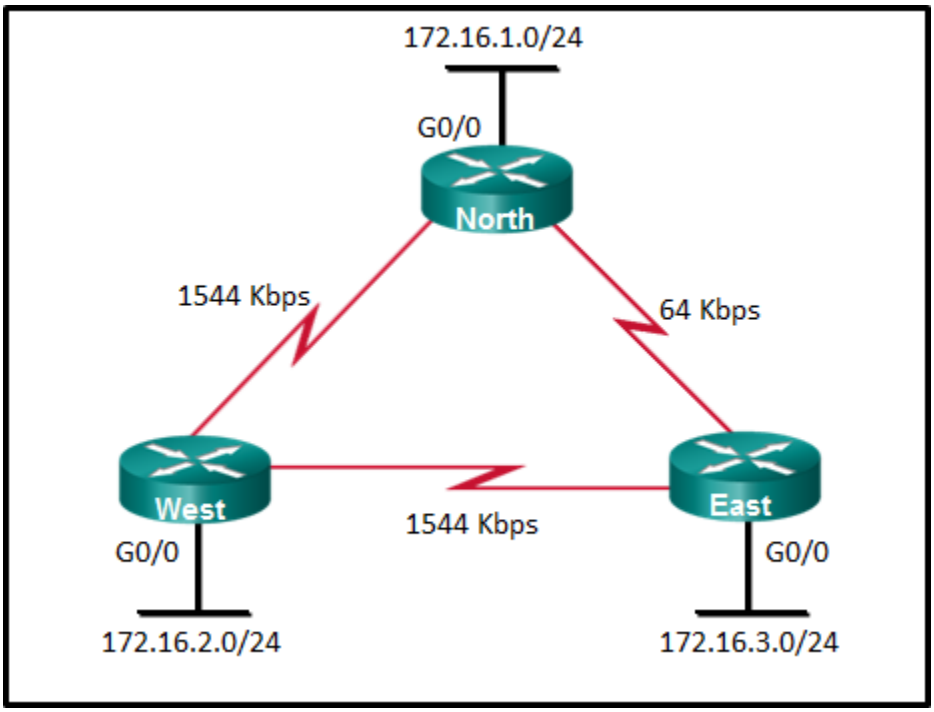
47. An administrator is configuring single-area OSPF on a router. One of the networks that must be advertised is 172.20.0.0 255.255.252.0. What wildcard mask would the administrator use in the OSPF network statement?

- 0.0.15.255
- **0.0.3.255**
- 0.0.7.255
- 0.0.1.255

48. Match the HTTP method with the RESTful operation.

POST –>> Create
GET –>> Read
PUT/PATCH –>> Update/Replace?Modify
Delete –>> Delete

49. Refer to the exhibit. What is the OSPF cost to reach the West LAN 172.16.2.0/24 from East?



- 782
- 74
- 128
- **65**

50. What is one reason to use the ip ospf priority command when the OSPF routing protocol is in use?

- to activate the OSPF neighboring process
- **to influence the DR/BDR election process**
- to provide a backdoor for connectivity during the convergence process
- to streamline and speed up the convergence process

Explanation: The OSPF priority can be set to a number between 0 and 255. The higher the number set, the more likely the router becomes the DR. A priority 0 stops a router from participating in the election process and the router does not become a DR or a BDR.

51. An ACL is applied inbound on a router interface. The ACL consists of a single entry:

```
access-list 210 permit tcp 172.18.20.0 0.0.0.31 172.18.20.32 0.0.0.31 eq ftp .
```

If a packet with a source address of 172.18.20.14, a destination address of 172.18.20.40, and a protocol of 21 is received on the interface, is the packet permitted or denied?

permitted

52. What is a characteristic of the two-tier spine-leaf topology of the Cisco ACI fabric architecture?

- The spine and leaf switches are always linked through core switches.
- The spine switches attach to the leaf switches and attach to each other for redundancy.
- The leaf switches always attach to the spines and they are interlinked through a trunk line.
- **The leaf switches always attach to the spines, but they never attach to each other.**

53. Which two scenarios would result in a duplex mismatch? (Choose two.)

- **connecting a device with autonegotiation to another that is manually set to full-duplex**
- starting and stopping a router interface during a normal operation
- connecting a device with an interface running at 100 Mbps to another with an interface running at 1000 Mbps
- configuring dynamic routing incorrectly
- **manually setting the two connected devices to different duplex modes**

54. A network technician is configuring SNMPv3 and has set a security level of auth . What is the effect of this setting?

- authenticates a packet by a string match of the username or community string
- **authenticates a packet by using either the HMAC with MD5 method or the SHA method**
- authenticates a packet by using either the HMAC MD5 or 3.HMAC SHA algorithms and encrypts the packet with either the DES, 3DES or AES algorithms
- authenticates a packet by using the SHA algorithm only

Explanation: For enabling SNMPv3 one of three security levels can be configured:
1) noAuth
2) auth
3) priv
The security level configured determines which security algorithms are performed on SNMP packets. The auth security level uses either HMAC with MD5 or SHA.

55. What are two types of attacks used on DNS open resolvers? (Choose two.)

- **amplification and reflection**
- **resource utilization**
- fast flux
- ARP poisoning
- cushioning

Explanation: Three types of attacks used on DNS open resolvers are as follows:DNS cache poisoning – attacker sends spoofed falsified information to redirect users from legitimate sites to malicious sites
DNS amplification and reflection attacks – attacker sends an increased volume of attacks to mask the true source of the attack
DNS resource utilization attacks – a denial of service (DoS) attack that consumes server resources

56. An ACL is applied inbound on a router interface. The ACL consists of a single entry:

```
access-list 101 permit udp 192.168.100.0 0.0.2.255 64.100.40.0 0.0.0.15 eq telnet .
```

If a packet with a source address of 192.168.101.45, a destination address of 64.100.40.4, and a protocol of 23 is received on the interface, is the packet permitted or denied?

- **denied**
- permitted

Case 2:

```
access-list 101 permit udp 192.168.100.0 0.0.2.255 64.100.40.0 0.0.0.0.15 eq telnet .
```

If a packet with a source address of 192.168.100.219, a destination address of 64.100.40.10, and a protocol of 54 is received on the interface, is the packet permitted or denied?

- **denied**
- permitted

57. Which type of resources are required for a Type 1 hypervisor?

- a dedicated VLAN
- **a management console**
- a host operating system

58. In JSON, what is held within square brackets [ ]?

- nested values
- key/value pairs
- an object
- **an array**

59. What are three components used in the query portion of a typical RESTful API request? (Choose three.)

- resources
- protocol
- API server
- **format**
- **key**
- **parameters**

60. A user reports that when the corporate web page URL is entered on a web browser, an error message indicates that the page cannot be displayed. The help-desk technician asks the user to enter the IP address of the web server to see if the page can be displayed. Which troubleshooting method is being used by the technician?

- top-down
- bottom-up
- **divide-and-conquer**
- substitution

61. Which protocol provides authentication, integrity, and confidentiality services and is a type of VPN?

- MD5
- AES
- **IPsec**
- ESP

62. Which statement describes a characteristic of Cisco Catalyst 2960 switches?

- They are best used as distribution layer switches.
- **New Cisco Catalyst 2960-C switches support PoE pass-through.**
- They are modular switches.
- They do not support an active switched virtual interface (SVI) with IOS versions prior to 15.x.

63. Which component of the ACI architecture translates application policies into network programming?

- the hypervisor
- **the Application Policy Infrastructure Controller**
- the Nexus 9000 switch
- the Application Network Profile endpoints

64. Which two pieces of information should be included in a logical topology diagram of a network? (Choose two.)

- device type
- cable specification
- **interface identifier**
- OS/IOS version
- **connection type**
- cable type and identifier

Explanation: The interface identifier and connection type should be included in a logical topology diagram because they indicate which interface is connected to other devices in the network with a specific type such as LAN, WAN, point-to-point, etc. The OS/IOS version, device type, cable type and identifier, and cable specification are typically included in a physical topology diagram.

65. Refer to the exhibit. A PC at address 10.1.1.45 is unable to access the Internet. What is the most likely cause of the problem?

```
R1# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 2 extended)
Peak translations: 33, occurred 00:00:46 ago
Outside interfaces:
  FastEthernet0/1
Inside interfaces:
  FastEthernet0/0
Hits: 42  Misses: 0
CEF Translated packets: 42, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool NATPOOL refcount 4
 pool NATPOOL: netmask 255.255.255.224
        start 209.165.201.10 end 209.165.201.11
        type generic, total addresses 2, allocated 2 (100%), misses 0

R1# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.201.10:6  10.1.1.33:6        209.165.200.226:6  209.165.200.226:6
--- 209.165.201.10     10.1.1.33          ---                ---
icmp 209.165.201.11:3  10.1.1.123:3       209.165.200.226:3  209.165.200.226:3
--- 209.165.201.11     10.1.1.123         ---                ---
```

- **The NAT pool has been exhausted.**
- The wrong netmask was used on the NAT pool.
- Access-list 1 has not been configured properly.
- The inside and outside interfaces have been configured backwards.

Explanation: The output of show ip nat statistics shows that there are 2 total addresses and that 2 addresses have been allocated (100%). This indicates that the NAT pool is out of global addresses to give new clients. Based on the show ip nat translations, PCs at 10.1.1.33 and

10.1.1.123 have used the two available addresses to send ICMP messages to a host on the outside network.

66. What are two benefits of using SNMP traps? (Choose two.)

- **They eliminate the need for some periodic polling requests.**
- **They reduce the load on network and agent resources.**
- They limit access for management systems only.
- They can provide statistics on TCP/IP packets that flow through Cisco devices.
- They can passively listen for exported NetFlow datagrams.

67. Which statement accurately describes a characteristic of IPsec?

- IPsec works at the application layer and protects all application data.
- IPsec is a framework of standards developed by Cisco that relies on OSI algorithms.
- IPsec is a framework of proprietary standards that depend on Cisco specific algorithms.
- IPsec works at the transport layer and protects data at the network layer.
- **IPsec is a framework of open standards that relies on existing algorithms.**

Explanation: IPsec can secure a path between two network devices. IPsec can provide the following security functions:
Confidentiality – IPsec ensures confidentiality by using encryption.
Integrity – IPsec ensures that data arrives unchanged at the destination using a hash algorithm, such as MD5 or SHA.
Authentication – IPsec uses Internet Key Exchange (IKE) to authenticate users and devices that can carry out communication independently. IKE uses several types of authentication, including username and password, one-time password, biometrics, pre-shared keys (PSKs), and digital certificates.
Secure key exchange- IPsec uses the Diffie-Hellman (DH) algorithm to provide a public key exchange method for two peers to establish a shared secret key.

68. In a large enterprise network, which two functions are performed by routers at the distribution layer? (Choose two.)

- connect users to the network
- provide a high-speed network backbone
- **connect remote networks**
- provide Power over Ethernet to devices
- **provide data traffic security**

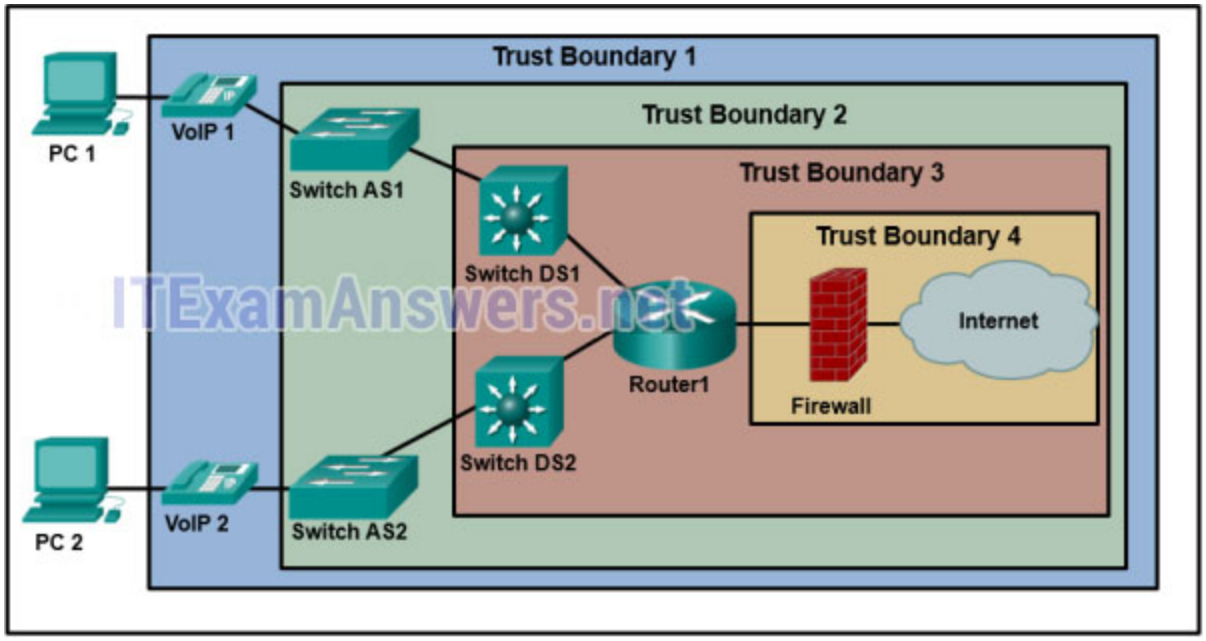
69. Which two statements describe the use of asymmetric algorithms? (Choose two.)

- Public and private keys may be used interchangeably.

- If a public key is used to encrypt the data, a public key must be used to decrypt the data.
- **If a private key is used to encrypt the data, a public key must be used to decrypt the data.**
- **If a public key is used to encrypt the data, a private key must be used to decrypt the data.**
- If a private key is used to encrypt the data, a private key must be used to decrypt the data.

Explanation: Asymmetric algorithms use two keys: a public key and a private key. Both keys are capable of the encryption process, but the complementary matched key is required for decryption. If a public key encrypts the data, the matching private key decrypts the data. The opposite is also true. If a private key encrypts the data, the corresponding public key decrypts the data.

70. Refer to the exhibit. A network administrator has deployed QoS and has configured the network to mark traffic on the VoIP phones as well as the Layer 2 and Layer 3 switches. Where should initial marking occur to establish the trust boundary?



- Trust Boundary 4
- Trust Boundary 3
- **Trust Boundary 1**
- Trust Boundary 2

Explanation: Traffic should be classified and marked as close to its source as possible. The trust boundary identifies at which device marked traffic should be trusted. Traffic marked on VoIP phones would be considered trusted as it moves into the enterprise network.

71. What are two benefits of extending access layer connectivity to users through a wireless medium? (Choose two.)

- **reduced costs**
- decreased number of critical points of failure
- **increased flexibility**
- increased bandwidth availability
- increased network management options

72. What are two purposes of launching a reconnaissance attack on a network? (Choose two.)

- **to scan for accessibility**
- to retrieve and modify data
- **to gather information about the network and devices**
- to prevent other users from accessing the system
- to escalate access privileges

73. A group of users on the same network are all complaining about their computers running slowly. After investigating, the technician determines that these computers are part of a zombie network. Which type of malware is used to control these computers?

- **botnet**
- spyware
- virus
- rootkit

74. An ACL is applied inbound on a router interface. The ACL consists of a single entry:

```
access-list 101 permit tcp 10.1.1.0 0.0.0.255 host 192.31.7.45 eq dns .
```

If a packet with a source address of 10.1.1.201, a destination address of 192.31.7.45, and a protocol of 23 is received on the interface, is the packet permitted or denied?

- permitted
- **denied**

75. Refer to the exhibit. From which location did this router load the IOS?

```
Router# show version
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1,
 RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

System returned to ROM by power-on
System image file is "flash:c1841-advipservicesk9-mz.124-15.T1.bin"

<output omitted>

Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947Z18E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102

Router#
```

- **flash memory**
- NVRAM?
- RAM
- ROM
- a TFTP server?

76. Refer to the exhibit. Which data format is used to represent the data for network automation applications?

- XML
- YAML
- HTML
- **JSON**

```
{
"message": "success",
"username": "jsmith01",
"user_info": {
"First_name": "John",
"Last_name": "Smith"
   }
}
```

Explanation: The common data formats that are used in many applications including network automation and programmability are as follows:

- **JavaScript Object Notation (JSON)** – In JSON, the data known as an object is one or more key/value pairs enclosed in braces { }. Keys must be strings within double quotation marks ” “. Keys and values are separated by a colon.
- **eXtensible Markup Language (XML)** – In XML, the data is enclosed within a related set of tags <tag>data</tag>.

- **YAML Ain't Markup Language (YAML)** – In YAML, the data known as an object is one or more key value pairs. Key value pairs are separated by a colon without the use of quotation marks. YAML uses indentation to define its structure, without the use of brackets or commas.

77. What QoS step must occur before packets can be marked?

- **classifying**
- shaping
- queuing
- policing

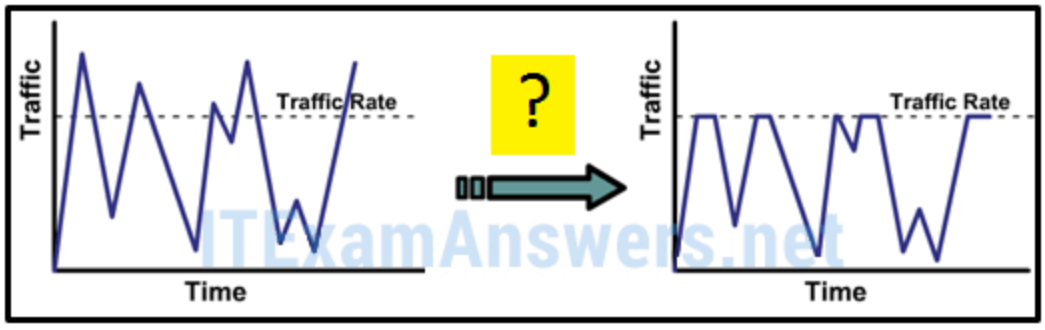
78. What is the main function of a hypervisor?

- **It is used to create and manage multiple VM instances on a host machine.**
- It is a device that filters and checks security credentials.
- It is a device that synchronizes a group of sensors.
- It is software used to coordinate and prepare data for analysis.
- It is used by ISPs to monitor cloud computing resources.

79. A company needs to interconnect several branch offices across a metropolitan area. The network engineer is seeking a solution that provides high-speed converged traffic, including voice, video, and data on the same network infrastructure. The company also wants easy integration to their existing LAN infrastructure in their office locations. Which technology should be recommended?

- Frame Relay
- **Ethernet WAN**
- VSAT
- ISDN

80. Refer to the exhibit. As traffic is forwarded out an egress interface with QoS treatment, which congestion avoidance technique is used?



- traffic shaping

- weighted random early detection
- classification and marking
- **traffic policing**

Explanation: Traffic shaping buffers excess packets in a queue and then forwards the traffic over increments of time, which creates a smoothed packet output rate. Traffic policing drops traffic when the amount of traffic reaches a configured maximum rate, which creates an output rate that appears as a saw-tooth with crests and troughs.

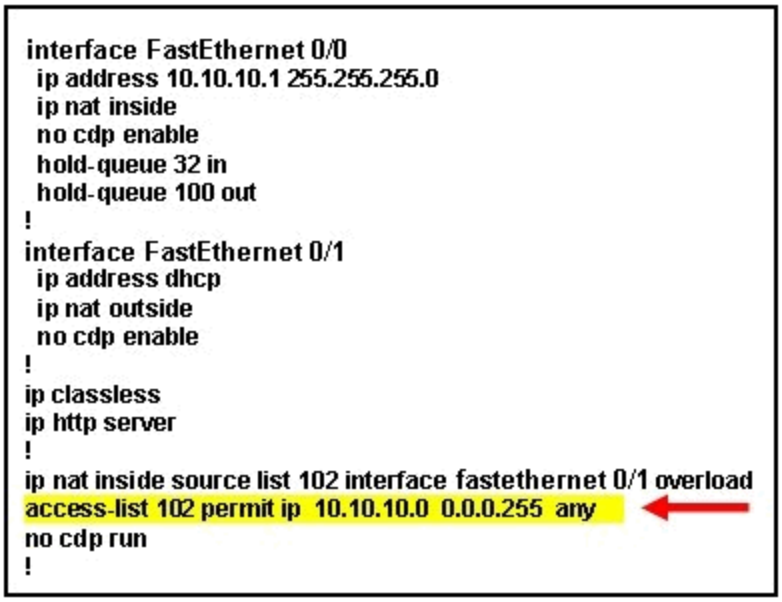
81. An ACL is applied inbound on a router interface. The ACL consists of a single entry:

```
access-list 101 permit tcp 10.1.1.0 0.0.0.255 host 10.1.3.8 eq dns .
```

If a packet with a source address of 10.1.3.8, a destination address of 10.10.3.8, and a protocol of 53 is received on the interface, is the packet permitted or denied?

- **denied**
- permitted

82. Refer to the exhibit. What is the purpose of the command marked with an arrow shown in the partial configuration output of a Cisco broadband router?



- defines which addresses are allowed into the router
- **defines which addresses can be translated**
- defines which addresses are assigned to a NAT pool
- defines which addresses are allowed out of the router

83. If a router has two interfaces and is routing both IPv4 and IPv6 traffic, how many ACLs could be created and applied to it?

- 12
- 4
- **8**
- 16
- 6

84. Refer to the exhibit. An administrator first configured an extended ACL as shown by the output of the show access-lists command. The administrator then edited this access-list by issuing the commands below.

```
Router(config)# ip access-list extended 101
Router(config-ext-nacl)# no 20
Router(config-ext-nacl)# 5 permit tcp any any eq
22
Router(config-ext-nacl)# 20 deny udp any any
```

```
Router# show access-lists
Extended IP access list 101
    10 deny tcp any any
    20 permit udp any any
    30 permit icmp any any
```

Which two conclusions can be drawn from this new configuration? (Choose two.)

- TFTP packets will be permitted.
- **Ping packets will be permitted.**
- Telnet packets will be permitted.
- **SSH packets will be permitted.**
- All TCP and UDP packets will be denied.

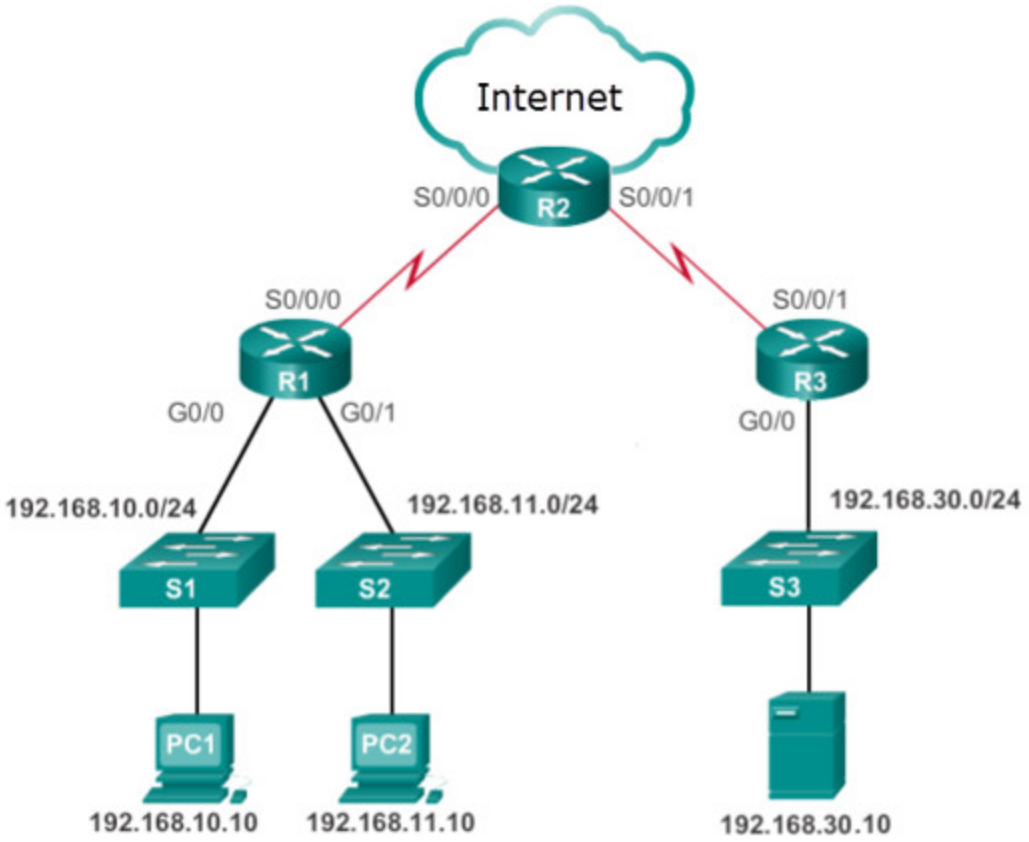
Explanation: After the editing, the final configuration is as follows:
Router# **show access-lists**
Extended IP access list 101
5 permit tcp any any eq ssh
10 deny tcp any any
20 deny udp any any
30 permit icmp any any
So, only SSH packets and ICMP packets will be permitted.

85. Which troubleshooting approach is more appropriate for a seasoned network administrator rather than a less-experienced network administrator?

- **a less-structured approach based on an educated guess**
- an approach comparing working and nonworking components to spot significant differences
- a structured approach starting with the physical layer and moving up through the layers of the OSI model until the cause of the problem is identified

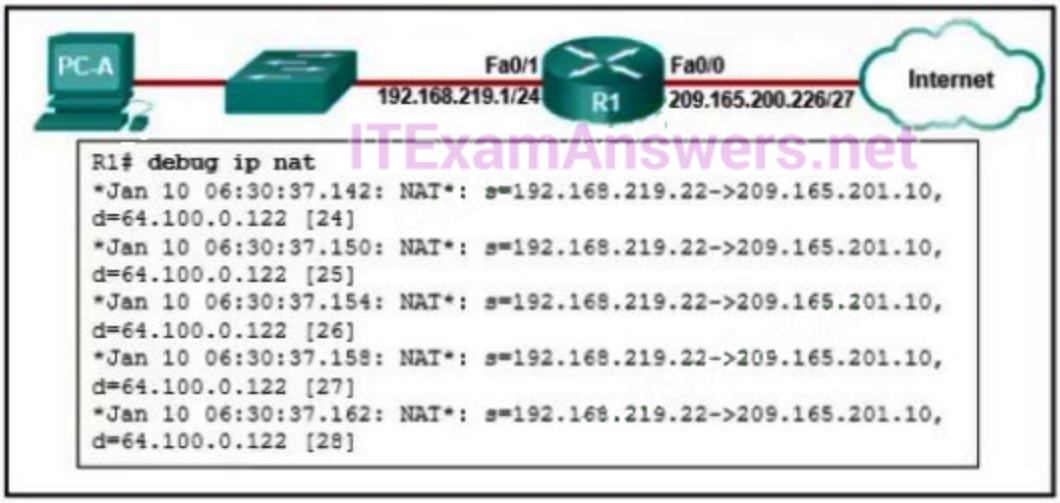
- an approach that starts with the end-user applications and moves down through the layers of the OSI model until the cause of the problem has been identified

86. Refer to the exhibit. Many employees are wasting company time accessing social media on their work computers. The company wants to stop this access. What is the best ACL type and placement to use in this situation?



- extended ACL outbound on R2 WAN interface towards the internet
- standard ACL outbound on R2 WAN interface towards the internet
- standard ACL outbound on R2 S0/0/0
- **extended ACLs inbound on R1 G0/0 and G0/1**

87. Refer to the exhibit. An administrator is trying to configure PAT on R1, but PC-A is unable to access the Internet. The administrator tries to ping a server on the Internet from PC-A and collects the debugs that are shown in the exhibit. Based on this output, what is most likely the cause of the problem?



- The inside and outside NAT interlaces have been configured backwards
- **The inside global address is not on the same subnet as the ISP**
- The address on Fa0/0 should be 64.100.0.1.
- The NAT source access list matches the wrong address range.

Explanation: The output of debug ip nat shows each packet that is translated by the router. The "s" is the source IP address of the packet and the "d" is the destination. The address after the arrow ("->") shows the translated address. In this case, the translated address is on the 209.165.201.0 subnet but the ISP facing interface is in the 209.165.200.224/27 subnet. The ISP may drop the incoming packets, or might be unable to route the return packets back to the host because the address is in an unknown subnet.

88. Why is QoS an important issue in a converged network that combines voice, video, and data communications?

- Data communications must be given the first priority.
- **Voice and video communications are more sensitive to latency.**
- Legacy equipment is unable to transmit voice and video without QoS.
- Data communications are sensitive to jitter.

89. Which statement describes a VPN?

- VPNs use logical connections to create public networks through the Internet.
- VPNs use open source virtualization software to create the tunnel through the Internet.
- VPNs use dedicated physical connections to transfer data between remote users.
- **VPNs use virtual connections to create a private network through a public network.**

Explanation: A VPN is a private network that is created over a public network. Instead of using dedicated physical connections, a VPN uses virtual connections routed through a public network between two network devices.

90. In which OSPF state is the DR/BDR election conducted?

- ExStart
- Init
- **Two-Way**
- Exchange

91. Two corporations have just completed a merger. The network engineer has been asked to connect the two corporate networks without the expense of leased lines. Which solution would be the most cost effective method of providing a proper and secure connection between the two corporate networks?

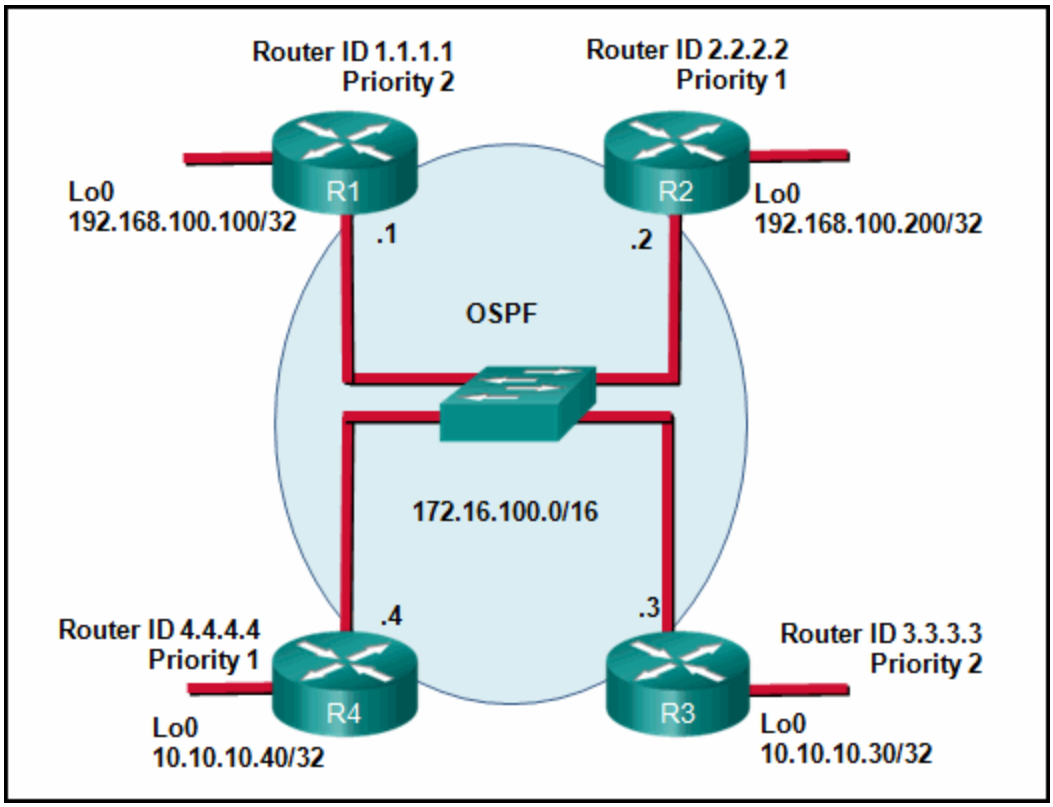
- Cisco Secure Mobility Clientless SSL VPN
- Frame Relay
- remote access VPN using IPsec
- Cisco AnyConnect Secure Mobility Client with SSL
- **site-to-site VPN**

Explanation: The site-to-site VPN is an extension of a classic WAN network that provides a static interconnection of entire networks. Frame Relay would be a better choice than leased lines, but would be more expensive than implementing site-to-site VPNs. The other options refer to remote access VPNs which are better suited for connecting users to the corporate network versus interconnecting two or more networks.

92. What is the final operational state that will form between an OSPF DR and a DROTHER once the routers reach convergence?

- loading
- established
- **full**
- two-way

93. Refer to the exhibit. If the switch reboots and all routers have to re-establish OSPF adjacencies, which routers will become the new DR and BDR?



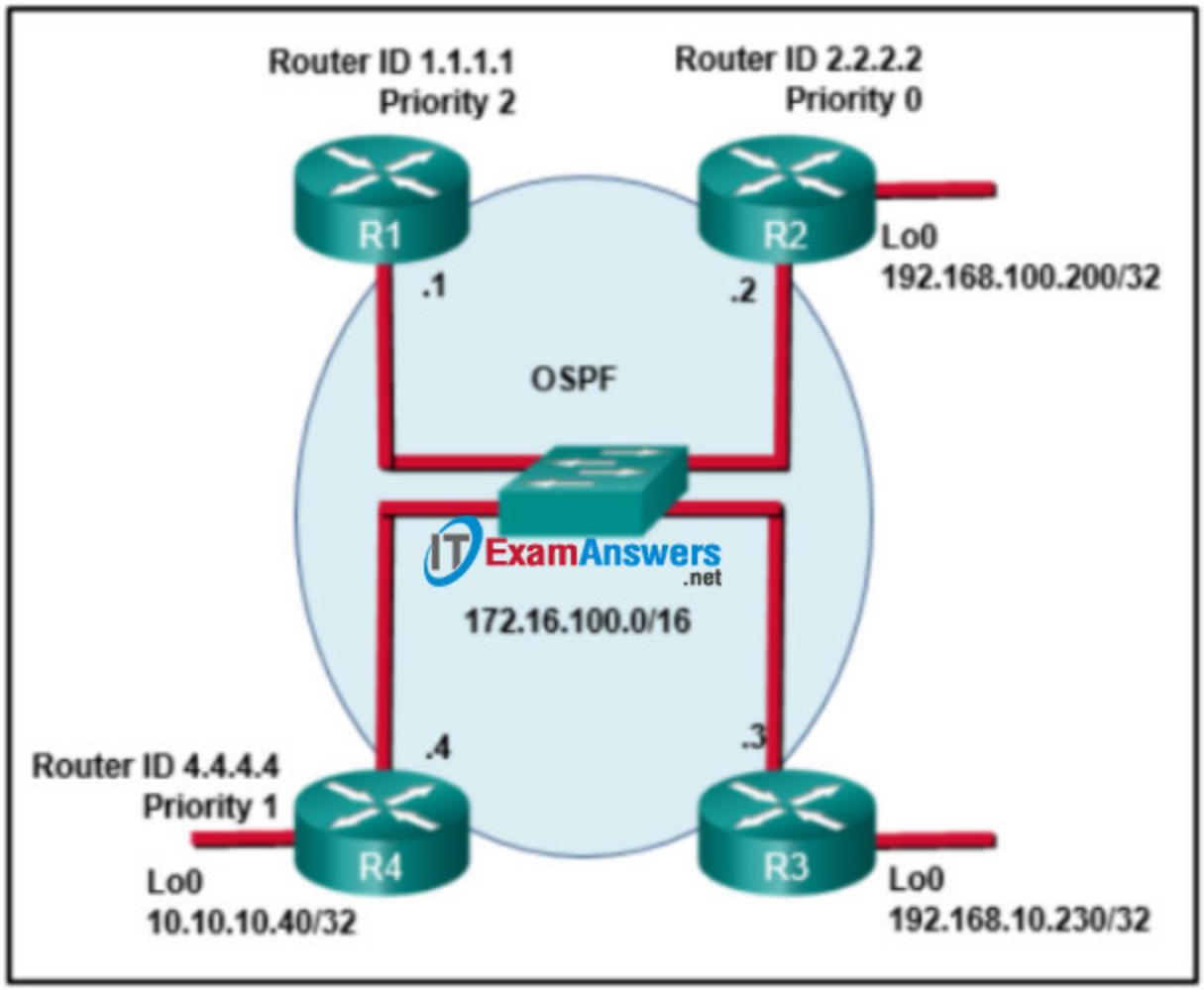
- **Router R3 will become the DR and router R1 will become the BDR.**
- Router R4 will become the DR and router R3 will become the BDR.
- Router R1 will become the DR and router R2 will become the BDR.
- Router R3 will become the DR and router R2 will become the BDR.

Explanation: OSPF elections of a DR are based on the following in order of precedence:

- highest pritority from 1 -255 (0 = never a DR)
- highest router ID
- highest IP address of a loopback or active interface in the absence of a manually configured router ID. Loopback IP addresses take higher precedence than other interfaces.

In this case routers R3 and R1 have the highest router priority. Between the two, R3 has the higher router ID. Therefore, R3 will become the DR and R1 will become the BDR.

Case 2:



Enterprise Networking, Security, and Automation (Version 7.00) – ENSA Final Exam

- Router R2 will become the DR and router R4 will become the BDR.
- **Router R1 will become the DR and router R3 will become the BDR.**
- Router R4 will become the DR and router R3 will become the BDR.
- Router R3 will become the DR and router R2 will become the BDR.

94. Which type of server would be used to keep a historical record of messages from monitored network devices?

- DNS
- print
- DHCP
- **syslog**
- authentication

95. When QoS is implemented in a converged network, which two factors can be controlled to improve network performance for real-time traffic? (Choose two.)

- packet addressing

- **delay**
- **jitter**
- packet routing
- link speed

Explanation: Delay is the latency between a sending and receiving device. Jitter is the variation in the delay of the received packets. Both delay and jitter need to be controlled in order to support real-time voice and video traffic.

96. In which step of gathering symptoms does the network engineer determine if the problem is at the core, distribution, or access layer of the network?

- Determine ownership.
- Determine the symptoms.
- **Narrow the scope.**
- Document the symptoms.
- Gather information.

97. What protocol sends periodic advertisements between connected Cisco devices in order to learn device name, IOS version, and the number and type of interfaces?

- **CDP**
- SNMP
- NTP
- LLDP

98. An administrator is configuring single-area OSPF on a router. One of the networks that must be advertised is 192.168.0.0 255.255.252.0. What wildcard mask would the administrator use in the OSPF network statement?

- 0.0.0.127
- 0.0.0.31
- **0.0.3.255**
- 0.0.0.63

99. Refer to the exhibit. An administrator configures the following ACL in order to prevent devices on the 192.168.1.0 subnet from accessing the server at 10.1.1.5:

```
access-list 100 deny ip 192.168.1.0 0.0.0.255 host 10.1.1.5
access-list 100 permit ip any any
```

Where should the administrator place this ACL for the most efficient use of network resources?

- **inbound on router A Fa0/0**
- outbound on router B Fa0/0
- outbound on router A Fa0/1
- inbound on router B Fa0/1

100. Which type of OSPFv2 packet is used to forward OSPF link change information?

- link-state acknowledgment
- **link-state update**
- hello
- database description

101. What protocol synchronizes with a private master clock or with a publicly available server on the internet?

- MPLS
- CBWFQ
- TFTP
- **NTP**

102. Which type of VPN allows multicast and broadcast traffic over a secure site-to-site VPN?

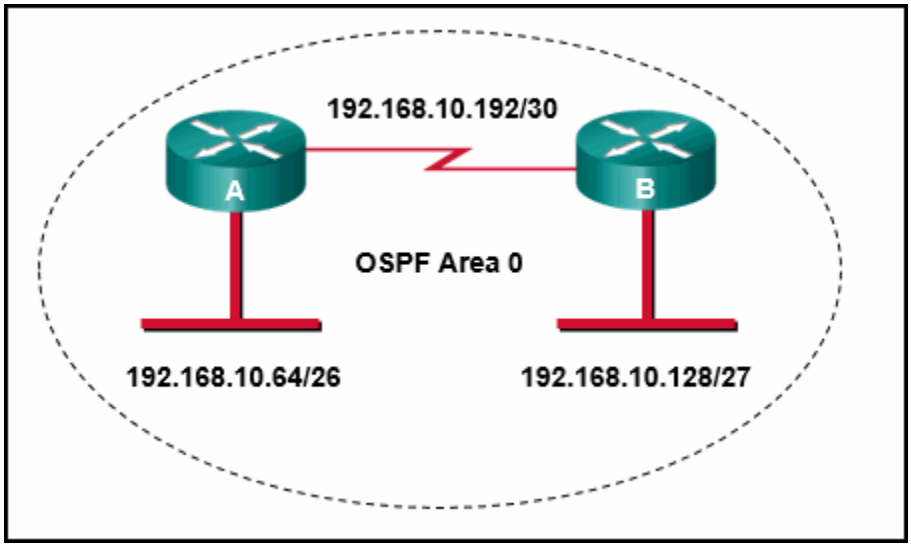
- dynamic multipoint VPN
- SSL VPN
- IPsec virtual tunnel interface

- **GRE over IPsec**

103. An OSPF router has three directly connected networks; 10.0.0.0/16, 10.1.0.0/16, and 10.2.0.0/16. Which OSPF network command would advertise only the 10.1.0.0 network to neighbors?

- **router(config-router)# network 10.1.0.0 0.0.255.255 area 0**
- router(config-router)# network 10.1.0.0 0.0.15.255 area 0
- router(config-router)# network 10.1.0.0 255.255.255.0 area 0
- router(config-router)# network 10.1.0.0 0.0.0.0 area 0

104. Refer to the exhibit. Which sequence of commands should be used to configure router A for OSPF?



i386046n1v2.gif

router ospf 1
network 192.168.10.0 area 0

router ospf 1
network 192.168.10.0

router ospf 1
network 192.168.10.64 255.255.255.192
network 192.168.10.192 255.255.255.252

router ospf 1
network 192.168.10.64 0.0.0.63 area 0
network 192.168.10.192 0.0.0.3 area 0

105. An administrator is configuring single-area OSPF on a router. One of the networks that must be advertised is 192.168.0.0 255.255.254.0. What wildcard mask would the administrator use in the OSPF network statement?

- 0.0.7.255
- **0.0.1.255**
- 0.0.3.255
- 0.0.15.255

106. How does virtualization help with disaster recovery within a data center?

- improvement of business practices
- supply of consistent air flow
- **support of live migration**
- guarantee of power

Explanation: Live migration allows moving of one virtual server to another virtual server that could be in a different location that is some distance from the original data center.

Case 2:

- Less energy is consumed.
- Server provisioning is faster.
- **Hardware at the recovery site does not have to be identical to production equipment.**
- Power is always provided.

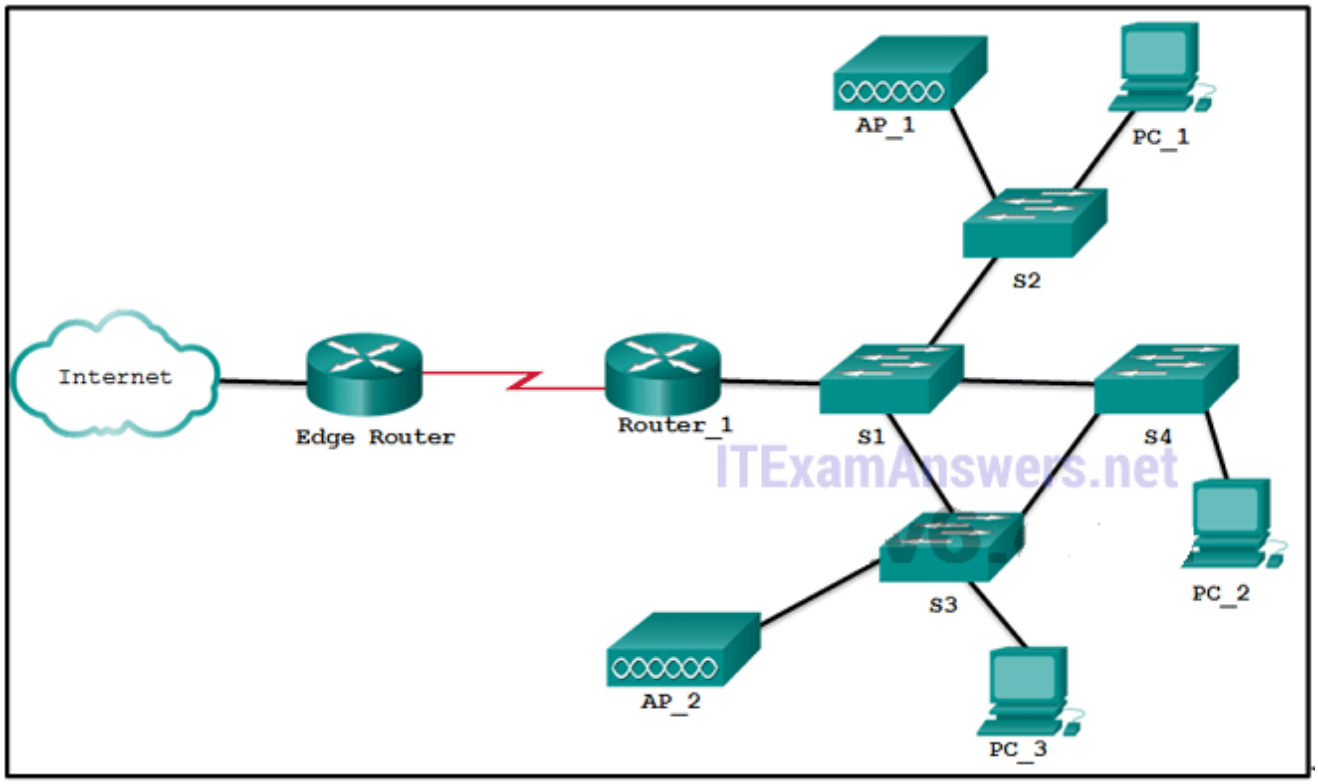
Explanation: Improved disaster recovery – Virtualization offers advanced business continuity solutions. It provides hardware abstraction capability so that the recovery site no longer needs to have hardware that is identical to the hardware in the production environment. Most enterprise server virtualization platforms also have software that can help test and automate the failover before a disaster does happen.

107. How does virtualization help with disaster recovery within a data center?

- **Hardware does not have to be identical.**
- **(Other case) Hardware at the recovery site does not have to be identical to production equipment.**
- Power is always provided.
- Less energy is consumed.
- Server provisioning is faster.

Explanation: Disaster recovery is how a company goes about accessing applications, data, and the hardware that might be affected during a disaster. Virtualization provides hardware independence which means the disaster recovery site does not have to have the exact equipment as the equipment in production. Server provisioning is relevant when a server is built for the first time. Although data centers do have backup generators, the entire data center is designed for disaster recovery. One particular data center could never guarantee that the data center itself would never be without power.

108. Refer to the exhibit. Which devices exist in the failure domain when switch S3 loses power?



- S4 and PC_2
- **PC_3 and AP_2**
- AP_2 and AP_1
- PC_3 and PC_2
- S1 and S4

A failure domain is the area of a network that is impacted when a critical device such as switch S3 has a failure or experiences problems.

109. 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

110. Refer to the exhibit. A network administrator needs to add an ACE to the TRAFFIC-CONTROL ACL that will deny IP traffic from the subnet 172.23.16.0/20. Which ACE will meet this requirement?

```
Router1# show access-lists
standard IP access list TRAFFIC-CONTROL
    10 permit 172.23.0.0, wildcard bits 0.0.255.255
    20 deny any
```

- **5 deny 172.23.16.0 0.0.15.255**
- 5 deny 172.23.16.0 0.0.255.255
- 15 deny 172.23.16.0 0.0.15.255
- 30 deny 172.23.16.0 0.0.15.255

111. Which step in the link-state routing process is described by a router building a link-state database based on received LSAs?

- executing the SPF algorithm
- **building the topology table**
- selecting the router ID
- declaring a neighbor to be inaccessible

112. What protocol uses agents, that reside on managed devices, to collect and store information about the device and its operation?

- SYSLOG
- TFTP
- CBWFQ
- **SNMP**

113. An administrator is configuring single-area OSPF on a router. One of the networks that must be advertised is 10.27.27.0 255.255.255.0. What wildcard mask would the administrator use in the OSPF network statement?

- 0.0.0.63
- **0.0.0.255**
- 0.0.0.31
- 0.0.0.15

114. When will an OSPF-enabled router transition from the Down state to the Init state?

- when an OSPF-enabled interface becomes active
- as soon as the router starts
- **when the router receives a hello packet from a neighbor router**
- as soon as the DR/BDR election process is complete

115. What type of traffic is described as having a high volume of data per packet?

- data
- **video**
- voice

116. What protocol is a vendor-neutral Layer 2 protocol that advertises the identity and capabilities of the host device to other connected network devices?

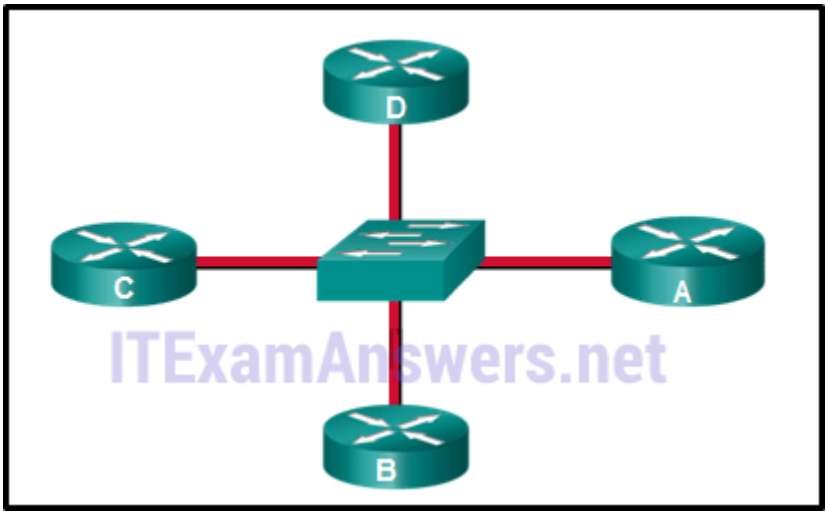
- **LLDP**
- NTP
- TFTP
- SNMP

117. Which step in the link-state routing process is described by a router running an algorithm to determine the best path to each destination?

- building the topology table
- selecting the router ID
- declaring a neighbor to be inaccessible

- **executing the SPF algorithm**

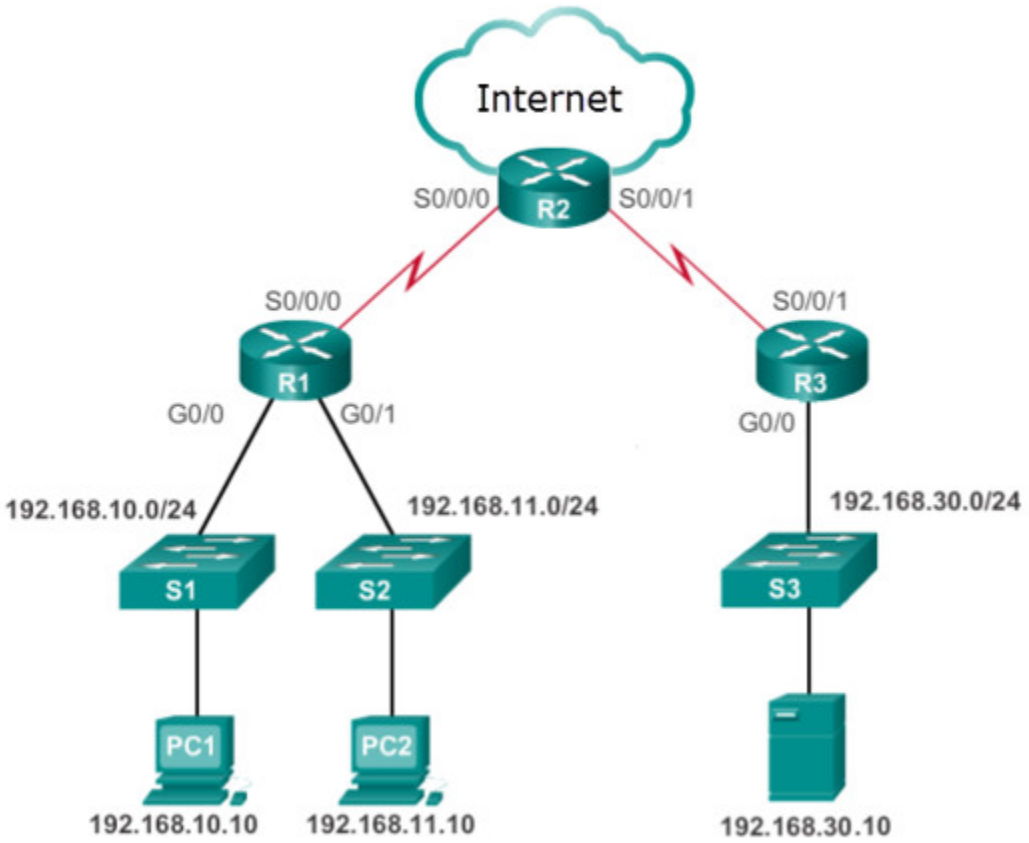
118. Refer to the exhibit. Which conclusion can be drawn from this OSPF multiaccess network?



- If the DR stops producing Hello packets, a BDR will be elected, and then it promotes itself to assume the role of DR.
- **With an election of the DR, the number of adjacencies is reduced from 6 to 3.**
- When a DR is elected all other non-DR routers become DROTHER.
- All DROTHER routers will send LSAs to the DR and BDR to multicast 224.0.0.5.

On OSPF multiaccess networks, a DR is elected to be the collection and distribution point for LSAs sent and received. A BDR is also elected in case the DR fails. All other non-DR or BDR routers become DROTHER. Instead of flooding LSAs to all routers in the network, DROTHERs only send their LSAs to the DR and BDR using the multicast address 224.0.0.6. If there is no DR/BDR election, the number of required adjacencies is n(n-1)/2 = > 4(4-1)/2 = 6. With the election, this number is reduced to 3.

119. Refer to the exhibit. The network administrator has an IP address of 192.168.11.10 and needs access to manage R1. What is the best ACL type and placement to use in this situation?



- extended ACL outbound on R2 WAN interface towards the internet
- **standard ACL inbound on R1 vty lines**
- extended ACLs inbound on R1 G0/0 and G0/1
- extended ACL outbound on R2 S0/0/1

Explanation: Standard ACLs permit or deny packets based only on the source IPv4 address. Because all traffic types are permitted or denied, standard ACLs should be located as close to the destination as possible.

Extended ACLs permit or deny packets based on the source IPv4 address and destination IPv4 address, protocol type, source and destination TCP or UDP ports and more. Because the filtering of extended ACLs is so specific, extended ACLs should be located as close as possible to the source of the traffic to be filtered. Undesirable traffic is denied close to the source network without crossing the network infrastructure.

120. Which type of VPN connects using the Transport Layer Security (TLS) feature?

- **SSL VPN**
- IPsec virtual tunnel interface
- GRE over IPsec
- dynamic multipoint VPN

121. Which group of APIs are used by an SDN controller to communicate with various applications?

- eastbound APIs
- westbound APIs
- **northbound APIs**
- southbound APIs

122. A company has consolidated a number of servers and it is looking for a program or firmware to create and control virtual machines which have access to all the hardware of the consolidated servers. What service or technology would support this requirement?

- Cisco ACI
- software defined networking
- **Type-1 hypervisor**
- APIC-EM

123. What command would be used as part of configuring NAT or PAT to identify inside local addresses that are to be translated?

- ip nat inside source list 24 interface serial 0/1/0 overload
- ip nat inside source list 14 pool POOL-STAT overload
- **access-list 10 permit 172.19.89.0 0.0.0.255**
- ip nat inside source list ACCTNG pool POOL-STAT

124. Anycompany has decided to reduce its environmental footprint by reducing energy costs, moving to a smaller facility, and promoting telecommuting, what service or technology would support requirement?

- **-Cloud services**
- Data center
- APIC-EM
- Cisco ACI

125. Refer to the exhibit. An administrator is trying to back up the current running configuration of the router to a USB drive, and enters the command `copy usbflash0:/R1-config running-config` on the router command line. After removing the USB drive and connecting it to a PC, the administrator discovers that the running configuration was not properly backed up to the R1-config file. What is the problem?

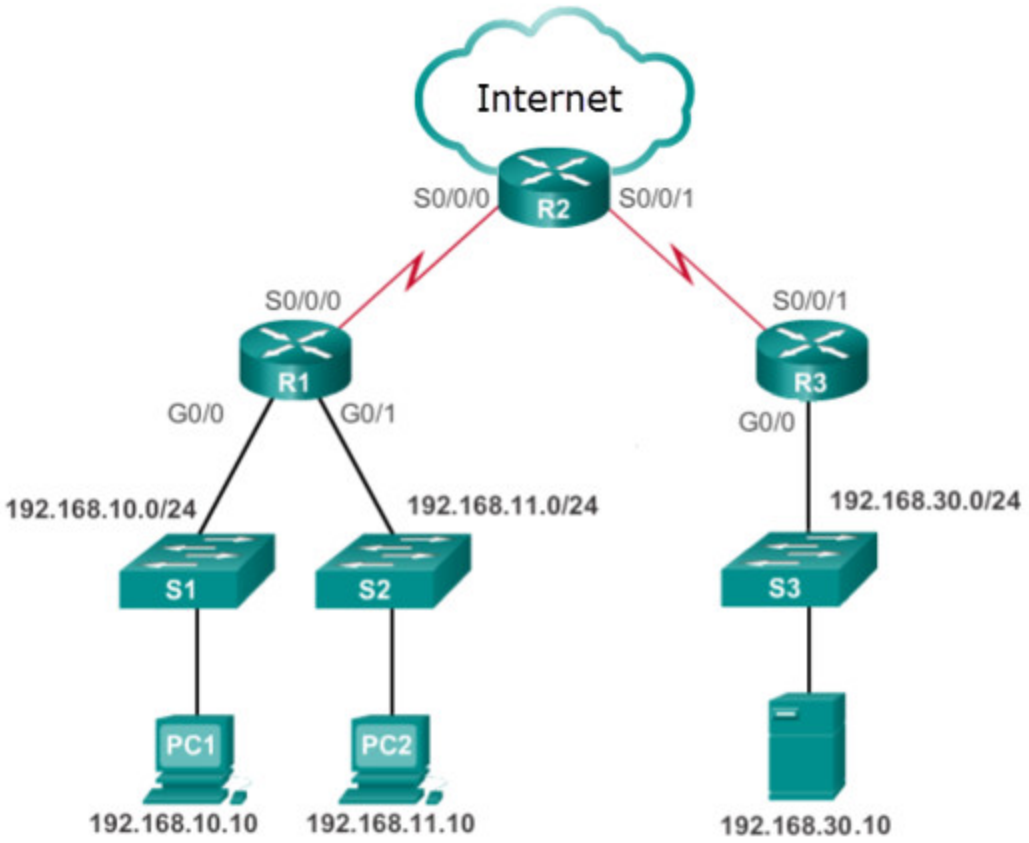
```
R1# show file systems
File Systems:

       Size(b)       Free(b)      Type  Flags  Prefixes
             -             -    opaque     rw   archive:
             -             -    opaque     rw   system:
             -             -    opaque     rw   tmpsys:
             -             -    opaque     rw   null:
             -             -   network     rw   tftp:
*    256487424     184819712      disk     rw   flash0: flash:#
             -             -      disk     rw   flash1:
        262136        249270     nvram     rw   nvram:
             -             -    opaque     wo   syslog:
             -             -    opaque     rw   xmodem:
             -             -    opaque     rw   ymodem:
             -             -   network     rw   rcp:
             -             -   network     rw   http:
             -             -   network     rw   ftp:
             -             -   network     rw   scp:
             -             -    opaque     ro   tar:
             -             -   network     rw   https:
             -             -    opaque     ro   cns:
    4050042880    3774152704  usbflash     rw   usbflash0:
```

- The file already exists on the USB drive and cannot be overwritten.
- The drive was not properly formatted with the FAT16 file system.
- There is no space left on the USB drive.
- The USB drive is not recognized by the router.
- **The command that the administrator used was incorrect.**

126. Which three types of VPNs are examples of enterprise-managed site-to-site VPNs? (Choose three.)

- Layer 3 MPLS VPN
- **IPsec VPN**
- **Cisco Dynamic Multipoint VPN**
- **GRE over IPsec VPN**
- clientless SSL VPN
- client-based IPsec VPN

127. Refer to the exhibit. Employees on 192.168.11.0/24 work on critically sensitive information and are not allowed access off their network. What is the best ACL type and placement to use in this situation?



- standard ACL inbound on R1 vty lines
- extended ACL inbound on R1 G0/0
- **standard ACL inbound on R1 G0/1**
- extended ACL inbound on R3 S0/0/1

128. In an OSPF network which two statements describe the link-state database (LSDB)? (Choose two.)

- **It can be viewed by using the `show ip ospf database` command.**
- A neighbor table is created based on the LSDB.
- It contains a list of only the best routes to a particular network.
- It contains a list of all neighbor routers to which a router has established bidirectional communication.
- **All routers within an area have an identical link-state database.**

129. In an OSPF network which OSPF structure is used to create the neighbor table on a router?

- **adjacency database**
- link-state database
- routing table
- forwarding database

130. What protocol is used in a system that consists of `three elements--a manager` , agents, and an information database?

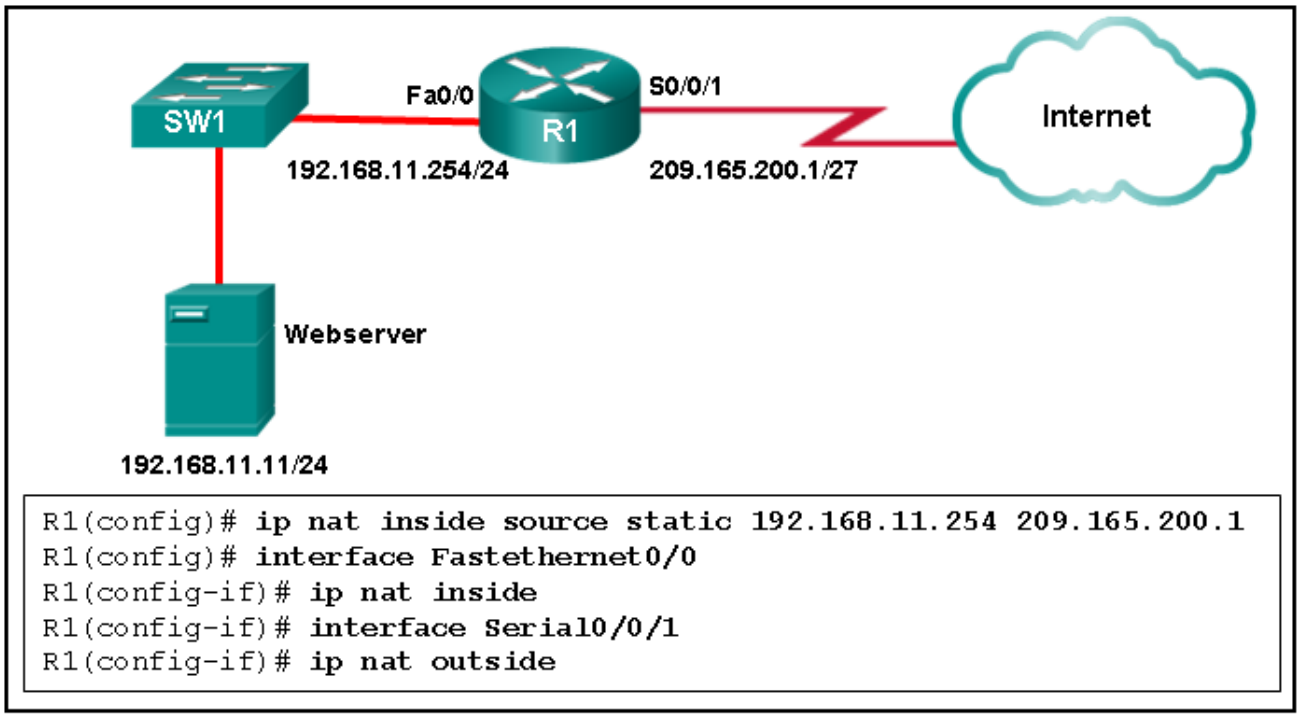
- MPLS
- SYSLOG
- **SNMP**
- TFTP

131. What type of traffic is described as not resilient to loss?

- data
- **video**
- voice

Explanation: Video traffic tends to be unpredictable, inconsistent, and bursty compared to voice traffic. Compared to voice, video is less resilient to loss and has a higher volume of data per packet.

132. Refer to the exhibit. Router R1 is configured with static NAT. Addressing on the router and the web server are correctly configured, but there is no connectivity between the web server and users on the Internet. What is a possible reason for this lack of connectivity?



- Interface Fa0/0 should be configured with the command ip nat outside .
- The inside global address is incorrect.
- **The router NAT configuration has an incorrect inside local address.**

- The NAT configuration on interface S0/0/1 is incorrect.

133. Which type of API would be used to allow authorized salespeople of an organization access to internal sales data from their mobile devices?

- open
- partner
- public
- **private**

134. Refer to the exhibit. Which data format is used to represent the data for network automation applications?

- **XML**
- HTML
- YAML
- JSON

```
<message>complete</message>
<username>efriends</username>
<user_info>
<First_name>Emily</First_name>
<Last_name>Friends</Last_name>
</user_info>
```

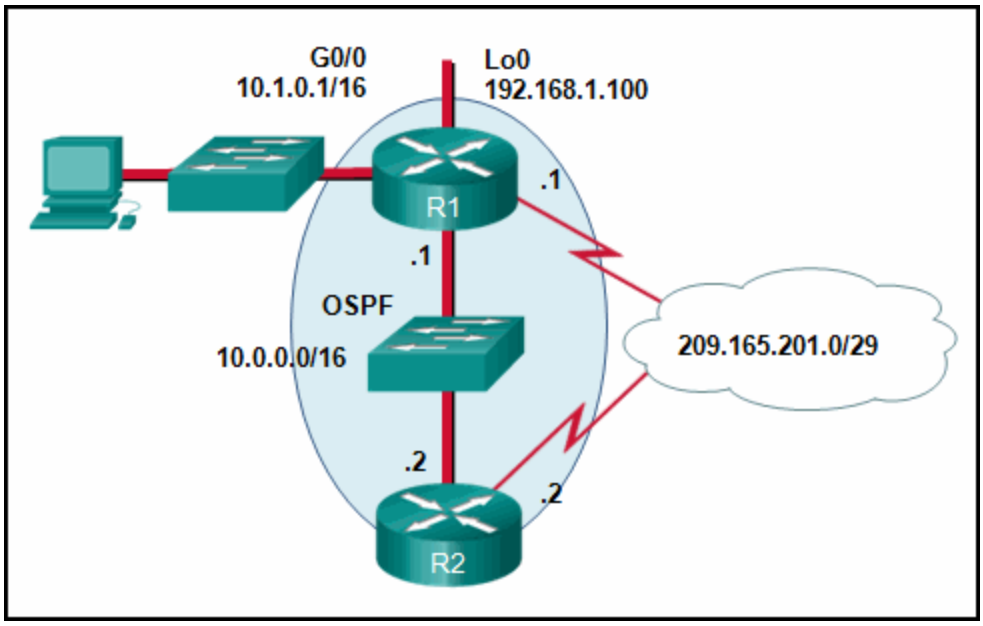
135. An ACL is applied inbound on a router interface. The ACL consists of a single entry:

```
access-list 101 permit udp 192.168.100.32 0.0.0.7 host 198.133.219.76 eq telnet .
```

If a packet with a source address of 198.133.219.100, a destination address of 198.133.219.170, and a protocol of 23 is received on the interface, is the packet permitted or denied?

- **denied**
- permitted

136. Refer to the exhibit. If no router ID was manually configured, what would router R1 use as its OSPF router ID?



- 10.0.0.1
- 10.1.0.1
- **192.168.1.100**
- 209.165.201.1

137. What protocol is a vendor-neutral Layer 2 protocol that advertises the identity and capabilities of the host device to other connected network devices?

- NTP
- **LLDP**
- SNMP
- MPLS

138. Which type of VPN uses a hub-and-spoke configuration to establish a full mesh topology?

- MPLS VPN
- GRE over IPsec
- IPsec virtual tunnel interface
- **dynamic multipoint VPN**

139. What is a characteristic of the REST API?

- evolved into what became SOAP
- used for exchanging XML structured information over HTTP or SMTP
- considered slow, complex, and rigid
- **most widely used API for web services**

141. A student, doing a summer semester of study overseas, has taken hundreds of pictures on a smartphone and wants to back them up in case of loss. What service or technology would support this requirement?

- Cisco ACI
- **cloud services**
- software defined networking
- dedicated servers

142. Consider the following access list that allows IP phone configuration file transfers from a particular host to a TFTP server:

```
R1(config)# access-list 105 permit udp host 10.0.70.23 host 10.0.54.5 range 1024 5000
R1(config)# access-list 105 deny ip any any
R1(config)# interface gi0/0
R1(config-if)# ip access-group 105 out
```

Which method would allow the network administrator to modify the ACL and include FTP transfers from any source IP address?

R1(config)# interface gi0/0
R1(config-if)# no ip access-group 105 out
R1(config)# access-list 105 permit tcp any host 10.0.54.5 eq 20
R1(config)# access-list 105 permit tcp any host 10.0.54.5 eq 21
R1(config)# interface gi0/0
R1(config-if)# ip access-group 105 out

R1(config)# access-list 105 permit tcp any host 10.0.54.5 eq 20
R1(config)# access-list 105 permit tcp any host 10.0.54.5 eq 21

R1(config)# interface gi0/0
R1(config-if)# no ip access-group 105 out
R1(config)# no access-list 105
R1(config)# access-list 105 permit udp host 10.0.70.23 host 10.0.54.5 range 1024 5000
R1(config)# access-list 105 permit tcp any host 10.0.54.5 eq 20
R1(config)# access-list 105 permit tcp any host 10.0.54.5 eq 21
R1(config)# access-list 105 deny ip any any
R1(config)# interface gi0/0
R1(config-if)# ip access-group 105 out

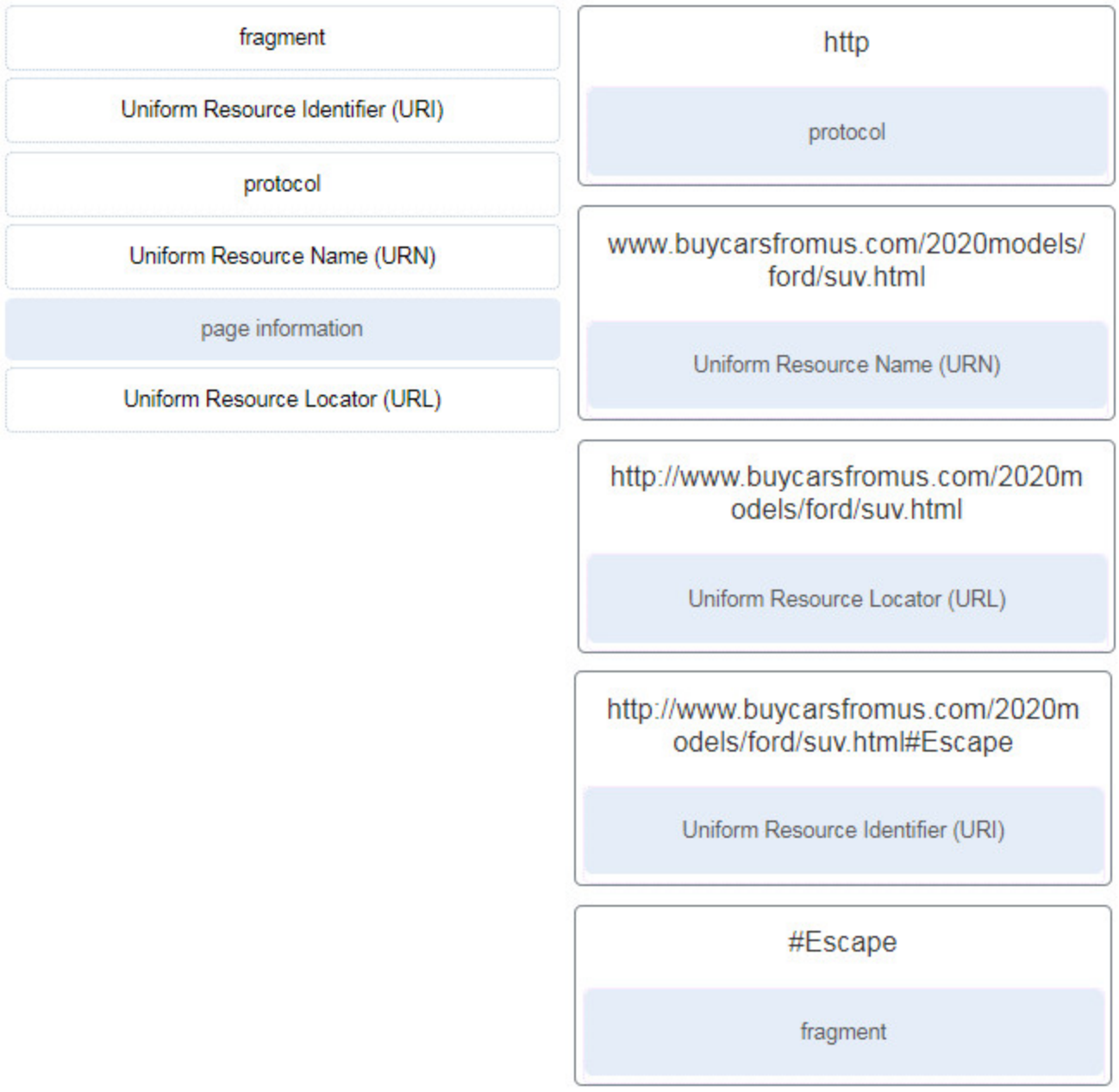
R1(config)# access-list 105 permit udp host 10.0.70.23 host 10.0.54.5 range 1024 5000
R1(config)# access-list 105 permit tcp any host 10.0.54.5 eq 20
R1(config)# access-list 105 permit tcp any host 10.0.54.5 eq 21
R1(config)# access-list 105 deny ip any any

143. Which three statements are generally considered to be best practices in the placement of ACLs? (Choose three.)

- **Filter unwanted traffic before it travels onto a low-bandwidth link.**
- **Place standard ACLs close to the destination IP address of the traffic.**
- Place standard ACLs close to the source IP address of the traffic.
- Place extended ACLs close to the destination IP address of the traffic.
- **Place extended ACLs close to the source IP address of the traffic.**
- For every inbound ACL placed on an interface, there should be a matching outbound ACL.

Explanation: Extended ACLs should be placed as close as possible to the source IP address, so that traffic that needs to be filtered does not cross the network and use network resources. Because standard ACLs do not specify a destination address, they should be placed as close to the destination as possible. Placing a standard ACL close to the source may have the effect of filtering all traffic, and limiting services to other hosts. Filtering unwanted traffic before it enters low-bandwidth links preserves bandwidth and supports network functionality. Decisions on placing ACLs inbound or outbound are dependent on the requirements to be met.

144. Match the term to the web link http://www.buycarsfromus.com/2020models/ford/suv.html#Escape component. (Not all options are used.)



145. What command would be used as part of configuring NAT or PAT to display all static translations that have been configured?

- **show ip nat translations**
- show ip pat translations
- show ip cache
- show running-config

146. A network administrator modified an OSPF-enabled router to have a hello timer setting of 20 seconds. What is the new dead interval time setting by default?

- 40 seconds

- 60 seconds
- **80 seconds**
- 100 seconds

147. Which type of VPN is the preferred choice for support and ease of deployment for remote access?

- **SSL VPN**
- GRE over IPsec
- dynamic multipoint VPN
- IPsec virtual tunnel interface

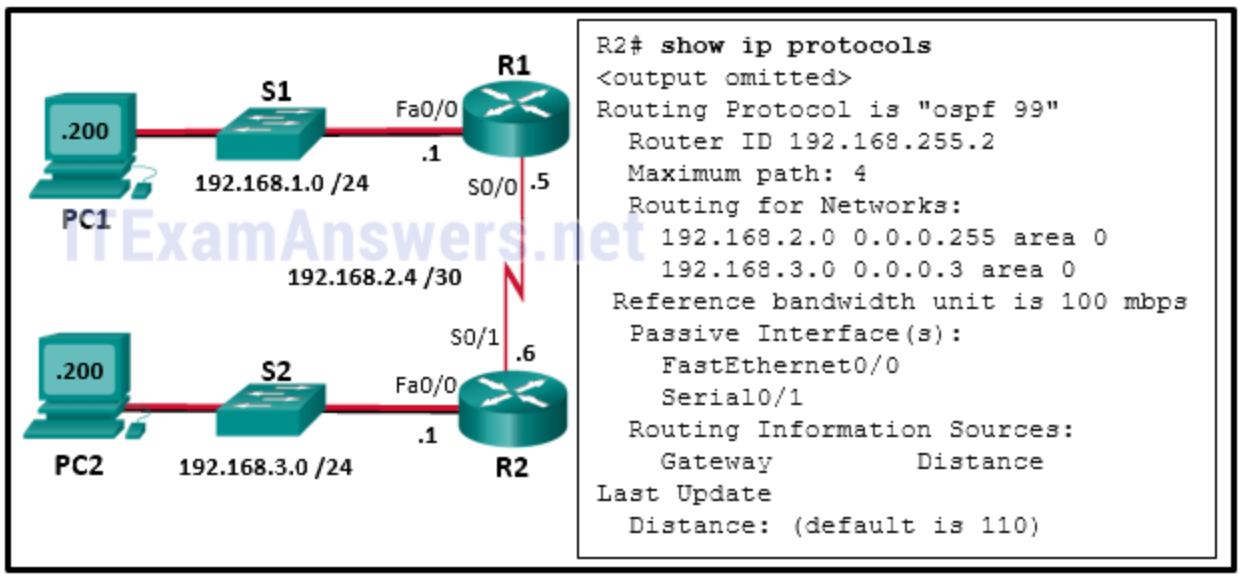
148. What type of traffic is described as predictable and smooth?

- video
- data
- **voice**

149. Which queuing mechanism has no provision for prioritizing or buffering but simply forwards packets in the order they arrive?

- **FIFO**
- LLQ
- CBWFQ
- WFQ

150. Refer to the exhibit. A network administrator has configured OSPFv2 on the two Cisco routers. The routers are unable to form a neighbor adjacency. What should be done to fix the problem on router R2?

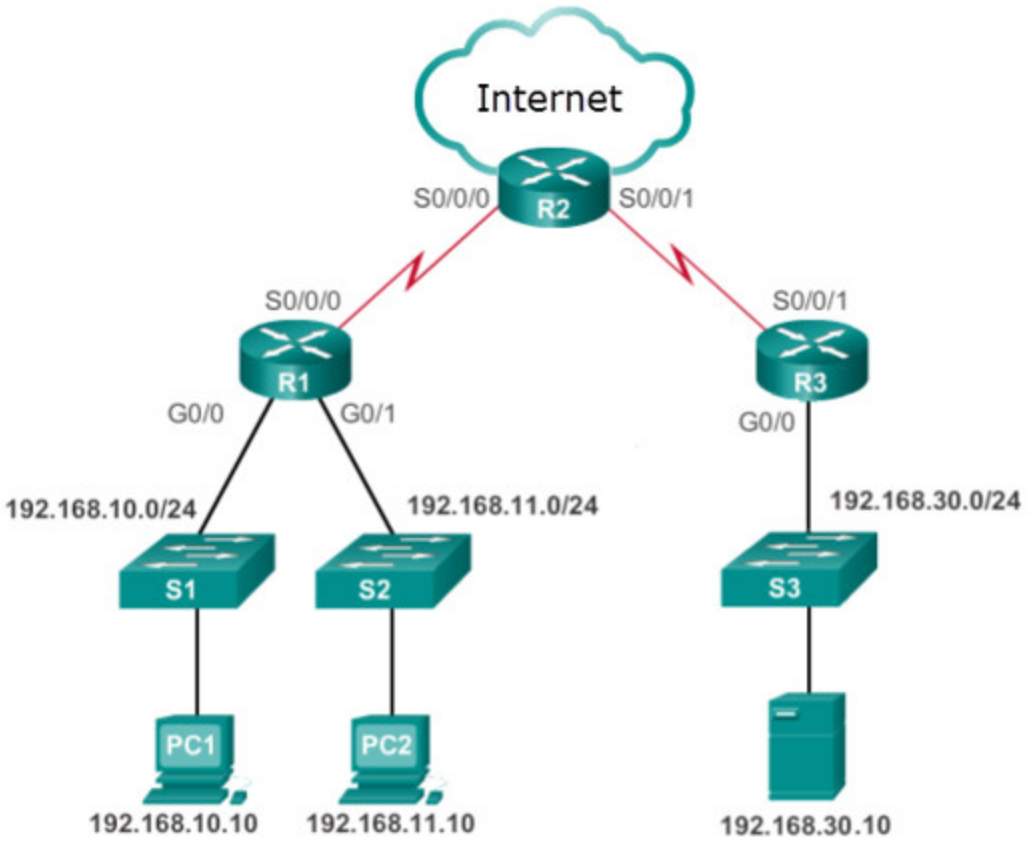


- **Implement the command no passive-interface Serial0/1.**
- Implement the command network 192.168.2.6 0.0.0.0 area 0 on router R2.
- Change the router-id of router R2 to 2.2.2.2.
- Implement the command network 192.168.3.1 0.0.0.0 area 0 on router R2.

151. A network administrator is troubleshooting an OSPF problem that involves neighbor adjacency. What should the administrator do?

- Make sure that the router priority is unique on each router.
- Make sure that the DR/BDR election is complete.
- Make sure that the router ID is included in the hello packet.
- **Make sure that the hello and dead interval timers are the same on all routers.**

152. Refer to the exhibit. Internet privileges for an employee have been revoked because of abuse but the employee still needs access to company resources. What is the best ACL type and placement to use in this situation?



CCNA 3 v7 Modules 3 – 5: Network Security Exam Answers 49

- standard ACL inbound on R2 WAN interface connecting to the internet
- **standard ACL outbound on R2 WAN interface towards the internet**
- standard ACL inbound on R1 G0/0

- standard ACL outbound on R1 G0/0

Explanation: – Standard ACLs permit or deny packets based only on the source IPv4 address. Because all traffic types are permitted or denied, standard ACLs should be located as close to the destination as possible.
– Extended ACLs permit or deny packets based on the source IPv4 address and destination IPv4 address, protocol type, source and destination TCP or UDP ports and more. Because the filtering of extended ACLs is so specific, extended ACLs should be located as close as possible to the source of the traffic to be filtered. Undesirable traffic is denied close to the source network without crossing the network infrastructure.

153. An ACL is applied inbound on a router interface. The ACL consists of a single entry:

```
access-list 100 permit tcp 192.168.10.0 0.0.0.255 172.17.200.0 0.0.0.255 eq www .
```

If a packet with a source address of 192.168.10.244, a destination address of 172.17.200.56, and a protocol of 80 is received on the interface, is the packet permitted or denied?

- denied
- **permitted**

154. A company has contracted with a network security firm to help identify the vulnerabilities of the corporate network. The firm sends a team to perform penetration tests to the company network. Why would the team use applications such as Nmap, SuperScan, and Angry IP Scanner?

- to detect installed tools within files and directories that provide threat actors remote access and control over a computer or network
- to detect any evidence of a hack or malware in a computer or network
- to reverse engineer binary files when writing exploits and when analyzing malware
- **to probe network devices, servers, and hosts for open TCP or UDP ports**

155. What command would be used as part of configuring NAT or PAT to display any dynamic PAT translations that have been created by traffic?

- show ip pat translations
- show ip cache
- show running-config
- **show ip nat translations**

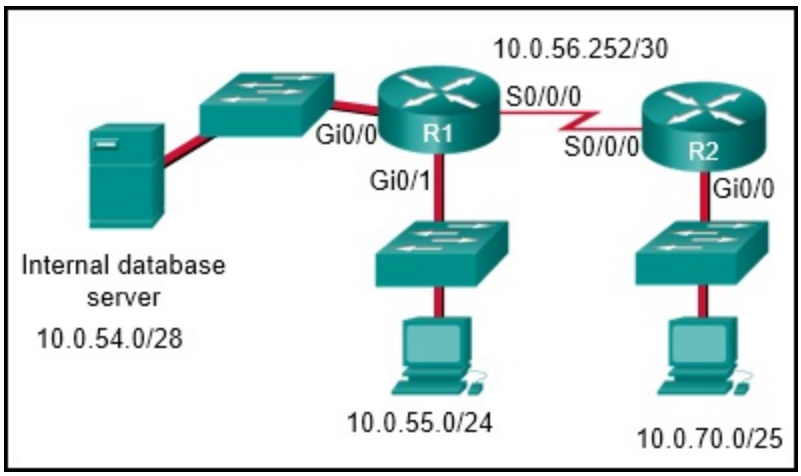
156. An administrator is configuring single-area OSPF on a router. One of the networks that must be advertised is 172.16.91.0 255.255.255.192. What wildcard mask would the administrator use in the OSPF network statement?

- 0.0.31.255
- **0.0.0.63**
- 0.0.15.255
- 0.0.7.255

157. What type of traffic is described as requiring latency to be no more than 400 milliseconds (ms)?

- **video**
- data
- voice

158. Refer to the exhibit. Which two configurations would be used to create and apply a standard access list on R1, so that only the 10.0.70.0/25 network devices are allowed to access the internal database server? (Choose two.)



A.
R1(config)# interface GigabitEthernet0/0
R1(config-if)# ip access-group 5 out

B.
R1(config)# access-list 5 permit 10.0.54.0 0.0.1.255

C.
R1(config)# interface Serial0/0/0
R1(config-if)# ip access-group 5 in

D.
R1(config)# access-list 5 permit 10.0.70.0 0.0.0.127

E.
R1(config)# access-list 5 permit any

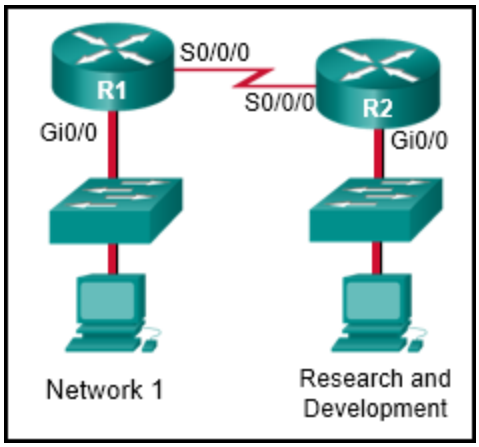
159. A network administrator is writing a standard ACL that will deny any traffic from the 172.16.0.0/16 network, but permit all other traffic. Which two commands should be used? (Choose two.)

- Router(config)# access-list 95 deny 172.16.0.0 255.255.0.0
- **Router(config)# access-list 95 permit any**
- Router(config)# access-list 95 host 172.16.0.0
- **Router(config)# access-list 95 deny 172.16.0.0 0.0.255.255**
- Router(config)# access-list 95 172.16.0.0 255.255.255.255
- Router(config)# access-list 95 deny any

Explanation: To deny traffic from the 172.16.0.0/16 network, the **access-list 95 deny 172.16.0.0 0.0.255.255** command is used. To permit all other traffic, the **access-list 95 permit any** statement is added.

160. Refer to the exhibit. The company has decided that no traffic initiating from any other existing or future network can be transmitted to the Research and Development network. Furthermore, no traffic that originates from the Research and Development network can be transmitted to any other existing or future networks in the company. The network administrator has decided that extended ACLs are better suited for these requirements. Based on the information given, what will the network administrator do?

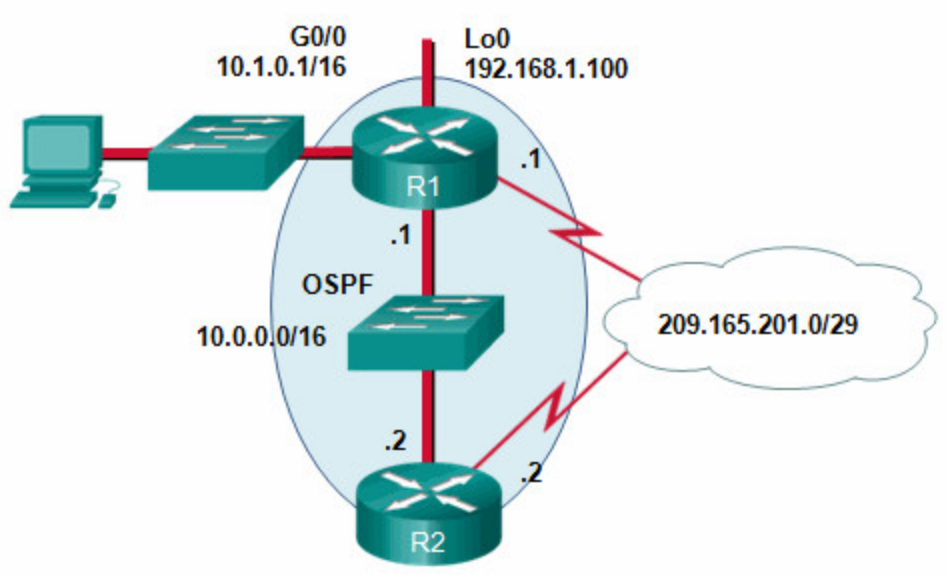
- One ACL will be placed on the R1 Gi0/0 interface and one ACL will be placed on the R2 Gi0/0 interface.
- Only a numbered ACL will work for this situation.
- One ACL will be placed on the R2 Gi0/0 interface and one ACL will be placed on the R2 S0/0/0 interface.
- **Two ACLs (one in each direction) will be placed on the R2 Gi0/0 interface.**



161. What protocol uses smaller stratum numbers to indicate that the server is closer to the authorized time source than larger stratum numbers?

- TFTP
- SYSLOG
- **NTP**
- MPLS

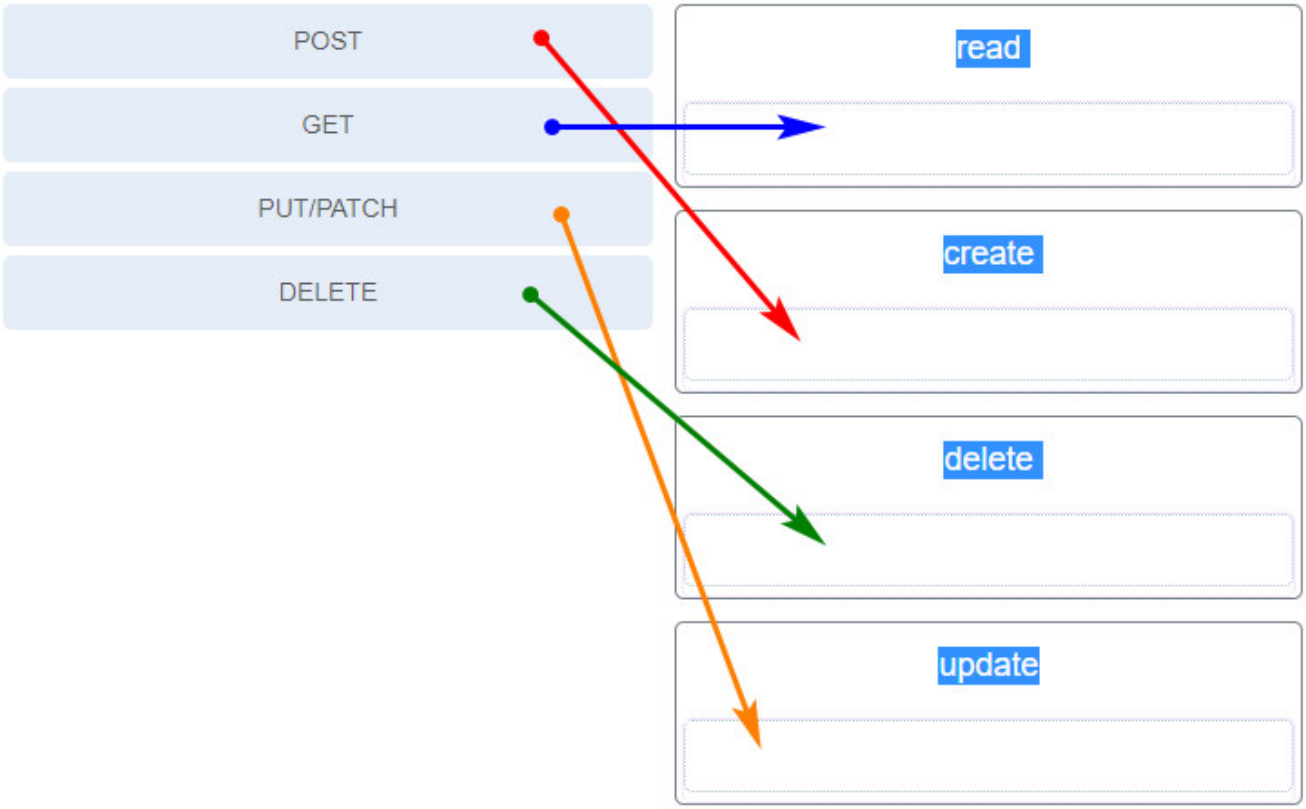
162. Refer to the exhibit. If no router ID was manually configured, what would router Branch1 use as its OSPF router ID?



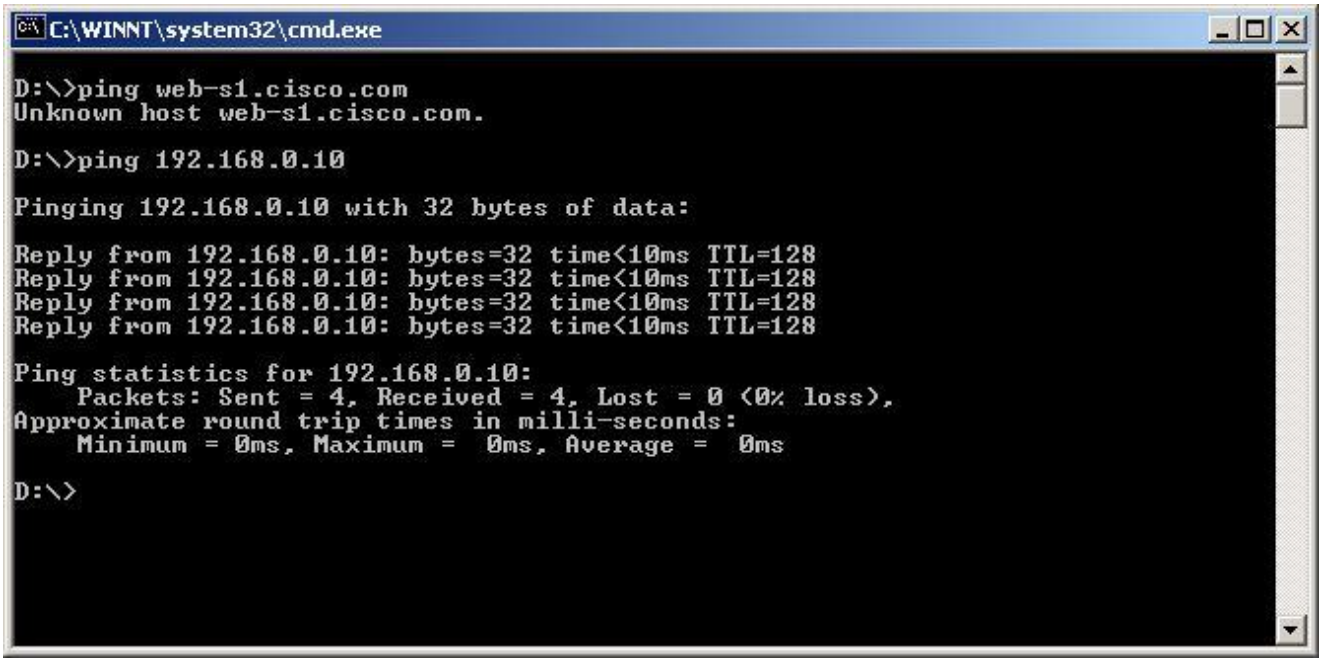
- 10.0.0.1
- 10.1.0.1
- 192.168.1.100
- 209.165.201.1

Explanation: In OSPFv2, a Cisco router uses a three-tier method to derive its router ID. The first choice is the manually configured router ID with the router-id command. If the router ID is not manually configured, the router will choose the highest IPv4 address of the configured loopback interfaces. Finally if no loopback interfaces are configured, the router chooses the highest active IPv4 address of its physical interfaces.

163. Match the HTTP method with the RESTful operation.



164. Refer to the exhibit. A web designer calls to report that the web server web-s1.cisco.com is not reachable through a web browser. The technician uses command line utilities to verify the problem and to begin the troubleshooting process. Which two things can be determined about the problem? (Choose two.)



- **The web server at 192.168.0.10 is reachable from the source host.**
- **DNS cannot resolve the IP address for the server web-s1.cisco.com.**
- A router is down between the source host and the server web-s1.cisco.com.

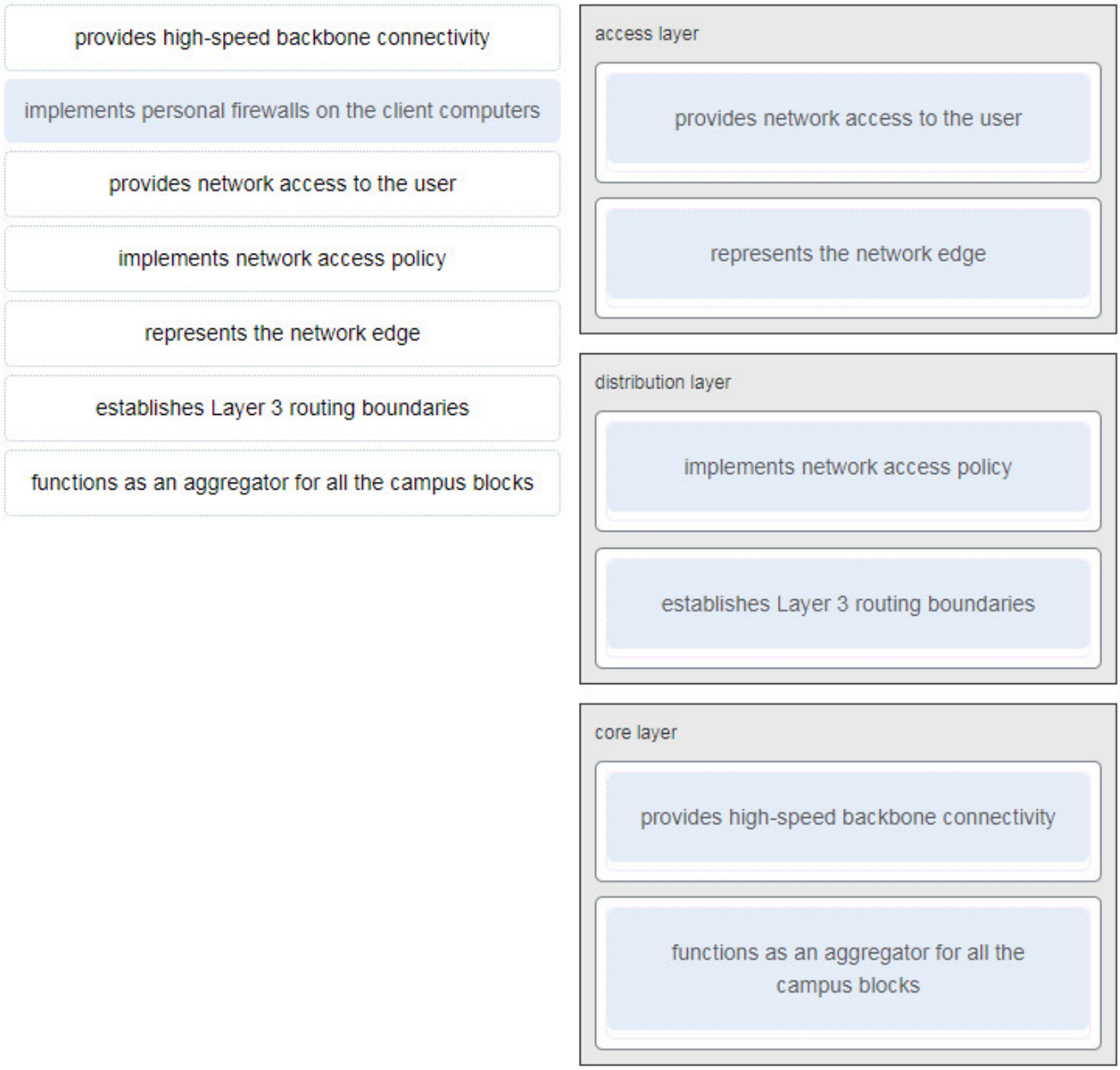
- There is a problem with the web server software on web-s1.cisco.com.
- The default gateway between the source host and the server at 192.168.0.10 is down.

Explanation: The successful result of the ping to the IP address indicates that the network is operational and the web server is online. However, the fact that the ping to the domain name of the server fails indicates there is a DNS issue, namely that the host cannot resolve the domain name to its associated IP address.

165. What type of traffic is described as tending to be unpredictable, inconsistent, and bursty?

- **video**
- voice
- data

166. Match the functions to the corresponding layers. (Not all options are used.)



167. What type of traffic is described as consisting of traffic that requires a higher priority if interactive?

- voice
- **data**
- video

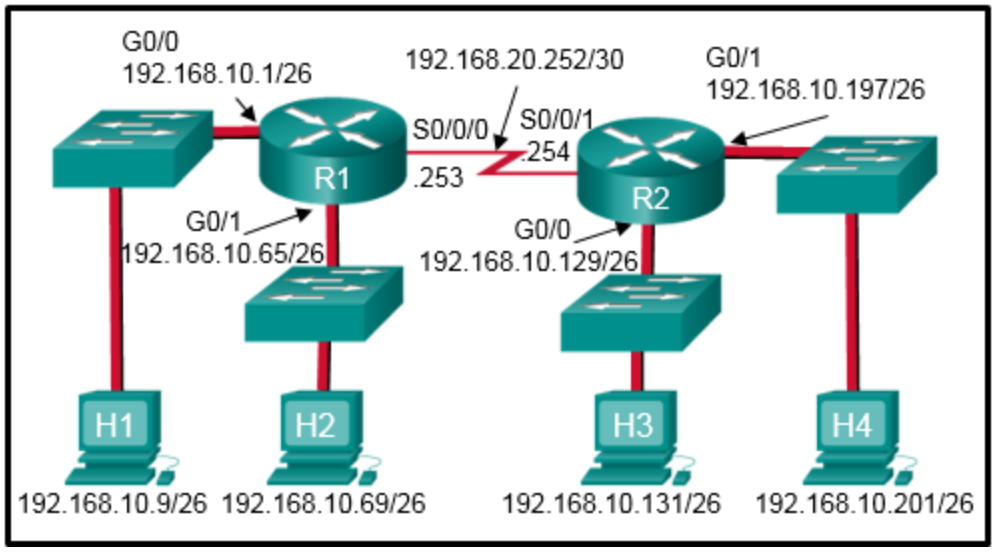
168. Which type of VPN provides a flexible option to connect a central site with branch sites?

- IPsec virtual tunnel interface
- MPLS VPN
- **dynamic multipoint VPN**
- GRE over IPsec

169. A company has contracted with a network security firm to help identify the vulnerabilities of the corporate network. The firm sends a team to perform penetration tests to the company network. Why would the team use fuzzers?

- **to discover security vulnerabilities of a computer**
- to detect any evidence of a hack or malware in a computer or network
- to reverse engineer binary files when writing exploits and when analyzing malware
- to detect installed tools within files and directories that provide threat actors remote access and control over a computer or network

170. Refer to the exhibit. A network administrator has configured a standard ACL to permit only the two LAN networks attached to R1 to access the network that connects to R2 G0/1 interface, but not the G0/0 interface. When following the best practices, in what location should the standard ACL be applied?



- R1 S0/0/0 outbound
- **R2 G0/0 outbound**
- R2 S0/0/1 outbound
- R1 S0/0/0 inbound
- R2 G0/1 inbound

171. Two OSPF-enabled routers are connected over a point-to-point link. During the ExStart state, which router will be chosen as the first one to send DBD packets?

- **the router with the highest router ID**
- the router with the lowest IP address on the connecting interface
- the router with the highest IP address on the connecting interface
- the router with the lowest router ID

Explain: In the ExStart state, the two routers decide which router will send the DBD packets first. The router with the higher router ID will be the first router to send DBD packets during the Exchange state

172. Which step in the link-state routing process is described by a router sending Hello packets out all of the OSPF-enabled interfaces?

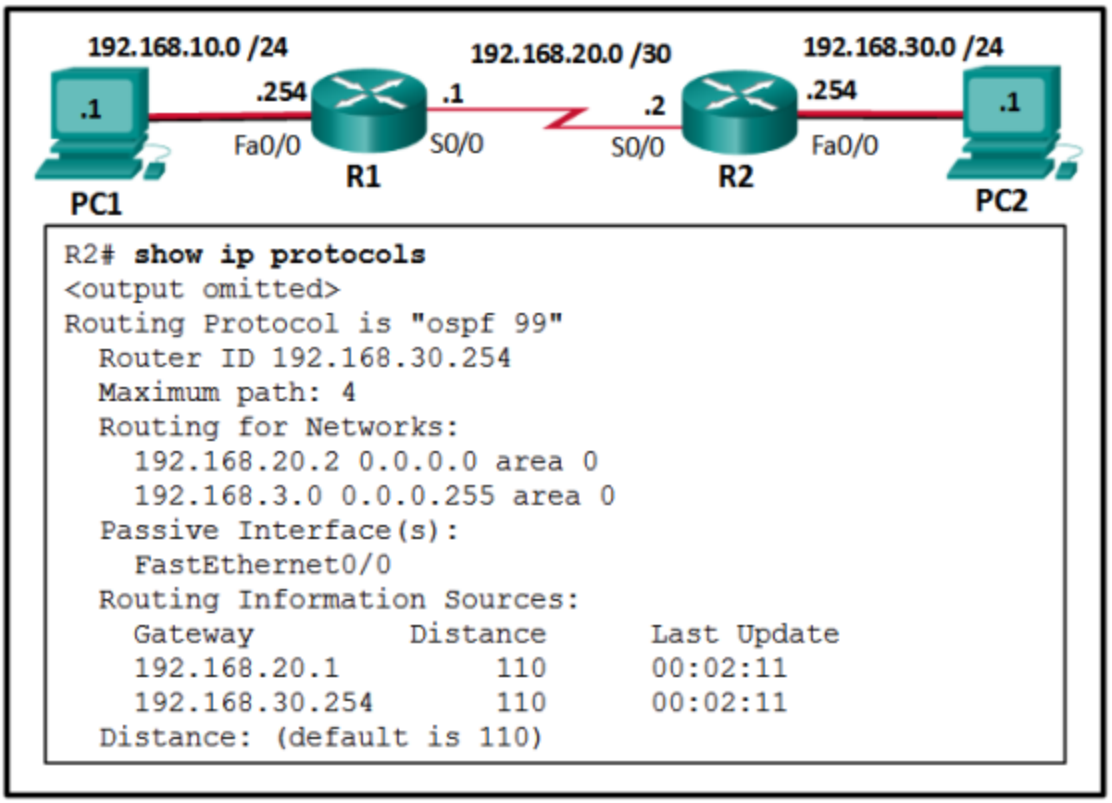
- exchanging link-state advertisements
- electing the designated router
- injecting the default route
- **establishing neighbor adjacencies**

Explanation: OSPF-enabled routers must recognize each other on the network before they can share information. An OSPF-enabled router sends Hello packets out all OSPF-enabled interfaces to determine if neighbors are present on those links. If a neighbor is present, the OSPF-enabled router attempts to establish a neighbor adjacency with that neighbor.

173. A company has contracted with a network security firm to help identify the vulnerabilities of the corporate network. The firm sends a team to perform penetration tests to the company network. Why would the team use forensic tools?

- to obtain specially designed operating systems preloaded with tools optimized for hacking
- **to detect any evidence of a hack or malware in a computer or network**
- to detect installed tools within files and directories that provide threat actors remote access and control over a computer or network
- to reverse engineer binary files when writing exploits and when analyzing malware

174. Refer to the exhibit. A network administrator has configured OSPFv2 on the two Cisco routers but PC1 is unable to connect to PC2. What is the most likely problem?



- **Interface Fa0/0 has not been activated for OSPFv2 on router R2.**
- Interface Fa0/0 is configured as a passive-interface on router R2.
- Interface S0/0 is configured as a passive-interface on router R2.
- Interface s0/0 has not been activated for OSPFv2 on router R2.

Explanation: If a LAN network is not advertised using OSPFv2, a remote network will not be reachable. The output displays a successful neighbor adjacency between router R1 and R2 on the interface S0/0 of both routers.

175. ABCTech is investigating the use of automation for some of its products. In order to control and test these products, the programmers require Windows, Linux, and MAC OS on their computers. What service or technology would support this requirement?

- dedicated servers
- software defined networking
- **virtualization**
- Cisco ACI

176. A network engineer has noted that some expected network route entries are not displayed in the routing table. Which two commands will provide additional information about the state of router adjacencies, timer intervals, and the area ID? (Choose two.)

- show ip protocols

- **show ip ospf neighbor**
- show running-configuration
- **show ip ospf interface**
- show ip route ospf

Explanation: The show ip ospf interface command will display routing table information that is already known. The show running-configuration and show ip protocols commands will display aspects of the OSPF configuration on the router but will not display adjacency state details or timer interval details.

177. Which type of VPN involves the forwarding of traffic over the backbone through the use of labels distributed among core routers?

- **MPLS VPN**
- GRE over IPsec
- IPsec virtual tunnel interface
- dynamic multipoint VPN

178. Which type of VPN involves a nonsecure tunneling protocol being encapsulated by IPsec?

- SSL VPN
- dynamic multipoint VPN
- **GRE over IPsec**
- IPsec virtual tunnel interface

179. A company has contracted with a network security firm to help identify the vulnerabilities of the corporate network. The firm sends a team to perform penetration tests to the company network. Why would the team use hacking operation systems?

- to detect any evidence of a hack or malware in a computer or network
- **to obtain specially designed operating systems preloaded with tools optimized for hacking**
- to encode data, using algorithm schemes, to prevent unauthorized access to the encrypted data
- to reverse engineer binary files when writing exploits and when analyzing malware

180. What command would be used as part of configuring NAT or PAT to identify an interface as part of the external global network?

- ip pat inside
- access-list 10 permit 172.19.89.0 0.0.0.255
- ip nat inside

- **ip nat outside**

181. To avoid purchasing new hardware, a company wants to take advantage of idle system resources and consolidate the number of servers while allowing for multiple operating systems on a single hardware platform. What service or technology would support this requirement?

- data center
- cloud services
- **virtualization**
- dedicated servers

Explain: Server virtualization takes advantage of idle resources and consolidates the number of required servers. This also allows for multiple operating systems to exist on a single hardware platform.

182. Which type of VPN routes packets through virtual tunnel interfaces for encryption and forwarding?

- MPLS VPN
- **IPsec virtual tunnel interface**
- dynamic multipoint VPN
- GRE over IPsec

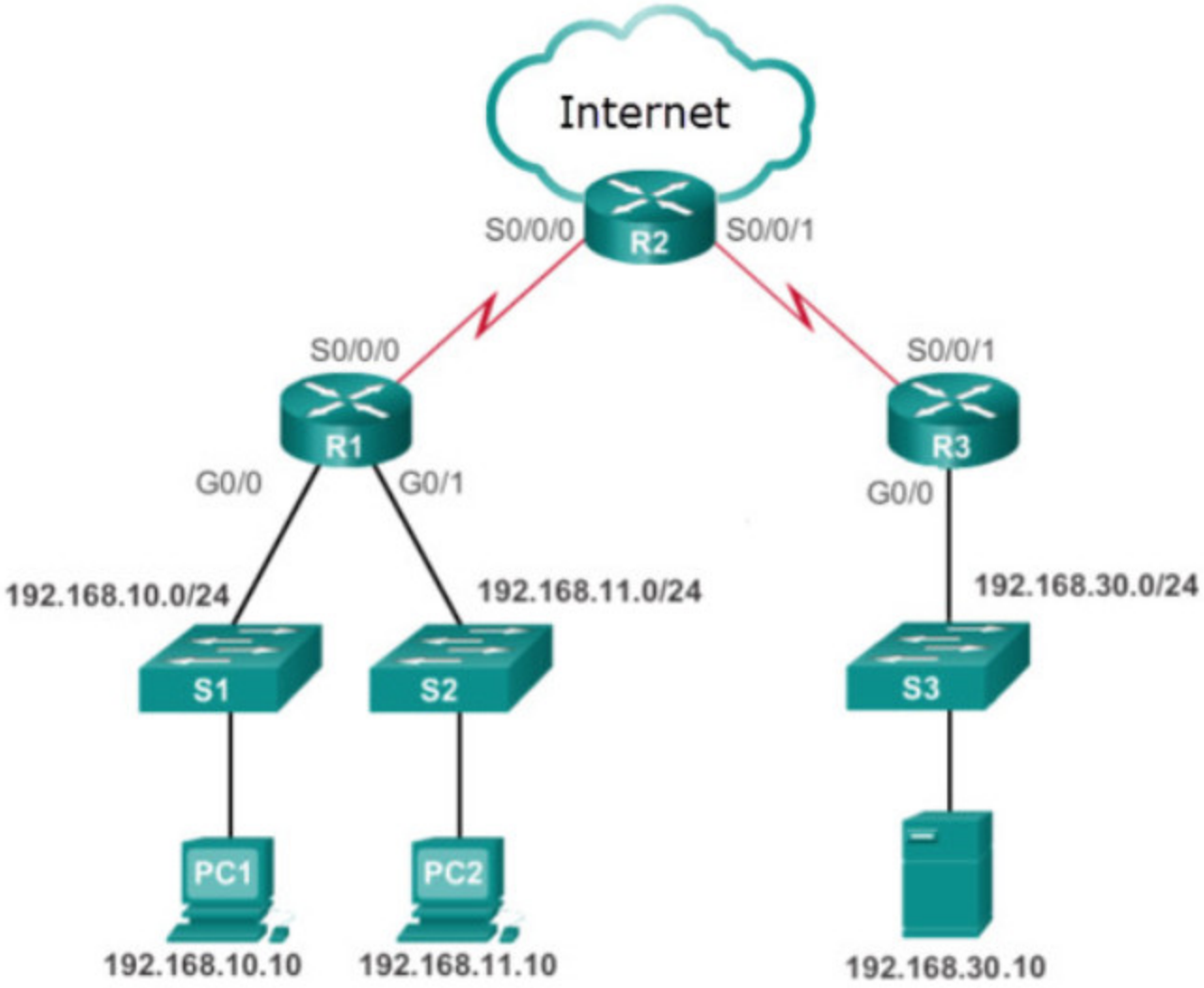
183. Which step in the link-state routing process is described by a router flooding link-state and cost information about each directly connected link?

- building the topology table
- selecting the router ID
- **exchanging link-state advertisements**
- injecting the default route

184. What type of traffic is described as using either TCP or UDP depending on the need for error recovery?

- video
- voice
- **data**

185. Refer to the exhibit. The company CEO demands that one ACL be created to permit email traffic to the internet and deny FTP access. What is the best ACL type and placement to use in this situation?



- **extended ACL outbound on R2 WAN interface towards the internet**
- standard ACL outbound on R2 S0/0/0
- extended ACL inbound on R2 S0/0/0
- standard ACL inbound on R2 WAN interface connecting to the internet

186. What command would be used as part of configuring NAT or PAT to define a pool of addresses for translation?

- ip nat inside source static 172.19.89.13 198.133.219.65
- ip nat inside source list 24 interface serial 0/1/0 overload
- **ip nat pool POOL-STAT 64.100.14.17 64.100.14.30 netmask 255.255.255.240**
- ip nat outside

187. What is the name of the layer in the Cisco borderless switched network design that is considered to be the backbone used for high-speed connectivity and fault isolation?

- data link
- access
- **core**
- network
- network access

Explanation: The three layers of the Cisco borderless switch network design are access, distribution, and core. The access layer switches are the ones used to connect end devices to the network. The distribution layer switches accept connections from access layer switches and provides switching, routing, and access policy functions. The core layer is called the backbone and core switches commonly have high-speed redundant connections.

188. An ACL is applied inbound on router interface. The ACL consists of a single entry:

```
access-list 210 permit tcp 172.18.20.0 0.0.0.47 any eq ftp
```

If a packet with a source address of 172.18.20.40, a destination address of 10.33.19.2, and a protocol of 21 is received on the interface, is the packet permitted or denied?

- **permitted**
- denied

189. What type of traffic is described as consisting of traffic that gets a lower priority if it is not mission-critical?

- video
- **data**
- voice

190. Which OSPF table is identical on all converged routers within the same OSPF area?

- routing
- neighbor
- adjacency
- **topology**

191. An ACL is applied inbound on a router interface. The ACL consists of a single entry:
access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq www .

If a packet with a source address of 192.168.10.45, a destination address of 10.10.3.27, and a protocol of 80 is received on the interface, is the packet permitted or denied?

- **permitted**
- denied

192. What protocol allows the manager to poll agents to access information from the agent MIB?

- CBWFQ
- SYSLOG
- TFTP
- **SNMP**

193. Match each component of a WAN connection to its description. (Not all options are used.)

customer premises equipment

demarcation point

data terminal equipment

data communications equipment

devices that put data on the local loop

data communications equipment

devices and inside wiring located on the enterprise edge and which connect to a carrier link

customer premises equipment

a point that is established in a building or complex to separate customer equipment from service provider equipment

demarcation point

the point of presence that is the local service provider facility or building that connects the CPE to the provider network

customer devices that pass the data from a customer network or host computer for transmission over the WAN

data terminal equipment

Case 2:

194. What type of traffic is described as being able to tolerate a certain amount of latency, jitter, and loss without any noticeable effects?

- **voice**
- video
- data

195. What term describes adding a value to the packet header, as close to the source as possible, so that the packet matches a defined policy?

- policing
- **traffic marking**
- weighted random early detection (WRED)
- traffic shaping
- tail drop

196. Which three traffic-related factors would influence selecting a particular WAN link type? (Choose three.)

- cost of the link
- **amount of traffic**
- distance between sites
- reliability
- **security needs**
- **type of traffic**

Explanation: The traffic-related factors that influence selecting a particular WAN link type include the type of traffic, amount of traffic, quality requirements, and security requirements. Quality requirements include ensuring that traffic that cannot tolerate delay gets priority treatment as well as important business transactional traffic.

197. What command would be used as part of configuring NAT or PAT to link the inside local addresses to the pool of addresses available for PAT translation?

- ip nat inside source list ACCTNG pool POOL-STAT
- ip nat translation timeout 36000
- **ip nat inside source list 14 pool POOL-STAT overload**
- ip nat inside source static 172.19.89.13 198.133.219.65

198. What protocol is a vendor-neutral Layer 2 discovery protocol that must be configured separately to transmit and receive information packets?

- SNMP
- MPLS
- **LLDP**
- NTP

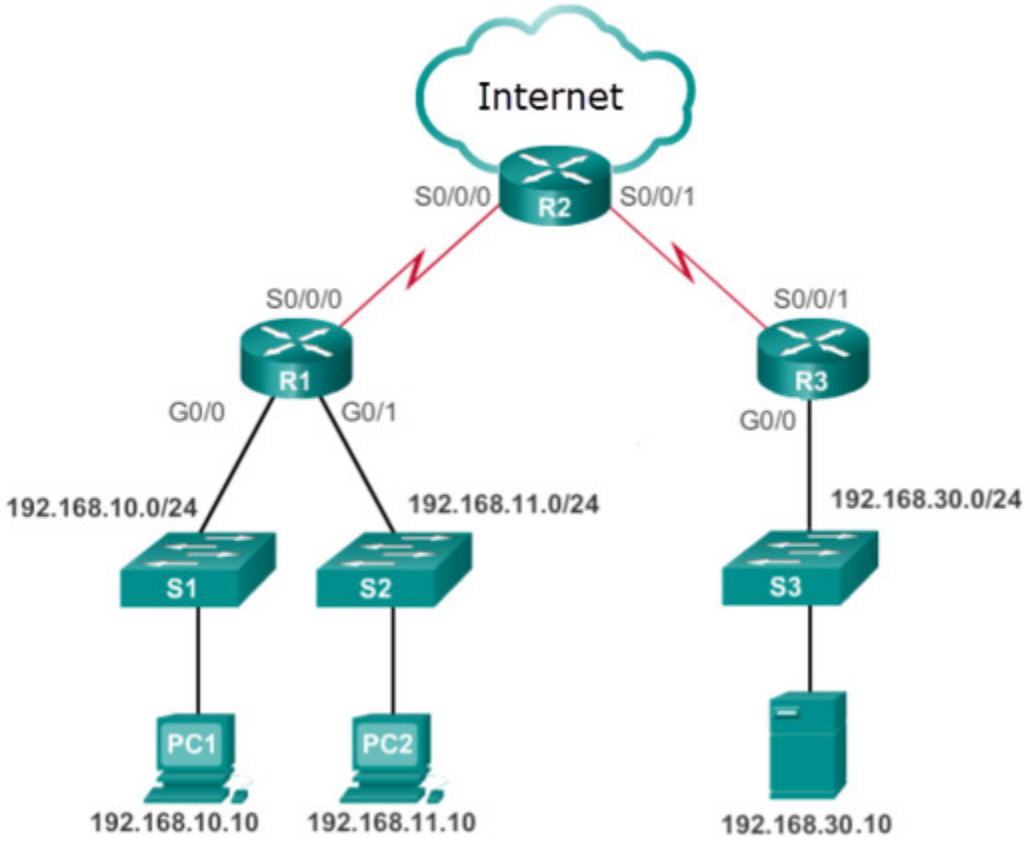
199. An ACL is applied inbound on a router interface. The ACL consists of a single entry:

```
access-list 210 permit tcp 172.18.20.0 0.0.0.31 172.18.20.32 0.0.0.31 eq ftp .
```

If a packet with a source address of 172.18.20.55, a destination address of 172.18.20.3, and a protocol of 21 is received on the interface, is the packet permitted or denied?

- permitted
- **denied**

200. Refer to the exhibit. Corporate policy demands that access to the server network be restricted to internal employees only. What is the best ACL type and placement to use in this situation?



Corporate policy demands that access to the server network be restricted to internal employees only. What is the best ACL type and placement to use in this situation

- **extended ACL outbound on R2 S0/0/1**
- standard ACL outbound on R2 S0/0/0
- standard ACL inbound on R2 WAN interface connecting to the internet
- extended ACL inbound on R2 S0/0/0

201. A technician is working on a Layer 2 switch and notices that a %CDP-4-DUPLEX_MISMATCH message keeps appearing for port G0/5. What command should the technician issue on the switch to start the troubleshooting process?

- show cdp neighbors

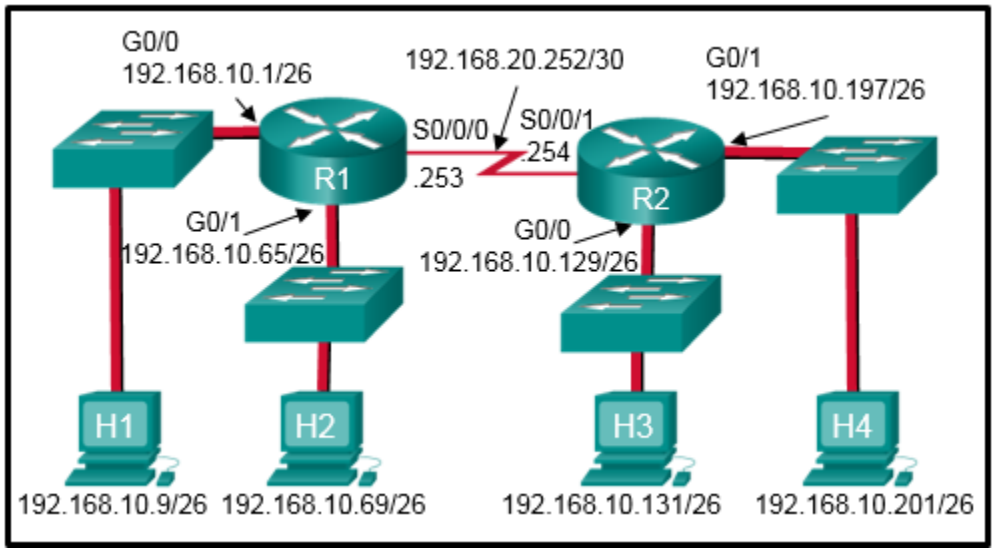
- show ip interface brief
- **show interface g0/5**
- show cdp

202. Which virtual resource would be installed on a network server to provide direct access to hardware resources?

- VMware Fusion
- a management console
- a dedicated VLAN
- **a Type 1 hypervisor**

Explanation: Type 1 hypervisors, the hypervisor is installed directly on the server or networking hardware. Then, instances of an OS are installed on the hypervisor, as shown in the figure. Type 1 hypervisors have direct access to the hardware resources. Therefore, they are more efficient than hosted architectures. Type 1 hypervisors improve scalability, performance, and robustness.

203. Refer to the exhibit. A network administrator has configured a standard ACL to permit only the two LAN networks attached to R1 to access the network that connects to R2 G0/1 interface. When following the best practices, in what location should the standard ACL be applied?



Enterprise Networking, Security, and Automation (Version 7.00) – ENSA Final Exam

- R2 G0/1 inbound
- R2 S0/0/1 outbound
- R1 S0/0/0 outbound
- **R2 G0/1 outbound**
- R2 G0/0 outbound

204. Which OSPF database is identical on all converged routers within the same OSPF area?

- neighbor
- forwarding
- **link-state**
- adjacency

Explanation: Regardless of which OSPF area a router resides in, the adjacency database, routing table, and forwarding database are unique for each router. The link-state database lists information about all other routers within an area and is identical across all OSPF routers participating in that area.

205. What are two features to consider when creating a named ACL? (Choose two.)

- **Use alphanumeric characters if needed.**
- Use special characters, such as ! or * to show the importance of the ACL.
- Modify the ACL using a text editor.
- **Be descriptive when creating the ACL name.**
- Use a space for ease of reading to separate the name from the description

Explanation: The following summarizes the rules to follow for named ACLs:

Assign a name to identify the purpose of the ACL.
Names can contain alphanumeric characters.
Names cannot contain spaces or punctuation.
It is suggested that the name be written in CAPITAL LETTERS.
Entries can be added or deleted within the ACL.

206. Match the RESTful API method to CRUD function.

Match the RESTful API method to CRUD function.

207. What type of traffic is described as requiring at least 384 Kbps of bandwidth?

- voice
- data
- **video**

208. Which step in the link-state routing process is described by a router inserting best paths into the routing table?

- declaring a neighbor to be inaccessible
- executing the SPF algorithm
- load balancing equal-cost paths
- **choosing the best route**

209. Anycompany has decided to reduce its environmental footprint by reducing energy costs, moving to a smaller facility, and promoting telecommuting. What service or technology would support this requirement?

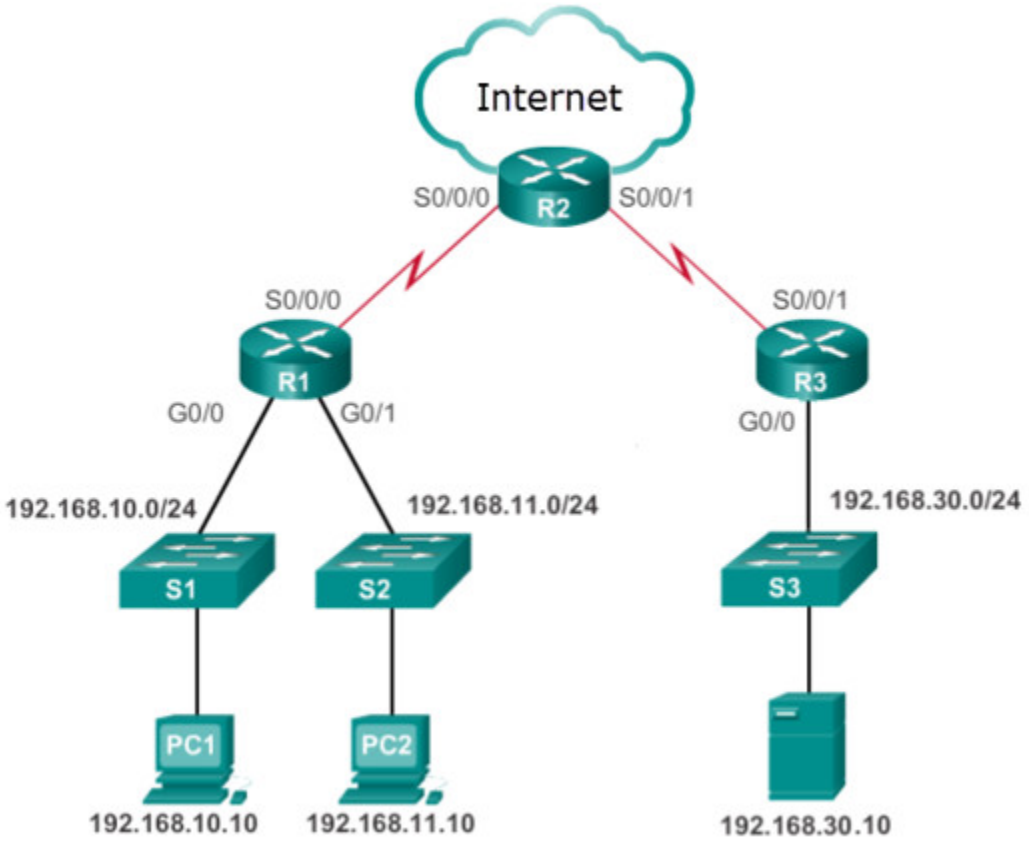
- data center
- virtualization
- **cloud services**

- dedicated servers

210. Which QoS technique smooths packet output rate?

- policing
- **shaping**
- weighted random early detection
- Integrated Services (IntServ)
- marking

211. Refer to the exhibit. The company has provided IP phones to employees on the 192.168.10.0/24 network and the voice traffic will need priority over data traffic. What is the best ACL type and placement to use in this situation?



- **extended ACL inbound on R1 G0/0**
- extended ACL outbound on R2 WAN interface towards the internet
- extended ACL outbound on R2 S0/0/1
- extended ACLs inbound on R1 G0/0 and G0/1

Explanation: Standard ACLs permit or deny packets based only on the source IPv4 address. Because all traffic types are permitted or denied, standard ACLs should be located as close to the destination as possible.

Extended ACLs permit or deny packets based on the source IPv4 address and destination IPv4 address, protocol type, source and destination TCP or UDP ports and more. Because the filtering of extended ACLs is so specific, extended ACLs should be located as close as possible to the source of the traffic to be filtered. Undesirable traffic is denied close to the source network without crossing the network infrastructure.

212. A network technician is configuring SNMPv3 and has set a security level of SNMPv3 authPriv. What is a feature of using this level?

- authenticates a packet by using the SHA algorithm only
- authenticates a packet by a string match of the username or community string
- **authenticates a packet by using either the HMAC with MD5 method or the SHA method**
- authenticates a packet by using either the HMAC MD5 or HMAC SHA algorithms and a username