CCNA Interviews questions Papers:

There are two processes to pair MAC address with IP addresses. Which process finds an IP address from a MAC address?

\* RARP

\* ARP

\* RIP

\* IGRP

Correct answer: A

ARP (Address Resolution Protocol) maps an IP address to the MAC address, RARP (Reverse Address Resolution Protocol) maps the MAC address to the IP address. ARP and RARP work at the internet layer of the Internet Model or the network layer of the OSI model.

When the router runs out of buffer space, this is called \_\_\_\_\_\_\_\_.

\* Source Quench

\* Redirect

\* Information Request

\* Low Memory

Correct answer: A

Source quench is the process where the destination router, or end internetworking device will “quench” the date from the “source”, or the source router. This usually happens when the destination router runs out of buffer space to process packets.

Which protocol carries messages such as destination Unreachable, Time Exceeded, Parameter Problem, Source Quench, Redirect, Echo, Echo Reply, Timestamp, Information Request, Information Reply, Address Request, and Address Reply?

\* ICMP

\* UDP

\* TCP

\* TFTP

\* FTP

Correct answer: A

ICMP (Internet Control Message Protocol) is a network layer internet protocol described in RFC # 792. ICMP reports IP packet information such as destination Unreachable, Time Exceeded, Parameter Problem, Source Quench, Redirect, Echo, Echo Reply, Timestamp, Information Request, Information Reply, Address Request, and Address Reply.

Two of the protocols that can be carried in the Protocol field of an IP packet are?

\* TCP

\* UDP

\* FTP

\* TFTP

Correct answer: A & B

The following are the fields in an IP segment,

their length, and their definitions:

VERS (Version number - 16 bits)

HLEN (Number of 32-bit words in the header - 4 bits)

Type of Server (How the datagram should be handled - 32 bits)

Total Length (Total length of header and data - 32 bits)

Identification (Provide fragmentation of datagrams to allow different MTUs in the internet - 4 bits)

Flags (Provide fragmentation of datagrams to allow different MTUs in the internet - 4 bits)

Frag Offset (Provide fragmentation of datagrams to allow different MTUs in the internet - 6 bits)

TTL (Time-To-Live - 6 bits)

Protocol (Upperlayer protocol sending the datagram - 16 bits)

Header Checksum )Integrity check on the header - 16 bits)

Source IP Address (32 bits)

Destination IP Address (32 bits)

IP Options (network testing, debugging, security and others - 4 bits)

Data (4 bits).

Where would network testing be included in an IP packet?

\* IP Options field

\* Identification field

\* Type of Service field

\* Reservation field

Correct answer: A

The following are the fields in an IP segment, their length, and their definitions:

VERS (Version number - 16 bits)

HLEN (Number of 32-bit words in the header - 4 bits)

Type of Server (How the datagram should be handled - 32 bits)

Total Length (Total length of header and data - 32 bits)

Identification (Provide fragmentation of datagrams to allow different MTUs in the internet - 4 bits)

Flags (Provide fragmentation of datagrams to allow different MTUs in the internet - 4 bits)

Frag Offset (Provide fragmentation of datagrams to allow different MTUs in the internet - 6 bits)

TTL (Time-To-Live - 6 bits)

Protocol (Upperlayer protocol sending the datagram - 16 bits)

Header Checksum )Integrity check on the header - 16 bits)

Source IP Address (32 bits)

Destination IP Address (32 bits)

IP Options (network testing, debugging, security and others - 4 bits)

Data (4 bits).

What field tells the Internet layer how to handle an IP packet?

\* Type of Service

\* Identification

\* Flags

\* Frag Offset

Correct answer: A

The following are the fields in an IP segment, their length, and their definitions:

VERS (Version number - 16 bits)

HLEN (Number of 32-bit words in the header - 4 bits)

Type of Server (How the datagram should be handled - 32 bits)

Total Length (Total length of header and data - 32 bits)

Identification (Provide fragmentation of datagrams to allow different MTUs in the internet - 4 bits)

Flags (Provide fragmentation of datagrams to allow different MTUs in the internet - 4 bits)

Frag Offset (Provide fragmentation of datagrams to allow different MTUs in the internet - 6 bits)

TTL (Time-To-Live - 6 bits)

Protocol (Upperlayer protocol sending the datagram - 16 bits)

Header Checksum )Integrity check on the header - 16 bits)

Source IP Address (32 bits)

Destination IP Address (32 bits)

IP Options (network testing, debugging, security and others - 4 bits) Data (4 bits).

Which fields of an IP packet provide for fragmentation of datagrams to allow differing MTUs in the internet?

\* Identification

\* Flags

\* Frag Offset

\* Type of Service

\* Total Length

Correct answer: A, B & C

The following are the fields in an IP segment, their length, and their definitions:

VERS (Version number - 16 bits)

HLEN (Number of 32-bit words in the header - 4 bits)

Type of Server (How the datagram should be handled - 32 bits)

Total Length (Total length of header and data - 32 bits)

Identification (Provide fragmentation of datagrams to allow different MTUs in the internet - 4 bits)

Flags (Provide fragmentation of datagrams to allow different MTUs in the internet - 4 bits)

Frag Offset (Provide fragmentation of datagrams to allow different MTUs in the internet - 6 bits)

TTL (Time-To-Live - 6 bits)

Protocol (Upperlayer protocol sending the datagram - 16 bits)

Header Checksum )Integrity check on the header - 16 bits)

Source IP Address (32 bits)

Destination IP Address (32 bits)

IP Options (network testing, debugging, security and others - 4 bits)

Data (4 bits).

Which processes does TCP, but not UDP, use?

\* Windowing

\* Acknowledgements

\* Source Port

\* Destination Port

Correct answer: A & B

UDP (User Datagram Protocol) does not use sequence or acknowledgement fields in transmission.

UDP is a connectionless and unreliable protocol, since there is no delivery checking mechanism in the UDP data format.

What is the UDP datagram format?

\* Source Port - 16 bits, Destination Port - 16 bits, Length - 16 Bits, Checksum - 16 bits, Data

\* Destination Port - 16 bits, Source Port - 16 bits, Length - 16 Bits, Checksum - 16 bits, Data

\* Source Port - 16 bits, Destination Port - 16 bits, Checksum - 16 Bits, Length - 16 bits, Data

\* Source Port - 8 bits, Destination Port - 8 bits, Length -8 Bits, Checksum - 8 bits, Data

Correct answer: A

The UDP format for a segment is as follows:

Source Port 16 bits

Destination Port 16 bits

Length 16 bits

Checksum 16 bits

Data xx bits

What is the function of DDR on Cisco routers?

\* DDR is dial–on-demand routing. It provides a continuous LAN only connection.

\* DDR is dial-on-demand routing. It provides routing for high volume traffic.

\* DDR is dial–on-demand routing. It provides a continuous WAN connection.

\* DDR is dial-on-demand routing. It provides routing for low volume and periodic traffic.

Correct answer: D

DDR is dial-on-demand routing. It provides routing for low volume and periodic traffic. It initiates a call to a remote site when there is traffic to transmit.

What are the two types of access lists that can be configured on a Cisco router?

\* Standard

\* Extended

\* Filtering

\* Packet

Correct answer: A & B

The access lists are standard and extended. Standard access lists for IP check the source address of packets that could be routed. Extended access lists can check the source and destination packet plus check for specific protocols, port numbers, etc.

When using access lists, what does a Cisco router check first?

\* To see if the packet is routable or bridgeable

\* The destination address

\* The source address

\* The packet contents

Correct answer: A

The first thing checked is to see if the packet is routable or bridgeable. If it is not, the packet will be dropped.

How many access lists are allowed per interface?

\* One per port, per protocol

\* Two per port, per protocol

\* Unlimited

\* Router interface +1 per port.

Correct answer: A

Only one access list is allowed per interface. An access list must have conditions that test true for all packets that use the access list.

What do the following commands accomplish?

access-list 1 deny 172.16.4.0 0.0.0.255

access-list 1 permit any interface ethernet 0

IP access-group 1 out

\* This will block traffic from subnet 172.16.4.0 and allow all other traffic.

\* This will allow traffic from subnet 172.16.4.0 and block all other traffic.

\* All traffic is allowed.

\* All traffic is blocked.

Correct answer: A

This will block traffic from subnet 172.16.4.0 and allow all other traffic. The first statement “access-list 1 deny 172.16.4.0 0.0.0.255″ will deny access to the subnet 172.16.4.0.

What do the following statements in an extended access list accomplish?

access-list 101 deny TCP 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21

access-list 101 deny TCP 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20

access-list 101 permit TCP 172.16.4.0 0.0.0.255 0.0.0.0 255.255.255.255

\* This will block ftp traffic.

\* This will block http traffic.

\* This will permit ftp traffic.

\* This will permit tftp traffic.

Correct answer: A

This will block ftp traffic since ftp uses ports 20 and 21.

Access lists are numbered. Which of the following ranges could be used for an IP access list?

\* 600 - 699

\* 100 - 199

\* 1 - 99

\* 800 - 899

\* 1000 - 1099

Correct answer: wer: B & C

AppleTalk access lists use numbers in the 600 - 699 range. IP uses 1 - 99 for standard access lists or 100-199 for extended access lists. IPX uses 800 - 899 or 900 - 999 for extended access lists. IPX SAP filters use 1000 - 1099.

Cisco routers use wildcard masking to identify how to check or ignore corresponding IP address bits. What does setting a wildcard mask bit to 0 cause the router to do?

\* It tells the router to check the corresponding bit value.

\* It tells the router to ignore the corresponding bit value.

\* It tells the router to check its alternate routing list.

\* It tells the router to use its primary routing list.

Correct answer: A

It tells the router to check the corresponding bit value.

You are a system administrator and you want to deny access to a group of computers with addresses 172.30.16.0 to 172.30.31.0. Which wildcard mask would you use?

\* 0.0.15.255

\* 0.0.255.255

\* 0.0.31.255

\* 0.0.127.255

\* 0.0.255.255

Correct answer: A

0.0.15.255 will check the last 13 bits of an address so that computers 172.30.16.0 to 172.30.31.0 will be denied access. 0.0.31.255 would check the last 6 binary digits and deny access to addresses 172.30.32.0 to 172.30.63.0. 0.0.127.255 would check the last 7 binary digits and deny access to addresses 172.30.64.0 to 172.30.127.0. 0.0.255.255 would deny 172.30.0.0 to 172.30.254.0. If you write decimal 15 in binary, you have 0001111, the 1’s tell the router to ignore address with these bits set; 0’s tell the router to check the bits. The third octet for 172.30.16.0 is 00010000. The third octet for 172.30.31.0 would be 00011111. So, traffic from these addresses would be denied.

In order to limit the quantity of numbers that a system administrator has to enter, Cisco can use which abbreviation to indicate 0.0.0.0?

\* host

\* any

\* all

\* include

Correct answer: A

Cisco uses host to specify 0.0.0.0. This tells the router to check all. Cisco uses any to specify 255.255.255.255. This tells the router to ignore all and permit any address to use an access list test.

What do the following commands accomplish?

access-list 1 permit 172.16.0.0 0.0.255.255

interface ethernet 0

IP access-group 1 out

interface ethernet 1

IP access-group 1 out

\* Only traffic from the source network 172.16.0.0 will be blocked.

\* Only traffic from the source network 172.16.0.0 will be forwarded. Non-172.16.0.0 network traffic is blocked.

\* Non-172.16.0.0 traffic will be forwarded.

\* All traffic will be forwarded.

Correct answer: B

Only traffic from the source network 172.16.0.0 will be forwarded. Non-172.16.0.0 network traffic is blocked. The wildcard mask 0.0.255.255 tells the router to check the first 2 octets and to ignore the last 2 octets.

When using access lists, it is important where those access lists are placed. Which statement best describes access list placement?

\* Put standard access lists as near the destination as possible. Put extended access lists as close to the source as possible.

\* Put extended access lists as near the destination as possible. Put standard access lists as close to the source as possible.

\* It isn’t import where access lists are placed since the router will read and cache the whole list.

\* Put access lists as close to corporate headquarters as possible.

Correct answer: A

Put standard access lists as near the destination as possible. Put extended access lists as close to the source as possible. Standard access lists don’t specify the destination address.

As the system administrator, you enter the following commands at the command prompt:

ipx routing

access-list 800 permit 2b 4d

int e0

ipx network 4d

ipx access-group 800 out

int e1

ipx network 2b

int e2

ipx network 3c

What did these command accomplish?

\* Traffic from network 4c destined for network 4d will be forwarded out Ethernet0.

\* Traffic from network 3c destined for network 4d will be forwarded out Ethernet0.

\* Traffic from network 2b destined for network 4d will be forwarded out Ethernet0.

\* Traffic from network 4d destined for network 2d will be forwarded out Ethernet0.

Correct answer: C

Traffic from network 2b destined for network 4d will be forwarded out Ethernet0. The other interfaces E1 and E2 are not subject to the access list since they lack the access group statement to link them to access list 800.

The following commands were entered at the command prompt of a Cisco router. What do they accomplish?

access-list 1000 deny 9e.1234.5678.1212 4

access-list 1000 permit -1

interface ethernet 0

ipx network 9e

interface ethernet 1

ipx network 4a

interface serial 0

ipx network 1

ipx output-sap-filter 1000

\* File server advertisements from server 9e.1234.5678.1212 will not be forwarded on interface S0.

\* All other SAP services, other than file server, from any source will be forwarded on S0.

\* All other SAP services, other than print server, from any source will be forwarded on S0.

\* Print server advertisements from server 9e.1234.5678.1212 will not be forwarded on interface S0.

Correct answer: A & B

File server advertisements from server 9e.1234.5678.1212 will not be forwarded on interface S0. All other SAP services, other than file server, from any source will be forwarded on S0.

You receive “input filter list is 800 and output filter list is 801″ as part of the output from a show interfaces command. What kind of traffic are you filtering?

\* IPX/SPX

\* TCP/IP

\* LocalTalk

\* DDR

Correct answer: A

Because the access list is numbered in the 800 range, you are filtering IPX/SPX traffic.

Which service uses telephone control messages and signals between the transfer points along the way to the called destination?

\* Signaling System 7 (SS7)

\* Time-division Multiplexing (TDM)

\* X.25

\* Frame relay

Correct answer: A

Signaling System 7 (SS7) uses telephone control messages and signals between the transfer points along the way to the called destination. Time-division Multiplexing (TDM) has information from multiple sources and allocates bandwidth on a single media. Circuit switching uses signaling to determine the call route, which is a dedicated path between the sender and the receiver. Basic telephone service and Integrated Services Digital Network (ISDN) use TDM circuits. X.25 and Frame Relay services have information contained in packets or frames to share non-dedicated bandwidth. X.25 avoids delays for call setup. Frame Relay uses permanent virtual circuits (PVCs).

Which service takes information from multiple sources and allocates bandwidth on a single media?

\* Time-division Multiplexing (TDM)

\* Signaling System 7 (SS7)

\* X.25

\* Frame relay

Correct answer: A

Which three devices can be used to convert the user data from the DTE into a form acceptable to the WAN service’s facility?

\* Modem

\* CSU/DSU

\* TA/NT1

\* CO

\* SS7

Correct answer: A, B & C

A modem, CSU/DSU (Channel Service Unit/Data Service Unit), or TA/NT1 (Terminal Adapter/Network Termination 1) can be used to convert the user data from the DTE into a form acceptable to the WAN service’s facility.

What is the juncture at which the CPE ends and the local loop portion of the service begins?

\* Demarc

\* CO

\* Local loop

\* Last-mile

Correct answer: A

The demarcation or demarc is the juncture at which the CPE ends and the local loop portion of the service begins. The CO (Central Office) is the nearest point of presence for the provider’s WAN service. The local loop or “last-mile” is the cabling that extends from the demarc into the WAN service provider’s central office.

You can access three forms of WAN services with Cisco routers. Select the three forms:

\* Switched or relayed services

\* Interface front end to IBM enterprise data center computers

\* Using protocols that connect peer-to-peer devices like HDLC or PPP encapsulation.

\* IPX/SPX

\* NetBEUI

Correct answer: A, B & C

You can access three forms of WAN services with Cisco routers. Switched or relayed services include X.25, Frame Relay, and ISDN. An interface front end to IBM enterprise data center computers includes SDLC. And, you can access the services of WAN providers using protocols that connect peer devices such as HDLC and PPP encapsulation. IPX/SPX and NetBEUI are LAN protocols.

Select the fields for the Cisco HDLC protocol:

\* Flag, Address, Control

\* Flag, Address, Control, Protocol, LCP (Code, Identifier, Length, Data), FCS, Flag

\* Flag, Address, Control, Data, FCS, Flag

\* Flag, Address, Control, Proprietary, Data, FCS, Flag

Correct answer: D

The Cisco HDLC frame format is Flag, Address, Control Proprietary, Data, FCS, Flag. The PPP frame format is Flag, Address, Control, Protocol, LCP (Code, Identifier, Length, Data), FCS, Flag. The SDLC and LAPB format is Flag, Address, Control, Data, FCS, Flag.

85: Select the physical interfaces that PPP can be configured on a Cisco router:

\* Asynchronous serial

\* HSSI

\* ISDN

\* Synchronous serial

Correct answer: A, B, C & D