NETWORK ACE

BOOK 1

The Basics of Computer Networks And How They Are Put Together

Clint Garrett

Introduction

“COMPUTER NETWORKING IS DIFFICULT!!"
“THERE’S TOO MUCH TO LEARN!”
“THE LEARNING CURVE IS TOO STEEP!”

That's what I used to think!

That's what a **lot** of people think when they're first starting out.

I GET IT...

We don't need to get into all the details of why it's a difficult topic. We don't need to explain ourselves to the world in why we FEEL that way!

Here's why I say that...

I've found there are 3 Categories of people around the topic of Computer Networking:

1.) Those that don't know anything about it and don't WANT to know
This is a majority of the world, your friends and family, the people in the town or city where you grew up.

They couldn't care less about computer networking...and they will look at you like you're crazy for wanting to get *into* the field.

Without trying, they'll make it seem more difficult to learn with comments like,"I don't know how you can UNDERSTAND all of that stuff!" "I would NEVER be able to do that!" etc. and etc.

Take my personal advice and recommendation: Take all of their comments with a grain of salt (and look at their comments as COMPLIMENTS to your OWN intelligence and resourcefulness for you WANTING to know about it, not as them painting the field of computer networking or I/T as being "difficult" or "hard to learn").

2.) Those like you (and like me when I started out) that WANT to know it, learn it, understand it and succeed in it

People like you, those new to the I/T industry, or more specifically those new to computer networking, find themselves in a state of confusion around the jargon, the tech, the software, the hardware, the acronyms.

It all feels like we're caught up on "The House That Jack Built" or a similar scenario. We WANT to learn it all and understand it all...but getting those that ALREADY understand it to take the TIME to explain it to us in a way that clarifies the topic and helps us see how everything works together - especially if we've not yet had the chance to work WITH the technology or have any hands-on experience ourselves - is the real "Secret" we're looking for.

Am I right?

3.) The Experts ALREADY in the field
The people I'm referring to here are the CURRENT network admins, engineers, technicians. They already know all the tech, the software, the hardware.

They just don't HAVE the time or want to TAKE the time to explain it to a "newbie"

Don't hold it against them. In most cases they are working 60-80 hour weeks for one or more companies or businesses and when they are off the clock, they're exhausted.

Why?

Because there *aren't enough people in the field* right now to keep up with the demand.
Note: Remember this point

Some retire after 10-15 years of it and take their investments from their high incomes and salaries (and their expertise, by the way) and don't want to be "bothered" to teach the new people what they know to help the "new blood" advance in the networking field.

There are very few people that fall outside these 3 categories.

So, putting that on the table and recognizing it for what it is, there are some of us - like me - that seriously WANT to help those new to the industry to not only get started quickly, but to help them see it from the 30,000 foot view when they're first starting out.

When I first started out, I felt alone. I felt alone in what I DIDN'T know and I was afraid to ADMIT what I didn't understand about networking.

Feeling isolated in my journey to get into the networking field, I struggled...a LOT!

As I worked with others over the years and got about 7-10 years into the field myself, I realized I *wasn't* alone...**EVERYONE** feels this way when they're first starting out.

If this is how you feel right now, **you're in the right place!**

I have helped hundreds of students and "newbies" get a firm grasp of computer networking from the basics to the advanced. And I've personally discovered that the difficulty with the field and topic of networking is not in the material or the tech itself, but rather in the WAY it's explained and taught in the beginning.

I've been able to help those students (and "newbies") get an expert understanding of it all within **1 to 3 months** easy, which helped them seriously hit the ground running!

That's what I want to do for YOU! STARTing with this Book!

So if you fall into Category 2 above (which I'm guessing you do or you wouldn't be reading this book)... WELCOME!

In this short book, I'm going to show you "The 30,000 Foot View" of Computer Networking. We're primarily going to be covering the physical components of a computer network and how a network is actually put together.

You're going to see it for what it is from a higher view point, then you're going to know how to EASILY get to the next step and how to dive deeper into specific aspects of computer networking that will help you start out at high speed and not stop until you're the "Expert of All Experts"!

In the *next* book, we get into the Software and the logical and configuration aspects of computer networking in more detail, so that you can learn how to not only design and build a network for its functionality, but you can configure switches, routers, firewalls, and yes the end devices like computers, laptops, servers and printers to work ON that computer network.

So without wasting any more time,
Let's Get Started...

CH. 1 - What Is a Network?

Two years into my being a Senior Enterprise-Level Network Engineer, I remember getting into a casual conversation with someone at a family get-together (in Category 1 we talked about in the Intro), and after telling them my official career title, they looked at me with a blank look on their face and asked,"So you work with computer networks? Networks where computers all connect together? Wow! What do you DO exactly with that?"

Now, I'm not trying to demean them or come down on them too hard, as they were for the most part just trying to create good conversation.

But that question always seems to ring a bell with those of us working in the field.

It leads to the question: **What is a Network?**

Most of your expensive study textbooks and material and study guides, etc. will always start out with that.

So in this 1st chapter, answering that is *exactly* how we're going to start.

What is a Network?
Quite simply: A Network is a system of computers and other devices that are connected together via cabling or wirelessly for the purpose of sharing resources, data, and applications.

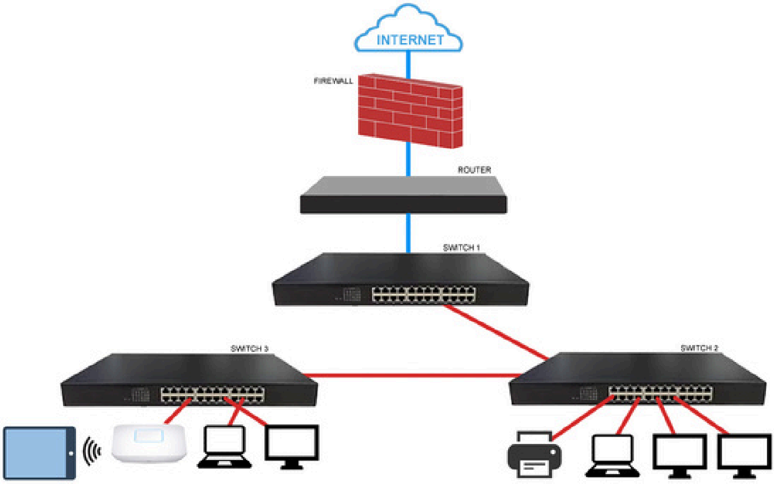
Now that we've dealt with that elephant in the room...

How do networks work?
How do we build them?
How do we maintain them?
What software do we use?
How do we troubleshoot them when something goes wrong or stops working?
What are Protocols and how to THEY work?

All good questions!

We can answer those by starting out up here at the “30,000 foot view” with the definition of a computer network...
and then slowly looking closer at what actually *makes up* a computer network and makes it work correctly.

This is the Network Diagram we’re going to use:

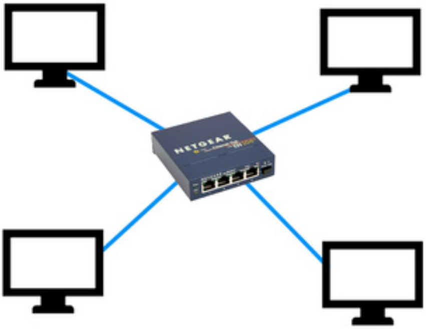


2 TYPES OF NETWORKS

Looking at computer networks from "up here" we first learn that there are 2 "types" of networks, Peer-to-Peer and Client-Server:

Peer-to-Peer

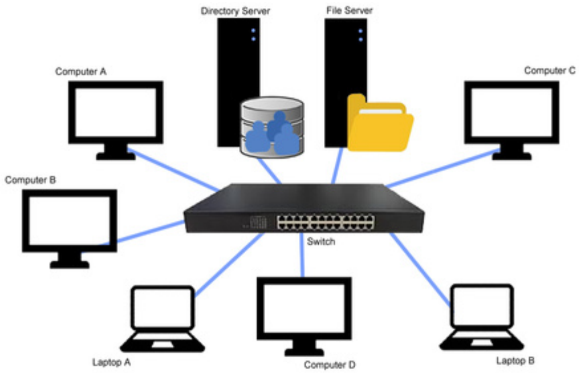
This is where there is no centralized management or security and the 2 or more computers in a peer-to-peer network are each in charge of their own local users and folder and file permissions. No servers and no centralized management.



Peer-to-Peer Network

Client-Server

These make up the **majority** of computer networks you encounter in the world today and are typically connected using a Switch like you see on this diagram.



Client-Server Network

In a Client-Server network, you have centralized management of users, files and folders, as well as permissions. All of that is done via the server (or servers, if you have more than one) and it's done using a Network Operating System (NOS) like MS Windows Server or Linux. Typically, you'll have a network-connecting Operating System like Windows 10 or later version or Linux running on the clients and devices connecting TO the Client-Server network.

WHY DO WE NEED TO KNOW THIS?

If you are starting out by designing, or building a new computer network (for you, a group, a business, an organization), you'll need to determine which of those 2 types you're going to use.

If you're changing, growing or adding to, or troubleshooting an existing computer network, you need to know which of those 2 types that existing network falls into.

Each has benefits and drawbacks, so understand those from the outset, and you won't need to get entrenched in the details...again, when you’re just starting out.

Each of those 2 types has different costs associated with them. Each is either more difficult to implement and maintain or easier to implement and maintain.

To make it easy, if you have a setup whereby you have a large number of resources (files, folders, printers, information, etc.) you need users on the network to be able to access and you want to centralize management of those users, computers, files and folders, you will want to go with the Client-Server model.

If you only have a few devices/computers and users and not that many resources to be used on a network and you don't need centralized management, you can go with the Peer-to-Peer model.

CH. 2 - Network “End” Devices

What are the actual COMPONENTS that need a computer network as well as make up a portion **of** the network?

So in the 1st chapter we looked at the 2 "types" of computer networks as far as their operation and logic are concerned.

Here in this section, we're going to take a look at the actual components that make up a computer network.

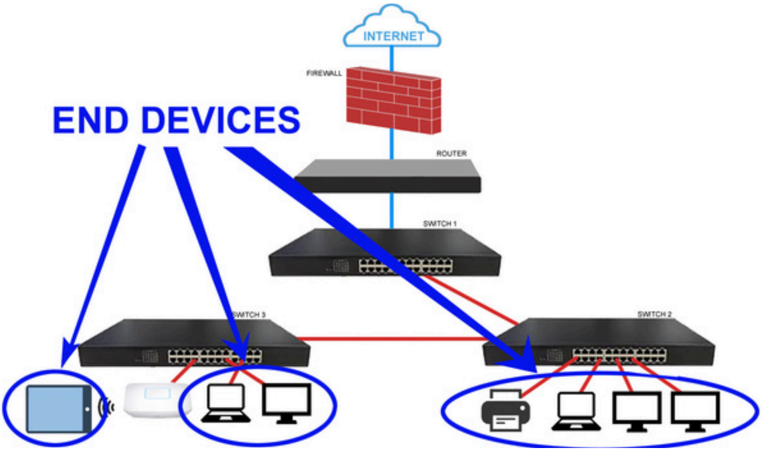
Again, we're not deep diving down into all the confusing details about networking.

We're continuing to keep it **simple**.

You'll find many or few (or sometimes not any at all) of these devices on a computer network:

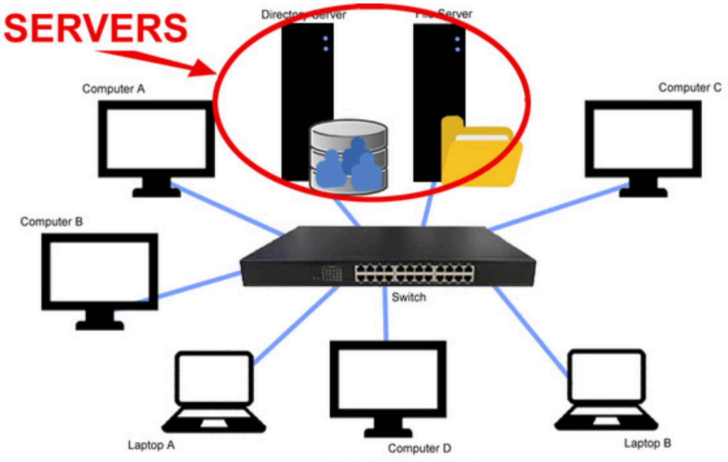
Computers

These can be desktop PCs, laptops, tablets, smartphones - Any of the what we refer to as "end devices" that actually need to connect to the network and USE the network



Servers

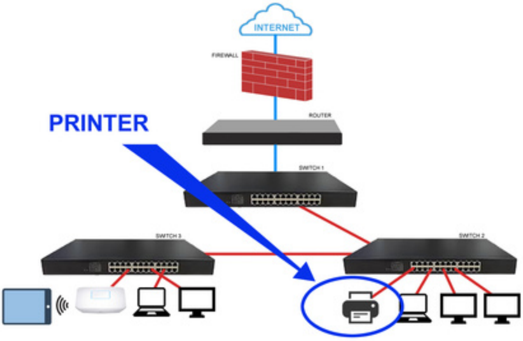
These are computers that house files, folders, applications. Servers may also be responsible for providing permissions to users or other devices on a network. Servers may run a printer or some type of multi-user software. Servers are what other end devices connect to for access to resources on a computer network



Client-Server Network

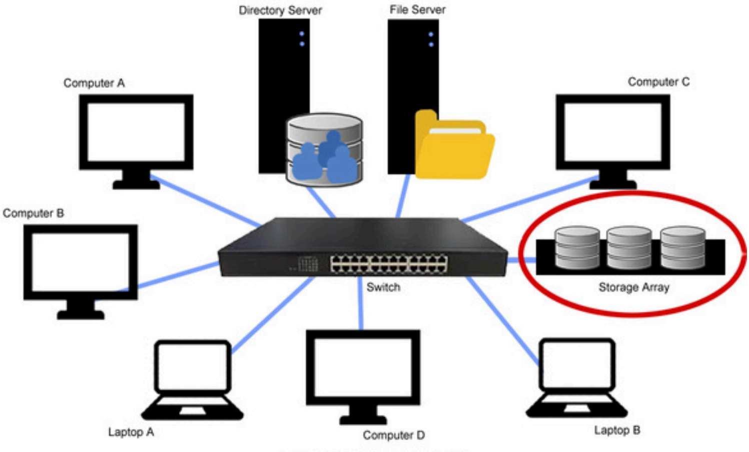
Printers

Small to professional printers and copiers can now be connected on a computer network for use by other users on that network from their end device(s). If someone wants to print a document in the office using the network printer, they can do so from the convenience of their desktop, laptop or smartphone



Storage Arrays

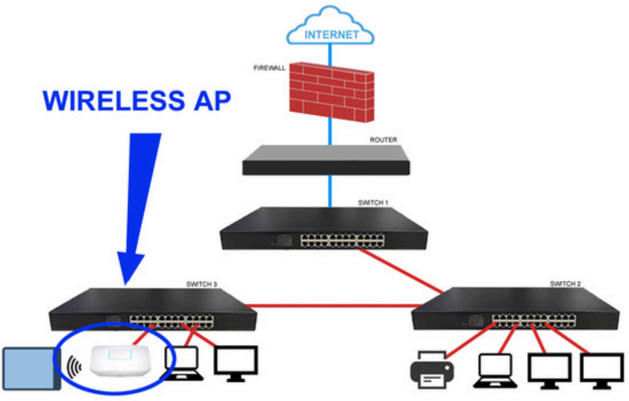
Similar to Servers, Storage Arrays provide access to large volumes of files and folders, but they're more like a data warehouse on a computer network. They provide multiple hard drives for storage and shared access to users on the network



Client-Server Network

Wireless Access Points (APs)

If you want multiple end devices to connect to an existing network wirelessly, you will need something that receives and transmits signals for connectivity to those devices. We’re going to get more into detail on Wireless APs in the section on components.



Again, typically those are the most *common* devices and components you'll see making up an actual *physical* computer network.

You can deep dive down into each one, but a little later in this book I'm going to show you the "Secret" shortcut to learning computer networking faster and easier using a Simple Method that will not fail you, so be watching for that!

So now that you know the “end” devices that are used on a computer network, the actual devices that need to connect to a network to communicate with each other and share resources, files and data with each other, what are the **primary** components that are use to actually connect these end devices together?

In the next chapter, we’re going to get into the components, so keep reading...

CH. 3 - Network Components

You will often find the big textbooks going into great detail about all of the hardware, how everything works and what it is used for and why.

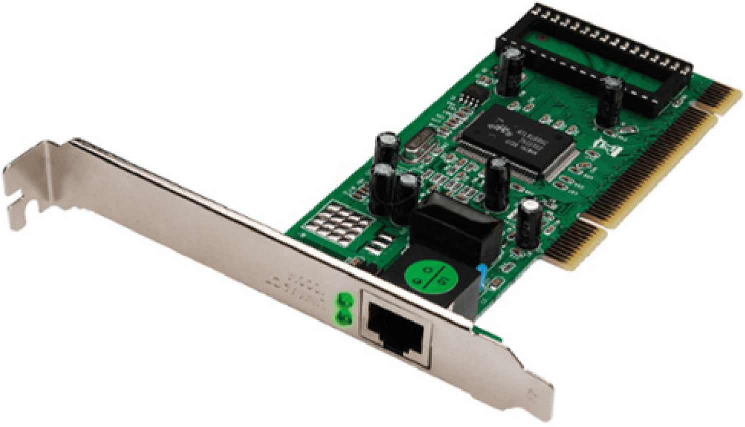
I'm not going to do that here in this book for several reasons. We can (you can) deep dive into each of these components in more detail later and if you get in my ‘Switch Ace’ course.

But when you're just starting out you only need the basics, so here they are...

NETWORK ADAPTER

It's one of the most basic, cheapest and abundant (thanks to mass manufacturing) items in computer networking, but it is necessary to allow a computer/device to actually CONNECT to a network.

You may see it referred to as a NIC (network Interface Card), but the network adapter is the life blood of a network.



Network Interface Card (NIC)

You can have more than one NIC on a single computer/device and/or you can have more than one physical connection port on a single NIC.

Some of the more common ports you'll see in network adapters are RJ45 (for twisted pair Ethernet cables), SFP, SC, LC, and GBIC (for fiber optic cables).

Keep in mind that with the network adapter, most of what is done on the 7 layers of the OSI Model (which we’ll get to in Book 2) are done on the processor of the network adapter (NIC).

HUB

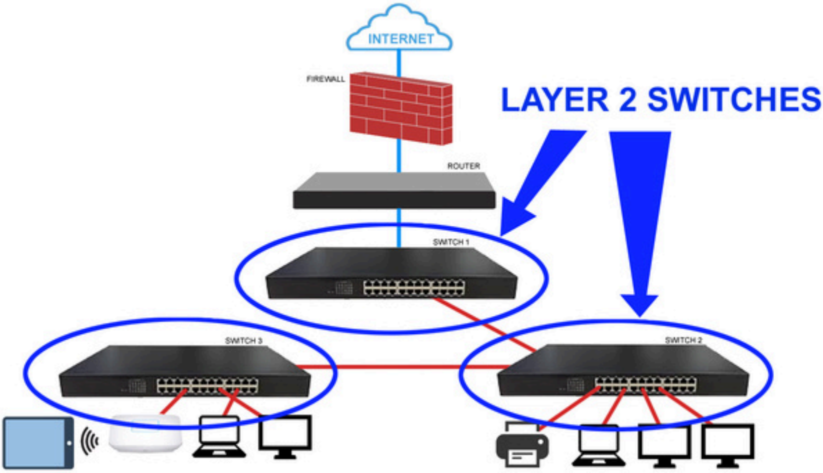
These are seldom if ever used anymore and have been replaced by Layer 2 Switches, but Hubs were originally used to connect multiple devices together to make a star topology. Hubs were essentially multiport repeaters.

SWITCH

The Layer 2 Switch is one of the most important devices on a computer network and within a LAN. A Layer 2 Switch filters traffic based on MAC addresses of the devices that send traffic to it and through it.

I like to begin with the Switch when teaching those new to networking, because once you **know** the Layer 2 Switch inside and out, you are well on your way to being a network expert.

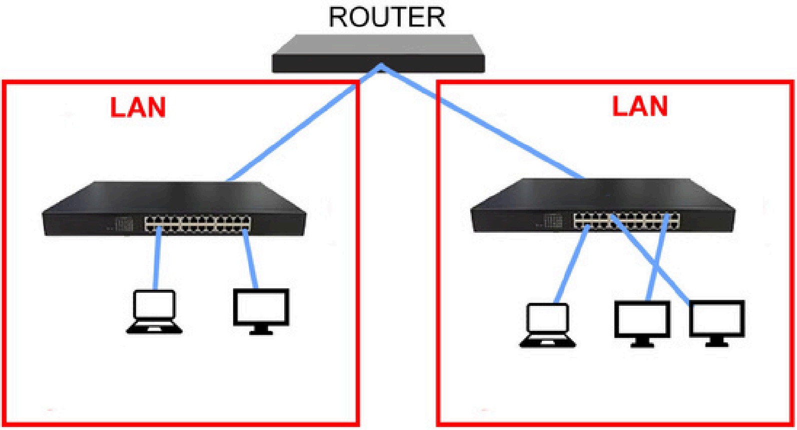
(More on this as we go along, as this is getting into the "Secret" I'm referring to later on).



ROUTER

If you need to route or pass traffic between 2 or more different LANs, you will need a device that filters at Layer 3 using IP addresses found in the header of a packet (inside a frame).

In most cases, this is the Router. Routers connect multiple Layer 2 LANs (Local Area Networks) together.

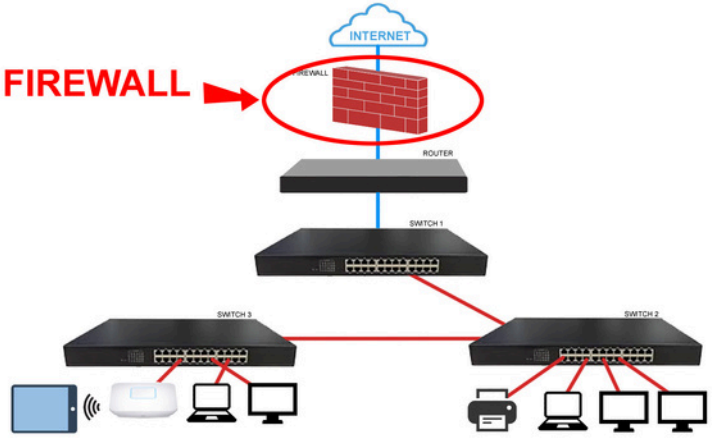


FIREWALL

Firewalls are set up to protect a network both from outside AND inside. They can be either hardware or software.

Hardware firewalls are the bigger network firewalls that do the following:

- Monitor inbound and outbound traffic
- Allow or deny traffic based on rules that were configured by an admin or tech
- Provide protection against threats
- Allow or deny traffic from other connected subnets (sub-networks)
- Provide VPN (Virtual Private Network) access to remote users outside the network
- Control user access to services like web and FTP
- Filter web content



(HARDWARE) FIREWALL

OVERVIEW

I'm going to get to the "Secret" Method shortly that I told you about in the beginning of this book, but we're going to talk about the other aspect of the physical components on a network, the “thing” that connects it all together…

Cables…

CH. 4 - Cables

If we're going to actually connect all of our hardware components together with computers and end devices to MAKE a network, we need to look at the most commonly used and reliable methods: Cables and Wireless

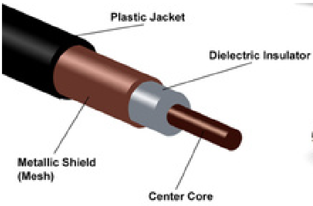
Now we can't just connect everything with cables and call it a network. We have to first learn the different aspects to the different types of cables, how they connect to different devices and how fast or slow they are, as well as how reliable those specific connections are.

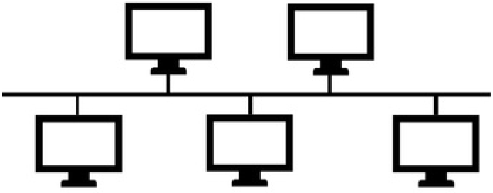
2 TYPES OF CABLES

There are essentially 2 types of cables we can connect networks together with to convey packets and data from one computer to another - Copper cabling and Fiber-Optic cabling

COPPER CABLE

When networks were first built, they were connected together with coaxial cable. Yes, this is the same or similar cable as what you see coming from your wall if you still buy cable streaming from a cable provider or ISP (Internet Service Provider).





Bus Topology Network
Using Coaxial Cable

They would connect multiple computers together on a single cable - which was known as a Bus Topology.

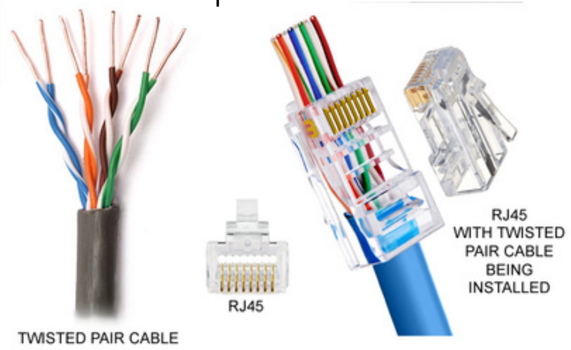
Coaxial cable was made with a thick copper core in the middle of the cable, surrounded by sheathing to protect that copper core from electrical interference and physical damage from things hitting the cable or crimping it (like chair legs, tools, desks, people walking on it, etc.).

So coaxial cable is one type of copper cable used in computer networks. You seldom see coaxial cable used anymore between devices on a network except maybe running from the Internet Service Provider box outside your house into the router/modem inside the house.

Twisted Pair

Twisted Pair Cables are the Ethernet cable with 4 pairs of copper wires each twisted around each other that started being used with RJ45 connectors on the ends for use with connecting devices with Hubs, Switches and Routers.

Twisted Pair Cables are still the predominantly used copper cable in today's networks. These are now found in different ratings and sizes from Category 3 up to Category 7 (most recently). Each category and rating offering different bandwidth and speed.



16 RJ45 PHYSICAL PORTS
ON THE FRONT OF A LAYER 2 SWITCH

SPEEDS AND CATEGORIES OF TWISTED PAIR

Keep in mind that the color of the sheathing on the ourside of a cable doesn’t necessarily indicate anything.

You may have someone managing a data center that wants nothing but blue sheathed wires to be used for aesthetic reasons.

You’ll also see different manufacturers that use color coding to indicate the different types and categories. Also keep in mind that most Ethernet twisted pair cabling will have type printed markings on the outside of the cable sheathing (about every 1-2 feet) indicating the Category of cabling within (Ex., Cat5, Cat6, Cat7, etc.).

Here is a quick summary of the Ethernet cable standards and their maximum speed capacity:

- **Category 3** - 10Mbps and 16MHz frequency
- **Category 4** - 16Mbps and 20MHz frequency
- **Category 5** - 100Mbps and 100MHz frequency
- **Category 5e** - 1Gbps and 100MHz frequency
- **Category 6** - 1Gbps and 250MHz frequency
- **Category 6a** - 10Gbps and 500MHz frequency
- **Category 7** - 100Gbps and 600MHz frequency

Obsiously, you will want to match up the type and category of cable you use with the correct physical port capability for the components and end devices you are connecting on a network.

If you attempt to use a Category 3 cable on a 1Gbps port, the device(s) will have to either throttle the speed down to match the cable you’re using, or the connection just simply will not work.

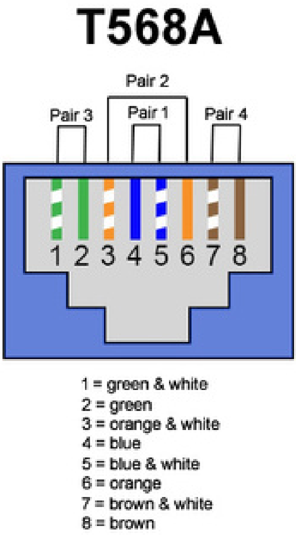
So does it matter HOW the wires inside the cable are arranged?

Yes it does! Keep reading...

There are 2 wiring layouts (sometimes called "schemes") for the ends of the Ethernet twisted pair cable that are still widely used across the industry:

T568A

The T568A is by far the less-used wiring layout on the end of an Ethernet Twisted Pair cable for use inside the RJ45 connector, but it nevertheless does have a purpose (which we're about to go over shortly)

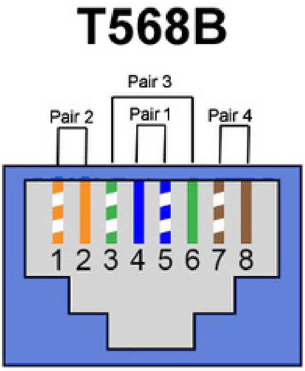


When you look at the T568A and compare it to the T568B (which we're about to take a look at), you'll see that the only difference between them is that the orange pair and the green pair trade places.

There is a reason you'll need to know these 2 wiring schemes for the RJ45 connectors on the ends of the cables, but before we get to that, let's take a look at the most commonly used wiring scheme, the T568B...

T568B

The T568B wiring scheme for an RJ45 connector on the Twisted Pair Ethernet cable is exactly like the T568A, but with a slight difference - The orange pair and the green pair are reversed (or trade places) from the T568A.



1 = orange & white
2 = orange
3 = green & white
4 = blue
5 = blue & white
6 = green
7 = brown & white
8 = brown

Here's what they WON'T tell you about these 2 wiring schemes/layouts...

You can use either/or on your network. But you don't want to mix and match them for reasons we're about to get into next, or you'll have serious communications and connectivity issues.

SIDE NOTE:
If you're using the older 10Mbs/100Mbs connection ports, they will only use 2 of the pairs of wires within the twisted pair cable - 1 pair for transmitting, 1 pair for receiving.

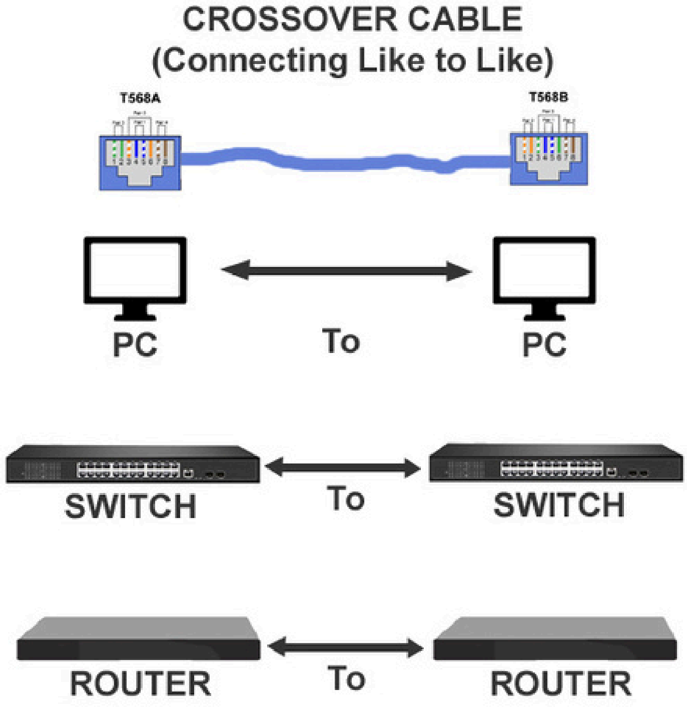
But if you're using 1Gbps or higher speed physical ports and connections, then all **4 pairs** of wires in the twisted pair cable will be utilized, as this is what provides more throughput and speed from the use of all of the wires within the cable - 2 pair for transmitting, 2 pair for receiving.

Crossover Cables

If we take one of the ends of a twisted pair cable and wire it with the T568A wiring scheme, and the other end of the same cable and wire it with the T568B wiring scheme, we have created what's known as a *Crossover Cable.*

By creating a Crossover Cable, you haven't "ruined" the cable. You HAVE however created a special type of cable that is only used between "like devices"

Example Connections for Crossover Cable:



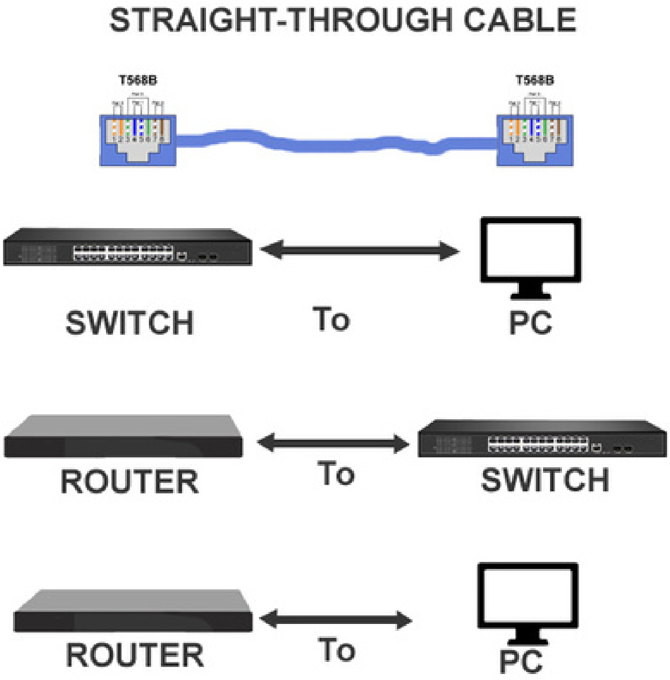
Straight-Through Cables

If we take both ends of a twisted pair cable and wire it with the T568A wiring scheme, OR we wire both ends of the cable with the T568B wiring scheme, we have created what's known as a *Straight-Through Cable.*

What makes it a Straight-Through Cable? Having the same wiring scheme on both ends.

The Straight-Through Cable is the most commonly used network cable on computer networks everywhere. And again, in the U.S. at least, the most often used ends on Straight-Through Cables are T568B on both ends.

Example Connections for Straight-Through Cable:



Rollover Cable

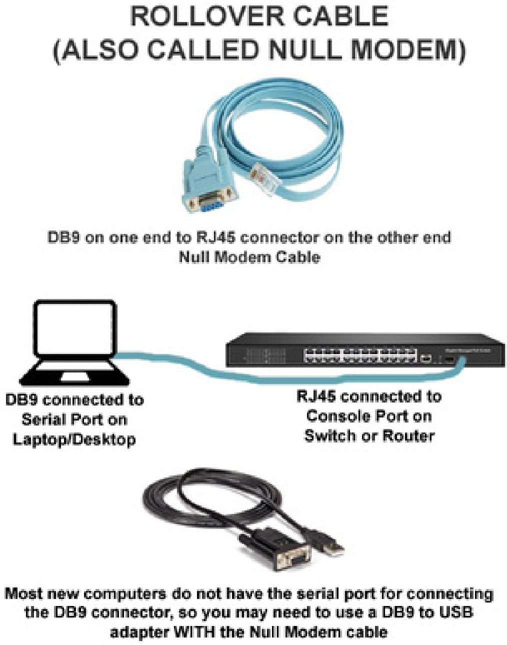
We'll get into more detail about the actual connection you need to make to a Switch or Router to add or change the configuration on them for how they handle traffic and operate, and we'll do that in Book 2 where we get into the logic and protocols used on computer networks.

For now, just understand that a Rollover Cable is what we use to directly, physically connect to a Switch or Router to access its settings/configuration.

It's called a Rollover Cable because the wires are rolled over in complete reverse from one end to the other. On one end, you'll use either the T568A or T568B wiring scheme, then on the other end you will completely reverse the wiring layout of the wires and connect it a DB9 connector for connection to a serial port on a laptop or desktop.

The Rollover Cable is also referred to as a Null Modem cable.

Example Connection for Rollover Cable:



ROLLOVER CABLE
(ALSO CALLED NULL MODEM)

DB9 on one end to RJ45 connector on the other end
Null Modem Cable

DB9 connected to Serial Port on Laptop/Desktop
RJ45 connected to Console Port on Switch or Router

Most new computers do not have the serial port for connecting the DB9 connector, so you may need to use a DB9 to USB adapter WITH the Null Modem cable

FIBER OPTIC CABLE

Ok, so we talked about the Copper Cables - Coaxial and Twisted Pair - and the only other thing you need to remember about Copper is that signals can only be transmitted so far (100 meters or roughly 300 feet) before they degrade. That degradation is known as “attenuation.”

NOW we’re going to take a look at cables that don’t transmit electric signals (electrons) like copper does, but rather they transmit the signals (1s and 0s) using light sent down a glass core in the middle of the cable.

This type of cable is known as *Fiber Optic Cable*.

Fiber Optic Cable uses either glass or polymer/plastic wrapped in a reflective sheath to carry light signals much longer distances faster (no attenuation like you get with copper). Since light isn’t affected by RFI (Radio Frequency Interference) or EMI (Electro-Magnetic Interference) from magnetic fields outside the cable, Fiber Optic cable is used for more permanent long-distance connections.

Keep in mind that Fiber Optic cannot be bent as sharply as copper cable can. It can also be physically damaged easily and will cease to work carrying light pulses and signals. So it has to be handled more delicately.

However, we are beginning to see Fiber Optic used much more than in years previous, and that trend may not change.

So what are the speeds and limitations of Fiber Optic?

Though Fiber Optic can transmit much greater distances using light than a copper cable can using electrical pulses/signals, Fiber Optic does still have limits.

In most cases, if you're using 100Mbps Fiber Optic cable, you will have a maximum distance of 2 kilometers (which is about 1.2 miles or 6,561 feet) before the signal needs to be repeated or regenerated. Remember with copper cable it is only 100 meters (approx. 300 feet).

10Gbps Fiber Optic cable has a distance of only about 1000 feet (or 300 meters). And we're starting to see more 40Gbps and 100Gbps speeds in the Fiber Optic cabling realm, so be aware of that.

Single Mode and Multimode

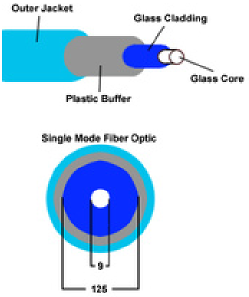
There are 2 main types of Fiber Optic cable found in the market today, and they have different distances and speeds at which they can transmit a signal.

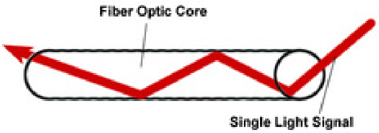
Single Mode

Single Mode fiber optic only allows 1 mode (or signal) of light to pass through the core at a time.

Since it is only 1 signal at a time, it can handle a higher bandwidth and is used for longer distances.

Single Mode fiber optic cable measures 9 microns on the inner core of the cable with a 125 micron cladding that reflects and retains the light inside the core.





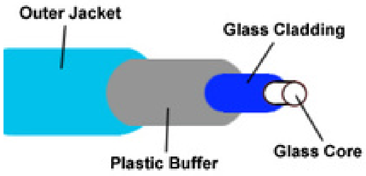
Multi Mode

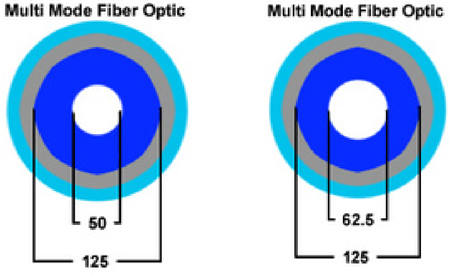
Multiple light signals can travel inside the glass core of a Multi Mode Fiber Optic cable - each using a different variant of light in the light spectrum.

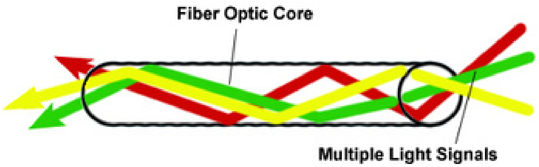
The Multi Mode Fiber Optic cable can allow more data to pass through at any given time (multiple signals simultaneously), but they cannot be used to carry light signals nearly the distance that a Single Mode cable can.

Since Multi Mode can carry more data at the same time, you typically see Multi Mode used in datacenters.

Multi Mode Fiber Optic cable core is usually made in 50 micron width and 62.5 micron width:







CH. 5 - Wireless

We live in the 21st Century, so why are we using antiquated methods of cabling everything together when we can do WITHOUT the cables and go Wireless?

Unfortunately (or fortunately depending on how you look at it) we can't just **stop** using cables and use wireless with everything - there are entirely too many security issues and vulnerabilities that could crop up.

But we CAN implement wireless connections on our network where it seems most feasible and provides convenience and portability to the users **of** that network.’

Enter Wireless...

Wireless Hardware

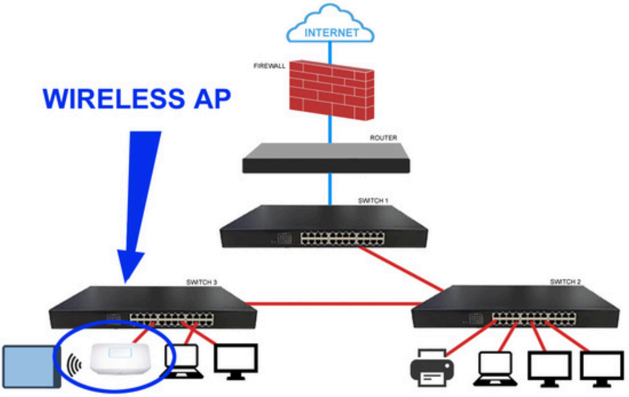
In this first book, we’re not going to get into the logic and the settings and configurations used in Wireless in networking.

We’re only going to discuss (for now) the actual *hardware* used to create wireless access to a computer network, then get into the logic, configuration and settings in the next book in this series.

For now, we know we have to have at least 2 components to connect end devices (PCs, laptops, tablets, smartphones, printers, etc.) to an existing wired network:

Wireless Access Point (AP)

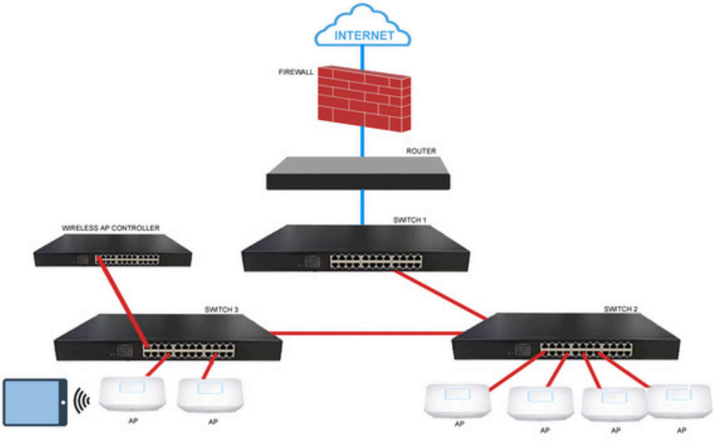
To connect wireless devices to a wired network, you have to have a device that transmits and receives wireless signals from those end devices and connects to the wired network. In computer networking, this is the Wireless Access Point (AP).



Shown above is a Wireless AP that is connected to a Layer 2 Switch on our wired network with an Ethernet cable. The easiest way to directly connect a single Access Point.

Depending on the capabilities of that AP (how many end devices can connect to it simultaneously, throughput, bandwidth), it may serve as sufficient wireless in its location.

However, once you get into bigger wireless setups, you will have multiple APs connected to a controller device that allows management and configuration of that wireless network.



Once you get into using a Wireless Access Point Controller, you are getting into larger wireless networks whereby someone using a wireless device (a laptop, for example) can roam and remain on the wireless network connection.

In other words, a laptop can connect to the first AP and get access to the network. Since the APs are all reporting back to a centralized Wireless AP Controller, they can all be used for the same wireless network. The laptop can then physically move to another location that's closer to one of the other APs and still remain connected.

Again, we won't get too bogged down in the details of that, as the only step we're trying to take now is to get an overview of the physical components of a computer network and how they basically connect and are used.

CONCLUSION

So to keep everything as simple as we can for someone just starting out, in this first book we covered the basic components and connection methods, the basic types of computer networks and why they may be needed or used.

If you'd like to go to the next step, be sure to sign up for the Waiting List for my Switch Ace course where we're going to take the next step and really get into the details of Layer 2 Switches and how they work.

See part of the "Secret" to learning computer networking so fast is to divide it up into physical components, then logical and software/applications. THEN, you'll find it easier to dive into learning about Layer 2 Switches on a LAN.

Once you get a firm understanding of Switches and LANs, becoming the expert in computer networking is not too far away.

In this 1st Book, we went over the hardware and physical components of what make up a computer network.

In Book 2, we're going to get into the software, applications and logical aspects of computer networks.

You'll learn not only how to connect to and setup/configure Switches and Routers, but we'll dive down into more detail about software and applications used on computer networks and how it all works together.

Here are just SOME of the things we'll cover in Book 2:

- Connecting to Network Devices
- IP Addressing, Subnet Masks, IPv4 vs. IPv6, DHCP, DNS, Private IP vs. Public IP, VLANs
- SSIDs on Wireless Networks
- Spanning Tree Protocol (STP)
- The OSI Model vs. TCP/IP Model
- Routing and Routing Protocols
- Access Lists
- Troubleshooting Basics