Module Practice and Quiz

14.8.1

Packet Tracer - TCP and UDP Communications

In this activity, you will explore the functionality of the TCP and UDP protocols, multiplexing, and the function of port numbers in determining which local application requested the data or is sending the data.

TCP and UDP Communications

TCP and UDP Communications

14.8.2

What did I learn in this module?

Transportation of Data

The transport layer is the link between the application layer and the lower layers that are responsible for network transmission. The transport layer is responsible for logical communications between applications running on different hosts. The transport layer includes TCP and UDP. Transport layer protocols specify how to transfer messages between hosts and is responsible for managing reliability requirements of a conversation. The transport layer is responsible for tracking conversations (sessions), segmenting data and reassembling segments, adding header information, identifying applications, and conversation multiplexing. TCP is stateful, reliable, acknowledges data, resends lost data, and delivers data in sequenced order. Use TCP for email and the web. UDP is stateless, fast, has low overhead, does not requires acknowledgments, do not resend lost data, and delivers data in the order it arrives. Use UDP for VoIP and DNS.

TCP Overview

TCP establishes sessions, ensures reliability, provides same-order delivery, and supports flow control. A TCP segment adds 20 bytes of overhead as header information when encapsulating the application layer data. TCP header fields are the Source and Destination Ports, Sequence Number, Acknowledgment Number, Header Length, Reserved, Control Bits, Window Size, Checksum, and Urgent. Applications that use TCP are HTTP, FTP, SMTP, and Telnet.

UPD Overview

UDP reconstructs data in the order it is received, lost segments are not resent, no session establishment, and UPD does not inform the sender of resource availability. UDP header fields are Source and Destination Ports, Length, and Checksum. Applications that use UDP are DHCP, DNS, SNMP, TFTP, VoIP, and video conferencing.

Port Numbers

The TCP and UDP transport layer protocols use port numbers to manage multiple simultaneous conversations. This is why the TCP and UDP header fields identify a source and destination application port number. The source and destination ports are placed within the segment. The segments are then encapsulated within an IP packet. The IP packet contains the IP address of the source and destination. The combination of the source IP address and source port number, or the destination IP address and destination port number is known as a socket. The socket is used to identify the server and service being requested by the client. There is a range of port numbers from 0 through 65535. This range is divided into groups: Well-known Ports, Registered Ports, Private and/or Dynamic Ports. There are a few Well-Known Port numbers that are reserved for common applications such at FTP, SSH, DNS, HTTP and others. Sometimes it is necessary to know which active TCP connections are open and running on a networked host. Netstat is an important network utility that can be used to verify those connections.

TCP Communications Process

Each application process running on a server is configured to use a port number. The port number is either automatically assigned or configured manually by a system administrator. TCP server processes are as follows: clients sending TCP requests, requesting destination ports, requesting source ports, responding to destination port and source port requests. To terminate a single conversation supported by TCP, four exchanges are needed to end both sessions. Either the client or the server can initiate the termination. The three-way handshake establishes that the destination device is present on the network, verifies that the destination device has an active service and is accepting requests on the destination port number that the initiating client intends to use, and informs the destination device that the source client intends to establish a communication session on that port number. The six control bits flags are: URG, ACK, PSH, RST, SYN, and FIN.

Reliability and Flow Control

For the original message to be understood by the recipient, all the data must be received and the data in these segments must be reassembled into the original order. Sequence numbers are assigned in the header of each packet. No matter how well designed a network is, data loss occasionally occurs. TCP provides ways to manage segment losses. There is a mechanism to retransmit segments for unacknowledged data. Host operating systems today typically employ an optional TCP feature called selective acknowledgment (SACK), negotiated during the three-way handshake. If both hosts support SACK, the receiver can explicitly acknowledge which segments (bytes) were received including any discontinuous segments. The sending host would therefore only need to retransmit the missing data. Flow control helps maintain the reliability of TCP transmission by adjusting the rate of data flow between source and destination. To accomplish this, the TCP header includes a 16-bit field called the window size. The process of the destination sending acknowledgments as it processes bytes received and the continual adjustment of the source's send window is known as sliding windows. A source might be transmitting 1,460 bytes of data within each TCP segment. This is the typical MSS that a destination device can receive. To avoid and control congestion, TCP employs several congestion handling mechanisms. It is the source that is reducing the number of unacknowledged bytes it sends and not the window size determined by the destination.

UPD Communication

UDP is a simple protocol that provides the basic transport layer functions. When UDP datagrams are sent to a destination, they often take different paths and arrive in the wrong order. UDP does not track sequence numbers the way TCP does. UDP has no way to reorder the datagrams into their transmission order. UDP simply reassembles the data in the order that it was received and forwards it to the application. If the data sequence is important to the application, the application must identify the proper sequence and determine how the data should be processed. UDP-based server applications are assigned well-known or registered port numbers. When UDP receives a datagram destined for one of these ports, it forwards the application data to the appropriate application based on its port number. The UDP client process dynamically selects a port number from the range of port numbers and uses this as the source port for the conversation. The destination port is usually the well-known or registered port number assigned to the server process. After a client has selected the source and destination ports, the same pair of ports are used in the header of all datagrams used in the transaction. For the data returning to the client from the server, the source and destination port numbers in the datagram header are reversed.

14.8.3

Module Quiz - Transport Layer

1. Which transport layer feature is used to establish a connection-oriented session?

- (•) TCP 3-way handshake
- ( ) UDP ACK flag
- ( ) UDP sequence number
- ( ) TCP port number

2. What is the complete range of TCP and UDP well-known ports?

- (•) 0 to 1023
- ( ) 256 - 1023
- ( ) 1024 - 49151
- ( ) 0 to 255

3. What is a socket?

- (•) the combination of a source IP address and port number or a destination IP address and port number
- ( ) the combination of the source and destination IP address and source and destination Ethernet address
- ( ) the combination of the source and destination sequence and acknowledgment numbers
- ( ) the combination of the source and destination sequence numbers and port numbers

4. How does a networked server manage requests from multiple clients for different services?

- ( ) Each request is tracked through the physical address of the client.
- ( ) The server sends all requests through a default gateway.
- ( ) The server uses IP addresses to identify different services.
- (•) Each request has a combination of source and destination port numbers, coming from a unique IP address.

5. What happens if part of an FTP message is not delivered to the destination?

- ( ) The message is lost because FTP does not use a reliable delivery method.
- ( ) The FTP source host sends a query to the destination host.
- ( ) The entire FTP message is re-sent.
- (•) The part of the FTP message that was lost is re-sent.

6. What type of applications are best suited for using UDP?

- ( ) applications that need reliable delivery
- ( ) applications that are sensitive to packet loss
- ( ) applications that require retransmission of lost segments
- (•) applications that are sensitive to delay

7. Network congestion has resulted in the source learning of the loss of TCP segments that were sent to the destination. What is one way that the TCP protocol addresses this?

- (•) The source decreases the amount of data that it transmits before it receives an acknowledgement from the destination.
- ( ) The destination sends fewer acknowledgement messages in order to conserve bandwidth.
- ( ) The destination decreases the window size.
- ( ) The source decreases the window size to decrease the rate of transmission from the destination.

8. Which two operations are provided by TCP but not by UDP? (Choose two.)

- [ ] identifying individual conversations
- [x] acknowledging received data
- [ ] identifying the applications
- [x] retransmitting any unacknowledged data
- [ ] reconstructing data in the order received

9. What is the purpose of using a source port number in a TCP communication?

- ( ) to assemble the segments that arrived out of order
- ( ) to inquire for a nonreceived segment
- ( ) to notify the remote device that the conversation is over
- (•) to keep track of multiple conversations between devices

10. Which two flags in the TCP header are used in a TCP three-way handshake to establish connectivity between two network devices? (Choose two.)

- [ ] PSH
- [x] ACK
- [x] SYN
- [ ] RST
- [ ] FIN
- [ ] URG

11. What TCP mechanism is used to enhance performance by allowing a device to continuously send a steady stream of segments as long as the device is also receiving necessary acknowledgements?

- ( ) socket pair
- (•) sliding window
- ( ) two-way handshake
- ( ) three-way handshake

12. Which action is performed by a client when establishing communication with a server via the use of UDP at the transport layer?

- (•) The client randomly selects a source port number.
- ( ) The client sends an ISN to the server to start the 3-way handshake.
- ( ) The client sets the window size for the session.
- ( ) The client sends a synchronization segment to begin the session.

13. Which two services or protocols use the preferred UDP protocol for fast transmission and low overhead? (Choose two)

- [ ] HTTP
- [x] DNS
- [x] VoIP
- [ ] POP3
- [ ] FTP

14. Which number or set of numbers represents a socket?

- ( ) 01-23-45-67-89-AB
- ( ) 10.1.1.15
- (•) 192.168.1.1:80
- ( ) 21

15. What is a responsibility of transport layer protocols?

- ( ) translating private IP addresses to public IP addresses
- (•) tracking individual conversations
- ( ) determining the best path to forward a packet
- ( ) providing network access

Check

Show Me

Reset