

JJINGO RONALD

2021/ITB/DAY/0089

COURSE: DATACOMMUNICATION AND COMPUTER NETWORKING 1

COMPUTER NETWORKS

Network Devices

INTRODUCTION:

It's a video by: NESO ACADEMY; https://Youtu.be/OpMm_QxCg3I combined with a video by SARADHI KANTHETY; <https://Youtu.be/8ONuDQF7gOY>

Outcomes:

- ✓ Listed all network devices, their structures and explained how they operate in different areas.

For example; Router, Repeater, Hub, Gateway, Switch, Modem, Bridge, Firewall (security device).

CONCEPTS:

NETWORK DEVICES

ROUTER:

Is a device that connects two or more packet-switched networks or sub networks. It serves two primary functions i.e., Managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same internet connection.



REPEATER

This is an electronic device that receives a signal and retransmits it. They are used to extend transmissions so that the signal can cover longer distances or be received on the other side of an obstruction.



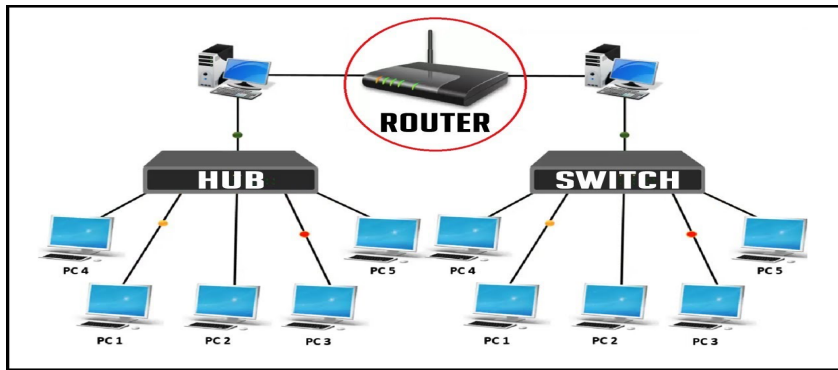
HUB:

This is a node that broadcasts data to every computer or Ethernet-based device connected to it. Also used to translate Data packets to all connected devices.



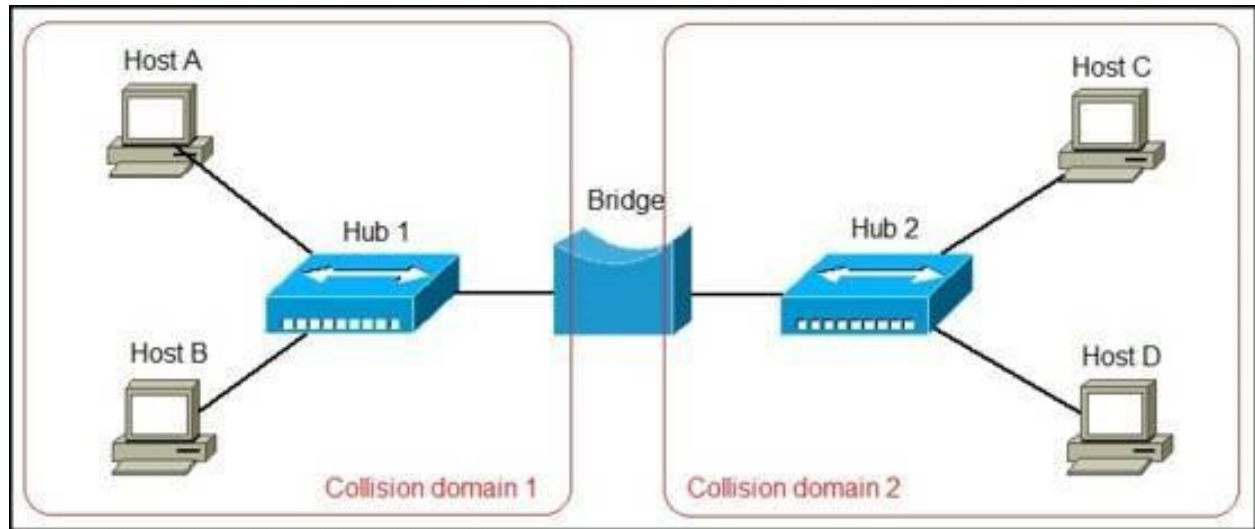
SWITCH:

A network switch is a networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device. Also used for error checking i.e., good packets will send to correct port the Data packets with errors will not be sent.



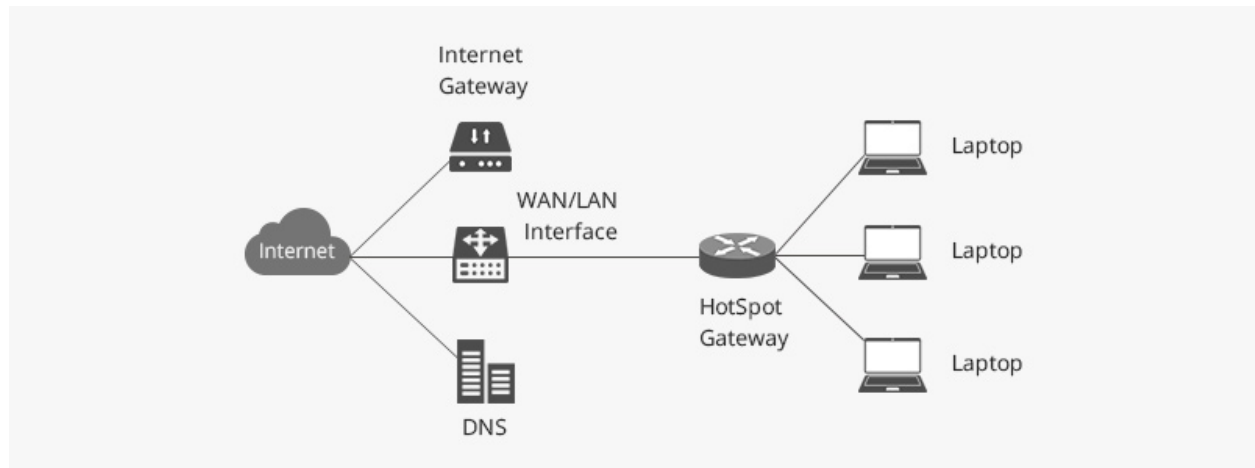
BRIDGE:

This is a class network device that's designed to connect networks at OSI Level 2/Data link layer. It is used in interconnecting two LANs working on the same Protocol i.e., (Data Link Layer).



GATEWAY:

Network gateways are tasked with linking networks by performing translation between different Protocols and data formats at the network boundary i.e., passing data to the networks of different networking models.



[VIDEO 2](#)

PHYSICAL TRANSMISSION MEDIA

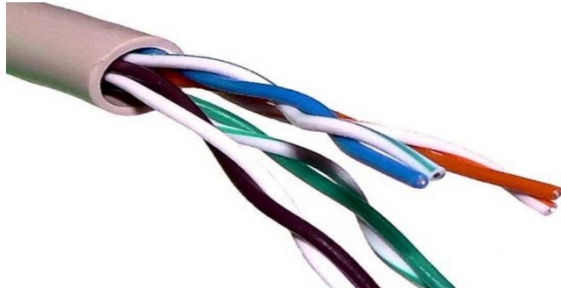


TYPES OF CABLES USED AS TRANSMISSION MEDIUM

- ❖ Twisted-Pair Cable
- ❖ Coaxial Cable
- ❖ Fiber Optic Cable

1. TWISTED PAIR CABLE

This is a type of cable that is made of two plastic insulated copper wires twisted together to form a single media. i.e., out of these two wires only one carries actual signal and another used for ground reference.



TYPES OF TWISTED PAIR CABLE

a) Unshielded twisted Pair cable:

These cables comprise of wires and insulators



b) Shielded Twisted Pair Cable:

These come with a braided, wired mesh that encases each pair of insulated copper wires.

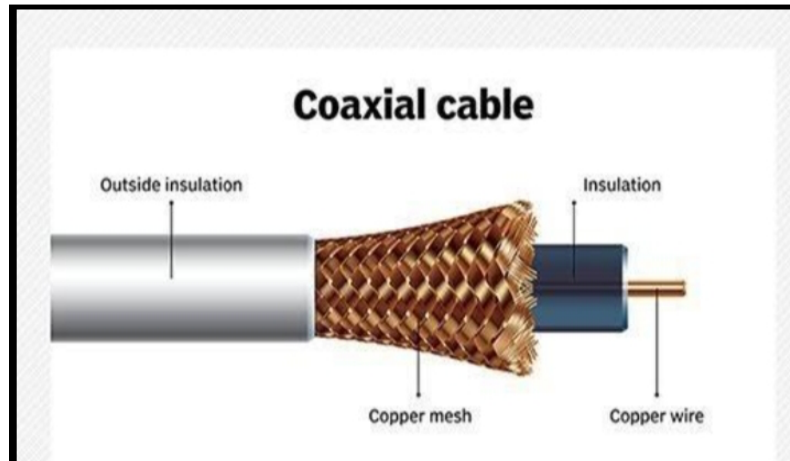


ADVANTAGES OF TWISTED PAIR CABLES

- They are Cheaper
- They are flexible
- They are light in weight and easy to install.

2. COAXIAL CABLE

This is a type of copper cable specially built with a metal shield and other components engineered to block signal interference. They are primarily used by cable TV companies to connect their satellite antenna facilities to customer homes or businesses.

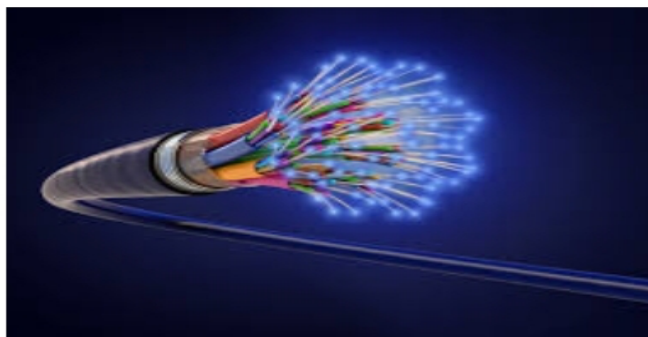


ADVANTAGES OF COAXIAL CABLES

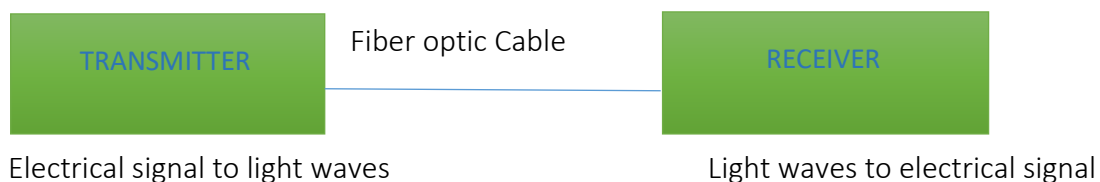
- ✓ They can transmit data much faster than twisted-pair.
- ✓ They are less prone to Noise.
- ✓ They can control multiple frequencies.

FIBER OPTIC CABLE

This is a cable that consists of one or more thin flexible fibers with a glass core through which light signals can be sent with very little loss of strength. It is also known as an optical-fiber cable since it contains one or more optical fibers that are used to carry light.



COMPONENTS OF FIBEROPTIC CABLE



ADVANTAGES OF FIBER OPTIC CABLE

- ✓ Minimizes the sparking Risk.
- ✓ Provides high bandwidth over long distance.

Ping

Ping is a command-line utility, available on virtually any operating system with network connectivity, that acts as a test to see if a networked device is reachable.

The ping command sends a request over the network to a specific device. A successful ping results in a response from the computer that was pinged back to the originating computer.

What does Ping stand for?

According to the author, the name Ping comes from sonar terminology. In sonar, a ping is an audible sound wave sent out to find an object. If the sound hits the object, the sound waves will reflect, or echo, back to the source. The distance and location of the object can be determined by measuring the time and direction of the returning sound wave.

Similarly, the ping command sends out an *echo request*. If it finds the target system, the remote host sends back an *echo reply*. The distance (number of hops) to the remote system can be determined from the reply, as well as the conditions in-between (packet loss and time to respond). While the author of the ping utility said the name of the program was simply based on the sound of sonar, others sometimes say that Ping is an acronym for Packet InterNet Groper. The Ping utility uses the echo request, and echo reply messages within the Internet Control Message Protocol (ICMP), an integral part of any IP network. When a ping command is issued, an echo request packet is sent to the address specified. When the remote host receives the echo request, it responds with an echo reply packet.

```
> ~ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
Request timeout for icmp_seq 0
64 bytes from 8.8.8.8: icmp_seq=1 ttl=113 time=177.138 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=113 time=147.257 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=113 time=147.761 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=113 time=147.188 ms
c64 bytes from 8.8.8.8: icmp_seq=5 ttl=113 time=155.409 ms
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 5 packets received, 16.7% packet loss
round-trip min/avg/max/stddev = 147.188/154.951/177.138/11.521 ms
> ~
```

Ipconfig

The ipconfig is a Windows command-line utility used often to troubleshooting computer network issues. If you are a Linux user, this utility is similar to ifconfig. This is often used to determine the local IP address, subnet mask, the gateway address, and other network configuration of a computer. Additionally, this tool is used to refresh DHCP (Dynamic Host Configuration Protocol) and DNS (Domain Name System) settings

While most of the information provided by the ipconfig command-line utility can be found via a more user-friendly graphical interface, sometimes that interface may not be available and command prompt is your only available option. If you are a help desk technician or a network professional, it is recommended that you understand the command-line method of retrieving a computer's network configuration, and in some cases, performing network functions.

```
Command Prompt
C:\>ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : hitronhub.home
    IPv6 Address. . . . . : 2607:fea8:3d20:949::2a
    IPv6 Address. . . . . : 2607:fea8:3d20:949:fd03:b57e:3676:2037
    IPv6 Address. . . . . : fd00:6477:7d99:6612:fd03:b57e:3676:2037
    Temporary IPv6 Address. . . . . : 2607:fea8:3d20:949:ad4f:576c:5f2b:b1f0
    Temporary IPv6 Address. . . . . : fd00:6477:7d99:6612:ad4f:576c:5f2b:b1f0
    Link-local IPv6 Address . . . . . : fe80::fd03:b57e:3676:2037%8
    IPv4 Address. . . . . : 192.168.0.98
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::6677:7dff:fe99:6612%8
                                192.168.0.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\>
```


Tracert

The TRACERT diagnostic utility determines the route to a destination by sending Internet Control Message Protocol (ICMP) echo packets to the destination. In these packets, TRACERT uses varying IP Time-To-Live (TTL) values. Because each router along the path is required to decrement the packet's TTL by at least 1 before forwarding the packet, the TTL is effectively a hop counter. When the TTL on a packet reaches zero (0), the router sends an ICMP "Time Exceeded" message back to the source computer.

TRACERT sends the first echo packet with a TTL of 1 and increments the TTL by 1 on each subsequent transmission, until the destination responds or until the maximum TTL is reached. The ICMP "Time Exceeded" messages that intermediate routers send back show the route. Note however that some routers silently drop packets that have expired TTLs, and these packets are invisible to TRACERT.

TRACERT prints out an ordered list of the intermediate routers that return ICMP "Time Exceeded" messages. Using the -d option with the tracert command instructs TRACERT not to perform a DNS lookup on each IP address, so that TRACERT reports the IP address of the near-side interface of the routers.

```
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.

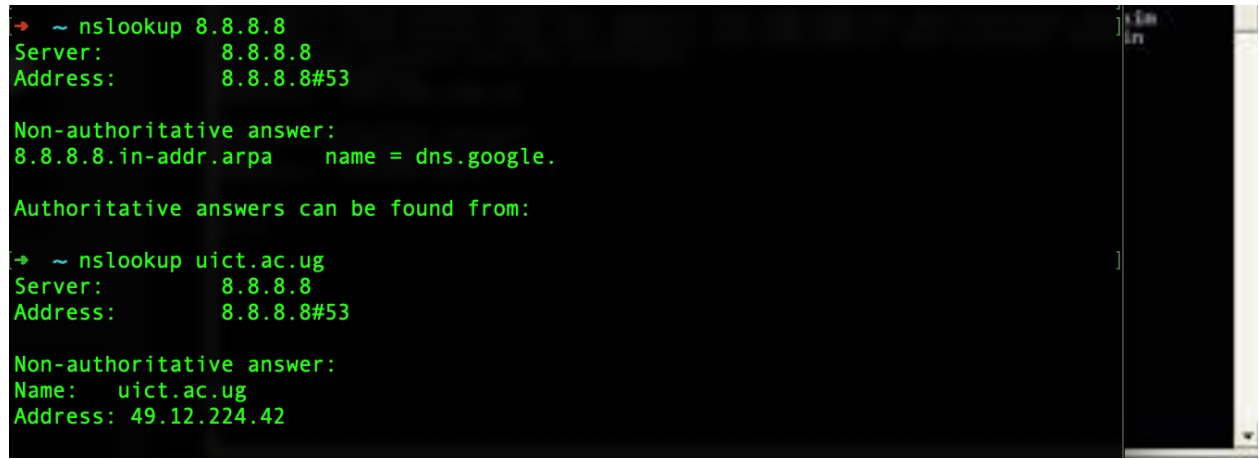
C:\Users\Admin>
```

nslookup

nslookup is the name of a program that lets an Internet server administrator or any computer user enter a **host name** (for example, "whatismyip.com") and find out the corresponding **IP address** or domain name system (**DNS**) record. The user can also enter a command for it to do a reverse DNS lookup and find the host name for an IP address that is specified.

nslookup is used to troubleshoot server connections or for security reasons. Such reasons include guard against phishing attacks, in which a domain name is altered -- for example, by substituting the numeral 1 for a lowercase l -- to make an unfriendly site look friendly and familiar (joes1lowerprices.com vs. joeslowerprices.com).

DNS, or nslookup, also helps deter cache poisoning, in which data is distributed to caching resolvers, posing as an authoritative origin server.



```
→ ~ nslookup 8.8.8.8
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
8.8.8.8.in-addr.arpa    name = dns.google.

Authoritative answers can be found from:

→ ~ nslookup uict.ac.ug
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   uict.ac.ug
Address: 49.12.224.42
```

Packet Tracer

Packet Tracer is a free network simulator tool for certification exam preparation, particularly for CCNA students. It's available directly through the Cisco Networking Academy. Download and install the Packet Tracer software by signing up for the Introduction to Packet Tracer course, which teaches you the basics of using the tool.

