**List Of Practicals**

1. Introduction to Networking Simulation Tools: Wireshark, Cisco Packet Tracer.

2. To understand the operation of TELNET by accessing the router in server room from a PC in IT office.

3. To implement an IP Addressing Scheme and Subnetting in small networks using Cisco Packet Tracer.

4. To implement the static routing using Cisco Packet Tracer.

5. To implement the DHCP onto the Network Topology using Cisco Packet Tracer.

6. To implement the DNS, Email Services in the Network using Cisco Packet Tracer.

7. To implement the Dynamic Routing Protocols: RIP, IGRP using Cisco Packet Tracer.

8. To construct multiple router networks and implement the EIGRP Protocol.

9. To implement the Network Address Resolution (NAT) using Cisco Packet Tracer.

10. Conducting a Network Capture and Monitoring with Wireshark Simulation Tool

Overview of Network Devices:

Overview:

Network devices are physical devices that enable communication and interaction between hardware on a computer network. Each networking device operates in a distinct computer network segment and performs distinct functions.

A network may require hundreds or thousands of different network devices to maintain and build out various LAN and WAN. Network devices like the hub, bridge, repeater, modem, router, gateway, etc., are the basic building blocks of an extensive network.

Definition:

Network devices are physical devices that enable communication and interaction between hardware on a computer network. Network devices are building blocks that permit communication between services and the endpoints that consume those services.

In other words, they're connectors that allow devices on a network to communicate with one another. Enabling communication on a network means anything that helps data get from source to destination.

When a network contains a large number of devices, too many data packets are transmitted over the same network path. This can cause congestion and performance reduction. The goal of networking devices is to provide for smooth communication between various hardware linked to a network. Adding a network device facilitates the seamless sharing of network resources between different systems.

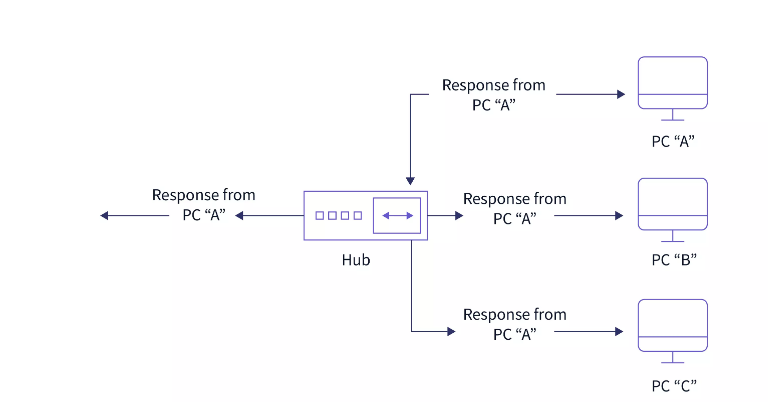
Types Of Network Devices

* Hub
* Switch
* Router
* Bridge
* Gateway
* Modem
* Repeaters
* Access point

**HUB:**

A hub is a physical-layer device that acts on individual bits rather than frames. When a bit, representing a zero or a one, arrives from one interface, the hub simply recreates the bit, boosts its energy strength, and transmits the bit into all the other interfaces. Whenever a hub receives a bit from one of its interfaces, it sends a copy to all other interfaces.

In particular, if a hub receives frames from two different interfaces at the same time, a collision occurs, and the nodes that created the frames must retransmit. A network hub does not have routing tables or intelligence that is utilized to transfer information and disseminate all network data across all connections.



Types of Hubs

There are generally three types of hubs that are given below.

Active Hub :

These hubs have their power source and can clean, enhance, and relay the network's signal. It functions as both a repeater and a wiring center. The active hub may repair damaged packets as they are being sent and can also hold the direction of the remaining packets and distribute them. If a port gets a weak but readable signal, the active hub reconstructs the weak signal into a more robust signal before distributing it to other ports. If any connecting device in the network is not operating, it can increase the signal.

Passive Hub :

The passive hubs are the wire connection points that aid in the construction of the physical network. It can detect faults and malfunctioning hardware. The passive hub accepts the packet through a port and distributes it to all ports. It comes with connectors (10base-2 port and RJ-45) that can be used in your network as a standard. All local area network (LAN) devices are linked to this connector. These hubs do not clean or enhance signals before relaying them to the network and cannot be utilized to extend the distance between nodes.

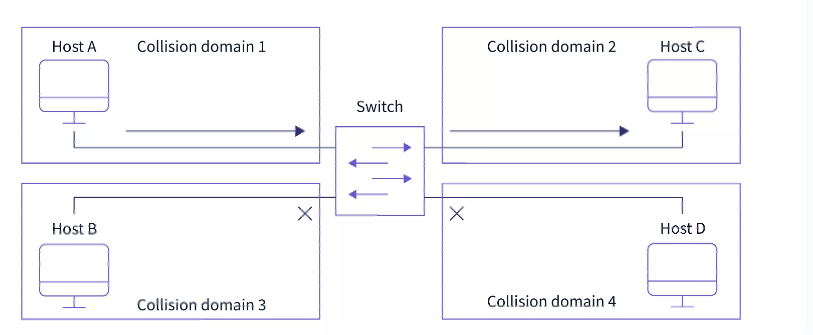
Intelligent Hub:

It functions similarly to active hubs and offers remote management capabilities. They also supply network devices with variable data speeds. It also allows an administrator to monitor traffic flowing through the hub and manage each port.

**Switch**

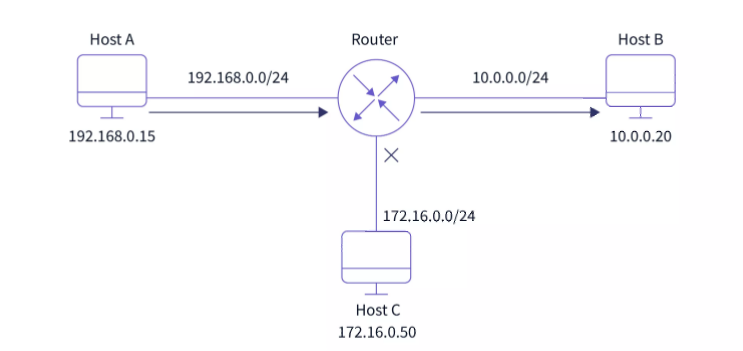
A switch is a multiport network device with a buffer and design that can improve its efficiency (having a large number of ports means less traffic) and performance. A switch is a networking device that operates at the data link layer. A switch has numerous ports into which computers can be plugged. When a data frame arrives at any network switch port, it evaluates the destination address(destination MAC address ), performs the necessary checks, and sends the frame to the associated device. The switch performs error checking before forwarding the data, making it very efficient because it does not forward packets with errors and only forwards good packets to the correct port.

The working of the switch can easily be illustrated by the diagram given below in which Host A wants to send some data to Host B.



**Router**

A router is a network device similar to a switch that routes data packets based on their IP addresses. The router is primarily a Network Layer device. A router is also known as an intelligent device because it can automatically calculate the best route to pass network packets from source to destination. A router examines a data packet's destination IP address and uses headers and forwarding tables to determine the best way to transfer the packets. It communicates between two or more networks using protocols such as ICMP.



Types of Routers

There are various types of routers used in networking as follows:

Wireless Router:

These routers can generate a wireless signal in your home or office, allowing computers to connect to routers within a specific range and access the internet. When connected indoors, the wireless router's range is approximately 150 feet, when connected outdoors, the range is up to 300 feet.

Brouter:

A brouter is a hybrid of a bridge and a router. It acts as a bridge, allowing data to be transferred between networks, and it can also route data within a network to individual systems, much like a router. As a result, it combines the functions of a bridge and a router by routing some incoming data to the appropriate systems while transferring the rest to another network.

Core Router:

A core router is a kind of router that can route data within a network but cannot route data between networks. It is a computer communication system device that serves as the backbone of networks by connecting all network devices. It is used by internet service providers and offers a variety of fast and powerful data communication interfaces.

Edge Router :

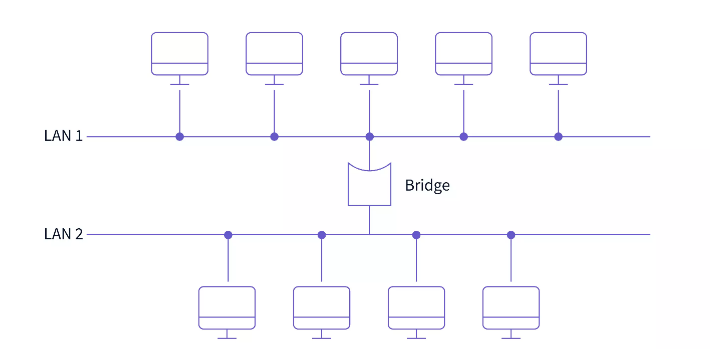
An edge router is a low-capacity device that sits at the network's edge. It enables an internal network to communicate with external networks. For internet-based connectivity with distant networks, it uses an external BGP (Border Gateway Protocol).

Broadband Router :

Broadband routers are primarily used to provide computers with high-speed internet access. It is required when connecting to the internet via phone and using Voice over IP technology (VoIP). All broadband routers have three or four Ethernet ports for connecting laptop and desktop computers.

**Bridge**

A bridge is a network device that operates at the data link layer device. A bridge is a repeater with the added functionality of filtering content by reading the MAC addresses of the source and destination. It is also used to connect two LANs that use the same protocol. It has a single input and output port, making it a two-port device.



Types of Bridges

There are generally two types of bridges used in networking:

Transparent Bridges:

A transparent bridge is a type of bridge that monitors incoming network traffic to determine media access control (MAC) addresses. These bridges operate in a manner that is transparent to all networked hosts. A transparent bridge stores MAC addresses in a table similar to a routing table and uses that information to route packets to their destination.

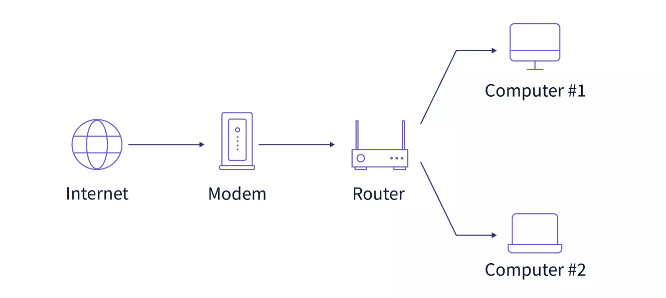
Source Routing Bridges:

The source station performs the routing operation in these bridges, and the frame specifies which route to take. The host can find the frame by sending a special frame known as the discovery frame, which propagates throughout the network using all possible paths to the destination.

**Gateway**

A gateway is a network node in telecommunications that connects two networks that use different transmission protocols. Gateways serve as network entry and exit points because all data must pass through or communicate with the gateway before being routed. Traffic that does not go through at least one gateway in most IP-based networks is traffic between the nodes on the same local area network (LAN) segment. The primary benefit of using a gateway in personal or business scenarios is that it consolidates internet connectivity into a single device. A gateway node in the enterprise can also serve as a proxy server and a firewall.

**Modem**



A modem is a network device that modulates and demodulates analog carrier signals (known as sine waves) to encode and decode digital data for processing. Because modems perform both of these tasks simultaneously, the term modem is a combination of "modulate" and "demodulate".

Types of Modem

There are generally five types of modem.

Optical Modem:

Instead of other metallic media, optical cables are used in optical modems. It converts digital data signals into light pulses transmitted via the optical fiber it employs.

Digital Modem:

Digital data are converted into digital signals by a digital modem. The digital data is modulated on the digital carrier signals before being transmitted over the digital transmission lines.

Acoustic Modem:

A specific modem called an "acoustic modem" can connect a phone handset to a gadget that traveling salespeople use to connect hotel phones. It has a microphone and speaker.

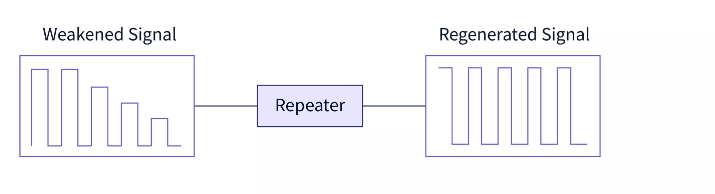
Smart Modem:

The smart modem has capabilities for auto-dialing, auto-redialing, and auto-answering. It has a microprocessor onboard that performs auto-dial and auto-answering tasks using the Hayes AT command set.

Short Haul Modem:

The short-haul modem is the one that is installed on your home computer. They are typically used to connect PCs in a building or office within this region and can transmit the data over distances of up to 20 miles.

**Repeater**



A repeater is a two-port device that operates at the physical layer. It is used to regenerate the signal over the same network before it becomes too weak or corrupted, allowing the signal to be transmitted for a longer distance over the same network. It is important to understand that repeaters do not amplify the signal. When the signal weakens, repeaters copy it bit by bit and regenerate it at its original strength.

Types of Repeaters

On the basis of signals that repeaters generate.

Analog Repeaters:

In an analog repeater, data is transmitted through analog signals to increase its amplitude. These repeaters are used in trunk lines to help broadcast multiple signals using frequency division multiplexing (FDM). It houses the linear amplifier as well as the filters.

Digital Repeaters:

In a digital repeater, data is transmitted in the form of binary digits such as 0s and 1s. While transmitting data, 0 and 1 values are generated, and it is capable of transmitting data over long distances.

**Access point**

A wireless device is typically meant by the term access point (AP), even though it technically refers to a wired or wireless connection. The Data Link layer of the OSI model is where an access point (AP) operates. An access point can function as a router or bridge, passing data transmissions from one access point to another. Wireless access points (WAPs) are devices that combine a transmitter and receiver (transceiver) to form a wireless LAN (WLAN). Access points are typically standalone network devices with an antenna, transmitter, and adapter built in. Access points use the wireless infrastructure network mode to connect WLANs to wired Ethernet LANs.

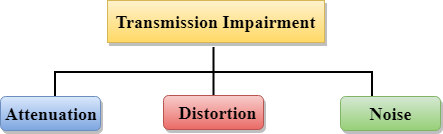
Transmission media

* In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver i.e. it is the channel through which data is sent from one place to another.
* Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals.
* The main functionality of the transmission media is to carry the information in the form of bits through **LAN**(Local Area Network).
* It is a physical path between transmitter and receiver in data communication.
* In a copper-based network, the bits in the form of electrical signals.
* In a fibre based network, the bits in the form of light pulses.
* In **OSI**(Open System Interconnection) phase, transmission media supports the Layer 1. Therefore, it is considered to be as a Layer 1 component.
* The electrical signals can be sent through the copper wire, fibre optics, atmosphere, water, and vacuum.
* The characteristics and quality of data transmission are determined by the characteristics of medium and signal.
* Transmission media is of two types are wired media and wireless media. In wired media, medium characteristics are more important whereas, in wireless media, signal characteristics are more important.
* Different transmission media have different properties such as bandwidth, delay, cost and ease of installation and maintenance.
* The transmission media is available in the lowest layer of the OSI reference model, i.e., **Physical layer**.

**Some factors need to be considered for designing the transmission media:**

* **Bandwidth:** All the factors are remaining constant, the greater the bandwidth of a medium, the higher the data transmission rate of a signal.
* **Transmission impairment:** When the received signal is not identical to the transmitted one due to the transmission impairment. The quality of the signals will get destroyed due to transmission impairment.
* **Interference:** An interference is defined as the process of disrupting a signal when it travels over a communication medium on the addition of some unwanted signal.

Causes Of Transmission Impairment:



* **Attenuation:** Attenuation means the loss of energy, i.e., the strength of the signal decreases with increasing the distance which causes the loss of energy.
* **Distortion:** Distortion occurs when there is a change in the shape of the signal. This type of distortion is examined from different signals having different frequencies. Each frequency component has its own propagation speed, so they reach at a different time which leads to the delay distortion.
* **Noise:** When data is travelled over a transmission medium, some unwanted signal is added to it which creates the noise.

# **Guided Media**

It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media.

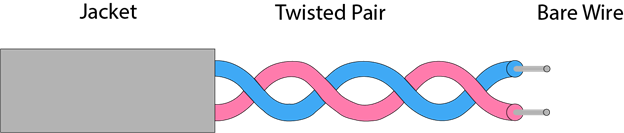
**Types Of Guided media:**

## Twisted pair:

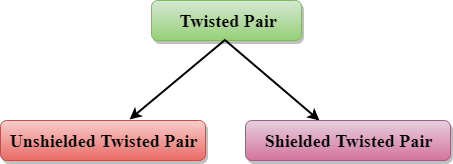
Twisted pair is a physical media made up of a pair of cables twisted with each other. A twisted pair cable is cheap as compared to other transmission media. Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from 0 to 3.5KHz.

A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.

The degree of reduction in noise interference is determined by the number of turns per foot. Increasing the number of turns per foot decreases noise interference.



**Types of Twisted pair:**



**Unshielded Twisted Pair:**

An unshielded twisted pair is widely used in telecommunication. Following are the categories of the unshielded twisted pair cable:

* **Category 1:** Category 1 is used for telephone lines that have low-speed data.
* **Category 2:** It can support upto 4Mbps.
* **Category 3:** It can support upto 16Mbps.
* **Category 4:** It can support upto 20Mbps. Therefore, it can be used for long-distance communication.
* **Category 5:** It can support upto 200Mbps.

**Advantages Of Unshielded Twisted Pair:**

* It is cheap.
* Installation of the unshielded twisted pair is easy.
* It can be used for high-speed LAN.

**Disadvantage:**

* This cable can only be used for shorter distances because of attenuation.

**Shielded Twisted Pair**

A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.

**Characteristics Of Shielded Twisted Pair:**

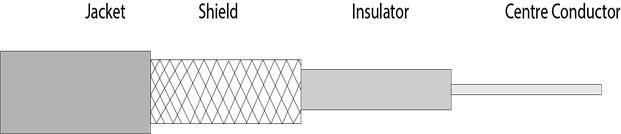
* The cost of the shielded twisted pair cable is not very high and not very low.
* An installation of STP is easy.
* It has higher capacity as compared to unshielded twisted pair cable.
* It has a higher attenuation.
* It is shielded that provides the higher data transmission rate.

**Disadvantages**

* It is more expensive as compared to UTP and coaxial cable.
* It has a higher attenuation rate.

**Coaxial Cable**

* Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable.
* The name of the cable is coaxial as it contains two conductors parallel to each other.
* It has a higher frequency as compared to Twisted pair cable.
* The inner conductor of the coaxial cable is made up of copper, and the outer conductor is made up of copper mesh. The middle core is made up of non-conductive cover that separates the inner conductor from the outer conductor.
* The middle core is responsible for the data transferring whereas the copper mesh prevents from the **EMI**(Electromagnetic interference).



**Coaxial cable is of two types:**

1. **Baseband transmission:** It is defined as the process of transmitting a single signal at high speed.
2. **Broadband transmission:** It is defined as the process of transmitting multiple signals simultaneously.

**Advantages Of Coaxial cable:**

* The data can be transmitted at high speed.
* It has better shielding as compared to twisted pair cable.
* It provides higher bandwidth.

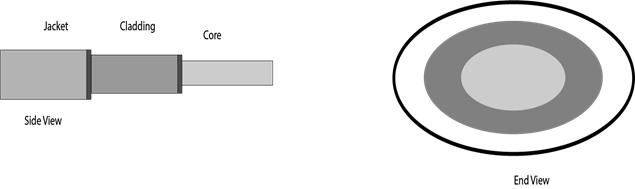
**Disadvantages Of Coaxial cable:**

* It is more expensive as compared to twisted pair cable.
* If any fault occurs in the cable causes the failure in the entire network.

**Fibre Optic**

* Fibre optic cable is a cable that uses electrical signals for communication.
* Fibre optic is a cable that holds the optical fibres coated in plastic that are used to send the data by pulses of light.
* The plastic coating protects the optical fibres from heat, cold, electromagnetic interference from other types of wiring.
* Fibre optics provide faster data transmission than copper wires.

**Diagrammatic representation of fibre optic cable:**



**Basic elements of Fibre optic cable:**

* **Core:** The optical fibre consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fibre. The more the area of the core, the more light will be transmitted into the fibre.
* **Cladding:** The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fibre.
* **Jacket:** The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fibre strength, absorb shock and extra fibre protection.

**Following are the advantages of fibre optic cable over copper:**

* **Greater Bandwidth:** The fibre optic cable provides more bandwidth as compared copper. Therefore, the fibre optic carries more data as compared to copper cable.
* **Faster speed:** Fibre optic cable carries the data in the form of light. This allows the fibre optic cable to carry the signals at a higher speed.
* **Longer distances:** The fibre optic cable carries the data at a longer distance as compared to copper cable.
* **Better reliability:** The fibre optic cable is more reliable than the copper cable as it is immune to any temperature changes while it can cause obstruct in the connectivity of copper cable.
* **Thinner and Sturdier:** Fibre optic cable is thinner and lighter in weight so it can withstand more pull pressure than copper cable.

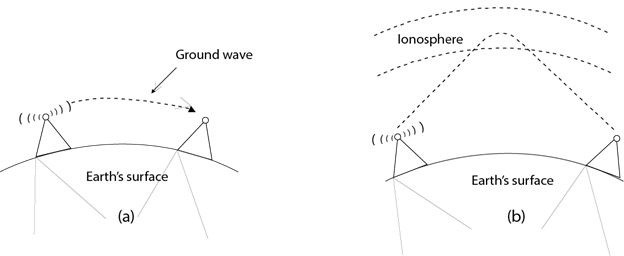
# **Unguided Transmission**

* An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as **wireless transmission**.
* In unguided media, air is the media through which the electromagnetic energy can flow easily.

Unguided transmission is broadly classified into three categories:

## Radio waves

* Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
* Radio waves are omnidirectional, i.e., the signals are propagated in all the directions.
* The range in frequencies of radio waves is from 3Khz to 1 khz.
* In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.
* An example of the radio wave is **FM radio**.



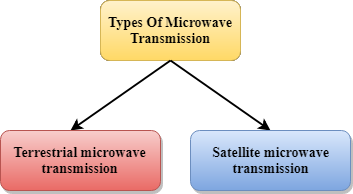
**Applications Of Radio waves:**

* A Radio wave is useful for multicasting when there is one sender and many receivers.
* An FM radio, television, cordless phones are examples of a radio wave.

**Advantages Of Radio transmission:**

* Radio transmission is mainly used for wide area networks and mobile cellular phones.
* Radio waves cover a large area, and they can penetrate the walls.
* Radio transmission provides a higher transmission rate.

**Microwaves**



Microwaves are of two types:

* Terrestrial microwave
* Satellite microwave communication.

**Terrestrial Microwave Transmission**

* Terrestrial Microwave transmission is a technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another.
* Microwaves are the electromagnetic waves having the frequency in the range from 1GHz to 1000 GHz.
* Microwaves are unidirectional as the sending and receiving antenna is to be aligned, i.e., the waves sent by the sending antenna are narrowly focussed.
* In this case, antennas are mounted on the towers to send a beam to another antenna which is km away.
* It works on the line-of-sight transmission, i.e., the antennas mounted on the towers are the direct sight of each other.

**Satellite Microwave Communication**

* A satellite is a physical object that revolves around the earth at a known height.
* Satellite communication is more reliable nowadays as it offers more flexibility than cable and fibre optic systems.
* We can communicate with any point on the globe by using satellite communication.

**Infrared**

* An infrared transmission is a wireless technology used for communication over short ranges.
* The frequency of the infrared in the range from 300 GHz to 400 THz.
* It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

**Characteristics Of Infrared:**

* It supports high bandwidth, and hence the data rate will be very high.
* Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.
* An infrared communication provides better security with minimum interference.
* Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.

# **Introduction of Wireshark**

## What is Wireshark?

Wireshark is an open-source packet analyzer, which is used for **education, analysis, software development, communication protocol development, and network troubleshooting**.

It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a **sniffer, network protocol analyzer, and network analyzer**. It is also used by network security engineers to examine security problems.

Wireshark is a free to use application which is used to apprehend the data back and forth. It is often called as a free packet sniffer computer application. It puts the network card into an unselective mode, i.e., to accept all the packets which it receives.

## Uses of Wireshark:

Wireshark can be used in the following ways:

1. It is used by network security engineers to examine security problems.
2. It allows the users to watch all the traffic being passed over the network.
3. It is used by network engineers to troubleshoot network issues.
4. It also helps to troubleshoot latency issues and malicious activities on your network.
5. It can also analyze dropped packets.
6. It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world.

What is a packet?

A packet is a unit of data which is transmitted over a network between the origin and the destination. Network packets are small, i.e., maximum **1.5 Kilobytes for Ethernet packets and 64 Kilobytes for IP packets**. The data packets in the Wireshark can be viewed online and can be analyzed offline.

### Color coding in Wireshark

The packets in the Wireshark are highlighted with **blue**, **black**, and **green color**. These colors help users to identify the types of traffic. It is also called as **packet colorization**. The kinds of coloring rules in the Wireshark are **temporary rules** and **permanent rules**.

* The temporary rules are there until the program is in active mode or until we quit the program.
* The permanent color rules are available until the Wireshark is in use or the next time you run the Wireshark. The steps to apply color filters will be discussed later in this topic.

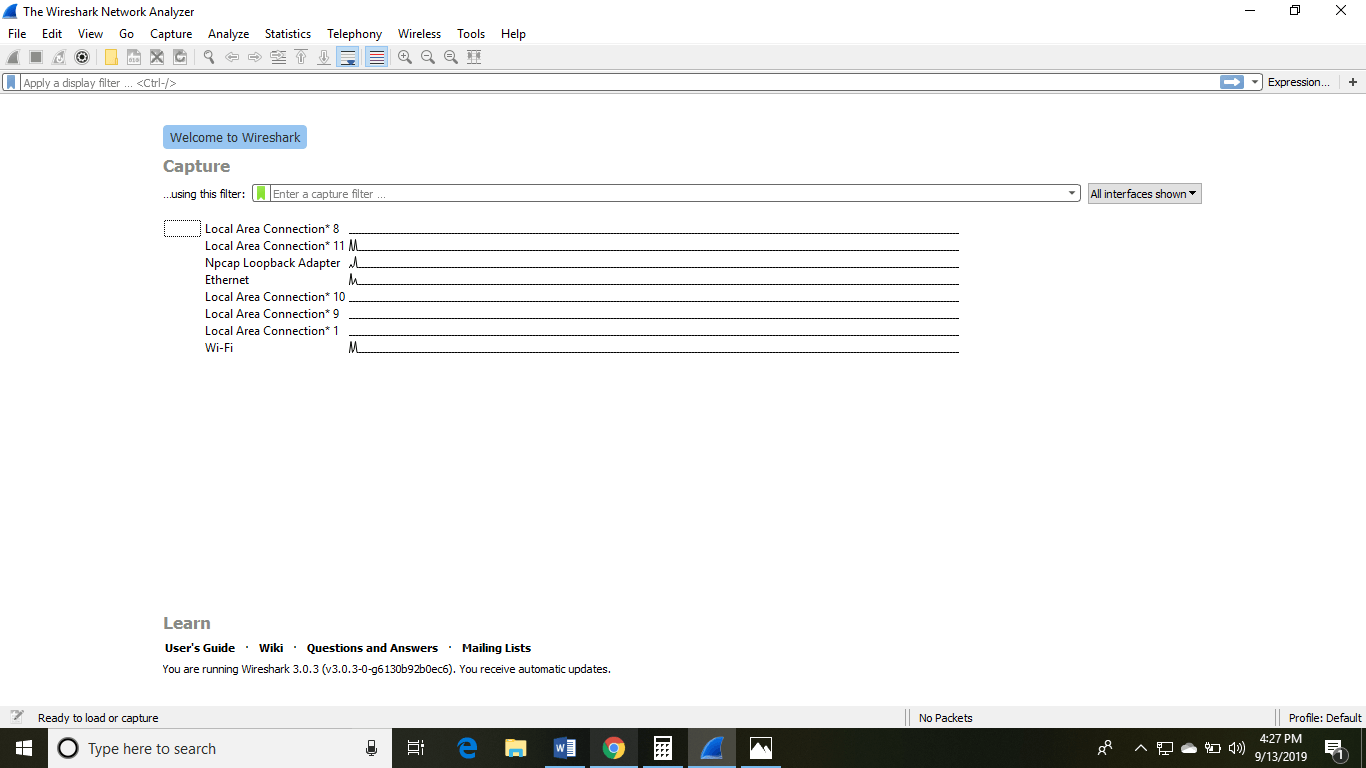
**Installation of Wireshark Software**

Below are the steps to install the Wireshark software on the computer:

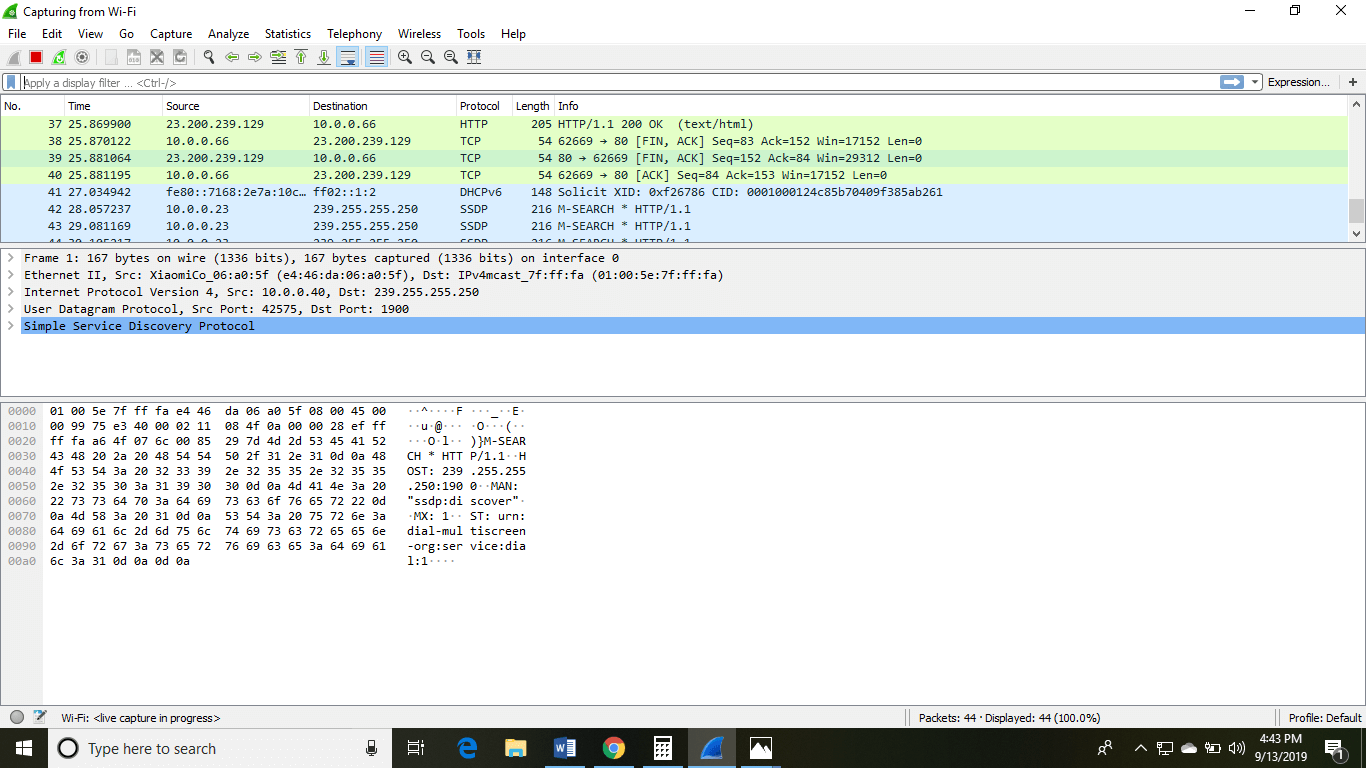
* Open the web browser.
* Search for '**Download Wireshark**.'
* Select the Windows installer according to your system configuration, either 32-bt or 64-bit. Save the program and close the browser.
* Now, open the software, and follow the install instruction by accepting the license.
* The Wireshark is ready for use.

On the network and Internet settings option, we can check the interface connected to our computer.

By selecting the current interface, we can get the traffic traversing through that interface. This version will open as:



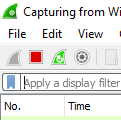
The options given on the list are the Interface list options. The number of interface options will be present. Selection of any option will determine all the traffic. **For example,** from the above fig. select the Wi-Fi option. After this, a new window opens up, which will show all the current traffic on the network. Below is the image which tells us about the live capture of packets and our Wireshark will look like:



The above arrow shows the packet content written in hexadecimal or the ASCII format. And the information above the packet content, are the details of the packet header.

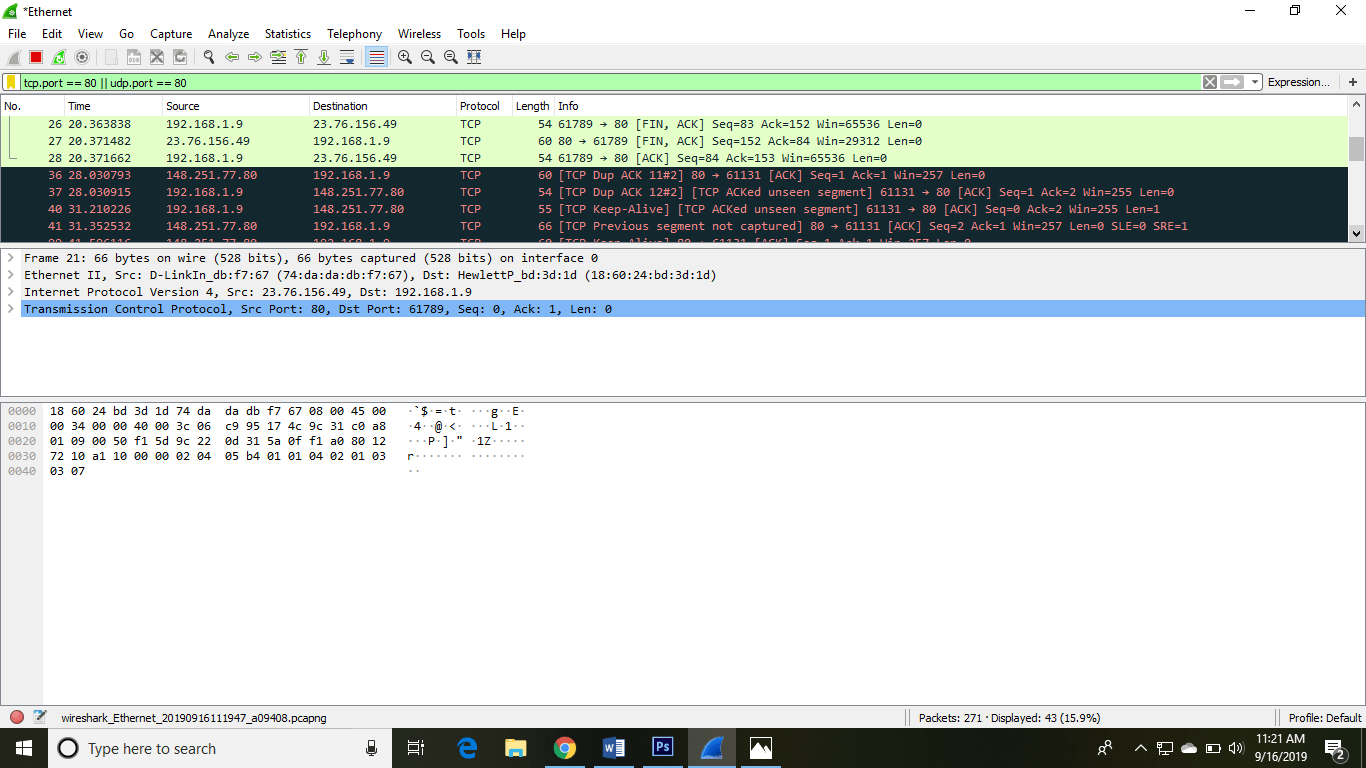
It will continue listening to all the data packets, and you will get much data. If you want to see a particular data, then you can click on the red button. The traffic will be stationary, and you can note the parameters like time, source, destination, the protocol being used, length, and the Info. To view in-depth detail, you can click on that particular address; a lot of the information will be displayed below that.

There will be detailed information on HTTP packets, TCP packets, etc. The red button is shown below:



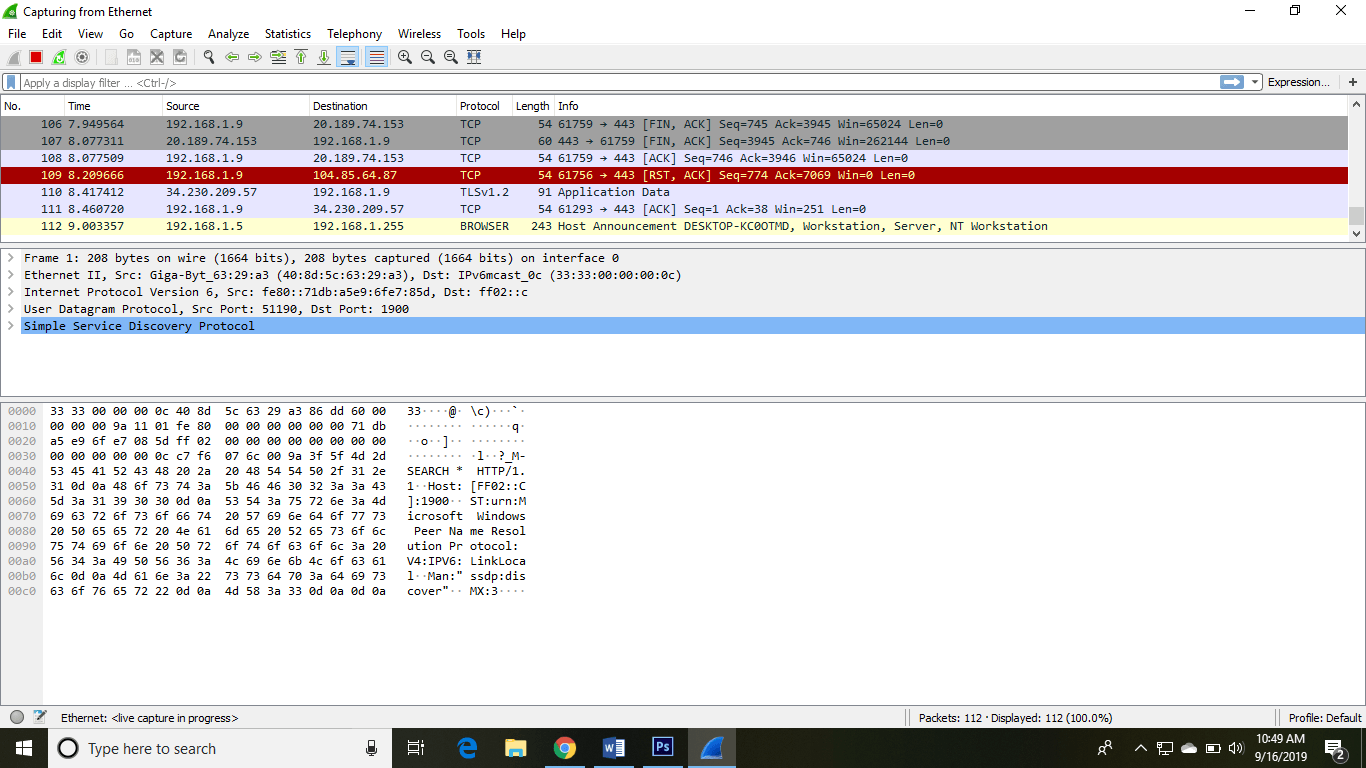
The screen/interface of the Wireshark is divided into five parts:

* First part contains a menu bar and the options displayed below it. This part is at the top of the window. File and the capture menus options are commonly used in Wireshark. The capture menu allows to start the capturing process. And the File menu is used to open and save a capture file.
* The second part is the packet listing window. It determines the packet flow or the captured packets in the traffic. It includes the packet number, time, source, destination, protocol, length, and info. We can sort the packet list by clicking on the column name.
* Next comes the packet header- detailed window. It contains detailed information about the components of the packets. The protocol info can also be expanded or minimized according to the information required.
* The bottom window called the packet contents window, which displays the content in ASCII and hexadecimal format.
* At last, is the filter field which is at the top of the display. The captured packets on the screen can be filtered based on any component according to your requirements. For example, if we want to see only the packets with the HTTP protocol, we can apply filters to that option. All the packets with HTTP as the protocol will only be displayed on the screen, shown below:

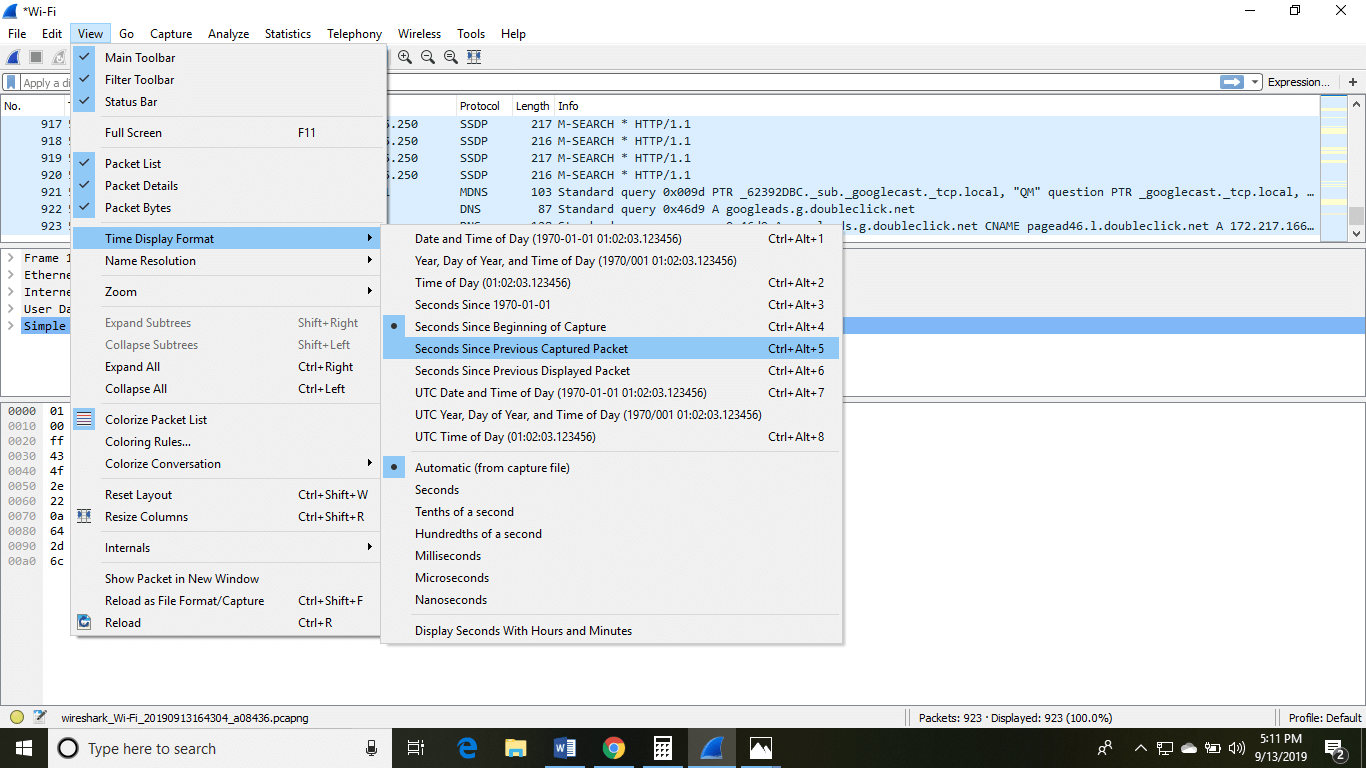


You can also select the connection to which your computer is connected. For example, in this PC, we have chosen the current network, i.e., the ETHERNET.

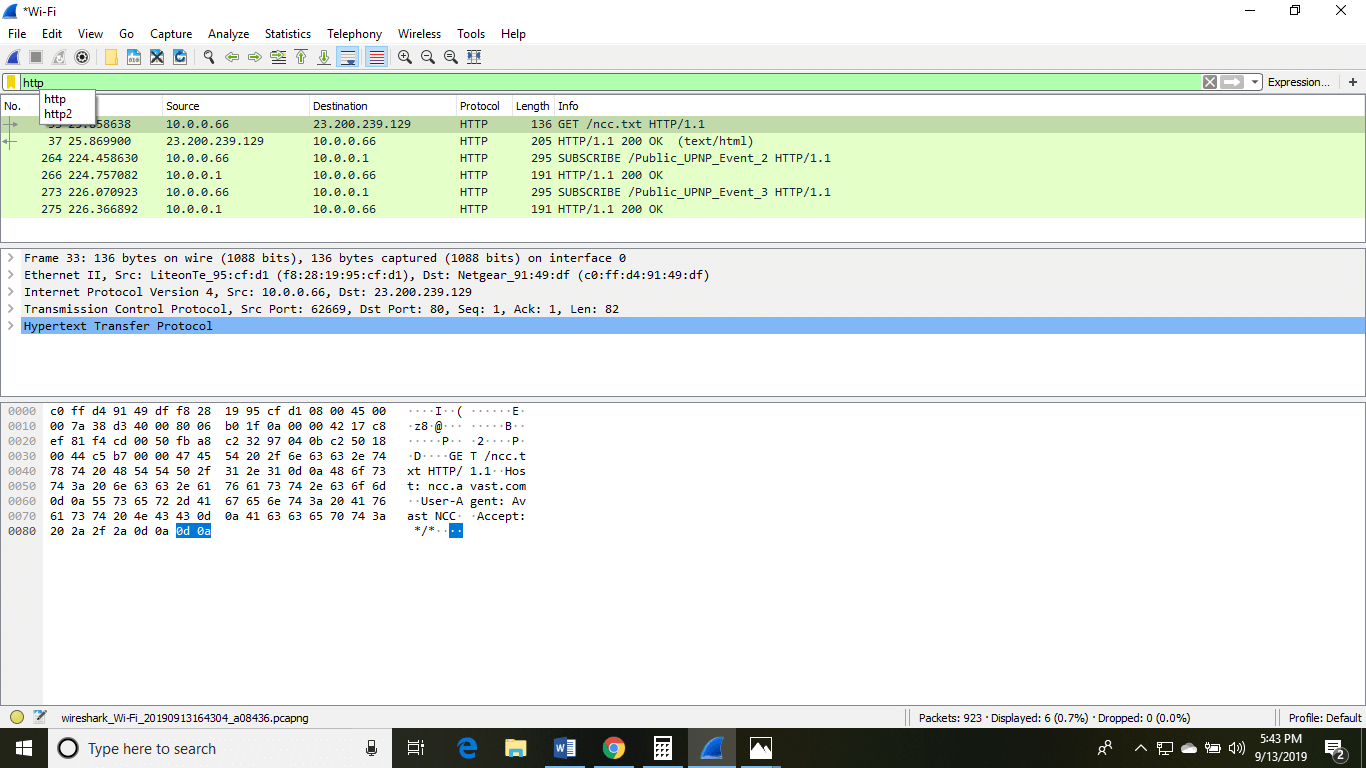
After connecting, you can watch the traffic below:



In view option on the menu bar, we can also change the view of the interface. You can change the number of things in the view menu. You can also enable or disable any option according to the requirements.

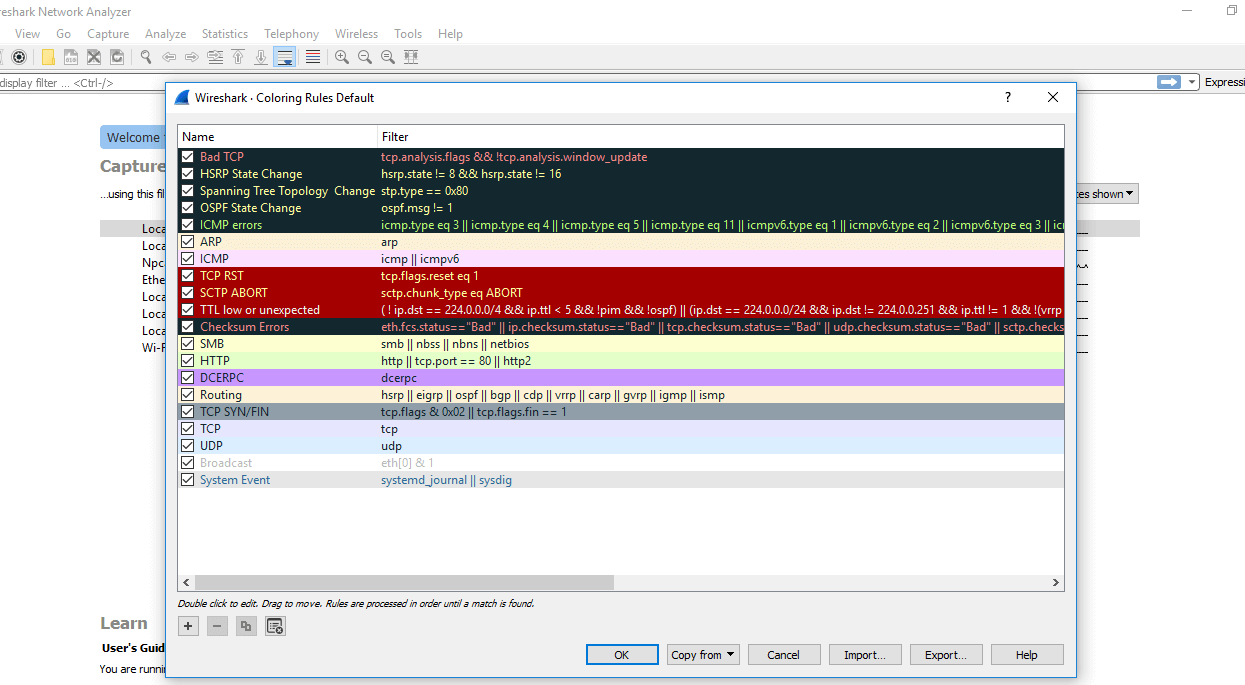


There is a filter block below the menu bar, from where a large amount of data can be filtered. For example, if we apply a filter for HTTP, only the interfaces with the HTTP will be listed.



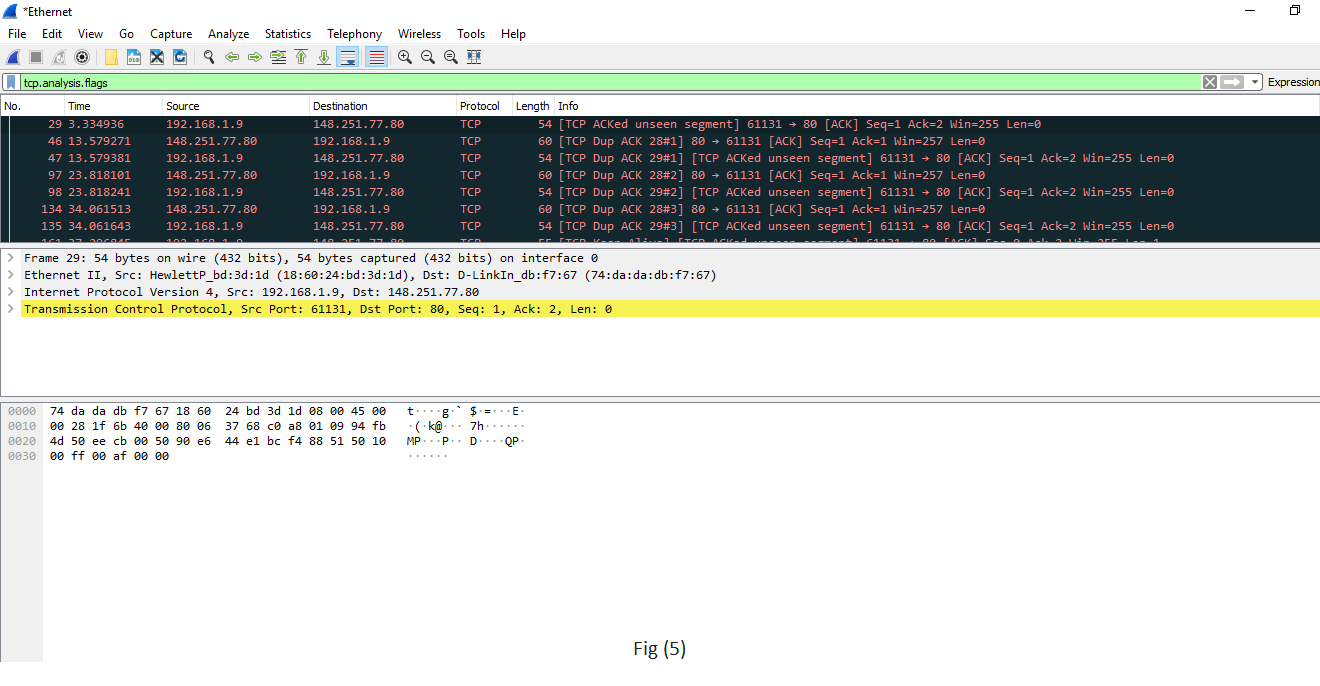
If you want to filter according to the source, right-click on the source you want to filter and select 'Apply as Filter' and choose '...and filter.'

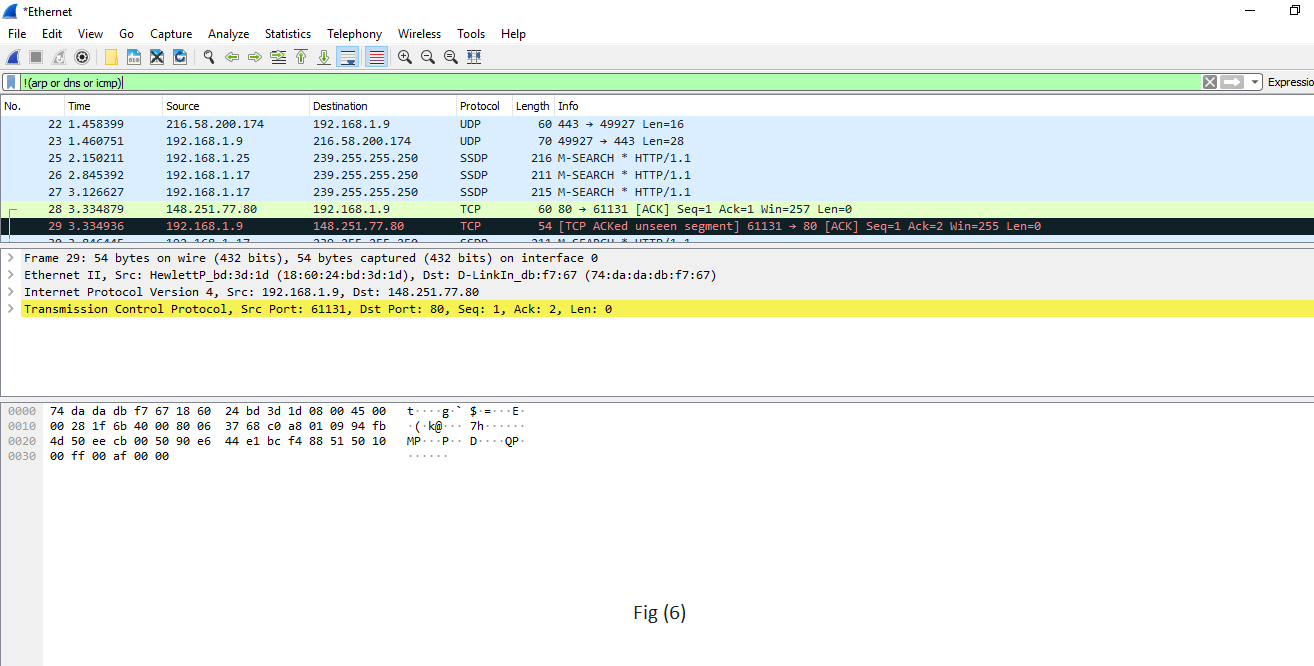
**Steps for the permanent colorization are:** click on the 'View' option on the menu bar and select 'Coloring Rules.' The table will appear like the image shown below:

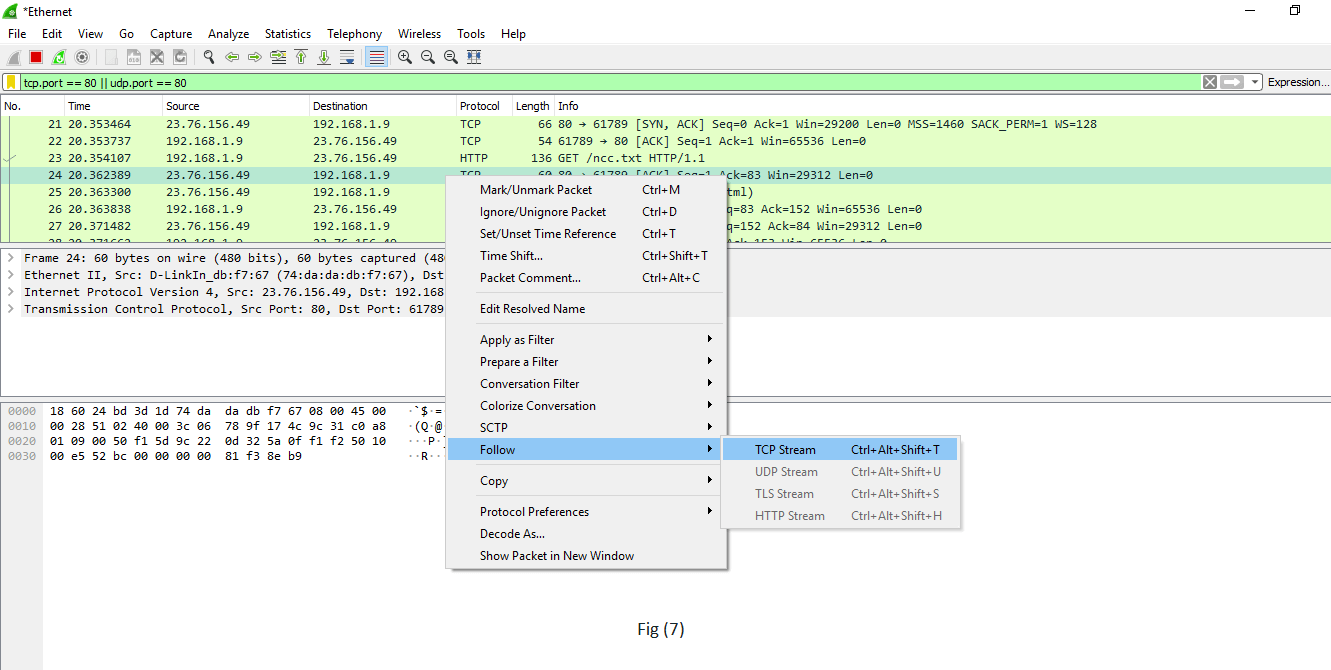


### Most used Filters in Wireshark

Whenever we type any commands in the filter command box, it turns **green** if your command is **correct**. It turns **red** if it is **incorrect** or the Wireshark does not recognize your command.







|  |  |
| --- | --- |
| **Filters** | **Description** |
| **ip.addr** Example- ip.addr==10.0.10.142 ip.src ip.dst | It is used to specify the IP address as the source or the destination. This example will filter based on this IP address as a source and a destination. If we want for a particular source or destination then, It is used for the source filter. It is used for the destination. |
| **protocol** Example- dns or http 'Dns and http' is never used. | This command filters based on the protocol. It requires the packet to be either dns protocol or http protocol and will display the traffic based on this. We would not use the command 'dns and http' because it requires the packet to be both, dns as well as http, which is impossible. |
| **tcp.port** Example: tcp.port==443 | It sets filter based on the specific port number. It will filter all the packets with this port number. |
| **4. udp.port** | It is same as tcp.port. Instead, udp is used. |
| **tcp.analysis.flags** example is shown in **fig(5)**. | Wireshark can flag TCP problems. This command will only display the issues that Wireshark identifies. Example, packet loss, tcp segment not captured, etc. are some of the problems. It quickly identifies the problem and is widely used. |
| **6.!()** For example, !(arp or dns or icmp) This is shown in **fig (6)**. | It is used to filter the list of protocols or applications, in which we are not interested. It will remove arp, dns, and icmp, and only the remaining will be left or it clean the things that may not be helpful. |
| Select any packet. Right-click on it and select 'Follow' and then select' TCP stream.' Shown in fig. (7). | It is used if you want to work on a single connection on a TCP conversation. Anything related to the single TCP connection will be displayed on the screen. |
| tcp contains the filter For example- tcp contains Facebook Or udp contains Facebook | It is used to display the packets which contain such words. In this, Facebook word in any packet in this trace file i.e., finding the devices, which are talking to Facebook. This command is useful if you are looking for a username, word, etc. |
| **http.request** For the responses or the response code, you can type http.response.code==200 | It will display all the http requests in the trace file. You can see all the servers, the client is involved. |
| **tcp.flags.syn==1** This is  tcp.flags.reset | This will display all the packets with the sync built-in tcp header set to 1. This will show all the packets with tcp resets. |

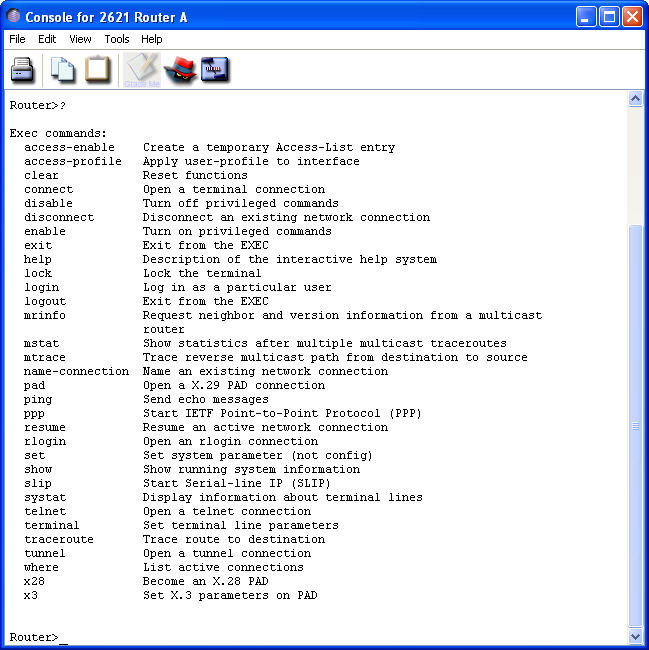
**Commands:**

1. User Prompt

Router>

2.View list of commands that can be entered in user mode

Router> ?



3. Enter privileged mode

Router> enable

Router#

4. View list of commands that can be entered in privileged mode

Router# ?



5. Exit privileged mode

Router# disable

Router>

6. Enter configuration mode

Router> enable

Router# configure terminal

Router> enable

Router(config)#

7. Configure Hostname

Router(config)# hostname Router1

Router1(config)#

8. View list of valid parameters to be used with enable command.

Configure an enable password of ‘acnlab’ that will not be encrypted when viewing the router configuration file

Configure an enable password of ‘cse2’ that will be encrypted

Router1(config)# enable ?

Router1(config)# enable password acnlab

Router1(config)# enable secret cse2

9. Configure an IP address for Ethernet and activate it

Router1(config)# interface fastethernet 0/1

Router1(config-if)# ip address 192.168.101.1 255.255.255.0

Router1(config-if)# no shut

10. Configure an IP address for a serial interface and activate it

Router1(config)# interface serial 0/1

Router1(config-if)# ip address 192.168.1.1 255.255.255.0

Router1(config-if)# no shut

11. Exit configuration mode

Router1(config-if)# Ctrl+Z

Router1#

12. Exit command-line interface

Router1# logout

13. Prompt for password entry in privileged mode

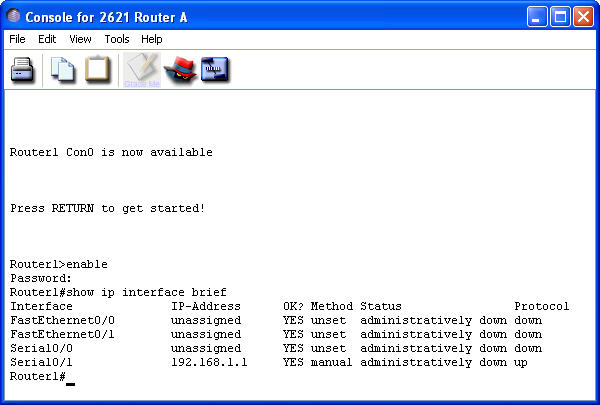
Router1> enable

password : cse2

Router1#

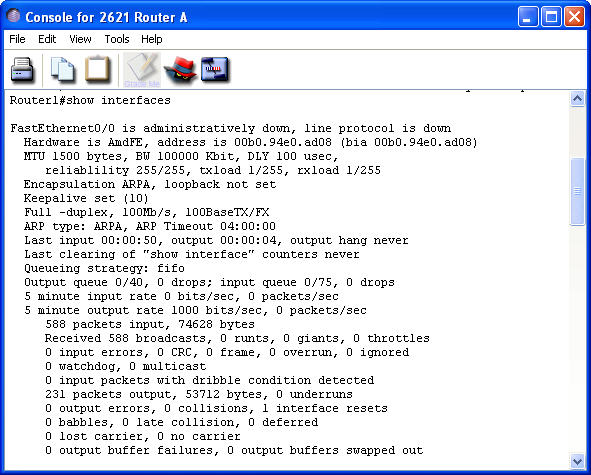
14. Summary of interfaces

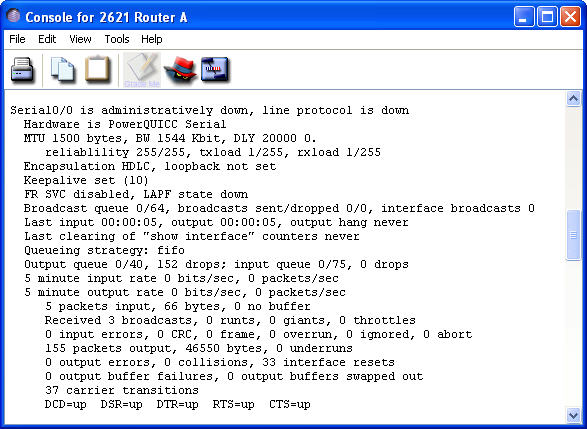
Router1# show ip interface brief



15. Detailed interface information

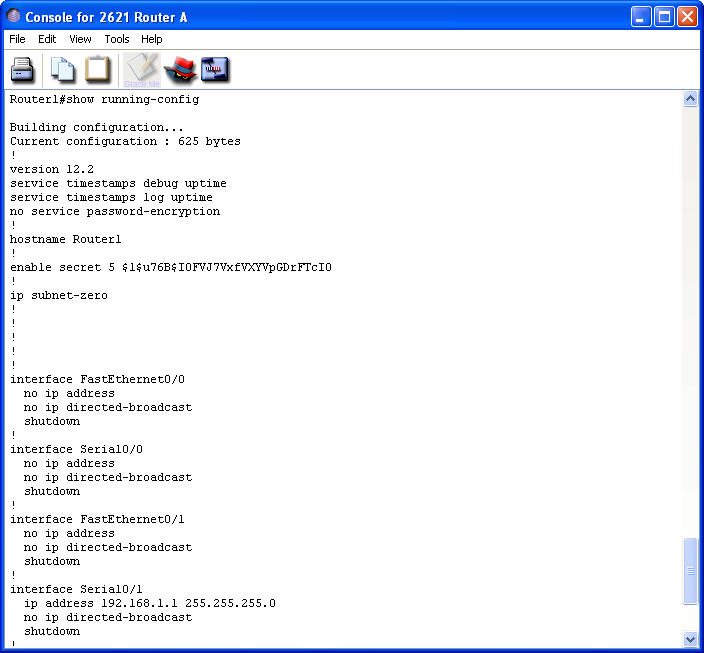
Router1# show interfaces





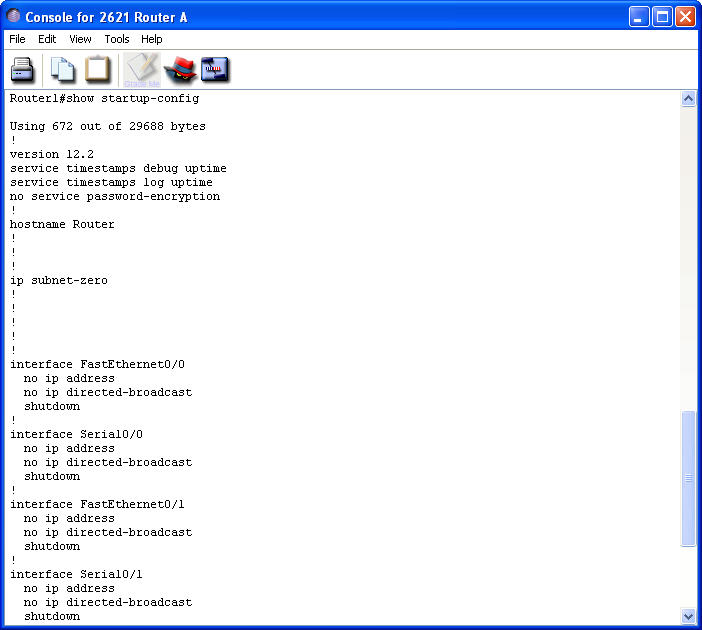
16. View active configuration in DRAM

Router1# show running-config



17. View saved configuration in NVRAM

Router1# show startup-config

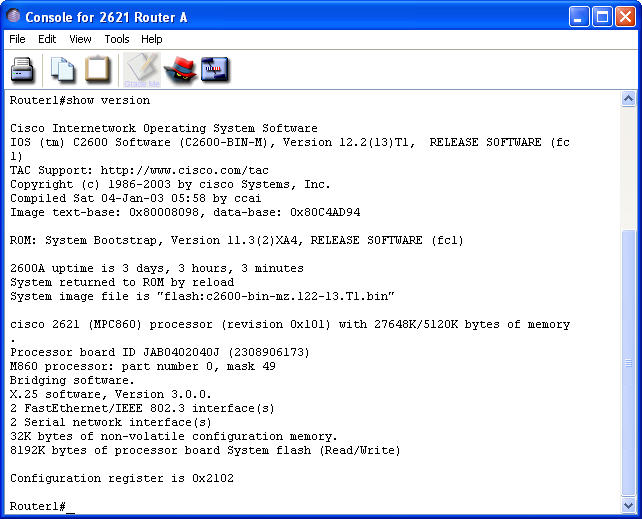


18. Save active(running) configuration to NVRAM

Router1# copy running-config startup-config

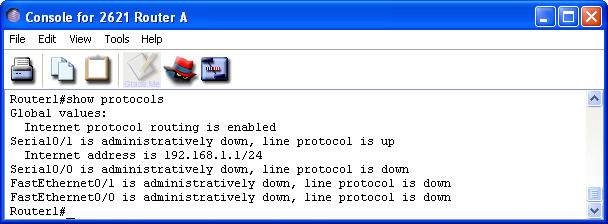
19. Version commands

Router1# show version



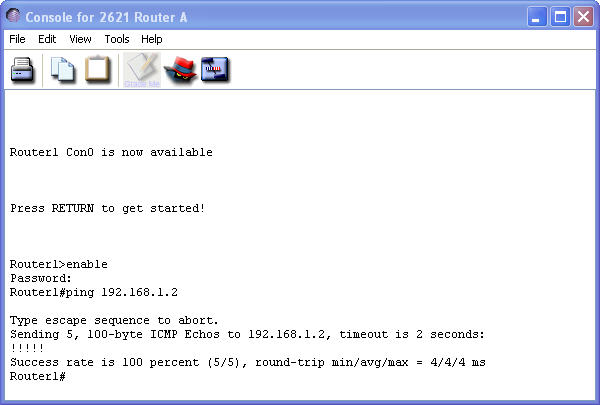
20. View current protocols on router

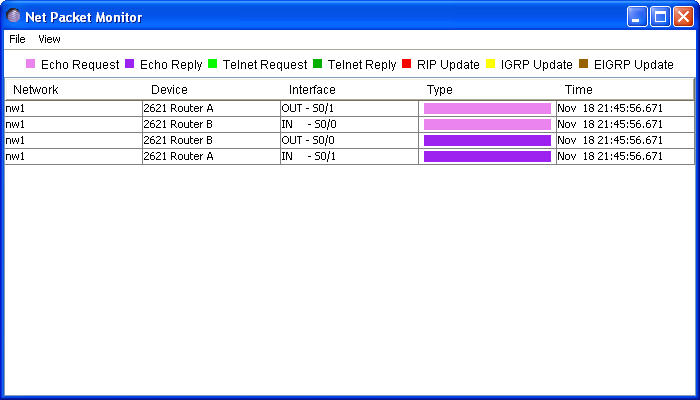
Router1# show protocols



21. Configure Router2 and ping Router2 from Router1

Router1# ping 192.168.1.2





**Commands:**

1. Configure a console password

Router1(config)# line console 0

Router1(config-line)#password cisco

Router1(config-line)#login

2. Configure a banner

Router1(config)# banner motd #

WELCOME TO ROUTER1 – Authorized Users Only !!!

3. Test Banner and Console Password

Router1#logout

enter

password: cisco

Router1>enable

password: cse2

Router1#



4. Configure a password for telnet users

Router1(config)#line vty 0 4

Router1(config-line)# password cisco

Router1(config)# login

5. Associate a name of Router2 with its remote ip address to Router1

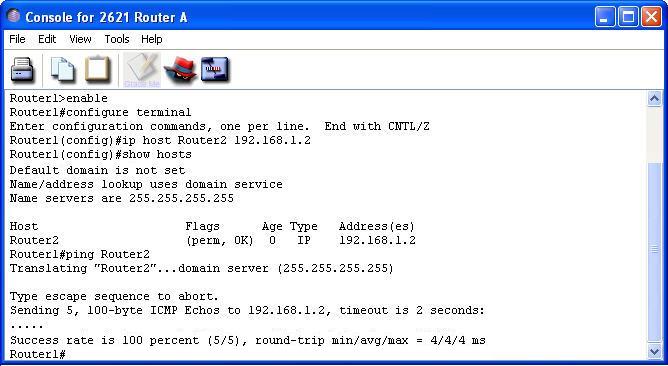
Router1(config)#ip host Router2 192.168.1.2

Router1# ping Router2

Success rate 100%

6. View Router1 host table

Router1# show hosts



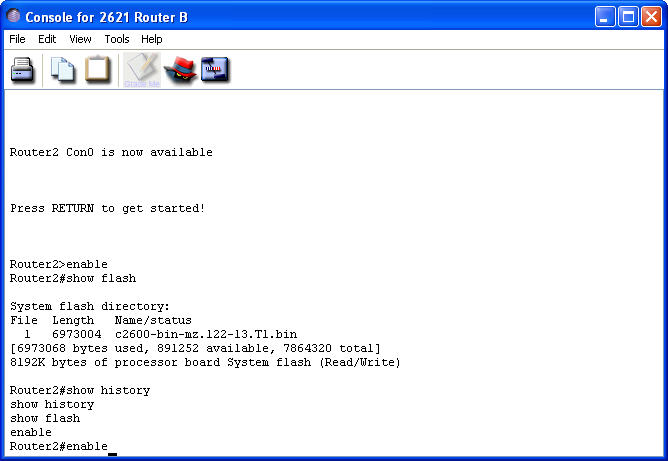
7. View Router1 flash memory

Router1# show flash

8. View history table and previously entered commands (ctrl+p)

Router1#show history

Router1#Ctrl+P



9. Configure interface

Router1#configure terminal

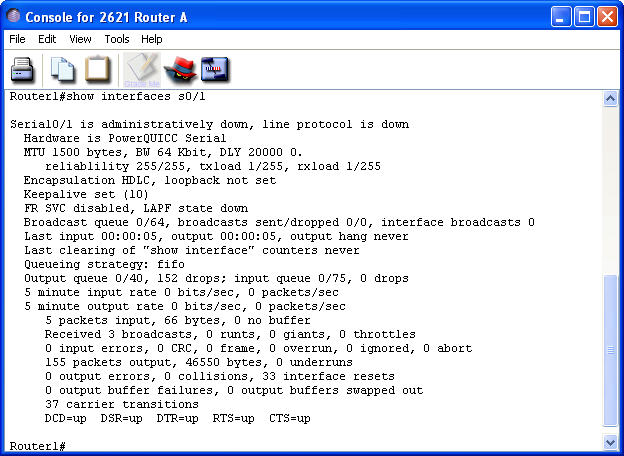
Router1(config)# interface s0/0

Router1(config-if)# bandwidth 64

Router1(config-if)# clock rate 64000

Router1(config-if)#Ctrl+Z

Router1# show interfaces serial 0/0



10. Add description to interface to serial0/0

Router1(config)#interface serial0/0

Router1(config-if)# description Serial Link to Router2

Router1(config-if)# exit

Router1(config)#exit

Router1#show interfaces serial0/0

