Question 1

In order to properly manage the network traffic in your organization, you need a complete understanding of protocols and networking models. In regards to the 7-layer OSI model, what is the function of the Transport Layer?

Options:

A- The Transport layer allows two applications on different computers to establish, use, and end a session. This layer establishes dialog control between the two computers in a session, regulating which side transmits, plus when and how long it transmits.

B- The Transport layer manages logical addresses. It also determines the route from the source to the destination computer and manages traffic problems, such as routing, and controlling the congestion of data packets.

C- The Transport layer packages raw bits from the Physical (Layer 1) layer into frames (structured packets for data). Physical addressing (as opposed to network or logical addressing) defines how devices are addressed at the data link layer. This layer is responsible for transferring frames from one computer to another, without errors. After sending a frame, it waits for an acknowledgment from the receiving computer.

D- The Transport layer transmits bits from one computer to another and regulates the transmission of a stream of bits over a physical medium. For example, this layer defines how the cable is attached to the network adapter and what transmission technique is used to send data over the cable.

E- The Transport layer handles error recognition and recovery. It also repackages long messages, when necessary, into small packets for transmission and, at the receiving end, rebuilds packets into the original message. The corresponding Transport layer at the receiving

end also sends receipt acknowledgments.

Answer:

E

Question 2

Question Type: **MultipleChoice**

When you took over the security responsibilities at your office, you noticed there were no warning banners on any of the equipment. You have decided to create a warning login banner on your Cisco router. Which of the following shows the correct syntax for the banner creation?

Options:

A- Banner login C Restricted access. Only authorized users allowed to access this device. C

B- Login banner C Restricted access. Only authorized users allowed to access this device. C

C- Banner login Restricted access. Only authorized users allowed to access this device.

D- Login banner Restricted access. Only authorized users allowed to access this device.

E- Banner logging C Restricted access. Only authorized users allowed to access this device. C
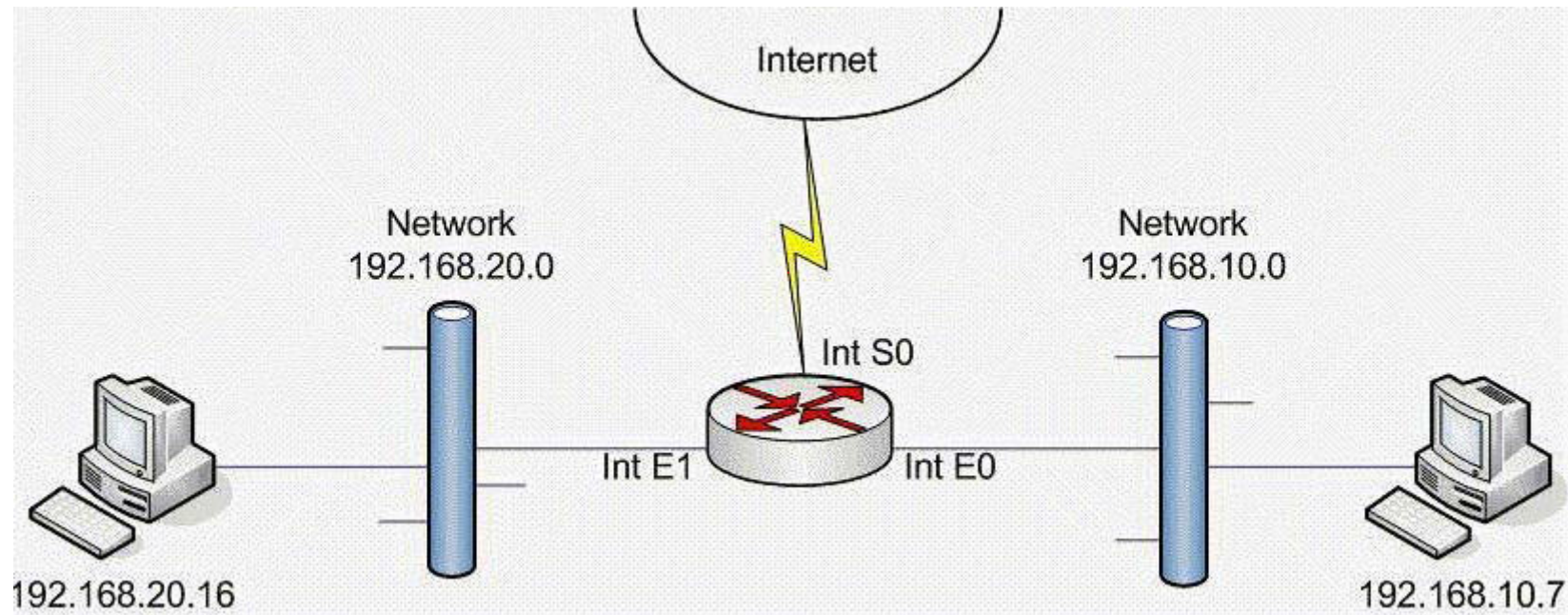
Answer:

A

Question 3

The exhibit shows a router with three interfaces E0, E1 and S0. Interfaces E0 and E1 are connected to internal networks 192.168.10.0 and 192.168.20.0 respectively and interface S0 is connected to the Internet. The objective is to allow two hosts, 192.168.20.16 and 192.168.10.7 access to the Internet while all other hosts are to be denied Internet access. All hosts on network 192.168.10.0 and 192.168.20.0 must be allowed to access resources on both internal networks. From the following, select all the access list statements that are required to make this possible.

Network 192.168.20.0 — Int E1 — Router — Int E0 — Network 192.168.10.0

Internet — Int S0

192.168.20.16

192.168.10.7

Options:

A- access-list 53 permit 192.168.20.16 0.0.0.0

B- access-list 80 permit 192.168.20.16 0.0.0.0

C- access-list 53 deny 0.0.0.0 255.255.255.255

D- access-list 80 permit 192.168.10.7 0.0.0.0

E- int S0, ip access-group 53 out

F- int S0, ip access-group 80 out

Question 4

Question Type: MultipleChoice

During a network capture in Network Monitor, you capture some UDP traffic. In a UDP Header, what is the function of the first sixteen bits?

Options:

A- To define the upper layer protocol

B- To define the source port number

C- To define the destination port number

D- To define the IP Version

E- To define the type

Answer:

B

Question 5

A. Frequency Hopping Spread Spectrum (FHSS)

Options:

B- Direct Sequence Spread Spectrum (DSSS)

C- Lamar Anthell Transmission (LAT)

D- Digital Band Hopping (DBH)

E- Digital Channel Hopping (DCH)

Answer:

B

Question 6

You have recently taken over the security of a mid-sized network. You are reviewing the current configuration of the IPTables firewall, and notice the following rule: ipchains -A output -p TCP -s 10.0.10.0/24 -d 0.0.0.0/0 80 -j ACCEPTWhat is the function of this rule?

Options:

A- This rule for the output chain states that any TCP traffic from the 10.0.10.0 network and destined for any IP address on port 80 is to be accepted.

B- This rule for the input chain states that any TCP traffic from the 10.0.10.0 network and destined for any IP address on port 80 is to be accepted.

C- This rule for the output chain states that all traffic from any network and destined for the 10.0.10.0 network on port 80 is to be accepted.

D- This rule states that all web traffic from any network is to jump to the accept rule.

E- This rule states that all incoming web traffic from any network is to be output to the accept rule.

Answer:

A

Question 7

There are several options available to you for your new wireless networking technologies, and you are examining how different systems function. What transmission system uses short bursts combined together as a channel?

Options:

A- Frequency Hopping Spread Spectrum (FHSS)

B- Direct Sequence Spread Spectrum (DSSS)

C- Lamar Anthell Transmission (LAT)

D- Digital Band Hopping (DBH)

E- Digital Channel Hopping (DCH)

Answer:

A

Question 8

Question Type: **MultipleChoice**

You have found a user in your organization who has managed to gain access to a system that this user was not granted the right to use. This user has just provided you with a working example of which of the following?

Options:

A- Intrusion

B- Misuse

C- Intrusion detection

D- Misuse detection

E- Anomaly detection

Answer:

A

Question 9

Question Type: MultipleChoice

You are configuring the new Intrusion Detection System at your office. Your CEO asks you what the IDS will do for the organization. You tell the CEO about the three main components of Network Security and explain how an IDS can be used to meet two of those components. What are the two major components of network security that an IDS can meet?

Options:

A- Prevention

B- Analysis

C- Detection

D- Interpretation

E- Response

Answer:

C, E

Question 10

Question Type: MultipleChoice

Your network is a mixed environment of Windows, Linux, and UNIX, computers. The routers are primarily Cisco and the network uses a T-1 to connect to the Internet. You are experimenting with setting up a mail server in a production environment for internal use only. You do not want this mail server to receive any requests from anywhere but the internal network. Therefore you have decided to block incoming SMTP traffic at the Firewall. Which port will you block at the Firewall?

Options:

A- 23

B- 25

C- 53

D- 80

E- 110

Answer:

B

Question 11

Question Type: **MultipleChoice**

You are configuring your new Intrusion Detection System, and studying the true-false matrix. You read about the different types of alarms and events. Which of the following defines an event where an alarm is indicating an intrusion when there is no actual intrusion?

Options:

A- True-negative

B- False-positive

C- True-positive

D- False-negative

E- Absolute-positive

Answer:

B

Question 12

Question Type: MultipleChoice

You have decided to implement SSH for communicating to your router. What does SSH use to establish a secure channel of communication?

Options:

A- RSA Public Key Cryptography

B- DES Public Key Cryptography

C- MD5 Private Key Cryptography

D- MD5 Public Key Cryptography

E- RSA Private Key Cryptography

Answer:

A