**Exploring the Networks [IT 307]**

SUBMITTED BY:

NAME:

ENROLLMENT NO:

B. TECH(CSE)

BATCH 2018-2022, 5th SEMESTER, SECTION-**5CSE3**

SUBMITTED TO:

FACULTY NAME: **Dr. Achyut Shankar**



`

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**AMITY SCHOOL OF ENGINEERING AND TECHNOLOGY**

**AMITY UNIVERSITY UTTAR PRADESH NOIDA**

|  |  |  |
| --- | --- | --- |
| **Ex No.** | **Name of Experiment** | **Signature of faculty** |
|  | Basic Networking Commands using Command Prompt/PowerShell |  |
|  | Basic Topology Creation and check connectivity of end points |  |
|  | Switch Configuration |  |
|  | Telnet and SSH Configuration on both Router and Switch. |  |
|  | DHCP Configuration for single interface as well as VLANs |  |
|  | Router Configuration |  |
|  | Setup Wireless Local Area Network |  |
|  | To capture and analyze packets in Wireshark for ICMP and DNS |  |
|  | To capture and analyze TCP handshake in Wireshark |  |
|  | To capture and analyze UDP packets in Wireshark using DNS query |  |
|  |  |  |

**Experiment – 1**

**Aim:** Basic Networking Commands using Command Prompt/PowerShell

**Theory and Commands:**

**Note: Attach all commands and screenshots which you performed during the lab sessions**

**Experiment – 2**

**Aim:** Basic Topology Creation and check connectivity of end points

**Theory:**

Topology is the logical design of a network in premises for providing quality of service, fault tolerance, etc. solutions to the end point users. The devices used in topologies are Routers, Switches, Endpoint Devices, etc.

**Commands:**

* **Ping**

**Objective:**

* Create a topology and assign IP address to networking as well as end devices.
* Configure router for communication across networks.
* Check network connectivity using Ping command from the endpoint devices.
* Send packet data units from one device to another and analyze their paths.
* Analyze mac address stick to IP address using the ARP command.

**Result:**

**Note: Attach Screenshots which you took during the lab sessions**

**Experiment – 3**

**Aim**: Switch & Router Configuration

**Theory**:

A network switch is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device. A network switch is a multiport network bridge that uses MAC addresses to forward data at the data link layer of the OSI model.

A router is a [networking device](https://en.wikipedia.org/wiki/Networking_device) that forwards [data packets](https://en.wikipedia.org/wiki/Data_packet) between [computer networks](https://en.wikipedia.org/wiki/Computer_network). Routers perform the traffic directing functions on the [Internet](https://en.wikipedia.org/wiki/Internet). Data sent through the internet, such as a [web page](https://en.wikipedia.org/wiki/Web_page) or [email](https://en.wikipedia.org/wiki/Email), is in the form of data packets. A packet is typically [forwarded](https://en.wikipedia.org/wiki/Packet_forwarding) from one router to another router through the networks that constitute an [internetwork](https://en.wikipedia.org/wiki/Internetwork) (e.g. the Internet) until it reaches its destination [node](https://en.wikipedia.org/wiki/Node_(networking)).

A wireless network is a computer network that uses wireless data connections between network nodes. There are basically three different types of wireless networks – WAN, LAN and PAN.

**Commands**:

* hostname,
* enable password \*\*\*\*\*\*
* enable secret \*\*\*\*\*
* login console 0
* login vty 0 15
* motd banner \* Message \*
* vlan (Number)
* name (Name of VLAN)
* hostname,
* enable password \*\*\*\*\*\*
* enable secret \*\*\*\*\*
* login console 0
* login vty 0 15
* motd banner \* Message \*
* int fa0/0.1

**Objective:**

* To configure the switch to provide most secure and reliable service
* Change hostname of the switch
* Privilege Login password protected
* Making both console and remote connection password protection
* Configure banner i.e. Message of the Day to be display while connected to the switch
* Configuring VLANs on switch for logical separation of networks
* To configure the router to provide most secure and reliable service
* Change hostname of the router
* Privilege Login password protected
* Making both console and remote connection password protection
* Configure banner i.e. Message of the Day to be display while connected to the router
* VLAN connection through a single physical connection through trunking.
* Create topology and configure wireless router either by browser on pc or by clicking on wireless router.
* Change username and password of wireless router.
* Configure security of wireless connection on wireless router.
* Configure LAN interface settings by configuring setup settings and network settings on wireless router.
* Configure DHCP server on router which will act as an internet service provider.
* Configure server.
* Ping pc with laptop within LAN and ping PC or laptop with server outside LAN.

**Result:**

**Note: Attach Screenshots which you took during the lab sessions**

**Experiment – 4**

**Aim:** Telnet and SSH Configuration on both Router and Switch.

**Theory:**

Telnet is an [application protocol](https://en.wikipedia.org/wiki/Application_layer) used on the [Internet](https://en.wikipedia.org/wiki/Internet) or [local area network](https://en.wikipedia.org/wiki/Local_Area_Network) to provide a bidirectional interactive text-oriented communication facility using a virtual [terminal](https://en.wikipedia.org/wiki/Text_terminal) connection. User data is interspersed [in-band](https://en.wikipedia.org/wiki/In-band_signaling) with Telnet control information in an 8-bit [byte oriented](https://en.wikipedia.org/wiki/Byte_oriented) data connection over the [Transmission Control Protocol](https://en.wikipedia.org/wiki/Transmission_Control_Protocol) (TCP). SSH provides a [secure channel](https://en.wikipedia.org/wiki/Secure_channel) over an unsecured network by using a [client–server](https://en.wikipedia.org/wiki/Client%E2%80%93server_model) architecture, connecting an [SSH client](https://en.wikipedia.org/wiki/SSH_client) application with an [SSH server](https://en.wikipedia.org/wiki/SSH_server). The protocol specification distinguishes between two major versions, referred to as SSH-1 and SSH-2. The standard TCP port for SSH is 22. SSH is generally used to access [Unix-like](https://en.wikipedia.org/wiki/Unix-like) operating systems, but it can also be used on [Microsoft Windows](https://en.wikipedia.org/wiki/Microsoft_Windows). [Windows 10](https://en.wikipedia.org/wiki/Windows_10) uses [OpenSSH](https://en.wikipedia.org/wiki/OpenSSH) as its default [SSH client](https://en.wikipedia.org/wiki/SSH_client) and [SSH server](https://en.wikipedia.org/wiki/SSH_server).

**Commands:**

* Line vty 0 4
* Transport input telnet
* Motd
* Int fa0/0
* Int vlan (VLAN Number) (For switch)
* Ip address (ip) (subnet mask)
* telnet (IP)
* ip domain-name (name)
* username (name) password (password)
* crypto key rsa 1024
* ip ssh version 2
* Line vty 0 4
* Transport input ssh
* Login local
* Motd
* Int fa0/0
* Int vlan (VLAN Number) (For switch)
* Ip address (ip) (subnet mask)
* Ssh -l (username) (IP)

**Objective:**

* Configure Telnet to remotely connect to switch and router over the network from the end point devices without physical access to the devices.
* Configure ssh for remotely secure connection to switch and router over the network from the end point devices without physical access to the devices.

**Result:**

**Note: Attach Screenshots which you took during the lab sessions**

**Experiment – 5**

**Aim**: DHCP Configuration for single interface as well as VLANs

**Theory**:

The Dynamic Host Configuration Protocol (DHCP) is a [network management protocol](https://en.wikipedia.org/wiki/Network_protocol) used on [Internet Protocol](https://en.wikipedia.org/wiki/Internet_Protocol) (IP) [networks](https://en.wikipedia.org/wiki/Computer_network), whereby a DHCP [server](https://en.wikipedia.org/wiki/Server_(computing)) dynamically assigns an [IP address](https://en.wikipedia.org/wiki/IP_address) and other network configuration parameters to each device on the network, so they can communicate with other IP networks. A DHCP server enables computers to [request](https://en.wikipedia.org/wiki/Request%E2%80%93response) IP addresses and networking parameters automatically from the [Internet service provider](https://en.wikipedia.org/wiki/Internet_service_provider) (ISP), reducing the need for a [network administrator](https://en.wikipedia.org/wiki/Network_administrator) or a [user](https://en.wikipedia.org/wiki/User_(computing)) to manually assign IP addresses to all network devices. In the absence of a DHCP server, a computer or other device on the network needs to be manually assigned an IP address, or to assign itself an [APIPA](https://en.wikipedia.org/wiki/APIPA) address, the latter of which will not enable it to communicate outside its local [subnet](https://en.wikipedia.org/wiki/Subnetwork).

**Commands**:

* Ip dhcp pool (name)
* network (network) (subnet mask)
* default-router (IP address)
* dns-server(IP address)

**Objective:**

* To reduce the manual burden of assigning IPs by provisioning DHCP on router such that IPs can be assigned automatically when the end point is detected in the network.

**Result:**

**Note: Attach Screenshots which you took during the lab sessions**

**Experiment – 6**

**Aim**:

**Experiment – 7**

**Aim**: Setup Wireless Local Area Network (WLAN)

**Theory**:

A wireless LAN (WLAN) is a wireless computer networks that links two or more devices using wireless communication to form a local area network within a limited area such as a home, school etc.To connect devices, we require a wireless interface card adapter, so we have to remove default Ethernet card and plug in the wireless interface card (WPC300N) into the devices.

**Commands**:

* Ip address (IP) (Subnet mask)
* No sh
* Ip dhcp pool (name)
* Network (network) (Subnet mask)
* Default-router (IP)
* Dns-server (IP)

**Objective:**

* To create topology and wireless connections between access point and devices.
* Remove default Ethernet card from devices and plug in wireless adapter like WPC300N.
* Assign security WEP key to access point and connect through devices wirelessly by providing WEP key in pc wireless.
* Ping pc connected to access point wirelessly with pc connected to access point with wires.
* Ping different devices and check connectivity by sending packed data unit through simulation mode.

**Result:**

**Note: Attach Screenshots which you took during the lab sessions**

**Experiment – 8**

**Aim**: To capture and analyze ICMP packets in Wireshark

**Theory**:

Wire shark is an open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

**Steps**:

* Select the interface for which you want to capture packets from the list shown on starting window in wire shark.
* Either double click on the interface or go to capture tab and select start to start capturing packets.
* When you are done capturing packets go to capture tab and select stop to stop capturing packets.
* Then you can apply filter if you want to see some specific protocol packets.
* You can plot graph between protocols.
* And by double clicking on the packet you will get detailed information about the packet.

**Result:**

**Note: Attach Screenshots which you took during the lab sessions**

**Experiment – 9**

**Aim**: To capture and analyze TCP handshake in Wireshark

**Theory**:

Wire shark is an open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

TCP 3-way handshake is connection initialization packets which setup the connection between the devices as, it occurs by the source first sending SYN packets to the destination, the destination send reply with SYN/ACK packet to which the source sends ACK packet and the connection is established, further for each data transmission ACK is send and checksum is verified for the data. When the connection needs to broken FIN handshake is done.

**Steps**:

* Select the interface for which you want to capture packets from the list shown on starting window in wire shark.
* Either double click on the interface or go to capture tab and select start to start capturing packets.
* When you are done capturing packets go to capture tab and select stop to stop capturing packets.
* Type TCP in the filter, and then analyze the TCP part of each packet.
* And by double clicking on the packet you will get detailed information about the packet.

**Result:**

**Note: Attach Screenshots which you took during the lab sessions**

**Experiment – 10**

**Aim**: To capture and analyze UDP packets in Wireshark using DNS query

**Theory**:

Wire shark is an open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

Analyze DNS queries which are transferred using UDP packets in most cases, it is not connection reliable protocol and hence no acknowledgment and checksum of each packets is done.

**Steps**:

* Select the interface for which you want to capture packets from the list shown on starting window in wire shark.
* Either double click on the interface or go to capture tab and select start to start capturing packets.
* Run Nslookup command and perform a dns query from your command prompt.
* When you are done capturing packets go to capture tab and select stop to stop capturing packets.
* Type UDP in the filter, and then analyze the UDP part of each packet.
* And by double clicking on the packet you will get detailed information about the packet.

**Result:**

**Note: Attach Screenshots which you took during the lab sessions**