2.1.10 Practice Questions

Candidate: Keith Hibbard (hibbarkm@miamioh.edu)
Date: 1/28/2025, 8:21:44 PM • **Time Spent:** 03:57

Score: 100%

Passing Score: 80%

Question 1. ✓ Correct

What is the purpose of a network model?

→ ◉ Standardize processes at each layer.

○ Provide the logical addressing required to locate your destination node.

○ Used to remotely access application on remote systems.

○ Provide an interface for submitting web requests.

Explanation

The purpose of a network model is to standardize processes at each layer so that the receiving system can make sense of what was sent. This includes data security, addressing, and formatting.

The browser's job is to provide you an interface for submitting web requests.

Telnet is used to either remotely access applications on remote systems or connect to a Cisco device remotely to reconfigure it.

The Internet Protocol (IP) provides the logical addressing required to locate your destination node.

References

2.1.1 Network Models Overview

2.1.2 TCP/IP Model

2.1.3 TCP/IP Model Overview Facts

2.1.4 Application Layer

2.1.5 Transport Layer

2.1.7 Link Layer

2.1.8 TCP/IP Model Facts

2.1.9 TCP and UDP Port Numbers

resources\text\t_tcpipoverview_ccna7\q_tcpipoverview_01_ccna7.question.xml

Question 2. ✓ Correct

Which of the following are limitations of the TCP/IP model? (Select two.)

- [ ] Forces modularity in networking features.
- [ ] Does not aid in troubleshooting.
- [x] TCP/IP layers are theoretical and do not actually perform real functions.
- [x] A particular protocol implementation may not represent every layer.
- [ ] Divides networking tasks into logical layers.

Explanation

You must remember the following limitations of the TCP/IP model:

- TCP/IP layers are theoretical and do not actually perform real functions.
- Industry implementations rarely have a layer-to-layer correspondence with the TCP/IP layers.
- Different protocols within the stack perform different functions, which help send or receive the overall message.
- A particular protocol implementation may not represent every layer (or it may spread across multiple layers).

References

2.1.1 Network Models Overview

2.1.2 TCP/IP Model

2.1.3 TCP/IP Model Overview Facts

2.1.4 Application Layer

2.1.5 Transport Layer

2.1.7 Link Layer

2.1.8 TCP/IP Model Facts

2.1.9 TCP and UDP Port Numbers

resources\text\t_tcpipoverview_ccna7\q_tcpipoverview_02_ccna7.question.xml

Question 3. ✓ Correct

Match the layers of the TCP/IP model to the corresponding layers of the OSI model. (Each option may be used more than once.)

Application

✓ Application

Presentation

✓ Application

Session

✓ Application

Transport

✓ Transport

Network

✓ Internet

Data Link

✓ Link

Physical

✓ Link

Explanation

The Application layer (also called the Process-to-Process layer) corresponds to the Session, Presentation, and Application layers of the OSI model.

The Transport layer (also called the Host-to-Host layer) is comparable to the Transport layer of the OSI model and is responsible for error checking and reliable packet delivery. At this layer, the data stream is broken into segments that must be assigned sequence numbers so that the segments can be reassembled correctly on the remote side.

The Internet layer is comparable to the Network layer of the OSI model. It is responsible for moving packets through a network. This involves the addressing of hosts and making routing decisions to identify how the packet traverses the network.

The Link layer corresponds to the functions of the Physical and Data Link layers of the OSI model. It is responsible for describing the physical layout of the network and how messages are formatted on the transmission medium. Sometimes, this layer is divided into the Data Link and Physical layers.

References

2.1.1 Network Models Overview

2.1.2 TCP/IP Model

2.1.3 TCP/IP Model Overview Facts

2.1.4 Application Layer

2.1.5 Transport Layer

2.1.7 Link Layer

2.1.8 TCP/IP Model Facts

2.1.9 TCP and UDP Port Numbers

resources\text\t_tcpipoverview_ccna7\q_tcpipoverview_03_ccna7.question.xml

Question 4. ✓ Correct

How does TCP handle data sequencing?

- TCP does not sequence the data; it simply passes numbered segments created at a higher layer in the sequence defined.
- → TCP breaks user data into segments, numbers each segment, places them in the correct sequence, and sends each one in order, waiting for an acknowledgement before sending the next segment.
- TCP breaks user data into segments, numbers each segment, and sends each segment in order, without waiting for an acknowledgement.
- TCP breaks the data into segments, numbers each segment, and passes them to UDP, which sequences the segments into the correct order.

Explanation

TCP preserves the sequence of the segments it creates and waits for an acknowledgement before sending the next segment.

UDP simply assigns each segment a number and sends them without paying attention to their order or checking to ensure they arrived at their destination.

References

2.1.1 Network Models Overview

2.1.2 TCP/IP Model

2.1.3 TCP/IP Model Overview Facts

2.1.4 Application Layer

2.1.5 Transport Layer

2.1.7 Link Layer

2.1.8 TCP/IP Model Facts

2.1.9 TCP and UDP Port Numbers

resources\text\t_tcpipmodf_ccna7\q_tcpipmodf_01_ccna7.question.xml

Question 5. ✓ Correct

Which of the following methods helps to detect lost packets? (Select two.)

- [x] Sequencing
- [ ] Buffering
- [x] Acknowledgements
- [ ] CRC
- [ ] Flow control

Explanation

Lost packets can be detected using sequencing or acknowledgements:

- Sequencing assigns a number to each packet. A missing sequence number in received packets indicates a lost packet.
- The receiving device sends acknowledgements to notify the sending device of received packets. If an acknowledgement is not received by the sending device, it assumes a lost packet and retransmits.

Flow control is the mechanism for controlling how much data is sent at a time. Various mechanisms exist for speeding up or slowing down the data transfer rate.

A Cyclical Redundancy Check (CRC) is a mathematical calculation added to each frame. The CRC detects errors in received frames.

Buffering is a method of holding data that needs to be sent. Buffering can be used in flow control to hold packets that cannot yet be transmitted.

References

2.1.1 Network Models Overview
2.1.2 TCP/IP Model
2.1.3 TCP/IP Model Overview Facts
2.1.4 Application Layer
2.1.5 Transport Layer
2.1.7 Link Layer
2.1.8 TCP/IP Model Facts

2.1.9 TCP and UDP Port Numbers

resources\text\t_tcpipmodf_ccna7\q_tcpipmodf_02_ccna7.question.xml

Question 6. ✓ Correct

Which of the following lists accurately describes TCP and UDP? (Select two.)

- → [x] TCP: connection-oriented, reliable, sequenced, high overhead
- [ ] UDP: connection-oriented, reliable, sequenced, high overhead
- [ ] TCP: connection-oriented, reliable, unsequenced, low overhead
- [ ] UDP: connectionless, reliable, sequenced, low overhead
- → [x] UDP: connectionless, unreliable, unsequenced, low overhead
- [ ] TCP: connectionless, unreliable, unsequenced, low overhead

Explanation

TCP and UDP are both Transport and Host-to-Host level protocols, but they have different characteristics.

TCP characteristics include:

- Connection-oriented
- Reliable
- Sequenced
- High overhead

UDP characteristics include:

- Connectionless
- Unreliable
- Unsequenced
- Low overhead

References

2.1.1 Network Models Overview

2.1.2 TCP/IP Model

2.1.3 TCP/IP Model Overview Facts

2.1.4 Application Layer

2.1.5 Transport Layer

2.1.7 Link Layer

2.1.8 TCP/IP Model Facts

2.1.9 TCP and UDP Port Numbers

resources\text\t_tcpipmodf_ccna7\q_tcpipmodf_03_ccna7.question.xml

Question 7. ✓ Correct

Match each layer of the TCP/IP model to its functions. (Each layer matches with two functions.)

Is responsible for how messages are electrically transmitted.

✓ Link

Is responsible for forwarding packets through multiple networks.

✓ Internet

Is responsible for describing the physical layout of the network.

✓ Link

Is responsible for error checking and reliable delivery.

✓ Transport

Is not concerned with reliable delivery of information.

✓ Internet

Integrates network functionality into the host operating system.

✓ Application

Provides the capability for services to operate on the network.

✓ Application

Uses ports to enable application-to-application communications between hosts.

✓ Transport

Explanation

The Application layer contains high-level protocols used by processes (applications) running on a host for network communications. The Application layer integrates network functionality into the host operating system and enables network services. The Application layer does not include specific applications that provide services, but rather provides the capability for services to operate on the network.

The Transport layer is responsible for error checking and reliable delivery. The Transport layer also uses ports to enable application-to-application communications between hosts.

The Internet layer is responsible for forwarding packets through multiple networks. This process is called routing. The Internet layer manages the host addressing and routing decisions to identify how packets traverse networks. The Internet layer is not concerned with reliable delivery of information. Instead, it relies on the Transport layer to establish a host-to-host communication channel and ensure information arrives correctly at the destination host.

The Link layer is responsible for describing the physical layout of the network and how messages are electrically transmitted. It is used to move information between hosts by controlling how individual bits are transmitted and received on the network medium.

References

2.1.1 Network Models Overview

2.1.2 TCP/IP Model

2.1.3 TCP/IP Model Overview Facts

2.1.4 Application Layer

2.1.5 Transport Layer

2.1.7 Link Layer

2.1.8 TCP/IP Model Facts

2.1.9 TCP and UDP Port Numbers

resources\text\t_tcpipmodf_ccna7\q_tcpipmodf_04_ccna7.question.xml

Question 8. ✓ Correct

An internet server has a single network interface that has been assigned an IP address. The server is running both the FTP and HTTP services. A client computer initiates a session with the HTTP server.

How is the HTTP request from the client routed to the correct service running on the server?

- IP address
- Sequence number
- → Port or socket number
- Routing Information Protocol (RIP)
- Session ID

Explanation

Port or socket numbers are used to identify a service running on the server. For example, FTP uses ports 20 and 21 to send communications to the FTP service running on the server, while port number 80 is used for HTTP.

Sequence numbers are used in packets to make sure that packets can be reassembled in the proper order and identify lost packets. The IP address identifies a network interface. Communication instances within the same service but between different clients (or multiple instances with the same client) are kept separate by session IDs. Routing Information Protocol (RIP) is a routing protocol for routing data through an internetwork.

References

2.1.1 Network Models Overview

2.1.2 TCP/IP Model

2.1.3 TCP/IP Model Overview Facts

2.1.4 Application Layer

2.1.5 Transport Layer

2.1.7 Link Layer

2.1.8 TCP/IP Model Facts

2.1.9 TCP and UDP Port Numbers

resources\text\t_com_port_ccna7\q_com_port_01_ccna7.question.xml

Question 9. ✓ Correct

The TCP/IP protocol stack uses port numbers to determine protocol use. Port usage is regulated by the Internet Corporation for Assigning Names and Numbers (ICANN). Which of the following are characteristics of registered ports? (Select two.)

- [ ] Has port numbers ranging from 0 to 1023.
- [x] → Has port numbers ranging from 1024 to 49151.
- [ ] Assigned for specific protocols and services.
- [ ] Has port numbers ranging from 49152 to 65535.
- [x] → Is assigned by ICANN for a network service.

Explanation

A registered port:

- Is assigned by ICANN for a network service.
- Has port numbers ranging from 1024 to 49151.

A well-known port is:

- Assigned for specific protocols and services.
- Has port numbers ranging from 0 to 1023.

A dynamic port:

- Is assigned when a network service establishes contact and released when the session ends.
- Allows applications to listen to the assigned port for other incoming requests. Traffic for a protocol can be received through a port other than the port which the protocol is assigned. This requires that the destination application or service is listening for that type of traffic on that port.
- Has port numbers ranging from 49152 to 65535.

References

2.1.1 Network Models Overview

2.1.2 TCP/IP Model

2.1.3 TCP/IP Model Overview Facts

2.1.4 Application Layer

2.1.5 Transport Layer

2.1.7 Link Layer

2.1.8 TCP/IP Model Facts

2.1.9 TCP and UDP Port Numbers

resources\text\t_com_port_ccna7\q_com_port_02_ccna7.question.xml

Question 10. ✓ Correct

Match each TCP and/or UDP ports to the service that uses it.

Dynamic Host Configuration Protocol (DHCP)

✓ UDP ports 67 and 68

Network News Transport Protocol (NNTP)

✓ TCP Port 119

Simple Network Management Protocol (SNMP)

✓ UDP ports 161 and 162

Domain Name System

✓ TCP and UDP port 53

Telnet

✓ TCP and UDP port 23

Trivil File Transfer Protocol (TFTP)

✓ UDP port 69

Explanation

TCP and UDP use port 23 for Telnet

TCP and UDP use port 53 for Domain Name System (DNS)

UDP uses ports 67 and 68 for Dynamic Host Configuration Protocol (DHCP)

UDP uses port 69 for Trivial File Transfer Protocol (TFTP)

TCP uses port 119 for Network News Transport Protocol (NNTP)

UDP uses ports 161 and 162 usually for Simple Network Management Protocol (SNMP)

References

2.1.1 Network Models Overview

2.1.2 TCP/IP Model

2.1.3 TCP/IP Model Overview Facts

2.1.4 Application Layer

2.1.5 Transport Layer

2.1.7 Link Layer

2.1.8 TCP/IP Model Facts

2.1.9 TCP and UDP Port Numbers

resources\text\t_com_port_ccna7\q_com_port_03_ccna7.question.xml