Network Basics

What’s a Network?

**To do:**Go through the activity to the end

What’s a Network?

A computer **network** is a collection of computers, servers, network devices, peripherals, or other devices connected to one another to share data. It doesn't matter whether the network contains two or thousands of machines; the concept is essentially the same. The devices on a network may be linked through cables, telephone lines, radio waves, or satellites.

|  |
| --- |
| *A network illustration* |

A network provides services to its users. In the past, these services have included access to shared files, folders, printers, and applications (email, database, etc.). Modern networks provide more distinct services, including web applications, voice over IP (VoIP), and multimedia conferencing.

Networks of different sizes are classified in different ways. A network in a single location is often called a **Local Area Network (LAN)**. This definition includes many different types and sizes of networks though. It can include both household networks with a couple of computers and enterprise networks with hundreds of servers and thousands of computers.

Networks in different geographic locations but with shared links are called **Wide Area Networks (WAN).**

A computer network has the following features:

|  |
| --- |
| *Features of networks* |

* **Performance:** Performance of a computer network is measured in terms of response time. On an efficient network, the response time of transmitted and received data from one device to another is minimal.
* **Data Sharing:** It is one of the main reasons why we use a computer network between different systems.
* **Backup:** A computer network must backup all the shared data, and keep that data on servers in order to recover the data faster in case of failures.
* **Reliability:** There should not be any failure in the network, but if it occurs the recovery from failure should be fast.
* **Security:** A computer network should be secure so that the data exchanged over a network should be safe from unauthorized access. Also, the transmitted data should be received without any loss.
* **Scalability:** A computer network should be scalable means adding new devices to the already existing computer network should always be possible.
* **Software and hardware compatibility:** A computer network must not limit all the computers to use the same software and hardware, instead, it should allow the users to use different software and hardware configurations on the network without any compatibility issues.

Q: What is a Computer Network?  
A: A computer network is a connection network between two or more nodes using [Physical Media](https://lms.clarusway.com/mod/lesson/view.php?id=1839" \o "Physical Media) Links viz., cable, or wireless to exchange data over pre-configured services and Protocols. A computer network is a collective result of – Electrical Engineering, Computer Science, Telecommunication, Computer Engineering, and Information Technology involving their theoretical as well as practical aspects into action. The most widely used Computer Network of Today is the Internet which supports the World Wide Web (WWW).

Local Area Network (LAN)

Just as the name implies, a **local area network (LAN)** is usually restricted to spanning a particular geographic location such as an office building, a single department within a corporate office, or even a home office. Due to the technological advances, we’re almost free from the restrictions forced by both the size and the distance coverage of LANs.

To easily manage the networks, it’s a good idea to split LANs according to the department divisions. For example, we can create a LAN for *Accounting*, and another for *Marketing*. The figure shows two separate LANs.

|  |
| --- |
| *Two separate LANs* |

In the above figure, there are two LANs: Accounting and Marketing. Any device connected to the Marketing LAN can access the resources inside the Marketing LAN—in this case, the servers and printer. There are two problems with this:

* One must be physically connected to the LAN to get the resources from it.
* Nobody can connect from one LAN to another.

This is a typical network issue that’s easily fixed by using a device called **router** to connect the two LANs, as shown below.

|  |
| --- |
| *A network with two LANs* |

And the problem is solved!

The devices *switch* and *router* will be explained in detail in the following sections.

Q: Explain what is LAN?  
A: A LAN or Local Area Network is the network between devices that are located within a small physical location. It can be either wireless or wired. One LAN differs from another based on the following factors:  
**Topology:** The arrangement of nodes within the network  
**Protocol:** Refer to the rules for the transfer of data  
**Media:** These devices can be connected using optic fibers, twisted-pair wires, etc.

- Interview Q&A

Common Network Components

**Node, Stations, and Hosts:** A **node** is any device that can connect to a network. The term **node** can be used to describe *endpoint devices*, such as *computers, laptops, servers, IP phones, smartphones, or printers*, and *connecting or forwarding devices*, such as *switches* and *routers*. A **node** on a wireless network is often called a *station*.

The term **host** is often used in *TCP/IP networking* to mean an *end system device*, such as a *computer*, with a unique IP address on the network.

**Workstations:** Workstation is a client **machine** used to deploy an **application** or **server**. They are usually powerful **computers** that have more than one CPU and its resources are available to other users on the network. Workstations are often equipped with systems for end-users to use daily.

**Servers:** Servers are also powerful **computers**. They are “at the service” of the network and run specialized software known as the network operating system to maintain and control the network. Servers are highly specialized and handle important labor-intensive jobs. In order to get better performance, a single task is often assigned to a dedicated server. Here’s a list of common dedicated servers:

* **File Server** - Stores and manages files
* **Mail Server** - It's the network’s post office; handles email functions
* **Print Server** - Manages printers on the network
* **Web Server** - Manages web-based activities by running Hypertext Transfer Protocol (HTTP) for storing web content and accessing web pages
* **Application Server** - Manages network applications
* **Telephony Server** - Handles the call center and call routing
* **Proxy Server** - Handles tasks in the place of other machines on the network, particularly an internet connection.

Whether servers are designated for simple or complex network tasks, they can maintain the network’s data integrity by backing up the network’s software and providing redundant hardware (for fault tolerance).

In the below figure, you can see a network topology consists of workstations and servers. Also notice that the hosts can access the servers across the network, which is the general idea of having a network!

|  |
| --- |
| *A classic network structure* |

**Transmission Media:** A link between network nodes is created using some form of transmission media like cables, or radio waves.

**Local Network Devices, Segments, and Backbones:** Relatively few networks are established to connect the hosts directly. Instead of direct links among them, each host is connected to a central node, such as a **switch** or **wireless access point**. The central node provides a forwarding function, that is, receives the data from one node and re-transmits it to the others.

A central device such as a **switch** implies that the connected nodes are part of the same physical network and use the same type of transmission media. The term **switching** is used for this forwarding function taking place within the same physical network. The addresses of interfaces within the same network are described as **local addresses**.

The term **segment** can be used to refer to a specific physical region of a network, though the scope of a segment depends on the exact technology in use. One typical usage now is to describe the link between a computer and a switch. Another usage is to refer to a region of the network where all the nodes use the same type of transmission media and have the same bandwidth.

A network is typically divided into segments either to cope with the physical restrictions of the network media used or to improve performance or to improve security (or all three). A **backbone** describes a fast link among other segments of a network. The backbone carries all the communications occurring between nodes in separate segments.

Q: What do you mean by a Node?  
A: The intersection point in a network is called a Node. Nodes can send or receive data/ information within a network. For example, if two computers are connected to form a network, there are 2 nodes in that network. Similarly, in the case of adding more computers, there will be more nodes and so on. It is not necessary for a node to be a computer, it can be any communication device such as a printer, servers, modems, etc..

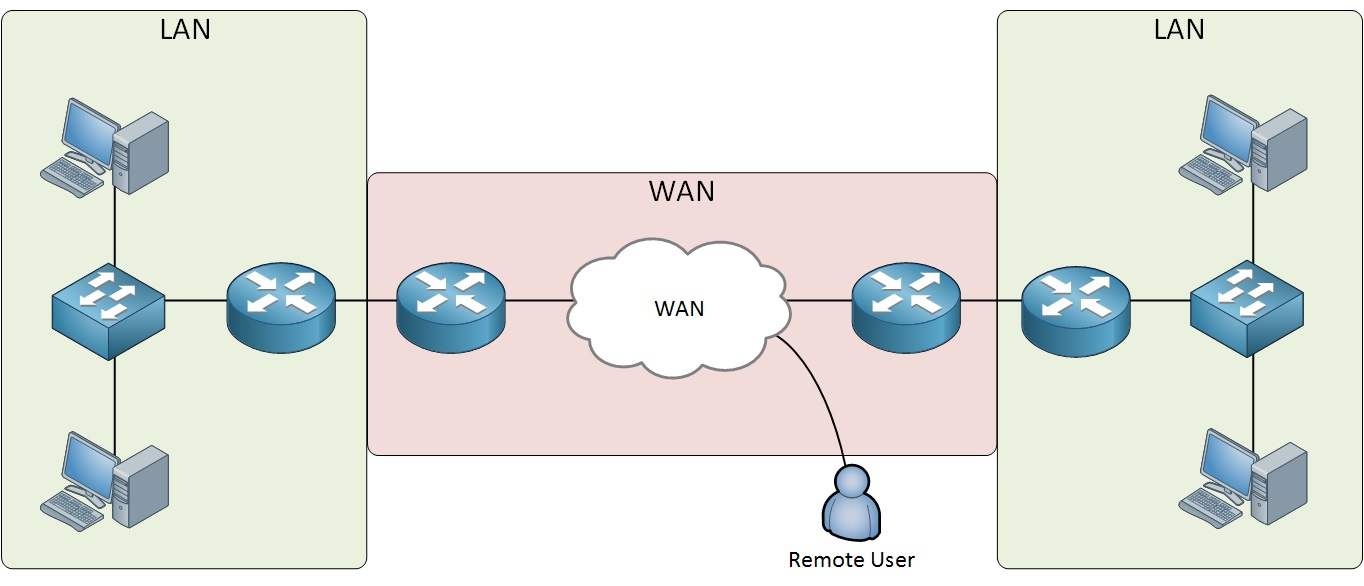
- Interview Q&A

Local and remote networks can be joined using nodes such as Routers  that can make distinctions between logically separate networks.

Wide Area Network (WAN)

Our own networks are called **LANs** (Local Area Network). We own and operate these networks. It’s called a **“local”** area network since all devices that make up the LAN are close to each other. Perhaps in one building or a few buildings close to each other (called a **campus**).

When we need to access other remote networks or give others access to our LAN, we need a **WAN (Wide Area Network)**. As the name implies, WANs cover *large geographical areas*. This could be a network between two cities or as large as the **Internet**.



On the **LAN**, the dominant protocol that we use is **Ethernet**. For **WAN**, there are dozens of technologies and protocols we can choose from.

Below is the list of some differences between WAN and LANs:

* WANs usually need a router.
* WANs span larger geographic areas and/or can link diverse locations.
* WANs are usually slower.
* We can choose when and how long we connect to a WAN. A LAN is all or nothing—our workstation is connected to it either permanently or not at all.
* WANs can utilize either private or public data transport media such as phone lines.

We get the word Internet from the term internetwork. An internetwork is a type of LAN and/or WAN that connects a bunch of networks or intranets. In an internetwork, hosts still use hardware addresses to communicate with other hosts on the same LAN. However, they use logical addresses (IP addresses) to communicate with hosts on a different LAN. And routers are the devices that make this possible.

Q: What is WAN?  
A: WAN stands for Wide Area Network. It is an interconnection of computers and devices that are geographically dispersed. It connects networks that are located in different regions and countries.

- Interview Q&A

Formun Üstü

Previous

Formun Altı

Formun Üstü

Next

Formun Altı

Which one is true regarding differences between a LAN and a WAN?

Select one:



WANs require a router.



WANs cover larger geographical areas.



WANs can utilize either private or public data transport.



All of the above.

Physical Network Topologies

**To do:**Go through the activity to the end

Physical Network Topologies

Network topology is the arrangement of the various nodes of a computer network. Essentially, it is the topological structure of a network and may be depicted **physically** or **logically** which are the two basic categories of network topologies.

The shape of the cabling layout used to link devices is called the **physical topology** of the network. This refers to the *layout of cabling, the locations of nodes*, *the interconnections between the nodes* and *the cabling*. The physical topology of a network is determined by:

* the capabilities of the network access devices and media,
* the level of control or fault tolerance desired,
* the cost associated with cabling or telecommunications circuits.

In opposition to the *Physical Topology*, the **logical topology** is the way that the *signals act on the network media*, or the *way that the data passes through the network* from one device to the next without regard to the physical interconnection of the devices.

**💡Tip:**

* A network’s logical topology is not necessarily the same as its physical topology.

The logical topologies are generally determined by network protocols as opposed to being determined by the physical layout of cables, wires, and network devices or by the flow of the electrical signals. In many cases, the paths that the electrical signals travel among the nodes may closely match the logical flow of data. That is why, the terms *logical topology* and *signal topology* can be interchangeably used.

Here’s a list of the topologies mostly used nowadays:

* Bus
* Star
* Ring
* Mesh
* Tree
* Point-to-point
* Point-to-multipoint
* Hybrid

|  |
| --- |
| *Physical network topologies* |

Q: What do you mean by network topology?  
A: Network topology specifies the layout of a computer network. It shows how devices and cables are connected to each other. Some types of topologies are: Bus, Star, Ring, Mesh, etc.

- Interview Q&A

The shape of the cabling layout used to link devices is called the physical topology of the network.

The logical topology , is the way that the signals act on the network media, or the way that the data passes through the network from one device to the next without regard to the physical interconnection of the devices.

Bus Topology

A bus topology consists of a single cable ( the *bus* ) with a terminator at each end. All nodes (file server, workstations, and peripherals) are connected to this cable. The signal travels down the bus in both directions from the source and is received by all nodes connected to the cable. The bus is terminated at both ends of the cable to absorb the signal when it has passed all connected devices.

|  |
| --- |
| *The bus topology* |

This type of physical bus topology is no longer in widespread use. Bus networks are comparatively difficult to reconfigure (adding or removing nodes can disrupt the whole network), impose limitations on the maximum number of nodes on a segment of cable, and are difficult to troubleshoot (a cable fault could be anywhere on the segment of cable). Perhaps most importantly, a fault anywhere in the cable means that all nodes will be unable to communicate.

The logical bus topology, however, remains the basis of most local networks.

**Advantages of bus topology:**  
1. Easy installation, each cable needs to be connected with the backbone cable.  
2. Fewer cables required than mesh and star topology (We'll see these topologies in the following lessons)

**Disadvantages of bus topology:**  
1. Difficulty in fault detection.  
2. Not scalable as there is a limit of how many nodes can be connected.

Star Topology

In star topology, every node (computer workstation or any other peripheral) is connected to a central node called **hub** or **switch**. The network does not necessarily have to resemble a star to be classified as a star network, but all of the nodes on the network must be connected to one central device. All traffic that traverses the network passes through the central hub.

The star topology is the most widely used physical topology. It is easy to reconfigure and easy to troubleshoot because all data goes through a central point, which can be used to monitor and manage the network. Faults are automatically isolated to the node (network card), or the hub, switch, or router at the center of the star.

|  |
| --- |
| *The star topology* |

**Advantages of Star topology:**  
1. Less expensive because each device only needs one I/O port and needs to be connected with a hub with one link.  
2. Easier to install.  
3. Less amount of cables required because each device needs to be connected with the hub only.  
4. Robust, if one link fails, other links will work just fine.  
5. Easy fault detection because the link can be easily identified.

**Disadvantages of Star topology:**  
1. If the central node goes down every node goes down, none of the devices can work without the central node.  
2. The central node requires more resources and regular maintenance because it is the central system of star topology.

Q: Describe star topology  
A: Star topology consists of a central hub that connects the nodes. This is one of the easiest way to setup and maintain.

- Interview Q&A

Q: What is the disadvantage of a star topology?  
A: One major disadvantage of star topology is that once the central hub or switch damaged, the entire network becomes unusable.

- Interview Q&A

Formun Üstü

Previous

Formun Altı

Formun Üstü

Next

Formun Altı

Which of the following is a disadvantage of the star topology?

Select one:



When the central concentrating device experiences complete failure, all attached devices lose connectivity to the rest of the network.

Congratulations!



When a single port on the central concentrating device fails, the entire network loses connectivity.



In a star topology, a more expensive type of host must be used compared to the host used when implementing a physical bus



It is more difficult to add stations and troubleshoot than with other topologies.

Physical Network Topologies

**To do:**Go through the activity to the end

Ring Topology

A network topology is set up in a circular fashion in which data travels around the ring in one direction and each device on the right acts as a repeater to keep the signal strong as it travels. Each device incorporates a receiver for the incoming signal and a transmitter to send the data to the next device in the ring. If a device wants to send data to another device then it sends the data in one direction, if the received data is intended for other devices then it forwards this data until the intended device receives it.

|  |
| --- |
| *The ring topology* |

The physical ring topology is no longer used on LANs but it does remain as a feature of many WANs. Two ring systems (dual counter-rotating rings) can be used to provide fault tolerance. These dual rings allow the system to continue to operate if there is a failure in one ring.

**Advantages of Ring Topology:**  
1. Easy to install.  
2. Management is easier because to add or remove a device from the topology only requires changing just two links.

**Disadvantages of Ring Topology:**  
1. A link failure can fail the entire network as the signal will not travel ahead due to failure.  
2. Data traffic issues, since all the data is circulated in a ring.

Q: What are some drawbacks of implementing a ring topology?  
A: In case one workstation on the network suffers a malfunction, it can bring down the entire network. Another drawback is that when there are adjustments and reconfigurations needed to be performed on a particular part of the network, the entire network has to be temporarily brought down as well.

- Interview Q&A

Formun Üstü

Previous

Formun Altı

Formun Üstü

Next

-------------------------------------------------------------------------------------

Mesh Topology

**Mesh network topologies** are commonly used in **WANs**, especially public networks like the Internet. In theory, a mesh network requires that each device has a point-to-point link with every other device on the network (**fully connected**). This approach is normally impractical, however. The number of links required by a full mesh is expressed as n(n-1)/2, where "n" is the number of nodes. For example, a network of just 4 nodes would require 6 links, while a network of 40 nodes would need 780 links!

|  |
| --- |
| *The mesh topology* |

Consequently, often a "**hybrid**" approach is used with only the most important devices interconnected in the mesh, perhaps with extra links for fault tolerance and redundancy. In this case, the topology is referred to as a **partial mesh.**

|  |
| --- |
| *Partial mesh topology* |

**Advantages of Mesh topology:**

1. No data traffic issues as there is a dedicated link between two devices which means the link is only available for those two devices.
2. Mesh topology is reliable and robust as a failure of one link doesn’t affect the other links and the communication between other devices on the network.
3. Mesh topology is secure because there is a point to point link thus unauthorized access is not possible.
4. Fault detection is easy.

**Disadvantages of Mesh topology:**

1. The amount of wires required to connect each system is tedious.
2. Since each device needs to be connected with other devices, the number of I/O ports required must be huge.
3. Scalability issues because a device cannot be connected with a large number of devices with a dedicated point to point link.

Q: What is mesh topology?  
A: Mesh topology is a setup wherein each device is connected directly to every other device on the network. Consequently, it requires that each device has at least two network connections.

- Interview Q&A

Q: What is one advantage of mesh topology?  
A: In the event that one link fails, there will always be another available. Mesh topology is actually one of the most fault-tolerant network topology.

- Interview Q&A

Formun Üstü

Previous

Formun Altı

Formun Üstü

Next

Formun Altı

You have completed 100% of th

Formun Altı

Tree Topology

A tree topology combines characteristics of linear bus and star topologies. It consists of groups of star-configured workstations connected to a linear bus backbone cable. Tree topologies allow for the expansion of an existing network.

|  |
| --- |
| *The tree topology* |

**Advantages of tree topology:**  
1. It is scalable. Secondary nodes allow more devices to be connected to a central node.  
2. Point to point connection of devices.  
3. Having different levels of network makes it more manageable hence easier fault identification and isolation.

**Disadvantages of tree topology:**  
1. Maintenance of the network may be an issue when the network spans a great area.  
2. Since it is a variation of bus topology, if the backbone fails, the entire network is down.

Formun Üstü

Previous

Formun Altı

Formun Üstü

Next

Formun Altı

Physical Network Topologies

**Done:**Go through the activity to the end

Point-to-Point Topology

It's the simplest topology where there is a permanent link between two endpoints. These endpoints may be hubs, routers, switches, computers, etc. which give you one communication path. Switched point-to-point topologies are the basic model of conventional telephony.

* **Permanent (dedicated)**

Easiest to understand, the variations of point-to-point topology, is a point-to-point communications channel that appears, to the user, to be permanently associated with the two endpoints. A children’s tin can telephone is one example of a physical dedicated channel.

Within many switched telecommunications systems, it is possible to establish a permanent circuit. One example might be a telephone in the lobby of a public building, which is programmed to ring only the number of a telephone dispatcher. “Nailing down” a switched connection saves the cost of running a physical circuit between the two points. The resources in such a connection can be released when no longer needed.

* **Switched**

Using circuit-switching or packet-switching technologies, a point-to-point circuit can be set up dynamically and dropped when no longer needed. This is the basic model of conventional telephony.

|  |
| --- |
| *Point-to-point topologies* |

Point-to-Multipoint Topology

A **point-to-multipoint** topology consists of a succession of connections between an *interface* on one router and *multiple destination routers*—one point of connection to multiple points of connection. Each of the routers and every one of their interfaces involved in the point-to-multipoint connection is part of the same network.

|  |
| --- |
| *Point-to-multipoint topology* |

The below figure shows another prime example of a point-to-multipoint network: a college or corporate campus.

|  |
| --- |
| *Point-to-multipoint topology* |

Hybrid Topology

**Hybrid topology** means just that—a combination of two or more types of physical or logical network topologies working together within the same network.

|  |
| --- |
| *Hybrid topology* |

Physical Media

**To do:**Go through the activity to the end

Coaxial Cable

**Coaxial cable** is a type of copper cable specially built with a *metal shield* and other components engineered to *block signal interference*. Thus, coaxial cable shields data transmissions from *electromagnetic interference (EMI)*. It is primarily used by cable TV companies to connect their satellite antenna facilities to customer homes and businesses and also to connect a cable modem to an Internet service provider (ISP). This connection enables a computer to access the Internet.

|  |
| --- |
| *Coaxial Cable* |

The cable is named coaxial because the central copper wire and the braided metal shield share a common axis or centerline. The metal wire is generally covered sequentially from the center to the outside by insulation (dielectric), foil shield, braided metal shield, and jacket layers. Many of these cables or pairs of coaxial tubes can be placed in a single outer sheathing and, with repeaters, can carry information for a great distance.

**💡Tip:**

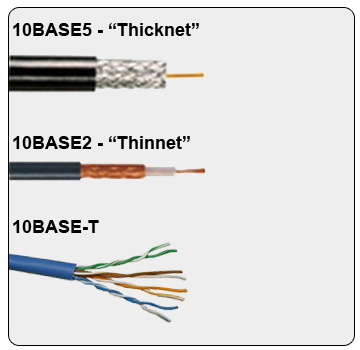
* Coaxial cable was invented in 1880 by English engineer and mathematician Oliver Heaviside, who patented the invention and design that same year. AT&T established its first cross-continental coaxial transmission system in 1940.

**Advantages of coaxial cable**

* Inexpensive
* Easy to wire and install
* Easy to expand
* Good resistance to EMI (Electromagnetic Interference)
* Up to 10Mbps capacity
* Durable

Another **benefit** of coaxial cable that it can be installed next to metal objects without losing power, unlike other types of transmission lines.

The main **disadvantage** of using the coaxial cable is that a single cable failure can take down an entire network.

**Thin Ethernet** (also referred to as *Thinnet* or *10Base2*) and **Thick Ethernet** (also referred to as *Thicknet* or *10Base5* are coaxial cable types. They have the same properties except for the thickness of the cables is different. (Thinnet is only about 5 mm, or 2/10″, diameter coaxial cable).

|  |
| --- |
| *Thicknet & Thinnet* |

If you use Thinnet (or Thicknet) cable, you’ve got to use BNC connectors to attach sta



tions to the network

|  |
| --- |
| *Male and female BNC connectors* |

The **F connector**, or **F-type** connector, is a form of coaxial connector that is used for cable TV.

|  |
| --- |
| *Male F-type connector* |

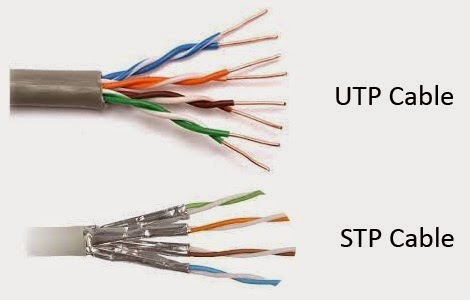
Formun Üstü

Previous

Twisted-Pair Cable

A **twisted-pair** cable is a type of cable made by putting two separate insulated wires together in a twisted pattern and running them parallel to each other. This type of cable is widely used in different kinds of data and voice infrastructures.

Two different types of twisted pair cable, **unshielded twisted pair (UTP)** and **shielded twisted pair (STP)** are used in different kinds of installations. **UTP** is common in *Ethernet* installations, while **STP** is used in various kinds of networks to *prevent crosstalk and electromagnetic interference*.



|  |
| --- |
| *UTP & STP Cable* |

In general, twisted-pair cabling may be preferred over a common alternative, coaxial cable, for different reasons. Coaxial cable involves a single, thicker wire. Twisted pair has a more accommodating bend radius, is easier to terminate, and provides more versatility in selecting network topologies.

Ethernet cable types are described using a code that follows this format:

**N <Signaling> X**.

The **N** refers to the *signaling rate in megabits per second*. **<Signaling>** stands for the *signaling type*—either baseband or broadband *(will be discussed in the following lessons)*—and the **X** is a *unique identifier* for a specific Ethernet cabling scheme.

Here’s a common example: 100BaseX. The 100 tells us that the transmission speed is 100 Mb or 100 megabits. The X value can mean several different things; for example, a T is short for twisted-pair. This is the standard for running 100-megabit Ethernet over two pairs (four wires) of Category 5, 5e, or 6 UTP.

So why are the wires in this cable type twisted? Because when electromagnetic signals are conducted on copper wires in close proximity—like inside a cable—it causes interference called crosstalk. Twisting two wires together as a pair minimizes interference and even protects against interference from outside sources. This cable type is the most common today for the following reasons:

* It’s cheaper than other types of cabling.
* It’s easy to work with.
* It allows transmission rates that were impossible 10 years ago.

|  |
| --- |
| *UTP Categories* |
| **BNC connectors** won’t fit very well on *UTP cable*, so a **registered jack (RJ)**  connector should be used. The connector used with UTP cable is called **RJ-11**  for phones that use four wires; **RJ-45** has four pairs (eight wires),  as shown in the below figure. |
| *RJ-11 & RJ-45 Connectors* |

Formun Altı

Formun Üstü

Formun Altı

*metin içeren bir resim

Açıklama otomatik olarak oluşturuldu*

Fiber-Optic Cable

**Optical fiber** is a very thin strand of pure glass that acts as a waveguide for light over long distances. It uses a principle known as *total internal reflection*.

|  |
| --- |
| *Fiber-Optic Cable* |

Fiber optic cable is actually composed of two layers of glass: The **core** which is thinner than hair *carries the actual light signal*, and the **cladding** is a *layer of a glass surrounding the core*. Most fibers operate in duplex pairs: one fiber is used to transmit and the other is used to receive. But it is possible to send both signals over a single strand.

|  |
| --- |
| *Fiber-Optic Cable Construction Layers* |

Because fiber-optic cable transmits digital signals using light impulses rather than electricity, it’s **immune to EMI and RFI**. Fiber cable allows light impulses to be carried on either a glass or a plastic core. Glass can carry the signal a *greater distance*, but plastic *costs less*.

Fiber-optic cable has advantages and disadvantages just like the other cable types.

Here are the advantages:

* It’s completely immune to EMI and RFI.
* It can transmit up to 40 kilometers (about 25 miles).
* It has a high carrying capacity (very broad bandwidth, THz or Tbits/s)
* It has very low transmission losses (<0.2dB/km, cf1dB/km microwave, 10db/km twisted copper pair)
* It does not produce heat

And here are the disadvantages:

* It’s difficult to install.
* It’s more expensive than twisted-pair.
* Troubleshooting equipment is more expensive than twisted-pair test equipment.
* It’s harder to troubleshoot.

There are two main types of fiber optic cables: **Single-Mode Fiber (SMF)** and **Multi-Mode Fiber (MMF)**. The difference is basically in the *size of the core*. **MMF** has a much wider core, allowing multiple modes (or “rays”) of light to propagate. **SMF** has a very narrow core which allows only a single mode of light to propagate. Each type of fiber has different properties with its own advantages and disadvantages.

|  |
| --- |
| *Single-Mode & Multi-Mode* |

Formun Üstü

Previous

Transceivers

A **transceiver (TRX)** is a device that can transmit and receive signals. Usually, a transceiver contains both a transmitter and a receiver, both of which share common circuitry. However, if the transmitter and receiver only share a common housing and nothing else, the device is called a **transmitter-receiver**. Transceivers are extremely important in the history of technology, as they have paved the way for many inventions such as two-way radios, mobile phones, and the internet.

|  |
| --- |
| *Fiber Transceiver* |

Transceivers can be found in radio technology, telephony as well as Ethernet in which transceivers are called **Medium Attachment Units (MAUs)**.

Formun Altı

Formun Üstü

Formun Altı

A transceiver (TRX)   is a device that can transmit and receive signals.

The  small form‑factor pluggable (SFP)  is a compact, hot-pluggable optical module transceiver used for both telecommunication and data communications applications.

Media Converters

Sometimes, we need to convert from one media type to another. Maybe we need to go from one mode of fiber to another mode or we need to go from fiber to Ethernet.

* **Single-Mode Fiber to Ethernet** - These devices accept a fiber connector and an Ethernet connector and convert the signal from Ethernet and single-mode fiber.

|  |
| --- |
| *Single-Mode Fiber to Ethernet Converter* |

* **Multimode Fiber to Ethernet** - These devices accept a fiber connector and an Ethernet connector and convert the signal from Ethernet and multi-mode fiber.

|  |
| --- |
| *Multimode Fiber to Ethernet Converter* |

* **Fiber to Coaxial** - These devices accept a fiber connector and a coaxial connector and convert digital signals from optical to coax.

|  |
| --- |
| *Fiber to Coaxial Converter* |

* **Single-Mode to Multimode Fiber** - These devices accept a single-mode fiber connector and a multimode fiber connector and convert the signals between the two.

|  |
| --- |
| *Single-Mode to Multimode Fiber Converter* |

The OSI Reference Model

**To do:**Go through the activity to the end

What is the OSI Reference Model?

**OSI** stands for *Open System Interconnection*. **The OSI Model** defines how **data is transferred** from one computer to another computer regardless of the operating system or vendor of the hardware.

In a very basic scenario, two computers connected with a LAN and transfer data using the Network Interface Card (NIC or Network Adapter). This forms a computer network, however, if both systems use different operating systems, for example, one system runs on Windows and the other one runs on macOS then how can data be exchanged between these two different systems? Here comes the role of an OSI model which is a seven-layered model that defines how data can be exchanged between different systems.

OSI model was introduced by the International Organisation for standardization (ISO) in 1984.

|  |
| --- |
| *The OSI Network Layers* |

As the complexity of computer hardware and software increases, the problem of successfully communicating between these systems becomes more difficult. Dividing these difficult problems into "sub-tasks" allows them to be solved more easily. Using this layered approach means that a vendor can work on the design for a particular layer without affecting any of the others.

Each layer performs a different group of tasks required for network communication. The OSI model is not a standard or a specification; it serves as a **functional guideline** for designing network protocols, software, and appliances and for troubleshooting networks.

The OSI Model’s seven layers are divided into two groups. The top three layers (**upper layers**) define the rules of how the applications working within host machines communicate with each other as well as with end-users. The bottom four layers (**lower layers**) define how the actual data is transmitted from end to end.

Advantages of OSI Reference Model

The OSI model is hierarchical. The main purpose of the OSI model, and all networking models, is to allow different vendors’ networks to interoperate smoothly. This short-list depicts some of the most important advantages we gain by using the OSI layered model:

* The OSI model divides network communication processes into smaller and simpler components, thus aiding component development, design, and troubleshooting.
* It allows multiple-vendor development through the standardization of network components.
* It encourages industry standardization by defining the specific functions that occur at each layer of the model.
* It allows various types of network hardware and software to communicate.
* It prevents changes in one layer from affecting other layers, facilitating development and making application programming much easier.

Physical Layer

The physical layer of the OSI model (layer 1) is responsible for the transmission and receipt of bits from one node to another. It specifies the following:

* Physical network topology - physical specifications for the network medium, such as cable specifications, the medium connector and pin-out details (the number and functions of the various pins in a network connector), or radio transceiver specifications.
* The process of transmitting and receiving signals from the network medium including modulation schemes and timing/synchronization.

|  |
| --- |
| *Transmission at Physical Layer* |

Devices operating at the physical layer include:

* **Transceiver** - the part of a network interface that sends and receives signals over the network media.
* **Media Converter** - converts one media signaling type to another.
* **Repeater** - amplifies the signal to extend the maximum allowable distance for a media type.
* **Hub** - a multiport repeater, deployed as the central point of connection for nodes wired in a star topology.
* **Modem** - a device that converts between digital and analog signal transmissions (**MO**dulator-**DEM**odulator).



Formun Üstü

Formun Altı

Data Link Layer

The data link layer (layer 2) is responsible for transferring data between nodes on the same network segment. The data link layer splits the message into pieces, each called a *data frame* and adds a customized header. This header contains a source and destination hardware (MAC) address and error checking values. Other information includes the frame length and network layer protocol identifier.

|  |
| --- |
| *A network frame* |

The last part of the frame usually contains some sort of error checking. Protocols at almost every layer perform a consistency check to verify that data has been transferred correctly. The data link layer is only capable of very basic error checking. There is no function to acknowledge or retransmit damaged frames. That function is handled at higher layers of the OSI model.

Connectivity devices found at the data link layer include:

* **Network adapter (or Network Interface Card [NIC])** - joins a host computer to network media (cabling or wireless) and enables it to communicate over the network by assembling and disassembling frames.
* **Bridge** - joins two network segments while minimizing the performance reduction of having more nodes on the same network.
* **Basic switch** - a multiport bridge that creates links between nodes more efficiently.
* **Wireless Access Point (AP)** - allows nodes with wireless network cards to communicate and joins wireless networks to wired ones.

|  |
| --- |
| *Data Link Layer devices* |

Formun Üstü

Formun Altı

Formun Üstü

Network Layer

The network layer (layer 3) is responsible for moving data around a network of networks, known as an internetwork or internet. While the data link layer moves data using hardware addresses within a single network segment, the network layer moves information around an internetwork using a logical network and host IDs.

|  |
| --- |
| *Network Layer* |

The network layer transfers information between networks by examining the destination network layer address or logical network address (IP address) and routing the packet through the internetwork using intermediate systems (routers). The packet moves, hop by hop, through the internetwork to the target network. Once it has reached the destination network, the hardware address can be used to move the packet to the target node. This process requires each logically separate network to have a unique network address.

The main appliance working at layer 3 is the **router**. Other devices include **Layer 3 switches** (combining the function of switches and routers) and basic firewalls.

Formun Üstü

Formun Altı

Formun Üstü

Transport Layer

The first 3 layers of the OSI model are primarily involved with moving **frames** and **datagrams** between nodes and networks. At the *transport layer* (also known as the end-to-end or host-to-host layer) the content of the packets starts to become significant.

Any given host on a network will be communicating with many other hosts using many different types of networking data. One of the critical functions of the transport layer is to identify each type of network application by assigning it a port number. For example, data from the HTTP web browsing application can be identified as port 80 while data from an email server can be identified as port 25.

At the transport layer, on the sending host, data from the upper layers are packaged as a series of segments and each segment is tagged with the application's port number. The segment is then passed to the network layer for delivery. The host could be transmitting multiple HTTP and email segments at the same time.

|  |
| --- |
| *Transport Layer* |

At the network and data link layers, the port number is not significant - it becomes part of the data payload and is "invisible" to routers and switches working at the network and data link layers. At the receiving host, each segment is extracted from its frame and then identified by its port number and passed up to the relevant handler at the upper session and application layers.

The transport layer is also responsible for ensuring reliable data delivery so that packets arrive error-free and without loss. The transport layer can overcome any lack of reliability in the lower level protocols. This reliability is achieved using **acknowledgment** messages that inform the sender the data was successfully received. The kinds of problems that may occur during the delivery of the data are non-delivery and delivery in a damaged state. In the first case, the lack of acknowledgment results in the retransmission of the data, and, in the second case, a **Negative Acknowledgement (NACK)** forces retransmission.

Devices working at the transport layer (or above) include multilayer switches and security appliances such as more advanced firewalls and Intrusion Detection Systems (IDS).

The OSI Reference Model

**To do:**Go through the activity to the end

Session Layer

Most application protocols require the exchange of multiple messages between the client and the server. This exchange of such a sequence of messages is called a **session** or **dialog**. The session layer (layer 5) represents the dialog control functions that administer the process of establishing the dialog, managing data transfer, and then ending (or "tearing down") the session.

|  |
| --- |
| *Session Layer* |

Sessions can work in three modes:

* **One-way/simplex** - only one system is allowed to send messages; the other receives only.
* **Two-Way Alternate (TWA)/half-duplex** - the hosts establish some system for taking turns to send messages, such as exchanging a token.
* **Two-Way Simultaneous (TWS)/duplex** - either host can send messages at any time.

The session layer can also provide a synchronization service for long transactions in which checkpoints are inserted into the data stream (dialog separation). If a problem occurs, only the data transferred after the last checkpoint is re-sent.

In summary, this layer primarily manages applications’ data by separating from each other application. For instance, multiple web browser sessions at the same time on your desktop are handled by the help of session layer.

Presentation Layer

The presentation layer (layer 6) transforms data between the format required for the network and the format required for the application. For example, the presentation layer is used for character set conversion. The communicating computers may use different character coding systems (such as American Standard Code for Information Interchange [ASCII] and Unicode); the peer presentation layers agree to translate the data into one of the formats or they will both translate the data into a third format. The presentation layer can also be conceived as supporting data compression and encryption (scrambling a message so that it can only be read in conjunction with a valid "key"). However, in practical terms, these functions are often implemented by encryption devices and protocols running at lower layers of the stack.

Formun Üstü

Previous

Formun Altı

Formun Üstü

Next

Application Layer

The application layer (layer 7) is at the top. An application layer protocol doesn’t encapsulate any other protocols or provide services to any protocol. An application layer protocol provides an interface for software applications on network hosts that have established a communication channel using the lower-level protocols to exchange data. For example, one of the most utilized services provided by the application layer is file transfer. Different file systems may use entirely different file naming conventions and data syntax and the application layer must overcome these differences. More widely, upper-layer protocols provide most of the services that make a network useful, rather than just functional, including network printing, electronic mail and communications, directory lookup, and database services.

|  |
| --- |
| *Application Layer* |

It is important to distinguish between network application protocols and the software application code (programs and shared programming libraries) that run on computers. Software programs and operating systems make use of the Application Programming Interface (API) to call functions of the relevant part of the network stack. Examples of APIs include:

* Network card drivers could use the Network Driver Interface Specification (NDIS) API to implement functions at the data link layer.
* The Sockets / WinSock APIs implement transport and session layer functions.
* High-level APIs implement functions for services such as file transfer, email, web browsing, or name resolution.

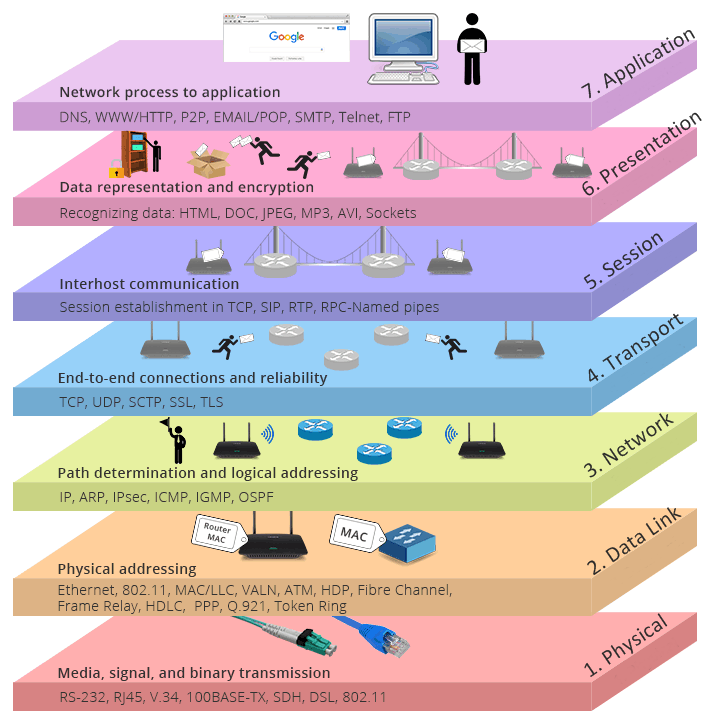
Formun Üstü

Previous

Formun Altı

Formun Üstü

Next

Formun Altı

Formun Altı

Formun Altı

Formun Altı

Data Encapsulation

When a host transmits data across a network to another device, the data goes through **encapsulation**: It’s wrapped with protocol information at each layer of the OSI model. Each layer communicates only with its peer layer on the receiving device.

To communicate and exchange information, each layer uses **Protocol Data Units (PDUs)**. These hold the control information attached to the data at each layer of the model. They’re usually attached to the header in front of the data field but can also be in the trailer, or end, of it.

Each **PDU** attaches to the data by *encapsulating* it at each layer of the OSI model, and each has a specific name depending on the information provided in each header. This PDU information is read-only by the peer layer on the receiving device. After it’s read, it’s stripped off, and the data is then handed to the next layer up.

The below figure shows the PDUs and how they attach control information to each layer. This figure demonstrates how the upper-layer user data is converted for transmission on the network. The data stream is then handed down to the Transport layer, which sets up a virtual circuit to the receiving device by sending over a synch packet. Next, the data stream is broken up into smaller pieces, and a Transport layer header (a PDU) is created and attached to the header of the data field; now the piece of data is called a segment. Each segment is sequenced so the data stream can be put back together on the receiving side exactly as it was transmitted.

|  |
| --- |
| *Data Encapsulation* |

In summary, at a transmitting device, the data-encapsulation method works like this:

1. User information is converted to data for transmission on the network.
2. Data is converted to segments, and a reliable connection is set up between the transmitting and receiving hosts.
3. Segments are converted to packets or datagrams, and a logical address is placed in the header so each packet can be routed through an internetwork.
4. Packets or datagrams are converted to frames for transmission on the local network. Hardware (Ethernet) addresses are used to uniquely identify hosts on a local network segment.
5. Frames are converted to bits, and a digital encoding and clocking scheme is used.

Q: What is data encapsulation?  
A: Data encapsulation is the process of breaking down information into smaller manageable chunks before it is transmitted across the network. These chunks are wrapped with protocol information at each layer of the OSI model. In this process, the source and destination addresses are attached into the headers, along with parity checks.

- Interview Q&A

Ethernet

Ethernet is the standard technology for connecting devices in a LAN or WAN and allowing them to communicate using a protocol, which is a collection of rules or a common network language. Ethernet explains how network devices format and transmit data in such a way that other devices on the same local area network segment can interpret, receive, and process it. An Ethernet cable is a physical connection between two computers.

Ethernet is popular because it’s readily scalable, meaning that it’s comparatively easy to integrate new technologies, such as *Fast Ethernet* and *Gigabit Ethernet*, into an existing network infrastructure. It’s also relatively simple to implement in the first place, and with it, troubleshooting is reasonably straightforward.

Ethernet uses both **Data Link** and **Physical layer** specifications.

Ethernet is not a single protocol but an entire collection of different standards. These standards come from the IEEE and all of them start with **802.3** in their name. Ethernet is also pretty old, the first memo about Ethernet was written by Bob Metcalfe back in 1973.

Despite its age, Ethernet is the dominant choice for LANs. There are many different standards with speeds of 10 Mbps (megabits per second) up to 100 Gbps (gigabits per second). Here’s an overview with some popular Ethernet standards:

| **Bandwidth** | **Common Name** | **Informal name** | **IEEE name** | **Cable Type** |
| --- | --- | --- | --- | --- |
| 10 Mbps | Ethernet | 10BASE-T | 802.3 | UTP 100m |
| 100 Mbps | Fast Ethernet | 100BASE-T | 802.3u | UTP 100m |
| 1000 Mbps | Gigabit Ethernet | 1000BASE-LX | 802.3z | Fiber 5000m |
| 1000 Mbps | Gigabit Ethernet | 1000BASE-T | 802.3ab | UTP 100m |
| 10 Gbps | 10 Gigabit Ethernet | 10GBASE-T | 802.3an | UTP 100m |

On the physical layer, there are different cable options and different speeds. One of the advantages of Ethernet, however, is that it uses the same data link layer standard. You can mix different Ethernet standards in your network.

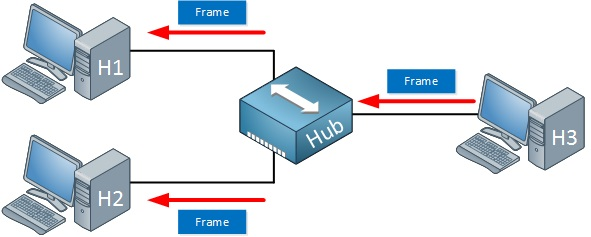
Q: What is ethernet?  
A: Ethernet is a network technology used in LAN and WAN that connects devices using cables for the transmission of data. It provides services on the Physical and Data Link layers of the OSI Model.

Collision Domain

The term **collision domain** is an Ethernet term that refers to a particular network scenario wherein one device sends a packet out on a network segment and thereby forces every other device on that same physical network segment to pay attention to it. This is bad because if two devices on one physical segment transmit at the same time, a collision event—a situation where each device’s digital signals interfere with another on the wire—occurs and forces the devices to retransmit later. Collisions have a dramatically negative effect on network performance.

The situation described is typically found in a **hub** environment where each host segment connects to a hub that represents only one collision domain and one broadcast domain.

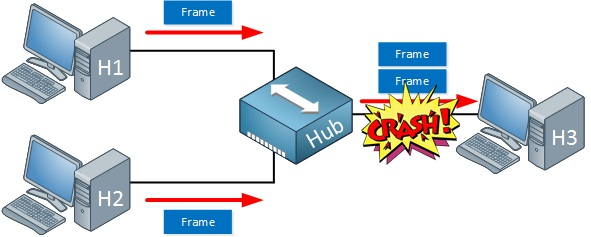
**Hubs** will be explained in detail in the further lessons but in order to understand the collision domain here is a brief definition of a hub: The hub is a simple device; it’s basically nothing more but a repeater. When it receives an electrical signal, it will repeat it on all ports except the one where it received the signal on. This logic works fine in the following situation:



Above we see that H3 sends an Ethernet frame. Let’s say that this frame is destined for H1. When the hub receives this frame, it will replicate it on the ports towards H1 and H2.

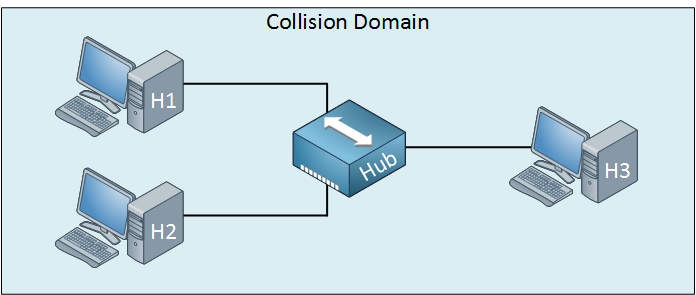
H1 wants to receive it, H2 doesn’t care about so it will discard the frame. No problem! Our goal to send a frame from H3 to H1 is accomplished.

We do have a problem when H1 and H2 both send a frame at the same time, like the following situation:



When H1 and H2 send a frame at the same time, our hub will replicate them on the port that is connected to H3. In this case, a collision will occur and H3 will receive nothing.

Don't forget, we can get **collisions** on every port that is connected to the **hub**, this all belongs to the same collision domain.

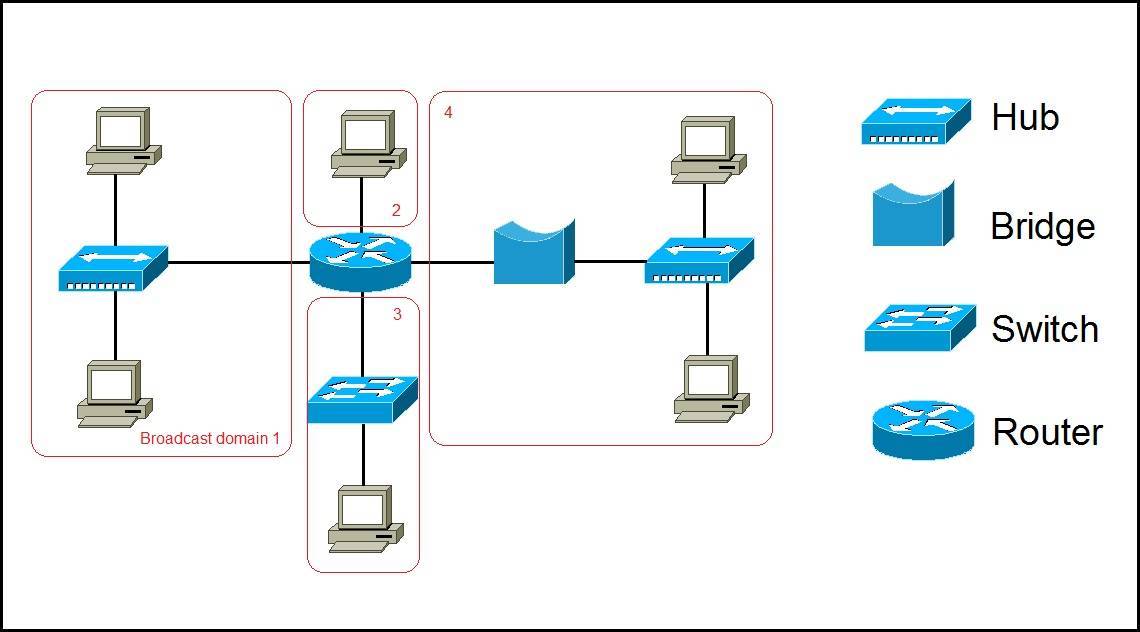


In further lessons, we will cover how to minimize/avoid the collision domain.

Broadcast Domain

The term **broadcast domain** is used to describe a group of devices on a specific network segment that can reach each other with Ethernet broadcasts. Broadcasts sent by a device in one broadcast domain are not forwarded to devices in another broadcast domain. This improves the performance of the network because not all devices on a network will receive and process broadcasts.

Routers separate a LAN into multiple broadcast domains (every port on a router is in a different broadcast domain). Switches (by default) flood Ethernet broadcast frames out all ports, just like bridges and hubs. All ports on these devices are in the same broadcast domain. To better understand the concept of broadcast domains, consider the following example:



In the picture above we have a network of six computers, two hubs, a bridge, a switch, and a router. The broadcast domains are marked in red. Remember, all devices connected to a hub, a bridge, and a switch are in the same broadcast domain. Notice that all hosts can communicate with each other by Data Link layer (hardware address) broadcast. Only routers separate the LAN into multiple broadcast domains. That is why we have four broadcast domains in the network pictured above.

Formun Üstü

Previous

Formun Altı

Formun Üstü

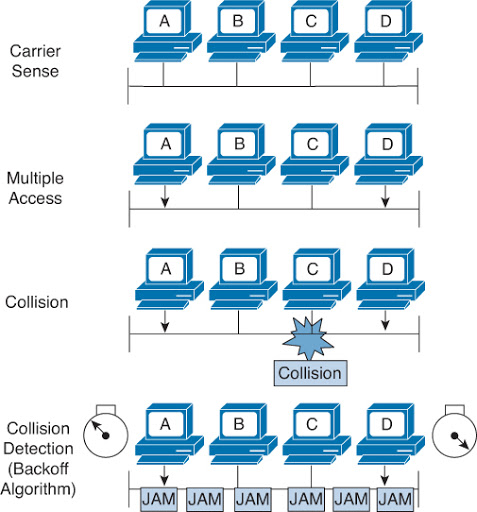
Next

Formun Altı

CSMA/CD

Ethernet networking uses **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)**, a media access control method that helps devices share the bandwidth evenly without having two devices transmit at the same time on the network medium. **CSMA/CD** was created to overcome the problem of those collisions that occur when packets are transmitted simultaneously from different hosts. Good collision management is crucial because when a host transmits in a CSMA/CD network, all the other hosts on the network receive and examine that transmission. Only **bridges, switches**, and **routers**, but not **hubs**, can effectively prevent a transmission from propagating throughout the entire network.

So, how does the CSMA/CD protocol work? Let’s start by taking a look at the below figure, where a collision has occurred in the network.



When a host wants to transmit over the network, it first checks for the presence of a digital signal on the wire. If all is clear, meaning that no other host is transmitting, the host will then proceed with its transmission. But it doesn’t stop there. The transmitting host constantly monitors the wire to make sure no other hosts begin transmitting. If the host detects another signal on the wire, it sends out an extended **jam signal** that causes all hosts on the segment to stop sending data (think busy signal). The hosts respond to that jam signal by waiting a while before attempting to transmit again. Backoff algorithms, represented by the clocks counting down on either side of the jammed devices, determine when the colliding stations can retransmit. If collisions keep occurring after 15 tries, the hosts attempting to transmit will then time out.

When a collision occurs on an Ethernet LAN, the following things happen:

* A jam signal informs all devices that a collision occurred.
* The collision invokes a random backoff algorithm.
* Each device on the Ethernet segment stops transmitting for a short time until the timers expire.
* All hosts have equal priority to transmit after the timers have expired.

And following are the effects of having a CSMA/CD network that has sustained heavy collisions:

* Delay
* Low throughput
* Congestion

Formun Altı

Broadband/Baseband

We have two ways to send analog and digital signals down a wire: **broadband** and **baseband**.

**Broadband** allows us to have both our analog voice and digital data carried on the same network cable or physical medium. Broadband allows us to send *multiple frequencies of different signals* down the same wire at the same time (called *frequency-division multiplexing*) and to send both analog and digital signals.

**Baseband** is what all LANs use. This is where all the bandwidth of the [physical media](https://lms.clarusway.com/mod/lesson/view.php?id=1839" \o "Physical Media) is used by *only one signal*. For example, Ethernet uses only one digital signal at a time, and it requires all the available bandwidth. If multiple signals are sent from different hosts at the same time, we get collisions; the same with wireless, except that, use only analog signaling.

|  |
| --- |
| *Baseband vs. Broadband* |

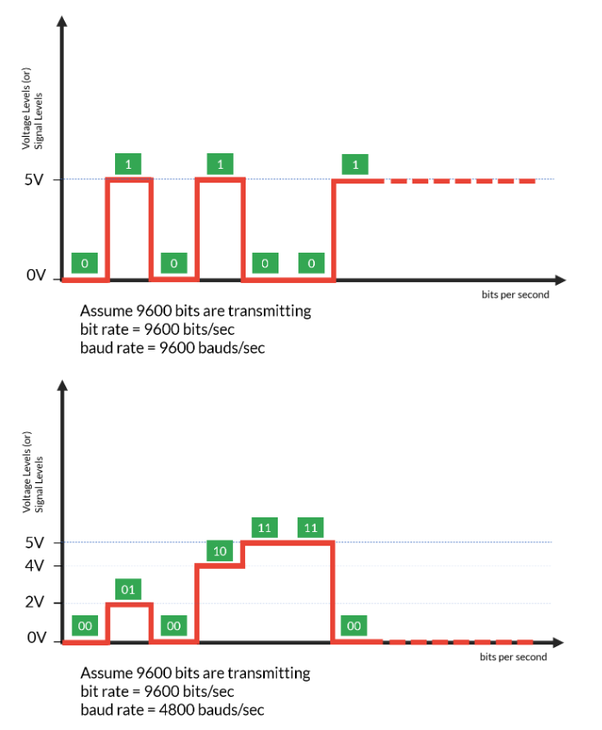
Formun Üstü

Bit Rates vs. Baud Rate

**Bit rate** is a measure of the number of data bits (0s and 1s) transmitted in one second in either a digital or analog signal. A figure of 56,000 bits per second (bps) means 56,000 0s or 1s can be transmitted in one second, which we simply refer to as bps.

In the 1970s and 1980s, we used the term **baud rate** a lot, but that was replaced by *bps* because it was more accurate. Baud was a term of measurement named after a French engineer, Jean-Maurice-Émile Baudot because he used it to measure the speed of telegraph transmissions.

One baud is one electronic state change per second—for example, from 0.2 volts to 3 volts or from binary 0 to 1. However, since a single state change can involve more than a single bit of data, the bps unit of measurement has replaced it as a more accurate definition of how much data you’re transmitting or receiving.



In the figure, the number of data elements carried by each signal element in the bottom one is double of upper one, that is why the baud rate in the bottom one is half of the upper one.

---------------------------------------------------------------------------------------------

Half- and Full-Duplex Ethernet

**Half-duplex** Ethernet is defined in the original *802.3 Ethernet specification*. Basically, when you run half-duplex, you’re using only one wire pair with a digital signal either transmitting or receiving. This really isn’t all that different from full-duplex because you can both transmit and receive—you just can't run half-duplex and full-duplex at the same time.

|  |
| --- |
| *Ethernet communication* |

Half-duplex Ethernet—typically 10BaseT—is only about 30 to 40 percent efficient because it will usually provide only 3 Mbps to 4 Mbps at most. Although it’s true that 100 Mbps Ethernet can and sometimes do run half-duplex, it’s just not very common to find that happening anymore.

In contrast, full-duplex Ethernet uses two pairs of wires at the same time instead of one measly wire pair like half duplex employs. Plus, full duplex uses a point-to-point connection between the transmitter of the sending device and the receiver of the receiving device (in most cases the switch). This means that with full-duplex data transfer, you not only get faster data-transfer speeds, but you also get collision prevention too. Full-duplex Ethernet is supposed to offer 100 percent efficiency in both directions—for example, you can get 20 Mbps with a 10 Mbps Ethernet running full-duplex or 200 Mbps for Fast Ethernet. But this rate is something known as an **aggregate rate**, which translates as “you’re supposed to get” 100 percent efficiency.

Full-duplex Ethernet can be used in many situations; here are some examples:

* With a connection from a switch to a host
* With a connection from a switch to a switch
* With a connection from a host to a host

**Note:** You can run full duplex with just about any device except a **hub**.

Formun Üstü

Formun Altı

Formun Altı