LAB 1

1. What is the primary purpose of Wireshark in networking? a) To analyze network traffic b) To configure network interfaces c) To perform traceroute checks d) To scan multiple IP addresses
2. Which command is used to capture packets with tcpdump? a) tcpdump -i any b) sudo ifconfig interface_name down c) sudo traceroute -n www.google.com d) nmap www.pes.edu
3. What does the TTL field in a ping packet stand for? a) Time To Leave b) Time To Load c) Time To Live d) Time To Listen
4. Which of the following tools is used to test connectivity between two systems? a) Wireshark b) Tcpdump c) Ping d) Traceroute
5. What does the command `sudo tcpdump -c5 icmp` do? a) Captures 5 ICMP packets b) Captures all packets in any interface c) Captures HTTP content of web requests d) Saves packets to a file instead of displaying them on the screen
6. What is the purpose of the `-I` option in the `traceroute` command? a) To speed up the process b) To disable the mapping of IP addresses with hostnames c) To specify the protocol used (ICMP) d) To test a TCP connection instead of ICMP
7. Which command is used to explore an entire network for information? a) sudo traceroute -I www.google.com b) nmap www.pes.edu c) nmap 163.53.78.128 d) sudo tcpdump -i any
8. What information can be obtained by analyzing HTTP packet capture using Wireshark? a) IP address and MAC address of the sender b) IP address and MAC address of the receiver c) Source and destination ports d) All of the above
9. Which of the following commands is used to save packets to a file instead of displaying them on the screen with tcpdump? a) -D b) -c10 c) -w d) -A
10. What does the `-T` flag in the `traceroute` command indicate? a) It specifies the protocol used (ICMP) b) It disables the mapping of IP addresses with hostnames c) It tests a TCP connection instead of ICMP d) It speeds up the process

1. a) To analyze network traffic
2. a) tcpdump -i any
3. c) Time To Live
4. c) Ping
5. a) Captures 5 ICMP packets
6. d) To test a TCP connection instead of ICMP
7. c) nmap 163.53.78.128
8. d) All of the above
9. c) -w
10. c) It tests a TCP connection instead of ICMP

LAB 2

1. What is the purpose of Cisco Packet Tracer in the context of this lab? a) To replicate network scenarios b) To configure PCs and routers c) To simulate data interactions d) All of the above
2. In Task 2, what is the objective of adding interfaces to the router? a) To increase network performance b) To configure network protocols c) To provide connectivity to different networks d) To monitor network traffic
3. Which command is used to add interfaces to a router in Cisco Packet Tracer? a) add interface b) configure terminal c) ip interface d) interface fastethernet

4. How many interfaces are typically available on a router in Cisco Packet Tracer? a) 1 b) 2 c) 4 d) 8
5. What is the function of configuring IP addresses on router interfaces? a) To connect to the internet b) To establish VPN connections c) To enable routing between networks d) To secure the router from attacks
6. Which tool in Cisco Packet Tracer is used to configure router interfaces? a) CLI (Command Line Interface) b) Simulation mode c) Configuration panel d) Device Manager

1. d) All of the above
2. c) To provide connectivity to different networks
3. d) interface fastethernet
4. c) 4
5. c) To enable routing between networks
6. c) Configuration panel

Lab 3

1. What is the purpose of configuring persistent and non-persistent HTTP connections in this experiment? a) To increase server security b) To decrease server load c) To measure performance impact d) To enhance browser compatibility
2. Which tool is used to capture packets between the client and server in this experiment? a) Apache HTTP server b) Wireshark c) Firefox browser d) Apache2 configuration file
3. What does setting the value of max-persistent-connection-per-server to 0 simulate in the experiment? a) Non-persistent connections b) 2 persistent connections c) 4 persistent connections d) 6 persistent connections
4. How is the time taken to load objects from the server measured in the experiment? a) Using the Apache2 configuration file b) By analyzing network packets with Wireshark c) Through browser settings in Firefox d) By accessing the server's landing page
5. What is the significance of the persistent-settings value being set to true in the experiment? a) It enables caching on the client-side b) It allows for persistent connections between client and server c) It increases server security d) It improves server performance
6. Which setting is adjusted to configure the number of persistent connections in the experiment? a) Max-persistent-connections-per-server b) Persistent-settings c) Cache-settings d) Apache2 configuration
7. What does a value of 2.429637133 - 2.070581279 represent in the experiment? a) Time taken to configure persistent connections b) Time taken to load objects with non-persistent connections c) Time taken to clear browser cache d) Time taken to load objects with persistent connections
8. Which step is necessary to clear cache before starting the web request in the experiment? a) Setting max-persistent-connection-per-server to 0 b) Running

Wireshark on the client-side c) Clearing browser cache in Firefox d) Setting persistent-settings to false

9. What is the optimal number of persistent connections for best performance based on the experiment? a) 2 b) 4 c) 6 d) 10
10. What is the significance of modifying the Apache2 configuration file in the experiment? a) To install Apache server b) To configure IP addresses c) To enable persistent connections d) To adjust browser settings

1. c) To measure performance impact
2. b) Wireshark
3. a) Non-persistent connections
4. b) By analyzing network packets with Wireshark
5. b) It allows for persistent connections between client and server
6. a) Max-persistent-connections-per-server
7. b) Time taken to load objects with non-persistent connections
8. c) Clearing browser cache in Firefox
9. d) 10
10. c) To enable persistent connections

Lab 4

1. What is the primary purpose of a DNS server? a) To configure network devices b) To assign IP addresses to devices c) To translate domain names to IP addresses d) To establish secure connections between devices
2. Which device is responsible for hosting the Local DNS server in the network topology? a) PC0 b) PC1 c) Router d) Server
3. What is the IP address of the Local DNS server? a) 192.168.1.1 b) 192.168.1.2 c) 192.168.1.3 d) 192.168.1.4
4. How is the DNS service enabled on the server in Cisco Packet Tracer? a) Click on Server, then DNS, and enable DNS service b) Run a command in the Command Prompt to enable DNS c) Edit the server's configuration file to enable DNS d) Access the server's web interface and enable DNS from there
5. What command is used to ping another device in the network by its IP address? a) ping b) traceroute c) nslookup d) ifconfig
6. In Task 2, what action do students need to perform to successfully ping a device by its name? a) Configure IP addresses manually b) Enable DHCP on the router c) Add entries in the DNS server d) Install additional network interfaces
7. Which service needs to be enabled on the Web Server to access HTML contents? a) FTP b) SSH c) HTTP d) DNS
8. How can students access the HTML contents hosted on the Web Server? a) By typing the IP address of the Web Server in the browser b) By typing the domain name of the Web Server in the browser c) By running a specific command in the Command Prompt d) By accessing the Web Server's configuration file

9. What is the purpose of editing the Index.html file on the Web Server? a) To configure DNS settings b) To assign IP addresses to devices c) To customize the web page content d) To enable secure connections
10. Which protocol is used to access web pages in a browser? a) FTP b) SSH c) HTTP d) DNS

1. c) To translate domain names to IP addresses
2. d) Server
3. a) 192.168.1.1
4. a) Click on Server, then DNS, and enable DNS service
5. a) ping
6. c) Add entries in the DNS server
7. c) HTTP
8. b) By typing the domain name of the Web Server in the browser
9. c) To customize the web page content
10. c) HTTP

Lab 5

1. What is the primary aim of the experiment on TCP Congestion Window using Wireshark? a) To analyze UDP traffic patterns b) To understand TCP flow control mechanisms c) To measure network latency d) To investigate DNS resolution issues
2. How can the Congestion Window (CW) be plotted using Wireshark? a) Through the HTTP filter b) Using the Statistics menu and selecting TCP Stream Graphs -> Window Scaling c) By analyzing DNS packets d) Through the ICMP filter
3. What triggers Fast Retransmit in TCP? a) Three consecutive duplicate packets b) Loss of SYN packets c) High network latency d) Full Congestion Window
4. Which parameter does TCP reduce to 1 during Fast Retransmit? a) Congestion Window b) Round-Trip Time c) Timeout Interval d) Maximum Segment Size
5. What does the first dip in the Congestion Window graph indicate? a) Slow Start b) Congestion Avoidance c) Timeout d) Fast Retransmit
6. Which option in Wireshark allows users to analyze the Congestion Window graph? a) TCP Insights b) Window Scaling c) Traffic Analysis d) Packet Filtering
7. How does TCP react to congestion after Fast Retransmit? a) Enters Slow Start phase b) Increases the Congestion Window linearly c) Enters Congestion Avoidance phase d) Initiates a timeout
8. What does the term "TCP flavor" refer to in the context of TCP Congestion Control? a) Type of encryption used in TCP packets b) Specific implementation of TCP congestion control algorithms c) Version of the TCP protocol d) Type of payload carried by TCP packets
9. In which phase does TCP gradually increase the Congestion Window until congestion is detected? a) Slow Start b) Fast Recovery c) Congestion Avoidance d) Fast Retransmit

1. b) To understand TCP flow control mechanisms
2. b) Using the Statistics menu and selecting TCP Stream Graphs -> Window Scaling
3. a) Three consecutive duplicate packets
4. a) Congestion Window
5. d) Fast Retransmit
6. b) Window Scaling
7. c) Enters Congestion Avoidance phase
8. a) GitHub repository
9. b) Specific implementation of TCP congestion control algorithms
10. a) Slow Start

---

1. Which command is used to display the IP configuration of a network interface in Linux? a) ipconfig b) ifconfig c) ping d) traceroute
2. What does the "ping" command do? a) Displays IP configuration details b) Traces the route to a destination c) Sends ICMP echo requests to test network connectivity d) Retrieves the DNS information of a domain
3. Which command is used to find the MAC address of a device in Windows? a) macconfig b) ifconfig c) arp d) netstat
4. What does the "arp" command do? a) Displays the IP configuration details b) Sends ICMP echo requests to test network connectivity c) Retrieves the DNS information of a domain d) Displays the ARP cache and MAC addresses associated with IP addresses
5. Which command is used to find the IP address of a domain in Linux? a) ping b) nslookup c) tracert d) ipconfig
6. What does the "nslookup" command do? a) Displays the IP configuration details b) Traces the route to a destination c) Sends DNS queries to resolve domain names to IP addresses d) Retrieves the DNS information of a domain
7. Which command is used to display the routing table in Linux? a) route b) ifconfig c) netstat d) traceroute
8. What does the "netstat" command do? a) Displays the routing table b) Sends DNS queries to resolve domain names to IP addresses c) Retrieves the DNS information of a domain d) Displays network connections, routing tables, interface statistics, masquerade connections, and multicast memberships
9. Which command is used to configure the IP address of a network interface in Linux? a) ipconfig b) ifconfig c) ping d) traceroute
10. What does the "ifconfig" command do? a) Displays IP configuration details b) Sends ICMP echo requests to test network connectivity c) Retrieves the DNS information of a domain d) Configures network interfaces on Linux systems

---

1. b) ifconfig
2. c) Sends ICMP echo requests to test network connectivity

3. c) arp
4. d) Displays the ARP cache and MAC addresses associated with IP addresses
5. b) nslookup
6. c) Sends DNS queries to resolve domain names to IP addresses
7. c) netstat
8. d) Displays network connections, routing tables, interface statistics, masquerade connections, and multicast memberships
9. b) ifconfig
10. d) Configures network interfaces on Linux systems