**Section 1: Study and Basics**

**1.Study Networking Components:** Study types of cables (Twisted Pair Cable, Coaxial Cable, Fiber Optic Cable), connectors (RJ-45, BNC connector), and networking devices (Hub, Switch, Router, Gateway).

2.**Study TCP/IP Utilities and Commands:** Explore basic TCP/IP utilities and commands (e.g., ping,

ifconfig, tracert, arp, tcpdump, whois, host, netstat, nslookup, ftp, telnet).

3.**Router Configuration Using CLI:** Configure a router's basic settings, including hostname,

banners, and password protection.

**Section 2: Routing**

**1.Configure a Router with Static and Dynamic Routing:** Configure a router (Ethernet and Serial

Interface) using router commands for: Static Routing, Dynamic Routing (RIPV1, RIPV2) on any network simulator (e.g., Cisco Packet Tracer).

**Rubrics for Evaluation (Scale of 10):**

* **Conceptual Understanding (3 marks):** Assesses the grasp of fundamental networking concepts. Focuses on the application of core ideas and principles.
* **Technical Implementation (3 marks):** Evaluates the accuracy of technical configurations, command syntax, and adherence to networking protocols.
* **Practical Application (2 marks):** Measures ability to use tools, write code, configure devices, and conduct analyses.
* **Analysis and Interpretation (1 mark):** Assesses the ability to analyze results and explain the outcomes of implementations.

**Completeness and Compliance (1 mark):** Evaluates adherence to instructions and the completion of all required tasks.

**Assignment 1: Study Networking Components**

**Title: “Building the Foundation: Exploring Networking Components for Scalable Infrastructure”**

**Assignment Statement:** Study the types of cables (Twisted Pair Cable, Coaxial Cable, Fiber Optic Cable), connectors (RJ-45, BNC connector), and networking devices (Hub, Switch, Router, Gateway).

**AIM:** To explore the physical components of computer networks and understand their characteristics, applications, and roles in building a scalable and robust network infrastructure.

**Objectives:**

1. Identify and differentiate between various types of networking cables.
2. Understand the specifications and applications of connectors like RJ-45 and BNC.
3. Study the purpose, functionality, and use cases of networking devices, including hubs, switches, routers, and gateways.
4. Develop an understanding of how these components contribute to the design of a reliable and scalable network.

###### Outcomes:

By the end of this assignment, students will be able to:

1. Recognize and categorize networking components based on their features and use cases.
2. Justify the choice of specific cables, connectors, and devices for different scenarios.
3. Demonstrate knowledge of physical network design and suggest improvements for scalability and robustness.

**Scenario:**

###### Industry Background: You have recently joined the IT support team of a medium-sized company that is relocating to a new office. The management is planning to deploy a robust network infrastructure to connect over 100 employees across multiple departments. As part of your onboarding, your team lead assigns you the task of exploring various types of network cables (Twisted Pair, Co-axial, and Fiber Optic) and connectors (RJ-45 and BNC) emphasizes the following requirements:

* + High-speed communication between desktop workstations and servers in the main office.
  + Secure connections to the IoT-enabled devices in the warehouse.
  + A scalable network that can handle future growth without significant rewiring. Additionally, you are asked to study and test the functionality of key networking devices

such as hubs, switches, routers, and gateways. Your goal is to create a practical demonstration to educate staff about the purpose and applications of these components. This knowledge will ensure the IT team is equipped to handle the installation and maintenance of the company’s new LAN setup. You must consider factors like bandwidth, cost, and security while presenting a solution.

###### Tasks to Be Performed:

1. Research and document the characteristics, advantages, and limitations of Twisted Pair Cables, Coaxial Cables, and Fiber Optic Cables.

MIT ADT University, Pune

1. Prepare a comparison table for RJ-45 and BNC connectors, highlighting their specific use cases.
2. Create a report explaining the functionality of hubs, switches, routers, and gateways, including a discussion on their placement in the network.
3. Propose a physical network design for the logistics company, selecting suitable cables, connectors, and devices.
4. Justify your choices in a presentation to your instructor or peers, simulating a client pitch.

##### THEORY:

**LAN:** A local area network (LAN) is a [computer network](http://en.wikipedia.org/wiki/Computer_network) that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media to communicate with one another and share resources such as printers.

**Cables**: Cable is the medium through which information usually moves from one network device to another. The type of cable chosen for a network is related to the network's topology, protocol, and size. There are several types of cable which are commonly used with LANs.

* + Twisted Pair Cable
  + Coaxial Cable
  + Fiber Optic Cable

###### Twisted Pair Cable

In its simplest form, twisted-pair cable consists of two insulated strands of copper wire twisted around each other.

Unshielded Twisted Pair Cable

UTP, using the 10BaseT specification, is the most popular type of twisted-pair cable and is fast becoming the most popular LAN cabling. The maximum cable length segment is 100 meters, about 328 feet. Traditional UTP cable, as shown in Figure 1, consists of two insulated copper wires.

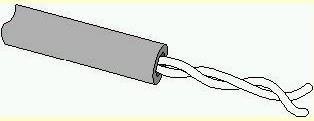


Fig.1 Unshielded Twisted Pair Cable

Shielded Twisted Pair Cable

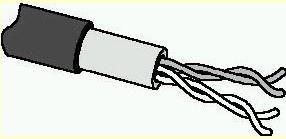
STP cable uses a woven copper-braid jacket that is more protective and of a higher quality than the jacket used by UTP. Figure 2 shows a two-twisted-pair STP cable. STP also uses a foil wrap around each of the wire pairs. This gives STP excellent shielding to protect the transmitted data from outside interference, which in turn allows it to support higher transmission rates over longer distances than UTP.

Fig.2 Shielded Twisted Pair Cable

Twisted Pair Cable Connector (RJ45 Connector)

Twisted-pair cabling uses RJ-45 telephone connectors to connect to a computer. The RJ- 45 connector houses

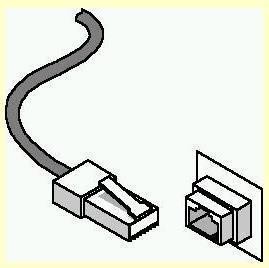
eight cable connections. An RJ-45 connector is shown in Figure 3.

Fig.3 RJ45 Connector

###### Coaxial cable

In its simplest form, coaxial cable consists of a core of copper wire surrounded by insulation, a braided metal shielding, and an outer cover. Figure 4 shows the various components that make up a coaxial cable.

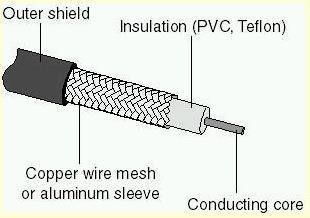


Fig.4 Coaxial Cable

Coaxial Cable Connector (BNC Connector)

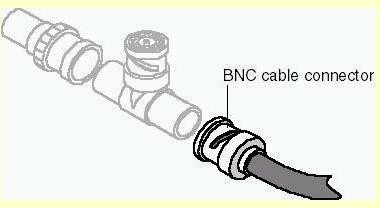
Coaxial cable uses a connection component, known as a BNC connector, to make the connections between the cable and the computers. Figure 5 shows a BNC connector.

Fig.5 BNC Connector Fiber optic Cable

###### Fiber optic Cable

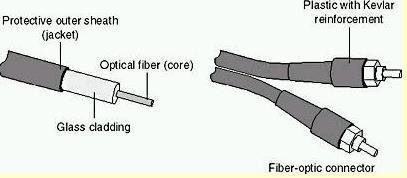
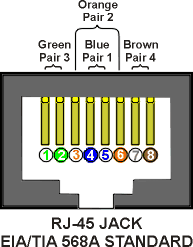
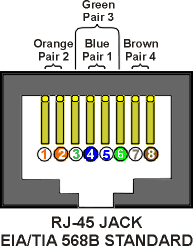
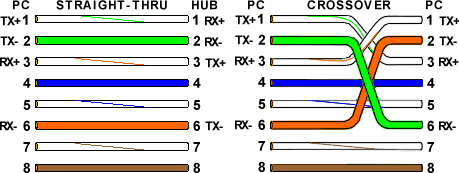
In fiber-optic cable, optical fibers carry digital data signals in the form of modulated pulses of light. An optical fiber consists of an extremely thin cylinder of glass, called the core, surrounded by a concentric layer of glass, known as the cladding.

Fig.6 Fiber optic Cable

###### Color-Code Standards:

Two wires color-code standards apply: EIA/TIA 568A and EIA/TIA 568B. The codes are commonly depicted with RJ-45 jacks as follows:

If we apply the 568A color code and show all eight wires, our pin-out looks like this:



Note that pins 4, 5, 7, and 8 and the blue and brown pairs are not used in either standard.

###### Hub

Operates at the Physical Layer (Layer 1). It broadcasts data to all connected devices without filtering, leading to network congestion. Commonly used in small networks.

##### SWITCH

Operates at the Data Link Layer (Layer 2). It forwards data to specific MAC addresses, reducing network traffic and improving efficiency.

##### ROUTER

Operates at the Network Layer (Layer 3). Directs data between different networks using IP addresses,

and uses routing tables and protocols like RIP, OSPF, and BGP.

##### GATEWAY

Operates at multiple layers of the OSI model. It connects two networks with different protocols and translates data between them, ensuring compatibility.

**CONCLUSIONS:** We have studied networking different cables, devices and topologies.

# Assignment 2: Study TCP/IP Utilities and Commands

**Title:** "Network Diagnostics and Troubleshooting Using TCP/IP Utilities and Commands"

##### AIM:

To understand and use various TCP/IP utilities to diagnose and troubleshoot network issues and monitor network performance effectively.

###### Objectives:

* 1. Learn the syntax and use of basic TCP/IP commands.
  2. Diagnose common connectivity issues in a network using tools like **ping** and **tracert**.
  3. Monitor and analyze network interfaces and connections using **ifconfig**, **netstat**, and

###### tcpdump.

* 1. Query domain and IP information using **whois**, **nslookup**, and **host**.

Test remote access and file transfer using **ftp** and **telnet** commands

###### Outcomes:

By the end of this assignment, students will:

1. Use TCP/IP commands to troubleshoot network connectivity problems.
2. Analyze and interpret the output of network diagnostic tools.
3. Demonstrate proficiency in monitoring and managing network health.

###### Scenario:

**Industry Background:** You are a network administrator at **Streamline Corp**, a global e- commerce company. Recently, the company has been facing connectivity disruptions between regional offices and the central data center. The IT head has asked you to investigate and resolve these issues using TCP/IP utilities.

Tasks assigned include:

1. Verifying the reachability of servers in the data center from regional offices using **ping**

and **tracert**.

1. Identifying bandwidth bottlenecks by analyzing network interfaces using **ifconfig** and

###### netstat.

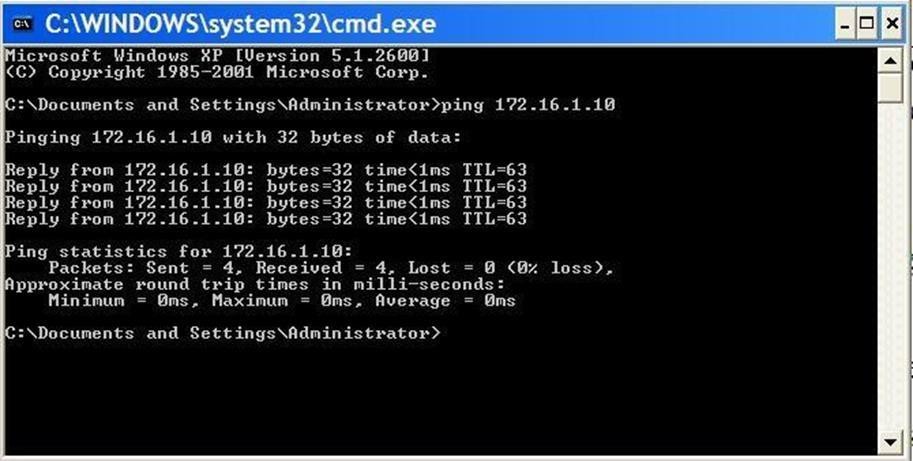
1. Checking domain resolution issues with **nslookup** and **host**.
2. Capturing network traffic for deeper analysis using **tcpdump**.

Additionally, the team must create a report summarizing their findings and suggesting solutions to prevent future disruptions. Your findings will be instrumental in creating a standard operating procedure for future troubleshooting efforts.

**Tasks to Be Performed:**

1. Run **ping** to verify connectivity between devices in the network. Document the results, including response times and packet loss.
2. Use **tracert** to trace the route from a client machine to a server. Identify any delays or failures in intermediate hops.
3. Execute **ifconfig** (or **ipconfig** on Windows) to analyze the status of network interfaces.
4. Use **netstat** to view active connections and diagnose unusual traffic.
5. Test domain resolution for the company’s website using **nslookup** and **host**.
6. Capture packets using **tcpdump** and analyze them for potential anomalies.
7. Test remote connectivity using **telnet** and simulate file transfers using **ftp**.

**THEORY:**

The PING utility tests connectivity between two hosts. PING uses a special protocol called the Internet Control Message Protocol (ICMP) to determine whether the remote machine (website, server, etc.) can receive the test packet and reply.

Also a great way to verify whether you have TCP/IP installed and your Network Card is working.

We‘ll start by Pinging the loopback address (127.0.0.1) to verify that TCP/IP is installed and configured correctly on the local computer.

Ping 127.0.0.1

This tells us that TCP/IP is working as well as Network Card.

To test out connectivity to a website all you have to do is ping espn.com

The results should tell us if the connection was successful or if we had any lost packets. Packet loss describes a condition in which data packets appear to be transmitted correctly at one end of a connection, but never arrive at the other. Why? Well, there are a few possibilities.

The network connection might be poor and packets get damaged in transit or the packet was dropped at a router because of internet congestion. Some Internet Web servers may be configured to disregard ping requests for security purposes.

Note the IP address of espn.com — 199.181.132.250. We can also ping this address and get

MIT ADT University, Pune

the same result.

However, Ping is not just used to test websites. It can also test connectivity to various servers: DNS, DHCP, your Print server, etc

###### Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS][-r count] [-s count] [[-j host- list] | [-k host-list]] [- w timeout] destination-list

|  |  |
| --- | --- |
| -t | Ping the specifed host until stopped. To see statistics  and continue - type Control-Break; To stop - type Control-C. |
| -a | Resolve addresses to hostnames. |
| -n count | Count Number of echo requests to send. |
| -l size | Send buffer size. |
| -f | Don't Fragment flag in packet. |
| -i ttl | TTL Time To Live. |
| -v tos | TOS Type Of Service. |
| -r count | Record route for count hops. |
| -s count | Timestamp for count hops. |
| -j host-list | Loose source route along host-list. |
| -k host-list | Strict source route along host-list |
| -w timeout | Timeout in milliseconds to wait for each reply. |

Examples:

1. I'm pinging 127.0.0.1 which is self. The 127.0.0.1 is called loopback. Thus when receiving replies I know my basic TCP/IP setup is working. The time provided is the roundtrip times and the "Time to Live" is the hop count for the packets being sent. The roundtrip time here is very short since all I'm doing is a wrap around to self

C:\>**ping 127.0.0.1**

Pinging 127.0.0.1 with 32 bytes of data:

**Reply from 127.0.0.1: bytes=32 time<10ms TTL=128 Reply from 127.0.0.1: bytes=32 time<10ms TTL=128 Reply from 127.0.0.1: bytes=32 time<10ms TTL=128 Reply from 127.0.0.1: bytes=32 time<10ms TTL=128**

**Ping statistics for 127.0.0.1:**

**Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds:**

**Minimum = 0ms, Maximum = 0ms, Average = 0ms Example 2:**

Here I'm pinging web site using the IP address; normally, you would do this after having done one above. The first established that your basic setup is fine. This establishes that your internet connection is working fine

###### C:\>ping 207.159.129.102

**Pinging 207.159.129.102 with 32 bytes of data:**

**Reply from 207.159.129.102: bytes=32 time=328ms TTL=250 Reply from 207.159.129.102: bytes=32 time=251ms TTL=250 Reply from 207.159.129.102:**

MIT ADT University, Pune

**bytes=32 time=358ms TTL=250 Reply from 207.159.129.102: bytes=32 time=296ms TTL=250**

###### C:\>Ping statistics for 207.159.129.102:

**Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds:**

**Minimum = 251ms, Maximum = 358ms, Average = 308ms**

It is not uncommon to get a few "request Timed out" responses. Example 3

Here I'm pinging the same place as above. If the two first worked and this does not, the most common problem is the DNS setup. It may also be caused by duplicates of some of the winsock files in win95.

###### C:\>ping [www.Winfiles.com](http://www.winfiles.com/)

**Pinging www3-pool.Winfiles.com [207.159.129.102] with 32 bytes of data: Reply from 207.159.129.102: bytes=32 time=202ms TTL=250**

**Reply from 207.159.129.102: bytes=32 time=245ms TTL=250 Reply from 207.159.129.102: bytes=32 time=330ms TTL=250 Reply from 207.159.129.102:**

**bytes=32 time=217ms TTL=250**

###### Ping statistics for 207.159.129.102:

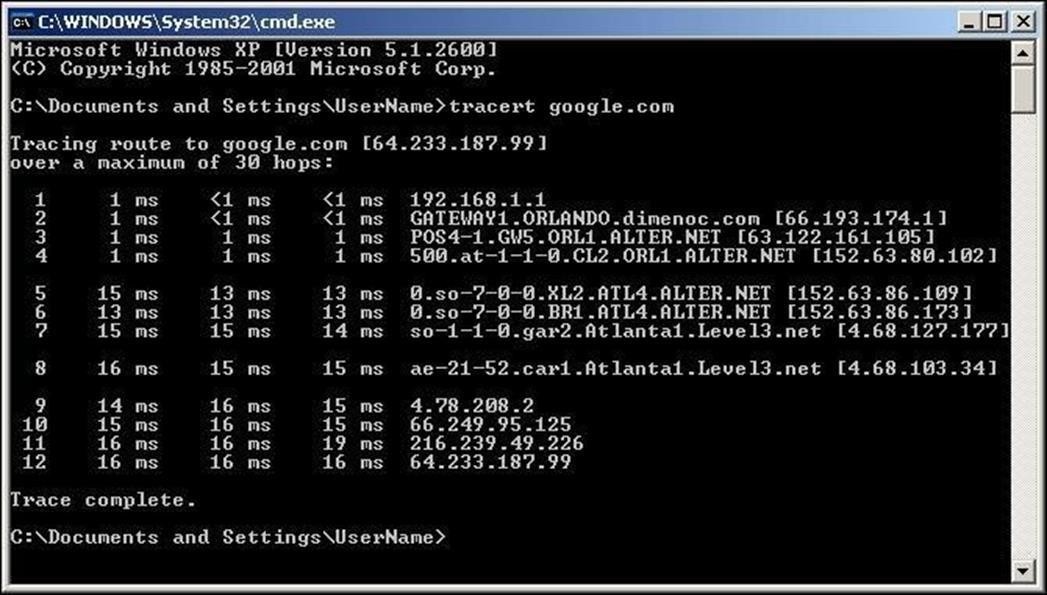
**Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds:**

**Minimum = 202ms, Maximum = 330ms, Average = 248ms**

#### Tracert

Tracert is very similar to Ping, except that Tracert identifies pathways taken along each hop, rather than the time it takes for each packet to return (ping). It is a nice little utility which can be used quite effectively for diagnosis of networks and routes. It can also be used to find IP addresses for items you only know by name. If I have trouble connecting to a remote host I will use Tracert to see where that connection fails. Any information sent from a source computer must travel through many computers / servers / routers (they‘re all the same thing, essentially) before it reaches a destination. It may not be your computer but something that is down along the way. It can also tell you if communication is slow because a link has gone down between you and the destination.

MIT ADT University, Pune



If you know there are normally 4 routers but Tracert returns 8 responses, you know your packets are taking an indirect route due to a link being down.

Tracert is a TCP/IP utility which determines the route taken. It does this by sending out packets with varying TTL (time to live). Each way station along the route is supposed to decrease the TTL value by 1 before passing it on. When the count reaches Zero, the router will return respond to the sender that the time was exceeded. Thus, the first packet is sent with a TTL (hop count) of 1 and then incremented until the destination is reached.

Some routers just drops packets with a Zero count and thus becomes invisible to tracert. tracert [-d] [-h maximum\_hops] [-j host-list] [-w timeout] target\_name

|  |  |
| --- | --- |
| -d | Do not to resolve addresses to host names |
| -h  maximum\_hops | specifies the max TTL (hop count) to use to find target |
| -j host-list | specifies a route along the host list - loose |
| -w timeout | Waits for the timeout milliseconds for repsonse |
| target\_name | specifies the name of the destination |

###### C:\>tracert [www.hildrum.com](http://www.hildrum.com/)

**Tracing route to hildrum.com [207.159.136.230] over a maximum of 30 hops:**

**1 1007 ms 839 ms 1477 ms max44.seattle.wa.ms.uu.net [207.76.5.50]**

**2 1148 ms 745 ms 155 ms ar1.seattle.wa.ms.uu.net [207.76.5.3]**

**3 168 ms 193 ms 159 ms Fddi0-0.CR2.SEA1.Alter.Net [137.39.33.42]**

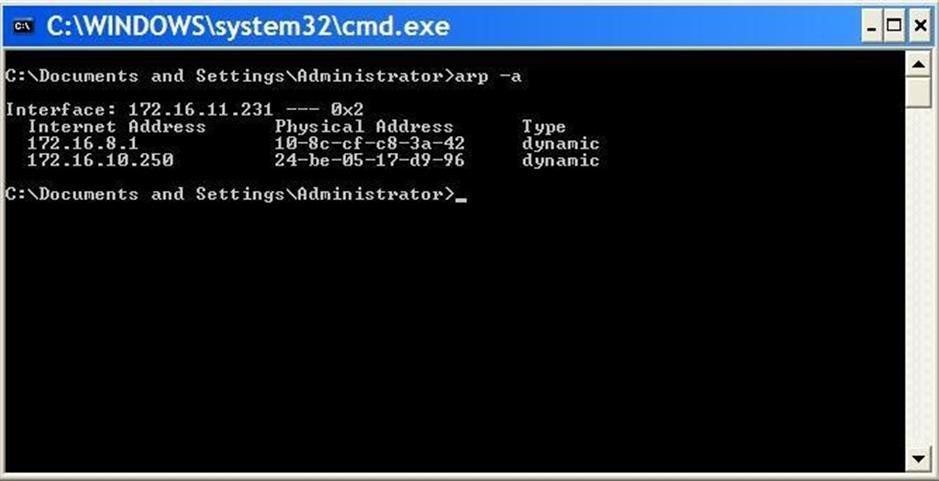
**4 194 ms 151 ms Fddi1-0.GW2.SEA1.Alter.Net [137.39.42.194]**

* 1. **203 ms 162 ms 184 ms lightrealm-gw.customer.ALTER.NET [157.130.176.50]**
  2. **220 ms 216 ms 183 ms hildrum.com [207.159.136.230] Trace complete.**

MIT ADT University, Pune

#### ARP

The ARP utility helps diagnose problems associated with the Address Resolution Protocol (ARP). TCP/IP hosts use ARP to determine the physical (MAC) address that corresponds with a specific IP address. Type arp with the – a option to display IP addresses that have been resolved to MAC addresses recently.



ARP stands for Address Resolution Protocol. This provides IP to Ethernet addresses. Each hardware card has an address coded in. This allows deletion and addition to the ARP cache. The switches to be used can be obtained by just typing arp at a DOS command prompt.

###### ARP -s inet\_addr eth\_addr [if\_addr] ARP -d inet\_addr [if\_addr] ARP -a [inet\_addr] [-N if\_addr]

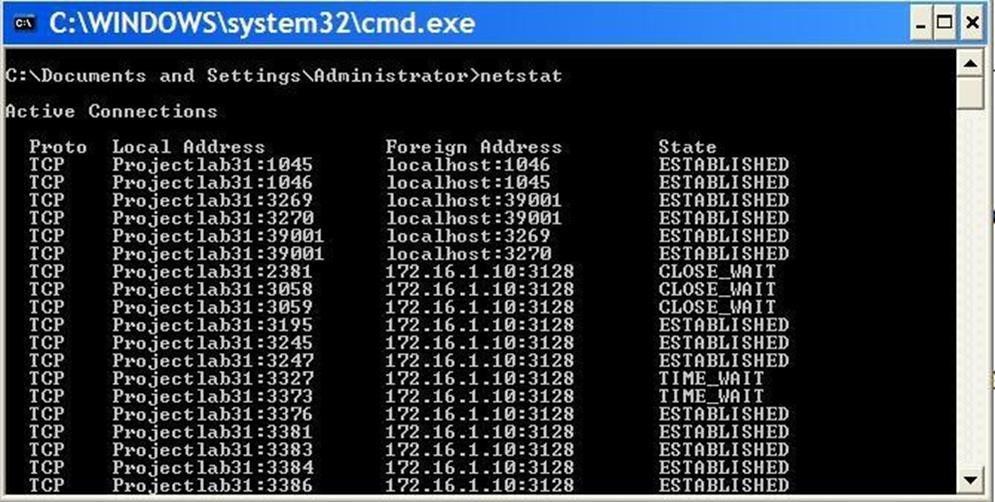
|  |  |
| --- | --- |
| -a | Displays current ARP entries by interrogating the current protocol data. If inet\_addr is specified, the IP and Physical addresses for only the specified computer are displayed. If more than one network interface uses  ARP, entries for each ARP table are displayed. |
| -g | same as –a |
| -N | if\_addr Displays the ARP entries for the network  interface specified by if\_addr. |
| -d | Deletes the host specified by inet\_addr. |
| -s | Adds the host and associates the Internet address inet\_addr with the Physical address eth\_addr. The Physical address is given as 6 hexadecimal bytes  separated by hyphens. The entry is permanent. |
| eth\_addr | Specifies a physical address. |
| if\_addr | If present, this specifies the Internet address of the interface whose address translation table should be  modified. If not present, the first applicable interface |

**C:\>arp -g**

**Interface: 153.34.131.179 on Interface 3**

|  |  |  |
| --- | --- | --- |
| **Internet Address** | **Physical Address** | **Type** |
| 16.1.0.4 | 20-53-52-43-00-00 | dynamic |
| 128.173.14.71 | 20-53-52-43-00-00 | dynamic |
| 129.132.98.11 | 20-53-52-43-00-00 | dynamic |
| 192.31.216.8 | 20-53-52-43-00-00 | dynamic |
| 204.118.34.6 | 20-53-52-43-00-00 | dynamic |
| 204.118.34.22 | 20-53-52-43-00-00 | dynamic |
| 204.123.2.72 | 20-53-52-43-00-00 | dynamic |
| 204.255.246.18 | 20-53-52-43-00-00 | dynamic |
| 208.215.43.40 | 20-53-52-43-00-00 | dynamic |

#### Netstat

Netstat (Network Statistics) displays network connections (both incoming and outgoing), routing tables, and a number of network interface statistics. It‘s a helpful tool in finding problems and determining the amount of traffic on the network as a performance measurement.

This utility provides the connection both the local and remote, ports and the state of the connection. It has several switches which maybe found by typing netstat /?

It provides the IP addresses and the ports of the remote computer(S) to which the socket is connected. If a port has not been established it is indicated by a \*. It shows the port numbers as well as IP address for the local computer.

MIT ADT University, Pune

It provides the type of protocol being used for the connection(s).It provides a status of the connection. Is it established?? Is it closed?? Or is it waiting?? And more

**NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]**

|  |  |
| --- | --- |
| -a | Displays all connections and listening ports. |
| -e | Displays Ethernet statistics. This may be combined with the -s option. |
| -n | Displays addresses and port numbers in numerical form. |
| -p prot o | Shows connections for the protocol specified by proto; proto may be TCP or UDP. If used with the  -s option to display per-protocol statistics, proto may be TCP, UDP, or IP. |
| -r | Displays the routing table. |
| -s | Displays per-protocol statistics. By default, statistics are shown for TCP,  UDP and IP; the -p option may be used to specify a subset of the default. |
| inter val | Redisplays selected statistics, pausing interval seconds between each display. Press CTRL+C to stop redisplaying statistics. If omitted, netstat  will print the current configuration information once. |

**C:\>netstat**

**Active Connections**

**Proto Local Address Foreign Address State**

**TCP dummy:3174** [**www.microsoft.com:80**](http://www.microsoft.com/) **ESTABLISHED TCP dummy:3175** [**www.microsoft.com:80**](http://www.microsoft.com/) **ESTABLISHED TCP dummyt:3176** [**www.microsoft.com:80**](http://www.microsoft.com/) **ESTABLISHED TCP dummy:3177** [**www.microsoft.com:80**](http://www.microsoft.com/) **ESTABLISHED TCP dummy:3178 208.8.204.14:telnet ESTABLISHED**

**TCP dummy:3181 chat.msn.com:6667 ESTABLISHED TCP dummy:3182 hildrum.com:ftp ESTABLISHED TCP dummy:3183 hildrum.com:ftp-data ESTABLISHED**

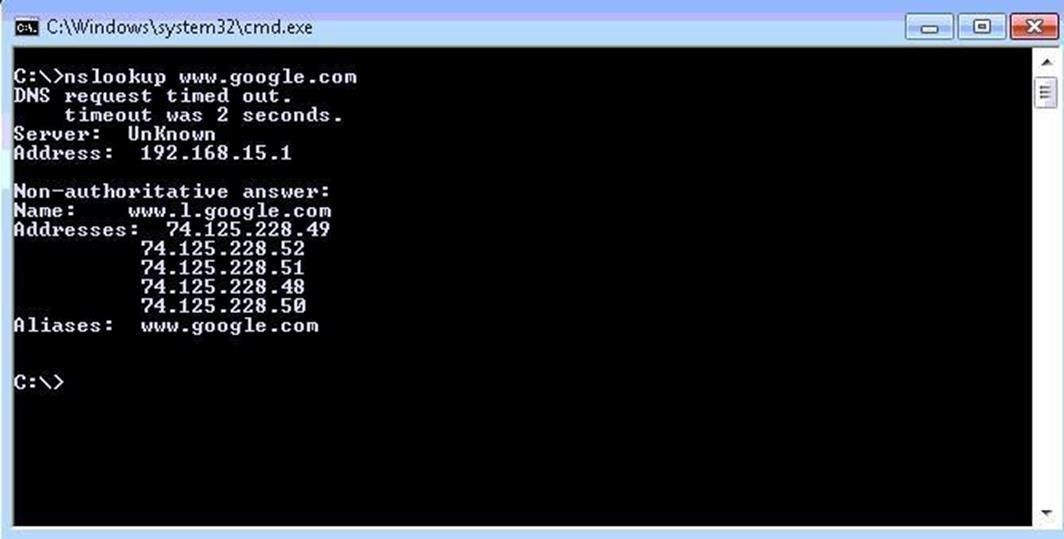
###### Nbtstat

Nbtstat (NetBios over TCP/IP) enables you to check information about NetBios names.It helps us view the NetBios name cache (nbtstat -c) which shows the NetBios names and the corresponding IP address that has been resolved (nbtstat -r) by a particular host as well as the names that have been registered by the local system (nbtstat –n).

# NSLookup

NSLookup provides a command-line utility for diagnosing DNS problems. In its most basic usage, NSLookup returns the IP address with the matching host name.

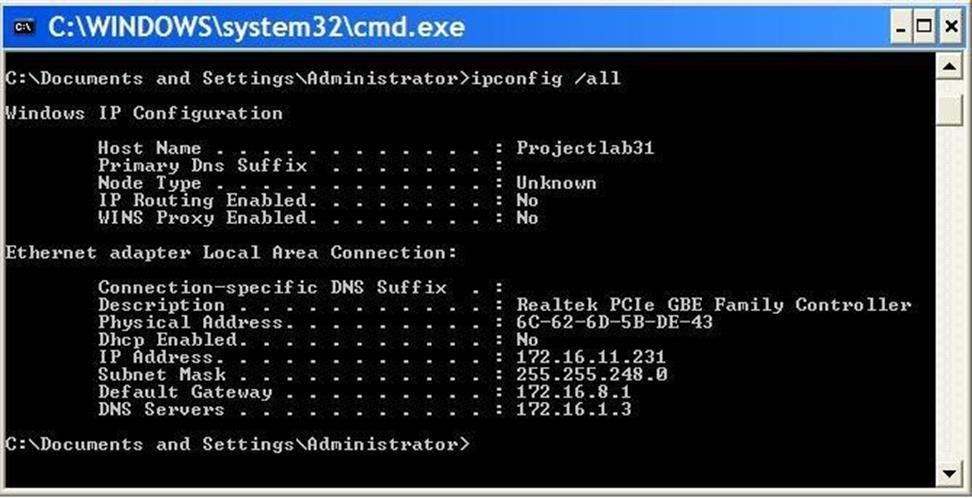
MIT ADT University, Pune



#### IPConfig

Not part of the TCP/IP utilities but it is useful to show current TCP/IP settings.The IPConfig command line utility will show detailed information about the network you are connected to. It also helps with reconfiguration of your IP address through release and renew.

Let‘s say you want to know what you‘re IP address is — ipconfig is what you type in the command prompt.



ipconfig will give a quick view of you IP address, your subnet mask and default gateway. ipconfig /all will give you more detailed information.

Through ipconfig /all we can find DNS severs, if we have DHCP enabled, MAC Address, along with other helpful information. All good things to know if we have trouble getting connected to the internet.

MIT ADT University, Pune

##### SYNTAX

**ipconfig [/? | /all | /renew adapter | /release adapter | /flushdns | /displaydns |**

**/registerdns | /showclassid adapter | /setclassid adapter classid**

**The adapter connection name can use wildcard characters (\* and ?).**

##### OPTIONS

/? Displays this help message

/all Displays full configuration information

/release Releases the IP address for the specified adapter

/renew Renews the IP address for the specified adapter

/flushdns Purges the DNS Resolver cache

/registerdns Refreshes all DHCP leases and reregisters DNS names

/displaydns Displays the contents of the DNS Resolver Cache

/showclassidDisplays all the DHCP ClassIds allowed for the specified adapter

/setclassid Modifies the DHCP ClassId

The default (with no parameters specified) is to display only the IP address, subnet mask, and default gateway for each adapter that is bound to TCP/IP.

For /all, Ipconfig displays all of the current TCP/IP configuration values, including the IP address, subnet mask, default gateway, and Windows Internet Naming Service (WINS) and DNS configuration.

For /release and /renew, if no adapter name is specified, the IP address leases for all adapters that are bound to TCP/IP are released or renewed.

For /setclassid, if no ClassId is specified, the ClassId is removed.

EXAMPLES

ipconfig Show information ipconfig /all Show detailed information ipconfig /renew Renew all adapters

ipconfig /renew EL\* Renew any connection whose name starts EL

ipconfig /release \*Con\* Release all matching connections, for example, "Local Area Connection 1" or "Local Area Connection2"

#### tcpdump

tcpdump command will work on most flavors of unix operating system. tcpdump allows us to save the packets that are captured, so that we can use it for future analysis. The saved file can be viewed by the same tcpdump command. We can also use open source software like wireshark to read the tcpdump pcap files.

###### Options:

* + -i any : Listen on all interfaces just to see if you're seeing any traffic.
  + -n : Don't resolve hostnames.
  + -nn : Don't resolve hostnames or port names.

MIT ADT University, Pune

* + -X : Show the packet's contents in both hex and ASCII.
  + -XX : Same as -X, but also shows the ethernet header.
  + -v, -vv, -vvv : Increase the amount of packet information you get back.
  + -c : Only get x number of packets and then stop.
  + -s : Define the snaplength (size) of the capture in bytes. Use -s0 to get everything, unless you are intentionally capturing less.
  + -S : Print absolute sequence numbers.
  + -e : Get the ethernet header as well.
  + -q : Show less protocol information.
  + -E : Decrypt IPSEC traffic by providing an encryption key.

The default snaplength as of tcpdump 4.0 has changed from 68 bytes to 96 bytes. While this will give you more of a packet to see, it still won't get everything. Use -s 1514 to get full coverage

Examples:

* + host // look for traffic based on IP address (also works with hostname if you're not using -n) # tcpdump host 1.2.3.4
  + src, dst // find traffic from only a source or destination (eliminates one side of a host conversation) # tcpdump src 2.3.4.5

# tcpdump dst 3.4.5.6

* + net // capture an entire network using CIDR notation # tcpdump net 1.2.3.0/24
  + proto // works for tcp, udp, and icmp. Note that you don't have to type proto # tcpdump icmp
  + port // see only traffic to or from a certain port # tcpdump port 3389
  + src, dst port // filter based on the source or destination port # tcpdump src port 1025

# tcpdump dst port 389

* + src/dst, port, protocol // combine all three

# tcpdump src port 1025 and tcp # tcpdump udp and src port 53

#### whois Command

To make it easier for administrators to find information about domains in this large distributed database, modern TCP/IP implementations generally come with an intelligent version of the whois utility. It is able to accept as input the name of a domain and automatically locate the appropriate registry in which that domain‘s information is located.

###### The utility is usually used as follows:

**whois [-h <whois-host>] <domain>**

In the above syntax, the term ―domain‖ represents the name about which registration information is requested. The administrator can use the ―-h‖ parameter to force the program to query a particular whois server, but again, this is usually not required**.**

#### FTP Command

To connect to another computer using FTP at the MS-DOS prompt, command line, or Linux

MIT ADT University, Pune

shell type FTP and press enter. Once in FTP> Type:

open ftp.example.com

In the above example, you'd substitute example.com for the name of your domain you want to connect to. In addition to the domain name the IP address of the computer you're trying to connected to can also be typed in, for example, open 192.168.1.12.

Once connected you will be asked for a username and password. If these are entered properly you'll be successfully connected to the server where you can browse the files, send files, or receive files depending on your rights. Some servers may also allow anonymous logins you can connect to these computers using guest or e-mail address.

###### Send and receive a file in FTP

To get files from the server onto your own computer use the get command as shown in the below example. In this example you'd get the file myfile.htm.

get myfile.htm

To send a file from your computer to the computer you are connected to assuming you have the rights use the send command as shown in the below example. In this example we're sending the myfile.htm to the directory we're currently in.

send myfile.htm

It is important to realize that the files being sent must be in your local working directory. In other words the directory you were in when you typed the FTP command. If you want to change to the directory that contains your files use the lcd command. For example, on Windows you'd type lcd c:\windows to set the local directory to the Windows directory.

###### FTP Commands

**dir** Lists files if connected.

**dir -C** = Will list the files in wide format.

**dir -1** = Lists the files in bare format in alphabetic order dir -r = Lists directory in reverse alphabetic order.

**dir -R** = Lists all files in current directory and sub directories. dir -S = Lists files in bare format in alphabetic order.

**disconnect** Exits from FTP.

**get** Get file from the computer connected to.

**glob** Sets globbing on or off. When turned off the file name in the put and get commands is taken literally and wildcards will not be looked at.

**hash** Sets hash mark printing on or off. When turned on for each 1024 bytes of data received a hash- mark (#) is displayed.

**help** Access the Help screen and displays information about command if command typed after help.

**lcd** Displays local directory if typed alone or if path typed after lcd will change local directory.

**ls** Lists files of the remotely connected computer.

**mdelete** Multiple delete.

**mdir** Lists contents of multiple remote directories.

**mget** Get multiple files.

MIT ADT University, Pune

**mkdir** Make directory.

**mls** Lists contents of multiple remote directories.

**mput** Sent multiple files

**open** Opens address.

**prompt** Enables or disables the prompt.

**put** Send one file

**pwd** Print working directory

**remotehelp** Get help from remote server.

**rename** Renames a file.

**rmdir** Removes a directory on the remote computer.

**send** Send single file.

**status** Shows status of currently enabled and disabled options

**trace** Toggles packet tracing.

**Type** Set file transfer type.

**user** Send new user information.

**CONCLUSION:** we have implemented the Network Diagnostics and Troubleshooting Using TCP/IP Utilities and Commands for the network.

**Assignment 3: Router Configuration Using CLI**

Title: "Setting Up Secure and Customized Routers Using CLI Commands"

**Assignment Statement:**

Configure a router's basic settings, including hostname, banners, and password protection.

##### AIM:

To configure basic router settings using CLI commands to ensure secure access and provide essential information for network administrators.

###### Objectives:

1. Learn the syntax and structure of router CLI commands.
2. Configure router settings such as hostname, login banners, and passwords.
3. Understand the importance of securing access to network devices.
4. Save and verify the configuration to ensure persistence after reboots.

###### Outcomes:

By the end of this assignment, students will:

1. Demonstrate proficiency in configuring router settings using CLI commands.
2. Enhance the security of network devices by setting up passwords and login restrictions.
3. Create a custom login banner to display essential information for administrators.

###### Scenario:

**Industry Background:** You are a junior network engineer at **NextGen IT Solutions**, a company that designs and manages networks for SMEs. A tech startup is setting up its first office and has procured a new router to connect its internal LAN to the internet. As a junior network engineer, you are tasked with configuring the router using Command-Line Interface (CLI) commands. This includes

1. A customized hostname for easier identification in a multi-router network.
2. Login banners displaying authorized access warnings.
3. Secure passwords for console, VTY, and enable access.

Your configuration will serve as a model for the startup’s future network expansion plans. Your supervisor has asked you to complete these configurations on a sample router using CLI commands and verify the settings.

###### Tasks to Be Performed:

1. Access the router's CLI and configure the following:
   * Set a custom hostname (e.g., ClientRouter1).
     + Configure a login banner displaying the message: "Authorized Access Only."
     + Set up enable, console, and VTY passwords.
2. Save the configuration to the router's startup configuration.
3. Verify the configured settings using relevant show commands (e.g., show running- config).

MIT ADT University, Pune

1. Test access security by simulating login attempts with and without passwords.

##### THEORY

###### Router

A Router is a layer 3 network device that moves data between different network segments and can look into a packet header to determine the best path for the packet to travel. Routers can connect network segments that use different protocols. They also allow all users in a network to share a single connection to the Internet or a WAN. It is used to improve network performance by :-

* segmenting the network and creating separate collision & broadcast domains.
* reducing competition for bandwidth.
* Broadcasts are not forwarded to other network segments.
* Increases security by using Access Lists.

###### Router Components (Internal)

**ROM**

ROM is used to store the router's bootstrap startup program, operating system software, and power-on diagnostic tests programs. In order to perform ROM upgrades you remove and replace pluggable chips on the motherboard

**Flash Memory**

It holds operating system image(s). Flash memory is erasable, reprogrammable ROM. You can perform Cisco® IOS software upgrades without having to remove and replace chips. Flash content is retained when you switch off or restart the router.

**RAM**

RAM is used to store operational information such as routing tables, router's running configuration file. RAM also provides caching and packet buffering capabilities. Its contents are lost when you switch off or restart the router.

**NVRAM**

NVRAM (nonvolatile RAM), is used to store the router's startup configuration file. It does not lose data when power is switched off. So the contents of the startup configuration file are maintained even when you switch off or restart the router.

###### Lab Setup:

**Hardware/Software Required:**

1. **Router Model:** [Specify model, e.g., Cisco 2911 or similar]
2. **Software:** Cisco Packet Tracer or GNS3

###### Network Topology:

· One router connected to a PC via a console cable.

###### Steps to Follow:

**Step 1: Connect to the Router**

1. Power on the router.

MIT ADT University, Pune

1. Use a console cable to connect your PC to the router.
2. Open a terminal emulator (Putty or built-in terminal).

**Step 2: Access CLI Mode**

1. Once connected, press Enter to access the CLI.
2. You will enter User EXEC Mode (indicated by Router>).

**Step 3: Configure Basic Settings**

1. **Set the Hostname**
   1. Enter **Privileged EXEC Mode**:

Router> enable

* 1. Enter **Global Configuration Mode**:

Router# configure terminal

* 1. Set the hostname:

Router(config)# hostname BranchRouter

**Result:** The prompt changes to BranchRouter(config)#.

1. **Configure a Banner**
   1. Add a login banner (e.g., for security warnings):
   2. BranchRouter(config)# banner motd #

Unauthorized access is prohibited. Violators will be prosecuted. #

**Result:** A login banner will display whenever someone accesses the router.

1. **Secure Access with Passwords**

###### Set Console Password:

* 1. Access the console line configuration: BranchRouter(config)# line console 0
  2. Set the console password: BranchRouter(config-line)# password c0ns0lePass
  3. Enable login to require a password: BranchRouter(config-line)# login
  4. Exit line configuration mode:

BranchRouter(config-line)# exit

###### Set Privileged EXEC Password:

* 1. Configure a privileged EXEC password: BranchRouter(config)# enable password enablePass
  2. Encrypt the password for security:

BranchRouter(config)# service password-encryption

###### Set a Virtual Terminal (VTY) Password:

* 1. Access the VTY line configuration: BranchRouter(config)# line vty 0 4
  2. Set the VTY password:

MIT ADT University, Pune

BranchRouter(config-line)# password vtyPass

* 1. Enable login on VTY lines:

BranchRouter(config-line)# login

* 1. Exit line configuration mode:

BranchRouter(config-line)# exit

**Step 4: Save the Configuration**

1. Save the configuration to NVRAM:

BranchRouter# write memory

1. Verify the saved configuration:

BranchRouter# show running-config

#### Verification:

1. **Hostname:** Ensure the hostname is correctly displayed in the CLI prompt.
2. **Banner:** Log out and log back in to check if the banner appears.
3. **Passwords:** Verify that accessing the console and VTY requires the configured passwords.

|  |  |
| --- | --- |
| **BASIC MODE CHANGING COMMANDS** | |
| router> enable | Move from User to Privilege mode.  Prompt changes from Routername> to routername# |
| router# configure terminal | Changes the routers interface from Privileged mode to Global Configuration mode.  Prompt becomes Routername(config)# |
| router(config)#CRTL Z | Will exit Global configuration modeand return to Privileged mode. |
| router(config)#exit | Will exit the level of configuration and drop you down one level or back to privileged mode. |
| router# copy running- config startup- config | Copies the Running‐config (ram) to the Startup‐config (nvram). The configuration in NVRAM will be saved when the router is powered off |
| router(config)#no | No followed by any command will negate or reverse the command. To unset or set the opposite behavior of a command. |
| router(config)#hostname Lab-B | Name the router Lab-B  Name is case sensitive |
| Lab-B(config)#enable secret class | Sets the encrypted version of the routers password to ―class‖  Secret password overrides standard password. |
| Lab-B(config)#enable password cisco | Sets standard clear text password for router access. |
| **INTERFACE CONFIGURATION –FAST ETHERNET PORT** | |
| Lab-B(config)#interface fastethernet 0/0 | Interface FastEthernet 0/0  Changes the configuration mode from Global to Interface for the FastEthernet (100 Mps) |
| Lab-B(config if) # ip address 219.17.100.1  255.255.255.0 | Assigns the IP address 219.17.100.1 to the interface. Subnet mask for Class C address. |
| Lab-B(config-  if)#description Connected to LAN B | Provides a description to an interface. |
| Lab-B(config-if)#no shutdown | Enables the interface. By default all interface are shutdown. You must use ―no shutdown‖ to remove the shutdown command |
| **INTERFACE CONFIGURATION –SERIAL PORT** | |
| Lab-B(config)#interface serial 0/0/0 | Interface Serial 0/0/0 Changes the configuration mode from Global to Interface for the Serial port. |

#### Conclusion:

We have successfully configured the basic settings of a router, including hostname, banners, and password protection. These steps help secure the router and prepare it for further configurations.

**Assignment 4: Configure a Router with Static and Dynamic Routing**

###### Title: "Enabling Efficient Traffic Flow with Static and Dynamic Routing Protocols

###### Assignment Statement:

Configure a router (Ethernet and Serial Interface) using router commands for:

1. Static Routing
2. Dynamic Routing (RIPV1, RIPV2) on any network simulator (e.g., Cisco Packet Tracer).

##### AIM:

To configure and verify static and dynamic routing protocols to manage traffic efficiently in a multi-router network.

###### Objectives:

1. Understand the differences between static and dynamic routing.
2. Learn to configure static routes for predefined traffic paths.
3. Implement dynamic routing protocols (RIPV1 and RIPV2) to enable automatic route updates.

###### Test and validate routing configurations using network simulators.

###### Outcomes:

By the end of this assignment, students wil

1. Configure static routes between routers for specific network segments.
2. Implement and troubleshoot dynamic routing protocols (RIPV1 and RIPV2).
3. Evaluate the advantages and limitations of static and dynamic routing.

###### Scenario:

**Industry Background:** You are part of the network design team at **GlobalLink Networks**, a logistics company with operations in different cities relies on a robust network to manage real- time shipment tracking and communication. The company needs static routes to establish direct connections between the head office and nearby branches and dynamic routing (using RIPV1 and RIPV2) for automatic updates in distant locations. As the network engineer, you are responsible for configuring these routing protocols on the company’s routers. This setup will ensure reliable communication between all offices and support the company’s rapid expansion and also the solution must optimize traffic flow and ensure connectivity across all branches.

###### Tasks to Be Performed:

1. Configure IP addresses for router interfaces and test connectivity between directly connected networks.
2. Set up static routes between the main office and a branch office.
3. Configure RIPV1 for older routers without subnetting capabilities.
4. Implement RIPV2 for modern routers with subnetted networks.
5. Verify configurations using ping and traceroute commands to test end-to-end connectivity.
6. Analyze and document routing tables to ensure proper traffic flow.

MIT ADT University, Pune

##### THEORY:

###### Static Routing

Static routing occurs when you manually add routes in each router's routing table. There are advantages and disadvantages to static routing, but that's true for all routing processes.

###### Static routing has the following advantages:

* There is no overhead on the router CPU.
* There is no bandwidth usage between routers.
* It adds security because the administrator can choose to allow routing access to certain networks only.

###### Static routing has the following disadvantages:

* The administrator must really understand the internetwork and how each router is connected in order to configure routes correctly.
* If a network is added to the internetwork, the administrator has to add a route to it on all routers— manually.
* It's not possible in large networks because maintaining it would be a full-time job in itself.

###### Command syntax for static route:

ip route [destination\_network] [mask] [next-hop\_address or exit\_interface] [administrative\_distance] [permanent]

**ip route :** The command used to create the static route. **destination\_network :** The network you're placing in the routing table. **mask :** The subnet mask being used on the network.

**next-hop\_address :** The address of the next-hop router that will receive the packet and

forward it to the remote network.

**exit\_interface :** Used in place of the next-hop address if you want, and shows up as a directly connected route.

**administrative\_distance** : By default, static routes have an administrative distance of 1 (or even 0 if you use an exit interface instead of a next-hop address).

**permanent Keyword (Optional) :** Without the permanent keyword in a static route statement, a static route will be removed if an interface goes down. Adding the permanent keyword to a static route statement will keep the static routes in the routing table even if the interface goes down and the directly connected networks are removed.

##### CONFIGURATION:

###### 

Configure IP address to routers go to global configuration mode in R1 and R2 configure connected interfaces.

###### In Router 1

Interface Fastethernet0/0 in global configuration mode

R1(config)#interface fastethernet 0/0 R1(config-if)#ip address 10.0.0.1 255.0.0.0 R1(config-if)#no shutdown

R1(config-if)#exit

Interface Serial 2/0

R1(config)#interface serial 2/0

R1(config-if)#ip address 20.0.0.1 255.0.0.0

R1(config-if)#clock rate 64000

R1(config-if)#bandwidth 64 R1(config-if)#no shutdown R1(config-if)#exit

###### In Router 2

Interface Fastethernet 0/0

R2(config)#interface fastethernet 0/0 R2(config-if)#ip address 30.0.0.1

255.0.0.0 R2(config-if)#no shutdown R2(config-if)#exit

**Interface Serial 2/0**

R2(config)#interface serial 2/0

R2(config-if)#ip address 20.0.0.2 255.0.0.0 R2(config-if)#no shutdown R2(config-if)# exit

MIT ADT University, Pune

Assign IP address for both PC's with appropriate ip and subnetmask and default gateway. Now configure both routers with static route. By default, Routers Know only directed connected networks here Router 1 know only 10.0.0.0 and 20.0.0.0 it doesn't know the 30.0.0.0 like this R2 doesn't know about 10.0.0.0.So We are going to add Static route to this both router

R1(config)# ip route Destination Network| Destination N/W SubnetMask |Next Hop Address

In Router R1,Just give this command, In this case Destination is 30.0.0.0 and its subnet mask is 255.0.0.0 next hop address is 20.0.0.2

###### R1(config)#ip route 30.0.0.0 255.0.0.0 20.0.0.2

In Router R2

###### R2(config)#ip route 10.0.0.0 255.0.0.0 20.0.0.1

That‘s it! Now both routers know all networks, check by ping IP address of hosts.