

The book cover features a dark olive green background with a repeating geometric pattern of interlocking circles. A solid yellow horizontal band is positioned in the lower third of the cover. The title is centered in the upper two-thirds.

250
NETWORKING
INTERVIEW
QUESTIONS
AND ANSWERS

250 Networking Interview Questions & Answers

www.tcpipguru.com

Preface

This book contains 250 questions based on networking concepts like Firewall, NAT, VPN, Wireless networking, TCP/IP, Frame relay, Routing and switching.

The book also includes scenario based questions with diagrams and detailed tutorials. It is ideal for candidates aspiring for networking job interview.

Question 1

What happens when a TCP based packet exits a NAT firewall

When a TCP packet exits a NAT firewall, the source port and destination port number in the TCP header along with the source and destination IP address in the IP header is added to the Network address translation table. After this operation is performed, the source IP address in the IP header is re-written with the IP address of the NAT firewall following which the packet exits the firewall.

Question 2

What happens when a TCP based packet returns to a NAT firewall

When a TCP packet which exited the NAT firewall returns, the firewall looks into the destination port in the TCP header. It would then identify the appropriate entry in the NAT table which has the corresponding entry. After the packet is identified, the destination IP address in the IP packet which now contains the IP address of the NAT firewall would be re-written with the actual initiators IP address, following which the packet is sent to the intended recipient.

Question 3

Explain a practical scenario why split tunneling is used

Assume a scenario where a user initiates a VPN tunnel using a remote access client. Once the connection is established, all packets would be sent through the VPN tunnel which is created. This would also apply for internet bound packets. Internet bound packets should not be sent through the VPN tunnel. To avoid internet packets to be sent through the tunnel, split tunneling feature is used. When the feature is enabled, all internet packets would be sent through the adapter which is associated with the internet connection on the client and not through the VPN tunnel.

Question 4

What is the difference between TCP 4 way handshake and WPA 4 way handshake

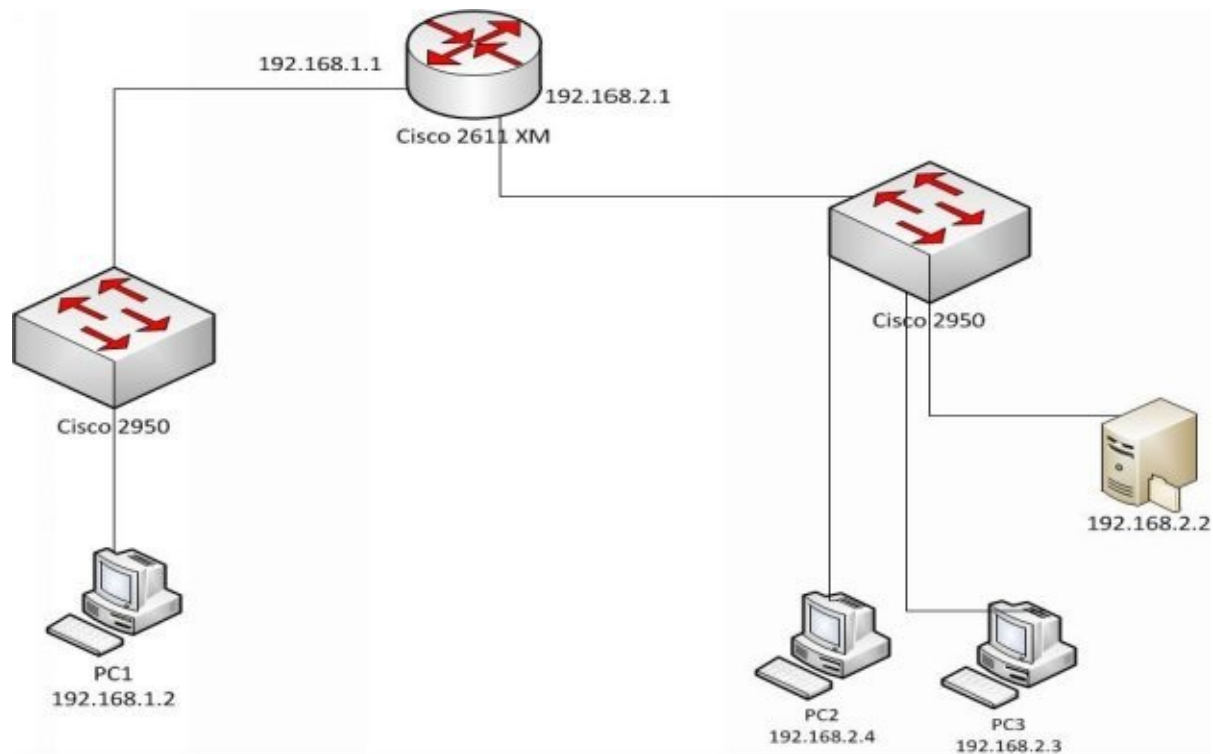
TCP 4 way handshake is used for tearing down a TCP session between a client and a server. WPA 4 way handshake is used by wifi clients and access points configured with WPA to derive session's keys for encryption and authentication.

Question 5

Which protocol would you block on a firewall for blocking tracert

Tracert uses ICMP at the network layer. ICMP should be denied on a firewall to block tracert.

The following questions are based with reference to the below diagram (Cisco router is used)



Question 6

Is a default gateway required to be configured on PC1 to ping 192.168.2.1

PC1 and PC2 are on two different networks. So a default gateway with the IP address 192.168.1.1 should be configured on PC1 for it to ping the IP address 192.168.2.1.

Question 7

How many route entry would be available on the routers routing table.

There would be two route entries, 192.168.1.0/24 and 192.168.2.0/24 which would be directly connected networks.

Question 8

It is required that the server should not be accessed by systems on the 192.168.1.0/24. Identify two techniques which can be used.

1. Configure an inbound ACL on the 192.168.1.1 interface which would

deny traffic from 192.168.1.0/24 to 192.168.2.0/24 network.

2. Configure an outbound ACL on the 192.168.2.1 interface, which would block all traffic from the 192.168.1.0/24 network.

Question 9

The gateway of PC1 is 192.168.1.1. Should it be configured on it for PC1 to be able to ping 192.168.1.1.

PC1 and the gateway are on the same network. To ping a gateway it need not be configured as gateways are required to reach systems on different networks.

Question 10

How many route entry would be available on the router, if the interface corresponding to 192.168.2.1 is shutdown.

The route entry corresponding to 192.168.2.0/24 would not be available and there would be only one entry which would be 192.168.1.0/24.

Question 11

Apart from interface configuration on the router, is any additional configuration required on the router for PC1 to access the 192.168.2.0 network.

No. When the interfaces are configured, the routing table of the router is populated with the appropriate entries which are 192.168.1.0/24 and 192.168.2.0/24. When PC1 pings PC2, the packet is sent to the router, which would then look up its routing table and forward to the appropriate interface to PC2.

% End of Question Based on Diagram%

Question 12

How does WEP derive keys which would be used for encrypting data sent over the wireless channel

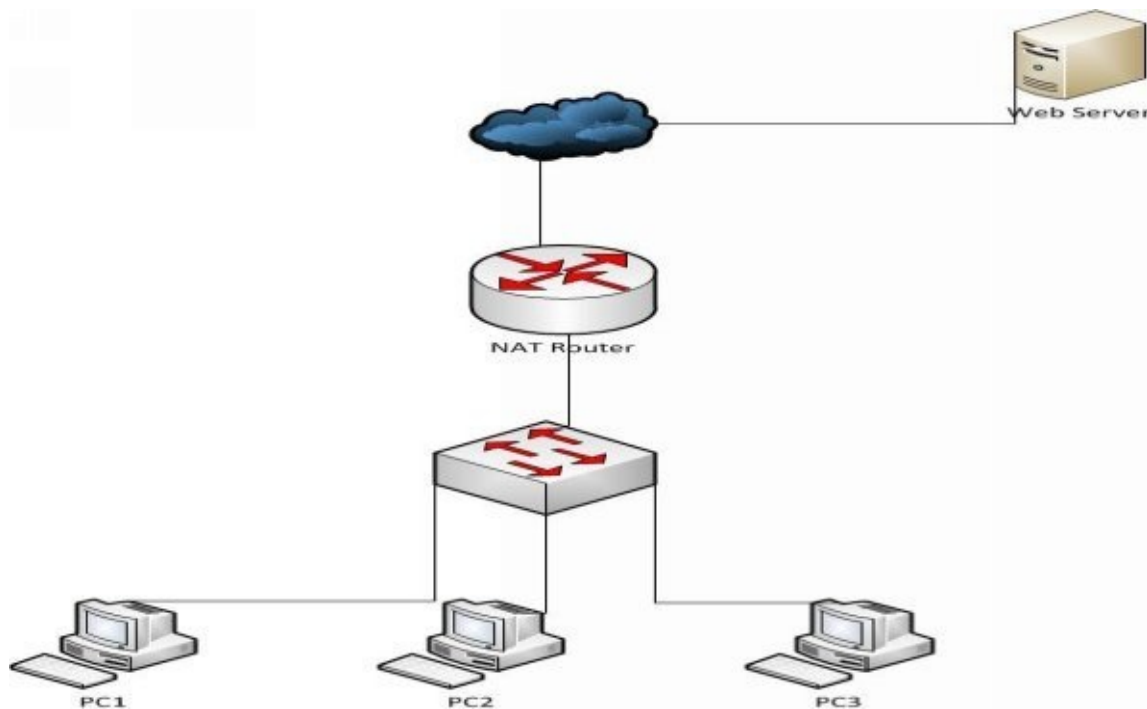
WEP pre-shared key is configured on the wifi client and the access point. Pre-shared keys are 40 bit or 104 bit in size. The key is combined with an IV (Initialization vector) which is 24 bits in size and randomly generated and is unique for every data frame which is encrypted. The total size of the key would then be 64 / 128 bits.

Question 13

How does a switch forward traffic from a trunk port to appropriate VLAN.

Trunk links are used for carrying multiple vlan traffic. Every packet which is sent over a trunk port would have the appropriate VLAN ID inserted in the frame. The switch would look into the VLAN ID and forward the packet to the appropriate VLAN based on this information.

Refer the below diagram for the following questions (Cisco router is used)



Question 14

PC1 PC2 and PC3 are connected to the internet via a NAT router which does port address translation. If the three PC's simultaneously initiate a HTTP session with the web server, explain how the NAT router would handle the communication

HTTP is based on TCP. When an http based communication is initiated to the web server, the TCP/IP on the operating systems would initiate a TCP 3 way handshake initially with the Web server. The TCP header would contain the source port number, which is used by the operating system and would be unique.

The NAT router, on receipt of the TCP header would maintain an entry in the NAT table which would contain the source port number and the source IP address of the actual system which has initiated the connection with a translated mapping which would contain the source port as the same or different number, based on the routers implementation, and the source IP address as the NAT routers IP address. The translated packet is sent to the Web server. When the response from the Web server reaches the router, every packet would contain the same destination IP address (NAT routers IP address), but the destination port number would be unique. The packet would be looked into and based on the destination port number, the correct entry in the NAT table would be used and forwarded to the actual recipient

Question 15

How does the NAT router differentiate two simultaneous connections which are initiated from PC1 to the web server.

The two simultaneous connections from PC1 would be two distinct TCP connections, which would contain unique source port numbers for each connection. Based on this information, the NAT router would differentiate the connection.

Question 16

What would the source IP address in the IP header which is sent from PC1 be when it reaches the web server.

When PC1 initiates a packet to the web server, the NAT router intercepts and re-writes the source IP address in the IP header with the IP address of the router. When the packet reaches the web server, the source IP address would contain the IP address of the router.

Question 17

What would the destination IP address in the IP header which is sent from the web server to PC1 when it reaches the router.

The packet sent from PC1 to the web server would contain the source IP address as the routers IP address (after NAT) and the destination IP address as the servers IP address. The server responds with the destination IP address as the routers IP address. When the packet reaches the router, the destination IP address in the header would be the routers IP address.

Question 18

What would the destination IP address in the IP header which is sent from the web server to PC1 when it reaches PC1.

When the packet from the web server reaches the router, the NAT table is looked into and checked for the actual initiator of the request. The router would then rewrite the destination IP address in the IP header with the initiators IP address which is the IP address of PC1. So when the packet reaches PC1, the destination IP address would be that of PC1.

Question 19

When PC2 initiates a request to the web server, would the destination IP address in the IP header be the routers or servers IP address

The IP header would contain the source IP address as PC2's IP address and the destination IP address as the servers IP address.

% End of Questions based on Diagram %

Recommended Book

250 + Network Engineer Interview Questions & Answers

[Click to view details in Amazon \(Ctrl +P\)](#)

Question 20

If NAT is configured for internet sharing on a router, is it required to setup additional routing for forwarding packets to the internet or would NAT take care of the same.

NAT and routing are two different concepts. NAT would not perform routing for the packet, which it has translated. The router should be setup for

additional routing as to how to forward the packet. A default route would ensure that all unknown packets are forwarded to the internet.

Question 21

If PAT is configured on the router, would it also take care of the packets be forwarded automatically to the internet

PAT does not perform routing services. A default route is required to be configured for forwarding packets to the internet.

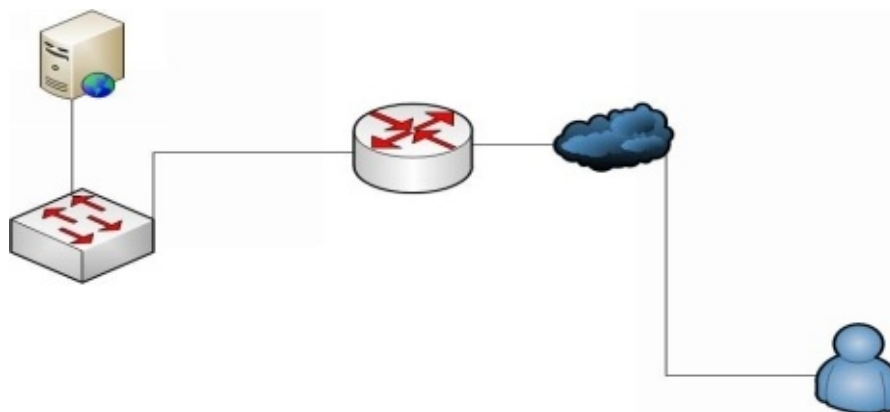
Question 22

Which flavor of NAT is configured on a Cisco router needs for sharing internet

Port Address translation is a feature which is used for internet sharing. The feature is used for sharing a single IP address with multiple internal IP addresses, a typical scenario encountered during internet sharing, where the public IP address configured on the router (Internet IP address) is shared among the internal LAN users for accessing internet.

Question 23

In the below topology, it is required that the server residing on the LAN should be accessible by users residing on the internet. How can the configuration be achieved. The router used is Cisco.



Static NAT is a feature which is available on routers to map public ip addresses with lan private ip addresses. In the above scenario, the organization can purchase a public ip address and use static nat feature to map the private ip address of the server. The option of connecting the server to the internet through the modem is also a viable solution but not recommended due to lack of security in the design.

Question 24

On a 24 port switch, there are 10 PC's connected. 5 PC's belongs to the 192.168.1.0/24 network and the other 5 PC's belong to 192.168.2.0/24. What address can be used to send a broadcast to PC's which are on the 192.168.2.0/24 network.

The address, 192.168.2.255, which is the broadcast address of the network 192.168.2.0/24, can be used for the same.

Question 25

Two PCs are connected to a switch. The IP address of PC1 is 192.168.1.33/27 and the IP address of PC2 is 192.168.1.65/27. Can PC1 ping PC2.

It can be observed that, PC1 belongs to the network address of 192.168.1.32/27 and PC2 belongs to the network, 192.168.1.64/27. As both reside on different networks, a router would be required for communication between PC1 and PC2. So in the current topology, PC1 would not be able to ping PC2.

Question 26

Can a PC be configured with an IP address 192.168.1.63 and subnet mask of 255.255.255.224.

The corresponding IP address for the above subnet mask would be the broadcast address for the network 192.168.1.32 /27. So it is not permitted to be used as an IP address to be configured on a host.

Question 27

How many computers can be setup with the network address 192.168.1.0/24 network.

The number of IP addresses in the network is 256, out of which the addresses 192.168.1.0 and 192.168.1.255 cannot be used as it is reserved for the network address and the broadcast address. Excluding the addresses, 254 IP addresses can be used. So, 254 computers can be configured using the available IP addresses.

Question 28

Would ARP protocol work on a frame relay network.

ARP protocol is used to find the mac-address corresponding to a known IP address. It uses layer 2 broadcast for the same. Frame relay does not support broadcast traffic, which would make ARP not workable on the network.

Question 29

An organization has a main office and 5 branch offices. It is required to connect the offices with options of using leased lines and frame relay. Give one reason from a business perspective why the organization should use frame relay for its WAN design.

Leased lines are very expensive. The costing for a linking up the offices with frame relay networks would be significantly lower as compared with leased lines. So, frame relay would be a cost effective solution for the organization.

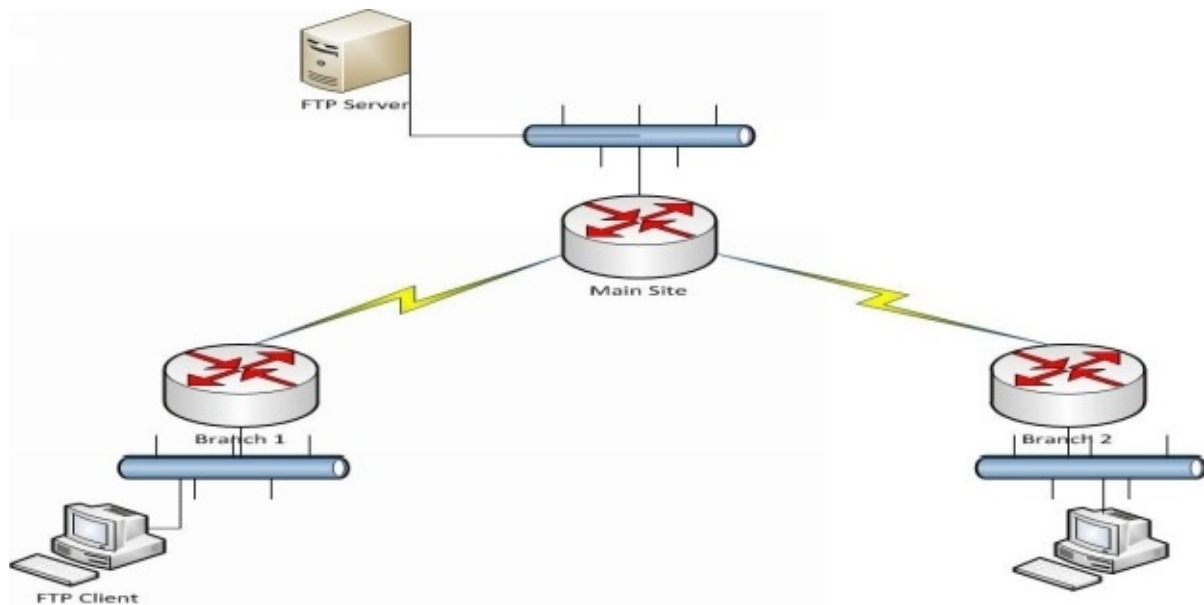
Question 30

Which networking concept is common in the use of inter-vlan routing and frame relay technology

Both technologies use virtual interfaces.

Question 31

In the below diagram, a frame relay point to multi point network is configured to link up between branch 1, branch 2 and main site. Can the FTP client access the FTP server on a point to multipoint frame relay network



FTP uses TCP at the transport layer for communication. The FTP packet is encapsulated in an IP header. Once the frame relay links are configured and appropriate routing for the networks are configured, the FTP client can access the FTP server without any issues.

Question 32

In the above topology diagram, how many physical interfaces would be required on the main site router if the organization were to consider the WAN options, leased line, frame relay and vpn.

Leased lines used dedicated lines. So two physical interfaces would be required for the main site router for leased line deployment. A frame relay network uses virtual circuits / interfaces for connection. So only one physical interface would be required which would be used to create virtual interfaces. If a VPN were to be used, the appropriate configuration would be performed on one physical interface.

Question 33

To transmit an IP packet over a WAN link like frame relay or leased line, is an encapsulation method required for the WAN link.

Without an encapsulation type or protocol, WAN links like leased lines and frame relay cannot transmit data, in this case an IP packet. On a leased line, encapsulation protocols like PPP, HDLC can be used. On a Frame relay network, encapsulation protocols like Cisco (For Cisco routers) or ietf.

Question 34

Can a router create a backup configuration on a TFTP server which is in a different location but reachable via IP network? Give an example of a TFTP server

TFTP uses client server architecture. If the router can access the TFTP server via IP, it can copy the configuration as IP connectivity is available. Solar Winds TFTP server is an example of the same.

Question 35

Which field in the TCP or UDP header identifies the application which is being requested

The destination port field in the TCP and UDP header corresponds to the application for which request is being initiated. The port number maps with a corresponding application. For ex; TCP port 80 corresponds to HTTP server and UDP port 53 corresponds to DNS servers.

Question 36

Two browser windows are opened on a PC and the webpage www.tcpipguru.com.com is accessed simultaneously. What would be the sequence number of the TCP connection for the TCP SYN segment for the first browser window.

Sequence numbers are generated by the operating system of the PC .A random number generated by the operating systems TCP/IP implementation would be the sequence number which would be used.

Question 37

A computer is connected to the internet via an ADSL router. The ADSL router is configured with appropriate DNS server IP address. Is it required to configure the DNS server IP address on the computer as well for internet access.

It is required for the DNS server IP address to be configured on the computer.

Take an example, where the user wishes to browse a website. When the user opens the browser and types the URL name of the website, a DNS resolution has to take place, for which the URL name has to be sent to a DNS server. The PC has to initiate the DNS request, for which the DNS server IP address has to be configured on the PC. If not configured, the DNS request would fail as the PC would be unaware of DNS server IP address and internet access would fail.

Question 38

An administrator of an organization is unable to telnet to a router, which is 10 hops away from the admin PC. What tool can be used to identify the location where the connection is dropped.

The admin can use traceroute command line tool to the router and check the location where the packets are being dropped.

Question 39

Telnet uses TCP port 23. Does this imply that the telnet connection initiated by a user connecting to the router from a computer uses TCP port 23

This is not true. When the user initiates a connection to the router, the TCP header in the connection would have a source port and destination port number. The destination port number would be port 23, indicating that the request is being initiated to the telnet server service which is identified by port 23. The source would be a random port number assigned by the TCP/IP on the operating system of the computer.

Question 40

Which is the protocol used by both traceroute and ping

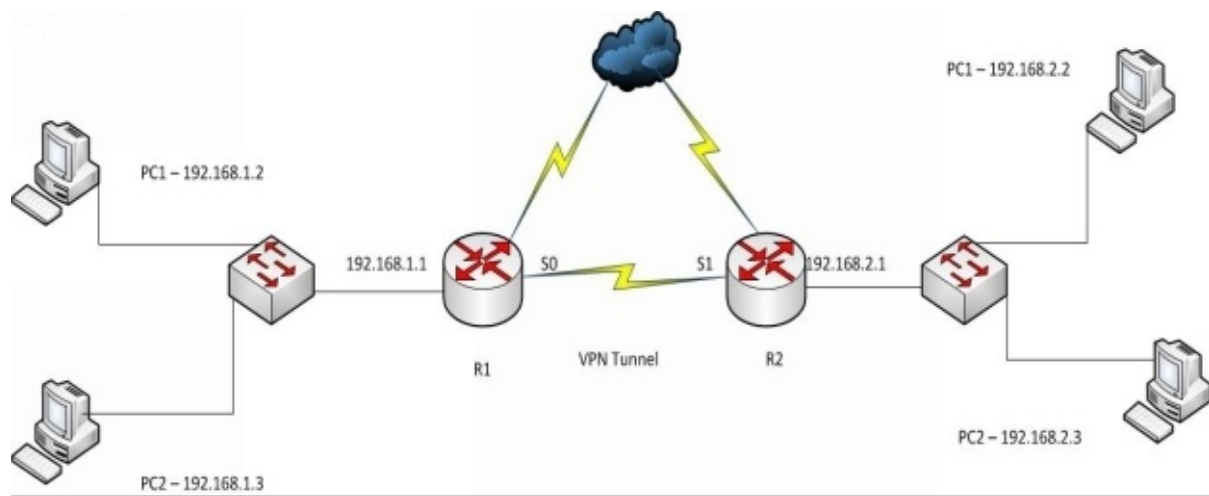
ICMP is used by both the protocols at the network layer.

Question 41

Name the two fields in the TCP header which is unavailable in a UDP header and is used for tracking the received and transmitted data.

Sequence and acknowledgement numbers are used for tracking the receipt and transmission of data in the TCP header.

The following questions are based on the diagram. Two sites are connected using Cisco VPN routers as shown. Every VPN router has three interfaces, one for LAN, VPN and internet.



Question 42

What should be configured to avoid internet packets to be not sent through the VPN tunnel.

The routers at each site should be configured with a default route, which should send packets through the interface which is connected to the internet.

Question 43

Will the packets which are sent to the internet encrypted by the VPN routers

Encryption is applied only to packets which are sent over the VPN tunnel. Internet bound packets are not encrypted.

Question 44

What would be the destination IP address in the IP header when a packet is initiated from 192.168.1.2 to 192.168.2.3 when it reaches S1 (R2)

When 192.168.1.2 initiates a packet to 192.168.2.3, it is sent to R1. This would have the source IP address in the IP header as 192.168.1.2 and destination IP address as 192.168.2.3. When the packet reaches R1, an additional header is added which would have the source IP address as S0 (R1) and destination IP address as S1 (R2). When the packet reaches R2, it would have the destination IP address as that of S1 (R2).

Question 45

What would be the destination IP address in the IP header when a packet is initiated from 192.168.1.2 to 192.168.2.3 when it reaches 192.168.2.3

When 192.168.1.2 initiates a packet to 192.168.2.3, it is sent to R1. This would have the source IP address in the IP header as 192.168.1.2 and destination IP address as 192.168.2.3. When the packet reaches R1, an additional header is added which would have the source IP address as S0 (R1) and destination IP address as S1 (R2). When the packet reaches R2, the outer header is discarded and the inner header which is the actual header would contain the source IP address as 192.168.1.2 and destination as the actual destination IP address which is 192.168.2.3. So when the packet reaches 192.168.2.3, it would have its IP address as the destination IP address.

Question 46

Should the public IP address which is configured on R1 (S0) and R2 (S1) be on the same network

This is not required. The VPN routers would be at different locations, where the public IP address provided by the respective ISP's would be on different networks.

Question 47

If a packet sniffer is used on the VPN tunnel can the inner IP header be viewed

The inner IP header is appended with the outer IP header which has the source IP address as R1 (S0) and R2 (S1). The inner IP header and its contents would be encrypted and cannot be viewed. (Provided IPSEC encryption protocol ESP is used. AH does not encrypt data)

Question 48

Are the pre-shared keys used between the routers used for data encryption between systems at the different sites.

No. The keys are derived dynamically as part of IPSEC phase 1 and phase 2 tunnel creation.

% End of questions based on Diagram %

Question 49

In which IPSEC Phase is the keys used for data encryption derived.

The keys are derived in IPSEC phase 2. The derived keys are used by IPSEC protocol ESP for encrypting the data.

Question 50

A PC is connected to a switch, to which a router is also connected. The management IP address of the switch is 192.168.1.2 and the IP address of the router is 192.168.1.1. What should the default gateway of the PC be, for it to access a remote network.

The default gateway IP address of the PC should be the IP address of the router, since routers are used for forwarding packets belonging to a different network.

Question 51

A router has two directly connected networks on its interfaces. Would an ARP request from one network reach the other network.

ARP request packets are broadcast packets. Routers do not forward broadcast packets to another network.

Question 52

What would be the type value in an ethernet frame, which is encapsulating an IP packet.

The type value would be IP. The type value in an ethernet frame refers to the protocol which is encapsulated by the ethernet frame. In this case since it is an IP packet, it would be IP.

Question 53

Name two operating system supports ARP protocol

Linux and Windows operating systems.

Question 54

Does IP fragment reassembly take place at intermediate routers or the destination

IP fragmentation reassembly takes place at the destination only.

Question 55

What is the destination mac-address of a frame whose destination IP

address is 192.168.1.255

Explanation

The destination IP address, 192.168.1.255 is a directed broadcast. This is a broadcast packet and the corresponding destination mac-address in the frame would be FF-FF-FF-FF-FF-FF

Question 56

Can two organizations have networks belonging to the same private IP address range

Private IP addresses are used by organizations for devices which reside within their network. It is not used for public communication (Internet). So this is possible.

Question 57

In a company network the following types of traffic is initiated from the clients namely FTP, HTTP (browsing), Telnet , ping, Custom applications. All these traffic require internet access. What would be the best technique the network administrator can use for achieving the same

Explanation

The organization can use Natting, specifically port address translation on a router for the purpose.

Question 58

How the IPSEC do protocols, ESP and AH provides replay protection.

ESP and AH include the sequence number fields in the respective headers. The values are used by the IPSEC peers to track duplicate packets. If a packet with an already received sequence number arrives, it would be rejected, thus providing replay protection.

Question 59

In IPSEC, If ESP provides both encryption and authentication, why is AH required.

ESP does not provide authentication to the outer IP header, which AH does.

Question 60

What is the security vulnerability in using a shared key authentication with WEP.

In a shared key authentication, the access point sends a challenge text to the client in clear, which would then be encrypted by the client using the shared key with WEP algorithm. The access point would decrypt the same with the shared key and verify. An attacker on the network can passively monitor the communication between the client and the access point and capture the challenge and encrypted text which can then be used to derive the shared key .

Question 61

In WEP, is the data packet which needs to be protected, encrypted with only the shared key on the client or is any other parameters used along with shared key.

The total key size in WEP is 64 or 128bit, out of which 40 and 104 bit respectively is used by the shared key and 24 bits, used by a value called Initialization vector. The initialization vector is created randomly and is combined with the actual WEP key for data encryption.

Question 62

Which two wireless standards are interoperable with each other and on what is the frequency on which they work.

802.11 b and 802.11 g are interoperable with each other and they both work on the 2.4 GHz range.

Question 63

Which encryption protocols are used by WEP and WPA.

WEP uses RC4 and WPA uses TKIP and AES for encryption.

Question 64

Why is mac-address authentication not recommended to be used for providing secure authentication.

In mac-address authentication, the mac-address of the client requiring access is configured on the access point. In wireless communication, an attacker can

passively sniff for packets on the network and retrieve information related to valid mac-address. The attacker then spoofs with the valid mac-address to gain access to the access point and on the network

Question 65

An application layer protocol uses UDP as it' transport layer protocol and IPv4 at network layer. If the application layer data is too large to be send in one packet, which option would be used?

- a) IP fragmentation
- b) UDP Sequence number and reassembly at the destination
- c) UDP Buffering
- d) None of these

Answer: A

IP fragmentation is the process which is used to transfer large chunk of data. Data is sent using fragmented IP packets, which is reassembled at the destination

Question 66

Which of the following is used as part of UDP check sum calculation

- a) Destination IP address
- b) Source IP address
- c) UDP header
- d) All of the above.

Answer: D

UDP check sum is calculated using destination IP address, Source IP address and the UDP header.

Question 67

Which field in a DHCP message exchange for a client would keep track of the message flow to avoid getting mismatched with a different DHCP packet from a different client .

- a) Sequence number in DHCP packets
- b) Transaction ID in DHCP packets

- c) Unicast packets
- d) Acknowledgment at the transport layer

Answer: B

DHCP messages contain unique transaction ID inside the packet. This field is used for differentiating between different packets.

Question 68

When will the DHCP client trigger for a lease renewal

- a. After the DHCP lease expires
- b. At the exact time when the DHCP lease expires
- c. Just before the DHCP lease expires
- d. None of these

Answer – c

DHCP Clients would request for a lease renewal just before the lease time expires. This is an automatic process.

Question 69

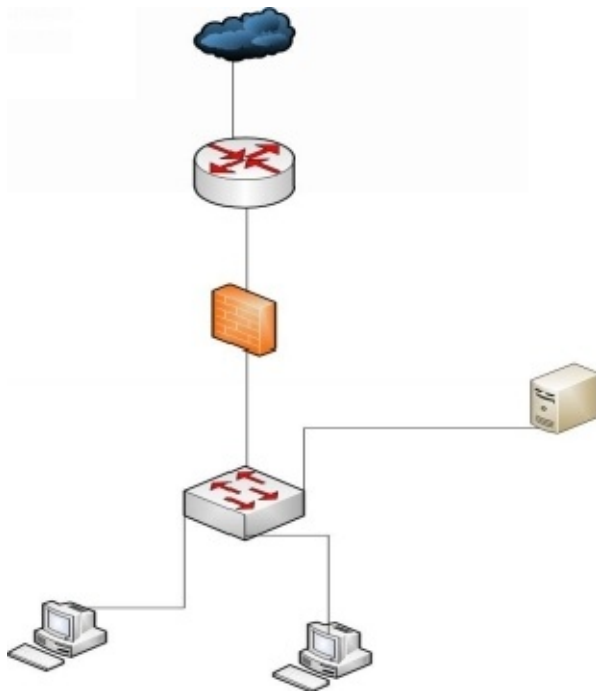
Which of the following parameter is not used for routing an inbound IP packet

- a. Destination IP address in the IP packet
- b. Route entry in the router
- c. Default route entry in the router
- d. Subnet mask of the sender of the packet

Answer –d

When an IP packet arrives on a router, the destination IP address is looked into, following by route entry and if the route entry is not available, the packet is sent through the default route. The subnet mask is not send or inserted in the IP header.

The following questions are based on the below topology. A firewall is setup behind a router. On the network, there is also a server which is available to be accessed by users on the internet.



Question 70

What type of firewall is to be used if access control has to be configured for users accessing the server based on IP address.

For basic access control based on IP address, a packet filter firewall would suffice. Access control lists can be configured which would permit or deny the required IP address or networks.

Question 71

In the above topology, it is required that users from the internet access only a specific application. What type of firewall and features can be used?

Every application has a specific port number. For ex, https uses TCP port 443, HTTP uses TCP port 80 etc. A packet filter firewall like a Cisco IOS router can be used to configure an access control list which would allow only the required port and deny the rest.

Question 72

What type of firewall is to be used for mitigating application layer attacks

on the server.

An application layer firewall or a deep packet inspection firewall which has the capacity to scan malicious content / signatures can be used for the purpose.

Question 73

It is required that users from the internet access only the required service on the server, but should not have access to the LAN network. What should be done.

A DMZ (De-Militarized Zone) has to be setup. The server should be placed in the DMZ. Appropriate ACL should be configured on the firewall which would permit access to the required application and deny access to the LAN network for internet users.

Question 74

It is required that users from the internet should not be able to ping the firewall. All ping requests should be dropped. How can this be achieved.

An access control list which denies ICMP requests can be configured on the firewall. Ping uses ICMP. When internet users pings the firewall IP address, the ping packets would be dropped and a response would not be sent.

Question 75

If the firewall is a statefull and a user on the LAN network access a website on the internet, which fields would be used for tracking the packet

HTTP uses TCP. Statefull firewall keeps track of the source and destination port, sequence and acknowledges numbers for TCP based connection.

% End of questions based on diagram %

Question 76

If a PC has two default gateways, which would be taken for routing the packets.

Every route entry would have a metric. If there are two default gateways, there would be two default entry. The entry which has a lower metric value would be taken by the packets.

Question 77

Is a DNS IP address mandatory to be configured on a PC for internet access.

When a user on a PC accesses a website, URL resolution for the website name has to be performed. This is done by the DNS protocol. This request has to be sent to a DNS server, for which the IP address of the DNS server should be configured on the client.

Question 78

How can the usage of RIP v2 improve the performance of a network w.r.t Rip v1.

Rip v2 is multicast as opposed to RIP v1 which is broadcast. Broadcast traffic would degrade the performance of a network, since packets are sent to all nodes as opposed to multicast which sends only to the required nodes.

Question 79

Name two methods by which the desktop of a Windows system can be viewed.

Remote desktop protocol or VNC can be used for the purpose.

Question 80

Name one technique which can be used for identifying existing IP addresses on a LAN network.

NMAP which is a scanning tool can be used to perform a scan on the network which would display the list of available IP addresses on the network. NMAP arp ping scan can be used for the same.

Question 81

Can the username and password sent from a HTTP client be viewed in clear text on the server.

HTTP does not encrypt data. This would cause the username and password to be viewed in clear text on the server.

Question 82

Can a FTP server installed on Linux accessed by a FTP client on Windows.

FTP is a TCP/IP protocol. TCP/IP is a vendor neutral protocol. So a FTP client

on Windows can access the FTP server which is installed on Linux.

Question 83

If there are two default routes on a Cisco router, which path would the packet take.

The packet would take the route which has a lower metric value associated with it.

Question 84

Explain a practical scenario where port mirroring can be used.

Port mirroring is a feature which is used on switch to monitor traffic on respective switch ports. A useful scenario would be to monitor packets which are flowing through a router which is connected to a switch to analyze the traffic distribution. For this purpose, a system with a protocol analyzer can be configured and the port mirrored to capture and analyze packets flowing through the router.

Question 85

How can the number of TCP connections be viewed on a Windows system.

netstat command can be used for the purpose. The command netstat -p tcp would display all tcp connections on the system.

Question 86

What is the use of a floating static route on a Cisco router

A floating static route is used as a back up for a primary static route. This is used in scenarios where a back route is configured for the network. The routing table is populated with the floating static route entry only when the primary route fails and is not available in the routing table.

Question 87

If there are multiple paths to a network on a Cisco router with RIP and OSPF, which path would the packet take and why.

The packet would take the path with a lower administrative distance, which in this case would be OSPF, the value of which is 110. The AD of RIP is 120.

Question 88

If there are multiple paths to a network on a Cisco router with static route and OSPF, which path would the packet take and why

The packet would take the path with a lower administrative distance, which in this case would be static route, the value of which is 1. The AD of OSPF is 110

Question 89

Does the routing table of a router needs to be configured for directly connected networks.

Directly connected networks are populated automatically by the router based on the IP address and subnet mask configured on it. It is not required to be configured additionally.

Question 90

Explain two methods by which two IPSEC routers can authenticate with each other.

IPSEC routers can be authenticated using pre-shared keys or using digital certificates.

Question 91

Explain how access to FTP server on a network can be restricted using a firewall.

An access control list can be configured on the firewall which would block access to FTP server ports which are TCP port 20 and 21.

Question 92

Which feature would allow a VLAN to be sent untagged on a trunk port.

The VLAN can be configured as a native vlan. VLAN's which are configured as native vlan are not sent tagged over the trunk port.

Question 93

How can the basic working of the functionality of an application on a server checked from a remote location.

Network applications works on port numbers. When an application is installed on a system, the appropriate port would be open. If the application is not

running, the port would be in closed state. A port scanner like nmap can be used for checking the appropriate port is in open or closed state.

Question 94

Name two reasons as to why ping response is not received from the destination

The ping can fail if the destination is shutdown or it can also be a firewall on the destination blocking the packet.

Question 95

How can a FTP server residing on a LAN network accessed from a PC on the internet. Assume that the LAN network has an internet connection using a router.

Port forwarding feature can be used to achieve the functionality. Port forwarding feature can be configured on the router to forward all requests to TCP port 20 and 21 which are used by FTP servers to the appropriate LAN IP address of the FTP server. Users can then FTP into the public IP address of the router which is connected to the internet. When the router receives the request, it forwards to the internal FTP server IP address.

Question 96

How can the desktop of a Linux system viewed from Windows.

VNC protocol can be used for the purpose. The Linux system can be setup as a VNC server and Window as the VNC client. The IP address of the Linux system can be configured in the VNC client, following which connectivity can be achieved.

Question 97

Explain a technique by which web access can be blocked on a network with a firewall.

An ACL can be configured which would block DNS packets originating from the network. DNS is used for resolving URL into IP address. If DNS is blocked, web communication would fail.

Question 98

How can web access be blocked for a specific group of users on a network with a firewall.

Create two networks to segregate users. Map 1 network with users which are allowed and the 2nd network with users which are not allowed. Create an ACL which would deny access to DNS for the 2nd network. As DNS is blocked, web access would not be allowed for the respective network.

Question 99

Which feature on a router can be used to block access to known websites.

URL filtering is a feature which is available on routers where the URL name of the websites can be provided and access to the same can be blocked.

Question 100

Does HTTPS use TLS/SSL protocol at the transport layer

HTTPS uses TCP at the transport layer. TCP port 443 is used. TLS/SSL is used by HTTPS for encrypting the data exchanged.

Question 101

Why should mac-filtering not be used as a security defense mechanism on wireless networks.

Mac-filtering is a feature which would allow the mac-address of wireless units on a network to be configured for allowing or denying access to the network. Wireless communication is a shared medium. Anyone with a protocol analyzer can view the mac-addresses on a network. The valid mac-addresses can then be used by hackers to gain connectivity to the network, by using spoofing techniques. This makes mac-filtering vulnerable, due to which it is not recommended.

Recommended Book

250 + Network Engineer Interview Questions & Answers

[Click to view details in Amazon \(Ctrl +P\)](#)

Question 102

How can a DHCP starvation attack be mitigated on a switch.

DHCP starvation attack occurs when an attacker sends multiple requests to the DHCP server impersonating different clients. To mitigate this, port-security can be configured which can be used for limiting the allowed number of mac-addresses on a switch port.

Question 103

Explain two access control techniques by which a router on a LAN can be configured for access only for the network admin.

Appropriate username and password can be used for the admin. An ACL can be configured which would allow only the IP address of the admin PC for access.

Question 104

What will a router do if it receives an IP packet with TTL value 2.

The router would decrement the value by 1 and forward the packet to the next hop.

Question 105

Which protocol is not used by IPv6 compared with IPv4 for identifying the mac-address of a peer.

The ARP protocol is used by IP v4 to detect the mac-address for a specific IP address. IP v6 does not use ARP.

Question 106

How can an admin configure only SSH protocol for remote access on a Cisco router.

The admin can configure an ACL which would allow only TCP port 22 for SSH and deny all other access.

Question 107

Can two vlans be assigned with two subnets from the same major network.

Vlans are used for segregating networks. So two subnets irrespective of whether they are from the same or different major networks can be used with two vlans.

Question 108

Give a practical instance where static NAT is configured on a router.

Static NAT is used in a scenario where a server which is residing on a LAN network needs to be accessed from users on the internet. In this case, the server would have a public IP address which would be mapped with the private IP address using static NAT.

Question 109

Which port number would you open on a firewall to allow access to a Windows remote desktop server on the LAN network.

Windows remote desktop servers work on TCP port 3389, which should be opened on the firewall for access.

Question 110

How can packet drops on a network be tested by using ping.

100 ping packets can be issued to a system on the network. On a Windows system this can be achieved by the use of command `ping -n 100 192.168.2.1`, where 100 suggests the number of packets and 192.168.2.1 is the system which is being pinged. The output can be analyzed to see how many ping responses have been lost, which would correspond to the packet loss.

Question 111

Will a router forward DHCP Discover packet

DHCP Discover is a broadcast packet. Routers do not forward broadcast packets.

Question 112

A user configures the internet firewall to block incoming IP packets originating from the subnet 192.168.1.0/24. What type of filtering is being performed.

An ACL configured to block inbound packets is termed as ingress filtering. Egress filtering is used for outbound packets.

Question 113

A user has an http proxy configured on the browser. He attempts to open the website www.tcpipguru.com on the browser. The IP address of the proxy server is 192.168.1.1/24 and the port configured is 80. How will the TCP connection from the user established with the website.

When the user initiates the connection to the website, a TCP 3 way connection is initially established with the proxy server which is 192.168.1.1. The proxy server would then, on behalf of the user, would initiate a TCP 3 way handshake with the website server. This process is transparent and the user is not aware of the same.

Question 114

Three switches sw1, sw2 and sw3 transmit STP BPDU packets with the following info in the Bridge ID. Which switch will be elected as the root bridge

sw1 : Bridge priority 3456, Mac-address : 00:1b:78:ab:9f:91.

sw2 : Bridge priority 1234, Mac-address : 00:1b:78:ab:9f:92.

sw3 : Bridge priority 2345, Mac-address: 00:1b:78:ab:9f:93.

STP protocol elects the switch with the lowest priority as the root bridge. Sw2 would be elected as the root bridge as it has the lowest priority.

Question 115

A switch port operating in full duplex mode is connected to a PC operating in half duplex. What would be the effective duplex settings for the communication

The effective duplex setting would be half duplex as a full duplex system cannot communicate as full duplex when the peer is operating in half duplex.

Question 116

In an 802.1q encapsulated ethernet frame, which field contains the value of the upper layer protocol

802.1q frames are used for carrying vlan tagged frames. The 802.1q header is inserted in the ethernet frame. The ethernet frame contains a field called type value which would indicate the type of upper layer protocol like IP, IPX etc.

Question 117

A 24 port switch receives a frame with destination mac-address unknown. To how many ports will the frame be flooded

When a switch receives a frame with an unknown destination address, it would flood the frame to all ports on it apart from the port on which it was received. So a 24 port switch would flood it to 23 ports on the switch.

Question 118

What would happen if the source and destination mac-address in an ethernet frame received on a switch port is the same.

The switch would filter the frame and discard it.

Question 119

A PC which is connected to switch port 23. The switch has learned the mac-address of the PC. The port is now shutdown. Will the switch retain the mac-address

The switch will not retain the mac-address. When the port is shutdown, the mac-address would be removed from the mac-address table of the switch.

Question 120

Explain a scenario where ARP protocol is not used to find the mac-address of the destination IP address

ARP protocol is not used on point to point links like a point to point WAN connection using PPP serial links.

Question 121

What would happen if an attacker sends a spoofed ARP response packet to a device

ARP is a stateless protocol which means that if a device receives an ARP response, there is no mechanism to check if an ARP request was actually sent earlier. This makes it possible for attackers to spoof ARP response packets and update the ARP table of the device with the info in the spoofed packet

Question 122

An attacker tries to spoof the IP address of a peer which is on the same local Ethernet segment but receives a Duplicate IP address message. Which protocol is responsible for the Duplicate IP address identification

Gratuitous ARP is a type of ARP packet which would have the Sender and Target IP address as itself. When a PC on the network receives this packet and if the Target IP address is the PC's IP address, it would reply stating that the Target IP address is already on the network and is in use. This would trigger the duplicate IP address message.

Question 123

Two PC's, PC1 and PC2 are deployed on different vlan's , vlan 3 and vlan 4 respectively on a layer 3 ethernet switch. Each of the vlans are configured with respective IP addresses. What should be the IP address of the default gateway of TCP/IP adapter setting of PC1 to communicate with VLAN 4.

PC1 should be configured with the IP address of VLAN 3. This would ensure that all packets to vlan 4 would be sent to the default gateway, where it would be forwarded to PC2, which is on VLAN 4.

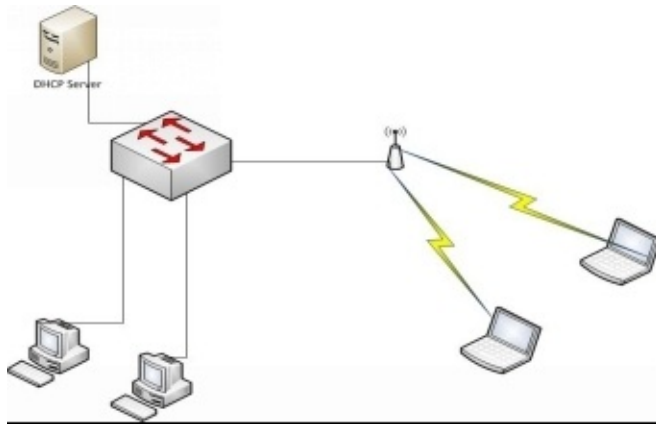
Question 124

On a network, a computer is connected to a switch, which is connected to a router. The router is connected to the internet. DNS server IP address is configured on the router, but not on the computer. If the computer pings a website name (Ex: ping www.tcpipguru.com), would a response be received

Since the DNS server is not configured on the computer, the website name would not be resolved into an IP address. The ping would ultimately fail. To be successful, the DNS server IP address should be configured on the computer.

Question 125

On a network, a DHCP server is available to provide ip addresses to desktop computers on the network. An access point is additionally setup and integrated with the network as shown in the diagram. Is it required to setup an additional dhcp server for providing ip addresses to the wireless users



It is not required to setup an additional DHCP server on the network. The existing DHCP server can be used provide dynamic ip addresses to the laptop users.

Question 126

On a layer 2 switch, port 1 is a member of vlan 2 and port 2 is a member of vlan 3. Two computers, PC1 and PC2 are connected to the ports. The IP addresses of the computers are 192.168.1.2 /24 and 192.168.1.3/24. Both the computers belong to the same network address of 192.168.1.0/24. If PC1 pings PC2, would a response be received.

A response would not be received. Although both the computers belong to the same network address of 192.168.1.0/24, they are connected to ports on the switch which are members of different vlans. For communication between vlans, a router is required.

Question 127

A switch port receives a broadcast frame (FF-FF-FF-FF-FF-FF) as the destination mac-address. What action would the switch perform when it receives the frame

The mac-address FF-FF-FF-FF-FF-FF is a broadcast mac-address. When a switch receives the mac-address it will broadcast it to all ports. This mac-address would not be learned or stored on the switch.

Question 128

A unmanageable layer 2 switch has 5 PC's connected to its ports. As part of firmware upgrade, the switch had to be restarted. What would happen to the mac-addresses available on the mac-address table of the switch

The mac-address table of a switch is volatile, which implies that the mac-address info is not saved and would be flushed on every reboot and will be learned again. In some Manageable layer 2 switches, static mac-addresses entries can be configured which would be persistent after reboot.

Question 129

An internet router fragments an IP packet and forwards it to its default gateway. Where the fragmented IP packet would be reassembled

The fragmented packet would be reassembled at the destination

Question 130

Which value in an IP header is not usually checked by a router but can optionally be configured

The source IP address in the IP header is not checked by the router. IP source-route feature can be optionally configured on the router to check the authenticity of the source, in which case the router looks into the source IP address information .

Question 131

Which of the following fields in an ethernet frame would be modified when it moves from port 1 to port 2 of a switch

When an Ethernet frame is generated, the destination mac-address would be the recipient's mac-address and not the switch ports address. When the frame passes through the port, none of the fields would be modified.

Question 132

What would the value of protocol field in a IP header in which the data is a HTTP

The protocol field in the IP header denotes the protocol which is present in the upcoming layer (transport layer). HTTP is the application protocol but TCP is

the protocol at transport layer for which the value in the IP header would be denoted as 6

Question 133

Two browser windows are opened on a PC and the webpage www.tcpipguru.com is accessed simultaneously. What would be the destination port number used by both the connections.

The destination port number would be TCP port 80, as both connections are initiated to the web server on which tcpipguru.com is hosted.

Question 134

If the IP address 192.168.1.0/31 was valid and usable, what would be the broadcast address for the network

The broadcast address for a network is the value when all the host bits is set to 1. In this case, the number of available host bits is 1 (31 bits are reserved for the network address) So setting the last bit of the network address to 1 (192.168.1.00000001) the value become 192.168.1.1.

Question 135

A router which supports classfull addressing receives an IP packet with destination IP address as 192.168.2.5. How many bits in the first octet of the destination IP address would be checked by the router to determine the class

Identification of a class C IP address is performed by checking the first three high order bits in the first octet of an IP address. If the first two bits are set to 1 and the third bit is set to 0 then it is a class C address

Question 136

What would be the value in the protocol field in an IP header which has DNS as the application data

The protocol field in the IP header denotes the protocol which is present in the upcoming layer (transport layer). DNS is the application protocol but UDP is the protocol at transport layer for which the value in the IP header would be denoted as 17

Question 137

What is the subnet mask in a routing table of a router used for

It is used to identify the number of interesting bits which should be looked up in the destination IP address in an IP packet. Let's take an example. Assume that an IP packet has arrived with the destination IP address as 192.168.1.5.

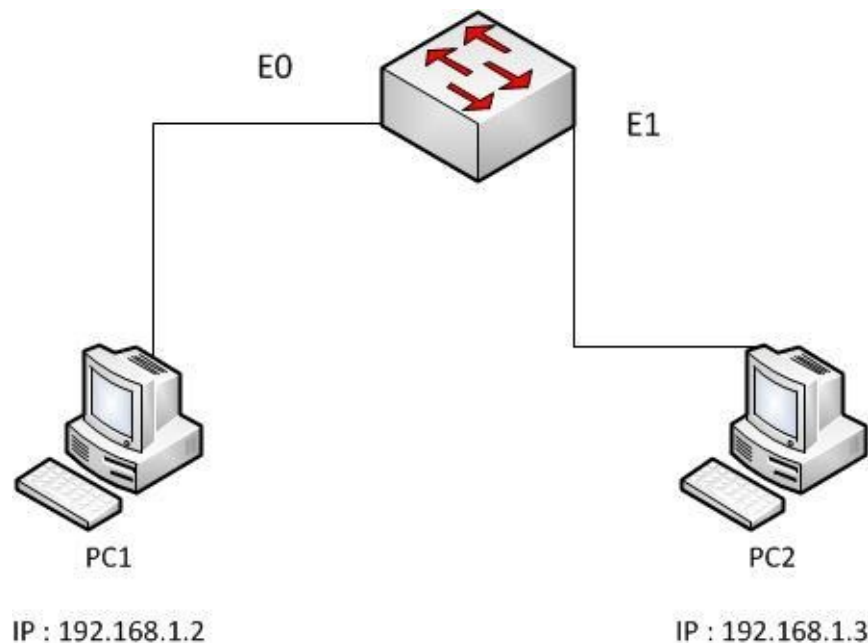
The route table contains the following entry.

192.168.1.0 255.255.255.0.

192.168.1.5 would be "And ed" with 255.255.255.0 and determined that the destination IP address is a member of the 192.168.1.0 network.

Question 138

What happens to a frame that has been tagged.

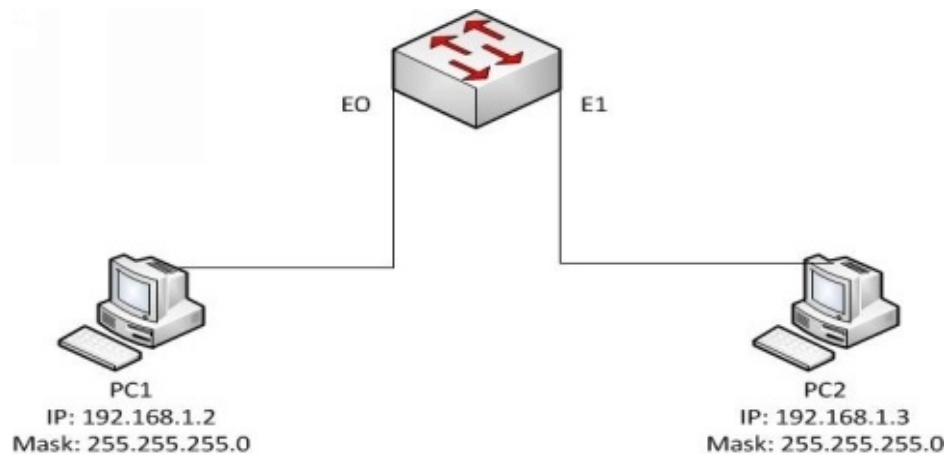


When PC1 sends a packet to PC2, the frame encapsulating the IP packet, does not contain information related to the vlan it belongs to. When the frame is tagged, the vlan information is inserted as an additional field, which is appended with the generic ethernet header. This information is typically used by the switch, to understand which vlan the frame belongs to.

Question 139

What happens when a switch receives a frame.

In the below diagram, PC1 pings PC2. The IP packet is encapsulated using an ethernet frame and is sent to the E0 interface on the switch. The frame has the source mac-address as the mac-address of PC1 and the destination mac-address as PC2



The switch looks into the source mac-address inside the frame. If it is unavailable on the cam table of the switch, the switch adds the information in the table. The switch then looks into the destination mac-address, and checks for the corresponding information in the cam table. If unavailable, the switch uses a technique called flooding, where the frame is sent out to all ports. When PC2 responds, the destination mac-address of PC2 is added to the corresponding port and the cam table updated. For subsequent packets, the frame is not flooded, but sent directly to E1 since, the information is already available in the cam table.

Question 141

What is the use of spanning tree protocol.

The spanning tree protocol is used to prevent layer 2 loops. Frames do not have a loop prevention field inside the header, unlike IP headers, which has a TTL field which is used to prevent looping of IP packets. For this purpose, the spanning tree protocol is used. The spanning tree protocol is a layer 2 protocol which is implemented on switches and used to prevent looping of frames.

Question 142

Is a frame with destination mac-address as FF-FF-FF-FF-FF-FF

broadcasted or flooded

Broadcasting is the technology where a frame is identified based on the destination mac-address of the frame and then sent to all ports in the domain. In flooding, the frame is also sent to all ports in the domain, but not based on the destination mac-address. Flooding is performed when the destination mac-address is unknown in the mac-address table of the switch. The destination mac-address of FF-FF-FF-FF-FF-FF is identified as a broadcast frame. This mac-address is not learned by the switch or updated in the mac-address table.

Question 143

What is the difference between tagged and untagged VLAN

Take a scenario where a switch port is a member of untagged vlan 2 and tagged vlan 3 and vlan 4. The generic design of the switch states that a port can be a member of only 1 untagged vlan and multiple tagged vlan. Assume that the switch port is connected to a hub, on which there are three PC's. PC1 is a member of vlan 2, PC2 is a member of vlan 3 and PC3 is a member of vlan 4. When the data from the PC's (ethernet frames) reaches the switch port, the switch would consider that all the frames are members of vlan 2, since the port is a member of untagged vlan 2. So how can we differentiate. The network cards on PC2 and PC3 should be configured with 802.1q tagged frames with the appropriate vlan numbers as 3 & 4. When this is configured, the data (frames) send by PC2 and PC3 would be 802.1q encapsulated with the appropriate vlan numbers. This is known as tagged frames. When the tagged frames reach the port on the switch, the differentiation can be made by looking into the value (3 or 4) inside the frame. Earlier since the frames were not tagged, the differentiation was not possible making the switch believe that all traffic belonged to untagged vlan 2.

Question 144

What is the difference between flooding and broadcasting on a switch port

When a switch receives a frame, and if the destination mac-address of the frame is unknown (not available in the mac-address table) the switch would "flood" the frame to all ports, which means a "copy" of the frame is send to all ports.

Broadcast frames has the destination mac-address has all F (FF-FF-FF-FF-FF-FF)

This characteristic is specific to the frame. Examples of broadcast frames are

ARP, DHCP Discover etc. When these frames are received on a switch port, the frames are "broadcasted" to all the ports since the destination mac-address is of type "broadcast". The destination mac-address of broadcast frame (FF-FF-FF-FF-FF-FF) is not added to the mac-address table.

Question 145

Explain in detail, the difference between hub and switch.

Hubs work on layer 1. They do not understand frames. So irrespective of whether it is a unicast or broadcast frame, the traffic would be broadcasted to all ports making the network slow and insecure, since data intended for a recipient is sent out to all ports.

Switches do not use a shared medium as opposed to hubs. Computers connected to a switch port can transmit data simultaneously without having the need to wait for other PC's to complete data transmission.

Question 146

What happens when a vlan is configured as native vlan.

When a vlan is configured as native, it implies to the switch that traffic originating from the specific vlan should not be tagged (Inserted with additional 802.1q or ISL header) and it should pass through the trunk as a normal ethernet frame.

Question 147

What is a directed broadcast

All F on a layer 2 address is a broadcast. For example, a DHCP request has the destination IP address as 255.255.255.255 and the corresponding layer 2 mac-address would be FF-FF-FF-FF-FF-FF. Let's say we ping whole range of a subnet, how do we do that ?? Take an example of 192.168.1.0 /24. The broadcast address of "this" subnet would be 192.168.1.255 (all 1's in the host). If we ping 192.168.1.255, that is also a layer 2 broadcast, but directed towards all the hosts in the specific subnet.

Question 148

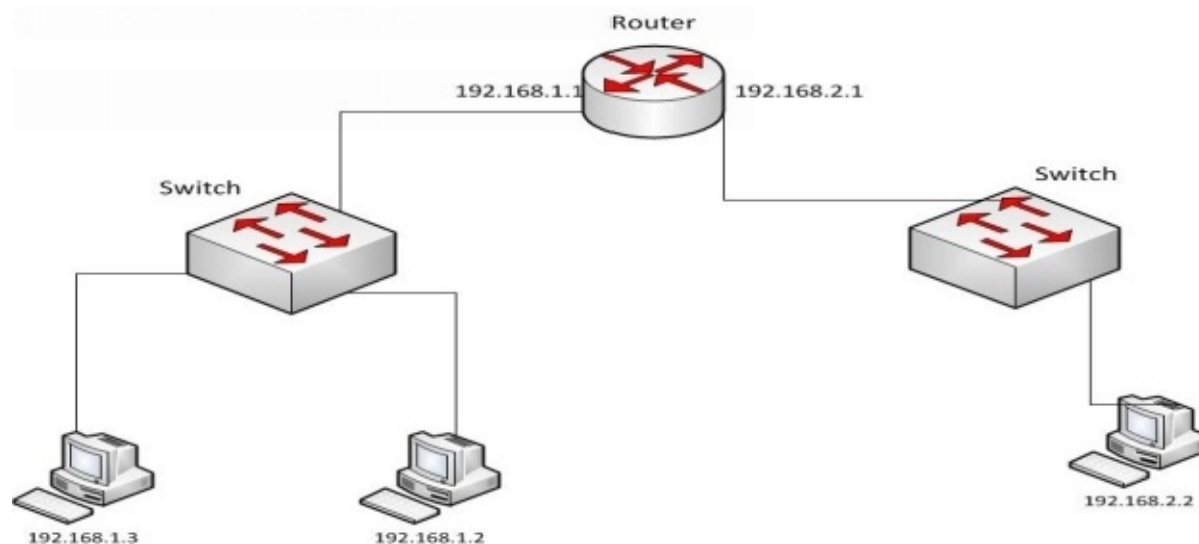
What is the use of a VLAN.

When a VLAN supported switch is used, two LAN's can be created on a single switch. Since two LAN's need to be created, we create two VLANs on the

switch, vlan 2 and vlan 3, where LAN 1 is logically mapped with vlan 2 and LAN 2 is logically mapped with VLAN 3. The ports to which computers in LAN 1 connect to are made members of vlan 2, and ports to which computers in LAN 2 connect are made members of vlan 3. In this way, two LAN's which were earlier created with two separate switches, are now created and setup on a single switch. As it can be observed from the above example, when vlans are used, manageability becomes simpler and also reduces the number of switches required to setup multiple LAN networks.

Question 149

In the below diagram, explain how a packet from 192.168.1.3 to 192.168.2.2 reaches the router from the switch.

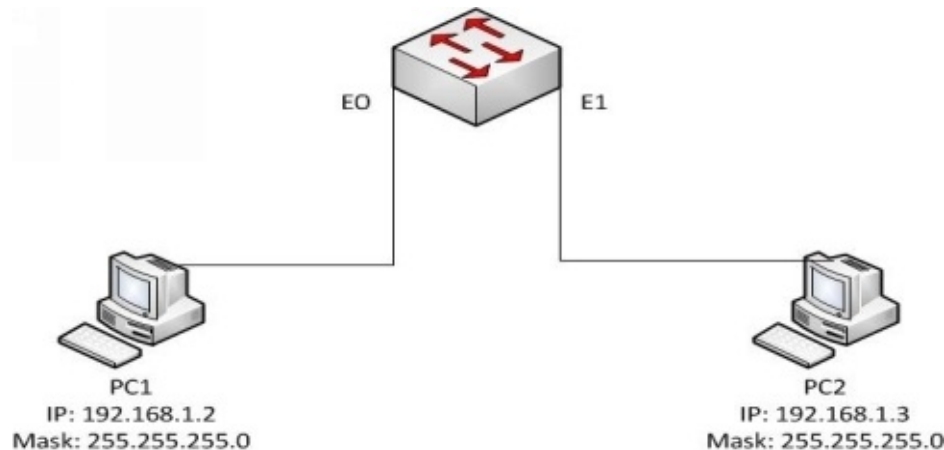


The packet, which is sent, is encapsulated in an ethernet frame which would contain the source mac-address as the systems (192.168.1.3) mac-address and the destination mac-address as the routers interface (192.168.1.2) mac-address, as packets bound for a different network is sent to the router. When the packet reaches the switch port, which is connected to the 192.168.1.3 system, the switch looks into the destination mac-address in the frame. The switch does not look into the IP packet, as it does not have the capacity to perform the same. After understanding the mac-address, it checks in its mac-address table for a match.

After identifying the port number on which the router is connected, the frame encapsulating the packet is forwarded to the appropriate port and further processed by the router.

Question 150

What happens if the destination is shutdown on a switch.



In the above topology, PC2 is shutdown. PC1 pings PC2. The first requirement in sending out the packet from PC1 is to identify the mac-address of PC2, for which, PC1 sends an ARP request. PC1 waits for an ARP reply. Since PC2 is shutdown, the ARP reply is not send, and the ARP request times out. So the packet is never sent out from PC1. In a second scenario, the ARP cache in PC1 contains the mac-address of PC2. In this case, the packet (icmp) is constructed and sent out from PC1. Since PC2 is shutdown, the reply is never sent and ultimately the packet times out.

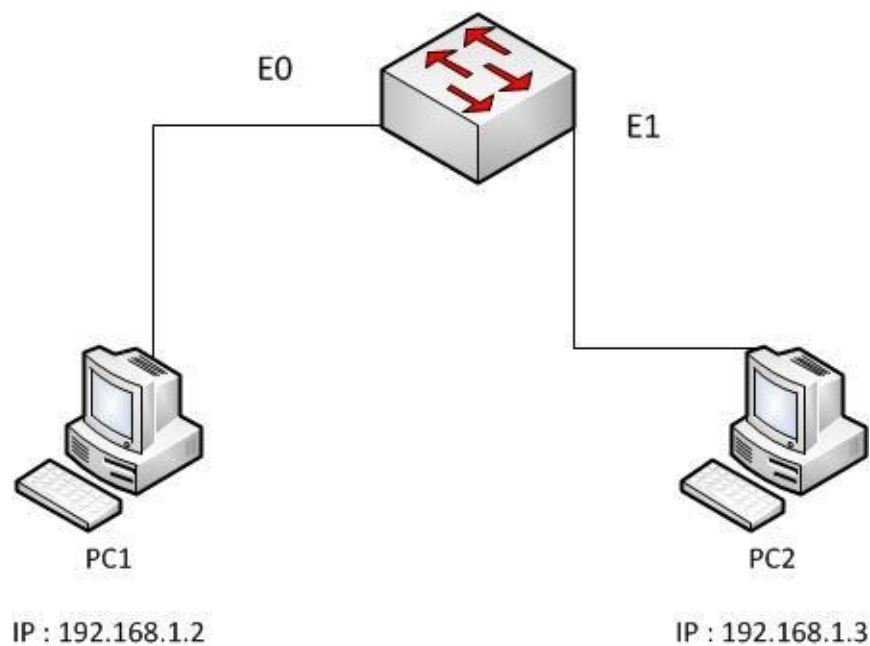
Question 151

What happens if a frame arrives damaged.

When a device , like a computer or a router receives a frame, the network card , which receives the frame, verifies the FCS value in it. The FCS value of the frame is calculated and inserted by the initiator. If the frame has been damaged in transit, the value would differ, when the FCS value is recalculated. If the FCS value differs, the frame is discarded by the recipient.

Question 152

How do two computers connected to a switch communicate with each other.



In the above diagram, PC1 pings PC2. An IP header with the source and destination IP address as 192.168.1.2 and 192.168.1.3 is created. PC1 sends an ARP request frame to find the mac-address of PC2. This is required to construct the ethernet frame to encapsulate the IP packet. After the mac-address of PC2 is received, the frame is constructed and the IP packet encapsulated. The frame is sent to the switch and is received on port on E0. The switch looks into the destination mac-address in the frame, which is PC2's mac-address and checks if the entry is available in it's mac-address table. If yes, the frame is forwarded to the port on which PC2 is connected. If unavailable, the switch floods the frame to all ports. After PC2, receives the frame, it looks into the destination mac-address to check if the frame is intended for itself. Once verified, the destination IP address is verified with it's own IP address. As it is a match, the ping packet is processed and the response to the ping packet created. The response packet would contain the source IP address as 192.168.1.3 and the destination IP address as 192.168.1.2, and a new frame would be created with the source and destination mac-address as PC2 and PC1 respectively.

Question 153

What is the use of TCP 3 way handshake.

TCP based clients and servers use the TCP 3 way handshake for establishing communication. The TCP 3 way handshake provides the first level of reliable communication which is guaranteed with TCP based applications. The client and the server uses the TCP 3 way handshake to guarantee that both the parties are up and running before data transfer. Sequence and Acknowledgement numbers which are required for tracking the data which has been sent and received are initially exchanged between the client and the server during the TCP 3 way handshake.

Question 154

How do two computers on different subnets communicate.

The network 192.168.1.0/24 has been sub netted. PC1 belongs to the 192.168.1.32/27 network and PC2 belongs to the 192.168.1.64/27. The IP address of PC1 is 192.168.1.33 and that of PC2 is 192.168.1.65. When PC1 pings PC2, the destination IP address, which is 192.168.1.65, is 'AND ed' with the subnet mask. The result would yield the address 192.168.1.64, which signifies that it is a different network address from the initiator's address. So to communicate with PC2, a router, which would be the default gateway for PC1 would be required.

Question 155

How do computers on the internet communicate.

Computers on the internet communicate using public IP addresses. On the internet, the identity of a computer is its public IP address. When a user is trying to access a website, the URL name is actually an IP address, which is resolved using DNS servers.

Question 156

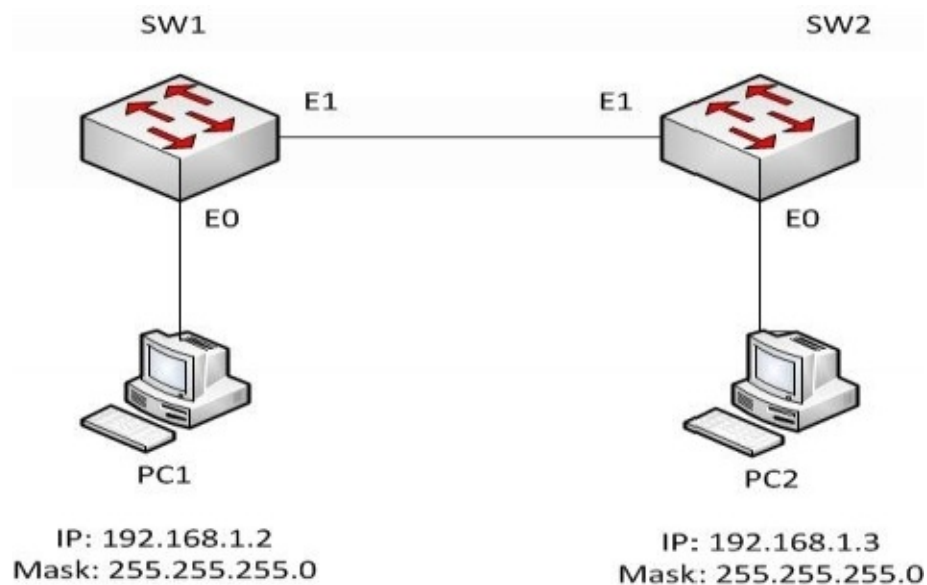
What is the difference between unicast and broadcast traffic

Unicast and broadcast traffic occurs at Layer 2 and Layer 3 of the OSI model. ARP (Address resolution protocol) is a layer 2 broadcast traffic, whereas DHCP (Dynamic Host configuration protocol) is a Layer 3 broadcast. ARP is a layer 2 protocol and does not have a layer 3 header. The destination mac-address of a layer 2 broadcast frame is FF-FF-FF-FF-FF-FF. The destination IP address of a Layer 3 broadcast IP packet is 255.255.255.255. The corresponding destination mac-address in the frame which carries the layer 3 broadcast traffic is FF-FF-FF-

FF-FF-FF. In Unicast traffic, both the destination IP address and the destination frame (On a Non-routed Segment) would be the actual value of the destination's IP or mac-address. Take a scenario where there are 3 PC's, PC1, PC2 and PC3 connected to a switch. The PC's are configured with IP addresses 192.168.1.1 /24, 192.168.1.2 /24 and 192.168.2.1 /24. If PC 1 sends unicast traffic to PC2, then the mac-address of the frame would be PC2' mac-address and the destination IP address in the IP packet would be PC2's mac-address. If PC1 sends a layer 2 broadcast, it would be received on all ports on the switch , including PC3 , which is on a different IP network. If PC1 sends a layer 3 broadcast, it would also be received on all ports on the switch, because, the destination mac-address in the frame carrying the layer 3 broadcast IP packet is broadcast. This is the scenario where one should use VLAN (Virtual Lan) such that broadcast traffic intended for one network would not reach the other network.

Question 157

How do computers connected to two different switches communicate.



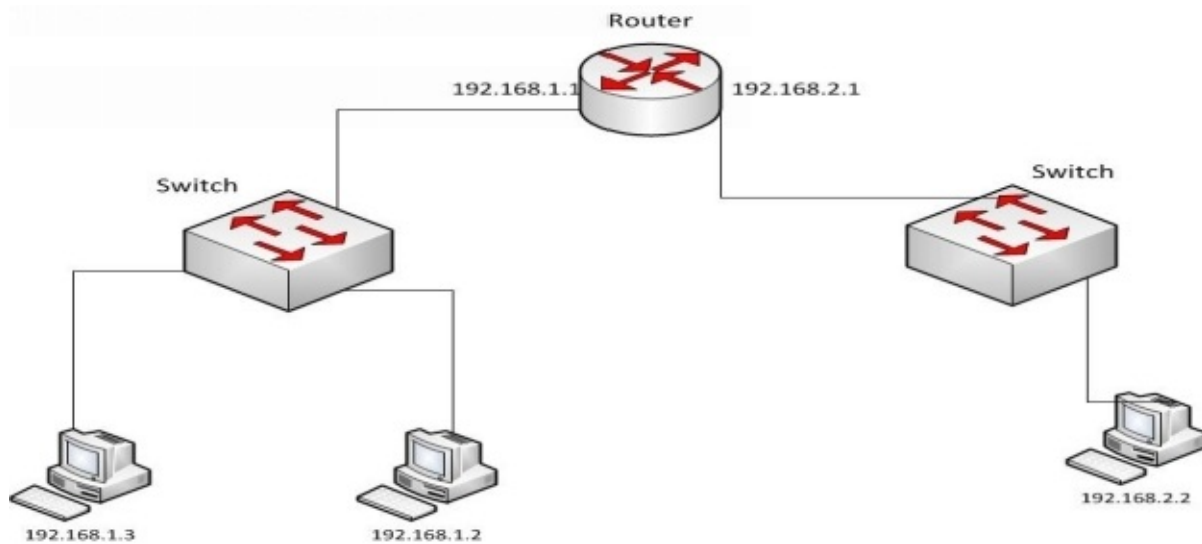
In the above diagram, PC1 and PC2 are connected to respective ports on the switch as shown below. The switches are connected to each other using the E1

ports on the respective switches. When PC1 pings PC2, an ARP request packet is generated, for identifying the mac-address of PC2. The ARP request packet is a broadcast packet, which is broadcasted to all ports on SW1. The ARP packet would be sent through the E1 interface on SW1, reach the E1 interface on SW2 and eventually reach PC2. PC2 would respond with it's mac-address to PC1. Now on SW2, the mac-address of PC1 is added to the E1 interface on SW2, as it had received the ARP request through the interface, which had the source mac-address as that of PC1. This information would be updated in the cam table of SW1. The ARP reply would be sent out through E1 on SW2 and E1 on SW1 and eventually would reach PC1. The next time PC1 pings PC2, the cam table of the switch would list the mac-address of PC1 on E1 on SW1. All packets would be sent to E1 on SW1, which would then be forwarded out to SW2.

Question 158

Can the default gateway be on a different subnet.

The default gateway should always be on the same network or subnet on which a PC is configured. In the below diagram, the default gateway for the systems on the network, 192.168.1.0/24 should be 192.168.1.1 and not 192.168.2.2. This is because, systems on the 192.168.1.0/24 network uses the gateway to reach systems on different networks. So the gateway should be a device which should be aware of both the networks, and the gateway for a system on the 192.168.1.0/24 network should be an IP address on the specific network or subnet.



Question 159

How does an application know as to which protocol is to be used at the transport layer

Applications are binded to transport later protocols. An application designer is the responsible authority for selecting the transport layer protocol (TCP or UDP) .For example, FTP uses TCP, HTTP uses TCP , TFTP uses UDP. When a FTP or HTTP based application is initiated on an operating system which implements TCP/IP, TCP would be used, since the application protocol is designed to work on the top of the specific transport protocol which is TCP

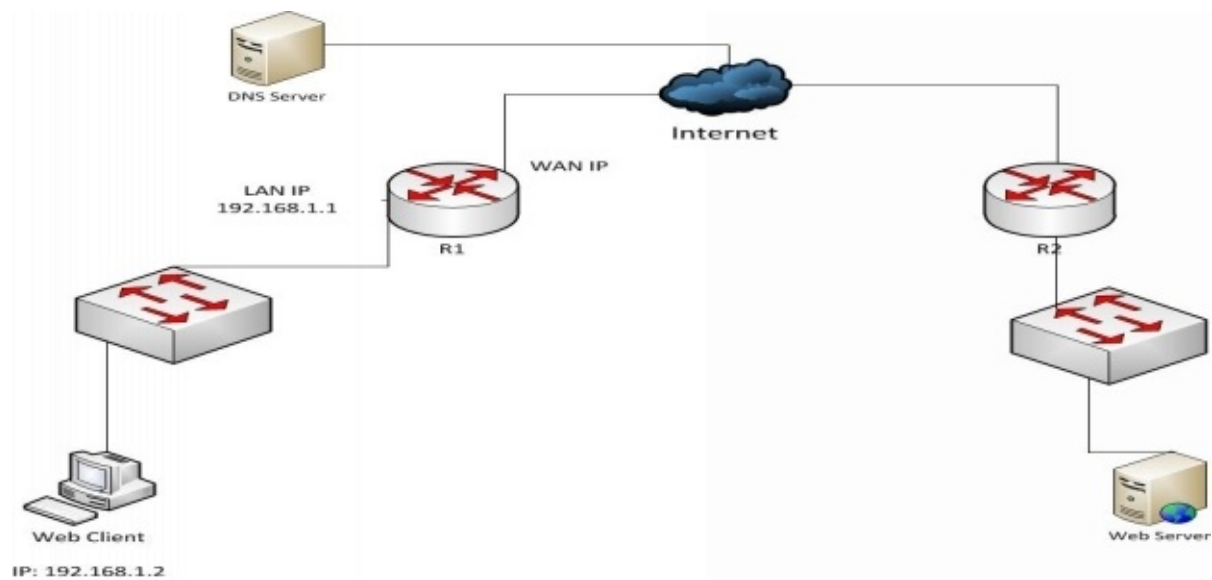
Question 160

What is TCP 4 way handshake

The TCP 4 way handshake is initiated when the application completes the data transfer. For example assume that a user has initiated a FTP connection to upload some files. Once the file upload is completed, the TCP session handling the FTP data would initiate a 4 way handshake from the client to the server signifying that the data transfer is complete and the session can be closed. If the server sending data (Download data from the client), the server would initiate the 4 way handshake to signify closure.

Question 161

What is the use of source port number.



Source port numbers is a field which is available in transport layers headers like TCP and UDP. This example explains the need of source port number in a TCP header. In the above diagram, assume that the web client opens two instances of a browser and access the website on the web server. The packet, which is sent from the web client, would contain the source IP address 192.168.1.2 and destination IP address as the web servers IP address. The source ports, in the TCP header would be unique and different for both the connections. If the source port number is not available, the web server would not be able to send a response to the appropriate browser instance, which has initiated the connection.

Question 162

What is the use of a destination port number.

The destination port number is used to identify the application, to which the connection needs to be established with. In the above diagram, when the web client opens the browser and attempts to access the website on the server, the destination port number 80 is used, which would be used the web server system to identify, which application the incoming packet is intended for.

Question 163

What happens when you ping a website

Take a scenario, where a user pings the website www.tcpipguru.com from a PC. On the PC screen from where the ping is issued, the reply is from an IP address and not from the website name www.tcpipguru.com. Network communications

are based on IP addresses and not domain names. When the command ping www.tcpipguru.com is typed, a DNS query is sent by the PC to the DNS server IP address which is configured on the TCP/IP adapter settings of the PC, to retrieve the IP address of www.tcpipguru.com. After the IP address is received, the ICMP request (Ping request) is sent to the IP address of the website to which the server sends a reply.

Question 164

What happens when a URL is typed in a browser

Take a scenario where you are accessing the internet at your home on your laptop. The laptop is configured behind a wireless router which is connected to the internet. You type http://www.tcpipguru.com on your browser. What exactly happens? The following are the list of events which happen before you see the home page of the website.

Type the URL on the browser. A DNS query is sent to the DNS Server configured on the TCP IP adapter settings of the laptop. The DNS server responds with the IP address of the website. (This is the IP address of the server which hosts the website). The TCP IP stack of the operating system initiates a TCP 3 way handshake with the IP address of the server. Once the handshake is successful, HTTP Get Message is sent by the TCP IP stack to the server. The server responds with the files and images of the home page of the website, which is displayed on the browser window.

Question 165

What is the main difference between TCP and UDP

Assume that there are two applications, application 1 and application 2. Application 1 uses TCP and Application 2 uses UDP. The client version of both the applications are installed on PC1 and the server version of both the applications are installed on PC2. If the application 1 client residing on PC1 wishes to send data to the corresponding server residing on PC2, it has to first establish transport layer connectivity. This transport layer connectivity is termed as the TCP 3 way handshake. Only after the handshake is successful, data can be sent. If the application 2 client wishes to send data to the corresponding server residing on PC2, then a transport layer connectivity is not required beforehand. The data can be sent instantaneously. Due to this, UDP is always a faster communication protocol.

Question 166

How does networking protocols work.

A protocol in computer networking can be defined as the 'language' for computer network communication. Whether you are browsing the internet, sharing files or printing a file, a network protocol is always involved. Network protocols are developed by protocol design and development engineers. Different protocols would be involved to achieve end to end computer network communication. All the network protocols that are involved are aggregated to form a suite or group of protocols is referred to as the 'protocol stack'. The protocol stacks are integrated as part of the Computers operating system.

Network protocols are broadly classified into the following

**Vendor neutral protocols **

These protocols are not dependent on the vendor. For example, if a computer network has to be setup between a mix of Windows and Linux machines, this protocol can be used. An example of a vendor neutral protocol is TCP/IP. Note: TCP/IP is a protocol stack, which is integrated as part of Windows and Linux operating system. Any operating system, can implement the TCP/IP stack.

Vendor dependent Protocols

These protocols are dependent on the vendor. These network protocols can only be used for network communication between computers or devices from the same vendors. Examples of vendor dependent protocols are IBM SNA Protocol, Cisco EIGRP. These network protocols are proprietary to the vendors and cannot be used on any other platforms apart from the vendor.

Question 167

What is a port number

A port number is a unique number which are used to identify network applications. Consider an analogy where, a person calls up an organization on the board telephone number, which is a unique number. Once the call is established, the automatic calling system would request the caller to enter the extension number to reach the required person. In networking, the board number and the extension number corresponds to IP address and port number. The concept of port numbers is explained in detail with the reference to the diagram below.

The PC with IP address, wishes to access the website www.tcpipguru.com. The website, is available on the Webserver.

What exactly is a website ? A website is a set of files , which are hosted (saved in a specific location on the hard disk) on the Web server. The IP address of the web server is to be known before the PC can establish connectivity to the Web server. This is done by the DNS resolution process. After , the DNS resolution process, the IP address of the web server is retrieved. Once the IP address is retrieved, the PC proceeds to establish connectivity to the IP address of the Web server. But the IP address here is like the board number. Every network applications would have a specific port number associated with it. There are client-server based networking applications like DNS, Telnet, HTTP etc. All of them uses specific port numbers. For example , telnet uses TCP port number 23 on the telnet server, DNS uses UDP port number 53 on the server, HTTP, which is the Web server uses TCP port number 80 on the server

So, in the above scenario, when the PC tries to access the website , which is hosted on the web server, it triggers a request to the IP address along with TCP port number 80. When the request reaches the webserver, it would behave like the analogy example provided above. A call is received (Packet is processed) and forwarded to the appropriate extension (Based on the TCP port number 80 in the request, the contents of the packet is forwarded to the appropriate application).

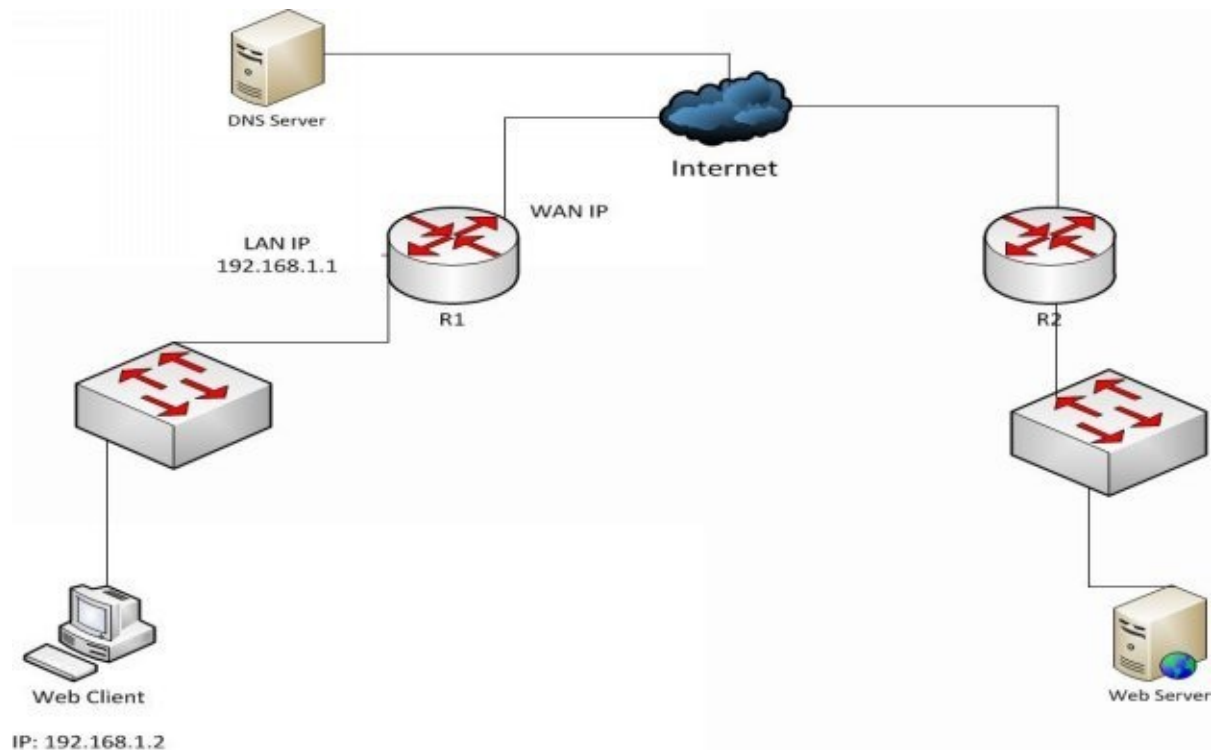
So in a real world scenario, what happens to the response, which is sent back from the Webserver ? When the client initiates the request, it would generate a random number, which would be used as the port number for identifying the return packet. This port number , which is termed as source port is embedded in the transport layer header (TCP or UDP) in the packet. The destination port number initiated from the client would be TCP port number 80. The server would send the response to the source port specified by the client.

Question 168

How does communication between webclient and web server work.

In the below diagram, the PC is on the internal network with the IP address 192.168.1.2. The default gateway of the PC is configured as 192.168.1.1, which is the LAN IP address of the router. The WAN interface of the router is connected to the internet and has a public IP address provided by the ISP. NAT is configured on the router for allowing internal IP addresses to be sent out to the

internet. The DNS server used by the ISP is as shown in the diagram.



The Web server, which hosts the Website, has a public IP. The DNS Server contains the IP address to domain name mapping for the IP address and domain name of the website on the Web Server. The following sequences of events are followed when a user on the PC types the URL of the website and views the website content on the browser.

1. User opens the browser on the PC and types the URL of the website - www.tcpipguru.com
2. The PC has to identify the IP address corresponding to the name www.tcpipguru.com. For this the TCP/IP on the PC sends a DNS request to the DNS server IP address which is configured on it's TCP/IP adapter alongside the IP address.

Note: If the DNS server IP address is not provided, the communication would fail and the website cannot be viewed.

3. In a typical scenario, the DNS server IP address is provided as the LAN IP address of the router. When the router receives the DNS request packet, it

forwards it to the actual DNS server residing on the internet.

4. The DNS server responds with the IP address corresponding to the domain name, www.tcpipguru.com to the PC.

5. Once the PC receives the IP address of the webserver on which the website is hosted, it initiates a TCP 3 way handshake to the Web server on destination port 80. This is because, HTTP communication on Web servers are on port 80.

6. Once the TCP 3 way handshake is successful, the Web client and the server exchanges data with TCP.

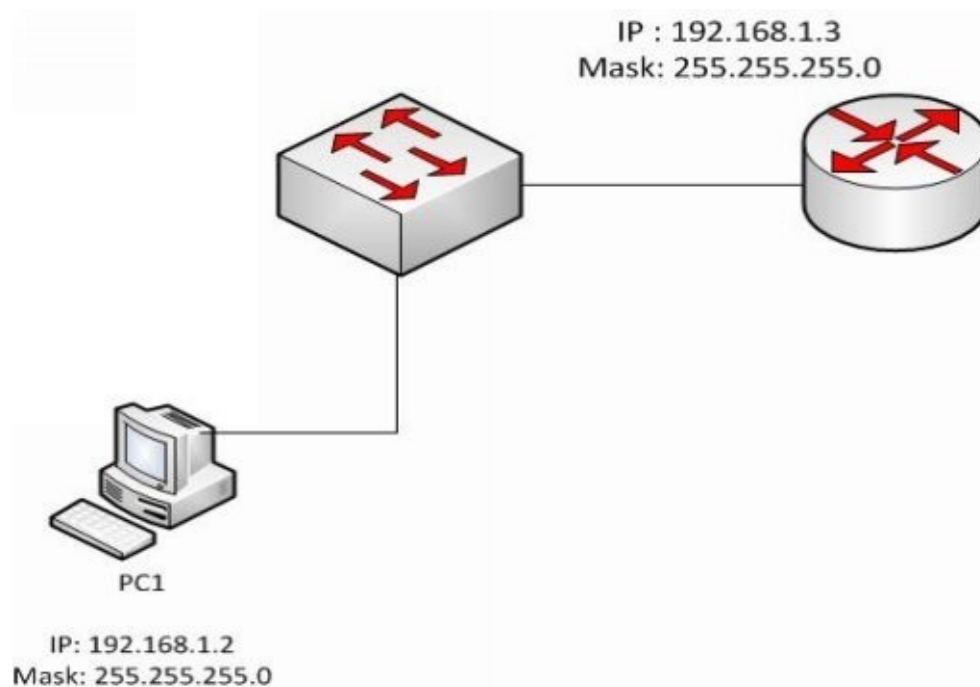
Question 169

How does a router forward packets.

When an IP packet is received on a router, the destination IP address is looked into. The network address corresponding to the IP address is looked into the routing table of the PC. If the network is a directly connected network, the packet is sent out using the interface which is directly connected to the network. For this purpose, a frame which would contain the source mac-address as the routers mac-address for the interface and the destination mac-address as the actual destinations mac-address is used. On an ethernet segment, ARP is used for identifying the mac-addresses. If the network is not directly connected, the router would then look for information about how to reach the network, which is typically, configured using static route. If a static route is not available, the default route on the router, which is used for forwarding packets to unknown destination, is used.

Question 170

What happens when a packet is received on a router.



In the above diagram, PC1 is configured with the IP address 192.168.1.2 and subnet mask 255.255.255.0. The router is configured with the IP address 192.168.1.3 and subnet mask 255.255.255.0. When PC1 pings the IP address of the router, the source IP address in the IP packet is 192.168.1.2 and the destination IP address in the IP packet would be 192.168.1.3. The IP packet is encapsulated in an ethernet frame, which would have the source mac-address as that of PC1 and destination mac-address as that of the routers interface configured with the IP address 192.168.1.3. When the packet reaches the router, the router would look into the destination mac-address inside the frame. After verification, the router would look into the destination IP address inside the packet. It would then understand that the packet is intended for itself, and would then process the upper layer of the packet.

Question 171

How does a router process a frame

Take a scenario where a router receives an ethernet frame which is encapsulating an IP Packet. The following are the operations that would be performed by the

router. The router looks into the destination mac-address inside the frame and checks if it is intended for itself. If the mac-address is incorrect, the frame is dropped. If correct, the router would calculate and verify the FCS value of the frame. Once verified, the router would look into the destination IP address in the IP Packet. The router would then analyze it's routing table and then see if a matching destination network is available in the table corresponding to the destination IP address. if no match is available, the packet is dropped. If a match is available, then the router would create a new frame for the exit interface and the IP Packet would be encapsulated in the new frame. The old frame would be discarded by the router.

Question 172

How is a routing table created.

Routing table is available on devices which work at layer 3 of the OSI model, which is the network layer. This includes computers, routers, layer 3 switches etc. A routing table is created based on the information configured and provided. For ex on router, when an IP address along with the subnet mask is configured, the network address is derived and the information included in the routing table as a directly connected network. Additional information related to different networks can be configured using routing techniques like static routing and dynamic routing. This information is also included in the routing table.

Question 173

How do routers forward packets to the internet.

When a packet reaches a router, the destination IP address in the IP packet is looked into and the corresponding network address is looked into the routing table. Typically, packets which are bound to the internet have varying destination IP address, which would not be available or know before. Due to this routers are configured with a default route, to forward packets with unknown destination addresses. All packets, bound to the internet would use the default route and would be forwarded to the IP address to which the default route points to, typically the gateway of the internet router.

Recommended Book

250 + Network Engineer Interview Questions & Answers

[Click to view details in Amazon \(Ctrl +P\)](#)

Question 174

How does routing work on a computer.

Computers build routing tables based on the information provided. When an IP address and subnet mask is configured on the computer, 'AND' ing operation is performed and the network address on which the computer belongs to is derived. The default gateway configured on the PC, would also be used along with the network address and these information would be used to populate the routing table of a PC. A packet bounded for a different network, uses the information in the routing table to understand, the gateway address details for forwarding to a different network.

Question 175

What is the use of TTL value in an IP header.

The TTL value in an IP header is used for preventing looping of IP packets on a network. The TTL value is inserted in the IP header by the initiator of the packet. Every time the packet crosses a router, the value is decremented by 1. When the TTL value in the packet reaches 1, the packet is dropped, thus avoiding loops incase the packet does not reach the destination.

Question 176

What is the difference between default route and default gateway.

A default route is a route entry in a routing table whereas a default gateway is a value, typically an IP address. When an IP packet is received by a router, it looks into the destination IP address in the packet. It then checks in its routing table if it is aware of the network address corresponding to the IP packet. It would then forward the packet out on the required interface to which the network is connected. If the destination network is unknown, the packet would be dropped. What if the router is directly connected to another router, which knows about the destination network in the IP packet. In this scenario, two options can be configured. The default gateway of the first router can be configured with the IP address of the second router. When this configuration is performed, a route entry

would be automatically populated in the routing table. This route entry is known as a default route. Instead of configuring the default gateway, a default route entry can also be configured directly on the router.

Question 177

How do Routers populate routing tables for directly connected interfaces

Let's take a router that has two interfaces. The IP address configured on one adapter is 192.168.1.1 and the subnet mask is 255.255.255.0 . The IP address configured on the second adapter is 10.0.0.1 and subnet mask 255.0.0.0 . Once this is configured it is observed that the routing table entries are created . How is this done ? “Anding” operation is performed between the IP address and subnet mask to derive the network entry. Anding operation (Every bit in the IP address is compared with the corresponding subnet bit. (Result between bits : $1\&1 = 1$, $1\&0 = 0$, $0\&1 = 0$, $0\&0 = 0$)

First Adapter:

Binary of IP 192.168.1.1 – 11000000.10101000.00000001.00000001

Binary of mask 255.255.255.0 11111111.11111111.11111111.00000000

Result 11000000.10101000.00000001.00000000

Value: 192.168.1.0

Second Adapter:

Binary of IP 10.0.0.1 – 00001010.00000000.00000000.00000001

Binary of mask 255.0.0.0 – 11111111.00000000.00000000.00000000

Result: 00001010.00000000.00000000.00000000

Value: 10.0.0.0

The routing table in the router would be displayed in the following format

Network Destination Network mask Interface

192.168.1.0 255.255.255.0 192.168.1.1

10.0.0.0 255.0.0.0 10.0.0.1

Question 178

Which field in an IP header is used by routers for matching routes in the

routing table.

When an IP packet arrives, the router looks into the destination IP address field in the IP header, which is then used for matching routes in the routing table.

Question 179

Are frames used on wired and wireless links the same or different

Frames used on wired and wireless links are different. Generic ethernet frames are used on wired links. On the wireless links, 802.11 frames are used.

Question 180

How many wireless devices can connect to a wireless access point.

This would depend on the capacity of the access point

Question 181

Does authentication or association takes place initially when a wireless client connects to an access point.

Wireless clients initially attempts authentication with the access point. On successful authentication, the clients associate with the access point.

Question 182

If a wireless network is secure and encrypted, is the data send from the source to the destination encrypted.

The data would be encrypted only between the wireless client and the access point. Assuming that the destination is on the wired link, to which the access point is connected, data from the access point to the destination would be unencrypted.

Question 183

How many keys are required to be configured for encrypting and decrypting based on WEP protocol between a wireless client and access point.

1 pre-shared key is required to be configured on the wireless client and access point which would be used for both encryption and decryption.

Question 184

What is common in the implementation of EAP-TLS and PEAP-MSCHAP

v2.

Both use TLS for communication.

Question 185

Explain the benefit of using radius servers for wireless networks as opposed to pre-shared keys between clients and access points.

When radius servers are used, the key which are used for encryption and decryption are derived dynamically between the client and the server and is unique for every session.

Question 186

Who decides the TTL value which should be inserted in an IP header.

The operating system decides on the value of TTL to be inserted in the IP header.

Question 187

What is the alternate way of transporting data if TCP 3 way handshake is unsuccessful between the client and the server.

There is no alternative way. If the TCP 3 way handshake is unsuccessful, data cannot be transported.

Question 188

Explain a technique by which a home desktop which is behind a home router can be viewed by a user on the internet.

The desktop can be configured to allow remote desktop connections. Port forwarding can be configured on the home router, to allow RDP port (Remote desktop) to be forwarded to the desktop. Users from the internet can RDP to the public IP of the router, which on receipt would forward the request to the desktop.

Question 189

How can ftp be blocked on internet facing Cisco router.

The internet facing interface can be configured with an inbound ACL which would deny TCP port 20 and 21 which is used by FTP service.

Question 190

A Cisco router has two interfaces, LAN and internet. How can users on the

LAN network be allowed only for http access to the internet.

An ACL can be configured on the router on the interface which is connected to LAN network as inbound which would permit only http access. All other traffic is denied.

Question 191

Name two techniques by which a single internet connection can be shared by multiple users on a LAN.

The requirement can be achieved by the use of NAT router (Network address translation) or a proxy server.

Question 192

How can unauthorized RIP updates be blocked on a Cisco router.

The interface which is connected to receive RIP updates can be configured with an ACL which would deny UDP packets with port number 520, which is used by RIP for communication. This would ensure that RIP updates are not processed by the appropriate interface.

Recommended Book

250 + Network Engineer Interview Questions & Answers

[Click to view details in Amazon \(Ctrl +P\)](#)

Question 193

Which TCP ports should be open on a firewall to allow traffic from a PPTP based VPN clients to a PPTP VPN server on the inside

TCP protocol 1723 should be configured on the firewall for communication between PPTP client and servers.

Question 194

Which UDP ports should be open on a firewall to allow traffic from a L2TP/IPSEC based VPN clients to a PPTP VPN server on the inside

UDP port 500 for IKE traffic, UDP port 1701 for L2TP communication between client and server and UDP port 4500 for NAT-T communication.

Question 195

Can a network layer firewall be used to block access to a wireless access point from a wireless client.

Access control to an access point should be configured on the wireless access point. The firewall would not be able to perform this requirement.

Question 196

Which protocol does OSPF use at the transport layer.

OSPF does not use any protocol at the transport layer. It encapsulates and sends data the IP layer.

Question 197

Which feature can be used to deny access between two systems connected to the same switch.

Mac-based ACL can be configured to deny access between two systems on the same switch,

Question 198

An access point is pre-configured for WPA authentication. There are 5 users connected to the access point. Will each user be pre-configured with the same key or different keys.

The keys used by the users would be the same key which is pre-configured on the access point.

Question 199

What is the fundamental difference in implementation between radius and tacacs.

Radius uses UDP protocol and tacacs uses TCP.

Question 200

Can radius servers and clients from different vendors communicate with each other.

Radius is a vendor neutral protocol. So a radius client and server from different

vendors would be able to communicate without any issues.

Question 201

Name two networking hardware devices which can be configured as radius clients.

Switches and access points can be configured as radius clients.

Question 202

What is the use of configuring ACL in IPSEC configuration on a Cisco router.

The ACL would make the router understand that the traffic corresponding to the network associated with the ACL, has to be sent encrypted over the IPSEC tunnel and all other traffic is to be sent unencrypted.

Question 203

Which IP protocol does AH and ESP headers use in IPSEC .

ESP and AH uses IP protocol 50 and 51 respectively.

Question 204

What feature on a Cisco router can be used to receive but not send routing updates.

The passive interface command can be used for the purpose. The command works for interior gateway protocols like RIP, OSPF etc.

Question 205

Which feature on a Cisco router can be used to send selective route updates through an interface.

Distribute list feature can be used for the purpose.

Question 206

What is the metric used by RIP and IGRP

RIP uses hop count and IGRP uses bandwidth and delay.

Question 207

How can an ACL be used to block BGP updates to be received on a Cisco router interface.

BGP works on TCP port 179. The interface can be configured with an ACL which would block TCP port 179, which would block all BGP updates.

Question 208

Which feature on an access point can be configured to hide the availability of the access point.

The Disable SSID broadcast would not broadcast the SSID configured on the access point. This would make users on the network unable to view the presence of the access point.

Question 209

Which layer of the OSI layer does ping and trace route work.

They work at the application layer.

Question 210

Is the administrative distance of a directly connected interface or static route higher on a Cisco router

The AD of directly connected interface is 0 and static route is 1, which makes static route higher.

Question 211

Does a packet takes a network path which has a lower or higher administrative distance.

A packet always takes the path which has a lower administrative distance.

Question 212

Name two devices which can be configured as an IPSEC server.

Cisco VPN routers and Windows 2008 servers can be configured as IPSEC servers.

Question 213

Name two protocols which are used for accessing a website and its need.

DNS is used for resolving the URL of the website to the IP address. TCP is used between the browser and the server for data transfer.

Question 214

Is a proxy server IP address required to be configured on a browser if NAT is used for sharing internet.

Proxy server and NAT are two different technologies. If NAT is used for sharing internet, proxy server is not required to be configured on the browser.

Question 215

Will internet work if the dns server is configured on a PC but not the default gateway.

All packets bound to the internet should be routed through an appropriate gateway. DNS is used only for name resolution. So internet would fail, if the PC is not configured with an appropriate gateway address.

Question 216

On which port do a DNS client and server work.

DNS clients do not work on a known port. When a DNS request is sent, the operating system assigns a random number for the port. DNS servers work on well known port number 53.

Question 217

How does a FTP server differentiate between two simultaneous connections from two FTP clients on a network.

FTP clients would have unique source port numbers in them. This would be used for differentiating the connections.

Question 218

Name two devices which can be configured as FTP Server

Windows 2008 server and Ubuntu operating system can be configured as FTP servers.

Question 219

Name two devices which can be configured as a DHCP server.

Windows 2008 server and Cisco routers can be configured as DHCP servers.

Question 220

Can an access point be configured as a DHCP server

Access points can be configured as DHCP server.

Question 221

Which field in the IP header is used at the destination for identifying fragmented IP packets.

The identification field in the IP header is used for identifying fragmented IP packets.

Question 222

Name one limitation of network layer firewall.

Network layer firewalls would be unable to detect and block vulnerabilities which are specific to application layer protocols. For ex, vulnerabilities specific to FTP protocol cannot be blocked by a network layer firewall.

Question 223

Can a packet filter firewall be used to block access to a DNS server on the network.

Packet layer firewalls work on IP and transport layer headers. Access to DNS server can be blocked by a packet filter firewall by creating an access control list which would block all ports to well known port UDP port 53 used by DNS servers.

Question 224

Which layer of the OSI model would respond to a ping request.

Ping works at the network layer, which is layer 3 of the OSI model

Question 225

Which layer of the OSI model would respond to a HTTP GET request from a client.

HTTP is an application layer protocol. Application layer corresponds to Layer 7 of the OSI model

Question 226

Name two protocols which are vulnerable to brute force attacks.

Telnet and FTP are two protocols which are vulnerable to brute force attacks.

Question 227

Which transport layer port number does 802.1x enabled ports on a switch use with the respective clients connected to it.

802.1x does not use any transport layer protocols. It is a layer 2 protocol.

Question 228

A router is configured for a static route entry. RIP is also configured on the router. The router learns the network address corresponding to the static route entry via Rip Update. What would happen?

The dynamic route entry would be rejected by the router and the static entry would be retained

Question 229

A PC is connected to a 5 port ethernet hub operating at 100 Mbps. Other ports of the hub are free and not connected to any other devices. At what duplex setting can the hub operate

Hubs used a shared medium for communication. It uses the CSMA/CD protocol and can work only in half duplex mode irrespective of the number of clients connected to it.

Question 230

If reliability is required at Layer 2, which type of LLC should be implemented in the design

LLC - Type 2 is to be implemented in the design

Question 231

What is the value of the high order bit in a Class A first Octet

The value is 0

Question 232

What would be the value of TYPE in an ethernet frame communicating in a TCP/IP environment in which the data is HTTP traffic

The Type field in the ethernet frame would contain the immediate upper layer protocol which is IP.

Question 233

A PC which has a 802.1x supplicant using the EAP-MD5 protocol is connected to port 2 of a switch configured as 802.1x authenticator. What would be mac-address learned by the switch on port 2 after successful authentication

After successful authentication, the switch port would learn the mac-address of the PC. This would be the behavior with or without any form of authentication.

Question 234

Where is TCP used in an environment where TACACS is deployed.

TCP is used between the authenticator and the authentication server. (Between the switch / access point and TACACS server)

Question 235

Which command on a Windows system would display the routing table.

The route print command can be used to display the routing table.

Question 236

Which command on a Cisco system would display the routing table.

show ip route

Question 237

Name an operating system which can be configured as a router.

Windows 2008 server can be configured with two network interface cards and can be setup as a router.

Question 238

Why is TCP/IP protocol used on the internet.

TCP/IP is vendor neutral protocol. On the internet there are devices from different vendors. The use of TCP/IP would make interoperability between multiple vendors possible.

Question 239

Name two protocols which are used by 802.1x supplicants

EAP-MD5 and EAP-TLS

Question 240

Name two techniques by which an 802.1x client authenticates with the server.

By using combination of username / passwords or with digital certificates.

Question 241

Which command is used to install Windows active directory from the command line

DCPROMO is used for the purpose.

Question 242

Which protocol does a router use to inform the source that a destination is unreachable.

Routers use ICMP protocol. Appropriate ICMP messages like ICMP destination unreachable / host unreachable is send to the initiator.

Question 243

Are inbound ACL's applied on Cisco routers globally on the router or specific to the interface.

Irrespective of inbound or outbound, ACL's are applied on the interface level.

Question 244

Which fields in an IP packet would a Cisco router look to make a matching decision when an ACL is configured.

This would be dependent on the parameters configured on the ACL. For ex, a standard ACL would look into the source IP address in the IP header whereas an extended ACL can be configured to look into the source and destination IP address in the IP header as well as the port numbers in the transport layer headers.

Question 245

Can a standard ACL on a Cisco router be used for blocking access to FTP service on a server.

Standard ACL's do not have the capacity to look into transport layer headers. For this an extended ACL would be required. FTP service works on TCP port 20/21.

So an extended ACL can be used for this purpose.

Question 246

Which command can be used on a Windows system to configure the IP address from the command line.

The command *netsh* along with appropriate parameters can be used for the purpose.

Question 247

Which feature on a Cisco router can be used for forwarding packets based on specific source address

Policy routing can be used for achieving the functionality.

Question 248

Does HTTPS encrypt data at the network or transport layer

HTTPS does not encrypt data at the network or transport layer. It encrypts at the application layer.

Question 249

At which layer does WEP encrypt data

WEP encrypts data the data link layer.

Question 250

Which type of VPN would you use if data has to be encrypted at the network layer

IPSEC VPN encrypts data at the network layer whereas SSL encrypts data at the application layer.

Recommended Book

250 + Network Engineer Interview Questions & Answers

[Click to view details in Amazon \(Ctrl +P\)](#)