**Supplementary Reading for The OSI Networking Model**

**In addition to the five layer model we are working with, it’s important to note that other models exist. The traditional TCP/IP Model only has four layers, as it doesn’t differentiate between the physical layer and the data link layer, but is otherwise very similar to the one we’ll be working with. The most well known other model is the OSI model. It’s the model taught by many other networking certificate programs, like Net+ and Cisco’s many networking certifications. The primary difference between our five layer model and the seven layer OSI model is that the OSI model abstracts the application layer into three layers total.**

**You can learn more about the OSI Networking Model by checking out these links:**

* [**https://www.sans.org/reading-room/whitepapers/standards/osi-model-overview-543**](https://www.sans.org/reading-room/whitepapers/standards/osi-model-overview-543)
* [**https://en.wikipedia.org/wiki/OSI\_model**](https://en.wikipedia.org/wiki/OSI_model)

**TCP/IP NETWORK MODEL**

To really understand networking, we need to understand all of the components involved. We're talking about everything from the cables that connect devices to each other to the protocols that these devices use to communicate. There are a bunch of models that help explain how network devices communicate but in this course we'll focus on a five layer model. By the end of this lesson, you'll be able to identify and describe each layer and what purpose it serves. Let's start at the bottom of our stack where we have what's known as the physical layer. The physical layer is a lot like what it sounds. It represents the physical devices that interconnect computers. This includes the specifications for the networking cables and the connectors that join devices together along with specifications describing how signals are sent over these connections. The second layer in our model is known as the data link layer. Some sources will call this layer the network interface or the network access layer. At this layer we introduce our first protocols. While the physical layer is all about cabling, connectors, and sending signals, the data link layer is responsible for defining a common way of interpreting these signals so network devices can communicate. Lots of protocols exist at the data link layer but the most common is known as ethernet. Although wireless technologies are becoming more and more popular. Beyond specifying physical layer attributes, the ethernet standards also define a protocol responsible for getting data to nodes on the same network or link. The third layer, the network layer, is also sometimes called the internet layer. It's this layer that allows different networks to communicate with each other through devices known as routers. A collection of networks connected together through routers is an inter network, the most famous of these being the internet. Hopefully you've heard of it. While the data link layer is responsible for getting data across a single link, the network layer is responsible for getting data delivered across a collection of networks. Think of one of the device on your home network connects with a server on the internet. It's the network layer that helps get the data between these two locations. The most common protocol used at this layer is known as IP or internet protocol. IP is the heart of the internet and most small networks around the world. Network software is usually divided into client and server categories with the client application initiating a request for data and the server software answering the request across the network. A single node may be running multiple client or server applications. So you might run an email program and a web browser. Both client applications on your PC at the same time and your email and web server might both run on the same server. Even so, emails end up in your email application and web pages end up in your web browser. That's because our next layer, the transport layer. While the network layer delivers data between two individual nodes, the transport layer sorts out which client and server programs are supposed to get that data. When you heard about our network layer protocol IP, you may have thought of TCPIP, which is a pretty common phrase. That's because the protocol most commonly used in the fourth layer, the transport layer, is known as TCP or transmission control protocol. While often said together as the phrase TCPIP, to fully understand and troubleshoot networking issues, it's important to know that they're entirely different protocols serving different purposes. Other transport protocols also use IP to get around including a protocol known as UDP or user data gram protocol. The big difference between the two is that TCP provides mechanisms to ensure that data is reliably delivered while UDP does not. Spoiler alert will cover differences between the TCP and UDP transport protocols in more detail later. For now, it's important to know that the network layer, in our case IP is responsible for getting data from one node to another. Also remember that the transport layer, mostly TCP and UDP is responsible for ensuring that data gets to the right applications running on those nodes. Last but not least, the fifth layer is known as the application layer. There are lots of different protocols at this layer and as you might have guessed from the name, they're application specific. Protocols used to allow you to browse the web or send and receive email are some common ones. The protocols that play in the application layer will be most familiar to you since there are ones you probably interacted with directly before even if you didn't realize it. You can think of layers like different aspects of a package being delivered. The physical layer is the delivery truck and the roads. The data link layer is how the delivery trucks get from one intersection to the next over and over. The network layer identifies which roads need to be taken to get from address A to address B. The transport layer ensures that delivery driver knows how to knock on your door to tell you your package has arrived. And the application layer is the contents of the package itself.

**CABLES**

Lots of different cables and network devices can be used to allow computers to properly communicate with each other. By the end of this lesson, you'll be able to identify and describe various networking cables and networking devices. Computer networking is a huge part of the day to day role of many IT specialists. And knowing how to differentiate different network devices will be essential to your success. Let's start with the most basic component of a wired network, cables. Cables are what connect different devices to each other, allowing data to be transmitted over them. Most network cables used today can be split into two categories, copper and fiber. Copper cables are the most common form of networking cable. They're made up of multiple pairs of copper wires inside plastic insulator. You may already know that computers communicate in binary, which people represent with ones and zeros. The sending device communicates binary data across these copper wires by changing the voltage between two ranges. The system at the receiving end is able to interpret these voltage changes as binary ones and zeros which can then be translated into different forms of data. The most common forms of copper twisted pair cables used in networking are Cat5, Cat5e and Cat6 cables. These are all shorthand ways of saying category five or category six cables. These categories have different physical characteristics like the number of twists in the pair of copper wires that result in different usable lengths and transfer rates. Cat5 is older and has been mostly replaced by Cat5e and Cat6 cables. From the outside, they all look about the same and even internally they're very similar to the naked eye. The important thing to know is that, differences in how the twisted pairs are arranged inside these cables can drastically alter how quickly data can be sent across them. And how resistant these signals are to outside interference. Cat5e cables have mostly replaced those older Cat5 cables because their internals reduce Crosstalk. Crosstalk is when an electrical pulse on one wire is accidentally detected on another wire, so the receiving end isn't able to understand the data causing a network error. Higher level protocols have methods for detecting missing data and asking for the data a second time. But, of course, this takes up more time. The higher quality specifications of a Cat5e cable make it less likely that data needs to be re transmitted. That means on average you can expect more data to be transferred in the same amount of time. Cat6 cables follow an even more strict specification to avoid Crosstalk making those cables more expensive. Cat6 cables can transfer data faster and more reliably than Cat5e cables can, but because of their internal arrangement, they have a shorter maximum distance when used at higher speeds. The second primary form of networking cable is known as fiber, short for fiber optic cables. Fiber cables contain individual optical fibers which are tiny tubes made out of glass about the width of a human hair. These tubes of glass can transport beams of light. Unlike copper, which uses electrical voltages, fiber cables use pulses of light to represent the ones and zeros of the underlying data. Fiber is even sometimes used specifically in environments where there's a lot of electromagnetic interference from outside sources. Because this can impact data being sent across copper wires. Fiber cables can generally transport data quicker than copper cables can, but they're much more expensive and fragile. Fiber can also transport data over much longer distances than copper can without suffering potential data loss. Now you know a lot more about the pros and cons of fiber cables. But keep in mind, you'll be way more likely to run into fiber cables in computer data centers than you would in an office or at home.

**Hubs and Switches**

Notes

[Discuss](https://www.coursera.org/learn/computer-networking/discussions/weeks/1)

We're going to do a rundown of network devices in this video and the next one. Almost every IT specialist will have to interact with these sorts of devices on a regular basis. Cables allow you to form point to point networking connections. These are networks where only a single device at each end of the link exists. Not to knock point to point networking connections but they're not super useful in a world with billions of computers. Luckily there are network devices that allow for many computers to communicate with each other. The most simple of these devices is a hub. A hub is a physical layer device that allows for connections from many computers at once. All the devices connected to a hub will end up talking to all other devices at the same time. It's up to each system connected to the hub to determine if the incoming data was meant for them or to ignore it if it isn't. This causes a lot of noise on the network and creates what's called a collision domain. A collision domain is a network segment where only one device can communicate at a time. If multiple systems try sending data at the same time, the electrical pulses sent across the cable can interfere with each other. This causes these systems to have to wait for a quiet period before they try sending their data again. It really slows down network communications and is the primary reason hubs are fairly rare. They're mostly a historical artifact today. A much more common way of connecting many computers is with a more sophisticated device known as a network switch, originally known as a switching hub. A switch is very similar to a hub, since you can connect many devices to it so they can communicate. The difference is that while a hub is a layer one or physical layer device, a switch is a layer two or data link device. This means that a switch can actually inspect the contents of the ethernet protocol data being sent around the network, determine which system the data is intended for and then only send that data to that one system. This reduces or even completely eliminates the size of collision domains on a network. If you guess that this will lead to fewer retransmissions and a higher overall throughput, you're right.

# Routers

Notes

[Discuss](https://www.coursera.org/learn/computer-networking/discussions/weeks/1)

Hubs and switches are the primary devices used to connect computers on a single network, usually referred to as a LAN or a Local Area Network. But we often want to send or receive data to computers on other networks. This is where routers come into play. A router, is a device that knows how to forward data between independent networks. While a hub is a layer one device and a switch is a layer two device. A router operates at layer three, a network layer. Just like a switch can inspect Ethernet data to determine where to send things, a router can inspect IP data to determine where to send things. Routers store internal tables containing information about how to route traffic between lots of different networks all over the world. The most common type of router you'll see is one for a home network or a small office. These devices generally don't have very detailed routing tables. The purpose of these routers is mainly just to take traffic originating from inside the home or office land and to forward it along to the ISP or Internet Service Provider. Once traffic is at the ISP a way more sophisticated type of router takes over. These core routers form the backbone of the internet and are directly responsible for how we send and receive data all over the internet every single day. Core ISP routers don't just handle a lot more traffic than a home or small office router. They also have to deal with much more complexity in making decisions about where to send traffic. A core router usually has many different connections to many other routers. Routers share data with each other via a protocol known as BGP or Border Gateway Protocol. That lets them learn about the most optimal paths to forward traffic. When you open a web browser and load it web page, the traffic between computers and the web servers could have traveled over dozens of different routers. The Internet is incredibly large and complicated, and routers are global guides for getting traffic to the right places.

**Servers and Clients**

Notes

[Discuss](https://www.coursera.org/learn/computer-networking/discussions/weeks/1)

All of the network devices you've just learned about exists so that computers can communicate with each other, whether they're in the same room or thousands of miles apart. We've been calling these devices nodes, and we'll keep doing that. But it's also important to understand the concepts of servers and clients. The simplest way to think of a server is as something that provides data to something requesting that data. The thing receiving the data is referred to as a client. Well, often talk about nodes being servers or clients. The reason our definition uses a word as vague as something is because it's not just nodes that can be servers or clients. Individual computer programs running on the same node can be servers and clients to each other too. It's also important to call out that most devices aren't purely a server or a client. Almost all nodes are both at some point in time, quite the multitasking overachievers. That all being said in most network topographies, each node is primarily either a server or a client. Sometimes we refer to an email server as an email server, even though it's itself a client of a DNS server. Why? Because its primary reason for existing is to serve data to clients. Likewise, if a desktop machine occasionally acts as a server in the sense that it provides data to another computer, its primary reason for existing is to fetch data from servers so that the user at the computer can do their work. To sum up, a server is anything that can provide data to a client, but we also use the words to refer to the primary purpose of various nodes on our network.

PREAMBLE 64 BIT 8 BYTE START FRAME DELIMITER

VLAN 4 BYTE

ETHER TYPE FIELD 16 BIT describe protocols of the frame

46-1500 BYTES

FRAME CHECK SEQ 4 BYTE

0 0 0 0 0 0 0 0 00000000 00000000 00000000

0 0 0 0 1 0 0 1

Interior gateway protocols

Link state routing protocols

Distance-vector protocols

0 1 1 0 0000