

LABORATORY MANUAL FOR NETWORKING LAB

4TH Semester

Diploma in Computer Science & Engineering



C. V. Raman Polytechnic

Bidya Nagar, Mahura, Janla, Bhubaneswar

S/N NO	LIST OF PRACTICALS	PAGE NO
1	Recognize the physical topology and cabling (coaxial, OFC, UTP, STP) of a Network	1-7
2	Recognition and use of various types of connectors RJ-45, RJ-11, BNC and SCST.	8-11
3	Making of cross cable and straight cable.	12-14
4	Install and configure a network interface card in workstation.	15-17
5	Identify the IP address of a workstation and the class of the address and configure the IP Address on a workstation.	18-24
6	Managing user accounts in windows and LINUX	25-26
7	Sharing of Hardware resources in the network.	27-28
8	Use of Netstat and its options	29
9	Connectivity troubleshooting using PING, IPCONFIG	30
10	Installation of Network Operating System (NOS).	31-33
11	Create a network of at least 6 computers	34-35
12	Study of Layers of Network and Configuring Network Operating System	36-42
13	Study of Routing and Switching, configuring of Switch and Routers, Troubleshooting of Networks.	43-53

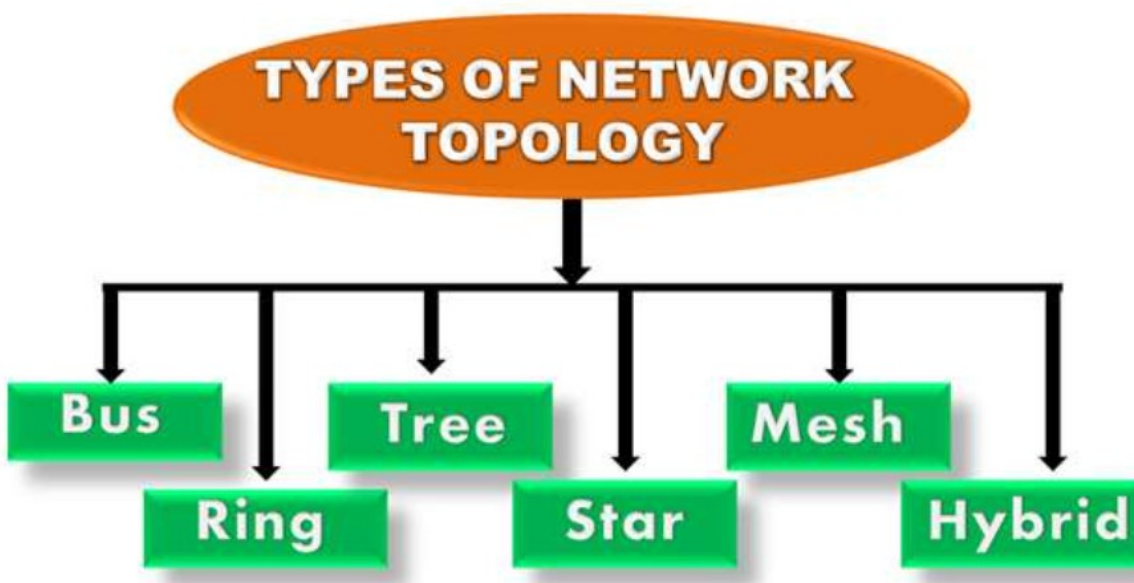
14	Study of Scaling of Networks, Design verities of LAN and forward of traffic	54-56
15	Study WAN concepts and Configure and forward Traffic in WAN	57-58
16	Configure IPv4 and IPv6 and learn Quality, security and other services	59-74
17	Learn Network programming	75-78
18	Troubles shoot Networks	79-152

Practical 1

Aim: Recognize the physical topology and cabling(coaxial, OFC, UTP, STP) of a network.

Physical Topology: -The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as network topology.

Topology is derived from two Greek words topo and logy, where topo means 'place' and logy means 'study'. In computer networks, a topology is used to explain how a network is physically connected and the logical flow of information in the network. A topology mainly describes how devices are connected and interact with each other using communication links.



A} Mesh Topology:

In a mesh topology, every device is connected to another device via a particular channel.

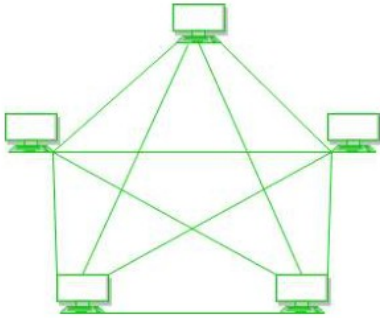
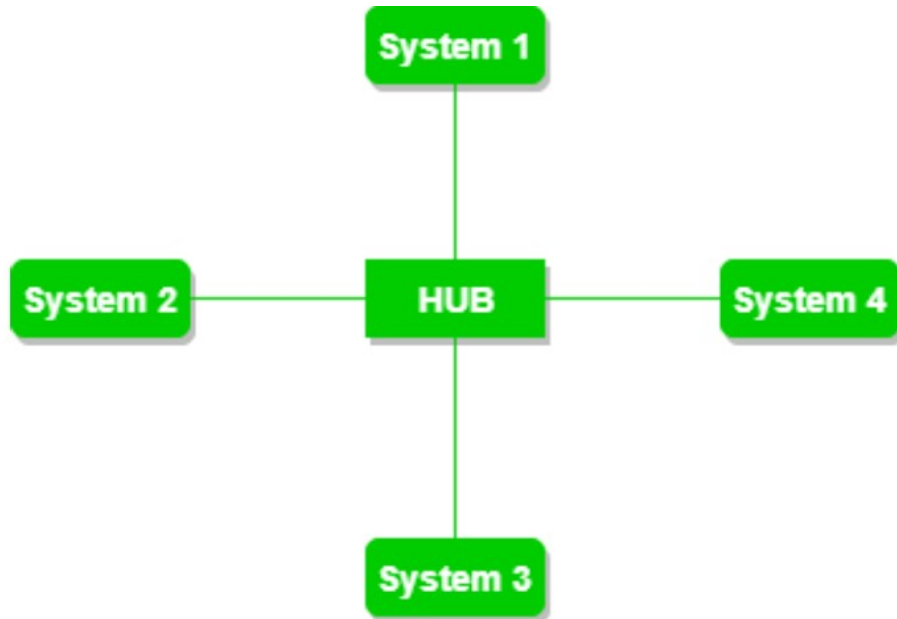


Figure 1: Every device is connected with another via dedicated channels. These channels are known as links.

- Suppose, N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is $N-1$. In Figure 1, there are 5 devices connected to each other, hence the total number of ports required by each device is 4. Total number of ports required = $N*(N-1)$.
- Suppose, N number of devices are connected with each other in a mesh topology, then the total number of dedicated links required to connect them is $\frac{N(N-1)}{2}$ i.e. $\frac{N(N-1)}{2}$. In Figure 1, there are 5 devices connected to each other, hence the total number of links required is $\frac{5*4}{2} = 10$.

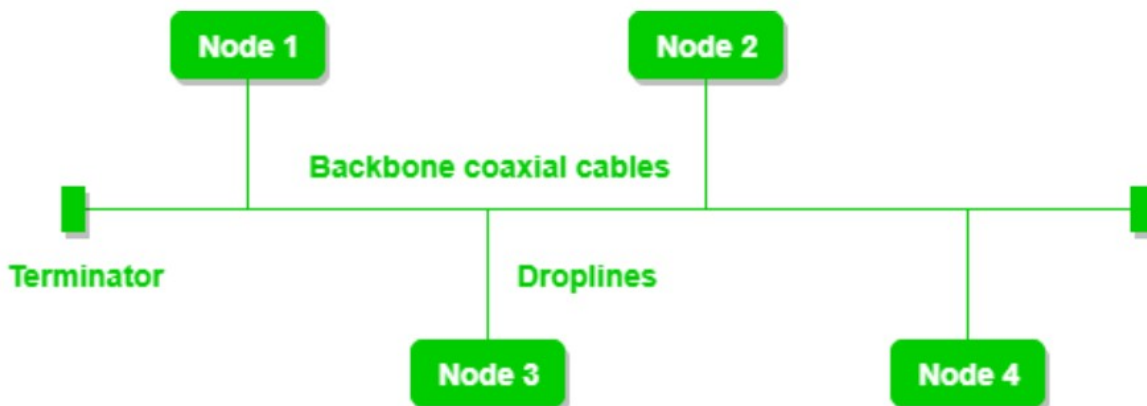
B} Star Topology:

In star topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them.



c) Bus Topology:

Bus topology is a network type in which every computer and network device is connected to a single cable. It transmits the data from one end to another in a single direction. No bi-directional feature is in bus topology. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.



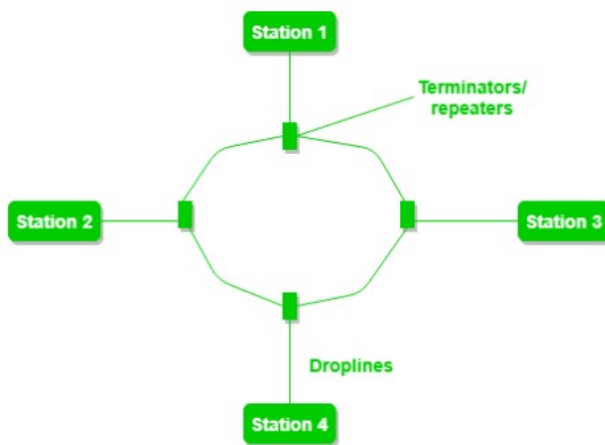
D} Ring Topology :

In this topology, it forms a ring connecting devices with itsexactly two neighbouring devices.

A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node.

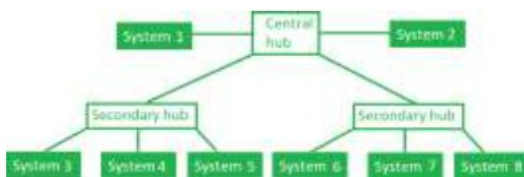
Hence to prevent data loss repeaters are used in the network.

The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology.



E} Tree Topology:

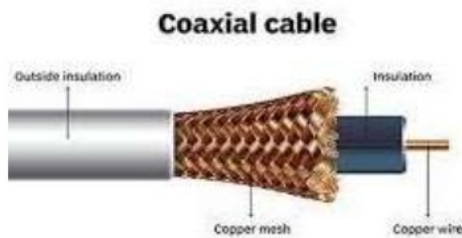
This topology is the variation of Star topology. This topology has a hierarchical flow of data.



➤ Cabling (networking)

Cabling is the set of wires made of either copper or glass that is used to connect computers and other network components to enable them to communicate, thus forming a network of computers.

coaxial→Coaxial cables, commonly called coax, are copper cables with metal shielding designed to provide immunity against noise and greater bandwidth. Coax can transmit signals over larger distances at a higher speed as compared to twisted pair cables.

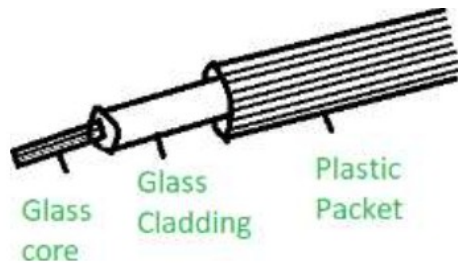


Structure of Coaxial Cables

Coax has a central core of stiff copper conductor for transmitting signals. This is covered by an insulating material. The insulator is encased by a closely woven braided metal outer conductor that acts as a shield against noise.

Optical Fiber→ An **Optical Fiber** is a cylindrical fiber of glass which is hair thin size or any transparent dielectric medium.

The fiber which is used for optical communication is waveguides made of transparent dielectrics.



Main element of Fiber Optics:

1. Core:

It is the central tube of very thin size made of optically transparent dielectric medium and carries the

light transmitter to receiver and the core diameter may vary from about 5um to 100 um.

2. Cladding:

It is outer optical material surrounding the core having reflecting index lower than core and cladding helps to keep the light within the core throughout phenomena of total internal reflection.

3. Buffer Coating:

It is a plastic coating that protects the fibre made of silicon rubber. The typical diameter of the fibre after the coating is 250-300 um.

UTP (Unshielded Twisted Pair) → UTP is an unshielded twisted pair cable used in computer and telecommunications mediums. Its frequency range is suitable for transmitting both data and voice via a UTP cable. Therefore, it is widely used in the telephone, computers, etc. It is a pair of insulated copper wires twisted together to reduce noise generated by external interference. It is a wire with no additional shielding, like aluminium foil, to protect its data from the exterior.

Unshielded Twisted Pair Cable



STP (Shielded twisted pair):

A shielded twisted pair is a type of twisted pair cable that contains an extra wrapping foil or copper braid jacket to protect the cable from defects like cuts, losing bandwidth, noise, and signal to the interference. It is a cable that is usually used underground, and therefore it is more costly than UTP. It supports higher data transmission rates across the long distance. We can also say it is a cable with metal sheath or coating that surrounds each pair of the insulated conductor to protect the wire from external users and prevent electromagnetic noise from penetrating.

Shielded Twisted Pair (STP)



Practical 2

Aim: Recognition and use of various types of connectors RJ-45, BNC and SCST.

Connectors A device that eliminates a section of cabling or implements a state of access for network devices, including PCs, hubs, and switches. Connectors can be famous for their physical presentation and mating features, including jacks and attachment (male connectors) or attachments and ports (female connectors).

Connectors are used to connect the guided (wired) transmission media to devices like the hub, server, workstations etc.



RJ45→RJ45 is newer, modular, self-securing and compact technology used for connecting the ethernet cables to different electronic devices. The RJ45 is an 8 pin connector used to attach the ethernet interfaces. It is known as an 8P8C connector.

1. Types of cables based on the termination: Straight-overcable
2. Crossover cable



RJ11→RJ11 is used to terminate the conventional PSTN telephone networks. RJ11 is a four pins connector which is used for terminating the telephone wires. The RJ11 technically uses the centre 2 contacts of 6 available and is used for wiring a singlephone line. It is the common connector for plugging a telephone into the wall and the handset into the telephone.



BNC→Virtually any standard connector is able to carry current over a mechanical connection for DC and low-frequency AC circuits. Radio frequency, on the other hand, requires a connection that will minimize changes in impedance, which could generate reflection and standing waves that can causedamage. Coaxial cables can carry radio frequencies while maintaining a characteristic impedance.

BNCs are constant impedance connectors—they have the same characteristic impedance across the whole connection, equal to that of coaxial cables. This makes BNC connectors well-suited for RF applications, as RF signals traveling along a coax cablewill not see any

impedance changes as they pass through the BNC connector, resulting in fewer reflections and a lower level of loss.



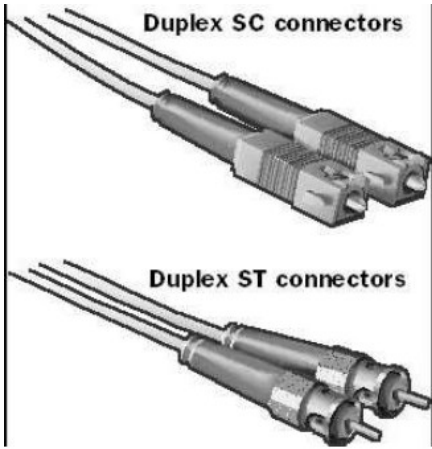
SCST

SC stands for subscriber connector and is a standard-duplex fiber-optic connector with a square molded plastic body and

push-pull locking features. SC connectors are typically used in data communication, CATV, and telephony environments.

ST stands for straight tip, a high-performance fiber-optic connector with round ceramic ferrules and bayonet locking features. ST connectors are more common than SC connectors.

You can generally use SC and ST connectors with either single-mode or multimode fiber-optic cabling. Coupling receptacles for these connectors come in either panel-mount or free-handing designs. For narrow space installations, you can get 90-degree boot versions instead of straight versions. SC and ST connectors come in both simplex and duplex form.



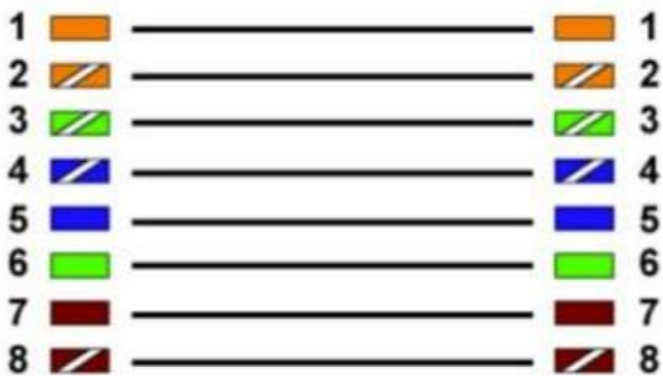
Practical 3

Aim: Making of cross cable and straight cable.

Ethernet straight-through cable

In this cable, wires are placed in the same position at both ends. The wire at pin 1 on one end of the cable connects to pin 1 at the other end of the cable. The wire at pin 2 connects to pin 2 on the other end of the cable; and so on.

Side A	Side B
Green White	Green White
Green	Green
Orange White	Orange White
Blue	Blue
Blue White	Blue White
Orange	Orange
Brown White	Brown White
Brown	Brown



The following image shows the straight-through cable.

A straight-through cable is used to connect the following devices.

- PC to Switch
- PC to Hub
- Router to Switch
- Switch to Server
- Hub to Server

Ethernet cross-over cable

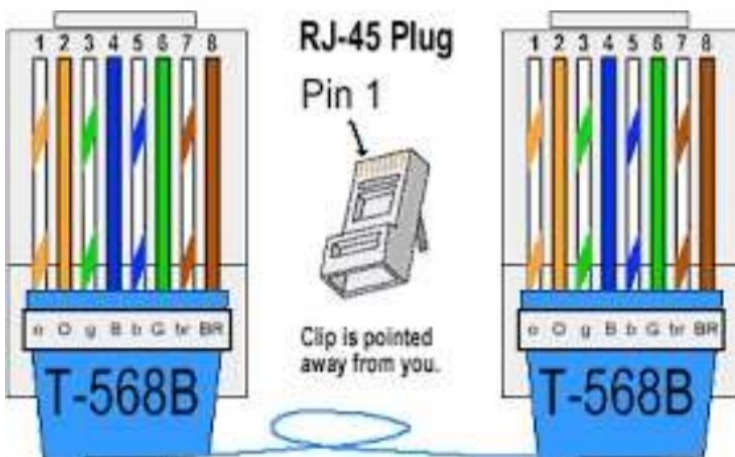
In this cable, transmitting pins of one side connect with the receiving pins of the other side.

The wire at pin 1 on one end of the cable connects to pin 3 at the other end of the cable. The wire at pin 2 connects to pin 6 on the other end of the cable. Remaining wires connect in the same positions at both ends.

The following table lists the wire positions of the cross-over cable on both sides.

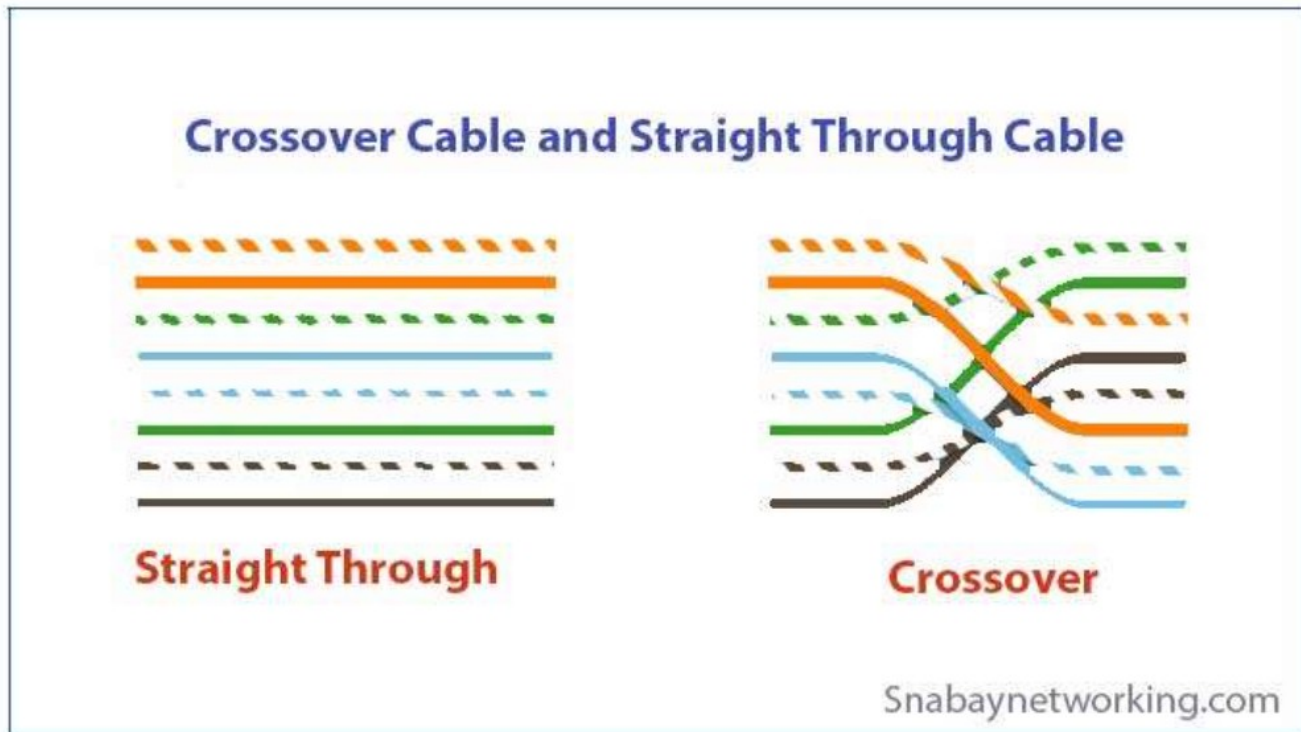
Side A	Side B
Green White	Orange White
Green	Orange
Orange White	Green White
Blue	Blue
Blue White	Blue White
Orange	Green
Brown White	Brown White
Brown	Brown

The following image shows the cross-over cable.



The cross-over cable is used to connect the following devices.

- Two computers
- Two hubs
- A hub to a switch
- A cable modem to a router
- Two router interfaces



Cross cable	Straight cable
Connecting devices from pc or router or sever to pc, router or server requires cross cable. Also connecting devices from switch or hub to switch or hub requires cross cable.	Connecting devices from pc or router or server to switch or hub requires straight cable
Here <u>pin</u> 1 is connected to 3, 2 is connected to 6, 3 is connected to 1 and 6 is connected to 2.	Here <u>pin</u> 1 is connected to 1, 2 is connected to 2, 3 is connected to 3 and 6 is connected to 6.

Practical 4

Aim: Install and configure a network interface card in a workstation.

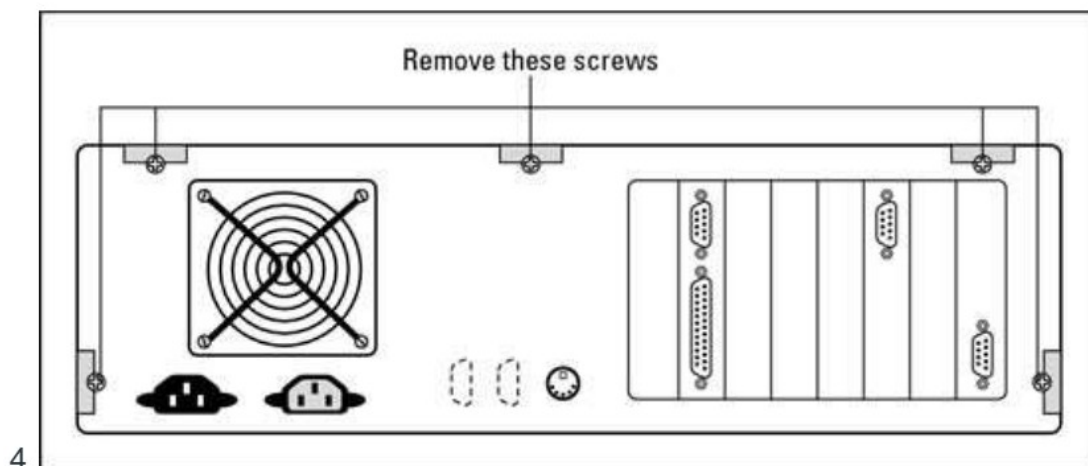
To connect a computer to your network, the computer must have a network interface. Virtually all computers sold in the last 10 years or so have a network interface built-in on the motherboard.

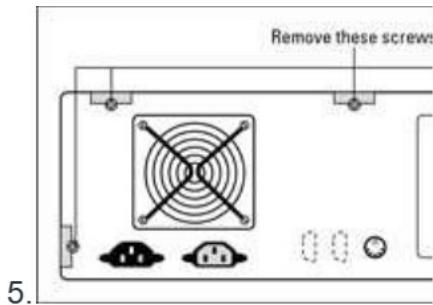
However, you may still encounter the occasional older computer that doesn't have a built-in network interface. In that case, you must install a network interface card to enable the computer for your network. Installing a network interface card is a manageable task, but you have to be willing to roll up your sleeves. If you've ever installed one of these cards, you can probably install a network interface card blindfolded.

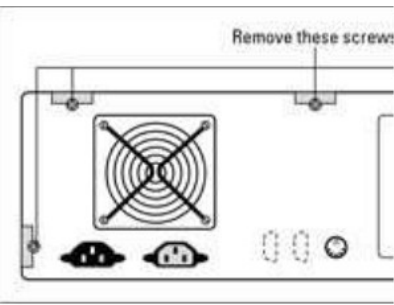
1. Assemble your materials.

Gather up the network card and the driver disks. While you're at it, get your Windows installation CD just in case.

2. Shut down Windows, turn off the computer and unplug it. Never work in your computer's insides with the power on or the power cord plugged in!
3. Remove the cover from your computer.





5. 
6. You must typically remove a number of screws to open the cover. Put the screws someplace where they won't wander off. If you have a name-brand computer such as a Dell or a Compaq, opening the cover may be trickier than just removing a few screws. You may need to consult the owner's manual that came with the computer to find out how to open the case.
7. Find an unused expansion slot inside the computer.
The expansion slots are lined up in a neat row near the back of the computer; you can't miss them. Any computer less than five years old should have at least two or three slots known as *PCI slots*.
8. Remove the metal slot protector from the back of the computer's chassis.
If a small retaining screw holds the slot protector in place, remove the screw and keep it in a safe place because you will need it later. Then pull the slot protector out and discard.
9. Insert the network interface card into the slot.
Line up the connectors on the bottom of the card with the connectors in the expansion slot and then press the card straight down. Sometimes you have to press uncomfortably hard to get the card to slide into the slot.
10. Secure the network interface card.
Remember that screw you put in a safe place? Use it to stabilize the network interface card.

11. Put the computer's case back together.

Watch out for the loose cables inside the computer; you don't want to pinch them with the case as you slide it back on. Secure the case with the screws that you removed earlier.

12. Plug in the computer and turn it back on.

If you're using a Plug and Play card with Windows, the card is automatically configured after you start the computer again. If you're working with an older computer or an older network interface card, you may need to run an additional software installation program. See the installation instructions that come with the network interface card for details.

Network Interface Card (NIC)

A network interface card (NIC) is a circuit board or [card](#) that is installed in a computer so that it can be connected to a network. A network interface card provides the computer with a dedicated, full-time connection to a network. Personal computers and workstations on a local area network ([LAN](#)) typically contain a network interface card specifically designed for the LAN transmission technology.



PCI Network Interface Card



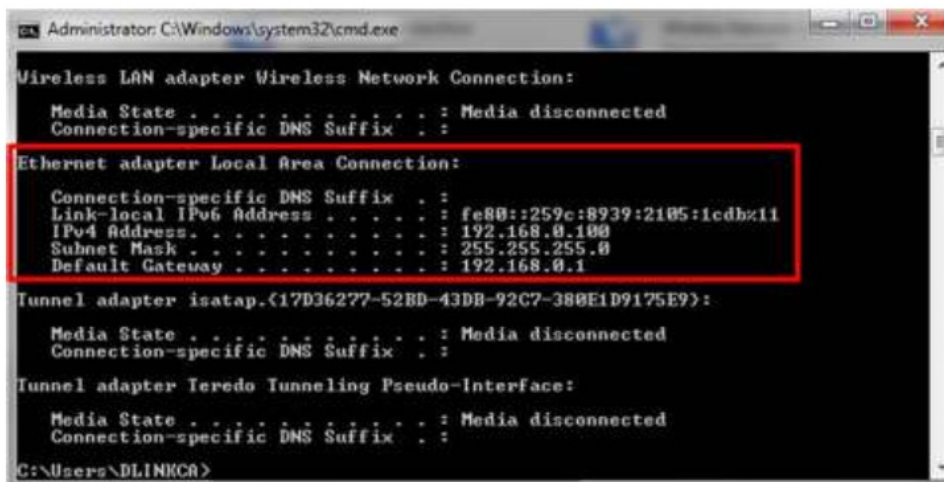
ComputerHope.com

Practical 5

Aim: Identify the IP address of workstation and the class of the address and configure the IP Address on a workstation.

All the computers of the world in the Internet network communicate with each other with underground or underwater cables or wirelessly. If I want to download a file from the internet or load a web page or literally do anything related to the internet, my computer must have an address so that other computers can find and locate mine in order to deliver that particular file or webpage that I am requesting. In technical terms, that address is called **IP Address or Internet Protocol Address**.

Similarly, your computer too needs an address so that other computers on the internet can communicate with each other without the confusion of delivering information to someone else's computer. And that is why each computer in this world has a unique IP Address. Or in other words, an IP address is a unique address that is used to identify computers or nodes on the internet. This address is just a string of numbers written in a certain format. It is generally expressed in the set of numbers for example 192.155.12.1. Here each number in the set is from 0 to 255 range. Or we can say that a full IP address ranges from 0.0.0.0 to 255.255.255.255. And these IP addresses are assigned by IANA (known as Internet Corporation for Internet Assigned Numbers Authority).



```
Administrator: C:\Windows\system32\cmd.exe
Wireless LAN adapter Wireless Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::259c:8939:2105:1cdb%11
IPv4 Address. . . . . : 192.168.0.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1

Tunnel adapter isatap.{17D36277-52BD-43DB-92C7-388E1D9175E9}:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

C:\Users\DLINKRA>
```

Working of IP addresses:

The working of IP addresses is similar to other languages. It can also use some set of rules to send information. Using these protocols we can easily send, receive data or files to the connected devices. There are several steps behind the scenes. Let us look at them

- Your device directly requests your Internet Service Provider which then grants your device access to the web.
- And an IP Address is assigned to your device from the given range available
- Your internet activity goes through your service provider, and that they route it back to you, using your IP address.
- Your IP address can change. For example, turning your router on or off can change your IP Address.
- When you are out from your home location your home IP address doesn't accompany you. It changes as you change the network of your device.

Types of IP Address

IP Address is of two types:

1. IPv4: Internet Protocol version 4. It consists of 4 numbers separated by the dots. Each number can be from 0-255 in decimal numbers. But computers do not understand decimal numbers, they instead change them to binary numbers which are only 0 and 1. Therefore, in binary, this (0-255) range can be written as (00000000 – 11111111). Since each number N can be represented by a group of 8 digit binary digits. So, a whole IPv4 binary address can be represented by 32-bits of binary digits. In IPv4, a unique sequence of bits is assigned to a computer, so a total of (2^{32}) devices approximately = 4,294,967,296 can be assigned with IPv4.

IPv4 can be written as:

189.123.123.90

Classes of IPv4 Address: There are around 4.3 billion IPv4 addresses and managing all those addresses without any scheme is next to impossible. Let's understand it with a simple example. If you have to find a word from a language dictionary, how long will you take? Usually, you will take less than 5 minutes to find that word. You are able to do this because words in the dictionary are organized in alphabetical order. If you have to find out the same word from a dictionary that doesn't use any sequence or order to organize the words, it will take an eternity to find the word. If a dictionary with one billion words without order can be so disastrous, then you can imagine the pain behind finding an address from 4.3 billion addresses.

- 2. IPv6:** But, there is a problem with the IPv4 address. With IPv4, we can connect only the above number of 4 billion devices uniquely, and apparently, there are much more devices in the world to be connected to the internet. So, gradually we are making our way to **IPv6 Address** which is a 128-bit IP address. In human-friendly form, IPv6 is written as a group of 8 hexadecimal numbers separated with colons (:). But in the computer-friendly form, it can be written as 128 bits of 0s and 1s. Since, a unique sequence of binary digits is given to computers, smartphones, and other devices to be connected to the internet

IPv4	IPv6
Deployed 1981	Deployed 1998
32-bit IP address	128-bit IP address
4.3 billion addresses	7.9×10^{28} addresses
Addresses must be reused and masked	Every device can have a unique address
Numeric dot-decimal notation 192.168.5.18	Alphanumeric hexadecimal notation 50b2:6400:0000:0000:6c3a:b17d:0000:10a9 (Simplified - 50b2:6400::6c3a:b17d:0:10a9)
DHCP or manual configuration	Supports autoconfiguration

IP Class	Address Range	Maximum number of networks
Class A	0-127	128
Class B	128-191	16384
Class C	192-223	2097157
Class D	224-239	Reserve for multitasking
Class E	240-254	Reserved for Research and development

IPv6 can be written as: But, there is a problem with the IPv4 address. With IPv4, we can connect only the above number of 4 billion devices uniquely, and apparently, there are much more devices in the world to be connected to the internet. So, gradually we are making our way to **IPv6 Address** which is a 128-bit IP address. In human-friendly form, IPv6 is written as a group of 8 hexadecimal numbers separated with colons (:).

2011:0bd9:75c5:0000:0000:6b3e:0170:8394

Classification of IP Address

An IP address is classified into the following types:

1. **Public IP Address:** This address is available publicly and it is assigned by your network provider to your router, which further divides it to your devices. Public IP Addresses is of two types:

- **Dynamic IP Address:** When you connect a smartphone or computer to the internet, your Internet Service Provider provides you an IP Address from the range of available IPAddresses. Now, your device has an IP Address and you cansimply

connect your device to the Internet and send and receive data to and from your device. The very next time when you try to connect to the internet with the same device, your provider provides you with different IP Addresses to the same device and also from the same available range. Since IP Address keeps on changing every time when you connect to the internet, it is called Dynamic IP Address.

- **Static IP Address:** Static address never changes. They serve as a permanent internet address. These are used by DNS servers. What are DNS servers? Actually, these are computers that help you to open a website on your computer. Static IP Address provides information such as device is located in which continent, which country, which city, and which Internet Service Provider provides internet connection to that particular device. Once, we know who is the ISP, we can trace the location of device connected to the internet. Static IP Addresses provide less security than Dynamic IP Addresses because they are easier to track.

2. **Private IP Address:** This is an internal address of your device which are not routed to the internet and no exchange of data can take place between a private address and the internet.
3. **Shared IP addresses:** Many websites use shared IP addresses where the traffic is not huge and very much controllable, they decide to rent it to other similar websites so to make it cost-friendly. Several companies and email sending servers use the same IP address (within a single mail server) to cut down the cost so that they could save for the time the server is idle.
4. **Dedicated IP addresses:** A dedicated IP Address is an address used by a single company or an individual which gives them certain benefits using a private Secure Sockets Layer (SSL) certificate which is not in the case of a shared IP address. It allows to access the website or log in via File Transfer

Types of IP Address

Private **Public** **Static/ Dynamic**

5.

Lookup IP addresses

To know your public IP, you can simply search “What is my IP?” on Google. Other websites will show you equivalent information: they will see your public IP address because, by visiting the location, your router has made an invitation/request and thus revealed the information. The location IP location goes further by showing the name of your Internet Service Provider and your current city.

Finding your device's private IP Address depends on the OS or platform you are using.

- **On Windows:** Click Start and type “cmd” in the search box and run the command prompt. In the black command prompt dialog box type “ipconfig” and press enter. You will be able to see your IP Address there.
- **On Mac:** Go to system preferences and select Network, you will be able to see the information regarding your network which includes your IP Address.

Protect and hide IP address:

To secure and hide your IP address from unwanted people always remember the following points:

- Use a proxy server.

- Use a virtual private network (VPN) when using publicWi-Fi, you are traveling, working remotely, or just wantsome privacy.
- Change privacy settings on instant messaging applications.
- Create unique passwords.
- Beware of phishing emails and malicious content.
- Use a good and paid antivirus application and keep it up to date.
- When you are using public wifi in a cafe or station or anywhere, you must hide your IP address by using VPN. Getting your IP from public wifi is just a cakewalk for these hackers and they are very good at stealing all yourinformation while using your computer's address. Thereare different phishing techniques in which they email you, call you, SMS you about giving vital information about you. They give links to vicious websites which are pre-rigged. The moment you open these websites, they steal all your device's information revealing all the information about you and your device which are to bekept private. These leaks help the hackers to exploit your device and you and install or download some spyware and malware in your device. But using a good anti-virus gives you web security as well, which will prevent those websites to launch and warn you about the information being passed to these websites.
- It is also not recommended to use torrent or pirated websites which are a threat to your online identity andcan compromise your device or mails or any otherinformation about you

Practical 6

Aim: Managing user accounts in windows and LINUX

Linux →



1. To add a user account, use the adduser command. See the adduser command page for additional information about this command.
2. To remove a user account, use the deluser command. See the deluser command page for additional information about this command.
3. To change the user settings, such as group membership, default login shell, and home directory, use the usermod command. See the usermod command page for additional information about this command.

Windows 10

1. Press the Windows key, type Control Panel, and then press Enter.
2. Select User Accounts.

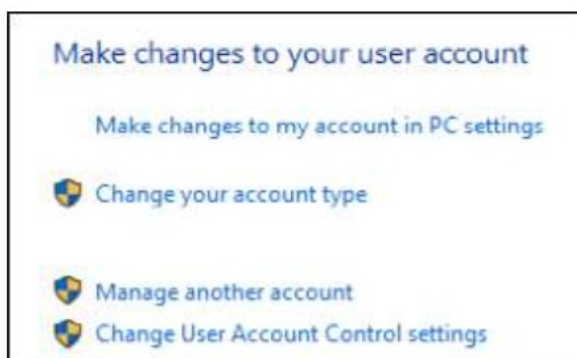


3. Click User Accounts again.



4. In the User Accounts window, the middle section allows you to change various aspects

of user accounts. Clicking the Manage another account link takes you to a menu where you may add, edit, or remove user accounts.

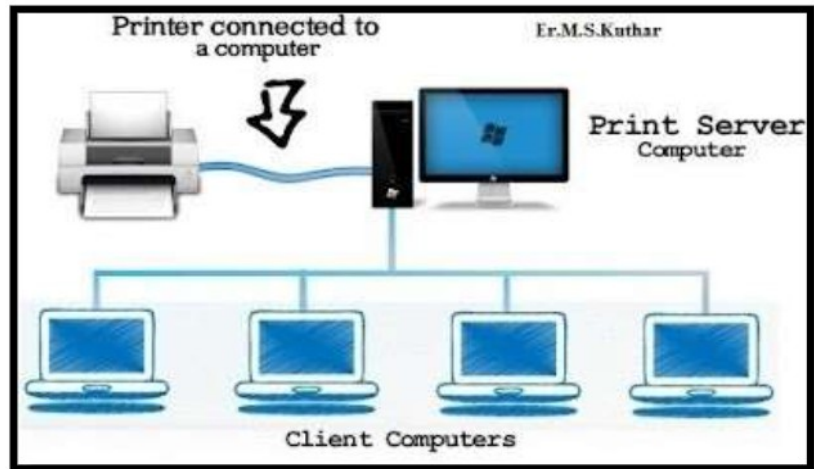


Parameters	LINUX	WINDOWS
Inception Year	1991	1985
Standard	Open source operating system which is freely available	Closed Source Operating system
Webserver share	70% share	23% share
Filesystem	ext2-4, FAT, NTFS, NFS, ISO 9660, JFS, KFS	NTFS, FAT, ISO 9660, UDF, HFS
Cost	Low cost Hardware	High cost hardware
Security	Secure	Insecure
Virus	60-100 virus listed	60,000 viruses listed
Developed by	Linus Torvalds	Microsoft
Source Code	There is full access to source code	There is no access to source code
Configuration storage	Maintains configuration in files	Maintains a registry to store configurations



Practical 7

Aim: Sharing of Hardware resources in the network.



Procedure to share hardware resources (printer) over network.

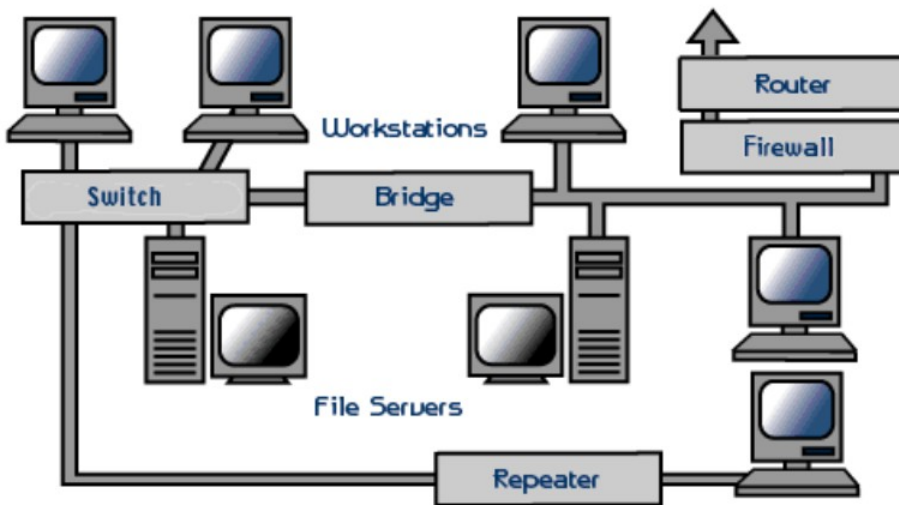
- Click on Start in the bottom left corner of your screen. Popup list will appear.
- Select Control Panel from the popup list. Type the word network in the search box.
- Click on Network and Sharing Center.
- Click on Change advanced shared settings, in the left pane.
- Click on the down arrow, which will expand the network profile.
- Select File and printer sharing and choose Turn on file and printer sharing.
- Click on Save changes.

You're now ready to share your printer.

1. Click on Start in the bottom left corner of your screen. A popup list will appear.
2. Click on Devices and Printers, from the popup list.
3. Right click the printer you want to share. A drop-down list will appear.
4. Select Printer properties from the drop-down list.
5. Click on the Sharing tab
6. Select the Share this printer check box.

In order for other people to connect to the printer, they just have to add the network printer that you just opened for sharing to their computers. Here's how to do this.

1. Click on Start in the bottom left corner of your screen. A popup list will appear.
2. Click on Devices and Printers from the popup list.
3. Select Add a printer.
4. Click on Add a network, wireless or Bluetooth printer.
5. Click the shared printer.
6. Click Next. Continue according to the instructions on the screen



SHARING RESOURCES

□ Types of resources are:

1. **Hardware:** A network allows users to share many hardware devices such as printers, modems, fax machines, CD ROM, players, etc.
2. **Software:** sharing software resources reduces the cost of software installation, saves space on hard disk.

Practical 8

Aim: Use of Netstat and its options.

Netstat — derived from the words network and statistics — is a program that's controlled via commands issued in the commandline. It delivers basic statistics on all network activities and informs users on which ports and addresses the corresponding connections (TCP, UDP) are running and which ports are open for tasks. In 1983, netstat was first implemented into the Unix derivative BSD (Berkley Software Distribution), whose version

4.2 supported the first internet protocol family, TCP/IP. netstat has been integrated into Linux since its debut in 1991 and has been present in Windows since the appearance of version

3.11 (1993), which could also communicate via TCP/IP with the help of extensions.

[OPTION]	Command	Description
	netstat	Standard listing of all active connections
-a	netstat -a	Displays all active ports
-b	netstat -b	Displays the executable file of a connection or listening port (requires administrator rights)
-e	netstat -e	Shows statistics about your network connection (received and sent data packets, etc.)
-f	netstat -f	Displays the fully qualified domain name (FQDN) of remote addresses
-i	netstat -i	Brings up the netstat overview menu
-n	netstat -n	Numerical display of addresses and port numbers
-o	netstat -o	Displays the process identifier (PID) associated with each displayed connection
-p Protokoll	netstat -p TCP	Displays the connections for the specified protocol, in this case TCP (also possible: UDP, TCPv6, or UDPv6)

Practical 9

Aim: Connectivity troubleshooting using PING, IPCONFIG, IFCONFIG.

Ping (Packet Internet Groper) is a method for determining communication latency between two networks. Simply put, ping is a method of determining latency or the amount of time it takes for data to travel between two devices or across a network. As communication latency decreases, communication effectiveness improves.

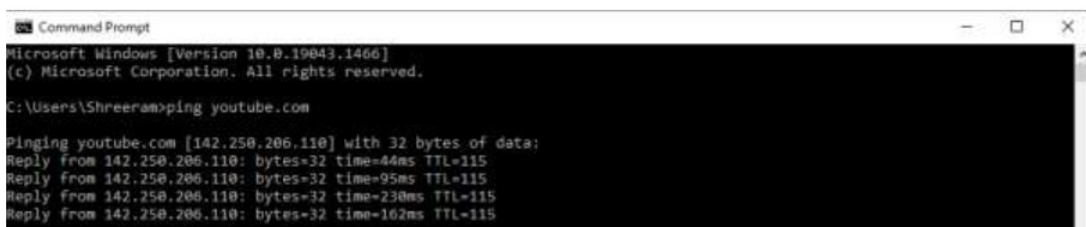
A low ping time is critical in situations where the timely delivery of data is more important than the quantity and quality of the desired information.

How To Get the Ping Value of Any Site Corresponding to Your Server?

- The ping value represents the strength of a connection between two computers or a network. You can check the ping of any website that corresponds to your computer using a command prompt for Windows or a terminal for Mac.
- Simply type the “ping<space>website name” into the command prompt or terminal to have your system send some data packets to that specific website and then acknowledge you with the value of ping that is occurring within your system and that specific website.

Example –

- As you can see in the image below. I entered “> ping youtube.com”, then my system sent and received four packets of data from YouTube to determine the minimum, maximum, and average ping values, which are 20ms, 22ms, and 21ms, respectively.



```
Command Prompt
Microsoft Windows [Version 10.0.19043.1466]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Shreeram>ping youtube.com

Pinging youtube.com [142.250.206.110] with 32 bytes of data:
Reply from 142.250.206.110: bytes=32 time=44ms TTL=115
Reply from 142.250.206.110: bytes=32 time=95ms TTL=115
Reply from 142.250.206.110: bytes=32 time=230ms TTL=115
Reply from 142.250.206.110: bytes=32 time=162ms TTL=115
```

- So, if an online game streamer has two network options, one with 10ms of ping and 10mbps internet speed, and the other with 100ms of ping and 500mbps internet speed, the gamer will obviously choose the first because he or she wants to interact with the audience in real-time. However, if a person wants to watch YouTube videos and download them, he or she will obviously select the second option in order to speed up the download process.

ipconfig (standing for "Internet Protocol configuration") is a console application program of some computer operating systems that displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings.

The ipconfig command supports the command-line switch /all. This results in more detailed information than ipconfig alone.

An important additional feature of ipconfig is to force refreshing of the DHCP IP address of the host computer to request a different IP address. This is done using two commands in sequence. First, ipconfig /release is executed to force the client to immediately give up its lease by sending the server a DHCP release notification which updates the server's status information and marks the old client's IP address as "available". Then, the command ipconfig /renew is executed to request a new IP address. Where a computer is connected to a cable or DSL modem, it may have to be plugged directly into the modem network port to bypass the router, before using ipconfig /Release and turning off the power for a period of time, to ensure that the old IP address is taken by another computer. The /flushdns parameter can be used to clear the Domain Name System (DNS) cache to ensure future requests use fresh DNS information by forcing hostnames to be resolved again from scratch.



Practical 10

Aim: Installation of Network Operating System (NOS)

Installation is the most prior to the build server. This installation includes two things, the installation of hardware and software. As a server that will serve the communication between the network, then a minimal server must have two networkcards. One for the internal network and the other for external network. Other requirements in the server installation to follow the general installation requirements Operating System, such as:

- The amount of RAM required
- Large hard disk space to be used
- The type and speed of the processor
- Resolution video / screen (required for the operating system GUI)

This information is normally supplied by the provider of the operating system is concerned. For example, for the Operating System Debian Wheezy with Desktop requires a computer device requirement such as the following.

- At least a Pentium IV processor 1 GHz
- A minimum of 128 MB RAM (512 MB is recommended)
- At least 5 GB hard drive

Operating System Installation Methods

The operating system is installed in a particular part of the disk. This particular location is usually known as a disk partition. There are a number of methods that can be used to install the operating system. The determination of these methods can be based on the condition of the hardware, the operating system's own requirements and user needs. Here are four choices of operating system installation:

1. New Installation

This option can be used when the network to be built is a new network, or the addition of new server hardware that does not support the network operating system available today. If you choose this option then all the data on the selected partition will be deleted. If there are applications that have been installed previously on the old operating system, then later needs to be reinstalled.



2. Upgrade

This option is widely used in network systems that are already running. This option is usually done because of the improvement features of the operating system used, as well as new features that are required. By selecting this option already installed applications that previously would likely still be used after the upgrade. This upgrade option will only replace the files of the previous operating system with a new one.



3. Multi-boot

If required to have more than one operating system on one computer, then this option can be selected to allow the use of more than one operating system. Later, each operating system will be placed on their respective partitions. Therefore, there needs to



4. Virtualization

Virtualization is a technique that allows the operating system installation performed on the operating system that exists today. Not in a specific partition but in a specific file. This file is a representation of a virtual computer system. One computer can have more than one virtual computer. Therefore, the installation of more than one operating system is also possible with this technique. Some applications which allow to create virtual system is VirtualBox, VMWare, and Virtual PC.



Practical 11

Aim: Create a network of at least 6 computers

Requirements:

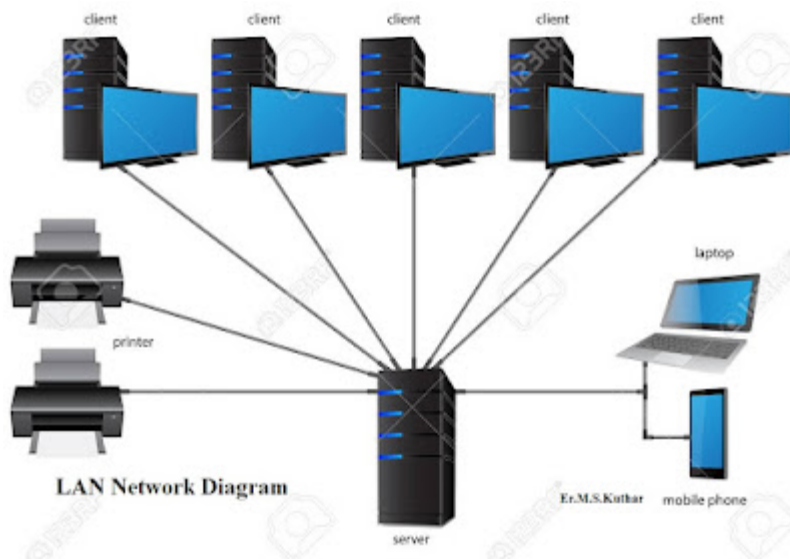
6 computers (laptops or desktops)

Ethernet cables or a switch/router with enough ports

Operating systems installed on each computer (e.g., Windows, Linux, macOS)

first of all In order to connect a computer to an Ethernet cable, the computer must have an interface. In a desktop this is usually a Network Interface Card (NIC) or USB adapter.

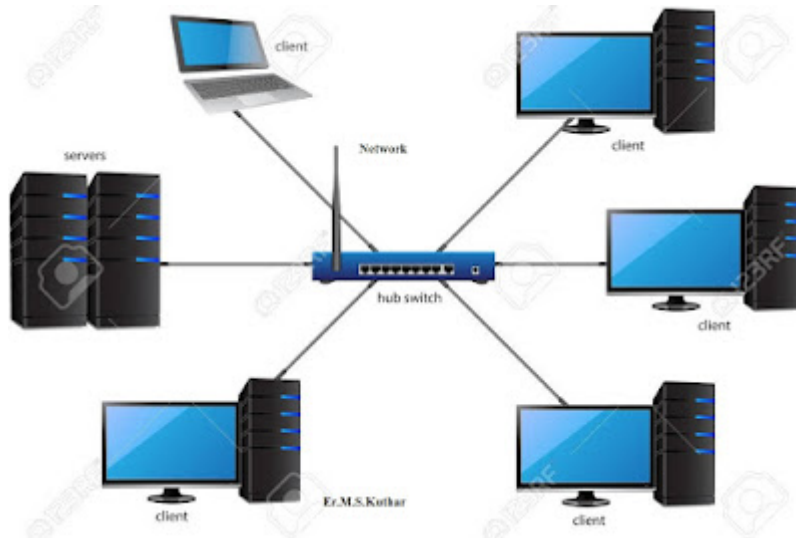
In a laptop, it is usually a PC card, a module that plugs into the laptop. The Ethernet jack may also be built into the laptop itself.



Procedure

1. Take the computer for which you are making server, insert the second LAN in that computer.
2. Connect your internet connection into the first LAN (inbuilt) on that computer.
3. Enter the IP address which you got from your ISP and check whether you can able to use internet on that system.
4. Now make sure that the second LAN is detected and is showing Unplugged.

5. Open properties of the first LAN (inbuilt LAN) and then go to "Advanced" option which is available on the top, then check both the boxes and say ok. and close everything.
 6. Now take an Internet cable which is crimped on both the sides with same colors of wires.
 7. Connect one end to the second LAN and the other end to the switch.
 8. Now open your second LAN properties and go to the TCP/IP properties and there enter IP address as (192.168.0.1) or anything you wish 9. Subnet Mask (255.255.255.0) and the gateway as (192.168.0.1).
 10. Now open click on the switch and you will get a notification on your server saying that "Local Area Connection 2" is connected.
 11. Now take an another Internet cable and one end of that cable should be in any one port of the Switch and the other should be in the second computer.
 12. Now you will get a notification that you are connected to internet, open the LAN properties and enter the IP address as (192.168.0.2) subnet mask and gateway should be same as server. say ok
 13. You will now be able to browse Internet on that particular system now.
 14. Do the same with the rest of the systems.
- And one more thing should be kept in mind that is you wont be able to browse internet Unless or Until your Server Pc is turned ON.



Set up appropriate security measures such as firewalls, antivirus software, and user authentication to protect the network from unauthorized access

Remember, this is a basic setup. For more complex networks or specific requirements like connecting different types of devices or configuring advanced settings, you might need more equipment or specific expertise.

Practical 12

AIM: Study of Layers of Network and Configuring Network Operating System

studying the layers of a network and configuring a Network Operating System (NOS) involves understanding the OSI (Open Systems Interconnection) model and practically configuring a NOS like Windows Server or Linux for networking purposes.

Understanding the OSI Model:

The OSI model consists of seven layers, each responsible for specific functions in network communication:

Physical Layer: Deals with the physical connection between devices, including cables, hubs, and switches.

Data Link Layer: Manages data frames, error detection, and MAC (Media Access Control) addressing.

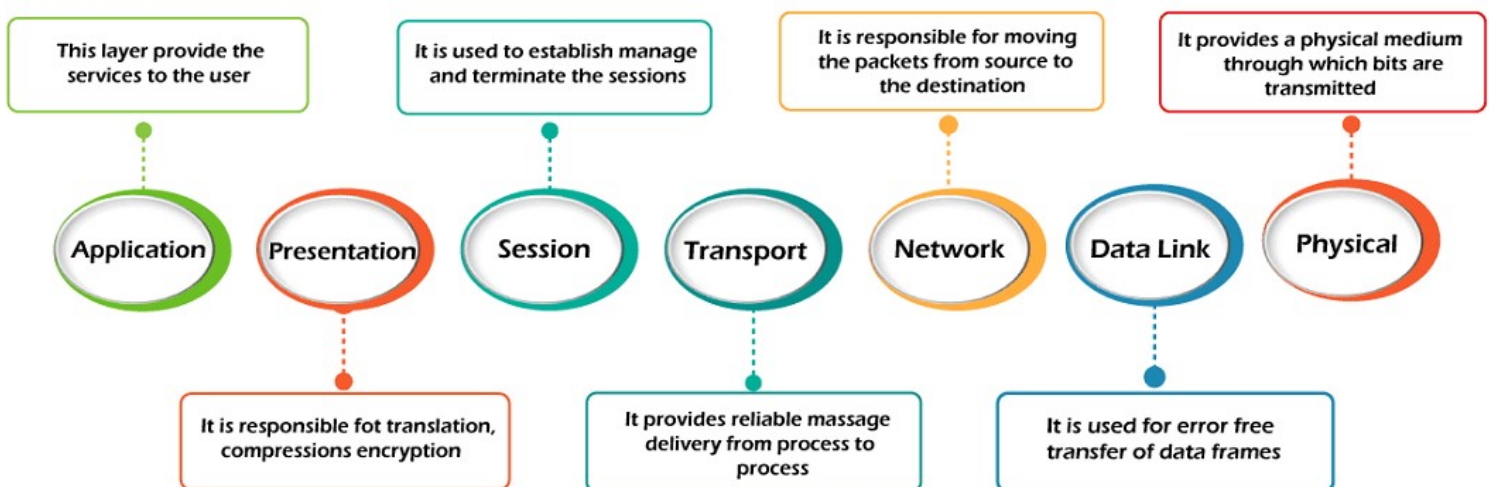
Network Layer: Focuses on logical addressing (IP addresses), routing, and packet forwarding.

Transport Layer: Manages end-to-end communication, ensures data integrity, and controls data flow.

Session Layer: Establishes, maintains, and synchronizes communication between devices.

Presentation Layer: Handles data translation, encryption, and decryption.

Application Layer: Provides network services to applications and end-users.



Configuring a Network Operating System (NOS):

Network Operating Systems:

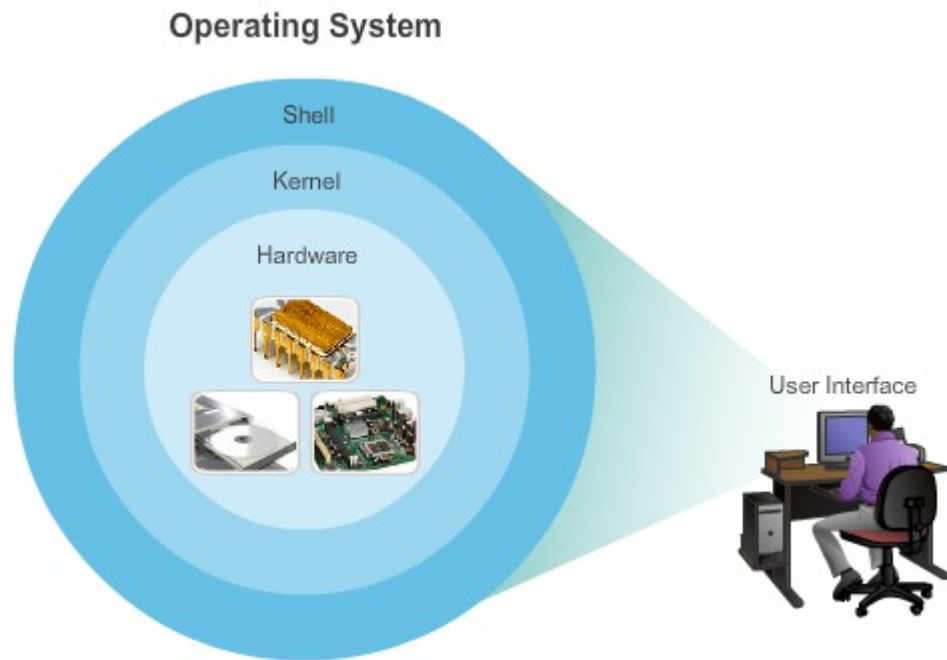
UNIX, Linux, Microsoft Windows Server 2008, Microsoft Windows Server 2003, Novell NetWare, Banyan's VINES, Artisoft's LANtastic, Mac OS X, and BSD

Let's consider configuring a Windows Server as a simple example.

Steps:

1. Installation: Install the Windows Server OS on a computer that will act as the server. Follow the installation prompts, set passwords, and configure basic settings.
2. Setting IP Addresses: Access network settings to assign a static IP address to the server. Use an address within the same subnet as other devices if you have an existing network.
3. Role Configuration: In Windows Server, roles and features determine what the server will do. You can configure it as a domain controller, file server, DHCP server, DNS server, etc. Use Server Manager to add roles and features based on your network requirements.
4. Configuration of Services:
 - DHCP Configuration: If you're setting up a DHCP server, configure the scope (range of IP addresses to assign), lease durations, and other settings for dynamic addressing.
 - DNS Configuration: Configure the DNS settings, create forward and reverse lookup zones, add DNS records for your network devices.
 - File Sharing: Set up shared folders and assign permissions to users/groups.
 - Firewall and Security Settings: Adjust the firewall settings to allow necessary network traffic and ensure security measures are in place. Configure user accounts with appropriate access permissions.

In other way A network operating system enables device hardware to function and provides an interface for users to interact. In the CCNA course of study, students learn to configure both devices that connect to the network (end devices such as PCs) and devices that connect networks together (intermediary devices like routers and switches). Learning to configure the Cisco Internetwork Operating System (Cisco IOS) on Cisco routers and switches is a large part of the Cisco CCNA program of study.



1. **Shell** – the user interface that allows users to request specific tasks from
2. the computer.
3. These requests can be made either through the CLI or GUI interfaces

Kernel – communicates between the hardware and software of a computer and manages how hardware resources are used to meet software requirements.

Hardware – the physical part of a computer including underlying electronics.

Access Methods

There are several ways to access the CLI environment and configure the device. The most common methods are:

- **Console** – A physical port of a cisco device that provides access to the device via a dedicated management channel, also known as out-of-band access
- **SSH** – A protocol to establish a remote secure CLI connection over the network.
- **Telnet** – An insecure method of remotely establishing a CLI session through a virtual interface, over a network.

Primary Command Modes

Command Mode	Description	Default Device Prompt
User Exec Mode	<ul style="list-style-type: none"> Mode allows access to only a limited number of basic monitoring commands. It is often referred to as "view-only" mode. 	Switch> Router>
Privileged EXEC Mode	<ul style="list-style-type: none"> Mode allows access to all commands and features. The user can use any monitoring commands and execute configuration and management commands. 	Switch# Router#

As a security feature, the Cisco IOS software separates management access into the following two command modes:

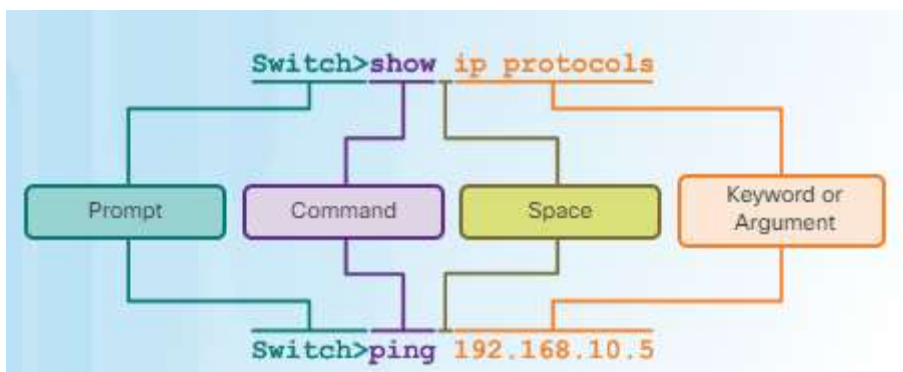
- **User EXEC Mode** – This mode has limited capabilities but is useful for basic operations. It allows only a limited number of basic monitoring commands but does not allow the execution of any commands that might change the configuration of the device. The user EXEC mode is identified by the CLI prompt that ends with the > symbol.
- **Privileged EXEC Mode** – To execute configuration commands, a network administrator must access privileged EXEC mode. Higher configuration modes, like global configuration mode, can only be reached from privileged EXEC mode. The privileged EXEC mode can be identified by the prompt ending with the # symbol.

Configuration Command Modes

Two common sub-configuration modes include:

- **Line Configuration Mode** – Used to configure console, SSH, Telnet, or AUX access.
- **Interface Configuration Mode** – Used to configure a switch port or router network interface.

Basic IOS Command Structure



- **Keyword**– a specific parameter defined in the operating system (in the figure, **ip protocols**)
- **Argument**– not predefined; a value or variable defined by the user (in the figure, **192.168.10.5**)

Device Names

Hostnames that appear in CLI prompts can be used in various authentication processes between devices, and should be used on topology diagrams. Identify network devices, hostnames should:

- Start with a letter
 - Contain no spaces
 - End with a letter or digit
- Use only letters, digits, and dashes
- Be less than 64 characters in length

Configure Hostnames

```
Switch# configure terminal
Switch(config)# hostname SW-Floor-1
SW-Floor-1(config)#
```

As shown in Figure, from the privileged EXEC mode, access the global configuration mode by entering the **configure terminal** command. Notice the change in the command prompt.

From global configuration mode, enter the command **hostname** followed by the name of the switch and press Enter. Notice the change in the command prompt name.

Note: To remove the configured hostname and return the switch to the default prompt, use the **no hostname** global config command.

Secure Device Access

The use of weak or easily guessed passwords continues to be a security issue in many facets of the business world. Network devices, including home wireless routers, should always have passwords configured to limit administrative access.

Cisco IOS can be configured to use hierarchical mode passwords to allow different access privileges to a network device.

Configure Passwords

The most important password to configure is access to the privileged EXEC mode, as shown in Figure 1. To secure privileged EXEC access, use the **enable secret password** global config command.

```
Sw-Floor-1> enable
Sw-Floor-1#
Sw-Floor-1# conf terminal
Sw-Floor-1(config)# enable secret class
Sw-Floor-1(config)# exit
Sw-Floor-1#
Sw-Floor-1# disable
Sw-Floor-1> enable
Password: ← class
Sw-Floor-1#
```

To secure the user EXEC access, the console port must be configured, as shown in Figure 2. Enter line console configuration mode using the **line console 0** global configuration command. The zero is used to represent the first (and in most cases the only) console interface. Next, specify the user EXEC mode password using the **password password** command. Finally, enable user EXEC access using the **login** command. Console access will now require a password before gaining access to the user EXEC mode.

```
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# exit
Sw-Floor-1(config)#
```

Virtual terminal (VTY) lines enable remote access to the device. To secure VTY lines used for SSH and Telnet, enter line VTY mode using the **line vty 0 15** global config command, as shown in Figure 3. Many Cisco switches support up to 16 VTY lines that are numbered 0 to 15. Next, specify the VTY password using the **password password** command. Lastly, enable VTY access using the **login** command.

```
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)#
```

Encrypt Password

The startup-config and running-config files display most passwords in plaintext. This is a security threat since anyone can see the passwords used if they have access to these files.

To encrypt passwords, use the **service password-encryption** global config command. The command applies weak encryption to all unencrypted passwords. This encryption applies only to passwords in the configuration file, not to passwords as they are sent over the network.

Use the **show running-config** command to verify that passwords are now encrypted.

Banner Messages

To create a banner message of the day on a network device, use the **banner motd # the message of the day #** global config command. The “#” in the command syntax is called the delimiting character. It is entered before and after the message. The delimiting character can be any character as long as it does not occur in the message. For this reason, symbols such as the “#” are often used. After the command is executed, the banner will be displayed on all subsequent attempts to access the device until the banner is removed.

Save the Running Configuration File

There are two system files that store the device configuration:

- **startup-config** – The file stored in Non-volatile Random Access Memory (NVRAM) that contains all of the commands that will be used by the device upon startup or reboot. NVRAM does not lose its contents when the device is powered off.
- **running-config** – The file stored in Random Access Memory (RAM) that reflects the current configuration. Modifying a running configuration affects the operation of a Cisco device. RAM is volatile memory. It loses all of its content when the device is powered off or restarted.

Practical 13

AIM: Study of Routing and Switching, configuring of Switch and Routers, Troubleshooting of Networks.

Network Switching

A switch is a dedicated piece of computer hardware that facilitates the process of switching i.e., incoming data packets and transferring them to their destination. A switch works at the Data Link layer of the OSI Model. A switch primarily hand the incoming data packets from a source computer or network and decides the appropriate port through which the data packets will reach their target computer or network.

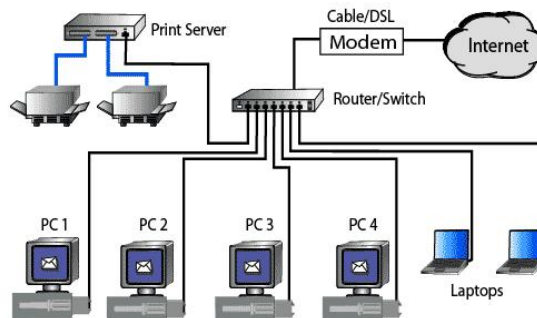
A switch decides the port through which a data packet shall pass with the help of its destination MAC(Media Access Control) Address. A switch does this effectively by maintaining a switching table, (also known as forwarding table).

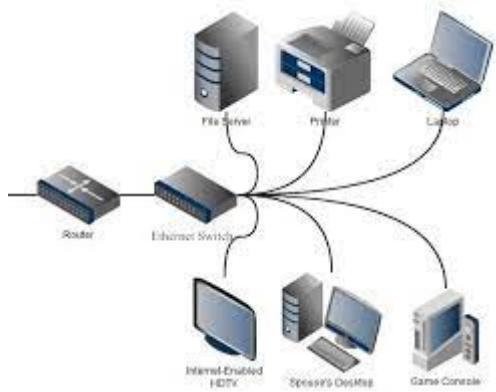
Network Switch Works:

When the source wants to send the data packet to the destination, the packet first enters the switch and the switch reads its header and finds the MAC address of the destination to identify the device then it sends the packet out through the appropriate ports that lead to the destination devices.

Switch establishes a temporary connection between the source and destination for communication and terminates the connection once the conversation is done. Also, it offers full bandwidth to network traffic going to and from a device simultaneously to reduce collision.

A network switch is more efficient than a network Hub or repeater because it maintains a switching table, which simplifies its task and reduces congestion on a network, which effectively improves the performance of the network.





Process of Switching

The switching process involves the following steps:

Frame Reception: The switch receives a data frame or packet from a computer connected to its ports.

MAC Address Extraction: The switch reads the header of the data frame and collects the destination MAC Address from it.

MAC Address Table Lookup: Once the switch has retrieved the MAC Address, it performs a lookup in its Switching table to find a port that leads to the MAC Address of the data frame.

Forwarding Decision and Switching Table Update: If the switch matches the destination MAC Address of the frame to the MAC address in its switching table, it forwards the data frame to the respective port. However, if the destination MAC Address does not exist in its forwarding table, it follows the flooding process, in which it sends the data frame to all its ports except the one it came from and records all the MAC Addresses to which the frame was delivered. This way, the switch finds the new MAC Address and updates its forwarding table.

Frame Transition: Once the destination port is found, the switch sends the data frame to that port and forwards it to its target computer/network.

switching methods:

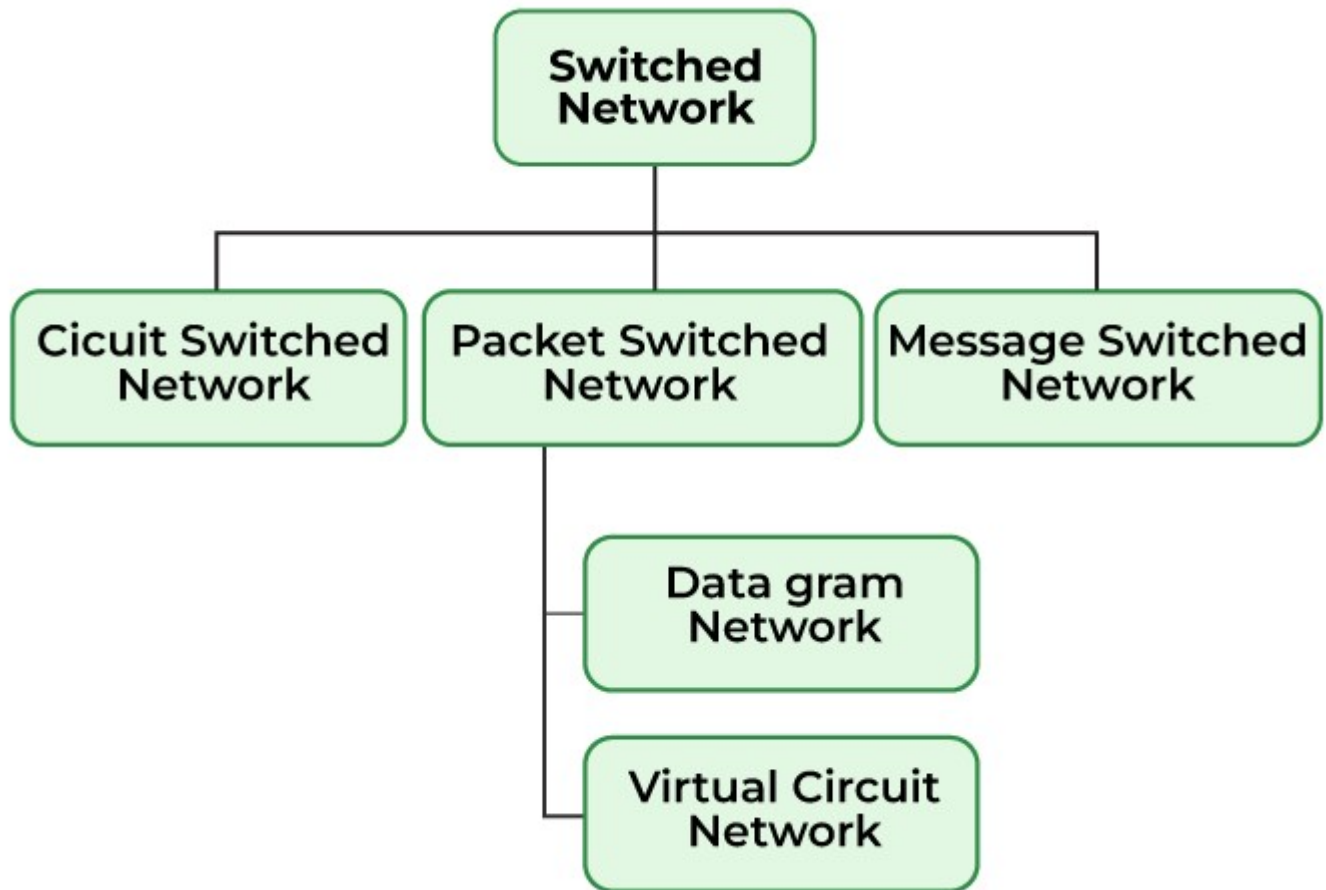
Message Switching

Circuit Switching

Packet Switching

Datagram Packet Switching

Virtual Circuit Packet Switching



Message Switching: This is an older switching technique that has become obsolete. In message switching technique, the entire data block/message is forwarded across the entire network thus, making it highly inefficient.

Circuit Switching: In this type of switching, a connection is established between the source and destination beforehand. This connection receives the complete bandwidth of the network until the data is transferred completely. This approach is better than message switching as it does not involve sending data to the entire network, instead of its destination only.

Packet Switching: This technique requires the data to be broken down into smaller components, data frames, or packets. These data frames are then transferred to their destinations according to the available resources in the network at a particular time. This switching type is used in modern computers and even the Internet. Here, each data frame contains additional information about the destination and other information required for proper transfer through network components.

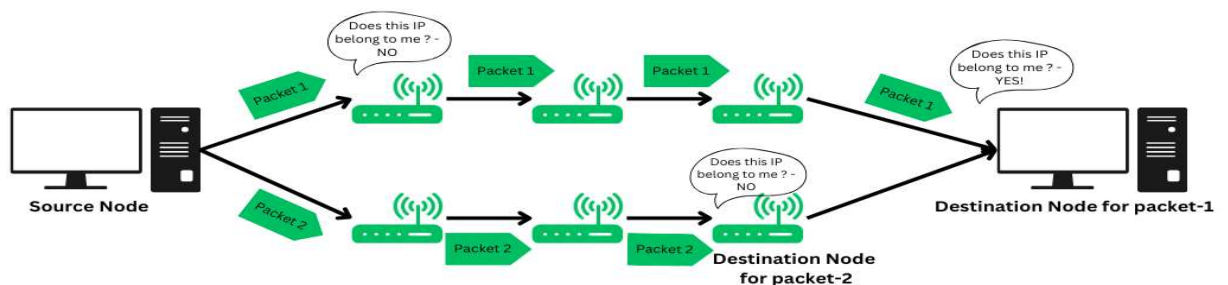
Datagram Packet Switching: In Datagram Packet switching, each data frame is taken as an individual entity and thus, they are processed separately. Here, no connection is established before data transmission occurs. Although this approach provides flexibility in data transfer, it may cause a loss of data frames or late delivery of the data frames.

Virtual-Circuit Packet Switching: In Virtual-Circuit Packet switching, a logical connection between the source and destination is made before transmitting any data. These logical connections are called virtual circuits. Each data frame follows these logical paths and provides a reliable way of transmitting data with less chance of data loss.

Routing :

Routing refers to the process of directing a data packet from one node to another. It is an autonomous process handled by the network devices to direct a data packet to its intended destination. Note that, the node here refers to a network device called – ‘Router’. Routing is a crucial mechanism that transmits data from one location to another across a network (Network type could be any like LAN, WAN, or MAN). The process of routing involves making various routing decisions to ensure reliable & efficient delivery of the data packet by finding the shortest path using various routing metrics which we will be discussing in this article.

Routing of a data packet is done by analyzing the destination IP Address of the packet. Look at the below image:



Source Node (Sender) sends the data packet on the network, embedding the IP in the header of data packet.

The nearest router receives the data packet, and based on some metrics, further routes the data packet to other routers.

Step-2 occurs recursively till the data packet reaches its intended destination.

Routing

Routing is typically of 3 types, each serving their own purpose and offering different

functionalities.

Types-of-Routing

Types of Routing

1. Static Routing

Static routing is also called as “non-adaptive routing”. In this, routing configuration is done manually by the network administrator. Let’s say for example, we have 5 different routes to transmit data from one node to another, so the network administrator will have to manually enter the routing information by assessing all the routes.

Network administrator has full control over the network, routing the data packets to their concerned destinations

Routers will route packets to the destination configured manually the network administrator.

Although this type of routing gives a fine-grained control over the routes, it may not be suitable for large scale enterprise networks.

2. Dynamic Routing

Dynamic Routing is another type of routing in which routing is an autonomous procedure without any human intervention. Packets are transmitted over a network using various shortest path algorithms and pre-determined metrics. This type of routing is majorly preferred in modern networks as it offers more flexibility and versatile functionality.

It is also known as adaptive routing.

In this, the router adds a new routes to the routing table based on any changes made in the topology of the network.

The autonomous procedure of routing helps in automating every routing operation from adding to removing a route upon updates or any changes made to the network.

3. Default Routing

Default Routing is a routing technique in which a router is configured to transmit packets to a default route that is, a gateway or next hop device if no specific path is defined or found. It is commonly used when the network has single exit point. The IP Router has the following address as the default route : 0.0.0.0/0.

Working Principle of Routing

Routing works by finding a shortest path from the source node to the destination node across a network. Here’s step-by-step working of routing:

Step1: Communication initiation

The first step that typically happens is, one node (client or server) initiates a communication across a network using HTTP protocols.

Step2: Data Packets

The source device now breaks a big chunk of information into small data packets for reliable and efficient transmission. This process is called de-assembling and encapsulating the data payload. And then each data packet is labelled with the destination node's IP address.

Step3: Routing Table

Routing table is a logical data structure used to store the IP addresses and relevant information regarding the nearest routers. The source node then looks up for the IP addresses of all the nodes that can transmit the packet to its destination and selects the shortest path using the shortest path algorithm and then routes accordingly.

Routing Table is stored in a router, a network device that determines the shortest path and routes the data packet.

Step4: Hopping procedure

In the procedure or routing, the data packet will undergo many hops across various different nodes in a network till it reaches its final destination node. Hop-count is defined as the number of nodes required to traverse through to finally reach the intended destination node. This hopping procedure has a certain criteria defined for every data packet, there's a limited number of hops a packet can take if the packet exceeds that, then its considered to be lost and it is retransmitted.

Step5: Reaching the destination node

Once all the data packets reach their intended destination node, they re-assemble and transform into complete information that was sent by the sender (source node). The receiver will perform various error checking mechanism to verify the authenticity of the data packets.

Overall, the data packet will be transmitted over least hop-count path as well as the path on which there is less traffic to prevent packet loss.

Routing-Working

Working of Routing

In the above image, we have 3 major components

Receiver

Routers

The shortest path is highlighted in red, the path with least hop-count. As we can see, there are multiple paths from source to node but if all the appropriate metrics are satisfied, the data packets will be transmitted through the shortest path (highlighted in red).

Routing Metrics and Protocols

The purpose of routing protocols is to learn about all the available paths to route data packets, build routing table and take routing decisions based on some specified metrics. There are two primary types of routing protocols rest of them ideate from these two only.

1. Distance Vector Routing

In this type of routing protocol, all the nodes that are a part of the network advertise their routing table to their adjacent nodes (nodes that are directly connected to each other) at regular intervals. With each router getting updated at regular intervals, it

may take time for all the nodes to have the same accurate network view.

Uses fixed length sub-net, not suitable for scaling.

Algorithm used: Bellman Ford Algorithm to find the shortest path.

2. Link State Routing

Link State Routing is another type of dynamic routing protocol in which routes advertise their updated routing tables only when some new updates are added. This results in effective use of bandwidth. All the routers keep exchanging the information dynamically regarding different links such as cost and hop count to find the best possible path.

Uses variable length sub-net mask, which is scalable and uses addressing more effectively.

Algorithm used: Dijkstra's Algorithm to find the shortest path.

Let's look at the metrics used to measure the cost to travel one node to another :-

1. Hop Count: Hop count refers to the number of nodes a data packet has to traverse to reach its intended destination. Transmitting from one node to another node counts as 1 – hop count. The goal is to minimize the hop count and find the shortest path.

2. Bandwidth Consumption: Bandwidth is the ability of a network to transmit data typically measured in (Kilobits per second)kbps, mbps(Megabits per second) or Gbps (Gigabits per second). The bandwidth depends on a number of factors such as – the volume of data, traffic on a network, network speed etc. Routing decision is made in a way to ensure efficient bandwidth consumption.

3. Delay: Delay is the time it takes for a data packet to travel from source node to its destination node. There are different types of delay such as – propagation delay, transmission delay, queuing delay.

4. Load: Load refers to the network traffic on a certain path in the context of routing. A data packet will be routed to the path with lesser load so that it reaches its destination in the specified time.

4. Reliability: Reliability refers to the assured delivery of the data packet to its intended destination although there are certain other factors, the data packet is routed in such a way so that it reaches its destination. The stability and availability of the link in the network is looked over before routing the data packet from a specific path.

Network Troubleshooting is a way to maintain your computer network, ensuring optimal performance, and addressing issues that may disrupt connectivity. When any problems arise, network administrators and IT professionals use tools such as Ping, Traceroute, and PathPing to identify and solve a problem.

Network Troubleshooting Tools

In addition to user reports and firsthand experience on the network, there are a number of tools available for you to use when it comes to diagnosing and treating network issues. These tools may exist in the computer's operating system itself, as standalone software applications or as hardware tools that you can use to troubleshoot a network.

Learn more about these topics in the Official CompTIA Network+ Study Guide.

Command-Line Tools

On Windows PCs, the command prompt can be accessed by searching for it in the start menu or by typing "cmd" into the Run window. On a Linux system, you can press Ctrl + Alt + T to open the command line.

The following commands can be entered into the command prompt one at a time to reveal specific information about the network status:

ping — A TCP/IP utility that transmits a datagram to another host, specified in the command. If the network is functioning properly, the receiving host returns the datagram.

tracert/traceroute — A TCP/IP utility that determines the route data takes to get to a particular destination. This tool can help you to determine where you are losing packets in the network, helping to identify problems.

nslookup — A DNS utility that displays the IP address of a hostname or vice versa.

This tool is useful for identifying problems involving DNS name resolution.

ipconfig — A Windows TCP/IP utility that verifies network settings and connections. It can tell you a host's IP address, subnet mask and default gateway, alongside other important network information.

ifconfig — A Linux or UNIX TCP/IP utility that displays the current network interface configuration and enables you to assign an IP address to a network interface. Like ipconfig on Windows, this command will tell you vital information about the network and its status.

iptables — A Linux firewall program that protects a network. You can use this tool if you suspect that your firewall may be too restrictive or too lenient.

netstat — A utility that shows the status of each active network connection. This tool is useful for finding out what services are running on a particular system.

tcpdump — A utility that is used to obtain packet information from a query string sent to the network interface. It's available for free on Linux but can be downloaded as a command for Windows.

pathping — A TCP/IP command that provides information about latency and packet loss on a network. It can help you troubleshoot issues related to network packet loss.

nmap — A utility that can scan the entire network for various ports and the services that are running on them. You can use it to monitor remote network connections and get specific information about the network.

route — A command that enables manual updating of the routing table. It can be used to troubleshoot static routing problems in a network.

arp — A utility that supports the Address Resolution Protocol (ARP) service of the TCP/IP protocol suite. It lets the network admin view the ARP cache and add or

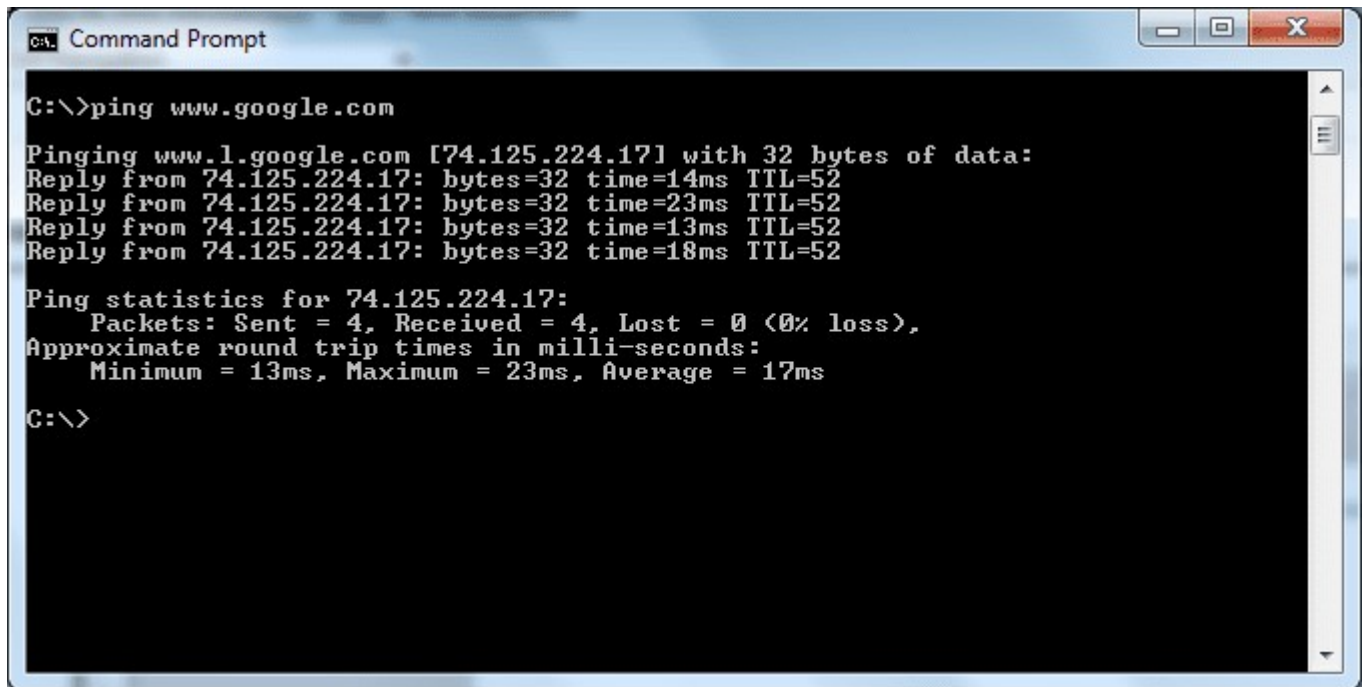
delete cache entries. It can be used to address problems having to do with specific connections between a workstation and a host.

dig — A Linux or UNIX command-line tool that will display name server information. It can be used to troubleshoot problems in DNS name resolution.

Ping is a command that sends a small packet of data to any network device and waits for its response. Traceroute traces the route from source to destination and it helps identify any delay or bottleneck. PathPing combines the functionality of both Ping and Traceroute commands to troubleshoot the network. In this article, we will learn about Ping, Traceroute, and PathPing tools, and how to use them to troubleshoot the network.

Ping

A Ping stands for Packet Internet Groper. It is a widely used command for identifying connectivity between two network connections. It uses Internet Control Message Protocol (ICMP) to send a request to the target host and wait for a response. It measures the round-trip time for data packets to travel from the source to the destination and back



```
C:\>ping www.google.com

Pinging www.l.google.com [74.125.224.17] with 32 bytes of data:
Reply from 74.125.224.17: bytes=32 time=14ms TTL=52
Reply from 74.125.224.17: bytes=32 time=23ms TTL=52
Reply from 74.125.224.17: bytes=32 time=13ms TTL=52
Reply from 74.125.224.17: bytes=32 time=18ms TTL=52

Ping statistics for 74.125.224.17:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 13ms, Maximum = 23ms, Average = 17ms

C:\>
```

Explanation

It shows that we have sent 4 request (packet) and received acknowledgment of all the requests and there is Zero loss. and It shows a minimum, maximum and average round trip time in milliseconds.

Traceroute

Traceroute is also called as a tracert. It traces the route from source to the destination. It is achieved by using ICMP to send a request. It reveals the all routers between source and destination by displaying their IP Address to detect where the packet loss or latency occurs.


```

C:\Users\Admin>tracert google.com

Tracing route to google.com [216.58.196.206]
over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    192.168.1.100
  1  12 ms     8 ms     5 ms     103.62.239.241
  2  *         4 ms     7 ms     172.22.22.37
  3  6 ms      7 ms     4 ms     172.22.22.1
  4  12 ms     12 ms    20 ms    45.120.248.10
  5  9 ms      5 ms     8 ms     108.170.251.113
  6  13 ms     12 ms    22 ms    216.239.56.253
  7  3 ms      3 ms     3 ms     del03s06-in-f14.1e100.net [216.58.196.206]

Trace complete.

C:\Users\Admin>

```

Explanation

Each line shows a route with round-trip time. The first line shows a router has 216.58.196.206 address and round-trip time is 1ms. and the second line has a timeout. This means that the router at hop 3 did not respond to the ICMP request within the time limit.

PathPing

PathPing command is a combination of ping and tracert command. It sends request to each router that comes between source and destination and compute result based on response from each router. It provides continuous monitoring of the network path which allows network administrator to observe changes in performance.

```
C:\WINDOWS\system32\cmd.exe
C:\Users\rmens>pathping 172.16.0.254

Tracing route to 172.16.0.254 over a maximum of 30 hops

  0  lab-book01.lazyadmin.local [192.168.1.19]
  1  192.168.1.1
  2  172.16.0.254

Computing statistics for 50 seconds...

Hop  RTT      Source to Here   This Node/Link   Address
     Lost/Sent = Pct Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                lab-book01.lazyadmin.local [192.168.1.19]
     |
  1   1ms      0/ 100 = 0%      0/ 100 = 0%      192.168.1.1
     |
  2   1ms      0/ 100 = 0%      0/ 100 = 0%      172.16.0.254

Trace complete.
```

Explanation

It shows Hop 0, Hop 1 , Hop 2 is a source with no packet loss, with round-time

Network Troubleshooting Applications

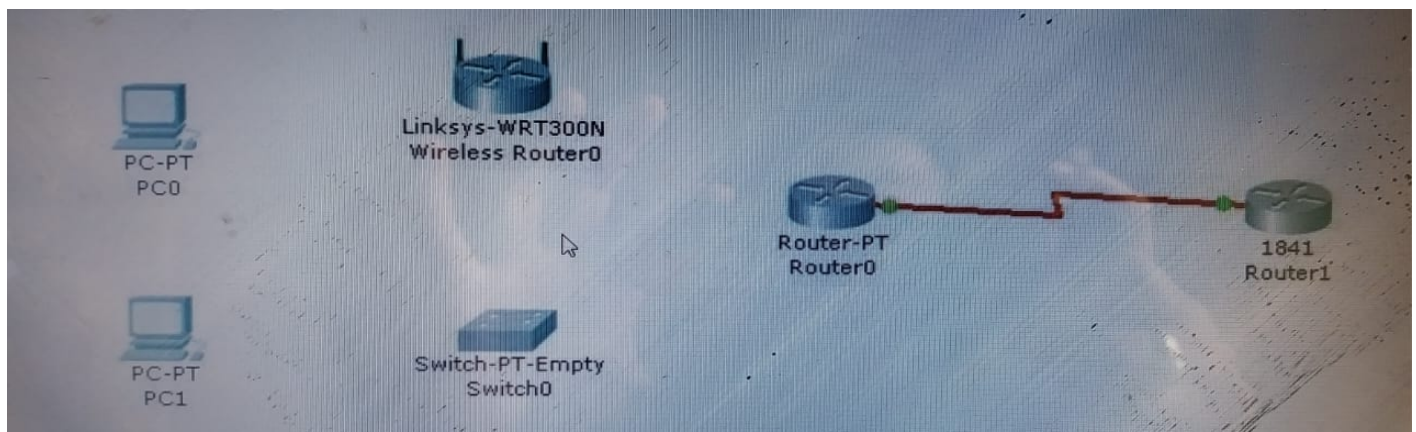
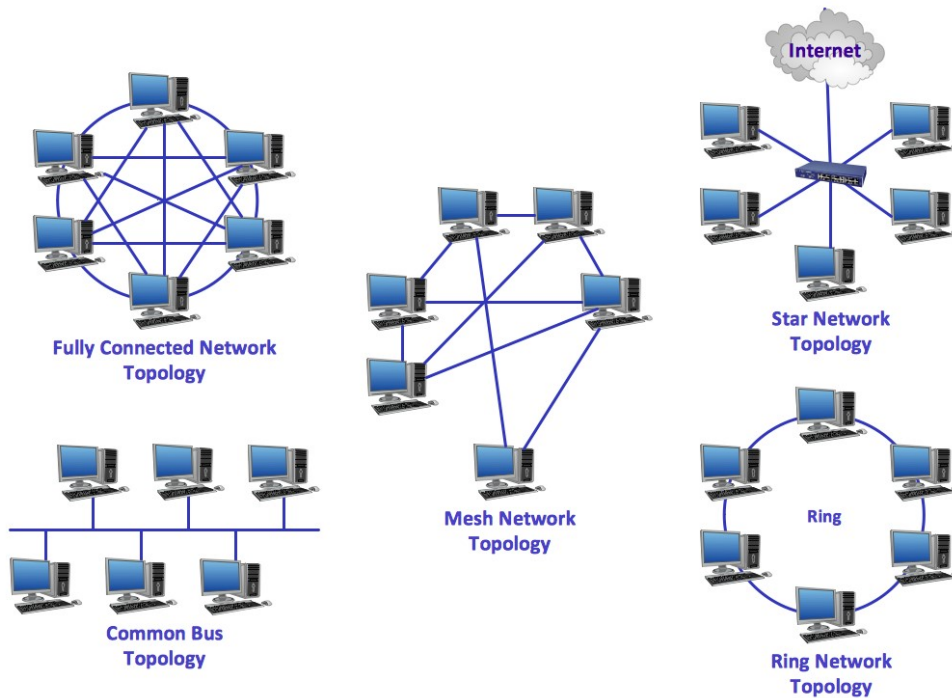
In addition to command-line tools, there are also a number of standalone applications that can be used to determine the status of a network and to troubleshoot issues. Some of these applications may be included in the system that you are working with, while others may need to be installed separately.

- **Packet Sniffer** — Provides a comprehensive view of a given network. You can use this application to analyze traffic on the network, figure out which ports are open and identify network vulnerabilities.
- **Port Scanner** — Looks for open ports on the target device and gathers information, including whether the port is open or closed, what services are running on a given port and information about the operating system on that machine. This application can be used to figure out which ports are in use and identify points in a network that could be vulnerable to outside attacks.
- **Protocol Analyzer** — Integrates diagnostic and reporting capabilities to provide a comprehensive view of an organization's network. You can use analyzers to troubleshoot network problems and detect intrusions into your network.
- **Wi-Fi Analyzer** — Detects devices and points of interference in a Wi-Fi signal. This tool can help you to troubleshoot issues in network connectivity over a wireless network.
- **Bandwidth Speed Tester** — Tests the bandwidth and latency of a user's internet connection. This application is typically accessed through a third-party website and can be used to confirm user reports about slow connections or download speeds

Experiment-14

AIM :Study of scaling of networks ,design verities of LAN and forward of traffic
Apparatus (Software): Command Prompt And Packet Tracer.

Topology Diagram



Objectives

- Determine the cable types to use to connect all devices to the switch.
- Add appropriate modules to switches and routers.

- Connect the devices to the switch using the appropriate cable types.

Background / Preparation

The results of a site survey for an ISP customer indicate that the customer needs to upgrade the LAN to include a new standalone switch. The network has an existing router (Router0) and a Linksys 300N router. It is necessary to determine which interfaces are needed on the new switch to provide connectivity to the router, the Linksys device, and the customer PCs. The customer wants to use copper cabling. Note: Links created with the switch may take a minute to change from amber to green. Switch between Simulation mode and Realtime mode to speed up this process.

Step 1: Determine the required connectivity options.

a. Click Router0. Using the information in the Physical Device View window on the Physical tab, determine what type of interface is available on the router to connect to the new switch.

Hint: Place the mouse pointer on the interface to display the interface type. Click on the interface type to display a description of the interface.

Which interface is available on the router to connect to the new switch? What type of cable is required?

Click the Linksys 300N. Using the picture on the Physical tab, determine what type of cable is necessary to connect to the new switch.

Which interface is available on the Linksys 300N to connect to the new switch? What type of cable is required?

Step 2: Configure the new switch with the required options.

a. Click Switch0.

On the Physical tab, explore each switch module available under the Modules option. Choose the appropriate interfaces to connect to Router0 and the Linksys 300N router. Choose the appropriate interfaces to connect to the existing PCs.

Power down the switch using the power button in the Physical Device View window on the Physical tab.

Choose the appropriate modules for the switch. Add the four necessary interfaces to

the switch.

Power up the switch using the power button shown in the Physical Device View window on the Physical tab.

Click the Config tab. Select each interface and ensure that the On box is checked.

Step 3: Connect the router to the switch.

a. Using the appropriate cable, connect the router port to the first available switch port. Click the Config

tab on the router. Select the interface and ensure that the On box is checked.

b. Verify connectivity. A green light appears on each end of the link if the cabling is correct.

Step 4: Connect the Linksys 300N to the switch.

a. Using the appropriate cable, connect the Linksys 300N to the second available port on the newswitch.

Verify connectivity. A green light appears on each end of the link if the cabling is correct.

Step 5: Connect the PCs to the switch.

a. Using the appropriate cable, connect the existing PCs to the new switch.

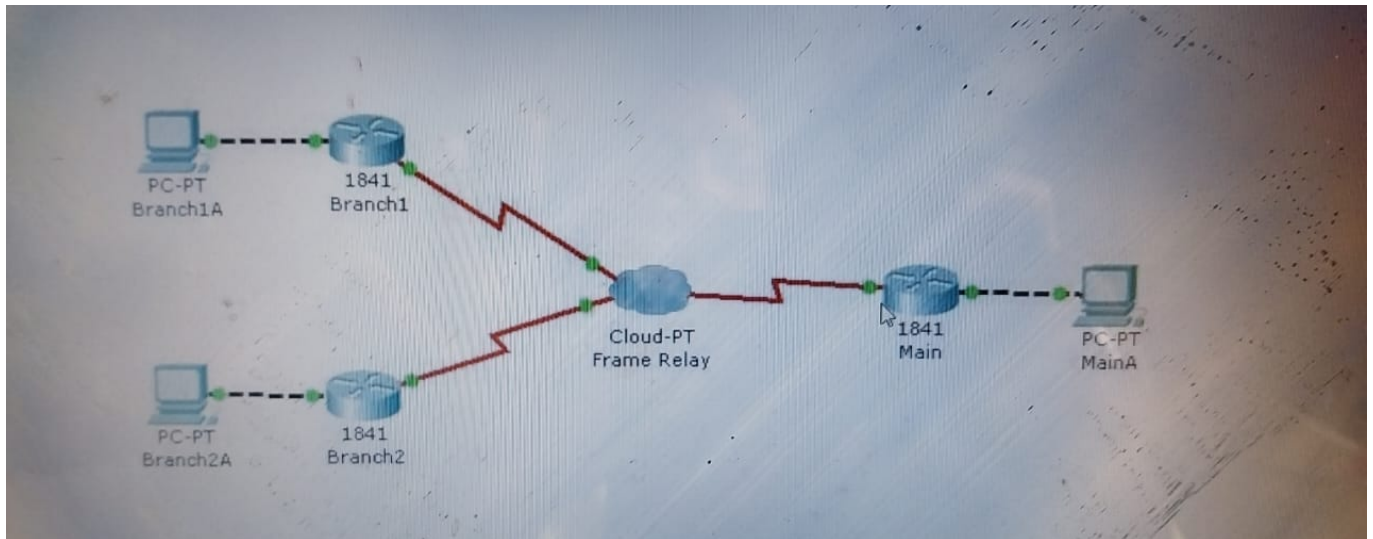
b. Verify connectivity. A green light appears on each end of the links if the cabling is correct.

c. Click the Check Results button at the bottom of this instruction window to check your work

Practical 15

Aim of experiment: Study WAN concepts and Configure and forward Traffic in WAN

Apparatus (Software): Command Prompt And Packet Tracer.



Objective

The show commands are very powerful commands for troubleshooting and monitoring networks. They

give a static image of the network at a given time. The use of a variety of show commands will give a

clear picture of how the networking is communicating and transferring data.

Background / Preparation

The physical topology of the network has been designed using Frame Relay. To test the network

connectivity, use a variety of show commands.

Required file: Examining WAN Connections.pka

Step 1: Examine the configuration of Branch1 and Branch2.

a. Click on Branch1 and use various show commands to view the connectivity to the network.

b. Use the show running-configuration command to view the router configuration.

c. Use the show ip interface brief command to view the status of the interfaces.

d. Use the various show frame-relay map, show frame-relay pvc, and show frame-relay lmi

commands to see the status of the Frame-relay circuit.

e. Click on Branch 2 and use various show commands to view the connectivity to the network.

f. Use the show running-configuration command to view the router configuration.

g. Use the show ip interface brief command to view the status of the interfaces.

h. Use the various show frame-relay map, show frame-relay pvc, and show frame-relay lmi

commands to see the status of the Frame-relay circuit.

Step 2: Examine the configuration of Main.

a. Click on Main and use a variety of show commands to view the connectivity to the network.

b. Use the show running-configuration command to view the router configuration.

c. Use the show ip interface brief command to view the status of the interfaces.

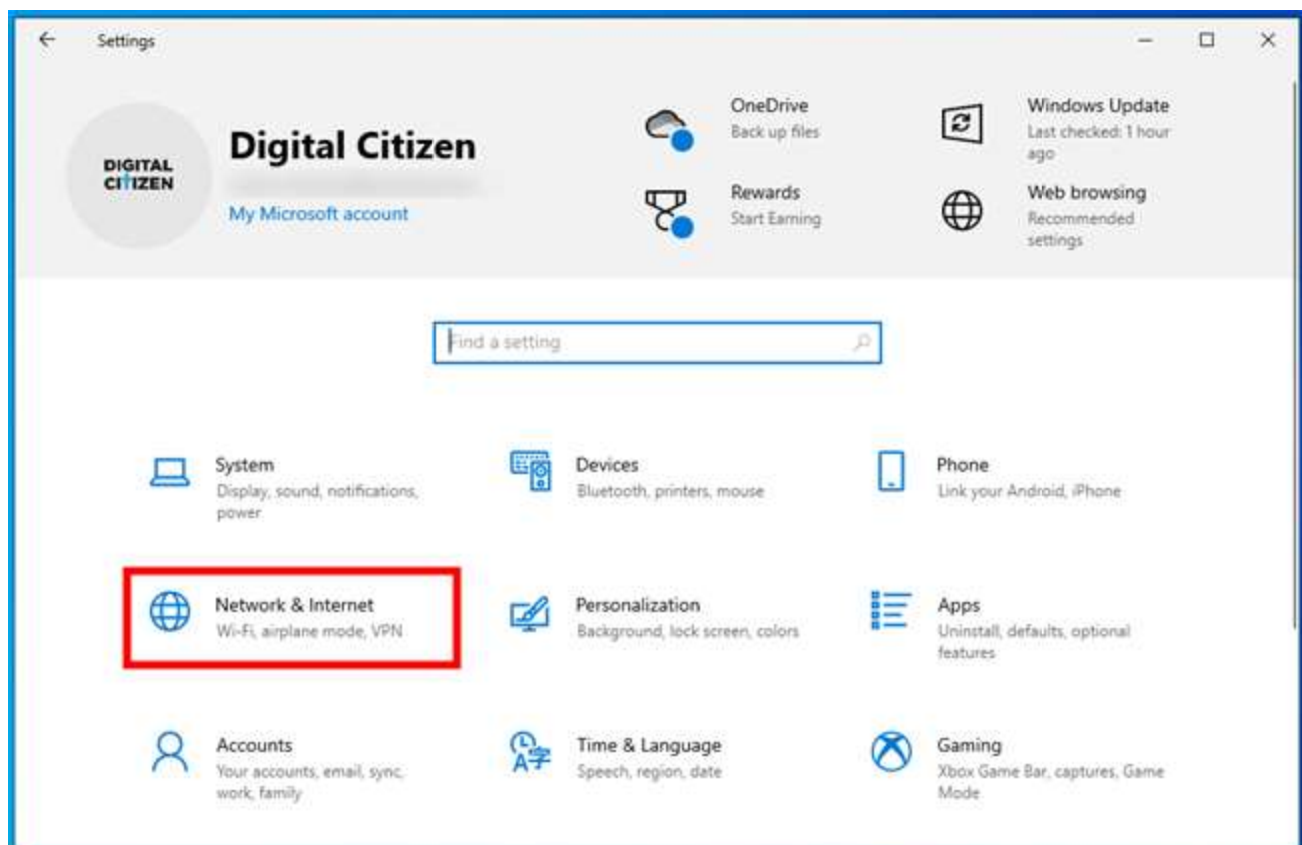
d. To view the status of the frame-relay configurations use the show frame-relay lmi, show framelay map, and show frame-relay pvc commands

Practical 16

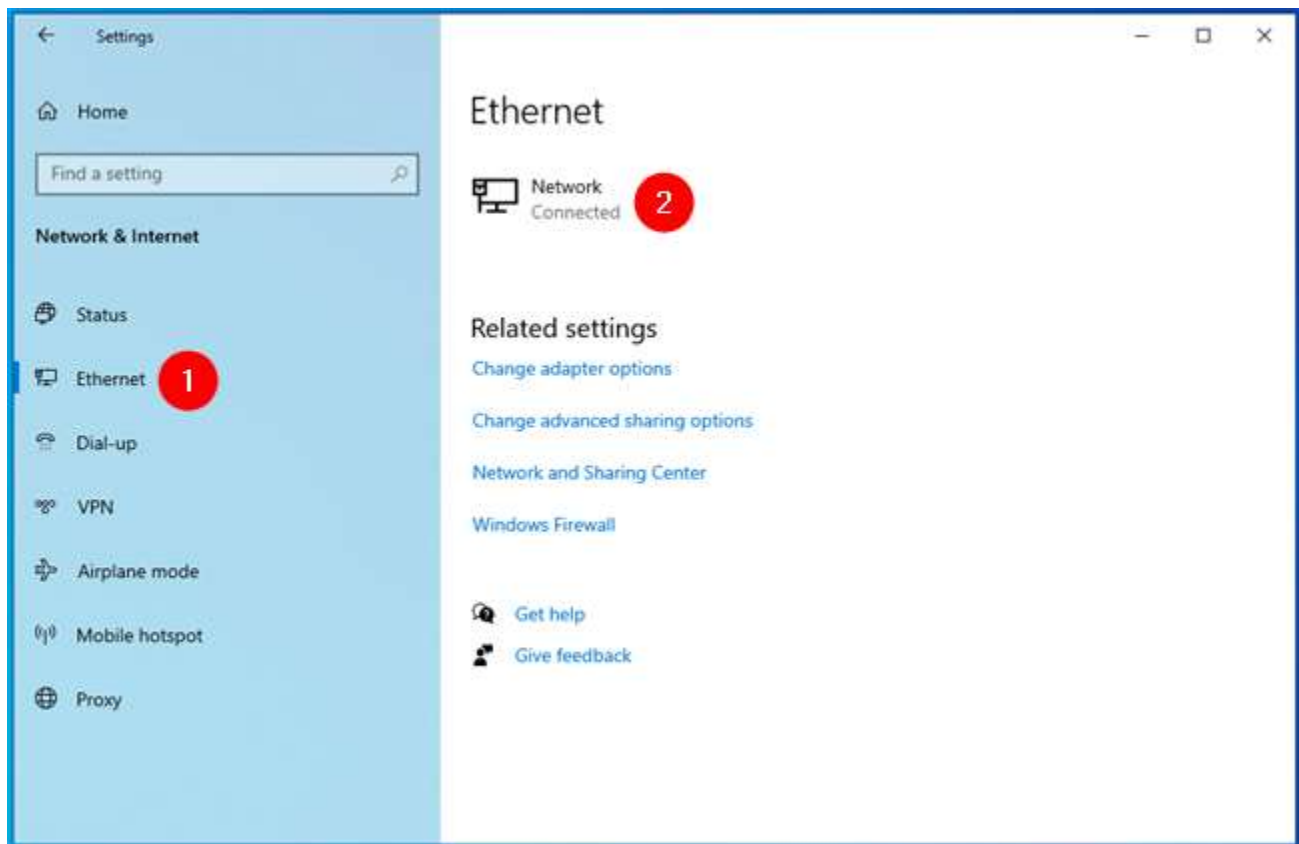
AIM: Configure IPv4 and IPv6 and learn Quality, security and other services

Configure IPv4 and IPv6 (win 10& 11)

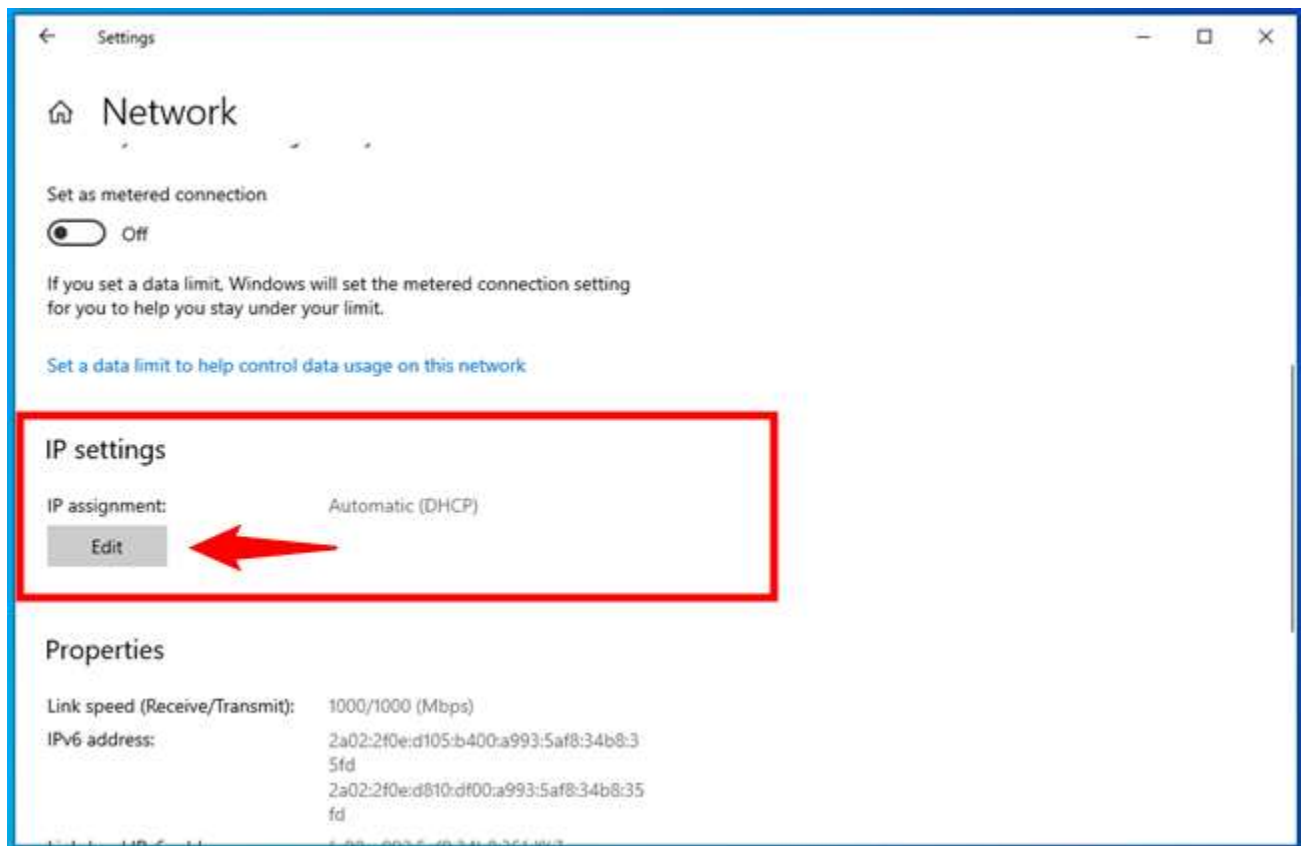
First, open the Settings app: a quick way to do that is to push the Settings button from the Start Menu or to press Windows + I on your keyboard simultaneously. In the Settings app, open the Network & Internet category.



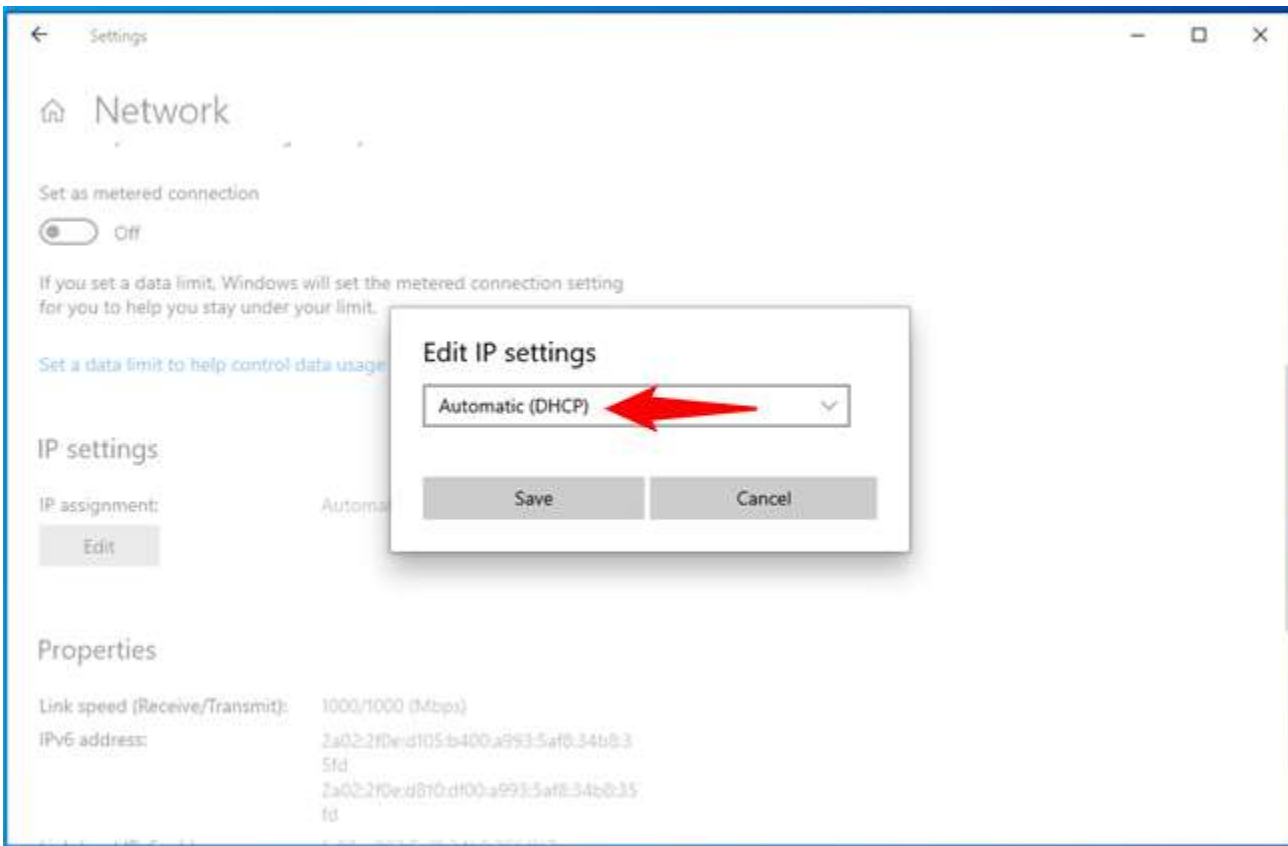
On the left sidebar, select your network type. If you're using a wireless card, click or tap on Wi-Fi. If you're using a wired connection, go to Ethernet. On the right side of the window, click or tap on the name of your network connection.



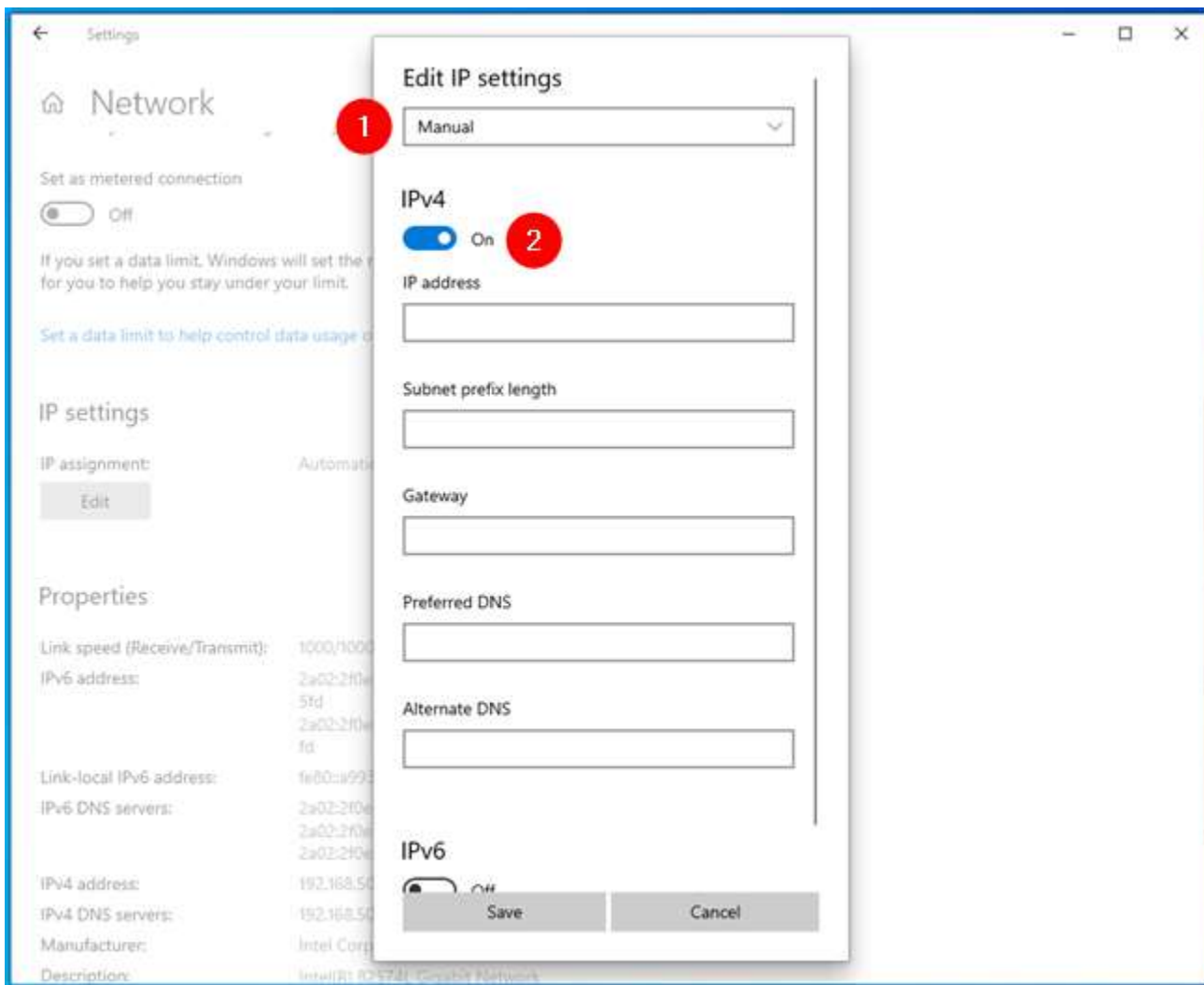
Scroll down on your network connection details page until you find the section called IP settings. Then, click or tap on Edit, under IP assignment.



The Settings app now shows the “Edit IP settings” dialog. This is where you can change the IP address of your computer or device. If you want the IP address of your Windows 10 PC to be assigned automatically by your router, select Automatic (DHCP). This is also called a dynamic IP address.

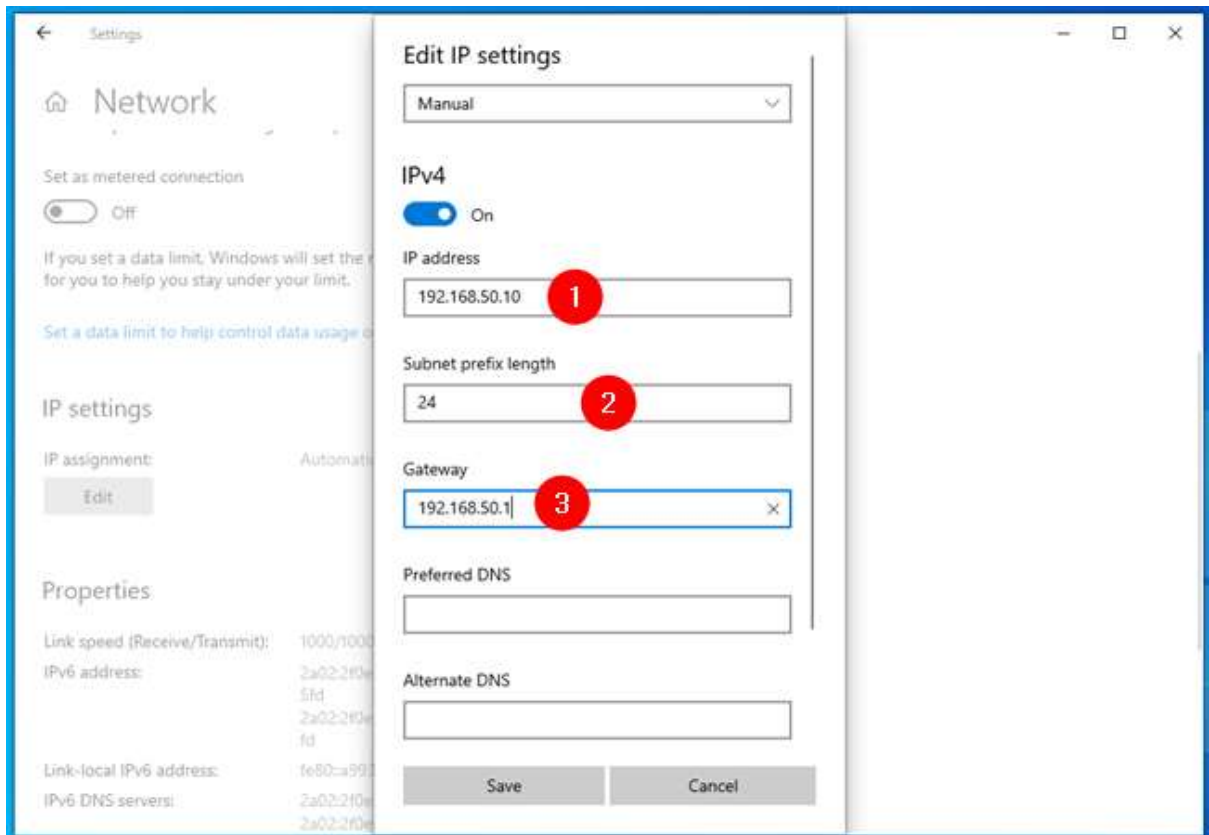


If you want to set your own static IP address, select Manual and then enable the IPv4 and/or IPv6 switches, depending on what internet protocols you want to use. Note that each of them has its own distinct IP address, so you must enter the required details for both IPv4 and IPv6 if you choose to enable both.



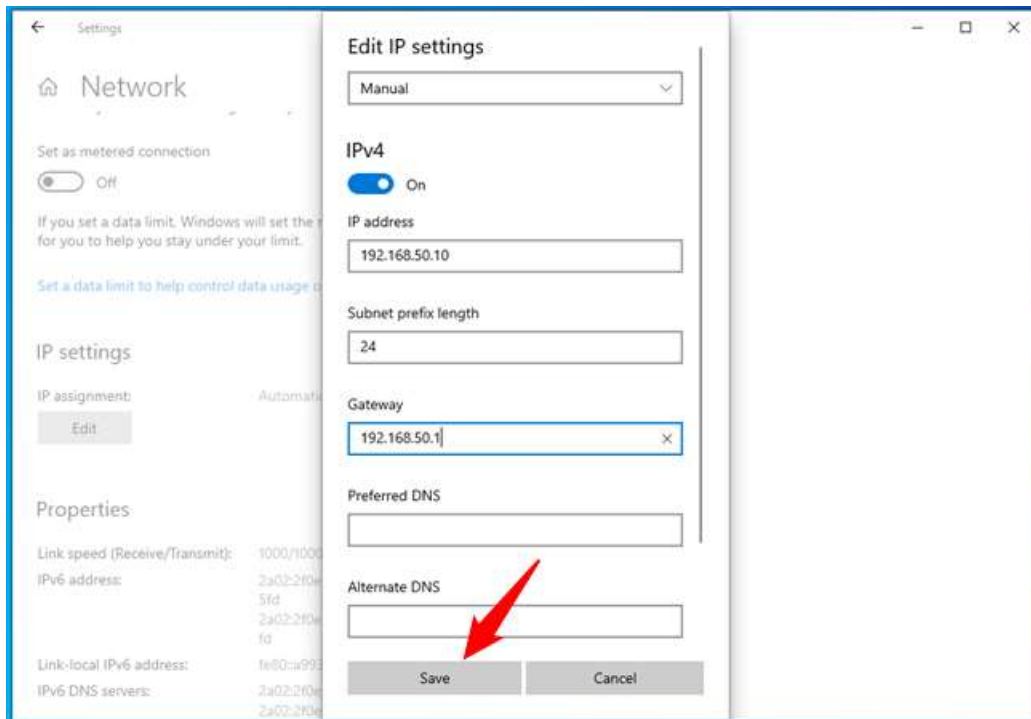
To change your IP address to a static one, regardless of whether you set it for your *IPv4* or *IPv6* protocols, you have to enter the following details:

- **IP address:** Type the static IP address that you want to use. For example, I want to change the IP address (IPv4) of my Windows 10 PC to 192.168.50.10.
- **Subnet prefix length:** Type the prefix length that determines the size of the subnet. For example, I configured my router to use a subnet mask of 255.255.255.0, which means that I have to enter a “*Subnet prefix length*” of 24 (the number of 1 bits in the netmask). If I had a subnet mask of 255.255.0.0, the prefix length would have been 16, and so on.
- **Gateway:** Type the IP address of your router. In my case, that’s 192.168.50.1.



The Preferred DNS and Alternate DNS settings are not mandatory - if you leave them blank, they are automatically assigned by your router. However, if you want to change them too, you can do so. TIP: Here are more ways to change DNS settings in Windows.

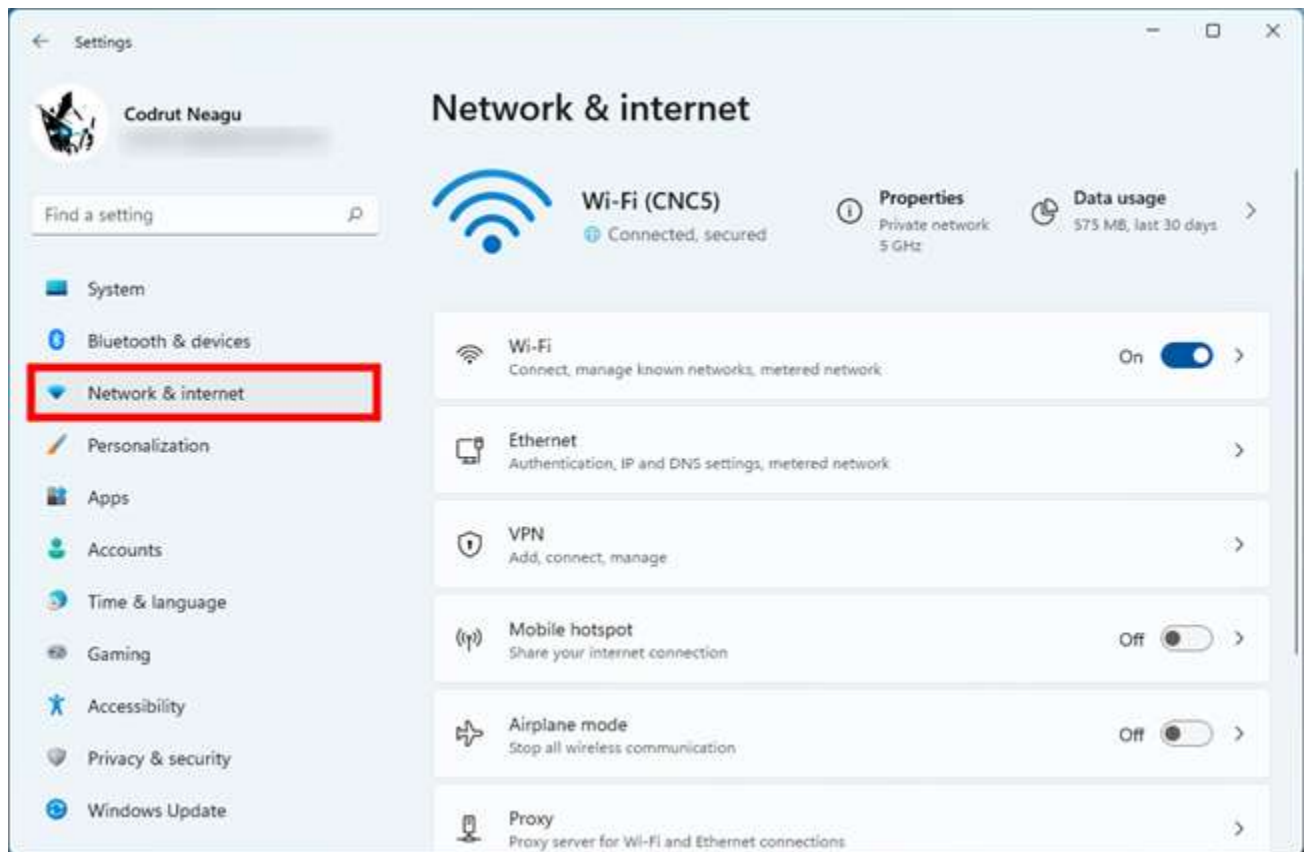
Once you've entered all the details, click or tap on Save, and Windows 10 changes your IP address.



IMPORTANT: If you choose to use a static IP address, ensure all the details you enter are correct; otherwise, your Windows 10 PC loses internet connectivity. If that happens, change your IP address back to *Automatic (DHCP)* so that your router can change it to something that works.

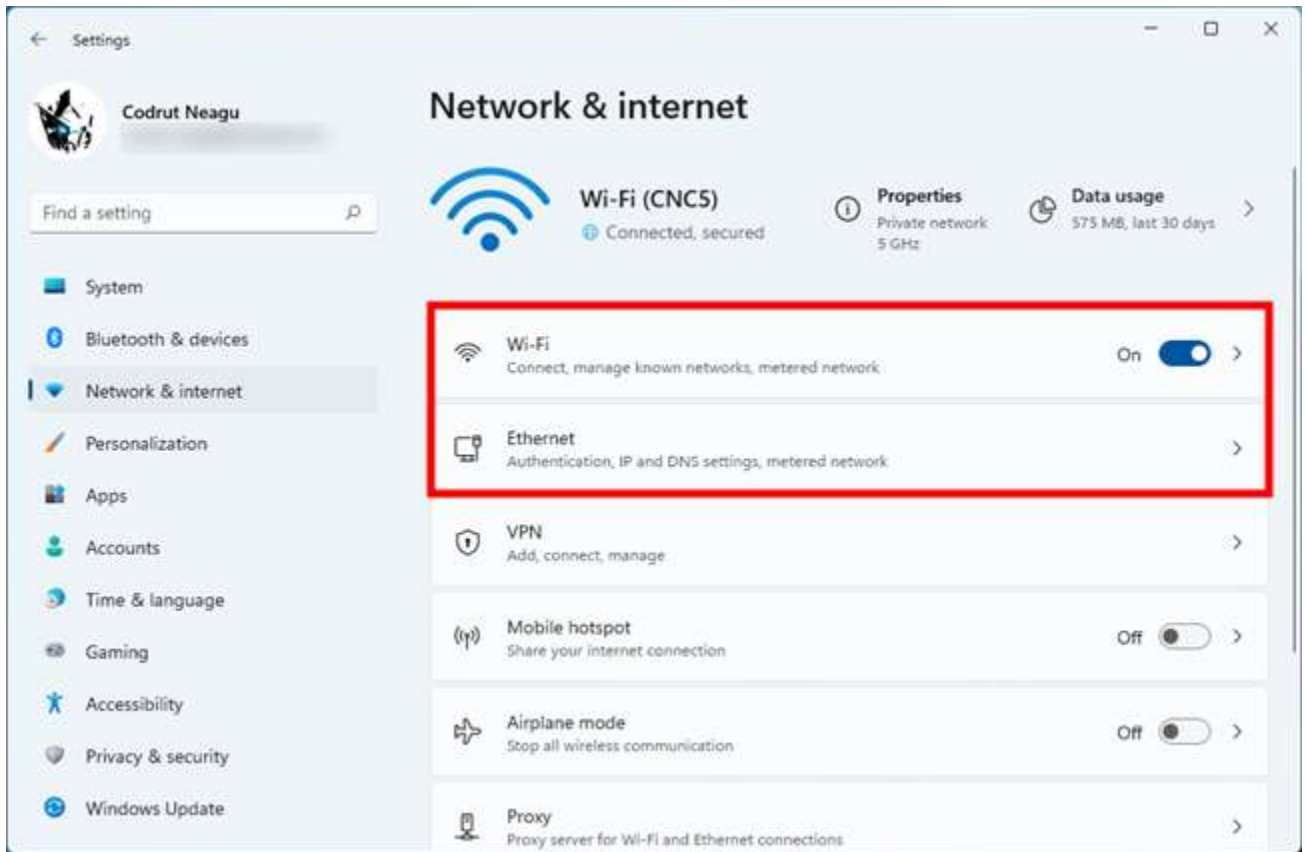
Win 11:

Open the Settings app: a quick way to do that is to use its Pinned shortcut from the Start Menu or press Windows + I on your keyboard. Once you've opened it, select Network & internet on the left sidebar.



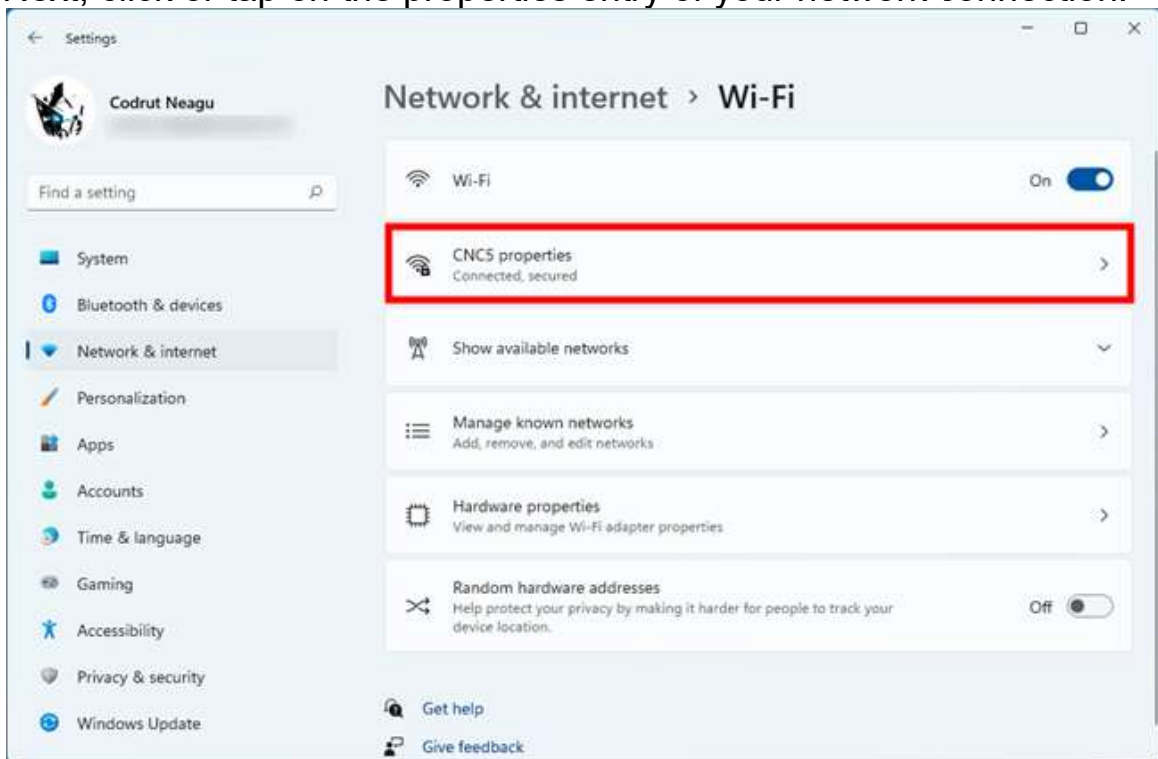
The Network & internet settings in Windows 11

On the right, click or tap on the type of network you're currently using. If you connect to the internet (or local area network) using a wireless card, select Wi-Fi. If you're accessing the internet (or LAN) using a wired connection, click or tap on Ethernet.



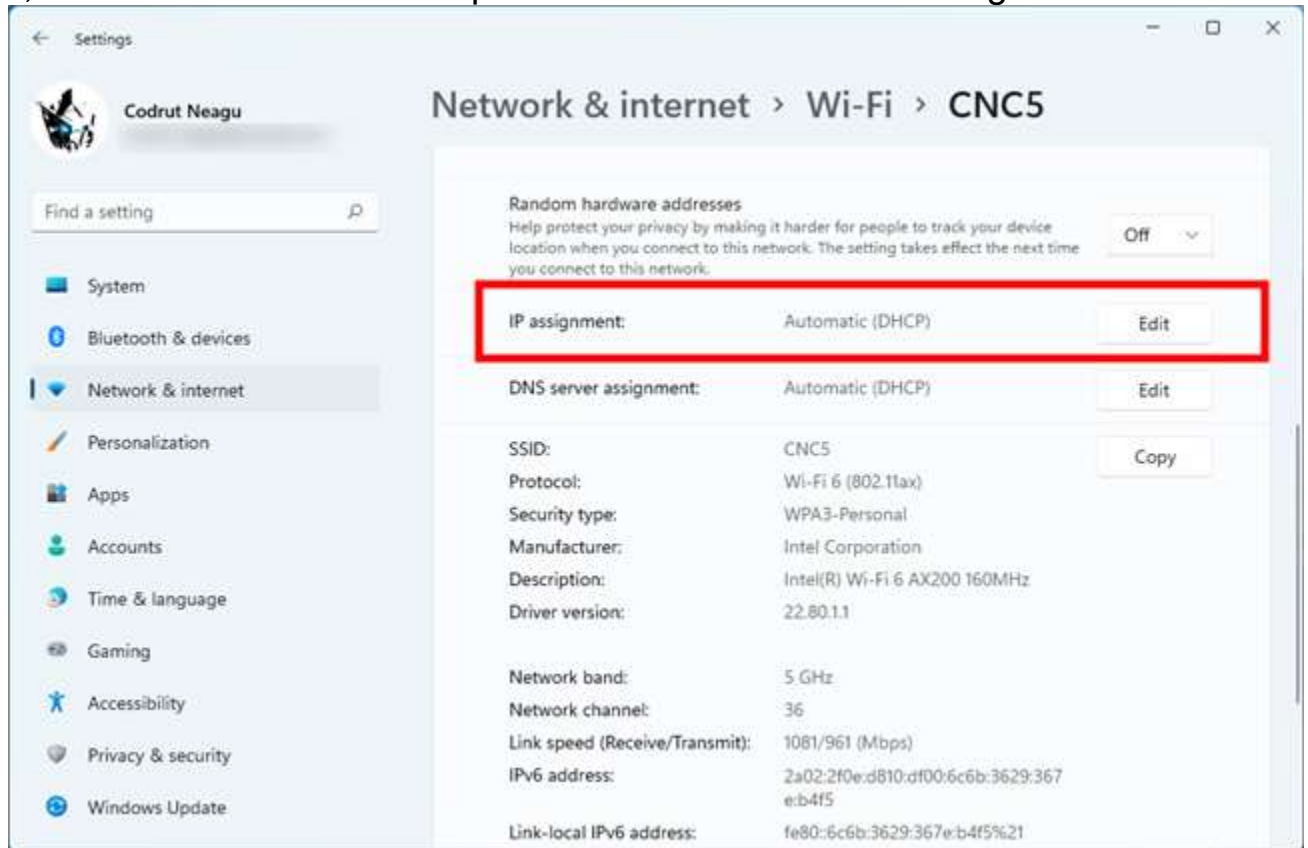
Wi-Fi or Ethernet network connection

Next, click or tap on the properties entry of your network connection.



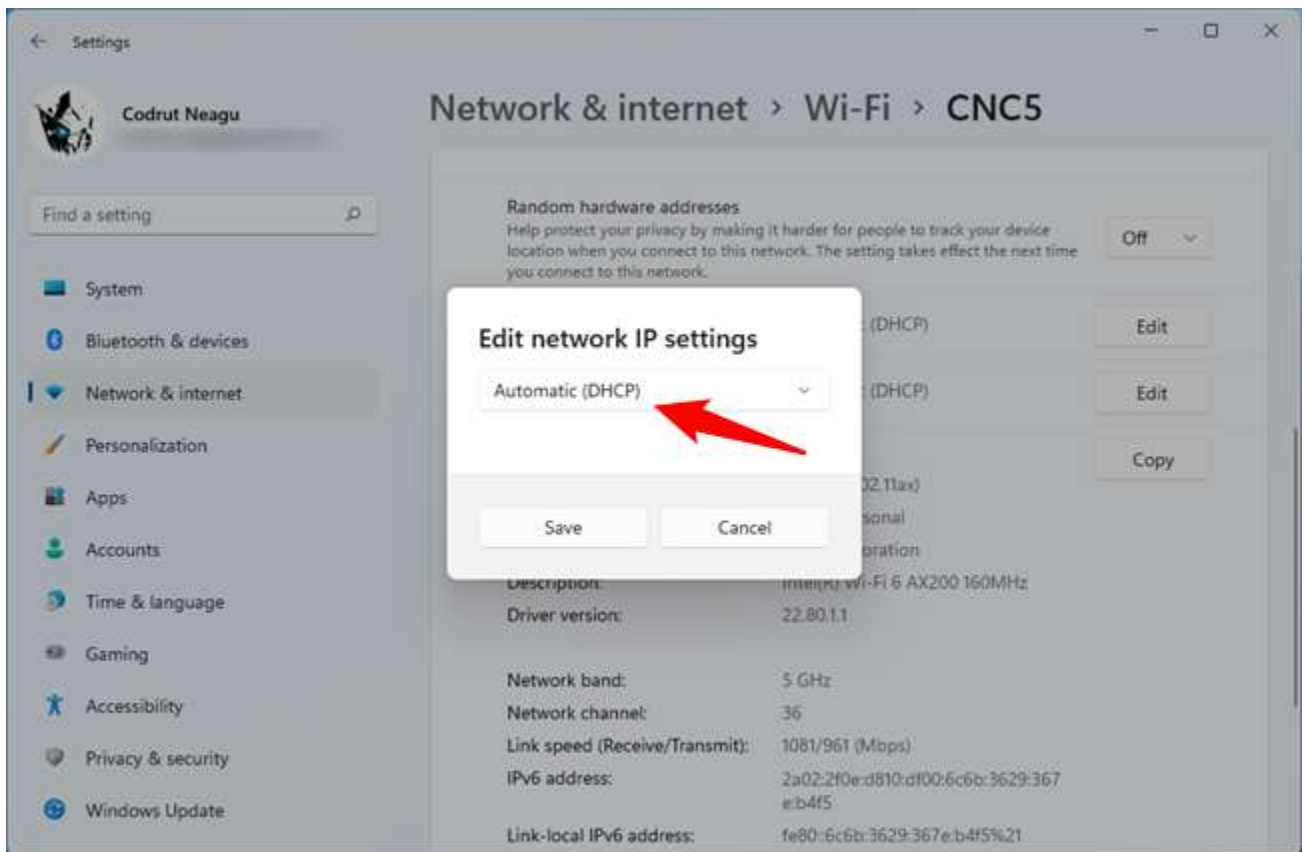
The network's properties

This opens a page filled with details about the selected network connection. On it, scroll down and click or tap the Edit button next to IP assignment.



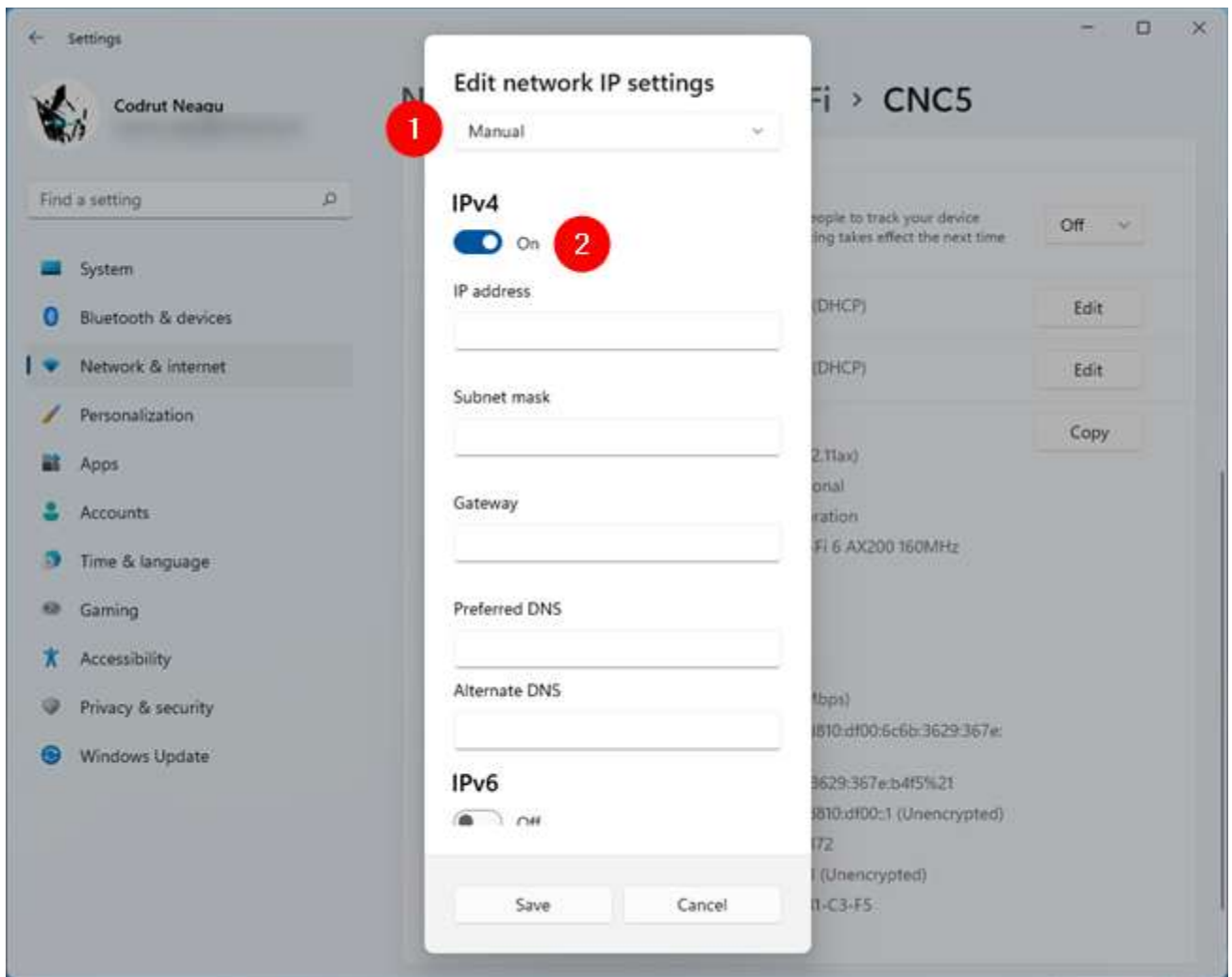
The Edit button next to IP assignment

As a result, the Settings app loads a dialog called “Edit network IP settings,” where you can set the IP address of your Windows 11 PC. If you want to use a dynamic IP address assigned automatically by the router, choose Automatic (DHCP).



Let Windows 11 get an IP address automatically via DHCP

If you want to set a static IP address for your Windows 11 computer, select Manual. Then, turn on the IPv4 and/or IPv6 switches, depending on the internet protocols you intend to use. Keep in mind that each one needs a distinct IP address, so you'll have to specify details for both IPv4 and IPv6 if you decide to enable both.



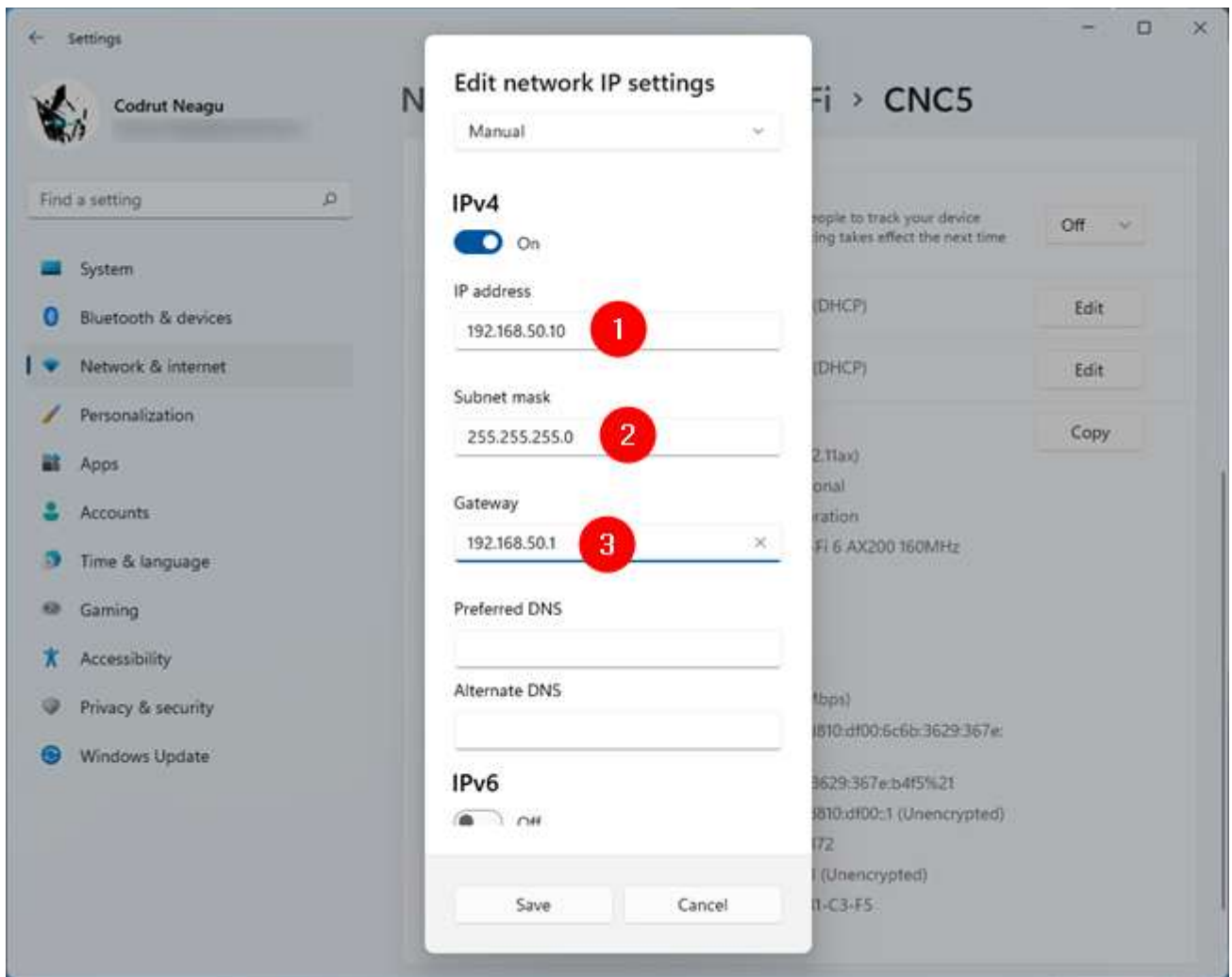
Edit IP settings to change the IPv4 address in Windows 11

In order to set a static IP address for either IPv4 or IPv6, you have to provide the next details:

IP address: Enter the static IP address you want to use. For instance, I'm changing the IP address (IPv4) of my Windows 11 computer to 192.168.50.10.

Subnet mask: Type the subnet mask used by your network. For example, I've configured my mesh Wi-Fi to use a 255.255.255.0 subnet mask, which means that this is the number sequence I need to enter.

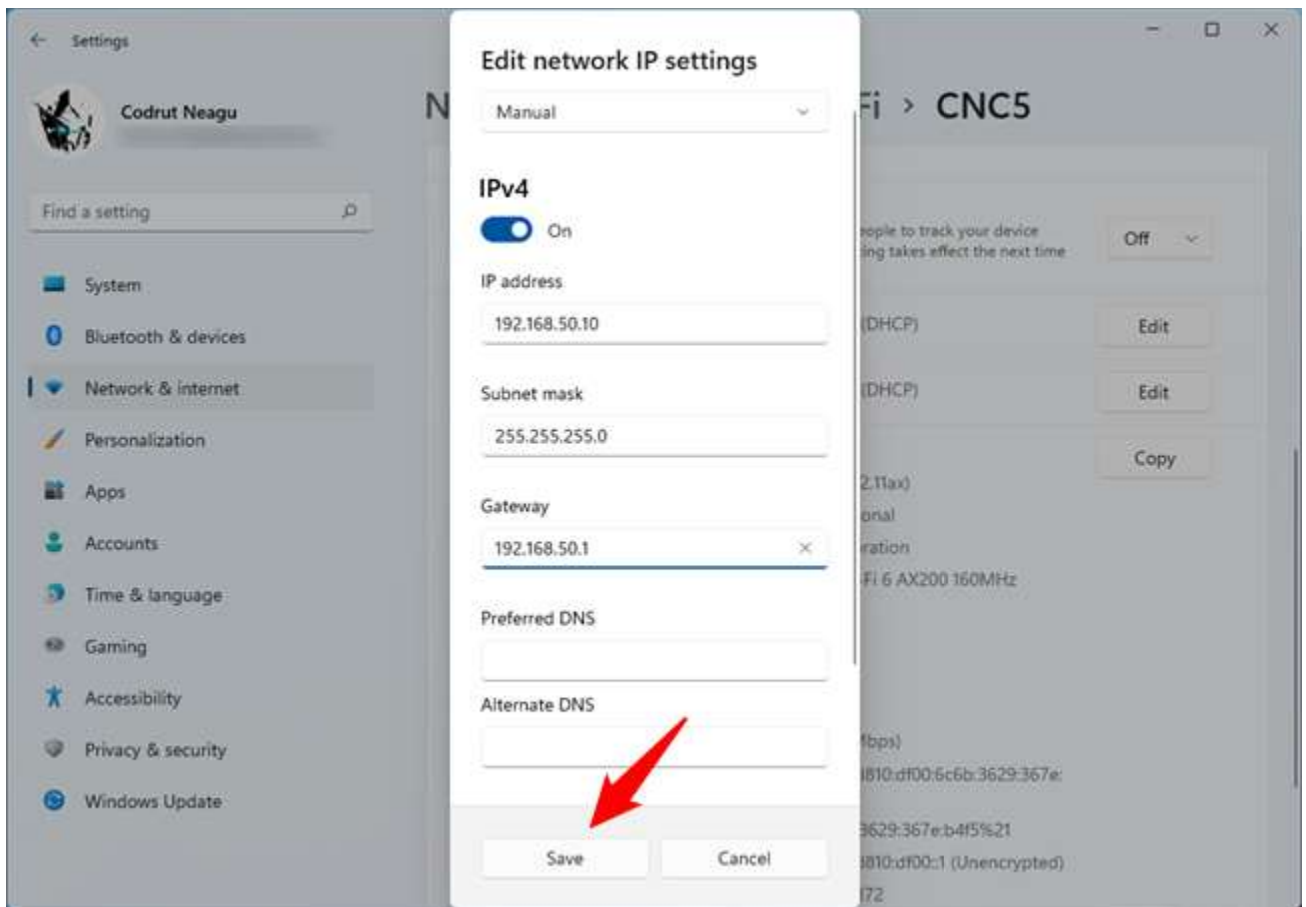
Gateway: Specify the IP address of your router or mesh Wi-Fi. In my case, that's 192.168.50.1.



Setting a static IP address in Windows 11

These are all the settings you need to configure in order to change your IP address in Windows 11. However, there are two more options in the “Edit network IP settings” dialog: Preferred DNS and Alternate DNS. While not necessarily required (if they’re blank, your router automatically assigns them), you can change them, too, if you want. Here are more details about DNS: [What is DNS? How is it useful?](#)

Once you’ve finished editing your network IP settings, click or tap the Save button, and your IP address is immediately changed in Windows 11.



How to set a static IP address in Windows 11

IMPORTANT: If you've changed your IP address and your Windows 11 PC lost internet connectivity, you've probably entered an incorrect IP address. In that case, switch back to using Automatic (DHCP) to let your router assign a new one for your computer, one that works.

IMPORTANT: If you've changed your IP address and your Windows 11 PC lost internet connectivity, you've probably entered an incorrect IP address. In that case, switch back to using Automatic (DHCP) to let your router assign a new one for your computer, one that works.

To set up IPv6 in Windows, you can follow these steps

Steps of configure ip6 :

Click Start, click Control Panel, and then double-click Network Connections. Right-click any local area connection, and then click Properties.

Click Install.

Click Protocol, and then click Add.

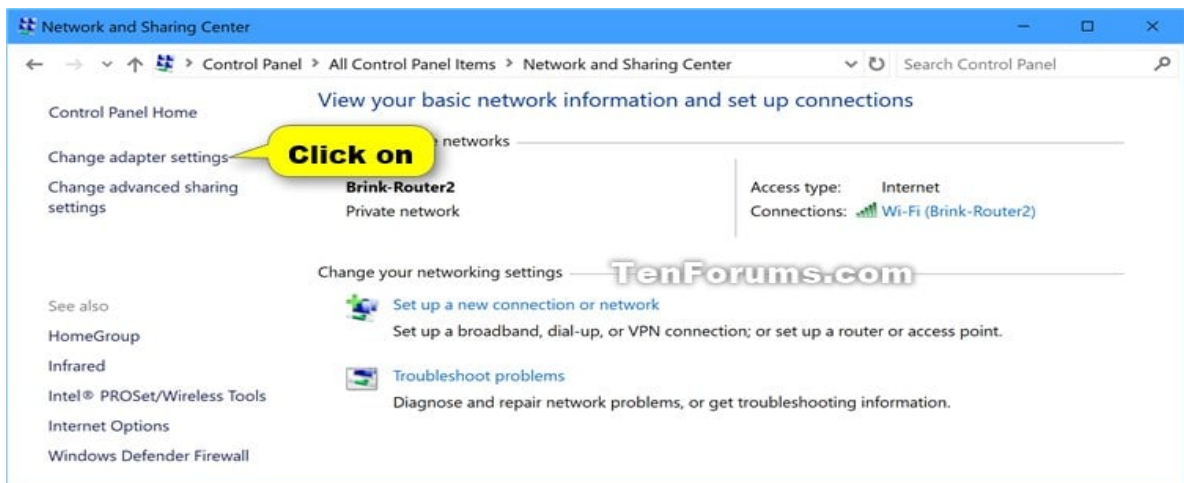
Click Microsoft TCP/IP version 6, and then click OK.

Click Close to save changes to your network connection.
Alternatively, you can enable IPv6 by going to Settings > Network & Internet > Properties > Edit > Manual > Enable IPv6 > Populate your settings54.

These steps assign ip6 using picture:-

1 Open the Control Panel (icons view), and click/tap on the Network and Sharing Center icon.

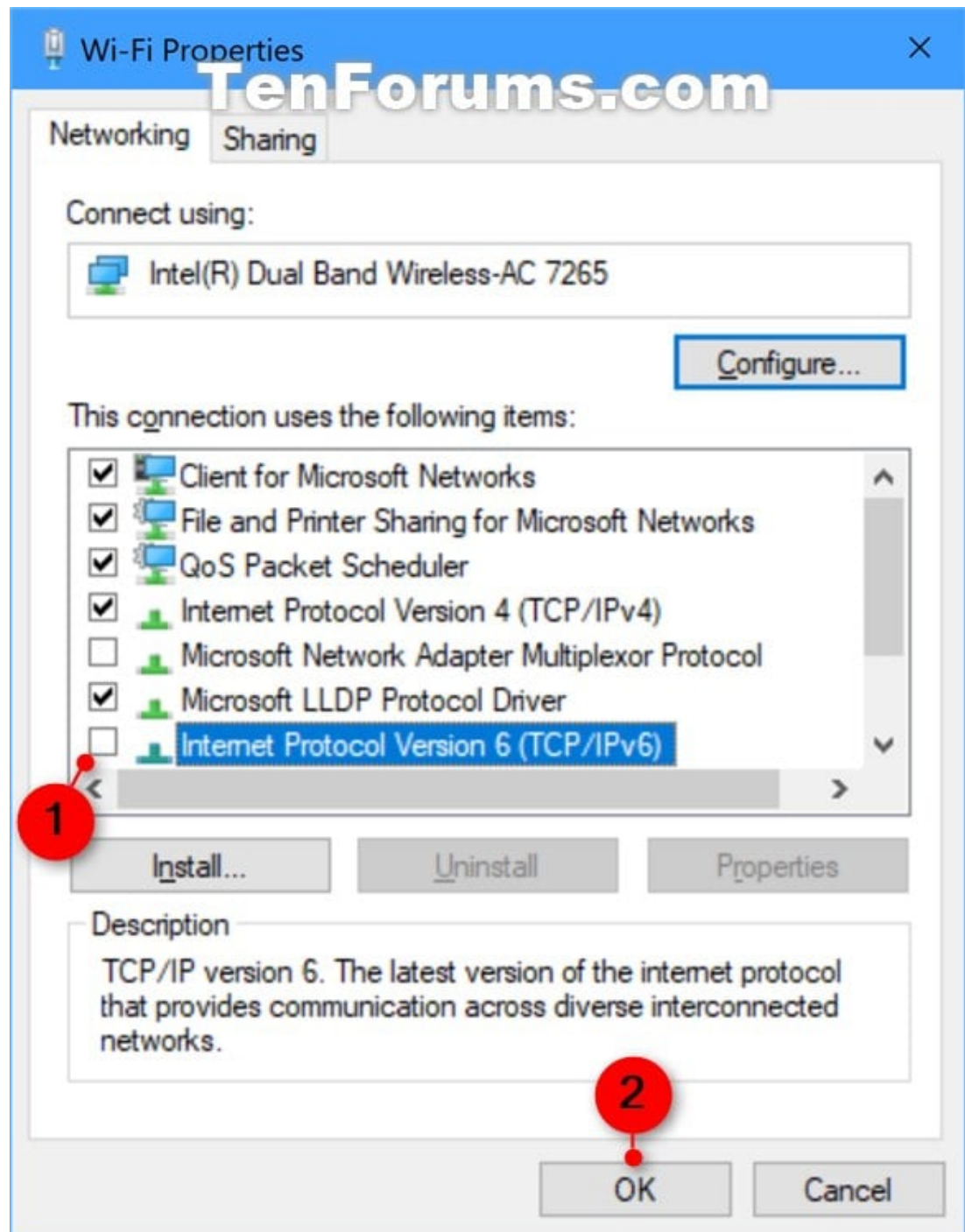
2 Click/tap on the Change adapter settings link on the left side, and close the Network and Sharing Center if you like. (see screenshot below)



3 Right click or press and hold on the network adapter (ex: "Wi-Fi") you want, and click/tap on Properties. (see screenshot below)



4 Check (enable) or uncheck (disable) the Internet Protocol Version 6 (TCP/IPv6) box for what you want to do, and click/tap on OK. (see screenshot below)



5 When finished, you can close Network Connections if you like.

2. Quality of Service (QoS):

Traffic Prioritization: Configure QoS to prioritize certain types of traffic (voice, video, critical applications) over others for better performance.

Bandwidth Allocation: Use QoS mechanisms like traffic shaping and policing to allocate and manage bandwidth effectively

3. Network Security Services:

IPv4 and IPv6 Security Measures:

Firewalls: Configure firewalls on routers or dedicated devices to filter traffic

based on security policies.

Access Control Lists (ACLs): Set up ACLs to control traffic flow and restrict access to specific IP addresses or protocols.

4. Other Network Services:

IPv4 and IPv6 Service Implementations:

DNS: Configure DNS servers for both IPv4 and IPv6 to resolve domain names.

DHCPv6: Implement DHCPv6 for dynamic IPv6 address assignment.

NAT (Network Address Translation): Configure NAT for IPv4 to map private IP addresses to a public IP address.

Practical 17

AIM: Learn Network programming

network programming concerning Python. But for this, the programmer must have basic knowledge of:

- Low-Level Programming using sockets
- Data encoding
- HTTP and web-programming
- High-Level client modules
- Basic networking terms and their concepts etc.

PYTHON NETWORK SERVICES:

There are two levels of network service access in Python. These are:

- Low-Level Access
- High-Level Access

In the first case, programmers can use and access the basic socket support for the operating system using Python's libraries, and programmers can implement both connection-less and connection-oriented protocols for programming.

Application-level network protocols can also be accessed using high-level access provided by Python libraries. These protocols are HTTP, FTP, etc.

socket :

A socket is the end-point in a flow of communication between two programs or communication channels operating over a network. They are created using a set of programming requests called socket API (Application Programming Interface). Python's socket library offers classes for handling common transports as a generic interface.

Sockets use protocols for determining the connection type for port-to-port communication between client and server machines. The protocols are used for:

Domain Name Servers (DNS)

IP addressing

E-mail

FTP (File Transfer Protocol) etc...

Python has a socket method that let programmers' set-up different types o

socket virtually. The syntax for the socket method is:

Python has a socket method that let programmers' set-up different types of socket virtually. The syntax for the socket method is:

SYNTAX:

```
g = socket.socket (socket_family, type_of_socket, protocol=value)
```

For example, if we want to establish a TCP socket, we can write the following code snippet:

```
# imports everything from 'socket'

from socket import *

# use socket.socket() - function

tcp1=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
```

Here's another example to establish a UDP socket. The code is:

```
udp1=socket.socket (socket.AF_INET, socket.SOCK_DGRAM)
```

After you defined the socket, you can use several methods to manage the connections. Some of the important server socket methods are:

listen(): is used to establish and start TCP listener.

bind(): is used to bind-address (host-name, port number) to the socket.

accept(): is used to TCP client connection until the connection arrives.

connect(): is used to initiate TCP server connection.

send(): is used to send TCP messages.

recv(): is used to receive TCP messages.

sendto(): is used to send UDP messages

close(): is used to close a socket.

Network program using python:

```
import socket
T_PORT = 60
TCP_IP = '127.0.0.1'
BUF_SIZE = 30
# create a socket object name 'k'
k = socket.socket (socket.AF_INET, socket.SOCK_STREAM)
k.bind((TCP_IP, T_PORT))
k.listen(1)
con, addr = k.accept()
print ('Connection Address is: ', addr)
while True :
    data = con.recv(BUF_SIZE)
    if not data:
        break
    print ("Received data", data)
    con.send(data)
con.close()
```

Save the file with filename - tcpserver.py

It will open a web server at port 60. In the above program, everything you write in the client goes to the server.

Now a simple Python client script:

```
import socket

T_PORT = 5006

TCP_IP = '127.0.0.1'

BUF_SIZE = 1024

MSG = "Hello karl"

# create a socket object name 'k'

k = socket.socket (socket.AF_INET, socket.SOCK_STREAM)

k.connect((TCP_IP, T_PORT))

k.send(MSG)

data = k.recv(BUF_SIZE)

k.close
```

Sending messages back and forth using different basic protocols is simple and straightforward. It shows that programming takes a significant role in client-server architecture where the client makes data request to a server, and the server replies to those machines.

Practical 18

AIM: Troubles shoot Networks

Network Troubleshooting Scenarios for Intermittent Network Problems

Intermittent network problems can be frustrating and challenging to troubleshoot because they occur sporadically and may not be immediately apparent. Here are some network troubleshooting scenarios to consider when dealing with intermittent network problems:

- **Loose or Damaged Cables:** Physical issues with network cables, such as loose connections or damaged cables, can lead to intermittent connectivity problems. Inspect cables and connectors for any visible damage or loose connections.
- **Wireless Interference:** In a wireless network, interference from other wireless devices, neighboring networks, or electronic devices can cause intermittent connectivity issues. Conduct a wireless site survey and identify potential sources of interference.
- **DHCP Issues:** Problems with the DHCP (Dynamic Host Configuration Protocol) server can result in intermittent IP address assignment, leading to connectivity problems. Check DHCP logs and ensure the DHCP server is properly configured and responsive.
- **DNS Problems:** DNS (Domain Name System) issues can cause intermittent access to websites and services. Verify DNS settings and check for any DNS-related errors in the logs.
- **Misconfigured Firewall or Security Software:** Overly aggressive firewall rules or misconfigured security software can block legitimate traffic and cause intermittent connectivity problems. Review firewall and security software settings for potential issues.
- **Bandwidth Saturation:** Periodic spikes in network traffic can saturate the available bandwidth and cause intermittent connectivity problems. Monitor network traffic patterns to identify potential bandwidth saturation points.
- **Network Device Overheating:** Overheating of network devices, such as routers or switches, can lead to intermittent network outages or services outages (ex.

Microsoft Teams outages). Ensure that network equipment is properly ventilated and not subjected to excessive heat.

- **Firmware or Software Bugs:** Firmware or software bugs in network devices can cause intermittent problems. Check for firmware updates and apply the latest patches from the manufacturer.
- **Duplicate IP Addresses:** Duplicate IP addresses on the network can result in intermittent connectivity issues. Use network scanning tools to check for duplicate IP addresses.

- **Routing Issues:** Incorrect or unstable routing configurations can lead to intermittent connectivity problems. Review routing tables and ensure they are correctly configured.
- **Power Fluctuations:** Power fluctuations or intermittent power supply issues can cause network devices to reboot or lose connectivity. Use uninterruptible power supply (UPS) units to provide stable power to critical network equipment.
- **Network Congestion:** During periods of high network usage, congestion can cause intermittent performance issues. Monitor network traffic during peak hours and consider implementing Quality of Service (QoS) policies.
- **Malware or Security Breaches:** Malware infections or security breaches can cause intermittent network disruptions. Regularly scan for malware and implement robust security measures.

Network Problem #2. High Bandwidth Usage

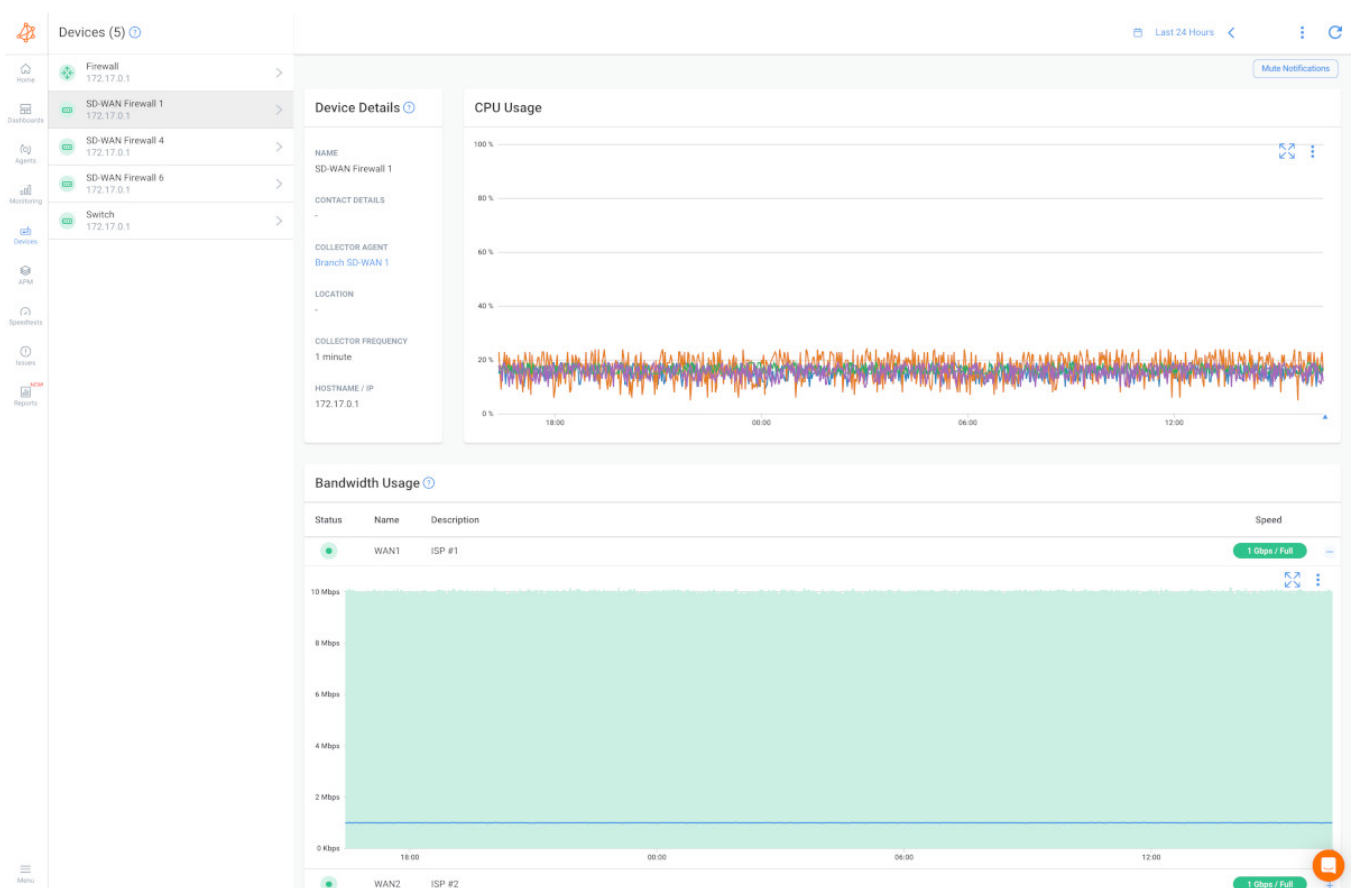
Bandwidth is the maximum amount of data transmitted over an Internet connection in a given amount of time.

It refers to a network's capacity to transfer data between devices or the Internet within a given span of time. Bandwidth is often mistaken for Internet speed when it's actually the volume of information that can be sent over a connection in a measured amount of time – calculated in megabits per second (Mbps).

Higher bandwidth allows data to be transferred across your network at a faster rate and can sustain a larger number of connected devices all at once - but it can significantly impact network performance and user experience.

It occurs when a considerable amount of data is being transmitted over the network, leading to increased congestion and potential bottlenecks. When someone or something, like a large application, on your network is monopolizing your bandwidth by downloading gigabytes worth of data, it creates a congestion in your network.

This excessive data transfer can result from various factors, both legitimate and non-legitimate, and it's essential to identify and address the root cause to maintain a smoothly functioning network.



high bandwidth usage - Common Network Problems

I. The Consequences of High Bandwidth Usage:

- **Network Congestion:** Network congestion caused by high bandwidth usage, also runs the risk of leaving insufficient amounts of bandwidth for other parts of your network that need it. When this happens, you may start experiencing problems like slow download speed over the Internet.
- **Slow Network Performance:** High bandwidth consumption can lead to slower network speeds, causing delays in accessing resources and data.
- **Latency and Packet Loss:** As network resources become saturated, latency (delay) and packet loss may increase, affecting real-time applications like VoIP or video conferencing.
- **Reduced Productivity:** Sluggish network performance can hamper productivity, as users may experience delays in performing critical tasks.
- **Increased Costs:** Excessive bandwidth usage can lead to overage charges from internet service providers (ISPs) if they exceed the Internet SLA, or the need to upgrade to higher-tier plans, resulting in higher operational costs.
- **Network Downtime:** In extreme cases, high bandwidth usage can lead to network outages if the infrastructure is not equipped to handle the traffic load.

II. The Causes of High Bandwidth

- **Large Downloads:** Downloads consisting of large files that are being placed on your computer's harddrive from the Internet, like file transfers or backups, can drastically increase bandwidth usage. The more bytes the file contains, the higher your bandwidth usage.
- **Latency:** Latency refers to the time it takes for a data packet to reach its destination in a network, can. Consistent delays or odd spikes in delay time are signs of major performance issues and can affect bandwidth time.
- **Packet Loss:** Packet Loss occurs when a data packet is dropped during its journey across a network and never makes it to its final destination and back. It can cause a great deal of problems depending on how much of the packet does not go through and how often it occurs.
- **Video Streaming:** Streaming videos from the Internet is a more common cause of high bandwidth usage. Streaming video in 7k can take up to 200 times more bandwidth than audio streaming.
- **Large Applications:** Different applications have different requirements. Applications that require Internet connection, like programs for web development, email, computer games, etc. require a lot of bandwidth to function and can therefore increase your bandwidth usage.
- **File Sharing:** There are programs that allow users to share files from computer-to-computer connection over the Internet. These programs can result in high

bandwidth usage as they require you to download and transfer large files, with large amounts of data, over the Internet.

- **Legitimate Traffic:** Legitimate high-bandwidth activities, such as large file transfers, video conferencing, cloud backups, and software updates, can consume significant network resources. While these activities are essential for business operations, they can lead to congestion during peak usage times.
- **Malware and Unauthorized Activities:** Malicious software or unauthorized users can exploit network resources, leading to unanticipated spikes in bandwidth usage. Botnets, malware downloads, or unauthorized file sharing can cause significant disruptions.
- **Background Updates:** Automatic updates for operating systems, applications, and antivirus software can utilize bandwidth without user intervention. These updates can coincide and cause temporary surges in bandwidth usage.
- **P2P File Sharing:** Peer-to-peer (P2P) file-sharing applications can lead to high bandwidth usage as users upload and download files directly from each other.

How to Measure Bandwidth: Techniques for Precise Network Measurement

How to Measure Bandwidth for Precise Network Measurement

How to measure bandwidth, identify issues & optimize network performance. Use Obkio's Network Performance Monitoring tool for easy bandwidth monitoring.

Learn more 

III. How to Identify & Troubleshoot High Bandwidth Usage

- **Network Monitoring:** Use a network monitoring tool like Obkio to measure bandwidth and track bandwidth usage in real-time. Observe usage patterns and identify any unusual spikes or sustained high traffic.
- **Application Analysis:** Analyze the bandwidth consumption of various applications to identify resource-intensive processes. This will help you pinpoint which applications are contributing the most to high usage.
- **Quality of Service (QoS) Policies:** Implement QoS policies to prioritize critical applications and services over less important ones. This ensures that essential operations receive sufficient bandwidth even during peak usage.
- **Bandwidth Optimization:** Utilize bandwidth optimization techniques such as compression, caching, or content filtering to reduce overall data transfer.

- Traffic Shaping: Employ traffic shaping mechanisms to control and limit bandwidth usage for specific applications or users.
- Identify Malware or Unauthorized Activity: Regularly scan for malware and unauthorized users on the network, and implement security measures to prevent exploitation.

By proactively identifying and addressing high bandwidth usage, businesses can maintain a responsive and efficient network, enhancing overall productivity and user satisfaction.

IV. Network Troubleshooting Scenarios for High Bandwidth Usage

High bandwidth usage can lead to various network performance issues and can be caused by several factors. Here are some network troubleshooting scenarios to investigate when experiencing high bandwidth usage:

- Malware or Botnet Activity: Malware-infected devices or botnet activity can consume significant bandwidth as they may be involved in malicious activities such as sending spam emails or participating in Distributed Denial of Service (DDoS) attacks. Use network monitoring tools to identify suspicious traffic patterns and isolate infected devices.
- Streaming and Video Content: High-quality video streaming or large file downloads can consume substantial bandwidth. Check for excessive video streaming or downloads that might be impacting the network, especially during peak hours.
- Cloud Services or Backups: Cloud services and data backups can utilize substantial bandwidth, especially if they are scheduled to occur during business hours. Check the bandwidth consumption of cloud services (with Microsoft Cloud Monitoring for example) and backup applications to see if adjustments can be made to their schedules.
- Peer-to-Peer (P2P) File Sharing: P2P file sharing applications can consume a significant amount of bandwidth, especially if multiple users are involved. Identify and control P2P traffic on the network.
- Software Updates: Automatic software updates from operating systems and applications can lead to sudden spikes in bandwidth usage. Ensure that updates are scheduled during off-peak hours

- **Network Misconfiguration:** Misconfigured network devices, such as routers or switches, can lead to unnecessary broadcast/multicast traffic or loops that cause high bandwidth usage. Verify the network configuration for any issues.
- **Bandwidth-Intensive Applications:** Some applications inherently consume more bandwidth than others. Identify and analyze bandwidth usage by specific applications and determine if any optimization or restriction is required.
- **Virtual Local Area Networks (VLANs):** Improperly configured VLANs can lead to unnecessary traffic and high bandwidth usage. Review VLAN configurations to ensure they are set up correctly.
- **Wireless Network Interference:** In a wireless network, interference from other devices, neighboring networks, or non-Wi-Fi devices operating in the same frequency range can cause high bandwidth utilization. Perform a wireless site survey and optimize Wi-Fi settings.
- **Data Backups and Replication:** Data backup and replication processes between geographically dispersed sites can consume significant bandwidth. Review backup and replication schedules and consider using deduplication and compression techniques.
- **Denial of Service (DoS) Attacks:** DoS attacks can overwhelm a network with an excessive amount of traffic, leading to high bandwidth usage. Implement DoS protection mechanisms and analyze traffic patterns for signs of an ongoing attack.
- **Internet of Things (IoT) Devices:** The proliferation of IoT devices can contribute to increased bandwidth consumption if they are transmitting large amounts of data. Monitor IoT device traffic and assess their impact on overall bandwidth.

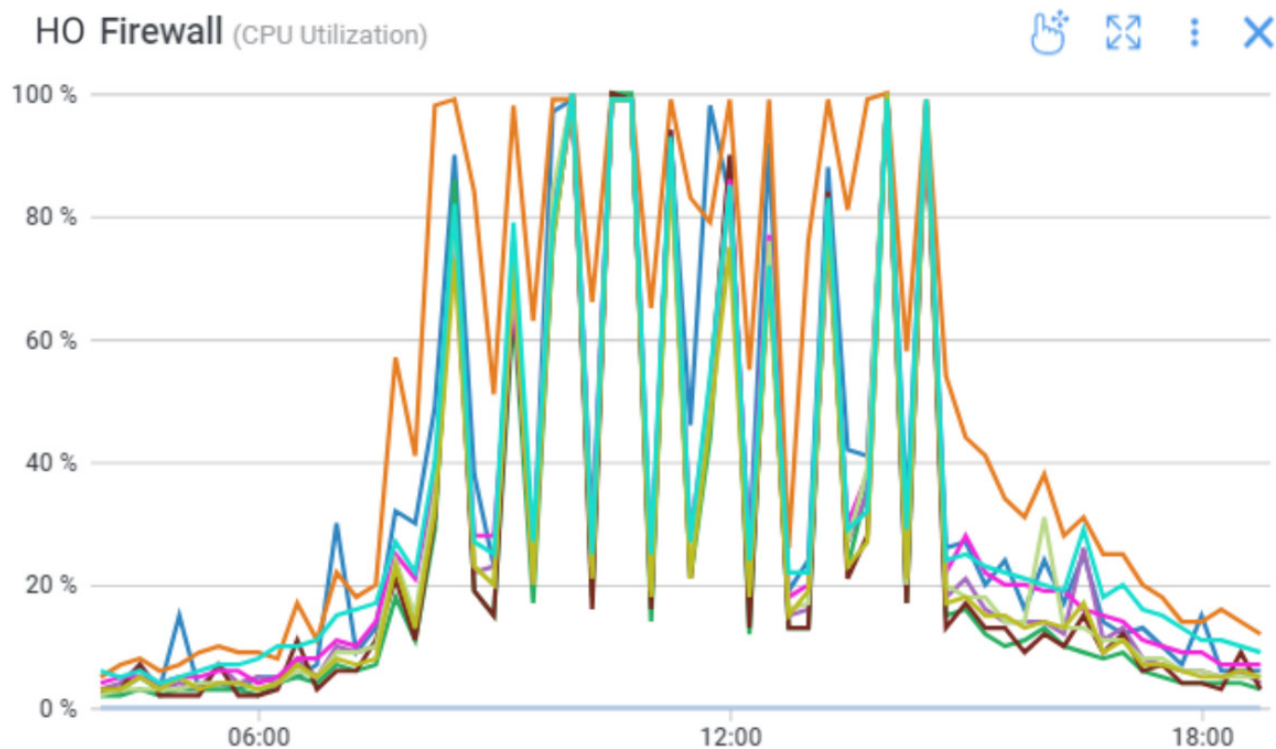
To troubleshoot high bandwidth usage, it is essential to use network monitoring tools that provide insights into traffic patterns, application usage, and device behaviour, like we mentioned in the last point. With this information, you can identify the root cause of the problem and take appropriate measures to optimize network performance.

Network Problem #3. High CPU Usage

CPU, or “ Central Processing Unit”, is the primary component of a computer that receives and processes instructions for operating systems and applications.

High CPU usage is another common network problem that can significantly impact the performance and stability of a network. It occurs when the central processing unit (CPU) of a network device, such as a router, switch, firewall, or server, is operating at or near its maximum capacity. This can lead to various issues that affect the overall network functionality and user experience.

With such a big job on its shoulders, the signs of high CPU usage on a network device are a very troubling sign for many of us. As your network devices continue to work harder to perform an increasing amount of tasks, it increases the chance that things can go wrong.



Network Firewall CPU Monitoring Network Problems

I. The Consequences of High CPU Usage

- **Sluggish Network Performance:** High CPU usage can lead to delays in processing network traffic, causing slow response times and increased latency.
- **Packet Loss:** When the CPU is overloaded, it may drop packets, resulting in packet loss, which can degrade the quality of real-time applications like VoIP or video conferencing.
- **Network Downtime:** In extreme cases, when the CPU is overwhelmed, the device may become unresponsive, leading to network outages and disruptions.

Security Vulnerabilities: High CPU usage can leave network devices more vulnerable to security threats as their ability to handle security tasks is compromised.

II. The Causes of High CPU Usage

The most common reason for high CPU usage occurs when your network becomes bogged down by enormous amounts of traffic. CPU usage can increase drastically when processes require more time to execute or when a larger number of network packets are sent and received throughout your network.

There are a number of network devices such as switches that have hardware components (ASICs or NPUs) that take charge and process packets super quickly. For this equipment, the CPU usage is not linked to the amount of traffic.

For equipment that analyzes or manipulates traffic, like firewalls, that's a whole different story. Depending on the features that you've enabled on your devices, the CPU may be in the critical path of packet routing or forwarding. If overused, network metrics like latency, jitter, and packet loss will increase, which will lead to significant levels of network performance degradation.

In summary, some common causes include:

- **Network Traffic Overload:** A sudden surge in network traffic or sustained high levels of data transfer can overwhelm the CPU, especially on devices handling routing, switching, or security tasks.
- **Network Security Operations:** CPU usage may spike during security-related activities such as deep packet inspection, intrusion detection, or denial-of-service attack mitigation.
- **Resource-Intensive Applications:** CPU usage can be driven up by resource-intensive applications running on servers or other network devices.
- **Firmware/Software Bugs:** Firmware or software bugs can cause abnormal CPU usage, leading to unexpected behavior and degraded performance.

III. Troubleshoot High CPU Usage

It can sometimes be difficult to gather the right information about the actual use of CPU. Several monitoring tools such as those included in the equipment's GUI or a poorly configured monitoring tool can report an average value on the use of 8 cores or over too long periods, such as every 5, 15 or 60 minutes. Which isn't enough - so to identify and troubleshoot - you need to go further!

- **Network Monitoring:** Employ a network monitoring tool like Obkio to track CPU utilization on network devices. Monitor CPU usage in real-time and set up alerts for abnormally high CPU levels.

Identify Resource-Intensive Processes: Use monitoring tools and device logs to identify resource-intensive processes or applications causing high CPU usage.

Adjust Network Traffic: Implement traffic shaping or quality of service (QoS) policies to prioritize critical traffic and prevent CPU overload during periods of heavy network usage.

Software/Firmware Updates: Regularly update device firmware and software to patch bugs and optimize performance.

Optimize Applications: Consider optimizing resource-intensive applications or distributing their load across multiple devices to reduce CPU burden.

Security Measures: Ensure that security policies and mechanisms are properly configured to manage security-related CPU tasks effectively.

Device Upgrades: If network devices are consistently experiencing high CPU usage, consider upgrading to more powerful hardware that can better handle the network load.

By promptly identifying and resolving high CPU usage issues, businesses can maintain a stable and responsive network environment, ensuring smooth operations and enhanced user satisfaction.

IV. Network Troubleshooting Scenarios for High CPU Usage

High CPU usage in a network can impact the performance of network devices, leading to sluggish response times, increased latency, and potential service disruptions. Here are some network troubleshooting scenarios to consider when dealing with high CPU usage on network devices:

Traffic Spikes: Monitor network traffic patterns to identify if there are sudden spikes in data volume that could be causing high CPU usage. Investigate the source of the increased traffic and determine if it is legitimate or if it indicates a potential DDoS (Distributed Denial of Service) attack.

Packet Storms or Broadcast Storms: Excessive packet storms or broadcast storms can overload the CPU of network devices. Use packet capture tools to analyze the traffic and identify any sources of storms.

Malware or Botnet Activity: Malware infections on network devices can cause high CPU utilization as they might be involved in malicious activities. Use security monitoring tools to detect and remove malware from affected devices.

Routing or Switching Loops: Misconfigured or redundant routing or switching paths can cause loops, leading to a significant increase in CPU usage. Review the device configurations to ensure there are no loop-causing issues.

Software Bugs or Memory Leaks: Software bugs or memory leaks within the operating system or network device firmware can cause CPU usage to spike over time. Ensure that the network devices have the latest firmware updates and patches.

Network Device Overloading: If a network device is overloaded with traffic due to the number of connected devices or the volume of data being processed, the CPU usage can increase. Consider load balancing or upgrading the device to handle higher traffic volumes.

Large Scale Routing Updates: In networks with dynamic routing protocols, large-scale routing updates can cause CPU spikes on routers. Analyze routing update events and fine-tune the routing protocols to minimize the impact.

Monitoring or Debugging Tools: Certain monitoring or debugging tools running on network devices might consume a significant amount of CPU resources. Evaluate the impact of such tools and adjust their configurations if necessary.

Quality of Service (QoS) Misconfiguration: Improperly configured QoS policies can lead to unnecessary CPU usage as the devices attempt to classify and prioritize traffic. Review and optimize QoS policies.

Hardware Issues: Faulty hardware components, such as failing CPUs or inadequate cooling systems, can lead to high CPU usage. Perform hardware diagnostics and replace any faulty components.

Intrusion Detection/Prevention Systems (IDS/IPS): IDS/IPS systems can be CPU-intensive, especially when handling a large number of network packets. Fine-tune the IDS/IPS settings and consider distributing the load across multiple devices if applicable.

Virtualization Overhead: In virtualized environments, the hypervisor's CPU overhead can impact network device performance. Adjust virtualization settings and resource allocations as needed.

How to Measure CPU Usage in Networking

How to Measure CPU Usage in Networking

Uncover the secrets of measuring CPU usage in networking. Navigate high seas of performance with insights. Optimize with Obkio's Monitoring tool.

Learn more 

Network Problem #4. Physical Connectivity Issues

It may seem obvious, but some network issues may occur with the hardware outside of the network.

When the time comes to troubleshoot network issues, our instinct is often to think about the most complex situations, when sometimes the problem is actually very simple and right in front of us.

Hardware problems like defective cables or connectors can generate network errors on the network equipment to which it is connected. You may think that this problem is due to a network outage or network failure, or Internet connection problem, but it's actually because you have a broken or malfunctioning cable.

This can also occur outside of the LAN network. If a copper cable, or fiber-optic cable is damaged, it will likely reduce the amount of data that can go through it without any packet loss.

I. The Consequences of Physical Connectivity Issues

Physical connectivity problems can manifest in various ways, leading to network outages, slow data transfer, or intermittent connectivity.

Network Outages: A complete loss of physical connectivity can lead to network outages, preventing users from accessing network resources.

Intermittent Connectivity: Loose or damaged cables may cause intermittent connectivity issues, resulting in unreliable network access.

Slow Data Transfer: Poor physical connections can lead to data transmission errors and retransmissions, slowing down data transfer rates.

Increased Downtime*: The time spent identifying and resolving physical connectivity issues can lead to increased network downtime and reduced productivity.

II. The Causes of Physical Connectivity Issues

Loose or Damaged Cables: Loose, damaged, or improperly connected cables can lead to signal loss and intermittent connectivity. Cables that are bent, frayed, or crushed may not transmit data effectively.

Faulty Connectors: Connectors that are not securely attached or have bent pins can result in poor connections between devices, leading to data transmission issues.

Cable Length: Using cables that exceed their maximum recommended length can lead to signal degradation and data loss.

Poorly Crimped or Terminated Cables: Improperly crimped or terminated cables may cause signal interference and connectivity problems.

Network Device Issues: Faulty network interface cards (NICs) or malfunctioning ports on switches or routers can cause physical connectivity problems.

Environmental Factors: External factors such as water damage, extreme temperatures, or physical disturbances can impact network cables and connectors.

III. How to Identify & Troubleshoot Physical Connectivity Issues

Network Monitoring: Checking every cable one by one can be repetitive, and can take a large amount of time out of your day. A simple way to monitor cables on a defective connector is to have a network performance monitoring software, like Obkio, that will measure network errors on all network interfaces and warn you if any problems arise.

Visual Inspection: Perform a physical inspection of cables, connectors, and network devices to identify any visible signs of damage or loose connections.

Cable Testing: Use cable testers to check for continuity and proper termination of network cables. **Swap Cables and Connectors:** If possible, try replacing suspect cables and connectors with known-good ones to determine if the issue persists.

Check Device Indicators: Examine network device indicators, such as LED lights, to see if they indicate any connectivity or link issues.

Environmental Assessment: Ensure that network equipment is kept in suitable environmental conditions, free from water damage, extreme temperatures, and physical obstructions.


Label and Organize Cables: Properly label and organize network cables to prevent accidental disconnections and make troubleshooting easier.

Update Firmware and Drivers: Ensure that network devices have up-to-date firmware and drivers to minimize the risk of hardware-related issues.

How to Troubleshoot Network Issues: Unleash Your Inner IT Hero

How to Troubleshoot Network Issues: Unleash Your Inner IT Hero

Learn how to troubleshoot network issues by identifying where, what, why network problems occur with Network Troubleshooting tools.

Learn more 

IV. Network Troubleshooting Scenarios for Physical Connectivity Issues

Physical connectivity issues can disrupt network communication and lead to various network problems. Troubleshooting physical connectivity issues requires a systematic approach and attention to detail. Here are some network troubleshooting scenarios to consider when dealing with physical connectivity issues:

Check Physical Connections: Verify that all network cables, connectors, and ports are properly connected and securely seated. Ensure that Ethernet cables are not damaged and have all pins intact.

Swap Cables and Ports: If possible, swap suspect cables with known-working ones and test different network ports on the devices to rule out faulty cables or ports.

Check Link Lights: Observe the link lights on network devices (routers, switches, and network interface cards) to determine if the devices are detecting link signals. If link lights are not active, it could indicate a physical connectivity problem.

Inspect Patch Panels and Wall Outlets: In structured cabling systems, examine patch panels and wall outlets to ensure cables are correctly terminated and properly labeled.

Use Cable Testers: Cable testers can help identify faulty cables, open circuits, or short circuits. Use a cable tester to check the integrity of network cables.

Check Power Over Ethernet (PoE): For PoE devices, ensure that power is being supplied correctly over the Ethernet cables.

Verify Power Status: Check the power status of network devices to ensure they are powered on and functioning correctly.

Check Physical Damage or Environmental Factors: Look for physical damage to network cables caused by bending, crushing, or exposure to environmental elements. Address any environmental factors that might be affecting the cables, such as excessive heat or moisture.

Review Network Topology: Review the network topology to ensure that cables are appropriately connected between devices and network segments.

Test Connectivity with Known Devices: Test connectivity with known working devices to isolate the issue to specific network segments or components.

Check Wiring Standards: Ensure that network cabling adheres to appropriate wiring standards (e.g., TIA/EIA 568) and that cables are of the correct category (e.g., Cat 5e, Cat 6, etc.) for the required network speeds.

Check Cable Lengths: Verify that the cable lengths do not exceed the maximum allowed length for the chosen cable category and network technology (e.g., Ethernet has specific cable length limits).

Inspect Network Devices' LEDs: Network devices like switches and routers often have LEDs that indicate port activity and speed. Observe these LEDs to identify any abnormal behavior.

Check Physical Security: Ensure that physical access to network devices and cables is restricted to authorized personnel to prevent accidental or intentional disconnections.

Consider EMI/RFI Interference: Electromagnetic Interference (EMI) or Radio-Frequency Interference (RFI) from nearby electrical devices can affect network connectivity. Isolate network devices from potential sources of interference

Inspect Fiber Optic Connections: If your network uses fiber optic cables, check the connectors and fiber ends for any dirt, damage, or misalignment.

Network Problem #5. Malfunctioning Devices or Equipment

Sometimes, network issues occur within network equipment or devices like Firewalls, Routers, Switches, Wifi APs.

Malfunctioning devices or equipment are a common network problem that can disrupt network operations and lead to various connectivity issues. This category encompasses hardware failures or malfunctions within network devices, such as routers, switches, firewalls, servers, or network interface cards (NICs). When devices malfunction, they may experience performance degradation or cease to function altogether, impacting the overall network performance and user experience.

You need to ensure that all the devices on your network are configured correctly in order for your network to work properly. Whenever you install or reconfigure a device, or upgrade equipment firmware on your network, you need to test that device to ensure that it's been configured correctly.

Many network performance issues are caused by device misconfigurations that can affect different parts of your network and turn into major problems down the line. That's why you need to pay attention to all the switches and devices on your network to ensure that they're always working as they should be, and react quickly if they aren't.

I. The Consequences of Malfunctioning Devices or Equipment

Network Downtime: When crucial network devices fail, it can result in network outages and disrupt communication and data transfer.

Slow Performance: Malfunctioning devices may struggle to process network traffic efficiently, leading to slow data transfer and increased latency.

Data Loss: Hardware failures can cause data loss, especially if the malfunctioning device is responsible for data storage or backups.

Reduced Reliability: Frequent device malfunctions erode the network's reliability, causing frustration for users and hindering business operations.

II. The Causes of Malfunctioning Devices or Equipment

Hardware Failure: Components within network devices can fail due to wear and tear, manufacturing defects, or age. Common hardware failures include power supply issues, memory failures, or fan malfunctions.

Overheating: Network devices that are not adequately cooled or positioned in poorly ventilated areas can overheat, leading to malfunctions and performance degradation.

Software Bugs: Firmware or software bugs within network devices can cause erratic behavior or crashes, impacting their ability to function correctly.

Power Surges or Electrical Issues: Power surges or electrical problems can damage network devices and render them inoperable.

Environmental Factors: Adverse environmental conditions, such as exposure to moisture, dust, or extreme temperatures, can contribute to device malfunction.

III. How to Identify & Troubleshoot Malfunctioning Devices or Equipment

Network Device Monitoring: Use network monitoring tools like Obkio to track device performance metrics, such as CPU usage, memory utilization, and temperature readings. Abnormal values may indicate potential device malfunctions. Obkio's network device monitoring solution is a simple and easy solution that offers advanced polling for SNMP Monitoring for all SNMP-enabled devices along your network to ensure they're all performing as they should be.

Device Logs: Review device logs and error messages to identify any hardware or software-related issues reported by the device.

Hardware Diagnostics: Many network devices come with built-in diagnostic tools that can identify hardware failures or malfunctions.

Hardware Replacement: If a device is suspected to be malfunctioning, consider replacing it with a known-working spare or a new device to confirm if the issue is resolved.

Firmware/Software Updates: Ensure that devices have the latest firmware and software updates to fix known bugs and optimize performance.

Temperature Management: Check the environmental conditions of network devices and ensure they are adequately cooled and placed in suitable locations.


Power Protection: Implement surge protectors and uninterruptible power supply (UPS) systems to safeguard devices against electrical issues.

By proactively identifying and addressing malfunctioning devices or equipment, businesses can reduce network downtime, maintain reliable operations, and ensure an efficient and responsive network infrastructure.

How to Identify Network Problems & Diagnose Network Issues

How to Identify Network Problems & Diagnose Network Issues

Learn how to identify network issues by looking at common problems, causes, consequences and solutions.

Learn more 

IV. Network Troubleshooting Scenarios for Malfunctioning Devices or Equipment

When dealing with malfunctioning network devices or equipment, prompt troubleshooting is essential to identify and resolve the issues efficiently. Here are some network troubleshooting scenarios to consider when facing malfunctioning devices or equipment:

Device Power Status: Check if the malfunctioning device is powered on and receiving adequate power. Verify power connections and consider testing the device with a different power source or power cable.

Device Reset or Reboot: Perform a controlled restart or reboot of the malfunctioning device. Sometimes, a simple restart can resolve temporary issues.

Check Device Status Lights: Observe the status lights or LEDs on the malfunctioning device to identify any error codes or abnormal behavior. Refer to the device's documentation for guidance.

Verify Firmware/Software Versions: Ensure that the device's firmware or software is up to date. If available, apply the latest firmware updates or patches from the manufacturer's website.

Inspect Device Logs: Review the device logs to identify any error messages or alerts that might indicate the cause of the malfunction.

Device Configuration: Verify the device configuration to ensure it aligns with the network's requirements and network monitoring best practices. Look for misconfigurations or conflicting settings.

Isolate Device from the Network: Temporarily disconnect the malfunctioning device from the network to determine if it is the cause of broader network issues.

Test Connectivity and Cable: Check the connectivity of the malfunctioning device by testing it with a known-working cable and connecting it to a different network port.

Temperature and Ventilation: Overheating can cause devices to malfunction. Ensure that the device has adequate ventilation and is not exposed to excessive heat.

Test with Different Ports: If the device has multiple ports, test with different ports to check for faulty hardware on specific interfaces.

Check for Hardware Faults: Examine the device's physical components for any signs of damage or hardware faults.

Reinstall or Reset Device: If appropriate, consider reinstalling or performing a factory reset on the malfunctioning device to rule out software-related issues.

Device Interoperability: Verify if the malfunctioning device is compatible with other devices on the network. Ensure that it supports required protocols and standards.

Replace or Repair Faulty Components: If hardware components are found to be faulty, consider replacing or repairing them.

Check for Environmental Factors: Determine if the malfunction could be caused by environmental factors such as electromagnetic interference or power fluctuations.

Update Drivers: For network interface cards and other peripheral devices, update drivers to the latest versions to address potential compatibility issues.

Verify Network Connectivity: Confirm that the malfunctioning device is connected to the correct network and VLAN (if applicable).

Seek Vendor Support: If the issue persists or is beyond your troubleshooting capabilities, contact the vendor's technical support for further assistance.

Always document the troubleshooting steps and any changes made to the device or network during the process. Thorough documentation helps in future reference and sharing information with others who might be assisting with the troubleshooting process.

Network Problem #6. DNS Issues

DNS or Domain Name System, controls how visitors find your website over the Internet.

It is essentially a directory for the Internet (and every Internet-connected device) that matches domain names with IP addresses. Every single website has its own IP address on the web, and computers can connect to other computers via the Internet and look up websites using their IP address. When you type in a domain name in your Internet browser, DNS works to find the information connected to that domain.

DNS issues are very common network problems that many people tend to overlook. DNS issues occur when you are unable to connect to an IP address, signalling that you may have lost network or Internet access. For example, your site can simultaneously appear online for you, but looks to be offline to your visitor

When DNS issues arise, users may experience difficulties accessing websites, sending emails, or connecting to network resources.

I. The Consequences of DNS Issues

The inability to access the Internet or particular sites can have a very immediate and negative impact on your business - especially if it means that users cannot access your site. Just a few hours offline can cost your company in more ways than one, which is why it's important to find and fix DNS problems as soon as possible.

Website Inaccessibility: Users may be unable to access websites or services due to failed DNS resolutions.

Email Delivery Issues: DNS problems can affect email delivery, causing delays or preventing emails from being sent or received.

Slow Internet Browsing: DNS lookup delays can result in sluggish website loading times and overall slow internet browsing experiences.

Security Risks: DNS hijacking or cache poisoning can lead to security vulnerabilities, exposing users to phishing attacks or other malicious activities

II. The Causes of DNS Issues

Bad Configurations: You may experience issues due to improper configuration of DNS records.

High DNS Latency: High Latency, which is the measure of time it takes for data to reach its destination across a network, can cause slow and abnormally long loading times.

High TTL Values: High "time to live" values on your records, will lead to high propagation wait times. Traceroute tools, like Obkio's Live Traceroutes feature and Obkio Vision Visual Traceroute tool, actually track and monitor TTL values.

Hardware/Network Failures: DNS problems can be caused by hardware failures on the host machine or network failures. Troubleshoot network/ hardware configuration settings using a network performance monitoring tool to identify the source of the problem.

DNS Server Outages: If the DNS server responsible for resolving domain names becomes unavailable or experiences downtime, users will be unable to access websites or services.

Misconfigured DNS Settings: Incorrectly configured DNS settings on network devices or client systems can lead to failed DNS lookups.

DNS Cache Poisoning: Malicious actors can compromise DNS caches, leading to incorrect or spoofed DNS records being served, redirecting users to malicious websites.

Network Connectivity Issues: Internet connectivity issues or problems or routing can prevent DNS queries from reaching DNS servers or receiving responses and lead to network connectivity issues

DNS Propagation Delays: After making changes to DNS records, it can take time for the changes to propagate across the internet. During this period, users may experience inconsistent DNS resolution.

DNS Hijacking: Cyber attackers may hijack DNS queries to redirect users to fraudulent websites or phishing pages.

New call-to-action

III. How to Identify & Troubleshoot DNS Issues

DNS Monitoring: Utilize network monitoring tools like Obkio to track DNS queries and response times. Monitor DNS servers' performance and ensure they are resolving queries promptly.

DNS Testing Tools: Use DNS testing tools to check the network response time and accuracy of DNS queries from different locations.

Flush DNS Cache: On client systems, flush the DNS cache to clear any outdated or corrupted entries that may be causing issues.

Check DNS Server Status: Verify the status of DNS servers to ensure they are operational and responsive.

Review DNS Settings: Check DNS settings on network devices, routers, and client systems for any misconfigurations.

DNSSEC Implementation: Consider implementing DNSSEC (DNS Security Extensions) to prevent DNS cache poisoning and improve DNS security.

Monitor DNS Logs: Review DNS server logs for any unusual activities or error messages that may indicate issues.

Update DNS Records: Ensure that DNS records are correctly updated and propagated across authoritative DNS servers.

By proactively identifying and resolving DNS issues, businesses can ensure smooth and reliable access to online resources, improve internet browsing experiences, and enhance overall network security.

How to Troubleshoot Intermittent Internet Connection: Don't Get Caught in the Spinning Wheel of Death

How to Troubleshoot Intermittent Internet Connection

Learn how to troubleshoot intermittent Internet connection issues with Network Monitoring. Find & fix the cause of intermittent Internet issues.

Learn more [right arrow](#)

IV. Network Troubleshooting Scenarios for DNS Issues

DNS (Domain Name System) issues can cause various network problems, including the inability to access websites, email services, or other network resources. Here are some network troubleshooting scenarios to consider when dealing with DNS issues:

Ping and Traceroute: Use the ping and traceroute commands to verify DNS resolution. If you can ping IP addresses but not domain names, it indicates a DNS resolution problem.

Check DNS Server Settings: Verify that the DNS server settings on the client devices are correct. Ensure that they are pointing to the appropriate DNS servers, such as those provided by the ISP or internal DNS servers.

DNS Server Reachability: Check if the DNS servers are reachable from the client devices. Use ping to confirm if the DNS servers respond to requests.

Flush DNS Cache: Clear the DNS cache on the client devices to ensure they fetch fresh DNS records from the DNS servers.

DNS Server Logs: Analyze the DNS server logs for errors or issues. Look for failed DNS requests or unusual patterns.

DNS Forwarding and Recursion: Ensure that DNS servers are properly configured for forwarding and recursion. Misconfigured forwarding can lead to failed DNS resolution.

DNSSEC Validation: If DNSSEC (Domain Name System Security Extensions) is enabled, check for DNSSEC validation issues that might prevent resolution for some domains.

Check DNS Records: Verify the DNS records for the domain in question (A, CNAME, MX, etc.) to ensure they are correctly configured.

Firewall and Filtering: Review firewall rules and content filtering settings that might block DNS traffic or DNS resolution.

ISP DNS Issues: Contact the Internet Service Provider (ISP) to check if there are any DNS issues or outages in their DNS infrastructure.

DNS Load Balancing: If using DNS-based load balancing, ensure that it is working correctly and directing traffic to the appropriate servers.

DNS Round Robin: If DNS round-robin is used, verify that all the IP addresses in the DNS response are functional.

Reverse DNS Lookup: Check reverse DNS lookup (PTR) records to ensure they match the corresponding forward (A) records.

DNS Timeouts: Monitor for DNS timeouts in application logs or network captures, which may indicate DNS server unresponsiveness.

DNS Hijacking or Spoofing: Investigate for any signs of DNS hijacking or spoofing, which could redirect users to malicious websites.

DNS Over HTTPS (DoH) or DNS Over TLS (DoT): If DoH or DoT is implemented, verify the configuration and connectivity to the chosen secure DNS resolver.

IPv6 DNS Configuration: Ensure that DNS resolution works correctly for both IPv4 and IPv6 addresses.

Third-Party DNS Services: If using third-party DNS services, verify their service status and reachability.

DNS Health Check Tools: Utilize DNS health check tools or online DNS diagnostics to assess DNS configuration and performance.

By systematically troubleshooting DNS issues, you can identify and resolve the root cause of the problem, ensuring smooth DNS resolution and proper network connectivity. If the issue persists or is beyond your expertise, don't hesitate to seek assistance from qualified network administrators or DNS experts.

Network Problem #7. Interference in the Wireless Network

WiFi problems are one of the most common complaints surrounding modern day connectivity.

Interference in the wireless network is a common and frustrating network problem that can significantly impact Wi-Fi performance and reliability. Wireless networks, such as Wi-Fi, rely on radio frequencies to transmit data between devices. Interference occurs when other devices or signals disrupt this communication, leading to slow or unreliable wireless connections.

Several factors contribute to wireless interference, and identifying and mitigating these issues is crucial for maintaining a stable wireless network.

Signs of wireless interference include:

Low signal strength even when close to a WiFi broadcast device

Slower Internet connection when using connected over WiFi

Slow file transfers between computers over WiFi

Inability to pair WiFi or Bluetooth devices even when in proximity to the receiver

Intermittently dropping of WiFi connection

I. The Consequences of Interference in the Wireless Network

Slow Data Transfer: Interference can lead to a variety of Internet problems like slow data transfer rates and reduced Internet speeds, affecting productivity and user experience.

Connection Drops: Wireless interference can cause frequent disconnections or dropped connections, disrupting ongoing tasks and communication.

Unreliable Connectivity: Users may experience intermittent connectivity issues, making it challenging to access network resources consistently.

Reduced Coverage: Interference can result in reduced Wi-Fi coverage, creating dead spots where wireless signals are weak or nonexistent.

II. The Causes of Interference in the Wireless Network

Very common household items, like microwave ovens or cordless phones, can slow down your home Wi-Fi network performance. If you live in a densely populated area, your neighbors' Wi-Fi networks could actually be interfering with your own. This is particularly true if you're using a 2.4GHz wireless router.

Seeing as a failure can occur at any time, the first challenge for network administrators is to quickly identify what can cause interference as well as the precise time they occurred.

Overlapping Wi-Fi Channels: In environments with multiple Wi-Fi networks, overlapping channels can lead to interference as signals interfere with each other.

Physical Obstructions: Physical obstacles like walls, floors, and large objects can attenuate Wi-Fi signals, reducing signal strength and causing interference.

Electronic Devices: Other electronic devices operating on similar frequencies, such as cordless phones, Bluetooth devices, and microwaves, can cause interference.

Nearby Access Points: When multiple access points are in close proximity, they can interfere with each other's signals, especially if they are on the same or overlapping channels.

Signal Reflection and Refraction: Wi-Fi signals can reflect off surfaces or refract through materials, creating signal interference and dead zones.

III. How to Identify and Troubleshoot Interference in the Wireless Network

While users are usually quick enough to report problems, it's ideal to identify and solve the problem before it affects users.

Real-Time Network Monitoring: Utilize network monitoring tool, like Obkio for real-time network monitoring to track Wi-Fi performance in real-time and detect sudden drops in signal strength or connectivity issues that may indicate interference.

Wi-Fi Site Surveys: Conduct site surveys using Wi-Fi analysis tools within the network monitoring platform to identify signal strength, coverage areas, and potential interference sources.

Channel Analysis: Utilize network monitoring tools to analyze Wi-Fi channel utilization and identify crowded or overlapping channels that may be contributing to interference.

Signal Strength Testing: Measure Wi-Fi signal strength across different areas of the workspace using network monitoring tools to identify weak or strong signal zones.

Device Interference Check: Identify and isolate devices or equipment that may be causing wireless interference, using network monitoring to detect their presence and impact on Wi-Fi performance.

Automated Alerts: Set up automated network monitoring alerts within the network monitoring tool to be notified immediately when Wi-Fi interference is detected, allowing for quick investigation and resolution.

Historical Analysis: Utilize historical data provided by the network monitoring platform to identify patterns of interference and assess the effectiveness of previous troubleshooting efforts.

Network Topology Mapping: Use network monitoring tools or network observability tools to create visual representations of the network topology, helping identify potential physical obstructions or sources of interference.

By leveraging network monitoring alongside these troubleshooting approaches, businesses can proactively identify and address wireless interference, ensuring a more reliable and efficient Wi-Fi network. Network monitoring provides real-time insights, historical data, and automated alerts, empowering IT teams to promptly resolve interference issues and optimize wireless performance for enhanced user satisfaction.

New call-to-action

IV. Network Troubleshooting Scenarios for Interference in the Wireless Network

Interference in a wireless network can cause signal degradation, reduced throughput, and disconnections. Troubleshooting wireless interference requires careful analysis and mitigation strategies. Here are some network troubleshooting scenarios to consider when dealing with interference in a wireless network:

Physical Obstructions: Identify and remove or reposition physical obstructions such as walls, furniture, metal objects, or large appliances that may block or attenuate the Wi-Fi signal.

Neighboring Wi-Fi Networks: Use a Wi-Fi analyzer tool to identify nearby Wi-Fi networks and the channels they are operating on. Choose a less congested channel for your wireless network to reduce interference.

Microwave Ovens and Cordless Phones: Microwave ovens and some cordless phones operate in the same frequency range as Wi-Fi networks (2.4 GHz). Keep Wi-Fi access points away from these devices to minimize interference.

Bluetooth Devices: Bluetooth devices can cause interference with Wi-Fi networks, especially in the 2.4 GHz frequency band. Separate Bluetooth devices from Wi-Fi access points or use Wi-Fi channels that are far from Bluetooth frequencies.

Electronic Devices: Identify and relocate electronic devices that emit electromagnetic interference (EMI) or radio-frequency interference (RFI), such as baby monitors, wireless cameras, or wireless speakers.

Dual-Band Wi-Fi Devices: If possible, use dual-band Wi-Fi devices that can operate in both 2.4 GHz and 5 GHz frequency bands. The 5 GHz band is typically less congested and offers better performance.

Wi-Fi Signal Strength: Check the Wi-Fi signal strength at different locations within the coverage area to identify areas with weak signals that might be susceptible to interference.

Wi-Fi Access Point Placement: Optimize the placement of Wi-Fi access points to achieve better coverage and reduce dead zones. Consider using Wi-Fi range extenders or mesh systems for larger areas.

Wi-Fi Signal Overlapping: Avoid overlapping Wi-Fi signal coverage from multiple access points, as it can lead to interference. Adjust access point transmit power or channel settings to minimize overlap.

Rogue Wi-Fi Devices: Look for rogue Wi-Fi access points or devices that might be interfering with your network. Use wireless intrusion detection systems (WIDS) to identify unauthorized devices.

DFS Channels (5 GHz): In the 5 GHz band, some channels require Dynamic Frequency Selection (DFS) due to radar detection requirements. Ensure your devices support DFS and are using appropriate DFS channels.

WLAN Optimization: Use Wi-Fi optimization techniques such as band steering and airtime fairness to balance client connections and reduce interference.

Wireless Site Survey: Perform a wireless site survey to assess the overall wireless environment and identify potential sources of interference.

Quality of Service (QoS): Implement QoS policies to prioritize critical Wi-Fi traffic and minimize the impact of non-essential traffic on network performance.

Regular Monitoring: Continuously monitor Wi-Fi performance, interference levels, and client connectivity to detect and address issues proactively.

Firmware Updates: Keep Wi-Fi access points and wireless devices' firmware up to date to take advantage of performance improvements and bug fixes.

By systematically troubleshooting wireless interference, you can optimize your Wi-Fi network's performance and deliver a more reliable wireless experience to users. Use appropriate network monitoring and diagnostic tools, like we mentioned in the section above, to analyze Wi-Fi performance and make informed decisions during the troubleshooting process.

Network Problem #8. Network Congestion

Network congestion is a prevalent network problem that occurs when there is an excessive amount of data traffic on the network, leading to congestion or bottlenecks. It can happen at various points in the network, such as routers, switches, or network links, where the capacity to handle data becomes overwhelmed by the volume of incoming traffic.

Network congestion can result from increased data demands, inefficient network configurations, or inadequate bandwidth allocation, and it can significantly impact the overall network performance and user experience.



Packet Loss - Common Network Problems

I. The Consequences of Network Congestion

Network congestion can have severe ramifications on network performance and user experience. Let's go over the impact of congestion, including:

Slow Data Transfer: Network congestion can result in slower data transfer rates, leading to delays in accessing resources and data.

Latency and Packet Loss: Congestion can cause increased latency (delays) and packet loss, affecting real-time applications such as video conferencing or online gaming.

Dropped Connections: Congestion can cause connections to drop or time out, resulting in failed file transfers or disrupted communication.

Reduced Productivity: Sluggish network performance can hinder productivity, as users may experience delays in performing critical tasks.

User Frustration: Network congestion can lead to frustration among users due to the inability to access resources or slow response times.

II. The Causes of Network Congestion

Understanding the root causes of network congestion is vital for devising appropriate solutions. Let's go over the most common causes of network congestion in more detail:

Increased Data Traffic: As the number of connected devices and users on the network grows, the demand for data transfer increases, leading to congestion.

Bandwidth Limitations: Insufficient available bandwidth can cause congestion, especially in networks with limited capacity or where data-intensive applications dominate.

Network Misconfigurations: Inefficient network configurations, such as incorrect Quality of Service (QoS) settings or improper routing, can lead to inefficient data flow and congestion.

DDoS Attacks: Distributed Denial of Service (DDoS) attacks involve overwhelming a network with an enormous amount of traffic, causing congestion and rendering services unavailable.

Software and Firmware Bugs: Network devices with software or firmware bugs can behave unpredictably, potentially contributing to network congestion.

III. How to Identify and Address Network Congestion

To mitigate network congestion, early detection and appropriate measures are essential.

Network Monitoring: Use network monitoring tools like Obkio to track network performance metrics, including bandwidth utilization and traffic patterns. Identify periods of high traffic and potential congestion.

Traffic Analysis: Analyze the type of data traffic and its volume to identify bandwidth-intensive applications or devices causing congestion.

Quality of Service (QoS) Implementation: Implement QoS policies to prioritize critical applications and services over less essential ones during periods of congestion.

Bandwidth Upgrades: Consider upgrading network bandwidth to accommodate increasing data demands and alleviate congestion.

Load Balancing: Utilize network load balancing techniques to distribute network traffic across multiple routes or devices, preventing bottlenecks in specific areas.

Traffic Shaping: Implement traffic shaping to control the flow of data, ensuring fair distribution of bandwidth among different applications or users.

Network Optimization: Regularly review network configurations and performance to identify areas for network optimization and improvement.

By proactively identifying and addressing network congestion, businesses can ensure a smoother and more responsive network, enhancing productivity and user

satisfaction. Network congestion management plays a crucial role in maintaining a reliable and efficient network infrastructure that meets the growing demands of modern businesses.

How to Detect Network Congestion Like A Pro: Don't Get Jammed Up

How to Detect Network Congestion Like A Pro

Learn how to detect network congestion & perform a network congestion test inside & outside your network with Network Monitoring & Network Device Monitoring.

Learn more [right arrow](#)

IV. Network Troubleshooting Scenarios for Network Congestion

Network congestion occurs when the network experiences high levels of traffic, causing slow data transmission, increased latency, and potential service disruptions. Here are some network troubleshooting scenarios to consider when dealing with network congestion:

Identify Peak Usage Hours: Monitor network traffic to identify peak usage hours when congestion is most likely to occur. Plan for additional resources during these periods.

Bandwidth Monitoring: Use network monitoring tools with SNMP Network Monitoring to track bandwidth usage and identify which applications or devices are consuming the most bandwidth.

Quality of Service (QoS): Implement QoS policies to prioritize critical traffic, such as VoIP or video conferencing, over non-essential traffic during periods of congestion. QoS for VoIP is essential for mitigation congestion.

Malware or Botnet Activity: Malware-infected devices or botnet activity can cause excessive traffic and contribute to network congestion. Use security tools to detect and isolate infected devices.

Cloud Services and Backups: Cloud services and data backups can consume significant bandwidth. Schedule backups during off-peak hours to avoid congestion.

Check Network Switches and Routers: Check network devices for errors or signs of packet drops. Upgrade hardware if required to handle increased traffic.

Analyze Network Topology: Review the network topology to identify potential bottlenecks or areas of contention.

Segment Network Traffic: Separate different types of traffic, such as voice, data, and video, into separate VLANs to reduce contention.

Update Firmware and Drivers: Keep network devices' firmware and drivers up to date to ensure optimal performance.

Optimize Protocols: Fine-tune network protocols to reduce overhead and improve efficiency.

Load Balancing: Distribute traffic across multiple links or paths using load balancing techniques.

Consider Network Upgrades: If congestion is chronic and impacting productivity, consider upgrading network infrastructure, such as increasing bandwidth or using faster network technologies.

Monitor Network Flow: Use flow analysis tools to understand traffic patterns and identify potential sources of congestion.

Implement Caching: Use caching solutions for frequently accessed content to reduce the need for repetitive data transfers.

Throttle Bandwidth-Intensive Applications: Limit the bandwidth usage of certain applications or devices that are causing congestion.

Review ISP Performance: If the congestion is beyond your local network, contact your Internet Service Provider (ISP) to assess the overall network performance.

Peer-to-Peer (P2P) Traffic Control: Implement policies to control and prioritize P2P traffic, which can consume a significant amount of bandwidth.

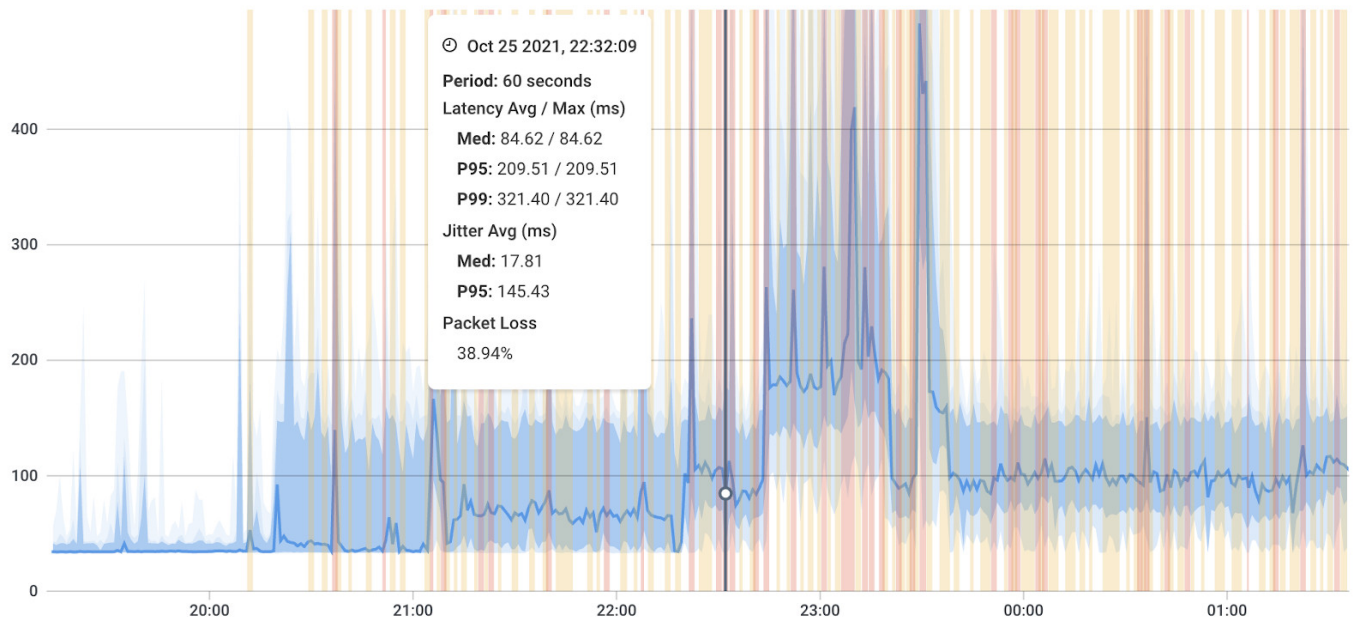
Educate Users: Educate users about responsible internet usage and the impact of excessive data consumption on network performance.

By thoroughly troubleshooting network congestion, you can identify the root causes and implement appropriate solutions to improve overall network performance and user experience. Regular monitoring and analysis of network traffic patterns will help you proactively address congestion issues before they become significant problems.

Network Problem #9. Packet Loss

Packet loss is a prevalent network problem characterized by the failure of data packets to reach their intended destination within a network. It occurs when one or more packets of data are lost or discarded during transmission, leading to incomplete or corrupted data delivery.

Packet loss can happen due to various factors, such as network congestion, hardware issues, or data transmission errors, and it can significantly impact network performance and user experience.



Packet Loss - Common Network Problems

In the same family of network issues, you may also encounter:

Packet Reordering: When network packets arrive at their destination out of sequence

Packet Duplication: The unintended replication of data packets during transmission. When packets are duplicated, multiple identical copies of the same packet are delivered to the destination.

I. The Consequences of Packet Loss

Data Corruption: Packet loss can lead to incomplete or corrupted data transmissions, affecting the accuracy and integrity of transmitted information.

Slow Data Transfer: Retransmitting lost packets can slow down data transfer rates, leading to increased latency.

Degraded Voice and Video Quality: In real-time communication applications like VoIP and video conferencing, packet loss can result in choppy audio or pixelated video.

Reduced Throughput: The loss of packets in data streams can reduce the overall throughput and efficiency of data delivery.

Impact on Applications: Packet loss can negatively affect the performance of applications, leading to slower response times and disrupted services.

II. The Causes of Packet Loss

Network Congestion: High levels of data traffic or network congestion can result in packets being dropped to alleviate the strain on the network.

Network Jitter: Variations in packet delay, known as jitter, can lead to packet loss when packets arrive out of order or too late to be processed.

Buffer Overflow: When network devices' buffers become overwhelmed due to high data rates, excess packets can be discarded.

Data Transmission Errors: Errors during data transmission can cause packets to be corrupted or lost, especially in unreliable transmission mediums.

Wireless Interference: Interference from other wireless signals or physical obstacles can lead to packet loss in Wi-Fi networks.

Network Hardware Issues: Faulty network switches, routers, or other hardware can cause packet loss as packets fail to traverse the network correctly.

III. How to Identify & Troubleshoot Packet Loss

Network Monitoring: Utilize network monitoring tools like Obkio to measure packet loss and track packet loss rates and identify periods of increased packet loss.

Packet Analysis: Conduct packet analysis to identify the root causes of packet loss and determine the affected network segments.

Bandwidth Optimization: Optimize bandwidth allocation and implement Quality of Service (QoS) to prioritize critical traffic and reduce packet loss.

Jitter Control: Minimize network jitter through QoS and traffic shaping to prevent packet loss due to variations in packet delay.

Network Hardware Inspection: Inspect network hardware to identify and replace faulty devices contributing to packet loss.


Wireless Signal Optimization: Optimize Wi-Fi signals to reduce wireless interference and decrease packet loss in wireless networks.

By proactively identifying and addressing packet loss, businesses can improve network performance, maintain data integrity, and enhance the overall user experience. Network monitoring, packet analysis, and appropriate network optimization techniques play a vital role in detecting and mitigating packet loss issues effectively.

How to Measure Packet Loss & Detect Packet Loss Issues

How to Measure Packet Loss & Detect Packet Loss Issues

How to measure packet loss with Obkio's Network & Packet Loss Monitoring tool. Check for packet loss in your network & read packet loss measurements.

Learn more 

IV. Network Troubleshooting Scenarios for Packet Loss

Packet loss can degrade network performance and cause disruptions in data transmission. Troubleshooting packet loss requires identifying the underlying causes and implementing appropriate solutions. Here are some network troubleshooting scenarios to consider when dealing with packet loss:

Ping and Traceroute: Use ping and traceroute commands to identify packet loss and latency issues between devices. This can help pinpoint the location and severity of packet loss.

Check Network Cables: Inspect network cables and connectors for damage, loose connections, or faulty wiring that could lead to packet loss.

Verify Network Interface Cards (NICs): Test and update network interface card drivers to ensure they are functioning correctly.

Physical Layer Troubleshooting: Examine physical network components, such as switches and routers, for signs of hardware issues or congestion.

Bandwidth Saturation: Monitor network traffic to see if bandwidth saturation is causing packet loss. Consider implementing Quality of Service (QoS) policies to prioritize critical traffic.

Check for Network Congestion: Analyze network traffic patterns to identify areas of congestion that may be causing packet loss.

Wireless Interference: In wireless networks, interference from neighboring Wi-Fi networks or other devices can lead to packet loss. Use a Wi-Fi analyzer to identify potential sources of interference.

Reduce MTU Size: If you are experiencing fragmentation-related packet loss, reduce the Maximum Transmission Unit (MTU) size to prevent fragmentation.

Jitter and Buffering: Examine network devices for excessive jitter or inadequate buffering that can contribute to packet loss.

Routing Issues: Verify routing configurations to ensure packets are being routed correctly without any loops or misconfigurations.

Firewall Settings: Check firewall rules to ensure they are not blocking legitimate traffic and causing packet loss.

Malware and DDoS Attacks: Monitor for signs of malware infections or Distributed Denial of Service (DDoS) attacks, as they can cause packet loss.

ISP Issues: If the packet loss is beyond your local network, contact your Internet Service Provider (ISP) to investigate potential problems with their network.

Buffer Bloat: Address buffer bloat issues by configuring QoS and traffic shaping to manage buffer size and prevent excessive queuing delay.

Ping Flood or DDoS Testing: If you suspect malicious activities, investigate for possible ping flood or DDoS testing targeting your network.

Update Firmware and Software: Keep network devices' firmware and software up to date to prevent known issues causing packet loss.

Trunk Port Errors: For VLANs and trunk ports, check for misconfigurations or errors that might cause packet loss.

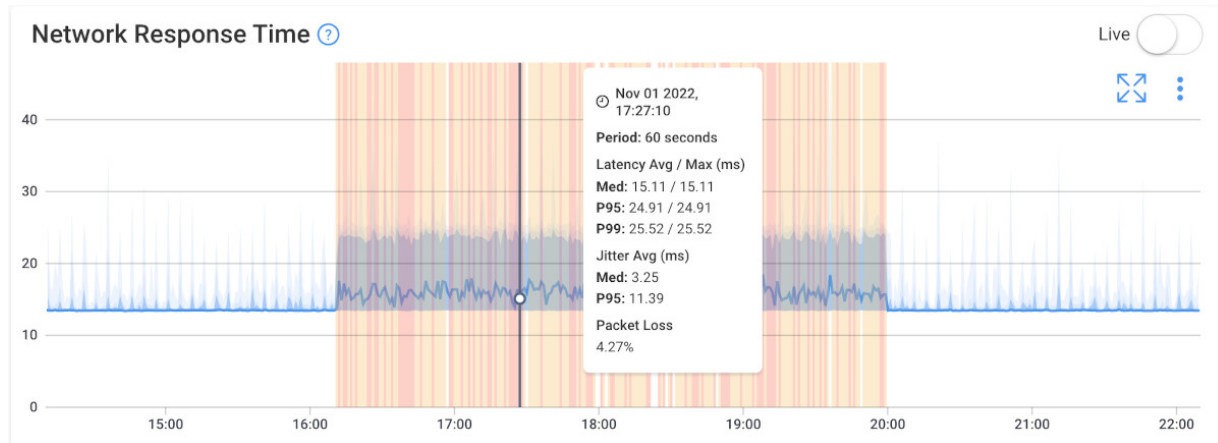
Segment and Isolate Network Traffic: Use VLANs and subnetting to isolate different types of network traffic and prevent congestion-related packet loss.

By methodically troubleshooting packet loss, you can identify the root causes and apply appropriate solutions to improve network performance and reliability.

Network Problem #10. Jitter

Jitter is a common network problem that refers to the variation in packet delay experienced during data transmission over a network. It occurs when data packets encounter fluctuations in the time it takes to traverse the network from the source to the destination.

Jitter is particularly relevant in real-time communication applications, such as Voice over Internet Protocol (VoIP) calls and video conferencing, where timing precision is crucial for smooth and seamless communication.



Jitter - Common Network Problems

I. The Consequences of Jitter

Voice and Video Quality Issues: In real-time communication applications like VoIP and video conferencing, excessive jitter can cause choppy audio or video, affecting the overall call quality.

Delayed Data Transmission: Jitter can lead to variations in data transmission delays, impacting the responsiveness of applications and services.

Synchronization Problems: For time-sensitive applications, jitter can cause synchronization issues between data packets, leading to data corruption or loss.

Interference with Real-Time Applications: Jitter can disrupt the flow of real-time data, making it challenging to maintain a smooth user experience.

II. The Causes of Jitter

Network Congestion: High levels of data traffic or network congestion can lead to varying packet queuing times and result in jitter.

Packet Routing: Different paths and routing delays taken by packets can cause varying arrival times at the destination.

Network Jitter: Variations in network jitter itself can compound the issue, leading to additional packet timing discrepancies.

Network Interference: Physical obstacles, wireless interference, or other external factors can introduce varying transmission delays.

Buffering: Buffering in network devices can introduce variations in packet arrival times due to the varying lengths of packets.

III. How to Identify & Troubleshoot Jitter

Network Monitoring: Use network monitoring tools like Obkio to measure jitter levels and identify periods of increased jitter. Obkio will also help you identify the cause, source and time of jitter spikes in your network so you know where and how to direct your troubleshooting efforts.

Quality of Service (QoS) Implementation: Implement QoS policies to prioritize real-time traffic, reducing the impact of jitter on critical applications.

Buffer Management: Optimize buffer settings in network devices to minimize the effects of buffering-induced jitter.

Traffic Shaping: Use traffic shaping techniques to regulate the flow of data and manage jitter more effectively.

Path Optimization: Optimize network paths to minimize variations in packet routing and reduce jitter.

Wireless Signal Optimization: In wireless networks, optimize Wi-Fi signals to reduce interference and decrease jitter.

By proactively identifying and addressing jitter, businesses can improve the performance of real-time communication applications, ensuring smooth voice and video calls, and enhancing the overall user experience. Network monitoring, QoS implementation, and network optimization play a crucial role in detecting and mitigating jitter effectively.

How to Measure Jitter & Keep Your Network Jitterbug Free

How to Measure Jitter & Keep Your Network Jitterbug Free

Learn how to measure network jitter using Obkio's Network Monitoring software to identify network problems & collect data to troubleshoot.

Learn more 

IV. Network Troubleshooting Scenarios for Jitter

Jitter is the variation in the delay of packet delivery in a network, which can lead to inconsistent and unpredictable performance. Troubleshooting jitter involves identifying the causes of delay variations and implementing measures to mitigate its impact. Here are some network troubleshooting scenarios to consider when dealing with jitter:

Ping and Traceroute: Use ping and traceroute commands to measure latency and identify potential variations in packet delivery times.

Check Network Utilization: High network utilization can contribute to jitter. Monitor network traffic to identify congestion points and take appropriate actions to alleviate it.

Quality of Service (QoS): Implement QoS policies to prioritize real-time traffic, such as VoIP and video conferencing, over non-time-sensitive traffic to reduce jitter.

Buffer Bloat: Buffer bloat occurs when excessively large buffers cause delays in packet delivery. Adjust buffer sizes on routers and switches to manage latency.

Packet Loss: Packet loss can exacerbate jitter. Address any packet loss issues, as it may lead to increased jitter levels.

Wireless Interference: In wireless networks, interference from other devices or neighboring networks can cause jitter. Use a Wi-Fi analyzer to identify sources of interference.

Network Congestion: Congestion on the network can lead to increased jitter. Identify and resolve congestion points to minimize its impact.

Physical Layer Issues: Inspect network cables and connectors for damage or faults that may cause delays in packet delivery.

Network Switches and Routers: Verify the performance of network switches and routers, as hardware issues can contribute to jitter.

Jitter Buffer: For real-time applications, such as VoIP, ensure that jitter buffer settings are appropriately configured to compensate for jitter.

Traffic Shaping: Use traffic shaping techniques to control the flow of traffic and prevent sudden bursts of data that may cause jitter.

Power Management: Disable power-saving features on network devices that may introduce latency variations.

Proper Synchronization: Ensure that clocks are synchronized across network devices to prevent timing discrepancies that contribute to jitter.

VoIP Codecs: For VoIP systems, consider using different codecs that are less sensitive to network jitter.

Update Firmware and Software: Keep network devices' firmware and software up to date to address known issues related to jitter.

ISP Performance: If jitter is beyond your local network, contact your Internet Service Provider (ISP) to assess and address potential issues on their network.

Monitor Network Performance: Continuously monitor network performance to identify patterns of jitter and take proactive measures to improve and check network stability.

Use Network Diagnostic Tools: Employ network diagnostic tools to analyze jitter levels and identify sources of delay variations.

By systematically troubleshooting jitter, you can identify the underlying causes and apply appropriate solutions to improve network performance and deliver a smoother experience for real-time applications.

Network Problem #11. Routing Problems

Routing problems are a common network issue that occurs when data packets are unable to reach their intended destination due to incorrect or inefficient routing decisions. Routing is the process of determining the best path for data to travel from the source to the destination across a network.

When routing problems arise, data packets may take suboptimal paths, experience delays, or even get lost, leading to disruptions in network communication and performance.

I. The Consequences of Routing Problems

Slow Data Transfer: Routing problems can lead to longer data transmission times, causing delays in accessing resources and services.

Packet Loss: Incorrect routing decisions can cause packets to be lost or dropped during transmission, affecting data integrity.

Network Inefficiency: Routing problems can lead to inefficient use of network resources, increasing network latency and reducing overall performance.

Disruptions in Communication: Critical services and applications may become unavailable or experience disruptions due to routing problems.

II. The Causes of Routing Problems

Misconfigurations: Incorrect configuration of routing protocols or routing tables can lead to suboptimal or incorrect routing decisions.

Network Congestion: High levels of network congestion can cause routers to make suboptimal routing choices, leading to delays and packet loss.

Link Failures: When a link between network devices fails, routers may need to reroute traffic, and if this process is not seamless, routing problems can occur.

BGP (Border Gateway Protocol) Issues: In large-scale networks, BGP misconfigurations or route flapping can cause routing problems and instability.

Inadequate Bandwidth: Insufficient bandwidth on certain links can cause congestion and result in suboptimal routing decisions.

III. How to Identify & Troubleshoot Routing Problems

Network Monitoring: Use network monitoring tools like Obkio to track routing metrics and identify anomalies or fluctuations in routing behavior.

Routing Protocol Analysis: Analyze the configuration of routing protocols and routing tables to identify misconfigurations or inconsistencies.

Route Flap Damping: In BGP environments, enable route flap damping to mitigate the impact of unstable routes.

Bandwidth Upgrades: Consider upgrading network links with inadequate bandwidth to alleviate congestion and improve routing efficiency.

Link Redundancy: Implement link redundancy and dynamic routing protocols to ensure seamless failover in case of link failures.

Regular Audits: Conduct regular audits of network configurations and routing tables to identify and rectify potential issues.

By proactively identifying and addressing routing problems, businesses can maintain a more efficient and reliable network infrastructure. Network monitoring, analysis of routing protocols, and proper network configuration play a vital role in detecting and resolving routing problems promptly. This ensures smooth and seamless data transmission, optimizing network performance and user experience.

IV. Network Troubleshooting Scenarios for Routing Problems

Routing problems can lead to communication issues between network devices and services. Troubleshooting routing problems requires careful analysis of the routing configuration and associated network components. Here are some network troubleshooting scenarios to consider when dealing with routing problems:

Ping and Traceroute: Use ping and traceroute commands to verify connectivity between devices and identify potential routing issues.

Routing Table Verification: Check the routing tables on routers and switches to ensure they are correctly configured and have the appropriate routes.

Routing Protocol Issues: If dynamic routing protocols are used, verify the protocol configurations and adjacencies between neighboring routers.

Default Gateway: Confirm that devices have the correct default gateway configured, which is critical for forwarding traffic to external networks.

Routing Loops: Check for routing loops in the network, which can cause packets to circulate indefinitely. Correct any misconfigurations causing loops.

Routing Redistribution: If multiple routing protocols are in use, check for proper redistribution to ensure that routes are distributed correctly.

Static Routes: Verify that any static routes are accurate and up-to-date, especially if they are used to override dynamic routing protocols.

Routing Metrics: Review routing metrics to ensure they are set appropriately, as improper metrics can lead to suboptimal routing decisions.

Routing Blackholes: Look for cases where routing paths unexpectedly drop packets (routing blackholes) and investigate the cause.

Network Topology Changes: If recent network topology changes have occurred, verify that routing configurations were updated accordingly.

Routing Protocol Authentication: Check if routing protocol authentication is enabled and configured correctly to prevent unauthorized routing updates.

Split Horizon: For networks using split horizon, ensure that the split horizon rule is properly applied to prevent routing information loops.

Routing Protocol Timers: Examine routing protocol timers to ensure they are set appropriately for the network environment.

Network Segmentation: Confirm that network segmentation is accurate and logical, and routes are correctly configured between segments.

Router Interface Status: Verify that router interfaces are operational and have the correct IP addressing and subnet masks.

Physical Connectivity: Check for physical connectivity issues that may prevent proper routing information exchange.

Backup Routes: If using backup or redundant routes, validate their configurations and failover mechanisms.

Update Firmware and Software: Keep router and switch firmware/software up to date to address known issues related to routing.

Monitor Routing Changes: Continuously monitor routing tables and log any changes to quickly identify and address unexpected alterations.

By methodically troubleshooting routing problems, you can identify and resolve issues that may be disrupting communication in the network. Regular network monitoring, like we mentioned in the previous section, thorough analysis of routing configurations, and prompt resolution of routing-related errors will help ensure smooth and reliable network operation. If the issue persists or is beyond your expertise, seek assistance from qualified network administrators or engage with vendor support.

Network Problem #12. VoIP Call Quality Issues

VoIP (Voice over Internet Protocol) call quality issues are a common network problem that affects the clarity and reliability of voice communications over the Internet.

VoIP enables real-time voice communication using the internet as the transport medium. However, various factors within the network environment can lead to degraded call quality, causing disruptions, echoes, or delays in voice conversations.



VoIP Issues - Common Network Problems

I. The Consequences of VoIP Call Quality Issues

Poor Call Clarity: VoIP call quality issues can result in poor audio quality, making it challenging to understand and communicate effectively.

Dropped Calls: Frequent call dropouts or disconnects due to packet loss or network issues can hinder communication.

Communication Delays: High latency can lead to noticeable delays in conversations, causing awkward pauses and communication difficulties.

Unreliable Communication: Call quality problems can lead to unreliable communication experiences, affecting business operations and customer service.

II. The Causes of VoIP Call Quality Issues:

Network Congestion: High data traffic and network congestion can lead to delayed or lost VoIP packets, resulting in poor call quality.

Jitter: Variations in packet delay, known as jitter, can cause voice packets to arrive out of order, resulting in choppy or distorted audio during calls.

Packet Loss: Packet loss occurs when VoIP packets fail to reach their destination, leading to gaps or dropouts in the conversation.

Latency: Latency, the delay between sending and receiving data, can lead to noticeable delays and interruptions in VoIP calls.

Insufficient Bandwidth: Inadequate bandwidth can restrict the amount of data that can be transmitted, leading to reduced call quality.

Network Interference: Interference from other devices or signals can impact VoIP calls, especially in wireless environments.

How to Identify & Troubleshoot VoIP Call Quality Issues

Network Monitoring: Use network monitoring tools like Obkio to measure VoIP quality metrics, such as MOS score, jitter, packet loss, and latency and identify issues affecting VoIP Quality right on the VoIP Quality graph.

QoS Implementation: Implement Quality of Service (QoS) policies to prioritize VoIP traffic and minimize the impact of other data traffic on call quality.

Bandwidth Allocation: Ensure sufficient bandwidth is allocated to VoIP traffic to avoid congestion and call quality issues.

Traffic Shaping: Utilize traffic shaping techniques to regulate data flow and prioritize VoIP packets.

Jitter Buffer Optimization: Optimize jitter buffer settings to compensate for jitter and ensure smoother audio playback.

Network Upgrades: Consider upgrading network infrastructure to handle increased VoIP traffic and improve call quality.

By proactively identifying and addressing VoIP call quality issues, businesses can ensure clear and reliable voice communication, improving collaboration and customer interactions. Network monitoring, QoS implementation, and network optimization are essential in detecting and mitigating VoIP call quality issues, enhancing overall communication experiences within the organization.

How to Measure VoIP Quality & MOS Score (Mean Opinion Score)

How to Measure VoIP Quality & MOS Score (Mean Opinion Score)

Learn how to measure VoIP Quality using MOS Score (Mean Opinion Score) & Obkio's VoIP monitoring solution to identify poor VoIP Quality issues & dropped calls.

Learn more 

IV. Network Troubleshooting Scenarios for VoIP Call Quality Issues

VoIP (Voice over Internet Protocol) call quality issues can negatively impact communication and user experience. Troubleshooting VoIP call quality issues requires identifying and resolving factors that affect voice transmission over the network. Here are some network troubleshooting scenarios to consider when dealing with VoIP call quality issues:

Check Bandwidth and Network Utilization: Insufficient bandwidth or high network utilization can lead to call quality degradation. Monitor network traffic and ensure sufficient bandwidth is available for VoIP traffic.

Quality of Service (QoS): Implement QoS policies to prioritize VoIP traffic over other types of data to ensure smooth transmission and reduced latency.

Ping and Jitter: Measure ping and jitter between endpoints to identify potential latency and jitter issues affecting call quality.

Packet Loss: Monitor for packet loss, which can significantly impact call quality. Address any packet loss issues on the network.

Buffer Bloat: Buffer bloat can introduce latency in the network. Optimize buffer sizes to prevent excessive delays in packet transmission.

Codecs: Check the codecs used for VoIP calls. Some codecs may prioritize bandwidth savings over call quality. Consider using codecs that offer better voice quality.

Network Congestion: Analyze network congestion points and address them to reduce the impact on VoIP call quality.

Network Equipment: Verify the performance of network switches and routers, as hardware issues can contribute to call quality problems.

Wireless Interference: In wireless networks, interference from neighboring Wi-Fi networks or other devices can affect VoIP call quality. Use a Wi-Fi analyzer to identify sources of interference.

Check for Dropped Packets: Identify and address any dropped packets affecting call quality.

VoIP Gateway Configuration: Verify the configuration of VoIP gateways and devices to ensure they are set correctly for the network environment.

Codec Mismatch: Ensure that both ends of the call are using compatible codecs. A codec mismatch can lead to poor call quality.

Router Configuration: Review router configurations for issues that may affect VoIP call quality, such as Access Control Lists (ACLs) or firewall settings.

Router Firmware Updates: Keep router firmware up to date to address known issues related to VoIP call quality.

SIP Trunk and Provider Issues: If using SIP trunks or a VoIP service provider, check for any issues with their service that may be affecting call quality.

Jitter Buffer Settings: Adjust jitter buffer settings to optimize the handling of packet variations and reduce jitter-related issues.

Network Monitoring: Continuously monitor network performance to detect any patterns of call quality degradation and identify the causes. Network monitoring tools with VoIP monitoring, like Obkio, are especially important for identifying VoIP Quality issues.

Network Latency: Address any latency issues in the network that may affect VoIP call quality.

ISP Performance: If VoIP call quality issues persist, contact your Internet Service Provider (ISP) to assess and address potential network problems.

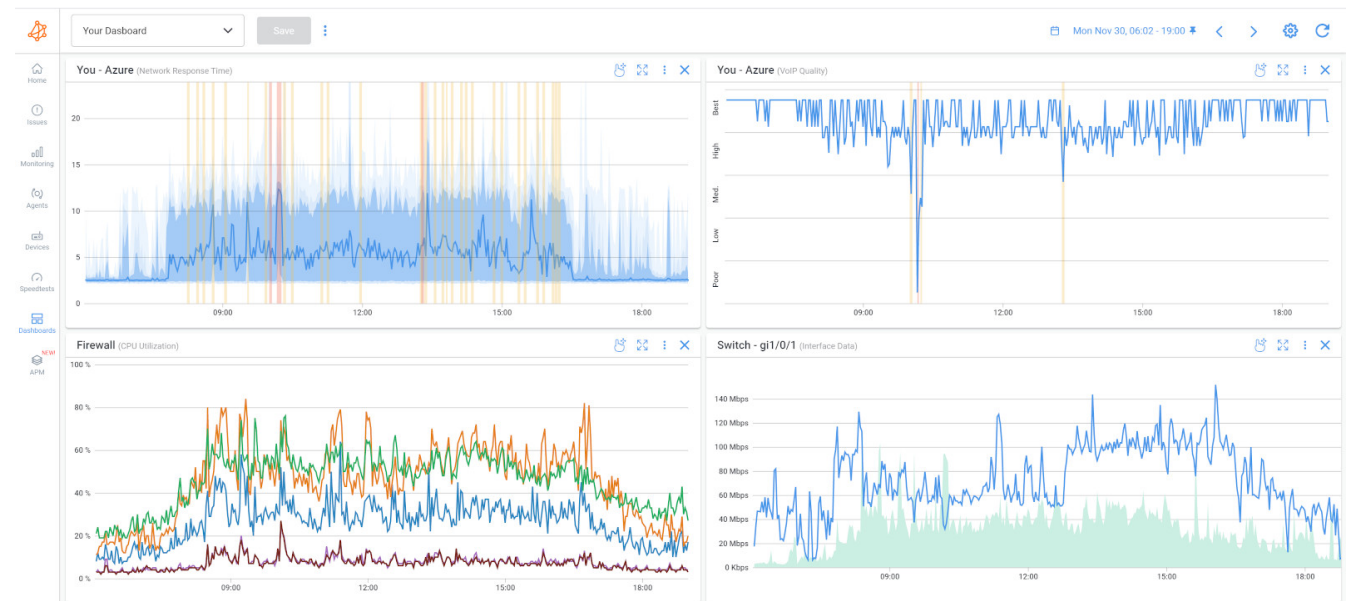
By methodically troubleshooting VoIP call quality issues, you can identify and resolve factors impacting call quality, leading to improved voice communication over the

network. Regular network monitoring and analysis will help you proactively detect and address VoIP call quality issues as they arise.

Network Problem #13. Network Device Failures

Network device failures are a common and potentially disruptive network problem that occurs when essential network devices, such as routers, switches, firewalls, or access points, stop functioning correctly.

Network devices play a crucial role in data transmission, routing, and security within a network infrastructure. When one of these devices fails, it can lead to service disruptions, connectivity issues, and downtime.



Network Device Failures - Common Network Problems

I. The Consequences of Network Device Failures

Network Downtime: When critical network devices fail, it can lead to network downtime and service interruptions.

Connectivity Issues: Failures in routers, switches, or access points can disrupt network connectivity, affecting communication and data transfer.

Security Vulnerabilities: Failed security devices like firewalls can expose the network to potential security breaches and unauthorized access. **Data Loss:** Network device failures can lead to data loss, especially if devices were responsible for data storage or backup.

II. The Causes of Network Device Failures

Hardware Malfunctions: Network devices can experience hardware failures due to wear and tear, overheating, power surges, or manufacturing defects.

Firmware or Software Errors: Faulty firmware or software updates can cause network devices to behave unpredictably or fail.

Configuration Errors: Incorrect or misconfigured settings in network devices can lead to malfunctions or instability.

Environmental Factors: Environmental conditions, such as exposure to extreme temperatures, humidity, or dust, can impact the reliability of network devices.

III. How to Identify & Troubleshoot Network Device Failures

Network Monitoring: Use network monitoring tools like Obkio, along with Obkio's Network Device Monitoring feature to continuously monitor the health and performance of core network devices to identify device availability, resource and performance issues.

Device Health Checks: Perform regular health checks on network devices to identify early signs of potential failures or abnormalities.

Firmware and Software Updates: Keep network device firmware and software up to date with the latest stable releases to minimize potential issues.

Configuration Backups: Regularly back up the configuration settings of network devices to facilitate quick recovery in case of failures.

Redundancy and Failover: Implement redundancy and failover mechanisms to ensure network continuity in the event of device failures.

Hardware Maintenance: Regularly inspect and maintain network devices to address any physical issues and ensure proper functioning.

By proactively monitoring and maintaining network devices, businesses can reduce the risk of network disruptions caused by device failures. Quick identification and timely resolution of network device failures play a crucial role in minimizing downtime, improving network reliability, and ensuring seamless communication and data transfer.

Mastering the Art of Network Device Monitoring: A Beginner's Guide

Mastering the Art of Network Device Monitoring

Learn about Network Device Monitoring to easily monitor performance of firewalls, routers & switches to identify problems like high CPU & bandwidth usage.

Learn more 

IV. Network Troubleshooting Scenarios for Network Device Failures

Network device failures can disrupt network communication and lead to service outages. Troubleshooting network device failures requires a systematic approach to identify the failing device and address the issue promptly. Here are some network troubleshooting scenarios to consider when dealing with network device failures:

Physical Inspection: Perform a physical inspection of the device to check for any visible signs of damage, loose connections, or hardware failures.

Power Cycle: Power cycle the device by turning it off and then back on. Sometimes, a simple reboot can resolve temporary issues.

Check Power and Power Supply: Verify that the device is receiving power and that the power supply is functioning correctly.

Check Device LEDs: Observe the status lights or LEDs on the device to identify any error codes or abnormal behavior.

Device Logs: Analyze the device logs for error messages or alerts that might indicate the cause of the failure.

Test Connectivity: Test connectivity to and from the device to see if it is responsive or if it is completely unreachable.

Replace Network Cables: If applicable, try replacing the network cables connecting the device to the network.

Isolate the Failing Device: If possible, isolate the failing device from the network to prevent it from causing further disruptions.

Swapping Redundant Components: If the device has redundant components (e.g., power supplies, interface cards), try swapping them with spare parts to see if it resolves the issue.

Verify Firmware/Software Versions: Ensure that the device's firmware or software is up to date. Apply the latest firmware updates or patches from the manufacturer's website.

Temperature and Ventilation: Overheating can cause devices to fail. Ensure that the device has adequate ventilation and is not exposed to excessive heat.

Check for Environmental Factors: Determine if the device failure could be caused by environmental factors such as power fluctuations or temperature variations.

Backup and Restore Configurations: If the device can be replaced, backup its configuration and restore it on the replacement device to minimize downtime.

RMA or Warranty: If the device is under warranty or support contract, contact the vendor for a possible replacement or repair.

Identify the Impact: Assess the impact of the failed device on the network and affected services.

Redundancy and Failover: Review the network design to ensure proper redundancy and failover mechanisms are in place to handle device failures.

Replacement and Spare Parts: Keep spare devices or critical components on hand to quickly replace failed devices when needed.

Document the Failure: Document all the troubleshooting steps, actions taken, and the resolution for future reference.

By following a systematic troubleshooting approach, you can quickly identify the failing device and take appropriate steps to address the issue, minimizing network downtime and ensuring smooth network operation. If the issue is beyond your expertise, seek assistance from qualified network technicians or engage with vendor support for further assistance.

Network Problem #14. VPN Connectivity Problems

VPN (Virtual Private Network) connectivity issues are a common network problem that can hinder remote workers or branch offices from securely accessing the corporate network. VPNs create encrypted tunnels over the public internet, allowing users to access internal resources and services as if they were directly connected to the corporate network.

However, various factors can lead to connectivity problems, preventing users from establishing or maintaining a stable VPN connection.

I. The Consequences of VPN Connectivity Issues

Limited Remote Access: VPN connectivity issues can restrict remote workers' access to critical resources and data.

Reduced Productivity: Users may experience delays or interruptions in their work due to VPN connection failures.

Security Risks: VPN connectivity problems can prompt users to seek alternative and potentially insecure ways to access corporate resources.

II. The Causes of VPN Connectivity Issues

Network Congestion: High levels of data traffic or network congestion can impact VPN performance and lead to connectivity problems.

Firewall or Security Settings: Misconfigured firewalls or security settings can block VPN traffic, preventing successful connections.

VPN Server Overload: An overloaded VPN server can struggle to handle incoming connection requests, leading to connection failures.

Client Software Conflicts: Interference from other software or settings on the client device can cause VPN connectivity issues.

Internet Connection Instability: Unstable or unreliable internet connections can disrupt VPN connections.

VPN Protocol Issues: Compatibility issues between VPN protocols and devices can lead to connection problems.

III. How to Identify & Troubleshoot VPN Connectivity Issues

Network Monitoring: Use network monitoring tools like Obkio to track VPN connectivity metrics and identify potential issues. Obkio has remote network monitoring features, which is especially important for monitoring remote workers connectivity towards VPNs.

Firewall and Security Configuration: Review and adjust firewall settings to ensure VPN traffic is permitted and secure.

VPN Server Load Balancing: Implement load balancing for VPN servers to distribute connection requests evenly and avoid network overload.

VPN Client Troubleshooting: Troubleshoot VPN client software on user devices to identify and resolve conflicts or configuration issues.

Internet Connection Stability: Address internet connection problems on user devices to ensure a stable VPN connection.

VPN Protocol Selection: Choose appropriate VPN protocols based on device compatibility and network requirements.

By proactively monitoring and troubleshooting VPN connectivity issues, businesses can ensure remote workers have reliable access to corporate resources. Network monitoring, VPN server optimization, and client device maintenance play a vital role in identifying and resolving VPN connectivity issues, enhancing productivity, and maintaining a secure remote work environment.

IV. Network Troubleshooting Scenarios for VPN Connectivity Issues

VPN (Virtual Private Network) connectivity issues can prevent users from securely accessing resources on a remote network. Troubleshooting VPN connectivity problems requires a careful examination of both client-side and server-side configurations. Here are some network troubleshooting scenarios to consider when dealing with VPN connectivity issues:

Check Client Credentials: Verify that the VPN client has the correct username, password, and any necessary authentication tokens or certificates.

VPN Client Software: Ensure that the VPN client software is installed correctly and up to date.

VPN Server Status: Check the VPN server's status to ensure it is operational and accepting connections.

Firewall and Security Software: Temporarily disable any third-party firewalls or security software that might be blocking VPN connections.

Check VPN Server Logs: Review the VPN server logs for any error messages or connection attempts from the problematic client.

Network Address Translation (NAT): If the VPN server is behind a NAT device, ensure that proper NAT traversal (like NAT-T) is configured.

VPN Protocol: Verify that both the client and server are using the same VPN protocol (e.g., OpenVPN, PPTP, L2TP/IPsec, IKEv2).

Firewall Rules: Check firewall rules on the VPN server to ensure that incoming VPN traffic is allowed.

Verify VPN Server and Client IP Addressing: Ensure that there are no IP address conflicts between the client and server networks.

Internet Connectivity: Verify that both the client and server have a stable internet connection.

ISP Blocking: Check if the internet service provider (ISP) is blocking VPN traffic. Try connecting from a different ISP to test.

MTU Settings: Test different Maximum Transmission Unit (MTU) settings on the client and server to avoid potential fragmentation issues.

VPN Split Tunneling: Confirm that VPN split tunneling is not causing conflicts with local or remote network access.

Restart VPN Services: Try restarting the VPN server and services.

VPN Routing: Ensure that VPN routing is correctly configured to allow traffic to flow between client and server.

VPN Server Certificates: Verify that server-side certificates (if used) are valid and not expired.

Check VPN Encryption Settings: Ensure that both the client and server agree on encryption and authentication settings.

Temporary Bypass VPN: Temporarily bypass the VPN and test regular internet connectivity to verify the issue is VPN-specific.

NAT Traversal: If the VPN client is behind a NAT device, ensure that NAT traversal methods are enabled on both client and server.

Update VPN Client and Server Software: Keep both the VPN client and server software up to date to address any known issues.

Client and Server Time Sync: Verify that the client and server clocks are synchronized, as time differences can cause authentication problems.

By systematically troubleshooting VPN connectivity issues, you can identify and resolve the root causes, allowing users to securely access remote resources over the VPN. Documenting the troubleshooting steps and actions taken will aid in future reference and assist others in resolving similar issues. If the issue persists or requires expertise beyond your capabilities, don't hesitate to seek assistance from qualified network administrators or VPN specialists.

Network Problem #15. Load Balancing Configuration Errors

Load balancing configuration errors are a common network problem that occurs when the distribution of network traffic across multiple servers or links is not optimized or balanced correctly.

Load balancing is a technique used to evenly distribute incoming network requests or data traffic among multiple resources, ensuring optimal utilization of resources and preventing overload on individual components. However, misconfigurations or errors in load balancing setups can lead to uneven distribution, causing performance issues and potential service disruptions.

I. Consequences of Load Balancing Configuration Errors

Overloaded Servers: Misconfigurations can lead to uneven distribution of traffic, overburdening certain servers while leaving others underutilized.

Service Degradation: Load balancing errors can cause performance issues, leading to slow response times and reduced service availability.

User Experience Issues: Users may experience inconsistent service quality or disruptions due to load balancing problems.

Increased Downtime Risk: Load balancing configuration errors can increase the risk of service outages or downtime during peak traffic periods.

II. Causes of Load Balancing Configuration Errors

Incorrect Weighting: Assigning improper weights to servers or links in the load balancing setup can result in disproportionate traffic distribution.

Inadequate Health Checks: Inaccurate or inadequate health checks on servers can lead to the inclusion of faulty or overloaded servers in the load balancing pool.

Session Persistence Misconfiguration: Misconfiguring session persistence can cause users to lose their session data when redirected to different servers.

Improper Load Balancer Placement: Placing the load balancer in an inefficient location within the network can lead to suboptimal traffic routing.

III. How to Identify & Troubleshoot Load Balancing Configuration Errors

Network Monitoring: Utilize network monitoring tools like Obkio to track server performance and identify any imbalanced traffic patterns.

Load Balancer Configuration Review: Regularly review load balancer settings and verify proper weightings and health checks.

Testing and Validation: Conduct network load testing and validation to ensure load balancing configurations work as intended under different traffic conditions.

Session Persistence Testing: Verify session persistence settings to ensure smooth user experience during server changes.

Load Balancer Placement: Review the placement of load balancers in the network to optimize traffic routing.

By proactively identifying and addressing load balancing configuration errors, businesses can ensure efficient resource utilization, enhance service performance, and reduce the risk of downtime. Network monitoring, load balancer configuration

reviews, and rigorous testing play a crucial role in detecting and resolving load balancing configuration errors, improving the overall reliability and network availability of network services.

Load balancing configuration errors can lead to uneven distribution of traffic, service disruptions, and degraded performance. Troubleshooting load balancing issues requires careful analysis of the load balancer's configuration and associated network components. Here are some network troubleshooting scenarios to consider when dealing with load balancing configuration errors:

Check Load Balancer Configuration: Review the load balancer's configuration to ensure it is set up correctly, including virtual server settings, server pools, and load balancing algorithms.

Monitor Server Health: Monitor the health and status of the backend servers to ensure they are properly configured and responsive to requests.

Verify Server Pool Membership: Check that all the intended backend servers are added to the appropriate server pools and that no servers are mistakenly excluded.

Check Load Balancer Status: Verify that the load balancer is operational and not experiencing any issues.

Load Balancer Firmware and Software Updates: Keep the load balancer's firmware and software up to date to address known issues and security vulnerabilities.

Algorithm Selection: Ensure the appropriate load balancing algorithm (e.g., round-robin, least connections, weighted) is selected based on the specific application and server requirements.

Monitor Traffic Distribution: Observe the traffic distribution among backend servers to identify any imbalances.

Session Persistence: Check session persistence settings to ensure that client requests are directed to the same backend server for the duration of a session, if required.

Health Checks and Monitors: Review health check settings to ensure they accurately monitor backend server availability and health.

Virtual IP Address and Network Configuration: Verify that the virtual IP address and network configuration are properly set up and accessible.

Firewall Rules and Security Groups: Check that firewall rules or security groups are not blocking the load balancer's traffic

Service Ports and Protocols: Confirm that the load balancer is configured to forward traffic to the correct service ports and protocols on the backend servers.

Log Analysis: Analyze load balancer logs for any error messages or indications of misconfiguration.

Service Check: Use network monitoring tools to perform service checks on the backend servers to identify any issues.

Load Test and Simulation: Conduct load testing or simulate traffic to observe how the load balancer handles various loads and conditions.

SSL Certificates: If using SSL termination, verify that the SSL certificates on the load balancer are valid and not expired.

Application-Specific Configuration: For certain applications, ensure that any application-specific configurations or settings are correctly configured in the load balancer.

Backup and Restore Configurations: Keep backups of load balancer configurations and restore them in case of accidental changes or misconfigurations.

Rollback Changes: If you recently made changes to the load balancer configuration, consider rolling back the changes to a known working state.

By systematically troubleshooting load balancing configuration errors, you can identify and resolve issues that affect traffic distribution and optimize the performance and reliability of the load balancer. Regular monitoring and analysis of traffic patterns will help you proactively detect and address load balancing issues as they arise. If the issue persists or is beyond your expertise, seek assistance from qualified network administrators or load balancing specialists.

Network Problem #16. Link Flapping

Link flapping is a common network problem characterized by the frequent and rapid oscillation of a network link between the up and down states.

When a link flaps, it continuously alternates between being connected (up) and disconnected (down). This rapid and inconsistent behavior can disrupt network communication, cause service interruptions, and lead to instability within the network infrastructure.

I. The Consequences of Link Flapping

Network Instability: Frequent link flapping can destabilize the network, leading to poor performance and service disruptions.

Packet Loss: During link flapping, data packets may be lost or delayed, affecting data integrity and delivery.

Connectivity Issues: Devices connected to the flapping link may experience intermittent connectivity or disconnections.

Spanning Tree Protocol (STP) Recalculation Delays: STP recalculations during link flapping can result in temporary network outages or increased convergence times.

II. The Causes of Link Flapping

Physical Connectivity Issues: Loose or damaged cables, connectors, or network ports can cause link flapping when there are intermittent connections.

Network Device Errors: Malfunctioning network switches, routers, or network interface cards (NICs) can lead to unstable link states.

Spanning Tree Protocol (STP) Misconfigurations: Incorrect STP configurations can create network loops, resulting in link flapping as STP tries to block or unblock redundant paths.

Ethernet Auto-Negotiation Problems: Inconsistent auto-negotiation settings between devices can cause link flapping due to mismatched speeds or duplex modes.

New call-to-action

III. How to Identify & Troubleshoot Link Flapping

Network Monitoring: Use network monitoring tools like Obkio to track link status and identify instances of link flapping.

Physical Inspection: Physically inspect network cables and connectors to ensure they are properly connected and not damaged.

Interface Errors: Check for interface errors or error counters on network devices to identify potential issues.

STP Configuration Review: Review and verify STP configurations to prevent network loops and link flapping.

Speed and Duplex Settings: Ensure consistent speed and duplex settings between connected devices to avoid negotiation issues.

Link Redundancy: Evaluate link redundancy and adjust configurations to avoid unintended loops.

By proactively identifying and addressing link flapping, businesses can maintain a stable and reliable network infrastructure. Network monitoring, physical inspections, and STP configuration reviews are essential in detecting and mitigating link flapping issues, ensuring smooth communication and data transfer within the network.

IV. Network Troubleshooting Scenarios for Link Flapping

Link flapping occurs when a network link experiences frequent up and down transitions, causing instability and disruptions in communication. Troubleshooting link flapping requires identifying the underlying causes and implementing solutions to stabilize the link. Here are some network troubleshooting scenarios to consider when dealing with link flapping:

Physical Inspection: Inspect the physical connections of the link for loose cables, damaged connectors, or faulty network equipment.
Cable Quality: Check the quality of the network cables. Use certified and properly shielded cables to reduce interference.

Link Speed and Duplex Settings: Verify that both ends of the link are set to the same speed and duplex settings (e.g., 1 Gbps, full duplex) to avoid negotiation issues.

Auto-Negotiation: Test the link with auto-negotiation enabled and disabled to see if it stabilizes the connection.

Check Network Equipment: Review the logs and statistics of the network switches or routers connected to the link for any errors or alerts related to the flapping link.

Firmware and Software Updates: Ensure that the firmware and software of network devices are up to date to address known issues.

STP (Spanning Tree Protocol) Issues: Check if the link is part of a spanning tree loop or blocked by Spanning Tree Protocol (STP) due to redundancy misconfigurations.

STP PortFast and BPDU Guard: If using STP, ensure that PortFast and BPDU Guard are configured correctly to prevent accidental loops.

Link Aggregation (EtherChannel/LACP): If the link is part of a link aggregation group, verify the configuration of the aggregation protocol (e.g., EtherChannel, LACP).

Power Fluctuations: Verify that the devices connected to the link have stable power sources to prevent link flapping due to power issues.

Update NIC Drivers: Keep network interface card (NIC) drivers up to date on connected devices to prevent compatibility issues.

Interference: Check for sources of electromagnetic interference or signal degradation that might affect the link stability.

Port Statistics: Monitor port statistics to check for excessive error counters, collisions, or other anomalies.

MTU Size: Test different Maximum Transmission Unit (MTU) sizes to avoid potential fragmentation issues.

Bypass Network Equipment: Temporarily bypass any intermediate network equipment (e.g., switches, routers) to determine if the issue is specific to a particular device.

Check Other Network Links: Investigate if any other links or devices in the network are causing network congestion or instability.

Isolate Devices: Isolate devices connected to the link to test if the problem lies with one of the connected devices.

Network Capture: Use network capture tools to analyze network traffic and look for patterns or events leading to link flapping.

By systematically troubleshooting link flapping, you can identify the root causes and implement appropriate solutions to stabilize the link and ensure reliable network communication. Regular monitoring and analysis of network performance will help you proactively detect and address link flapping issues as they arise. If the issue persists or requires expertise beyond your capabilities, seek assistance from qualified network administrators or network equipment vendors.

How to Troubleshoot the Most Common Network Problems: Steps & Tips

Now that we've gone over some of the most common network problems that businesses encounter in enterprise networks, it's essential to equip ourselves with effective troubleshooting steps. When network issues arise, swift and systematic troubleshooting is crucial to minimize downtime, ensure smooth operations, and maintain a reliable network infrastructure.

Identifying network issues is the first step to solving them - and it all comes down to pinpointing who, what, where, and when.

Step 1: Network Assessment

The first step when it comes to identifying network problems, with your Network Monitoring tool in hand, is performing a network assessment to collect some key information about your network. Obkio's Network Monitoring tool, which we helped you deploy earlier in this blog post, plays a vital role in this process.

Get started with Obkio for free!

By conducting a thorough network assessment, you can gain valuable insights into your network's health, performance, and potential bottlenecks. This information serves as a solid foundation for efficient troubleshooting and enables you to pinpoint the root causes of network issues more effectively. Now, let's delve into the general troubleshooting steps to address common network problems and make the most out of your network monitoring capabilities

What actions to take: After you've collected all the information you need to identify the network issue, can then start network troubleshooting. That could include reaching out to your ISP or MSP, or bringing the problem to your network administrator to fix it internally.

For all the details about identifying network issues, check out our article on how to identify network issues!

Troubleshooting common network problems involves identifying the "what" issue is occurring, determining "where" the problem is located in the network, understanding "when" the issue is happening, identifying "who" is affected, and then taking appropriate actions to resolve the problem. Here are some steps to help troubleshoot common network problems:

Step 2: Identify the Issue (What)

To know how to solve these problems, you need to actually understand what they are. A network performance monitoring software will measure network metrics and report back if it finds any issues, with details about what the issue is, and what caused it.

Gather information from users or monitoring tools to determine the symptoms and specific problem experienced.

Clearly define the issue, such as slow internet speed, intermittent connectivity, or VoIP call quality problems.

Step 3: Locate the Problem (Where)

It's important to identify where exactly in your network an issue has occurred. Using Monitoring Agents, Obkio allows you to deploy Agents in key network locations for end-to-end visibility over your network to provide you with details about where problems have occurred. This end-to-end network monitoring approach gives you visibility of every end of your network, from your LAN to your WAN.

Determine which part of the network is affected, such as a specific network segment, device, or service.

Use network monitoring tools and analysis to identify potential network bottlenecks, high utilization areas, or devices showing errors.

Step 4: Determine the Timeframe (When)

Identifying the specific timeframe in which a network problem occurs is essential for effective troubleshooting. Pinpointing when the issue started and its recurrence patterns using historical data from Obkio's NPM tool can help correlate the problem with network changes or events, streamlining the resolution process.

Find out when the problem started occurring to correlate with any changes in the network or configurations.

Analyze network logs and timestamps to pinpoint when the issue typically happens, if it's intermittent.

Step 5. Identify Affected Users (Who)

Understanding which users or devices are experiencing network issues is crucial in troubleshooting. By pinpointing the affected users, network administrators can focus their efforts, assess the scope of the problem, and provide targeted support, ensuring a prompt resolution and improved user experience."

Determine which users or devices are experiencing the problem to understand the scope of the issue.

If the problem is widespread, identify common factors among affected users.

Step 6. Who is Responsible For the Network Segment

Once you know where a network problem is located, and what exactly it is, you can then easily decide who in your business is responsible for that network segment.

Identifying the responsible party helps streamline communication and coordination, ensuring a more effective and targeted approach to resolving the issue.

By involving the right stakeholders, you can facilitate a faster resolution and prevent delays in troubleshooting efforts.

Step 7. Take Initial Actions (What Actions to Take)

When network issues arise, it's essential to swiftly address the problem with initial actions. This step focuses on quick checks and basic troubleshooting to resolve common issues that might be causing the network problem. By taking these immediate actions, you can potentially resolve the problem right away or narrow down the root cause, setting the stage for further targeted troubleshooting.

Perform basic checks, such as verifying cable connections, power cycling affected devices, or checking for software updates.

Review network configuration changes or recent updates that might have contributed to the problem.

Step 8. Isolate the Issue

To efficiently troubleshoot network problems, isolating the issue is crucial. This step involves narrowing down the problematic area or component in the network. By systematically eliminating potential causes, you can pinpoint the specific source of the problem, leading to a more precise and effective resolution.

Monitor network devices, like switches or routers, using Obkio's Network Device Monitoring feature, to identify if they are causing the problem or experiencing resource issues.

Divide the network into segments and test each segment independently to narrow down the location of the problem.

Use Visual Traceroutes to determine if the problem is in your local network or ISP network.

Step 9. Implement Solutions

After identifying the root cause of the network problem, it's time to implement targeted solutions. This step focuses on making necessary adjustments, configurations, or replacements to address the issue directly. By applying the appropriate solutions, you can effectively restore network functionality and prevent the problem from recurring.

Based on the gathered information, apply appropriate solutions, such as adjusting configurations, updating firmware, or replacing faulty hardware.

If the network problem is beyond your organization's control and is related to the Internet Service Provider (ISP) or Managed Service Provider (MSP network) infrastructure, promptly reach out to them for assistance.

Collaborating with your ISP or MSP can expedite the resolution process for issues that lie outside your network's scope.

Document the changes made during troubleshooting for future reference.

Step 10. Test, Verify & Continuously Monitor Network Performance

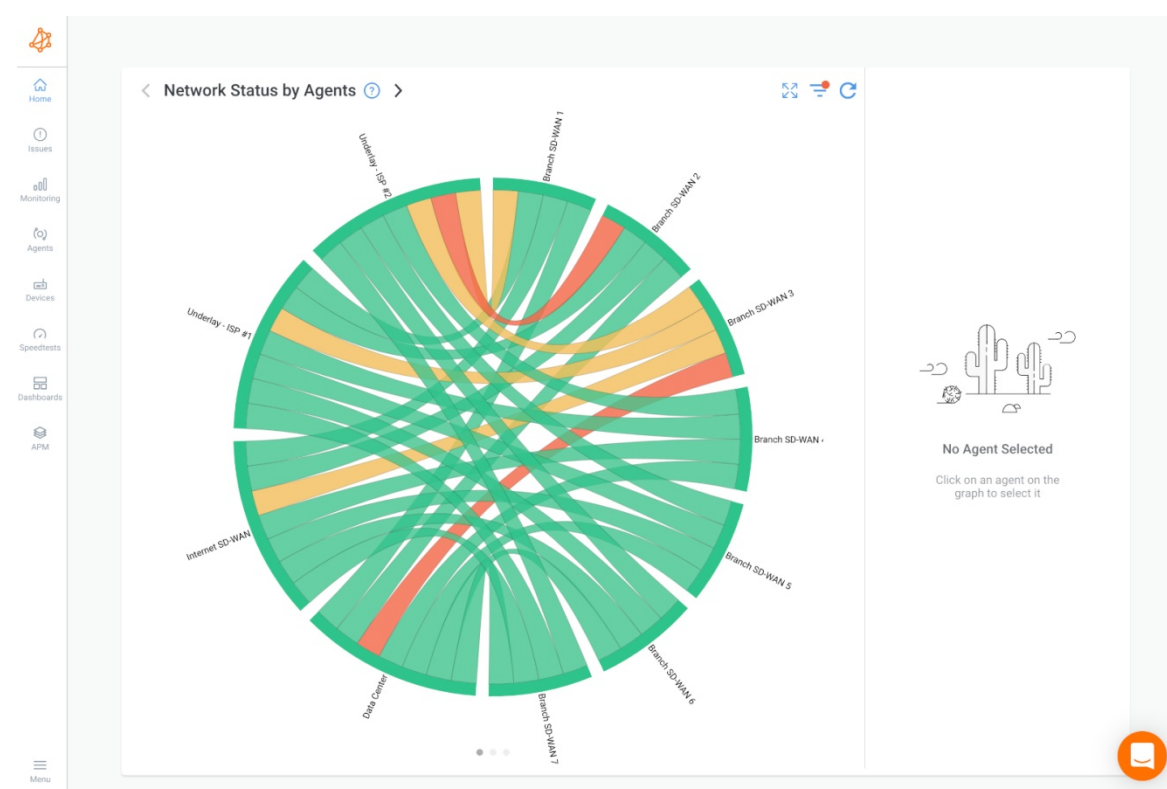
Culminating the troubleshooting process, this section outlines the essential steps to verify the effectiveness of the implemented solutions and ensure a stable network environment. From thorough network testing to continuous monitoring, these practices ensure that network issues are promptly resolved and potential future problems are proactively addressed.

After implementing solutions, thoroughly test and continuously monitor network performance with your Network Monitoring tool to ensure the problem is resolved.

Verify that the network is functioning as expected and the previously identified issues are no longer present. Monitor the network post-resolution to verify the stability and effectiveness of the applied changes.

Continuously monitor network performance using tools like Obkio to ensure the problem does not reoccur and to detect any new issues that may arise.

By ongoing monitoring, you can proactively address potential problems before they impact the network's stability and user experience.



Obkio - Common Network Problems

Why Should Businesses Find & Fix Network Problems Anyways?

In this section, we'll delve into why finding and troubleshooting network problems is a critical mission for businesses. From bolstering productivity and enhancing customer

experience to safeguarding data and gaining a competitive edge, we'll explore the myriad reasons why proactive network monitoring is an indispensable investment.

Maintaining Productivity: A smooth and reliable network is the backbone of business productivity. When network problems occur, they disrupt communication, data access, and collaborative efforts, leading to downtime and decreased efficiency. By identifying and resolving these issues promptly, businesses can minimize disruptions and keep productivity levels at their peak.

Enhancing Customer Experience: In a digitally interconnected world, customer satisfaction hinges on swift and seamless interactions. Network problems can affect customer-facing services, leading to slow response times, website downtime, and impaired online transactions. By proactively addressing network issues, businesses can provide a positive customer experience, which can bolster loyalty and brand reputation.

Cost Savings: Network problems can be costly in terms of both time and resources. Extended downtime can result in revenue losses, missed opportunities, and

increased operational expenses as IT teams rush to troubleshoot and fix issues. By resolving problems swiftly, businesses can mitigate these financial impacts and avoid potential long-term consequences.

Security and Data Protection: Network problems, especially those related to security breaches, can expose sensitive data and compromise the overall integrity of the business. Troubleshooting network vulnerabilities and promptly addressing security threats is essential for safeguarding valuable information and maintaining regulatory compliance.

IT Team Efficiency: Persistent network issues can place an immense burden on IT teams, overwhelming them with repetitive troubleshooting tasks. By proactively identifying and resolving problems, IT teams can focus on strategic initiatives and improvements, ultimately making the best use of their expertise and time.

Business Continuity: In today's digital-dependent landscape, uninterrupted business operations are crucial for survival and growth. Network problems, if left unchecked, can lead to extended outages and interruptions, threatening business continuity. By troubleshooting and resolving issues, businesses can ensure a more robust and resilient infrastructure.

Competitive Advantage: In a competitive market, businesses must deliver a seamless user experience to stand out from their rivals. A well-maintained and

efficient network allows companies to differentiate themselves by providing reliable services and smooth interactions, ultimately gaining a competitive edge.

Employee Satisfaction: A functional network translates to a smoother work experience for employees. When network problems are addressed promptly, employees can focus on their tasks without the frustration and stress caused by technology-related hurdles.

In conclusion, finding and troubleshooting network problems is crucial for businesses to maintain productivity, enhance customer experience, save costs, protect data, streamline IT operations, ensure business continuity, gain a competitive advantage, and foster employee satisfaction. It's an essential investment in the overall success and growth of any modern business.