5

Ethernet (802.3) Switched LANs

## LEARNING OBJECTIVES

By the end of this chapter, you should be able to:

* Explain basic Ethernet terminology and how Ethernet LAN technology is standardized.
* Describe digital and binary signaling and why they reduce transmission errors.
* Explain the technologies of 4-pair UTP and optical fiber and compare and contrast their relative strengths and weaknesses.
* Explain full duplex transmission and the distinction between serial and parallel transmission.
* Design a physical network based on knowledge of transmission requirements and Ethernet physical link standards, including link aggregation.
* Describe the Ethernet frame. Explain basic Ethernet data link layer switch operation.
* Describe security threats to Ethernet LANs and explain how 802.1X and Virtual LANs (VLANs) increase security.

# Ethernet Begins

Bob Metcalfe, a PhD student at Harvard University, wrote his dissertation on the new ARPANET. His committee rejected it, deeming it insufficiently theoretical. Metcalfe was devastated. He had been offered a position at the Xerox Palo Alto Research Center, which was doing cutting-edge technology research. In particular, PARC had just built the Alto, which looked like a PC but was far more powerful. It had a full-page display and a graphical user interface using the mouse, which PARC adopted from Doug Engelbart’s Augmentation Research Center at Stanford Research Institute. Apple later popularized this interface with the Macintosh.

When Metcalfe told Xerox that he would not be graduating, PARC told him to come anyway and finish his dissertation while he worked. Metcalfe asked for a brief delay so that he could first visit the University of Hawai`i’s ALOHAnet project. PARC accepted the delay. ALOHAnet did packet switching using radio. Stations could transmit any time they wished, and a central hub would retransmit correctly received packets. If two stations transmitted at the same time, their colliding packets would be garbled and would not be retransmitted. During his visit, Metcalfe analyzed the ALOHAnet protocol and found ways to reduce collisions. He added the analysis to his dissertation. This time, his committee accepted it.

At Xerox, he was given the task of networking the Altos. Metcalfe realized that his improvements to the ALOHAnet protocol would permit him to run a similar network over physical transmission media. There were several physical media that he could use. To keep his options open, he referred to physical media generically as *the Ether*, after a discredited 19th century theory about how light propagated. He hand-soldered printed circuit boards to implement his protocol. When his Ethernet network became operational it ran at 2.94 Mbps, which was enormous speed for that time.

When Xerox decided not to commercialize Ethernet, Metcalfe started his own company. In 1982, the IEEE started the 802 Committee to set standards for networks on and near a customer site. The committee assigned Ethernet standardization to its 802.3 Working Group.

In those days, Ethernet had competition from other local area network standards. However, the brilliant simplicity of Metcalfe’s protocol meant that Ethernet products were substantially cheaper and quicker to develop than products following competing protocols. Ethernet 802.3 quickly blew the competition out of the water. Since then, Ethernet’s speed has increased to 100 Gbps, and Ethernet has continued its dominance in local area networks. Metcalfe’s simple but elegant protocol became the stuff of legend.

Although Ethernet was a testimony to Bob Metcalfe’s technical brilliance and commercial persistence, the 802.3 Working Group had to use equal brilliance to keep increasing Ethernet’s performance from one seemingly impossible speed to another. As we will see in Chapter 10, Ethernet has even expanded into wide area networking, using long-distance transmission. IP over Ethernet promises to be a dominant pattern for the future of networking.

Test Your Understanding

1. a) What IEEE committee creates LAN standards? b) What working group of this committee creates Ethernet standards. c) Are the terms *802.3* and *Ethernet* synonymous today?

# Introduction

Ethernet Local Area Networks

Ethernet was created for local area networks (LANs). These are networks that operate on a customer premises,[[1]](#footnote-1) which is the property owned by the organization that uses the network. This might be a home, an entire building, a university campus, or an industrial park. On its own premises, the company can use whatever technology standards it wishes.

Ethernet was created for local area networks (LANs), which are networks that operate on a customer premises—the property owned by the organization that uses the network.

Figure 5-1: Local Area Networks (LANs) (Study Figure)

Local Area Networks (LANs)

Operate on a customer premises

The property owned by the organization that uses the network

Companies can use whatever technology standards they wish

Examples

A home

An entire building

A university campus

An industrial park

Etc.

Ethernet

Dominates wired LANs today

Wired switched LANs

Layers 1 and 2 (frames)

OSI architecture, governed by the ITU-T and ISO

Ethernet standards are created by the IEEE 802.3 Working Group of the 802 LAN/MAN standards committee

Then submitted to ITU-T and ISO

Called 802.3 standards

802.1 Working Group creates security standards

802.11 Working Group creates Wi-Fi standards

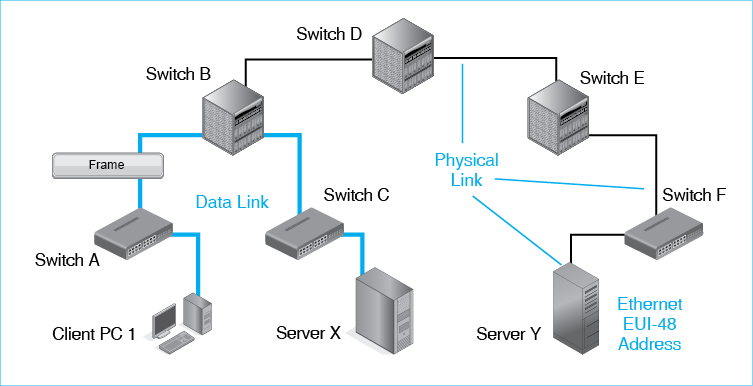
Test Your Understanding

2. What is a local area network (LAN)?

Layer 1 and Layer 2 Standards

Figure 5-2 shows a switched Ethernet network. Ethernet is a single-network standard, so it is governed by physical and data link layer standards. The messages that travel from the source host to the destination host are *frames*, forwarding devices are *switches*, and Ethernet uses *EUI-48* data link layer addresses instead of IP addresses. The path that a frame travels through an Ethernet network is a *data link*. The transmission links that connect pairs of devices are *physical links*. *Ethernet signaling standards* govern physical layer transmission.

Figure 5-2: Switched Ethernet Network



Standards at the physical and data link layers are OSI standards. How does an IEEE standard become an OSI standard? The answer is that after the IEEE has accepted an 802 committee standard, the standard is submitted to the International Organization for Standardization. ISO always accepts Ethernet standards without change, so as soon as the 802 Committee accepts standards, vendors begin developing products. In fact, as soon as the 802.3 Working Group finishes its work and sometimes even before it finishes, vendors today begin selling products.

Test Your Understanding

3. a) At what two layers are Ethernet standards defined? b) Are Ethernet messages packets or frames? c) Are Ethernet forwarding devices switches or routers? d) Is the path an Ethernet message takes from the source host to the destination host a physical link, a data link, or a route? e) Does Ethernet use data link layer addresses or IP addresses? f) What type of addresses does Ethernet use? g) Do vendors wait for Ethernet standards become OSI standards?

A Closer Look

Workgroup Switches and Core Switches  Figure 5-3 shows that Ethernet networks have two types of switches.

* Workgroup switches connect individual hosts to the network. They are the edges of the network.
* In turn, core switches connect switches to other switches. An Ethernet network’s collection of core switches is called the network’s core.

Workgroup switches connect individual hosts to the network.  
Core switches connect switches to other switches.

Figure 5-3: Types of Ethernet Switches and Transmission Links

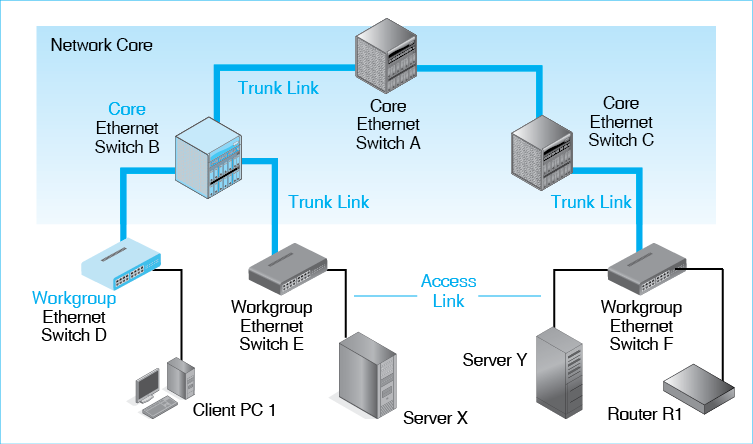


Figure 5-4 shows a typical workgroup switch. It is 48 cm (19 inches) wide so that it can fit into a standard equipment rack. This particular switch is 9 cm (3.5 inches) tall. Core switches are the same width and depth but their heights typically range from about 18 cm (7 inches) to a meter tall.

Figure 5-4: Ethernet Workgroup Switch with 48 Ports



Access Links and Trunk Links  The hosts and switches in an Ethernet network must be connected by physical links. Just as there are two types of Ethernet switches, there are two types of physical links in Ethernet networks.

* Access links connect individual hosts to their workgroup switches. Access links are the on ramps to an Ethernet network.
* Trunk links connect switches to other switches. (In railroads, trunk lines are rail lines that connect different cities.)

Switch and Link Capacity  Access links usually connect a single host to the network and are not shared. In contrast, trunk links must carry the traffic of many host-to-host conversations. Consequently, trunk links require many times the capacity of access links. Typical access link speeds are about 1 Gbps. Trunk speeds can be 10 Gbps or even 100 Gbps.

In the same vein, workgroup switches only need to connect a few hosts to the network. A workgroup switch therefore only has to forward a small amount of traffic, so its frame processing requirements are small. This makes workgroup switches inexpensive. Core switches, in contrast, must forward the traffic of many conversations. This makes them far more expensive than workgroup switches. The core switches highest in the network core must carry the most traffic and are the most expensive.

Test Your Understanding

4. a) \_\_\_\_\_ switches connect users to the network. b) \_\_\_\_\_ switches connect switches to other switches. c) \_\_\_\_\_ links connect users to workgroup switches. d) \_\_\_\_\_ links connect switches to other switches. e) Which needs more capacity—workgroup switches or core switches? f) Which needs higher speed—access links or trunk links?

# Ethernet Physical Layer Standards

Physical layer standards govern connectors, transmission media, and signaling. We will look at Ethernet signaling first because it introduces concepts we will need when we look at UTP and optical fiber transmission media.

Test Your Understanding

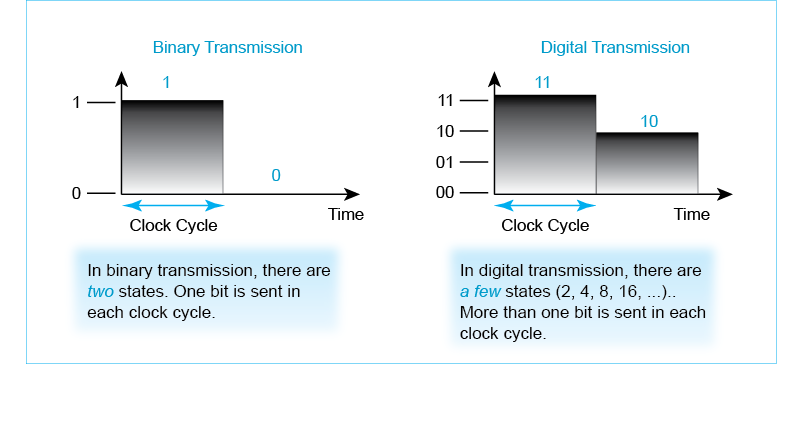
5. What three things do physical layer standards govern?

## Signaling

Bits and Signals  A frame is a long series of 1s and 0s. To transmit the frame over a physical medium, the sender must convert these 1s and 0s into physical signals. These signals will propagate (travel) down the transmission link to the device at the other end of the physical link. That device will convert the signal back into the 1s and 0s of transmitted frames.

Binary and Digital Signaling  Figure 5-5 illustrates two popular types of signaling, binary and digital signaling. Binary signaling has two states (conditions), which may be two voltage levels or light being turned on or off. One state represents a 0. The other state represents a 1. In the figure, a 1 is represented as a high voltage, and a 0 is represented as a 0 voltage. In optical signaling, a light being turned typically represents a 1, while light being turned off typically represents a 0.

Figure 5-5: Binary and Digital Signaling



In binary signaling, again, there are *two* possible states. This makes sense because “bi” is Latin for two. The figure also shows digital signaling, in which there are a *few* states (2, 4, 8, etc.).[[2]](#footnote-2) How many “is few?” In some systems, there can be 32 or even 256 states, but the number of states is usually much lower. The number of states is always a multiple of two—four, eight, sixteen, and so forth.

In binary signaling, there are *two* possible states.  
In digital signaling, there are *a few* possible states (2, 4, 8, etc.).

Having more than two states adds to the complexity and therefore the cost of signaling. However, Figure 5-5 shows that if you have multiple states, you can send multiple bits in a single clock cycle. With two states, you can only represent a single 1 or a 0. With four states, however, the lowest state might represent 00, the next lowest state might represent 01, the next 10, and the highest 11. With four states, then, you can send two bits at a time.

In Chapter 2, we saw that the number of alternatives is two to the power of the number of bits. Equation 1 expresses this in symbols, a = 2b. In digital signaling, a is the number of alternative states, and b is the number of bits to be transmitted. For example, if you transmit one bit per clock cycle, then b is one, and a is 2. This is binary signaling. The two alternatives are 1 and 0. If you transmit 3 bits per clock cycle, you need 8 alternative states.

Equation 1: a = 2b

What if you want to know how many bits you can transmit if you are told how many states the signaling uses? Now, you solve for b knowing a. The simplest way is to keep increasing b until you get to the given a value. For example, suppose you are told that there are four states. If b is 1, then a is 2. This is too small. If b is 2, then a is 4. This is the number of states that you know the system has. So you can transmit 2 bits per clock cycle.

We have talked about binary and digital transmission systems as if they were different. Actually, binary transmission is a subset of digital transmission. In binary transmission, *few* means two. Although binary transmission is the most common form of digital transmission and deserves its own name, all transmission in a typical network can properly be called digital.

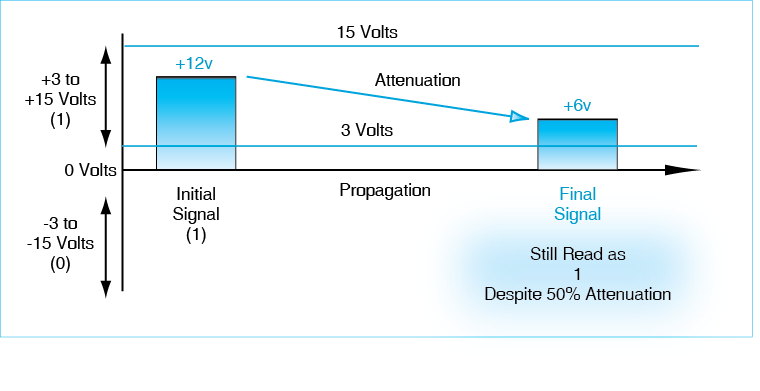
Binary transmission is a type of digital signaling. Not all digital signaling, however, is binary signaling.

Test Your Understanding

6. a) What must a sender do to send the bits of a frame over a transmission medium? b) Distinguish between binary and digital signaling. c) if you wish to transmit 3 bits per clock cycle, how many states must the system have? d) If you want to transmit 5 bits per clock cycle, how many states must the system have? e) If you know that a system has 64 states, how many bits can it send per clock cycle? f) If you know that a system has 256 states, how many bits can it send per clock cycle? g) In general, to transmit twice as many bits per clock cycle, how much must you increase the number of alternatives? (The answer is not in the text.)

Error Resistance  Why use digital transmission? The answer is that digital transmission is fairly resistant to transmission impairments. In Figure 5-6, a 1 is represented by a signal between 3 volts and 15 volts, while a 0 is represented by a signal between minus 3 volts and minus 15 volts. No device signals precisely in this way, but actual signaling today is too complex to describe briefly.

Figure 5-6: Error Resistance in Binary and Digital Signaling



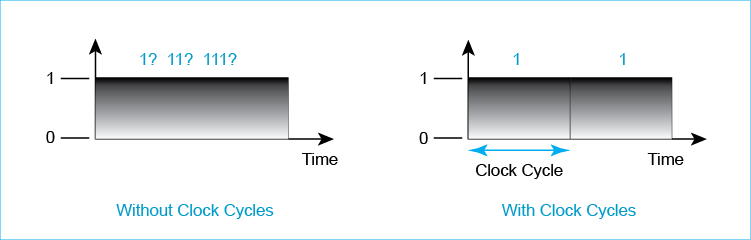
Digital transmission gives partial immunity to errors.

In Figure 5-6, the sender transmits a 12-volt signal. This is a 1. As the signal propagates, it attenuates to 6 volts. This is 50% attenuation, a substantial loss. However, the receiver will still correctly record the signal as a 1 because 6 volts is between 3 volts and 15 volts. The attenuation does not cause an error in reading the signal. This is why binary transmission is error-resistant.

However, think about what happens to error resistance as the number of states increases. Even with four states, a much smaller propagation effect might cause 11 to be misinterpreted as 10. In general, as the number of states grows, error resistance declines proportionally. Consequently, there is a strong tendency to use binary signaling in practice. In examples in this book, we will use binary signaling almost exclusively.

Clock Cycles  When a device transmits, it holds the signal constant for a brief period of time called the clock cycle. Why have clock cycles? Consider Figure 5-7. On the left, we have the situation with no clock cycles. Does the long high signal mean a single 1, two 1s, three 1s, or even more? We cannot say by looking at the representation on the left. However, on the right, we have the same signal with clock cycles. This is clearly two 1s.

Figure 5-7: Clock Cycles



To transmit more bits per second, the sender uses either more states per clock cycle or briefer clock cycles. The latter is much common. Suppose that you are transmitting in binary and the clock cycle is 1/1000th of a second. This means that you can transmit a thousand bits per second. To transmit 50 gigabits per second with binary signaling, each clock cycle needs to be *one-fifty-billionth* of a second long. The limiting factor on transmission speed today is the ability of sending and receiving devices to work properly over ever shorter clock cycle times.

Test Your Understanding

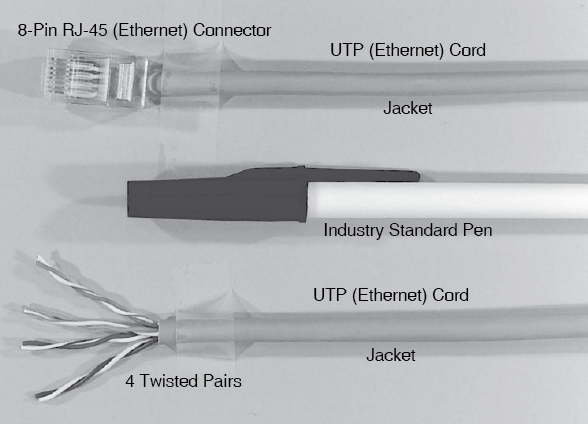
7. a) Why is binary transmission error-resistant? b) In Figure 5-6, by what percentage could the signal attenuate before it became unreadable? c) Compare error resistance in binary and digital signaling. d) If the binary transmission rate is 100 Mbps, how long will a clock cycle be? Express you answer as a fraction of a second.

## UTP and Optical Fiber

Physical layer standards govern transmission media. Ethernet uses two types of cabling today to link hosts to workgroup switches and switches to other switches.

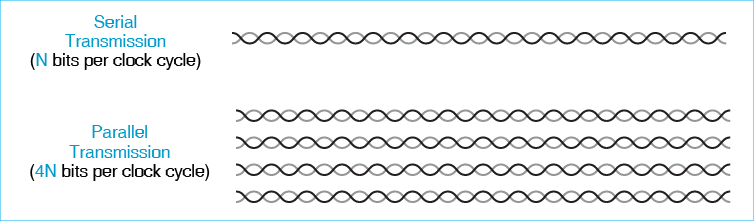
UTP Ethernet often uses copper wire to carry signals. This wiring is called 4-pair unshielded**[[3]](#footnote-3)** twisted pair cabling because the cord contains eight wires arranged in four pairs. The two wires of each pair are twisted around each other several times per inch.[[4]](#footnote-4) Signals are sent by changing voltage or other characteristics of an electrical signal. It is common to refer to this type of cable simply as UTP. Ethernet uses RJ-45 connectors, which snap into RJ-45 jacks. These are popularly called Ethernet connectors and Ethernet jacks.

Figure 5-8: 4-Pair Unshielded Twisted Pair (UTP) Ethernet Cable



As Figure 5-9 shows, Ethernet transmits data on all four pairs in each direction simultaneously. This is called parallel transmission. With four pairs, Ethernet can transmit four times as fast as it could if it only used a single pair.[[5]](#footnote-5) The benefit of parallel transmission is higher speed.

Figure 5-9: Parallel Transmission in Ethernet



Test Your Understanding

8. a) How many wires are there in Ethernet cable? b) How is each pair organized? c) What are the two names for connectors and jacks? d) How does Ethernet use parallel transmission? e) What is the benefit of parallel transmission?

Optical Fiber (Fiber) In optical fiber, light travels through glass. Typically, light is turned on to represent a 1 and off to represent a 0. A fiber cord typically consists of two strands—one for propagation in each direction. Two strands permit simultaneous two-way transmission; which is called full-duplex transmission. While there is only a single UTP connector standard, there are several optical fiber connector standards.

Figure 5-10: Optical Fiber (Fiber) Cable

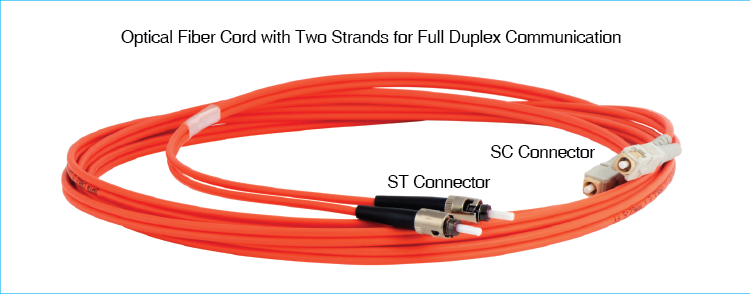
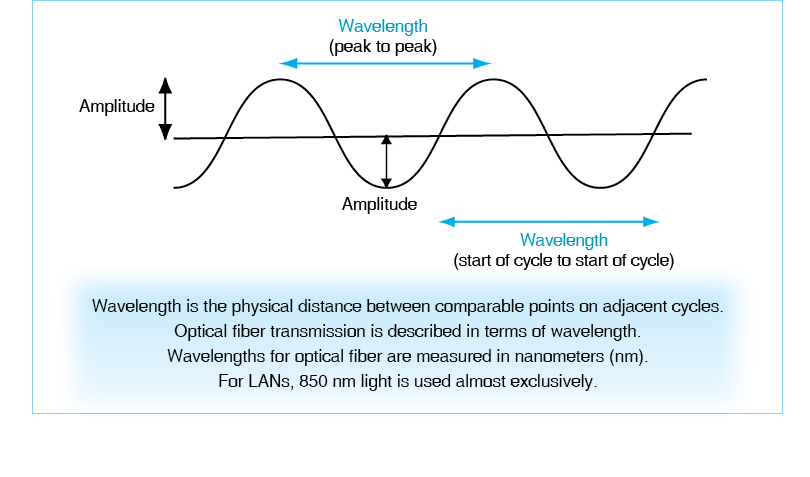


Figure 5-11 shows that light waves are measured in terms of wavelength. This is the physical distance between comparable parts of two consecutive waves. This might be the beginning of one cycle and the beginning of the second, two consecutive peaks, two consecutive troughs, and so forth. The amplitude of the wave, in turn, is its strength or brightness.

Figure 5-11: Light Transmission



Wavelengths are measured in nanometers (nm). In optical fiber, there are three wavelength “windows” in which light travels especially well. These are centered on 850 nm, 1,310 nm, and 1,550 nm. Light using longer wavelength can travel farther, but it costs more to generate. In LANs, 850 nm light dominates signaling because it travels far enough for normal LAN distances, as we will see later.

Test Your Understanding

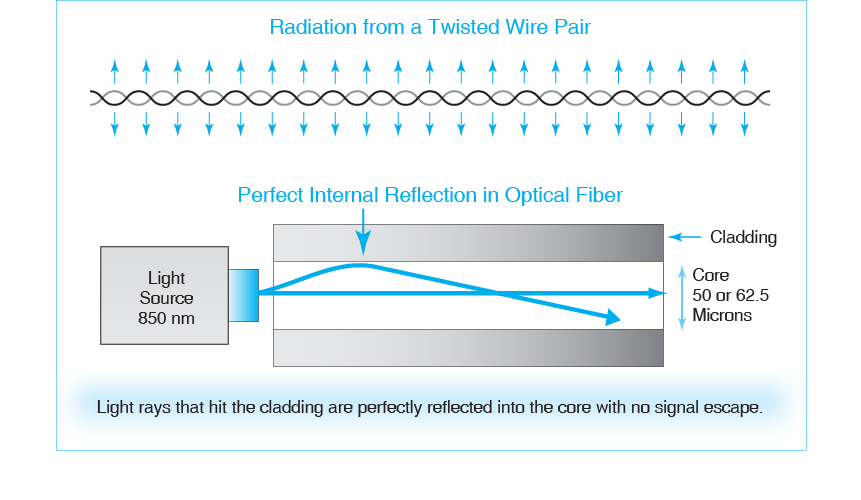
9. a) How does fiber usually transmit a 1? b) How does fiber usually transmit a 0? c) What is full-duplex transmission, and how do fiber cords typically provide it? d) In what units are light waves measured? e) What wavelength dominates in local area networking? f) Why does this wavelength dominate? g) What is amplitude?

## Transmission Distances

When signals propagate, they inevitably attenuate (get weaker) with distance. If they get too weak, they cannot be read reliably. As we will see in the next subsection, maximum cable lengths for UTP are considerably less than they are with optical fiber. We should take a brief look at why that happens before we look at specific distance limitations.

Attenuation in Ethernet Cable  Why are maximum transmission distances short with Ethernet cable? As Figure 5-12 shows, the individual pairs of copper wire that carry signals between devices inevitably act as antennas. They transmit some energy from the signal into the outside world. This dissipates the signal intensity. In addition, copper wire heats up as it carries signals. This also drains energy from the signal. Thanks to both effects, signal attenuation is rapid in Ethernet cable.

Figure 5-12: UTP and Optical Fiber Attenuation



Attenuation in Optical Fiber  Figure 5-12 also shows losses in optical fiber transmission. Transmitted light travels through a very thin glass core about the thickness of a human hair. Around the core is a tightly-fitting glass tube called the cladding. When a light ray hits the core/cladding boundary, the ray bounces back into the core with perfect internal reflection. There is no signal loss. Attenuation comes only from the core’s glass absorbing the light. The glass used in fiber is incredibly transparent, so absorption tends to be very low. Thanks to both effects, signals travel long distances in optical fiber than in UTP.[[6]](#footnote-6)

Test Your Understanding

10. a) Compare UTP and fiber in terms of signal energy loss to the environment. b) Compare them for transmission distance.

## Ethernet Signaling Standards, Media Quality Standards, and Maximum Transmission Distance

ISO/IEC (the International Organization for Standardization and the International Electrotechnical Commission)—not than the 802.3 Working Group—creates *media* standards for copper wiring and optical fiber. These are standardized as ISO/IEC 11801.

The 802.3 Working Group, in turn, standardizes how *signals* will be transmitted over these media. It specifies how 1s and 0s are represented at different speeds over ISO/IEC 11801 media.

Test Your Understanding

11. a) For Ethernet, what organization creates standards for transmission media? Just give the abbreviation. b) What organization creates signaling standards for transmission over these media?

4-Pair UTP For 4-pair UTP, ISO/IEC 11801 quality standards are given numbers, sometimes with letter modifiers. Higher category numbers mean higher cord quality. Figure 5-13 shows that there are three quality levels of Ethernet cable sold today. These are Category 5e (enhanced), Category 6, and Category 6A (augmented). Higher-quality cable is slightly more expensive than lower-quality cable but carries the signal more cleanly. Category is usually abbreviated as “Cat.”

Figure 5-13: Ethernet Signaling Speed, 4-Pair UTP Quality Standards, and Maximum Transmission Distance

|  |  |  |  |
| --- | --- | --- | --- |
| Ethernet Signaling Standard | Speed | ISO UTP Quality Category | Maximum Transmission Distance |
| 100BASE-TX | 100 Mbps | 5e, 6, 6A | 100 meters |
| 1000BASE-T | 1 Gbps | 5e, 6, 6A | 100 meters |
| 10GBASE-T | 10 Gbps | 6 | 55 meters |
| 10GBASE-T | 10 Gbps | 6A | 100 meters |

The figure shows that the Ethernet signaling standard for transmission at 100 Mbps is 100BASE-TX. For 1 Gbps it is 1000BASE-T, and for 10 Gbps, it is 10GBASE-T. The initial number designates the transmission speed, while the “T” stands for “twisted-pair.”

Up to a gigabit per second, the situation is very simple. It does not matter if you use Cat 5e, Cat 6, or Cat 6A. every cable sold, and every cable installed, has sufficient quality. You can always transmit up to 100 meters.

At 10GBASE-T, quality level becomes important. Cat 5e cannot be used at all. For 10 Gbps signaling, ISO created the Cat 6 UTP standard. Unfortunately, when the corresponding Ethernet 10GBASE-T standard was finished, it could only run 55 meters over Cat 6 cabling. ISO responded by creating the Cat 6A cabling quality standard. This brought 10GBASE-T signaling up to the 100 meters that has long been the design goal for Ethernet signaling. Fortunately, there is little use for 10GBASE-T signaling outside of server rooms and other specialized facilities. However, if 10 Gbps is needed, UTP must be purchased carefully.

How can you use the table? Suppose that you have a 75-meter Cat 5e UTP cord connecting a server to the nearest workgroup switch. You need to transmit at a gigabit per second. Using the table, you can see that the cable category is unimportant. However, suppose instead that you had to transmit 120 meters. This is simply too much for UTP. You would have to use optical fiber cabling.

Test Your Understanding

12. a) If I wish to run Ethernet over UTP using 1000BASE-T signaling over a distance of 90 meters, what are my options? b) If I wish to run Ethernet over UTP using 10GBASE-T signaling over a distance of 90 meters, what are my options? c) If I wish to run Ethernet over UTP using 10GBASE-T signaling over a distance of 30 meters, what are my options? d) If I wish to connect two switches with UTP at a speed of 2 Gbps, what options do I have? e) Which should I choose? Justify your answer.

Optical Fiber For the type of optical fiber used in LANs, ISO/IEC 11801 uses OM quality designations. OM stands for optical multimode. Light rays entering at different angles are called modes. LAN fiber being sold today has a core diameter of 50 microns and a cladding diameter of 125 microns. Although the core diameter is only about as thick as a human hair, that is pretty big as far as light rays are concerned. Multiple light modes can propagate. This gives the fiber the designation multimode fiber. Companies can buy thinner fiber, with a core diameter of only 8.3 microns. Only a single mode can travel through this single-mode fiber—the mode propagating straight down the center of the core. Single-mode fiber can carry signals tens of kilometers. Multimode fiber cannot carry signals as far, but its distance limits are typically fine for local area networks, and it is substantially cheaper than single-mode fiber. Consequently, multimode fiber is the norm in LANs.

Figure 5-14 shows maximum transmission distances over the two ISO multimode fiber quality standards that govern fiber sold today. These are OM3 and OM4, which stand for Optical Multimode 3 and Optical Multimode 4. At speeds up to 10 Gbps, both types of fiber easily span the 200 meter to 300 meter distances commonly used for optical fiber in LANs. For speeds of 100 gigabits per second, however, maximum transmission distances are shorter.[[7]](#footnote-7)

Figure 5-14: Ethernet Signaling Speed, Optical Fiber Quality Standards, and Maximum Transmission Distance

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ISO Optical Fiber Quality | Ethernet Signaling Standard | Light Wavelength | Transmission Speed | Maximum Transmission Distance |
| OM3 | 1000BASE-SX | 850 nm | 1 Gbps | 550 meters |
|  | 10GBASE-SR | 850 nm | 10 Gbps | 300 meters |
|  | 100GBASE-SR4 | 850 nm | 100 Gbps | 70 meters |
|  | 100GBASE-SR-10 | 850 nm | 100 Gbps | 100 meters |
| OM4 | 1000BASE-SX | 850 nm | 1 Gbps | 1,000 meters |
|  | 10GBASE-SR | 850 nm | 10 Gbps | 440 meters |
|  | 100GBASE-SR4 | 850 nm | 100 Gbps | 100 meters |
|  | 100GBASE-SR10 | 850 nm | 100 Gbps | 150 meters |

To see how to use the figure, suppose you need to provide 10 Gbps signaling over 279 meters. On OM3 cabling, 10GBASE-SR has a maximum transmission distance of 300 meters, while OM4 fiber will raise this to 440 meters. Either would be fine, but OM3 fiber is less expensive and so would be the correct choice. In turn, if the required distance is 330 meters, only more expensive OM4 fiber would work.

Now suppose that the maximum transmission distance is 85 meters, which is close to the length of a football field. OM3 and OM4 fiber would both work. However, from Figure 5-13, so would Cat 6A UTP. UTP is less expensive than fiber, so when UTP can do the job, it is the correct choice.

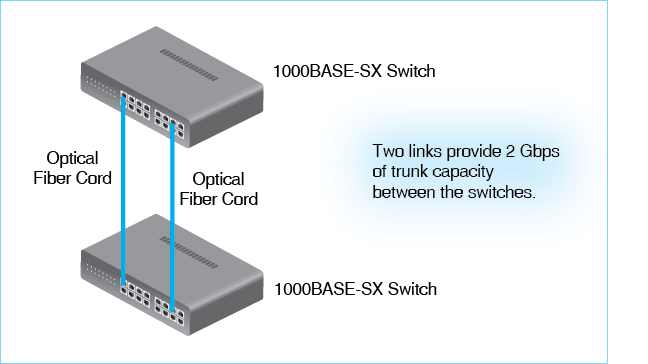
Test Your Understanding

13. a) If I wish to run Ethernet over fiber using 1000BASE-SX signaling over a distance of 500 meters, what are my options? b) Which should I choose? Justify your answer. c) If I wish to run Ethernet over fiber using 10GBASE-SR signaling over a distance of 250 meters, what options do I have? d) Which should I choose? Justify your answer. e) If I wish to run Ethernet over fiber using 10GBASE-SR signaling over a distance of 700 meters, what options do I have? f) What is the farthest I can transmit a signal with 100GBASE-SR signaling?

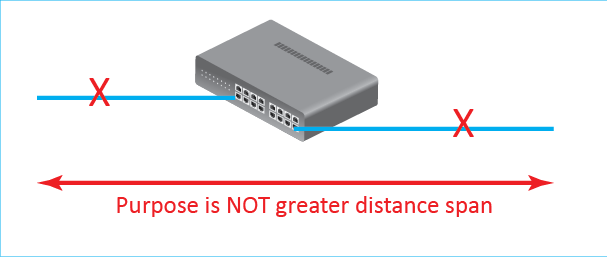
Link Aggregation (Bonding) Ethernet standards usually increase speeds by factors of 10. What should you do if you only need slightly more speed than a certain standard specifies? For example, suppose that you have a pair of 1000BASE-SX switches that you need to connect at 1.8 Gbps? One could replace the switches with 10GBASE-SR switches. However, that would be expensive.

Figure 5-15 illustrates that a company can also use two or more UTP or fiber trunk links to connect a pair of switches. The IEEE calls this link aggregation. Networking professionals also call this bonding. Ethernet supports link aggregation with both UTP and fiber. If you need 1.8 Gbps of capacity to connect two switches, then, two bonded fiber cords using 1000BASE-SX is probably the best choice. Of course, if the distance is small enough to permit UTP, then a pair of bonded UTP cords would be the best choice.

Figure 5-15: Link Aggregation (Bonding)



NOT Link Aggregation



Link aggregation uses existing ports and usually is inexpensive compared to purchasing new faster switches. However, after two or three aggregated links, the company should compare the cost of further link aggregation with the cost of a tenfold increase in capacity by moving up to the next Ethernet speed.

Test Your Understanding

14. a) If I wish to connect two switches with fiber at a speed of 30 Gbps, what options do I have? b) Which would you choose? Justify your answer.

15. a) Who creates UTP and optical fiber cable standards? b) What does the 802.3 Working Group add to these standards? c) Is “Cat 6” an 802.3 standard or an ISO standard? d) Is OM3 an 802.3 standard or an ISO standard? e) Is 1000BASE-SX an Ethernet standard or an ISO standard? f) At what layer is 1000BASE-SX a standard?

# Ethernet Data Link Layer Standards

Single switched networks, like all single networks, require standards at the physical and data link layers. We have just seen that Ethernet has many physical layer standards. We will now turn to Ethernet’s single data link layer standard. Figure 5-16 shows that despite having many physical layer standards, Ethernet only has a single data link layer standard to govern switch forwarding. This is the 802.3 MAC Layer Standard, which governs frame organization and switch operation. Ethernet also has some less common standards at the data link layer, including the Rapid Spanning Tree Protocol we will see later in this chapter.

Figure 5-16: Ethernet Standards for Signaling and Frame Forwarding

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Layer | Standard | | | | |
| Data Link Layer | 802.2 MAC Standard | | | | |
| Physical Layer | 1000BASE-T | 1000BASE-SX | 10GBASE-SR | 100GBASE-SR4 | … |

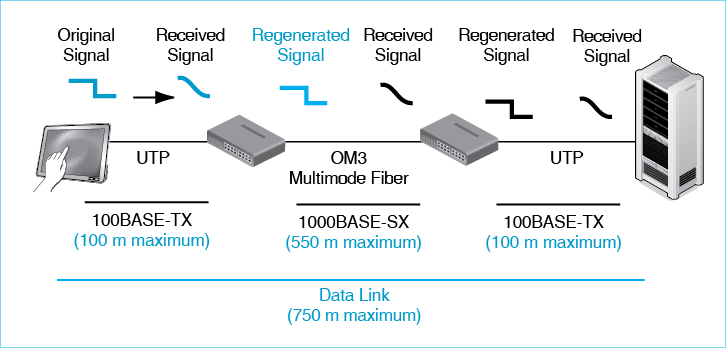
## Physical Link and Data Link Length Restrictions

In the previous section, we looked at distance limitations for physical links in Ethernet. However, network design focuses on data links between two hosts or a host and a router. For data links, there are no distance limitations.

Figure 5-17 shows how multiple physical links are organized into a data link.

* The source sends a signal that is “High-Low.” It transmits this to the first switch via a UTP link. By 100 meters or even less, the signal becomes distorted, but it is still readable as a 1 or 0.
* The first switch completely regenerates the signal by sending a brand-new High-Low undistorted signal. The link between the first and second switches has a maximum span of 550 meters. The signal again becomes distorted as it propagates but is still readable when it arrives because it conforms to the link’s distance limitation..
* The second switch, like the first, regenerates the arriving signal so that it can travel up to 100 meters to the destination host.

Figure 5-17: Physical Links versus Data Links



In the figure, the maximum length of the data link between the source and destination host is 750 meters. However, this can be easily lengthened by adding more switches and transmission lines. The maximum distances we saw earlier in the chapter were for physical links. There is no maximum distance for data links in switched networks, so there is no limit to the size of switched networks.

The maximum distances we saw earlier in the chapter were for physical links. There is no maximum distance for data links in switched networks, so there is no limit to the size of switched networks.

Test Your Understanding

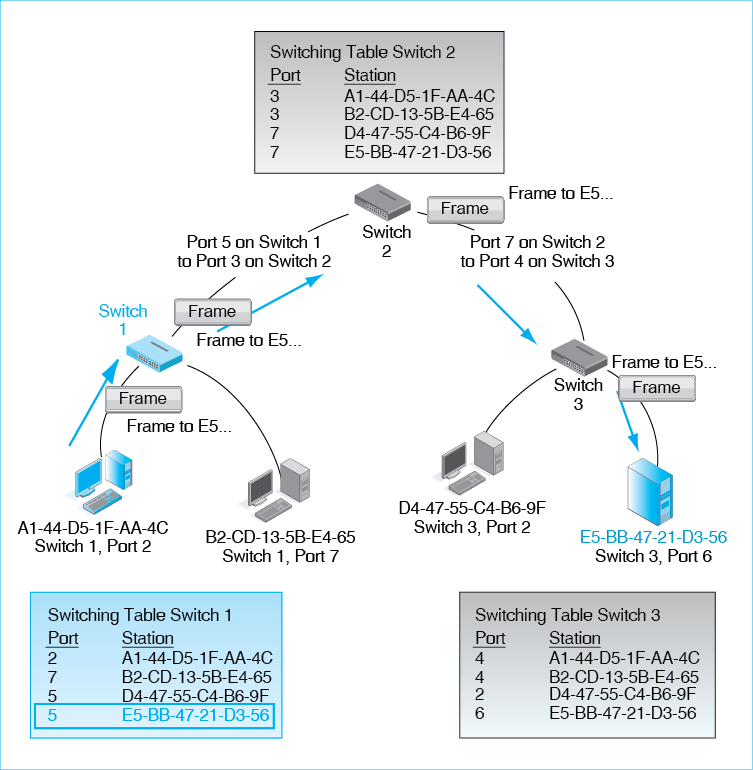
16. a) Were the maximum distances on UTP and optical fiber transmission in Figure 5-13 and Figure 5-14 limits for physical links or data links? b) In Figure 5-17, what would the maximum data length be if both the physical link on the left and the physical length in the middle were changed to OM4 fiber? c) If you need to span 600 meters at 1 Gbps, what options do you have? (Include the possibility of using an intermediate switch.) d) How would you decide which option to choose?

## Ethernet Data Link Layer Switch Operation

In this section, we will discuss the basic data link layer operation of Ethernet switches. This is also governed by the 802.3 MAC Layer Standard. In the section after this one, we will discuss other aspects of Ethernet switching that a firm may or may not use.

Frame Forwarding Figure 5-18 shows an Ethernet LAN with three switches. Larger Ethernet LANs have dozens or hundreds of switches, but the operation of individual switches is the same whether there are a few switches or many. Each individual switch makes a decision about which port to use to send the frame back out to the next switch or to the destination host.

Figure 5-18: Multi-Switch Ethernet Operation



In the figure, Host A1 (we abbreviate the address) wishes to send a frame to Host E5. This frame must go to Switch 1, then Switch 2, and then Switch 3. Switch 3 will send the frame to Host E5.

To begin this process, Host A1 puts E5-BB-47-21-D3-56 in the destination address field of the frame. It sends the frame to Switch 1, into Port 2.

* Switch 1 looks up the address E5-BB-47-21-D3-56 in its switching table. It sees that E5 is associated with Port 5, so it sends the frame out Port 5. This is a very simple process, so it requires little processing power. This means that Ethernet switches are inexpensive for the volume of traffic they carry.
* Port 5 on Switch 1 connects to Port 3 on Switch 2. Switch 2 now looks up the address E5-BB-47-21-D3-56 in its own switching table. This address is associated with Port 7, so Switch 2 sends the frame out Port 7.
* The frame arrives at Switch 3 through Port 4. Switch 3 now looks up the address E5-BB-47-21-D3-56 in its own switching table. This time, the address is associated with Port 6. Switch 3 sends the frame out Port 6. This takes it to the destination Host E5-BB-47-21-D3-56.

Note that each switch only knows the information in its switching table. More specifically, it only knows what port to use to send the frame back out. Switches do not know the entire data link between the source host and the destination host.

Test Your Understanding

17. a) Do switches know the entire data link between the source and destination host? b) What does a switch know?

Hierarchical Switch Organization  Note that the switches in Figure 5-18 form a hierarchy, in which each switch has only one parent switch above it. In fact, the Ethernet standard requires a hierarchical topology (topology is the physical organization of switches and transmission links). Otherwise, loops would exist, and a single loop will cause the network to shut down. Figure 5-2 earlier showed a larger switched Ethernet LAN organized in a hierarchy.

Ethernet requires a hierarchical switch topology.

In a hierarchy, there is only a single possible path between any two hosts. (To see this, select any two hosts at the bottom of the hierarchy in Figure 5-2 and trace a path between them. You will see that only one path is possible.) If there is only a single possible path between any two hosts, it follows that, in every switch along the path, the destination address in a frame will appear only once in each switching table—in a row for the specific port to be used to send the frame on its way.

In a hierarchy, there is only a single possible path between any two hosts.

If an Ethernet address only appears once, then a very simple and quick lookup will find the row. This is very fast and therefore costs little per frame handled. Inexpensive lookup for each arriving frame is what makes Ethernet switches inexpensive. As noted in the introduction, simple switching operation and therefore low cost has led to Ethernet’s dominance in LAN technology.

The fact that there is only a single possible path between any two end hosts in an Ethernet hierarchy makes Ethernet switch forwarding simple and therefore inexpensive. This low cost has led to Ethernet’s dominance in LAN technology.

In Chapter 8, we will see that routers have to do much more work when a packet arrives. Routers are connected in a mesh, so there are multiple alternative routes between any two hosts. Each of these alternative routes appears as a row in the routing table. Therefore, when a packet arrives, a router must first identify all possible routes (rows) and then select the best one—instead of simply finding a single match. This additional work per packet makes routers very expensive for the traffic load they handle.

Test Your Understanding

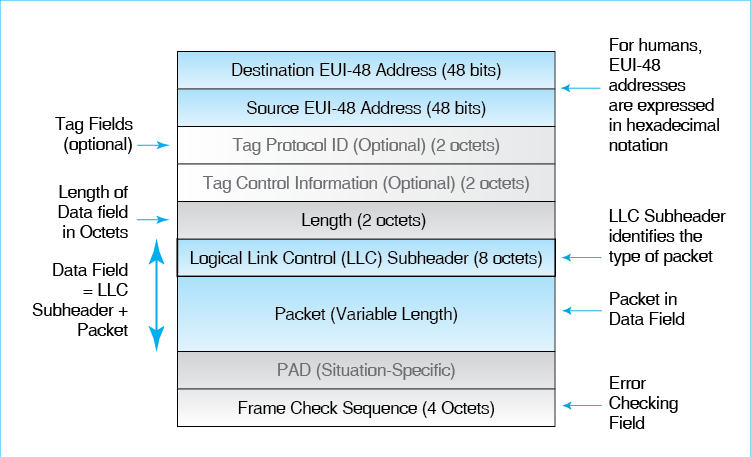
18. a) How are switches in an Ethernet LAN organized? b) Because of this organization, how many possible paths can there be between any two hosts? c) In Figure 5-2, what is the single possible path between Client PC 1 and Server X? Just give the letters of the switches. d) Between Client PC 1 and Server Y? Just give the letters of the switches.

19. a) What is the benefit of having a single possible path through an Ethernet network? b) Why has Ethernet become the dominant LAN technology?

## The Ethernet Frame

Figure 5-19 shows an Ethernet 802.3 frame, which we saw briefly in Chapter 2. We will now look at some elements in the Ethernet frame in more detail.[[8]](#footnote-8) Recall that an *octet* is a byte.

Figure 5-19: Ethernet 802.3 Frame



Source and Destination Address Fields  We saw in Chapter 2 that Ethernet address are EUI-48 addresses. While computers work with this raw 48-bit form, humans normally express these addresses in Base 16 hexadecimal (hex) notation. To convert a 48-bit Ethernet address into hex notation, follow these three steps:

* First, divide the 48 bits into twelve 4-bit units, which computer scientists call nibbles.
* Second, convert each nibble into a hexadecimal symbol, using Figure 5-20. For example, 1100 is a C.
* Third, write the symbols as six pairs with a dash between each pair—for instance, B2-CC-66-0D-5E-BA. (Each pair represents 1 octet.) In this case, the first byte would be 10110010, which becomes B2, followed by a dash.

Figure 5-20: Hexadecimal Notation

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 4 Bits | Decimal (Base 10) | Hexadecimal (Base 16) |  | 4 Bits\* | Decimal (Base 10) | Hexadecimal (Base 16) |
| 0000 | 0 | 0 hex |  | 1000 | 8 | 8 hex |
| 0001 | 1 | 1 hex |  | 1001 | 9 | 9 hex |
| 0010 | 2 | 2 hex |  | 1010 | 10 | A hex |
| 0011 | 3 | 3 hex |  | 1011 | 11 | B hex |
| 0100 | 4 | 4 hex |  | 1100 | 12 | C hex |
| 0101 | 5 | 5 hex |  | 1101 | 13 | D hex |
| 0110 | 6 | 6 hex |  | 1110 | 14 | E hex |
| 0111 | 7 | 7 hex |  | 1111 | 15 | F hex |

Divide a 48-bit Ethernet address into 12 four-bit “nibbles.” (1010, 0001, etc.)

Convert each group of 4 bits into a Hex symbol. (A, 1, etc.)

Combine two hex symbols into pairs and place a dash between pairs A1-etc.)

For example, 10100001 becomes 1010 0001, which becomes A 1, which becomes A1 (followed by a dash)

The finished hex expression might be: A1-36-CD-7B-DF-01 hex

To convert a hex address back to binary, change each symbol pair back to its 8-bit pattern. For example, if a hex pair is 2E, 2 is 0010, and E is 1110, so 2E is equivalent to the octet 00101110. Note that you must keep the two leading 0s in 0010.

Test Your Understanding

20. a) What were Ethernet addresses originally called? b) What are they called today? c) What are the steps in converting EUI-48 addresses into hex notation? d) Convert 11000010 to hex. e) Convert 7F hex to binary. f) Convert the EUI-48 address A1-B2-C3-44-5D-3C to binary. Leave a space between each octet. As a check, there must be 48 bits.

Tag Fields (Optional)  In Chapter 4, we saw that companies may give frames priority levels so that high-priority frames for latency-intolerant applications can go first. This was not in the original 802.3 standard. If a company wishes to use priority, it must configure its equipment to recognize two optional tag fields. The first indicates that the frame is tagged, while the second gives the tagged information. These fields are inserted just before the length field. Three bits in the Tag Control Information field are for priority level. With three bits, there can be eight priority levels. We will see later that another 12 bits are used to specify VLANs. Note that these tag fields are optional. If priority and the other matters they handle are not used, there are no tag fields in the frame.

Length Field  The length field contains a binary number that gives the *length of the data field* (not of the entire frame) in octets. The maximum length of the data field is 1,522 octets. There is no minimum length for the data field.[[9]](#footnote-9)

The Data Field  The data field contains two subfields: the LLC subheader and the packet that the frame is delivering.

* The logical link control layer (LLC) subheader is 8 octets long. The purpose of the LLC subheader is to describe the type of packet contained in the data field. For instance, if the LLC subheader ends with the code 08-00 hex, then the data field contains an IPv4 packet. To give another example, the code 86-DD hex indicates an IPv6 packet.
* The data field also contains the packet that the MAC layer frame is delivering. The packet usually is far longer than all other fields combined.

Frame Check Sequence Field  The last field in the Ethernet frame is the Frame Check Sequence Field, which permits error detection. This is a 4-octet field. The sender does a calculation based on other bits in the frame and places the 32-bit result in the Frame Check Sequence Field. The receiver redoes the calculation and compares its result with the contents of the Frame Check Sequence Field. If the two are different, there is an error in the frame. If there is an error, the receiver simply discards the frame. There is no retransmission of damaged frames.

Test Your Understanding

21. a) In what fields is priority and VLAN information conveyed? b) What are the two components of the Ethernet data field? c) What is the purpose of the LLC subheader? d) What is the purpose of the Frame Check Sequence Field? e) What happens if the receiver detects an error in a frame?

# Ethernet Security

Until recently, few organizations worried about the security of their wired Ethernet networks. Only someone within the site could get access to the LAN, and this seemed unlikely. Unfortunately, experience has shown that attackers *usually* can get into sites. Once into the site network, the attacker can plug into any wall jack. This bypasses the border firewall. While site networks are hard and crunchy to outside attackers, they tend to be soft and chewy to attackers who get inside.

## Port-Based Access Control (802.1X)

To thwart the ability of attackers to simply plug into the internal network, companies can implement 802.1X, which is a standard for Port-Based Access Control on the workgroup switches that give users access to the network. With 802.1X, whenever a host connects to the network, its user must prove his or her identity before the workgroup switch will pass further traffic.

Figure 5-21: 802.1X Port-Based Access Control on an Ethernet Switch

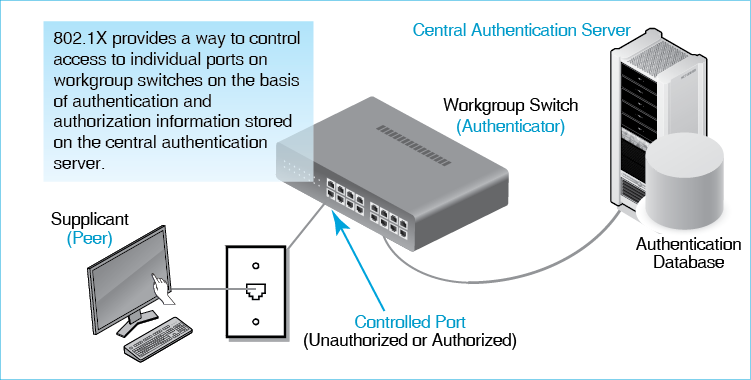


Figure 5-21 illustrates 802.1X. The supplicant is called the peer. The workgroup switch is called the authenticator. It gets this name because the workgroup switch provides authentication service to the supplicant computer. The 802.1X standard also uses a central authentication server to do the actual supplicant credentials checking.

When the supplicant host (peer) transmits its authentication credentials (password, etc.), the authenticator passes these credentials on to the authentication server. The authentication server checks these credentials against its authentication database. If the authentication server authenticates the credentials, it sends back a confirmation to the workgroup switch. The workgroup switch then allows the supplicant PC to send frames to other devices in the network.

Using a central authentication server provides four benefits.

* Switch Cost. First, having the central authentication server check credentials instead of having the switch doing this minimizes the processing power needed in the workgroup switch. Given the large number of workgroup switches in firms, this reduces overall cost.
* Consistency. Second, having all credentials on the authentication server gives consistency in authentication. Attackers cannot try many different workgroup switches until they find one that is misconfigured and gives them access.
* Reduced Management Cost. Third, management cost is reduced because credentials only need to be changed on the central authentication server when a user joins the firm, leaves the firm, or needs other credential changes. Making these changes on many workgroup switches separately would be prohibitively expensive.
* Rapid Changes. Fourth, the credentials of individuals who are fired or suspended can be invalidated in seconds, removing access to all workgroup switches.

Note from its name that the 802.1X standard was created by the 802.1 Working Group, not by the 802.3 Working Group that creates Ethernet standards. The 802.1 Working Group produces standards that cut across all 802 network technologies. This includes security standards.

The 802.1 Working Group produces standards that cut across all 802 network technologies. This includes security standards.

Test Your Understanding

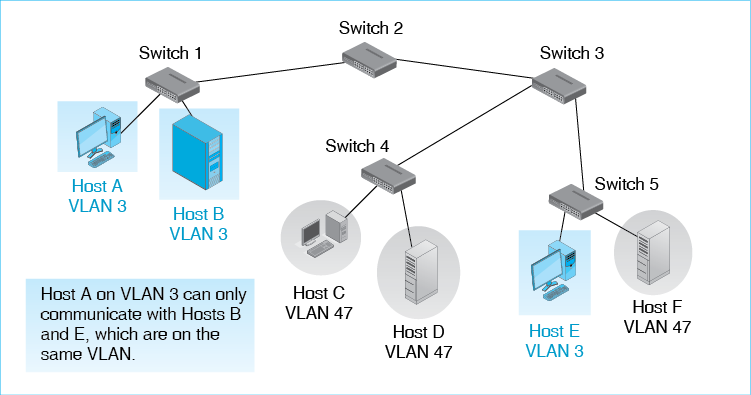
22. a) What threat does 802.1X address? b) In 802.1X, what device is the authenticator? c) What are the four benefits of using a central authentication server instead of having the individual authenticators do all authentication work?

Virtual LANs (VLANs)

By default, any host on an Ethernet network can send frames to any other host. Unfortunately, this is not always a good thing. For example, one might wish to isolate sensitive accounting traffic so that employees in other departments (and attackers who “own” computers in other departments) cannot read this traffic. Ethernet supports this through the creation of virtual LANs (VLANs), which segregate traffic on switches and shared trunk links to give the illusion that each VLAN is a real LAN. People working in accounting seem to have their own private LAN that nobody else shares.

In Figure 5-22, a small Ethernet network has two VLANs. Client hosts A and E can communicate with server host E because all three are on the same VLAN, VLAN 3. However, they cannot reach servers D and E because they are on a different VLAN, VLAN 47.

Figure 5-22: Virtual LANs (VLANs)



In some cases, the hosts on a particular VLAN can be assigned IP addresses on a single subnet. This allows switches to segregate traffic on the basis of IP addresses as well. This saves money because if someone in a workgroup moves to a different physical location, they can take their IP address with them. Normally, physical movement will connect a host to a different router port, requiring a change in IP address.

Test Your Understanding

23. a) In Figure 5-22, what servers can Host C reach? b) Why do VLANs add to security? c) What is the benefit of a host being able to keep its IP address after a physical move?

# Conclusion

## Synopsis

In this chapter, we looked at Ethernet switched wired LANs. In contrast to wide area networks (WANs), LANs are inexpensive per bit transmitted, so organizations can afford to provide extremely high-speed LAN service. There once were several switched wired LAN technologies, but Ethernet, which is standardized by the IEEE 802 Committee’s 802.3 Working Group, is the only significant switched wired LAN technology today.

All LANs are governed by physical and data link layer standards. We began by looking at physical layer concerns, specifically binary and digital signaling, which give resistance to transmission error. Ethernet uses two major transmission media. Four-pair unshielded twisted pair (UTP) copper wiring dominates in access links between hosts and the workgroup switches to which they connect. Optical fiber, which can span longer distances, is used primarily in trunk links to connect switches to other switches. LANs use inexpensive 850 nm multimode fiber, which can span the distances needed in LANs. Normally, a single UTP or optical fiber link connects a pair of switches. However, with link aggregation (also called bonding), a pair of switches can be connected by two or more UTP or fiber links. Ethernet has many physical layer standards for both UTP and optical fiber signaling. Standards set both transmission speed and maximum distance. They allow network designers to select media standards for specific media runs within the customer premises. For UTP, quality levels are indicated by category numbers. Today, Category 5e, 6, and 6A wiring are dominant. Optical fiber quality is standardized with OM numbers. Current fiber on sale fires the OM3 and OM4 standards.

Although Ethernet has many physical layer standards, it only has a single data link layer standard, the 802.3 MAC Layer Standard. We looked at some aspects of Ethernet’s frame organization. The source and destination EUI-48 addresses are 48 bits long and are expressed for human consumption in hexadecimal notation. Optional tag fields allow priority and VLANs. The data field has two subfields. The first is the 8-bit logical link control (LLC) subheader, which specifies the type of packet contained in the data field. The second is the packet itself—usually an IP packet, although other types of packets can be carried. The final Frame Check Control Sequence field is for error checking.

We looked at how Ethernet switches forward frames. Ethernet networks must be organized as a hierarchy, in which there are no loops among the switches. Consequently, there is only a single path between any two hosts. This makes Ethernet switching tables very simple, so Ethernet switches are both fast and inexpensive.

Ethernet security has not been seen as a major issue in most firms. However, we reviewed the 802.1X standard that requires a host to authenticate itself to a switch port before it is allowed to use the network. This prevents attackers from walking into a firm and simply plugging into any Ethernet wall jack. In 802.1X, the host is called a peer, the switch is the authenticator, and there is a back-end authentication server that actually checks authentication credentials. Having a central authentication server that keeps authentication data and makes authentication decisions reduces the work that must be done by the switch. This minimizes switch cost. Centralizing authentication data and decisions on the authentication server also brings consistency to authentication, reduces switch and management cost, and allows the status of individual users to be changed instantly. Note that this security standard comes from the 802.1 Working Group, not the 802.3 Working Group.

Finally, we saw how Ethernet can support virtual LANs (VLANs), which segregate traffic so that certain hosts can only communicate with other hosts. This makes it very difficult for an attacker who is on a different VLAN to reach servers on a protected VLAN.

## End-of-Chapter Questions

Thought Questions

5-1 a) List the security planning principles from Chapter 4. b) When implementing SNMP for managed switches, what security planning principle must be considered?

5-2. If you add VLANs to your network, what security planning principle is enhanced?

5-3. In Chapter 3, we saw the distinction between supplicants and verifiers. In Figure 5-21, the peer is the supplicant. Which device is the verifier? (This is a trick question, but it gets at an important point.)

5-4. In Figure 5-22, which server host(s) can Host C access?

Design Questions

5-5. Design an Ethernet network to connect a single client PC to a single server. Both the client and the server will connect to their workgroup switches via UTP. The two devices are 900 meters apart. They need to communicate at 800 Mbps. Your design will specify the locations of any switches and the transmission link between the switches.

5-6. Add to your design in the previous question. Add another client next to the first client. Both connect to the same switch. This second client will also communicate with the server and will also need 800 Mbps in transmission speed. Again, your design will specify the locations of switches and the transmission link between the switches.

Troubleshooting Question

5-7. You connect two switches in a large Ethernet switch with 32 switches. You are using 4-pair UTP. Immediately after you make the connection, the network stops transmitting traffic. What do you think might have happened? If you cannot come up with a good hypothesis, reread the synopsis and see which points might apply. Do not do other steps in the troubleshooting process.

Perspective Questions

5-8. What was the most surprising thing you learned in this chapter?

5-9. What was the most difficult part of this chapter for you?

1. “Customer premises” is always spelled as plural, although it is used as if it is singular. It’s a legal jargon thing. [↑](#footnote-ref-1)
2. If “bi” means two, where does “digital” come from? It comes from the fact that we call our ten fingers *digits*. In fact, some early computer systems operated on Base 10 arithmetic, the same arithmetic that we ten-fingered people use. Very quickly, however, the advantages of building computers and transmission systems that used two or a multiple of two states brought about binary and digital computation and so binary and digital signaling. [↑](#footnote-ref-2)
3. Ethernet cable is unshielded. To operate in harsh electromagnetic environments, cords may be protected by surrounding the entire cord and perhaps even individual pairs with metal foil shielding. While placing tin foil on your head may not protect you from the government’s eavesdropping on your thoughts, metal foil prevents the electromagnetic background energy from interfering with the cable signal. Today, shielded cabling is rarely needed. [↑](#footnote-ref-3)
4. Why are the wires of each pair twisted around each other? The answer is that it limits the effects of nearby electromagnetic interference from lights, electrical motors, and other wire pairs, even in the same four-pair cable. In the 19th century, Alexander Graham Bell realized that if the two wire of a pair were twisted around each other, interference that would add a signal on one half of the twist would subtract this signal over the other half. Over an entire twist, the interference would cancel out. Does it really work this perfectly? No, it but it works quite well. [↑](#footnote-ref-4)
5. Ethernet is not the only transmission technology to use parallel transmission. In the past, many printer interfaces uses eight or more transmission lines in each direction. Most computers, in turn, connect their components with a transmission bus that has 100 or more wires for transmission. [↑](#footnote-ref-5)
6. For the multimode fiber used in LANs, there is a third factor that limits propagation distance. This is modal dispersion. Light can only enter the core at a small number of angles. These are called modes. In single-mode fiber, there is only a single mode that travels straight down the middle of the core, never hitting the cladding. For this, the core’s diameter must be extremely small, about 8.3 microns. In multimode fiber, which has a core diameter of about 50 microns, several modes can transmit, as Figure 5-11 shows. For any given distance, the mode traveling straight down the middle of the core will arrive faster than modes that bounce off the core/cladding boundary multiple times. This arrival time difference is modal dispersion. Beyond some distance, the modes of successive clock cycles will begin to overlap, making the signal unreadable. However, single-mode fiber is substantially more expensive than multimode fiber, and multimode fiber is sufficient for LAN distances of a few hundred yards. [↑](#footnote-ref-6)
7. Actually, some OM3 and OM4 fiber can carry signals for a given speed farther than the maximum transmission distance shown in the figure. Fiber quality is measured as *modal bandwidth*. OM3 and OM4 specify a minimum modal bandwidth at various speeds, and these specifications create the distance limits shown in the figure. Fiber manufacturers, however, are free to offer OM3 and OM4 fiber with higher modal bandwidth than the standards specify. This “beyond-standard” fiber can carry signals farther for a given transmission speed. [↑](#footnote-ref-7)
8. We will not look at two fields sometimes shown in an Ethernet frame, the preamble and start of frame delimiter. These are synchronization fields that are now considered part of Ethernet’s physical layer operation. Nor will we look at the PAD field, which was important in the early days of Ethernet technologies but no longer has a meaningful role to play. In any case, networking professionals do not look at the PAD field when inspecting the contents of an 802.3 frame. [↑](#footnote-ref-8)
9. Although there is no minimum length, if the data field is less than 46 octets long, additional PAD bits are added so that the total of the data field and the PAD are 46 bits long. As noted in an earlier footnote, this is a holdover from early Ethernet technologies and is irrelevant today. However, it is still in the standard for backward compatibility. [↑](#footnote-ref-9)