How Ethernet Works

by Nick Pidgeon

In today's business world, reliable and efficient access to information has become an important asset in the quest to achieve a competitive advantage. File cabinets and mountains of papers have given way to computers that store and manage information electronically. Coworkers thousands of miles apart can share information instantaneously, just as hundreds of workers in a single location can simultaneously review research data maintained online.

Computer networking technologies are the glue that binds these elements together. The public Internet allows businesses around the world to share information with each other and their customers. The global computer network known as the World Wide Web provides services that let consumers buy books, clothes, and even cars online, or auction those same items off when no longer wanted.

Networking allows one computer to send information to and receive information from another. We may not always be aware of the numerous times we access information on computer networks. Certainly the Internet is the most conspicuous example of computer networking, linking millions of computers around the world, but smaller networks play a roll in information access on a daily basis. Many public libraries have replaced their card catalogs with computer terminals that allow patrons to search for books far more quickly and easily. Airports have numerous screens displaying information regarding arriving and departing flights. Many retail stores feature specialized computers that handle point-of-sale transactions. In each of these cases, networking allows many different devices in multiple locations to access a shared repository of data.

In this edition of **HowStuffWorks**, we will take a very close look at networking, and in particular the Ethernet networking standard, so you can understand the actual mechanics of how all of these computers connect to one another. Before getting into the details of a networking standard, we must first understand some basic terms and classifications that describe and differentiate network technologies -- so let's get started!

Local Area vs. Wide Area

We can classify network technologies as belonging to one of two basic groups. **Local area network** (LAN) technologies connect many devices that are relatively close to each other, usually in the same building. The library terminals that display book information would connect over a local area network. **Wide area network** (WAN) technologies connect a smaller number of devices that can be many kilometers apart. For example, if two libraries at the opposite ends of a city wanted to share their book catalog information, they would most likely make use of a wide area network technology, which could be a dedicated line leased from the local telephone company, intended solely to carry their data.

In comparison to WANs, LANs are faster and more reliable, but improvements in technology continue to blur the line of demarcation. Fiber optic cables have allowed LAN technologies to connect devices tens of kilometers apart, while at the same time greatly improving the speed and reliability of WANs.

The Ethernet

In 1973, at Xerox Corporation’s Palo Alto Research Center (more commonly known as PARC), researcher **Bob Metcalfe** designed and tested the first Ethernet network. While working on a way to link Xerox’s "Alto" computer to a printer, Metcalfe developed the physical method of cabling that connected devices on the Ethernet as well as the standards that governed communication on the cable. Ethernet has since become the most popular and most widely deployed network technology in the world. Many of the issues involved with Ethernet are common to many network technologies, and understanding how Ethernet addressed these issues can provide a foundation that will improve your understanding of networking in general.

The Ethernet standard has grown to encompass new technologies as computer networking has matured, but the mechanics of operation for every Ethernet network today stem from Metcalfe's original design. The original Ethernet described communication over a **single cable** shared by all devices on the network. Once a device attached to this cable, it had the ability to communicate with any other attached device. This allows the network to expand to accommodate new devices without requiring any modification to those devices already on the network.

Ethernet is a local area technology, with networks traditionally operating within a single building, connecting devices in **close proximity**. At most, Ethernet devices could have only a few hundred meters of cable between them, making it impractical to connect geographically dispersed locations. Modern advancements have increased these distances considerably, allowing Ethernet networks to span tens of kilometers.

Protocols

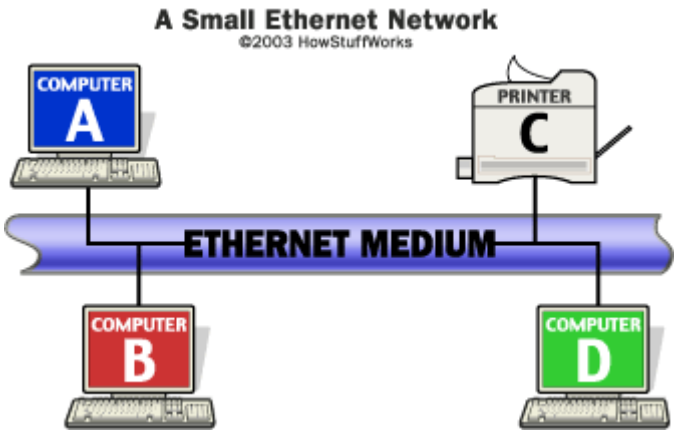
In networking, the term **protocol** refers to a set of rules that govern communications. Protocols are to computers what language is to humans. Since this article is in English, to understand it you must be able to read English. Similarly, for two devices on a network to successfully communicate, they must both understand the same protocols.

Ethernet Terminology

Ethernet follows a simple set of rules that govern its basic operation. To better understand these rules, it is important to understand the basics of Ethernet terminology.

- **Medium** - Ethernet devices attach to a common medium that provides a path along which the electronic signals will travel. Historically, this medium has been coaxial copper cable, but today it is more commonly a twisted pair or fiber optic cabling.
- **Segment** - We refer to a single shared medium as an Ethernet segment.
- **Node** - Devices that attach to that segment are stations or nodes.
- **Frame** - The nodes communicate in short messages called frames, which are variably sized chunks of information.

Frames are analogous to sentences in human language. In English, we have rules for constructing our sentences: We know that each sentence must contain a subject and a predicate. The **Ethernet protocol** specifies a set of rules for constructing frames. There are explicit minimum and maximum lengths for frames, and a set of required pieces of information that must appear in the frame. Each frame must include, for example, both a **destination address** and a **source address**, which identify the recipient and the sender of the message. The address uniquely identifies the node, just as a name identifies a particular person. No two Ethernet devices should ever have the same address.



critical to identify the intended recipient of the frame. For example, in the figure above, when computer B transmits to printer C, computers A and D will still receive and examine the frame. However, when a station first receives a frame, it checks the destination address to see if the frame is intended for itself. If it is not, the station discards the frame without even examining its contents.

One interesting thing about Ethernet addressing is the implementation of a **broadcast address**. A frame with a destination address equal to the broadcast address (simply called a broadcast, for short) is intended for every node on the network, and every node will both receive and process this type of frame.

CSMA/CD

The acronym **CSMA/CD** signifies **carrier-sense multiple access with collision detection** and describes how the Ethernet protocol regulates communication among nodes. While the term may seem intimidating, if we break it apart into its component concepts we will see that it describes rules very similar to those that people use in polite conversation. To help illustrate the operation of Ethernet, we will use an analogy of a dinner table conversation.

Let’s represent our Ethernet segment as a dinner table, and let several people engaged in polite conversation at the table represent the nodes. The term **multiple access** covers what we already discussed above: When one Ethernet station transmits, all the stations on the medium hear the transmission, just as when one person at the table talks, everyone present is able to hear him or her.

Now let's imagine that you are at the table and you have something you would like to say. At the moment, however, I am talking. Since this is a polite conversation, rather than immediately speak up and interrupt, you would wait until I finished talking before making your statement. This is the same concept described in the Ethernet protocol as **carrier sense**. Before a station transmits, it "listens" to the medium to determine if another station is transmitting. If the medium is quiet, the station recognizes that this is an appropriate time to transmit.

Carrier-sense multiple access gives us a good start in regulating our conversation, but there is one scenario we still need to address. Let’s go back to our dinner table analogy and imagine that there is a momentary lull in the conversation. You and I both have something we would like to add, and we both "sense the carrier" based on the silence, so we begin speaking at approximately the same time. In Ethernet terminology, a **collision** occurs when we both spoke at once.

In our conversation, we can handle this situation gracefully. We both hear the other speak at the same time we are speaking, so we can stop to give the other person a chance to go on. Ethernet nodes also listen to the medium while they transmit to ensure that they are the only station transmitting at that time. If the stations hear their own transmission returning in a garbled form, as would happen if some other station had begun to transmit its own message at the same time, then they know that a collision occurred. A single Ethernet segment is sometimes called a **collision domain** because no two stations on the segment can transmit at the same time without causing a collision. When stations detect a collision, they cease transmission, wait a random amount of time, and attempt to transmit when they again detect silence on the medium.

The random pause and retry is an important part of the protocol. If two stations collide when transmitting once, then both will need to transmit again. At the next appropriate chance to transmit, both stations involved with the previous collision will have data ready to transmit. If they transmitted again at the first opportunity, they would most likely collide again and again indefinitely. Instead, the random delay makes it unlikely that any two stations will collide more than a few times in a row.

Limitations of Ethernet

A single shared cable can serve as the basis for a complete Ethernet network, which is what we discussed above. However, there are practical limits to the size of our Ethernet network in this case. A primary concern is the length of the shared cable.

Electrical signals propagate along a cable very quickly, but they weaken as they travel, and electrical interference from neighboring devices (fluorescent lights, for example) can scramble the signal. A network cable must be short enough that devices at opposite ends can receive each other's signals clearly and with minimal delay. This places a distance limitation on the maximum separation between two devices (called the **network diameter**) on an Ethernet network. Additionally, since in CSMA/CD only a single device can transmit at a given time, there are practical limits to the number of devices that can coexist in a single network. Attach too many devices to one shared segment and contention for the medium will increase. Every device may have to wait an inordinately long time before getting a chance to transmit.

Engineers have developed a number of network devices that alleviate these difficulties. Many of these devices are not specific to Ethernet, but play roles in other network technologies as well.

Repeaters

The first popular Ethernet medium was a copper coaxial cable known as "thicknet." The maximum length of a thicknet cable was 500 meters. In large building or campus environments, a 500-meter cable could not always reach every network device. A **repeater** addresses this problem.

Repeaters connect multiple Ethernet segments, listening to each segment and repeating the signal heard on one segment onto every other segment connected to the repeater. By running multiple cables and joining them with repeaters, you can significantly increase your network diameter.

Bridges and Segmentation

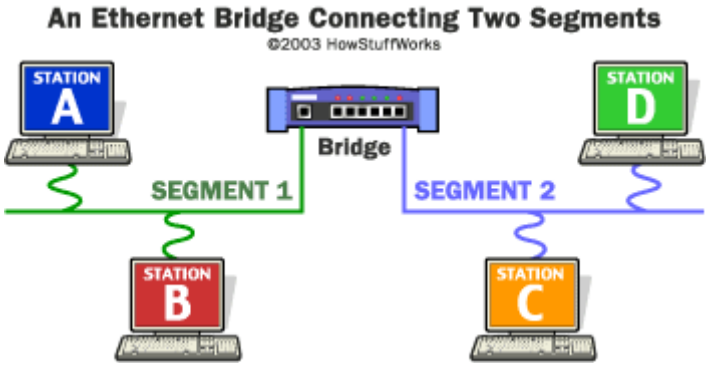
In our dinner table analogy, we had only a few people at a table carrying out the conversation, so restricting ourselves to a single speaker at any given time was not a significant barrier to communication. But what if there were many people at the table and only one were allowed to speak at any given time?

In practice, we know that the analogy breaks down in circumstances such as these. With larger groups of people, it is common for several different conversations to occur simultaneously. If only one person in a crowded room or at a banquet dinner were able to speak at any time, many people would get frustrated waiting for a chance to talk. For humans, the problem is self-correcting: Voices only carry so far, and the ear is adept at picking out a particular conversation from the surrounding noise. This makes it easy for us to have many small groups at a party converse in the same room; but network cables carry signals quickly and efficiently over long distances, so this natural segregation of conversations does not occur.

Ethernet networks faced **congestion** problems as they increased in size. If a large number of stations connected to the same segment and each generated a sizable amount of traffic, many stations may attempt to transmit whenever there was an opportunity. Under these circumstances, collisions would become more frequent and could begin to choke out successful transmissions, which could take inordinately large amounts of time to complete. One way to reduce congestion would be to split a single segment into multiple segments, thus creating **multiple collision domains**. This solution creates a different problem, as now these now separate segments are not able to share information with each other.

To alleviate these problems, Ethernet networks implemented **bridges**. Bridges connect two or more network segments, increasing the network diameter as a repeater does, but bridges also

help **regulate traffic**. They can send and receive transmissions just like any other node, but they do not function the same as a normal node. The bridge does not originate any traffic of its own; like a repeater, it only **echoes** what it hears from other stations. (That last statement is not entirely accurate: Bridges do create a special Ethernet frame that allows them to communicate with other bridges, but that is outside the scope of this article.)



Remember how the multiple access and shared medium of Ethernet meant that every station on the wire received every transmission, whether it was the intended recipient or not? Bridges make use of this feature to relay traffic between segments. In the figure above, the bridge connects segments 1 and 2. If station A or B were to transmit, the bridge would also receive the transmission on segment 1. How should the bridge respond to this traffic? It could automatically transmit the frame onto segment 2, like a repeater, but that would not relieve congestion, as the network would behave like one long segment.

One goal of the bridge is to **reduce unnecessary traffic** on both segments. It does this by examining the destination address of the frame before deciding how to handle it. If the destination address is that of station A or B, then there is no need for the frame to appear on segment 2. In this case, the bridge does nothing. We can say that the bridge **filters** or drops the frame. If the destination address is that of station C or D, or if it is the broadcast address, then the bridge will transmit, or **forward** the frame on to segment 2. By forwarding packets, the bridge allows any of the four devices in the figure to communicate. Additionally, by filtering packets when appropriate, the bridge makes it possible for station A to transmit to station B at the same time that station C transmits to station D, allowing two conversations to occur simultaneously!

Switches are the modern counterparts of bridges, functionally equivalent but offering a **dedicated segment** for every node on the network (more on switches later in the article).

Routers: Logical Segmentation

Bridges can reduce congestion by allowing multiple conversations to occur on different segments simultaneously, but they have their limits in segmenting traffic as well.

An important characteristic of bridges is that they forward Ethernet broadcasts to all connected segments. This behavior is necessary, as Ethernet broadcasts are destined for every node on the network, but it can pose problems for bridged networks that grow too large. When a large number of stations broadcast on a bridged network, congestion can be as bad as if all those devices were on a single segment.

Routers are advanced networking components that can divide a single network into two logically separate networks. While Ethernet broadcasts cross bridges in their search to find every node on the network, they do not cross routers, because the router forms a logical boundary for the network.

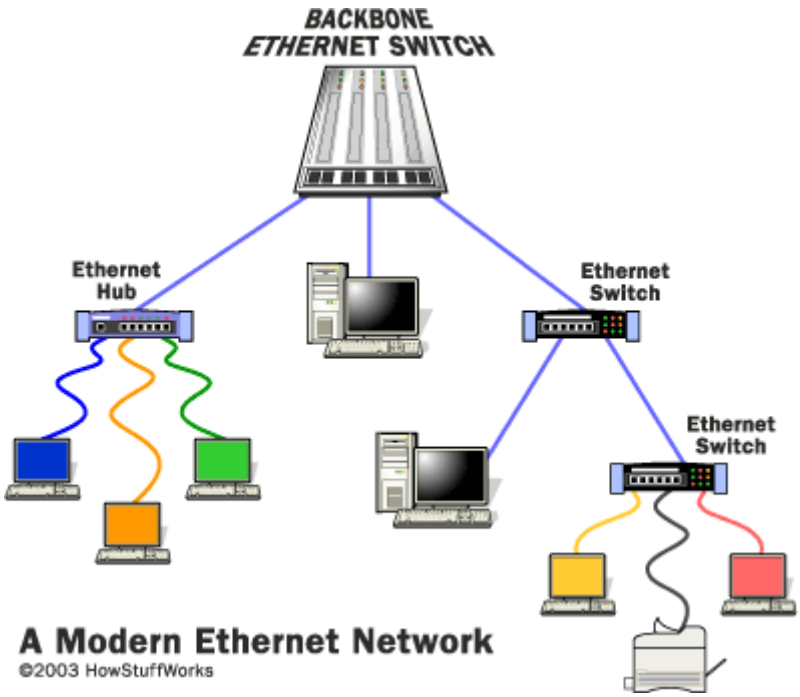
Routers operate based on protocols that are independent of the specific networking technology,

like Ethernet or token ring (we'll discuss token ring later). This allows routers to easily interconnect various network technologies, both local and wide area, and has led to their widespread deployment in connecting devices around the world as part of the global Internet.

See How Routers Work for a detailed discussion of this technology.

Ethernet Today

Modern Ethernet implementations often look nothing like their historical counterparts. Where long runs of coaxial cable provided attachments for multiple stations in legacy Ethernet, modern Ethernet networks use twisted pair wiring or fiber optics to connect stations in a **radial pattern**. Where legacy Ethernet networks transmitted data at 10 megabits per second (Mbps), modern networks can operate at 100 or even 1,000 Mbps!



Perhaps the most striking advancement in contemporary Ethernet networks is the use of **switched Ethernet**. Switched networks replace the shared medium of legacy Ethernet with a dedicated segment for each station. These segments connect to a switch, which acts much like an Ethernet bridge, but can connect many of these single station segments. Some switches today can support hundreds of dedicated segments. Since the only devices on the segments are the switch and the end station, the switch picks up every transmission before it reaches another node. The switch then forwards the frame over the appropriate segment, just like a bridge, but since any segment contains only a single node, the frame only reaches the intended recipient. This allows many conversations to occur simultaneously on a switched network. (See How LAN Switches work to learn more about switching technology.)

Ethernet switching gave rise to another advancement, full-duplex Ethernet. **Full-duplex** is a data communications term that refers to the ability to send and receive data at the same time. Legacy Ethernet is half-duplex, meaning information can move in only one direction at a time. In a totally switched network, nodes only communicate with the switch and never directly with each other. Switched networks also employ either twisted pair or fiber optic cabling, both of which use separate conductors for sending and receiving data. In this type of environment, Ethernet stations can forgo the collision detection process and transmit at will, since they are the only potential devices that can access the medium. This allows end stations to transmit to the switch at the same time that the switch transmits to them, achieving a **collision-free** environment.

Ethernet or 802.3?

You may have heard the term **802.3** used in place of or in conjunction with the term Ethernet. "Ethernet" originally referred to a networking implementation standardized by Digital, Intel and Xerox. (For this reason, it is also known as the **DIX** standard.)

In February 1980, the Institute of Electrical and Electronics Engineers, or **IEEE** (pronounced "I triple E"), created a committee to standardize network technologies. The IEEE titled this the 802 working group, named after the year and month of its formation. Subcommittees of the 802 working group separately addressed different aspects of networking. The IEEE distinguished each subcommittee by numbering it 802.X, with X representing a unique number for each subcommittee. The 802.3 group standardized the operation of a CSMA/CD network that was functionally equivalent to the DIX Ethernet.

Ethernet and 802.3 differ slightly in their terminology and the data format for their frames, but are in most respects identical. Today, the term Ethernet refers generically to both the DIX Ethernet implementation and the IEEE 802.3 standard.

Alternative Network Technologies

The most common local area network alternative to Ethernet is a network technology developed by IBM, called **token ring**. Where Ethernet relies on the random gaps between transmissions to regulate access to the medium, token ring implements a strict, orderly access method. A token-ring network arranges nodes in a logical ring, as shown below. The nodes forward frames in one direction around the ring, removing a frame when it has circled the ring once.

1. The ring initializes by creating a **token**, which is a special type of frame that gives a station permission to transmit.
2. The token circles the ring like any frame until it encounters a station that wishes to transmit data.
3. This station then "captures" the token by replacing the token frame with a data-carrying frame, which encircles the network.
4. Once that data frame returns to the transmitting station, that station removes the data frame, creates a new token and forwards that token on to the next node in the ring.

Token-ring nodes do not look for a carrier signal or listen for collisions; the presence of the token frame provides assurance that the station can transmit a data frame without fear of another station interrupting. Because a station transmits only a single data frame before passing the token along, each station on the ring will get a turn to communicate in a deterministic and fair manner. Token-ring networks typically transmit data at either 4 or 16 Mbps.

a pair of fiber optic rings, with each ring passing a token in opposite directions. FDDI networks offered transmission speeds of 100 Mbps, which initially made them quite popular for high-speed networking. With the advent of 100-Mbps Ethernet, which is cheaper and easier to administer, FDDI has waned in popularity.

A final network technology that bears mentioning is **asynchronous transfer mode**, or ATM. ATM networks blur the line between local and wide area networking, being able to attach many different devices with high reliability and at high speeds, even across the country. ATM networks are suitable for carrying not only data, but voice and video traffic as well, making them versatile and expandable. While ATM has not gained acceptance as rapidly as originally predicted, it is nonetheless a solid network technology for the future.

Ethernet's popularity continues to grow. With almost 30 years of industry acceptance, the standard is well known and well understood, which makes configuration and troubleshooting easier. As other technologies advanced, Ethernet has evolved to keep pace, increasing in speed and functionality.