

4: Layer 1 – Electronics and Signals

4.3.1.1. Compare and contrast analog and digital signals.

Signal refers to a desired electrical voltage, light pattern, or modulated electromagnetic wave. All of these can carry networking data.

One type of signal is *analog*. An *analog* signal has the following characteristics:

- is wavy
- has a continuously varying voltage-versus-time graph
- is typical of things in nature
- has been widely used in telecommunications for over 100 years

The graphic on the left shows a pure *sine wave*. The two important characteristics of a *sine wave* are its *amplitude* (*A*), its height and depth, and its *period* (*T* = length of time) to complete 1 cycle. You can calculate the *frequency* (*f*), wiggly-ness, of the wave with the formula $f = 1/T$.

Another type of signal is *digital*. A *digital* signal has the following characteristics:

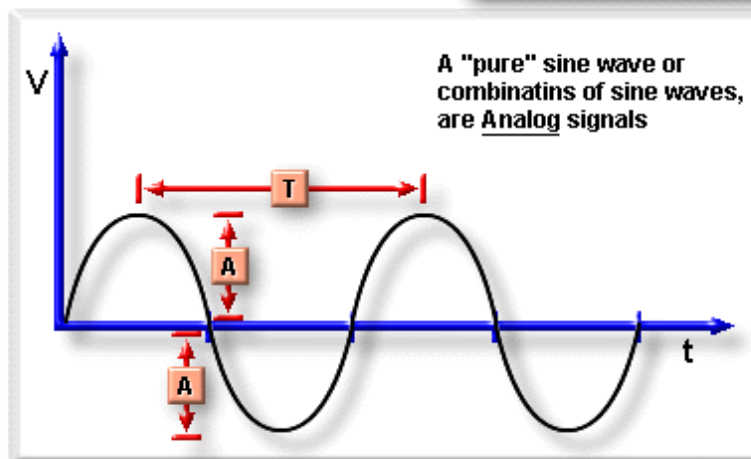
- has discrete, or jumpy, voltage-versus-time graphs
- is typical of technology, rather than nature

The graphic shows a digital networking signal. Digital signals have a fixed amplitude, even though their pulse, width, *T*, and frequency, can be changed. Digital signals from modern sources can be approximated by a *square wave*, which has seemingly instantaneous transitions from low to high voltage states, with no wiggles. While this is an approximation, it is a reasonable one, and will be used in all future diagrams.

Analog Signals

- Continuous voltage
- Can have any value
- "Wavy" voltage as time progresses
- Many encodings possible
- The most basic analog signal
- More complex analog signal

A = Amplitude (height or depth of wave)
T = Period (time to complete 1 wave cycle)
F = Frequency (cycles per second) = $1/T$



4: Layer 1 – Electronics and Signals

4.3.2.1. Explain how digital signals can be built by analog signals.

Jean Baptiste Fourier made one of the greatest mathematical discoveries. He proved that a special sum of sine waves, of harmonically related frequencies, which are multiples of some basic frequency, could be added together to create any wave pattern. This is how voice recognition devices in spy movies, and heart pacemakers work. Complex waves can be built out of simple waves.

A *square wave*, or a *square pulse*, can be built by using the right combination of sine waves. The graphic shows how the square wave (digital signal) can be built with sine waves (analog signals). This is important to remember, as you examine what happens to a digital pulse as it travels along networking media.

4: Layer 1 – Electronics and Signals

4.3.3.1. Recognize and define one bit on a physical medium

Data networks have become increasingly dependent on digital (binary, two-state) systems. The basic building block of information is 1 binary digit, known as the bit or *pulse*.

One bit, on an electrical medium, is the electrical signal corresponding to binary 0 or binary 1. This may be as simple as 0 volts for binary 0, and +5 volts for binary 1, or a more complex encoding. *Signal reference ground* is an important concept relating to all networking media that use voltages to carry messages.

In order to function correctly, a *signal reference ground* must be close to a computer's digital circuits. Engineers have accomplished this by designing ground planes into circuit boards. The computer cabinets are used as the common point of connection for the circuit board ground planes to establish the *signal reference ground*. *Signal reference ground* establishes the 0 volts line in the signal graphics.

With optical signals, binary 0 would be encoded as a low, or no light, intensity (darkness). Binary 1 would be encoded as a higher light intensity (brightness), or other more complex patterns.

With wireless signals, binary 0 might be a short burst of waves; binary 1 might be a longer burst of waves, or another more complex pattern.

You will examine six things that can happen to 1 bit:

- propagation
- attenuation
- reflection
- noise
- timing problem
- collisions

4: Layer 1 – Electronics and Signals

4.3.4.1. Explain propagation of network signals

Propagation means travel. When a NIC card puts out a voltage or light pulse onto a physical medium, that square pulse, made up of waves, travels along the medium, or *propagates*. *Propagation* means that a lump of energy, representing one bit, is traveling. The speed at which it *propagates* depends on the actual material used in the medium, the geometry, or structure, of the medium, and the frequency of the pulses. The time it

takes the bit to travel from one end of the medium and back again is referred to as the *round trip time*, (*RTT*). Assuming no other delays, the time it takes the bit to travel down the medium to the far end is $RTT/2$.

The fact that the bit travels does not cause a problem for the network. All of the networking actually occurs so fast, that sometimes you must account for the amount of time it takes the signal to travel.

There are two extreme situations to consider. Either the bit takes no time to travel, meaning it travels instantaneously, or it takes forever to travel. The first case is wrong according to Einstein, whose "Theory of Relativity" says no information can travel faster than the speed of light in vacuum. This means that the bit takes at least a small amount of time to travel. The second case is also wrong, because with the right equipment, you can actually time the pulse. Lack of knowledge, of propagation time, is a problem because you might assume the bit arrives at some destination either too soon, or too late.

This problem can be resolved. Again, propagation time is not a problem, it's simply a fact that you should be aware of. If the propagation time is too long, you should re-evaluate how the rest of the network will deal with this delay. If the propagation delay is too short, you may have to slow down the bits, or save them temporarily (known as *buffering*), so that the rest of the networking equipment can catch up with the bit.

4: Layer 1 – Electronics and Signals

4.3.5.1. Recognize and define attenuation as it applies to networking

Attenuation is a fancy word for a signal losing energy to its surroundings. This means our one bit voltage signal loses height, or amplitude, as energy is given from the message to the cable. While careful choice of materials, such as copper instead of carbon, and geometry, the shape and positioning of the wires, can reduce the electrical attenuation, some loss is always unavoidable when electrical resistance is present.

Attenuation also happens to optical signals -- the optical fiber absorbs and scatters some of the light energy as the light pulse, one bit, travels down the fiber. This can be minimized by the wavelength, or color, of the light chosen. This can also be minimized by whether or not single mode or multimode fiber is used and the actual glass used for the fiber. Even with these choices, signal loss is unavoidable.

Attenuation also happens to radio waves and microwaves, as they are absorbed and scattered by specific molecules in the atmosphere.

Attenuation can effect the network since it limits the length of network cabling on which a message can be sent. If the cable is too long or too attenuating, one bit sent from the source can look like a zero bit by the time it gets to the destination.

This can be resolved through the networking media that are chosen, and if their structures are designed to have low amounts of attenuation. One way to fix the problem is to change the medium. A second way is to have a device called a "repeater" after a certain distance. There are repeaters for electrical, optical, and wireless bits.

To view a java applet of the attenuation process, go to

<http://bugs.wpi.edu:8080/EE535/>

4: Layer 1 – Electronics and Signals

4.3.6.1. Recognize and define reflection as it pertains to networking

To understand *reflection*, imagine that you have a slinky, or a jump rope stretched, out with a friend holding the other end. Now, imagine sending them a "pulse" or a 1-bit message. If you watch carefully, a small part of your original pulse will be reflected back at you.

Reflection occurs in electrical signals. When voltage pulses, or bits, hit a discontinuity, some energy can be reflected. This occurs in any change in a material's final stop, or connection to another material, even if it's the same material. If not carefully controlled, this energy can confuse other bits. Real networks send millions and billions of bits every second. This requires constant awareness of the reflected pulse energy. Depending on the cabling and connection used, reflections may or may not be a problem.

Reflection also happens with optical signals. Optical signals reflect whenever they hit a discontinuity in the glass (medium), such as when a connector is plugged into a device. You can see this effect at night when you look out a window. You see your own reflection in the window, even though the window is transparent. This phenomenon also occurs with radio waves and microwaves, as they encounter different layers in the atmosphere. This may cause problems on your network.

For optimal network performance, it is important that the network media have a specific impedance, in order to match the electrical components in the NIC cards. If the network media have the incorrect impedance, signals can sustain some reflection, and interference can occur, then multiple reflecting pulses can occur. Whether the system is electrical, optical, or wireless, impedance mismatches cause reflections, and if enough energy is reflected, the binary (2-state) system can become confused by all the extra energy that is bouncing around. Discontinuities in impedance can be avoided through a variety of technologies.

4: Layer 1 – Electronics and Signals

4.3.7.1. Recognize and define noise

Noise is unwanted additions to a voltage pulse, optical pulse, or electromagnetic wave pulse. No electrical signal is without noise, however, it is important to keep the signal-to-noise (S/N) ratio as high as possible. In other words, each bit receives additional unwanted signals from various sources. Too much noise can corrupt a binary 1 into a binary 0, or a 0 into a 1, destroying the 1-bit message.

The graphic shows five sources of noise that can affect 1 bit that is on a wire:

- *NEXT-A, NEXT-B*
- *thermal noise*
- *AC power/reference ground noise*
- *EMI/RFI*

Optical and wireless systems experience some of these forms of noise but are immune to others. For example, optical fiber is immune to NEXT and AC power/reference ground noise, and wireless systems are particularly prone to EMI/RFI. We will focus on noise in copper-based wiring systems.

NEXT-A and NEXT-B

When electrical noise on the cable originates from signals on other wires in the cable, this is known as *crosstalk*. *NEXT* stands for *near end crosstalk*. When two wires are near each other and untwisted, energy from one wire can wind up in an adjacent wire and vice versa. This can cause noise at both ends of a terminated cable. There are actually many forms of cross-talk which must be considered when building networks.

Thermal Noise

Thermal noise, due to the random motion of electrons, is unavoidable but usually relatively small compared to our signals.

AC Power Line and Reference Ground Noise

AC Power and *reference ground noises* are crucial problems in networking. AC line noise creates problems in our homes, schools, and offices. Electricity is carried to appliances and machines via wires concealed in walls, floors, and ceilings. Consequently, inside these buildings AC power line noise is all around us. If not properly addressed, power line noise can present problems for a network.

You will discover that AC line noise coming from a nearby video monitor or hard disk drive can be enough to create errors in a computer system. It does this by burying the desired signals and preventing a computer's logic gates from detecting the leading and trailing edges of the square signal waves. This problem can be further compounded when a computer has a poor ground connection.

Ideally the signal reference ground should be completely isolated from the electrical ground. Isolation would keep AC power leakage and voltage spikes off the signal reference ground. However, engineers have not found it practical to isolate the signal reference ground in this manner. Instead, the chassis of a computing device serves as the signal reference ground, it also serves as the AC power line ground.

The links between the signal reference ground and the power ground can lead to problems. Since there is a link between the signal reference ground and the power ground, problems with the power ground can lead to interference with the data system. Such interference can be difficult to detect and trace. Usually, they stem from the fact that electrical contractors and installers don't care about the length of the neutral and ground wires that lead to each electrical outlet. Unfortunately, when these wires are long, they can act as an antenna for electrical noise. It is this noise that interferes with the digital signals a computer must be able to recognize.

EMI/RFI

External sources of electrical impulses that can attack the quality of electrical signals on the cable include lighting, electrical motors, and radio systems. These types of interference are referred to as *electromagnetic interference (EMI)*, and *radio frequency interference (RFI)*.

Each wire in a cable can act like an antenna. When this happens, the wire actually absorbs electrical signals from other wires in the cable and from electrical sources outside the cable. If the resulting electrical noise reaches a high enough level, it can become difficult for NIC cards to discriminate the noise from the data signal.

This is particularly a problem because most LANs use frequencies in the 1–100 megahertz (MHz) frequency region, which happens to be where FM Radio signals, TV signals, and lots of appliances have their frequencies as well.

To understand how electrical noise, regardless of the source, impacts digital signals, imagine that you want to send data, represented by the binary number 1011001001101, over the network. Your computer converts the binary number to a digital signal. (This graph shows what the digital signal for 1011001001101 looks like.).

The digital signal travels through the networking media to the destination. The destination happens to be near an electrical outlet that is fed by long neutral, and ground, wires. These wires act as an antenna for electrical noise. (This graph shows what electrical noise looks like.).

Because the destination computer's chassis is used for both the earth ground and the signal reference ground, this noise interferes with the digital signal the computer receives. This graph shows what happens to the signal when it is combined with electrical noise. Instead of reading the signal as 1011001001101, the computer reads the signal as 1011000101101, because of the electrical noise on top of the signal.

The problem of NEXT can be addressed by termination technology, strict adherence to standard termination procedures, and the use of quality twisted pair cables.

There is nothing that can be done about thermal noise, other than to give the signals a large enough amplitude so that it doesn't matter.

In order to avoid the problem of AC/reference ground as described above, it is important to work closely with your electrical contractor and power company. This will enable you to get the best and shortest electrical ground. One way to do this is to investigate the cost of installing a single power transformer, dedicated to your LAN installation area. If you can afford this option, you can control the attachment of other devices to your power circuit. Restricting how and where devices, such as motors or high-current electrical heaters, are attached can eliminate much of the electrical noise generated by them.

When working with your electrical contractor, you should ask that separate power distribution panels, known as breaker boxes, be installed for each office area. Since the neutral wires and ground wires from each outlet come together in the breaker box, taking this step will increase your chances of shortening the length of the signal ground. While installing individual power distribution panels for every cluster of computers can increase the up-front cost of the power wiring, it reduces the length of the ground wires, and limits several kinds of signal-burying electrical noise.

There are a number of ways to limit EMI and RFI. One way is to increase the size of the conductors. Another way is to improve the type of insulating material used. However, such changes increase the size and cost of the cable faster than they improve its quality. Therefore, it is more typical for network designers to specify a cable of good quality, and to provide specifications for the maximum recommended cable length between nodes.

Two techniques that cable designers have used successfully, in dealing with EMI and RFI, are *shielding* and *cancellation*. In cable that employs shielding, a metal braid or foil surrounds each wire pair or group of wire pairs. This shielding acts as a barrier to any interfering signals. However, as with increasing the size of the conductors, using braid or foil covering increases the diameter of the cable, and the cost as well. Therefore, cancellation is the more commonly used technique to protect the wire from undesirable interference.

When electrical current flows through a wire, it creates a small, circular magnetic field around the wire. The direction of these magnetic lines of force is determined by the direction in which current flows along the wire. If two wires are part of the same electrical circuit, electrons flow from the negative voltage source to the destination along one wire. Then the electrons flow from the destination to the positive voltage source along the other wire. When two wires in an electrical circuit are placed in close proximity, their magnetic fields will be the exact opposite of each other. Thus, the two magnetic fields cancel each other out. They also cancel out any outside magnetic fields. Twisting the wires can enhance this cancellation effect. By using cancellation in combination with twisting of wires, cable designers can provide an effective method of providing self-shielding for wire pairs within the network media

<http://epics.aps.anl.gov/techpub/lnotes/l232/l232.html>

4: Layer 1 – Electronics and Signals

4.3.8.1. Recognize and describe timing issues: dispersion, jitter, and latency

While *dispersion*, *jitter*, and *latency* are actually three different things that can happen to a bit, they are grouped together because they each effect the timing of the 1 bit. Because you are trying to understand what problems might happen when millions and billions of these bits are travelling on the medium in ONE second, timing matters a lot.

Dispersion is when the pulse broadens in time. It is a function of the material properties and geometry of the medium involved. If serious enough, 1 bit can start to interfere with the next bit and confuse it with the bits before and after it. Since you want to send billions of bits per second, you have to be careful if they are getting too spread out in time.

All digital systems are clocked, meaning clock pulses cause everything to happen. Clock pulses cause a CPU to calculate, data to get written to memory, and bits to get sent out of the NIC card. If the clock on the source host is not synchronized with the destination, which is quite likely, we can get timing jitter. This means bits will be arriving a little earlier and later than expected.

Latency, also known as delay, has two main causes. First, Einstein's theory of relativity states, " nothing can travel faster than the speed of light in vacuum (3.0×10^8 m/s)." Networking signals on wireless travel slightly less then the speed of light (2.9×10^8 m/s), on copper cables they travel 2.3×10^8 m/s), and in optical fiber they travel 2.0×10^8 m/s. So to travel a distance, our bit takes time to get to where it's going. Second, if the bit goes through any devices, the transistors and electronics introduce more latency (delay).

Modern networks work typically work at speeds from 1 Mbps to 155 Mbps and greater. Soon they will work at 1 Gbps or 1 billion bits in one second. This means timing matters a lot. If bits are broadened by dispersion, then ones can be mistaken for zeros and zeros for ones. If our groups of bits get routed differently and we do not account for timing, the jitter can cause errors as the receiving computer tries to reassemble packets into a message. If groups of bits are "late", the networking devices and other computers we are trying to communicate with might get hopelessly lost and overwhelmed by our billion bits per second.

Dispersion can be fixed by proper cable design, limiting cable lengths, and finding the proper impedance. In optical fibers, dispersion can be controlled by using laser light of a very specific wavelength. For wireless communications, dispersion can be minimized by the frequencies we use to transmit.

Jitter can be fixed by a series of complicated clock synchronizations, including hardware and software, or protocol, synchronizations.

Latency can be improved by careful use of internetworking devices, different encoding strategies, and various layer protocols.

4: Layer 1 – Electronics and Signals

4.3.9.1. Recognize and define collision

A collision occurs when two bits from two different communicating computers are on a shared-medium at the same time. In the case of copper media, the voltages of the two binary digits add, and cause a third voltage level. This is not allowed in a binary system, which only understands two voltage levels. The bits are "destroyed".

Some technologies, such as Ethernet, deal with a certain level of collisions to handle whose turn it is to transmit on the shared media when communicating between hosts. In some instances collisions are a natural part of the functioning of a network. However, excessive collisions can slow the network down or bring it to a halt. Therefore, a lot of network design goes into minimizing and localizing collisions.

There are many ways to deal with collisions. You can use them to your advantage and simply have some set of rules for dealing with them when they occur, as in Ethernet. You can require that only one computer on a shared media environment is allowed to transmit at any one time and requires a special bit pattern called a token to transmit, as in token –ring and FDDI.

To view a java applet depicting collisions on Ethernet Media, go to

<http://bugs.wpi.edu:8080/EE535/>

4: Layer 1 – Electronics and Signals

4.3.10.1. Understand the relationship of one bit to a message

Once a bit is placed on medium, it propagates, and may experience attenuation, reflection, noise, dispersion, or collision. You want to transmit far more than one bit. In fact, you want to transmit billions of bits in one second. All of the effects, so far described, that can occur to one bit, apply to the various protocol data units (PDUs) of the OSI model. Eight bits equal a byte. Multiple bytes equal 1 frame. Frames contain packets. Packets carry the message you wish to communicate. Networking professionals often talk about attenuated, reflected, noisy, dispersed, and collided frames and packets

4: Layer 1 – Electronics and Signals

4.4.1.1. Explain that, throughout history, messages (data) have been encoded for long distance communications.

Whenever you want send a message over a long distance, there are two problems you must solve: how to express the message, called encoding or modulation, and what method to use to transport it, called the carrier. Encoding means converting the binary data into a form that can travel on a physical communications link; modulation means using the binary data to manipulate a wave.

Throughout history there have been a variety of ways in which the problem of long distance communication has been solved: runners, riders, horses, optical telescopes, carrier pigeons, and smoke signals. In each case there was a form of encoding involved, such as an agreed upon language used by runners, or the definition of two puffs of smoke, and there were carriers, such as light signals reflected on messengers, carrier pigeons, or light reflected on smoke.

In more modern times, the creation of Morse code revolutionized communications. Two symbols, the dot and the dash, were used to encode the alphabet. For instance, **• • • • • • • • • •** means SOS, the universal distress signal. Modern telephones, FAX, AM, FM, short wave radio, and TV all encode their signals electronically, typically using the modulation of different waves from different parts of the electromagnetic spectrum.

Computers use three particular technologies, all of which have their counterparts in history. These technologies are: encoding messages as voltages on various forms of copper wire; encoding messages as pulses of guided light on optical fibers; and encoding messages as modulated, radiated electromagnetic waves.

4: Layer 1 – Electronics and Signals

4.4.2.1. Describe modulation and encoding.

Encoding means converting 1s and 0s into something real and physical, like:

- an electrical pulse on a wire
- a light pulse on an optical fiber
- a pulse of electromagnetic waves into space.

Two methods of accomplishing this are NRZ encoding and Manchester encoding.

NRZ, non–return to 0, encoding is the simplest. It is characterized by a high signal and a low signal, often +5 or + 3.3 Volts for binary 1 and 0 Volts for binary 0. In optical fibers, binary 1 might be bright LED or laser light and binary zero dark, or no light. In wireless networks, binary 1 might be carrier wave present and binary 0 as no carrier at all.

Manchester encoding is more complex, but is more immune to noise and better at remaining synchronized. In Manchester encoding, the voltage on copper wire, the brightness of LED or laser light in the optical fiber, or the power of the EM wave in wireless has the bits encoded as transitions. Specifically in Manchester encoding, upward transitions in the signal mean binary 1 and downward transitions mean binary 0.

Other common, but more complicated, encodings are non–return to 0 inverted (NRZI), differential Manchester encoding (related to regular Manchester encoding), and 4B/5B which uses special groups of 4 and 5 bits to represent 1s and 0s. All encoding schemes have advantages and disadvantages.

Closely related to encoding is modulation, which specifically means taking a wave and changing, or modulating, it so it carries information. To give an idea of what modulation is, we examine three forms of modifying, modulating, a "carrier" wave to encode bits: *AM*, *FM*, and *PM*. Other more complex forms of modulation also exist. The diagram shows three ways our binary data can be encoded onto a carrier wave by the process of modulation.

In AM, amplitude modulation, the modulation, or height, of a carrier sine wave is varied to carry the message.

In FM, frequency modulation, the frequency, or wiggly–ness, of the carrier wave is varied to carry the message.

In PM, phase modulation, the phase, or beginning and ending points of a given cycle, of the wave is varied to carry the message.

Binary 1 and 1 can be communicated on a wave by either AM (Wave ON/Wave OFF), FM (Wave wiggles lots for 1s, a little for 0s), or PM (one type of phase change for 0s, another for 1s).

4: Layer 1 – Electronics and Signals

4.4.3.1. Explain how messages can be encoded as voltages on copper.

At one time, messages were encoded as voltages on copper.

On copper–based networks today, Manchester and NRZI encodings are popular.

4: Layer 1 – Electronics and Signals

4.4.4.1. Explain how messages can be encoded as guided light.

At one time, messages were encoded as smoke signals.

On fiber based networks, Manchester and 4B/5B encodings are popular.

http://www.rad.com/networks/1994/digi_enc/main.htm

4: Layer 1 – Electronics and Signals

4.4.5.1. Explain how messages can be encoded as radiated EM waves.

Messages have been encoded as modulated radio waves since the time of Marconi.

On wireless networks, a wide variety of encoding schemes (variations on AM, FM, and PM) are used.