**Assignment No:2**

**Title:** Setting up small wireless computer network and hands-on networking command

**Problem Statement:** Set up a small wired network of 2 to 4 computers using access point and ask students to access it on their wireless gadgets. Hands on for network commands - ping, pathping, ipconfig/ifconfig, arp, netstat, nbtstat, nslookup, route, traceroute/tracert, nmap.

**Course Objective:** To learn transmission mediums, networking devices and topologies used in the Internet.

**Course Outcome:** Select topology, essential components of physical layer and networking devices to design computer networks.

**Tools Required:** Access point, Personal Computer/Laptop with wireless connectivity.

**Theory:**

**1. Access Point (AP)**

An Access Point (AP) is a networking hardware device that allows wireless devices to connect to a wired network using Wi-Fi or related standards. It acts as a bridge between wireless clients (like laptops, smartphones, tablets) and the wired LAN (Local Area Network).

**1.1 Key Functions of Access Point:**

1. **Wireless Connectivity**: Enables wireless communication within a local area by transmitting and receiving wireless signals.
2. **Data Bridging**: Connects wireless clients to a wired Ethernet network.
3. **Network Extension**: Extends the range of a wired network to accommodate mobile devices.
4. **Authentication and Security**: Supports security protocols like WPA2/WPA3 to protect the wireless network from unauthorized access.
5. **Traffic Management**: Manages wireless traffic by distributing bandwidth among multiple clients.

**1.2 Working of an Access Point:**

* The AP connects to a router or switch via an Ethernet cable.
* It broadcasts a wireless signal (SSID – Service Set Identifier).
* Wireless devices detect this signal and connect using proper credentials.
* The AP forwards the wireless traffic to the router/switch, which then routes it to the Internet or local resources.

**1.3 Advantages:**

* Provides mobility to users within the network coverage area.
* Reduces cabling costs.
* Easily scalable for more devices and larger areas.

**1.4 Common Standards:**

* IEEE 802.11 a/b/g/n/ac/ax (Wi-Fi standards)

**2. Wireless Gadgets – Theory (for CN Subject)**

Wireless gadgets are electronic devices that connect to a network or other devices without using physical cables, typically through Wi-Fi, Bluetooth, or cellular networks. These devices rely on wireless communication standards to exchange data, enabling mobility and ease of use.

**2.1 Common Wireless Gadgets in Networking:**

| **Gadget** | **Description** |
| --- | --- |
| **Smartphone** | Mobile device with Wi-Fi and cellular connectivity for internet access and communication. |
| **Laptop** | Portable computer that connects wirelessly to a network via Wi-Fi. |
| **Tablet** | Touchscreen device, similar to a smartphone, used for internet access, reading, and multimedia. |
| **Smart TV** | Television that connects to the internet via Wi-Fi to stream online content. |
| **Wi-Fi Printer** | Printer that connects to devices over a wireless network, allowing remote printing. |
| **Smartwatch** | Wearable device that connects via Bluetooth or Wi-Fi for syncing with phones and receiving notifications. |
| **IoT Devices** | Gadgets like smart bulbs, thermostats, or security cameras that operate wirelessly over a home or office network. |
| **Wireless Headphones** | Use Bluetooth to connect to computers or phones for audio communication. |

**2.2 Wireless Technologies Used:**

* **Wi-Fi (IEEE 802.11)** – For connecting to wireless LANs.
* **Bluetooth** – For short-range device-to-device communication.
* **Cellular (3G/4G/5G)** – For wide-area network access using SIM-enabled devices.
* **Zigbee/Z-Wave** – For smart home and IoT connectivity.

**2.3 Advantages of Wireless Gadgets:**

* **Mobility** – Use anywhere within signal range.
* **Ease of Use** – No cables required.
* **Flexibility** – Easily connect and disconnect.
* **Portability** – Lightweight and travel-friendly.

**3. Networking Commands:**

**3.1 tracert:** The traceroute command (or tracert on Windows) is used to track the path that a packet takes from your computer to a destination (like google.com). It helps in understanding network hops and identifying latency or failure points in a network.

|  |
| --- |
| **Linux/macOS**  traceroute google.com  **Windows**  tracert google.com |
| Tracing route to google.com [2404:6800:4009:812::200e]  over a maximum of 30 hops:  1 2 ms 2 ms 2 ms 2401:4900:52fb:51a0::16  ……. |

**What It Shows**

Each line in the output tells:

* The hop number (router in the path)
* The IP address (and domain if resolved)
* Response times for three packets (in milliseconds)

**3.2 pathping:** The pathping command is a Windows network diagnostic tool that combines the features of ping and tracert. It provides detailed information about the route and packet loss between your computer and a destination (like a website or IP address).

|  |
| --- |
| pathping [www.google.com](http://www.google.com) |
| Tracing route to google.com [2404:6800:4009:830::200e]  over a maximum of 30 hops:  0 LAPTOP-1HQO4D8I [2409:4042:4e15:34a8:b9ca:4b52:7ba6:1d63]  1 jiofi.local.html [2409:4042:4e15:34a8:cc3:4945:643d:9c0d]  2 \* \* \*  Computing statistics for 25 seconds...  Source to Here This Node/Link  Hop RTT Lost/Sent = Pct Lost/Sent = Pct Address  0 LAPTOP-1HQO4D8I [2409:4042:4e15:34a8:b9ca:4b52:7ba6:1d63]  1/ 100 = 1% |  1 6ms 1/ 100 = 1% 0/ 100 = 0% jiofi.local.html [2409:4042:4e15:34a8:cc3:4945:643d:9c0d]  Trace complete. |

**What pathping Does**

1. **Traces the route** your packets take to the destination (like tracert).
2. **Pings each hop** (router) multiple times to measure:
   * **Latency (delay)**
   * **Packet loss** at each hop

**3.3 ipconfig:** The ipconfig command is used in Windows to view and manage your network configuration details. "ipconfig helps users find out their current IP configuration.

|  |
| --- |
| ipconfig |
| Ethernet adapter Ethernet:  Connection-specific DNS Suffix . :  Link-local IPv6 Address . . . . . : fe80::5e7f:98ff:fe20:7c3a%5  IPv4 Address. . . . . . . . . . . : 192.168.1.5  Subnet Mask . . . . . . . . . . . : 255.255.255.0  Default Gateway . . . . . . . . . : 192.168.1.1 |

* ipconfig /all → Shows **detailed info**, including DNS, MAC address, DHCP server.
* ipconfig /release → Releases current IP address.
* ipconfig /renew → Requests a new IP from the DHCP server.

**3.4 arp:** The arp command in Windows is used to view and manage the Address Resolution Protocol (ARP) cache, which maps IP addresses to MAC (hardware) addresses on your local network.

|  |
| --- |
| arp -a |
| Interface: 192.168.225.138 --- 0xe  Internet Address Physical Address Type  169.254.169.254 fa-69-9c-67-91-2d dynamic  192.168.225.1 fa-69-9c-67-91-2d dynamic  192.168.225.255 ff-ff-ff-ff-ff-ff static  224.0.0.2 01-00-5e-00-00-02 static  224.0.0.22 01-00-5e-00-00-16 static  224.0.0.251 01-00-5e-00-00-fb static  224.0.0.252 01-00-5e-00-00-fc static  239.255.255.250 01-00-5e-7f-ff-fa static  255.255.255.255 ff-ff-ff-ff-ff-ff static |

**Useful Commands:**

| **Command** | **Description** |
| --- | --- |
| arp -a | View ARP table |
| arp -d <ip> | Delete an ARP entry (e.g., arp -d 192.168.1.1) |
| arp -s <ip> <mac> | Manually add a static ARP entry |

**3.5 netstat:** The netstat (Network Statistics) command is used to display network connections, routing tables, interface statistics, and port usage on your computer.

|  |
| --- |
| Netstat -a |
| Active Connections  Proto Local Address Foreign Address State    TCP 127.0.0.1:2030 LAPTOP-1HQO4D8I:0 LISTENING  TCP 127.0.0.1:5500 LAPTOP-1HQO4D8I:0 LISTENING  TCP 127.0.0.1:27017 LAPTOP-1HQO4D8I:0 LISTENING  TCP 127.0.0.1:49682 LAPTOP-1HQO4D8I:49683 ESTABLISHED  TCP 192.168.225.138:61634 23.100.109.78:https ESTABLISHED  TCP 192.168.225.138:63985 www:https CLOSE\_WAIT  TCP 192.168.225.138:64202 download:http CLOSE\_WAIT  TCP [2409:4042:4e15:34a8:b9ca:4b52:7ba6:1d63]:49921 whatsapp-chatd-edge6-shv-02-pnq1:5222 ESTABLISHED |

**Useful Options (Windows):**

| **Command** | **Description** |
| --- | --- |
| netstat -a | Show **all** active connections and listening ports |
| netstat -n | Show addresses and ports in **numeric** format (IP instead of hostname) |
| netstat -o | Show connections with **Process ID (PID)** |
| netstat -b | Show **which executable (program)** is using each connection |
| netstat -an | Combine -a and -n for detailed info |
| netstat -r | Show the routing table (like route print) |
| netstat -e | Show Ethernet statistics |

**3.6 nbtstat:** The nbtstat command is used to troubleshoot NetBIOS name resolution issues in Windows systems. It displays NetBIOS over TCP/IP (NetBT) protocol statistics, name tables, and name caches.

|  |
| --- |
| nbtstat -n |
| Bluetooth Network Connection:  Node IpAddress: [0.0.0.0] Scope Id: []  No names in cache  Wi-Fi:  Node IpAddress: [192.168.203.185] Scope Id: []  NetBIOS Local Name Table  Name Type Status  ---------------------------------------------  LAPTOP-1HQO4D8I<20> UNIQUE Registered  LAPTOP-1HQO4D8I<00> UNIQUE Registered  WORKGROUP <00> GROUP Registered  Local Area Connection\* 1:  Node IpAddress: [0.0.0.0] Scope Id: []  No names in cache  Local Area Connection\* 2:  Node IpAddress: [0.0.0.0] Scope Id: []  No names in cache |

**Useful Options:**

| **Command** | **Description** |
| --- | --- |
| nbtstat -n | Shows local NetBIOS names and their status |
| nbtstat -c | Displays the NetBIOS name cache (recently resolved names) |
| nbtstat -R | Clears the NetBIOS name cache |
| nbtstat -r | Lists names resolved by broadcast and WINS |
| nbtstat -S | Shows NetBIOS sessions with IP addresses |
| nbtstat -a <hostname> | Displays NetBIOS table of a remote computer by hostname |
| nbtstat -A <IP> | Displays NetBIOS table of a remote computer by IP address |

**3.7 nslookup:** The nslookup command is used to **query DNS (Domain Name System)** servers and obtain domain name or IP address mapping information.

|  |
| --- |
| nslookup google.com |
| Server: UnKnown  Address: 192.168.203.48  Non-authoritative answer:  Name: google.com  Addresses: 2404:6800:4009:812::200e  142.250.67.174 |

**3.8 route:** The route command is used to view, add, delete, or modify entries in the IP routing table on your system. It shows how packets are forwarded when sent across networks.

|  |
| --- |
| route print |
| ===================================================================  Interface List  16...a0 e7 0b 36 79 79 ......Microsoft Wi-Fi Direct Virtual Adapter #3  18...a2 e7 0b 36 79 78 ......Microsoft Wi-Fi Direct Virtual Adapter #4  14...a0 e7 0b 36 79 78 ......Intel(R) Wireless-AC 9560  5...a0 e7 0b 36 79 7c ......Bluetooth Device (Personal Area Network)  1...........................Software Loopback Interface 1  ===================================================================  IPv4 Route Table  ===================================================================  Active Routes:  Network Destination Netmask Gateway Interface Metric  0.0.0.0 0.0.0.0 192.168.203.48 192.168.203.185 50  127.0.0.0 255.0.0.0 On-link 127.0.0.1 331  127.0.0.1 255.255.255.255 On-link 127.0.0.1 331  ……. |

**3.9 nmap:** nmap is a powerful open-source tool used for network discovery, security auditing, and port scanning. It’s widely used by system administrators and cybersecurity professionals.

|  |
| --- |
| 1. **Scan a single IP:**   nmap 192.168.0.1   1. **Scan a range of IPs:**   nmap 192.168.0.1-10   1. **Scan a subnet:**   nmap 192.168.0.0/24   1. **Scan for open ports and services:**   nmap -sV 192.168.0.1   1. **Detect operating system:**   nmap -O 192.168.0.1   1. **Aggressive scan (OS, services, traceroute, scripts):**   nmap -A 192.168.0.1   1. **Scan top 100 ports:**   nmap --top-ports 100 192.168.0.1 |

**Conclusion:** Hence, a small network we have successfully established using an access point, and relevant networking commands were executed effectively..