NAGINDAS KHANDWALA COLLEGE

Practical - 1

Aim: Study of basic network command and Network configuration commads. ipconfig, netstat, ARP, ping, hostname, tracert, getmac, nslookup etc.

Theory:

- ipconfig: 1) This diagnostic command displays all current TCP/IP network configuration values. This command is useful on computers running DHCP because it enables users to determine which TCP/IP configuration values have been configured by DHCP.

2) The ipconfig command display current TCP/IP configuration values such as IP address, sub net mask, and default gateway.

Syntax: ipconfig [/all] / renew [adapter] | / release [adapter]]

Parameter:

→ /all : Shows a full display of TCP/IP details.

→ /renew [adapter] : Renews DHCP configuration; applicable only on systems with the DHCP client service.

→ /release [adapter] : Releases the current DHCP

configuration and disables TCP/IP; available only for DHCP clients.

Note: To specify an adapter, use the name shown by running 'ipconfig' without parameters

- Netstat:) This diagnostic command displays protocol statistics and current TCP/IP network connections.

Syntax: netstat [-a] [-e] [-n] [-s] [-p protocol] [-r] [interval]

parameters:

→ -p: protocol shows connections for the protocol specified.

→ -r: Displays the contents of the routing table.

- arp: this diagnostic command display and modifies the IP-to-Ethernet or Token Ring physical address translation tables used by the Address Resolution Protocol (ARP).

Syntax:
arp -a [inet_addr] [-N [if_addr]]
arp -s inet_addr ether_addr [if_addr]
arp -d inet_addr [if_addr]

Parameters:

→ -a : displays current ARP entries by quering TCP/IP
→ -d : delete the entry specified by inet_addr
→ -s : Adds an entry in the ARP cache to associate the IP address inet_addr with the physical address ether_addr.

● Ping: This diagnostic command verifies connection to one or more remote computers.

Syntax: ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j host-list] | [-k host-list]] [-w timeout] destination-list.

Parameters:

→ -t : pings the specified host until interrupted.
→ -a : Resolves addresses to host names.
→ -n : count Sends the number of ECHO packets specified by count. The default is 4.
→ -l : length Sends ECHO packets containing the amout of data specified by length. The default is 64 bytes; the maximum is 8192.
→ -f : Sends a DO NOT fragment flag in the packet. The packet will not be fragmented by gateways on the route.

→ -ittl : Sets the time to live field to the value specified by ttl.

→ -v : tos sets the type of service field to the value specified by tos.

→ -r : count Records the route of the outgoing and the returning packet in the record route field. A minimum of 1 to a maximum of 9 hosts must be specified by count.

→ -s : count specifies the timestamp for the number of hops specified by count.

→ -j host-list : Routes pakets through a specified list of hosts (losse source routed) up to 9 hosts allowed by IP.

→ -k host-list : Routes packets through a specified list of hosts without intermediate gateways (strict source routed). up to 9 hosts allowed by IP.

→ -w timeout : Specifies a timeout interval in milliseconds.

→ Destination-list : Specifies the remote hosts to ping.

- hostname: This diagnostic command prints the name of the host on which the command is used.

Syntax: hostname -- This command has no parameters.

- Tracert google.co.in: This 'tracert' utility tracks the route to a destination by sending ICMP echo packets with varying TTL values. Each router reduces the TTL, and when it hits 0, the router sends a Time Exceeded message back to the source

Syntax: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name.

Parameters:

→ -d: Prevents address resolution to host names.

→ -h maximum_hops: Sets the maximum number of hops to search for the target.

→ -j host-list: specifies a loose source route.

→ -w timeout: waits the specified number of milliseconds for each reply.

→ target_name: Specifies the target host name.

- getmac: This command returns the MAC address and network protocols for all network cards on a computer, locally or across a network. It's useful for entering the MAC address into a network analyzer or analyzer or checking the protocols in use on each network adapter.

Syntax: getmac [/s ComputerName] [/u UserName] [/p Password] [/fo {TABLE | LIST | CSV}] [/nh] [/v]

Parameters:

→ /s ComputerName: specifies the remote computer to connect to.

→ /u UserName: Specifies Run the command as a specific user.

→ /p Password: provide the user's password.

→ /fo {TABLE | LIST | CSV}: choose the output format.

→ /nh: Hide column headers (for 'TABLE' or 'CSV' formats).

→ /v: show detailed output.

- nslookup: is a command-line tool for discovering the IP address or DNS record of a domain name and for reverse DNS lookups. Use 'nslookup' in command prompt or terminal.

There are various types of nslookup commands for requesting different domain information. The most commonly used commands include:

Syntax: nslookup [option] [name | IP_address]

Parameters:

→ name: Displays info about the domain or hostname.

→ server [name]: changes the defaults DNS server.

→ root: sets the root server as default.

→ help: Lists 'nslookup' commands.

→ exit: Exits 'nslookup'. and returns users to the CLI.

Practical 3

Aim :- Configure IP static routing

Theory :-

- Static routing is a type of network routing technique. Static routing is not a routing protocol; instead, it is the normal configuration and selection of a network route, usually managed by the network administrator.
- Static routing performs routing decisions with preconfigured routes in the routing table, which can be changed manually only by administration
- Static routes are normally implemented in those situations where the choices in route selection are limited or there is only a single default route available.
- Also Static routing can be used if you have only few devices for route configuration and there is no need for route change in the future.
- Static routing is considered the simplest form of routing.

Practical - 1

Aim: Configure IP routing with RIP

Theory:

- RIP stands Routing Information protocol. RIP is an intra-domain routing protocol used within an autonomous system. Here, intra-domain means routing the packets in a defined domain, for example, web browsing within an institutional area.
- RIP is uni cast routing protocol. The whole internet is divided into multiple group of networks called as autonomous systems. There are few protocols which are used to send the data among multiple autonomous system, they are called as inter domain protocols and second type of protocols are called as intra domain routing protocols because they are used to send the data packets within the autonomous system. RIP is intra domain routing protocol, it shares the information about its directly connected networks with the neighbouring routers the information is shared periodically after few milliseconds automatically in RIP protocol.

Practical - 5

Aim: Configure Simple OSPF.

Theory:

- Open shortest path first (OSPF) is a link-state routing protocol which is used to find the best path between the source and the destination router using its own shortest path first (SPF) algorithm.
- When configured, OSPF will listen to neighbours and gather all link state data available to build a topology map of all available paths in its network and then save the information in its topology database, also known as its Link-State Database (LSDB). Using the information from its topology database, from the information gathered. It will calculate the best shortest path to each reachable subnet/network using an algorithm called Shortest Path First (SPF).
- OSPF offers a very distinguishable feature named: Routing Areas. It means dividing routers inside a single autonomous system running OSPF into areas where each area consists of a group of connected routers.

- The idea of dividing the OSPF network into areas is to simplify administration and optimize available resources.
- Areas are a logical collection of routers that carry the same Area ID or number inside of an OSPF network, the OSPF network itself can contain multiple areas, the first and main Area is called the backbone area "Area 0", all other areas must connect to Area 0.

Practical - 7

Aim: Configuring DNS, HTTP, DHCP server and client

Theory: 1) DHCP

- Dynamic Host configuration protocol (DHCP) is a network management protocol used to dynamically assign an IP address to any device or node on a network so they can communicate using IP (Internet Protocol). DHCP automates and centrally manages these configurations. There is no need to manually assign IP address to new devices. Therefore there is no requirement for any user configuration to connect to a DHCP based network.

- DHCP can be implemented on local networks as well as large enterprise networks. DHCP is the default protocol used by the most routers and networking equipments.

- DHCP runs at the application layer of the TCP/IP protocol stack to dynamically assign IP addresses to DHCP clients/nodes and to allocate TCP/IP configuration information to the DHCP clients. Information includes subnet mask information, default gateway, IP address as well as information about client configuration

and domain name system addresses.

- DHCP is based on client-server protocol in which servers manage a pool of unique IP addresses, as well as information about client configuration parameters, and assign addresses out of those address pools.

2) DNS:

- DNS stands for Domain Name System.
- DNS is a directory service that provide a mapping between the name of a host on the network and its numerical address.
- DNS is client/server network communication protocol. DNS clients send requests to the server while DNS servers send responses to the client.
- client request contain a name which is converted into an IP address known as a forward DNS lookup while requests containing an IP address which is converted into a name known as reverse DNS lookups.
- DNS implements a distributed database to store the name of all the hosts available on the internet.

- If a client like a web browser sends a request containing a hostname, then a piece of software such as DNS resolver sends a request to the DNS server to obtain the IP address of a hostname. If DNS server does not contain the IP address associated with a hostname, then it forwards the request to another DNS server. If IP address has arrived at the resolver, which in turn completes the request over the internet protocol.

3) HTTP:

- HTTP Stands for HyperText Transfer Protocol
- It is a protocol used to access the data on the World wide web (www).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.