

Final Term
Handwritten Short Notes: Fall 2024
CS206 – NETWORK DESIGN AND ANALYSIS
MADE BY MUHAMMAD AYAZ

Here are some important lines from the provided topics:

Topic 73: Digital Subscriber Line (DSL)

- "Digital subscriber line (DSL) is an alternative technology for sending and receiving data to and from an ISP, using the same old phone line, but running at much faster speeds."
- "Also, you can make phones calls and surf (send IP packets) at the same time."
- "DSL allows the same old analog voice signal to be sent over the line by a phone. At the same time, DSL allows a separate digital signal to go over the same phone line."
- "The DSLAM splits out the digital signal and analog signal from the local loop." Topic

74: Sending Data without a Phone Line

- "Cable Internet access makes use of the cable television company's existing cable television infrastructure."
- "Fiber optics connects the cable head end to neighborhood-level junctions, from which traditional coaxial cable is then used to reach individual houses."
- "Frequency division multiplexing: different channels transmitted in different frequency bands."

Topic 75: Introduction to AAA Security Model

- "AAA stands for authentication, authorization, and accounting."
- "Authentication is a five-step process."
- "The second 'A' in AAA is for Authorization. It refers to the process of figuring out what a particular user is allowed to do."
- "The last 'A' in AAA is accounting. The same servers that perform authentication and authorization services can keep a record of each request to authenticate or authorize a user."

Topic 76: Password Authentication Protocol (PAP)

- "ISPs authenticate users before they can even use the network."

Muhammad Ayaz WhatsApp 03429311964

- "Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) are used by ISPs."
- "PAP sends the username and password in clear-text."
- "To protect against password theft, CHAP does not send the password as clear- text."
- "CHAP uses six steps to authenticate the user."

Topic 77: Virtual Private Network (VPN)

- "Encryption allows a computer to apply a mathematical formula to data."
- "These days, it is common for users to encrypt data before sending it over the Internet."
- "VPNs create a private network, but they do so logically, or virtually."
- "For Barney to use the VPN, he must encrypt the packet as he creates it."
- "A VPN device inside the corporate network is called a VPN concentrator." Topic

78: Enterprise Network and the Internet

- "When you connect an enterprise network to the Internet, one of the first things you must decide is what you want to allow to pass to and from the Internet."
- "To secure Fredsco's network, two things have to be kept in mind: Between which two hosts do packets need to flow? Which host begins that communication?"
- "Typical types of traffic allowed between an enterprise and the Internet."
- "Traffic that is typically not allowed between an enterprise and the Internet." Topic

79: Firewalls, Demilitarized Zone, IDS:

- "A network engineer configures the firewall with a set of rules that tells it what's legal and what isn't."
- "The firewall allows some packets to pass through it and discards others to

enforce the rules."

- "Cisco's firewall product is called a PIX firewall."
- "As a firewall watches the traffic entering the network, it knows the nature of the traffic that is allowed to flow through it."
- "A host who is initiating a new flow can be recognized by looking at: The first TCP segment used to create a TCP connection SYN flag bit =1, and source IP address of the packet."
- "Firewalls are like routers. They forward packets based on destination IP address."
- "They have at least two physical interfaces. They can have more than two interfaces. Outside interface connects to Internet. Inside interface connects to internal network."
- "A third interface connected to a LAN called a demilitarized zone (DMZ), somewhere between inside & outside interfaces."
- "With a DMZ, Internet-accessible servers can be placed on a different LAN."
- "A stronger firewall rule: No TCP connections can be initiated from outside to the inside. The only flows allowed are for servers in the DMZ."
- "Intrusion detection systems (IDSs) watch packets that a firewall allows through."
- "They look for things in the packets to determine if someone is cheating the firewall and doing bad things to servers in the network."
- "Some IDS devices sit in the network, watching packets that pass over a LAN and are called network-based IDSs."
- "Those IDS software that sit on the servers are called host-based IDSs." For

Topic 80: Introduction to Wireshark, here are some important lines:

- "Wireshark is a network packet analyzer which captures network packets and displays that packet data as detailed as possible."
- "Wireshark is a free open-source software program."

- "Intended purposes of Wireshark: learning network protocol internals, troubleshooting network problems, examining security problems, and debugging protocol implementations."
- "Features of Wireshark: available for UNIX and Windows, live packet data capture, detailed protocol information display, packet filtering, and saving captured packet data."
- "Installation components of Wireshark: Wireshark (the analyzer), TShark (command-line analyzer), plugins & extensions, tools, and user's guide."
- Description and features of the main window in Wireshark. Topic

81: Five Common Network Problems:

- "A service is not running on a server or perhaps a firewall is preventing the connection."
- "TCP connection refusals may also be due to a closed port."
- "Connection Blocked by a Host-Based or Network Firewall"
- "Slow Application at Server"
- "Slow Load of Remote Content"

Topic 82: Next 5 Common Network Problems:

- "The server is up and running, but not responding to requests."
- "Content Redirection"
- "TCP Receive Buffer Full"
- "TCP Send Buffer Full"
- "Altered TCP Attributes along a Path"

Topic 83: Next 6 Common Network Problems:

- "Mismatched TCP Parameters across a Proxy Device"

- "Routing Loops"
- "Weak Signal (WLAN)"
- "Asymmetric Routing"
- "Packet Loss"
- "High Path Latency"

Topic 84: Next 4 Common Network Problems:

- "Lousy Routing Path"
- "Bandwidth Throttling"
- "Delayed ACK"
- "Queued Packets (Overloaded Router)"

Topic 85: Next 5 Common Network Problems:

- "Route Redirections"
- "Broadcast or Multicast Storms"
- "Switch Loop"
- "Virus/Malware on Network Hosts"
- "Network Name Resolution"

Topic 86: Next 8 Common Network Problems:

- "Network Address Resolution"
- "Hardware Address Resolution"
- "No Support for Selective ACK"
- "No Support for Window Scaling"
- "Client Misconfiguration"
- "Low Packet Size/Low MTU Size"
- "TCP Port Number Reuse"
- "Slow Application"

Topic 87: A Four-Part Analysis Methodology:

- Task 1: Define the problem
- Task 2: Collect system, application and path information
- Task 3: Capture and analyze packet flows
- Task 4: Consider tools

Topic 88: Using a Troubleshooting Checklist:

- Verify Trace File Integrity and Basic Communications
- Focus on Complaining User's Traffic
- Detect and Prioritize Delays
- Look for Throughput Issues
- Check Miscellaneous Traffic Characteristics
- Determine TCP Connection Issues/Capabilities for TCP-Based Applications
- Identify Communication Issues for UDP-Based Applications
- Spot Application Errors

Topic 89: Wireshark Lab 1 - Creating a Troubleshooting Profile:

- Creating a new profile in Wireshark
- Customizing profiles with buttons, colors, etc.
- Creating separate profiles for different needs
- Switching between profiles
- Steps to create a Troubleshooting Book Profile

Topic 90: Wireshark Lab 2 - Enhancing Packet List Pane Columns:

- Adding columns to the Packet List pane in Wireshark
- Customizing columns to display additional packet information
- Creating a custom column to locate HTTP delays

Wireshark Lab 3 - Changing Time Column Settings:

- Changing the Time column settings in Wireshark
- Setting the time display format to measure delta time between packets Topic

92: Wireshark Lab 4 - Applying a Filter on Host, Subnet, or Conversation:

- Applying a display filter based on a host address, subnet address, or conversation
- Extracting and saving specific conversations to separate trace files Topic

93: Wireshark Lab 5 - Applying a Filter Using Port Number:

- Defining a display filter based on an application name or port number
- Filtering traffic based on port numbers or application names Topic

94: Wireshark Lab 6 - Applying a Filter Using a Field Value:

- Identifying packets containing specific field values using display filters
- Applying a filter based on field names (e.g., HTTP request method)
- Using right-click to apply a filter based on a field value

Topic 95:

Wireshark Lab 7 focuses on locating buffer problems using the Calculated Window Size field in Wireshark. The steps involved are as follows:

Step 1: Open the file "tr-winsize.pcapng" in Wireshark.

Step 2: Expand any TCP header in the Packet Details pane. Right-click on the Calculated window size field and select "Prepare a Filter | Selected."

Step 3: Change the display filter value to "tcp.window_size < 1000" and click Apply. This filter will display Packet 374, where the client is advertising a 536-byte receive buffer.

Step 4: Click Clear to remove the filter.

The purpose of this exercise is to understand the impact of a low Window Size value on data transmission. When the Window Size value reaches zero, the host cannot accept any more data, leading to a Zero Window condition. In Packet 374, the client's window size is only 536 bytes, which means it can't accept more data. Consequently, data

transmission is halted until the client's buffer size increases. Topic 96:

Wireshark Lab 8 focuses on filtering out "Normal" traffic to focus on anomalies in Wireshark. Here are the steps:

Step 1: Open the file "tr-general.pcapng" in Wireshark.

Step 2: In the display filter area, type "! tcp && !arp" and click Apply. This filter excludes TCP and ARP traffic, displaying 40 packets that match the filter.

Step 3: To remove DNS and DHCP from view, expand the filter by adding "&& !dns && !bootp." This will further narrow down the displayed packets to eight.

By applying these filters, you can isolate and analyze specific types of traffic, allowing you to focus on anomalies or specific network behavior.

Topic 97:

Wireshark Lab 9 demonstrates how to create filter expression buttons in Wireshark. The steps involved are:

Step 1: Open the file "tr-smbjoindomain.pcapng" in Wireshark.

Step 2: Right-click on the TCP header of Packet 11 (the first SYN packet) and select "Expand Subtrees." This will show the SYN bit set to 1.

Step 3: Right-click on the "SYN: Set" line and select "Prepare a Filter | Selected." Wireshark will place the first part of the filter in the display filter area.

Step 4: Scroll down to the TCP Options area and click on the "TCP SACK Permitted Option: True" line. This will display "tcp.options.sack_perm" in the Status Bar area.

Step 5: Expand the filter by typing "&& !tcp.options.sack_perm" to observe TCP handshake packets that do not contain the SACK option.

Step 6: Add "|| !tcp.options.wscale.multiplier" and put parentheses around the options. Step 7:

Click the Save button, name your new button "TCP-HS," and click OK.

Step 8: Click your new TCP-HS button to display the 38 packets that match the filter.

By creating filter expression buttons, you can quickly apply display filters to your traffic, allowing you to identify common network problems or specific packet characteristics.

Topic 98:

Wireshark Lab 10 explains how to launch and navigate through the Expert Infos in Wireshark. The steps are as follows:

Step 1: Open the file "tr-twohosts.pcapng" in Wireshark.

Step 2: Click the Expert Infos button in the bottom left corner of the Status Bar. This will open the Expert Infos window.

Step 3: The Expert Infos window is divided into six tabs: Errors, Warnings, Notes, Chats, Details, and Packet Comments. Explore these.

Topic 99: Wireshark Lab 11

- "Response Code in the Info column for Packet 6 cannot be seen because the Allow subdissector to reassemble TCP streams preference setting is enabled."
- "The Time Since Request (http.time) field indicates the HTTP response time was over 276 seconds."
- "To find the actual HTTP response time, in the Packet Details pane of any packet, right-click the TCP header, select Protocol Preferences and toggle off the Allow subdissector to reassemble TCP streams preference setting."
- "Now click the Go to First Packet button. Notice we see that Packet 6 actually contains the 200 OK response. Examine the HTTP response time value in Packet 6. It is just over 300 ms."

Topic 100: Wireshark Lab 12

- "We are interested in the most active TCP conversation (in bytes) in this trace file. Click the TCP tab and then click the Bytes column heading twice to sort from high to low."
- "The most active conversation is between 192.168.1.72 on port 32313 and 192.87.106.229 on port 80 (listed as http)."
- "Right-click on this top conversation and select Apply as Filter | Selected A <- >B."

Wireshark applies the filter and displays the 123 packets of this conversation." Topic 101:

Wireshark Lab 13

- "By default, Wireshark displays the packets per second rate (packet per tick with a default tick rate of one second)."
- "Click on the first drop in throughput in the graph. Wireshark jumps to that point in the trace file so we can investigate the problem further."
- "Click on the second problem point in the graph. From Wireshark's window, we can see what is happening at this point in the file download process."

Topic 102: Wireshark Lab 14

- "Let's build a coloring rule to highlight DNS errors."
- "When the Reply Code field inside the Flags section contains a 0, the DNS response was successful. If it contains any other value, the response indicates there is a DNS error."
- "Right-click on the Reply Code field and select Colorize with Filter | New Coloring Rule."
- "Enter DNS Errors as the name of your new coloring rule. Change the String value to `dns.flags.rcode > 0`."
- "Your new coloring rule appears at the top of the list of color filters. Packets are processed in order through this list. Now, DNS errors will appear with an orange background."
- "With dns filter still in place, scroll through the packets to see if you notice the two DNS errors in the trace file. Packets 83 & 84 appear with orange."

Topic 103: Capture Options for a Switched Network

- "Because of this, when you connect a system running Wireshark directly to a switch port, you cannot listen to other users' traffic."
- "In order to capture the traffic between the client and the upstream switch (and ultimately a remote host), you need to either (a) Install Wireshark or another capture tool on the user's machine, (b) Make the switch send a copy of the traffic down your analyzer port, or (c) Tap in and obtain a copy of the traffic between the client and the switch."
- "Install Wireshark on User's Machine: This is a great option—if you possible."

- "Switch Port Spanning: The next option to consider is to make the switch send a copy of the traffic down to your analyzer port (aka 'spanning')."
- "Use a Test Access Port ('Tap'): A tap is a simple device that copies all the traffic flowing through it (including those corrupt packets) out to a monitor port."

Topic 104: Wireshark Lab 15

- "You are lucky if your native WLAN adapter can capture WLAN Management and Control traffic. In Monitor Mode, you should be able to see traffic from any network as well."
- "To test the capture capabilities of your WLAN Native Adapter, follow the given steps."
- "If your native adapter is suitable for network capture, you should see some WLAN management and Control traffic (such as Beacon packets and Probe Request/Probe Response packets)."
- "Also, when you look at the data packets you should see an 802.11 header on the data packets. If your adapter strips off the 802.11 header, Wireshark will apply an Ethernet header. In case, you do not see these traffic types or characteristics, consider another solution for WLAN capture."

Topic 105: Wireshark Lab 16

- "Capturing to file sets is an important task when you are working in high traffic situations."
- "File sets are groups of trace files that are linked based on their file name."
- "In this lab exercise, we will use an autostop condition to only capture three files." Topic

106: Wireshark Lab 17

- "Capture filters can reduce the traffic that you need to examine."
- "Here, we will create and use a capture filter based on the MAC address."
- "This will enable us to see all of the traffic to or from our machine." Topic

107: Verify the Target Host Traffic

- "The first step of any analysis process is to verify that the hosts are able to communicate and you can see their traffic in the trace file."
- "If hosts are not able to communicate, there can be several reasons for this."

- "Check Your Capture Process: If you do not see any traffic, something may have gone wrong during the capture process."
- "Consider the TCP/IP Resolution Process: All applications must go through a basic resolution process to build the packet to communicate with another host on a TCP/IP network."

Topic 108: Wireshark Lab 18

- "If a client does not know the IP address of a target (either in cache or a local hosts file), the client can send a DNS query to obtain this information."
- "Step 2: Type dns in the display filter area and click Apply."
- "You can observe from the Status Bar that 32 packets match this filter."
- "From the Info column, you can see a number of No Such Name responses indicating the name resolution process failed."

Topic 109: Wireshark Lab 19

- "Before a client can send a packet to a local target or a local router, it must obtain the MAC (Media Access Control) address of that local target or router."
- "If the client does not have the MAC address information in cache, the client sends out an Address Resolution Protocol (ARP) request."
- "If no response is received when trying to acquire the local target's MAC address, the client is done."
- "Step 2: Scroll through this trace file. Look at the ARP requests sent to discover the MAC address of 192.168.1.45. There are no responses."

Topic 110: Wireshark Lab 20

- "There are several reasons why a server may not respond to a TCP connection attempt."
- "The TCP handshake request packet (SYN) may not arrive at the server."
- "Maybe the SYN packet was lost."
- "A firewall along the path dropped the SYN packet, or a host-based firewall on the server blocked access to the port."
- "Step 2: Scroll through this trace file. This trace file contains only SYN packets from 192.168.1.72 to 192.168.1.66. None of the SYN packets have received

SYN/ACK responses." Topic

111: Wireshark Lab 21

- "The TCP handshake completes successfully in Packets 1-3."
- "The client requests the default file from the web site's root directory in Packet 4."
- "Packet 5 contains acknowledgment no. 288, which indicates that the server has received every sequence no. up to 287, and it expects sequence no. 288 next."
- "The client's browser appears to time out and sends a FIN/ACK after almost 8 seconds."
- "The client waits almost 120 seconds before sending a RST/ACK."
- "TCP appears to be functioning properly in this trace file."
- "The symptoms indicate the application has failed at the server side." Topic

112: Do not Focus on Acceptable Delays

- "You can safely ignore some delays in your trace files."
- "Such acceptable delays should not raise an alarm." Topic

113: Watch for the Delays that DO Matter

- "A large delay before the SYN/ACK is an indication of a high round trip time between the hosts."
- "Time between SYN/ACK and client's ACK to finish TCP handshake can be used by server to determine the round trip time."
- "If you observe that a server quickly sent an ACK to a client's request, but there is a long delay before the server's response, then this is not a path latency issue."
- "There can be several reasons for delays that occur during a file download or file upload process."
- "This situation arises when ACKs from a receiver get delayed because of the path latency or delayed ACK function."
- "A host must wait for a Window Update before sending a packet if it finds that the Window Size advertised is too small to fit a full-sized data segment."

Topic 114: Wireshark Lab 22

- "Delays between requests and responses are a measure for UDP-based applications."
- "UDP conversation statistics such as packet rate, bps rate, etc. can be obtained with Conversations Window."

Topic 115: Wireshark Lab 23

- "In Wireshark, the default Time column setting is Seconds Since Beginning of Capture."
- "It becomes easier to locate delays when a time column displays delta times."
- "We can locate the largest delays in a trace file by sorting the delta time column." Topic

116: Wireshark Lab 24

- "Delays between displayed packets can be identified by using a delta displayed time column."
- "Let's create such a time column to show the delta times of DNS traffic only."
- "Cause for Delays: If a local DNS server does not have these names in its cache, it needs to perform recursive queries to obtain the data."

Topic 117: Wireshark Lab 25 (Plotting UDP Delays)

Step 5: Select the MAX(*) Graph 1 Calc option and enter frame.time_delta_displayed in the Calc area.

Step 6: Click the Graph 1 button to plot the results. If your trace file contains both UDP and TCP-based traffics and you want to plot UDP delays, then enter udp in the Graph 1 filter area before you click the Graph 1 button.

There is a sudden increase in the delta time at approx. 1.2 seconds of the trace file. On clicking these points, Wireshark jumps to that point in the trace file and enables to do additional analysis.

Topic 118: Wireshark Lab 26 (Obtaining TCP Conversation Statistics)

Step 4: Right-click on the top entry and select Apply as Filter | Selected | A <-> B. Wireshark creates a filter based on the source/destination address and source/destination port fields.

Step 5: Click Clear to remove your filter when you are finished. If there are many TCP

conversations contained in your trace file, the method we learned in this topic can be used to find the most active conversation and then quickly apply a filter on that conversation.

Topic 119: Wireshark Lab 27 (Filtering TCP Conversations by Stream Index)

Step 3: Right-click on the [Stream index: 7] field in the TCP header. Select Apply as Filter | Selected.

We can see that Wireshark creates a filter for `tcp.stream==7` in the filter display area and applies it to the trace file. There are 66 packets matching this filter as indicated on the Status Bar.

Topic 120: Wireshark Lab 28 (Adding TCP Stream Index Column)

Step 2: Expand the TCP header in Packet 1. Right-click on the [Stream index: 0] line and select Apply as Column.

Step 3: Click on your Stream index column once to sort the trace file by conversations. Jump to the end of the trace file and you find that there are 23 TCP conversations. Counting TCP streams starts at 0.

Topic 121: Wireshark Lab 29 (Adding/Sorting TCP Delta Time Column)

Step 2: Expand the TCP header in Packet 1. Right click anywhere on the TCP header, select Protocol Preferences and ensure that Calculate conversation timestamps is enabled.

Step 3: At the end of the TCP header, go to the [Timestamps] section, locate and right- click on the Time since previous frame in this TCP stream field. Select Apply as Column.

Step 6: Click the new TCP Delta column heading twice to sort from high to low. The packets with the largest delays before them in a TCP conversation appear at the top of the list.

Topic 122: Wireshark Lab 30:

- Step 2: In the display filter area, enter the following filter: `tcp.time_delta > 1`
- Step 3: Click the Save button on the display filter toolbar. Enter TCP Delay as the

label when prompted. Click OK to save your new button.

- Step 4: Click your new TCP Delay button. You will find that 37 packets match the filter.
- Step 5: Select Edit | Preferences | Filter Expressions, update TCP Delay filter expression to: `tcp.time_delta > 1 && tcp.flags.fin==0 && tcp.flags.reset==0` and then click OK.
- Step 6: Click your TCP Delay button again. 23 packets are displayed because TCP FIN and RST packets have been removed. Let's further remove HTTP GET requests from the TCP Delay button. Add the following string to the end of your filter: `&& !http.request.method=="GET"`. The highest TCP Delta delay is under 6 seconds and is a SYN retransmission pkt. There are 12 SYN retransmissions between the client and 184.73.250.227. There is one SYN/ACK as the RTT is 1.28957 seconds.

Topic 123: Wireshark Lab 31:

- Step 2: Enter `tcp.flags.syn==1` in the display filter area and then click Apply.
- Step 3: Click your TCP Delta column heading twice to sort from high to low. We are interested in the delays preceding SYN/ACK packets.
- We can see that there are three packets that are marked as Retransmissions. These are because of connection establishment problems. We can also observe the RTT to various servers.

Topic 124: RTT: Packets 2 and 3 of TCP Handshake:

- The SYN/ACK packet can be detected by applying the filter: `tcp.flags.syn==1 && tcp.flags.ack==1`.
- Detection of the third packet of the handshake is difficult. Use characteristics such as `tcp.seq==1`, `tcp.ack==1`, `tcp.len > 0`, and `tcp.push==1`.
- The filter becomes `(tcp.flags.syn==1 && tcp.flags.ack==1) || (tcp.seq==1 && tcp.ack==1)`.

Topic 125: Wireshark Lab 32:

- Step 2: Enter the filter `tcp.flags.syn==1` in the display filter area and then click Apply.
- The first two packets are sent from the client port 35,621. Packet 3 and Packet 4 are the first two packets of a new TCP connection.

- The RTT is about 17 ms between the TCP SYN from port 35,622 and the SYN/ACK to that same port.
- Step 3: Enter the filter `(tcp.flags.syn==1 && tcp.flags.ack==1) || (tcp.seq==1 && tcp.ack==1)` and click Apply.
- Step 4: Enhance the filter with the conditions `(tcp.flags.syn==1 && tcp.flags.ack==1) || (tcp.seq==1 && tcp.ack==1) && tcp.len==0 && tcp.flags.fin==0`.

Topic 126: Wireshark Lab 33:

- Step 2: Select Statistics | IO Graph.
- Step 3: In the Y Axis Unit area, select Advanced...
- Step 4: Select the MAX(*) Graph 1 Calc option and enter `tcp.time_delta` in the Calc area.
- Step 5: Click the Graph 1 button to graph the results.
- From the graph, a spike in the RTT values around 25 seconds can be observed.
- Step 6: Enter the expression `tcp.time_delta > 1 && tcp.flags.fin==0 && tcp.flags.reset==0 && !http.request.method=="GET"` in the Filter area of Graph1.

Topic 127: Wireshark Lab 34:

- Step 2: Packet 3 is the first DNS response packet in the trace file. Expand the Domain Name System (response) section.
- Step 3: Right-click on the [Time: 0.107083000 seconds] line and click Apply as Column.
- Step 4: The newly created column appears to the left of the Info column. Drag the new column to the right of the TCP Delta column.
- Step 5: Right-click on the new column heading, select Edit Column Details, and rename the new column to DNS Delta.
- Step 6: Click the DNS Delta column heading twice to sort it from high to low. Topic

128: Wireshark Lab 35:

- Step 2: Type `dns.time > 1` in the display filter area and click Save.
- Step 3: Name the button DNS Delay and click OK.

- Step 4: Click the DNS Delay button to observe the packets that matched the filter. Topic

129: Wireshark Lab 36:

- Step 2: Select Statistics | IO Graph.
- Step 3: In the Y Axis Unit area, select Advanced...
- Step 4: Select the MAX(*) Graph 1 Calc option and enter dns.time in the Calc area.
- Step 5: Click the Graph 1 button to plot the results.
- Step 6: Click on the highest point in the graph to locate the corresponding packet (in this case, packet 3).

Topic 130: Wireshark Lab 37:

- Step 2: Right-click on the TCP header in Packet 5 and select Protocol Preferences. Uncheck "Allow subdissector to reassemble TCP streams" to disable it.

Topic 131: Wireshark Lab 38:

- Step 2: Packet 10 (HTTP 303 See Other) is the first HTTP response packet in the trace file. Right-click on the Hypertext Transfer Protocol section and select "Expand Subtrees".
- Step 3: Right-click on the "[Time since request: 0.026416000 seconds]" line and select "Apply as Column".
- Step 4: Drag the new column to a visible location.
- Step 5: Right-click on the column heading, select "Edit Column Details", and rename it to "HTTP Delta".
- Step 6: Click the "HTTP Delta" column heading twice to sort HTTP responses from high to low.

Topic 132: Wireshark Lab 39:

- Step 2: Type "http.time > 1" in the display filter area and click Save. Name the button "HTTP Delay".

Topic 133: Wireshark Lab 40:

- Step 2: Select Statistics | IO Graph.
- Step 3: In the Y Axis Unit area, select Advanced...

- Step 4: Select the MAX(*) Graph 1 Calc option and enter "http.time" in the Calc area.
- Step 5: Click the Graph 1 button to plot the results.

Topic 134: Wireshark Lab 41:

- Step 2: The first SMB response packet is Packet 5 (Negotiate Protocol Response).
- Step 3: Expand the SMB section and the SMB Header section of Packet 5. Right-click on the "[Time from request: 0.000766000 seconds]" line and click "Apply as Column".
- Step 4: Drag the new column to a visible location.
- Step 5: Right-click on the column heading, select "Edit Column Details", and rename it to "SMB Delta".
- Step 6: Click the "SMB Delta" column heading twice to sort packets from high to low.

Topic 135: Wireshark Lab 42:

- Step 2: Select Statistics | Service Response Time | SMB. Click "Create Stat" when prompted by Wireshark.
- The SMB Service Response Time statistics window shows the minimum, maximum, and average Service Response Time (SRT).
- This window provides a list of all the request procedures. Topic

136: Wireshark Lab 43:

- Step 2: Type "smb.time > 1 || smb2.time > 1" in the display filter area and click Save. Name the button "SMB/SMB2 Delay".

Topic 137: Wireshark Lab 44:

- Step 2: Select Statistics | IO Graph.
- Step 3: In the Y Axis Unit area, select Advanced...
- Step 4: Select the MAX(*) Graph 1 Calc option and enter "smb.time" in the Calc area.

- Step 5: Click the Graph 1 button to plot the SMB response times.
- Step 7: Clicking on the highest points in the graph will take you to the corresponding packets for further analysis.

Topic 138: Wireshark's Expert Infos System:

- Wireshark's Expert Infos System provides alerts and packet comments for network concerns seen in the trace file.
- The Expert Infos button in the Status Bar opens the Expert Infos window.
- Expert infos are classified into categories: Errors, Warnings, Notes, Chats, Details, and Packet Comments.

Topic 139: Wireshark's Packet Loss Detection:

- Packet loss is often caused by overloaded or faulty interconnecting devices like switches or routers.
- Wireshark uses the TCP sequencing process to detect lost packets.
- The nextseq value is used to determine the next expected sequence number, and Wireshark detects lost packets when the sequence number jumps beyond nextseq.

Topic 140: Packet Loss Recovery Methods:

- TCP provides packet loss recovery mechanisms, while UDP does not.
- Fast Recovery is a method where the receiver sends Duplicate Acknowledgments upon observing a jump in sequence numbers.
- Sender Retransmission Timeout (RTO) is a method where the sender retransmits a packet if it hasn't been acknowledged within the RTO value.

Topic 141: Wireshark Lab 45:

- Applying the filter `tcp.analysis.lost_segment` in Wireshark helps count previous segment losses.
- Wireshark can detect packet loss by tracking TCP sequence numbers.
- The "Previous Segment Not Captured" warning indicates missing previous packets in a TCP communication.

Topic 142: Wireshark Lab 46:

- Three columns are created to understand TCP sequencing in Wireshark: SEQ#, NEXTSEQ#, and ACK#.
- The columns help determine the number of lost packets when Wireshark displays "Previous Segment Not Captured."
- The mismatch between SEQ# and NEXTSEQ# values indicates lost packets. Topic

143: Wireshark Lab 47:

- A bad TCP filter expression is built in Wireshark to view key TCP problems.
- The expression is `tcp.analysis.flags && !tcp.analysis.window_update`.
- The Bad TCP button is created to apply the filter and view packets matching the expression.

Topic 144: Wireshark Lab 48:

- Expert Infos in Wireshark are used to find packet loss counts.
- The Warnings tab shows 5 packet losses due to a sudden jump in sequence numbers.
- The Expert Infos window can be expanded to analyze specific packet problems. Topic

145: Wireshark Lab 49:

- The Expert Infos window is opened to examine packet loss.
- Duplicate ACKs are observed after the missing packet indication.
- Duplicate ACKs indicate Fast Recovery and request sequence number 9,164,761.
- Traffic is captured downstream from the point of packet loss. Topic

146: Duplicate ACKs and their Causes:

- Duplicate ACKs inform the sender about packet loss or indicate out-of-order packets.
- Duplicate ACKs are generated if Fast Recovery is supported and a packet arrives with a sequence number beyond the calculated next sequence number.
- Wireshark marks packets as duplicates based on Data bytes, Window Size, Sequence Number, and ACK Number fields.
- Out-of-Order packets are marked if the missing sequence number packet arrives

within 3 ms.

Topic 147: Wireshark Lab 50:

- A filter (`tcp.analysis.duplicate_ack`) is used to count Duplicate ACKs in Wireshark.
- Wireshark detects 1,019 Duplicate ACKs.
- The Duplicate ACKs are requests for a single missing packet with sequence number 9,164,761.

Topic 148: Wireshark Lab 51:

- The Expert Infos window is used to find Duplicate ACKs.
- Duplicate ACKs are grouped based on their number.
- Fast Recovery process is launched multiple times, and recovery occurs with varying numbers of Duplicate ACKs.
- The TCP receiver requested the missing packet 809 times, indicating a significant recovery time.

Topic 149: Wireshark Lab 52:

- Selective ACK (SACK) is examined by analyzing Duplicate ACKs in Wireshark.
- If SACK is in use, only missing packets are retransmitted.
- Duplicate ACKs can indicate if SACK is enabled on the connection.
- SACK Left Edge (SLE) and SACK Right Edge (SRE) information can be found in the packet's Options area of the TCP header.

Topic 150: Out-of-Order Packets and their Causes:

- TCP cannot pass received data to the application layer until all bytes are in the correct order.
- Wireshark labels a packet as out-of-order if it contains data, does not advance the sequence number value, and arrives within 3 ms of the highest sequence number seen.
- Causes of out-of-order packets include multiple speed paths, poorly configured queuing, and asymmetric routing.

Topic 151: Wireshark Lab 53:

- A filter (tcp.analysis.out_of_order) is used to count out-of-order packets in Wireshark.
- Wireshark detects 8 out-of-order packets, with packets 4206 and 32018 identified as out-of-order packets and the remaining 6 packets as a group of out-of-order packets in close proximity.
- Multiple out-of-order packets in close proximity suggest a set of lost packets that are retransmissions arriving within 3 ms.

Topic 152: Wireshark Lab 54:

- The Expert Infos window is used to find out-of-order packets in Wireshark.
- The Out-of-Order segment section is expanded to locate the first entry and examine the packet.
- Sequence number (SEQ#) and Next Sequence Number (NSEQ#) columns are created to analyze the order of packets.
- The out-of-order packet arrived 85 microseconds after the previous packet. Topic

153: Causes of Fast Retransmissions:

- Fast retransmissions occur when three identical ACKs (original ACK and two Duplicate ACKs) arrive at the receiving host.
- Characteristics of fast retransmissions include data or SYN/FIN bits set, no sequence number advancement, matching sequence number and acknowledgment number, and arrival within 20 ms of the last Duplicate ACK.
- Fast retransmissions are a sign of packet loss and are part of the Fast Recovery process.
- Packets are typically lost at infrastructure devices. Topic

154: Wireshark Lab 55:

- A filter (tcp.analysis.fast_retransmission) is used to count fast retransmission packets in Wireshark.
- Wireshark has detected two Fast Retransmissions in the provided trace file.
- Expert Infos in Wireshark mark the Fast Retransmission packet and indicate it as a Retransmission.

Topic 155: Wireshark Lab 56:

- Expert Infos in Wireshark are used to find fast retransmission packets.
- The first entry (Packet 12,035) in the Fast Retransmissions section is examined.
- There are 808 Duplicate ACKs before the Fast Retransmission packet.
- The Fast Retransmission occurred within 20 ms of the last Duplicate ACK. Topic

156: Causes of Retransmissions:

- Wireshark considers a packet to be a Retransmission if it meets certain criteria, such as containing data or having the SYN/FIN bits set.
- Retransmissions can be triggered by a Retransmission Time Out (RTO) at the sender.
- The RTO timer is used to ensure data delivery continues even if the TCP peer stops communicating.
- The sender retransmits the unacknowledged data packet if the RTO timer expires without receiving an ACK.

Topic 157: Wireshark Lab 57:

- The filter `tcp.analysis.retransmission` in Wireshark counts retransmission packets, including Fast Retransmissions.
- To exclude Fast Retransmissions from the filter, the additional condition `tcp.analysis.fast_retransmission && !tcp.analysis.fast_retransmission` is used.
- Wireshark detected 580 Retransmissions in the trace file, including two Fast Retransmissions.

Topic 158: Wireshark Lab 58:

- Expert Infos in Wireshark are used to find retransmission packets.
- Packet 12,259 is examined in the Retransmissions section. Topic

159: Causes of ACKed Unseen Segments:

- ACKed Unseen Segments occur when Wireshark sees an ACK but did not see the corresponding data packet.
- Problems during the capture process, such as dropped packets or asymmetric routing, can cause ACKed Unseen Segments.

Topic 160: Wireshark Lab 59:

- The filter expression `tcp.analysis.ack_lost_segment` is used to count ACKed Unseen Segment warnings in Wireshark.
- Wireshark detected 24 ACKed Unseen Segments in the provided trace file. Topic

161: Wireshark Lab 60:

- Expert Infos in Wireshark are used to find ACKed Unseen Segment indications.
- The first entry, Packet 15, is examined in the Warnings tab. Topic

162: Causes of Keep Alives:

- Keep Alives are TCP packets used to detect dead connections, dead TCP peers, and prevent connection termination when idle.
- Wireshark detects Keep Alives by tracking the Sequence Number field values in TCP streams.
- Applications written to use Keep Alives generate them, and three parameters are defined: Keep Alive Time, Keep Alive Interval, and Keep Alive Probes.

Topic 163: Wireshark Lab 61:

- The filter `tcp.analysis.keep_alive || tcp.analysis.keep_alive_ack` is used to count Keep Alive/Keep Alive ACK packets in Wireshark.
- Only two packets match the filter in the provided trace file. Topic

164: Wireshark Lab 62:

- Expert Infos in Wireshark are used to find Keep Alive/Keep Alive ACK packets.
- Keep Alives and Keep Alive ACKs are used to check for dead TCP peers and avoid timeouts of idle connections.
- Packet 61 is identified as a Keep Alive packet.

Topic 165: Wireshark Lab 63:

- Keep Alive Packets used in Zero Window Conditions are identified in Wireshark.
- TCP hosts can send Keep Alives when the peer is advertising a Zero Window condition.
- Keep Alive ACK responses are not seen in this scenario.

Topic 166: Causes of Reused Ports:

- Reused Ports can cause delays in communications if the previous TCP connection is not terminated.
- Wireshark marks SYN packets with the Reused Ports Expert Analysis definition when it detects a previous SYN packet with the same IP address/port number combination.

Topic 167: Wireshark Lab 74:

- The filter `tcp.analysis.reused_ports` is used to count reused port packets in Wireshark.
- Wireshark detects one reused port in the provided trace file.
- The [SEQ/ACK analysis] section of the reused port packet (number 317) is expanded and colored cyan.

Topic 168: Wireshark Lab 75:

- Expert Infos in Wireshark are used to find reused port packets.
- Packet 317 is identified as a SYN packet with a reused port.
- The sequence number field is used to determine if the SYN packet belongs to a unique connection request, retransmission, or reused port.

Topic 169: Causes of Checksum Errors:

- Checksums are used to detect errors in transmitted segments.
- Faulty Network Interface Cards (NICs) or devices that alter packet content can cause checksum errors.
- Task offloading and enabled checksum validation processes in Wireshark can also lead to checksum errors.

Topic 170: Wireshark Lab 76:

- Checksum validation for IPv4, TCP, and UDP can be enabled in Wireshark's Preferences.
- Packets with bad IPv4, TCP, and UDP checksums are highlighted in the Packet List pane.
- Expert Infos in Wireshark display the number of bad checksums for each protocol.

Topic 171: Wireshark Lab 77:

- DNS errors include server failure (Reply Code 2) and name error (Non-Existent Domain, Reply Code 3).
- Creating a button in Wireshark can help identify DNS errors.
- The filter `dns.flags.rcode > 0` is used to locate DNS error packets.
- DNS error responses can be due to a server upstream from the local server not responding to recursive DNS queries.

Topic 172: Wireshark Lab 78:

- A button is created to identify HTTP errors in trace files using the filter `http.response.code >= 400`.
- Clicking the button identifies the two HTTP error responses in the trace file (404 "Not Found" errors).
- Packet 61 is analyzed using the Follow TCP Stream option to determine the item that was not found on the server.

Topic 173: Introduction to Packet Tracer:

- Packet Tracer is a network simulator from Cisco that allows users to simulate Cisco devices and troubleshoot networks.
- It supports logical and physical workspaces for building network topologies.
- Packet Tracer has two operating modes: real-time mode and simulation mode.
- The latest version of Packet Tracer can be downloaded for free from the given website.

Topic 174: Packet Tracer's Interface Overview:

- The layout of Packet Tracer includes components like the menu bar, main toolbar, physical/logical workspace tabs, common tools bar, workspace, and real-time/simulation tabs.
- The user-created packet box and network component box are used to create customized packets and access network devices.

Topic 175: Creating a Simple topology:

- Steps are provided for creating a simple topology in Packet Tracer, including

selecting end devices, connecting them using Copper Cross-Over, configuring IP addresses, and testing connectivity.

Topic 176: Introduction to Cisco and PT devices

- "Routers, switches are used to Interconnect end devices such as PCs, laptops, servers."
- Description of various Cisco routers and their specifications.
- Description of various Cisco switches and their specifications.
- Explanation of Bridge PT, Generic Switch PT, Hub PT, Repeater PT, and Coaxial Splitter PT.

Topic 177: Customizing Devices with Modules

- Explanation of adding and removing modules in devices.
- Naming conventions for router interfaces based on their types. Topic

178: Accessing CLI of a Device

- Explanation of accessing the Command Line Interface (CLI) of a device in Packet Tracer.
- Description of accessing CLI through the CLI Tab and Console port. Topic

179: Configuring Devices with Config Tab

- Explanation of configuring routers and switches using the Config tab in Packet Tracer.
- Overview of Global, Interface, and Routing settings in the Config tab.
- Mention of VLAN database for configuring VLANs on a switch.

Topic 180: Generic IP End Devices in PT

- "Network devices such as switches, routers are the core of a network."
- "End devices (PCs, servers) are the ones that use this core."
- "A) Clients: Desktops and laptops: As far as usability is concerned, there is no difference between them."
- "B) Servers: Space for two network interfaces."

- "HTTP service: Both HTTP and HTTPS (HTTP employing Secure Sockets Layer (SSL) protocol) protocols can be supported by a web server."
- "DHCP service: can assign IP addresses to routers."
- "DNS service: resolves domain names to IP addresses."
- "AAA service: Authentication, Authorization, and Accounting and supports RADIUS and TACACS authentication protocols."
- "NTP: Network Time Protocol ensures that the clocks of all devices are synchronized properly."
- "EMAIL services: SMTP and POP3 services are supported."
- "FTP Services: Users can be created and permissions can be granted to them."
- "Firewall: You can configure rules based on source/destination IP addresses and source/destination port numbers."

Topic 181: Configuring End Devices in PT

- "Click on an end device in the workspace, then go to the Desktop tab."
- "IP Configuration: With this utility, you can assign a dynamic or static IP address to an end device."
- "Dial-up: End devices such as PC-PT and Laptop-PT have the PC-HOST-NM-1AM. This utility allows simulating a modem dialer."
- "Terminal: This utility can be used for accessing the CLI through the console port."
- "Web Browser: It can be used with a Server-PT configured with HTTP."
- "VPN: Virtual private network (VPN) is used to create a connection for secure communication."
- "Email: You can send and receive emails with the help of this utility."
- "Text Editor: You can use this utility to create, edit, and save text files." Topic

182: Packet Tracer's Simulation Mode

- "In Packet Tracer's simulation mode, you can observe packets flowing from one device to another."
- "Step 5: Click on the real time/simulation tab and switch to the simulation mode."

- "Step 6: Click on the Auto Capture / Play button. Packet capture begins."
- "To view a packet's TCP/IP layers information, click on a packet (the envelope icon)."
- "The simulation mode has control buttons: Back, Auto Capture / Play, Capture/Forward."

Topic 183: Connecting Devices and Link Status

- "In Packet Tracer, there are a number of cables available to connect devices."
- "Console: The console port of a network device can be connected to the RS-232 port on a PC/laptop."
- "Copper straight-through: It is a standard Ethernet cable that connects devices operating in different layers of the OSI model."
- "Copper cross-over: This Ethernet cable connects devices such as hub to hub, PC to PC, PC to router, and PC to printer."
- "Fiber: Connects Fast Ethernet and Gigabit Ethernet ports of a fiber port."
- "Serial DCE and DTE: Serial cables connect routers together."
- "Link status: Once you have connected devices together, you will find a light, at each end of the cable."

Topic 184: Testing Connectivity with PDUs

- "Connectivity can be tested by using either simple or complex Protocol Data Units (PDUs) or pinging devices from their command-line interface."
- "Simple PDU: The Add Simple PDU tool relies on Internet Control Message Protocol (ICMP)."
- "Complex PDU: We use the previous example to understand the working of Complex PDU."

Topic 185: Clustering a Topology

- "Clustering combines several devices that you choose into a single cloud icon."
- "Upon double-clicking the cluster, it will get expanded and will display the devices normally."
- "Step 1: Let's create a topology that consists of three switches and nine PCs."

- "Step 2: Combine PC0, PC1, PC2 and Switch0."
- "Step 3: Form a group of PC3, PC4, PC5 and Switch1."
- "Step 4: Repeat the same procedure done in Steps 2 and 3 for combining PC6, PC7, PC8 and Switch2."
- "Double-clicking on a cluster expands it and displays only the devices within it." Topic

186: Creating Cities, Offices & Wiring Closets

- "Packet Tracer can simulate the required environment logically and physically."
- "There are 4 environments available in the physical workspace: Intercity, City, Building, and Wiring closet."
- "1-Intercity: Being the largest environment, it consists of cities. You can create cities, buildings, and wiring closets in this layer."
- "2-Cities: Buildings and wiring closets are part of it."
- "3-Buildings: It contains only wiring closets."
- "4-Wiring closet: This layer contains only devices."
- "Step 1: Create a topology consisting of two PCs in the logical workspace."
- "Step 2: As Ethernet has distance restrictions, switch off both the PCs and replace their default modules with PT-HOST-NM-1FGE."
- "Step 3: Connect both of the PCs with a fiber cable and assign IP addresses."
- "Step 4: Switch to the physical view, and click on the New City button. Rename it Lahore."
- "Step 5: Use the NAVIGATION button and go to Home City | Corporate Office | Main Wiring Closet. Both the PCs we inserted in the logical workspace are located here."
- "Step 6: Use the Move Object button and move one of the PCs to Lahore| Office Building | Wiring Closet."

Topic 187: Managing Cables and Distances

- "In physical view, we can measure a cable's distance by placing the pointer on the cable."
- "The length of Standard copper Ethernet cables can extend up to 100 meters."

- "Step 1: Create a topology consisting of two PCs in the logical workspace."
- "Step 2: Connect both of the PCs with a copper cable and assign IP addresses."
- "Step 3: Switch to the physical view, and click on the New City button. Rename it Lahore."
- "Step 6: Check the distance between them. In case the distance is less than 100 meters, move them further apart, so that the distance becomes greater than 100 meters."

Topic 188: Static Routing with GUI

- "In static routing algorithms, routes change very slowly over time, often as a result of human intervention."
- "Step 1: Drag and drop 4 routers in the workspace."
- "Step 2: Click on a router icon, go to the Config tab, select an interface, and configure the IP address."
- "Step 3: Now go to the ROUTING section, and click on Static."
- "Step 4: Test the connectivity between all of the routers with the help of simple PDU."
- "Step 5: Let's view the routing table of a router. Go to the Common tools bar, click on the inspect icon. Select a router and click on it. Then select Routing Table."

Topic 189: Static Routing with CLI

- "Step 1: Drag and drop 4 routers in the workspace."
- "Step 2: Click on a router icon, go to the CLI tab. As the device boots up, then you will see the prompt."
- "Step 3: Assign IP addresses to R1's interfaces."
- "Step 4: Configure static routing."
- "Step 5: Test the connectivity between all of the routers with the help of simple PDU."

Topic 190: Configuring RIP with GUI

- "Dynamic Routing Protocols: A) Form 'neighbor ship' with other routers. B) Send them the directly-connected routes and other received routes."

- "A GUI to configure a dynamic routing protocol called Routing Information Protocol (RIP) is available in Packet Tracer."
- "Step 1: Drag and drop 4 routers in the workspace."
- "Step 2: Click on a router icon, go to the Config tab, select an interface, and configure the IP address."
- "Step 3: Click on RIP. Enter Network IP of its own interfaces."
- "Step 4: Once the topology is configured, use the simple PDU to check for connectivity."
- "Step 5: Use the delete tool and remove one link. Let's say we remove the link between R1 and R2. Use the simulation mode and test connectivity with the simple PDU. The packet takes the alternate, longer route and succeeds in reaching the destination."

Topic 191: Configuring RIP with CLI

- "Let's assume a network consisting of four routers in a ring topology, with no PCs or loopback interfaces."
- "Step 1: Drag and drop 4 routers in the workspace."
- "Step 2: Click on a router icon, go to the CLI tab. As the device boots up, then you will see the prompt."
- "Step 3: Assign IP addresses to R1's interfaces:"
- "Repeat Step 3 for the remaining routers with the following configurations for their interfaces:"
- "Step 4: Enter into the config mode of RIP:"
- "Step 5: Enter the network IP addresses:"
- "Step 6: Test the connectivity between all of the routers with the help of simple PDU."

Topic 192: Load Sharing

- "When a source router has multiple paths to a target path, then it can load balance traffic across them."
- "Assume a network that consists of four routers in a ring topology with no PCs."

- "Step 1: Drag and drop 4 routers in the workspace."
- "Step 2: Configure the IP address."
- "Step 3: Configure Network IP of its own interfaces."
- "Step 4: On Router 4, let's add a loopback interface (a virtual interface that works like a real interface and needs IP address)."
- "Step 5: Go to the RIP config mode and enter the network IP for this loopback interface."
- "Step 6: Create a complex PDU that is sent every two seconds."
- "Step 7: Turn on the simulation mode. You will find that the first packet takes the R1-R2-R4 route while the second takes the R1-R3-R4 route."

Here are the important topics :

Topic 185: Clustering a Topology

Topic 186: Creating Cities, Offices & Wiring Closets Topic

187: Managing Cables and Distances

Topic 188: Static Routing with GUI Topic

189: Static Routing with CLI Topic 190:

Configuring RIP with GUI Topic 191:

Configuring RIP with CLI Topic 192: Load

Sharing