# COMPTIA NETWORK+ N10-006 STUDY GUIDE

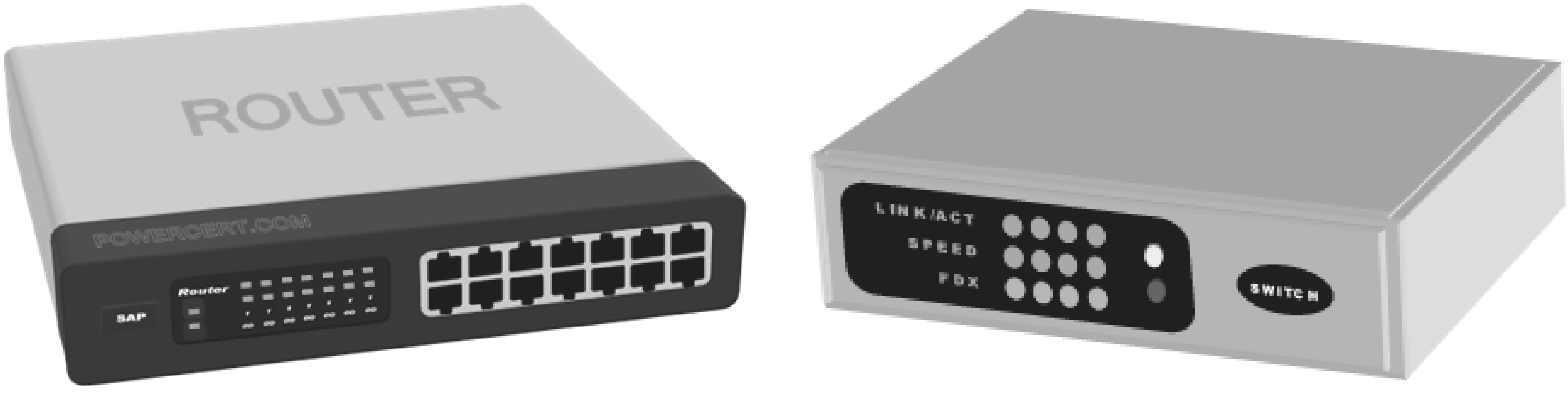
**Written by Scott Prieto**

From the creator of PowerCert Animated Videos on YouTube

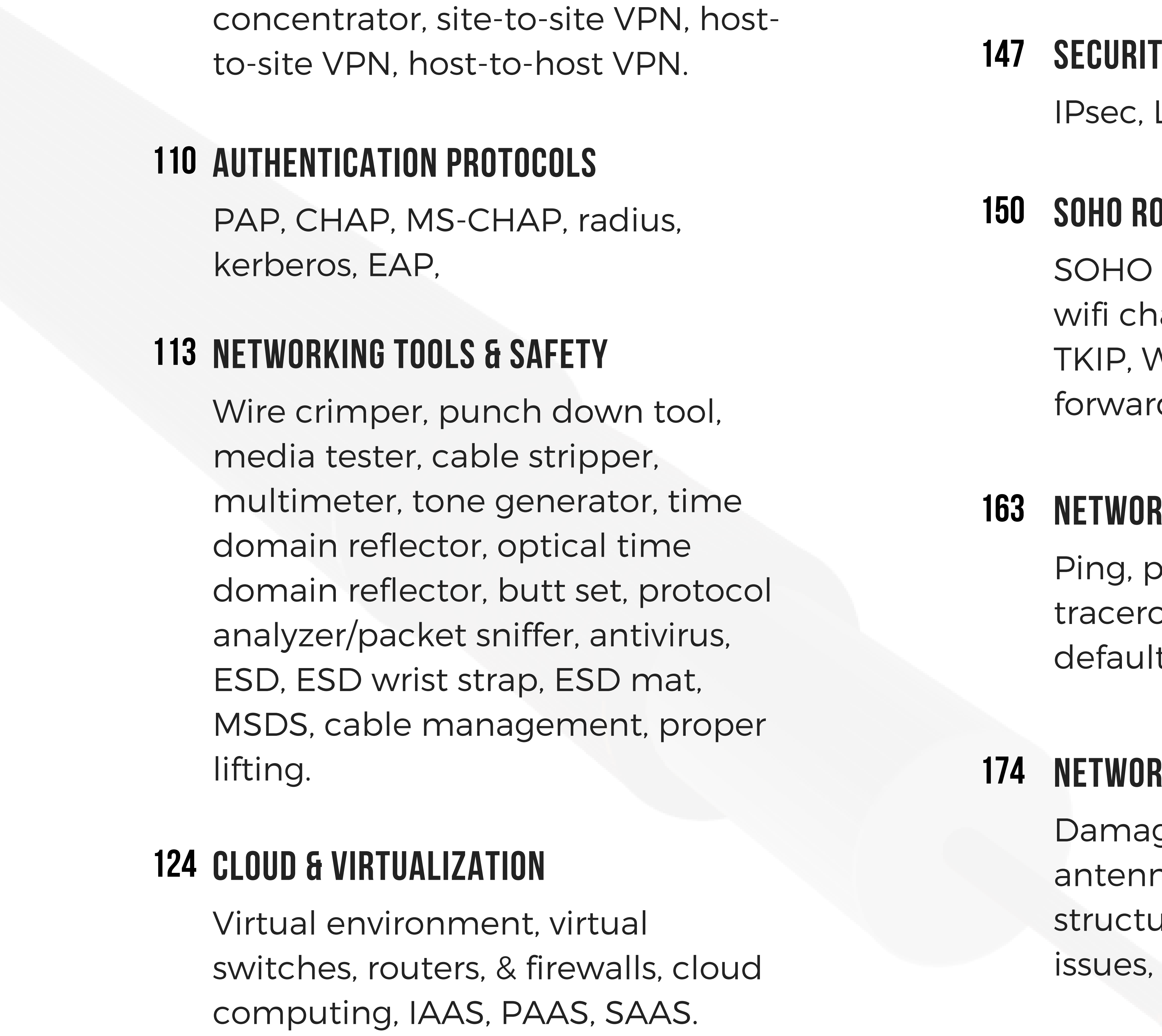
Version 2.0

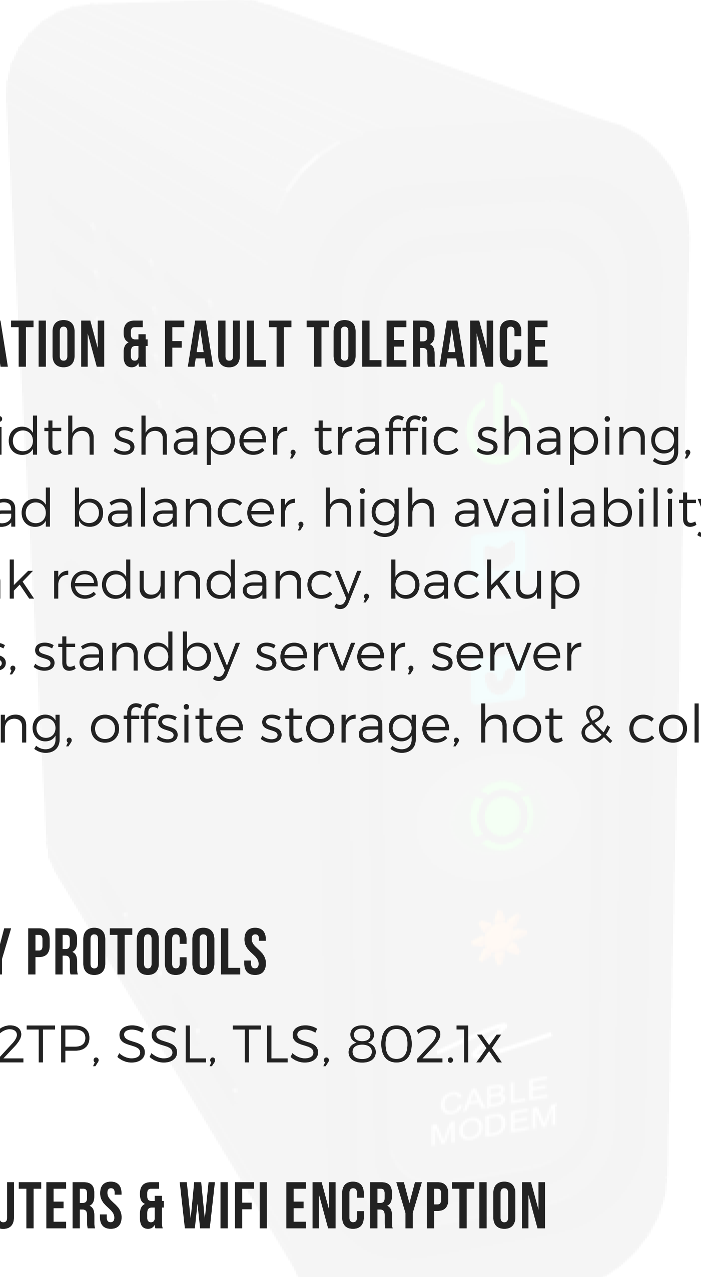
## This ebook is designed to study for the CompTIA Network+ N10-006 exam.

## Check out my youtube channel: PowerCert Animated Videos



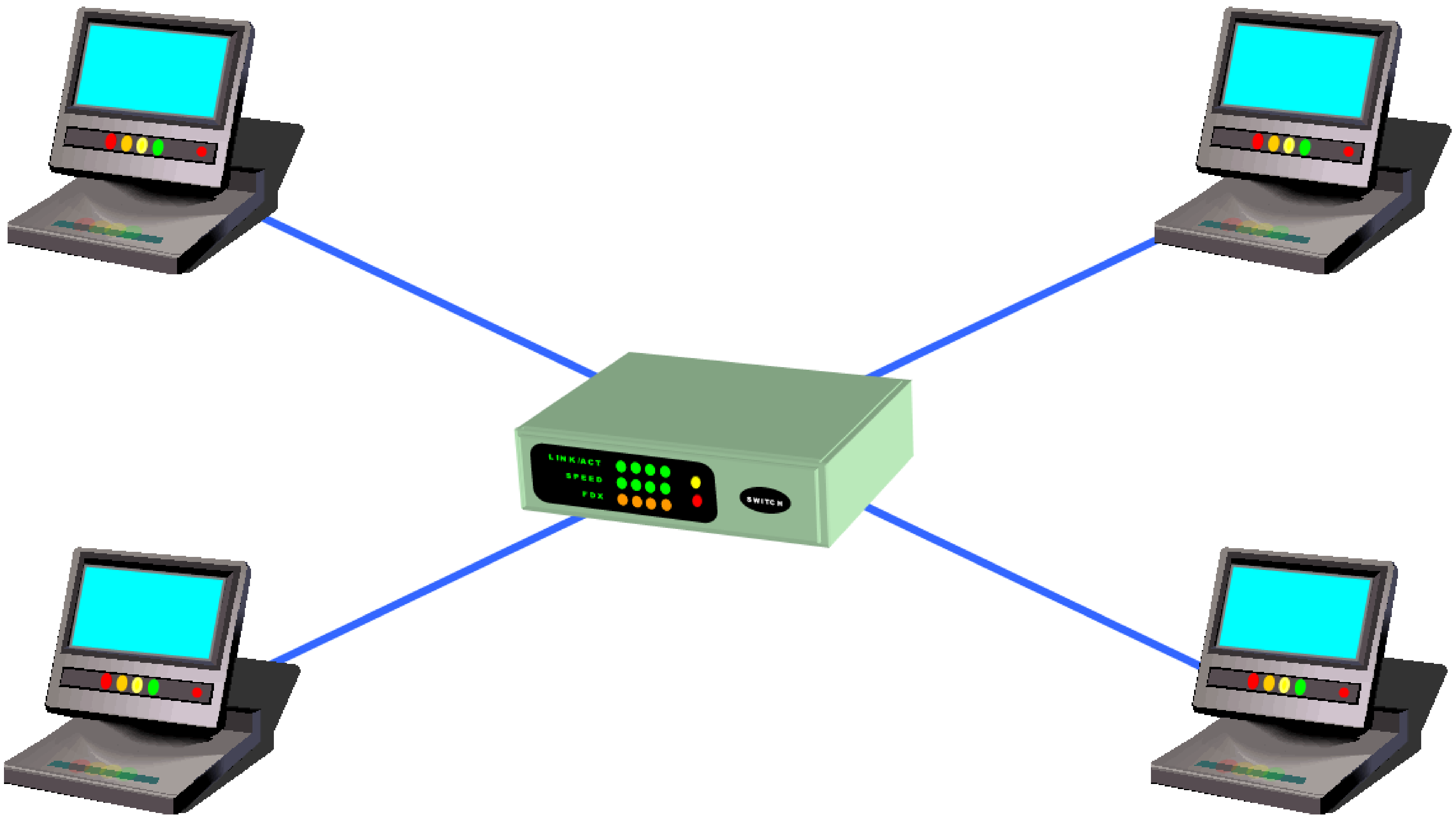
# TABLE OF CONTENTS




CABLE MODEM

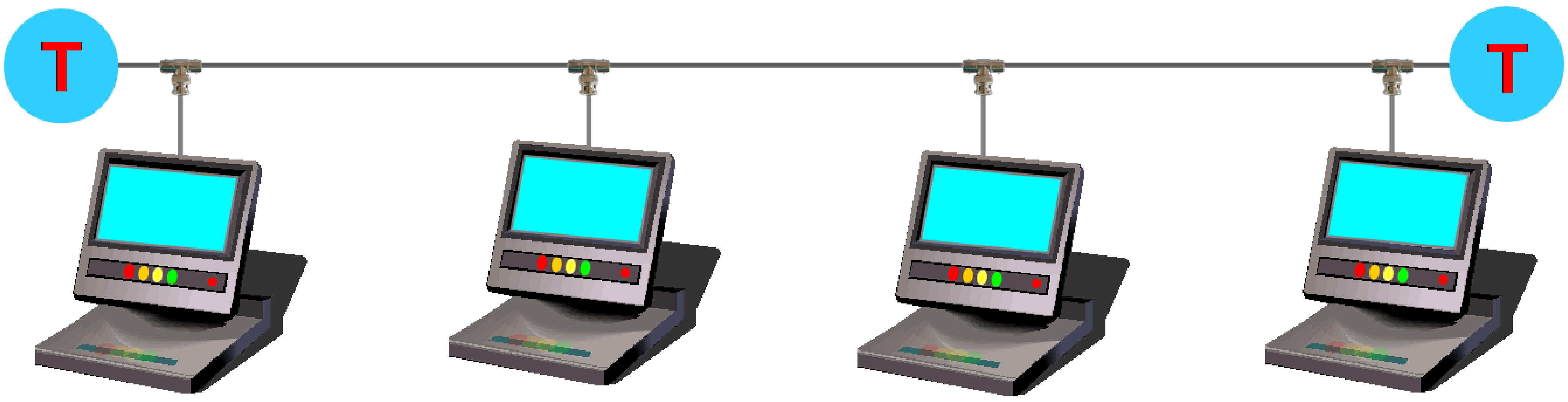
# Topologies

The layout of how a network communicates with different devices is called a **topology**.  The most common topology is the **star topology**.  In a star topology, all computers are connected to a central wiring point, such as a hub or a switch.  All data on a star network passes through this central point before continuing to its destination.  One of the major benefits of this topology is that if one computer failed or if there was a break in the cable, the other computers would not be affected because each computer has their own cable connection.  However, a disadvantage of the star topology is that if the central hub or switch fails, then all the computers on that central point would be affected. This is called a single point of failure.  If this happens the entire network goes down.



**Star topology**

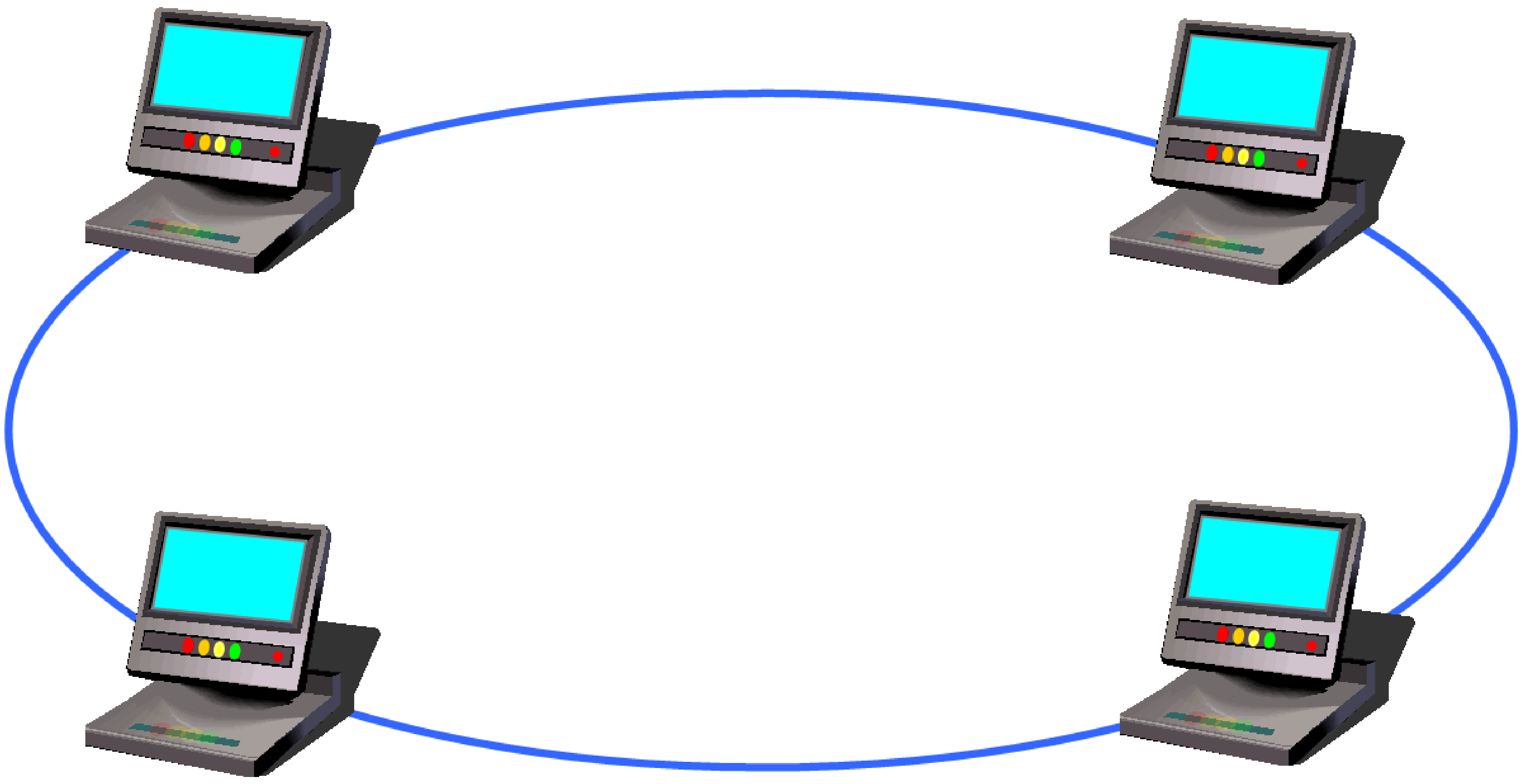
The **bus topology** is very old technology and it is not used today that much.  This is the kind of network setup where each of the computers and network devices, are connected to a single cable or backbone.  This backbone is a coaxial cable.



**Bus topology**

The computers connect to this cable using special connectors called BNC, which are also known as T-connectors.  One of the advantages of the bus topology is that it is fairly cheap and easy to implement. However, a disadvantage of the bus topology is that it requires that the cable is terminated at both ends using terminators.  In order for this setup to remain operational, there must not be any open connections, including the ends that attach to the computers.  If a computer is removed or added or if the terminators are loose or missing, then the cable would be open and data would bounce back.  This bounce is known as signal reflection, and if this happens data flow would be disrupted.

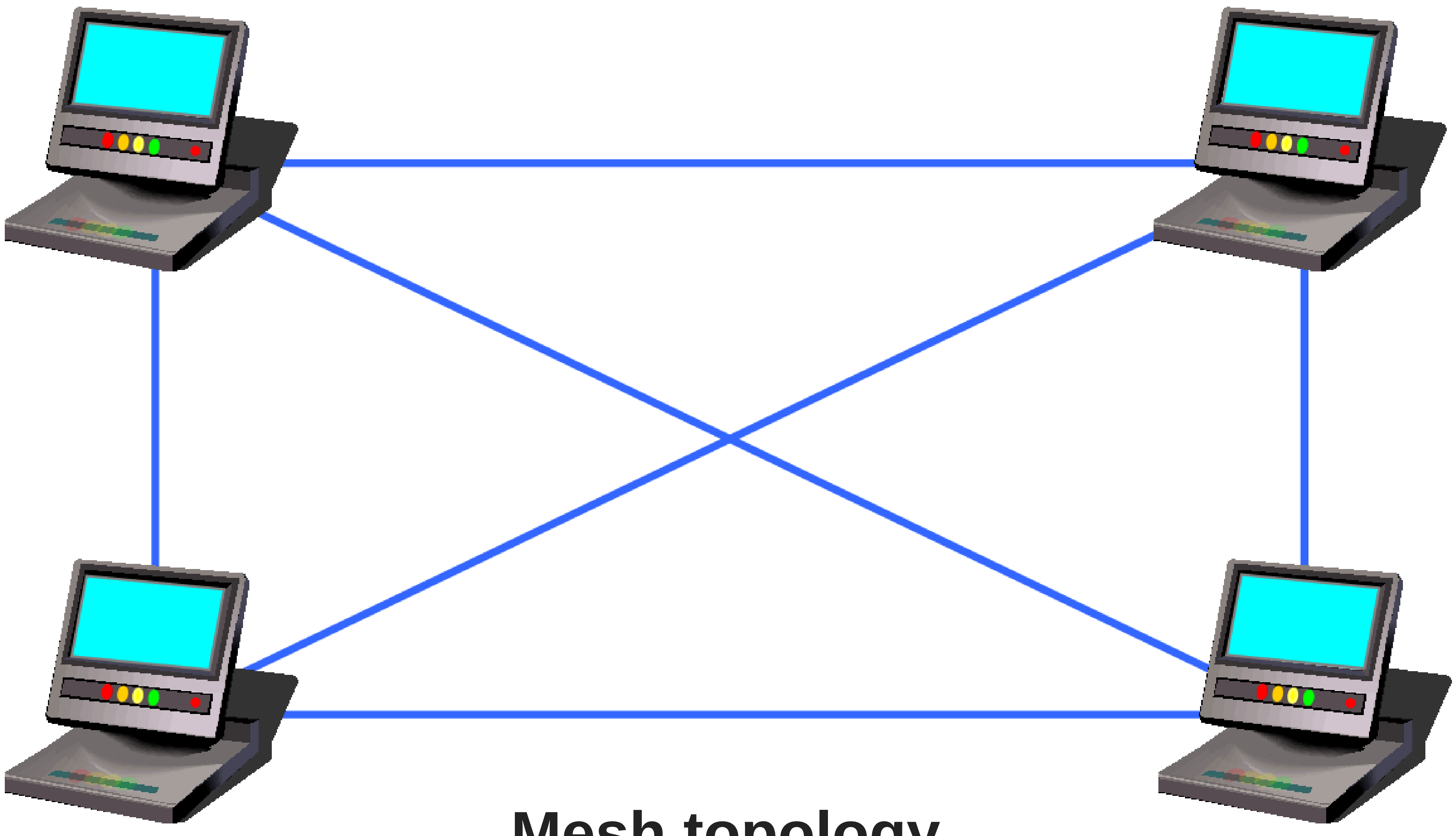
The **ring topology** is a type of network configuration where each computer is connected to each other in the shape of a closed loop or ring.  So every computer on



**Ring topology**

this ring has exactly two neighbors for communication purposes.  Each data packet is sent around the ring until it reaches its final destination.  This kind of topology is rarely used today.  The advantage of a ring topology is that they are easy to install and easy to troubleshoot. However, the disadvantage would be, that if just one of these computers goes down or if there was a single break in the cable, then all data flow would be disrupted.

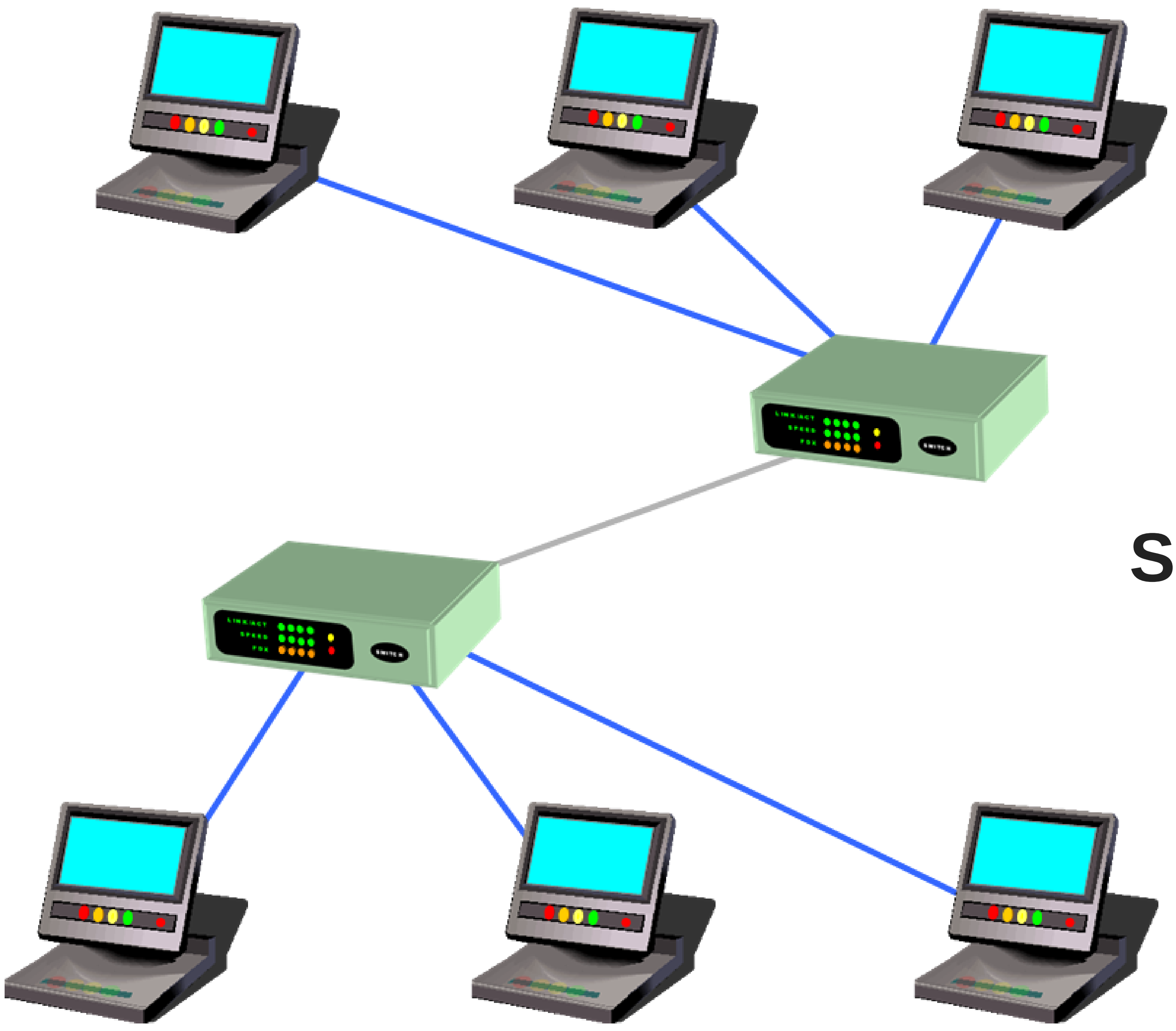
There is also the **mesh topology**.  In a mesh topology, each computer on the network is connected to every other computer on the network.  So by having so many



**Mesh topology**

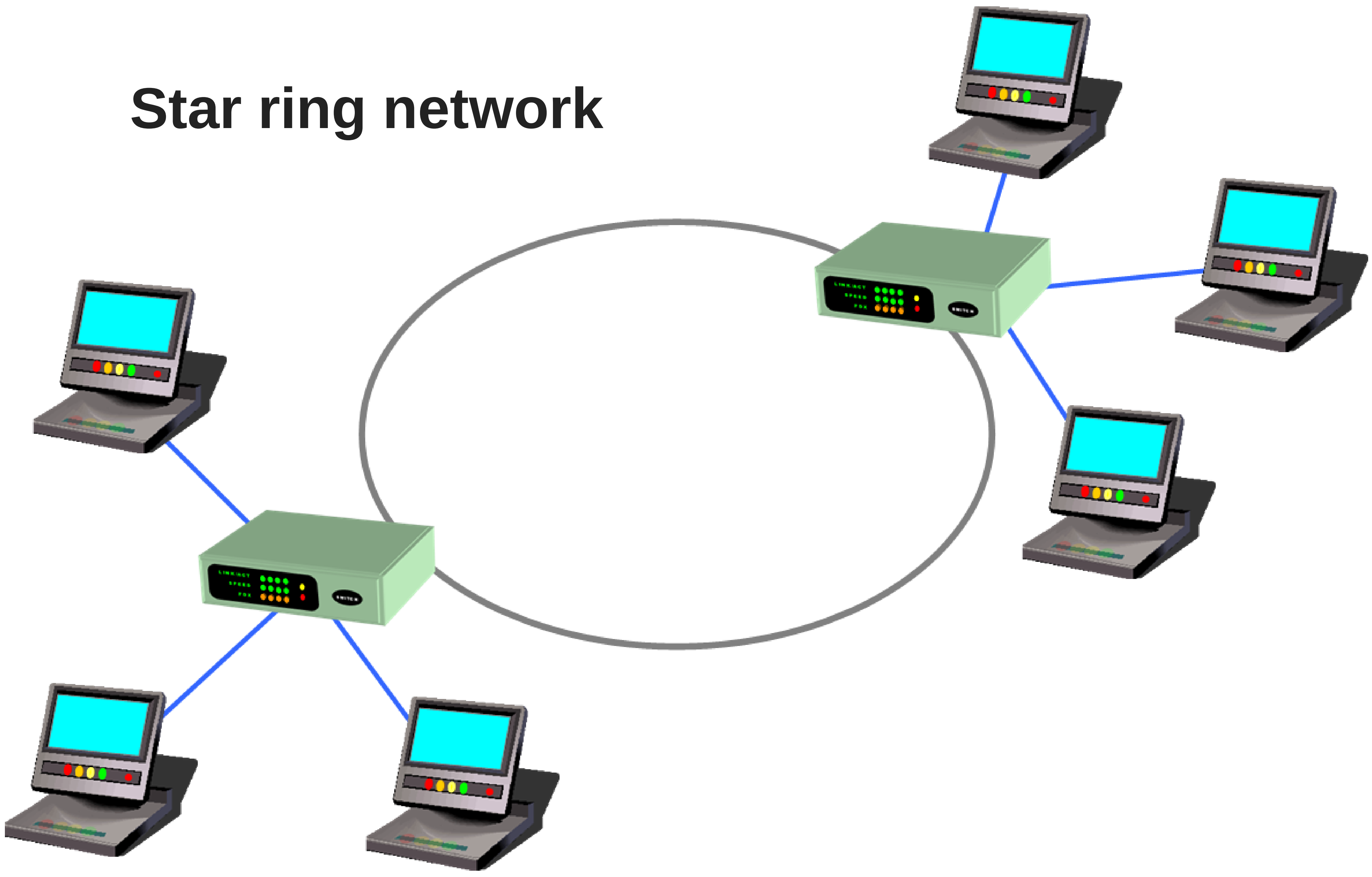
connections it handles failure very well.  In this illustration above, there are 4 computers with 3 connections on each computer, which makes a total of 12 connections for this network.  But because of the amount of cabling and network cards that have to be used, mesh topologies can be expensive, so they are rarely used on local area networks or LANs.  They are mainly used on wide area networks, like the internet.  In fact, the internet is a perfect example of a mesh topology.  The advantage of a mesh topology is that it creates a high redundancy level.  Because if one or more connections fail, the computers would still be able to communicate with each other.

Topologies can also be combined with other topologies if needed, and these are known as **hybrid topologies**. Hybrid topologies can offer the best of both worlds.  In fact, a lot of businesses use some form of a hybrid topology to suit their growing needs.  The most common forms of hybrid topologies are the **star bus network** and the **star ring network**.



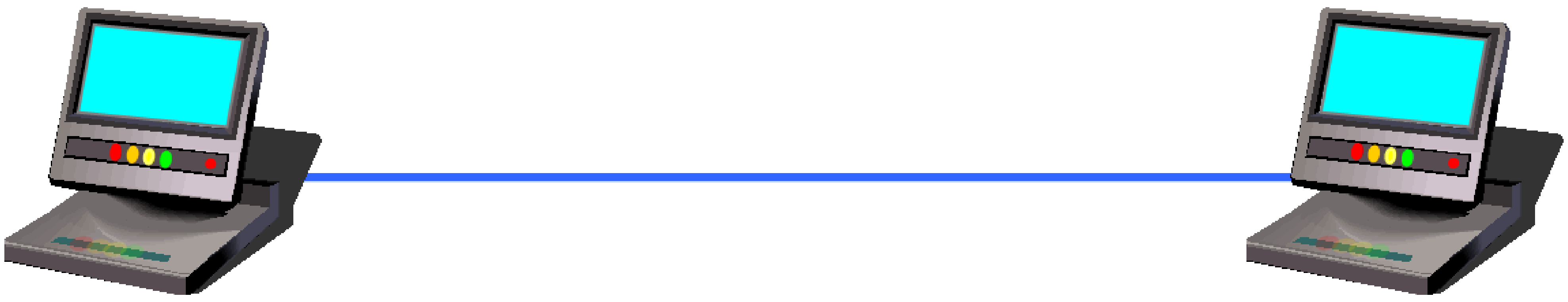
**Star bus network**

In a star bus network, two or more star topologies are linked together using a single bus connection.  In a star ring network, two or more star topologies are linked together to form a large ring network.



Star ring network

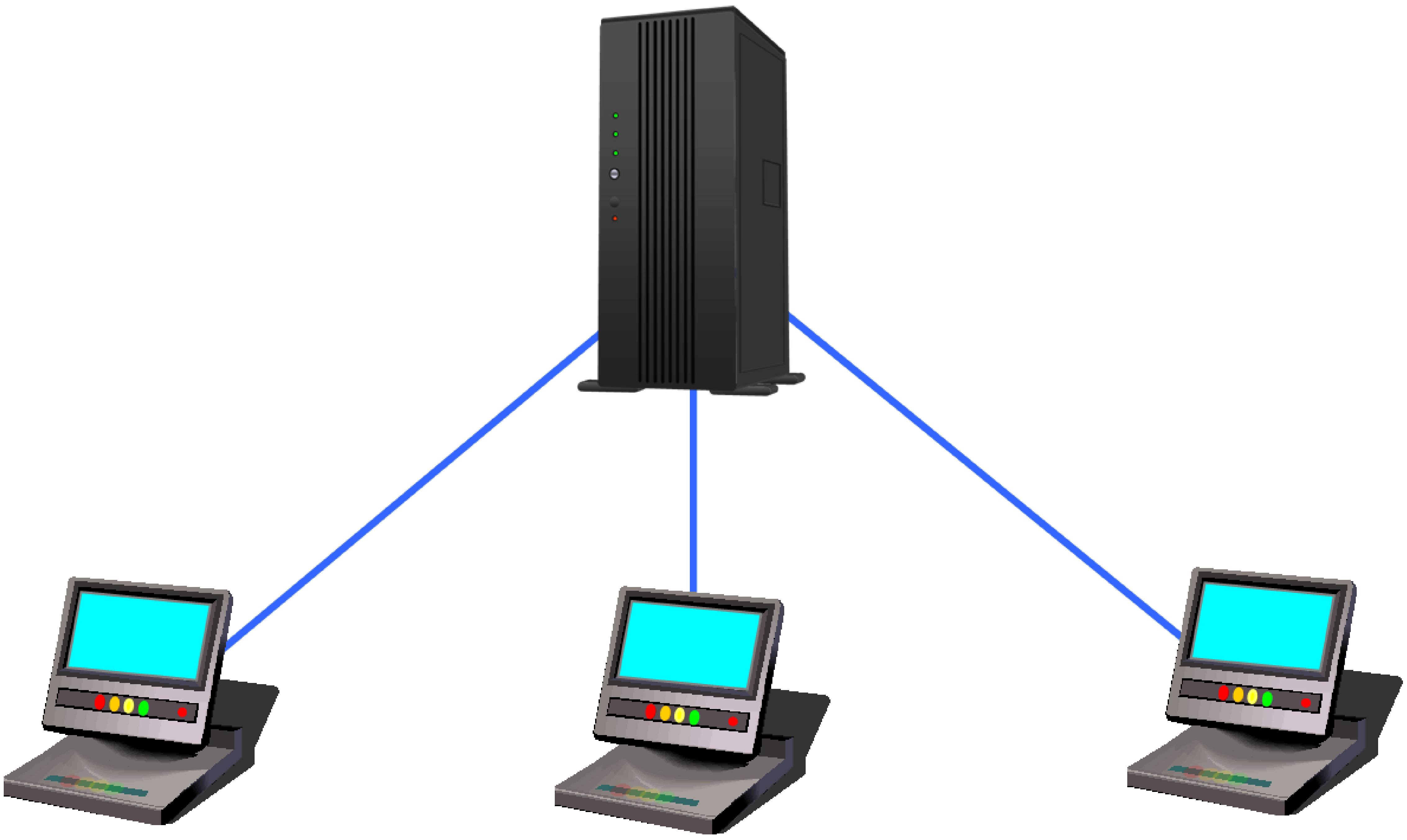
A **point-to-point topology** is two hosts that are directly connected to each other using a single cable.  These hosts could be computers, switches, routers, servers, and so on.  A point-to-point topology is the simplest form of topology there is.



Point-to-point topology

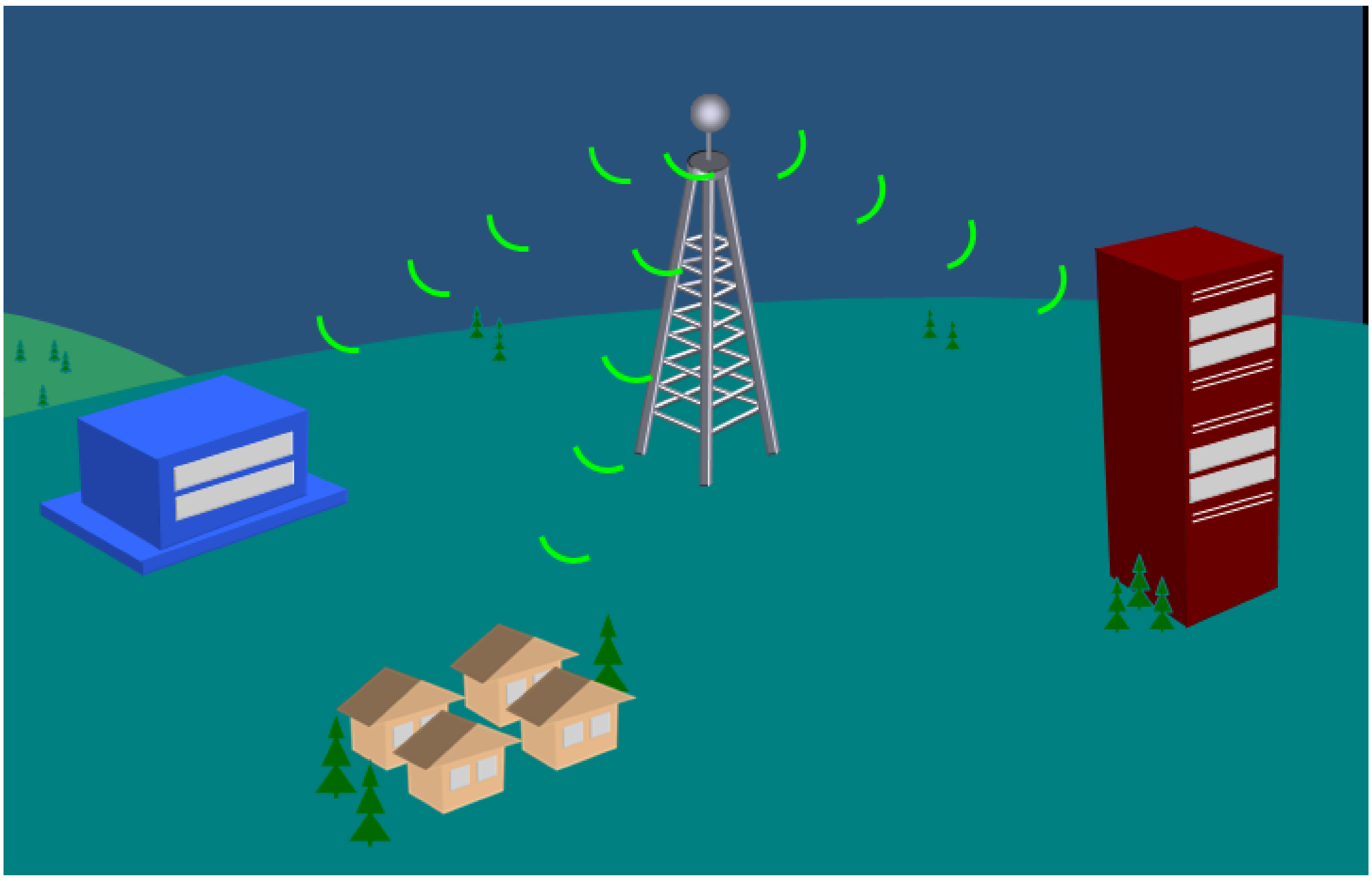
A **client-server topology** is where clients connect directly to a centralized dedicated server to access resources rather than connecting to each other.

Typically a lot of businesses use this type of topology because instead of having to put all the resources on each computer, which is a lot more work, the administrator can just put all the data on one machine. Then all the clients can access the resources when they need it.  So obviously putting the resources on just one machine is a lot less work than putting the data on multiple clients.  It makes the administration a lot simpler.



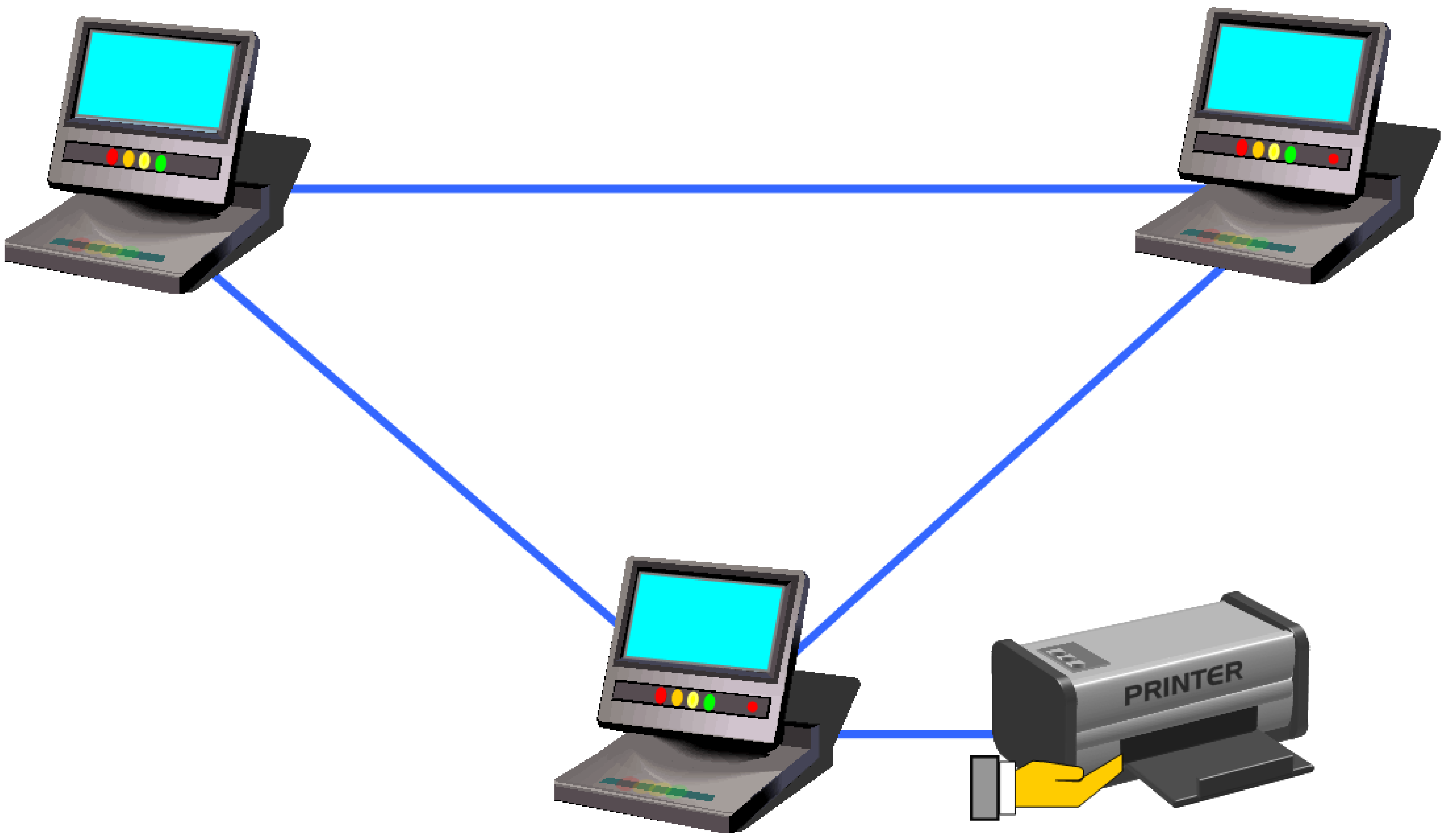
**Client-server topology**

A **point-to-multipoint topology** is a network architecture that is commonly used in wireless outdoor networks.  So what you would have is a central wireless base station and then there would be other wireless locations around it that connect to the single central location.   Now, these other locations will not directly communicate to the other locations.  They will all only communicate to the central location.  The wireless locations are commonly called clients.  The central location is commonly called an access point or a base.



**Point-to-multipoint topology**

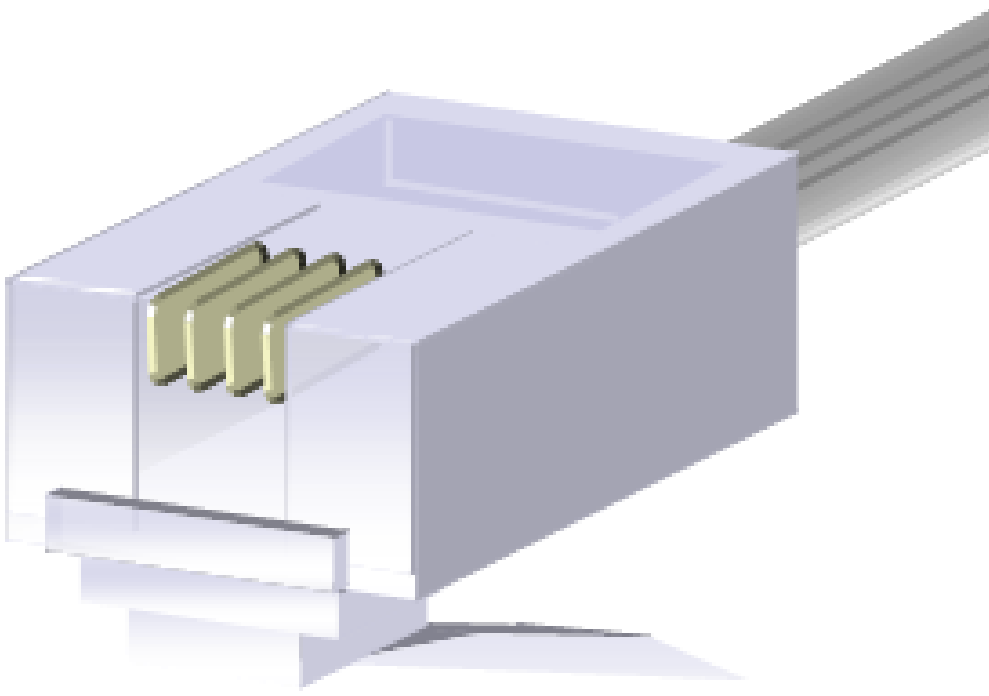
A **peer-to-peer topology** is where all the clients on the network talk to every other client on the network to share their resources with each other.  So for example, one computer can share their printer, another computer can share their files on their hard drive, and so on.



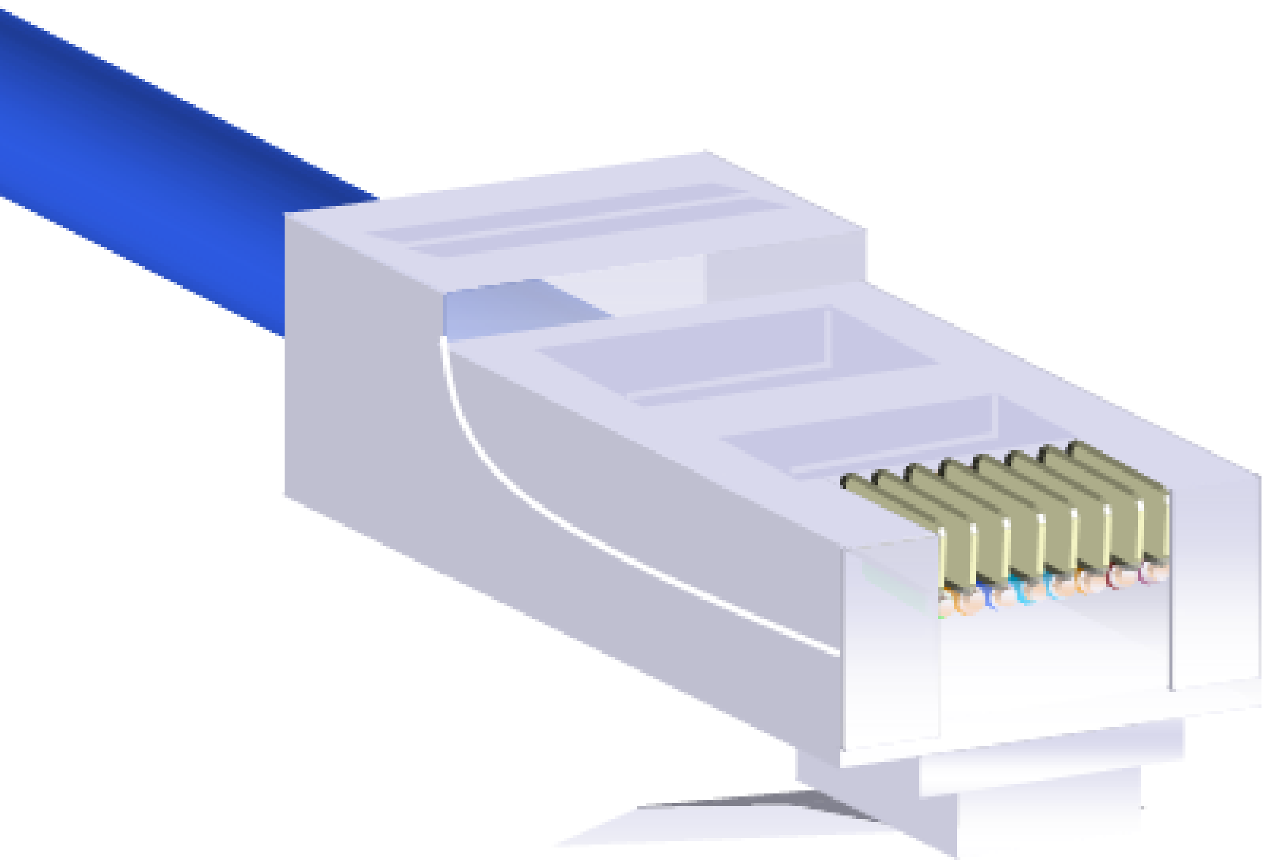
**Peer-to-peer topology**

# Networking Cables & Connectors

This is the **RJ-11** connector.  RJ stands for **registered jack**.  This is a 4 wire connector, used mainly to connect telephone equipment.  But as far as networking, the RJ-11 is used to connect computers to local area networks through the computer's modem.  The RJ-11 locks itself and to place by a single locking tab, and it resembles an RJ-45, but it's a little bit smaller.



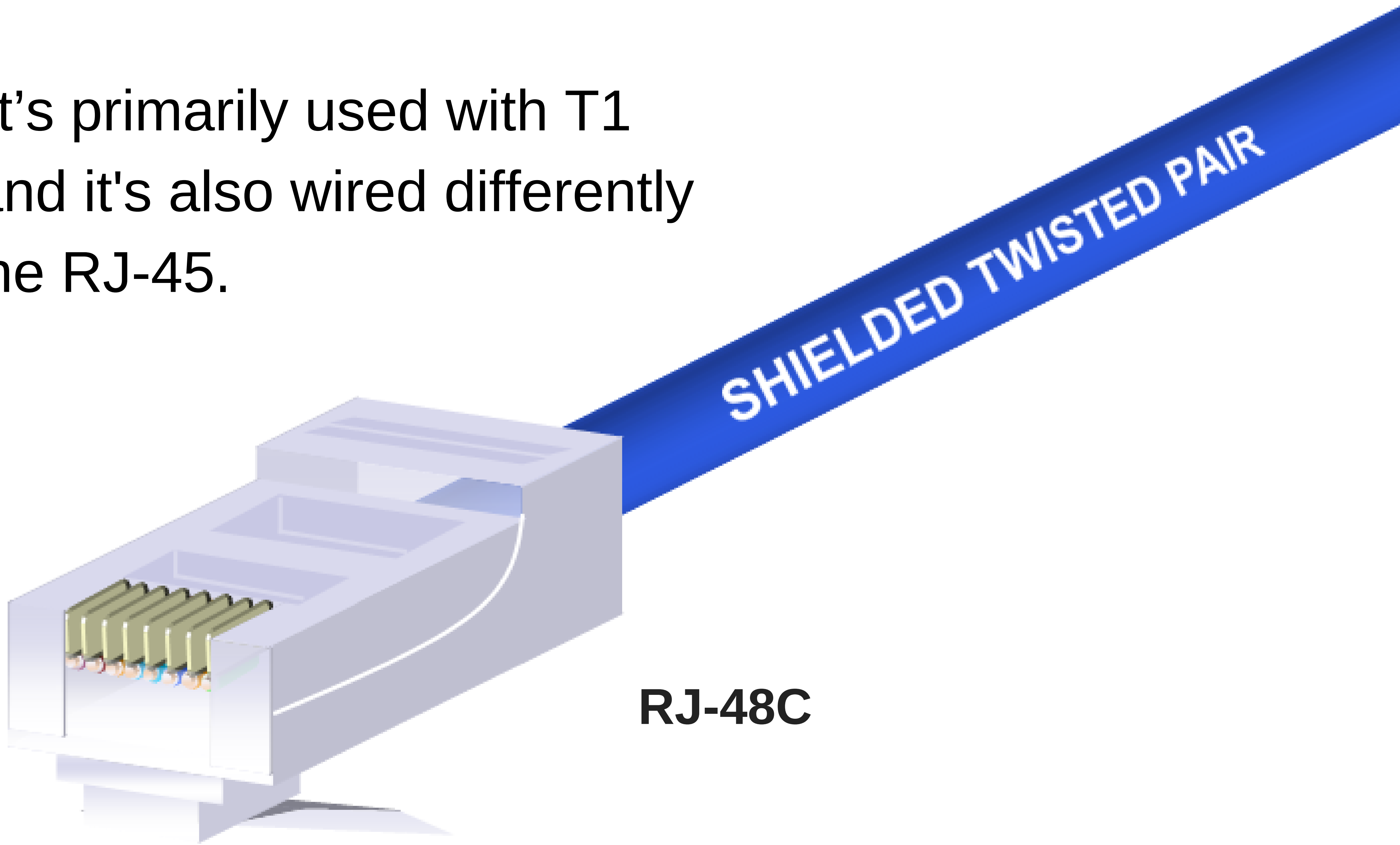
**RJ-11**



**RJ-45**

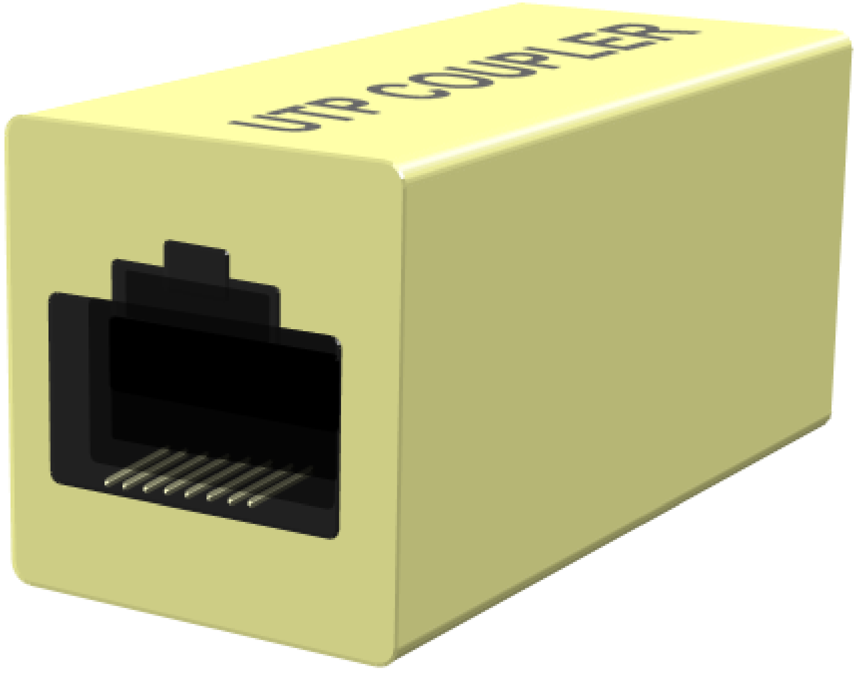
Now the **RJ-45** is by far the most common network connector.  This is an 8 wire connector, used to connect computers to local area networks.  And like the RJ-11, it also locks itself into place by a single locking tab, and it also resembles or RJ-11, but it's a little bit larger.

The **RJ-48C** looks very similar to the RJ-45.  The difference between the two is that the RJ-48C is used with shielded twisted pair, instead of unshielded twisted pair.  It’s primarily used with T1 lines and it's also wired differently than the RJ-45.

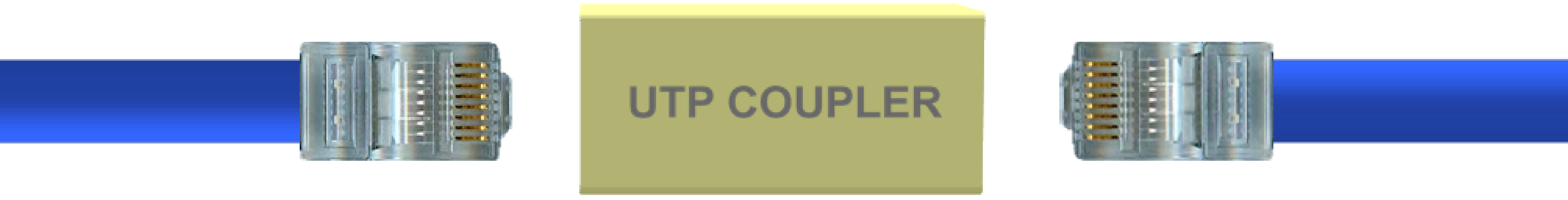


RJ-48C

A **UTP coupler** is used for connecting UTP cables with RJ-45 connectors to each other. This is typically used when running a longer cable is not an option.  You just plug one end of the cable into the coupler and then add another cable on the other side.  And now you have successfully extended your UTP cable.

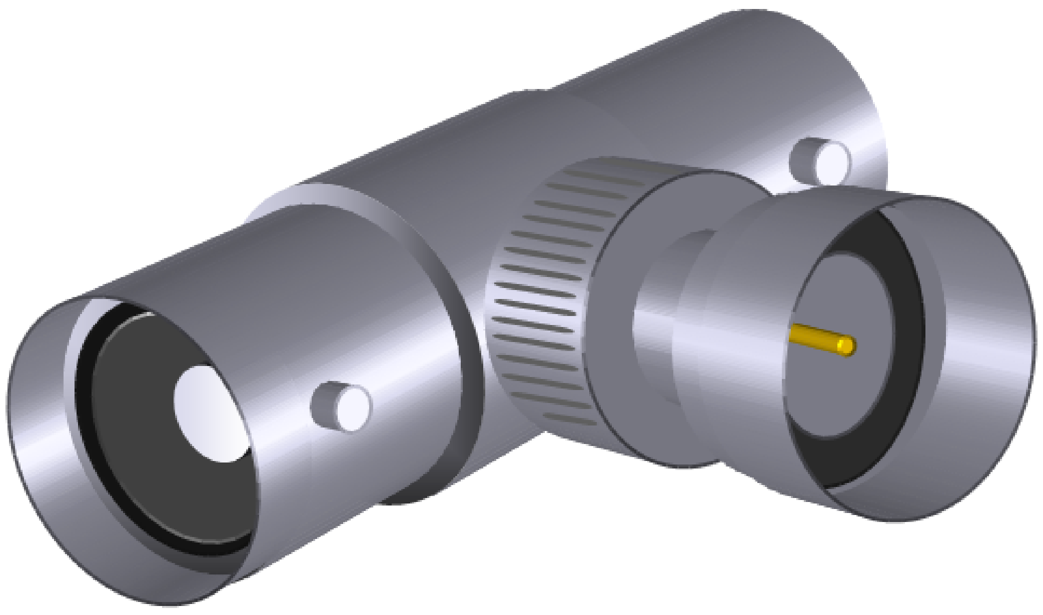


UTP coupler

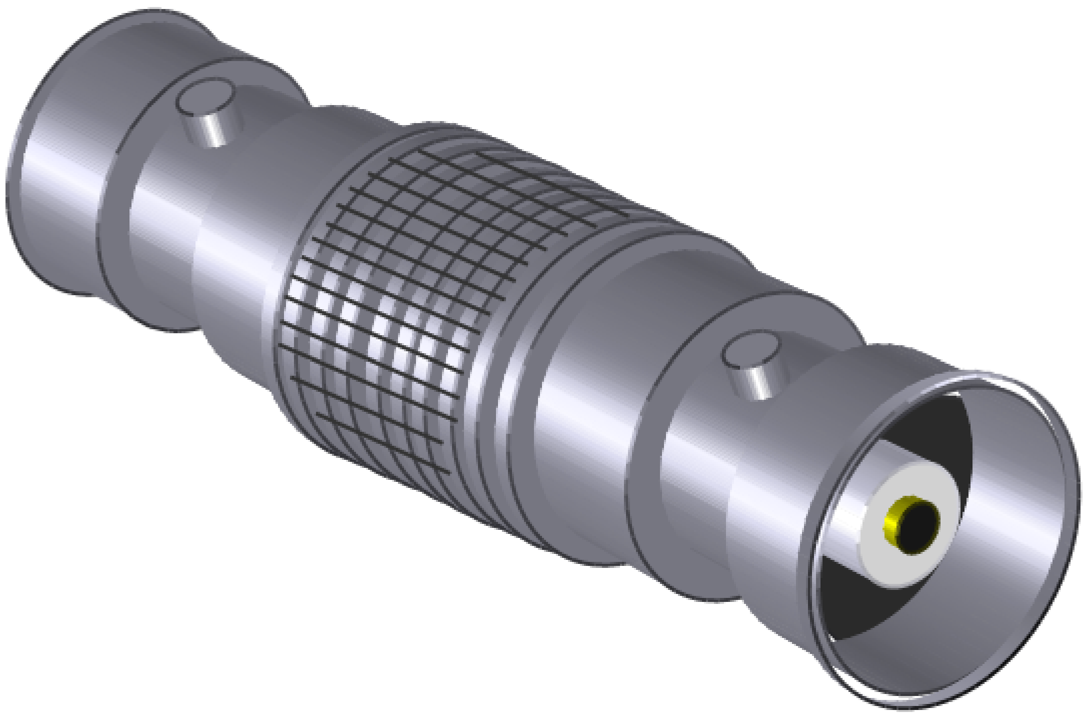


The **BNC** connector is a common type of RF connector that is used on coaxial cable.  BNC stands for **bayonet**

**neill concelman**. And the BNC is used for both analog and digital video transmissions, as well as audio.



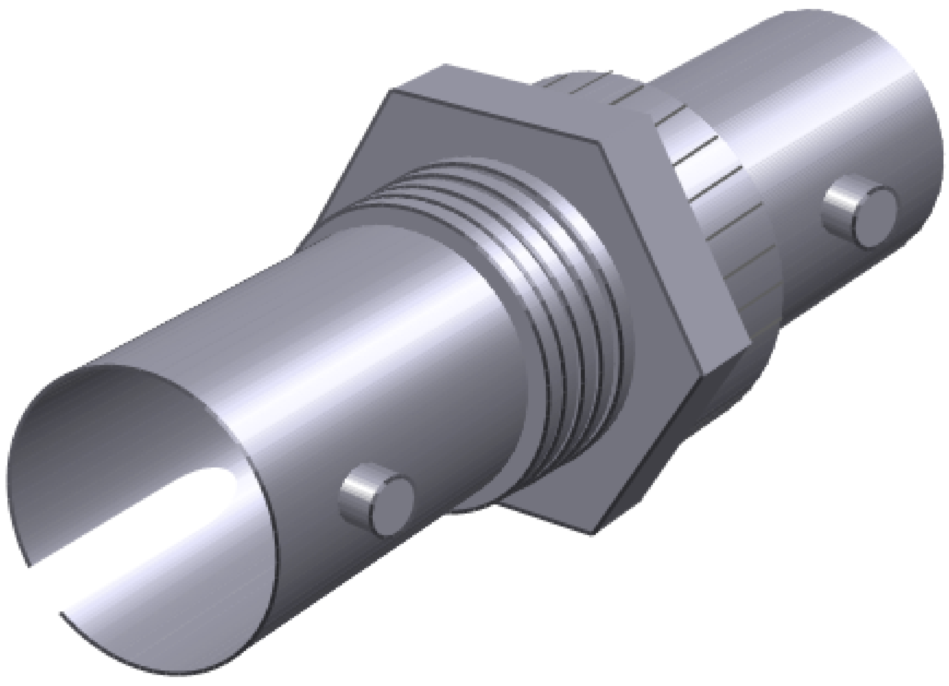
BNC



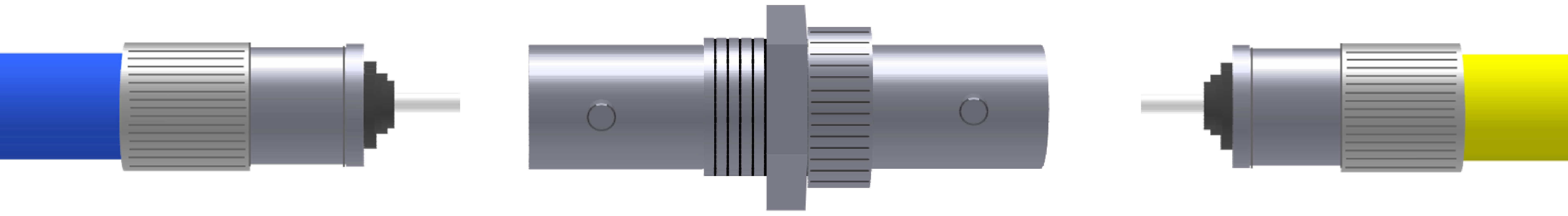
BNC coupler

A **BNC coupler** is used to connect together two coaxial cables with BNC connectors attached to them. This particular coupler is a BNC female to female coupler.

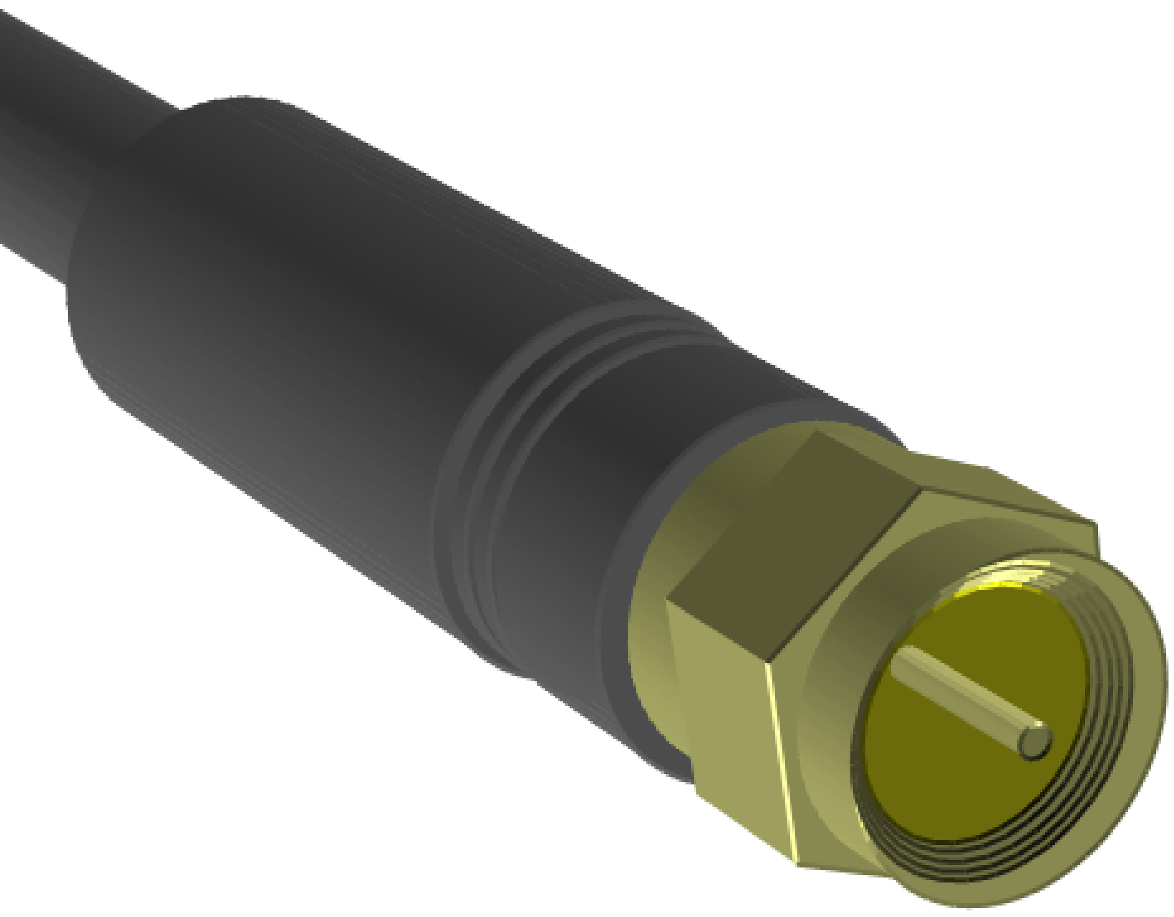
If you wanted to join two fiber optic connectors, you would use a **fiber coupler**. Fiber couplers are used to couple or join two of the same fiber optic connectors. The two connectors have to be the same.



Fiber coupler



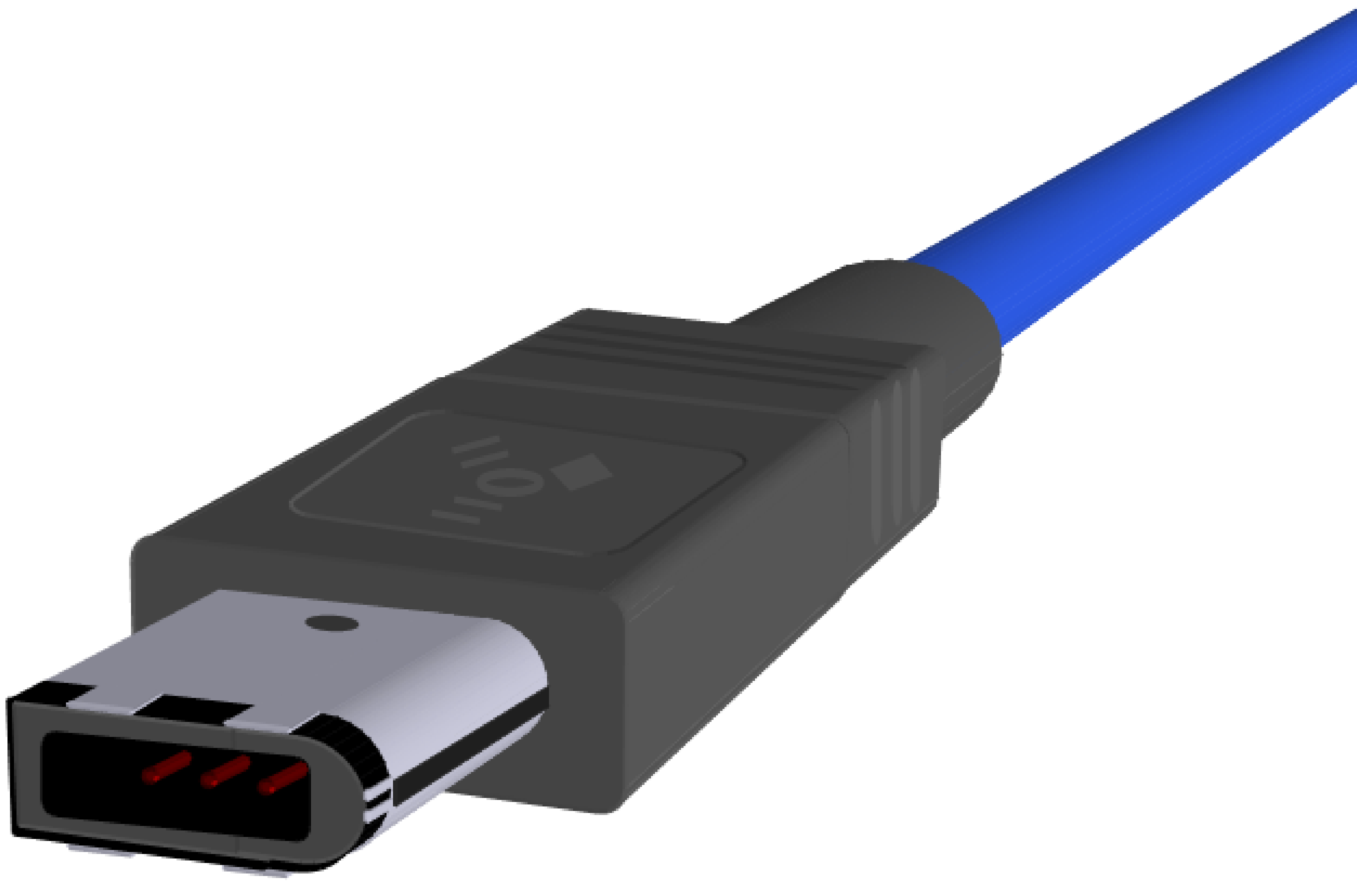
Fiber coupler used to join two fiber connectors together.



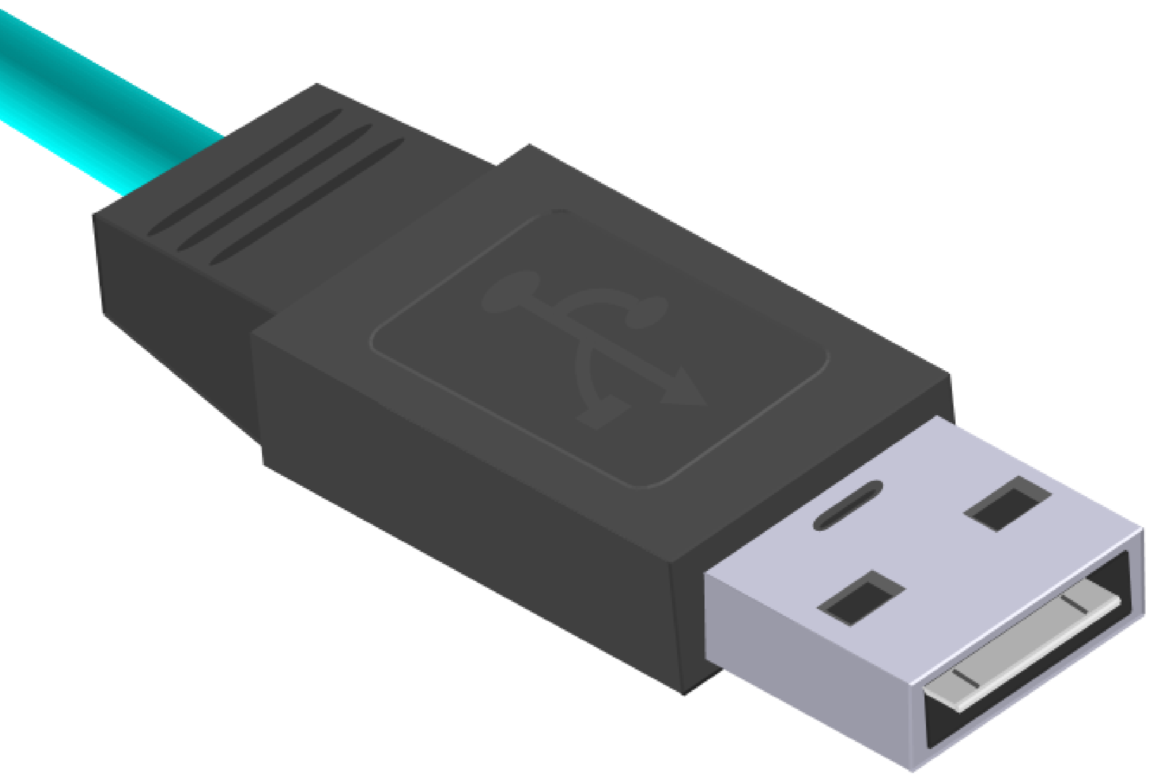
F-type

This connector is called the **F-type**. Now, this is a threaded connector typically used on coaxial cables. These are primarily used by cable providers to attach to cable modems. The F-type hand tightens by an attached nut.

This is the IEEE 1394 connector, and this is also known as **firewire**. Firewire is recognized by its D shape. This type of connector is becoming less popular on desktops and laptops. It's commonly associated with attaching peripheral devices such as digital cameras and printers rather than being used as network connections.



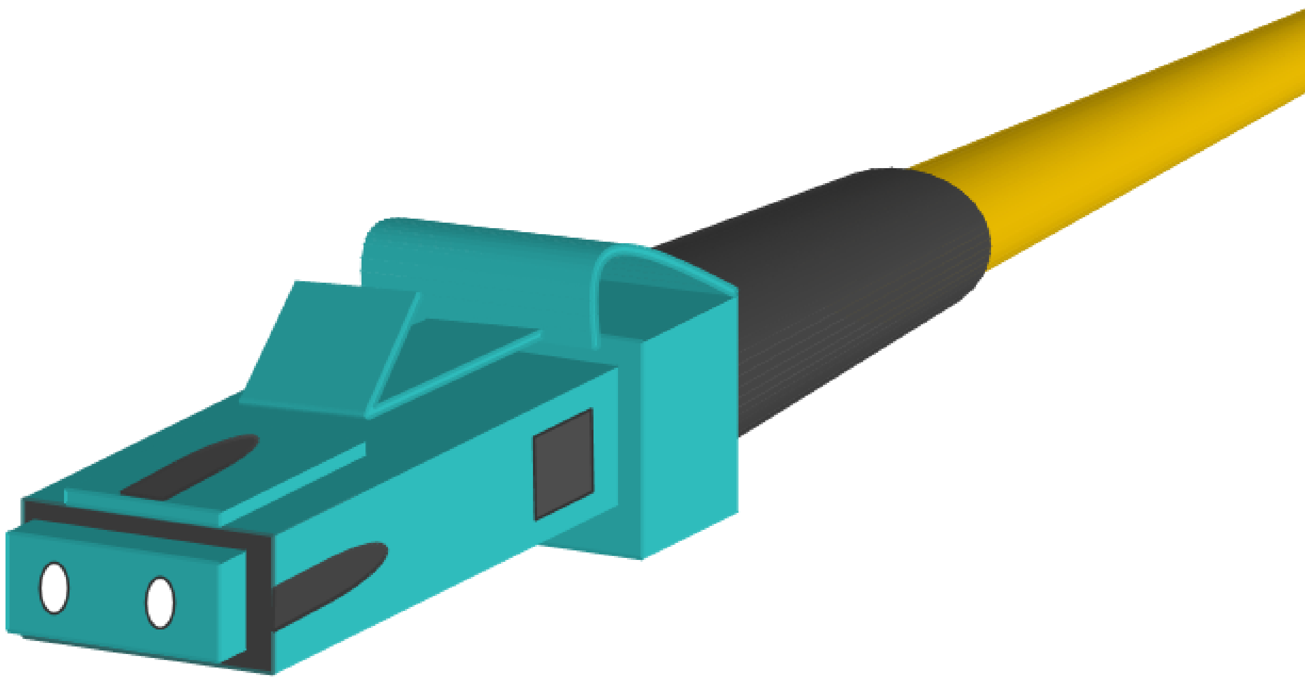
Firewire



USB

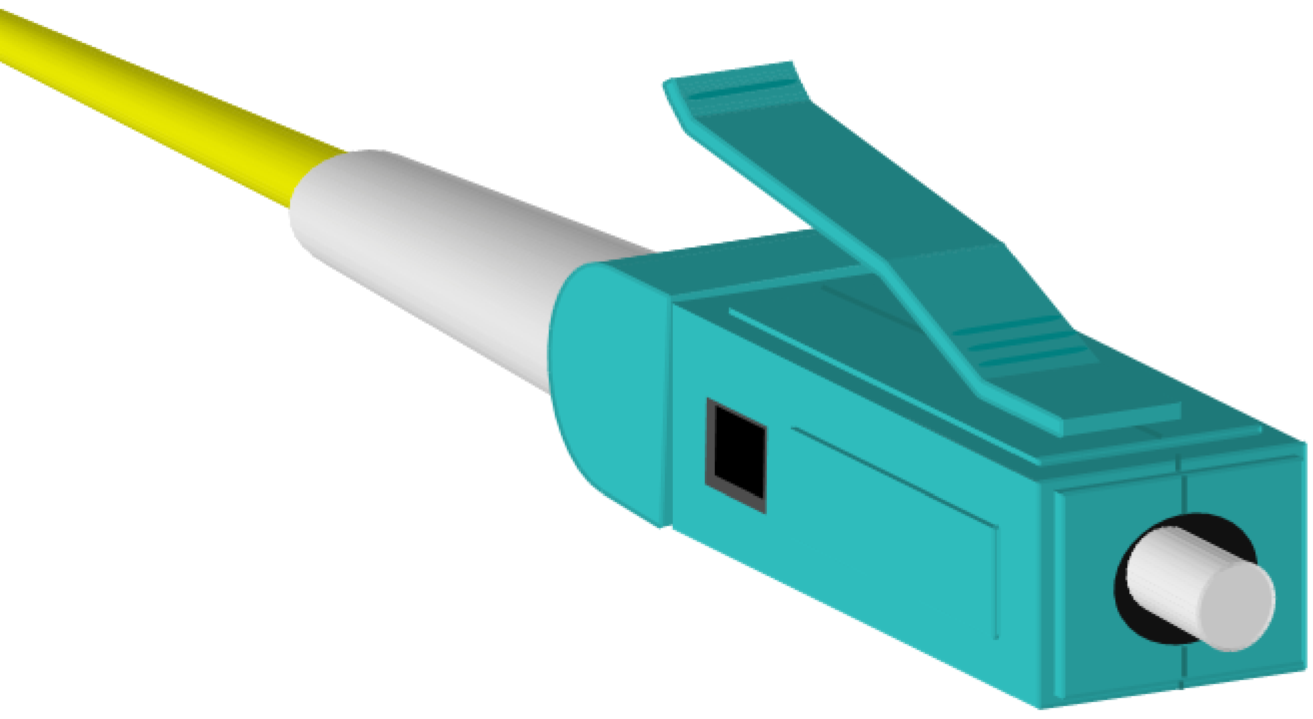
This is a **USB** connector. The USB is very common on desktops and laptops. Many manufacturers make wireless network cards that plug into a USB port. The USB has two different connector types: type A and type B.

Now we're getting into fiber optic connectors. This connector is called the **MTRJ** which stands for **mechanical transfer registered jack**. And this is a fiber optic cable connector that uses a latched push-pull connection. It has a small form factor used for high packed density.



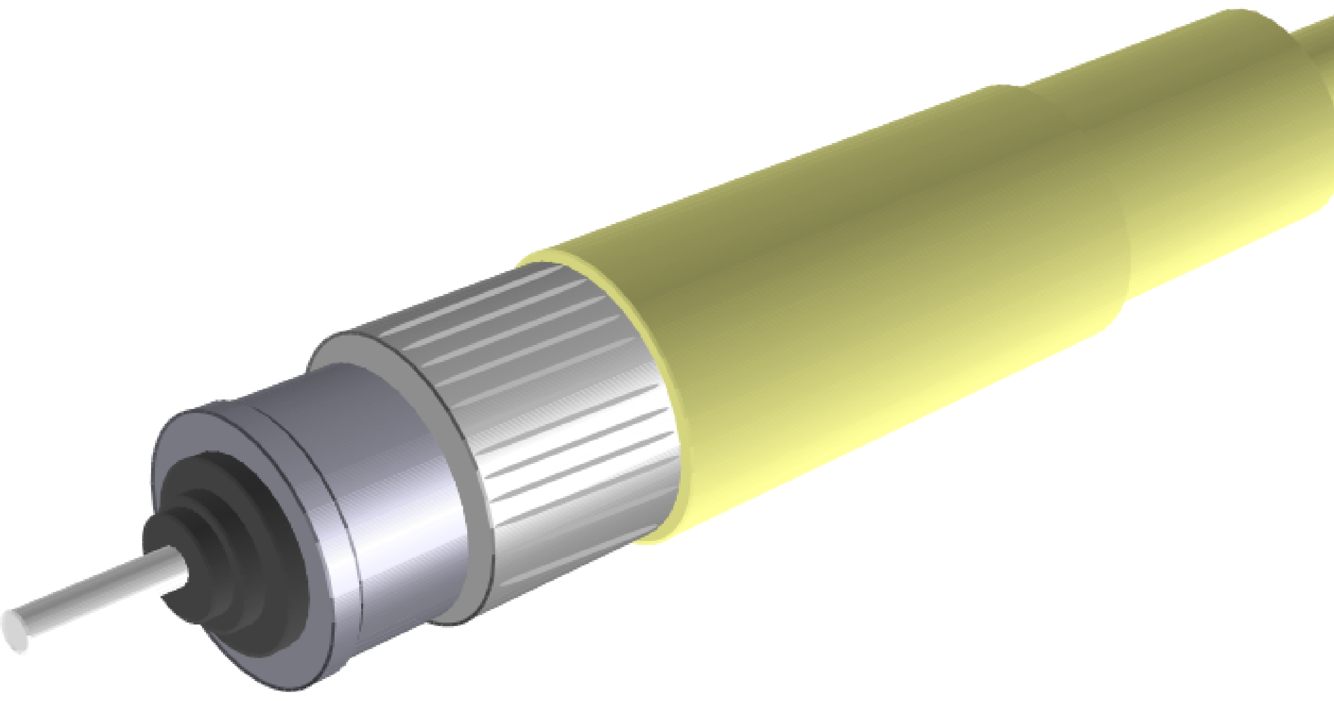
MTRJ

Our next connector is called the **LC** or **local connector**. This is a fiber optic connector. It uses a jack similar to the RJ-45. This type of connector is commonly used between floors in a building.

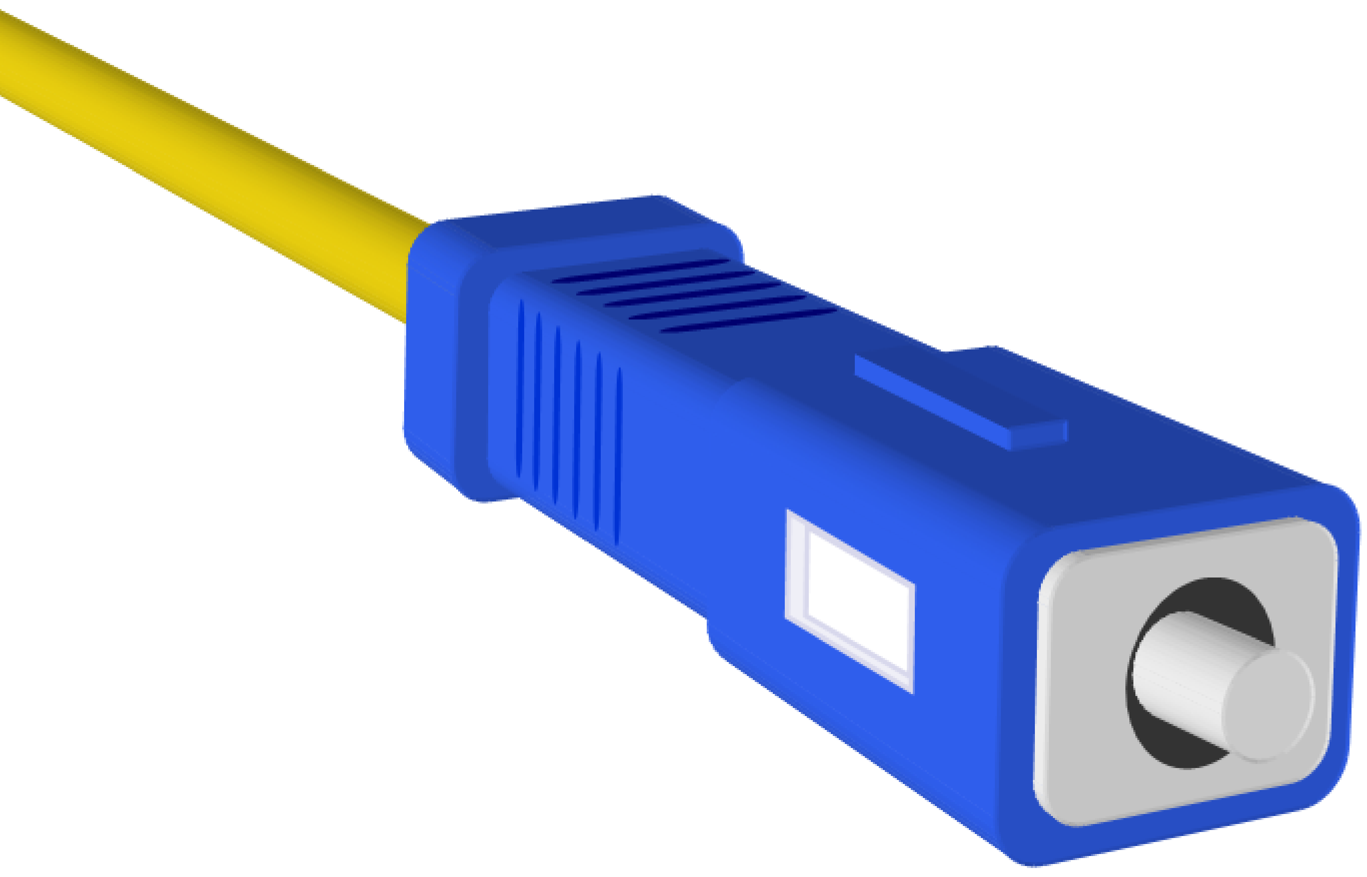


LC

This fiber optic connector is called the **ST** or **straight tip**. This uses a half-twist bayonet type of lock and is commonly used with single mode fiber optic cable.



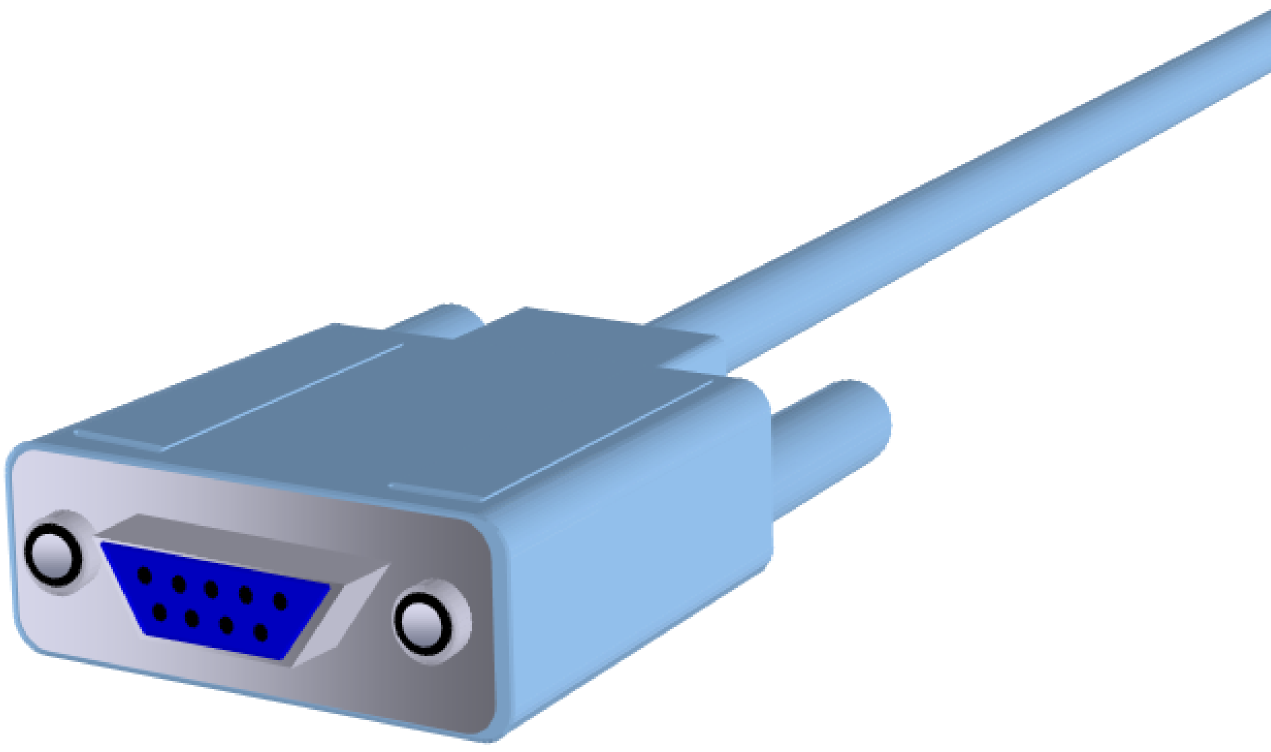
ST



SC

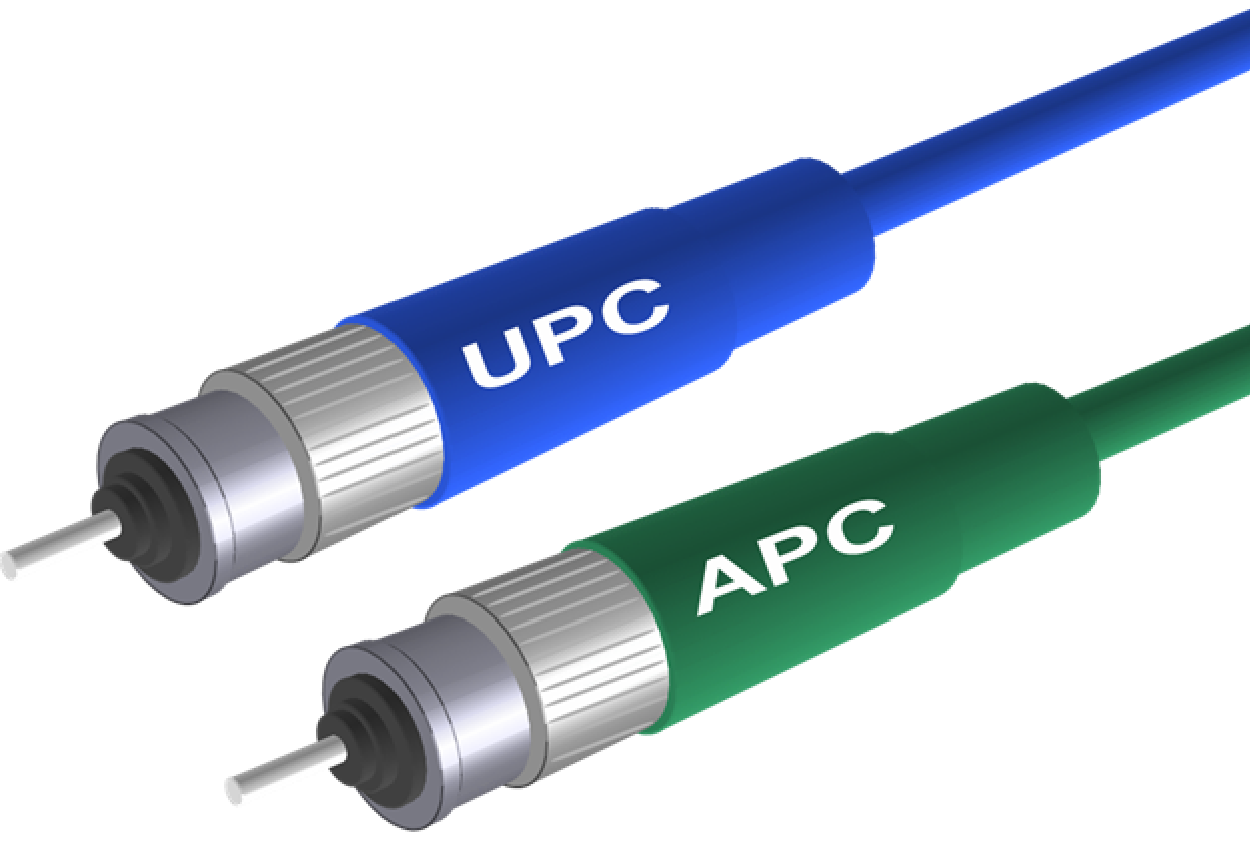
Our last fiber optic connector is called the **SC** or **standard connector**. This uses a push-pull connector similar to audio and video plugs.  And like the LC connector, this is also commonly used between floors in a building.

The term serial refers to sending data one bit at a time.  Serial cables are cables that carry serial data transmission.  The most common form of serial cables uses the **RS-232** standard, which uses the common D connectors, such as the **DB-9** and **DB-25**.



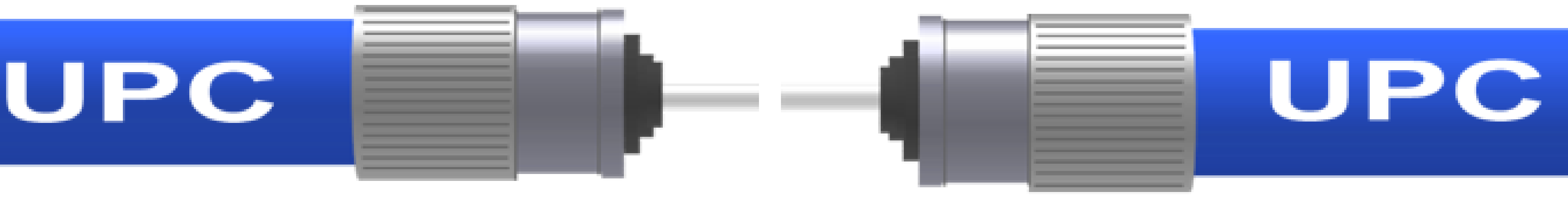
RS-232

Now we're going to talk about the difference between **UPC** and **APC** connectors.  And as examples, we're going to use a group of ST fiber connectors  equipped with UPC and APC connectors.

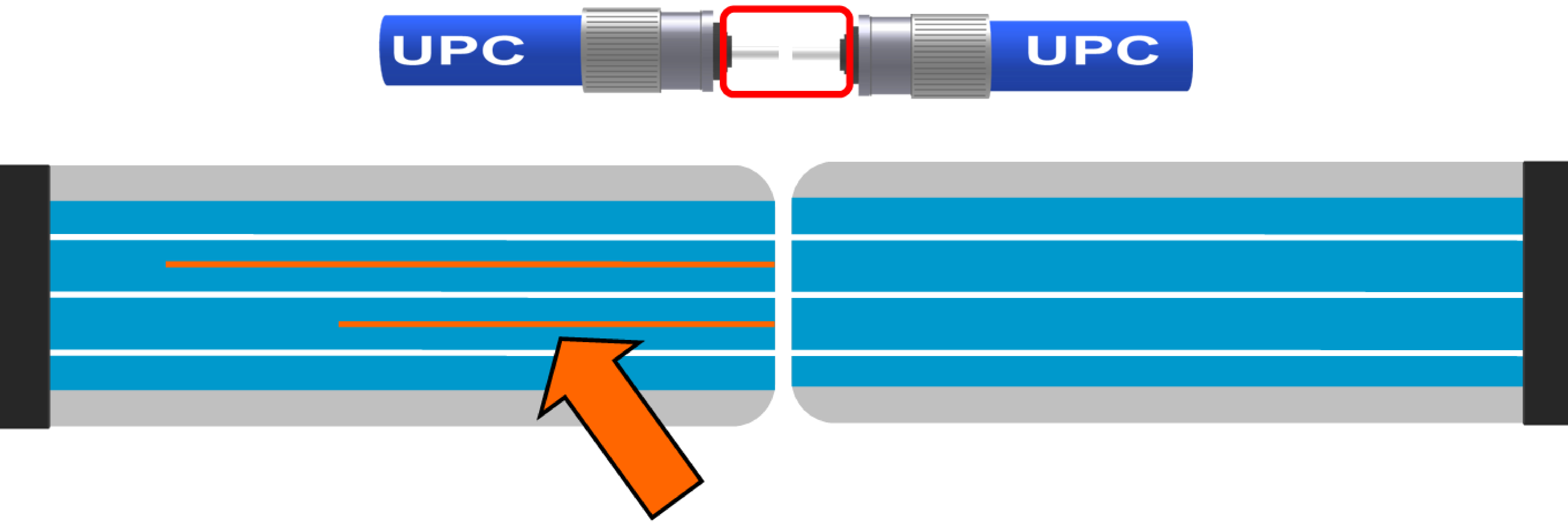


ST connectors with UPC and APC tips.

When fiber optic connectors make a connection to each other, the point at which the connection is made is not perfect because of the small imperfections of the flat surfaces.

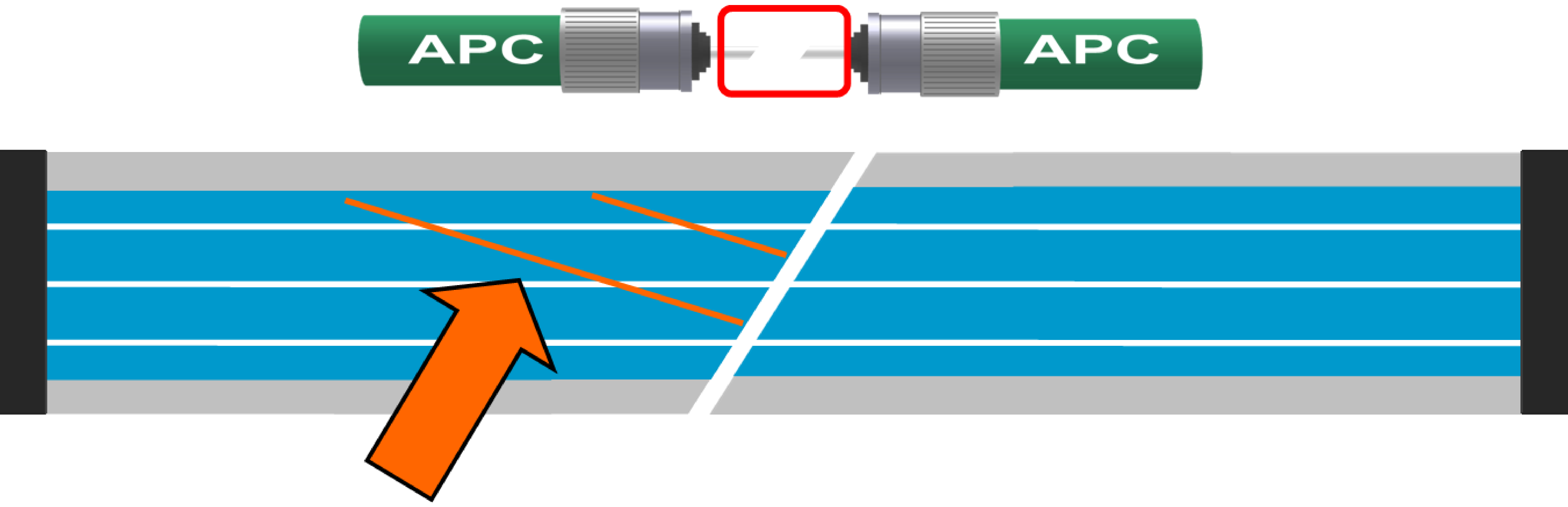


So what happens, is at the point where the connectors join, light is transmitted from one connector to the other connector.  But at the point where light passes to the other connector, the light will reflect back in the opposite direction towards the light source.  When this happens, there is signal loss.  This is what happens in UPC connectors.  The light is reflected directly back.



**With UPC connectors, the light is reflected directly back towards the light source.**

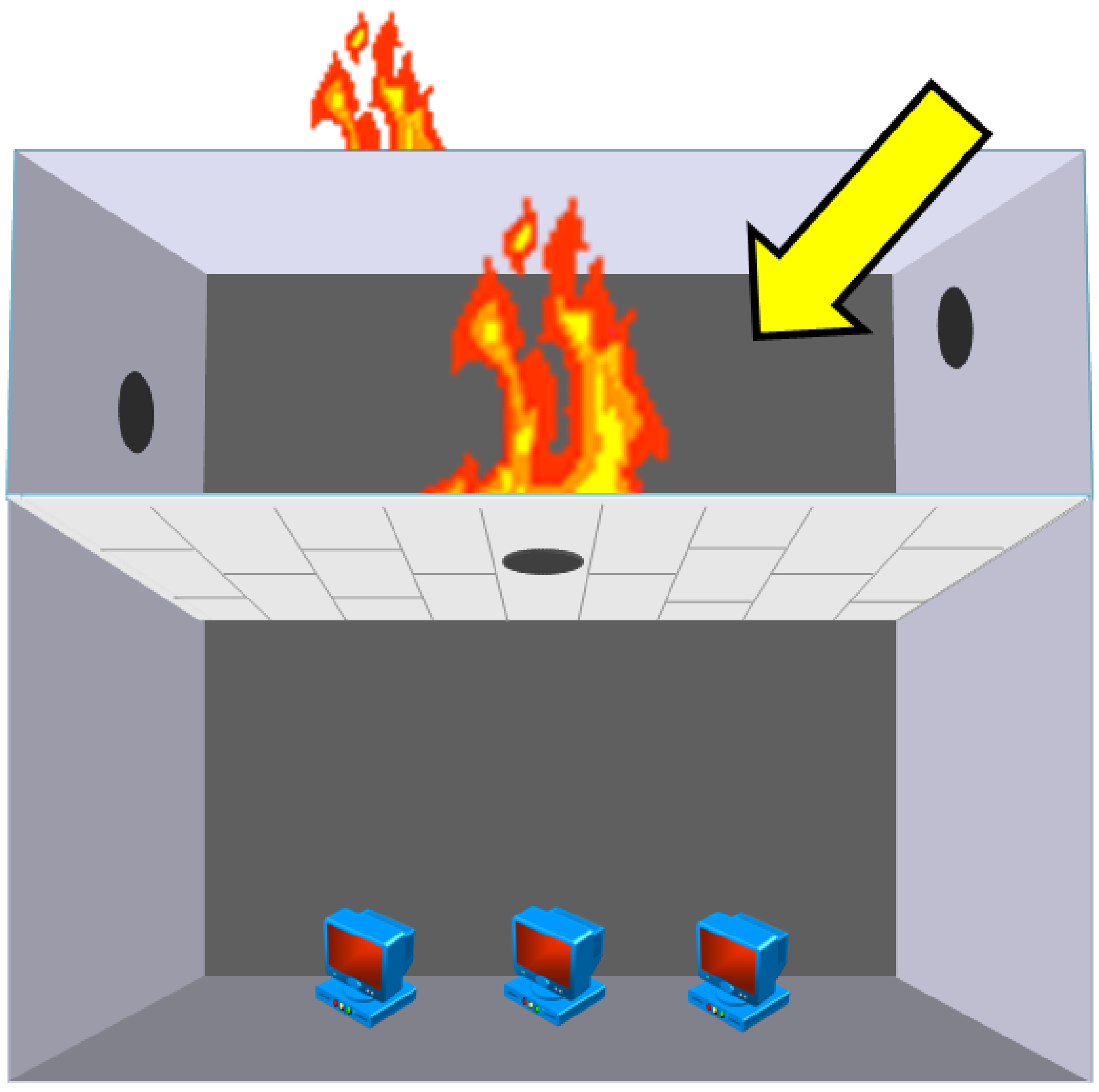
So as technology progressed, a new connector was developed to decrease the signal loss.  This new connector is called the APC connector.  The difference between the UPC and the APC is the angle of the tip where the connection is made.  With the UPC, the light reflects back towards the light source. But with the APC, with its angled connection, the light doesn't reflect back towards the light source, it reflects back at an angle into the wall of the cable.  And as a result, this greatly reduces the signal loss.



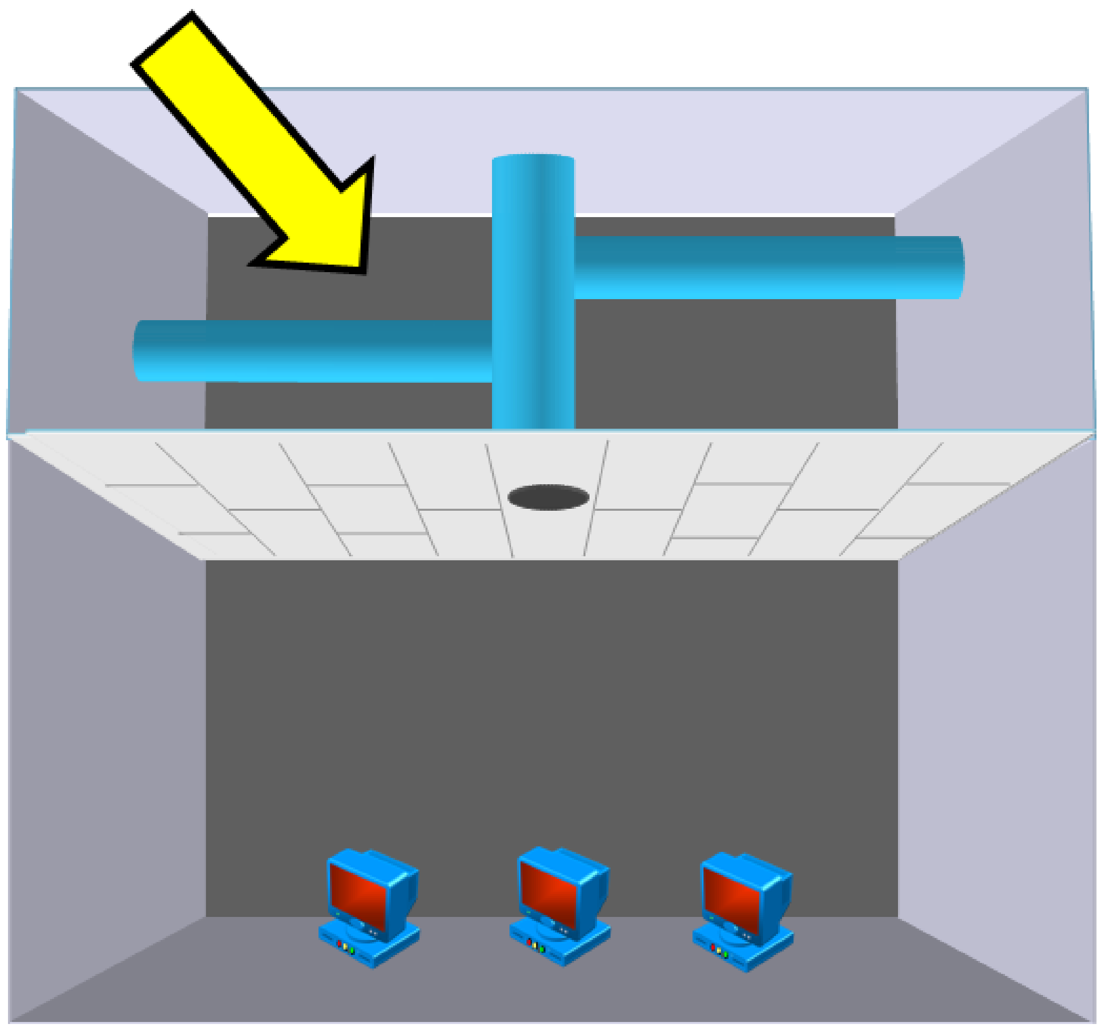
**With APC connectors, the light is reflected back at an angle into the wall of the cable.**

## Cable Standards

The term **plenum** refers to a space in a building where there is open airflow circulation.  This is usually between the drop ceiling and the structural ceiling. Buildings that don't have plenum spaces have air ducts encapsulating the airflow.  So as a result, buildings that have plenum spaces, where there is adequate open airflow, are more prone to fires than buildings that don't have plenum spaces.  Therefore, cables that run

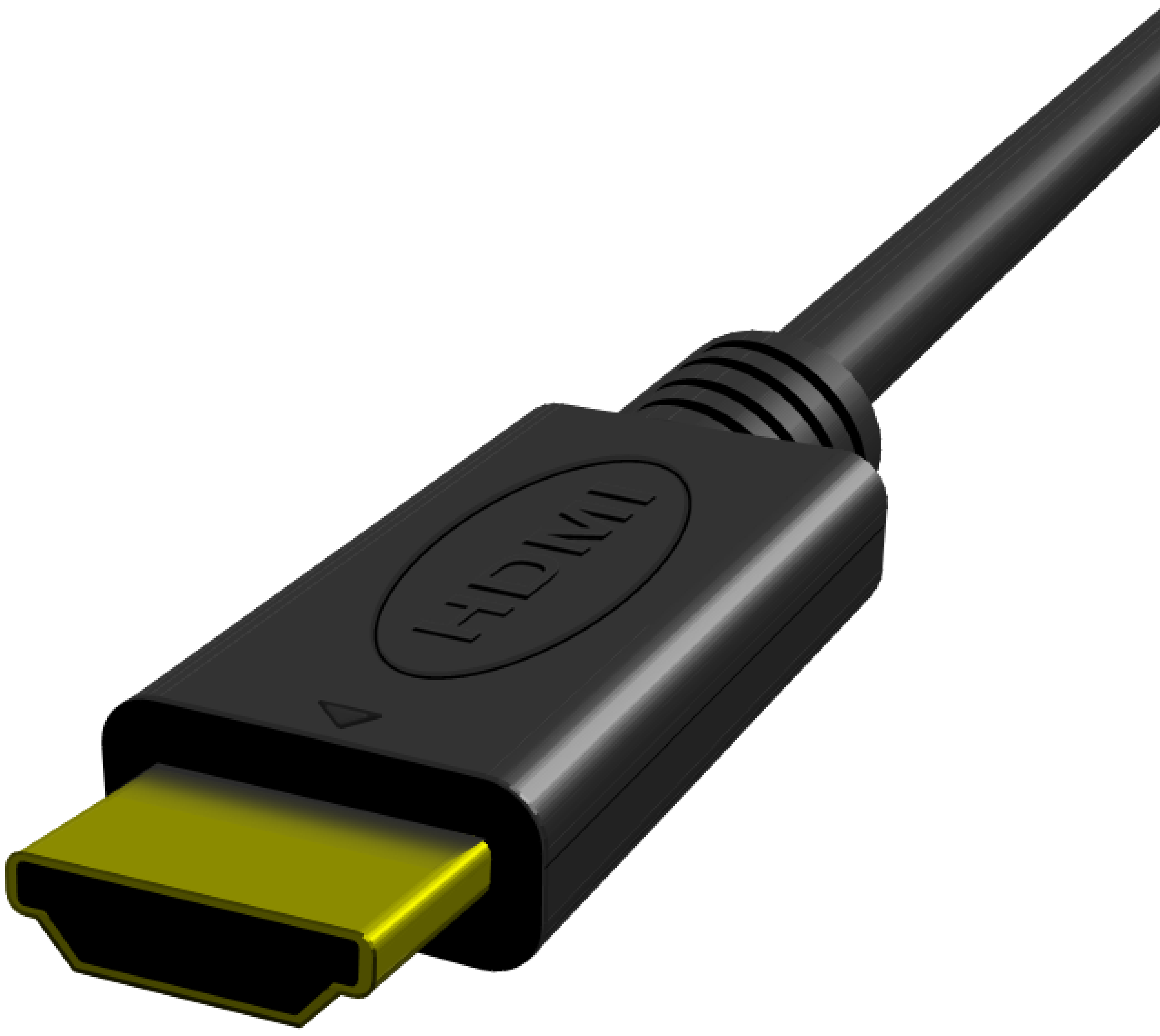


**Plenum**
**Open air flow (dangerous)**



**Non Plenum**
**Encapsulated air flow (safer)**

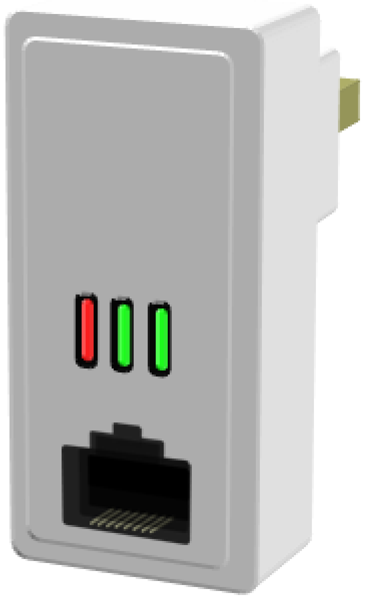
through plenum spaces must meet certain requirements. First, they must be more fire-resistant, and secondly, they must not produce any toxic fumes if they are burned.



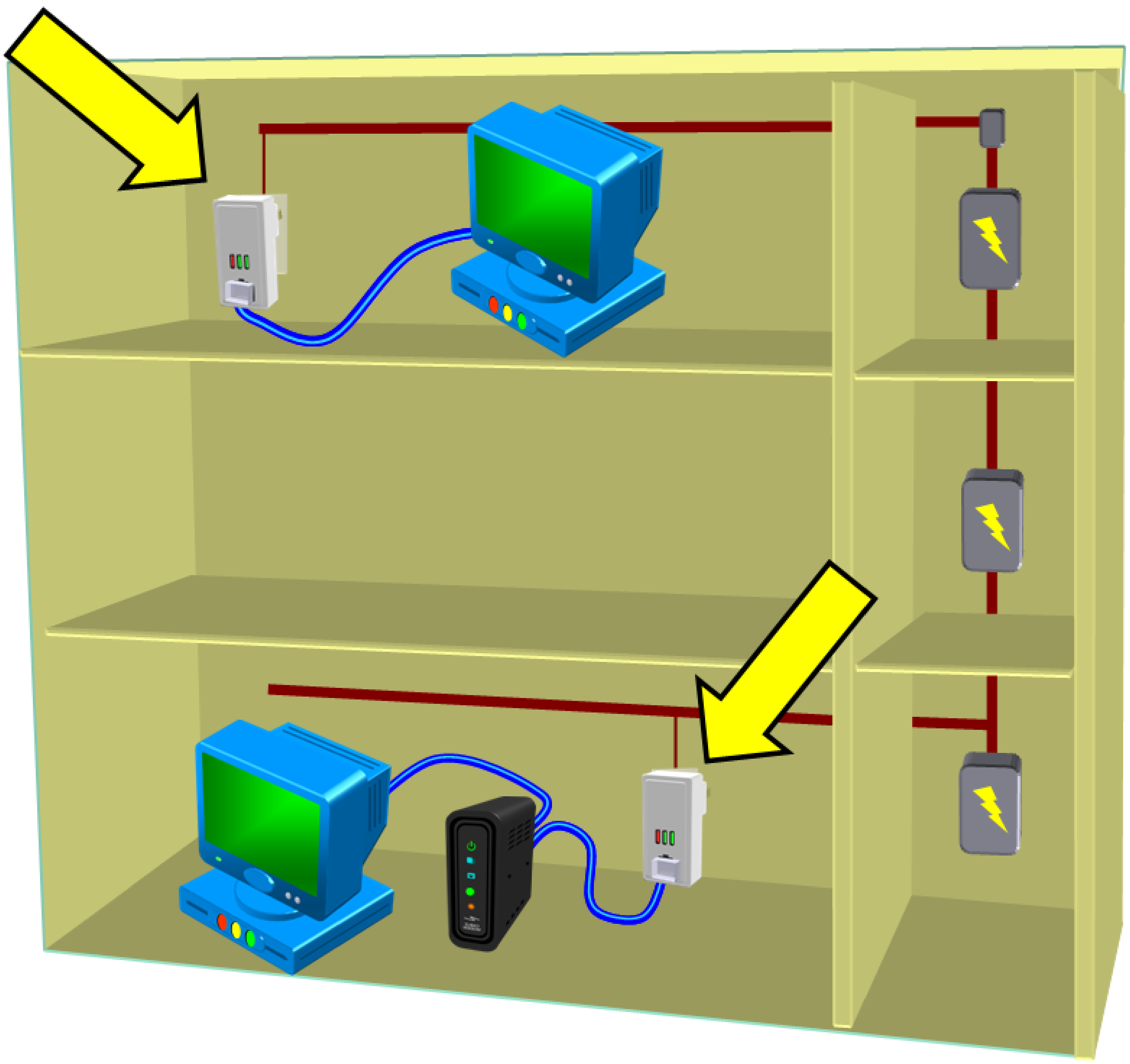
**HDMI cable**

Another standard is called **Ethernet over HDMI**. The HDMI 1.4 specification adds another channel to an HDMI cable for data, which will have the capability of network communication. So the connected devices that use this feature will have the ability to send and receive data at 100 Mbit/s Ethernet. So, in addition to video and audio on a single cable, the HDMI cable will have another ability of Ethernet networking.

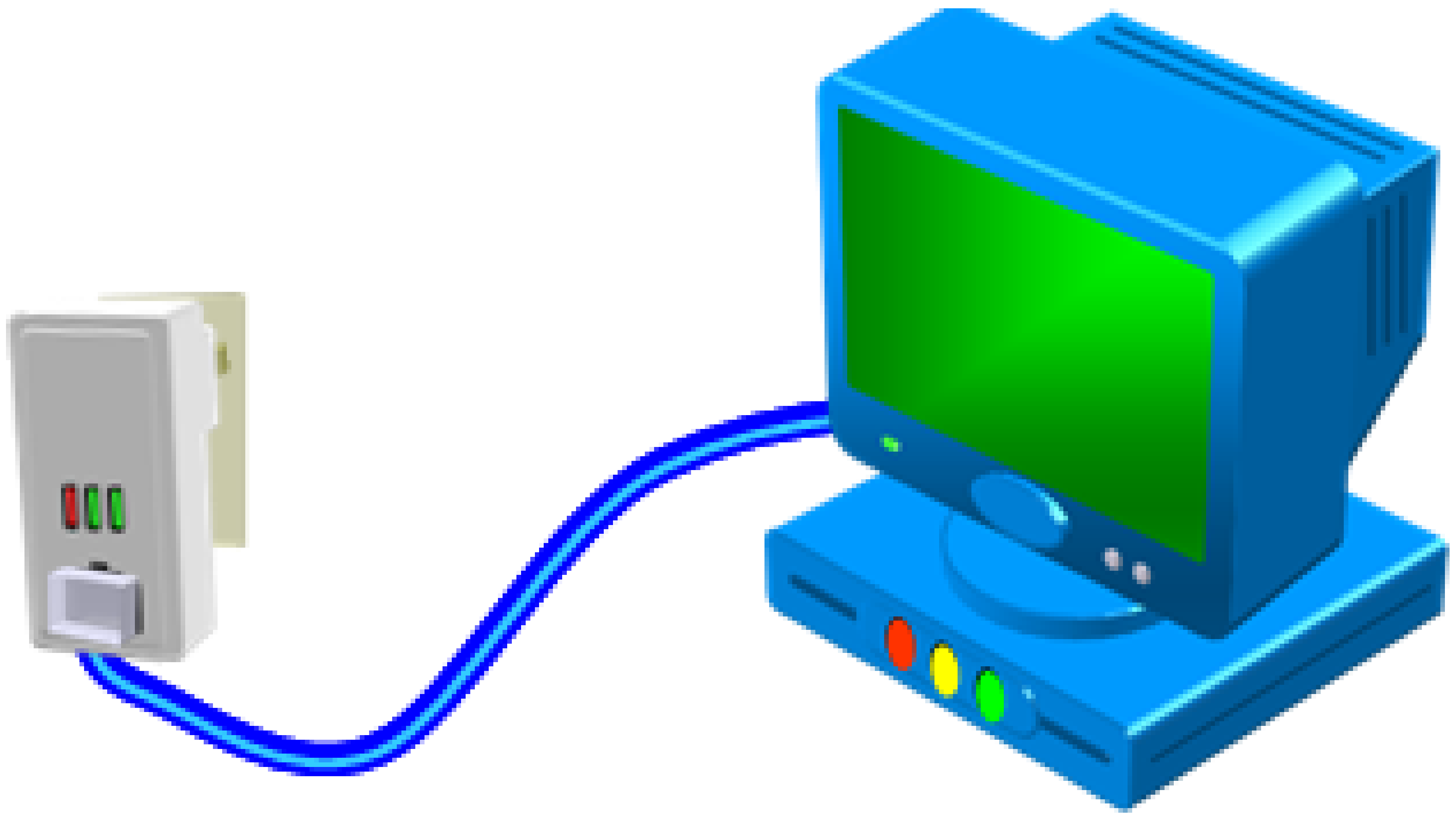
Sometimes there might be cases in your home or office where you wanted a certain computer in a certain part of the building to be able to access the internet or to be networked.  But for whatever reason, network cabling or Wi-Fi just wasn't an option in that part of the building.  Maybe because of difficulties in the structure of the building, interference, or whatever.  So a new technology gave the ability to network using the existing electrical system of the building.  **Ethernet over powerline** gives the ability of Ethernet networking over power.



**Powerline network adapter**

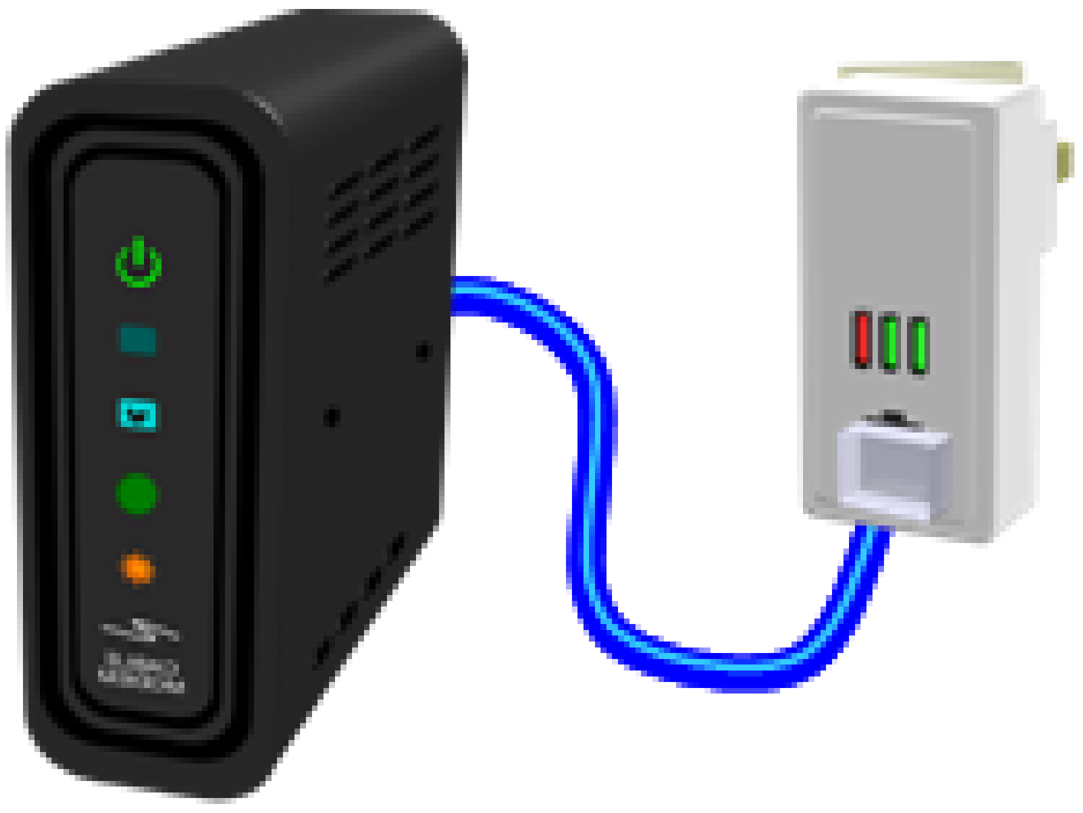


So, for example, let's say you needed a computer to be able to access the internet.  But for some reason, you can't get any network cables or any Wi-Fi signal to reach that computer.  So, in this case, we're going to use Ethernet over power.  So we're going to need a couple of powerline adapters.  These powerline adapters plug directly into a power outlet and they have a built-in Ethernet port for an RJ-45 connector.



**Computer plugged into a powerline network adapter.**

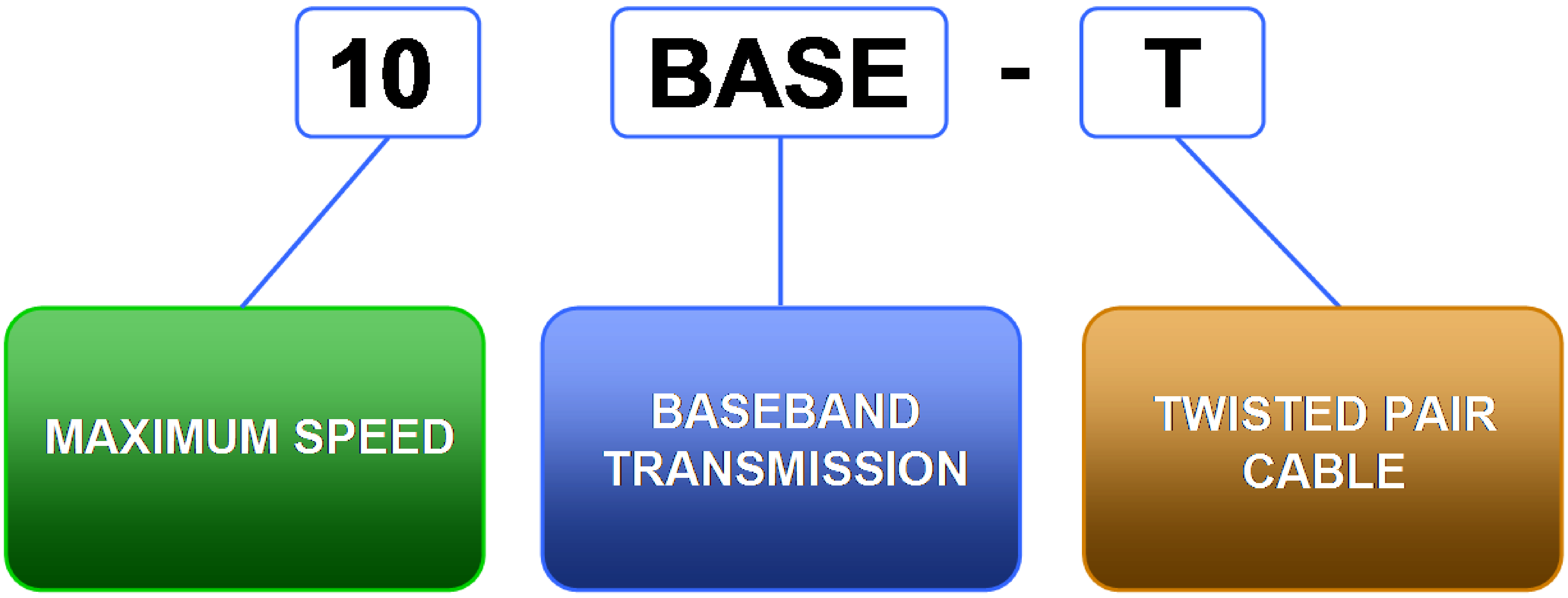
So one adapter plugs into a power outlet next to the computer that you want to have internet access (above).  Then you would connect a network cable from the adapter to the computer.  Then the other adapter plugs into the power outlet next to the modem or router (below) and then connected to a network cable.



**Modem plugged into a powerline network adapter.**

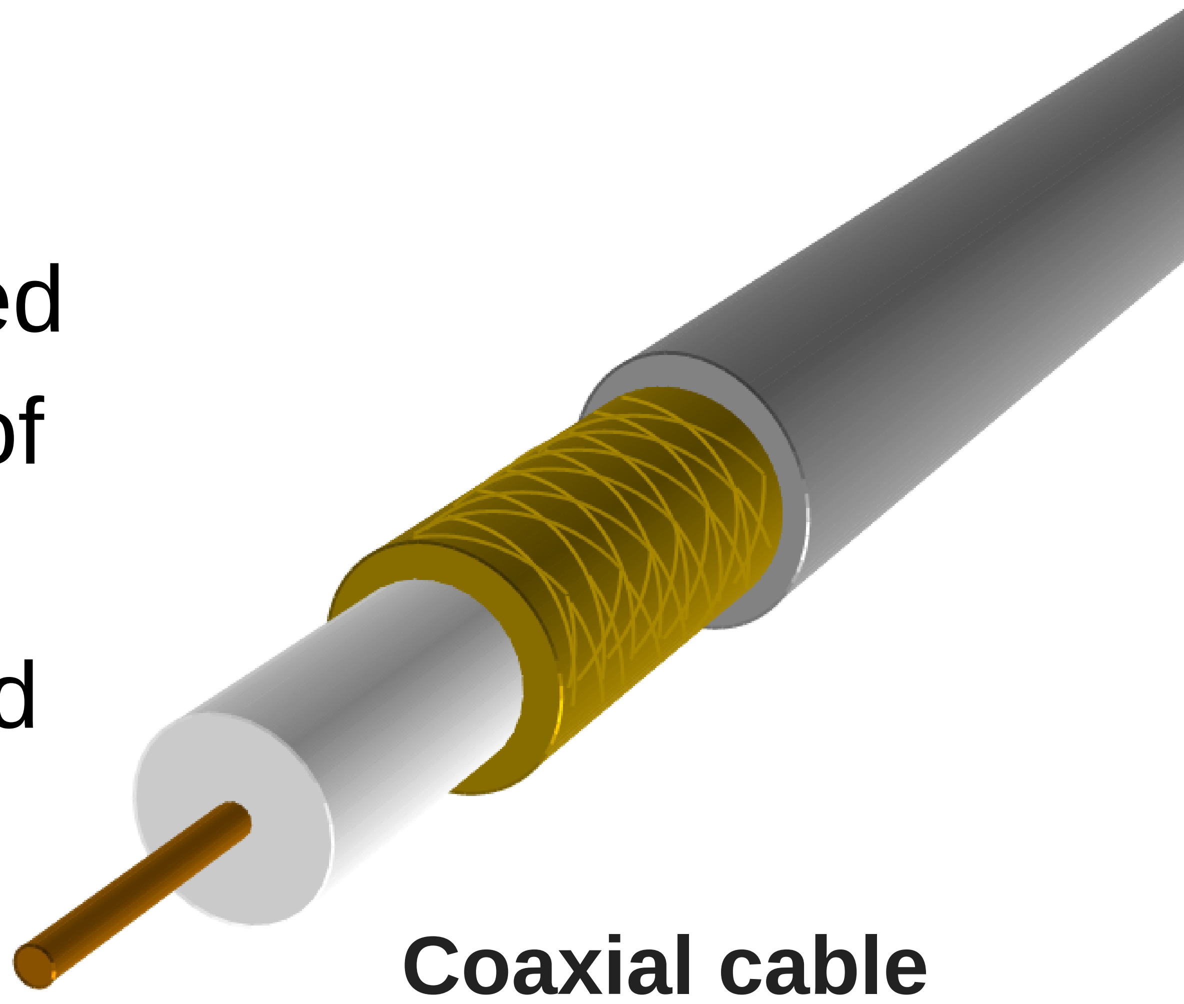
So now Ethernet data will use the building's electrical wiring to deliver networking data to the other powerline adapter so that the computer can access the internet.

Today there are many different cable standards that are used on networks. These cables are categorized and named according to their speed, type, and media.



Above is an example of a cable labeled **10 BASE-T**. 10 stands for the maximum speed of this cable. The maximum speed of this cable is 10 Mbit/s. BASE stands for baseband transmission. T stands for twisted pair cable.

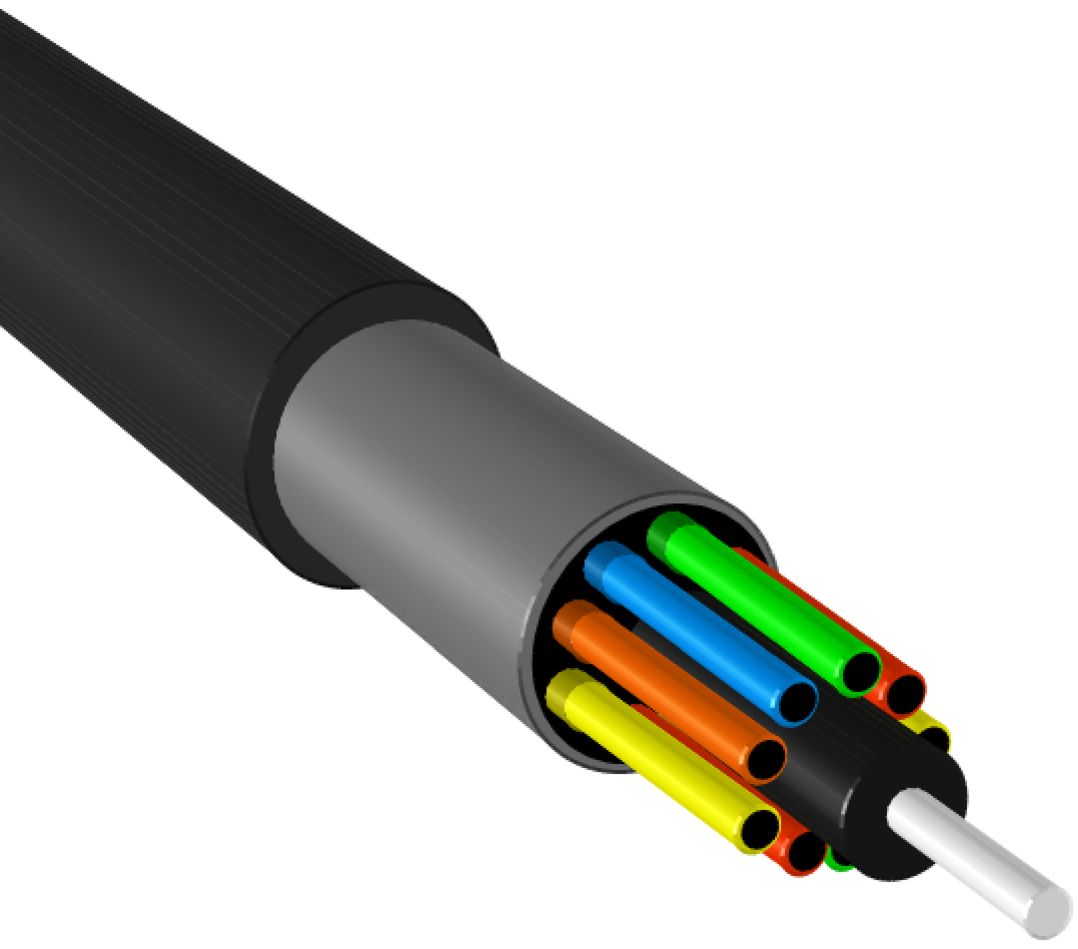
**10 BASE-2**, which is also referred to as thin Ethernet, is a version of Ethernet that uses coaxial cable as opposed to unshielded twisted pair cable. It has a maximum speed of 10 Mbit/s and has a maximum length of 200 meters.



Coaxial cable

Other cable standards include **100 BASE-T**. This, as its name states, has a speed of 100 Mbit/s, which is 10 times faster than 10 BASE-T. This uses category 5 UTP cable or higher, and it also has a maximum length of 100 meters. 100 BASE-T is also known as fast Ethernet.

**Unshielded twisted pair (UTP) cable**

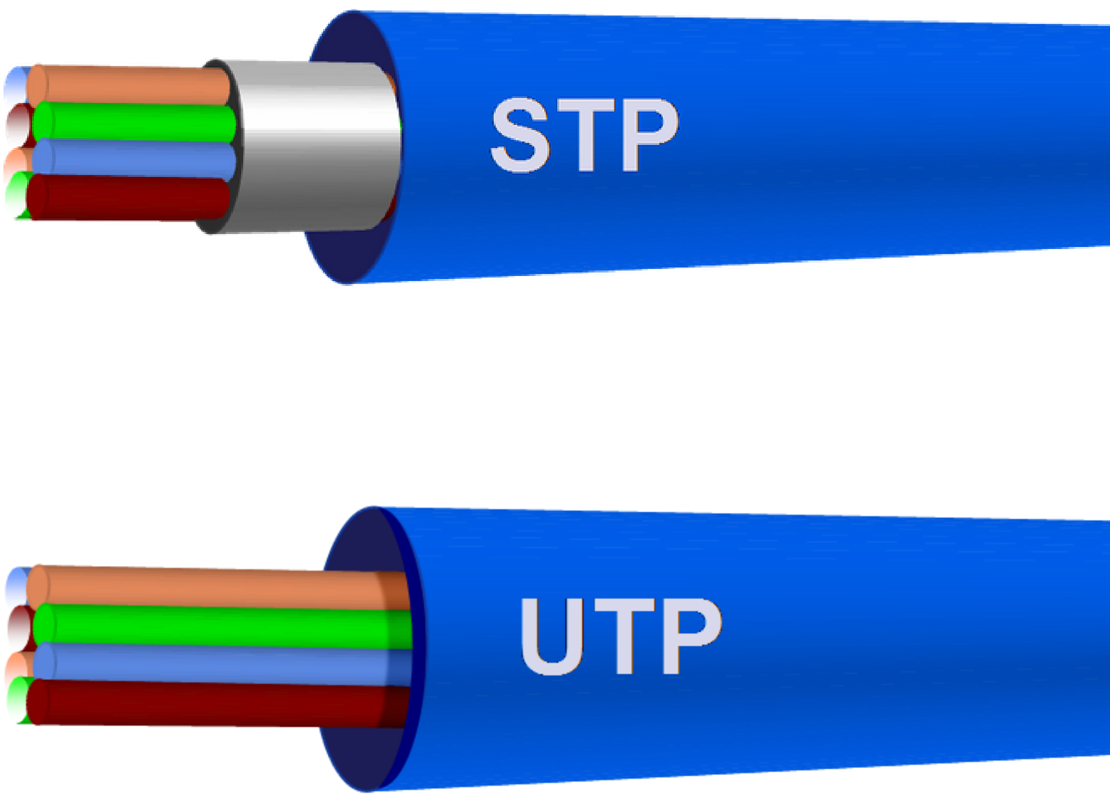


**Fiber-optic cable**

**100 BASE-FX**, just like 100 BASE-T, has a speed of 100 Mbit/s. But the difference is, that FX uses fiber-optic cable, whereas 100 BASE-T uses copper cabling. It has a maximum length of 400 meters in half duplex mode, and 2 kilometers in full duplex mode.

Moving on to the gigabit standards, there is **1000 BASE-T**. This has a speed of 1,000 Mbit/s. It uses category 5 UTP cabling or higher and has a maximum length of 100 meters. **1000 BASE-TX** is similar to 1000 BASE-T with the exception that it was supposed to be an easier set up because it only uses two unidirectional pairs of wires for communication, whereas 1000 BASE-T uses four bidirectional wires. But 1000 BASE-TX never caught on and is known as a failure in commercial implementation.

Moving on to the 10 gigabit standard, there is **10G BASE-T**. This has a speed of 10 Gbit/s.  It was developed in 2006 and it uses both shielded and unshielded twisted pair cabling. It has a maximum distance of 100 meters when using category 6a cabling.  Or, if it's using category 6, it has a maximum length of 55 meters.



**10G BASE-T uses both STP and UTP cables.**

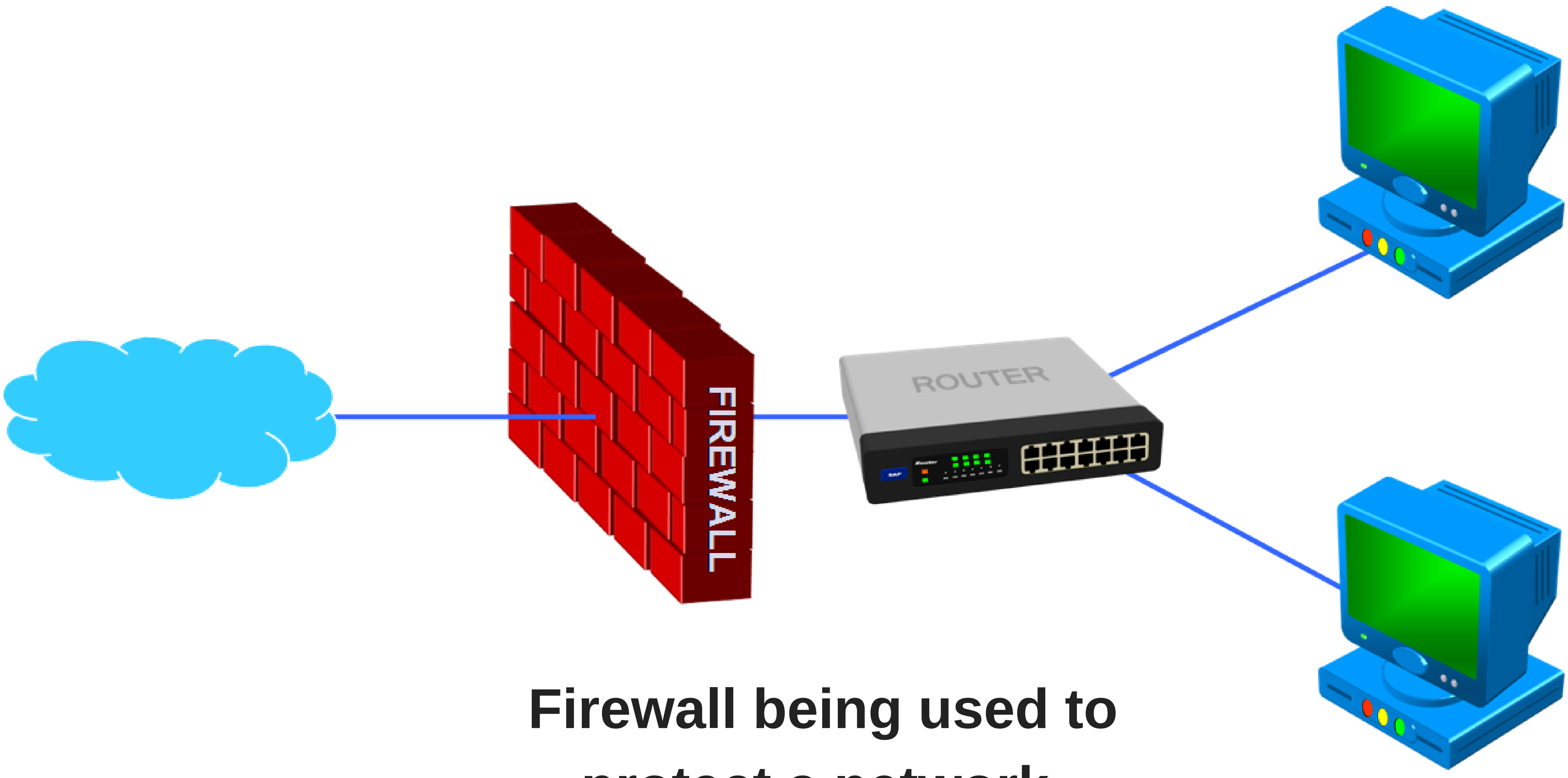
Next is **10G BASE-SR**.  The SR stands for short-range.  This is a commonly used with multi-mode fiber optics, and has a maximum length of 300 meters.

**10G BASE-ER** or extended reach has a range of 40 kilometers using single-mode fiber optics.

**10G BASE-SW** has the same specification as 10G BASE-SR but is specifically used to operate over SONET, which stands for synchronous optical networks.

# Firewalls

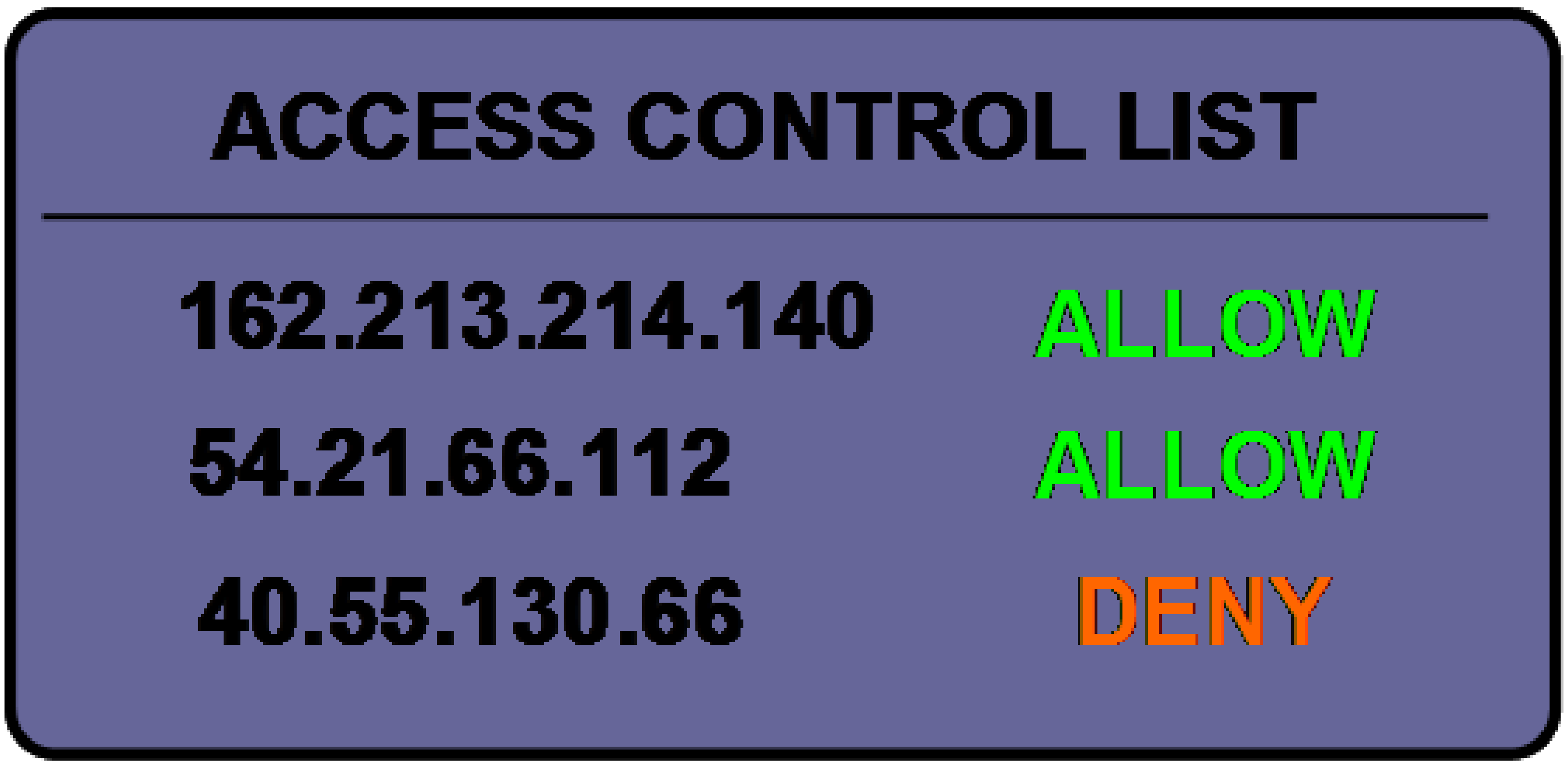
A **firewall** can be either software or hardware.  It is a system that is designed to prevent unauthorized access from entering a private network by filtering the information that comes in from the internet.  It blocks unwanted traffic and permits wanted traffic.



**Firewall being used to protect a network.**

So basically it filters the incoming network data packets and determines by its access rules if it is allowed to enter the network.  In today's high-tech world, a firewall is essential to every business to keep their network safe.

One way that a firewall controls the flow of traffic coming into and out of a network is through its **access control list** or ACL.  The ACL is a list of rules on what can access the network.  It either allows or denies permission.  So as an example, here we have a very simplified ACL with a list of IP addresses that have been allowed or denied on this firewall.

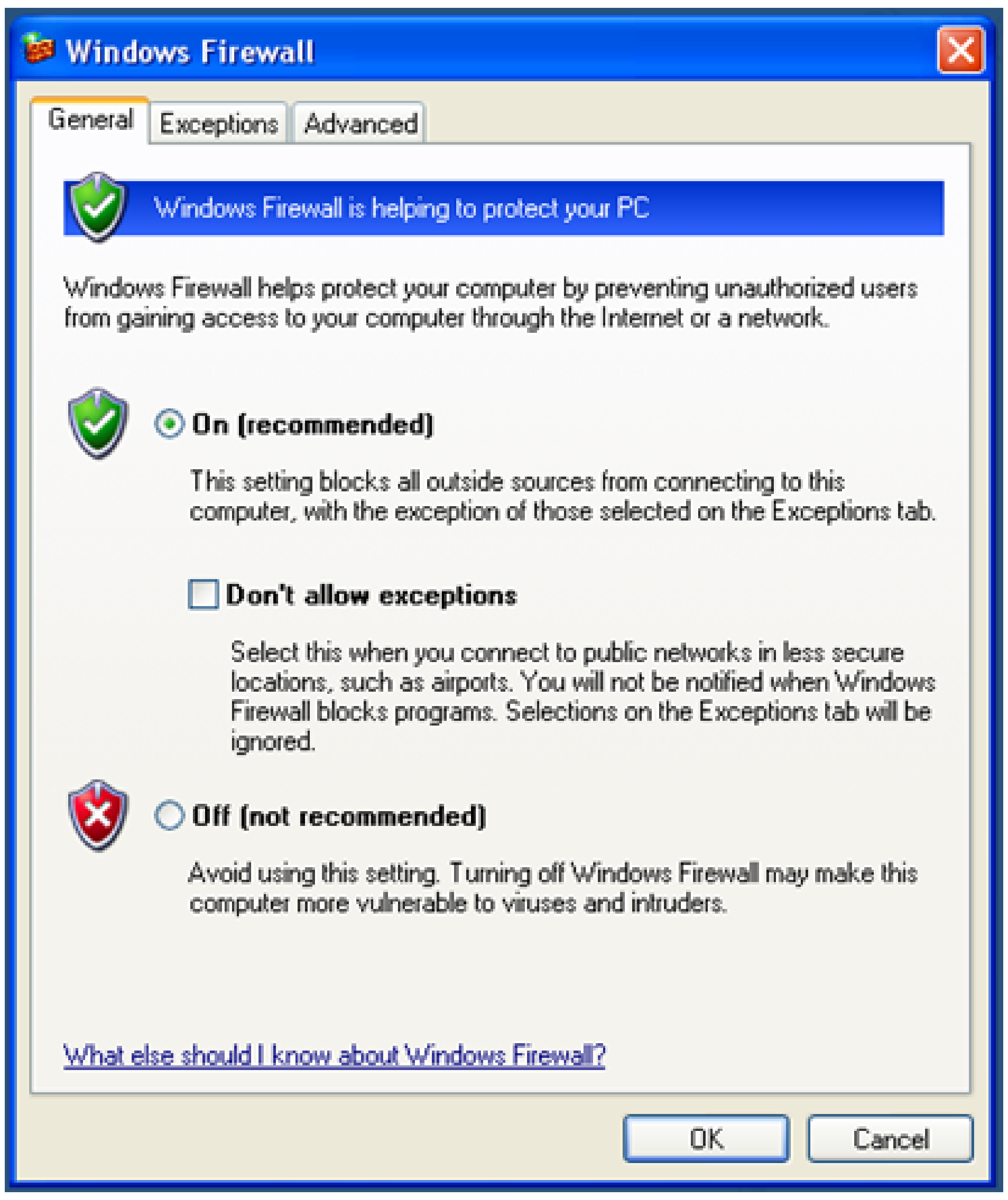


ACCESS CONTROL LIST

| | |
|---|---|
| 162.213.214.140 | ALLOW |
| 54.21.66.112 | ALLOW |
| 40.55.130.66 | DENY |

So, if data from the (40.55.130.66) IP address tried to get into this network, the firewall will deny it because of the rules that are set in the ACL.  But the other IP addresses are granted access because the ACL allows them.

Most firewalls come with a default rule of **implicit deny**.  What this basically means is that the firewall will only allow traffic to enter the network that the ACL specifically says that it will allow.   So as an example, if your ACL only has one rule, and let's say that the rule has allowed port number 80, which is web pages. Then that means that you'll be allowed to access web pages on your network, but nothing else.  You won't be able to use any FTP, https, or incoming POP or IMAP email because the firewall has implicitly denied those ports.  So the only way to access those services, is you have to specifically allow them by granting them access in the ACL.



Windows Firewall is helping to protect your PC

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

● On (recommended)

This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.

□ Don't allow exceptions

Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.

○ Off (not recommended)

Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

What else should I know about Windows Firewall?

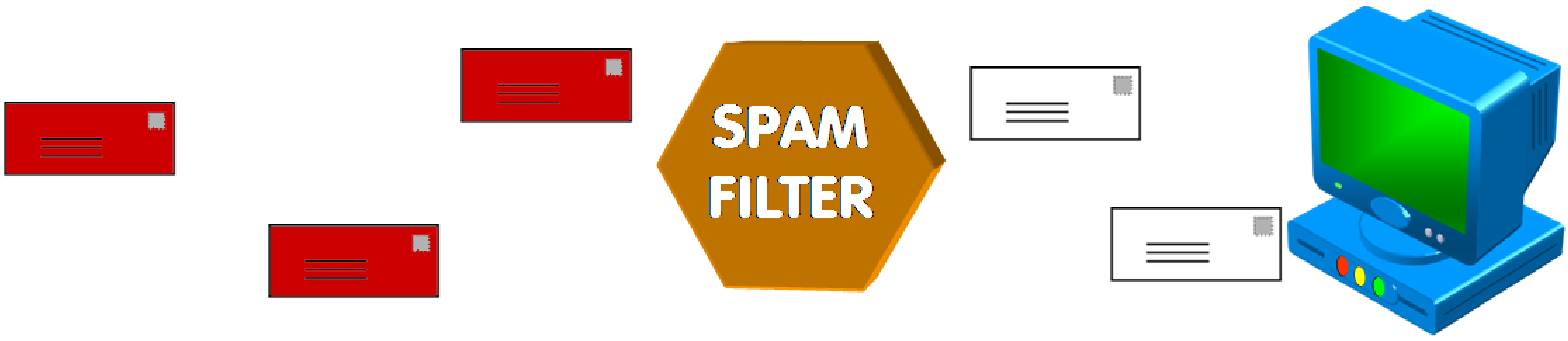
**Host-based firewall on a Microsoft OS.**

Firewalls come in different types. One type is called a **host-based firewall**, and this is a software firewall. This is the kind of firewall that is installed on a computer and it protects that computer only and nothing else. For example, later versions of Microsoft operating systems come pre-packaged with a host-baseball firewall. You can turn the firewall on or off if you want, and you can also create exceptions to the firewall based on the application name on the exceptions tab. And of course, you can always purchase a third party firewall and install it on your computer.

Another type of firewall is called a **network-based firewall**. A network-based firewall is a combination of hardware and software, and it operates at the network layer. It is placed between a private network and the internet. But unlike a host-based firewall, where it only protects its own computer, a network-based firewall protects an entire network, and it does this through management rules that are applied to the entire network so that any harmful activity can be stopped before it reaches the computers.

Firewalls also inspect traffic in a couple of different ways.  One way is called **stateful**.  A stateful firewall monitors all the connections and data streams that are passing through and keeps a record of it.  It uses the connection information that comes from the applications and previous sessions, and factors that in when allowing or denying the flow of data packets.  It does a thorough job of protecting a network dynamically.  A **stateless** firewall, on the other hand, does not do a thorough job as a stateful firewall does.  A stateless firewall uses an access control list to allow or deny traffic.  It does not thoroughly inspect a data packet.  It only looks into the header portion of the data packet, and it does not keep a record of previous data packets.

**Content filtering** is a technology that is commonly used in email.  As its name implies, it filters data based on their content and not on the source.  This type of filter is commonly used to filter email spam.



**Content filtering is commonly used to filter email spam.**

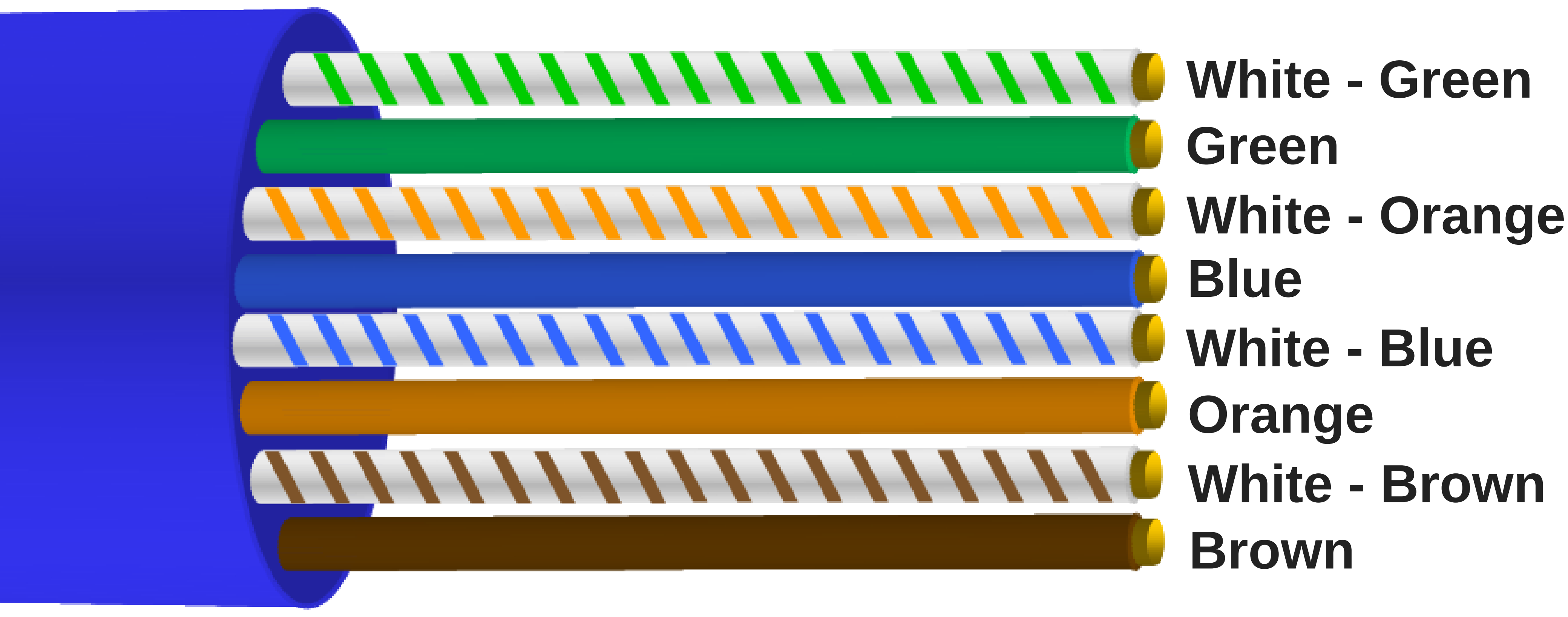
Another type of filter is called **signature identification**. This is used to detect viruses that have a well-known behavior pattern.  Certain viruses and malware have a common behavior, and firewalls that use signature identification are programmed to spot this behavior. Then once it's spotted, it takes action to block the intruder.

**Intrusion detection or prevention system** is a hardware tool that is typically placed between the internet and the firewall.  Its job is to alert and prevent a network from outside attacks.  These attacks include viruses, malware, and hackers who are trying to sabotage an internal network.  It monitors traffic flowing through a network, looking for suspicious patterns, and if it finds any, it alerts the network administrator of a pending danger.

# Wiring Standards

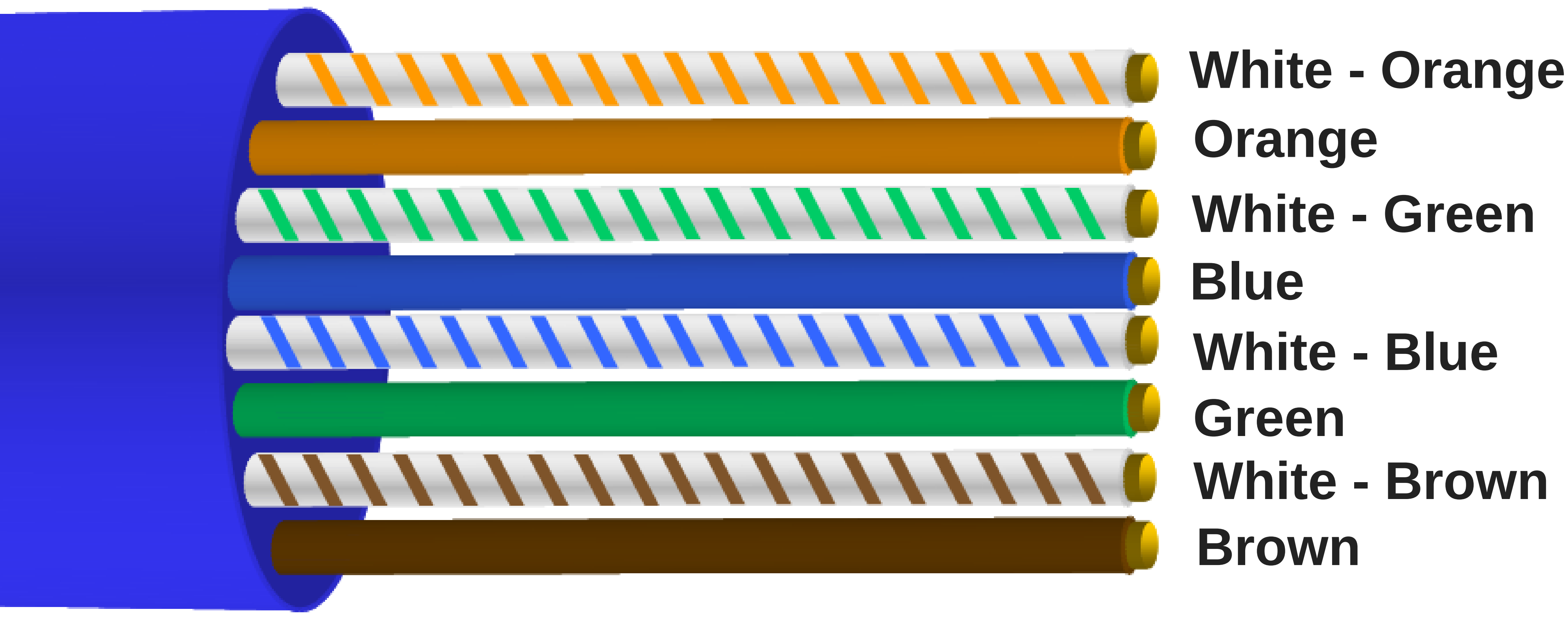
The terms **568A** and **568B**, refer to a set of wiring standards developed by TIA / EIA, which is also known as the Telecommunications Industry Association. These terms define the rules on how twisted pair cables should be wired to RJ-45 connectors.

The 568A standard is wired in this order: White/green, green, white/orange, blue, white/blue, orange, white/brown, and brown.



**568A wiring standard**

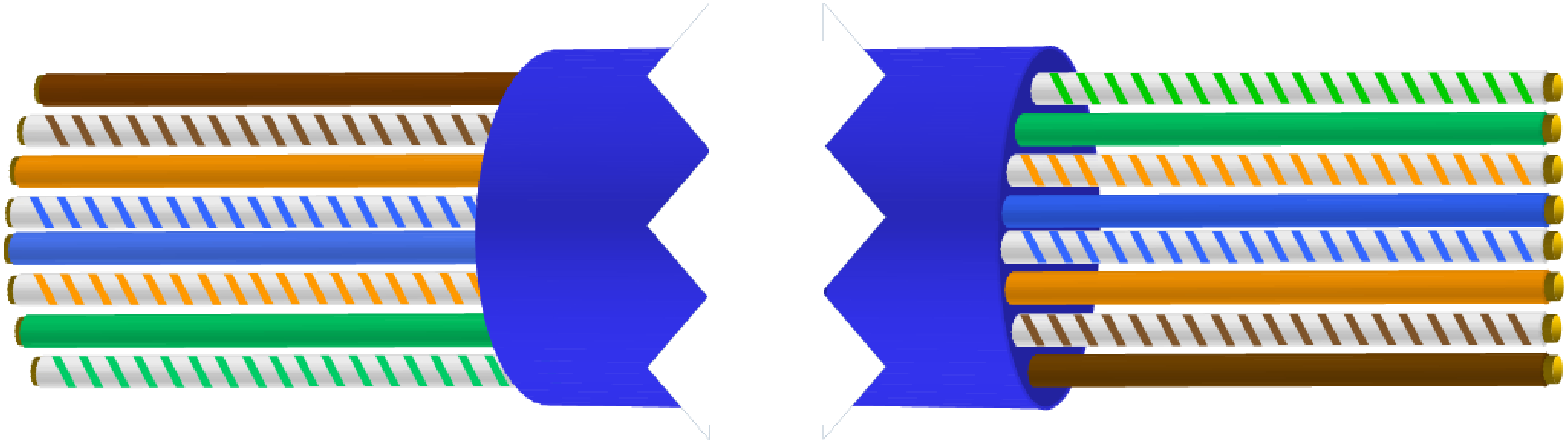
And the 568B standard is wired in the following order: white/orange, orange, white/green, blue, white/blue, green, white/brown, and brown.



**568B wiring standard**

There is no difference in the functionality as to which standard is used.

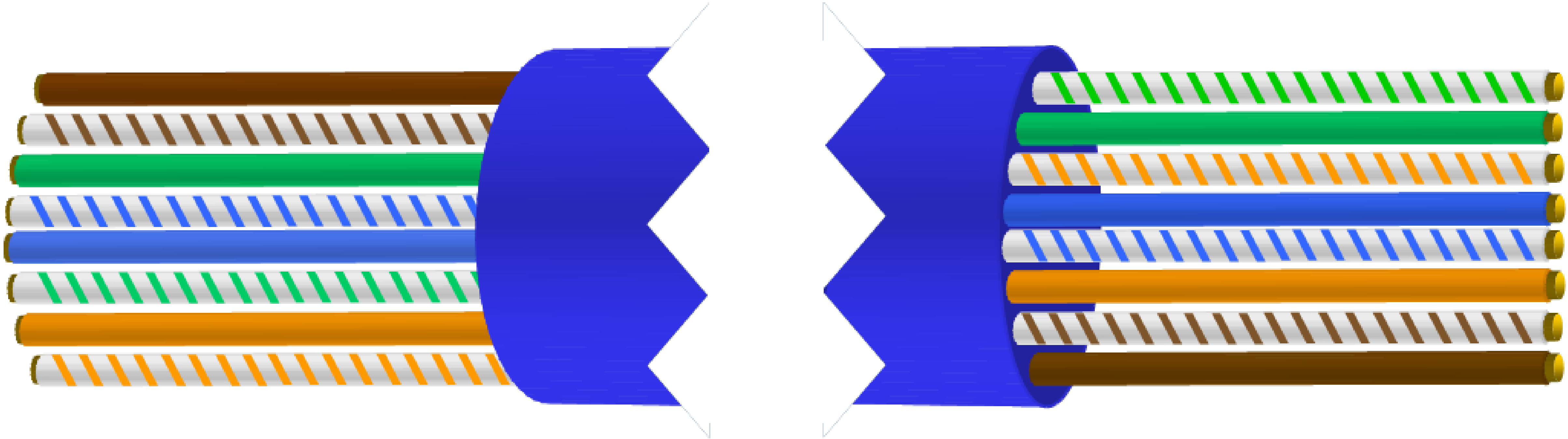
Whether you choose to use the A or B wiring standard, if both ends of the cable are wired using the same standard, then this is known as a **straight cable**.  For example, this cable is wired on both ends using the 568A standard.



**Straight cable**

A straight cable allows signals to pass straight through from end to end.  This is the most common type of cable and it's used to connect computers to hubs, switches, or modems.

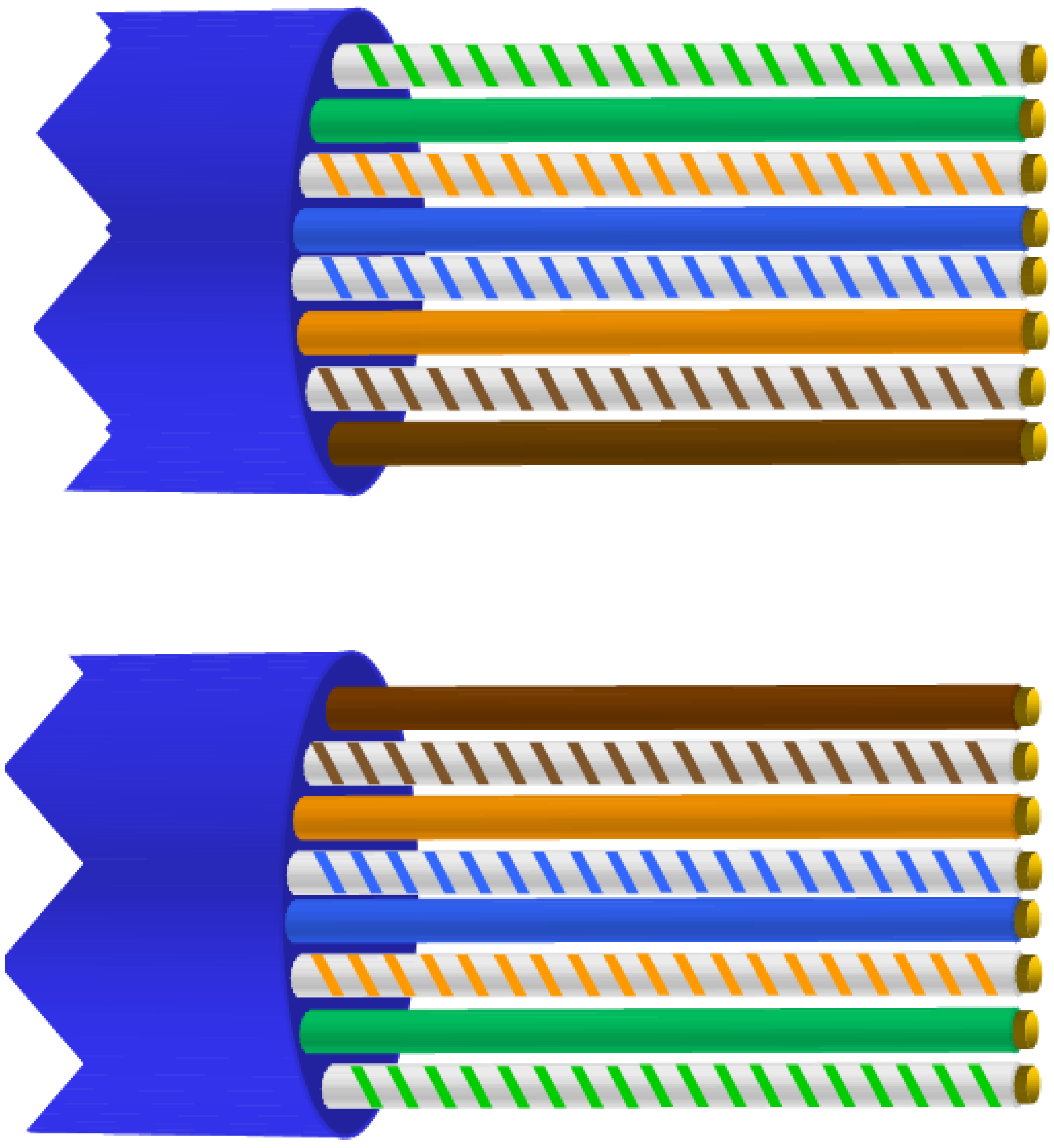
Another type of cable is called a **crossover**.  A crossover cable is created when both ends of the cable are wired using the two different standards.  For example, one end is wired using the A standard, and the other end is wired using the B standard.



**Crossover cable**

Crossover cables are used to connect two similar devices together.  For example, you can use a crossover cable to connect two computers directly to each other without using a hub or switch.  They are also used to connect hubs or switches to each other.

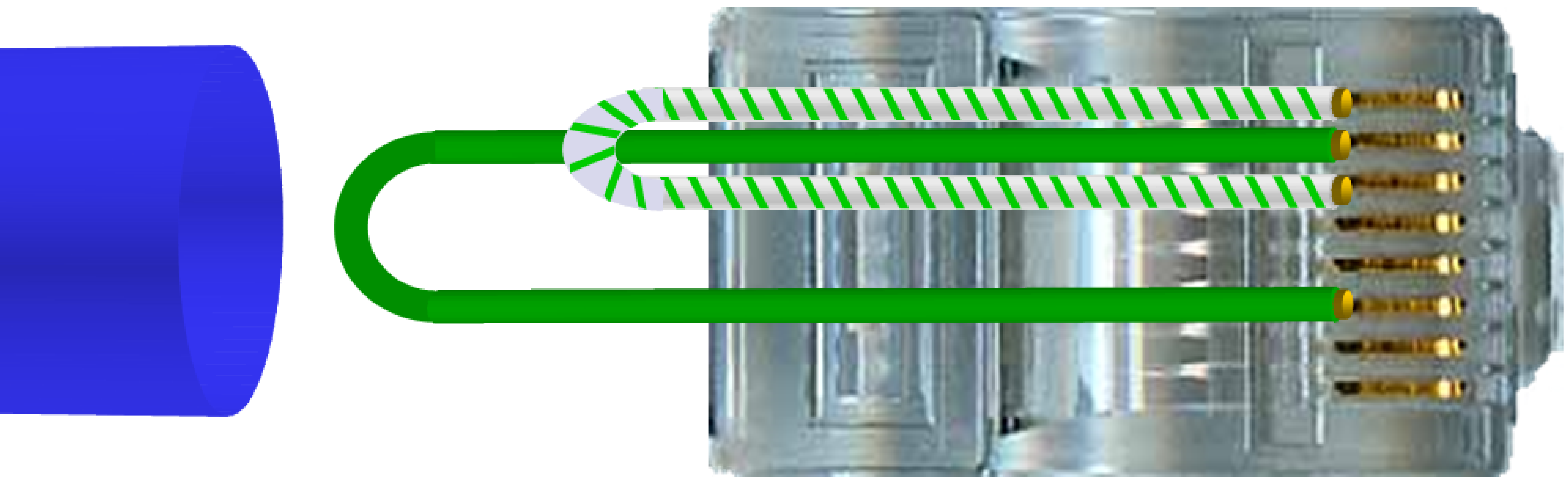
A **rollover cable** is created when both ends are wired completely opposite of each other.  These are used to connect a computer or a terminal to a router’s console port.



**Both ends are wired completely opposite from each other.**

**Rollover cable**

A **loopback cable** is used for testing purposes.  It’s to make a computer think that it's connected to a network. To make a loopback cable, you connect pin 1 to pin 3 and pin 2 to pin 6.



**Loopback cable**

# Media Types

Today there are several different categories of twisted pair cables that you're going to need to know for the exam.  The difference between these is the maximum speed that can handle without having any crosstalk (interference).  The numbers of these categories represent the tightness of the twists that are applied to the wires.  And you can see an illustration below of the categories and speeds of different twisted pair cables.

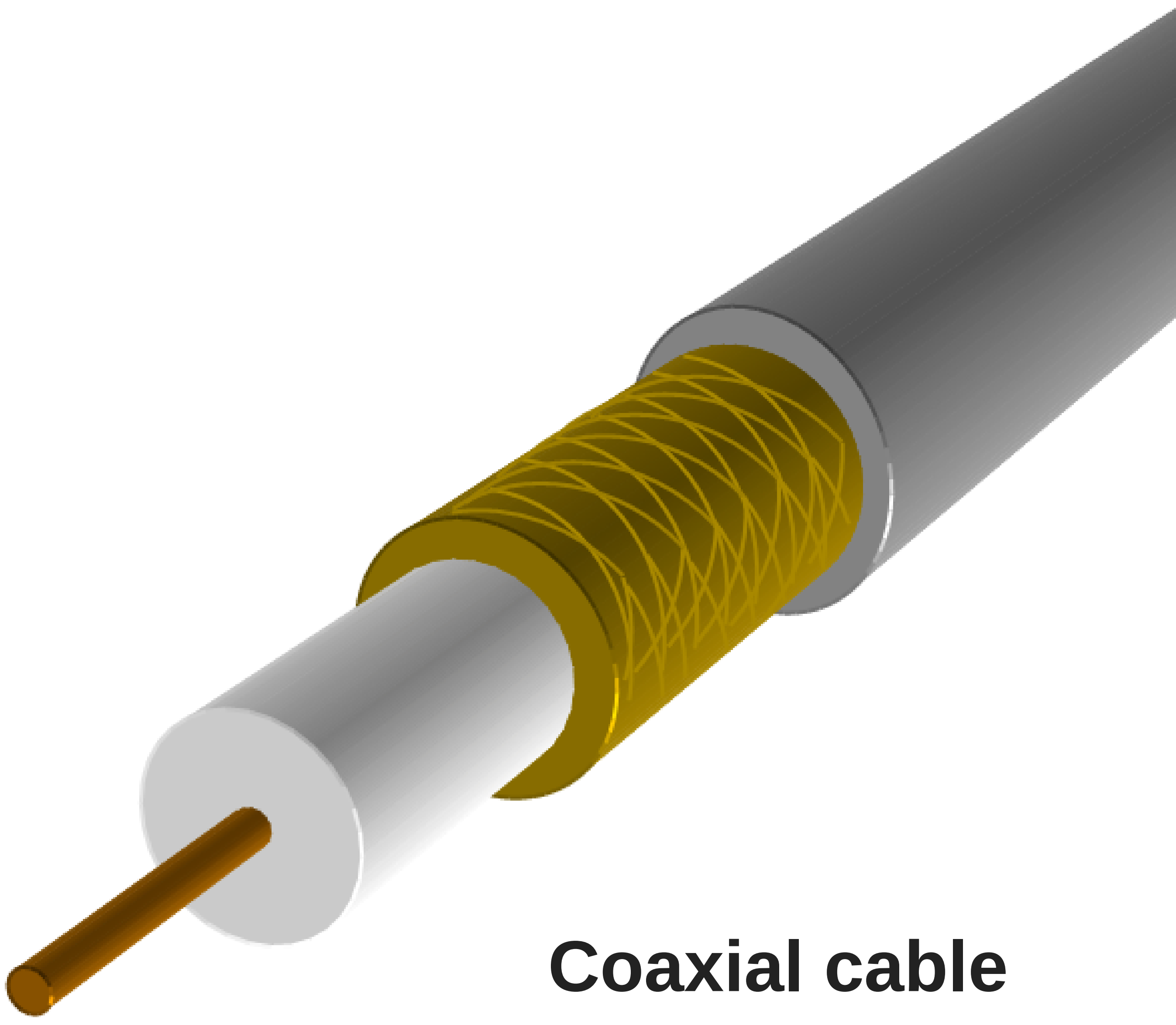
| CATEGORY | SPEED | |
|---|---|---|
| CATEGORY 3 | 10 Mbps | |
| CATEGORY 5 | 100 Mbps | |
| CATEGORY 5e | 1,000 Mbps | e = enhanced |
| CATEGORY 6 | 1,000 Mbps | 10,000 Mbps (cable length under 100 meters) |
| CATEGORY 6a | 10,000 Mbps | a = augmented |
| CATEGORY 7 | 10,000 Mbps | Added shielding to the wires. |

**Unshielded twisted pair** (UTP) is by far the most common type of table that is used today.  It consists of 4 pairs of unshielded wires twisted around each other.  The wires are twisted to prevent electromagnetic interference or crosstalk.  This type of cabling is mainly used on local area networks.

**Unshielded twisted pair (UTP) cable**

Now **shielded twisted pair** (STP) is very similar to unshielded twisted pair, except that it has a foil shield that covers the wires. This shielding adds a layer of protection against electromagnetic interference leaking into and out of a cable.

**Shielded twisted pair (STP) cable adds a foil shield that covers the wires.**

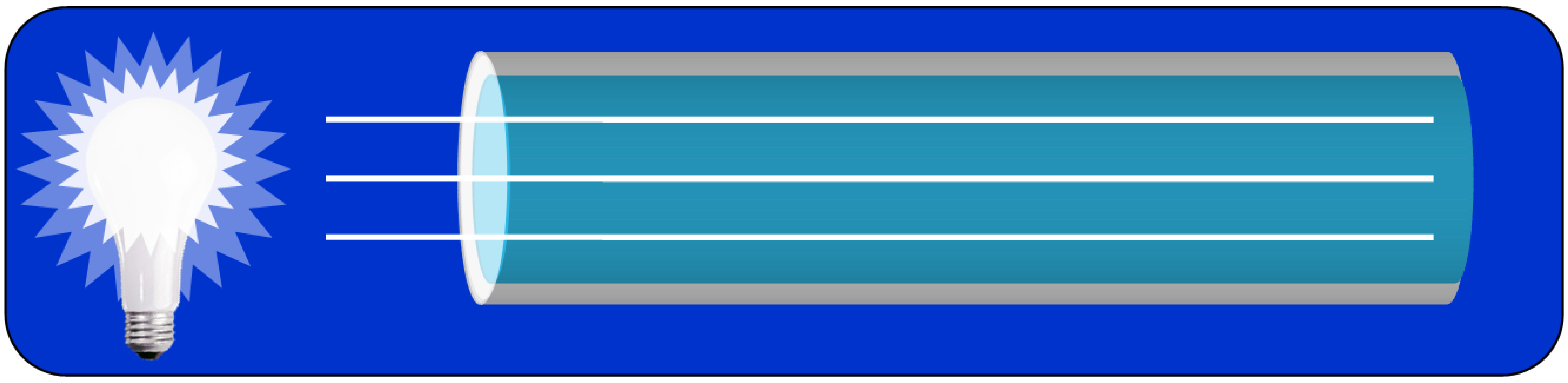


**Coaxial cable**

This is a **coaxial cable**. This is used today primarily by cable providers to provide a computer with broadband internet connection. Early on it was used as a backbone for networks, such as a bus network. There are also two common types of coaxial cable. The first type is **RG-6**. RG-6 is made for long distances and is commonly used for cable television and internet connection.  The second type is **RG-59**, and this is made for short distances and is commonly used for high definition and high quality video.

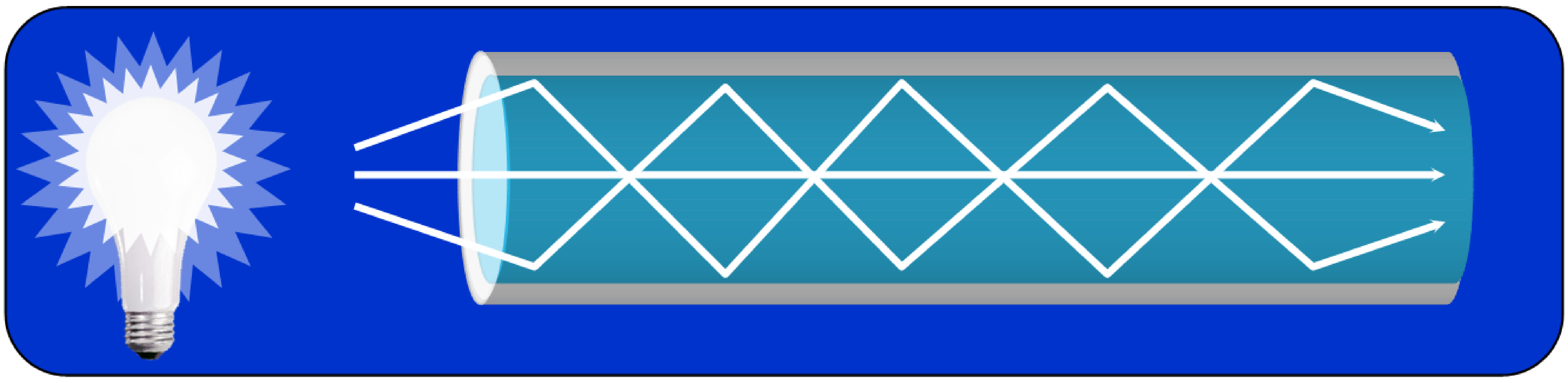
Now we're getting into fiber optic cables.  Below, are cutaway views of fiber optic cables and a light source. Fiber optic cable uses pulses of light to send data, and as a result, it is very fast and it can span for great distances.

There are two different modes of fiber optics: **Single-mode** fiber and **multi-mode** fiber.  Single-mode fiber is a fiber optic cable that allows light to enter only at a single angle.  So when this type of transmission of light enters at this angle, it can span for long distances.



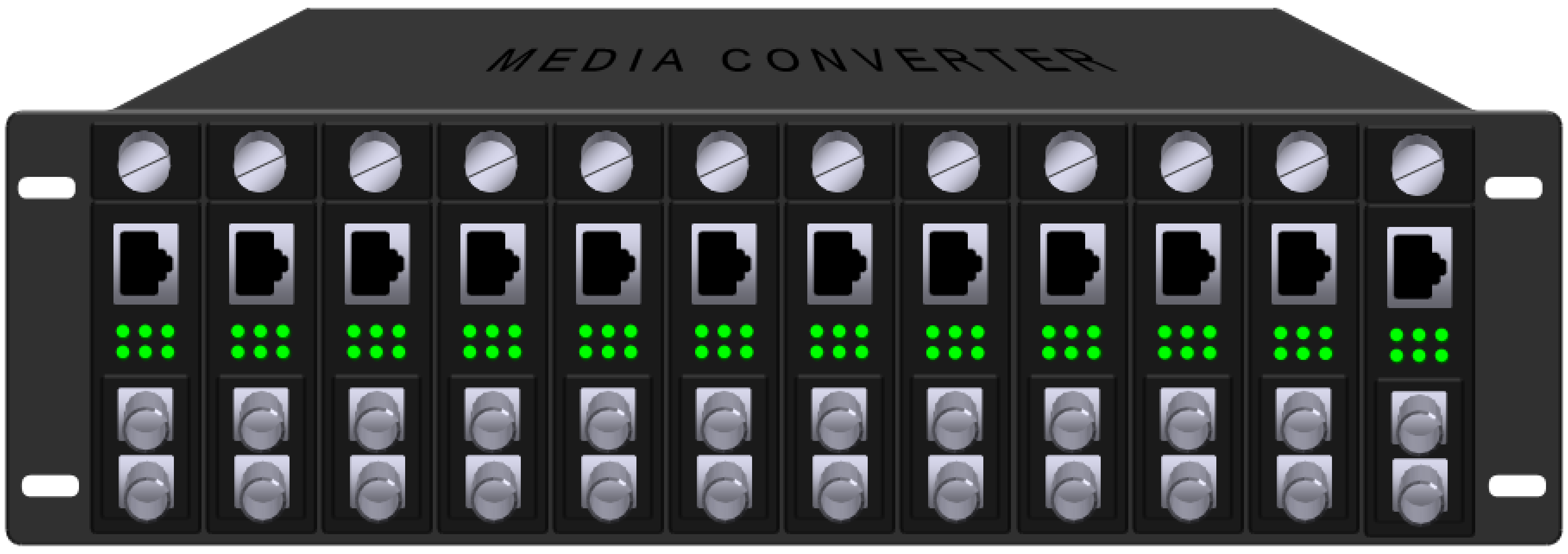
**Single-mode fiber -  Light enters at a single angle.  Made for long distances.**

Below, is **multi-mode** fiber.  The difference between multi-mode and single-mode is that in multi-mode, light travels in multiple beams that reflect off the walls of the cable.  And unlike single-mode fiber, multi-mode fiber is made for short distances.



**Multi-mode fiber - Light reflects off the walls of the cable. Made for short distances.**

Sometimes you may need to convert different media types in your network. So if you're running different types of media such as fiber, Ethernet, or coaxial within your network, well then you can convert and connect all these different types by using a **media converter**. Media converters allow you to convert to different types of media such as converting single and multi-mode fiber to Ethernet, fiber to coaxial, and single-mode fiber to multi-mode fiber and so on.



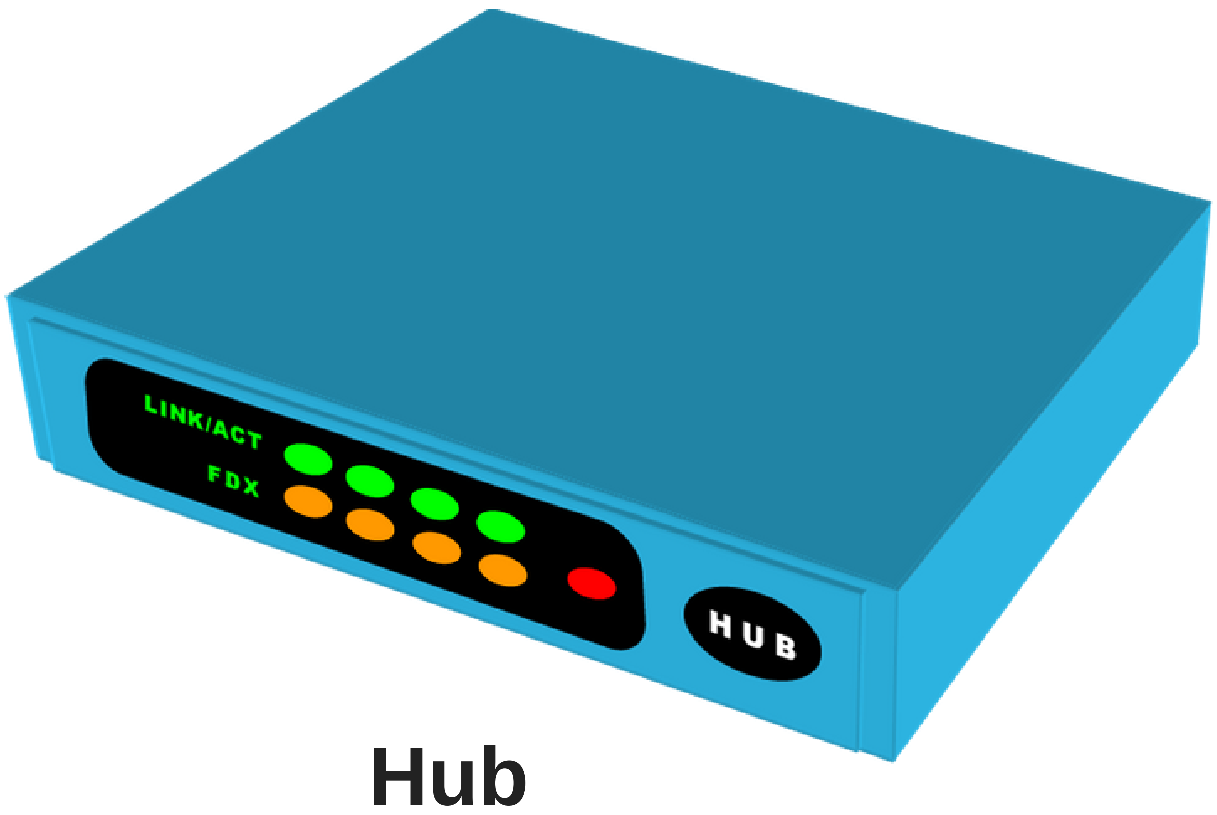
**Media converter**

# Network Components

CABLE MODEM

Cable modem

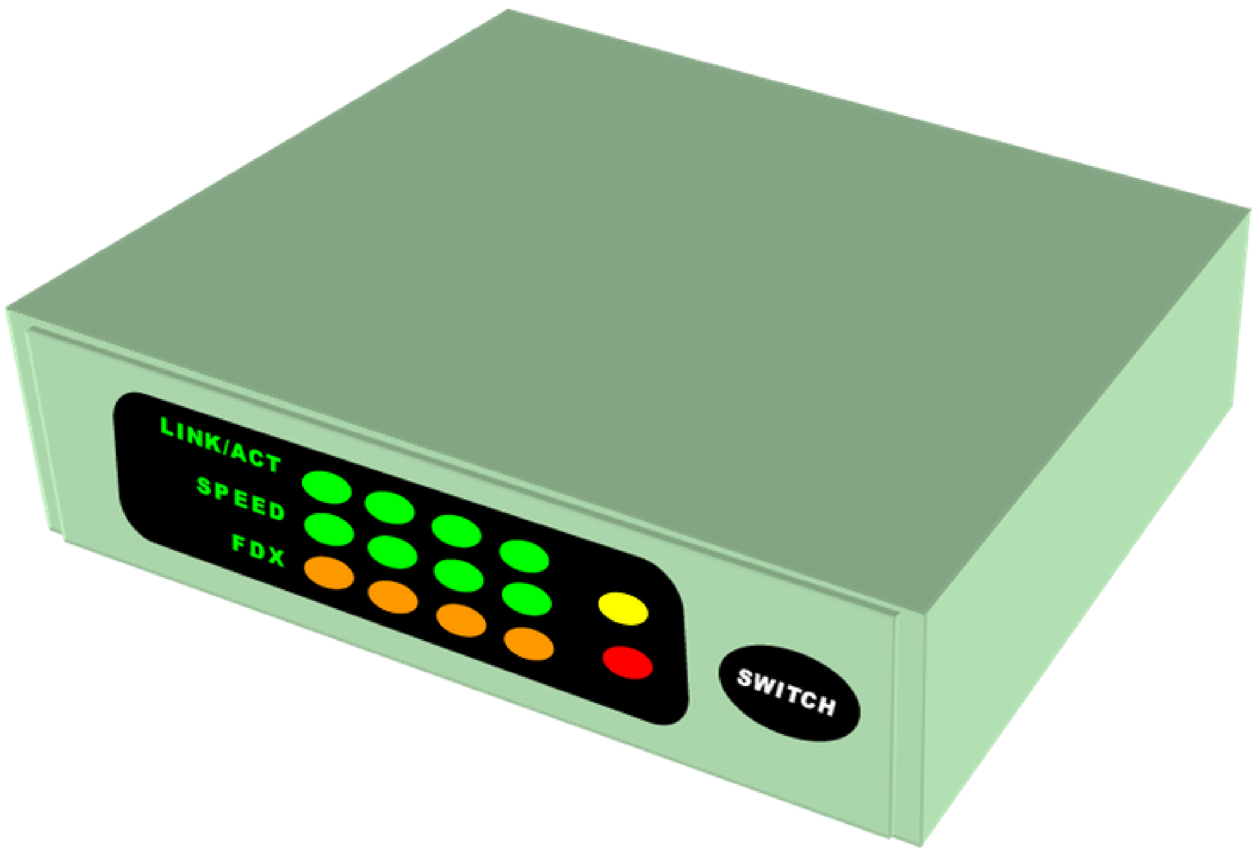
Those of you who have broadband cable internet will recognize this device.  And yes, this is your typical DOCSIS **cable modem**.  DOCSIS stands for data over cable service interface specifications.  The DOCSIS 3.1 specification supports speeds of 10 gigabit downstream and 1 gigabit upstream.  The DOCSIS modem handles both incoming and outgoing data signals, including internet, video, and voice.



Hub

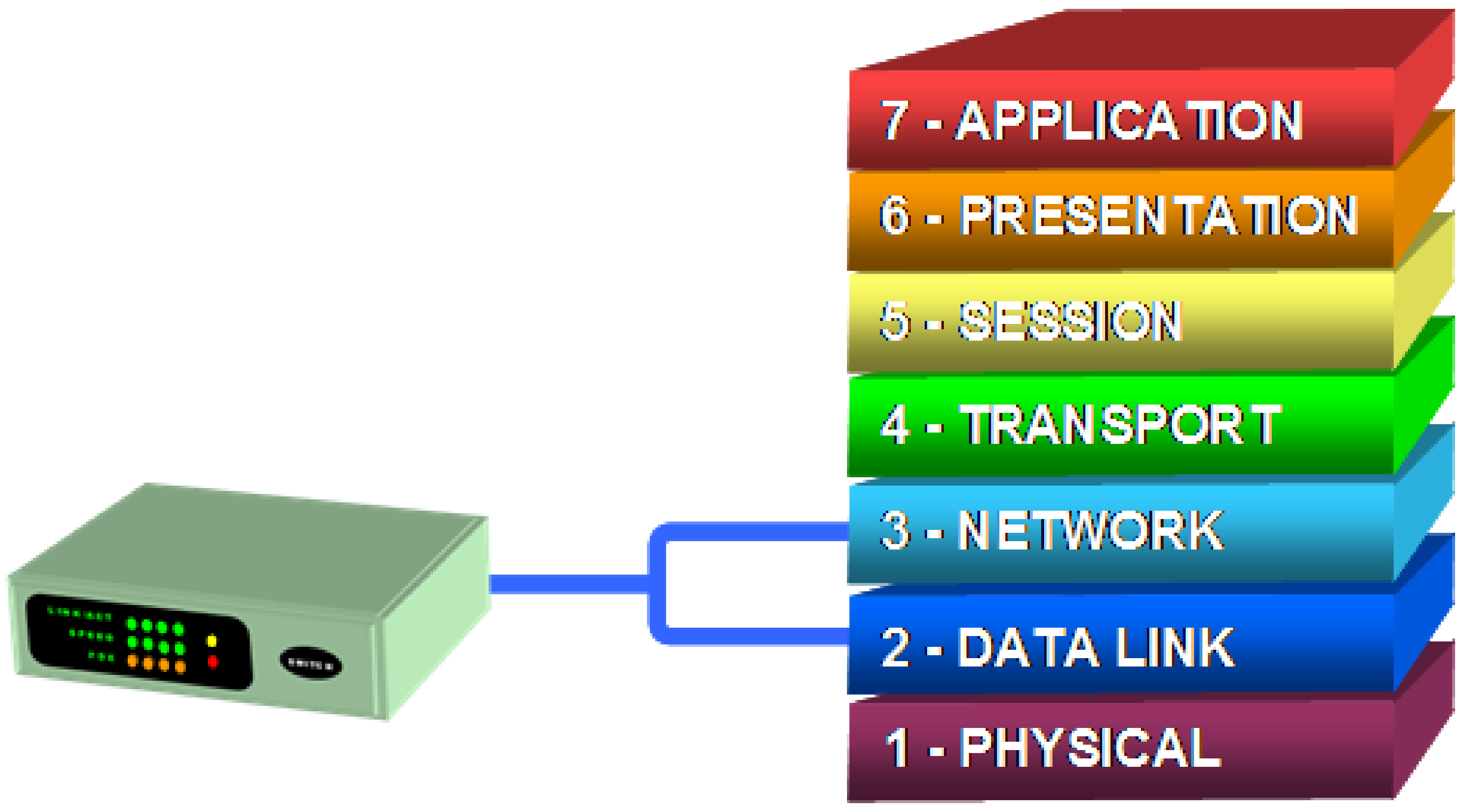
A **hub** is a device that has multiple ports that accepts Ethernet connections from network devices.  A hub is considered not to be intelligent because it does not filter any data or has any intelligence as to where data is supposed to be sent.  When a data packet arrives at one of the ports, it is copied to all other ports, so all the devices on that hub see that data packet.  So this not only creates security concerns, but it also creates unnecessary traffic on the network.

Now a **switch** is very similar to a hub.  It's also a device that has multiple ports that accepts Ethernet connections from network devices.  But unlike a hub, a switch is intelligent.  A switch can actually learn the physical addresses of the devices that are connected to it, and it stores these addresses in a table.  So when a data packet is sent to a switch, it's directed only to the intended destination port. That's the major difference between a hub and a switch.  So as a result, switches are far more preferred over hubs, because they reduce any unnecessary traffic on the network.



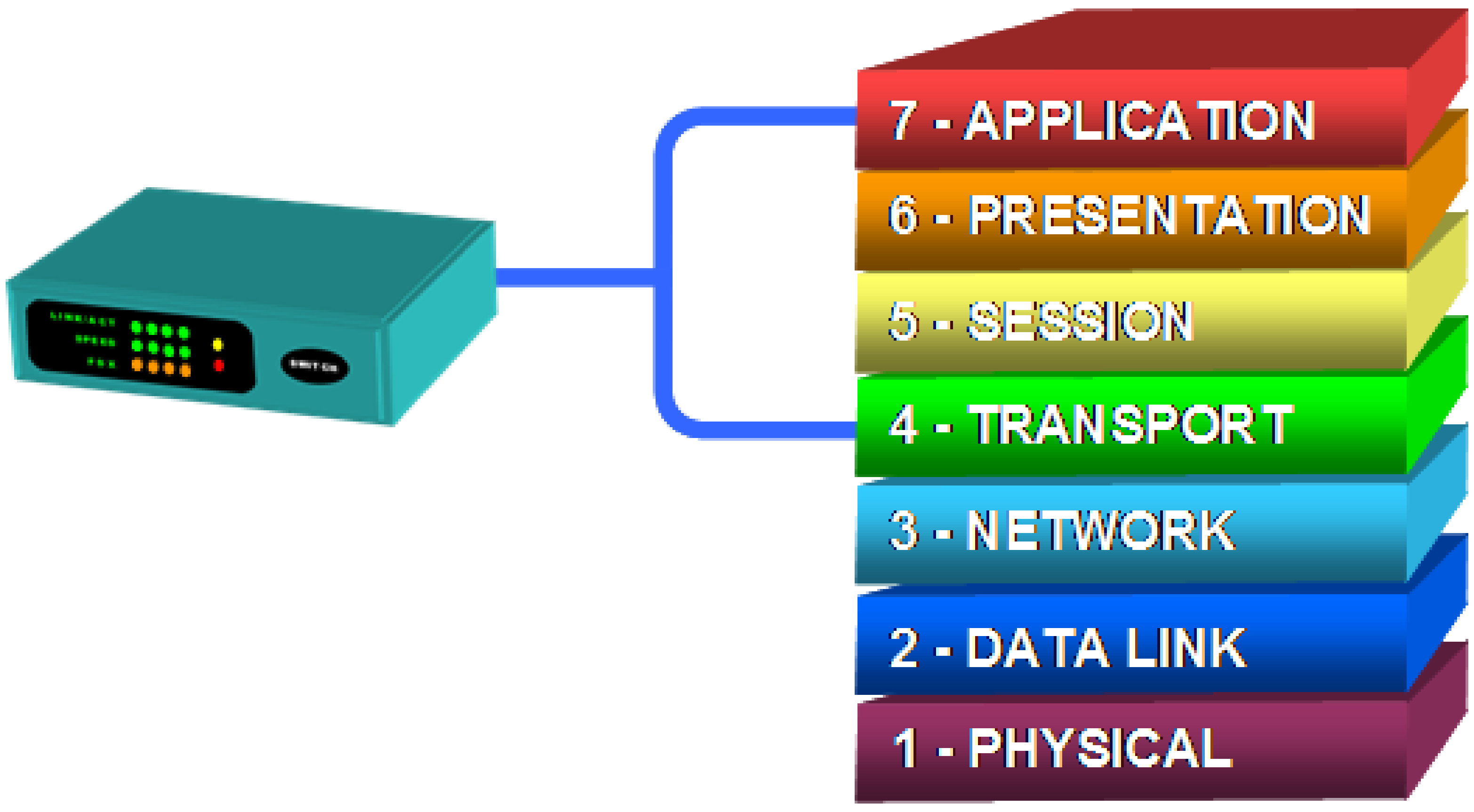
**Switch**

Regular switches operate at layer 2 of the OSI model, and we'll talk about the OSI model in a later lesson.  But there are other types of switches that operate at higher levels of the OSI model.  One of these is called a **multi-layer switch**.  A multi-layer switch can operate at layer 2 and layer 3 of the OSI model.  It's able to interpret layer 3 data similar to a router.



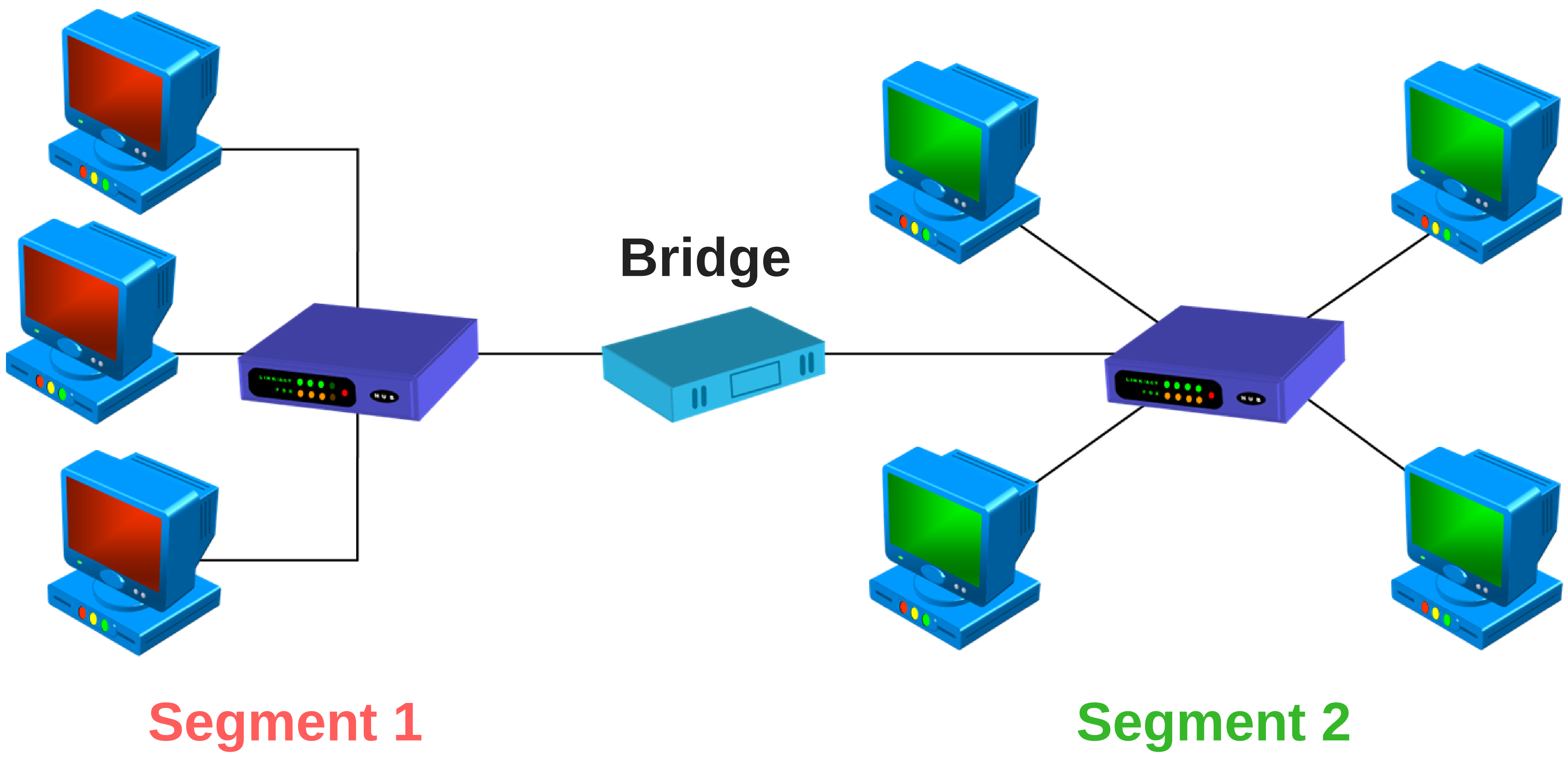
**Multi-layer switch operates at layer 2 & 3 of the OSI model.**

Another type of switch is called a **content switch**. A content switch can operate at layers 4 through 7 of the OSI model.  This type of switch can perform load balancing and advanced filtering and these switches are also very expensive.



**Content switch operates at layer 4 - 7 of the OSI model.**

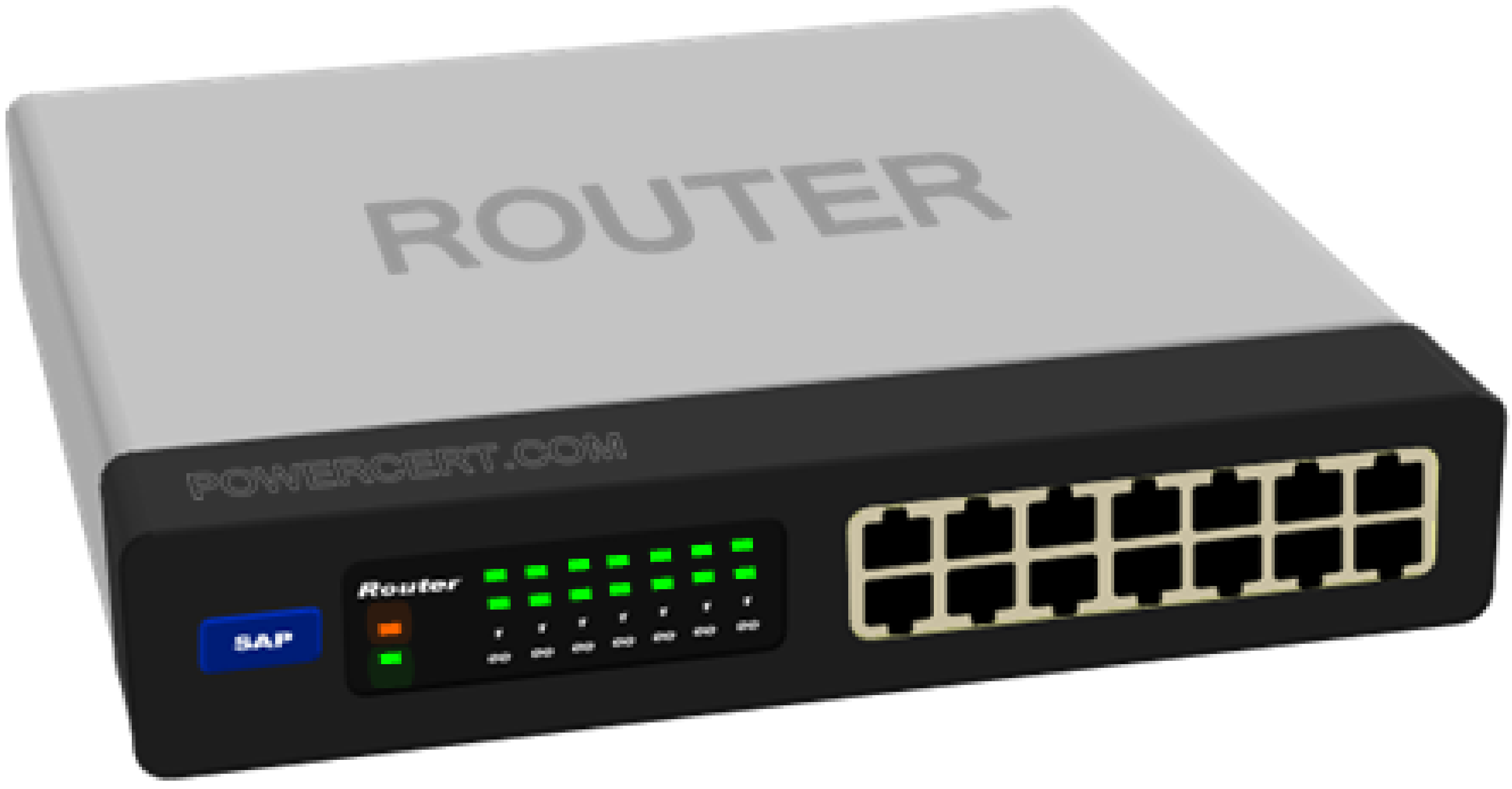
A **bridge** is used to divide a network into separate collision domains.  For example, if you have a network that is segmented into two by a couple of hubs, then all the broadcast traffic from the two segments are seen by all the computers.  And this causes unnecessary traffic. So that is where a bridge can be helpful.  If you add a bridge to this network, it will reduce any unnecessary traffic between the two segments by filtering the data based on their MAC address.  The bridge only allows data to crossover if it meets the required MAC address of the destination, because a bridge keeps a record of all the MAC addresses of the NICs (network interface card) that are connected to it.  And it will also block all data from crossing over if it fails to meet this requirement.



**Bridges reduce unnecessary traffic on a network by allowing or blocking data based on their MAC address.**

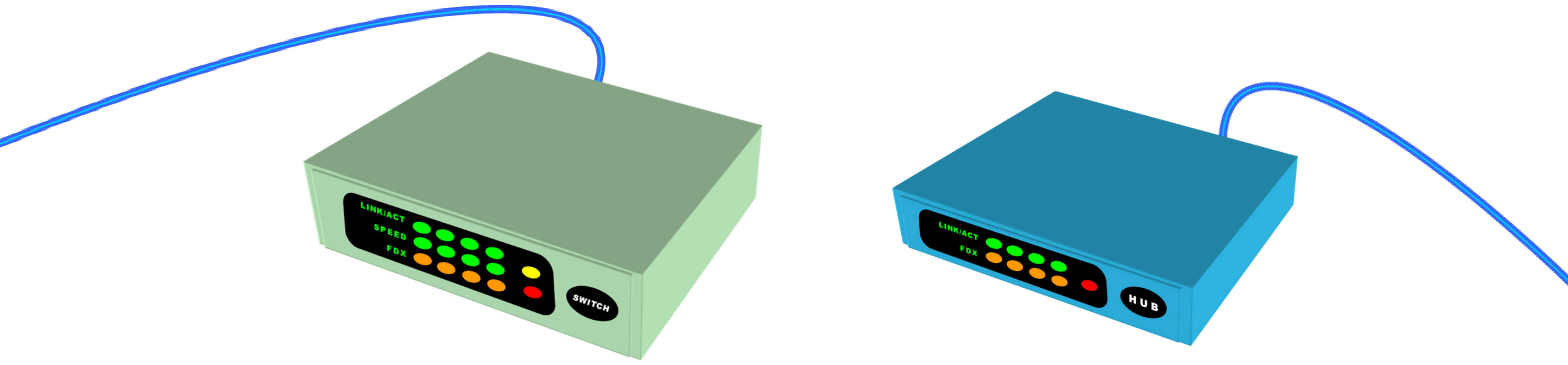
**A segment is part of a network that is separated from the rest of the network by a device, such as a hub, switch, bridge, or router.**

A **router** does exactly what its name implies.  A router is a device that routes or forwards data from one network to another based on their IP address.  When a data packet is received from the router, the router inspects the packet and determines if the packet was meant for its own network or if it's meant for another network.  If the router determines that the data packet is meant for its own network, it receives it.  But if it's not meant for its own network, it sends it off to another network.  So a router is essentially the gateway for a network.



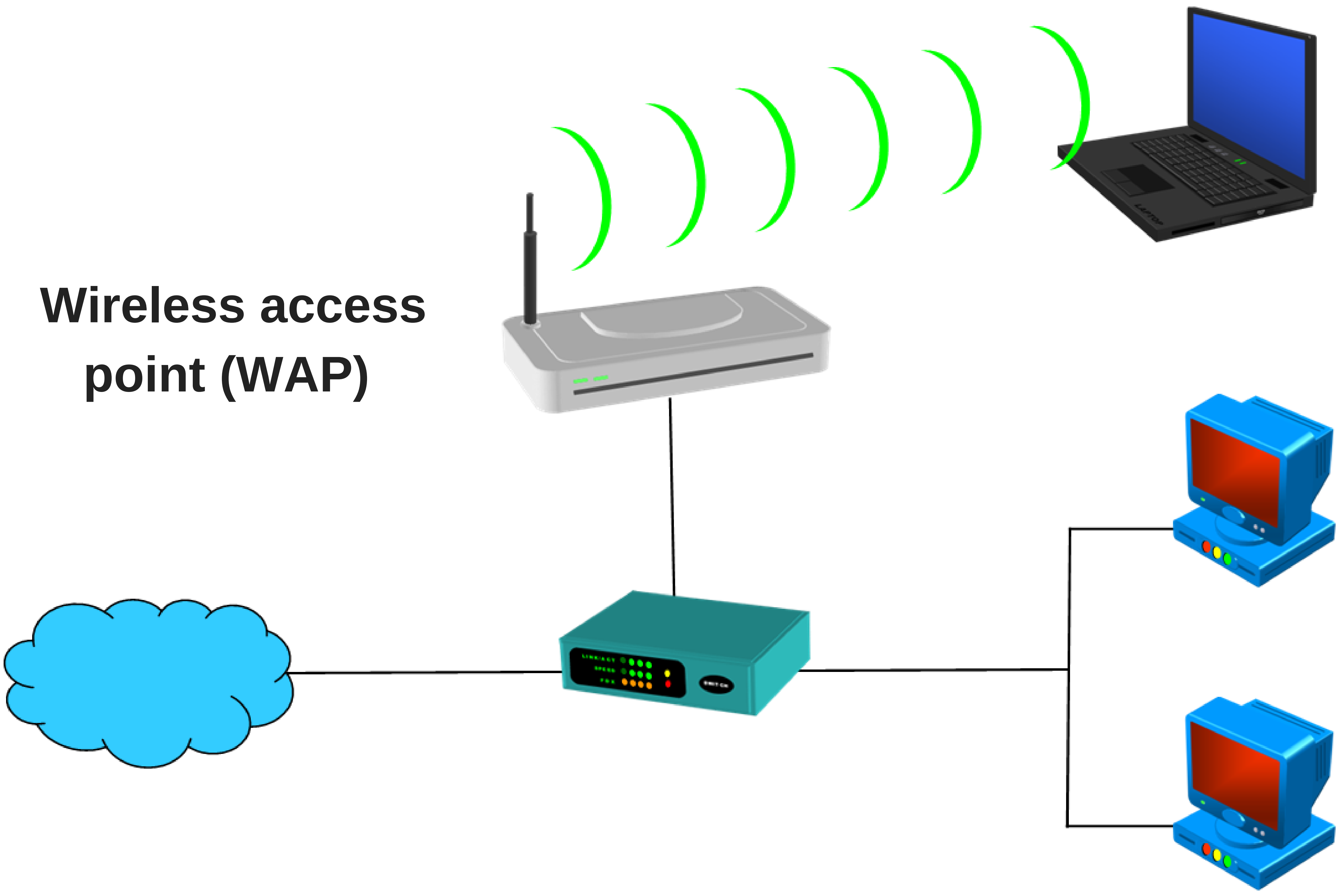
**Router**

Networking devices need electrical power to function and that's why they have a separate power cable.  But some networking devices don't have a power cable. It’s not that they don't need electrical power, it's just that they get their power and data from the same cable, which is through the Ethernet cable.  This technology is known as **PoE**, which stands for **power over Ethernet**.

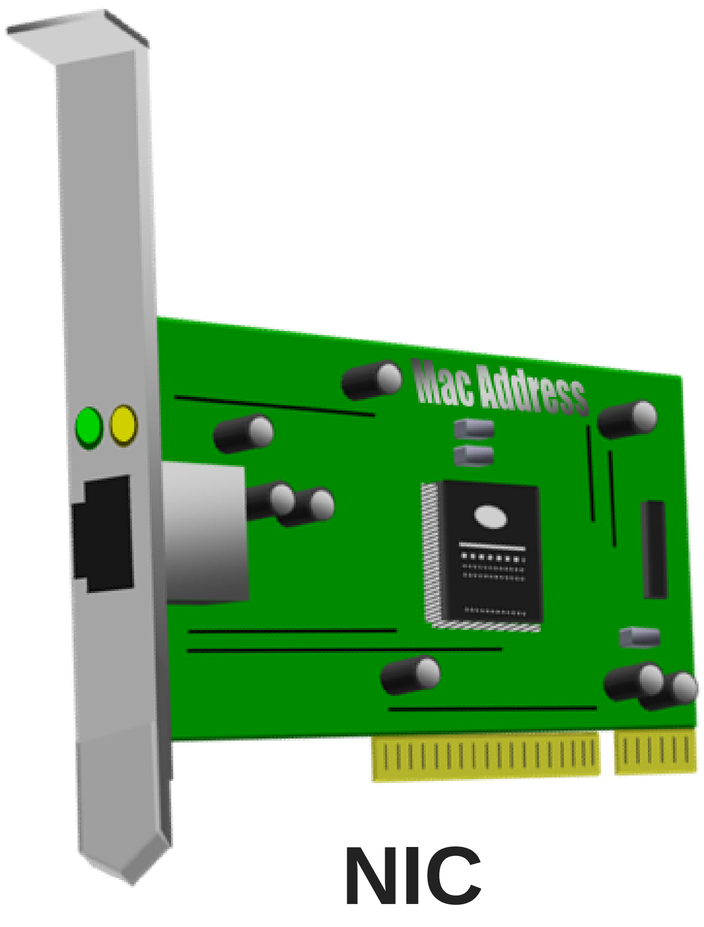


**Here is a switch and a hub that receive power from the network Ethernet cable, instead of a separate power cable.**

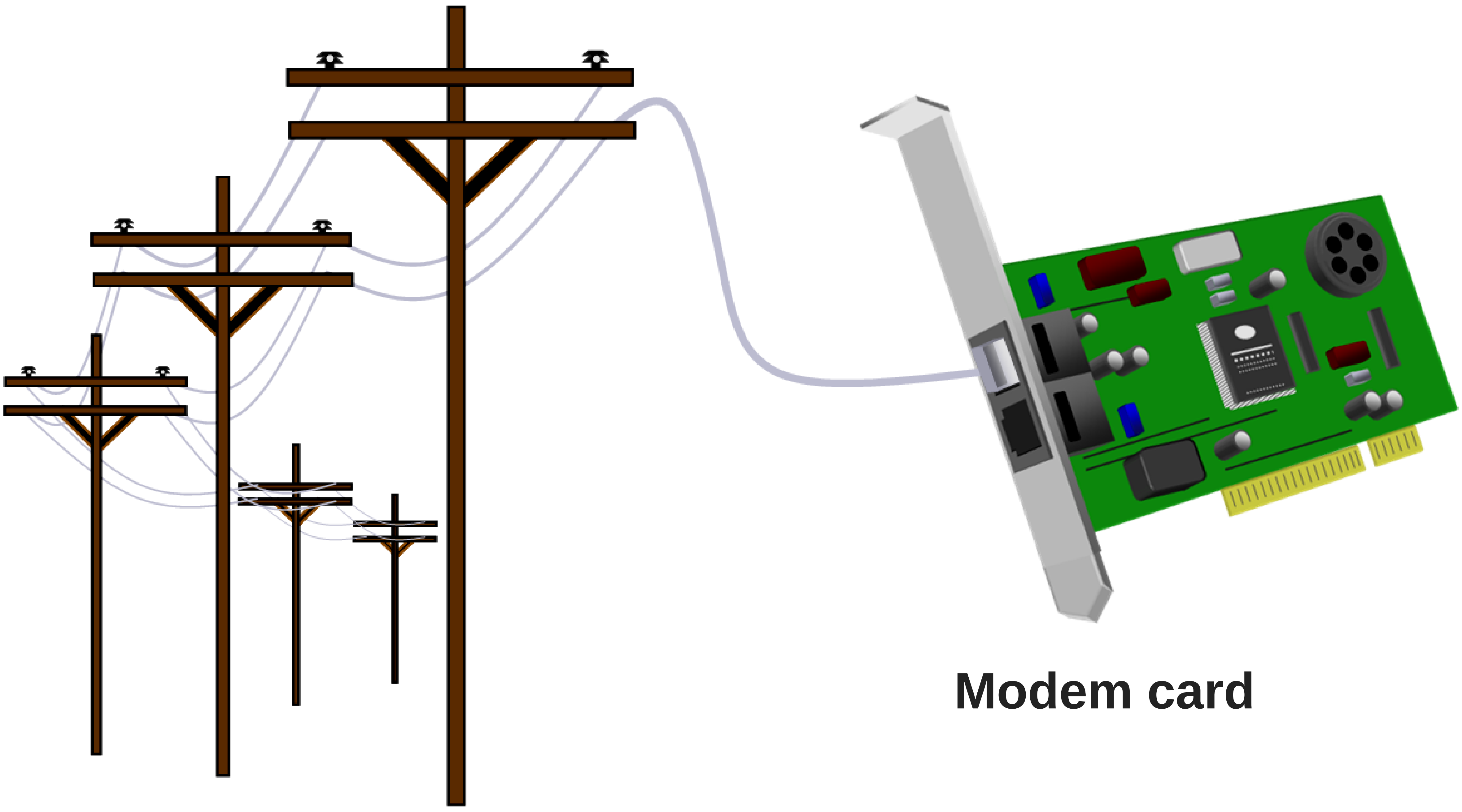
A **wireless access point** is basically a wireless hub that is used by wireless devices.  It connects to a wired network and relays data between the wired network and the wireless device for communication purposes. In the illustration below, you see a wireless access point that's wired to a network so that the wireless laptop can communicate with the network.



A **network interface card** or **NIC** is used to connect a computer to a network.  It is basically a circuit board with a network adapter that is installed on your computer.  Its job is to convert incoming serial data into parallel data so that the computer can understand it.   A NIC provides a constant dedicated connection to a network.  And every NIC has its own unique identifier, called a **MAC address**.



A **modem card** is a device that allows a computer to transmit data over normal telephone lines.  The data coming in from the telephone lines is analog, however, the data in a computer is all digital.  So when the analog data comes in from the telephone lines, the modem's job is to convert into a digital form so the computer can understand it.  So that's basically what a modem does, it converts analog data into digital data. The maximum speed of most modems today is 56 kbit/s.

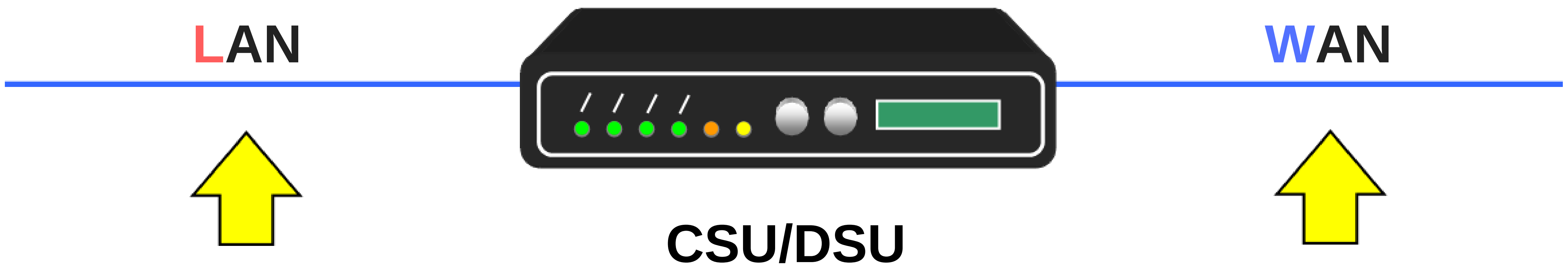


Modem card

A **transceiver** is a device that has both a transmitter and a receiver in the same package.  The term applies to wireless communication devices like cell phones and two-way radios.  It's basically a term used for any device that receives data, converts it, and then transmits the data to another location.

A **gateway** can be defined as a device that joins two networks together.  They interconnect networks with different or incompatible communication protocols.  A gateway, however, does not change the data, it only changes the format of the data.

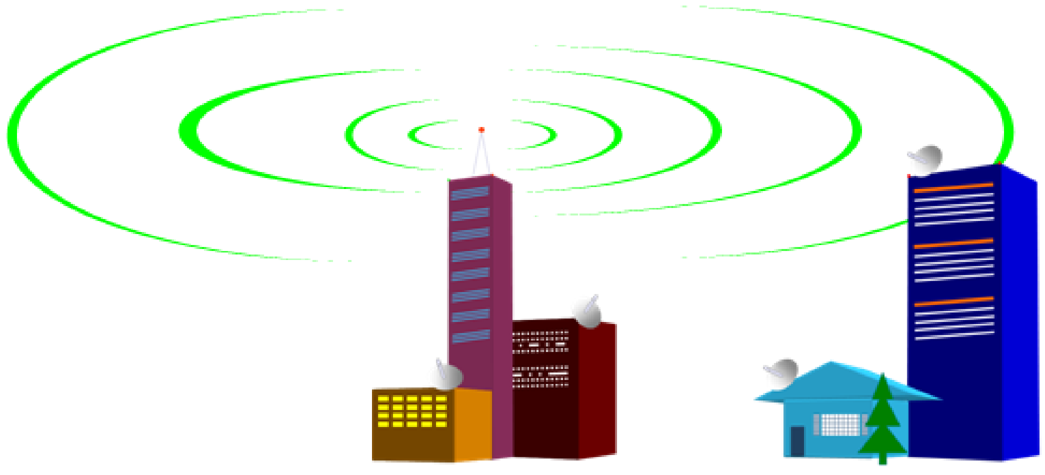
A **CSU/DSU** is a device about the size of a modem. What this device does is it converts data from a local area network to a wide area network.  And this has to happen because the data formats between a LAN and a WAN are different.



**Converts data from a LAN to a WAN.**

# Wireless Technologies

The **IEEE** is an international organization for the advancement of technology related to electricity.  They are responsible for a set of standards for a project called the 802 project.  One of these standards is the **802.11** standard, which is wireless.  Wireless technology is becoming more and more popular, and today there are five wireless standards.  There are the A, B, G, N, and AC standards.  Below is a chart of the speed, frequencies, and release year for each one.  So starting with the first wireless standard, which is 802. 11a, which came out in 1999, and the latest standard is the 802.11ac standard, which was released in 2014.



| | 802.11a | 802.11b | 802.11g | 802.11n | 802.11ac |
|---|---|---|---|---|---|
| SPEED | 54 Mbps | 11 Mbps | 54 Mbps | 600 Mbps | 6,933 Mbps |
| FREQUENCY | 5 Ghz | 2.4 Ghz | 2.4 Ghz | 2.4 or 5 Ghz | 5 Ghz |
| RELEASED | 1999 | 1999 | 2003 | 2009 | 2014 |

**Bluetooth** is a short-range radio that provides a way to connect and exchange information between devices such as laptops, cell phones, and tablets.  It operates at 2.4 GHz and is capable of transmitting both voice and data. The latest standard of bluetooth has a transfer speed of 24 Mbit/s and has a maximum range of approximately 100 meters.

**Bluetooth is used in devices such as laptops, tablets, and cell phones.**

**Infrared** is a technology that was developed by IRDA, which stands for the infrared data association. The term infrared actually means below red. It's a wireless technology where data is transmitted in rays of light, rather than using radio waves. Many companies have now utilized this technology to transmit and receive data in their products. However, the drawbacks of infrared are that it requires a direct line of sight. If any object comes in between the two infrared devices, the communication will be blocked. Infrared also does not work in direct sunlight. If this happens the communication will be weakened and most likely will be blocked.

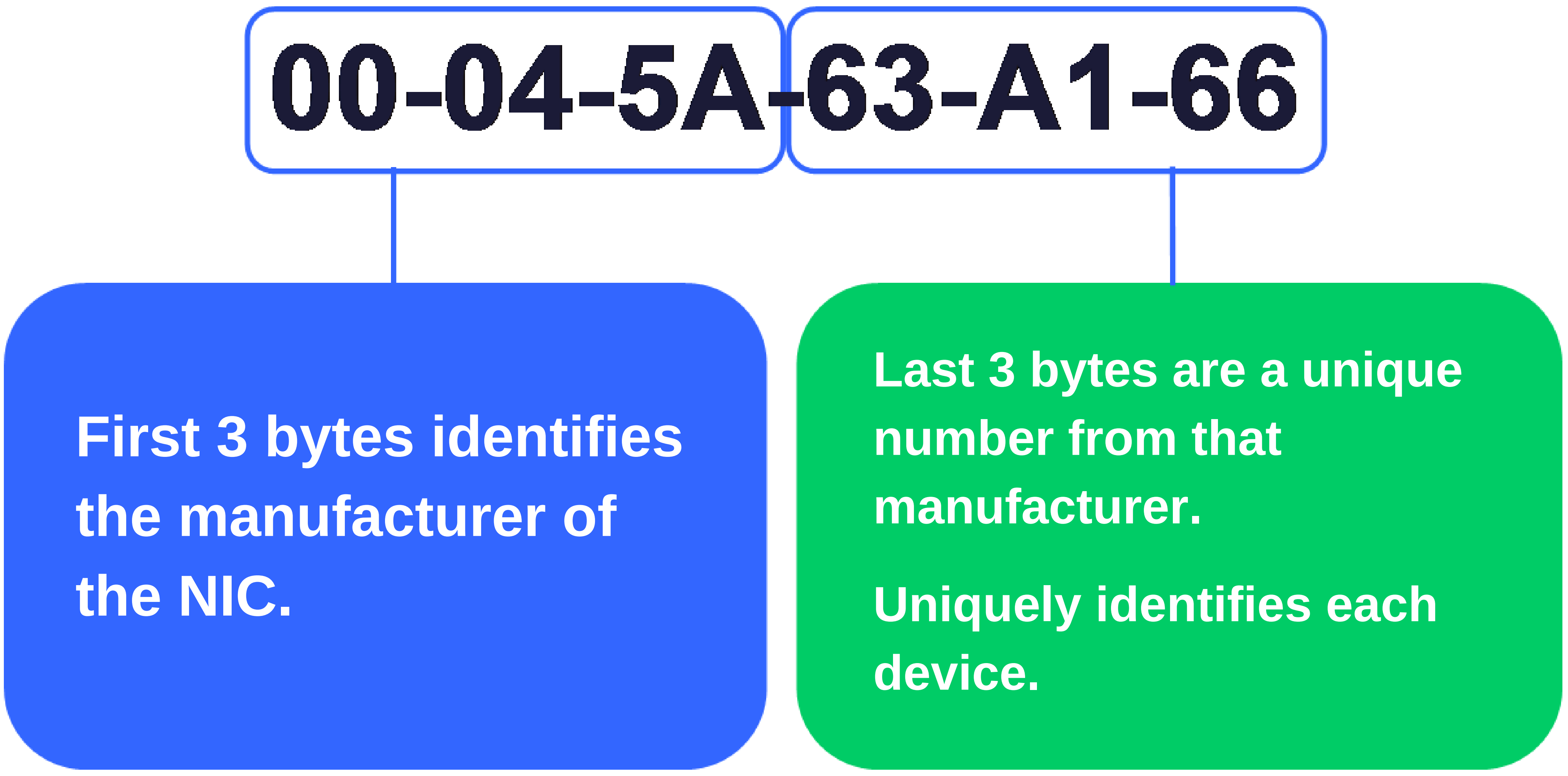
# MAC Address

The **MAC** or **media access control address** is an identifier that every network device uses to uniquely identify itself on a network.  So no two devices anywhere in the world will have the same MAC address.

**00-04-5A-63-A1-66**

**A MAC address**

The MAC address is made up of a 6 byte, hexadecimal number that is burned into every NIC by its manufacturer.  The MAC address can contain any number and it also contains alphabets from a through f.  The MAC address is broken up into two parts.  The first three bytes identify the manufacturer of the NIC, such as Linksys, Netgear, or Belkin.  The last three bytes are a unique number from the manufacturer that identifies each device on a network.



00-04-5A-63-A1-66

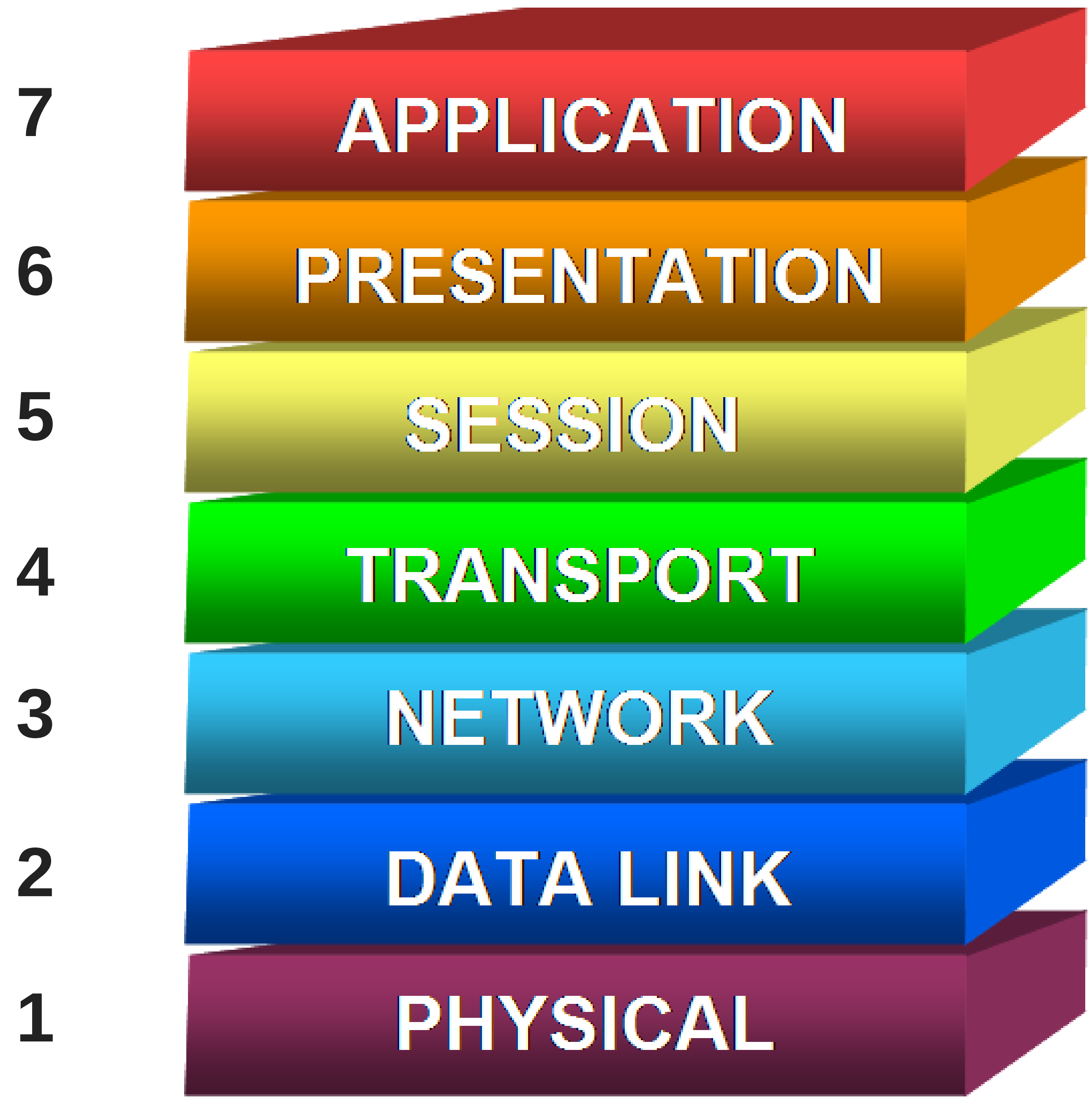
First 3 bytes identifies the manufacturer of the NIC.

Last 3 bytes are a unique number from that manufacturer.

Uniquely identifies each device.

# OSI Model

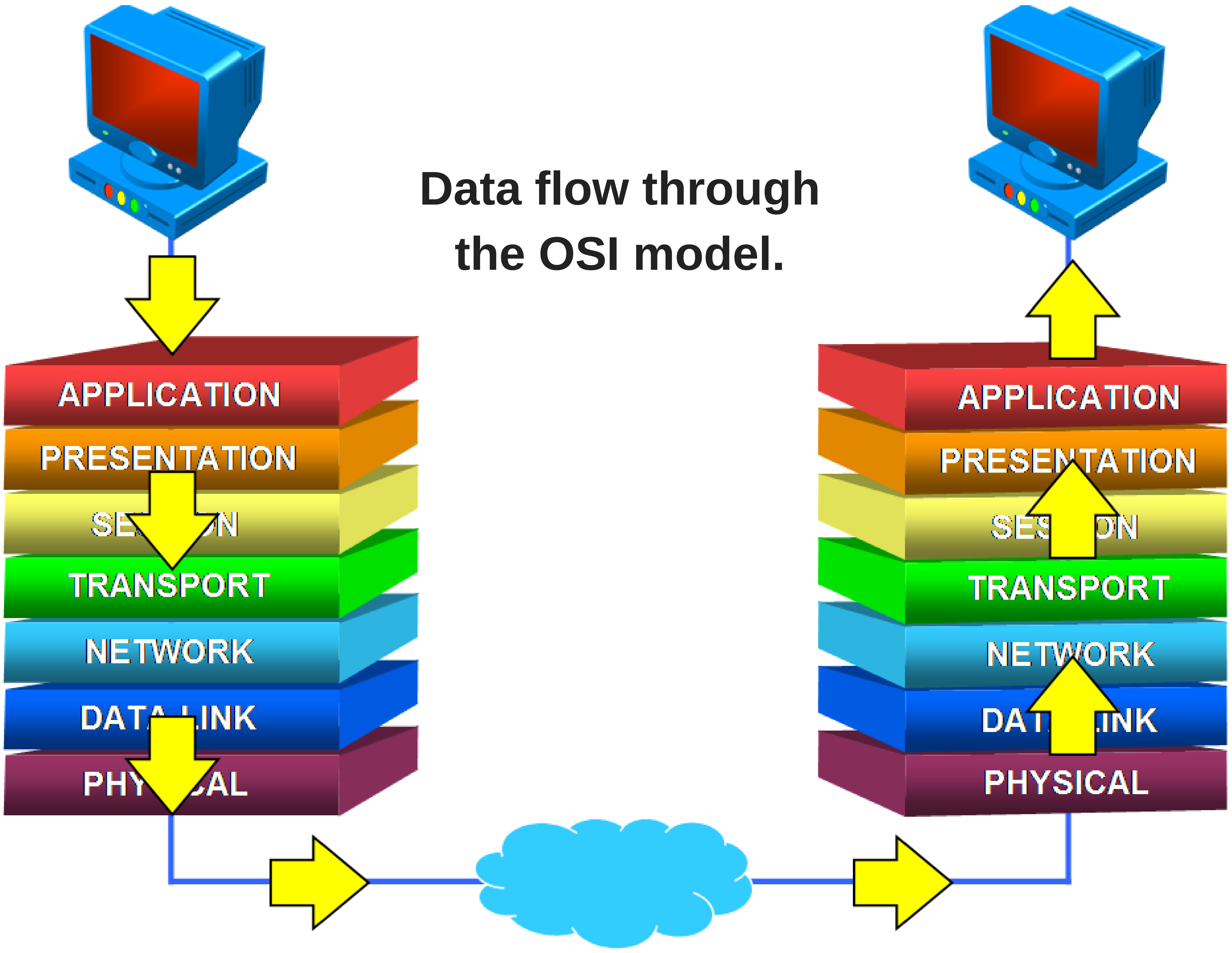
In order for network communication to take place, there needs to be a set of standards, and that's why the **OSI model** was developed.  The OSI model describes how information from software in one computer, moves through a network to reach software on another computer.  It does this by breaking down this huge task of data communication into 7 different layers; giving control of the data being sent from one layer to another.



**OSI model**

These layers are numbered from 1 to 7, starting from the bottom.  These layers are the physical, data link, network, transport, session, presentation, and application.

This illustration below shows how data flows through the OSI model.  When two computers want to communicate, the data flows down the OSI model, and when the data crosses over the network media, such as the internet, it flows back up the OSI model to its destination.



Data flow through the OSI model.

The top layer of the OSI model is the **application layer**. In this layer, as you might have guessed, deals with applications.  The purpose of this layer is to manage communications between applications.  It supports application protocols such as email, HTTP, and FTP. At this layer, data still resembles something that you can actually read.

The **presentation layer** is where data is first converted into a form that can be sent over a network.  Data is compressed or decompressed, and encrypted or decrypted. This layer is sometimes referred to as the translation layer.

The **session layer** controls the dialogue during communications. It establishes, manages, and terminates the connections between local and remote applications. This layer is also known as the traffic cop because it directs network traffic.

The **transport layer** provides the transfer of data between end users. It's responsible for re-sending any packets that do not receive an acknowledgment from the destination; ensuring that the data packets were received by the destination. This layer can guarantee that the packets are received.

The **network layer** is responsible for routing the data packet based on its logical IP address. It fragments and reassembles the packets and it instructs the data on how to find its ultimate destination.

The **data link layer** is responsible for sending data to the physical layer. Data packets are encoded and decoded into bits. It handles flow control and frame synchronization, and it's also divided into two sublayers: the media access control layer, and the logical link control layer.

The bottom of the OSI model is the **physical layer**. This layer defines the network standards and physical characteristics of a network, such as the connectors, media types, cables, voltages, etc.  This layer defines the topology of a network.

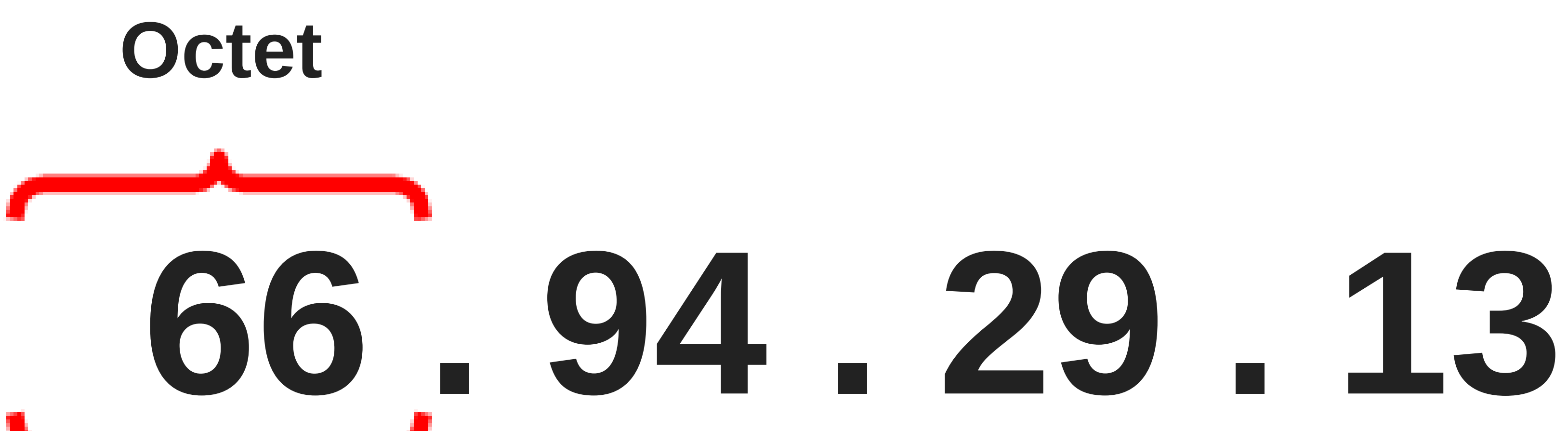
# IP Address

An **IP address** is a numeric address.  It's an identifier for a computer or device on a network.  Every device has to have an IP address for communication purposes. The IP address consists of two parts, the first part is the network address, and the second part is the host address.  There are also two versions of IP addresses. The first one is the most common one, it's called IP version 4 (**IPv4**).  And the second type is IP version 6 (**IPv6**).

**66 . 94 . 29 . 13**

**IPv4 address**

IPv4 is the current version (but not for long) of IP addresses.  It's a 32-bit numeric address, written as four numbers, separated by periods.  Each group of numbers that are separated by periods is called an **octet**.



**IPv4 address**

The number range in each octet is 0 - 255.  This address version can produce over 4 billion unique addresses.

In the world of computers and networks, this IP address below, in this format here, is meaningless.

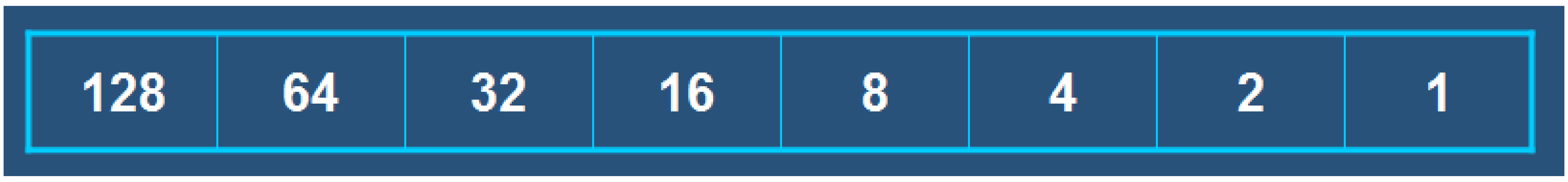
**66 . 94 . 29 . 13**

Computers and networks don’t read IP addresses in this standard numeric format.  And that’s because they only understand numbers in a binary format.  A binary format is a number that only uses 1s and 0s.  The binary number for this IP address is this number below.

**01000010 . 01011110 . 00011101 . 00001101**

**IPv4 in a binary format.**

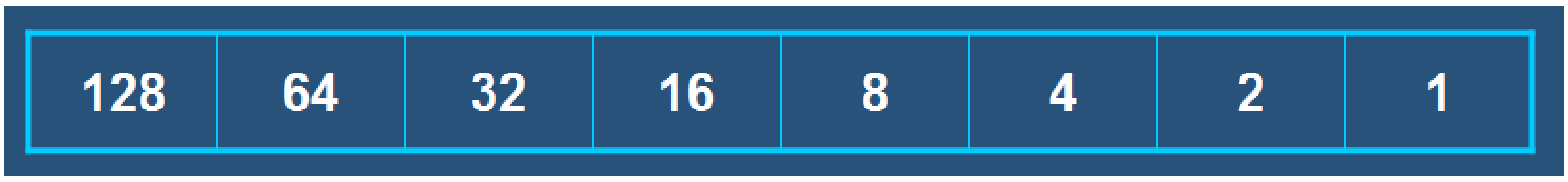
The bits in each octet are represented by a number.  So starting from the left, the first bit has a value of 128, then 64, then 32, and so on, all the way down to 1.



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |

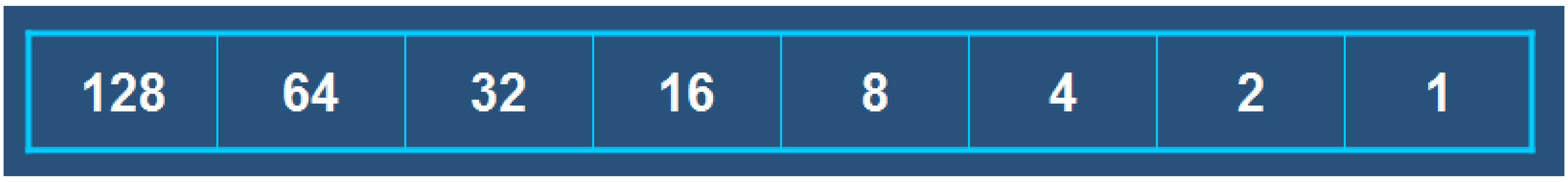
**8 bit octet chart**

Each bit on the octet can be either a 1 or a 0.  If the number is a 1, then the number that it represents counts.  If the number is a 0, then the number that it represents does not count.  So by manipulating the 1s and the 0s in the octet, you can come up with a range from 0 - 255.  So for example, the first octet in this IP address is 66.  So how do we get a binary number out of 66?  First, you look at the octet chart, and you would put 1s under the numbers that would add up to the total of 66.  So you would put a 1 in the 64 slot.



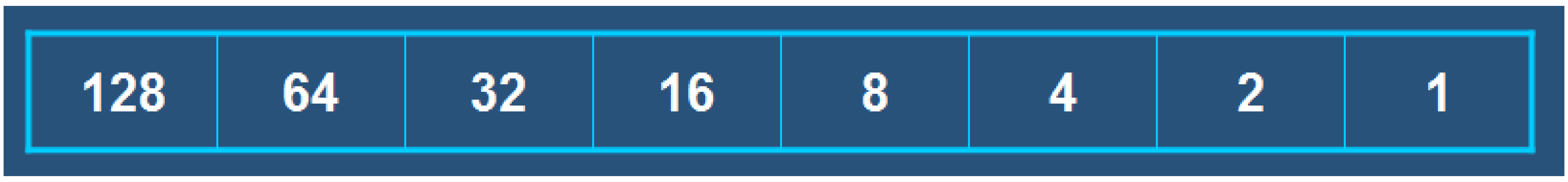
| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
|---|---|---|---|---|---|---|---|
|  | **1** |  |  |  |  |  |  |

So now you already have 64, so we need 2 more.  So let's put a number 1 in the 2 slot.



| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
|---|---|---|---|---|---|---|---|
|  | **1** |  |  |  |  | **1** |  |

So now if we count all the numbers that we have 1s underneath them, you will get a total of 66.



| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
|---|---|---|---|---|---|---|---|
|  | **1** |  |  |  |  | **1** |  |

**64 + 2 = 66**

All of the other bits would be 0s because we don't need to count them since we already have our number.  So the binary number underneath the chart is the binary bit version of 66.

| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |

So let's do the next number which is 94.  So let's put a 1 under 64, 16, 8, 4, and 2.  So if we were to add all the numbers that we have 1s underneath them, we will get a total of 94.

| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 |

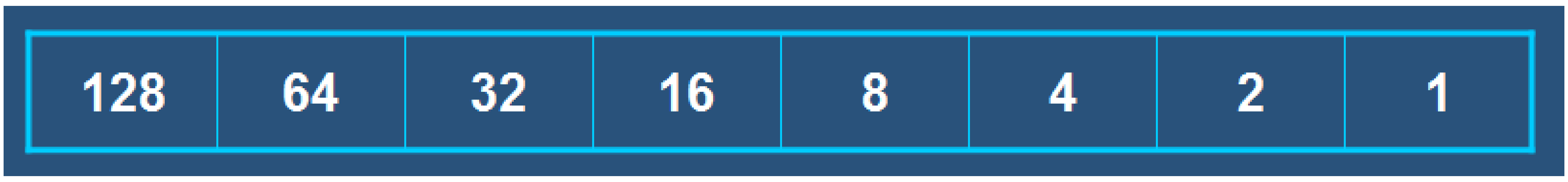
**64 + 16 + 8 + 4 + 2 = 94**

So the next number is 29.  So let’s put a 1 under 16, 8, 4, and 1.  And when you add all the numbers up, you get 29.

| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 |

**16 + 8 + 4 + 1 = 29**

Our last number is 13. So let's select 8, 4, 1, and when you add those up, you get 13.



| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 |

**8 + 4 + 1 = 13**

**66 . 94 . 29 . 13**

**01000010 . 01011110 . 00011101 . 00001101**

**IP address with its binary equivalent.**

When the internet was first developed, programmers didn't realize how big it would become. They thought that IPv4, which produced over four billion addresses, would be enough. But they were wrong. **IPv6** is the next generation of IP addresses. The main difference between IPv4 and IPv6 is the length of the address. The IPv4 address is a 32-bit numeric address, whereas IPv6 is 128-bit hexadecimal address. Hexadecimal uses both numbers and alphabets in the address.

**76DC:4F59:34CF:71CD:9DC6:89CD:45D6:67A2**

**IPv6 address**

So with this type of address, IPv6 can produce an unbelievable 340 undecillion IP addresses. That's the number 340 with 36 digits after it. So as you might have guessed, IPv6 is more than enough for the foreseeable future.

As stated previously, an IP address has two parts, one part is designated for the network, and the remaining is designated for the host. So the way to tell which portion belongs to either the network or the host is where the **subnet mask** comes in. A subnet mask is a number that resembles an IP address. It reveals how many bits in the IP address are used for the network by masking the network portion of the IP address.

| | |
|---|---|
| **IP address** | **173 . 16 . 0 . 0** |
| **Subnet mask** | **255 . 255 . 0 . 0** |

So in this subnet mask, the first two octets are 255. So if we were to look at this subnet mask in binary form, the first two octets would be all 1s, because when you count all the numbers in an octet, it will equal 255.

**Subnet mask**

**255 . 255 . 0 . 0**

**11111111 . 11111111 . 00000000 . 00000000**

**Subnet mask in binary form.**

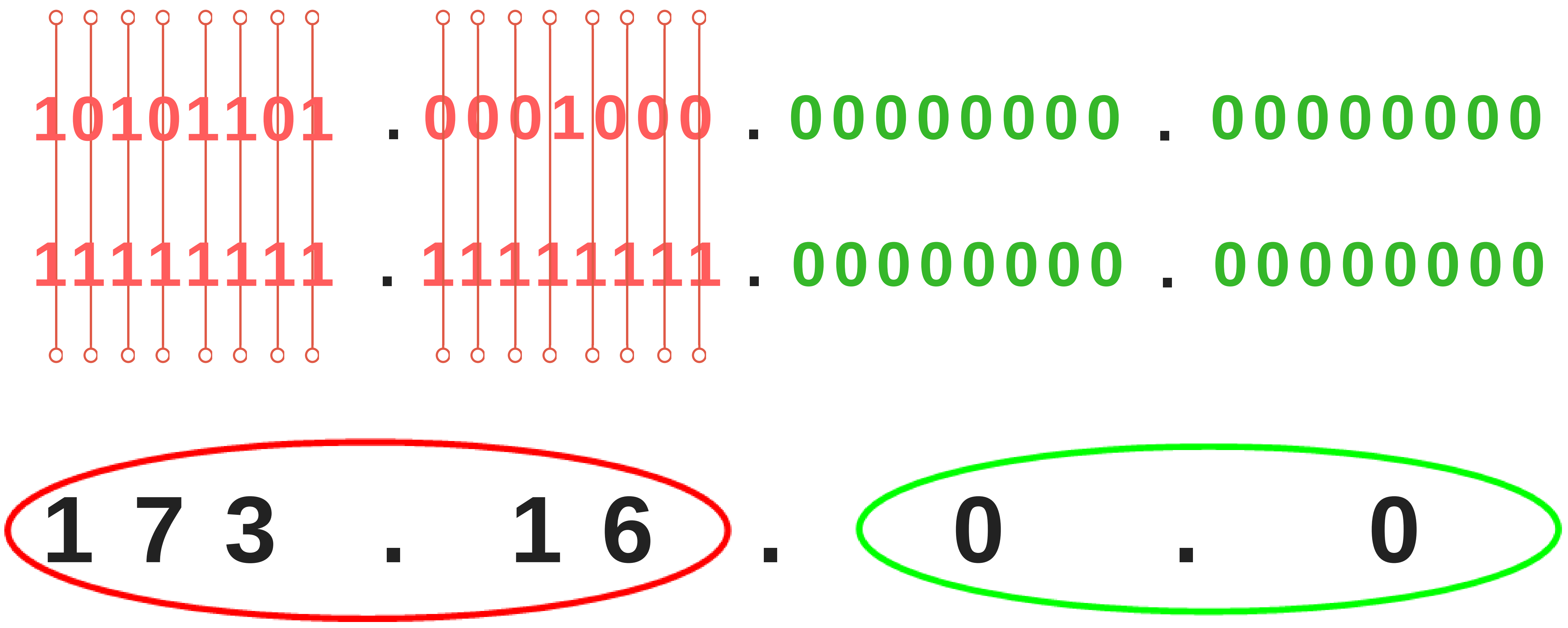
**IP address in binary form.**

10101101 . 0001000 . 00000000 . 00000000

11111111 . 11111111 . 00000000 . 00000000

**Subnet mask in binary form.**

So above, we have our IP address and subnet mask in binary form.  So the way to tell which portion of this IP address is the network portion is when the subnet mask binary digit is a 1, it will indicate the position of the IP address that defines the network.  So we'll cross out (below) all the digits in the IP address that line up with the 1s in the subnet mask.  And when you do this, it will reveal that the first two octets are the network portion, and the remaining is the host portion.



10101101 . 0001000 . 00000000 . 00000000

11111111 . 11111111 . 00000000 . 00000000

173 . 16 . 0 . 0

**Network portion** **Host portion**

Below is a chart of the default subnet masks for class A, B, and C, IP addresses. Noticed the change of the locations of the network and host portions between them. You should memorize these default subnet mask classes.

| Class | Subnet Mask | |
|---|---|---|
| A | 255.0.0.0 | NNNNNNNN . hhhhhhhh . hhhhhhhh . hhhhhhhh |
| B | 255.255.0.0 | NNNNNNNN . NNNNNNNN . hhhhhhhh . hhhhhhhh |
| C | 255.255.255.0 | NNNNNNNN . NNNNNNNN . NNNNNNNN . hhhhhhhh |

N = NETWORK

h = HOST

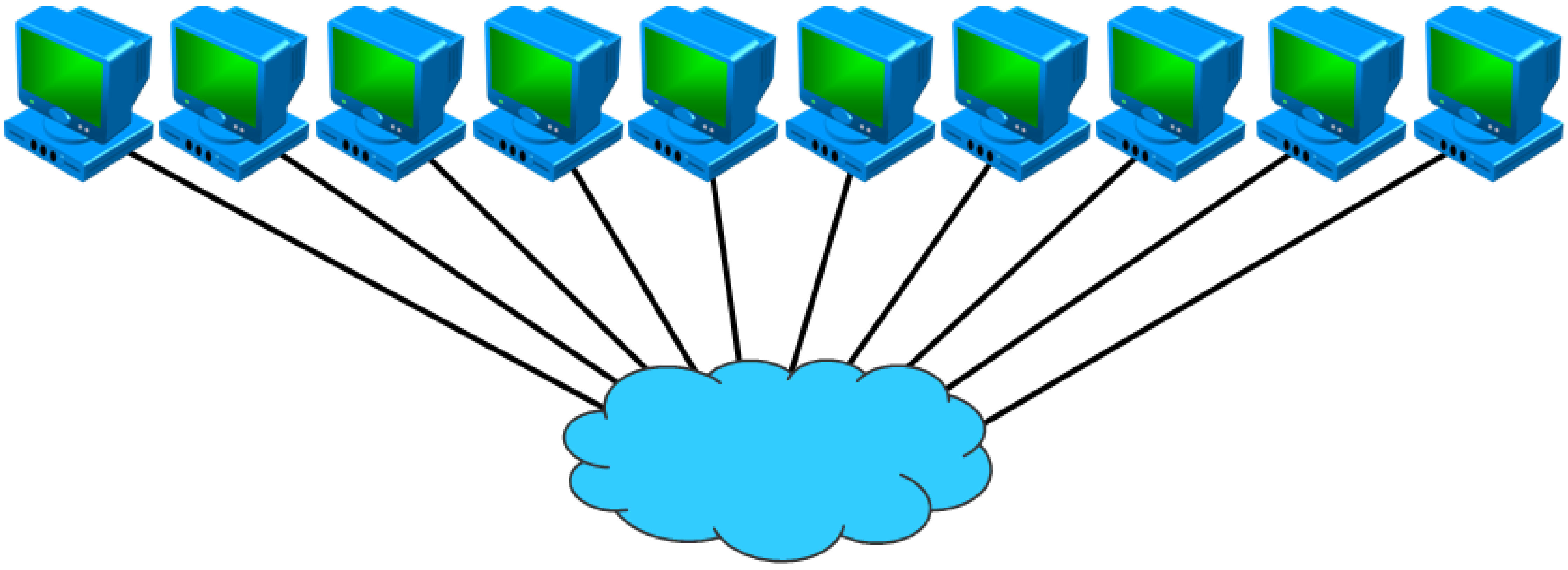
**Chart for the default subnet mask for the different classes.**

IP addresses are assigned to different organizations in blocks. These blocks are divided into five classes. But for the exam, you only need to know 3 of them (see below). They are class A, class B, and class C. You can tell by the number in the first octet which class an IP address belongs to.

| Class | First Octet Address | Default Subnet Mask |
|---|---|---|
| A | 1-126 | 255.0.0.0 |
| B | 128-191 | 255.255.0.0 |
| C | 192-223 | 255.255.255.0 |

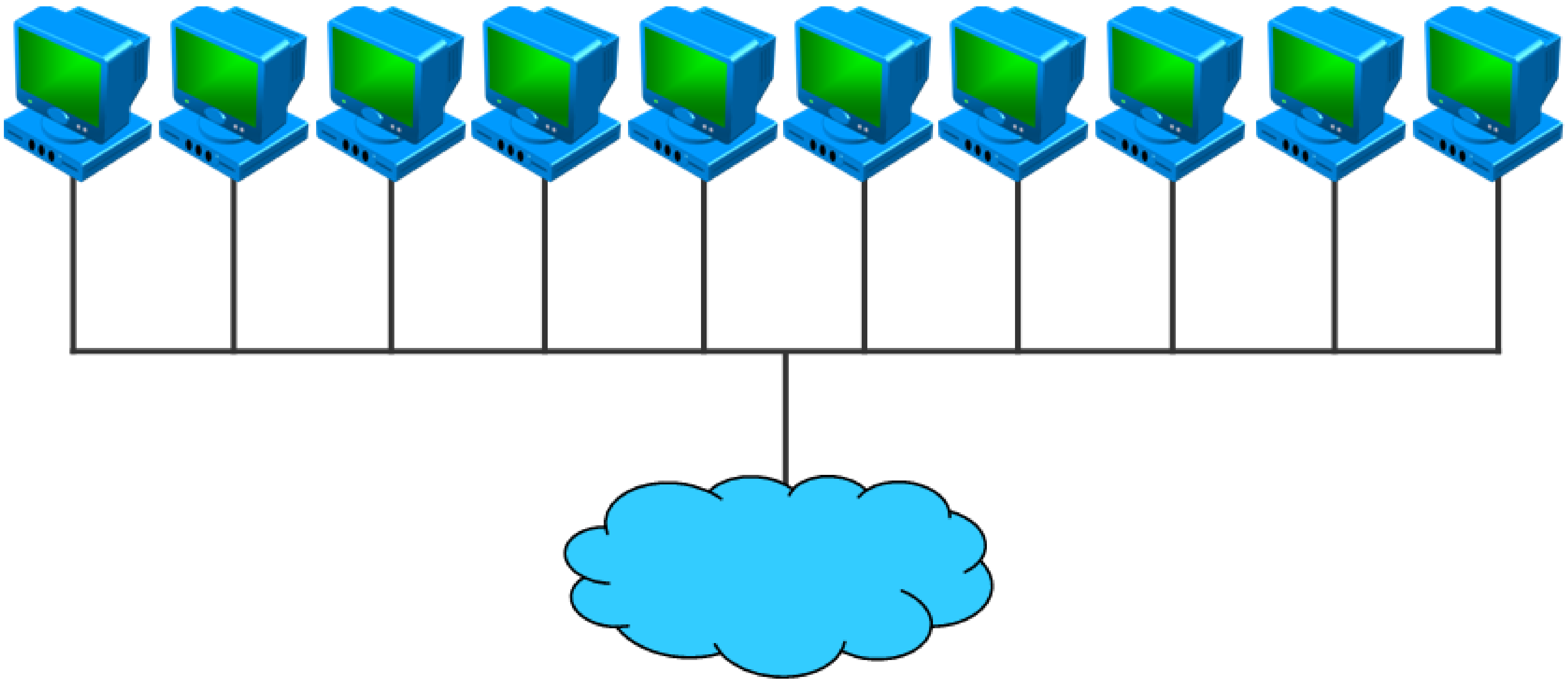
**NOTE: 127 is reserved for loopback testing.**

**Public IP addresses** are publicly registered on the internet. Which basically means that if you have a public IP address, you have access to the internet. But private IP addresses are different. A private IP is not publicly registered, so you can't directly access the internet with a private IP. So, for example, let's say you have a small business and you need 10 public IP addresses so your employees can access the internet. Now you could contact your ISP and ask them for these additional IP addresses, but that would be very expensive and unnecessary.



**10 public IP addresses being used.**

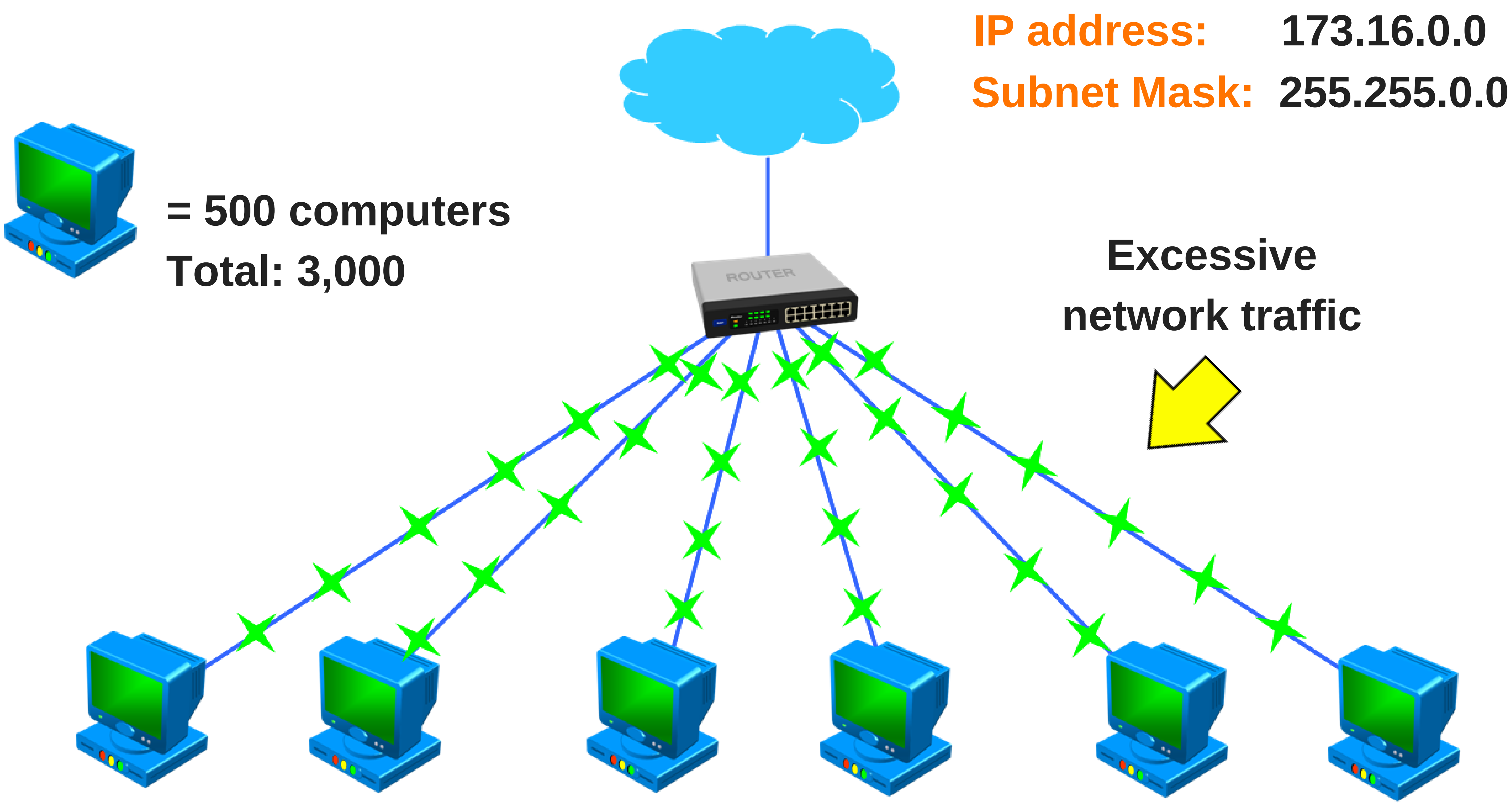
So that's where private IP addressing comes in. In private IP addressing, you can create these ten private IP addresses and just have one publicly registered IP address from your ISP (see below). These ten private IPs would then be translated into the one public IP, so your employees can have access to the internet. This not only saves money, but it also helps prevent having a shortage of public IP addresses.



**1 public IP address being used.**

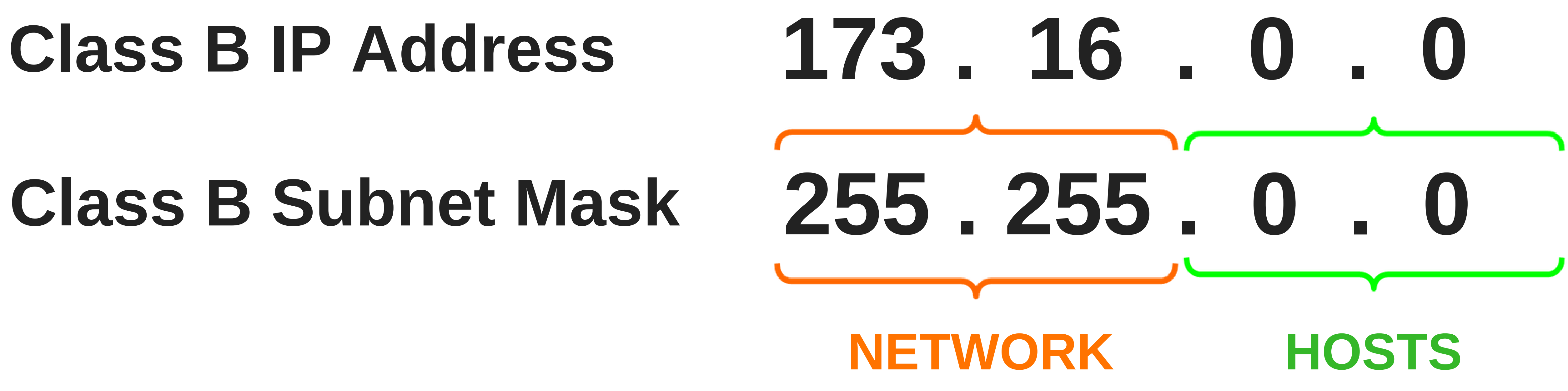
# Subnetting

The word subnet is short for subnetwork.  Which means a smaller network within a larger one.  **Subnetting** is basically breaking down a large network into smaller networks or subnets.  It's mainly done to make your network more manageable.  So for example, let's say you have a company with 3,000 employees and your ISP assigned you with a Class B IP address with a default subnet mask.  So as you know from the previous lesson, a Class B IP address will allow you approximately 65,000 IP's for all your computers.  Now you could put all of your employees in one large network, and if you had a small business, then this would be fine.  But if you had a fairly large business, with for example 3,000 computers, then this could be a problem because of traffic issues caused by so many broadcasts.  And if a problem word to occur, it'll be very hard to pinpoint on one large network.



Or, in another scenario, what if your business was scattered into three different geographical locations, then this would also be a problem.  So a better way would be to break down your network into smaller ones or subnets.

Subnetting is basically done by changing the default subnet mask by borrowing some of the bits that were designated for hosts and using them to create subnets. So, a default Class B subnet mask is 255.255.0.0.  The first two octets are for the network, the last 2 octets are designated for hosts.  So let's say we want to break down this network into three smaller ones.  The formula we would use is 2 to the *n* power -2, where *n* equals the number of bits we need to borrow from the host portion of the subnet mask.



**Class B IP Address** **173 . 16 . 0 . 0**

**Class B Subnet Mask** **255 . 255 . 0 . 0**

***formula*** $2^n - 2$ **n equals the number of bits**

So we need to make a custom subnet mask that is equal to at least 3 subnets or larger.  So if we put **2** in the place of n, then 2 x 2 = 4 - 2 = 2.  So 2 is not going to work because we need at least 3 subnets.  So let's try **3** and see if that works for us. So 2 x 2 x 2 = 8 and 8 - 2 would equal 6. So borrowing 3 bits will give us 6 subnets. Which will be fine because we need at least 3 subnets.

**255 . 255 . 0 . 0**

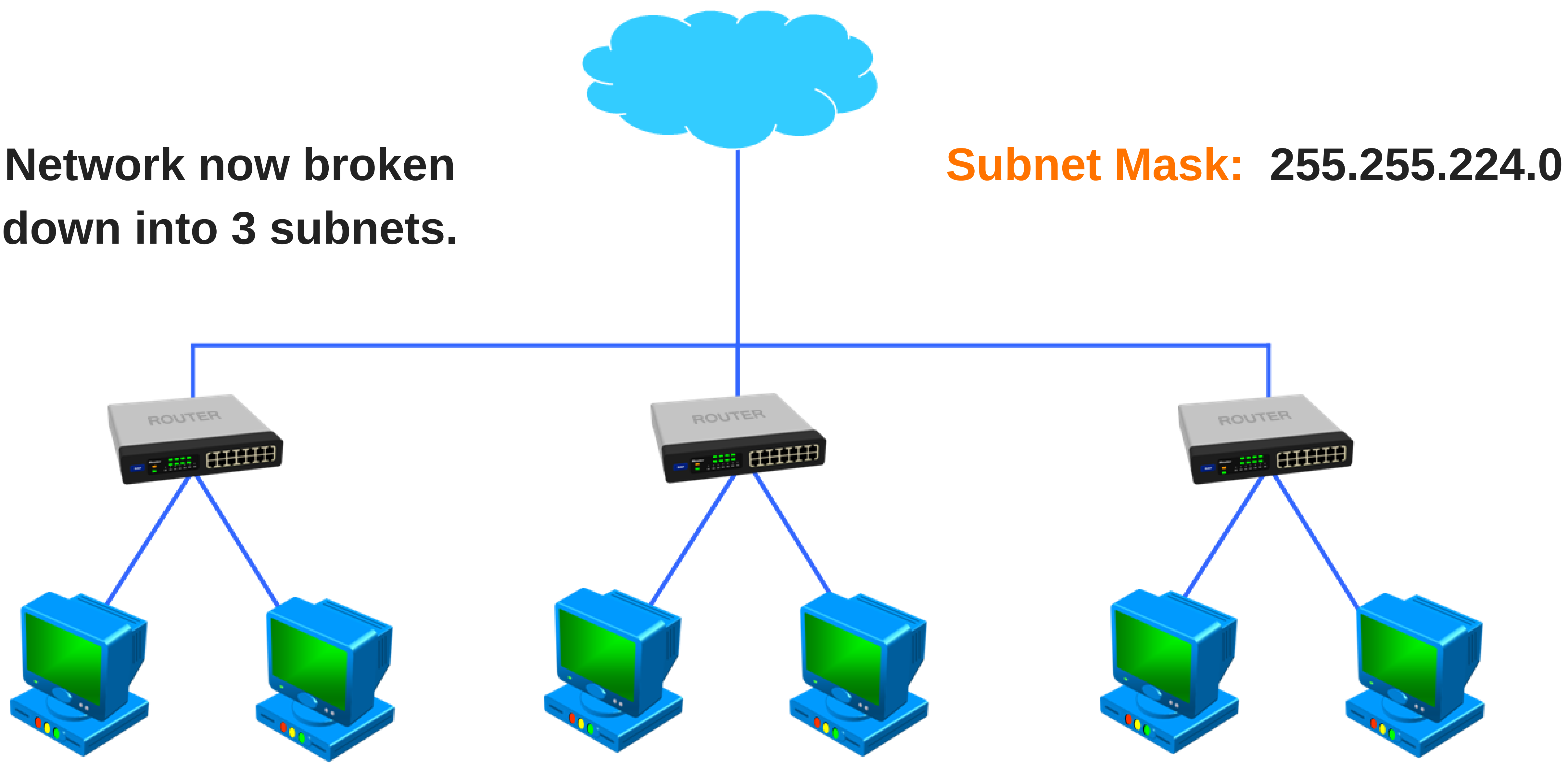
**11111111 . 11111111 . ~~000~~00000 . 00000000**

**Borrowing 3 bits from the host portion.**

**255 . 255 . 224 . 0**

**11111111 . 11111111 . 11100000 . 00000000**

So, our new custom subnet mask is **255.255.224.0** which will give us 8,000 hosts per subnet. And now our network is broken down into 3 subnets.

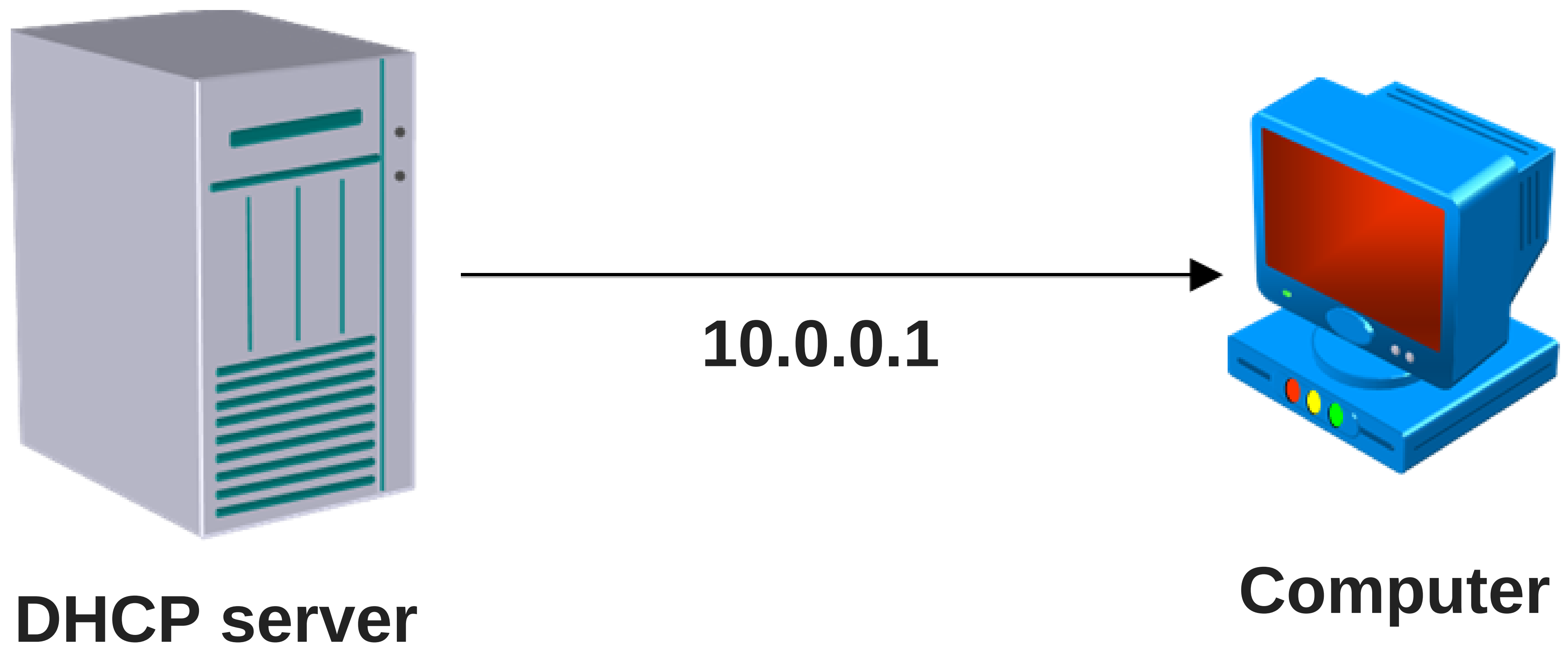


**Network now broken down into 3 subnets.**

**Subnet Mask: 255.255.224.0**

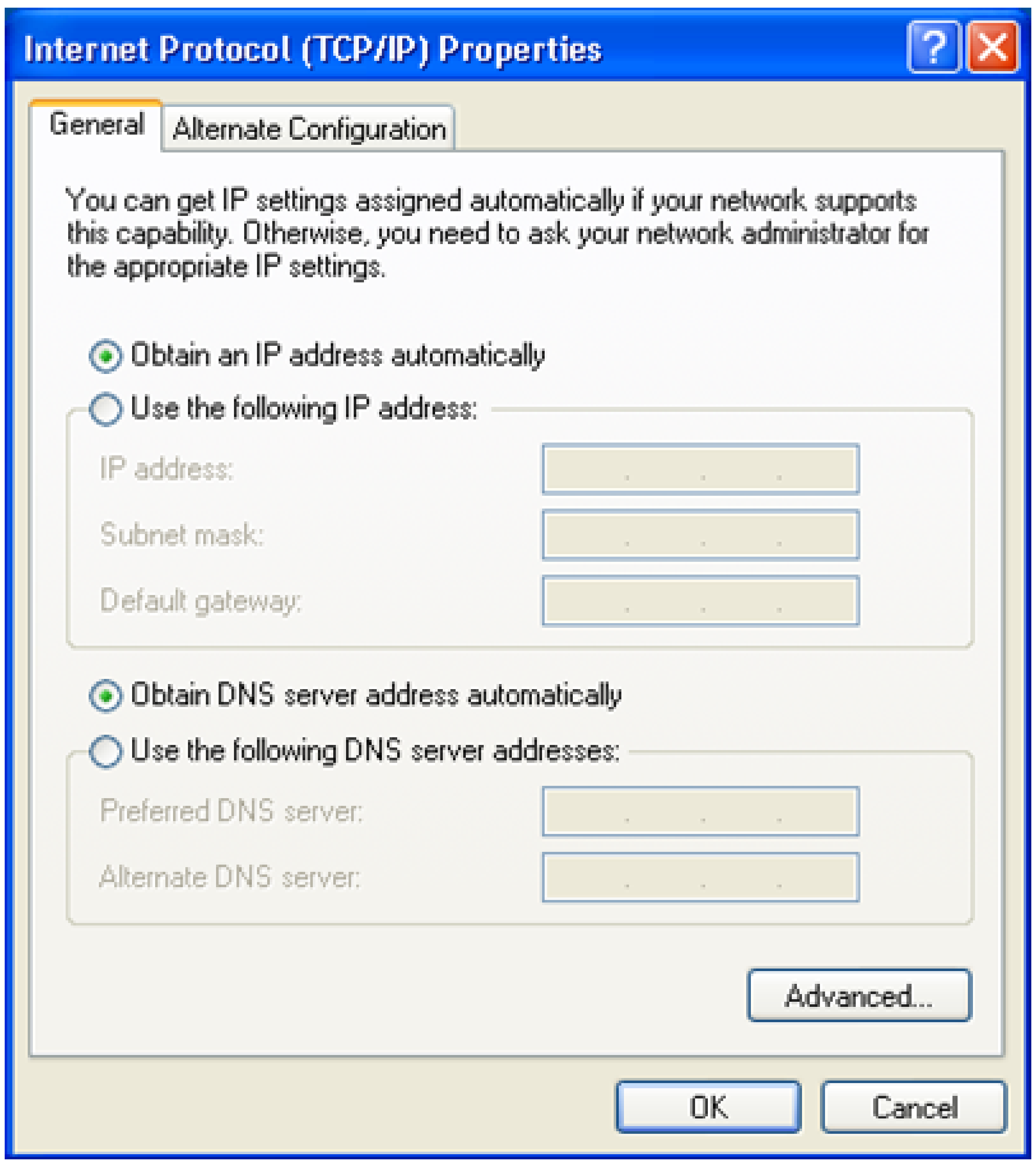
# IP Addressing Methods

Every computer on a network has to have an IP address for communication purposes. There are two ways that a computer can be assigned an IP address. It could be done either by using a dynamic IP, or a static IP. A **dynamic IP** is where a computer gets an IP address automatically from a DHCP server. **DHCP** stands for **dynamic host configuration protocol**. A DHCP server automatically assigns a computer with an IP address, and in addition to an IP address, it can also assign a subnet mask, default gateway, and a DNS server.



**DHCP server assigning an IP address to a computer.**

Below, we have the TCP/IP properties window open for the network interface card on a Windows machine. And as you can see, this computer is set to obtain an IP address automatically. So when you choose this option, the computer will send out a request for an IP address. Then the DHCP server will assign an IP address from its pool and deliver it to the computer. Dynamic IP addressing is the best choice because it makes managing a network a lot easier.



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

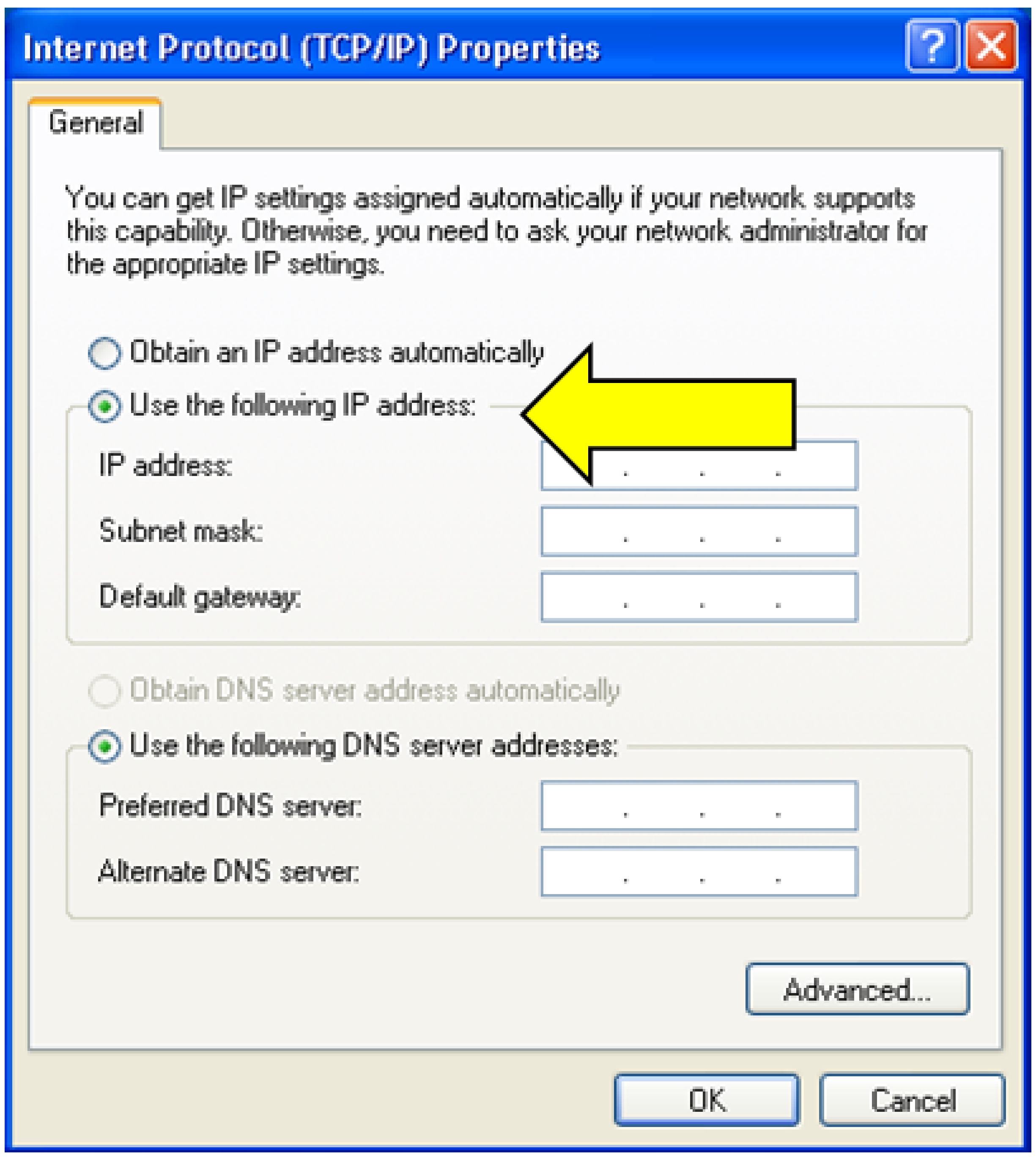
○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

**TCP/IP properties window for a Windows computer.**

You can also assign a computer with an IP address manually, and this is called a **static IP**. A static IP is where a user manually assigns an IP address for the computer. So there is no need for a DHCP server. This kind of IP addressing is also known as permanent, because unlike dynamic addressing, where the IP address can change automatically, a static IP only changes if a user decides to.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

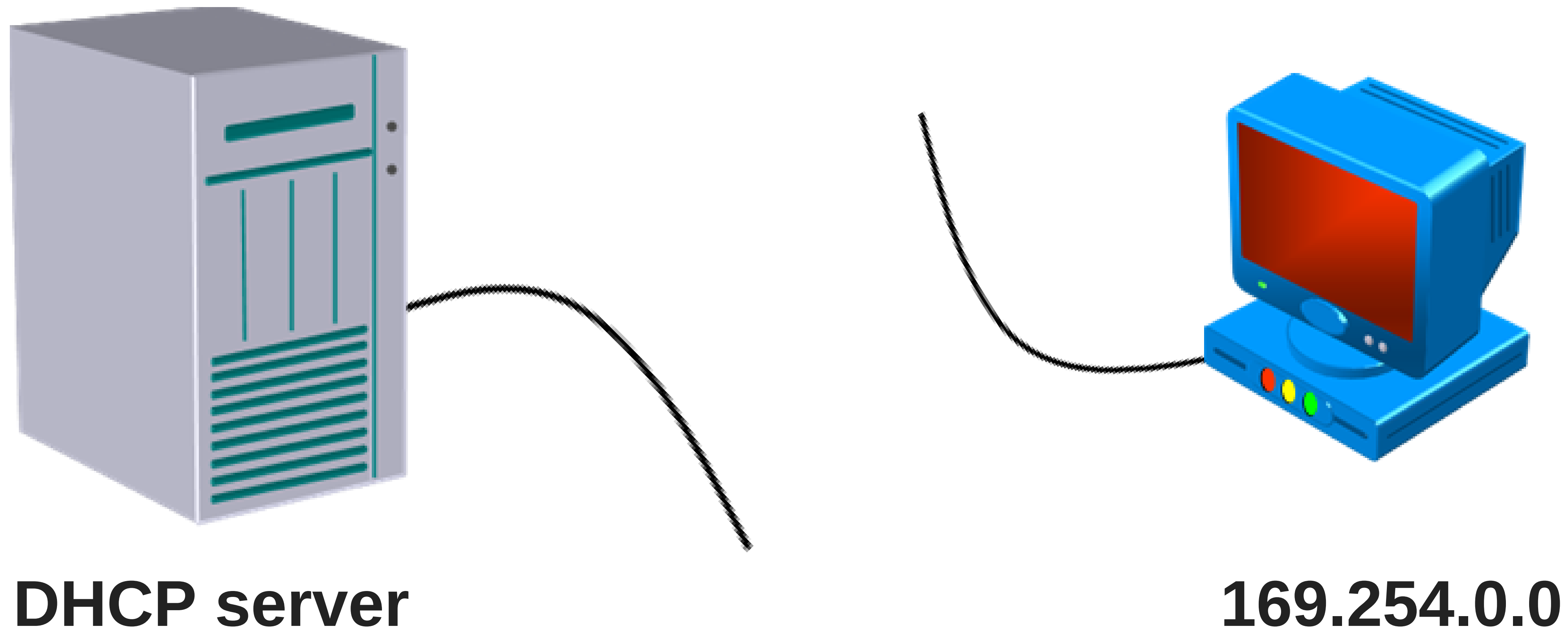
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

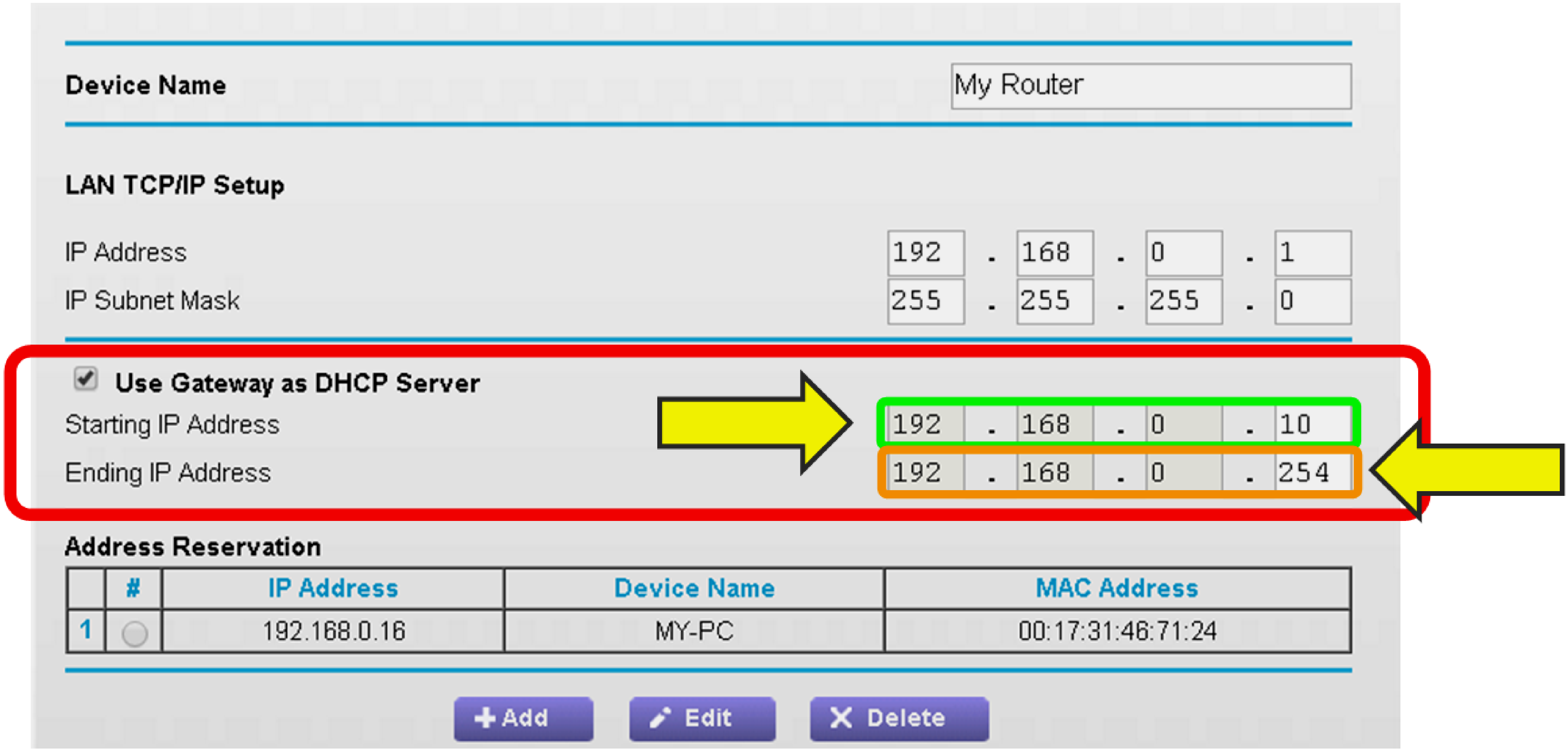
When a computer is set to automatically obtain a dynamic IP address, it gets the IP from a DHCP server. But what happens if this computer cannot reach a DHCP server? For instance, what happens if a DHCP server goes down or if the connection to the DHCP server is lost. If this happens, then the computers that are running Microsoft Windows 98 or later, the computer itself will assign its own IP address.



**Connection lost to the DHCP server. Windows assigns itself with an IP address (APIPA).**

This IP address will be on the 169.254.0.0 network. This type of self-assigned IP addressing is called **APIPA**, which stands for **automatic private IP address assignment**. Computers running Microsoft Windows 98 or later, do this so they can still be able to communicate with other computers on the same network that also have self-assigned IP addresses. If a DHCP server later becomes available, the computer changes its IP address to one that's obtained from a DHCP server.

A DHCP server assigns IP addresses to computers on a subnet from its **scope**.  A scope is a group of consecutive IP addresses for computers that automatically get their IP address from a DHCP server. So for example, below we see a scope of IP addresses from a DHCP server that's built into a Netgear router.



Device Name: My Router

LAN TCP/IP Setup

IP Address: 192 . 168 . 0 . 1

IP Subnet Mask: 255 . 255 . 255 . 0

☑ Use Gateway as DHCP Server

Starting IP Address: 192 . 168 . 0 . 10

Ending IP Address: 192 . 168 . 0 . 254

Address Reservation

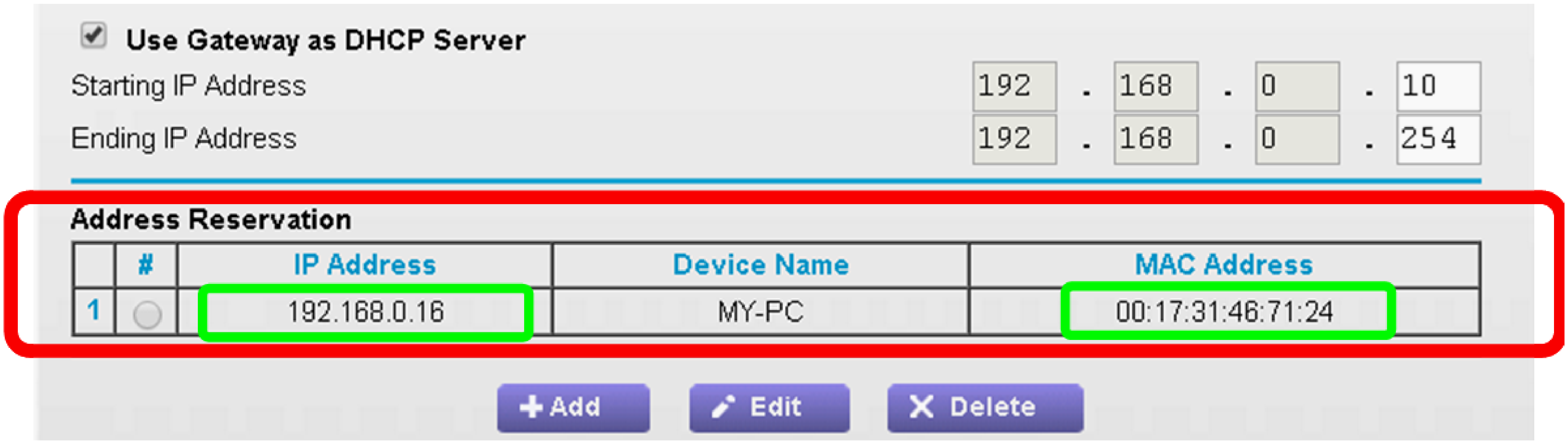
| | # | IP Address | Device Name | MAC Address |
|---|---|---|---|---|
| 1 | ○ | 192.168.0.16 | MY-PC | 00:17:31:46:71:24 |

**Scope settings in a Netgear router configuration page.**

The range starts with the 192.168.0.10 IP address and ends with the 192.168.0.254 IP address.  These values can be customized to either increasing or decreasing the range.

If you wanted a computer on your network to have a specific IP address all the time, you can create a **reservation** on the DHCP server.  A reservation ensures that a specific computer or device, identified by its MAC address, will always be given the same IP address when that computer or device accesses the DHCP server.

So for example, on this router, if I create a reservation for my computer, the DHCP server on the router will recognize my MAC address and will always give me the same specific IP address.  Reservations are not typically given to regular computers.  They are typically given to special devices or computers, such as network printers and servers, which require using the same IP address constantly.



☑ Use Gateway as DHCP Server

Starting IP Address 192 . 168 . 0 . 10

Ending IP Address 192 . 168 . 0 . 254

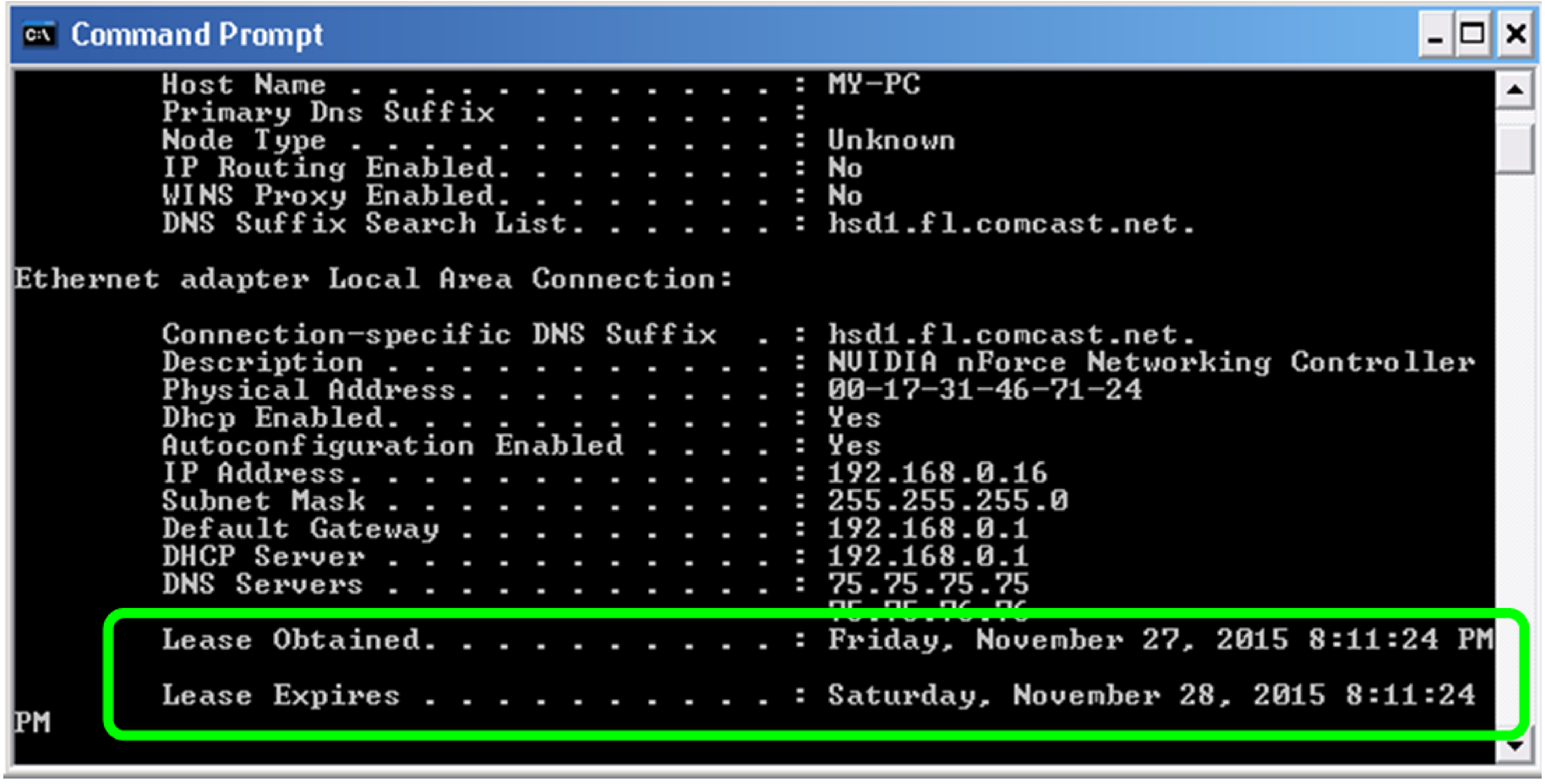
Address Reservation

|   | # | IP Address | Device Name | MAC Address |
|---|---|---|---|---|
| 1 | ○ | 192.168.0.16 | MY-PC | 00:17:31:46:71:24 |

**Address reservation settings in a Netgear router.**

When computers obtain an IP address from a DHCP server, the DHCP server assigns the IP address as a **lease**.  So the computer doesn't actually own the IP address, it's actually a lease.  A lease is the amount of time an IP address is assigned to a computer.  The lease duration could be a day or more depending on the lease settings of the DHCP server.  So for example, if I do an ipconfig /all in a command prompt on my computer (see below), you can see that the DHCP server on my router has assigned my computer an IP address with a lease of one day.  Typically a DHCP server will automatically renew the IP address for you.

So you won't have to do anything or even notice that the IP address is being renewed.  You can just continue on like normal and go about your business.



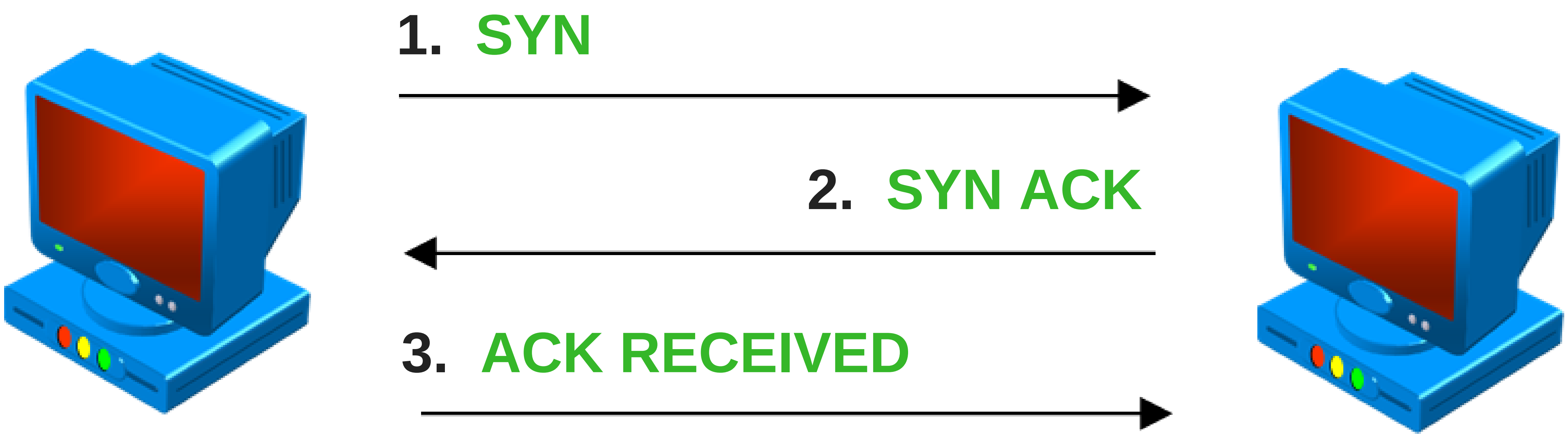
```
        Host Name . . . . . . . . . . . . : MY-PC
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : hsd1.fl.comcast.net.

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : hsd1.fl.comcast.net.
        Description . . . . . . . . . . . : NVIDIA nForce Networking Controller
        Physical Address. . . . . . . . . : 00-17-31-46-71-24
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.0.16
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1
        DHCP Server . . . . . . . . . . . : 192.168.0.1
        DNS Servers . . . . . . . . . . . : 75.75.75.75
                                            75.75.76.76
        Lease Obtained. . . . . . . . . . : Friday, November 27, 2015 8:11:24 PM

        Lease Expires . . . . . . . . . . : Saturday, November 28, 2015 8:11:24
PM
```

**IP address lease duration.**

As stated previously, when a computer needs an IP address, it will broadcast its request to a DHCP server. If a DHCP server is on the same subnet as the computer, in other words, if they are using the same IP address settings, then the DHCP server will receive the request and assign the computer an IP address. However, if the computer and the DHCP server are not on the same subnet, in other words they are not using the same IP address settings, then the DHCP server will not receive the request because broadcasts cannot go outside their own subnet.   So that's where a **DHCP relay** comes in.  A DHCP relay or **IP helper** is a service that is enabled on a router that relays a DHCP broadcast it receives, and then forwards it.  So when a computer broadcasts a request for an IP address, and if the DHCP server is on a different subnet, the DHCP relay on the router will receive the broadcast and will forward the broadcast to the DHCP server.  Then the DHCP server will send the IP address back to the computer.

# TCP/IP Protocol Suites

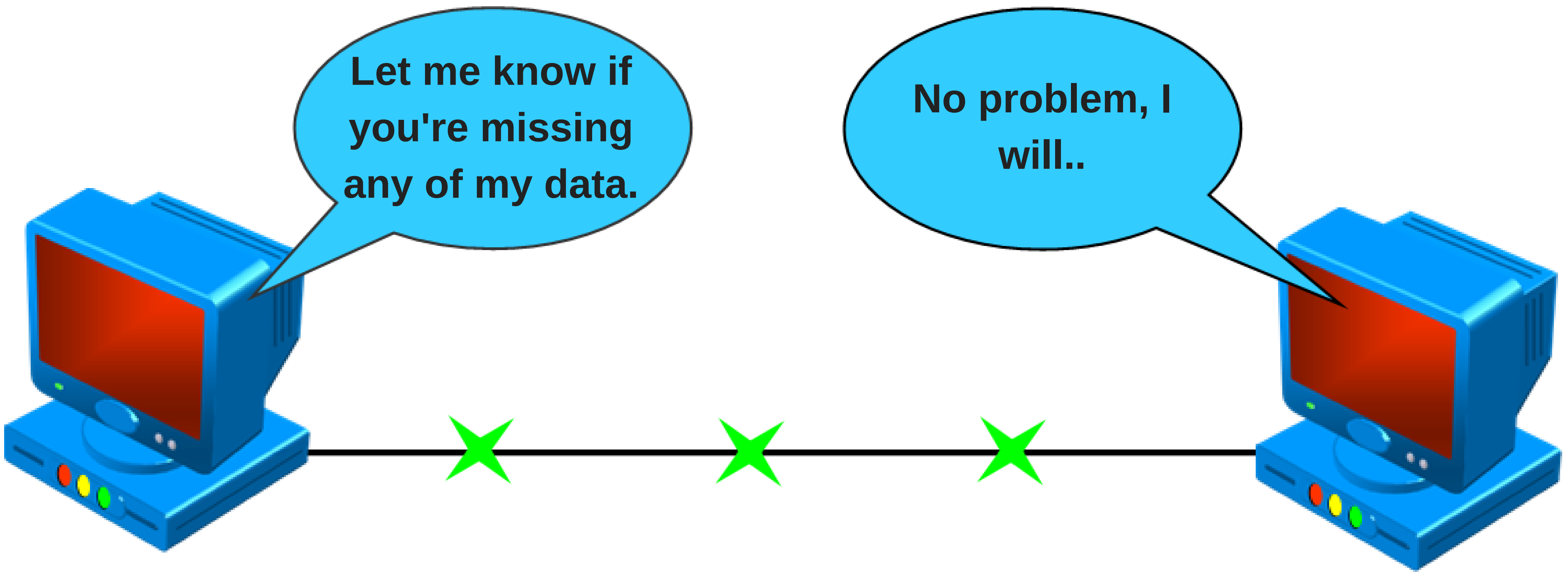
**TCP** (**transmission control protocol**) is one of the main protocols used in a TCP/IP network.  Now, this is a connection oriented protocol, which basically means that it must first acknowledge a session between two computers that are communicating.  And it does this by using a three-way handshake.  The first step is that a computer will send a message called a SYN.  Then the receiving computer will send back an acknowledgment message telling the sender that it has received the message.  And finally, the sender computer sends another acknowledgment message back to the receiver.



**TCP 3-way Handshake**

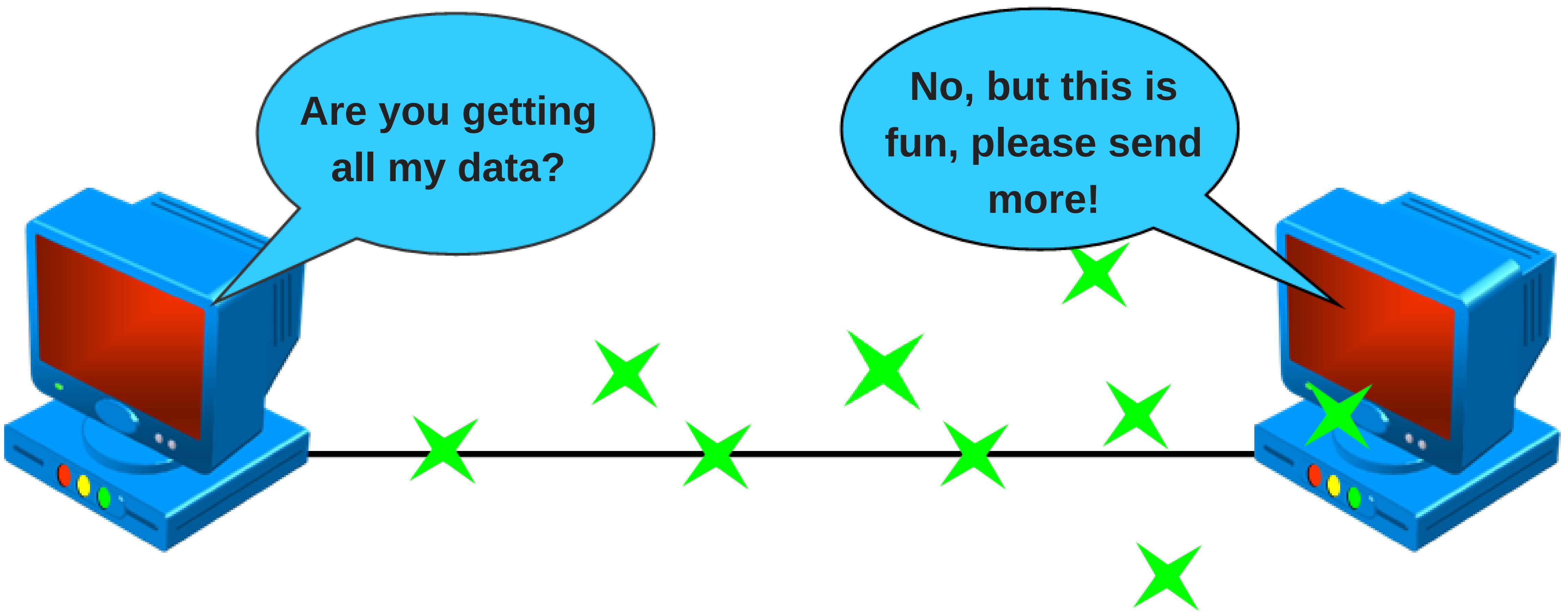
Once this has taken place, data can be delivered. Another important thing to remember about TCP is that it guarantees the delivery of the data.  So if a data packet goes astray and doesn't arrive, then TCP will resend it.

Now, **UDP** (**user datagram protocol**) is very similar to TCP. UDP is also for sending and receiving data, but the main difference is that UDP is connectionless. Which means that it does not establish a session and does not guarantee data delivery. So when a computer sends their data, it doesn't really care if the data is received at the other end. And that's why UDP is known as the 'fire and forget' protocol because it sends data and it doesn't really care what happens to it.



**TCP**

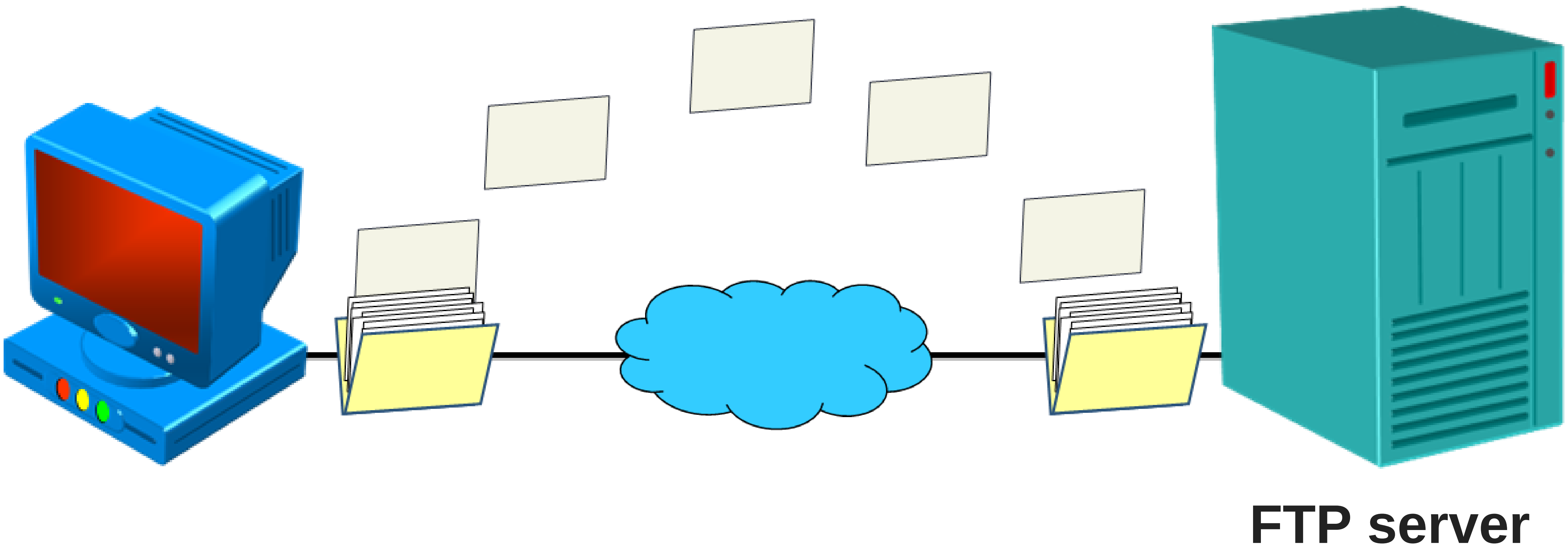
**Guarantees data delivery.**


Are you getting all my data?
No, but this is fun, please send more!

**UDP**

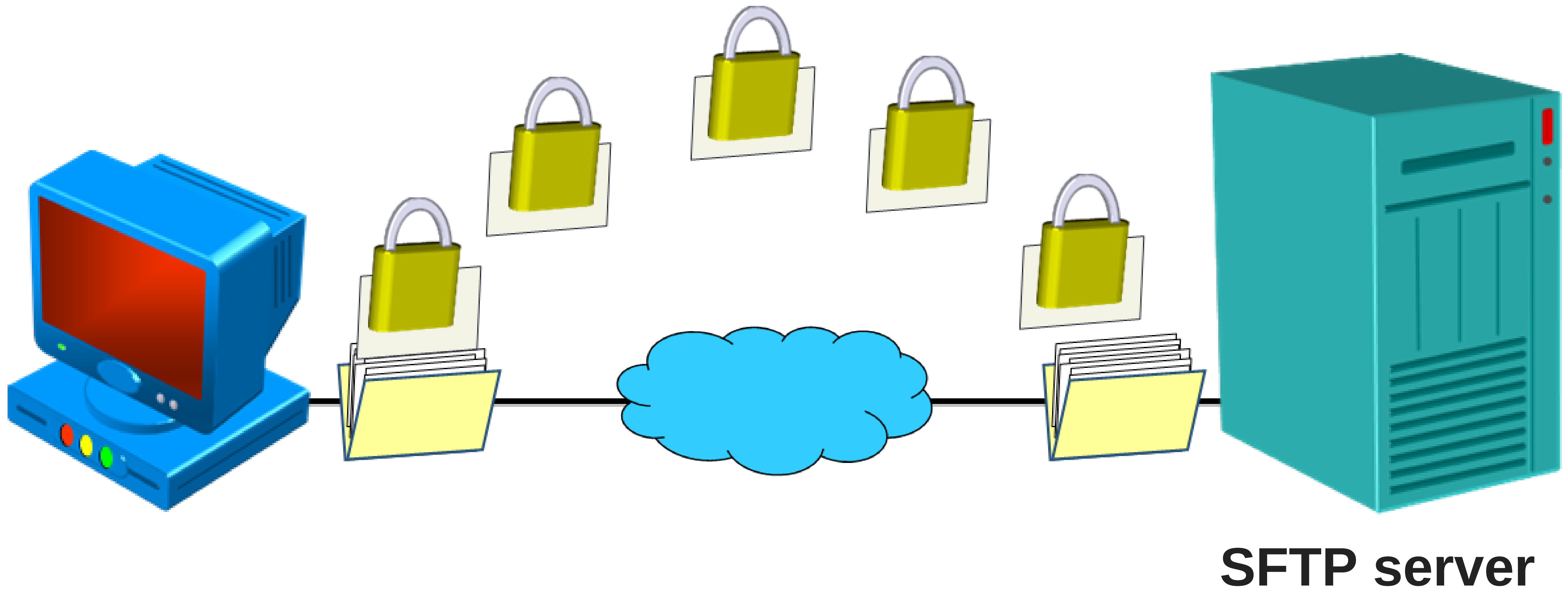
**Does not guarantee data delivery.**

**FTP** stands for **file transfer protocol**, and this is the standard protocol that is used by web users to upload and download files between computers on the internet. So if a user wanted to make their files available to download for other users, all they would have to do is simply upload their files to an FTP server and then a user can simply download them.  Now there are a few ways to transfer files using FTP.  You can use your standard internet browser or you can use special FTP software.  It is also important to note that FTP is a connection oriented protocol that uses TCP for file transfer.



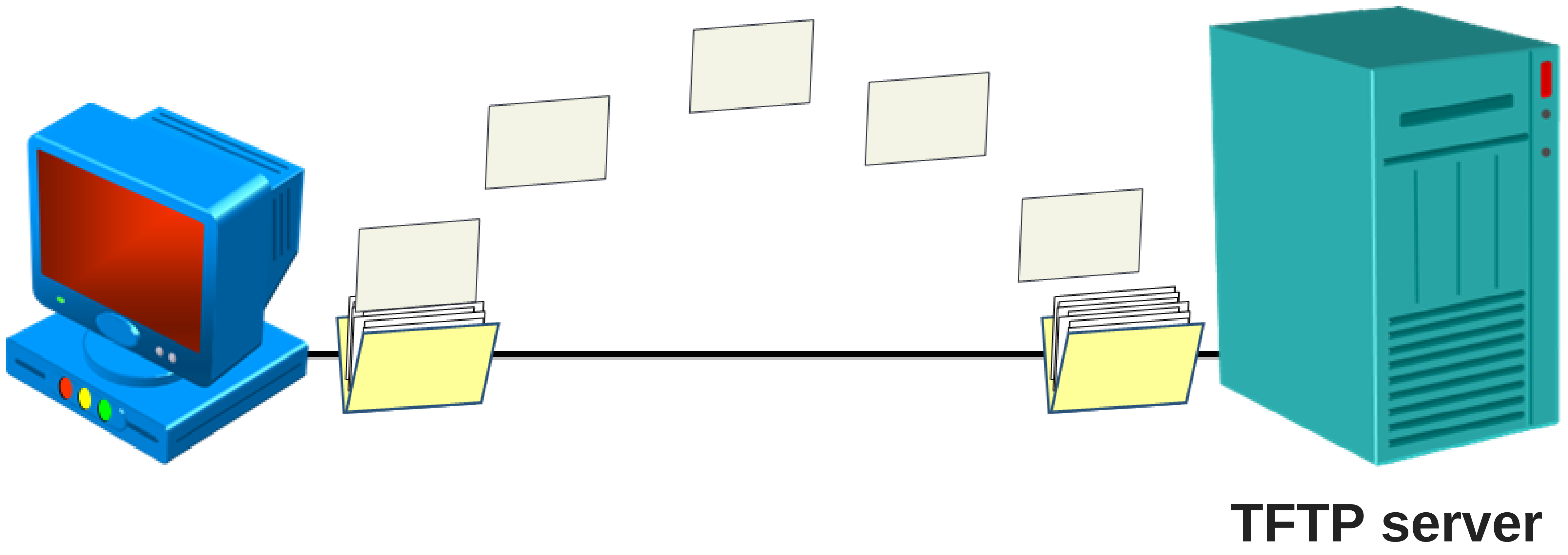
**A computer downloading files using FTP.**

Now **Secure FTP** is just like FTP, except that it adds a layer of security.  The data using secure FTP is actually encrypted using secure shell during data transfer.  So no sensitive data, like passwords, are sent in clear text.



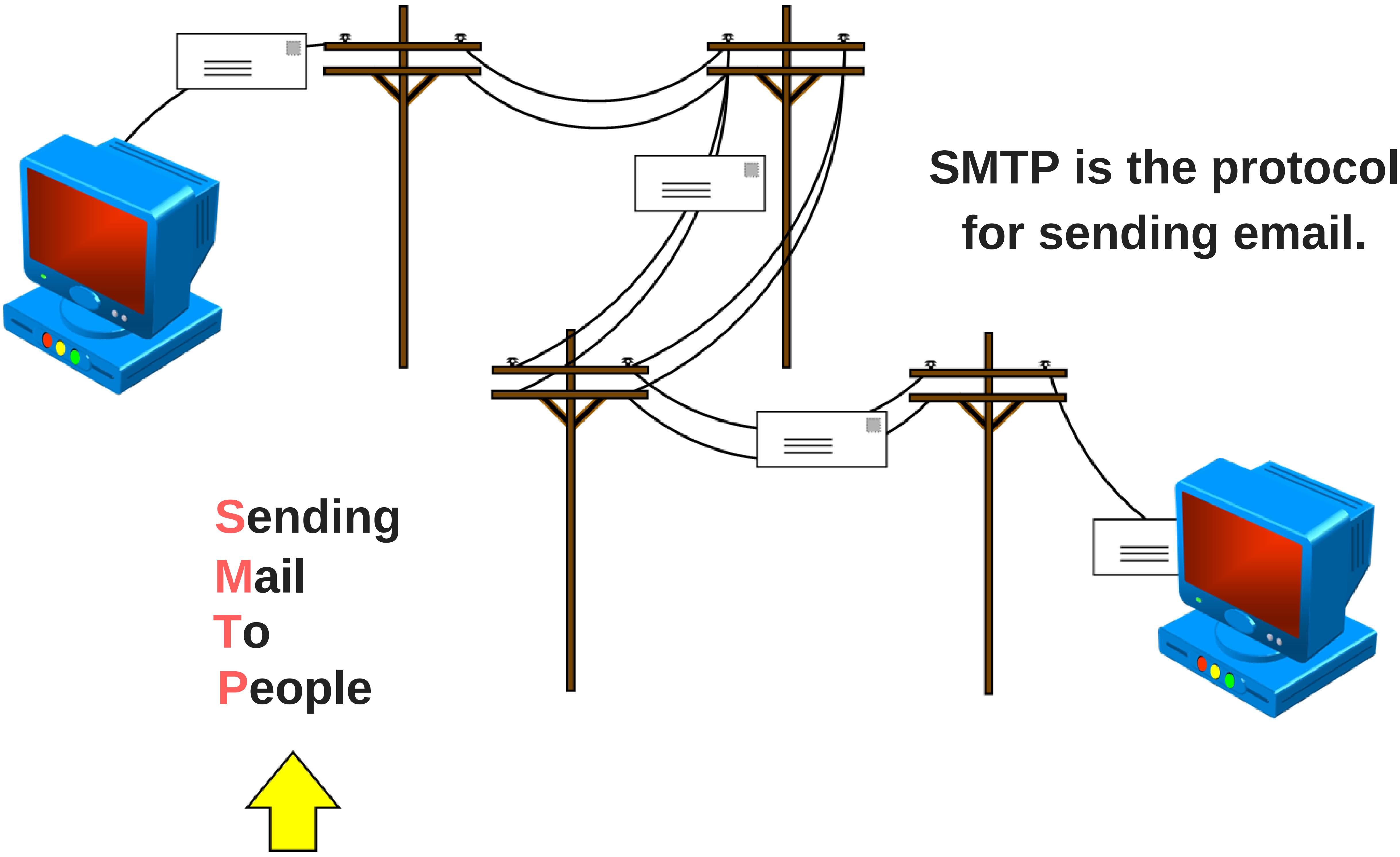
**A computer downloading files using SFTP.**

**TFTP** stands for the **trivial file transfer protocol**. This is a very simple transfer protocol. It is not used to transfer files over the internet like FTP does. It's mainly used for transferring files within the same network and it does not provide any security during the transfer. And unlike FTP, that uses the TCP protocol for file transfer, TFTP is a connectionless protocol that uses UDP as its transfer protocol.



**A computer downloading files within a local area network (not over the internet) using TFTP.**

**SMTP** stands for **simple mail transfer protocol**. Now this, as you might have guessed, is the protocol that is used to send email. A good way to remember this is by looking at the acronym SMTP, and translating that to: ‘sending mail to people’. SMTP uses the TCP protocol, and as you know by now, it is connection oriented. So if an email you send does not reach its destination, you'll get that familiar mail delivery error in your mailbox, informing that the email you sent, failed.



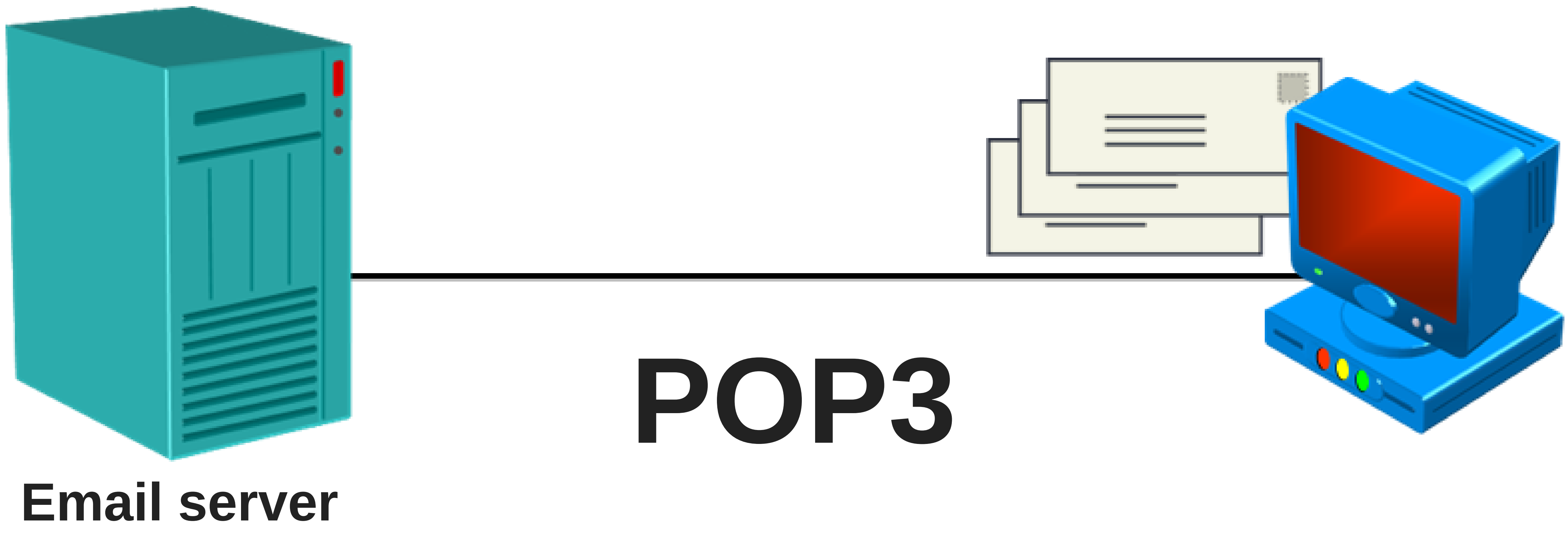
**SMTP is the protocol for sending email.**

**Sending**
**Mail**
**To**
**People**

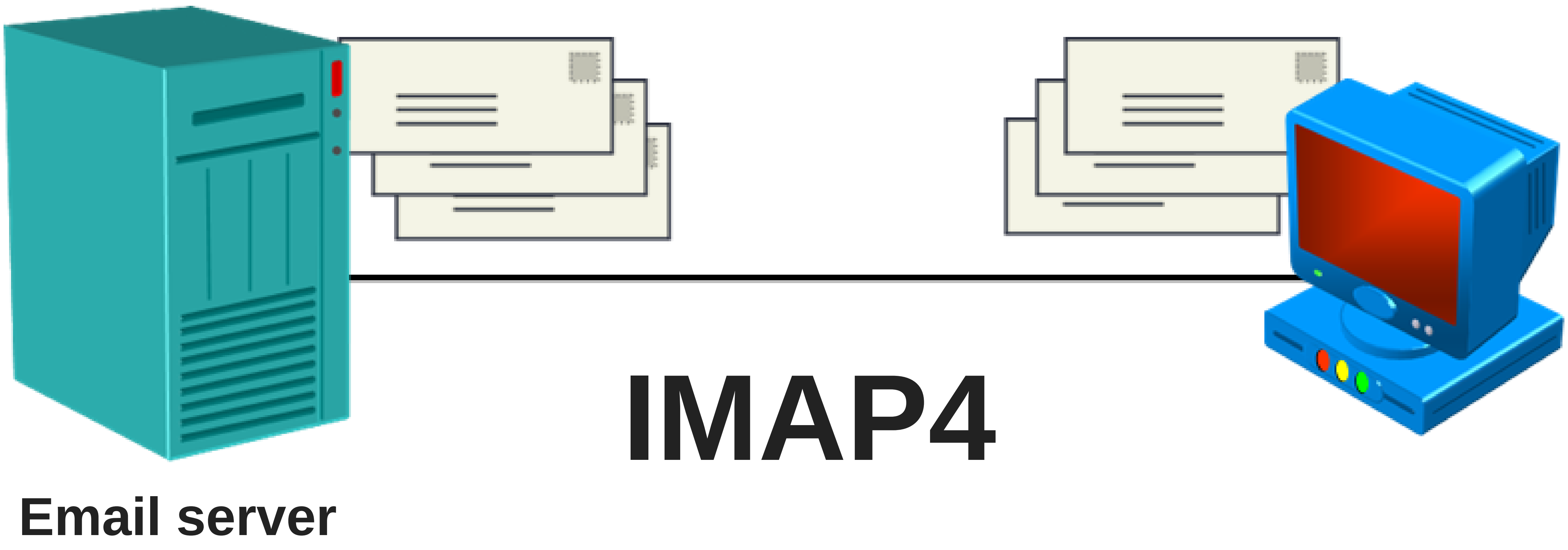
**A quick way to remember what SMTP does.**

Where SMTP is used for sending email, **POP3** is the protocol that is used for receiving email. Whenever an email arrives at your email server, you can retrieve it using the POP3 protocol and download it to your computer. The main characteristic about POP3 is that all it does is grab the email from the email server and downloads it to your computer. It does not sync any email or folders from the mail server unlike IMAP4, which we'll talk about next.  POP3 strictly downloads the email.  Typically when your email application using POP3 retrieves the email from the mail server, no copy of the email is left on the email server, unless you specify in your email application to keep a copy on the email server.  POP3 is commonly used with email applications such as Microsoft Outlook.

**IMAP4** is another protocol that is used for receiving email.  IMAP4 is similar to POP3 because they are both used for receiving email from an email server, but IMAP4 has better features.  With IMAP4 you can access and manage your email on the server from your local computer.  So if you wanted to read your email and keep a copy of it on the server, IMAP4 will allow you to do just that.  And unlike POP3, IMAP4 syncs your email and your email folders from the mail server with all your devices.  And IMAP4 is also commonly used with Microsoft Outlook.



**POP3 only downloads the email.  Does not keep a copy of the email on the email server.**



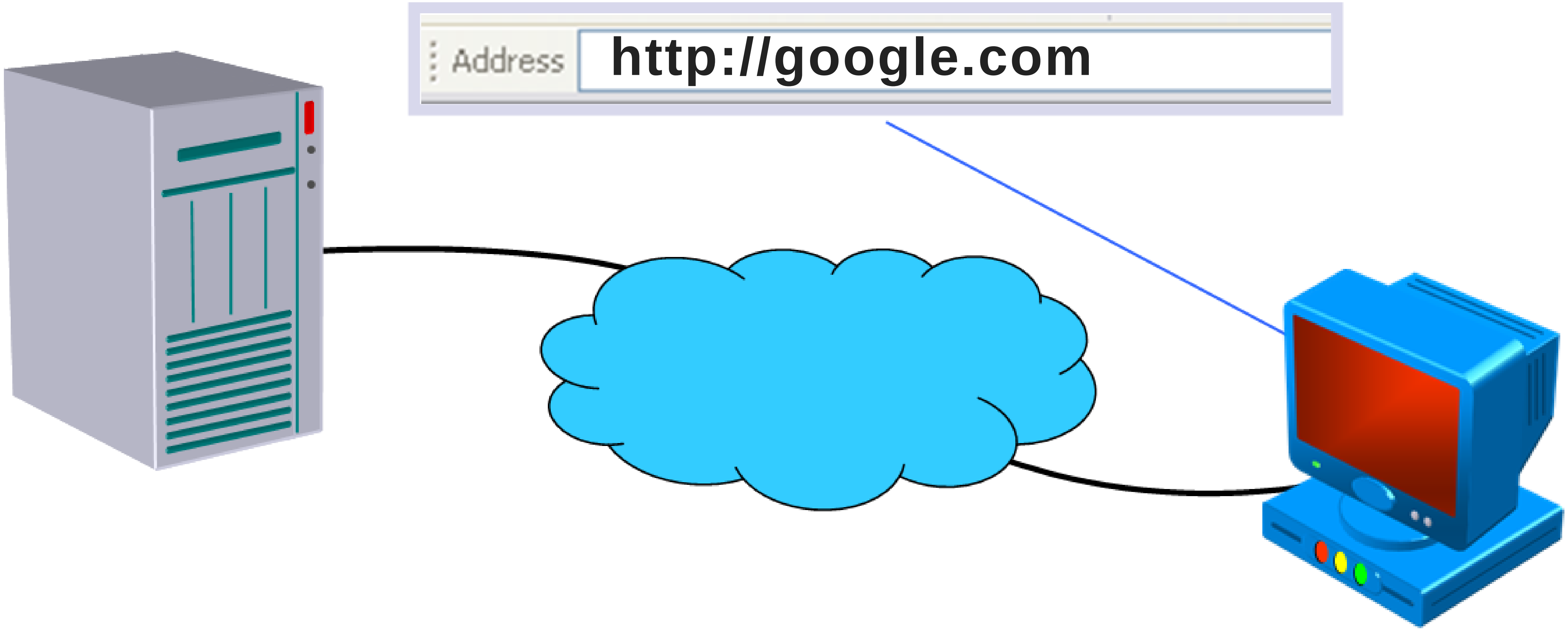
**IMAP4 syncs email and folders with all your devices.  Keeps a copy of the email on the email server.**

**NTP** stands for **network time protocol**, and this is an internet standard that is used to synchronize the clocks of computers with the US Naval Observatory master clocks.  This protocol runs on each computer and it sends out periodic requests to the server to make sure the time is in sync.

**SCP** stands for **secure copy protocol**.  This protocol simply uses secure shell to safeguard data as it's being transferred over a network.

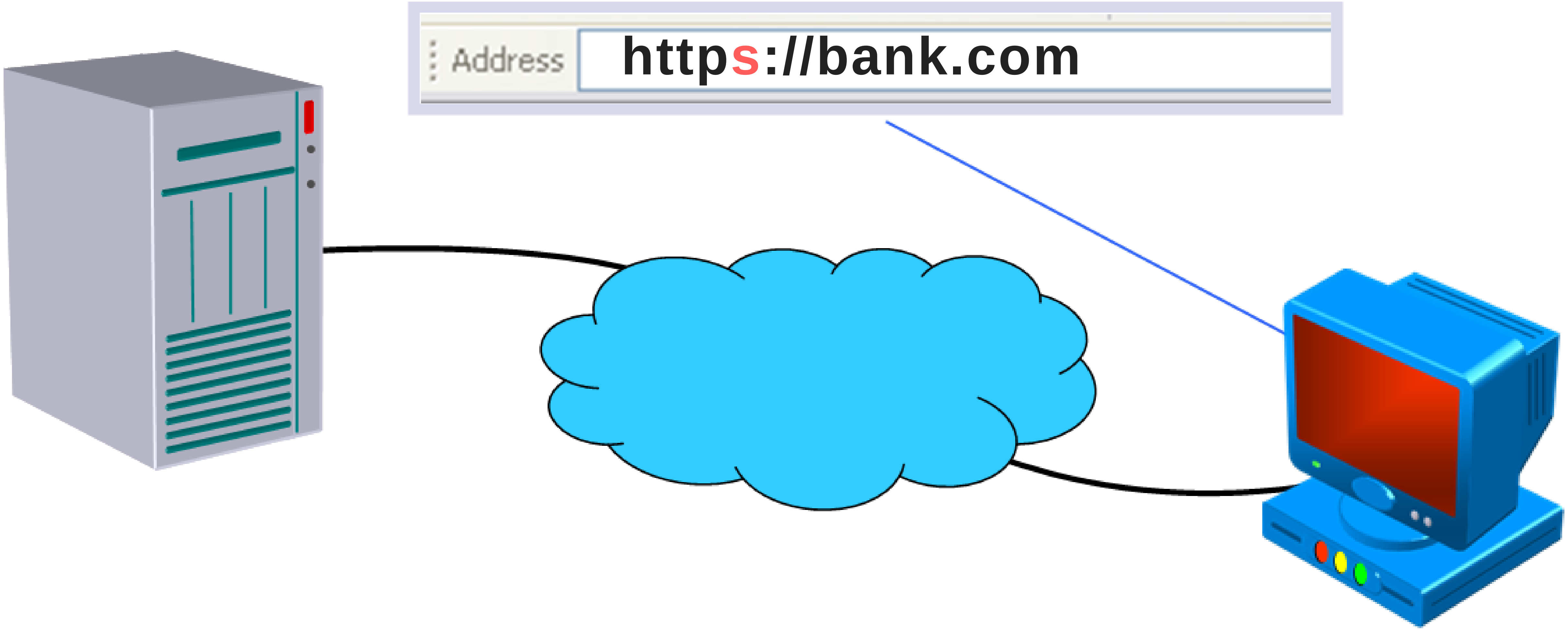
**Secure copy protocol**

**HTTP** stands for **hypertext transfer protocol**. Now, this is probably the most widely used protocol in the world today. HTTP is the protocol that is used for viewing web pages on the internet. So when you type in a web address, for example, google.com, you'll notice that HTTP is automatically added at the beginning of the address. This indicates that you are now using HTTP to retrieve this web page.



**HTTP being used to retrieve the google.com webpage.**

In standard HTTP, all information is sent in clear text. Now, normally this would be okay if you were just browsing regular websites. But if you were at a website where you had to enter sensitive data, such as passwords or credit card information, then this would be a problem as far as security. **HTTPS** stands for **secure hypertext transfer protocol**, and this is HTTP with a security feature. HTTPS encrypts the data that is being retrieved by HTTP. So for example, if you wanted to go to your bank's website to check your account, you would notice that an ‘S’ will be added to the HTTP in the web URL.

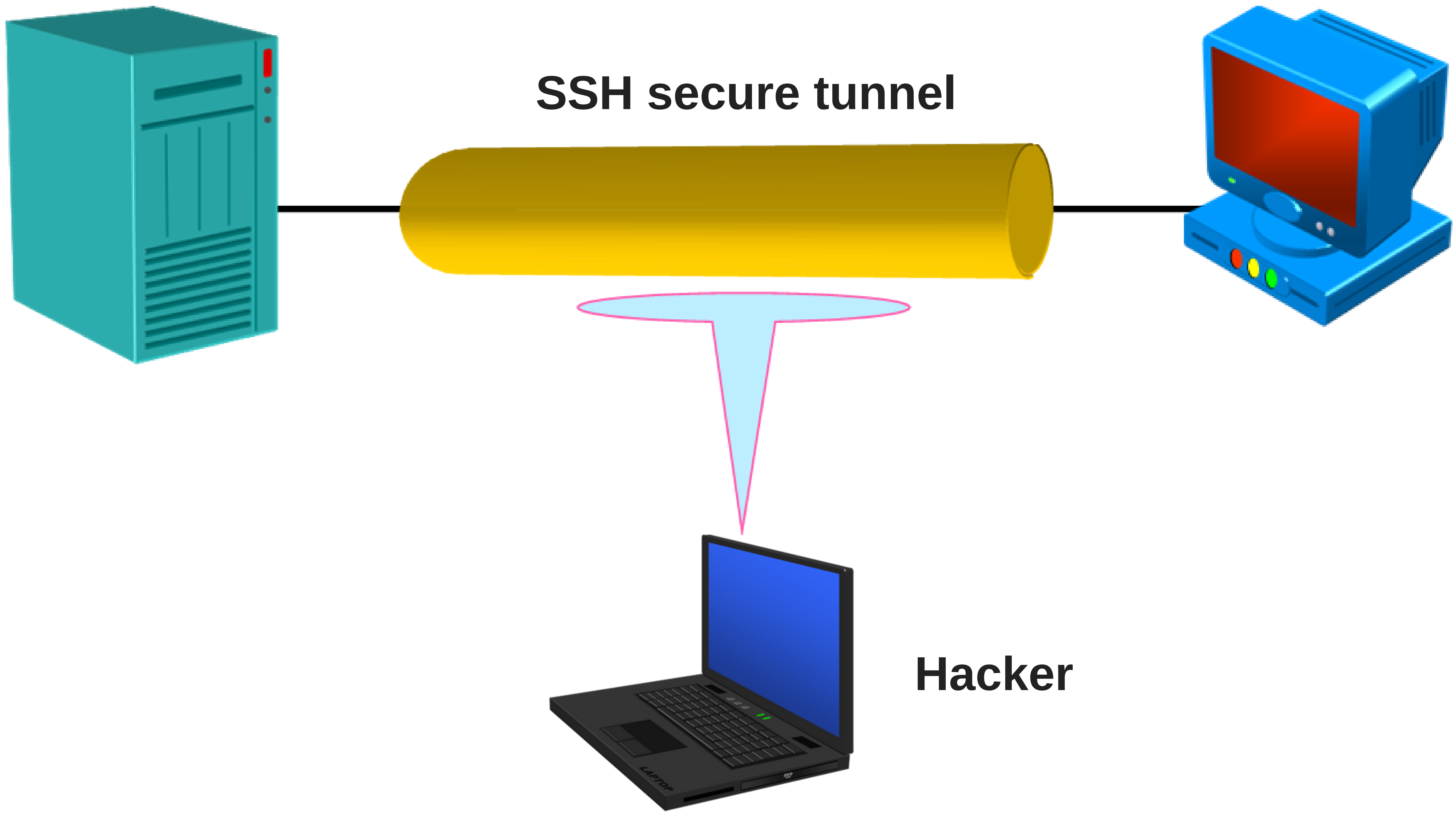


**An 'S' has been added to http. This indicates that secure HTTP is being used.**

This 'S' indicates that you are now using HTTPS and have entered a secure website where sensitive data is going to be passed, and that data needs to be protected. Some other examples where HTTPS is used, would be email servers and e-commerce (shopping) websites.

**Telnet** a terminal emulation program that is used to access remote servers. It's a simple tool that runs on your computer and it will allow you to send commands remotely. And because it only sends commands and not graphics, it's very fast. But the drawback is that it's not secure. All commands are sent in clear text. So today, telnet is mainly used to access devices within a local network and not over the internet.

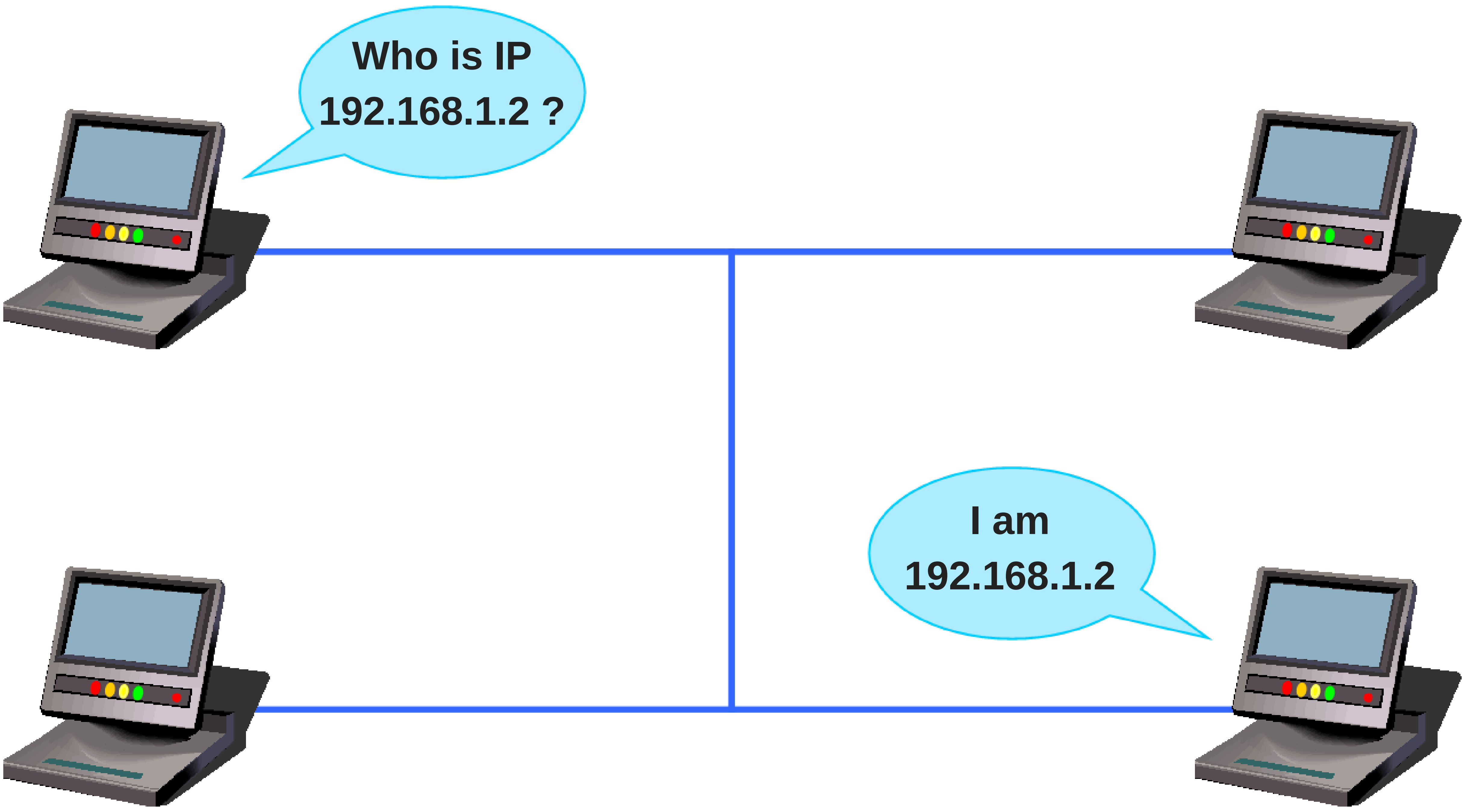
Now **SSH** or **secure shell** is a better alternative to telnet. Secure shell protects the data from being attacked or stolen as it's being transferred over a network. So for example, if you were sending sensitive, like a login or password, a potential hacker could be listening and steal the data. And that’s the reason for secure shell. Secure shell acts like a secure tunnel that forms around the data transfer and protects it from potential threats.



**SSH acts like a secure tunnel, protecting the data from being stolen.**

**SNMP** or **simple network management protocol** is used for network management. It's used to manage network devices such as routers, printers, and servers.

**ARP** stands for **address resolution protocol**. This is a protocol that is used to resolve IP addresses to MAC addresses. Whenever a computer needs to communicate with another computer on a local area network, it needs the MAC address for that computer. So for example, let's say a computer wants to communicate with another one. Now it will first look at its internal list, called an ARP cache, to see if the targeted computer's IP address already has a matching MAC address in its table. And if it doesn't, it will send out a broadcast message on the network asking which computer has the IP address.

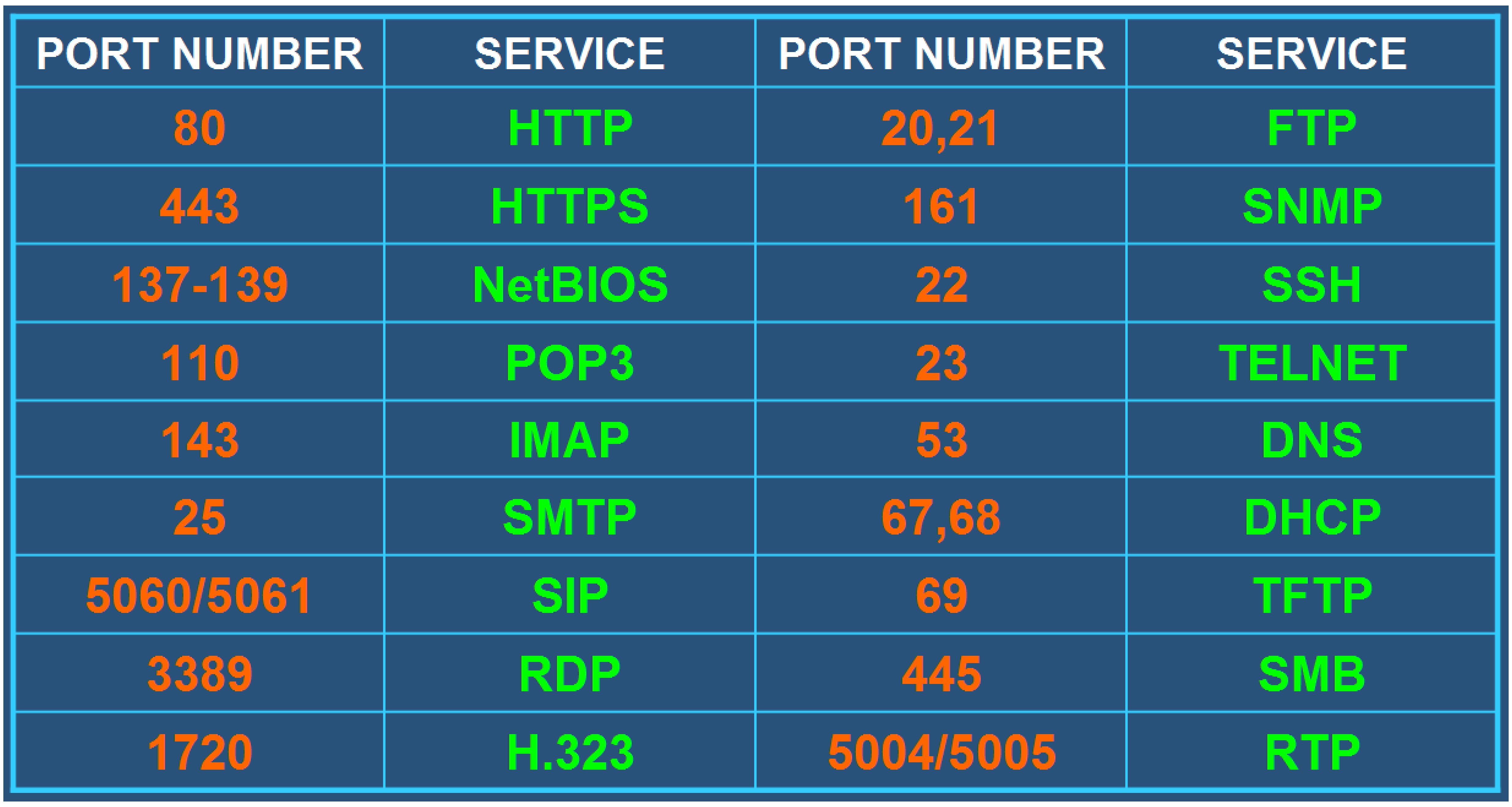


The computer that has the matching IP address will then respond back informing that it has the IP it's looking for. Then the original computer will ask for their MAC address.  Then once it receives the MAC address, the communication will take place between the two.

**RARP** stands for **reverse address resolution protocol**.  And as you might have guessed, this is just the opposite of ARP.  It’s used to resolve MAC addresses to IP addresses.

# Ports

A **port** is a logical connection that is used by programs and services to exchange information.  These ports have a unique number that identifies them.  The number ranges from 0 to 65535, but for the exam, you only need to know a few of them.  So, below is a chart of the ports that you need to know for the exam.  Some of these ports are very common and are used every single day, such as port 80, which is used for bringing up web pages on the internet.  Another one is port 443, which is used for logging into secure web pages that require a login and password.  And another common one is port 25, and this is used for sending email from an email application such as Microsoft Outlook.



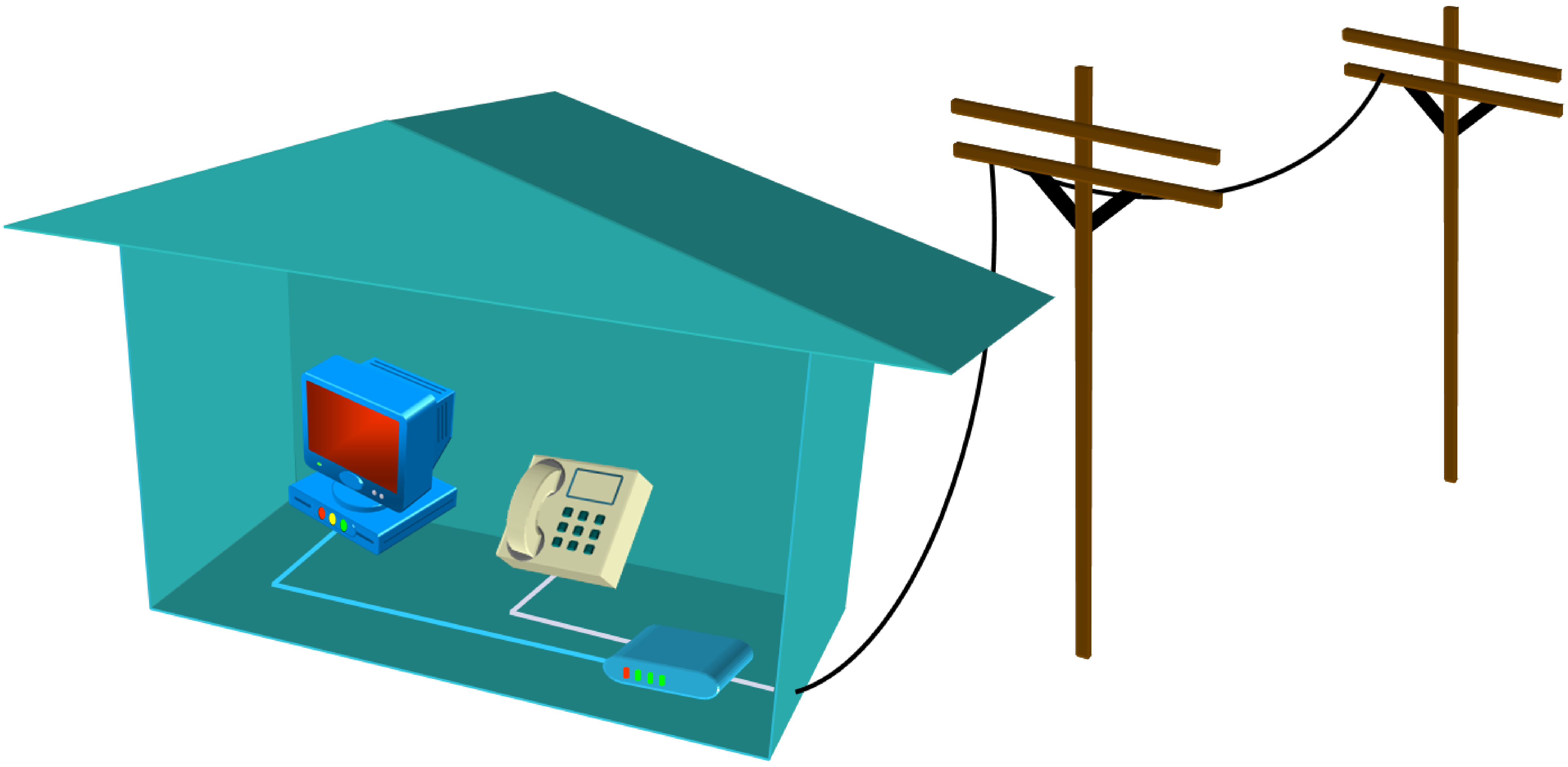
| PORT NUMBER | SERVICE | PORT NUMBER | SERVICE |
|---|---|---|---|
| 80 | HTTP | 20,21 | FTP |
| 443 | HTTPS | 161 | SNMP |
| 137-139 | NetBIOS | 22 | SSH |
| 110 | POP3 | 23 | TELNET |
| 143 | IMAP | 53 | DNS |
| 25 | SMTP | 67,68 | DHCP |
| 5060/5061 | SIP | 69 | TFTP |
| 3389 | RDP | 445 | SMB |
| 1720 | H.323 | 5004/5005 | RTP |

**Port numbers with their associated service.**

# Internet Access Technologies

**DSL** stands for **digital subscriber line**.  This is a popular technology that is used by homes and businesses to access broadband data over the internet.

DSL can carry both voice and data at the same time. It has a DSL modem that uses common telephone lines to carry its data. It's a high-speed connection that is much faster than your regular dial-up modems.



**DSL carries voice and data over normal telephone lines.**

There are a few different forms of DSL, and one is called **ADSL**, which stands for **asymmetric digital subscriber line**. This is called asymmetric because the download speed is considerably faster than the upload speed. This type of DSL is typically used in homes and is the cheapest form of DSL.

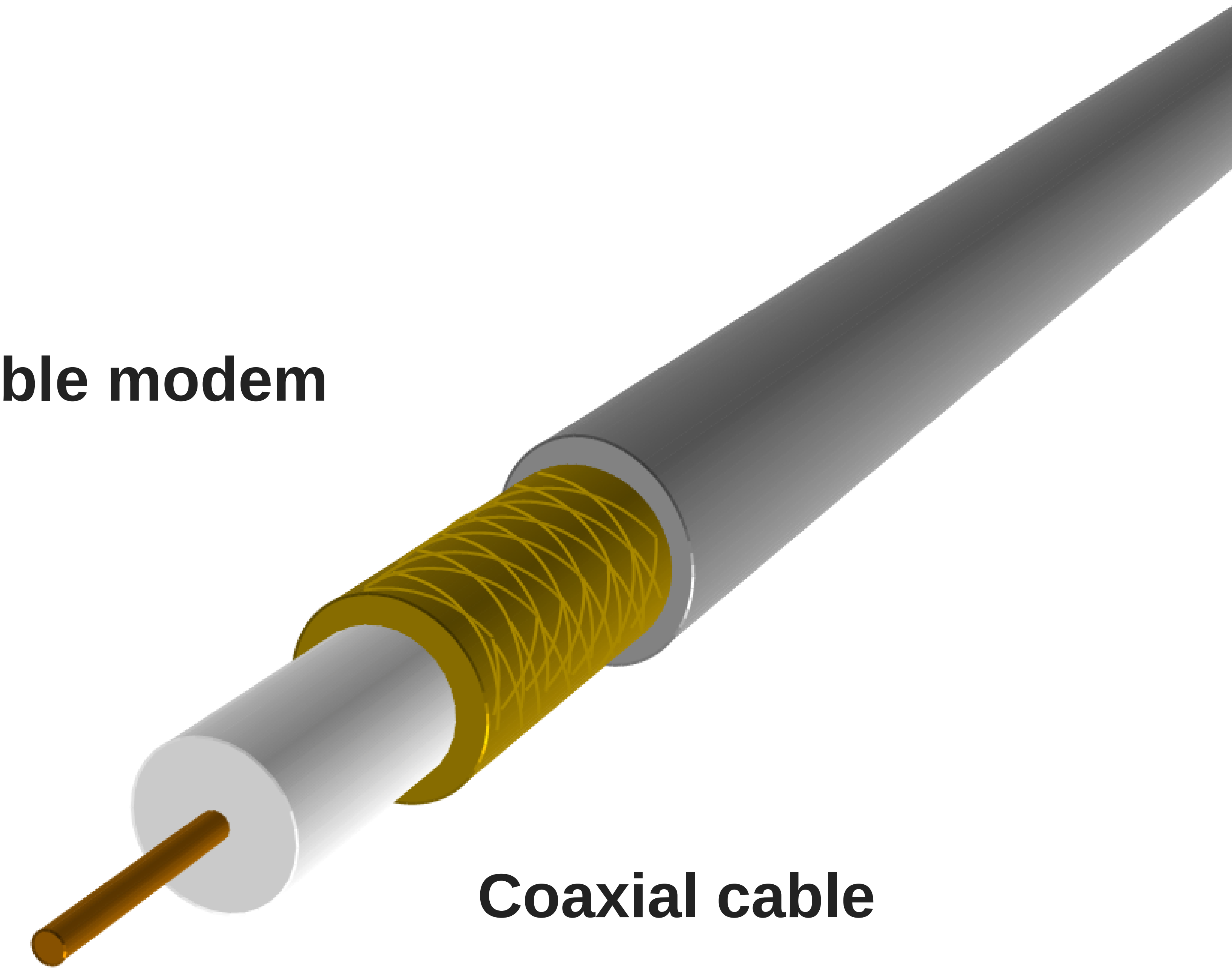
**SDSL** stands for **symmetric digital subscriber line**. And as the name implies, the download and upload speeds are the same. This type is typically used in businesses.

**VDSL** stands for **very high bit DSL**, and this is a very fast form of DSL. It has download speeds of over 50

Mbit/s over a copper wire.  But because it uses copper wire, it's only made for short distances.  For long distances, it can also use fiber optic cable.

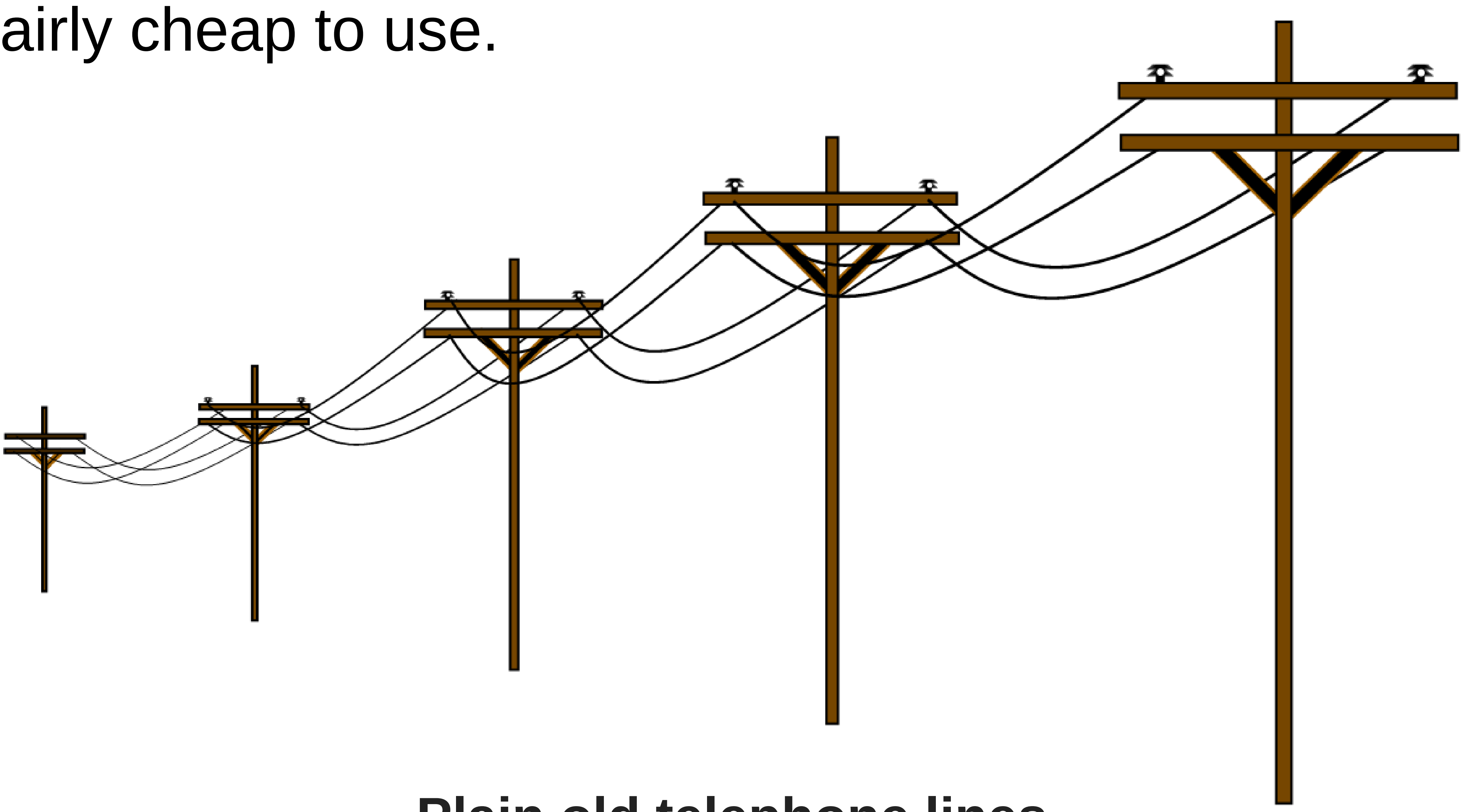
Another popular technology that is used to access the internet is **broadband cable**.  Cable is by far becoming the technology of choice by many homes to access the internet.  It uses a cable modem with an attached coaxial cable, which provides a link to the internet service provider.  Like DSL, cable is very fast, with speeds of over 50 Mbit/s.  Broadband cable is typically provided by the same provider that provides cable television to their customers.

**Cable modem**



**Coaxial cable**

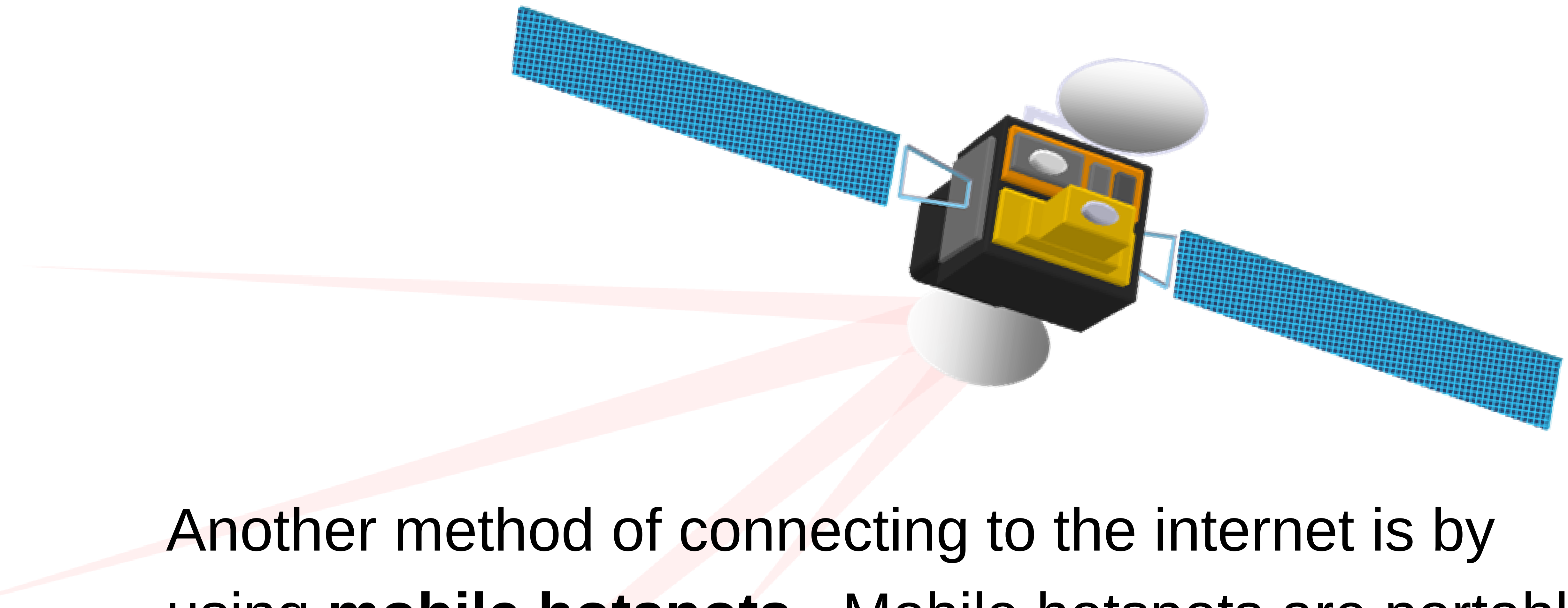
**POTS/PSTN** stands for **plain old telephone service and public switched telephone network**.  And these are just your plain old telephone lines.  These are slowly becoming obsolete by people who use the internet because of their slow speeds.  So if you have ever used a high-speed internet such as broadband, you will never go back to using the slow speeds of 56 Kbps, which is the speed of a standard dial-up modem. However, telephone lines do have an advantage, and that is that they are basically everywhere and they are fairly cheap to use.



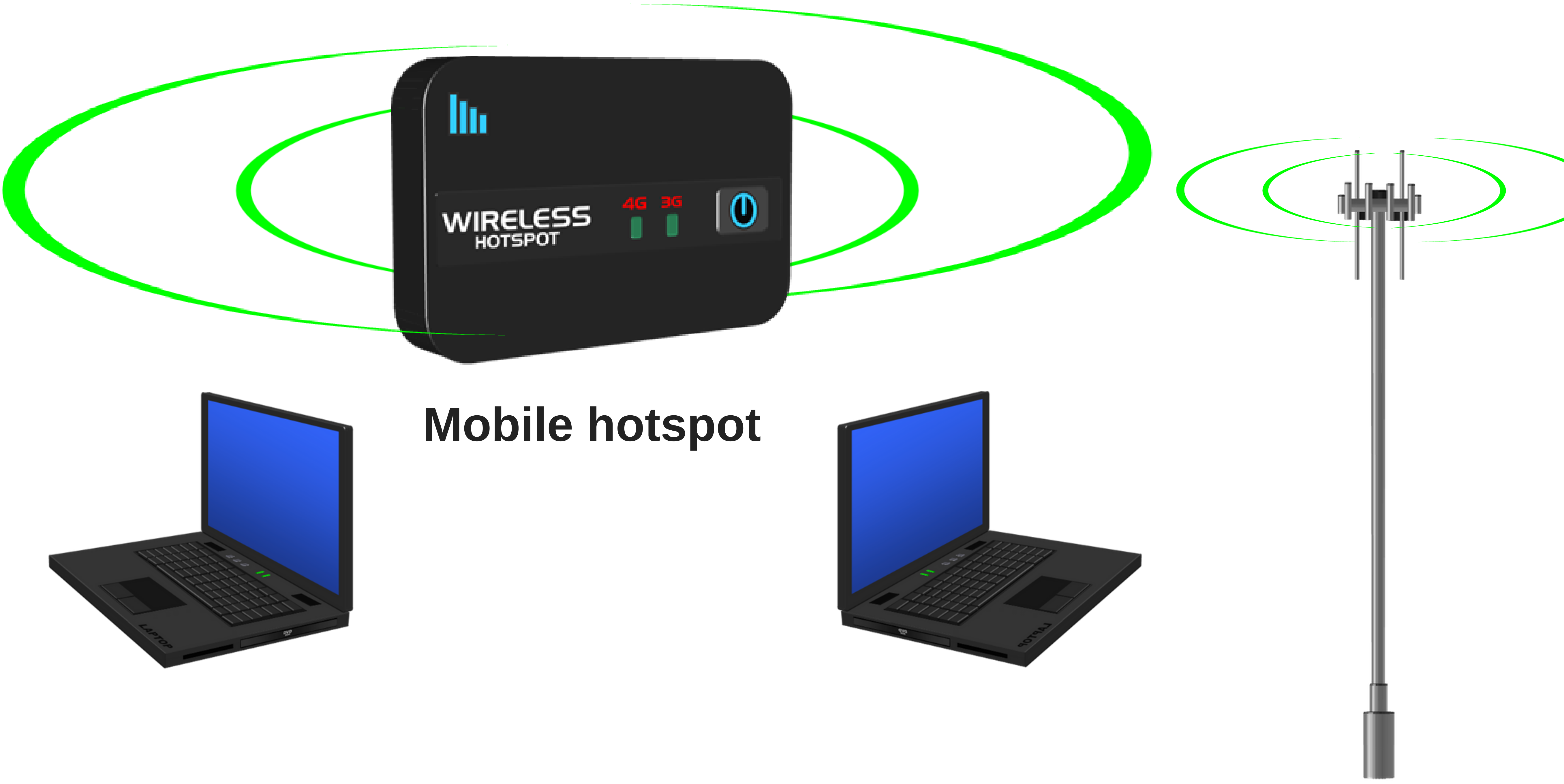
**Plain old telephone lines**

**ISDN** stands for **integrated services digital network**. This is an international standard for digital transmission over ordinary telephone lines.  In order to use ISDN, users had to install ISDN modems.  This was a significant improvement in speed over the standard modem because a standard modem sends data at a maximum speed of 56 Kbps, but ISDN sends data at 128 Kbps.  However, ISDN never really caught on because of the faster speeds of DSL and cable.

**Satellite** communication is pretty expensive and it's mainly used where no other services are provided, like phones, cable, or DSL.  But because of the increasing availability of these other options, satellite is rarely used.  The speed of satellite has increased throughout the years, with speeds maxing out around 15 Mbit/s, with only a fraction of that in upload speeds.

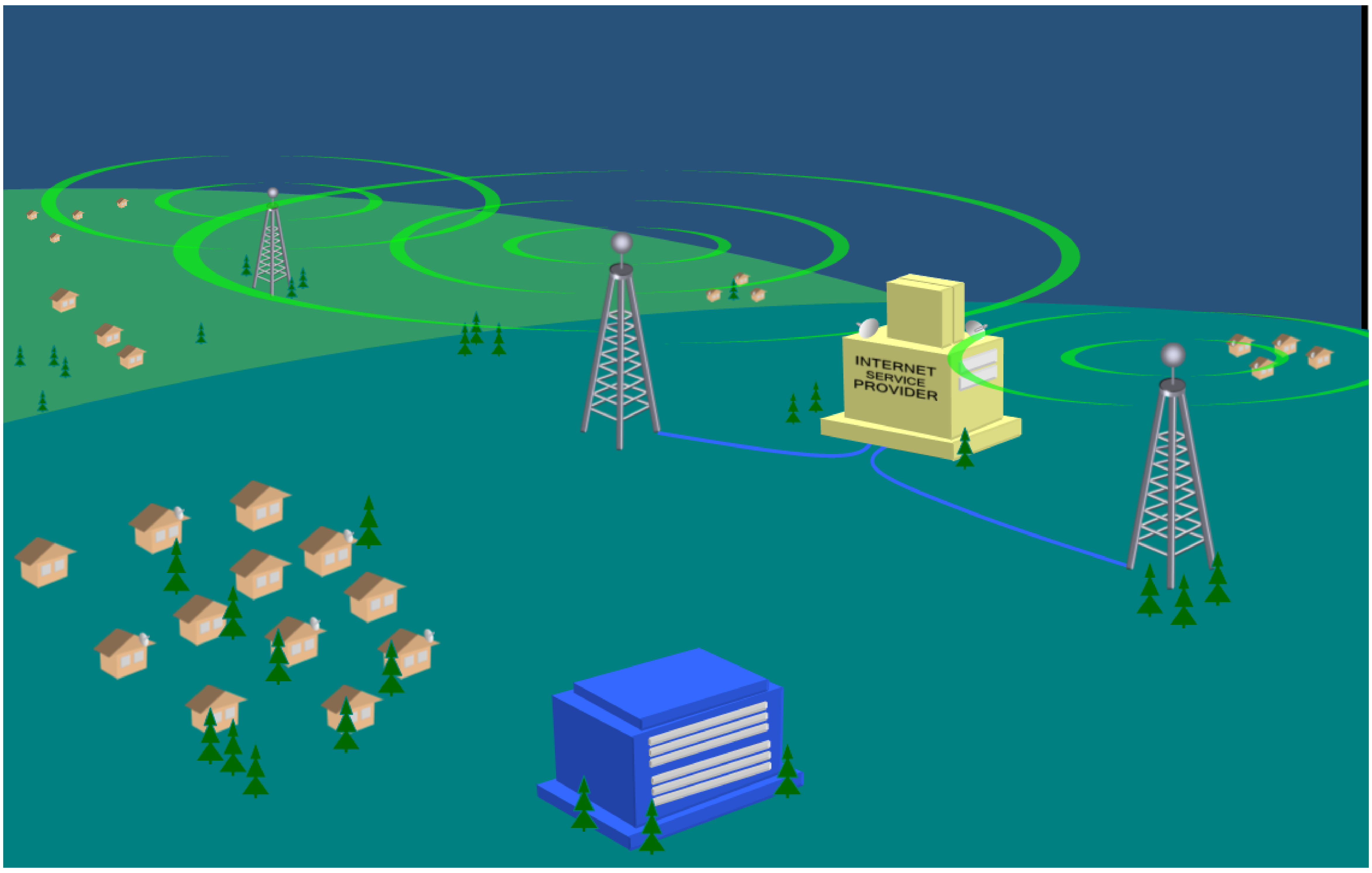


Another method of connecting to the internet is by using **mobile hotspots**.  Mobile hotspots are portable devices that use cellular networks to connect wireless devices to the internet.  So if there are wireless devices within 30 ft. of a mobile hotspot, they can join it and have access to the internet.  Mobile hotspots come in two forms.  They will either be a free-standing device like you see below, or they can come as a feature built into a smartphone.  Mobile hotspots are available through cell phone carriers such as Verizon, AT&T, T-Mobile, and Sprint.



**Mobile hotspot**

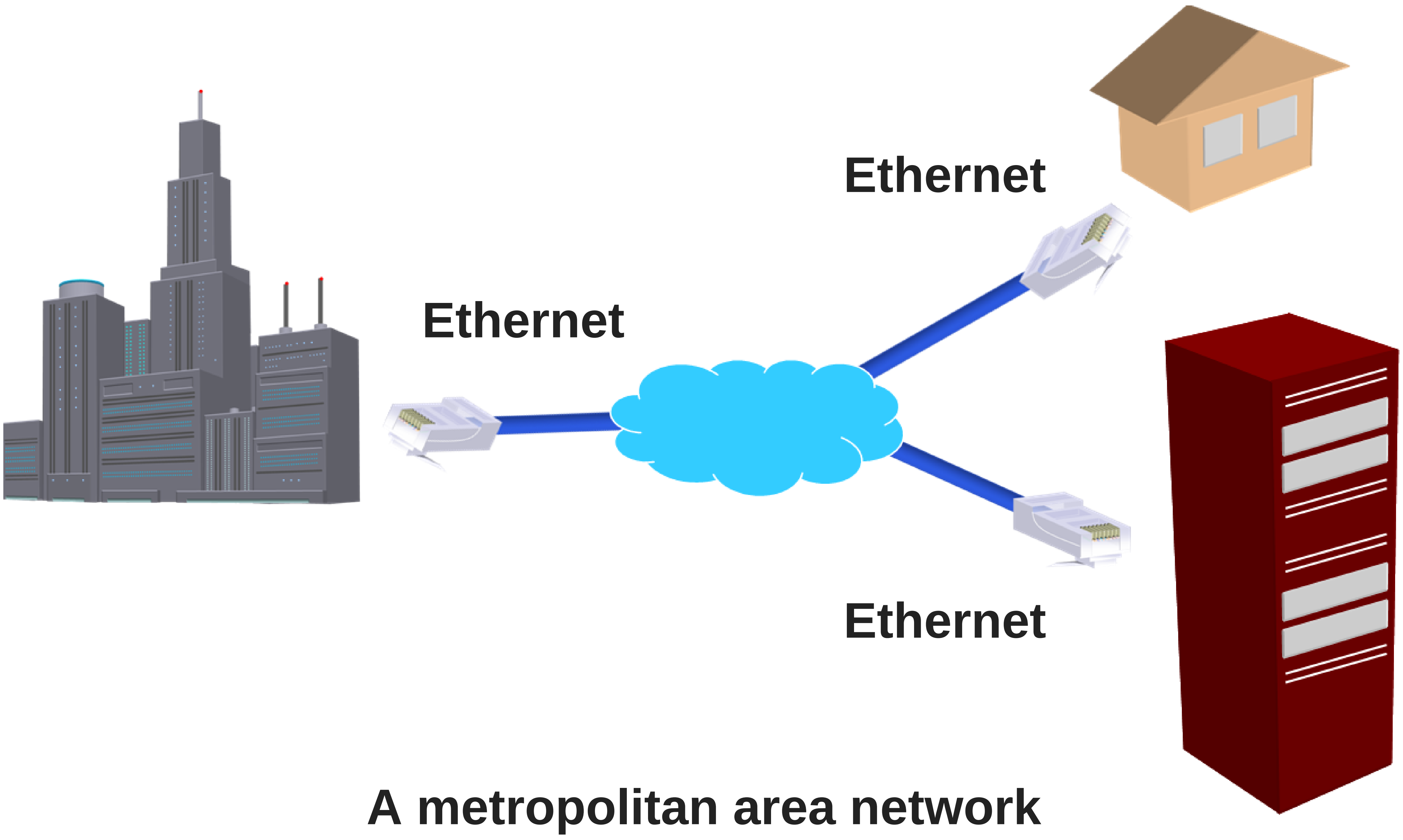
Another broadband internet technology is called **WiMAX**. And much like your home wireless network, where it covers your home, WiMAX covers much larger areas. WiMAX is basically a super wireless network that can cover entire cities or countries.



**WiMAX**

WiMAX works with WiMAX towers that are scattered in different geographical locations. These towers directly connect to an internet service provider, typically with a T3 line. Each tower covers a certain area just like a cell phone tower does. To pick up the transmission of these towers, you need a receiver in your home or computer, to receive the signal. Then once that is done, you can now access the internet. WiMAX does have the potential of replacing DSL and cable because it can provide internet access to places where cable and DSL can't reach.

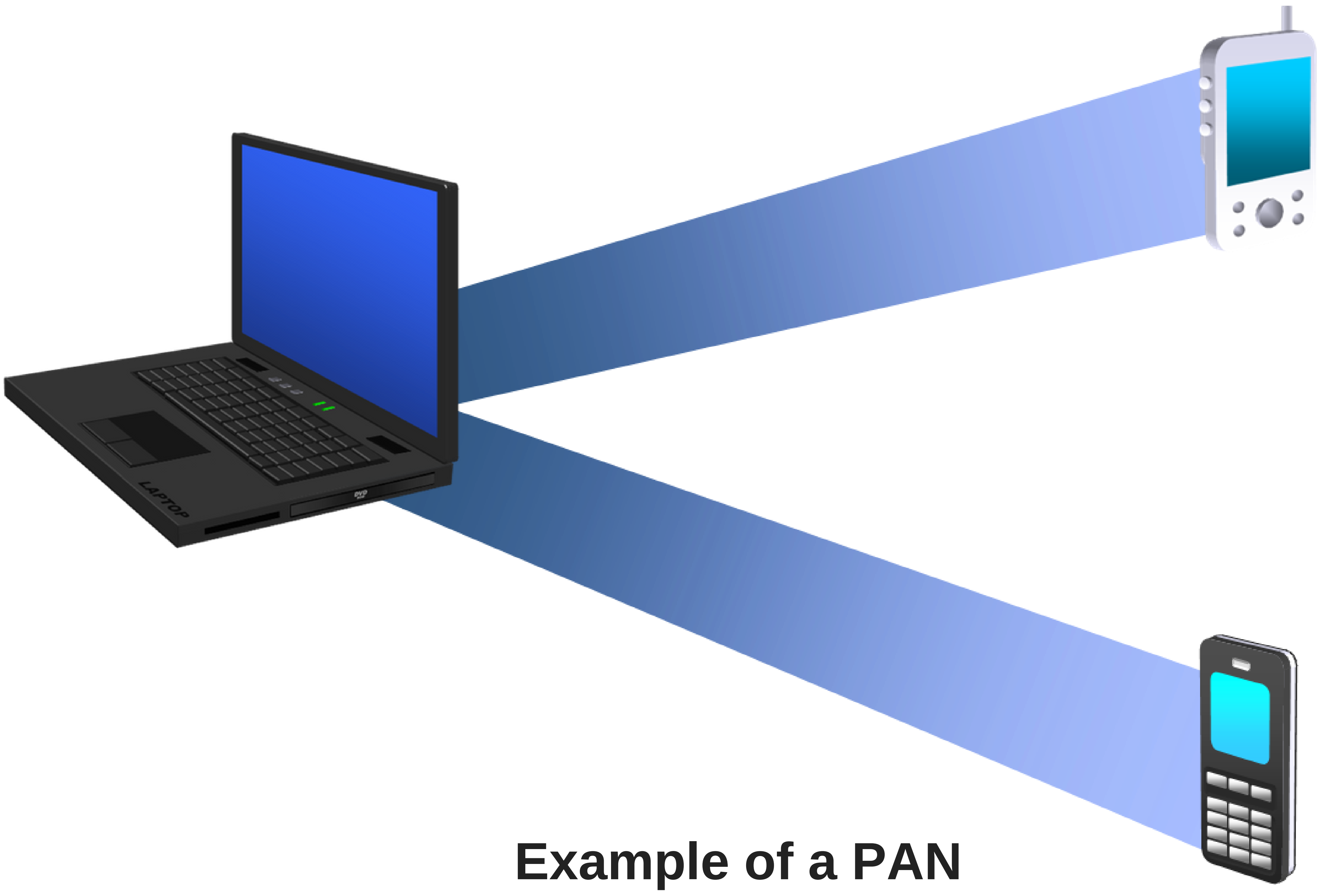
**Metro Ethernet** is simply a metropolitan area network or MAN, which is based on Ethernet standards.  It's basically used to connect businesses and residential users to a larger network, such as the internet, using Ethernet.  Metro Ethernet is fairly simple and cheap to use because it doesn't require any specialized cabling or equipment like other expensive technologies need. It only uses equipment and cabling related to Ethernet, which is by far the most common internet technology today.  So even though end users are not sure what technology their internet service provider is providing in the middle, what matters is, that on both ends, it's using Ethernet connectivity.



A metropolitan area network

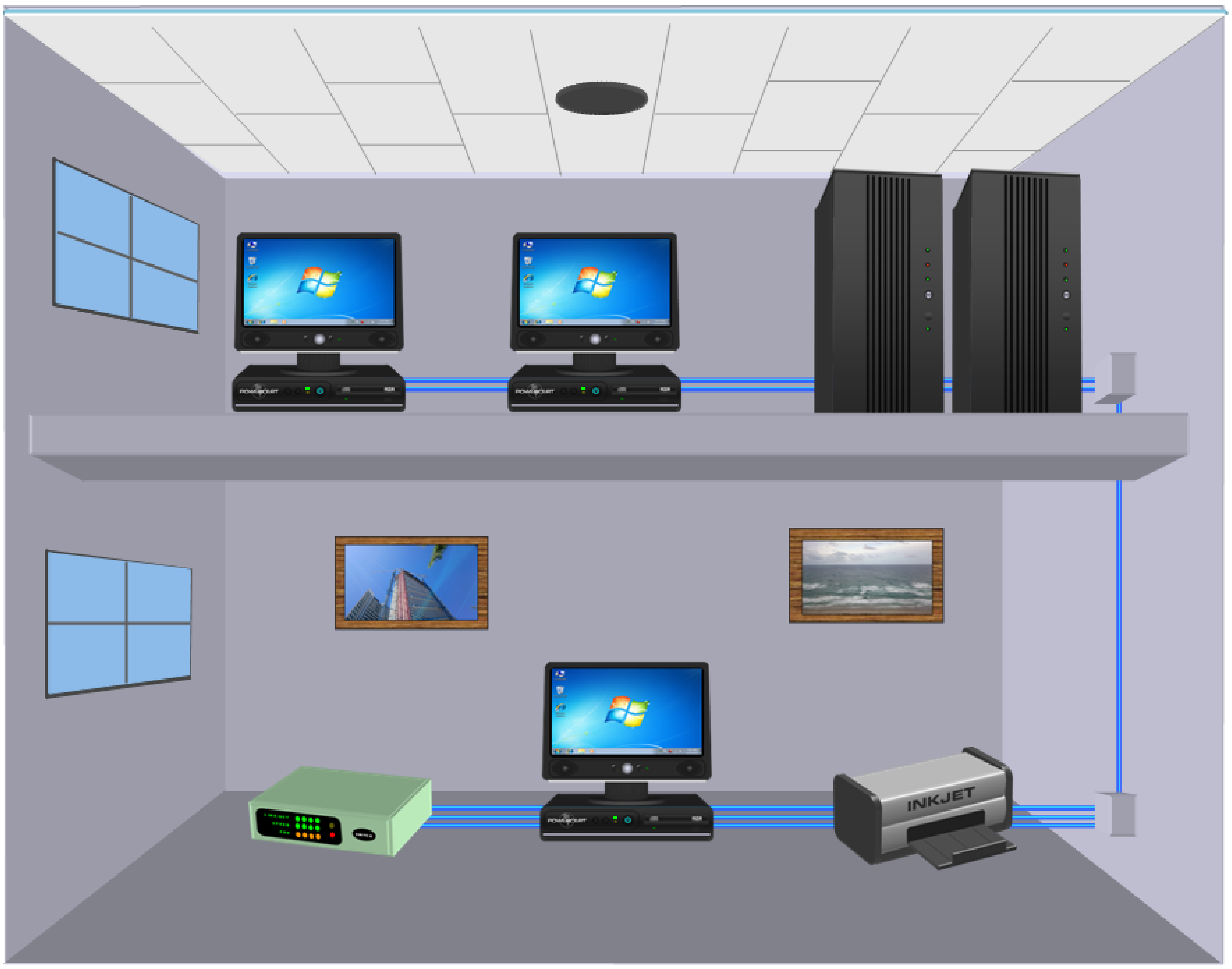
# Network Types

**PAN** stands for **personal area network**. This is a type of network that is used on a personal level. It's a small network that is basically used for connecting things like mobile phones, PDAs, and laptops to each other using bluetooth. PANs are generally used for transferring small files, such as music, photos, calendar appointments, and so on.



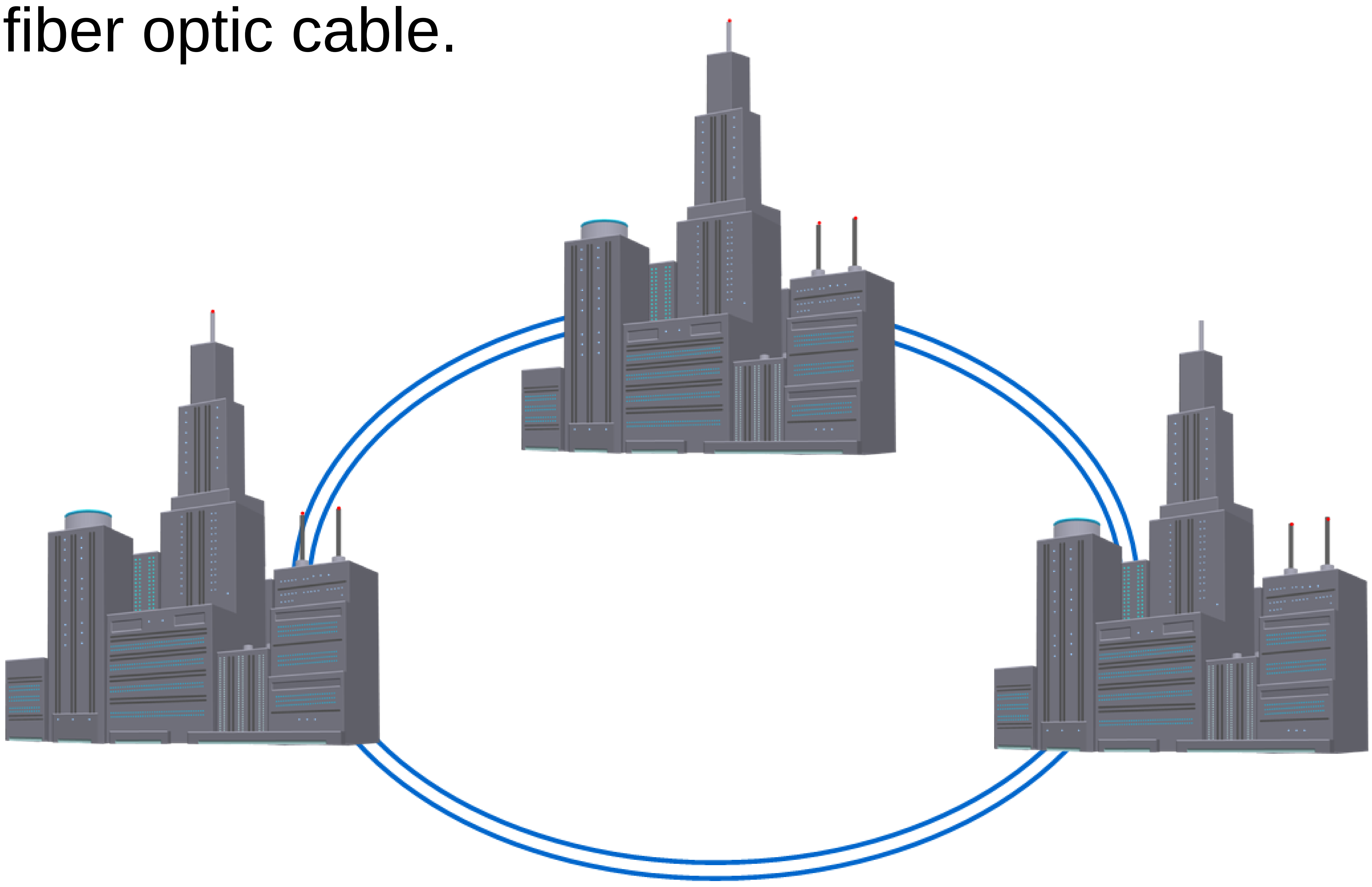
**Example of a PAN (personal area network)**

**LAN** stands for **local area network**. A local area network is a group of devices such as computers, servers, and printers, which are basically located in the same building. In other words, in close proximity to each other. The most common type of LAN is an Ethernet LAN, where two or more computers are connected to CAT5 Ethernet cables using a switch.



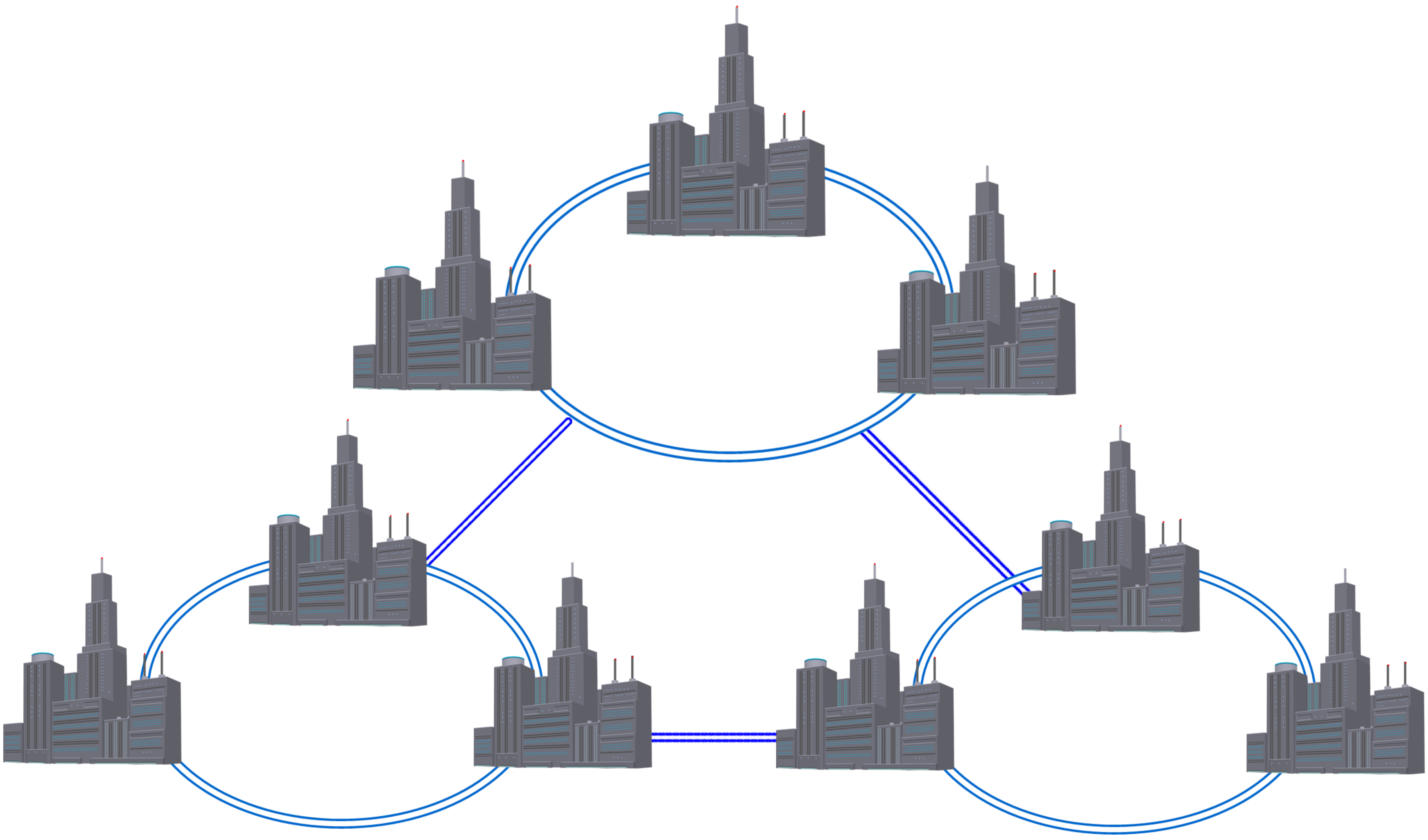
Example of a LAN (local area network)

**MAN** stands for **metropolitan area network**.  This is a larger network than a LAN.  It's a network that spans over several buildings in a city or town.  MAN's are typically connected using a high-speed connection such as fiber optic cable.



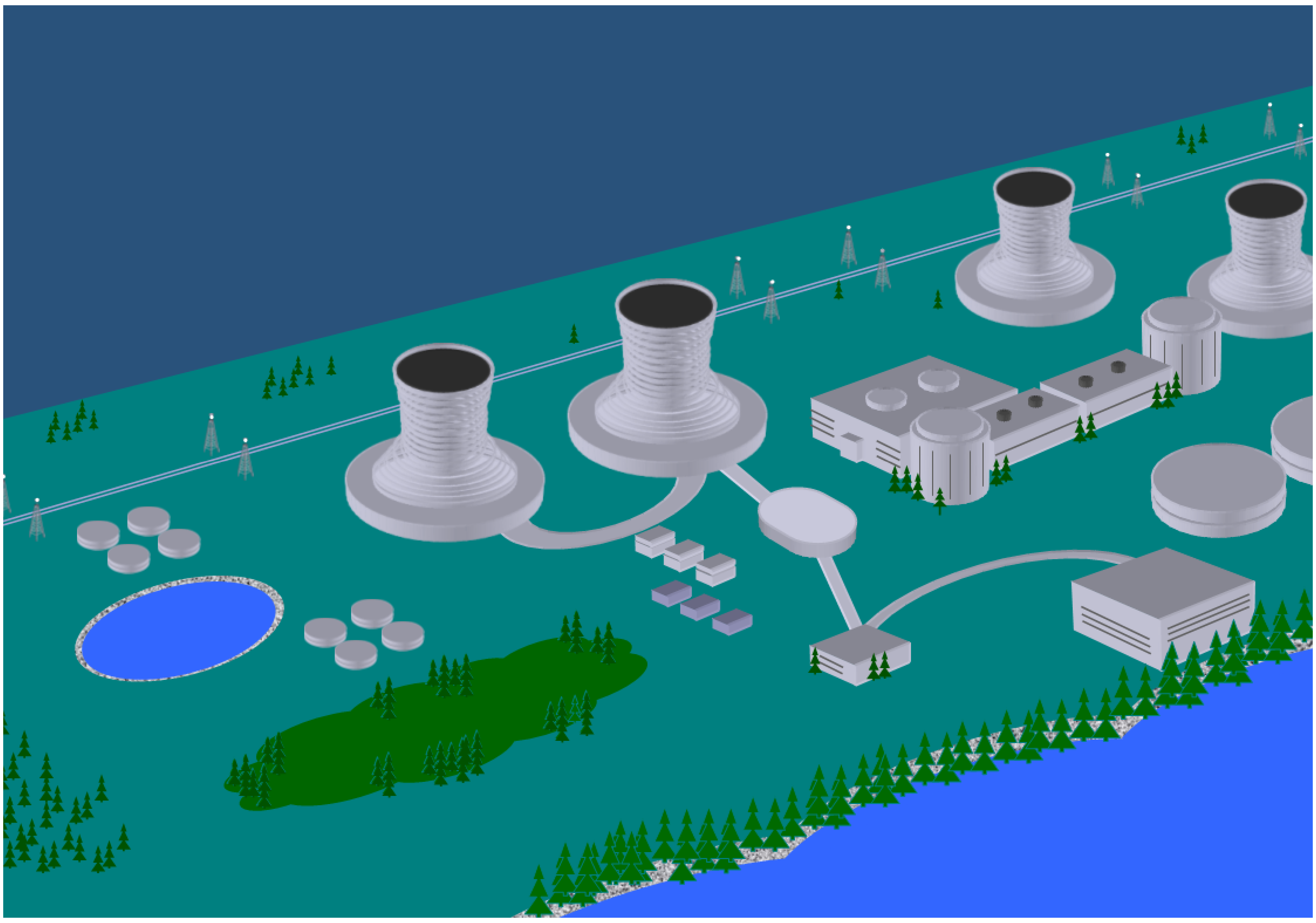
Example of a MAN (metropolitan area network)

Finally, there is the **wide area network** or **WAN**. A WAN is the largest type of network. It's a network that spans over a large geographical area, such as a country, continent, or even the entire globe. A good example of a wide area network is the internet.



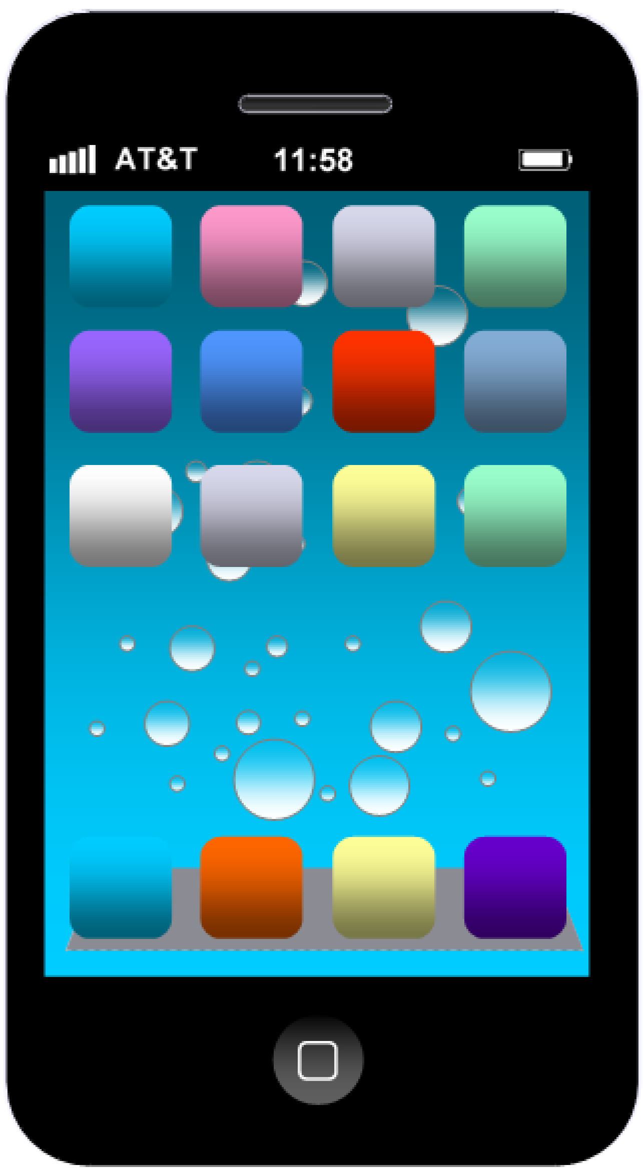
**Example of a WAN (wide area network)**

**SCADA** stands for **supervisory control and data acquisition**. This is software that is used for controlling and monitoring equipment that is used in industrial facilities, such as power plants, water treatment plants, or refineries. SCADA communicates with sensors and systems in real-time that are out in these industrial facilities. Those sensors and systems send back information to **PLC**s or **programmable logic controllers** and **RTU**s or **remote terminal unit**s, which then sends it to the SCADA computers to be analyzed. This information could be things like, how to reduce waste, or how to improve efficiency, or if there are any problems.  SCADA is also often referred to as **ICS** which stands for **industrial control system**, which is a general term that encompasses SCADA systems.



**SCADA is used in industrial facilities.**

Cell phones also access the internet and make phone calls by using radio systems such as **GSM** and **CDMA**.  GSM stands for **global system for mobiles** and is the largest radio system that is being used around the world, including major carriers such as AT&T and T-Mobile, and



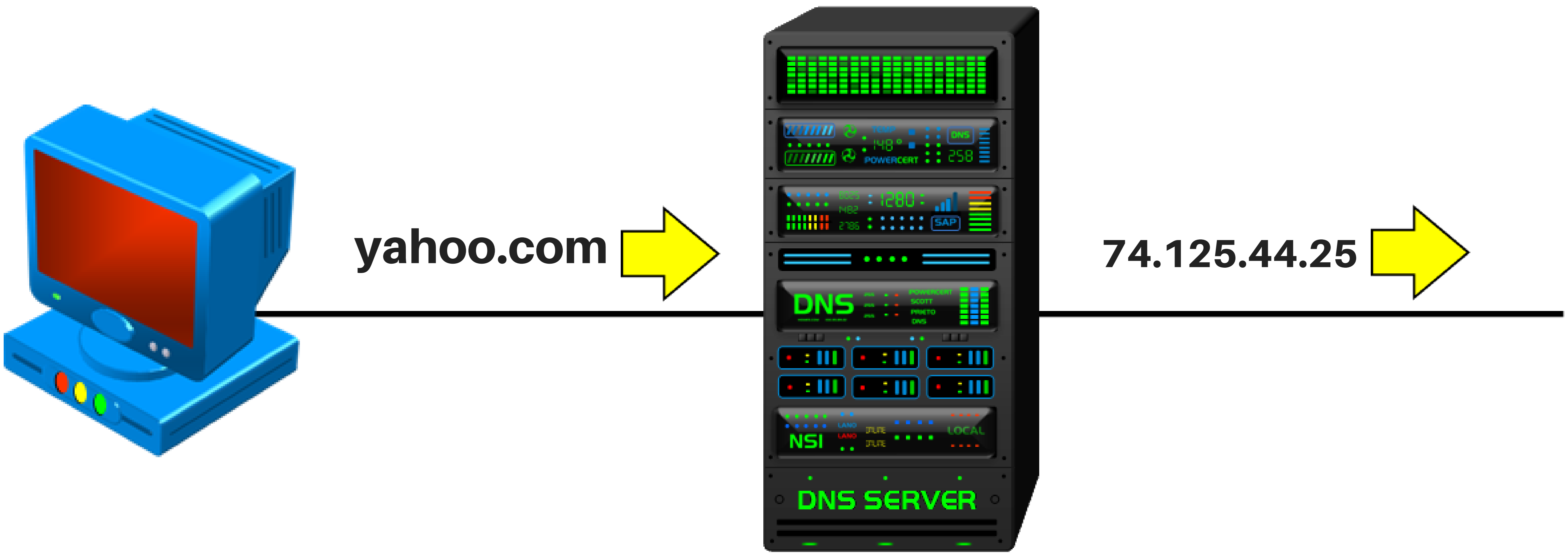
**Cell phone**

it's widely used in Europe.  GSM works by changing your voice into a digital form and that data is assigned a time slot.  Then as the data is received on the other end, the assigned time slotted data puts the call back together.  **CDMA**, which stands for **code division multiple access**, is another radio technology that is not as widely used as GSM, but it's the system that is used by major carriers such as Verizon and Sprint.  CDMA works by data being encoded with a unique key.

**4G LTE**, which stands for **4th generation long term evolution** is a technology that was developed by the 3rd generation partnership project.  Currently it offers the fastest wireless communication speed available, with speeds of over 100 Mbit/s, which is many times faster than the speed of **3G** or **3rd generation**.  3G technology offers speeds anywhere from 384 Kbit/s - 2 Mbit/s.  And prior to 3G was **Edge**, which stands for **enhanced data rates for GSM evolution**.  Edge is a painfully slow technology that has speeds not much different than using a regular dial-up modem, with speeds starting around 75 kbps.

# Networking Services

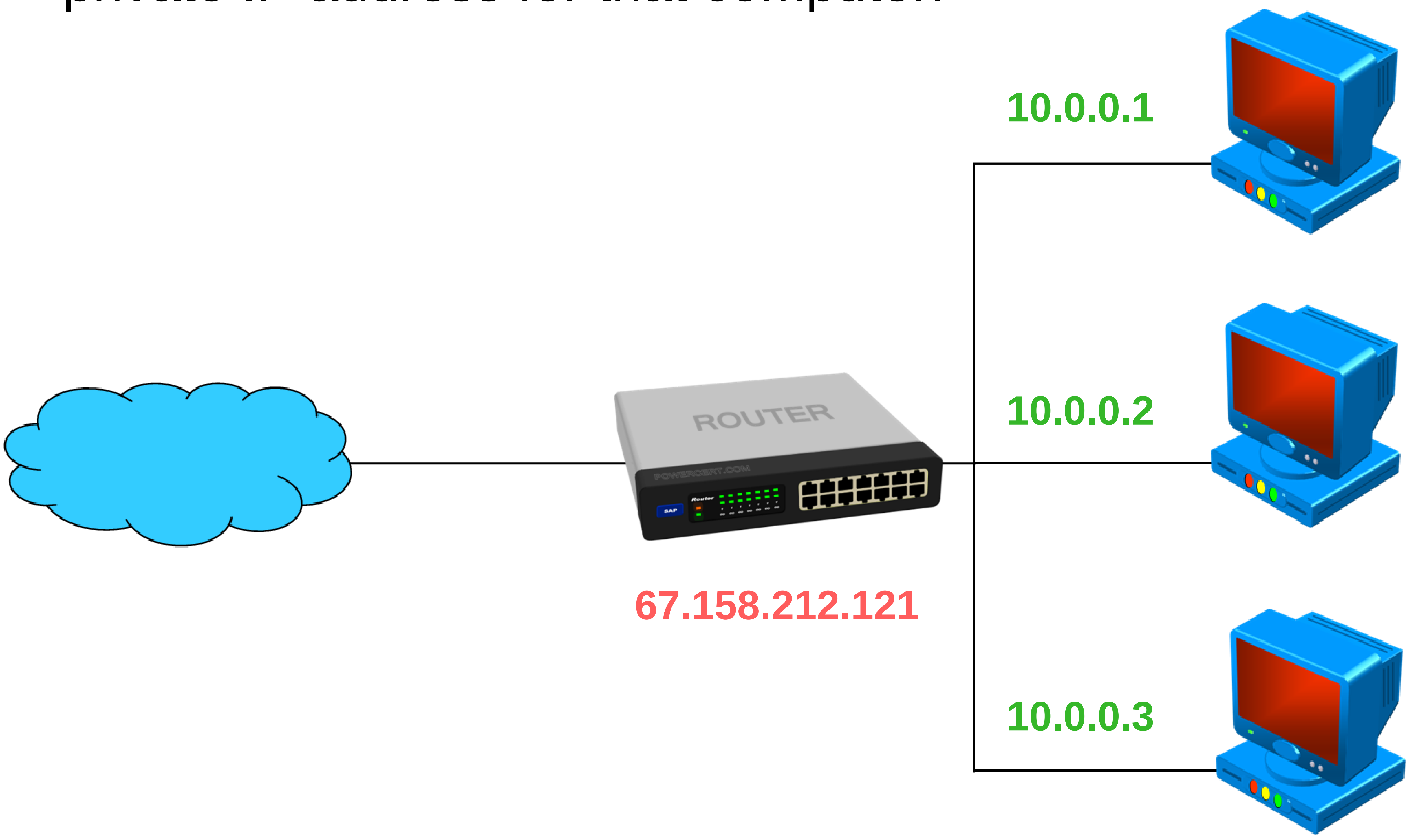
**DNS** stands for **domain name system**. This resolves domain names to IP addresses. In the world of networking, computers don't go by names like humans do, they go by numbers. So if you type in a web address in your web browser, DNS will transform the name into a number, because all computers know are numbers. So for example, when you type in yahoo.com in your web browser, the DNS server will search through its database to find a matching IP address for that domain name. And when it finds the IP, it will transform that domain name to the IP address of the yahoo web server. So DNS basically works like a phone book. When you want to find a phone number, you don't look up the number first, you look up the name first, and then it will give you the number.



**The DNS server will transform the domain name: yahoo.com, into an IP address.**

**Network address translation** or **NAT** is a service that is typically used in routers. This is used to translate a set of IP addresses to another set of IP addresses.

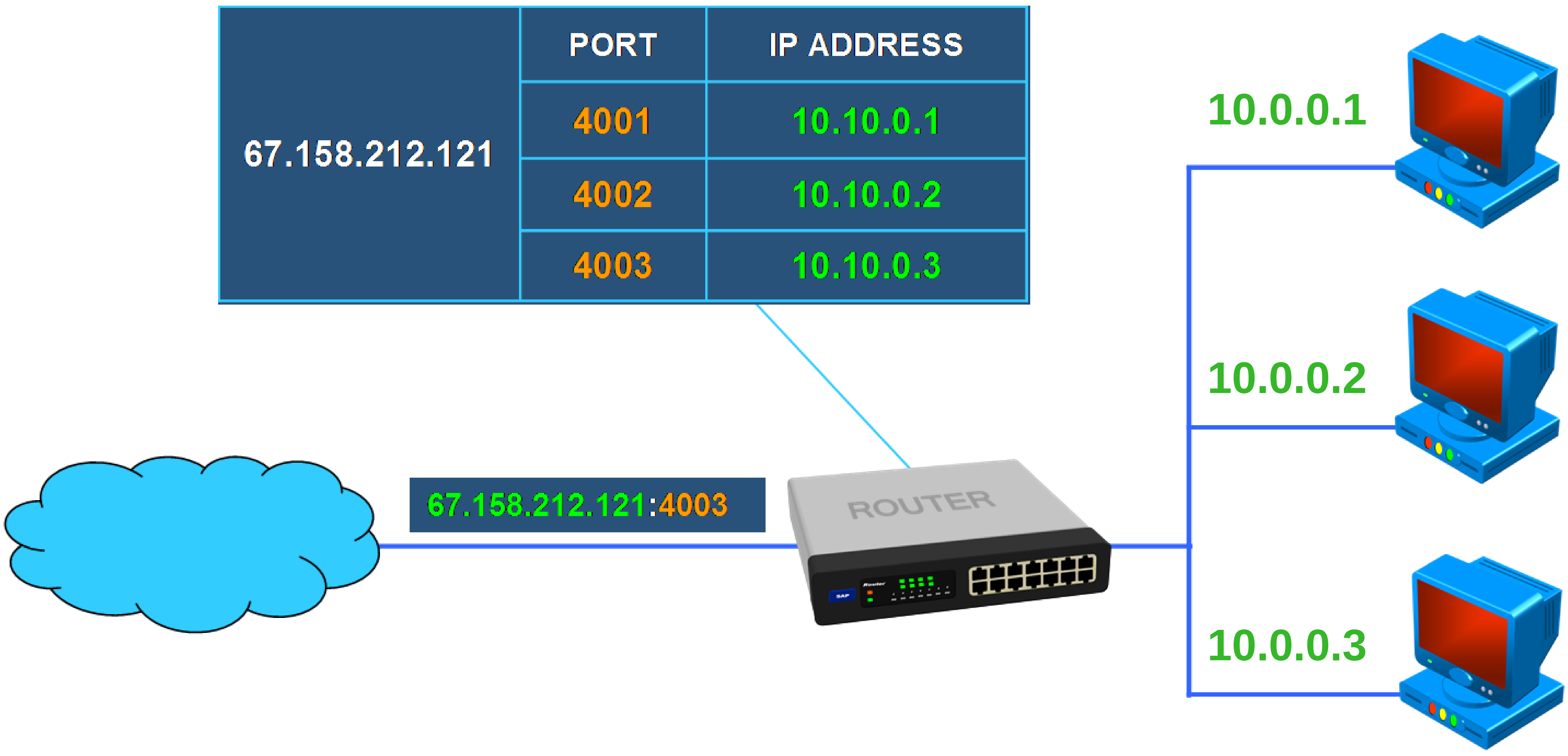
So for example, below we have a private network, and it's using a set of private IP addresses internally.  In the middle, we have the router with its public IP address, and this router is running the NAT service.  If a computer on this network wanted to communicate over the internet, it needs to translate its private IP address to the internet's public IP address.  And this goes both ways.  If your computer on the internet wants to communicate with a computer on this private network, then the public IP address needs to be translated to the private IP address for that computer.



**A private network with computers using private IP addresses, along with the router with its public IP address.**

Another version of network address translation is called **PAT**, which stands for **port address translation**.  PAT translates IP addresses based on port numbers.  Each computer in a private network is issued not only a unique IP address, but they are also issued a unique port number.  This is done so that external data packets from the internet knows which computer on the private network it wants to talk to.  So for example, if a device on a network wanted to communicate with a computer on another network, the IP address along with its port number will be translated by PAT to find the correct computer.

**Port address translation chart**

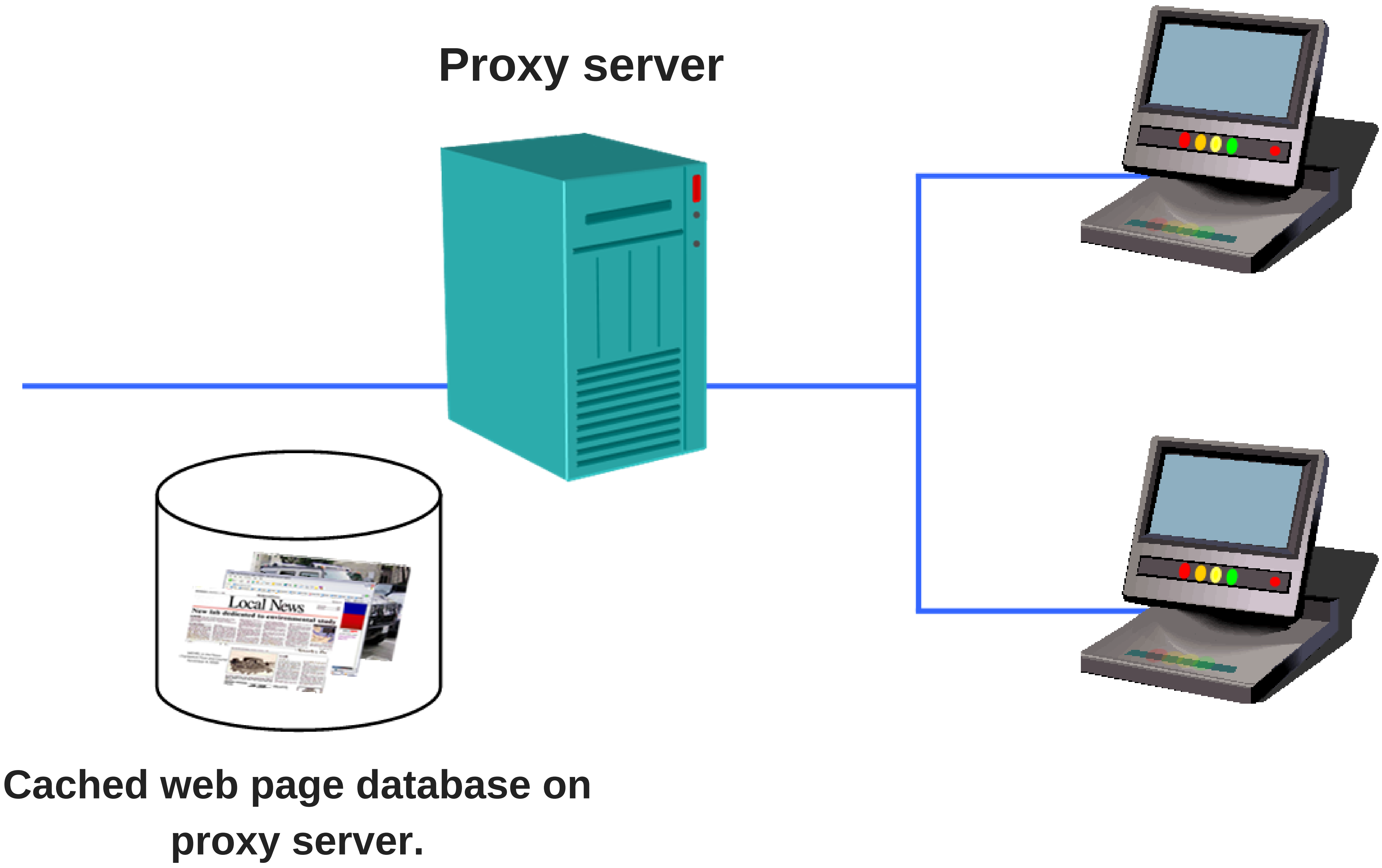


| | PORT | IP ADDRESS |
|---|---|---|
| 67.158.212.121 | 4001 | 10.10.0.1 |
| | 4002 | 10.10.0.2 |
| | 4003 | 10.10.0.3 |

**A private network with computers using private IP addresses, along with a PAT chart.**

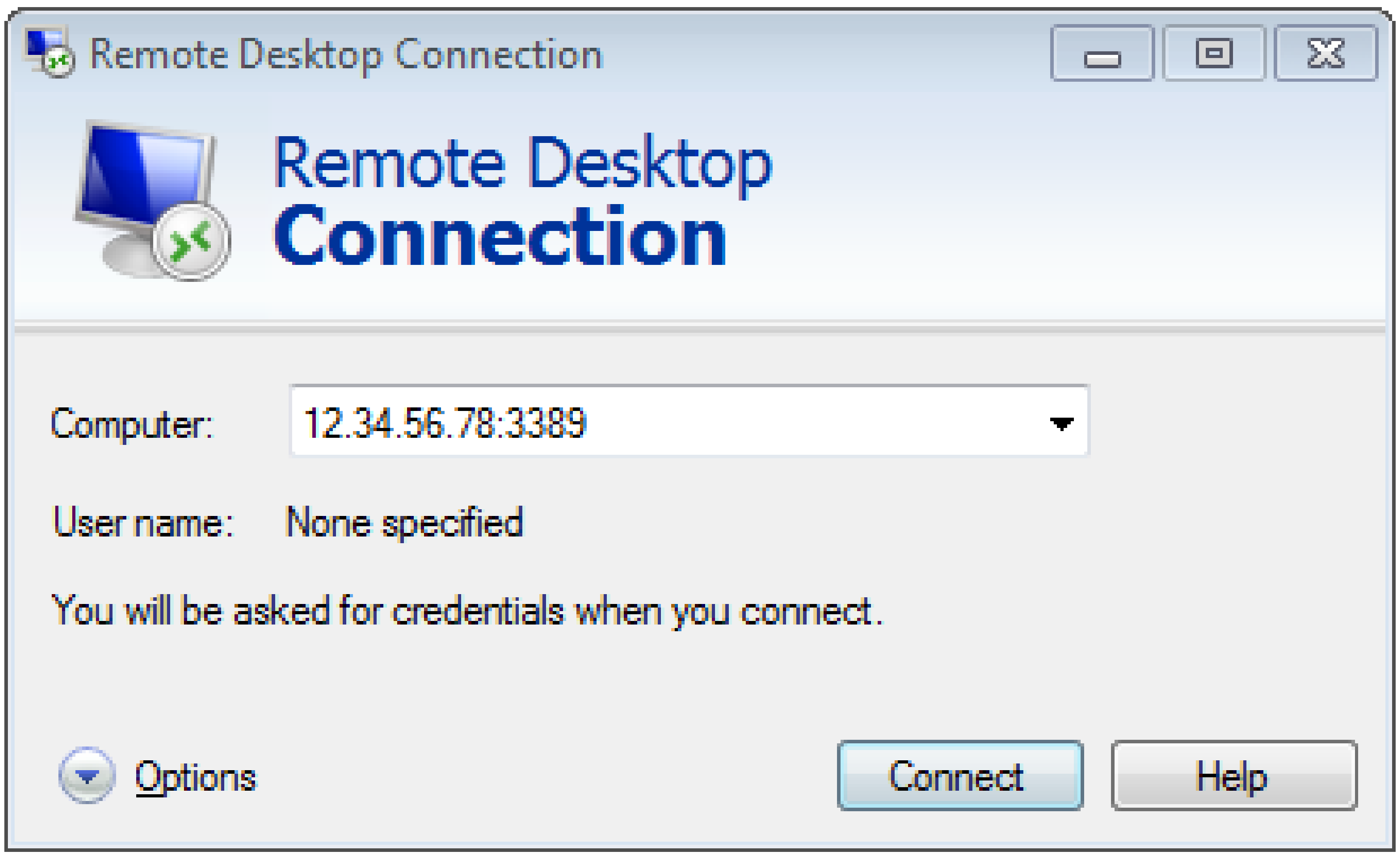
**SNAT** stands for **static network address translation**. As you recall from a previous lesson, NAT translates a private network's IP addresses to a public IP address. Private IP addresses will be translated to a single public IP address and vice versa.  So what SNAT does, is that it can link a public IP address with a private IP address permanently (statically). This is useful when a computer or server needs to be accessed from outside the network. For example, if a server was an email server.

A **proxy** server is similar to your web browser. Whenever you look at a web page, your web browser will store that web page into cache. So at a later time, if you were to look at that web page again, your browser retrieves it much faster, because it doesn't have to download the contents of that web page all over again since it's already stored in your computer. A proxy server does the same thing.



So for example, if a company uses a proxy server, and whenever a user wants to retrieve a web page, the proxy server will retrieve the web page from the internet on behalf of the user, and then it will store that web page into a centralized cached database.  So, if another user on a different computer goes to a web page that has been stored in the proxy database, the proxy server does not have to go out on the internet to retrieve the web page.  It can simply retrieve it from its database and send it to the user.  So a benefit of using a proxy is speed since web page retrieval is much faster.  Another benefit is that it saves bandwidth because a proxy server reduces the need to go out on the internet.  And finally, it provides security because it reports what web pages are retrieved to the network administrator.

**Remote desktop protocol** is a technology from Microsoft to access a remote computer's desktop.  RDP is based on Microsoft terminal services.  So, if a user wanted to access another computer, the user can simply type in the remote computer's IP address, along with the proper credentials, and then the user can have the remote computer’s desktop displayed on their own computer screen.



Remote Desktop Connection

Remote Desktop Connection

Computer: 12.34.56.78:3389

User name: None specified

You will be asked for credentials when you connect.

**RDP login interface**

When you have a lot of computers on a network and they're all sending data, the potential for collisions is present. Therefore, when you have collisions, data communication is lost. So that's why they developed a protocol called **CSMA/CD**, which stands for **carrier sense multiple access collision detection**. This is the access method used on Ethernet networks. This method works by each computer first sensing if the wire is idle, and if it is, it sends its data, therefore avoiding any collisions. But if you have two computers trying to send data at the same time, a collision will happen. If a collision happens, the computers will wait a random amount of time and retries to send their data.

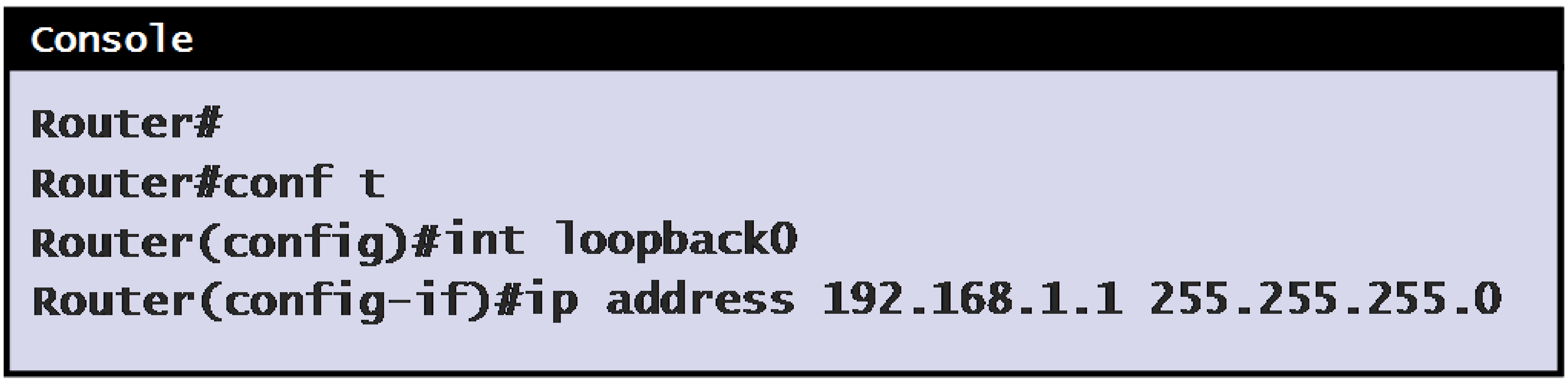
**CSMA/CD was developed to prevent collisions.**

**CSMA/CA** stands for **carrier sense multiple access with collision avoidance**. This is the access method used for carrier transmission in wireless networks. This method is similar to the CSMA/CD, except that when a computer wants to send its data, it first sends out a small data packet to make sure that the channel is clear before sending out its main data. If the packet is successfully transmitted, then the computer is cleared to send out its main data.

# Routing Protocols

For the Network+ exam, there are a few routing concepts and protocols that you're going to need to know.  One of them is called a **loopback interface**.  A loopback interface is a fake or virtual interface that is created on a router.  It’s not a physical interface, it's virtual.  This virtual interface is assigned an IP address of your choice, and its purpose is for testing and administration.

So as an example, let's assign an IP address to a loopback interface on a Cisco router.  So in a terminal window, (*you don't need to know all this, as far as creating one, you just need to know that for the exam that it's used for administration and testing*) and while we are in configuration mode, we enter *int* for interface, then *loopback0*, then an IP address of our choice, and then a subnet mask, and then you're done.



```
Router#
Router#conf t
Router(config)#int loopback0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
```

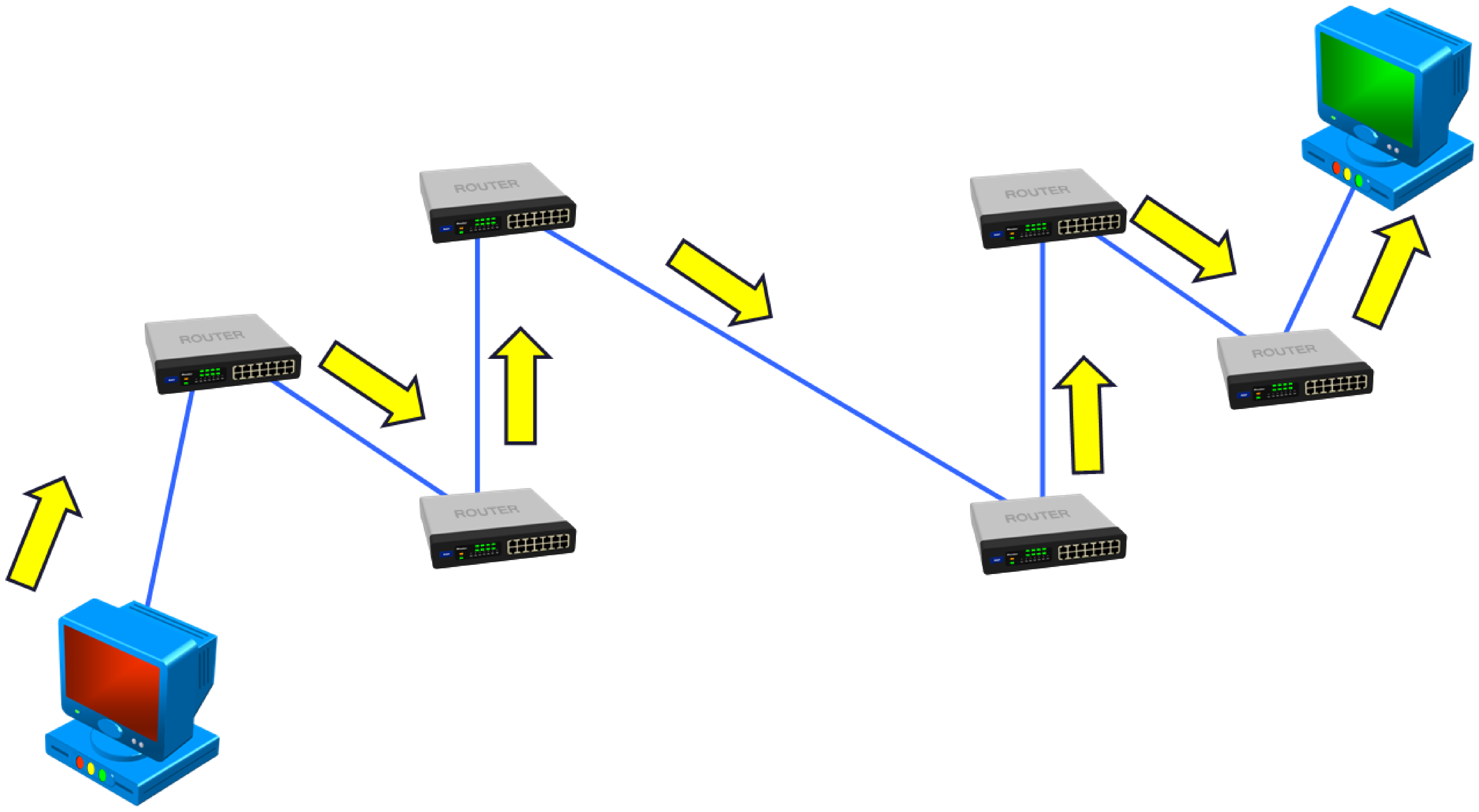
**Creating a loopback interface on a Cisco router.**

A **routing table** is a file that contains a set of rules that shows information on what path a data packet takes to its destination.  For example, a router uses routing tables, and as a data packet arrives at the router, the router looks at its routing table to find out where to forward the data packet along the best path to its destination.

**Routing table & router**

A basic routing table contains a network destination, which is an IP address of the final destination.  A subnet mask, which determines which part of the IP address is the host and network portion.  A gateway, which tells the router which IP address the data packet should be forwarded to.  The interface, which is the outgoing IP address of a device that's sending the data. Next hop, which is the IP address to which the IP address is forwarded to.  Finally, a metric, and this determines the best route among multiple destinations.

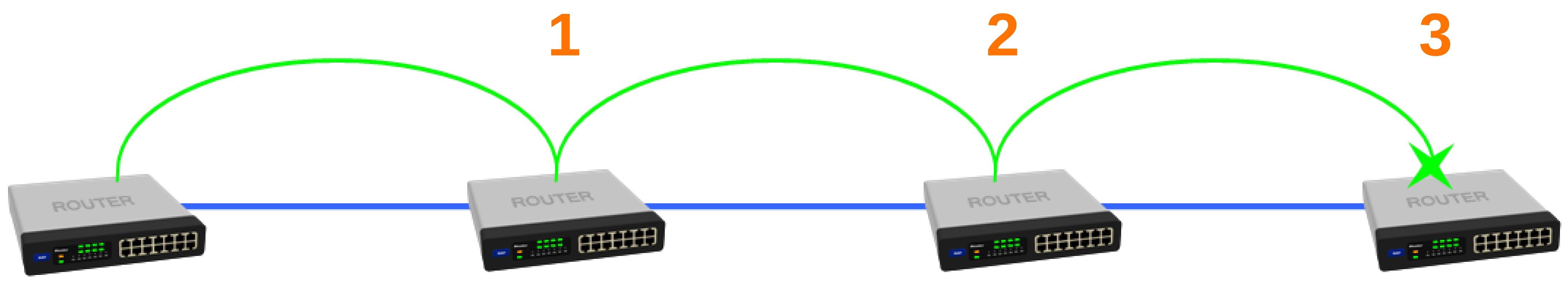
If you were traveling to a certain destination anywhere in the world, for example on vacation, most likely you will need directions or a map on how to get there.  In the world of networking, it works the same way.  In order for data to travel across a network and reach its destination, it needs a map to determine the best path to take.  The way it does this is by using **routing protocols**.  Routing protocols collect information about the current network status and map out the best path for data packets to take to their specific destination.



**Routing protocols map out directions for data to their destination.**

There are three different types of routing protocols. There is **distance vector**, **link state**, and **hybrid**.

Distance vector protocols factor in distance to the destination based on how many hops.  A **hop** refers to how many routers a data packet has to go through to reach its destination.  So for example, for data to travel between these two end routers below, it would take three hops: one, two, and three.



**Data packet taking 3 hops to its final destination.**

One of the distance vector protocols is called **RIP**, which stands for **routing information protocol**. RIP is the oldest routing protocol. Routers that use RIP broadcast the routing information to other routers every 30 seconds regardless if the routing information has changed or not. So as a result of this, as networks got larger, this caused a lot of unnecessary traffic on a network. So the developers created RIP version 2 (**RIPv2**), which solved the problem of excessive broadcast traffic that RIP caused.

Another distance vector routing protocol is called **BGP**, which stands for **border gateway protocol**. This is the standard routing protocol of the internet. It determines routing directions that are based on paths and policies.

In addition to distance vector protocols, there is also **link state**. Link state is a routing protocol that is used by routers to share information and independently map out the best path on a network. Two examples of link state protocols, are OSPF and IS-IS.

**OSPF** stands for **open shortest path first**. This is a routing protocol that is used to determine the correct route for data packets to take to their destination. It collects information from other routers using IP, and it creates a topology map of the network.

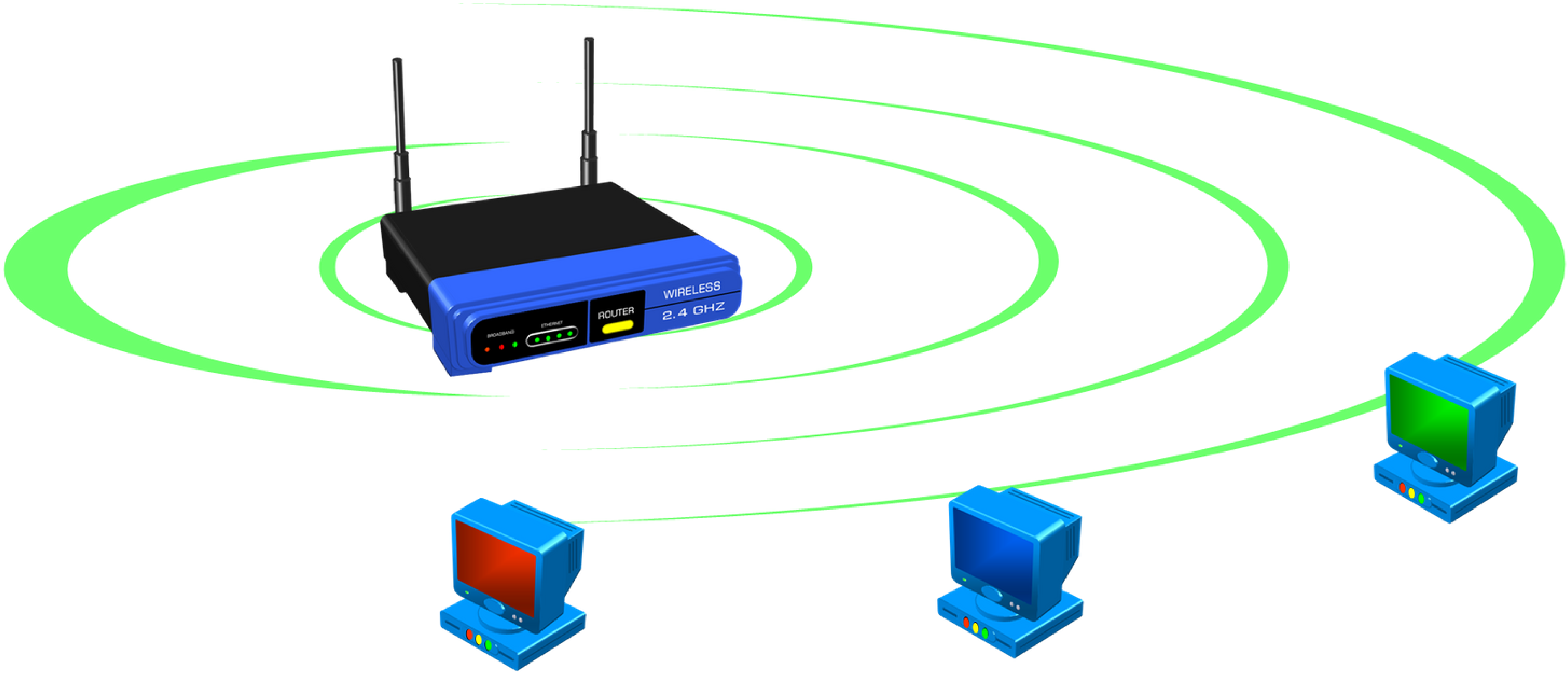
Another link state protocol is called **IS-IS**, which stands for **intermediate system to intermediate system**. In this system the routers are organized into a domain, which means that the routers are organized into groups.  This is how IS-IS primarily functions, is within these domains.  But unlike OSPF, where it uses IP to communicate, IS-IS uses CLNS instead, which is a connectionless network service.

Another type of routing protocol is called a **hybrid**, and in this case, we’re talking about **EIGRP**, which stands for **enhanced interior gateway routing protocol**. This is a combination of distance vector and link state protocols, and it only runs on Cisco routers.  It is fast, it has less overhead, and it can support many network layer protocols.

**SIP** stands for **session initiation protocol**.  This protocol is used for establishing communication sessions over the Internet.  For example, voice over IP, which is a term that is used for voice communications over IP networks.  It is also used for services such as instant messaging and conferencing.  And SIP operates at the application layer in the OSI model.

**RTP** stands for **real time transport protocol**, and this protocol is the internet standard for transporting real-time data, such as streaming audio and video.  RTP is often used over UDP, so it doesn't guarantee data delivery.  RTP is also used with **RTCP**, which stands for **real time transport control protocol**, and this enables you to monitor the quality of the data being delivered. And lastly, RTP can be used to send data over both unicast and multicast.

The term **broadcast** refers to when there was a single transmitter of data, and that data is being received by multiple receivers.  For example, a wireless router can broadcast its wireless signal and be picked up by multiple computers to access the internet.



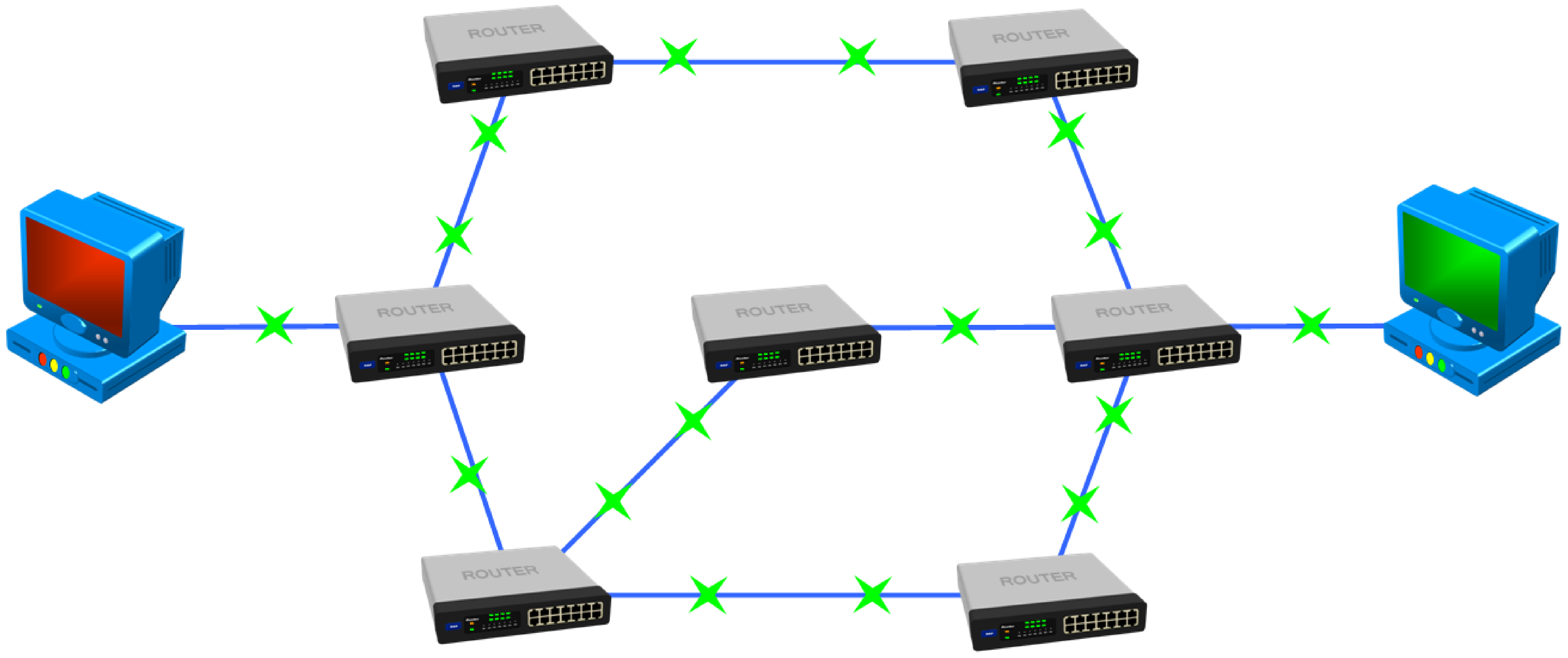
**A wireless router broadcasting its signal.**

The difference between **unicast** and **multicast**, is that with unicast, the data packets are sent to a single destination.  And with multicast, the data packets are sent to multiple destinations at the same time.

Some networks are designed to be more fault tolerant. For example, in some networks multiple switches are installed in case a switch does fail.  So in case of a failure, the data can bypass a failed switch and use the others to get to their destination.  But a potential problem can happen with this setup, and that problem is with broadcast traffic loops.  These loops can happen when there are multiple active paths between the destinations, and when this happens, it can slow down the network because of the excess traffic.  So to solve this problem, the **spanning tree protocol** was created.  The spanning tree protocol allows for fault tolerance and prevents unnecessary traffic loops in the network, and it does this by allowing the switches to talk to each other to find if loops are happening in the network.

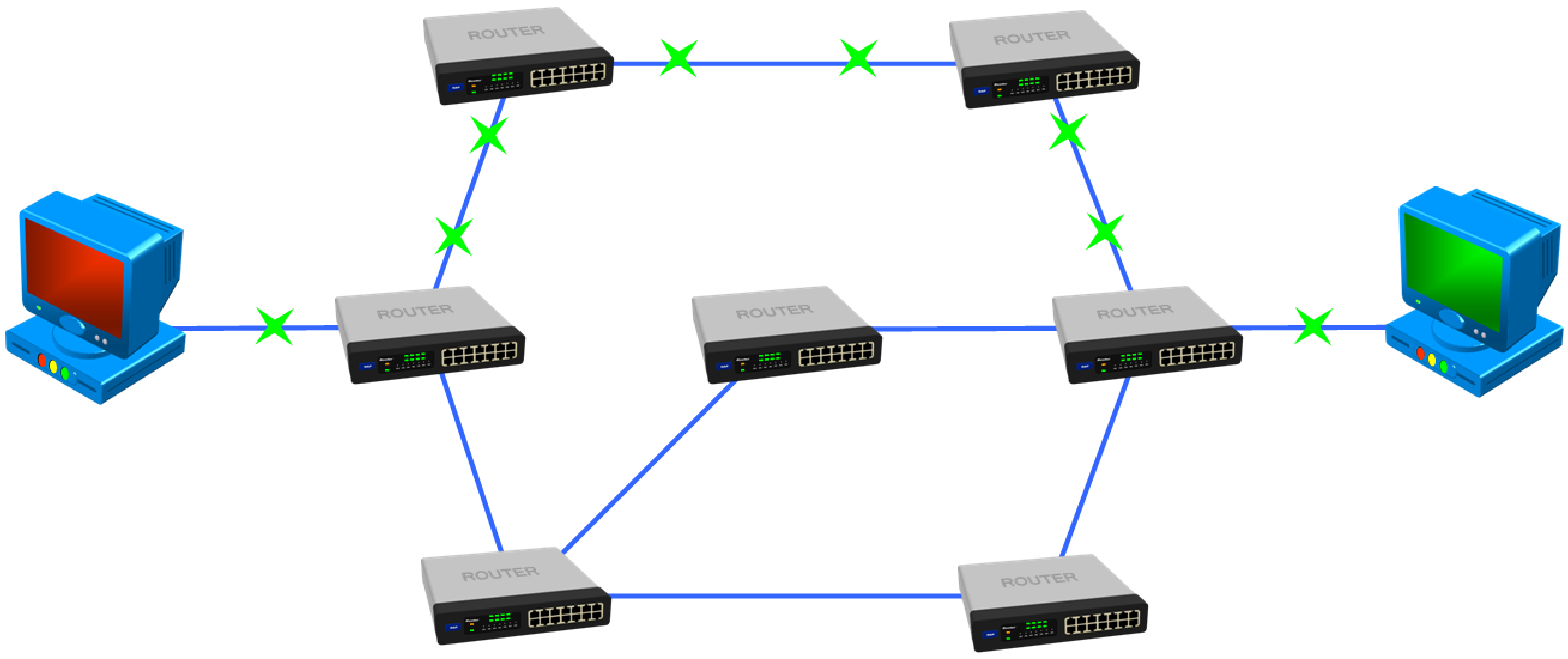
# WAN Technologies

When data is sent across a network, it is not sent as one large piece.  The data is actually divided into smaller pieces or data packets, and then they are sent individually.  These data packets are sent using two different methods, **packet switching** and **circuit switching**.  In packet switching, the data packets take different routes to their destination.  Then once all the data packets reach their destination, they are recompiled into the original message.  This method of communication is also known as connectionless.  The internet mostly uses packet switching technology.

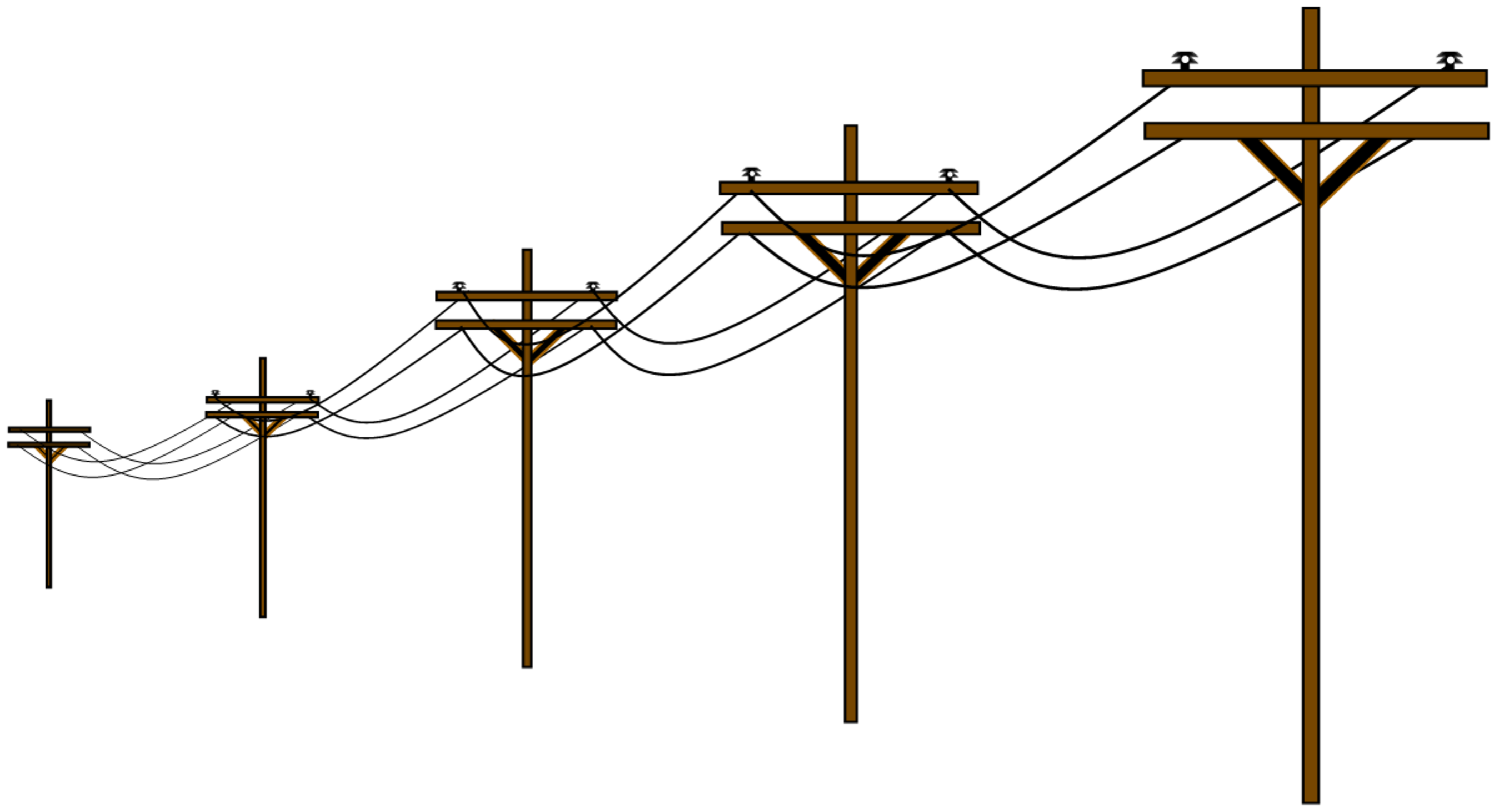


**Data takes multiple different routes in packet switching.**

Circuit switching also sends data packets individually, but unlike packet switching, which sends data on different routes, circuit switching does the opposite.  In circuit switching, all the data is sent along the same dedicated route.  A good example of circuit switching would be telephone lines.



**Data takes the same dedicated route in circuit switching.**



**Telephone lines using circuit switching.**

**T1** lines are a commonly used internet service for businesses today.  It's a dedicated connection that supports data rates of 1.544 Mbit/s.  A T1 line consists of 24 individual channels that each carries a rate of 64 Kbps.  Each of these channels can carry data or voice traffic.

A **T3** line is a high-speed internet connection that supports rates of 43 Mbit/s.  It consists of 672 individual channels, and each of these carries a rate of 64 Kbps. T3 lines are mainly used by internet service providers to connect directly to the backbone of the internet.

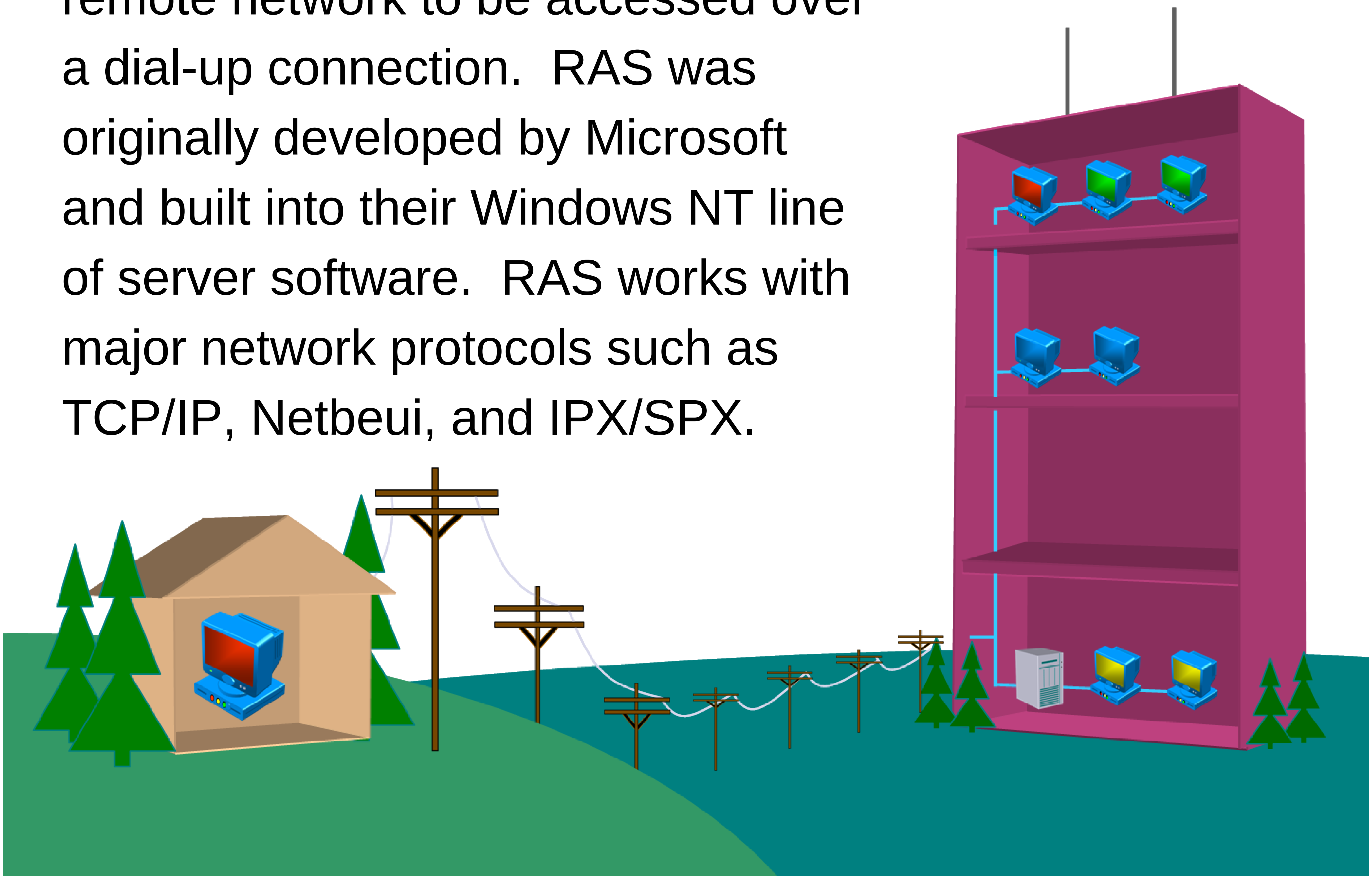
An **E1** line is similar to a T1 line, but an E1 line is the format that is used in Europe for digital transmission. The speed is 2 Mbit/s and consists of 32 channels that carry 64 Kbps of data.

An **E3** line is the European equivalent of a T3 line.  It has a speed of 34 Mbit/s and has fewer channels than a T3 line.

**OCx** stands for **optical carrier**.  These are levels that describe the speed of networks that can be carried on **SONET**, which stands for **synchronous optical network**.  It's a fiber-optic technology that delivers voice, data, and video, at high speeds.  The OC levels are calculated by multiples of 51.84 Mbit/s.

# Remote Access Protocols & Services

**RAS** or **remote access service** is a technology that enables you to connect to a computer from a remote location, for example, from your home to your job.  It allows the services which would be available on a remote network to be accessed over a dial-up connection.  RAS was originally developed by Microsoft and built into their Windows NT line of server software.  RAS works with major network protocols such as TCP/IP, Netbeui, and IPX/SPX.

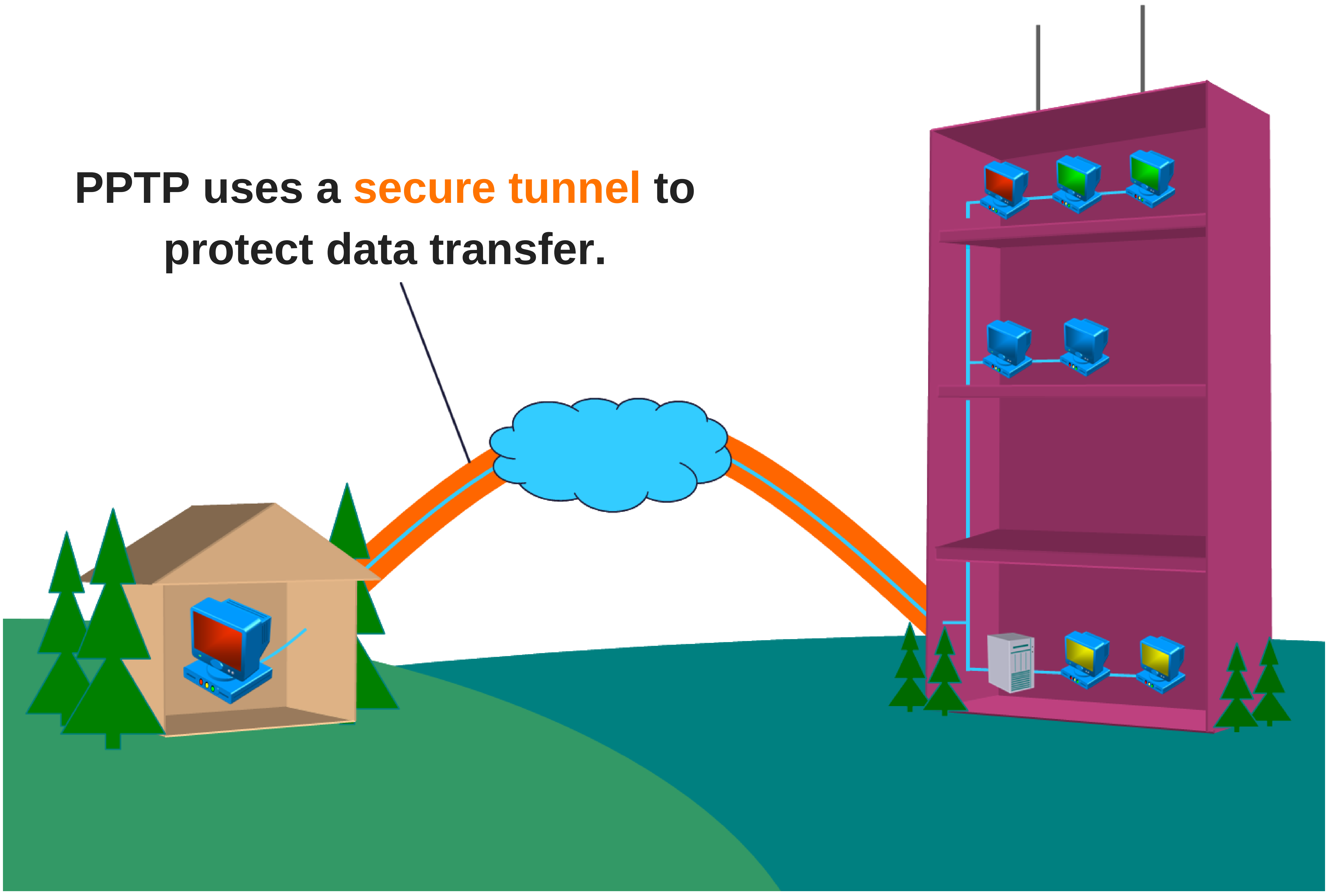


**SLIP** stands for **serial line internet protocol**.  This is a protocol for communication between two computers using a serial connection, such as a typical phone line. But SLIP is rarely used anymore because it's not a secure protocol.  During a dial-up connection, it sends all data, including sensitive data like passwords, in clear text.  So SLIP falls short because security is a major issue in today's world.  SLIP also does not provide any error checking and is limited to using only the TCP/IP protocol.  So a better protocol was needed to address these issues, and that protocol was PPP.

**PPP** stands for **point-to-point protocol**.  This is a standard remote access protocol that is used today.  It was developed to replace SLIP's limitation in security, error checking, and protocol support.  And like SLIP, this is a protocol that's used for communication between two computers using a serial connection, such as a typical phone line.  But unlike SLIP, this is a secure protocol.  Most internet service providers use this protocol for their customers who want to access the internet using a dial-up connection.

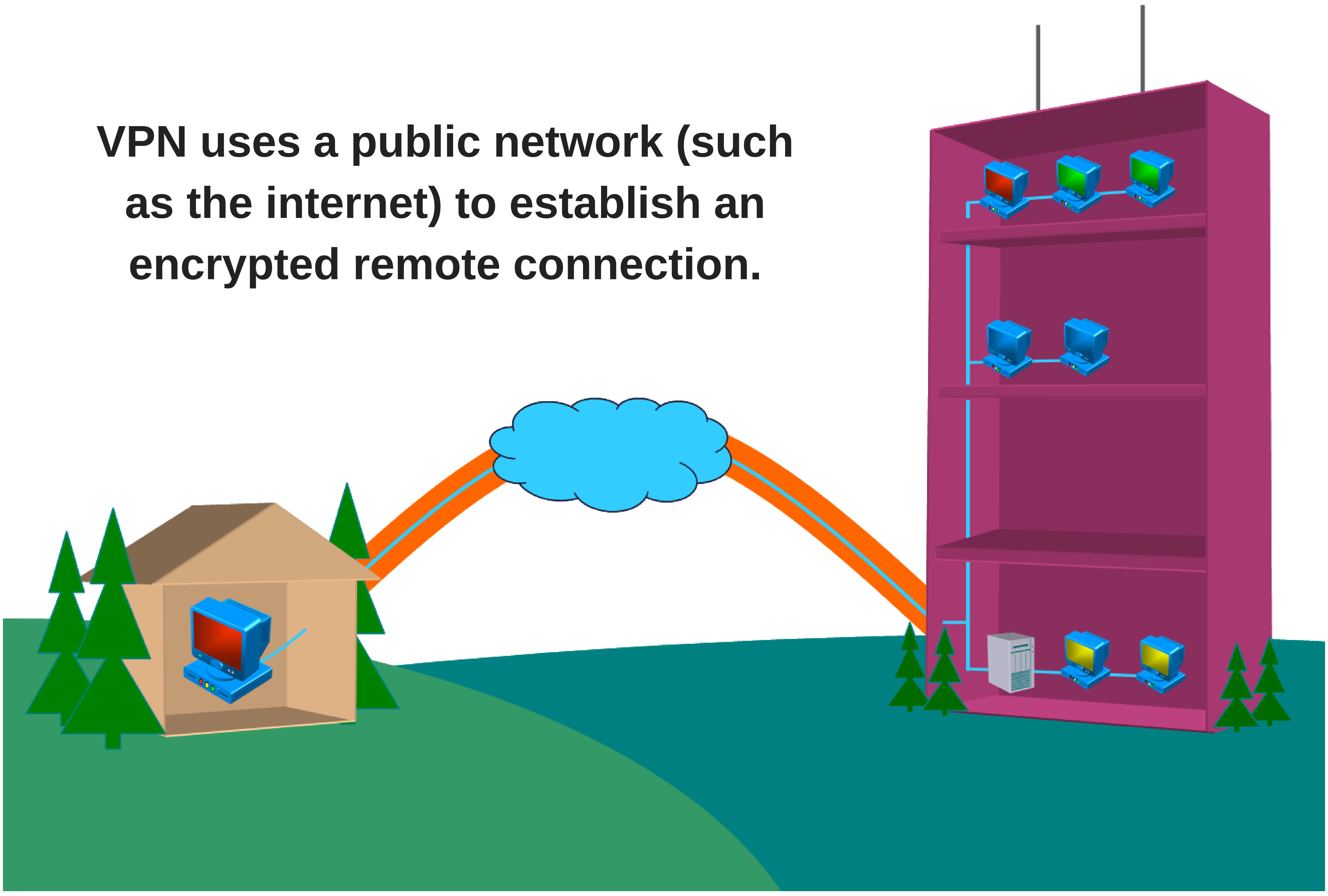
**PPPoE** or **point-to-point protocol over Ethernet** is exactly what its name implies.  This protocol uses PPP over Ethernet.  It works by encapsulating PPP frames in Ethernet frames.  People who use this protocol have a DSL, broadband, or wireless connection to the internet. It's also used for connecting multiple users on a local area network to a remote site sharing a common device.

**PPTP** or **point-to-point tunneling protocol** is a technology that is used for creating virtual private networks or VPNs.  In fact, this is the default protocol associated with VPNs.  This ensures that the transfer of data between one device to another is secure by creating a secure tunnel between the two points.



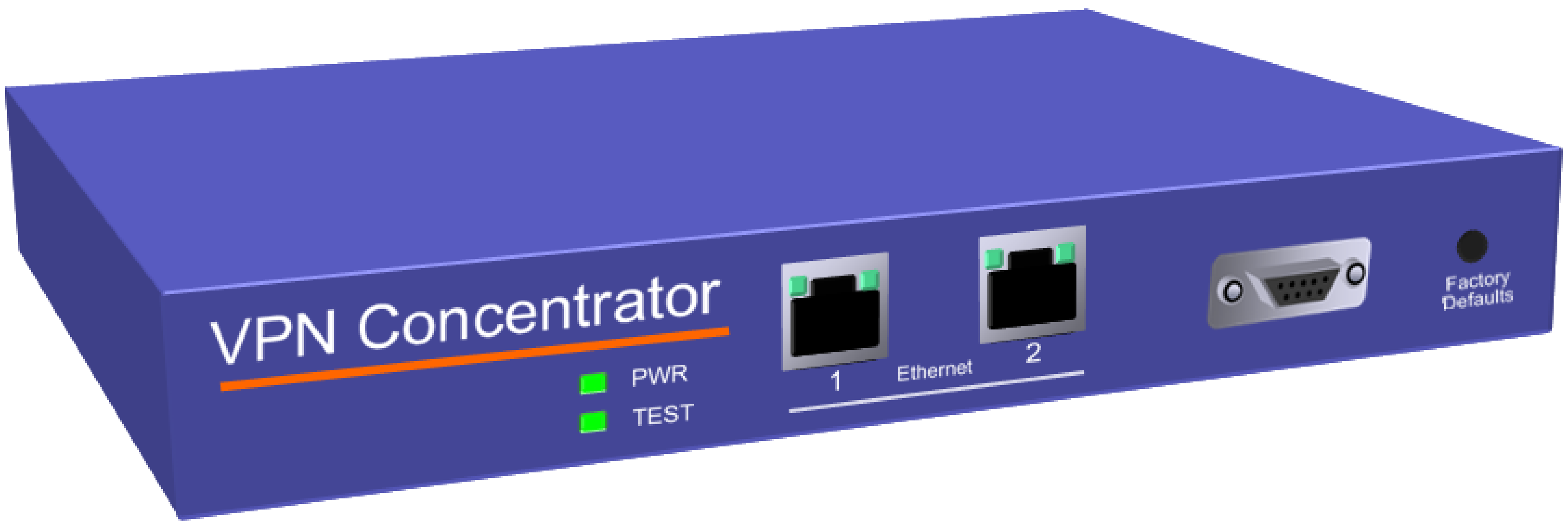
**GRE** or **generic route encapsulation** is a protocol that is used with point-to-point tunneling protocol in the creation of a VPN network.  GRE is what actually creates the tunnel in PPTP.  It is used to encapsulate the data in a secure manner.

A **VPN** is a **virtual private network**.  It's a private network that uses a public network, such as the internet, to establish a remote connection.  The data is encrypted as it sends and decrypted when received.  It provides a dedicated link between two points over the internet.



**VPN uses a public network (such as the internet) to establish an encrypted remote connection.**

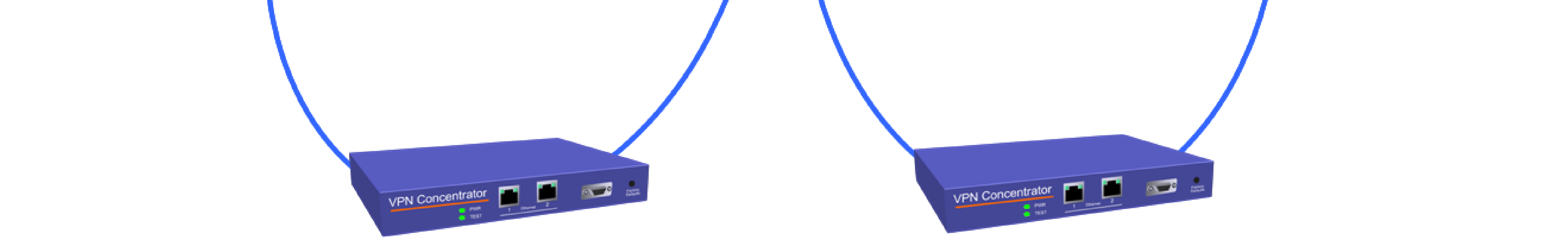
The way a VPN is created and managed is by using a **VPN concentrator**. A VPN concentrator is a device that creates the VPN connection and manages the delivery of the messages between the VPN computers and devices. It also authenticates users and encrypts and decrypts the data. It also assigns tunnel IP addresses to users.



**VPN concentrator**

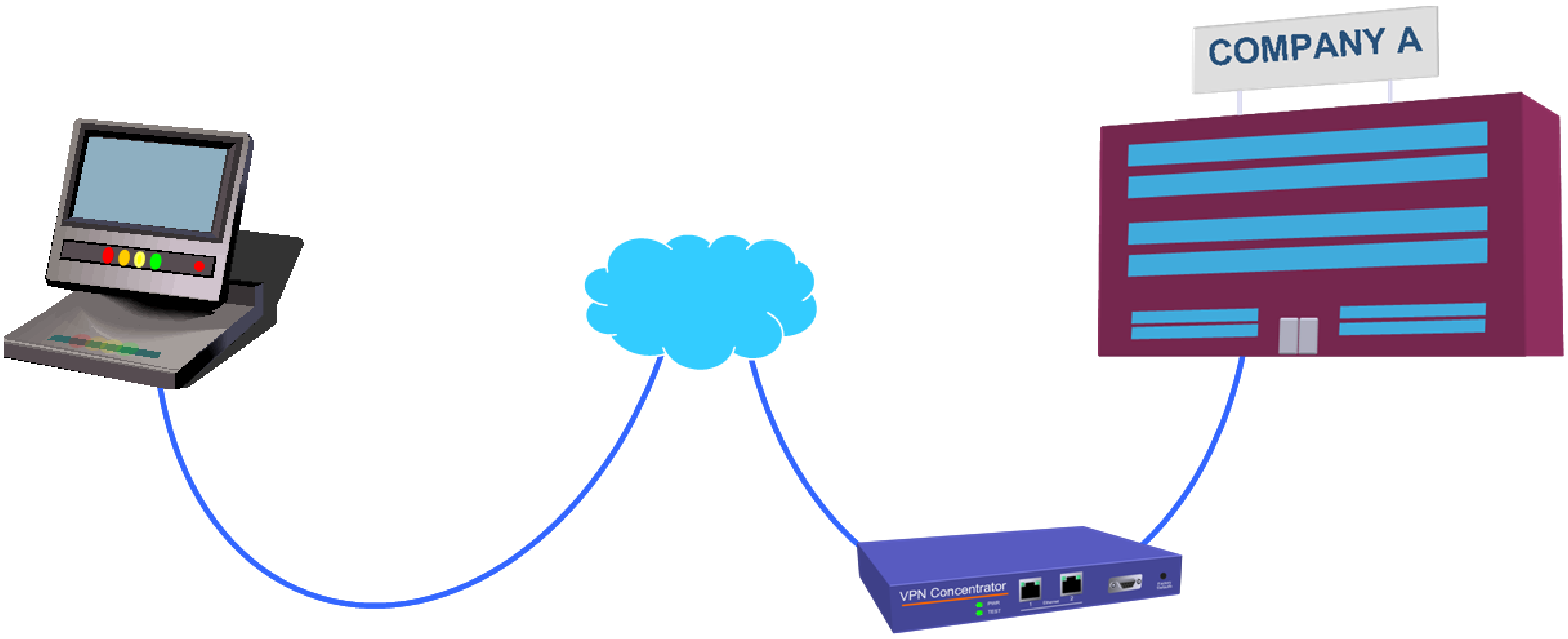
However, VPN concentrators are not always needed to manage and create VPNs. They are mainly used in organizations that are going to use a lot of VPN connections and they need a device to handle the heavy traffic that VPNs create.  If an organization is only going to use a few VPN connections, then they can just use the VPN software that is built into their router or firewall, rather than using a VPN concentrator.

There are three different types of VPN connections. One type is called **site to site**.  This is when an organization has two offices in different geographical locations, and they want those offices to be networked and share data with each other over the public internet. So they would just need to set up a site to site VPN connection.  Then the VPN will encrypt the data as it goes through the internet and then decrypt the data as it enters the organization's private network.  Creating a site to site VPN creates an alternative to an internet leased line at a much cheaper cost.



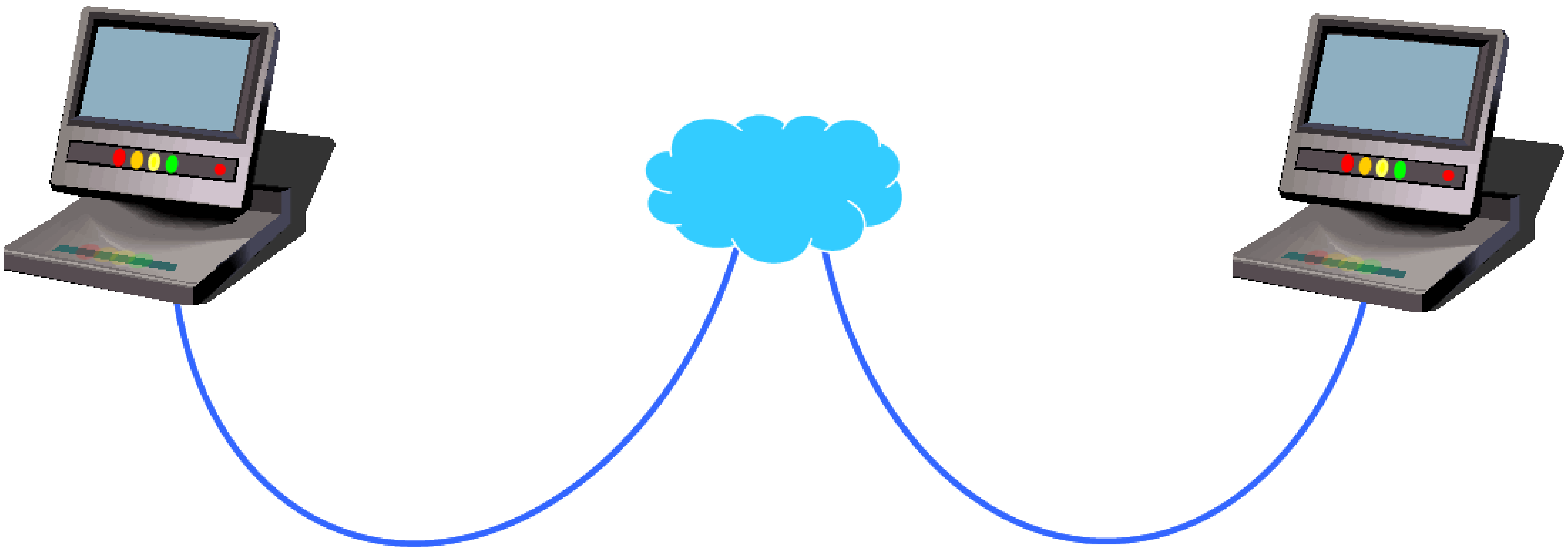
**Site to site VPN**

Another type of VPN connection is called **host to site**. So, for example, if you're at home with your computer and you needed to connect to your office at a different location so you can access files, then you would need to set up a host to site VPN connection. Now generally this type of connection doesn't require any additional hardware on your end at home. You would basically just need your computer's operating system to connect to your office's VPN hardware. Then once the connection is made, you can then access your office's network over the internet. So all the special VPN hardware would be on the office or the site side of the connection and not at your home.



**Host to site VPN**

Finally, there is the **host to host** VPN connection. This is simply when you want to establish a VPN connection between two computers over the internet. This type doesn't require any additional VPN hardware at either end. It only requires the software on each computer to create a simple host to host VPN connection.

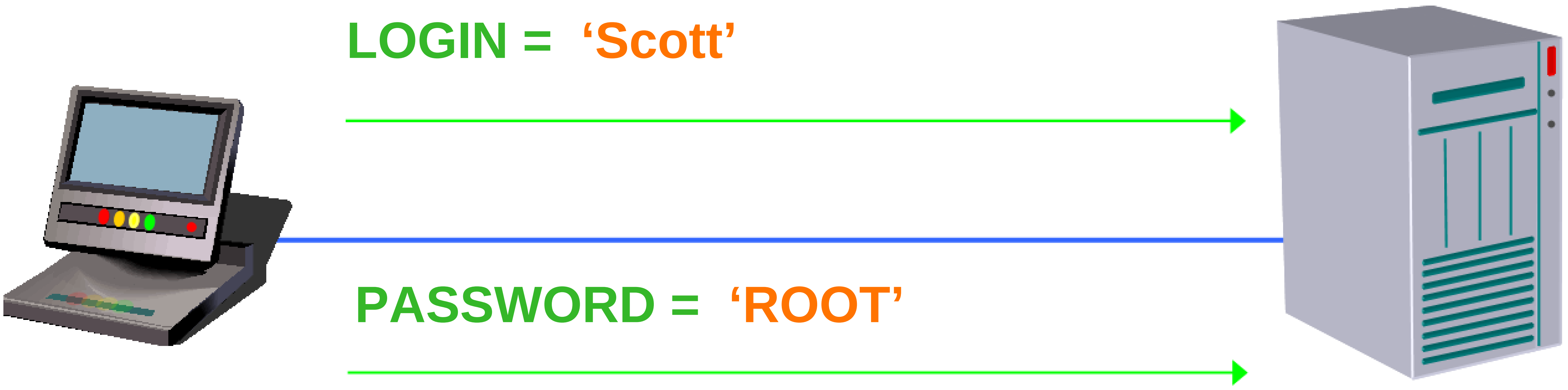


**Host to host VPN**

# Authentication Protocols

Authentication is confirming something that is authentic or true. In computers, authentication is the process of verifying the identity of a user, such as a username or a password. In the world of networking, there are several protocols that are used to achieve authentication.

So, the first protocol we're going to discuss is called **PAP** or **password authentication protocol**. This is a very simple authentication protocol. In fact, it's so simple, that it's compatible with just about everything. However, the downside is that it's not very safe.
All sensitive data, like usernames and passwords, are sent in clear text.



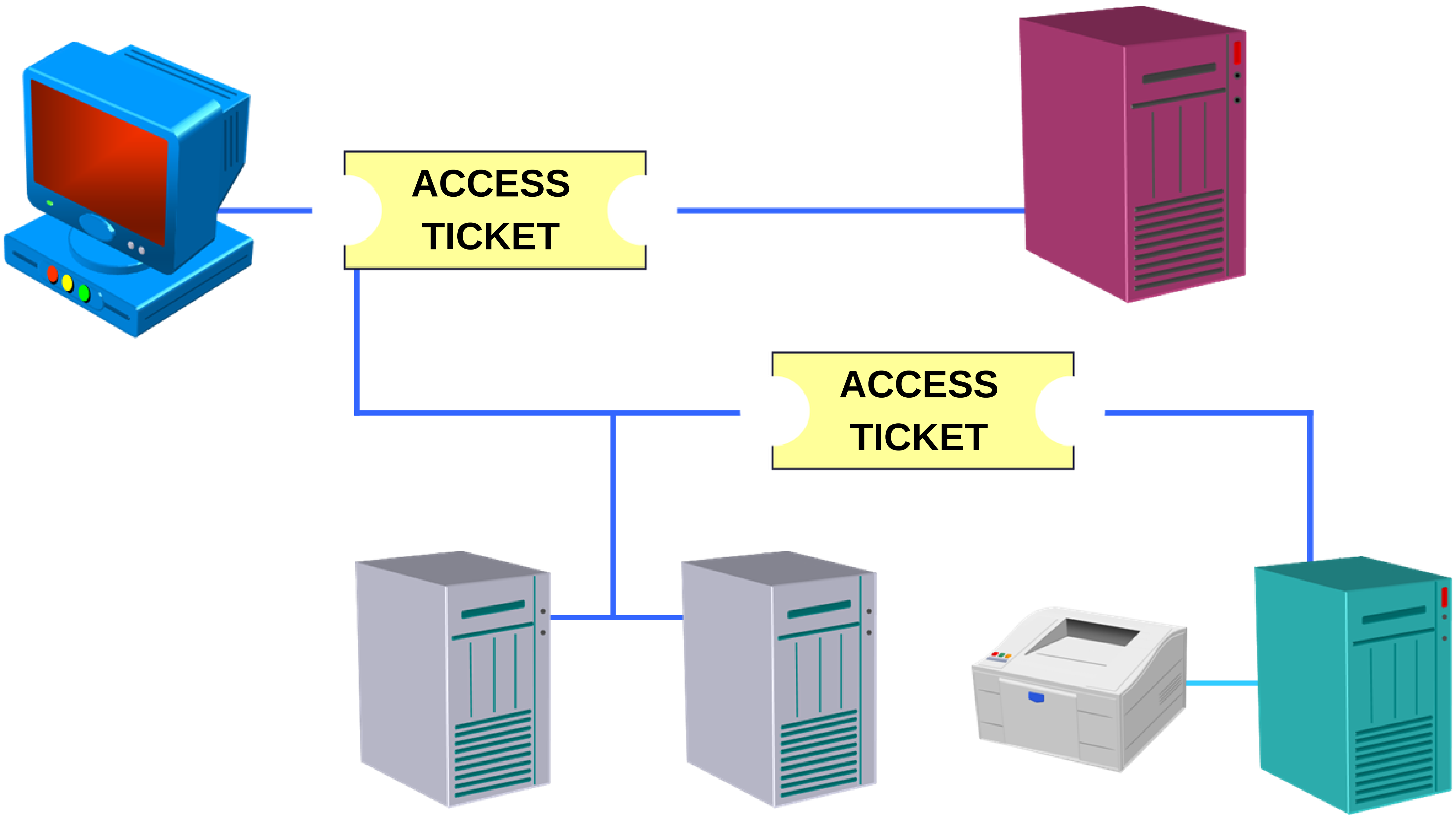
**In PAP, all usernames and passwords are sent in clear text. It's not secure.**

**Challenge handshake authentication protocol** or **CHAP**, is a better alternative to PAP because it encrypts usernames and passwords. This protocol authenticates by the server asking or challenging the client to validate itself by using a three-way handshake. So, after a connection has been made, the (**1**) server sends a challenge to the client. Then the (**2**) client responds by using a one-way hash function with the answer. Then the (**3**) server checks the response against its own calculation, and if the value matches, then the authentication is passed.

**MS-CHAP** is Microsoft's version of CHAP. There are two versions of MS-CHAP: MS-CHAP and **MS-CHAP v2**. MS-CHAP is basically CHAP, so it only authenticates the client. But MS-CHAP v2 offers mutual authentication. Both the client and the server are authenticated, so it's more secure.

**RADIUS** is a protocol that enables a single server, such as a domain controller, to handle all authentication. It allows a company to store user access data in a central location.  Users log in to the radius server and that makes the request on the user's behalf after authenticating.

**Kerberos** is an authentication protocol that was developed by MIT.  It authenticates by using tickets.  In order for a client to access network resources, it first authenticates itself with the Kerberos server.  Then after authentication, the client is issued a ticket which then gives the client access to the network resources.



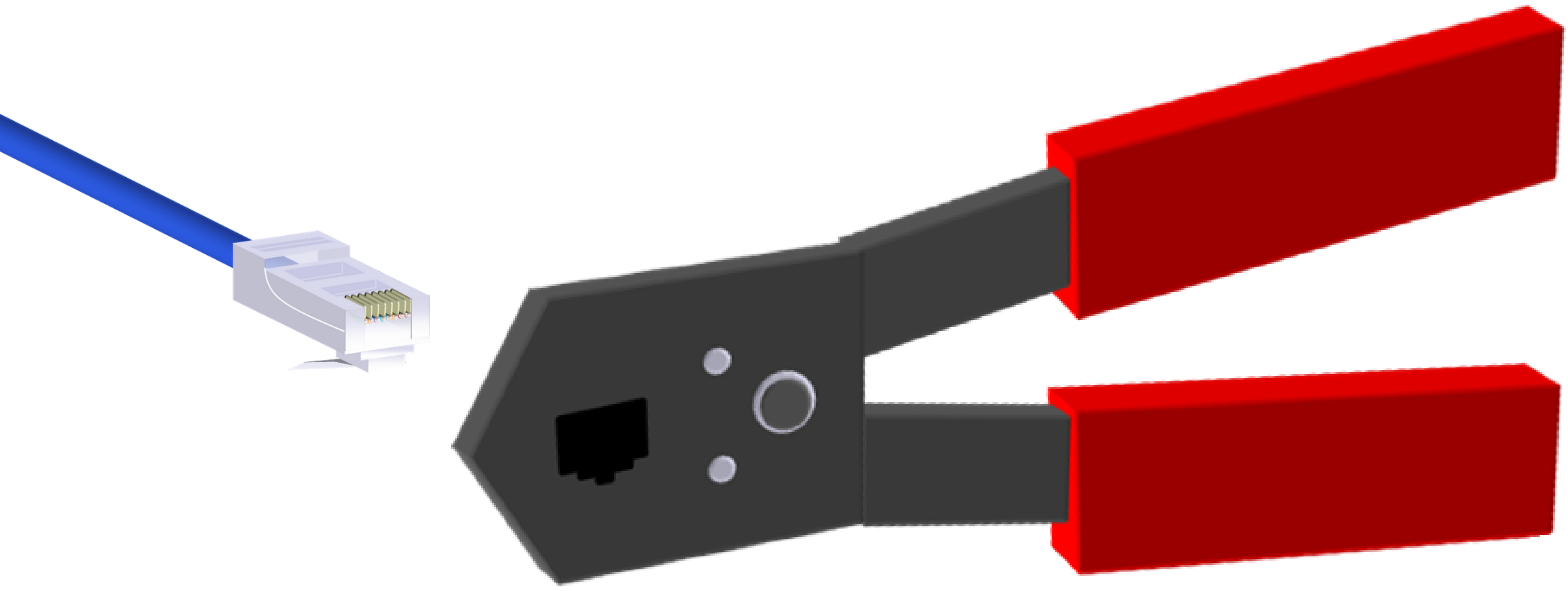
**Kerberos grants access to network resources by using tickets.**

**EAP** stands for **extensible authentication protocol**. This is an extension to PPP.  It's a general protocol that supports many methods of authentication.  The most common one that is associated with, is smart cards.

**EAP is commonly used with smart cards.**

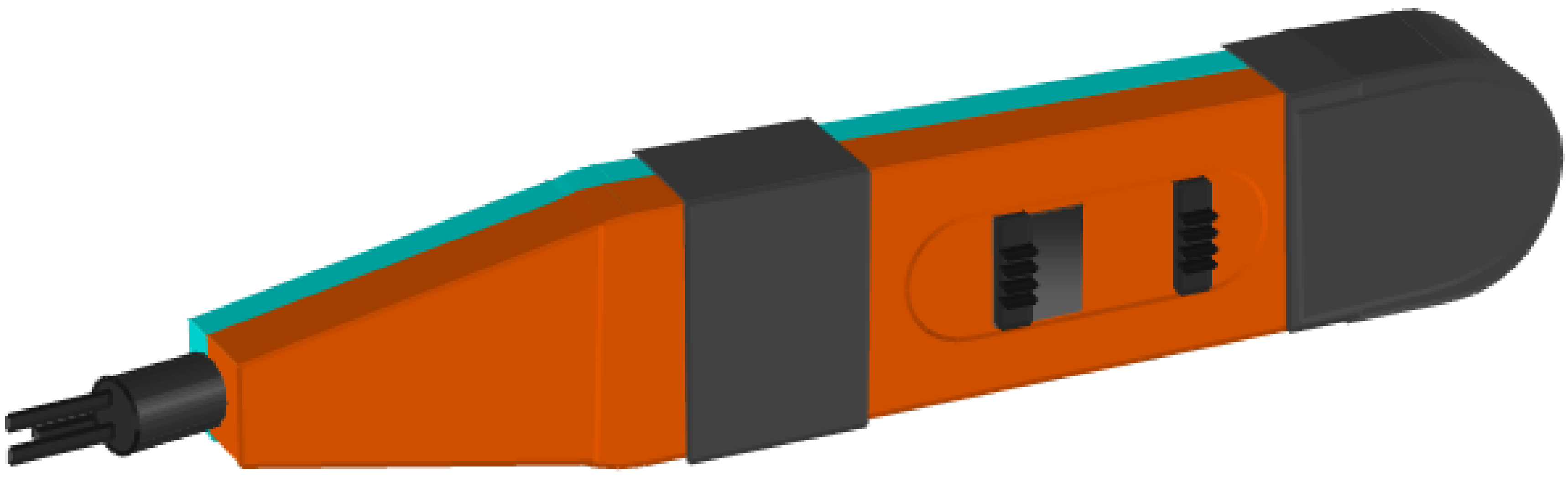
# Networking Tools & Safety

If you're already a network administrator, then the most common tool that you've probably used is the **wire crimper**.  This tool is used to make custom length network cables.  It crimps adapters, such as the RJ-45, to twisted pair cables.  So after you have attached your RJ-45 adapter to your cable, you just place it into the crimper, give it a squeeze, and the cable is done.



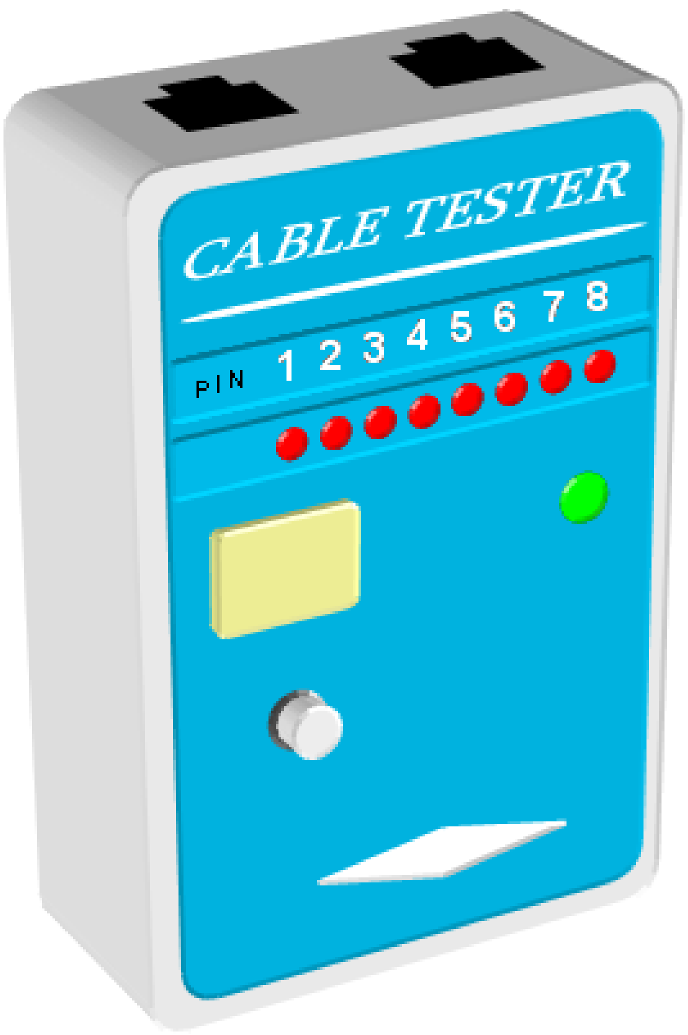
**Wire crimper**

A **punch down tool** is a tool that resembles a screwdriver.  This is simply used to connect or punch wires into a punch down block.



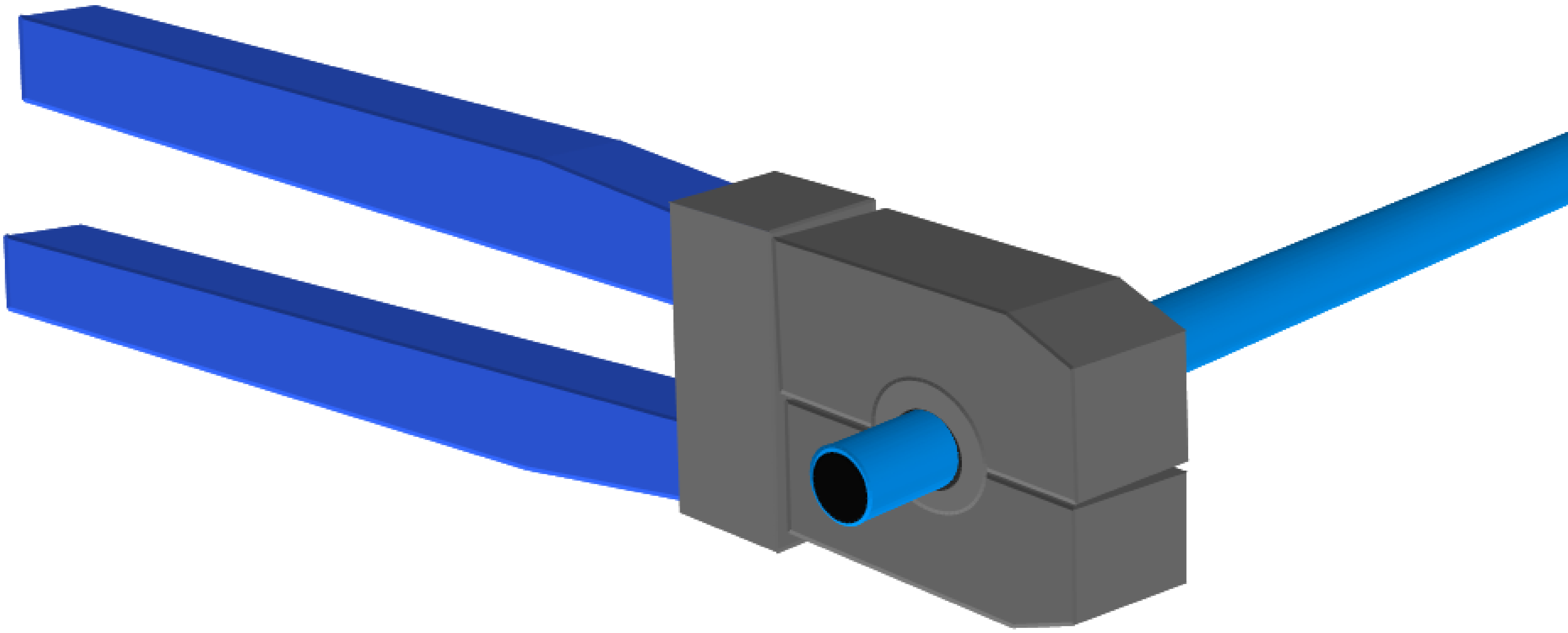
**Punch down tool**

Another network tool is a **media tester**.  So after making a custom length cable using your wire crimper, it's a good idea to test the cable to make sure it's wired correctly.  So you would just connect both ends of the cable into the tester, and then the tool will check the cable for you.



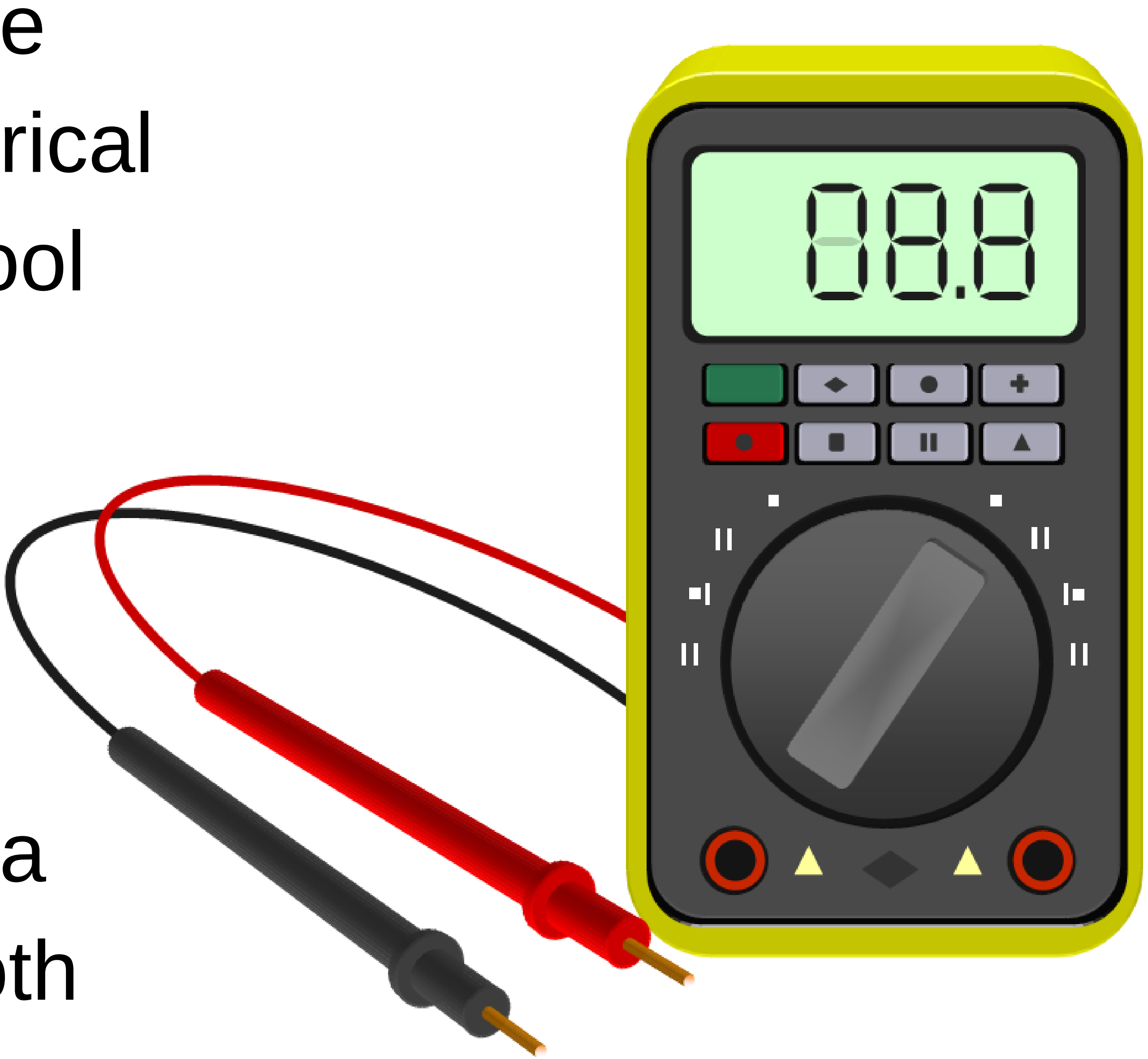
**Media tester**

The plastic shielding around a network cable must be removed in order to crimp a connector.  This is done by using a **cable stripper**.  The cable is inserted into the tool and then the outer plastic shielding is removed.



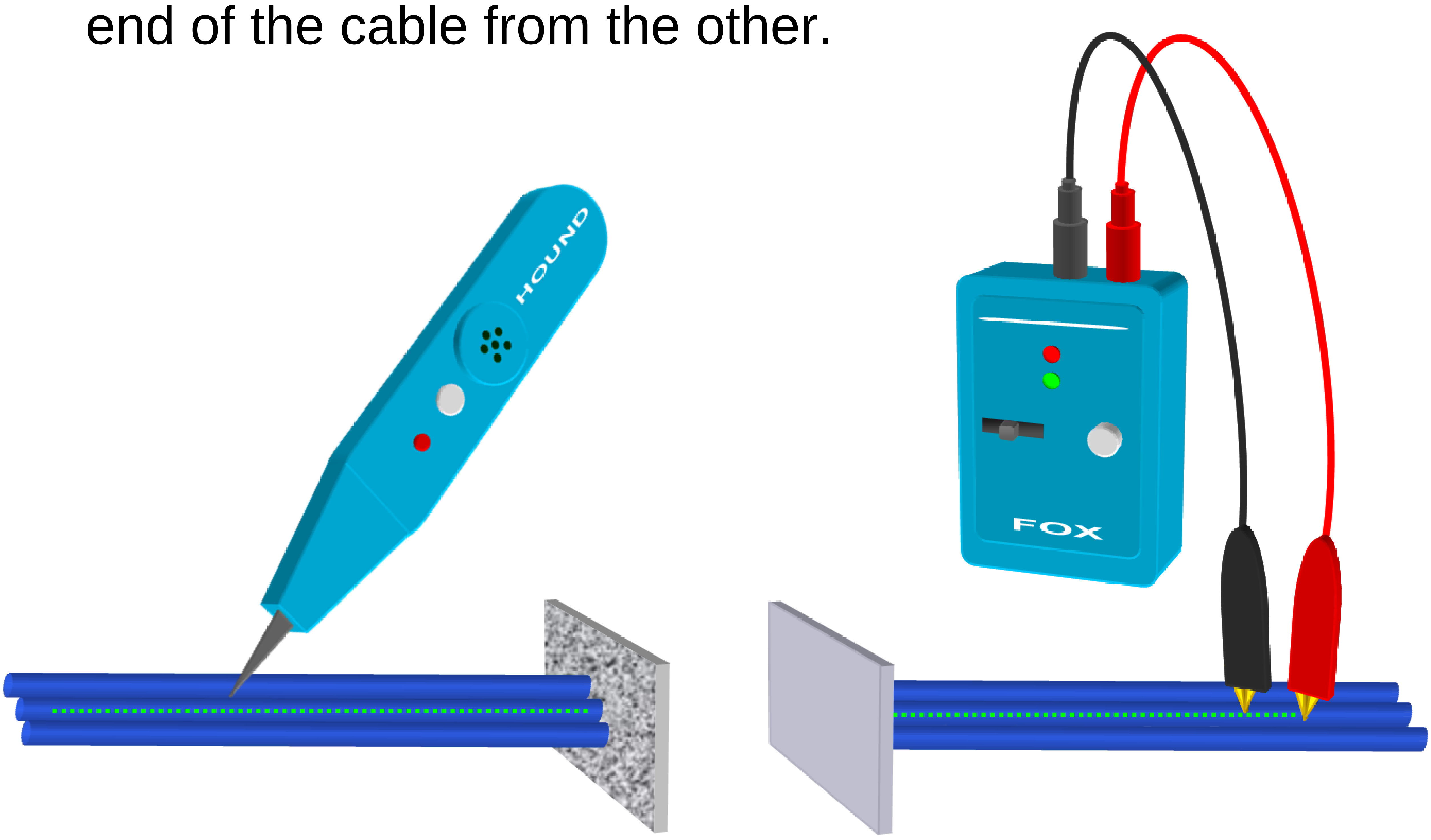
**Cable stripper**

A **multimeter** is a device that is used to test electrical circuits. It's a popular tool that is used for many different trades. It can measure voltage, resistance, current, and continuity, just to name a few. And it comes in both analog and digital versions.



Multimeter

A **tone generator** is also known as a Fox and Hound. It's a tool that is used for locating cables from one end to the other. So for example, if you suspect that you have a bad cable that was grouped with a lot of other cables, and that group was stretched over a long distance, it would be very difficult to isolate one end of the cable from the other.

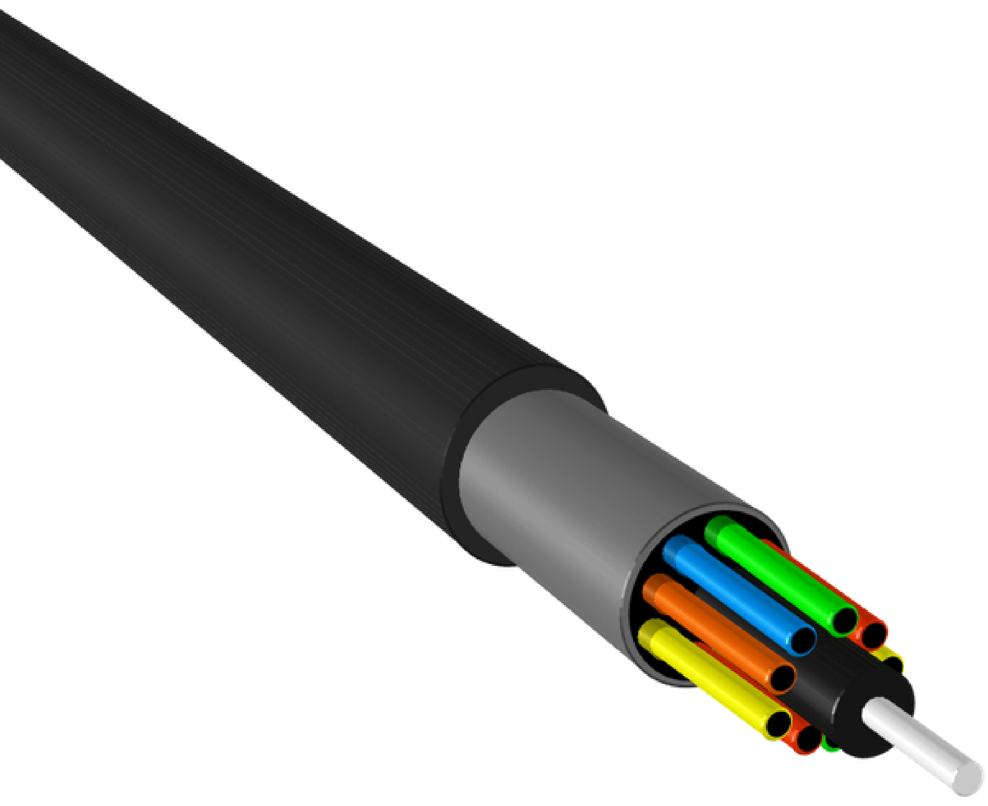


Tone generator generating a tone through a cable to pinpoint it at the other end.

So that's where a tone generator comes in. So you just connect the tool at one end of the cable, and then it would generate a tone through the cable, where the other part of the tool would detect the sound and pinpoint the cable.

A **time domain reflector** is a piece of electronic equipment used to test cables, such as unshielded twisted pair and coaxial cable. This test is done by transmitting a signal through a cable and then the signal is reflected back to the TDR. The TDR then analyzes the reflected signal and from there it's able to pinpoint if there are any problems. These problems include conductors, loose connectors, shorts, crimps, bends, and so on.

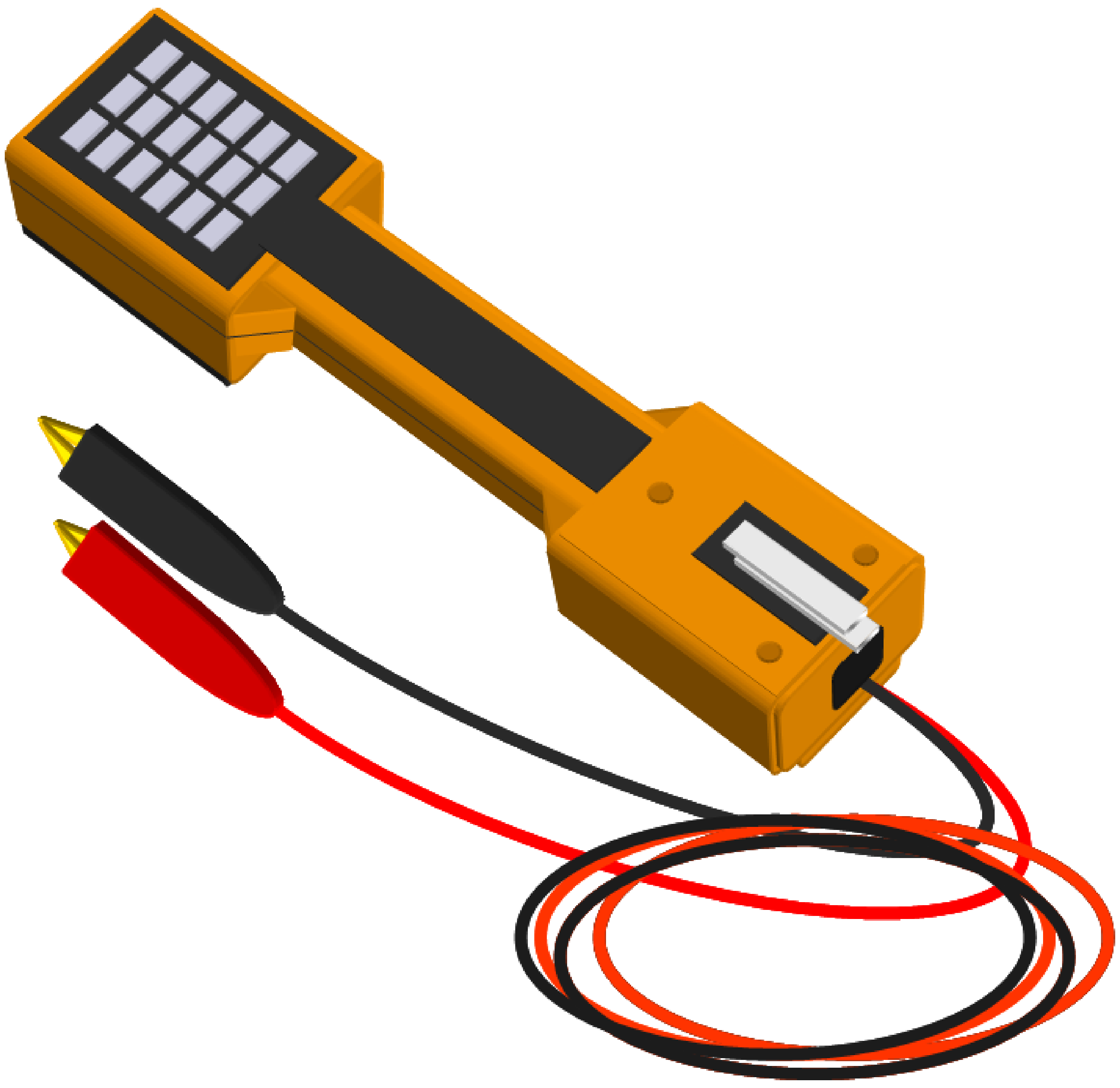
**A TDR tests cables, such as coaxial and UTP.**



**An OTDR tests fiber optic cables.**

An **optical time domain reflector** or **OTDR** does the same thing as a TDR, but it is used on fiber optic cable. Instead of transmitting a signal, an OTDR transmits light through the cable to detect problems.

A lot of telephone technicians carry a piece of equipment called a **butt set**.  A butt set is a device that resembles a telephone.  It's used to test and monitor telephone lines.  The technician will hook up the device, and as its name implies, 'butt' into a line to hear a conversation to determine if there are any problems.  Problems such as noise, or something simple, like just detecting if there is a dial tone.

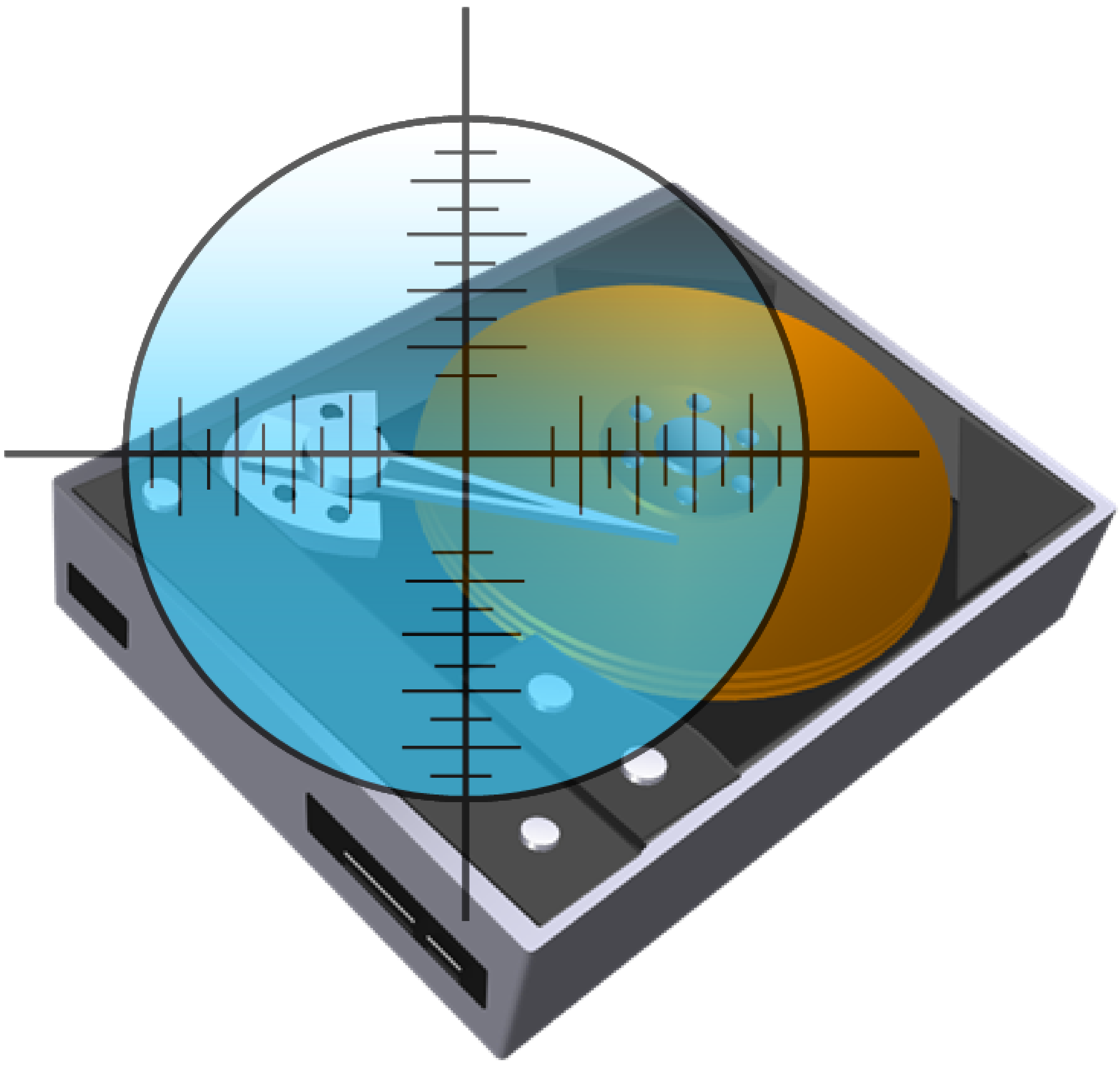


**Butt set**

A **protocol analyzer** is also known as a **packet sniffer**.  This is a software or hardware tool that is used to troubleshoot and analyze traffic on a network.  It can troubleshoot and analyze things such as logs, data packets, broadcasts, and so on.  It can detect network problems, intrusion attempts, and monitor networking issues so a technician can correct the problem.  A very common software protocol analyzer is called Wireshark, and it can be downloaded for free at wireshark.org.

A virus is a harmful program that is written to alter the way a computer operates.  Most of the time users do not know that they have a virus until it's too late. Most viruses are transferred from the internet such as websites, downloadable programs, and email. If a computer virus is not detected and removed it could spread and cause serious damage to computers and servers in a network.

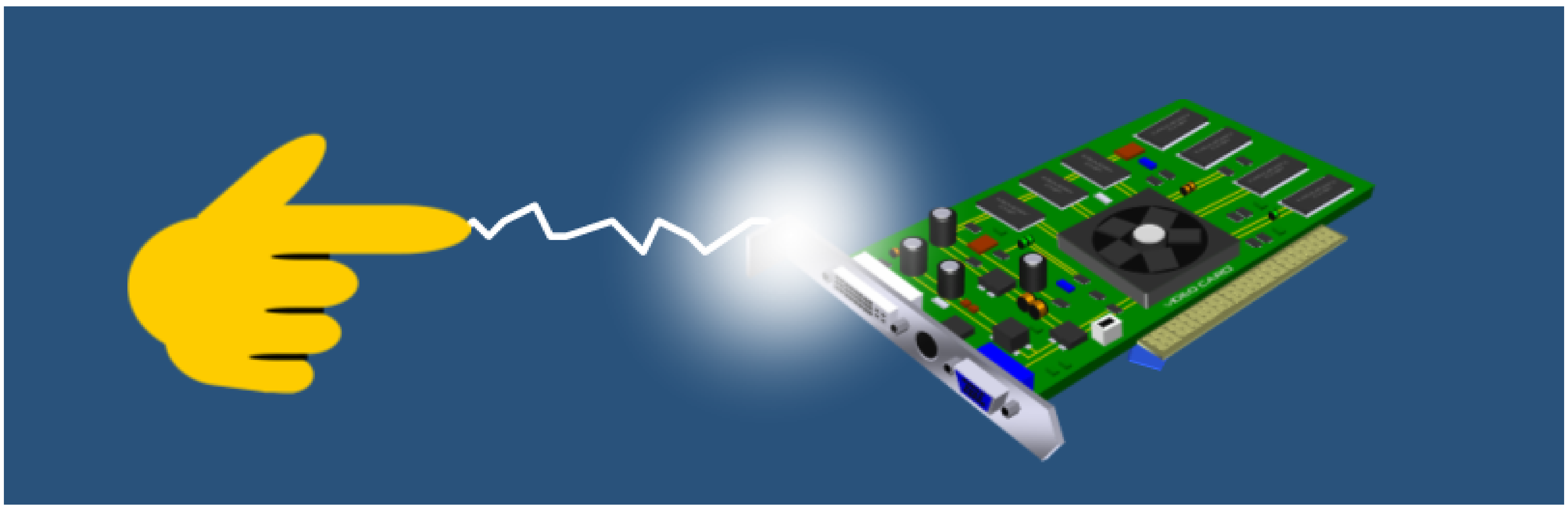
So that's why today, network administrators need to use **antivirus software**. Antivirus software is the number one protection against viruses. It's a software program that scans for viruses on your computer's hard drive, targets them, and destroys them before any damage can be done. It's also important to remember to always keep your antivirus software updated. Most updates, if not all, can be downloaded over the internet. In order to maintain optimum protection against viruses, you need to scan the computers on your network on a regular basis.



**Antivirus scanning a hard drive for viruses.**

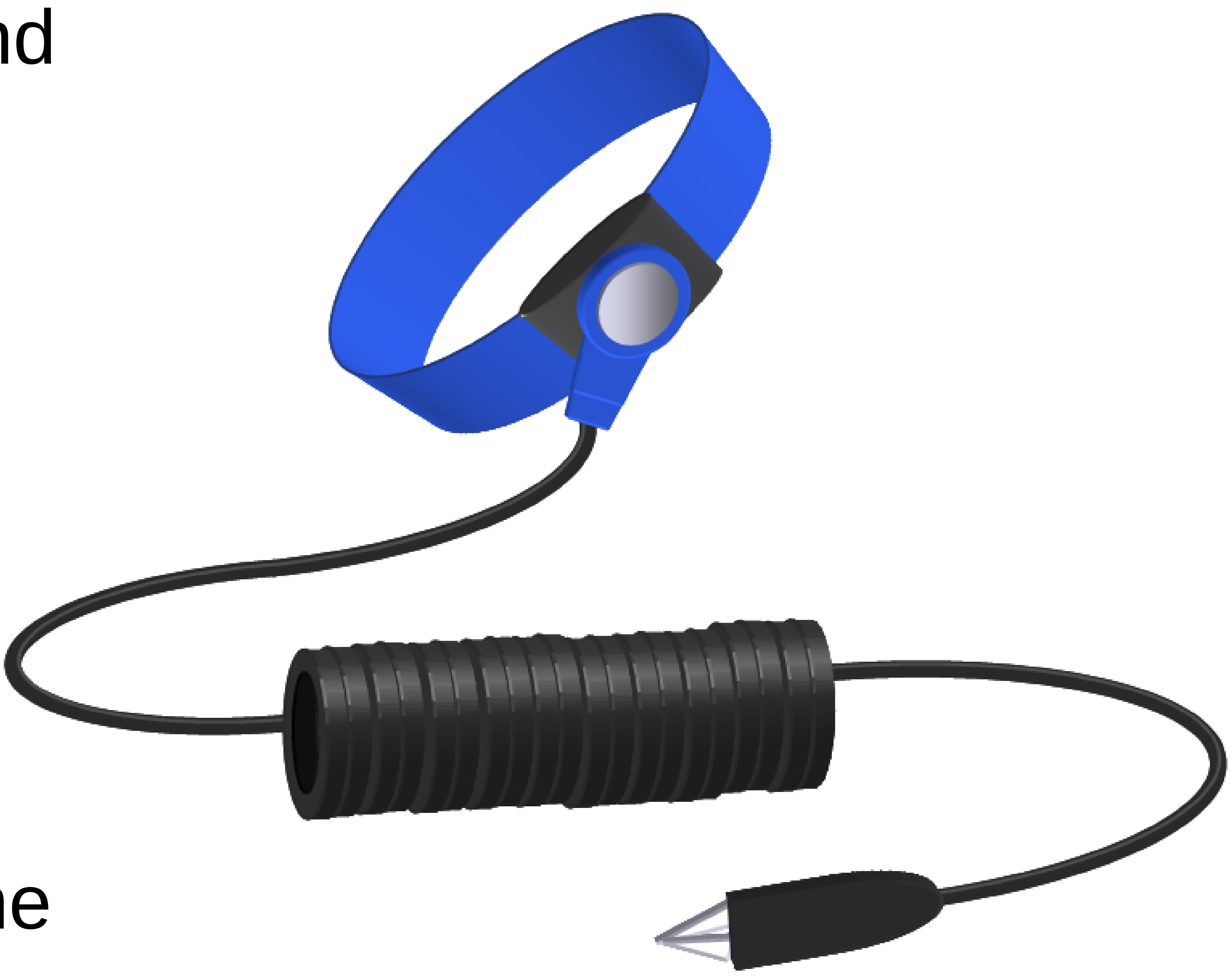
When working on a computer, it's important to not do any damage to the computer components that could be caused by **ESD** which stands for **electrostatic**

**discharge**. ESD happens when two objects of the opposite charge, such as your hand and a computer part, come in contact with each other. When this happens, a sudden charge of electricity flows through the two objects.



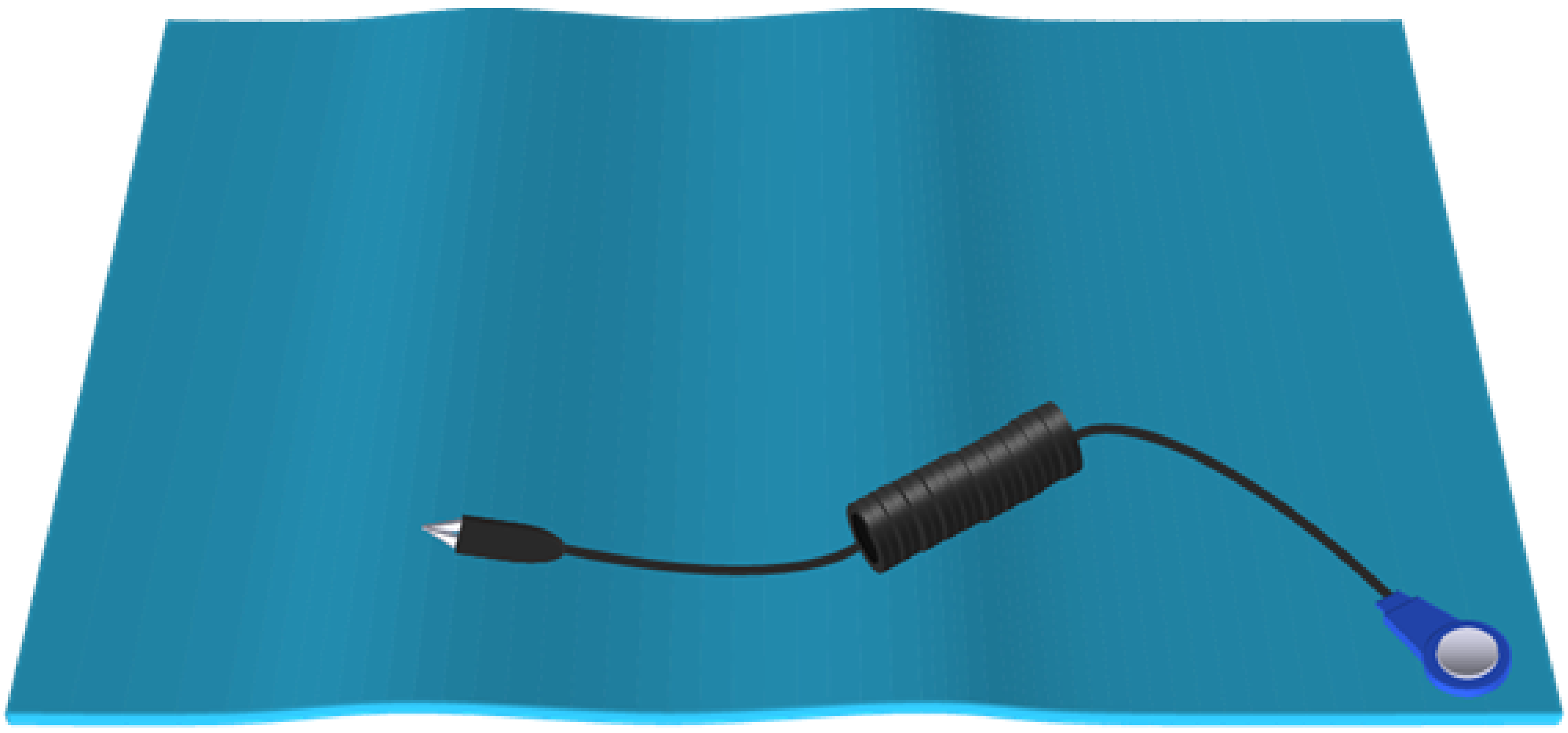
**ESD can damage computer components.**

This sudden charge of electricity can damage computer components. So to prevent this from happening, it's important to wear an **ESD wrist strap**. By wearing an ESD wrist strap, it can stop the build-up of static electricity in your body by safely grounding you. One end of the ESD strap fits around your wrist and the other end is grounded. The grounded end can be either attached to the ground pin in a power outlet or clipped onto the metal case of the computer you're working on.



**ESD wrist strap**

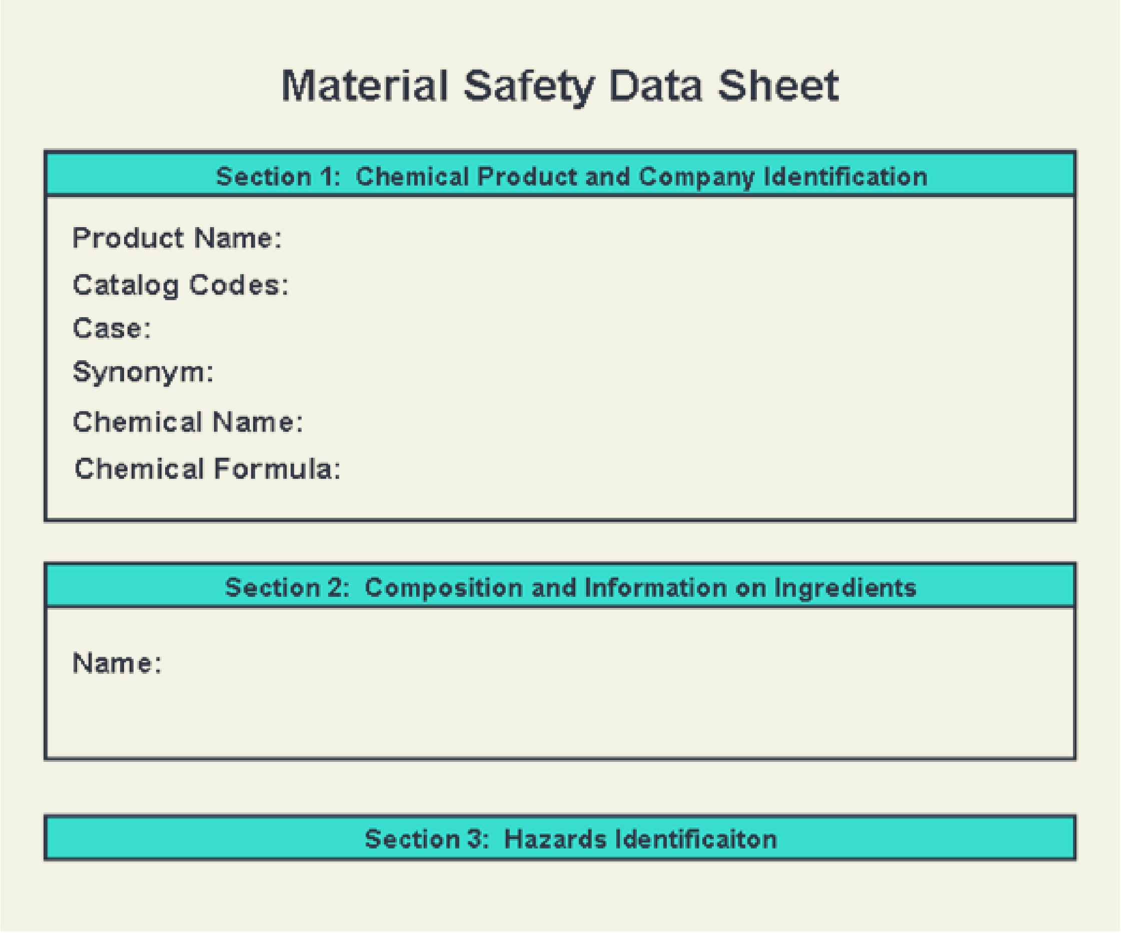
Another thing you can do to protect against ESD is by using an **ESD mat**.  An ESD mat is typically placed on a desk where assembly takes place.  The mat removes any electrical charge from the components that are placed on it.  And just like an ESD wrist strap, an ESD mat is also connected to a ground.



**ESD mat**

When dealing with our environment, it's important to understand what is the proper way to dispose certain pieces of equipment so that it doesn't affect the environment in a negative way.  Computer related equipment is no exception.  For example, computers contain lead and harmful chemicals, such as mercury, that is harmful to the environment.  So, for this reason, they must be disposed of in a proper way.  However, if you're not sure how to dispose it, there's a datasheet you can find called the **MSDS**,

which stands for **material data safety sheet**. This will tell you the proper way to dispose that particular piece of equipment. The MSDS would typically be offered by the manufacturer or you can download a copy of it from the EPA.



Material Safety Data Sheet

Section 1: Chemical Product and Company Identification

Product Name:
Catalog Codes:
Case:
Synonym:
Chemical Name:
Chemical Formula:

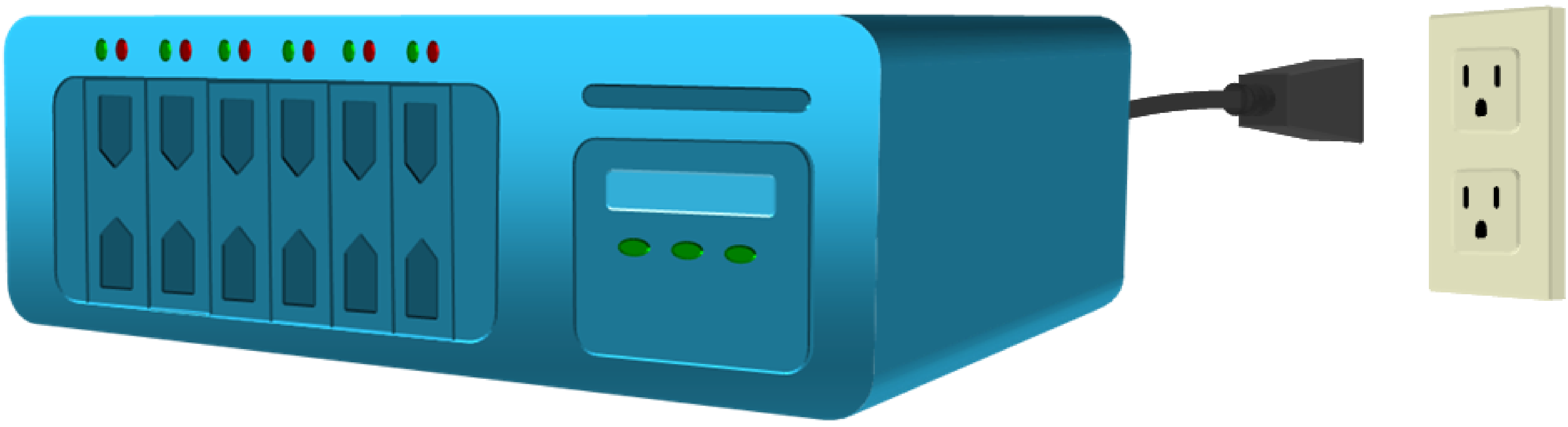
Section 2: Composition and Information on Ingredients

Name:

Section 3: Hazards Identificaiton

**MSDS**

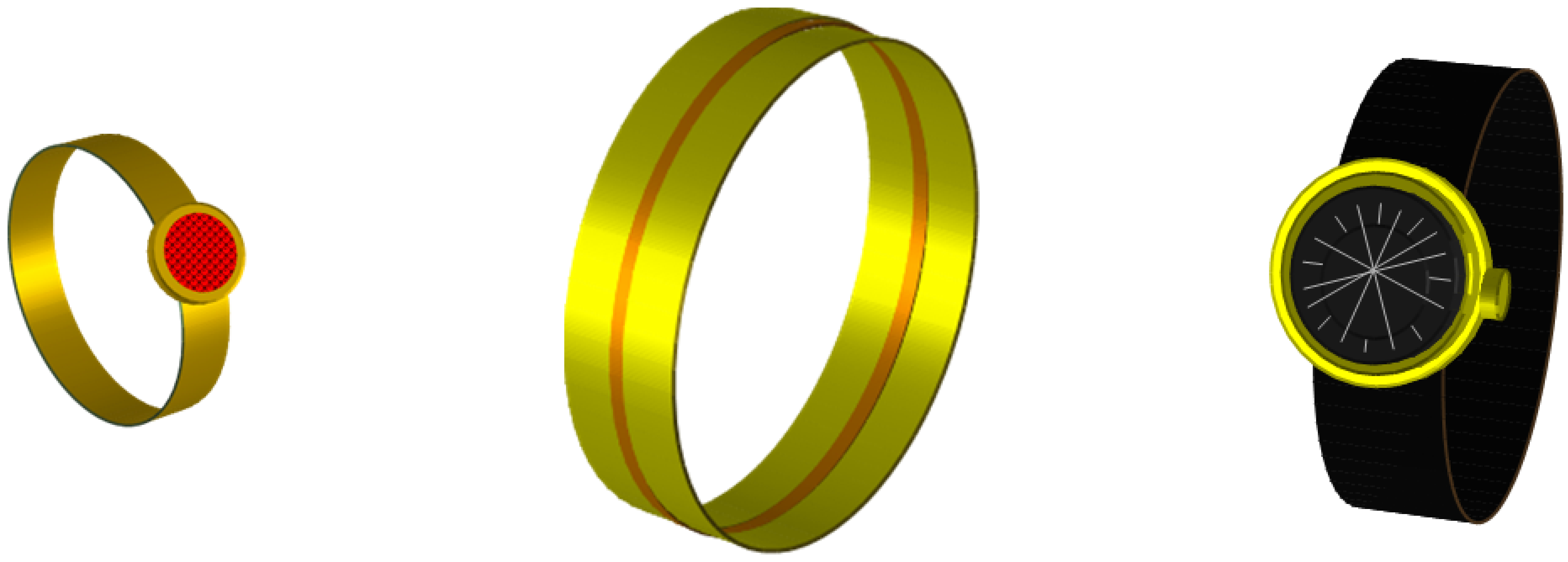
As a computer technician, it's always important to put safety as a priority when doing any kind of repair work. And if you put certain safety rules into practice, you'll save yourself a lot of time, money, and potential physical harm. So, for example, always be sure to turn off the power and unplug the power cable before doing any hardware repair work.



**Turn off and unplug the power cable is a good safety tip.**

This should be your first step before doing anything. This will protect you from being shocked and prevent damage to the hardware.

Another precaution you can take is to remove any hand jewelry that you might be wearing, such as rings, bracelets, or wrist watches.  These can potentially conduct electricity.

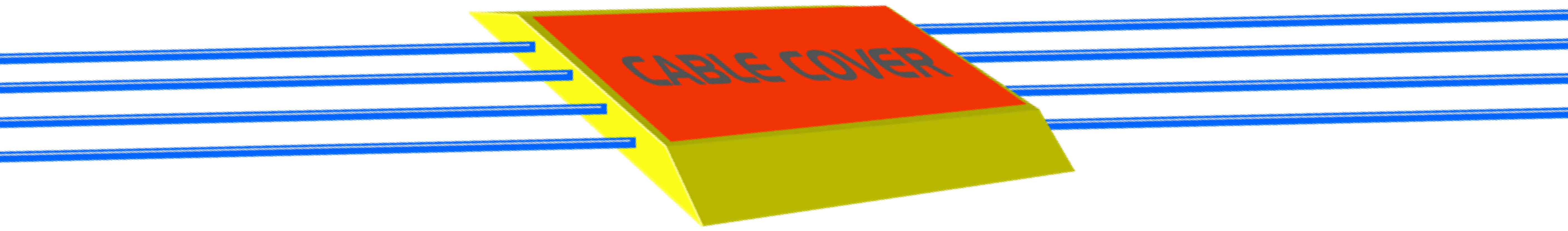


**Hand jewelry can conduct electricity.**

**Fire extinguisher**

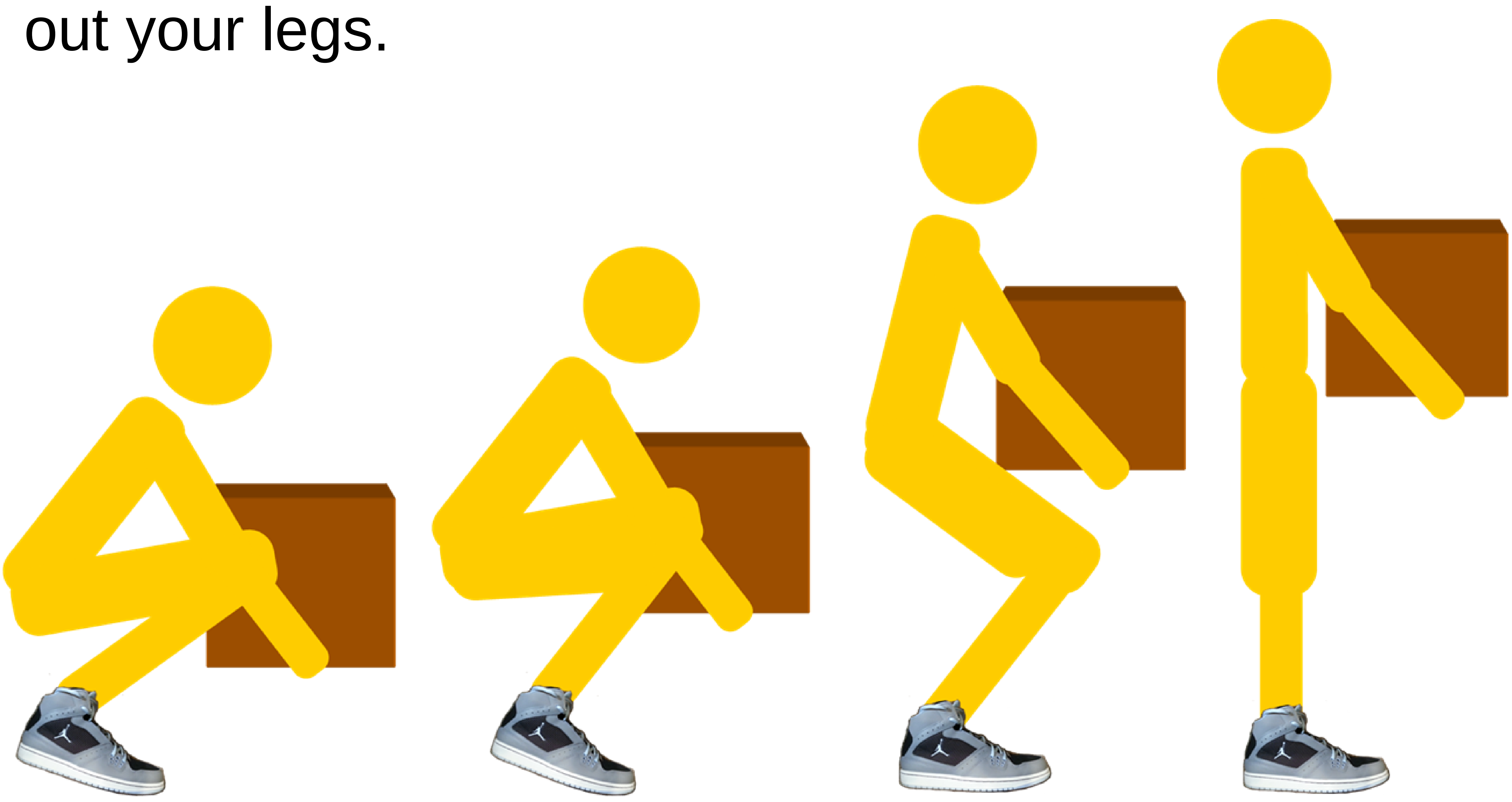
Another tip is to always take note where a **fire extinguisher** is located and how to use it properly in case a fire happens.  And in the computer field, a class C fire extinguisher is what you need because class C is made for electrical fires.  It uses a dry chemical powder to extinguish the flames.

Another safety tip is **cable management**. Maintaining a safe work environment is a major part of any job, and tripping hazards is a vital part of it. So if you have cables running across walkways, you could be at a high risk of a tripping accident.  So the quickest way to fix this is to simply relocate any cables that go across any walkway and move them somewhere else.  Or, if by some reason this can't be done, then you can always use something like a cable manager cover, which neatly organizes the cables in a way where you can't be tripped by them in high traffic walking areas.



**Cable manager cover**

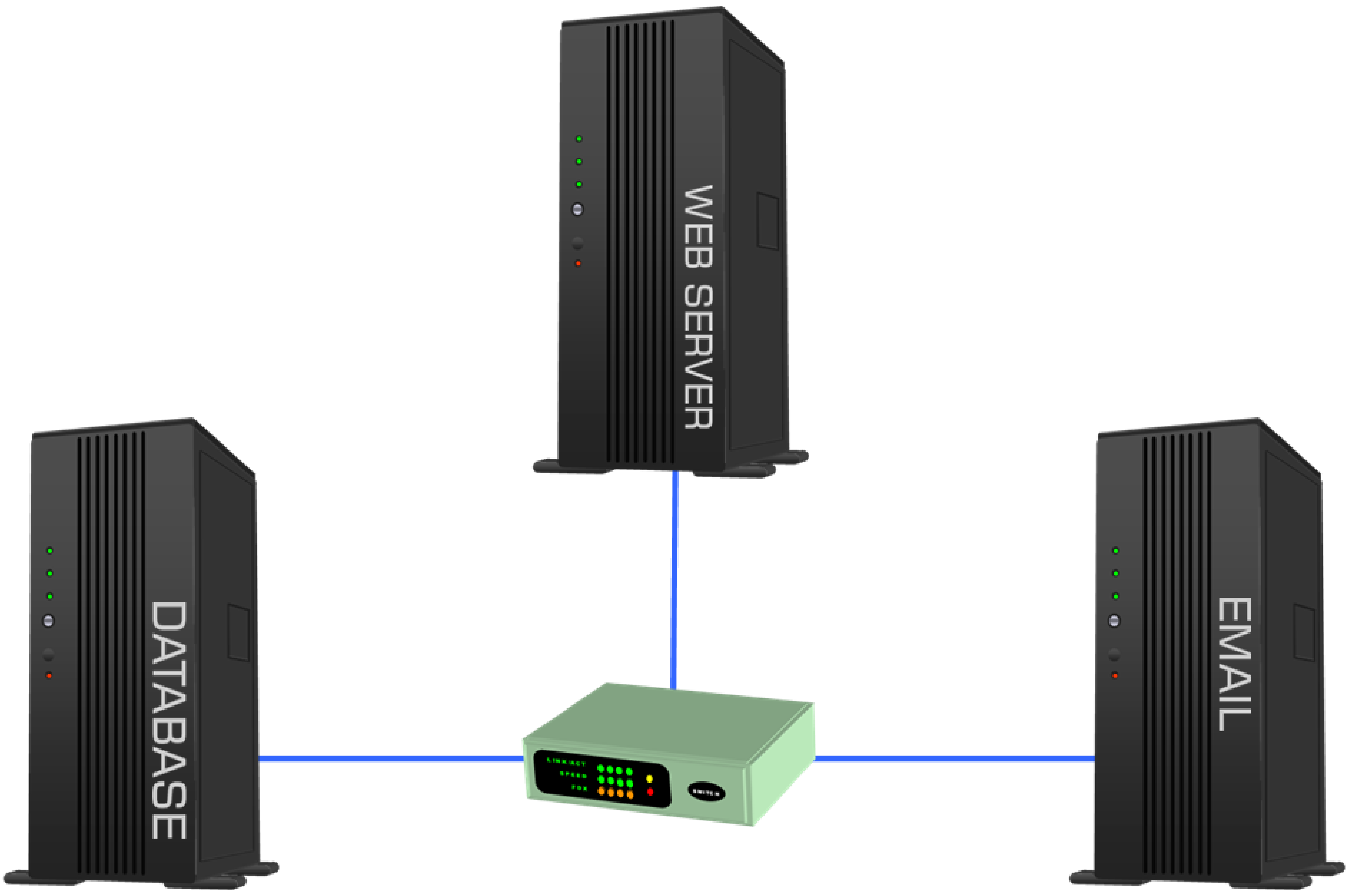
Another tip is **proper lifting**.  So if you have to lift a heavy object, it's important that you lift the object properly to avoid any injury.  You never use your back to lift a heavy object.  You always use your legs. So start out with your feet shoulder-width apart, squat down, maintain good posture by keeping your back straight at all times, and slowly lift by straightening out your legs.



**Proper lifting (those are actually my sneakers)**

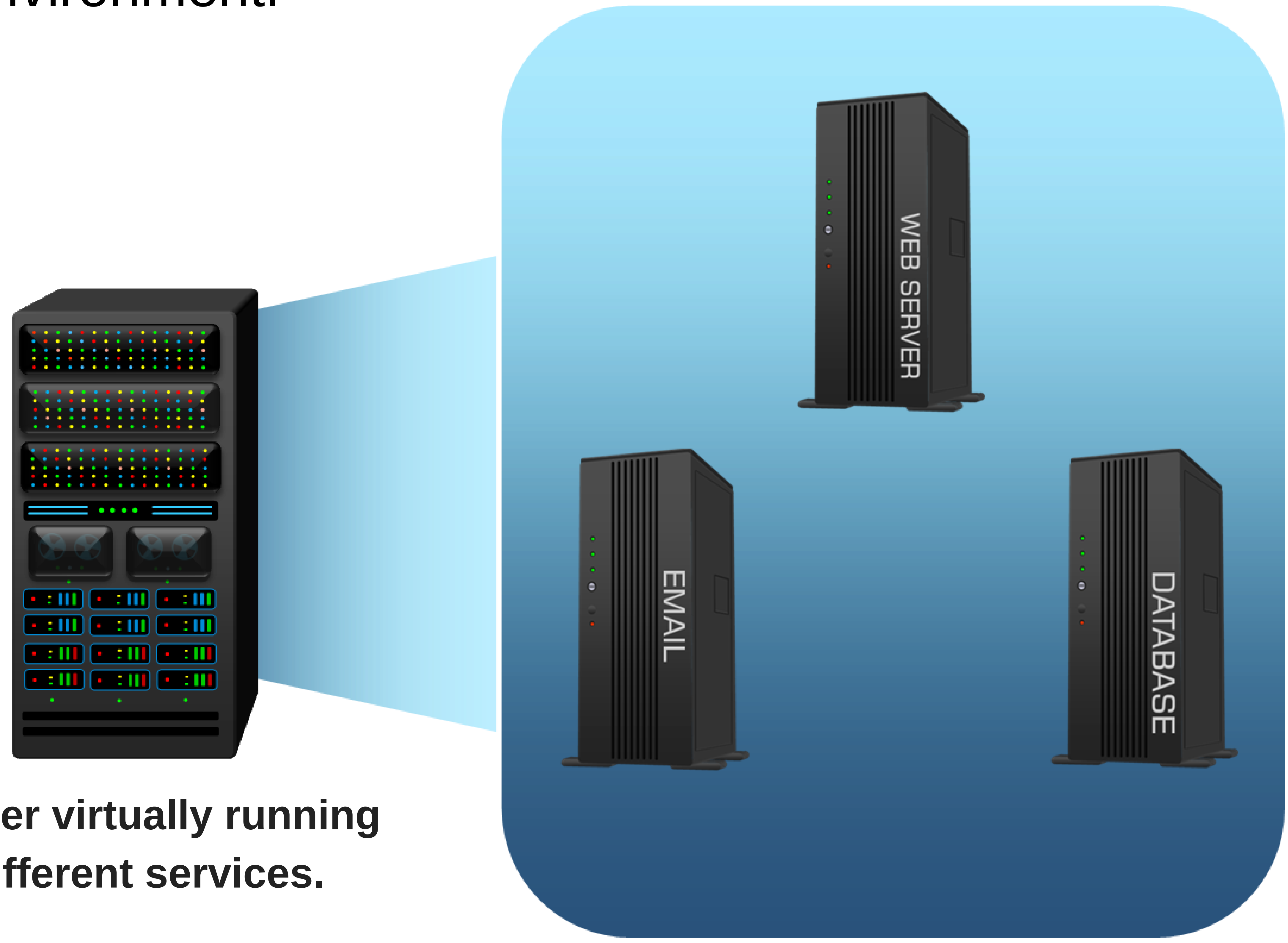
# Cloud & Virtualization

The traditional way a business operates is by using different machines or servers to run different services according to what the business needs.  For example, a business would use a server to run their database, another server will be used to run their website, and another server would be used to run their email service, and so on.  The servers also could be running different operating systems.  One could be running Linux, the other could be running Solaris, and the other one could be running Windows.  So needless to say, running a server environment like this can be expensive.  Not only do you have to pay for the server hardware, but you also have to pay for the floor space, the management, and the maintenance of the equipment.



**The traditional way a business operates.  Different servers doing a specific job.**

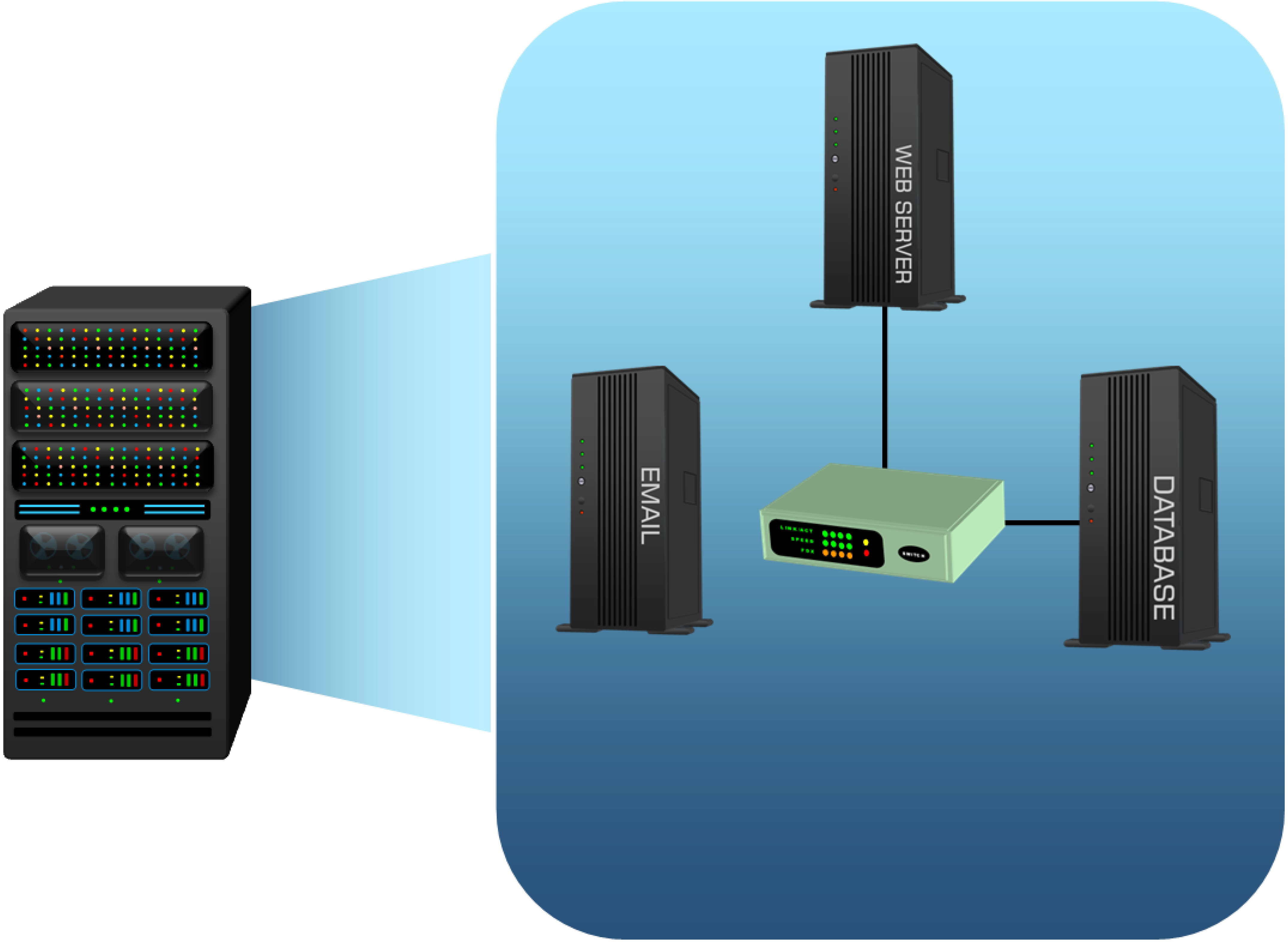
But there is a new trend that is happening in the world of I.T., and this is called a **virtualization**. Virtualization is basically consolidating all of these physical servers, with their different operating systems and applications, and running them on just one physical server in a virtual environment.



Server virtually running different services.

So now, this one server (above) is running all of the different applications, like databases, web services, and email, all running side-by-side on one machine. But not only the applications, but also running the different operating systems side-by-side. So users that interact with a virtual server would interact the same way as if they were still on multiple physical servers. They won't be able to tell the difference. So needless to say, virtualization saves money. Not only does it save money on hardware, but also on storage space, maintenance, and management.

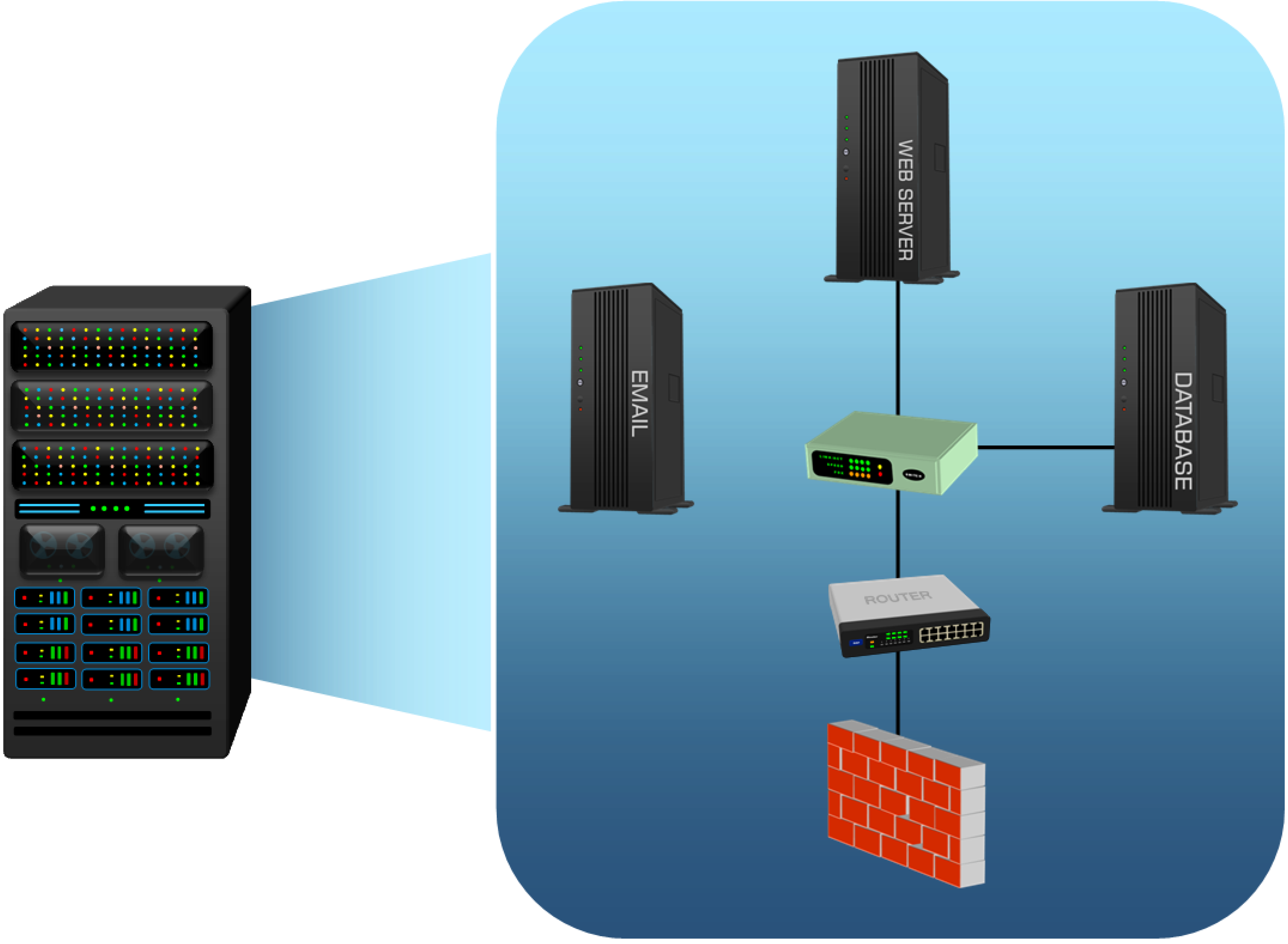
In addition to virtual servers, there are other virtual devices such as **virtual switches**. A virtual switch is not a physical switch, but it's a software switch that's created in a virtual environment. So for example, if you wanted your virtual database server to be able to network and communicate with your virtual web server, you can just add a virtual switch to do that. Then once the virtual switch is added, those two virtual servers can now communicate with each other.



**Virtual switch added**

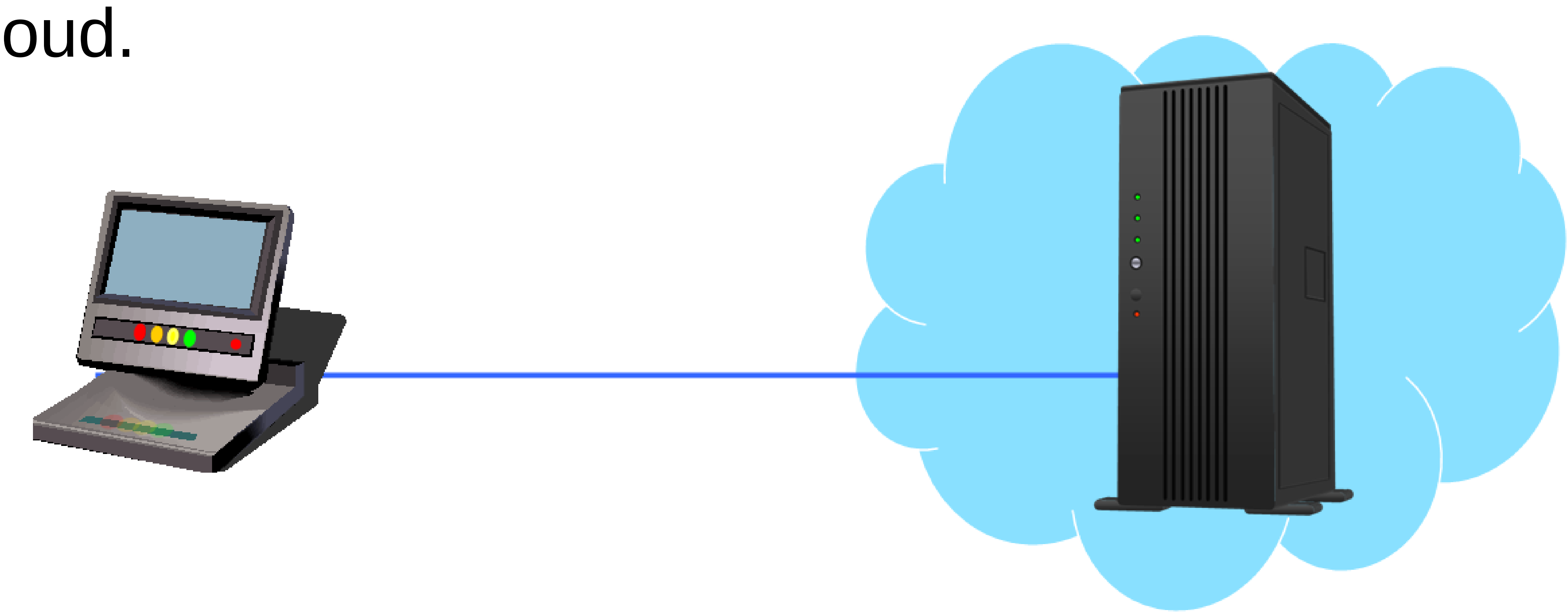
There is also a **virtual router**. A virtual router performs just like a physical router. It can route data packets between your virtual servers and the internet, according to what the business needs are.

Finally, there is a **virtual firewall**, which is another virtual device that can filter network traffic.  A virtual firewall monitors traffic for your virtual servers just like a physical firewall does.



**Virtual router and virtual firewall added.**

The term **cloud computing** refers to data and applications being stored and run on remote servers rather than being on your local computer.  Then this data and the applications, which are on these remote servers, are accessed and run via the internet.  So the workload is no longer on your local computer, it's in the cloud.



So back in the old days before cloud computing, and as an example, we'll use email. So at your home or office, if you wanted to use email, you would have your own physical email server. So you would have a server, an operating system, and email software like Microsoft Exchange. Then, you would be able to use email.

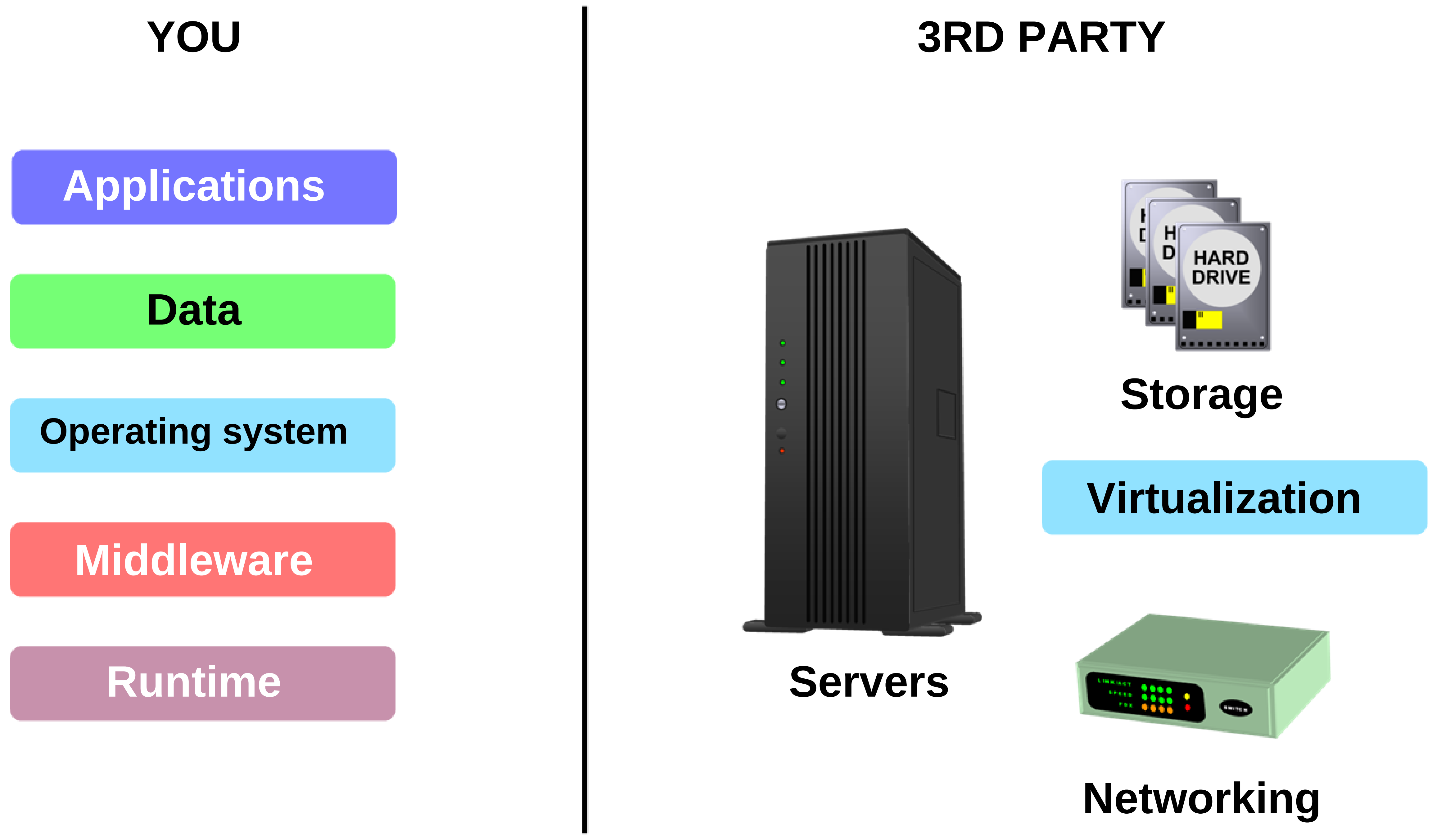
EMAIL
SOFTWARE
EMAIL
OPERATING SYSTEM
SOFTWARE

But the problem is, that if anything goes wrong, such as a hardware failure, or a software problem, or if the operating system crashed, well then you would be responsible for fixing the problem. Not to mention any maintenance that is needed to keep the server running. However, you do have the option of eliminating all the hassle and upkeep of your own email server and have a company host all your email on their servers in the cloud for you. For example, Hotmail and Gmail. But email is just one example of cloud computing. There are also other services, such as productivity software, web servers, and databases.

There are three different types of cloud computing. There's **infrastructure as a service** or **IAAS**.

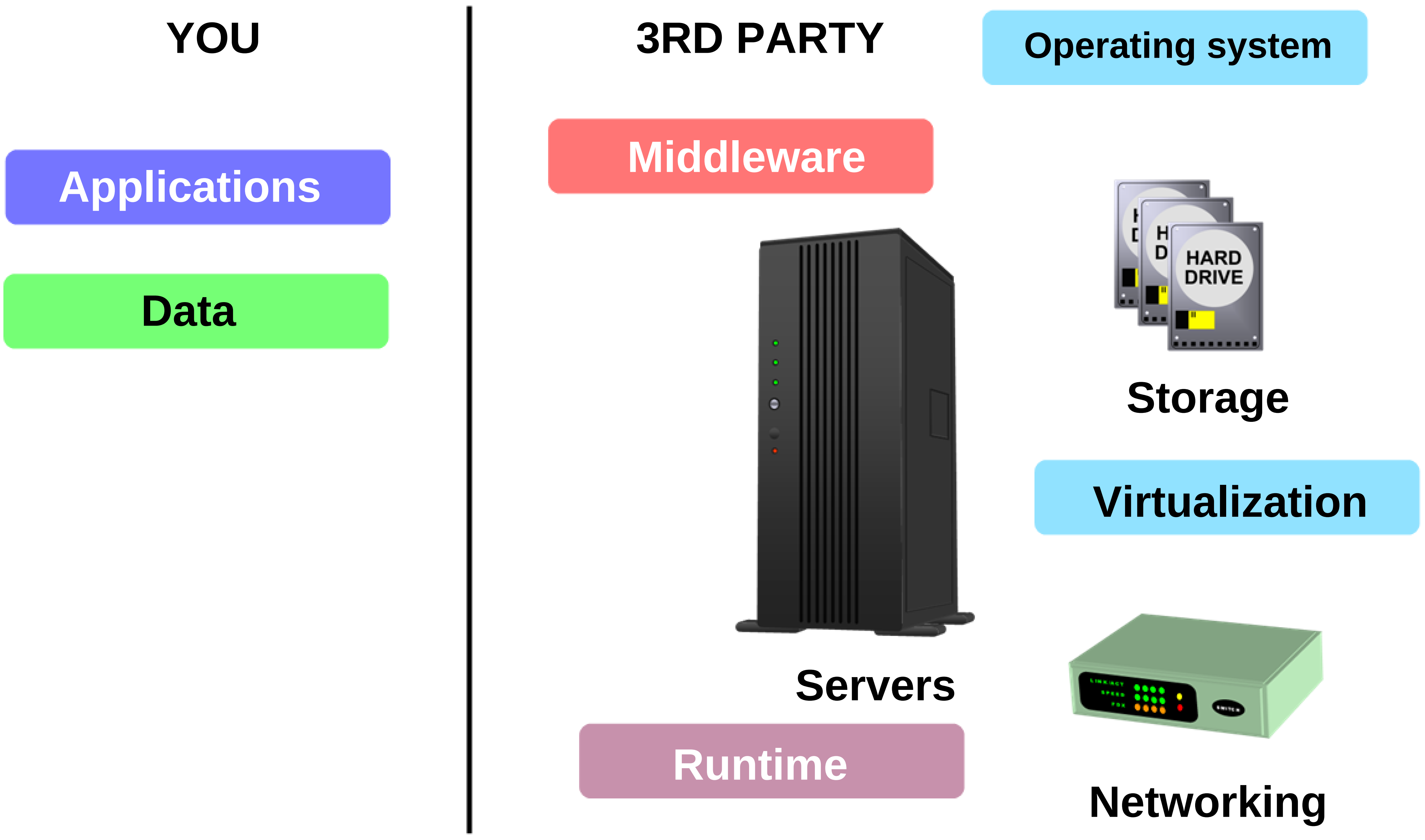
**Platform as a service** or **PAAS**.  And **software as a service** or **SAAS**.  These three vary in control and flexibility.  So it's up to the user as to decide what suits their needs.

The first one is infrastructure as a service.  This type is basically when you're going to let the third party vendor manage a portion of your business, which is going to be the hardware portion.  The third party vendor will manage the servers, storage, virtualization, and the networking portion.  You, on the other hand, will still have control over the software portion, such as the applications, data, operating system, middleware, and runtime.  A good example of IAAS would be a web service company like Amazon web services.



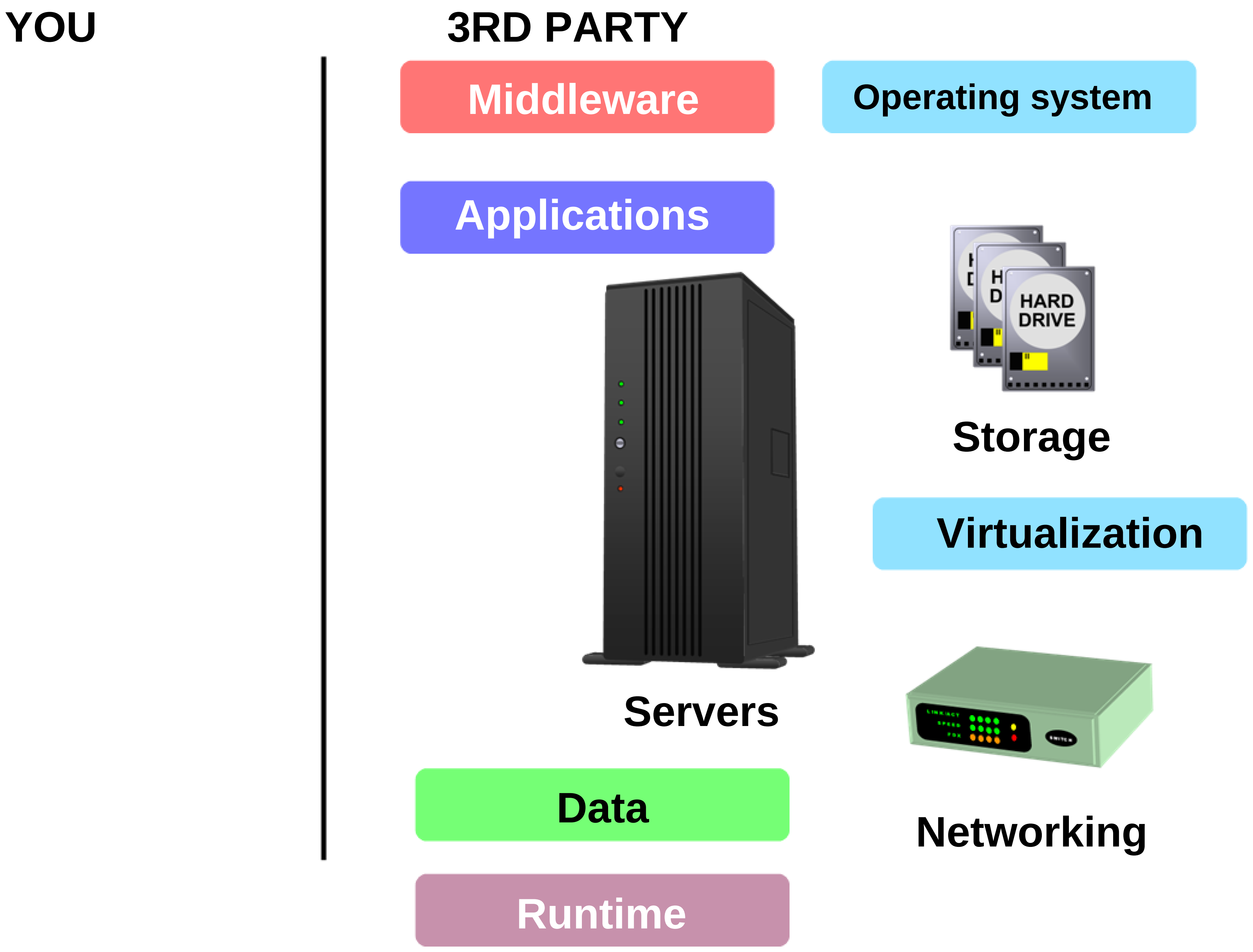
**IAAS**

The next one is called platform as a service.  PAAS, like IAAS, allows the third party to manage a portion of your business.  But the third party has more control.  In a PAAS, the third party vendor not only manages the hardware, such as servers, storage, and networking. But they also manage the operating system, middleware, and runtime.  You are only responsible for the applications and the data.  A good example of a PAAS would be Microsoft Azure which is a cloud computing platform from Microsoft.



**PAAS**

Finally, there's software as a service or SAAS.  This type is probably the most common cloud service by far. All the applications are hosted by a third party vendor on the internet.  There is no software to install on your computer, and no hardware to manage.  You just simply access and run the application from your computer when you connect to the cloud service via the internet. So the third party vendor manages all the hardware, software, networking, operating system, and storage. And Google apps is a great example of SAAS.



SAAS

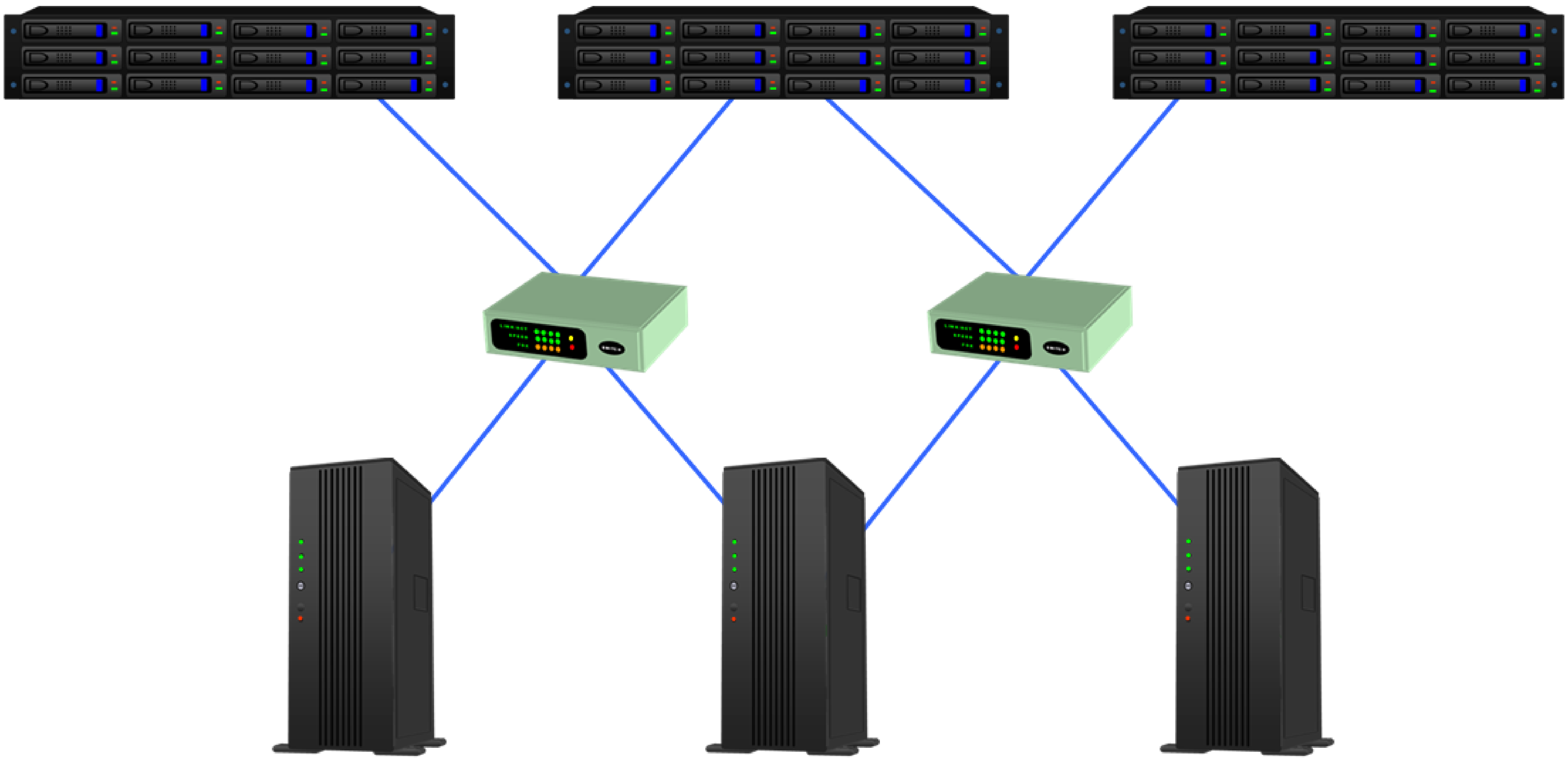
# NAS & SAN Storage

If you wanted to store data in a centralized location where it can be accessed from all of your other devices on your network, you can do this by using a **network attached storage** device or **NAS**. A NAS is a storage

**NAS (network attached storage)**

device that is used strictly for storing data.  It doesn't do anything else besides storing data.  Typically a NAS will have multiple hard drives in a RAID configuration for redundancy, and a network interface card that directly attaches to a switch or router so that the data can be accessed over a network.  Then once it's on the network it can be accessed from other devices such as desktops, laptops, and servers, through a shared folder.

A **SAN** or **storage area network** is a special high-speed network that stores and provides access to large amounts of data.  This network consists of multiple disk arrays and servers that access this data as if it was a local hard drive.  Because that's how operating systems recognize a SAN.  It's recognized as a local attached hard drive rather than a shared drive, like a NAS. SANs are independent of servers.  They are not limited or owned by a single server.  In fact, multiple servers are attached to a SAN.  So all the data is available to all the servers simultaneously.

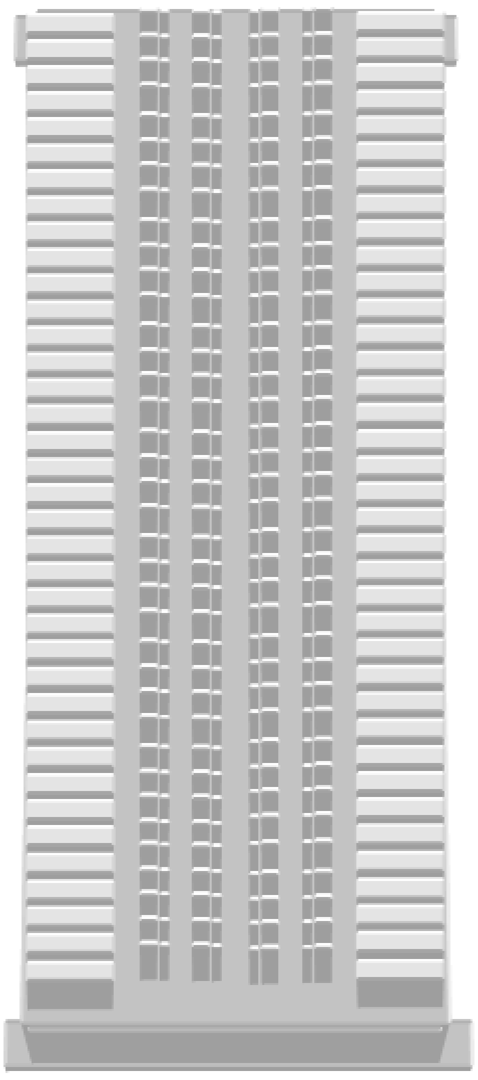


**SAN (storage area network)**

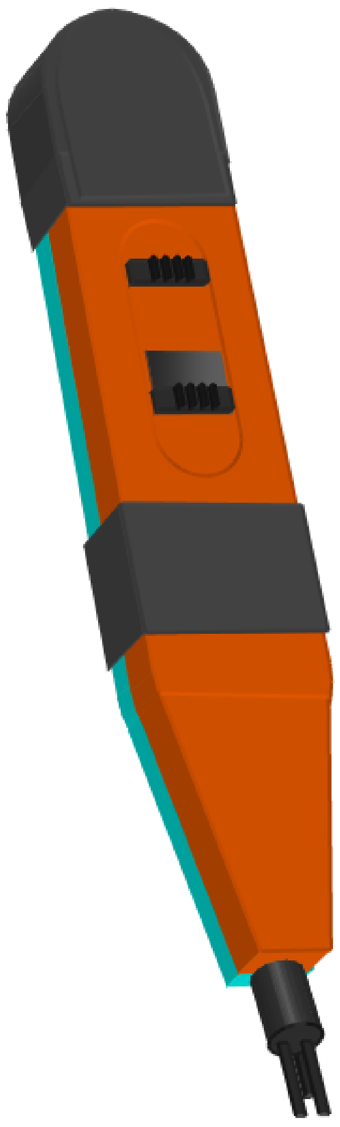
SANs are also easily expandable and they are very redundant because all the data is shared among several disk arrays.  So if a disk array fails, then the data is not lost because the data will be stored in multiple areas.   As stated before, a SAN is a high-speed network, and that's because in a SAN all the devices are interconnected using **Fibre Channel**, which is a standard for SAN that has network speeds starting at over 2,000 Mbit/s.  As an alternative to using Fibre Channel, there is **iSCSI**.  iSCSI stands for **internet small computer system interface** which is a data storage protocol that transports SCSI requests over standard TCP/IP.

# Wiring Distribution

A **66 block** is a punch down block where wires are inserted. The wires are inserted using a punch down tool and then they are punched down into the block.  66 blocks are considered outdated and they are not used that much anymore.



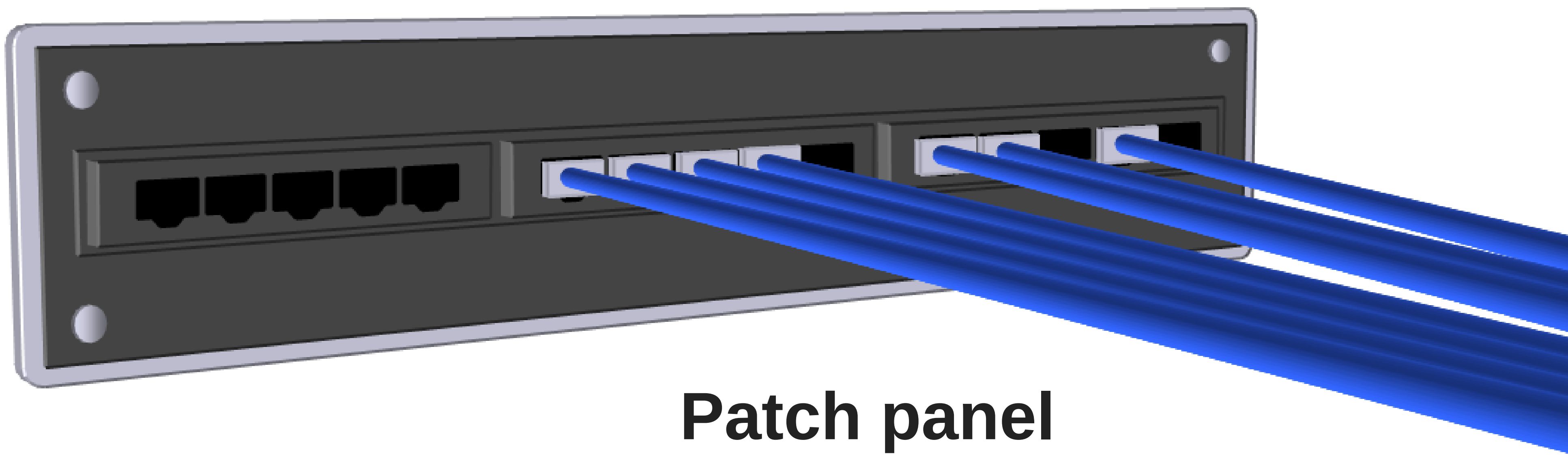
**66 block**



**Punch down tool**

A modern-day punch down block is called a **110 block**.  A 110 block is better than a 66 block because it can support higher frequencies and use less space. It also meets the standard that is needed for category 5 UTP cable.

A **patch panel** is a panel that has multiple cable connections that connect incoming and outgoing patch cables in a local area network.  It allows network administrators the convenience of arranging or rearranging circuits if necessary.  For example, here we have a patch panel that has several UTP patch cables attached.



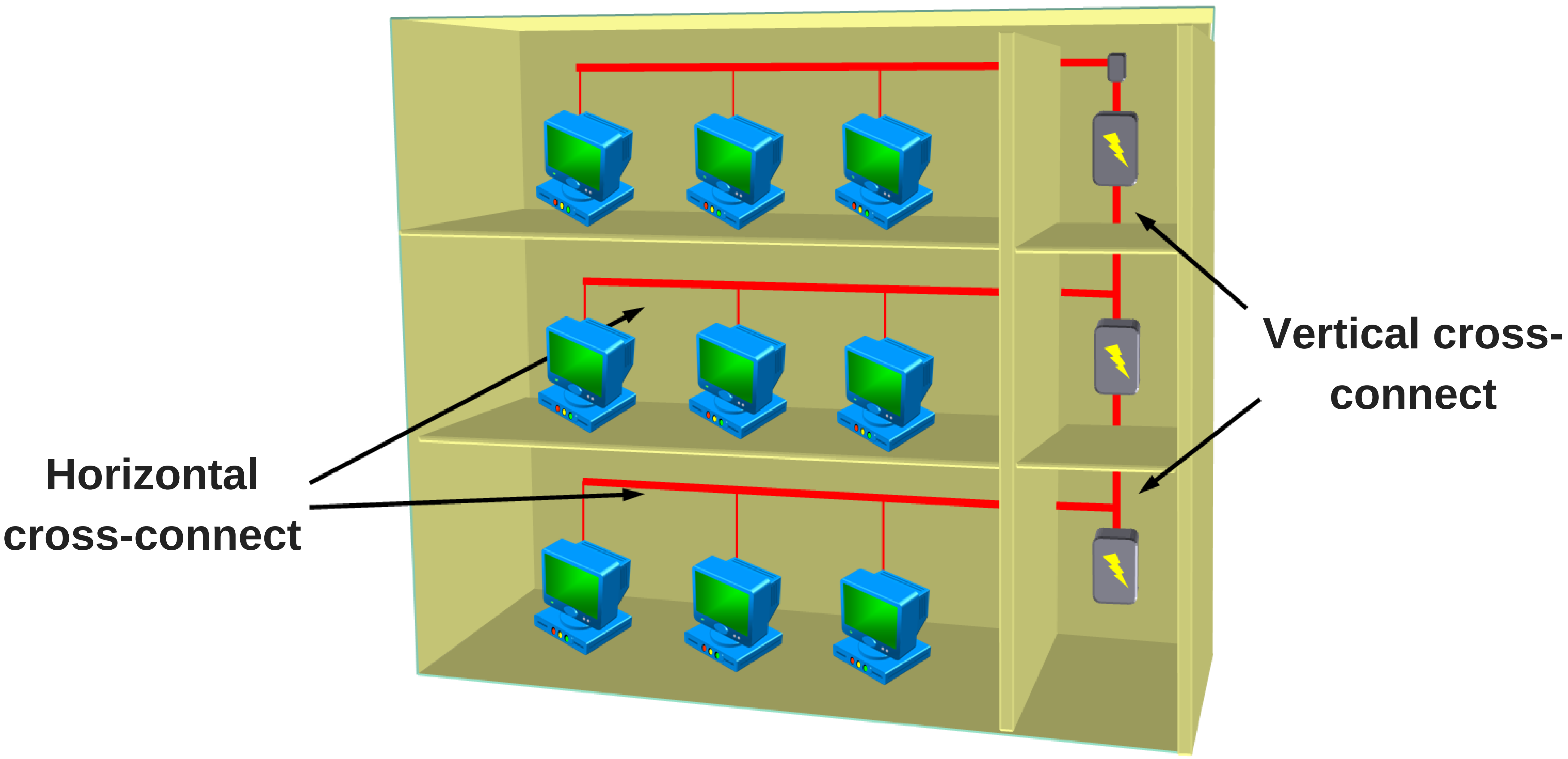
**Patch panel**

The **demarc** or demarcation is the point where the customer's network equipment meets with the service providers network equipment.  It defines where the service provider's responsibility for their equipment ends and where the customer's responsibility for their equipment begins.  If the demarc needs to be extended further inside the customer's building, then this is known as a **demarc extension**.

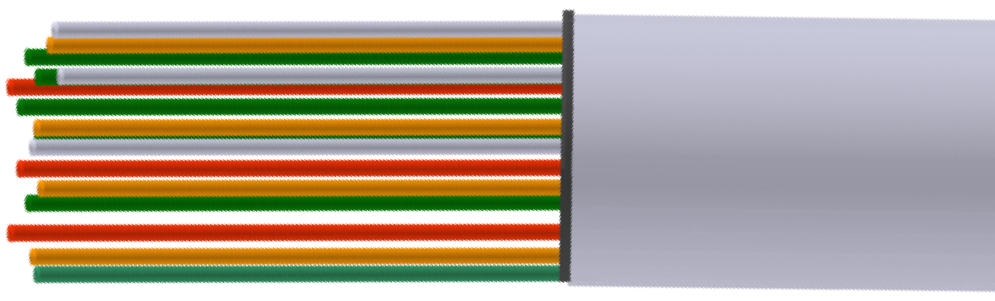
A **smart jack** is also known as a network interface device or NID.  It's often located at the demarcation point.  A smart jack's job is to terminate the T carrier's service wires at the customer's building.  In addition, smart jacks are used for monitoring a network for errors and connectivity issues.  They also have LEDs that indicate errors to a network technician.

**Smart jack**
**Network interface device (NID)**

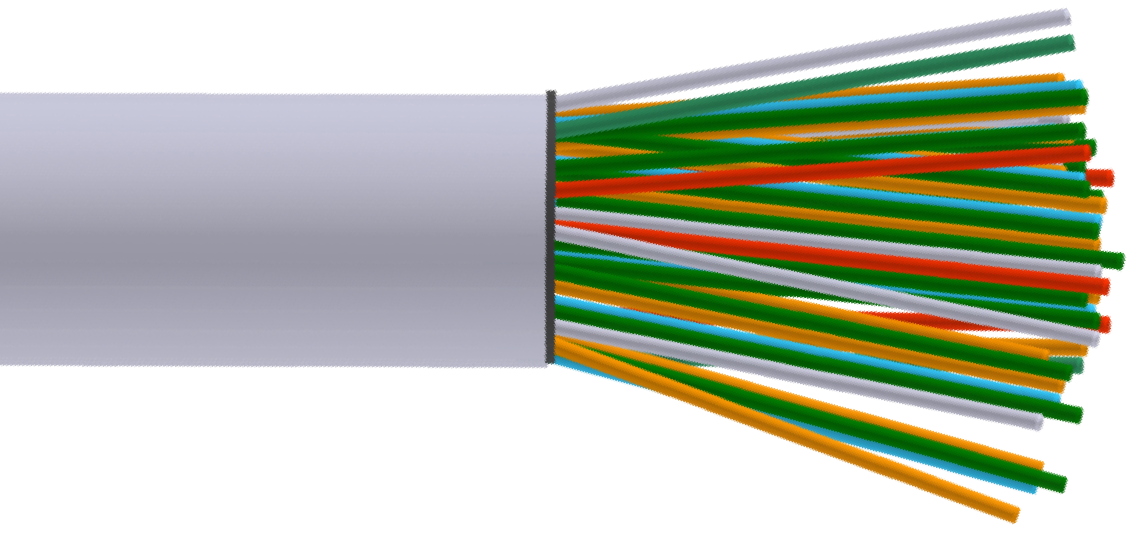
The term **cross-connect** refers to points in a building where cables and wires connect together.  A **vertical cross-connect** is the main backbone that runs vertically and spans between floors.  A **horizontal cross-connect** is where cables are run horizontally from cable closets to wall outlets.



**25 pair** is a cable that has 25 pairs of smaller wires inside. The wires are color-coded to identify the individual conductors.  Each pair of wires is uniquely colored giving the cable 25 different 2-color combinations.



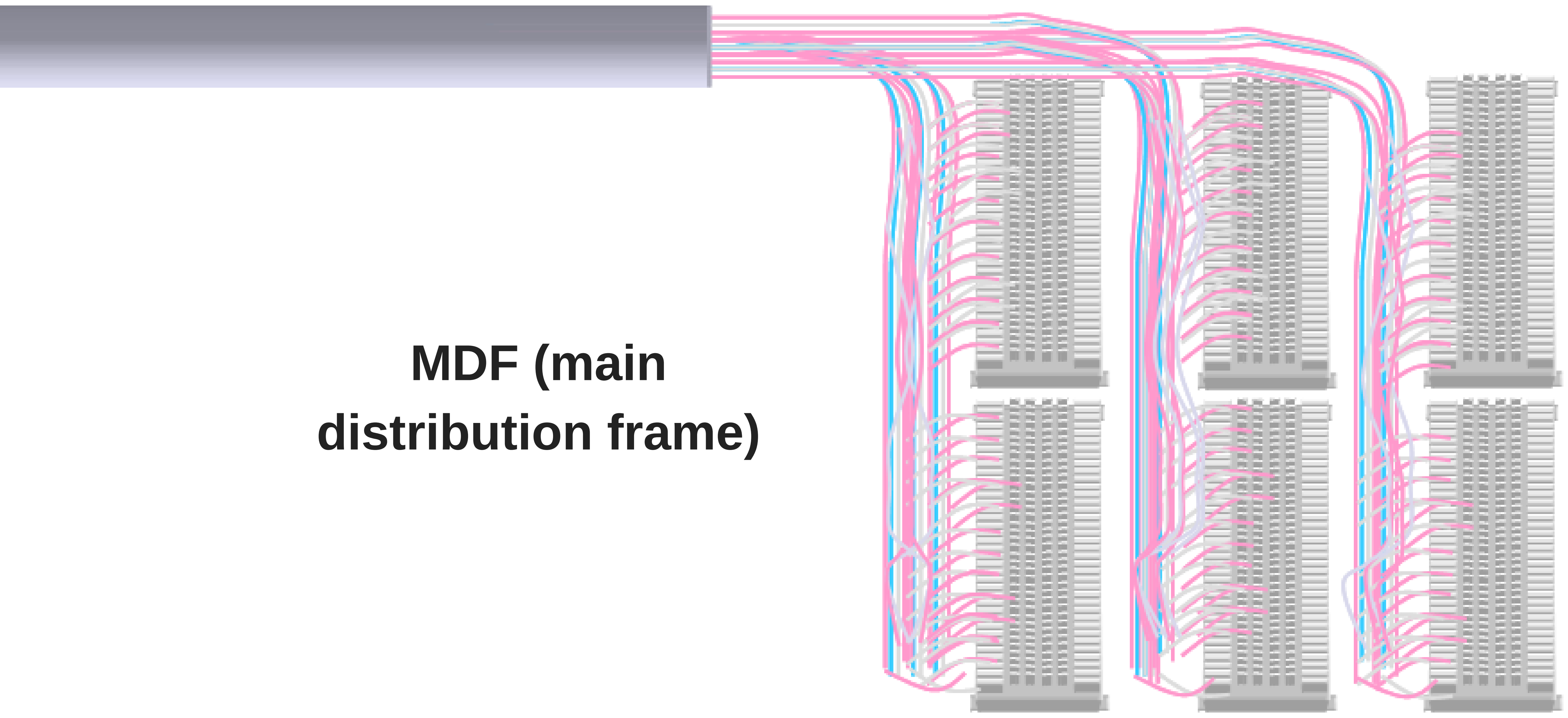
25 pair



100 pair

**100 pair** has 100 pairs of wires inside.  These are used for larger industrial jobs compared to 25 pair.  Each pair of wires is also uniquely colored to give 100 different 2-color combinations.

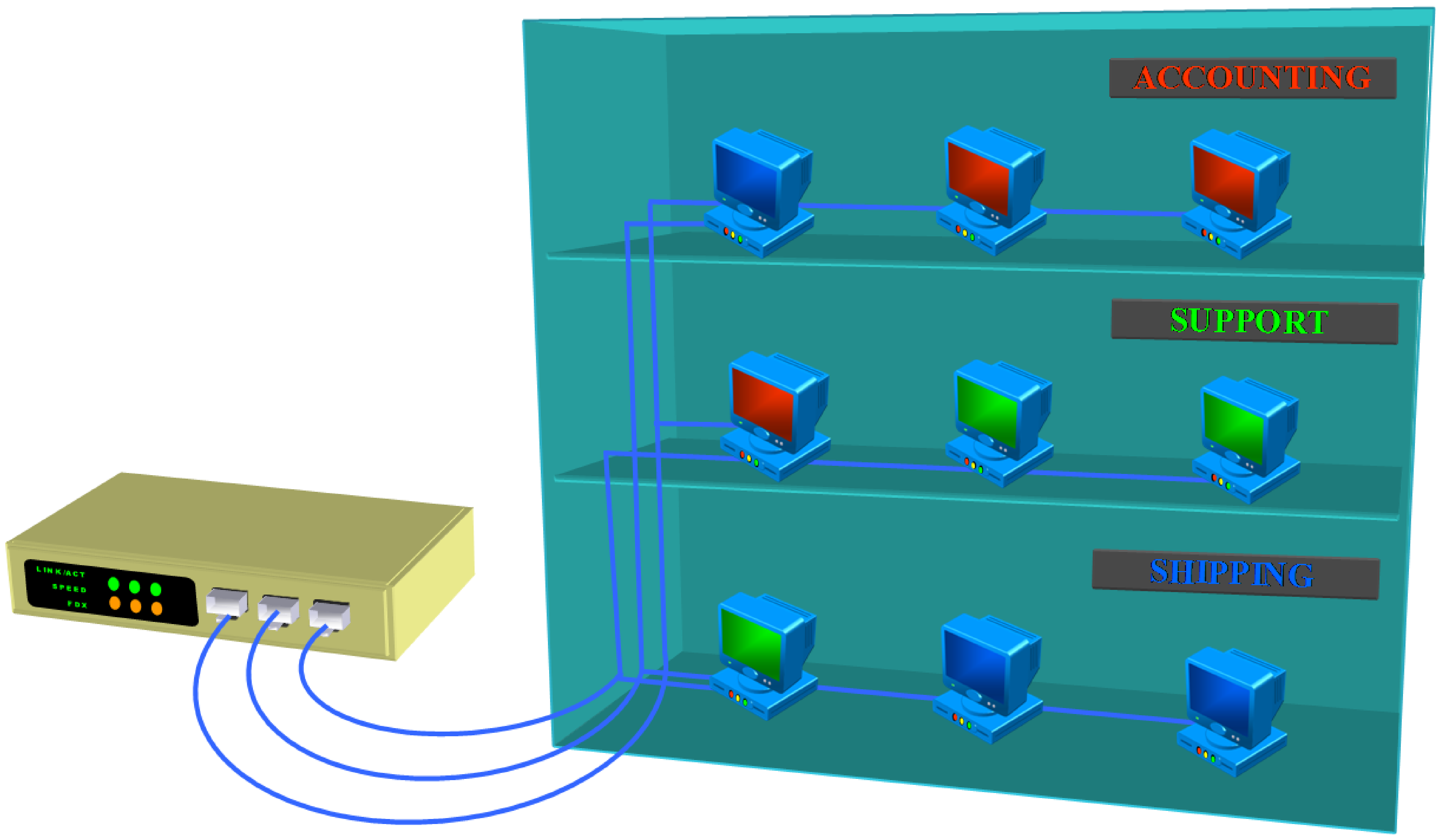
**MDF** stands for **main distribution frame**.  This is the main wiring frame that is used as a distributing point for all the wiring in a building.  All of the internal lines in a building connect to the MDF and from there the external lines connect also, therefore, completing the circuit.



There is also the **IDF** or **intermediate distribution frame**.  These are smaller distribution frames that are located in various locations in a building.  These provide better flexibility to distribute wires to the main distribution frame.

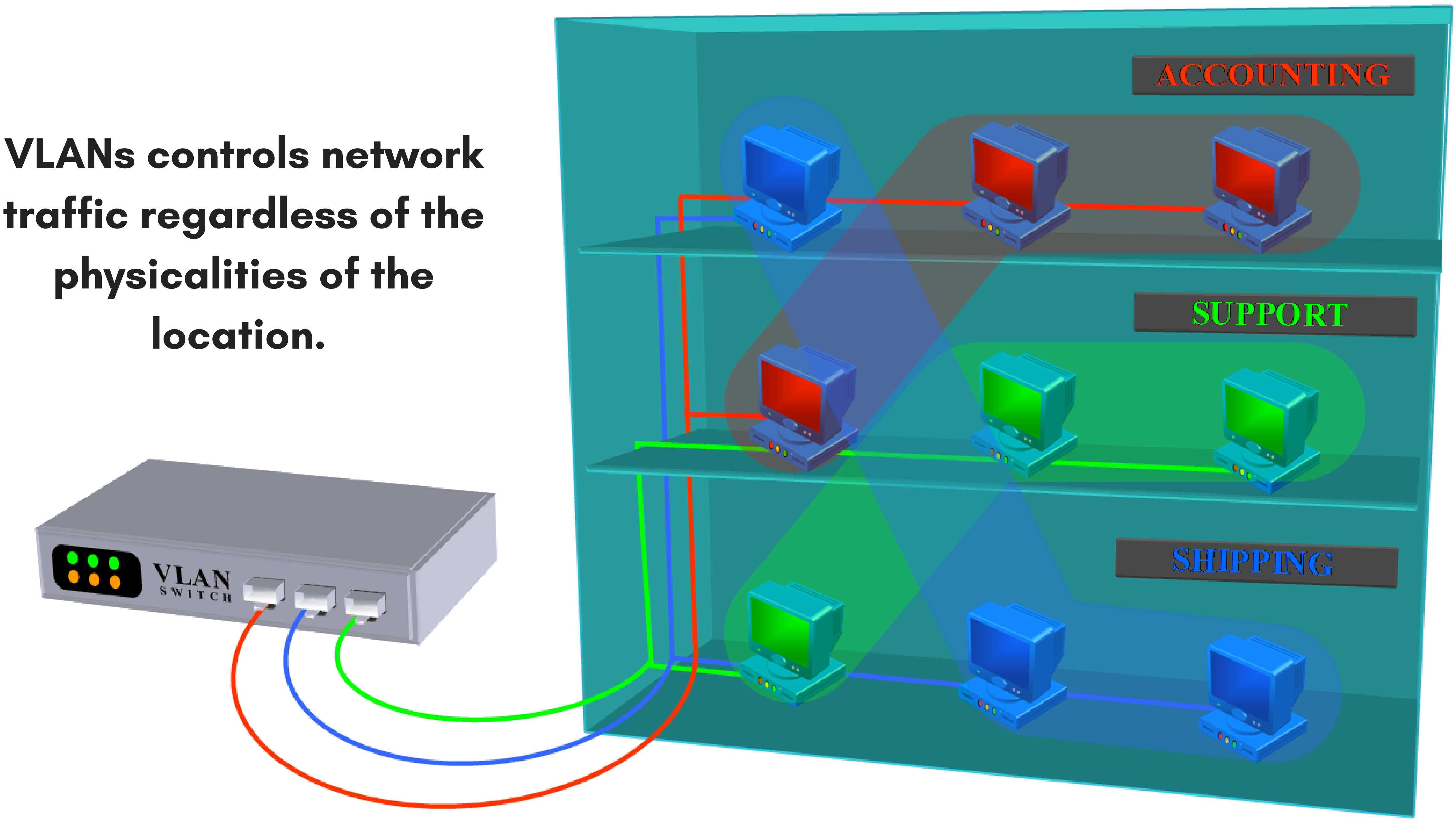
# VLAN,
# Intranet & Extranet

**VLAN** stands for **virtual local area network**. A VLAN is a logical area network that can control network traffic regardless of the physicalities of their location. So for example, let's say you have a three-story office building and you have different departments mixed in with others on the same floor (see below).



Now, suppose you wanted to separate the network broadcast activity between the departments from each other, so that the accounting department does not see any traffic from support, support doesn't see any traffic from accounting, and so forth.

Now, one way to solve this is to physically move the computers to their proper floor and put them on the same subnet with a router.  But there is an easier way to accomplish this, and that way is to use a VLAN switch.  By installing a VLAN switch you can logically create several virtual networks to separate network broadcast traffic.  So now, the three departments don't see any traffic created by the other departments (see below).  They only see their own.  There's also a couple of ways that VLANs can be created.  They can be created by ports on a VLAN switch or they can be created by using the MAC addresses of the computers.

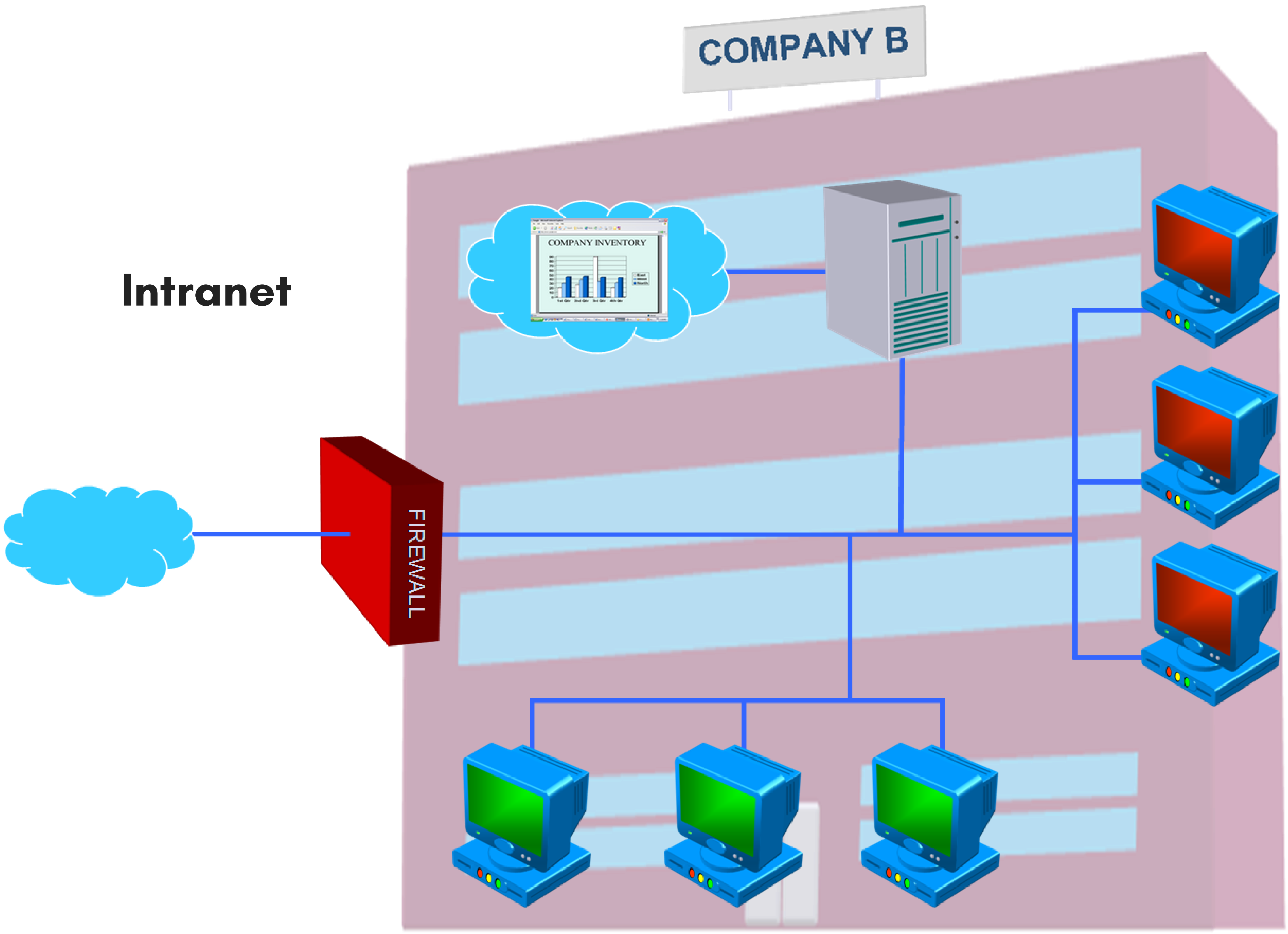


**VLANs controls network traffic regardless of the physicalities of the location.**

**A VLAN switch separating the traffic from different departments.**

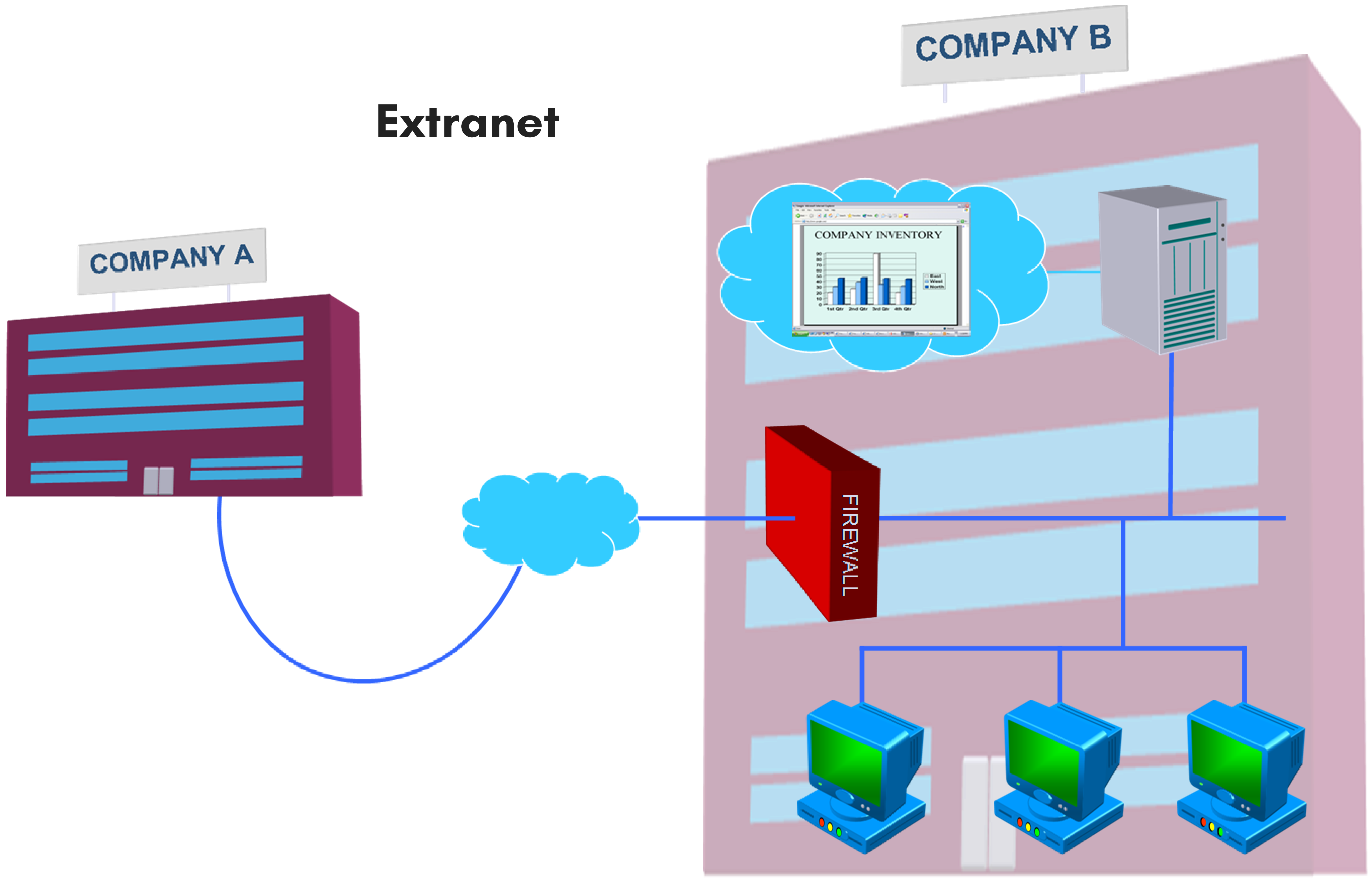
An **intranet** is a private network that belongs to an organization.  This is usually an internal website that only the employees of that organization can access.

The website usually contains information about the company, for example, company sales, inventory, or history.  And this website is also behind a firewall.  So no one outside the company can access it.



Now, an **extranet** is similar to an intranet because they are both private networks within an organization.  But an extranet is different from an intranet because an extranet is accessible from outside the organization on a restricted basis.  So, for example, below we have two companies.  Company B contains a private network that contains a website with their company's information. Now suppose company A is a business partner with them and they need to access certain information.  So what happens, is that Company B will grant company A access to their website to effectively do business.

## Extranet



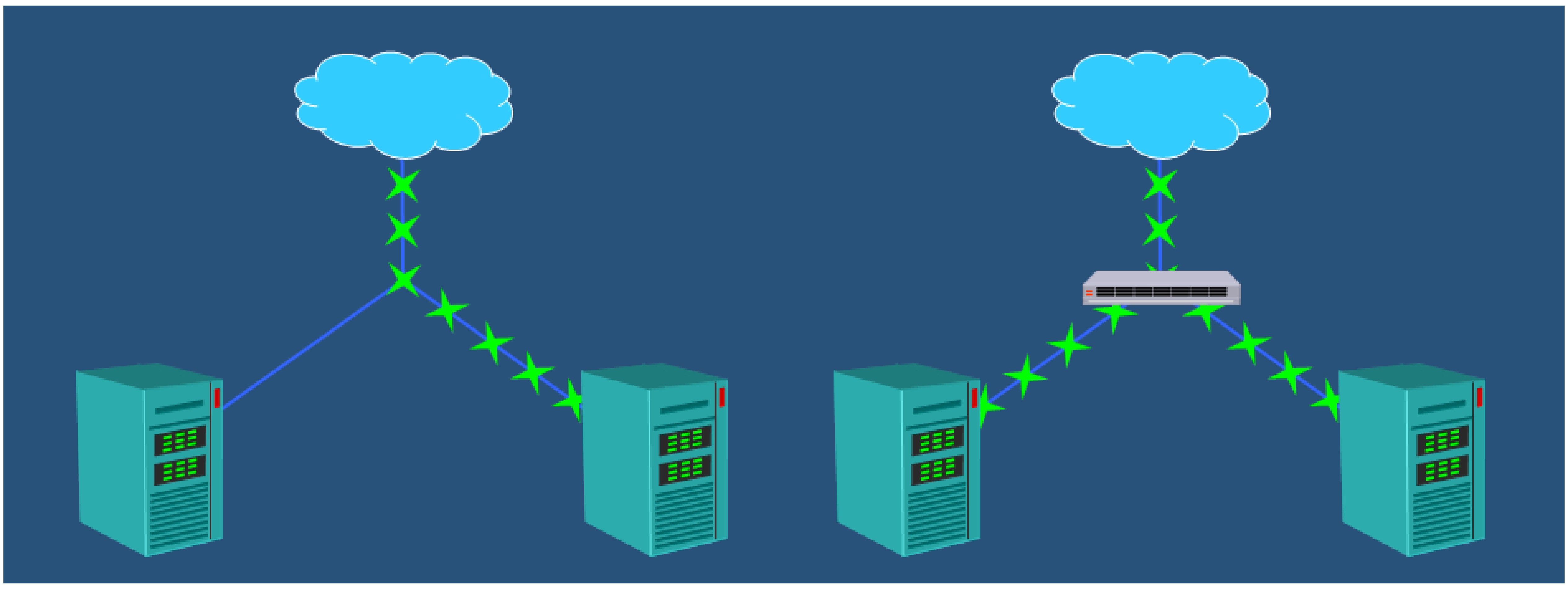
# Optimization & Fault Tolerance

A **bandwidth shaper** is used to control network traffic. It can be used to set upload and download limits on less important data such as recreation.  You can also prioritize important data, like business needs, and make sure that it has the highest upload and download limits.

The term **traffic shaping** is similar to what a bandwidth shaper does.  It prioritizes applications and guarantees bandwidth for more important services.

**QoS** stands for **quality of service**.  In computer networking, this is a term that is used to provide a guarantee of data delivery within a certain period of time.

A **load balancer** is a piece of hardware or software that is used to evenly distribute data activity across a network so that no single server or computer becomes overwhelmed with the workload.

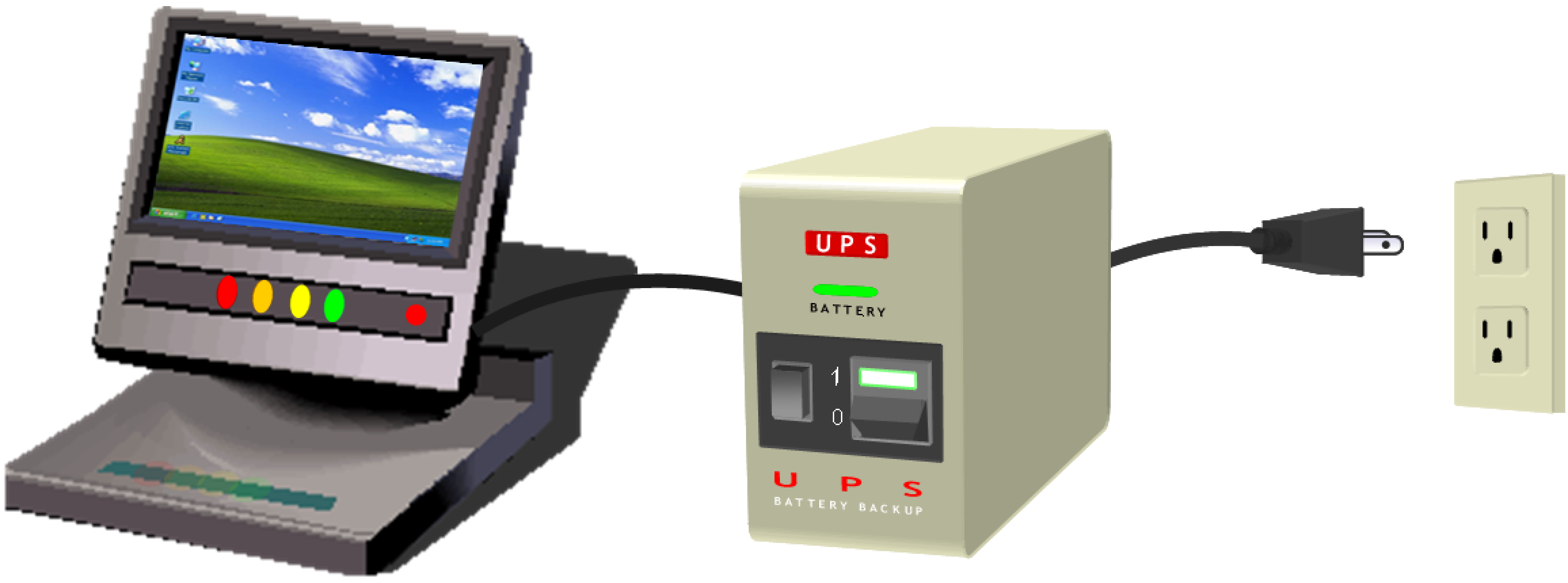


**Without a load balancer**

**With a load balancer**

**High availability** is a term that is used to guarantee a period of uptime continuous operation.

In order to keep a network in constant operation, you need to make sure that it always has power. But unfortunately, in our world, this doesn't always happen. Power outages can happen for several reasons, such as storms and blackouts. So in order to prevent a disruption in network operation from a loss of power, you need to use as **UPS**. UPS stands for **uninterrupted power supply.** A UPS is a battery backup that supplies power to your equipment if a power outage were to happen.

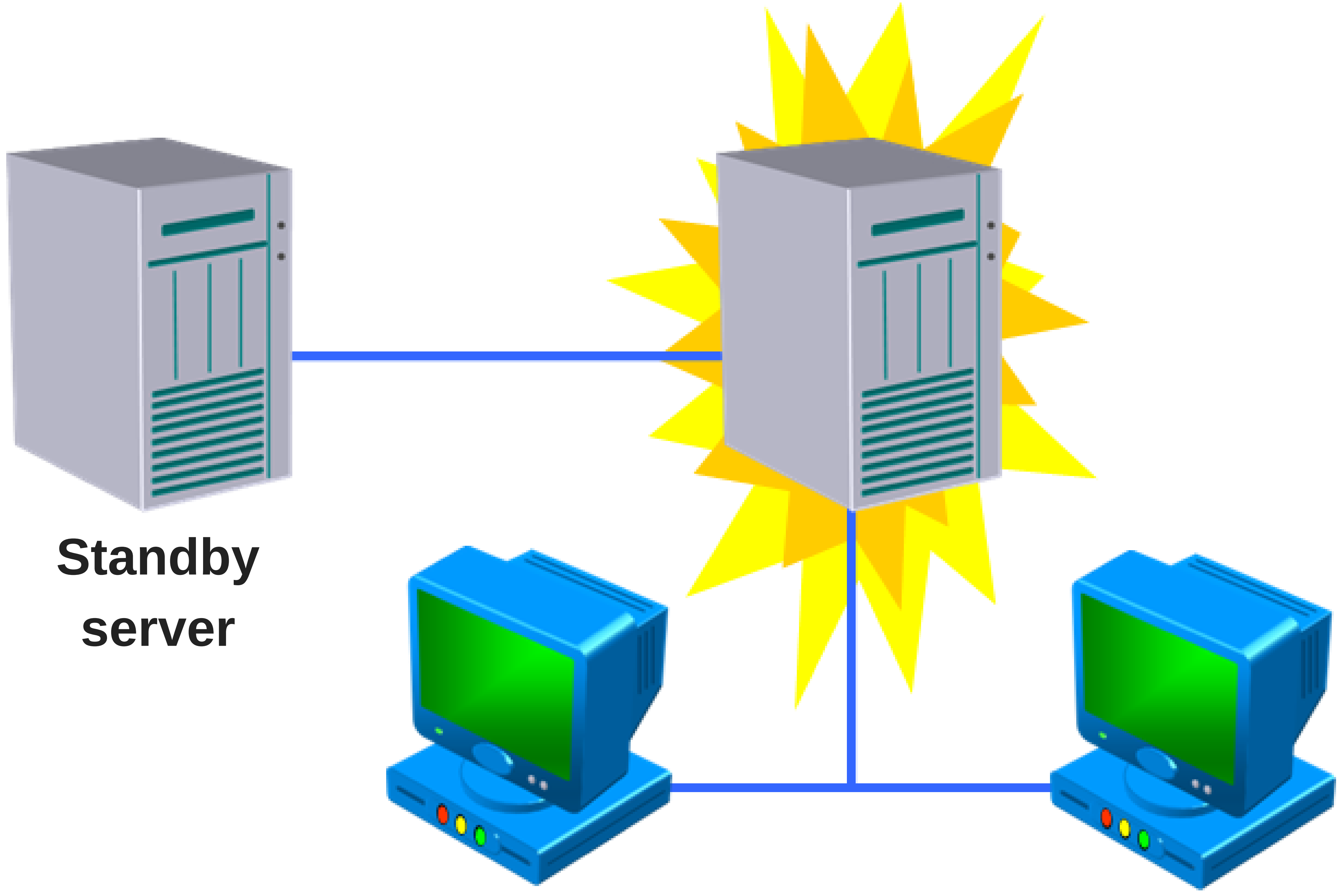


**UPS**

So in the example above, if we were to disconnect the AC power from this computer, the computer will remain on because it's connected to a UPS. The computer is now running on battery power from the UPS. In addition to supplying backup power, a UPS also protects against surges and spikes.

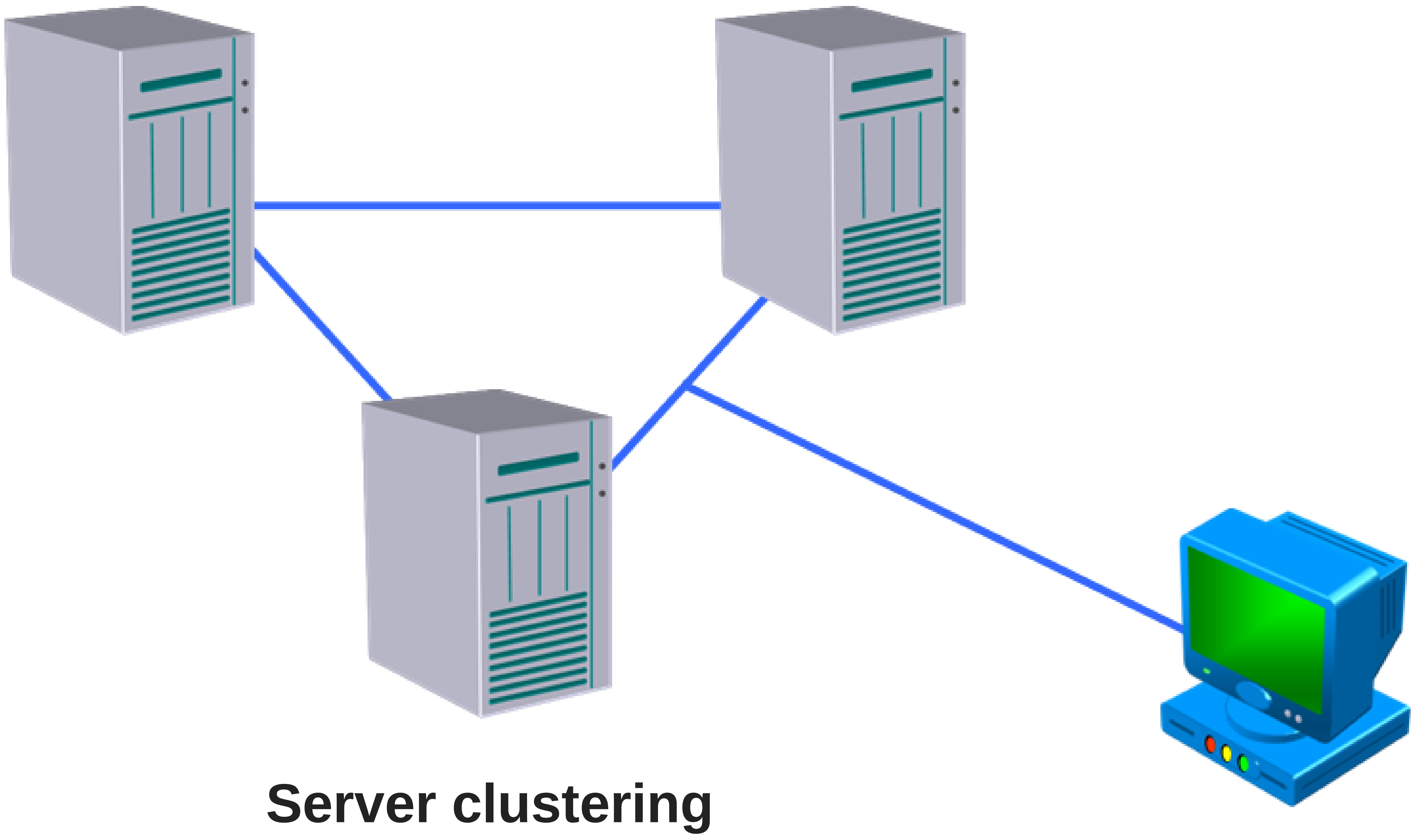
**Link redundancy** is having the ability to have a continuous connection to the network in the event of a failure.  So for example, if you are using a broadband connection, you can have an ISDN line as a backup if the broadband line were to fail.  You can also have a secondary network card.  One network card would be the primary, and the other would be a secondary.  So if the primary card were to fail, the secondary card would automatically kick in so you would still have a continuous connection.

There's also **backup services**.  This could be defined as having backup servers to keep your network in constant operation.  For example, a **standby server**.  A standby server is a secondary server with the exact configuration as a primary server.  The standby server is not actually being used, but its data is constantly being updated with the primary server.  So if something were to happen to the primary server, the standby server would immediately take over.



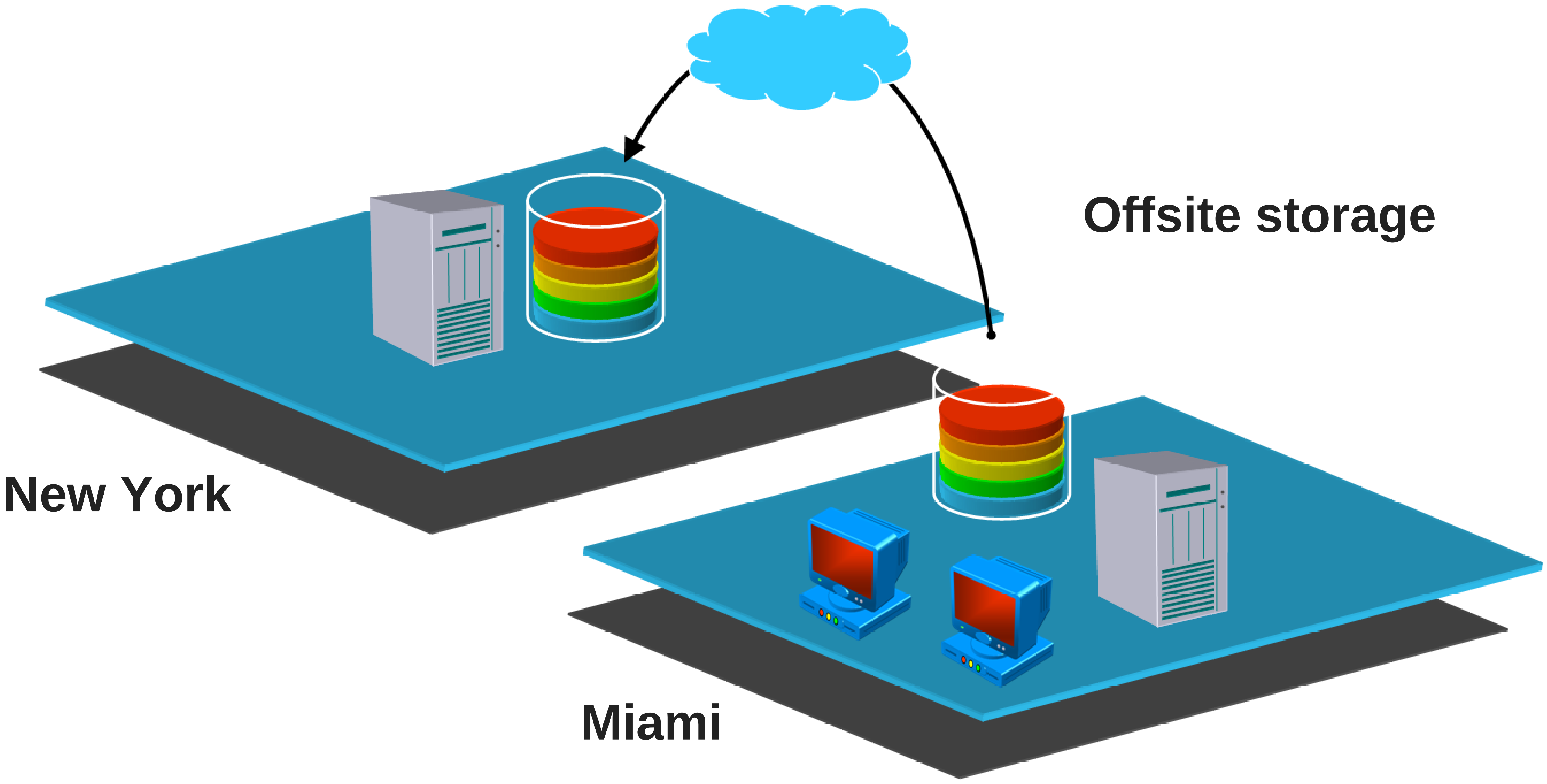
**Standby server would take over if the primary server failed.**

Another type of backup service would be **server clustering**. Server clustering is when a company has a group of servers that's used for load balancing and fault tolerance. In this setup, the server's would share the workload in case one of the servers fails. This type of setup works best if the servers were in different geographical locations in case of a natural disaster were to happen at one location.

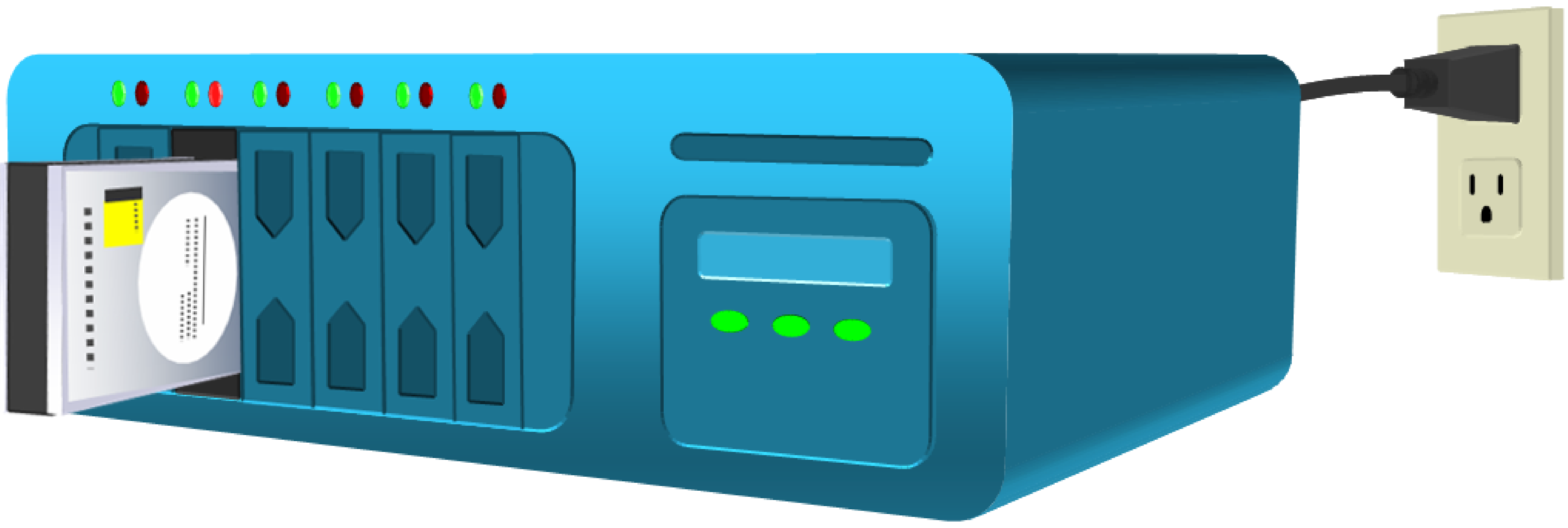


**Server clustering**

**Offsite storage** is where you can backup your data and have it stored in a different geographical location. So for example, let's say your main office is in Miami and you chose to have an offsite storage database in New York. If some kind of natural disaster were to happen in Miami, for example, a hurricane, and your main office along with the data was destroyed, you will still have a copy of all your data in New York where it is safe.



A **hot spare** is defined as equipment that can be swapped out without the need of turning off the power. So for example, if you had a server with multiple hot-swappable hard drives and if a hard drive were to fail, you wouldn't need to shut down the server. You just simply remove the hard drive and replace it with a new one while the power is still on.

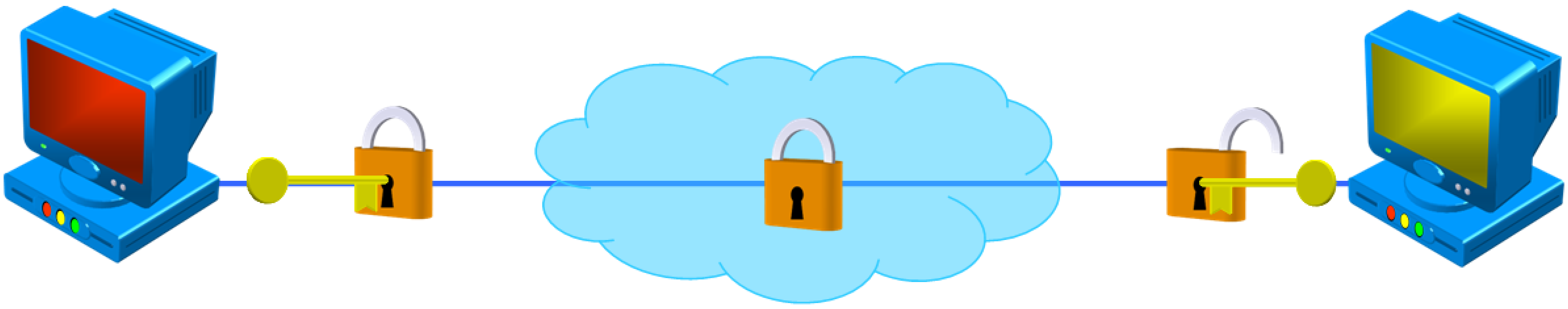


**A hard drive being hot-swapped on a server.**

A **cold spare** is similar to a hot spare, but with a cold spare, you must turn off the power in order to replace that piece of equipment.

# Security Protocols

**IPsec** is a set of protocols for security at the network layer of the OSI model.  IPsec encrypts the data when communication is happening between two computers.  But in order to use IPsec, both sender and receiver must share a public key.  This key is what locks and unlocks the data as it travels across a network.  This ensures that the data cannot be read or tampered with.

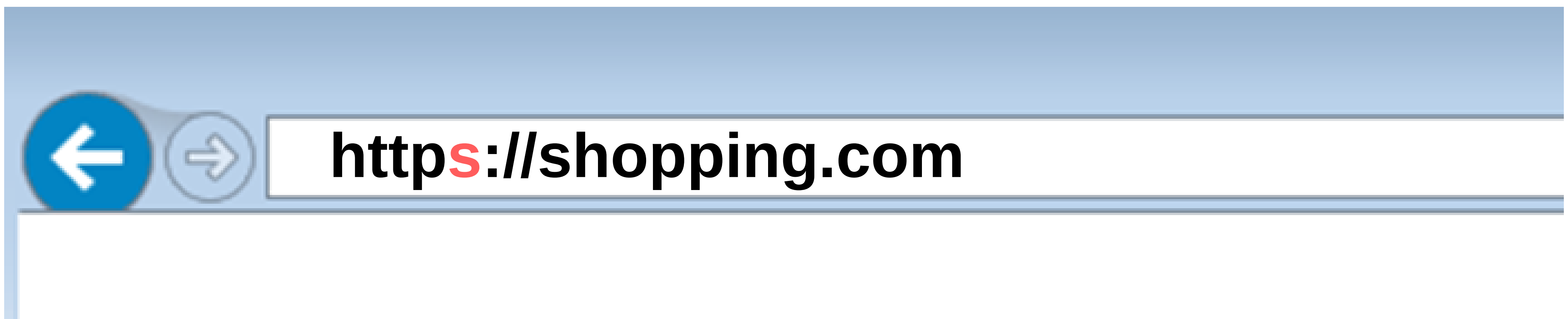


**In IPsec, the sender and receiver share a public key to lock and unlock data as it travels across a network.**

In addition to encryption, IPsec also verifies the data to make sure the data is received exactly as when it was sent.  IPsec also has two modes: transport and tunnel.  In transport mode, only the message portion of the data packet is encrypted.  But in tunnel mode, the entire data packet is encrypted.

**L2TP** or **layer 2 tunneling protocol** is a combination of Cisco's layer 2 forwarding and point-to-point tunneling protocol (PPTP).  This protocol authenticates in two ways using digital certificates.  It authenticates both the computer and the user and it also ensures that the data is not tampered with during the authentication process, which is known as **man-in-the-middle attack**.

**SSL** or **secure sockets layer** is a protocol that is used to ensure security on the internet.  SSL uses public key encryption to secure data, and it's commonly associated with HTTP.  So for example, if you were to go to an e-commerce website, you would notice that an 'S' has been added to HTTP, which indicates that you are now using SSL in your web browser.  SSL provides protection and three ways.  SSL authenticates the server, the client, and it encrypts the data.



https://shopping.com

**The 's' indicates that SSL is being used.**

**TLS** or **transport layer security** is the latest industry standard SSL protocol.  It's the successor to SSL and it's based on the same specifications.  Like SSL, it also authenticates the server, client, and encrypts the data. TLS is also made up of two layers.  The first layer is the TLS record protocol, which provides connection security by making sure the connection is private and reliable. The second layer is the TLS handshake protocol.  This protocol allows the server and client to authenticate each other, and negotiate an encryption algorithm and cryptographic keys before data is sent out.  The goal for TLS is to make SSL safer and more secure.

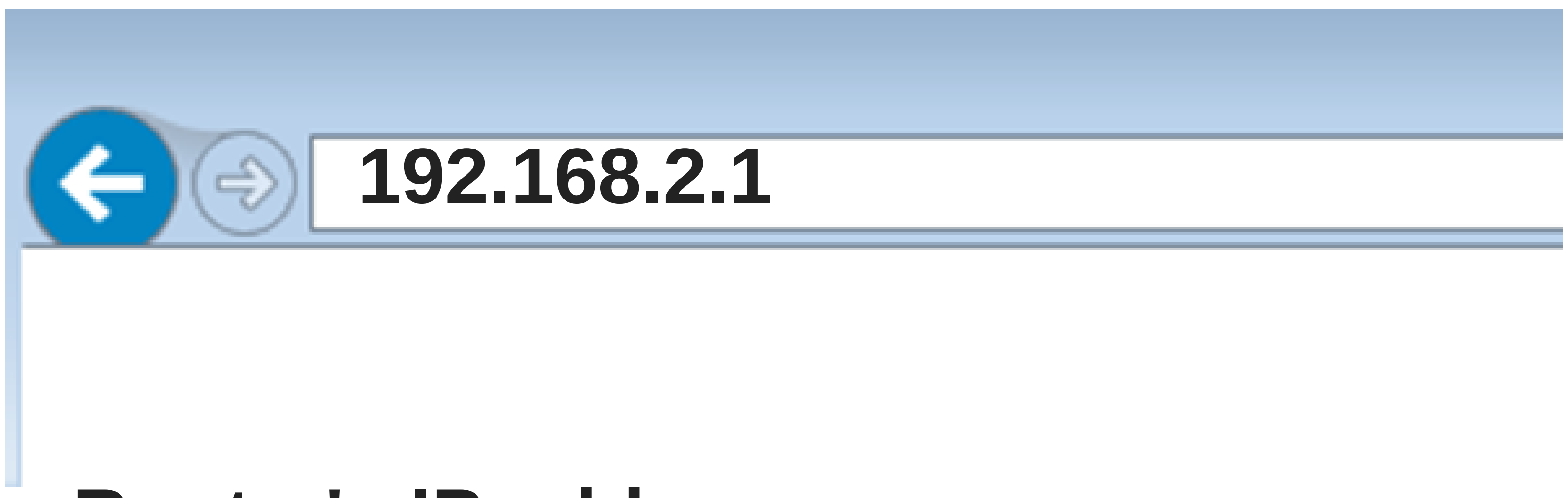
Our last security protocol is **802.1x**.  This standard is used for both wired and wireless networks.  It controls network access by ports.  So if authentication passes, the port is opened, and if the authentication fails, the port is closed.

# SOHO Routers & WIFI Encryption

Next, we're going to talk about **SOHO routers**, which stands for **small office home office** router. And these are your common inexpensive routers that are used in homes and small businesses. These are fairly easy to set up, but if you don't configure the router correctly, you will not have access to your network or the internet.

SOHO router

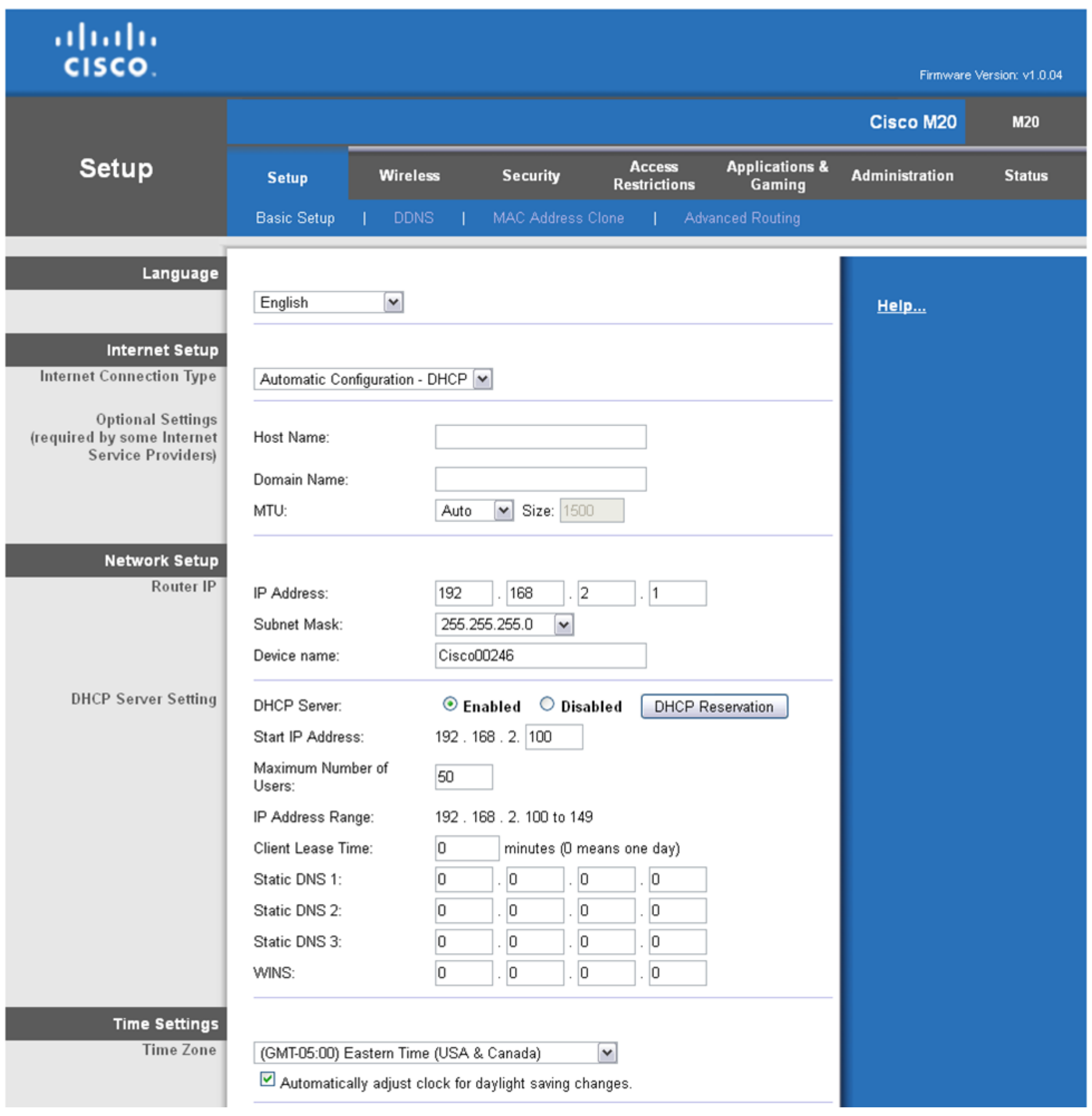
To set up and configure your SOHO router, you need to go to the router's built-in configuration web page. So you would just open up a web browser and in the address field, you would type in the router's IP address. So, for example, our router has an IP address of 192. 168. 2. 1. And once you type that in, you press enter on your keyboard and now you're in.



192.168.2.1

Router's IP address

So here is an example of the configuration page for a Cisco SOHO router.  And this is where you would set up the router with custom settings to make it work for your particular network.  So for example, like most SOHO routers, this one has a **DHCP** server built into it. And as you recall, a DHCP server automatically assigns an IP address to each computer on your network, because all computers need an IP address to function on a network.  So by default, the DHCP server is enabled but if you want to, you can disable the DHCP server by clicking 'Disabled' and then just save your settings.



Language
English

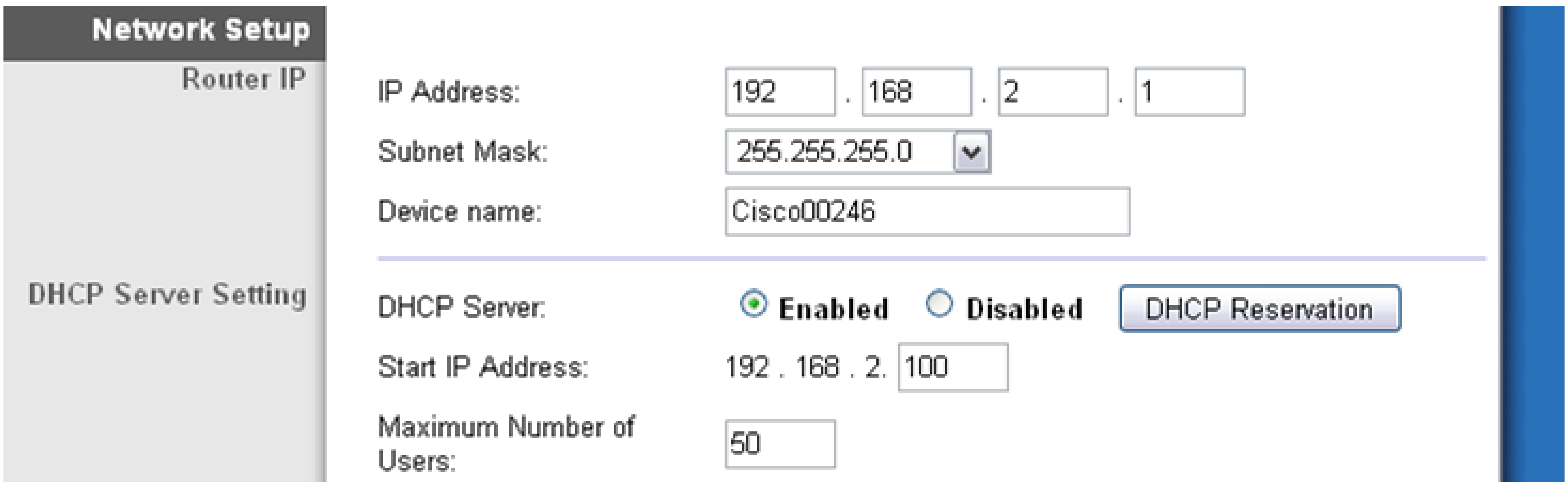
Internet Setup
Internet Connection Type: Automatic Configuration - DHCP
Optional Settings (required by some Internet Service Providers)
Host Name:
Domain Name:
MTU: Auto Size: 1500

Network Setup
Router IP
IP Address: 192 . 168 . 2 . 1
Subnet Mask: 255.255.255.0
Device name: Cisco00246

DHCP Server Setting
DHCP Server: ● Enabled ○ Disabled DHCP Reservation
Start IP Address: 192 . 168 . 2. 100
Maximum Number of Users: 50
IP Address Range: 192 . 168 . 2. 100 to 149
Client Lease Time: 0 minutes (0 means one day)
Static DNS 1: 0 . 0 . 0 . 0
Static DNS 2: 0 . 0 . 0 . 0
Static DNS 3: 0 . 0 . 0 . 0
WINS: 0 . 0 . 0 . 0

Time Settings
Time Zone: (GMT-05:00) Eastern Time (USA & Canada)
☑ Automatically adjust clock for daylight saving changes.

**Router's configuration page**

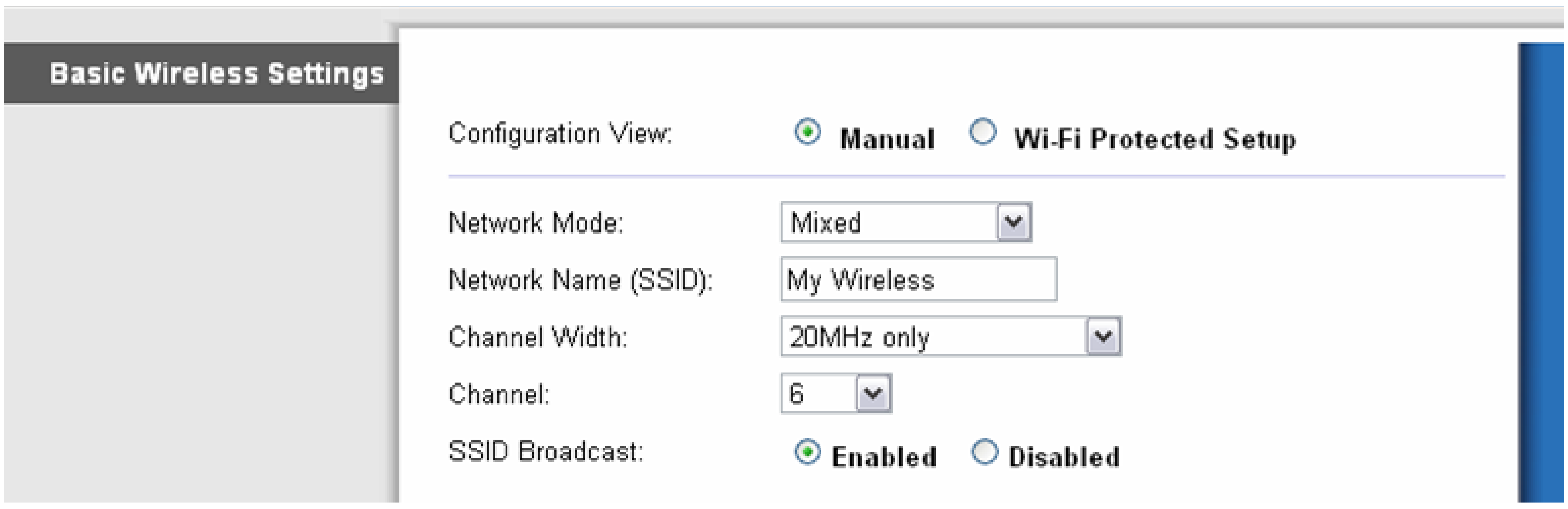


Network Setup
Router IP
IP Address: 192 . 168 . 2 . 1
Subnet Mask: 255.255.255.0
Device name: Cisco00246

DHCP Server Setting
DHCP Server: ● Enabled ○ Disabled DHCP Reservation
Start IP Address: 192 . 168 . 2. 100
Maximum Number of Users: 50

**DHCP settings for the router.**

Also in a router's web page, there are the wireless settings.  Now in here you can configure the wireless settings for your network.  So for example, you can set the **SSID** which stands for **service set identifier**, which is basically the name of your wireless network. The SSID is shared among all wireless devices and it's customizable, so you can name it whatever you want. And as you can see below, this SSID is called 'My Wireless'.



Basic Wireless Settings

Configuration View: ● Manual ○ Wi-Fi Protected Setup

Network Mode: Mixed

Network Name (SSID): My Wireless

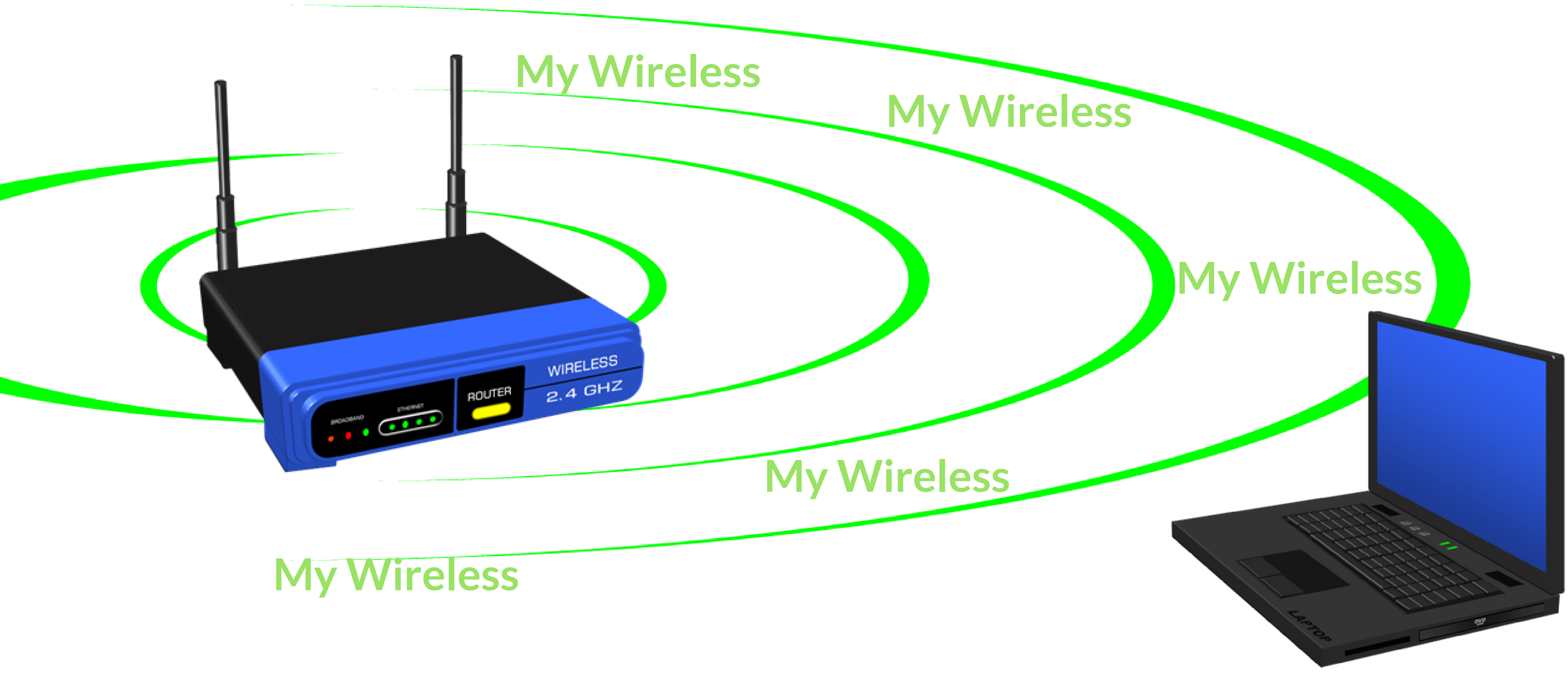
Channel Width: 20MHz only

Channel: 6

SSID Broadcast: ● Enabled ○ Disabled

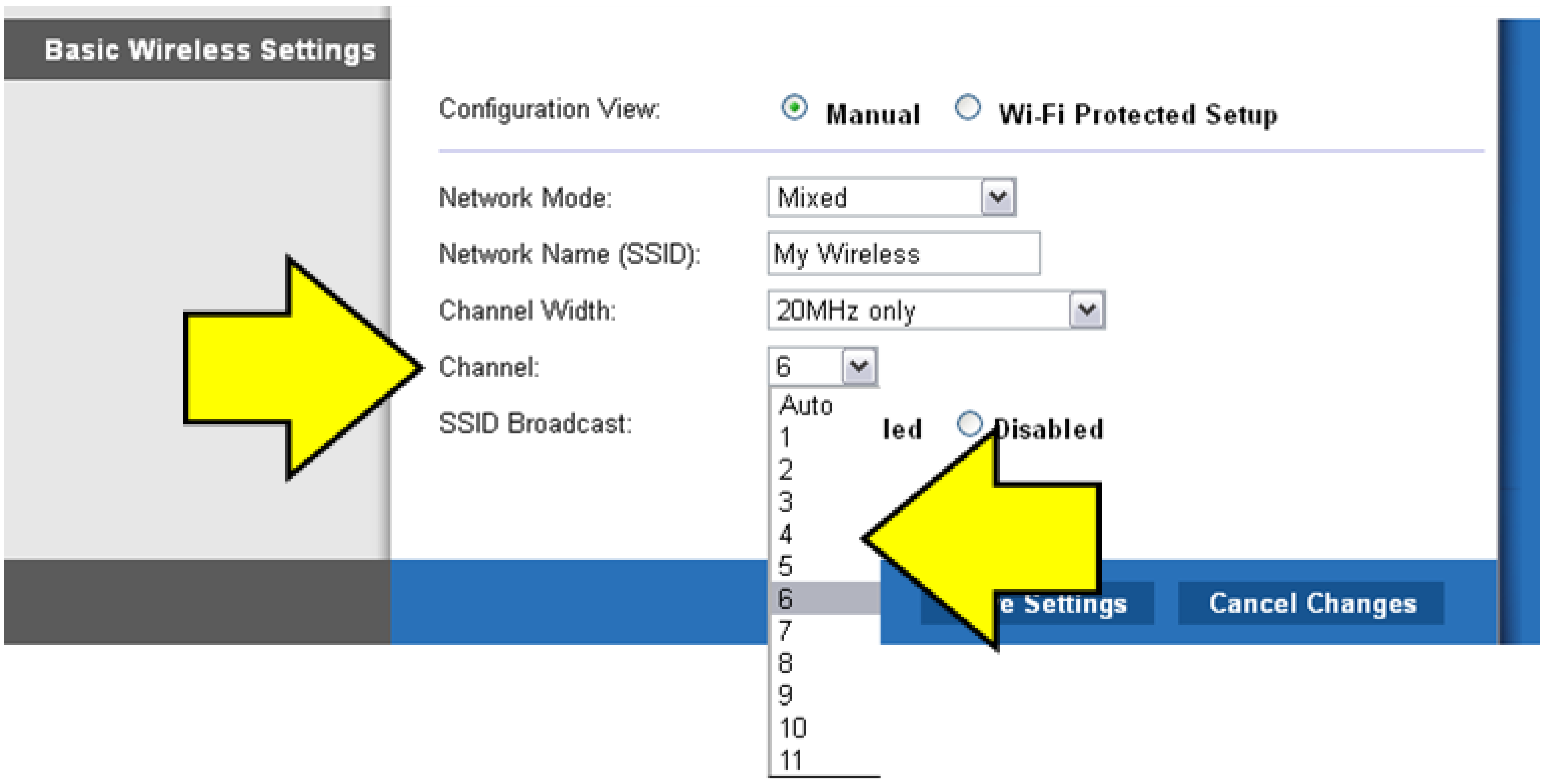
**Wireless settings for the router.**

So as an example, when a laptop scans for a wireless network to join.  And if the laptop is in the range of this router, the laptop will see the router's SSID broadcast, called 'My Wireless', and if it has the proper credentials, it can join the network.



**Router broadcasting its SSID**

You can also set the **channel** for your wireless network. Channels are used to avoid interference with other wireless networks nearby, or even wireless devices such as cordless phones.  So if you are experiencing any connectivity issues to your wireless router, there might be interference with another nearby wireless network or device, that's operating on the same channel as yours.  So, in this case, you can try changing to a different channel and see if it solves your problem.



Basic Wireless Settings

Configuration View: ● Manual ○ Wi-Fi Protected Setup

Network Mode: Mixed

Network Name (SSID): My Wireless

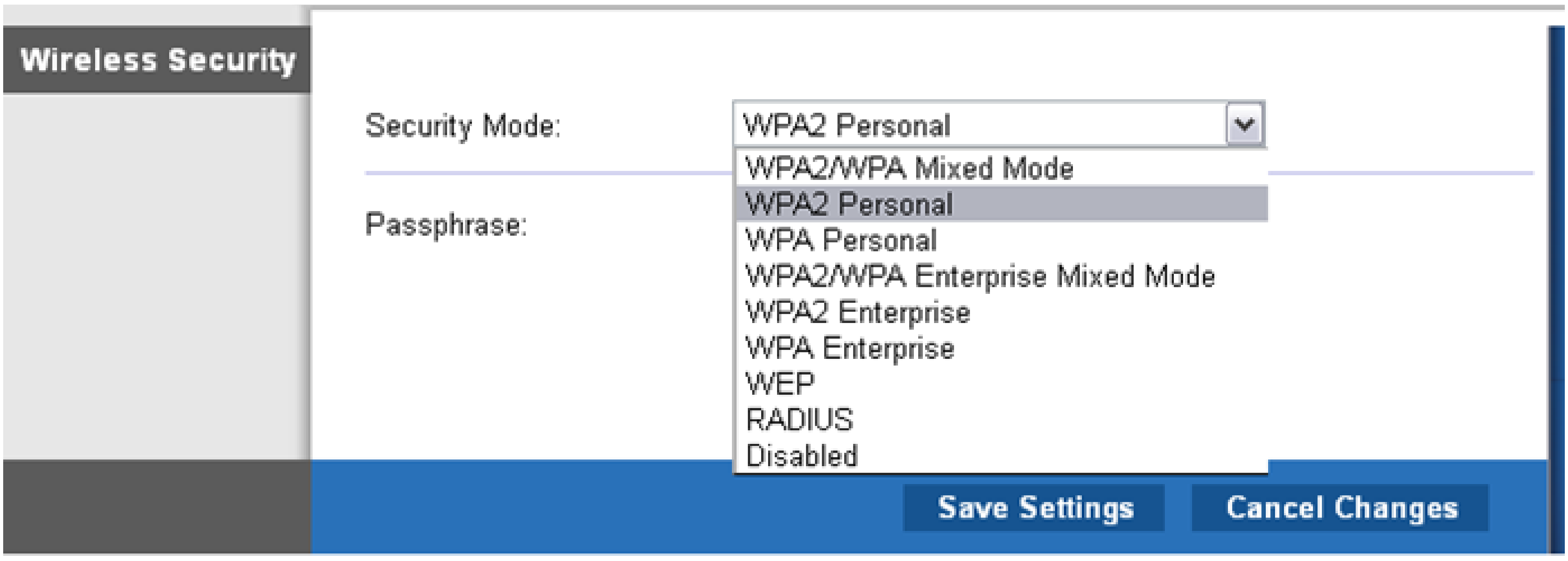
Channel Width: 20MHz only

Channel: 6

SSID Broadcast: led ○ Disabled

**Wireless channel settings page**

If you click on the wireless security section, you can configure the security of your wireless network (graphic below).  So here, you can choose to disable security and have your wireless network wide open.  Or you can password protect your wireless network with one of these security modes.  And as you can see, this router supports the following security options, such as WEP, WPA, and WPA2.



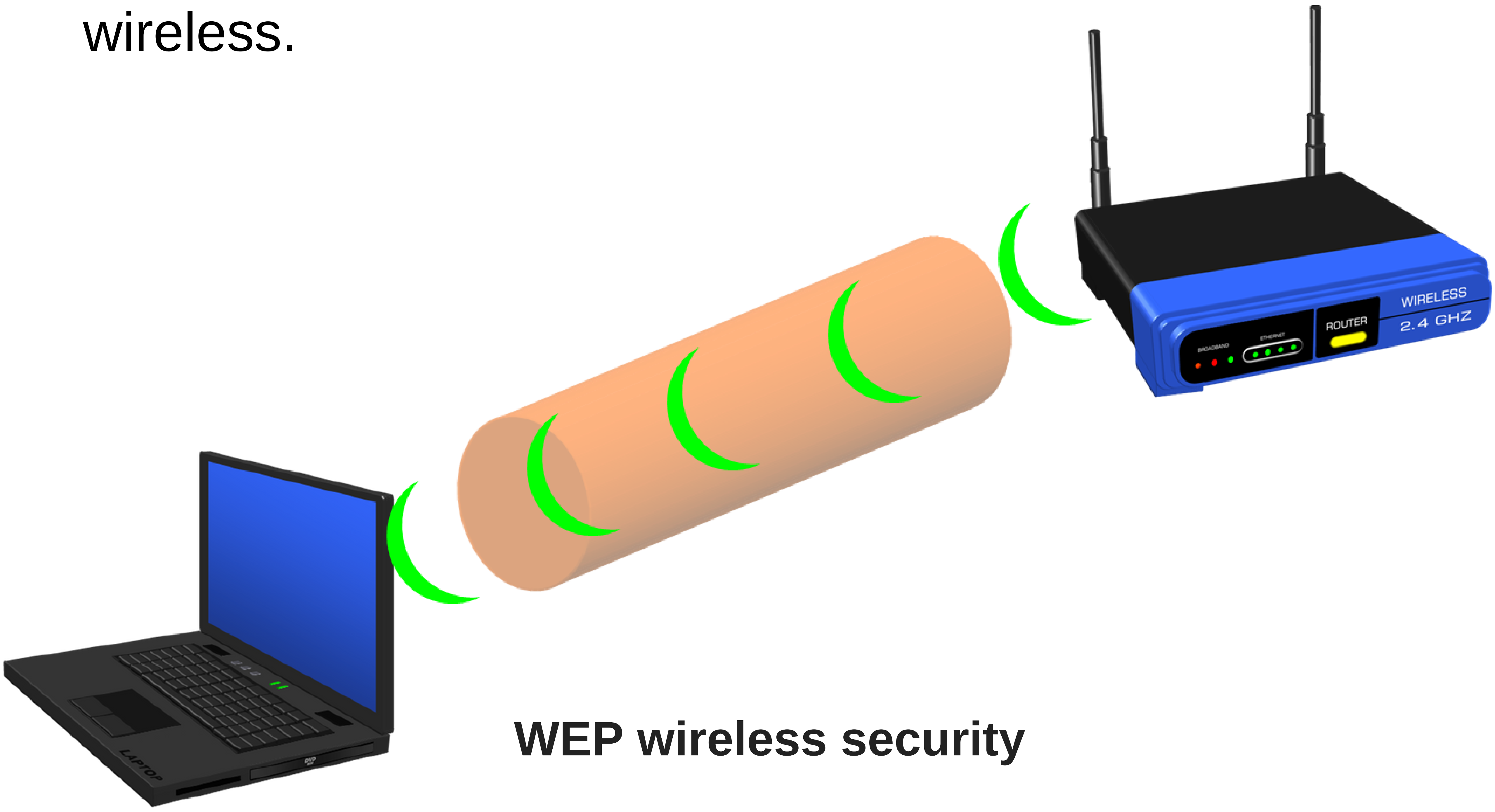
Wireless Security

Security Mode: WPA2 Personal

Passphrase:

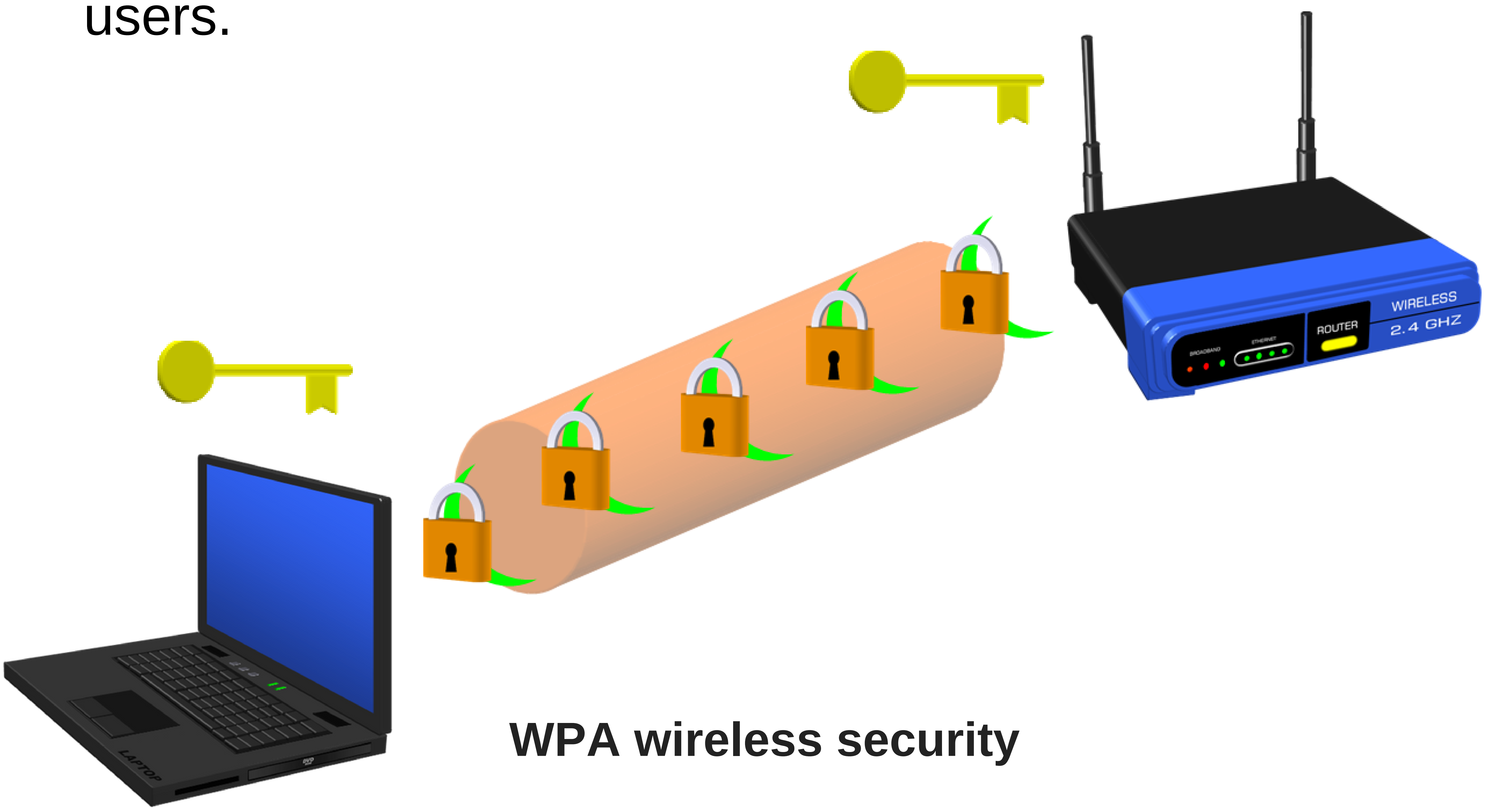
**Wireless security options for the router**

**WEP** or **wired equivalent privacy**, is one of the security protocols that are used for wireless networks. And as its name implies, it's meant to supply the same security to wireless networks, as it did for wired networks. But this turned out not to be the case. After a time, it was found out that the 40-bit encryption key that WEP used, was not secure and it was easily hackable. So a better security protocol was needed for wireless.



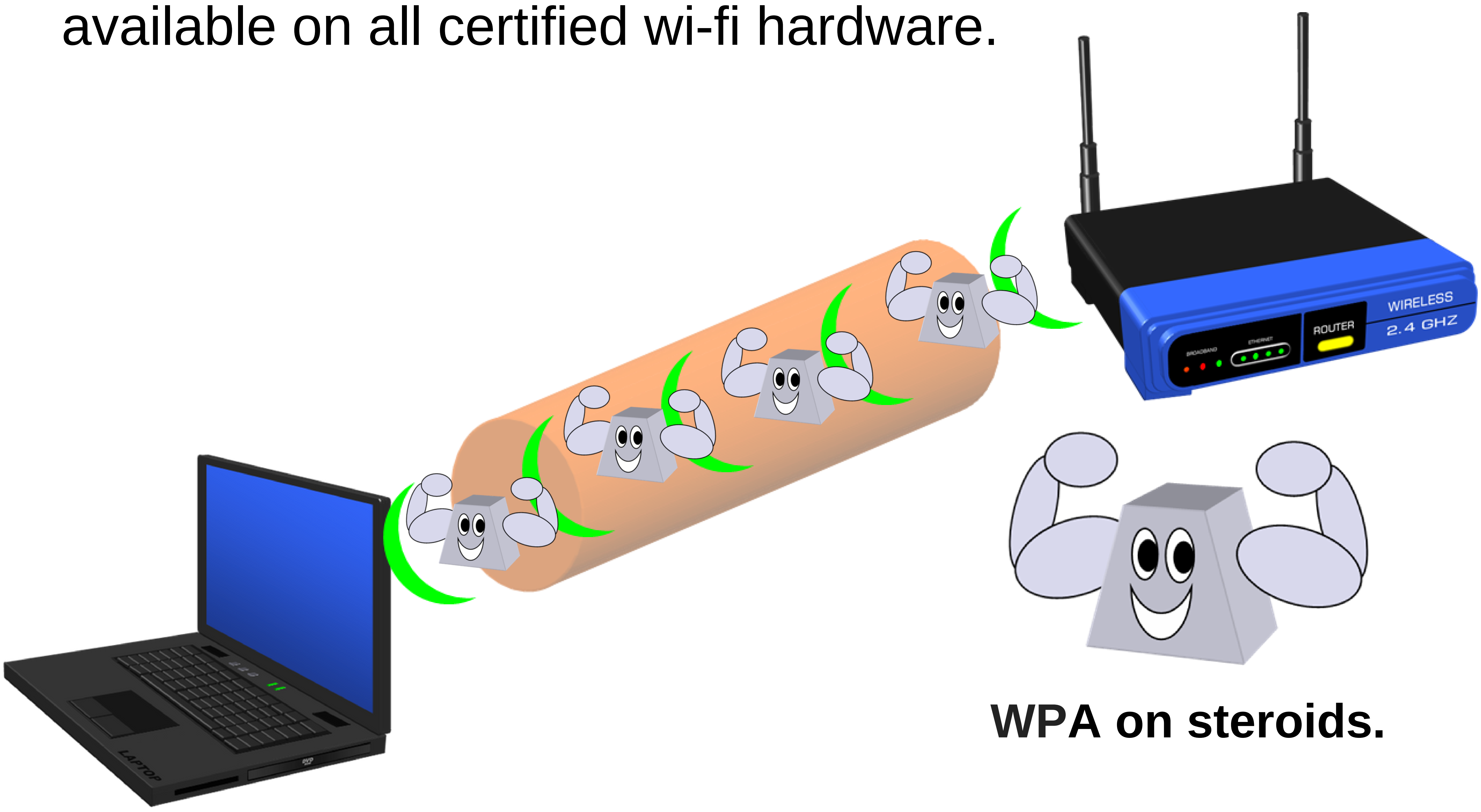
**WEP wireless security**

**WPA** or **Wi-Fi protected access**, is another wireless security protocol that was developed to solve the security problems of WEP.  WPA is far better than WEP in two ways.  First, it uses a stronger encryption method using **TKIP**, which stands for **temporal key integrity protocol**, which dynamically changes his keys as it's being used.  This ensures data integrity.  And secondly, WPA uses EAP which verifies authorized network users.



**WPA wireless security**

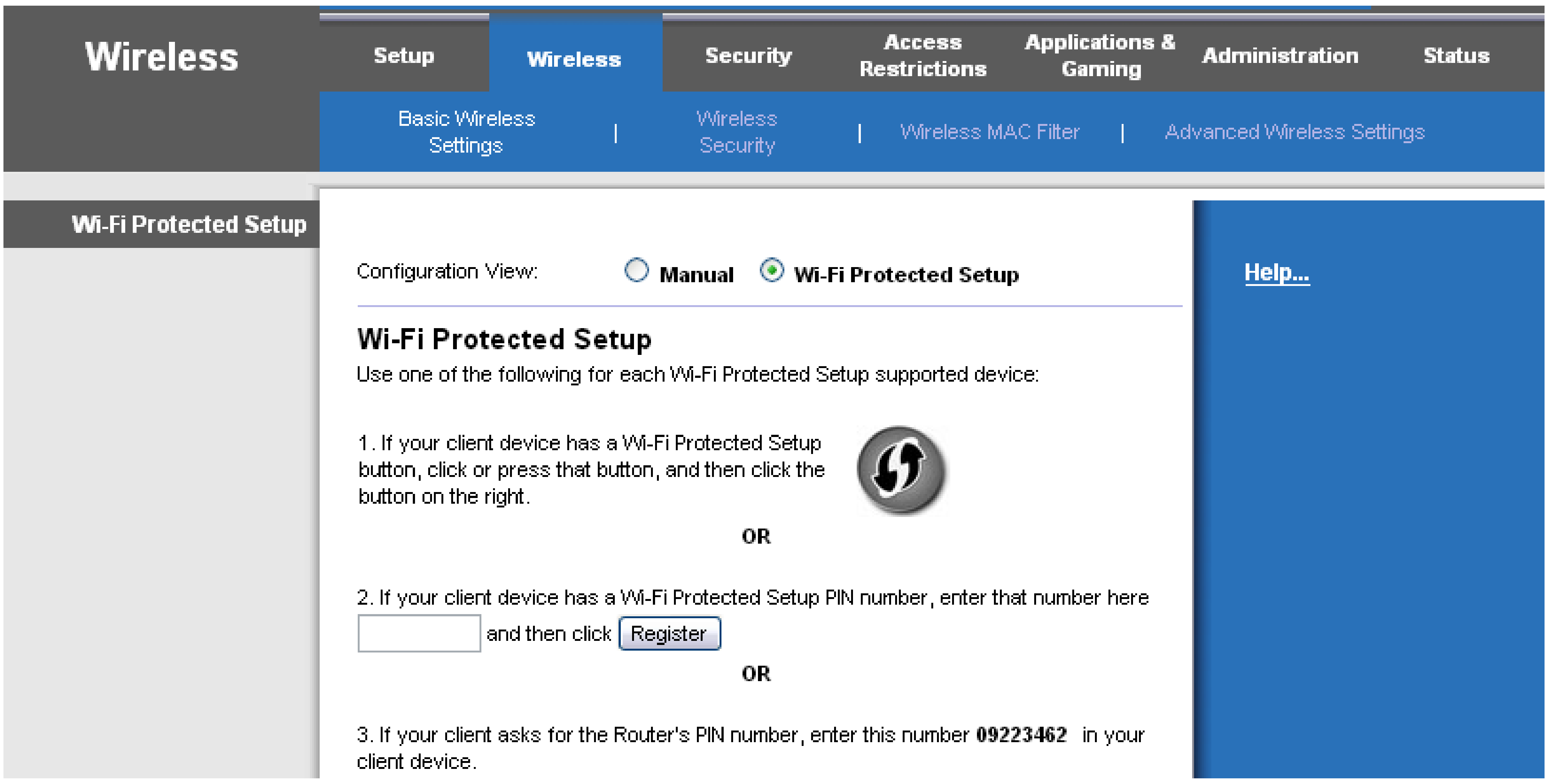
Building on the security of WPA.  **WPA2** was developed to provide even stronger security than WPA.  And it does this by requiring the use of a stronger wireless encryption method.  While WPA uses temporal key Integrity protocol for encryption, which is known to have some limitations, WPA2 uses CCMP (counter Mode cipher block chaining message authentication code protocol) for encryption.  And CCMP is more secure because it uses an enhanced data cryptographic encapsulation mechanism.  And since 2006, WPA2 is available on all certified wi-fi hardware.



WPA on steroids.

**WPA2 wireless security**

Another wireless security protocol is **WPS**.  WPS stands for **wi-fi protected setup**.   WPS was designed for users who know little about wireless networks, to make it as easy as possible for them to join a secure wireless network.  So here's the WPS configuration page for our router.



Configuration View: ○ Manual ● Wi-Fi Protected Setup

Wi-Fi Protected Setup

Use one of the following for each Wi-Fi Protected Setup supported device:

1. If your client device has a Wi-Fi Protected Setup button, click or press that button, and then click the button on the right.

OR

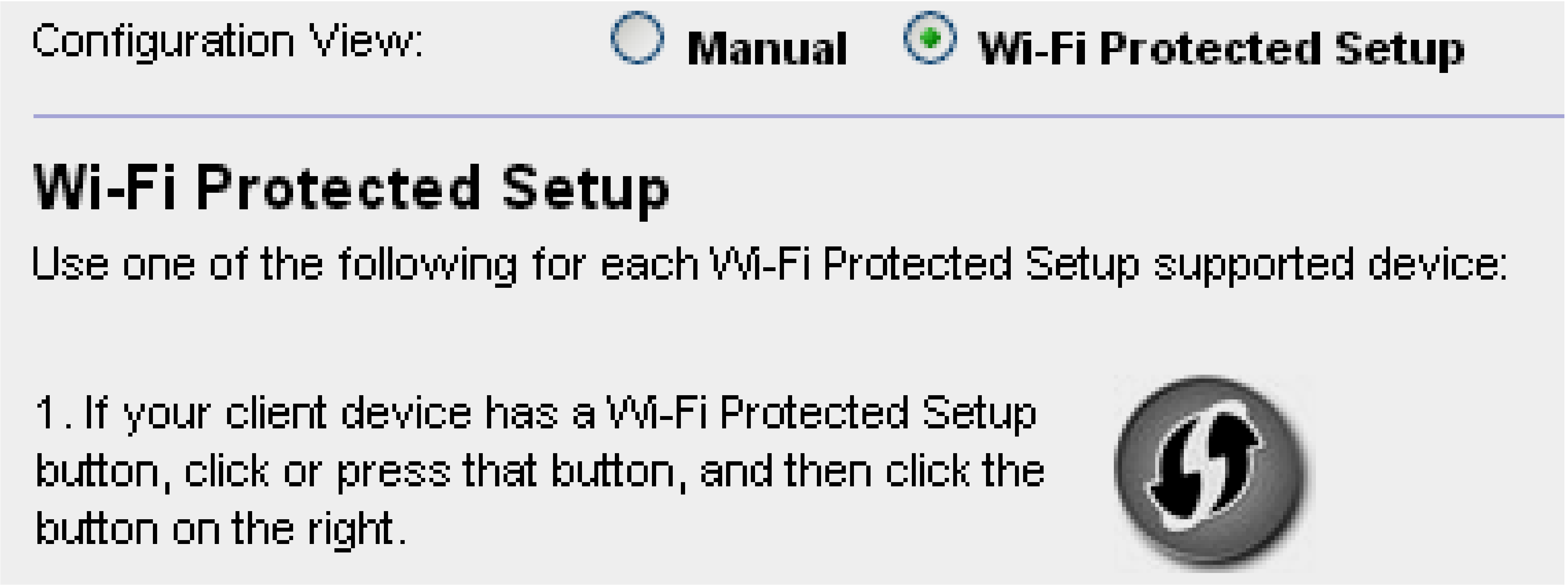
2. If your client device has a Wi-Fi Protected Setup PIN number, enter that number here ____ and then click Register

OR

3. If your client asks for the Router's PIN number, enter this number **09223462** in your client device.

**WPS wireless security settings**

And as you can see, there are three different WPS methods that you can use to join this wireless network. So you could use method 1 if your client has a wi-fi protected setup button.  You would just press that button on your device, then within two minutes you would press the WPS button here on this page, or you can just press that physical WPS button on the router itself, and then you'll be connected.



Configuration View: ○ Manual ● Wi-Fi Protected Setup

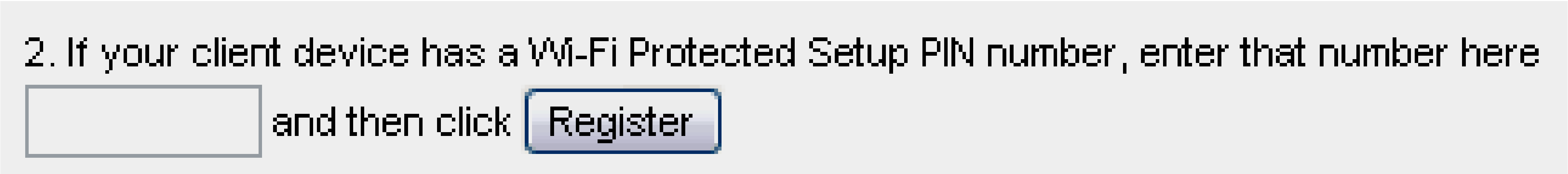
**Wi-Fi Protected Setup**

Use one of the following for each Wi-Fi Protected Setup supported device:

1. If your client device has a Wi-Fi Protected Setup button, click or press that button, and then click the button on the right.

**Method 1 of WPS wireless security settings**

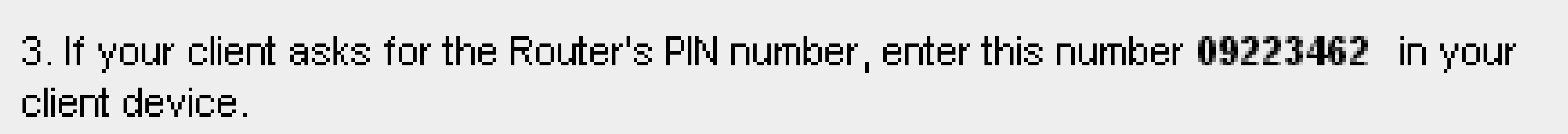
You can also use method 2 if your client has a WPS pin number.  You would just enter that number in the field below, and then press register.



2. If your client device has a Wi-Fi Protected Setup PIN number, enter that number here ▭ and then click Register

**Method 2 of WPS wireless security settings**

And finally, you can use method 3 if your client asks for the router's pin number.  So you would just enter the router's pin number that's displayed on this page, and enter it into your device, and then you'll be connected.

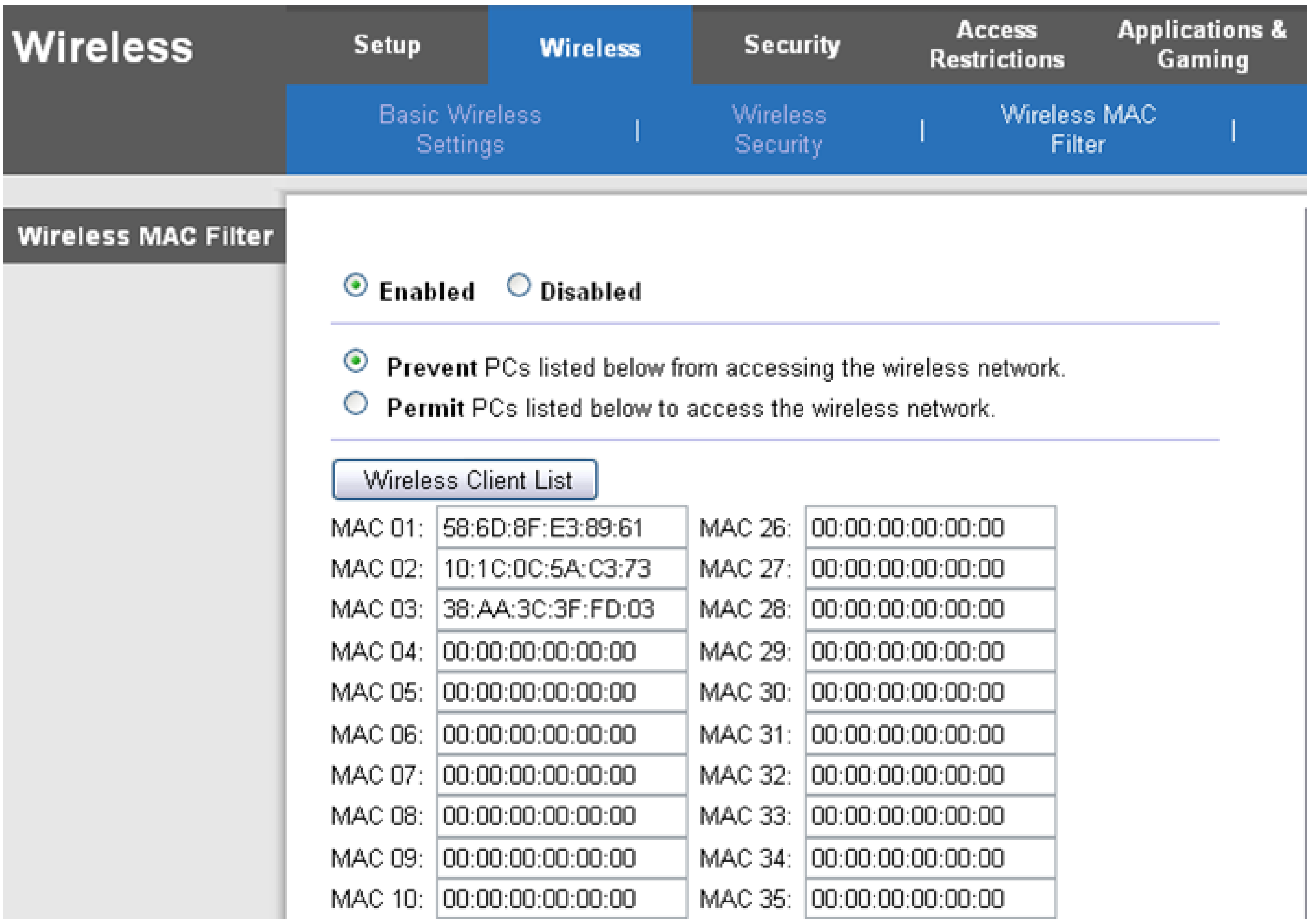


3. If your client asks for the Router's PIN number, enter this number **09223462** in your client device.

**Method 3 of WPS wireless security settings**

So as stated before, WPS is the easiest way to join a wireless network.  And a lot of manufacturers are building their wireless products with WPS, to make it as simple as possible for their customers to join their device to a wireless network.

Another wireless security feature is the **MAC filter**. Every wireless adapter has a MAC address.  A MAC address is a hexadecimal number that uniquely identifies each device on a network.  And with the wireless MAC filter, you can either prevent or permit access by using the device's MAC address.



● Enabled ○ Disabled

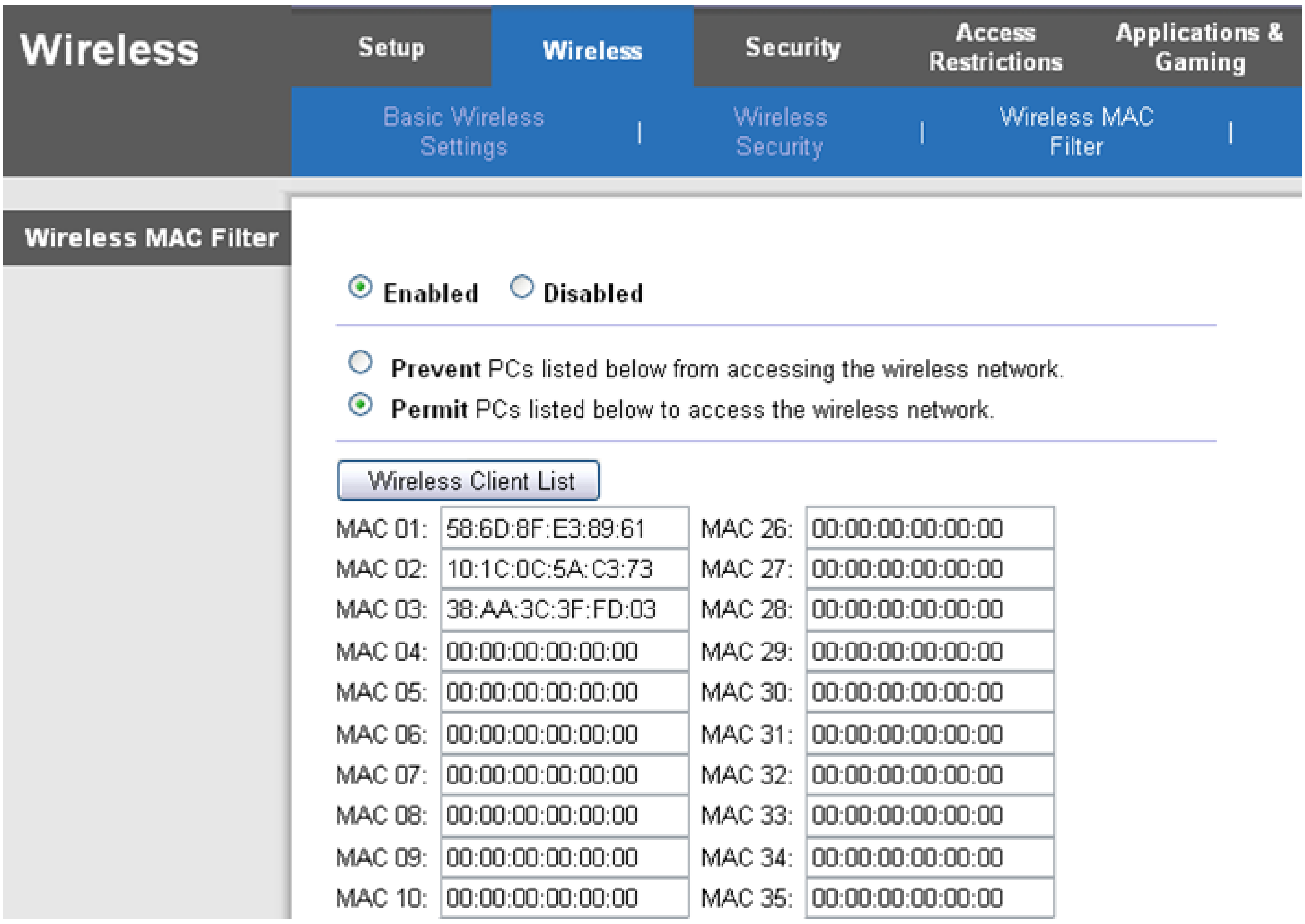
● **Prevent** PCs listed below from accessing the wireless network.
○ **Permit** PCs listed below to access the wireless network.

| | | | |
|---|---|---|---|
| MAC 01: | 58:6D:8F:E3:89:61 | MAC 26: | 00:00:00:00:00:00 |
| MAC 02: | 10:1C:0C:5A:C3:73 | MAC 27: | 00:00:00:00:00:00 |
| MAC 03: | 38:AA:3C:3F:FD:03 | MAC 28: | 00:00:00:00:00:00 |
| MAC 04: | 00:00:00:00:00:00 | MAC 29: | 00:00:00:00:00:00 |
| MAC 05: | 00:00:00:00:00:00 | MAC 30: | 00:00:00:00:00:00 |
| MAC 06: | 00:00:00:00:00:00 | MAC 31: | 00:00:00:00:00:00 |
| MAC 07: | 00:00:00:00:00:00 | MAC 32: | 00:00:00:00:00:00 |
| MAC 08: | 00:00:00:00:00:00 | MAC 33: | 00:00:00:00:00:00 |
| MAC 09: | 00:00:00:00:00:00 | MAC 34: | 00:00:00:00:00:00 |
| MAC 10: | 00:00:00:00:00:00 | MAC 35: | 00:00:00:00:00:00 |

**Wireless MAC filter settings (devices prevented)**

So in the example above, once we enable the MAC filter, we can choose the option to **prevent** devices that are listed above from accessing the wireless network. So all of these devices listed above are now blocked from joining the network.

Or the other option, we can choose the **permit** option. And this will allow only the devices listed below access to the network.



● Enabled ○ Disabled

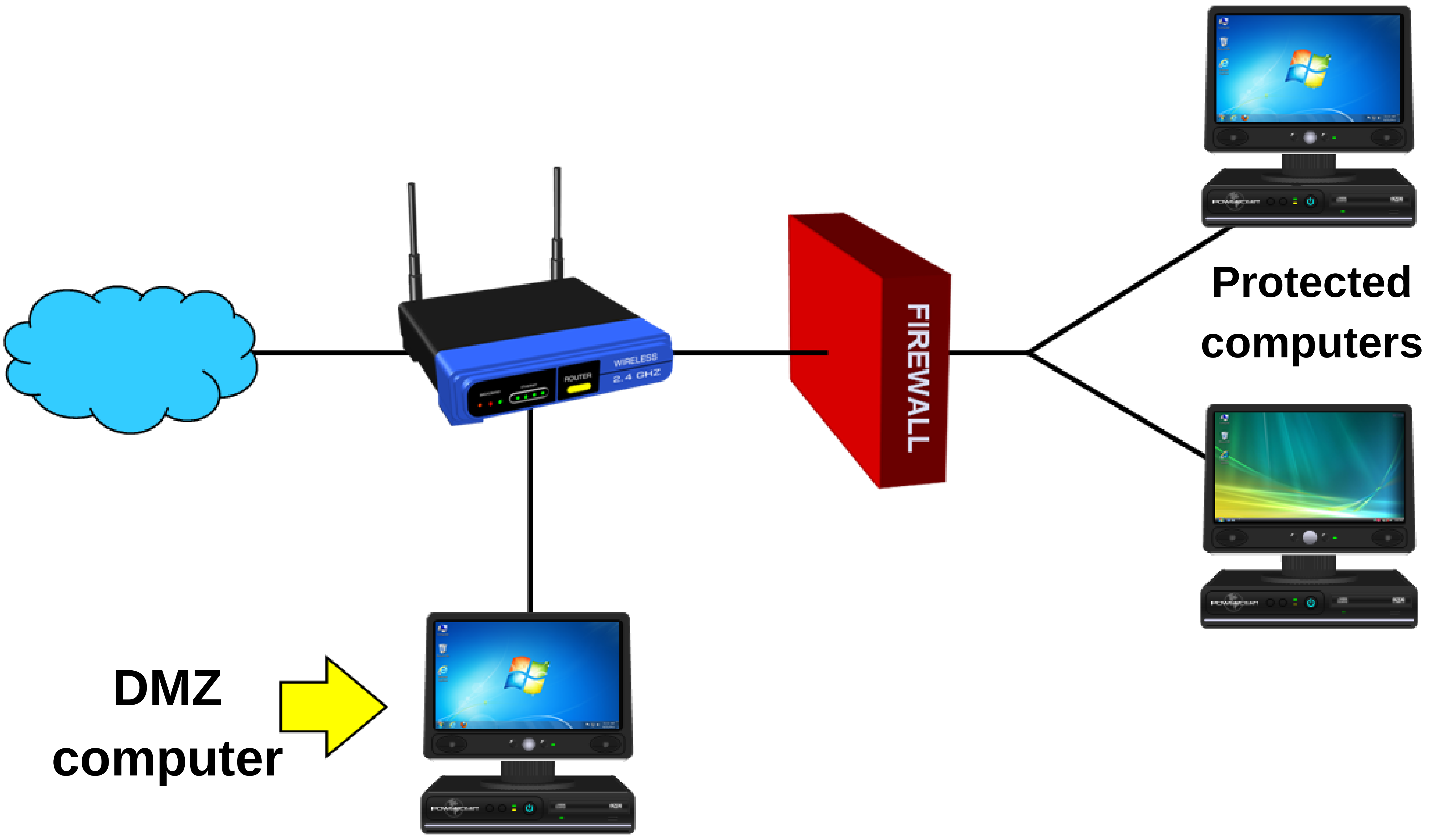
○ **Prevent** PCs listed below from accessing the wireless network.

● **Permit** PCs listed below to access the wireless network.

| | | | |
|---|---|---|---|
| MAC 01: | 58:6D:8F:E3:89:61 | MAC 26: | 00:00:00:00:00:00 |
| MAC 02: | 10:1C:0C:5A:C3:73 | MAC 27: | 00:00:00:00:00:00 |
| MAC 03: | 38:AA:3C:3F:FD:03 | MAC 28: | 00:00:00:00:00:00 |
| MAC 04: | 00:00:00:00:00:00 | MAC 29: | 00:00:00:00:00:00 |
| MAC 05: | 00:00:00:00:00:00 | MAC 30: | 00:00:00:00:00:00 |
| MAC 06: | 00:00:00:00:00:00 | MAC 31: | 00:00:00:00:00:00 |
| MAC 07: | 00:00:00:00:00:00 | MAC 32: | 00:00:00:00:00:00 |
| MAC 08: | 00:00:00:00:00:00 | MAC 33: | 00:00:00:00:00:00 |
| MAC 09: | 00:00:00:00:00:00 | MAC 34: | 00:00:00:00:00:00 |
| MAC 10: | 00:00:00:00:00:00 | MAC 35: | 00:00:00:00:00:00 |

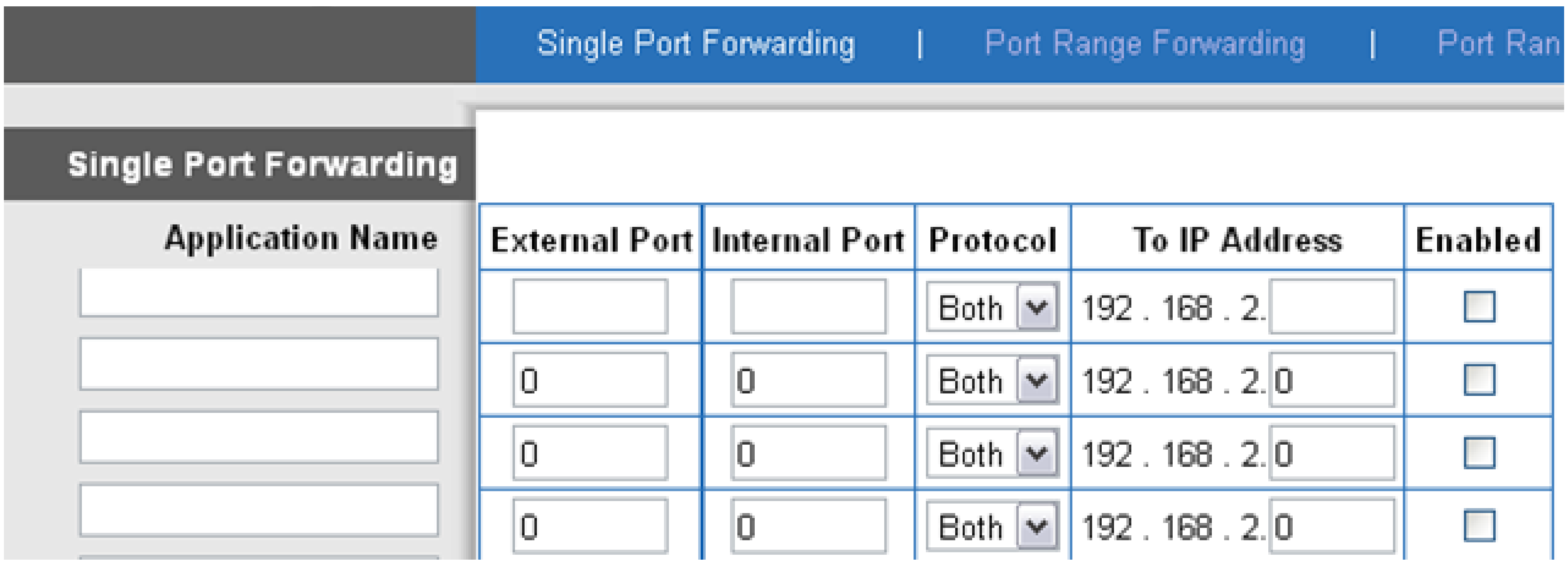
**Wireless MAC filter settings (devices permitted)**

There's also what's called the **DMZ**, which stands for **demilitarized zone**. The DMZ allows a designated computer on your network to be fully exposed to the internet. And it does this by the router forwarding all ports at the same time to the designated DMZ computer.



So while some computers here on our network are protected inside the firewall, the DMZ computer is outside the firewall and is not protected.  The DMZ is typically used for testing purposes.  So if you just set up a computer that you want to be accessed from the internet, and if you're having a problem configuring a firewall and applications so that it can be accessed from the internet, you can simply bypass all firewall security and put the computer in the DMZ temporarily to make sure everything is working until you can pinpoint the problem you are having.  For instance, you could be having a problem with a firewall setting.  It's also important to note, that the DMZ computer should be assigned a static IP address and not automatically from a DHCP server.

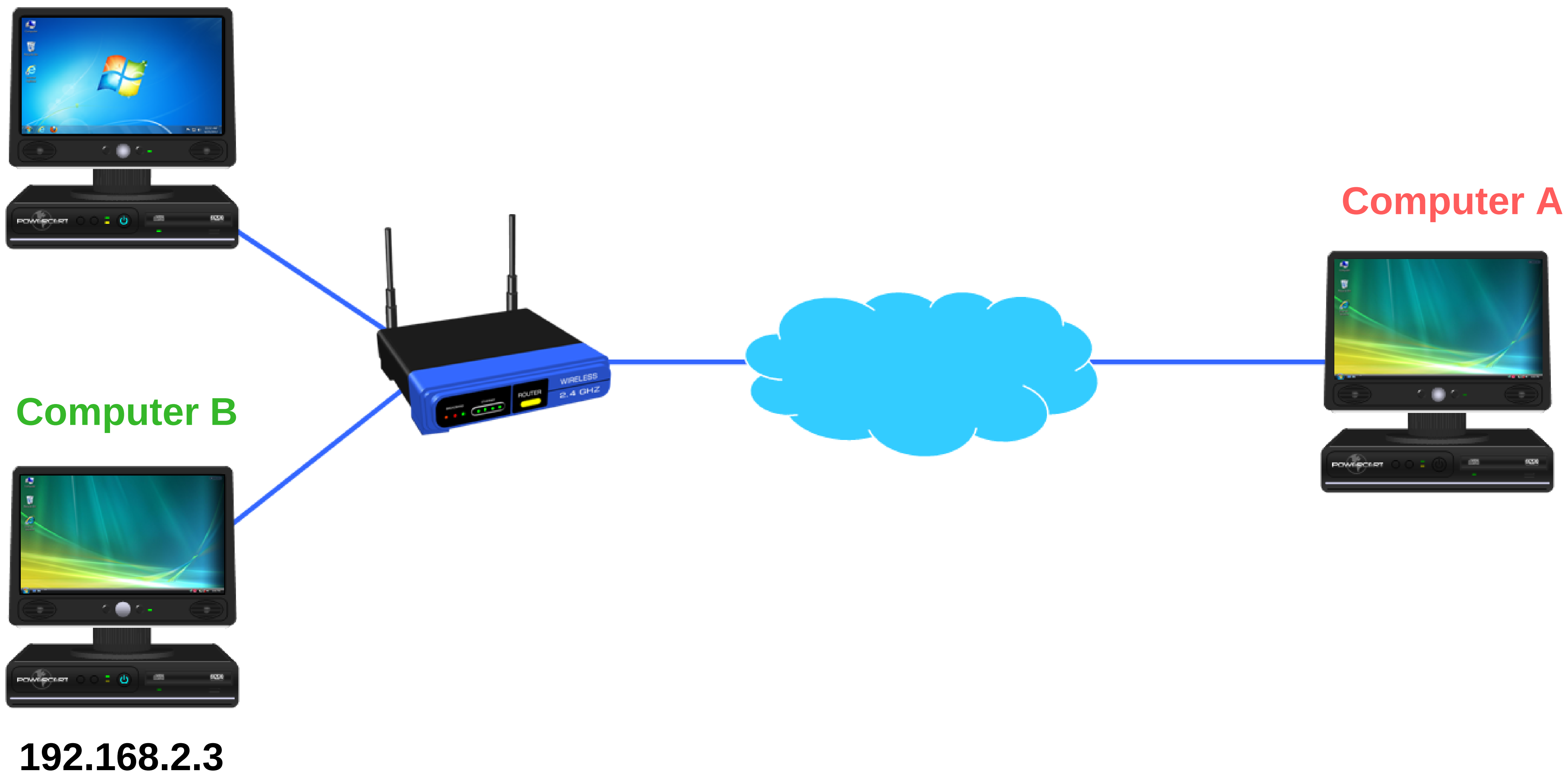
Another option on a configuration page is **port forwarding**.  On this page, you can customize port services for certain applications.  So when a user sends these types of requests to your network from the internet, the router will forward those requests to the appropriate computer.



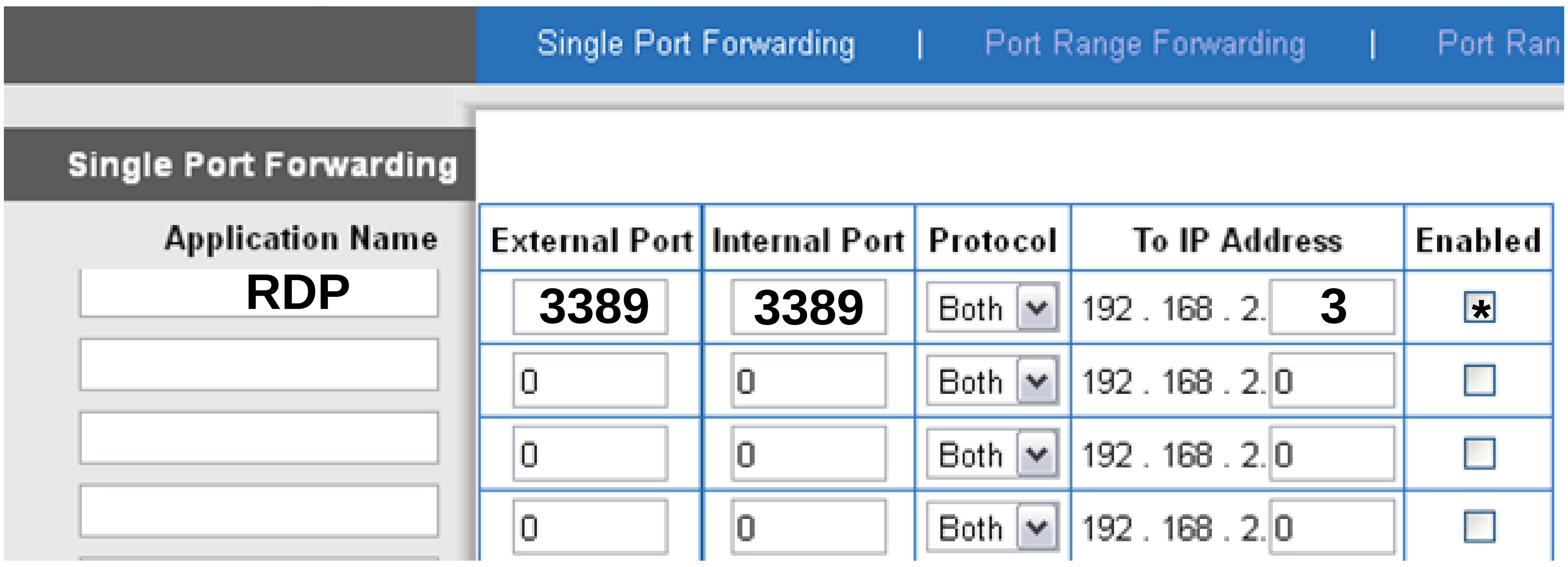
| Application Name | External Port | Internal Port | Protocol | To IP Address | Enabled |
|---|---|---|---|---|---|
| | | | Both | 192 . 168 . 2. | □ |
| | 0 | 0 | Both | 192 . 168 . 2. 0 | □ |
| | 0 | 0 | Both | 192 . 168 . 2. 0 | □ |
| | 0 | 0 | Both | 192 . 168 . 2. 0 | □ |

**Port forwarding section**

So for example (below), let's say **Computer A** wants to access **Computer B** on a home network using RDP or remote desktop protocol.  And as you know from an earlier lesson, that RDP uses port 3389.  So what happens is, when **Computer A** starts the RDP service on their computer, it will put in the public IP address of **Computer B's** router.  Then once the request reaches the router, the router needs to know which computer on its network to forward that request, so **Computer A** can access **Computer B**.  So that's where port forwarding comes in.

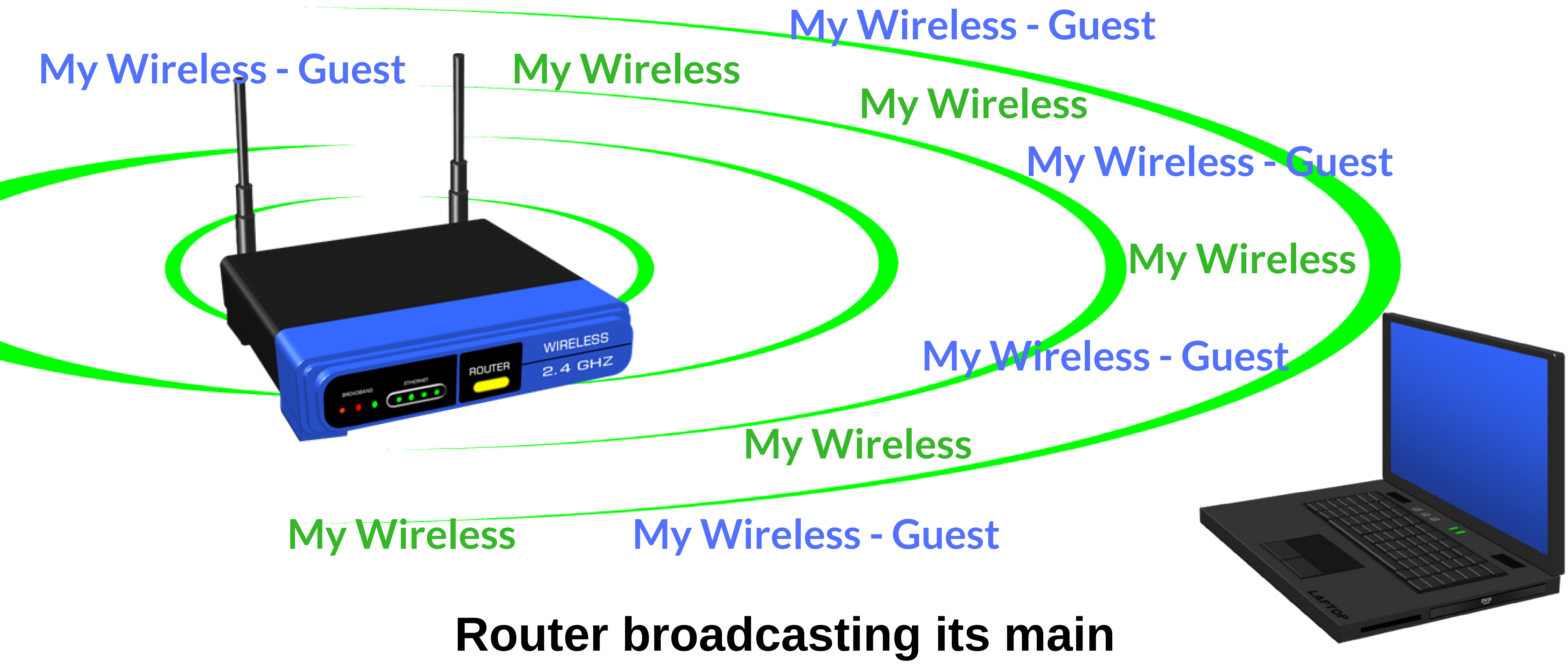


On the port forwarding configuration page (below), you have to forward the RDP port to **Computer B**. So, you type in the RDP port number, which is *3389* and then you have to point it to the IP address of **Computer B,** which is *192.168.2.3.* Then once that is done, the router knows where to forward the request and the configuration is now complete.



| Application Name | External Port | Internal Port | Protocol | To IP Address | Enabled |
|---|---|---|---|---|---|
| RDP | 3389 | 3389 | Both | 192 . 168 . 2. 3 | ☒ |
| | 0 | 0 | Both | 192 . 168 . 2. 0 | □ |
| | 0 | 0 | Both | 192 . 168 . 2. 0 | □ |
| | 0 | 0 | Both | 192 . 168 . 2. 0 | □ |

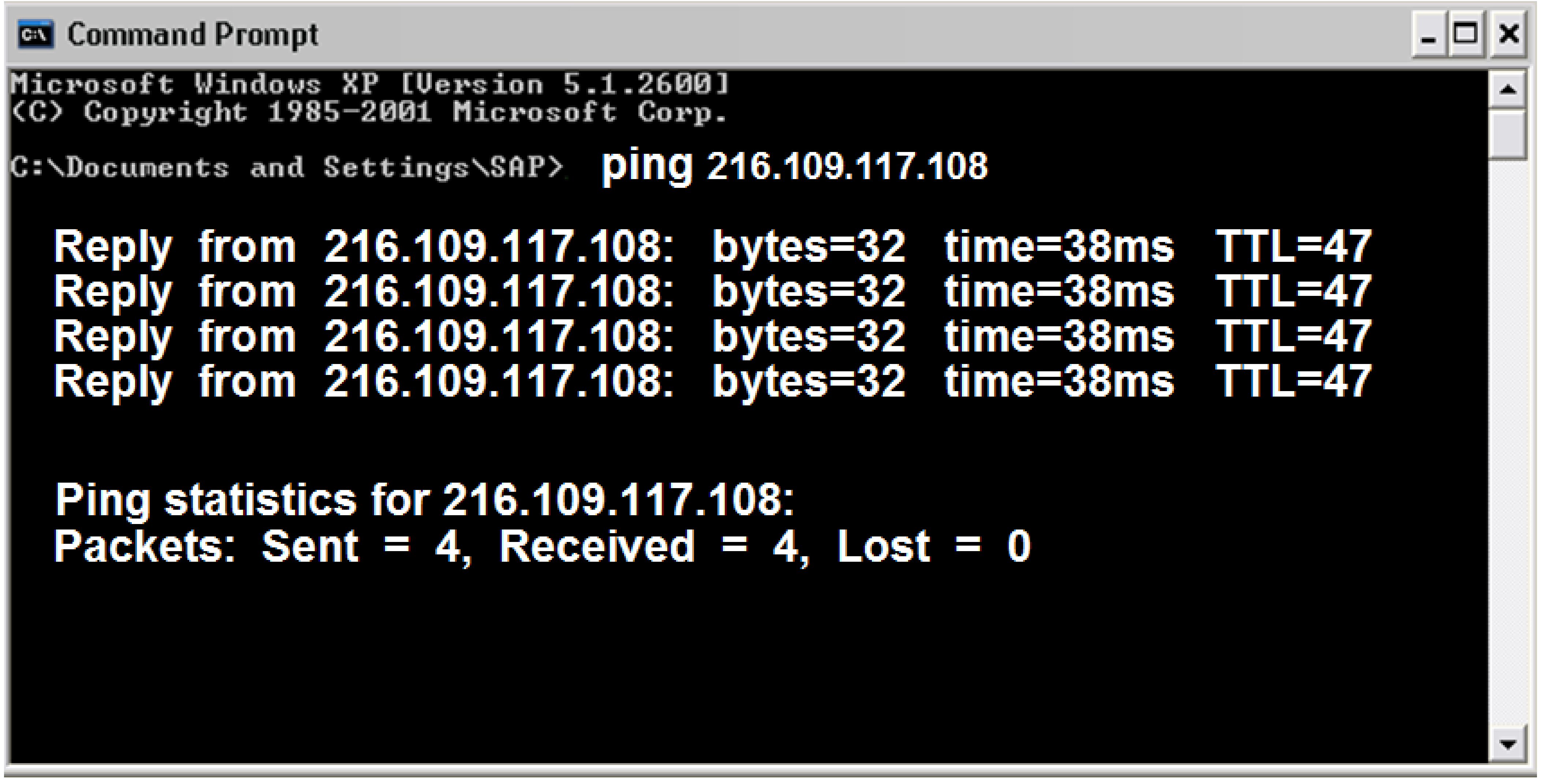
A feature that's built into most wireless routers is called a **guest network**. A guest network is a separate wireless network that's built into a wireless router that guests can join so they can have internet access. The guest network will have its own SSID and it's typically the same name as your main network's SSID, but by default, it may have a minus guest suffix added to the SSID.



**Router broadcasting its main SSID and its Guest SSID.**

# Network Utilities

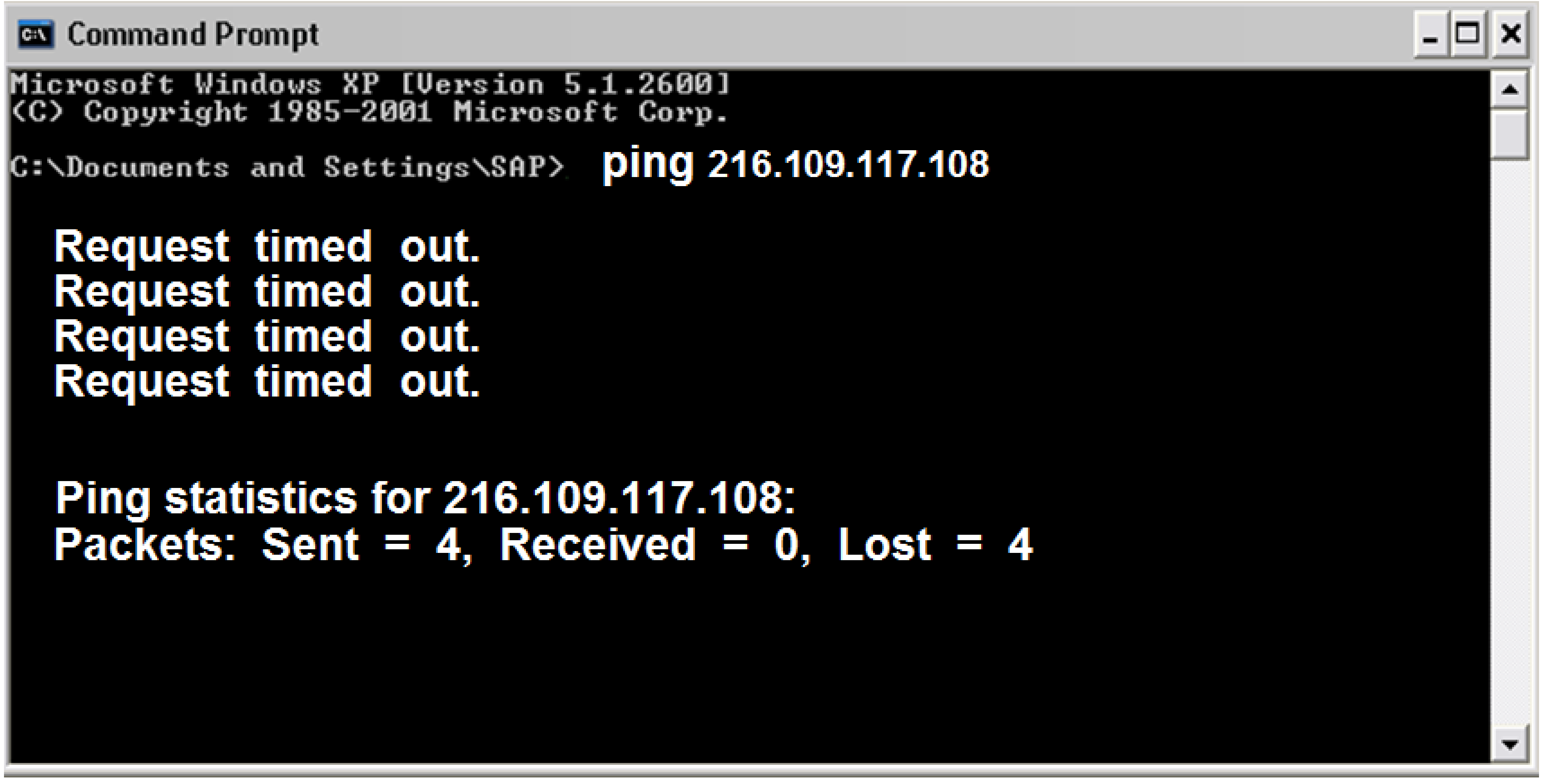
The **ping** command is the most widely used of all network utilities.  It's a tool that is used to test issues such as network connectivity and name resolution.  So, for example, to ping a host IP address, you would open up a command prompt and you would type the word 'ping', along with an IP address, and then press enter.  Then the ping utility will send out four data packets to the destination IP address you chose.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\SAP> ping 216.109.117.108

  Reply  from  216.109.117.108:  bytes=32  time=38ms  TTL=47
  Reply  from  216.109.117.108:  bytes=32  time=38ms  TTL=47
  Reply  from  216.109.117.108:  bytes=32  time=38ms  TTL=47
  Reply  from  216.109.117.108:  bytes=32  time=38ms  TTL=47


  Ping statistics for 216.109.117.108:
  Packets:  Sent  =  4,  Received  =  4,  Lost  =  0
```

**Successful ping.  4 packets sent and 4 packets received.**

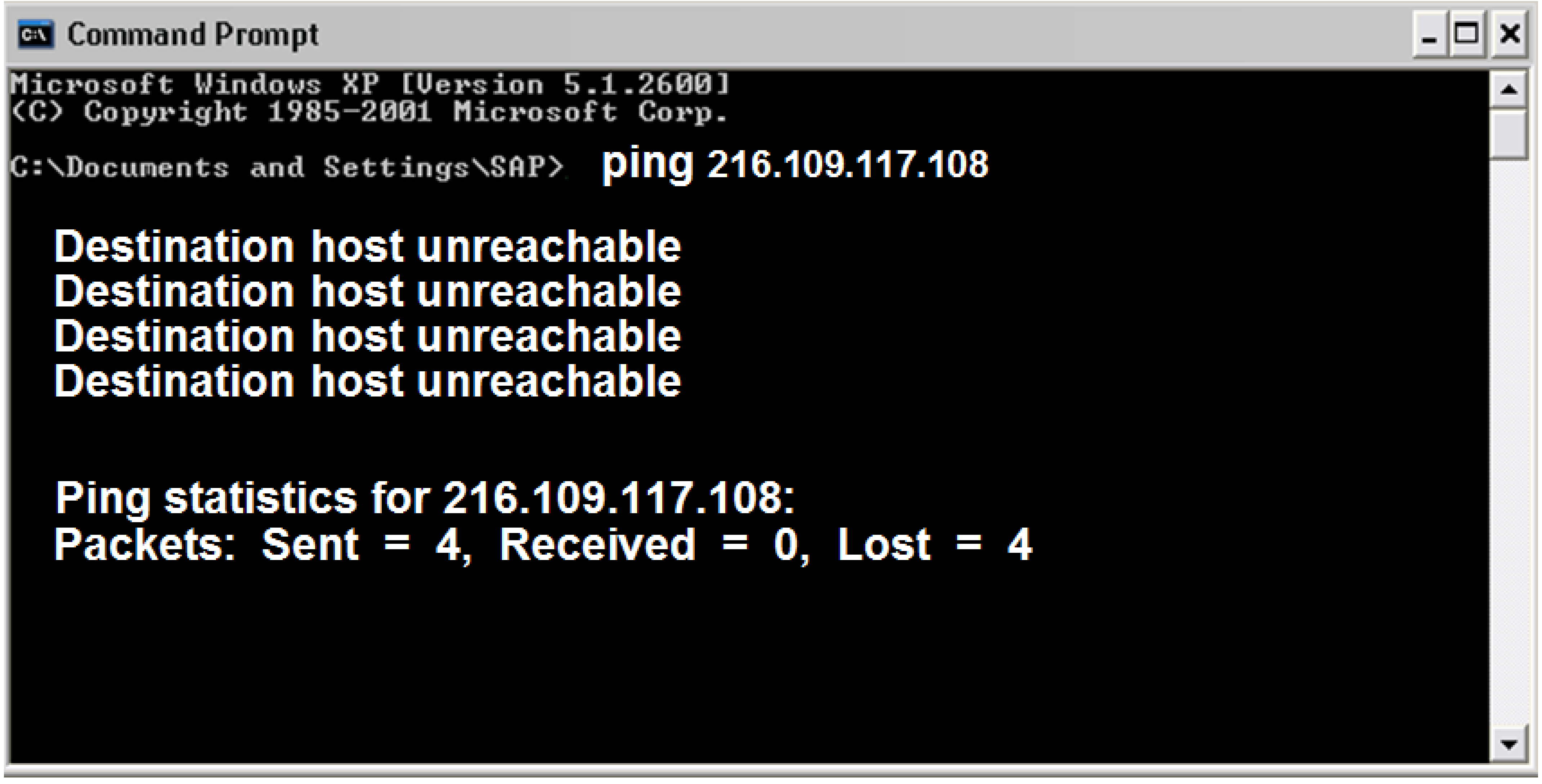
Then the destination will send the data packets back to us, as a reply.  These replies are called echo reply requests.  These replies inform you about what's happening with the destination host we pinged.  For example, if we received a reply then that means that there is general network connectivity between us and the destination.  But if we did not get a reply, then that means that there is no reply from the host and it could mean that there is no network connectivity between your computer and the IP address that you're trying to ping.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\SAP> ping 216.109.117.108

  Request timed out.
  Request timed out.
  Request timed out.
  Request timed out.


  Ping statistics for 216.109.117.108:
  Packets: Sent = 4, Received = 0, Lost = 4
```

**Unsuccessful ping. 4 packets sent and 0 packets received.**

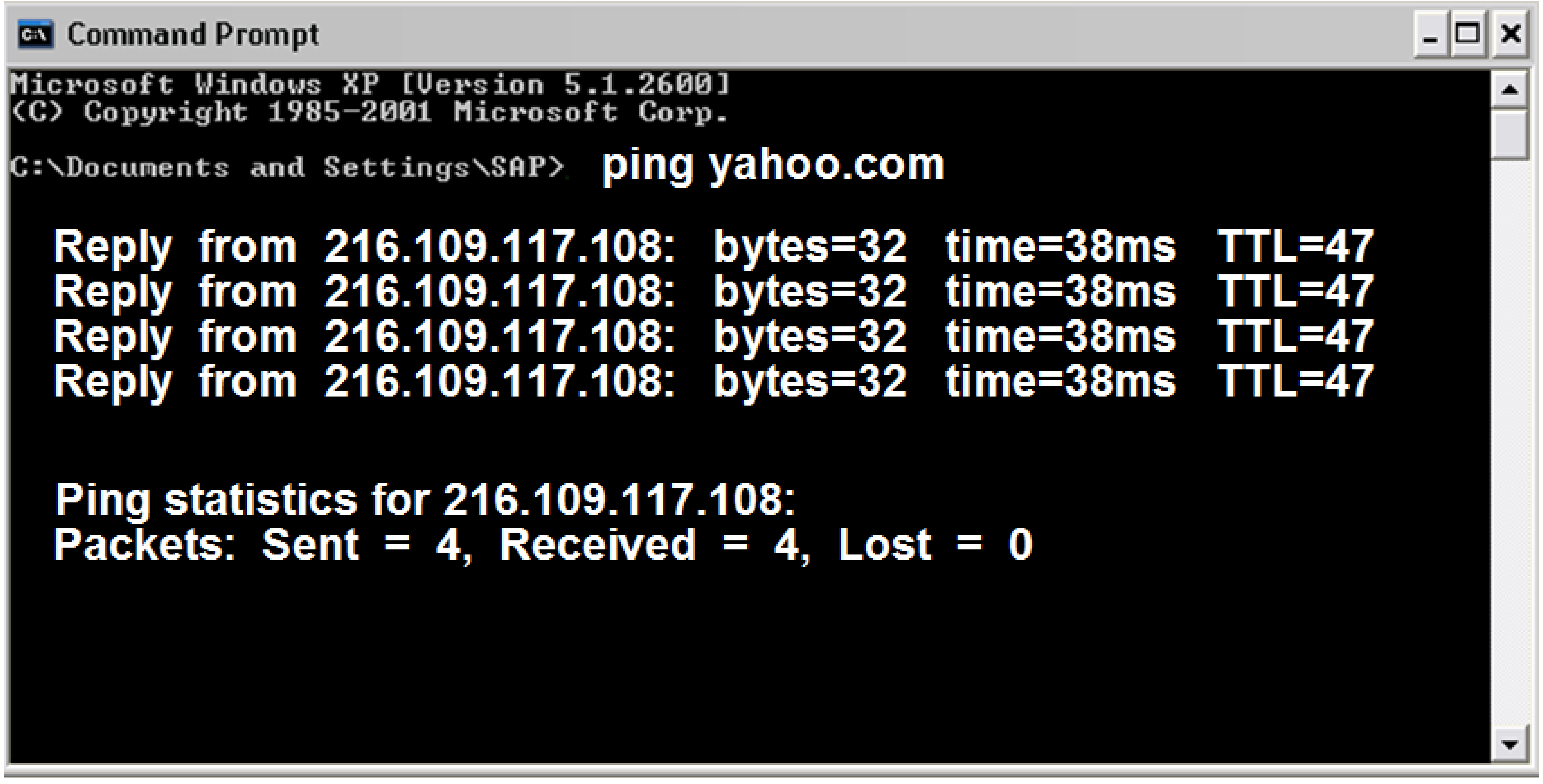
But if we pinged the host and we got a message that says 'request timed out', then that could mean that the host is down, or that it's blocking all ping requests. Or after we pinged, and we get a message that says 'destination host unreachable', then that message is coming from a router and it means that a route to the destination cannot be found.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\SAP> ping 216.109.117.108

  Destination host unreachable
  Destination host unreachable
  Destination host unreachable
  Destination host unreachable


  Ping statistics for 216.109.117.108:
  Packets: Sent = 4, Received = 0, Lost = 4
```

**Destination host unreachable means that the route could not be found.**

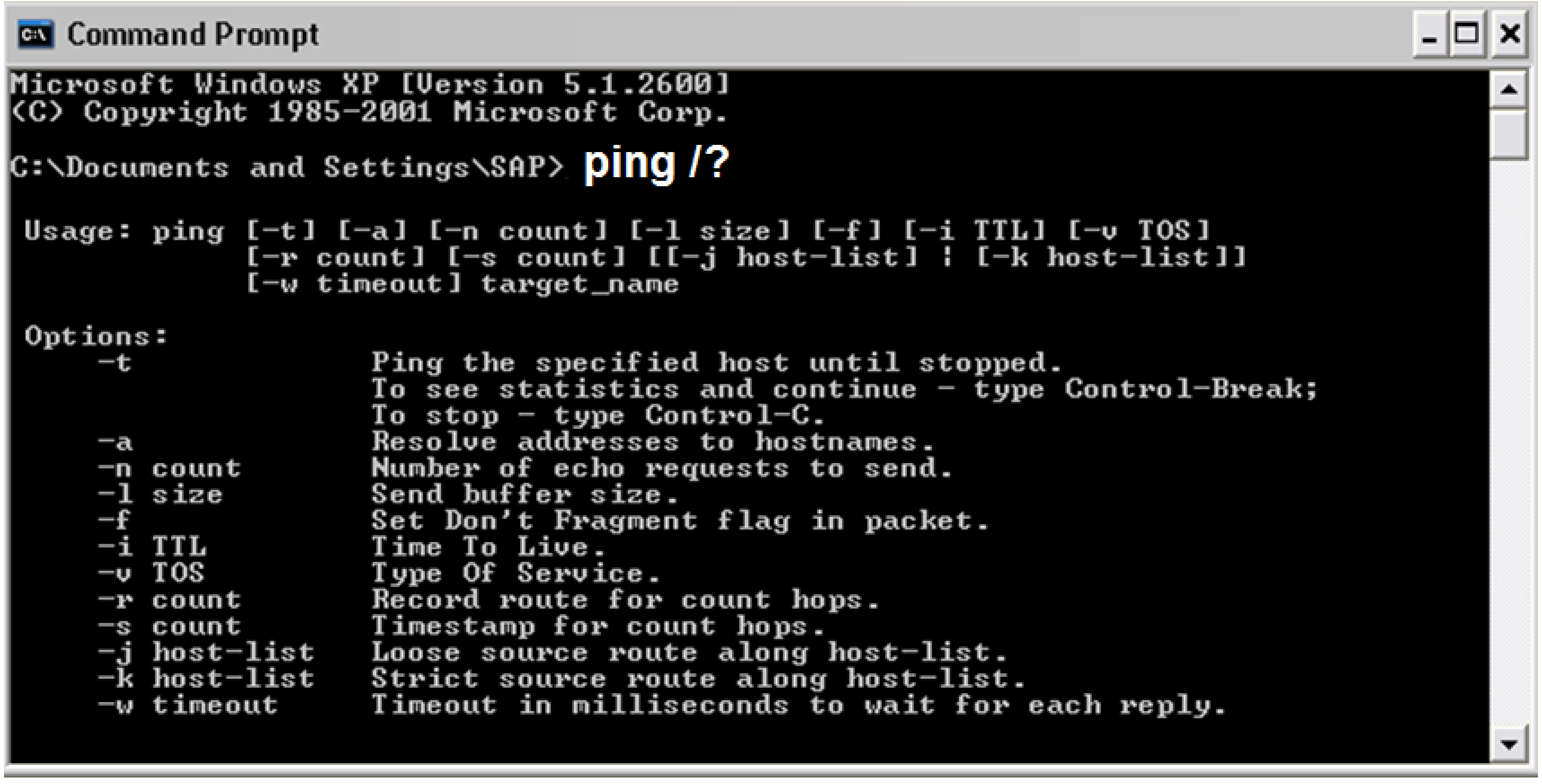
The ping command can also be used to test a DNS name resolution issues.  For example, before we used the ping command with an IP address, but we could also use it with a domain name.  For example, we could type 'ping' then the domain name 'yahoo.com'.  So if by pinging the domain name and if we got the same successful result by typing the IP address, then this would indicate that the name resolution by DNS is working fine.  But let's just suppose that pinging the domain name failed.  The next step will be typing the IP address instead.  So if by typing the IP address, and if the ping was successful this time, then we now know that we are having a problem with DNS.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\SAP> ping yahoo.com

  Reply  from  216.109.117.108:  bytes=32  time=38ms  TTL=47
  Reply  from  216.109.117.108:  bytes=32  time=38ms  TTL=47
  Reply  from  216.109.117.108:  bytes=32  time=38ms  TTL=47
  Reply  from  216.109.117.108:  bytes=32  time=38ms  TTL=47


  Ping statistics for 216.109.117.108:
  Packets:  Sent  =  4,  Received  =  4,  Lost  =  0
```

**Pinging domain names instead of IP addresses are used to test DNS issues.**

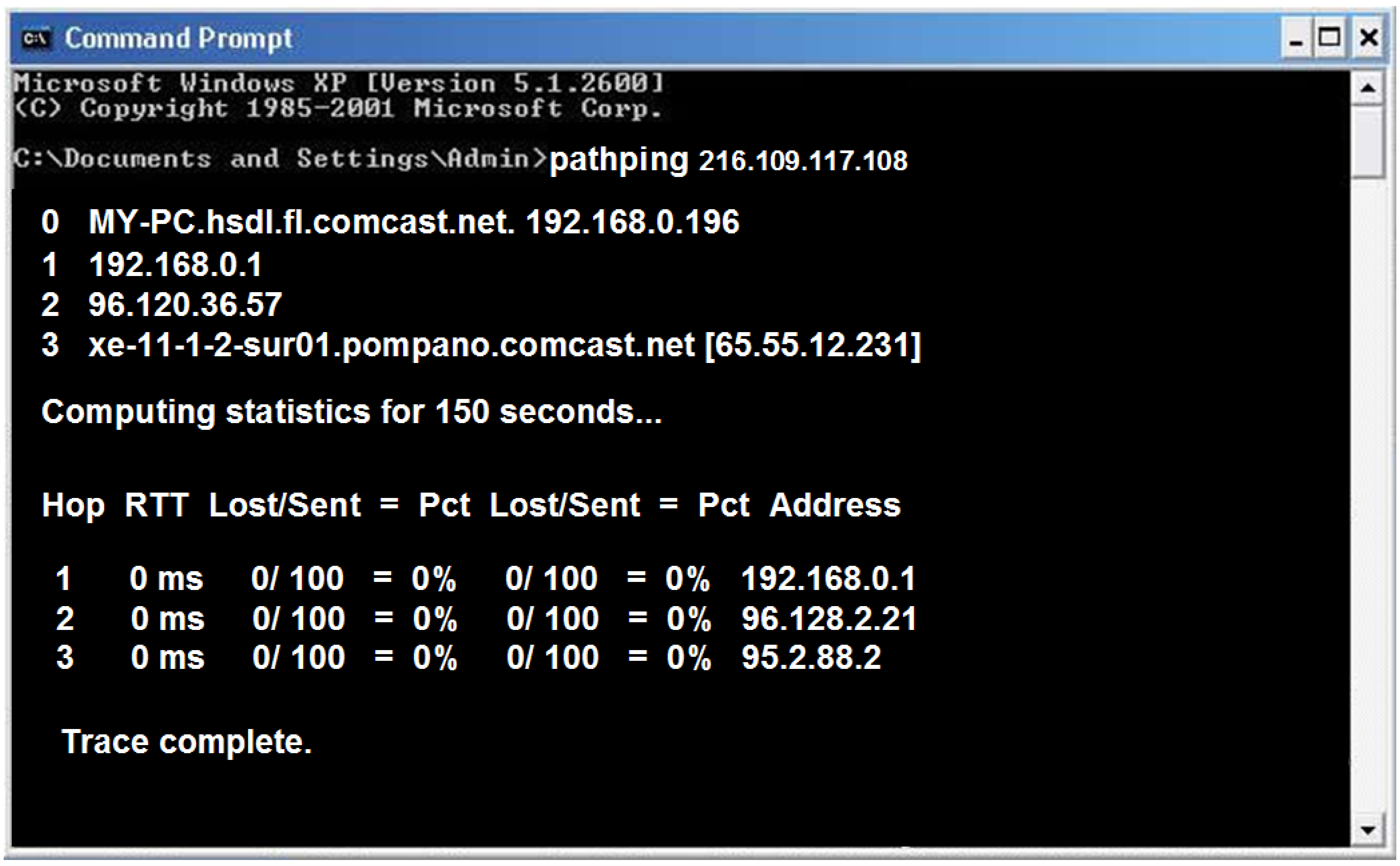
The ping command can also be combined with other sub commands called **switches**.  And switches are used to alter the parameters of the ping utility.  You can view a full list of these switches by typing **ping /?**



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\SAP> ping /?

 Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
             [-r count] [-s count] [[-j host-list] | [-k host-list]]
             [-w timeout] target_name

 Options:
     -t             Ping the specified host until stopped.
                    To see statistics and continue - type Control-Break;
                    To stop - type Control-C.
     -a             Resolve addresses to hostnames.
     -n count       Number of echo requests to send.
     -l size        Send buffer size.
     -f             Set Don't Fragment flag in packet.
     -i TTL         Time To Live.
     -v TOS         Type Of Service.
     -r count       Record route for count hops.
     -s count       Timestamp for count hops.
     -j host-list   Loose source route along host-list.
     -k host-list   Strict source route along host-list.
     -w timeout     Timeout in milliseconds to wait for each reply.
```

**The ping sub commands**

**Pathping** is another Windows network utility that combines the functionality of ping and traceroute.  So at a command prompt, just type 'pathping' and then the IP address or the domain name, and then press enter.  And the pathping output shows the details of the path a data packet takes between two devices.  It also gives ping like statistics for each device that the data packet takes on his way to its destination.

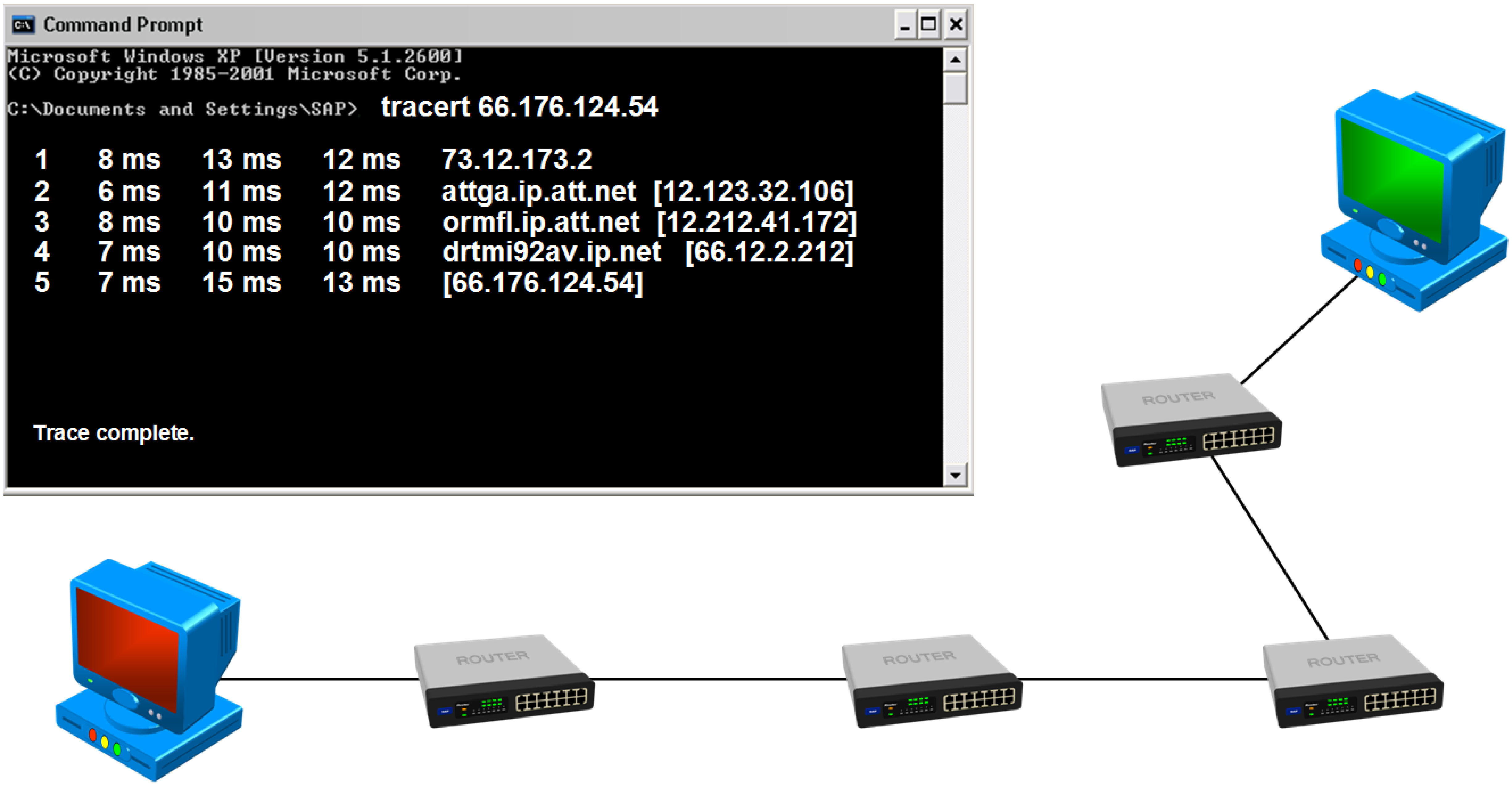


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Admin>pathping 216.109.117.108

  0   MY-PC.hsdl.fl.comcast.net. 192.168.0.196
  1   192.168.0.1
  2   96.120.36.57
  3   xe-11-1-2-sur01.pompano.comcast.net [65.55.12.231]

  Computing statistics for 150 seconds...

  Hop  RTT  Lost/Sent  =  Pct  Lost/Sent  =  Pct  Address

   1    0 ms    0/ 100   = 0%    0/ 100   = 0%   192.168.0.1
   2    0 ms    0/ 100   = 0%    0/ 100   = 0%   96.128.2.21
   3    0 ms    0/ 100   = 0%    0/ 100   = 0%   95.2.88.2

   Trace complete.
```

**Pathping output**

If you want to check a connection to a device that's on a LAN using the ping command, and if you fail to get a response because the firewall on that device has blocked all ping requests, you can use the **ARP ping** command instead.  The ARP ping command uses ARP data packets to ping network devices.  And since it uses ARP packets, a firewall will not block any ARP data because ARP data is never blocked or should we never blocked on a LAN.  It's also important to note that the ARP ping command cannot be used over the internet, because ARP data is not routable, it only works on a LAN.

Our next utility is called **tracert** which stands for a **traceroute**.  And this is used to find out the exact path a data packet is taking on its way to the destination.  So for example, let's go ahead and trace the route from our computer to another computer.

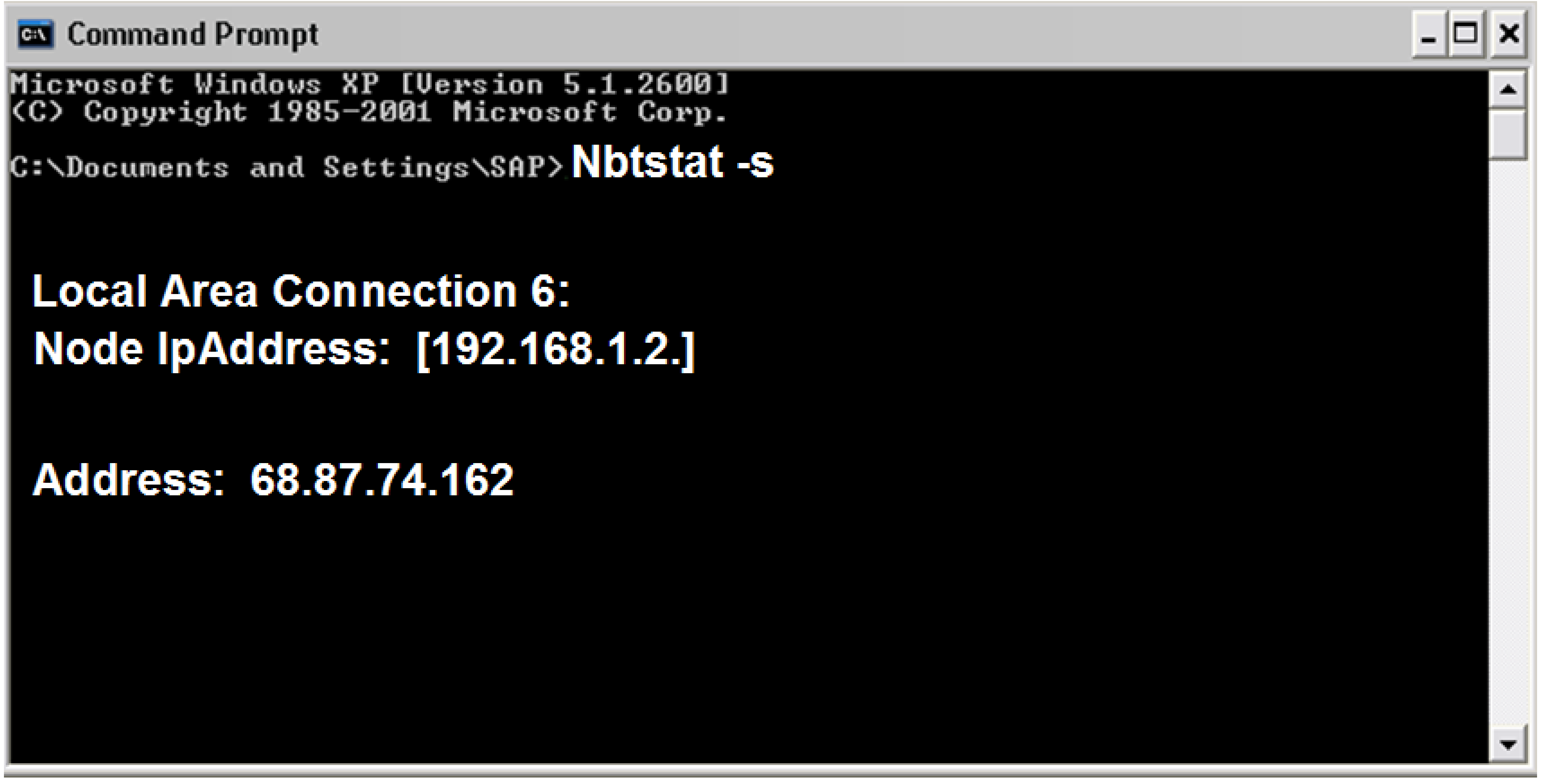


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\SAP>  tracert 66.176.124.54

  1    8 ms    13 ms    12 ms    73.12.173.2
  2    6 ms    11 ms    12 ms    attga.ip.att.net  [12.123.32.106]
  3    8 ms    10 ms    10 ms    ormfl.ip.att.net  [12.212.41.172]
  4    7 ms    10 ms    10 ms    drtmi92av.ip.net   [66.12.2.212]
  5    7 ms    15 ms    13 ms    [66.176.124.54]


Trace complete.
```

**Traceroute example**

So at a command prompt, we would type 'tracert' space and then the IP address and press enter.  Then the data packet will find its way to the destination, and each time it reaches a router on its path, it will report back information about that router, such as the IP address and the time it took between each hop.  So the tracert utility is a great tool that can be used to pinpoint where a problem lies on a network if the data packet cannot reach the destination.

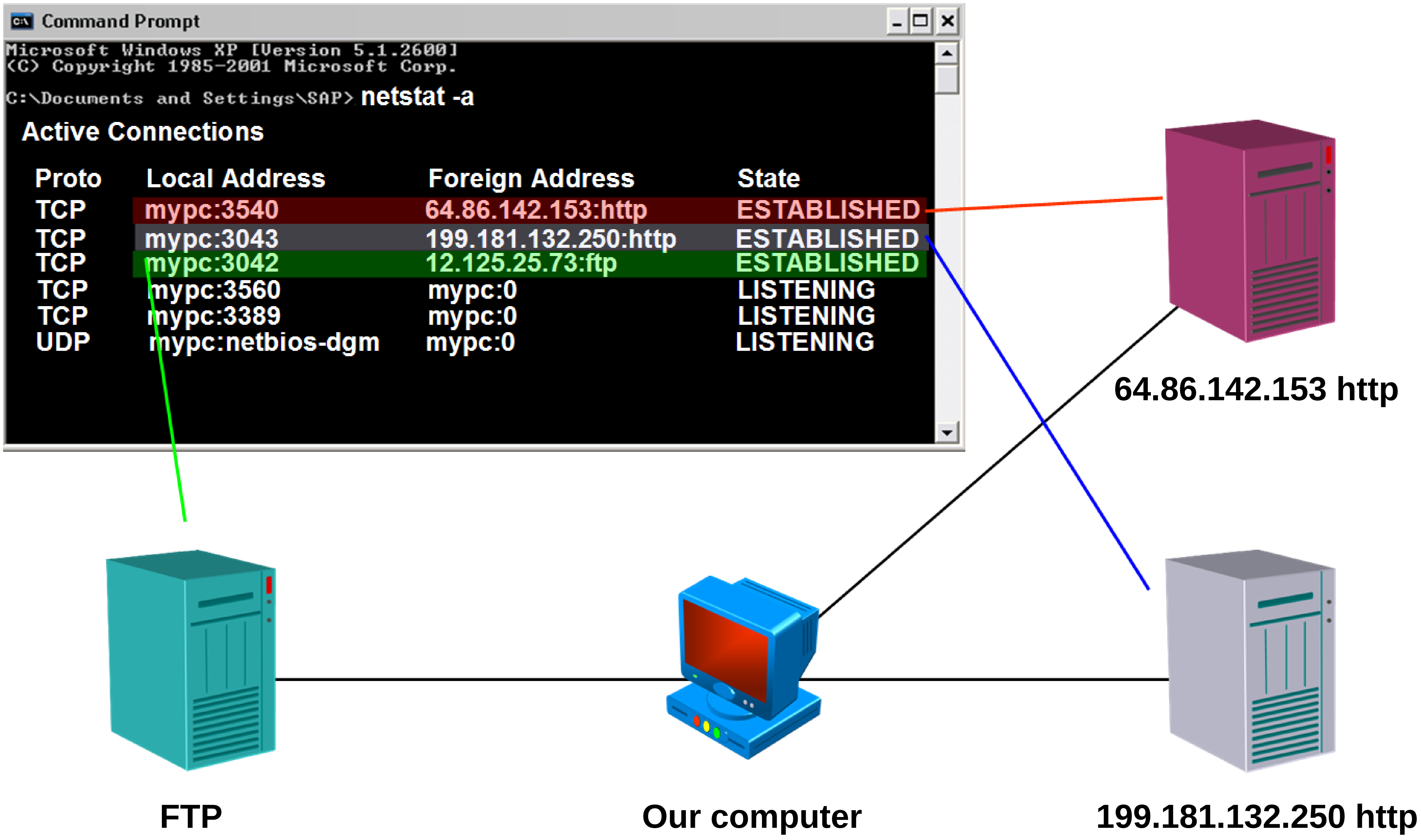
The **nbtstat** utility is used to resolve NetBIOS names to IP addresses.  So at a command prompt, just type in 'nbtstat' with a **-s** switch, and below is an example of the result.  The nbtstat utility is probably the least common utility that you would ever use.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\SAP>Nbtstat -s


 Local Area Connection 6:
 Node IpAddress:  [192.168.1.2.]


 Address:  68.87.74.162
```

**Nbtstat utility used with a -s switch**

Our next utility is called **netstat**.  Netstat is a very useful tool and it's used to display current network connections to your computer.  So in our example here, we can visually see that our computer is currently communicating with an FTP server, and two HTTP web servers.

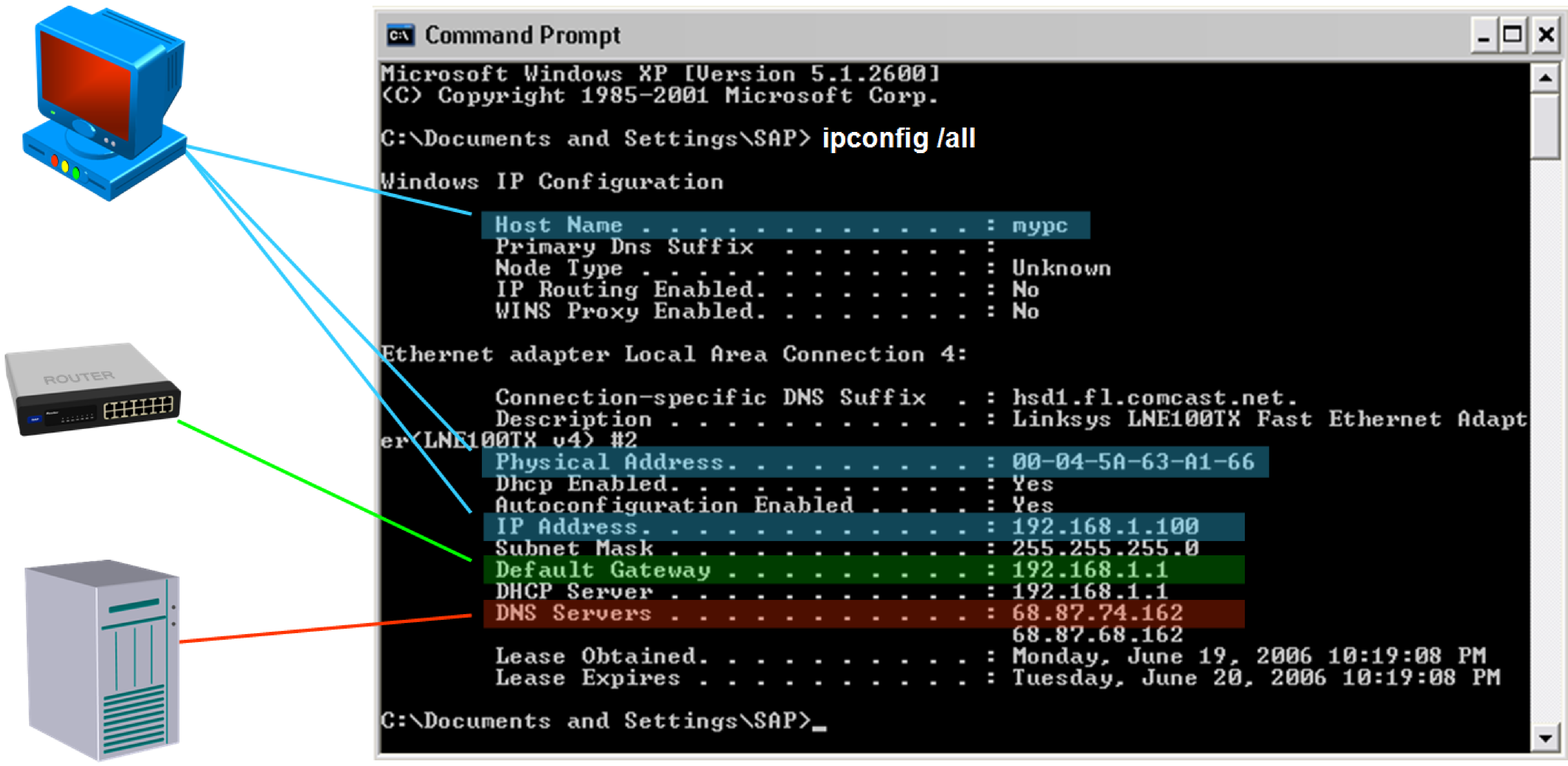


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\SAP> netstat -a
 Active Connections

  Proto   Local Address         Foreign Address          State
  TCP     mypc:3540             64.86.142.153:http       ESTABLISHED
  TCP     mypc:3043             199.181.132.250:http     ESTABLISHED
  TCP     mypc:3042             12.125.25.73:ftp         ESTABLISHED
  TCP     mypc:3560             mypc:0                   LISTENING
  TCP     mypc:3389             mypc:0                   LISTENING
  UDP     mypc:netbios-dgm      mypc:0                   LISTENING
```

**Netstat utility showing 3 current connections to our computer.**

And we can verify this by using the netstat utility. So at a command prompt, we type 'netstat', and in this case, we're going to use a **-a** switch, and then press enter. Now in our display above, we can see the two http servers and the FTP connection. So even if you're not sure what connections your computer currently has, you can use the netstat utility to find out. And in addition to connections, it also displays which ports are open and listening for a connection.

The **ipconfig** utility is very common. This utility is a powerful tool that's used to display the network configuration for our computer.  And this information can be used for problem-solving.  So for example, if we open up a command prompt and type in '**ipconfig /all**', this will display the full TCP/IP configuration for our computer.  Such as our computer name, MAC address, IP address, **default gateway** - which is the router, DNS servers, and so on.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\SAP> ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : mypc
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection 4:

        Connection-specific DNS Suffix  . : hsd1.fl.comcast.net.
        Description . . . . . . . . . . . : Linksys LNE100TX Fast Ethernet Adapt
er(LNE100TX v4) #2
        Physical Address. . . . . . . . . : 00-04-5A-63-A1-66
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DHCP Server . . . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . : 68.87.74.162
                                            68.87.68.162
        Lease Obtained. . . . . . . . . . : Monday, June 19, 2006 10:19:08 PM
        Lease Expires . . . . . . . . . . : Tuesday, June 20, 2006 10:19:08 PM

C:\Documents and Settings\SAP>_
```

**The Ipconfig utility can be used to display the full TCP/IP configuration for a computer.**

By using this information we can find solutions if we are experiencing problems.  For example, if we had a problem with our IP address, we can see from this information that DHCP is enabled, which means that this computer is getting its IP address from a DHCP server.  It also tells us the IP address of the DHCP server.  It also tells us the IP address of the DNS server.  So if we are experiencing any problems browsing the internet with domain names, then there might be a problem with the DNS server itself.

Using the ipconfig utility by itself displays the IP address, subnet mask, and default gateway.  But using this utility when combined with subcommands, called switches, changes the output slightly.  So for example, when we use **ipconfig /all**, which we just used in our previous illustration, displays the full TCP/IP configuration for our computer.  When we use **ipconfig /renew**, this releases and renews the lease of the IP address given to us from the DHCP server.  And **ipconfig /release**, releases the IP address, but does not renew it.

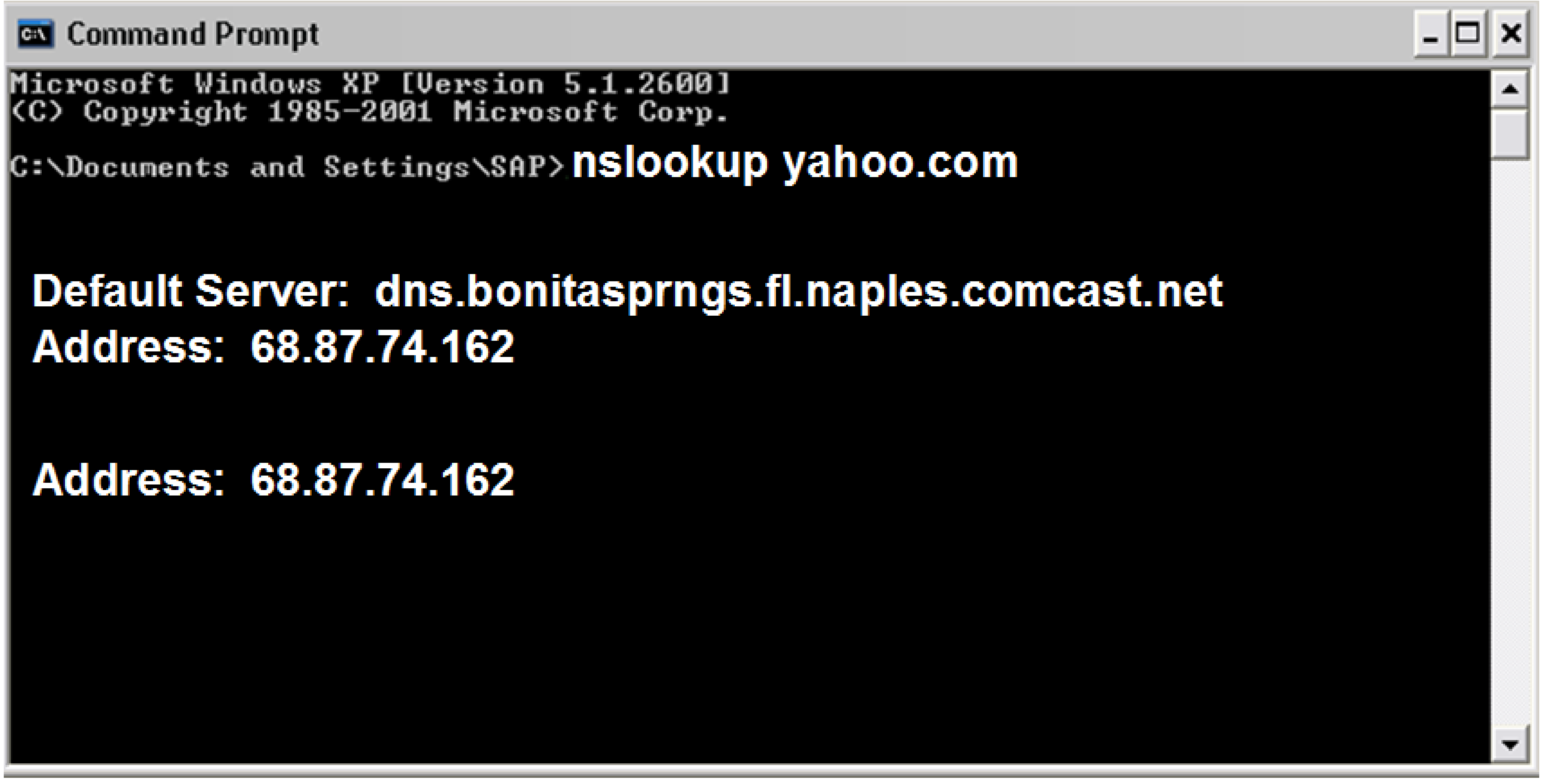
To see a complete list of all the switches that can be used with ipconfig or any command utility, just type the name of the utility along with a **/?** - and that'll show you all the switches that are available for that specific utility.

## Ipconfig /?

**Example of a utility using a subcommand to display all switches that are available.**

Similar to the ipconfig utility that used in Windows, there is also the **ifconfig** utility.  The ifconfig utility is a command that's used in UNIX and Linux operating systems.  It displays configuration information from the network interface card, such as the IP address, subnet mask, how many packets it has received and sent, any errors, and so on.  And like ipconfig, it can also be combined with switches to alter the output.

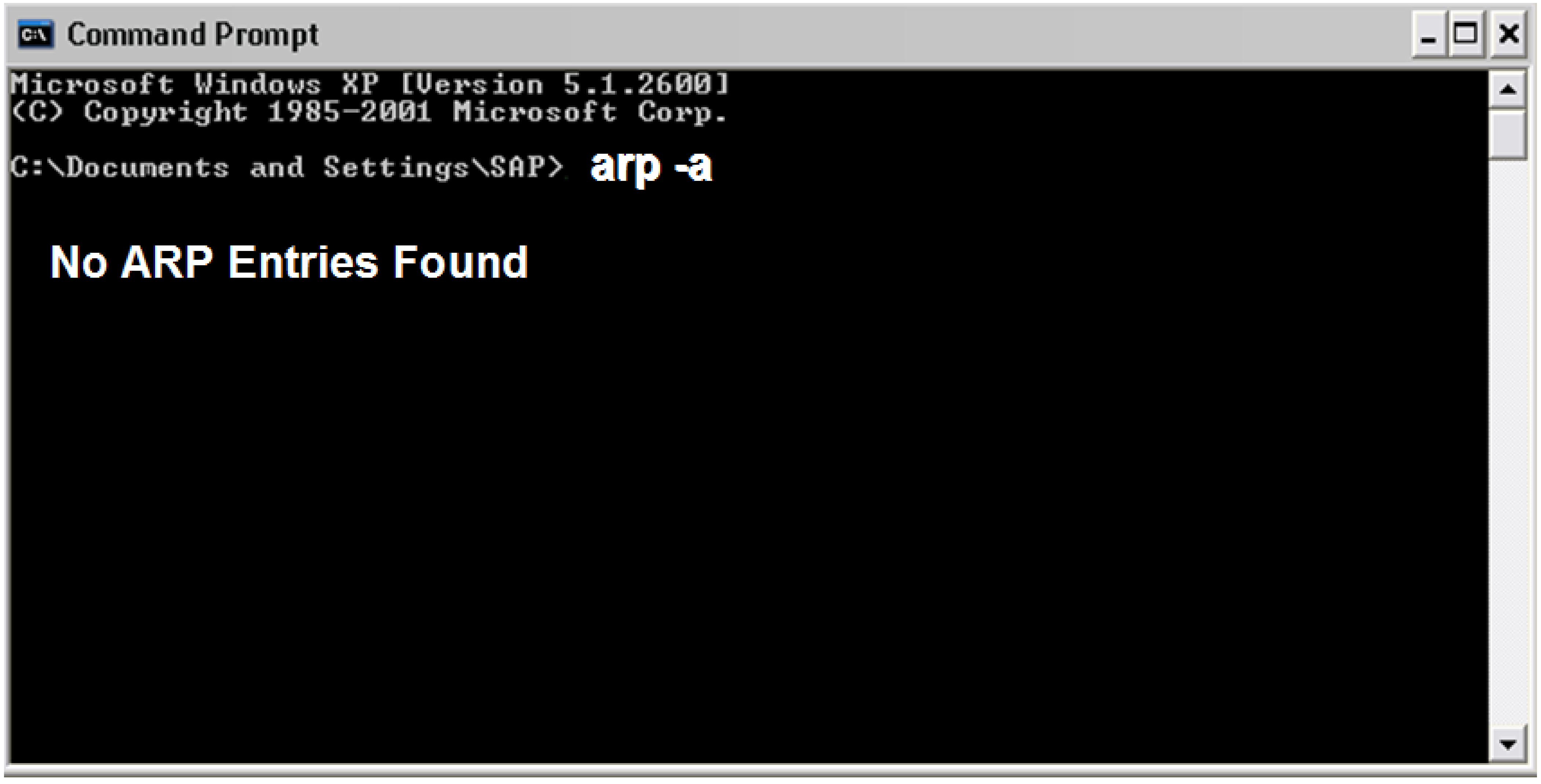
Our next utility is called **nslookup**.  This name is short for name server look up.  And this utility is used to look up DNS information. So for example, at a command prompt, if you type in **nslookup**, along with a domain name such as yahoo.com, the result will give you the information for the Yahoo domain. And the **dig** command is the UNIX version of nslookup. It does the same thing.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\SAP>nslookup yahoo.com


 Default Server:  dns.bonitasprngs.fl.naples.comcast.net
 Address:  68.87.74.162


 Address:  68.87.74.162
```

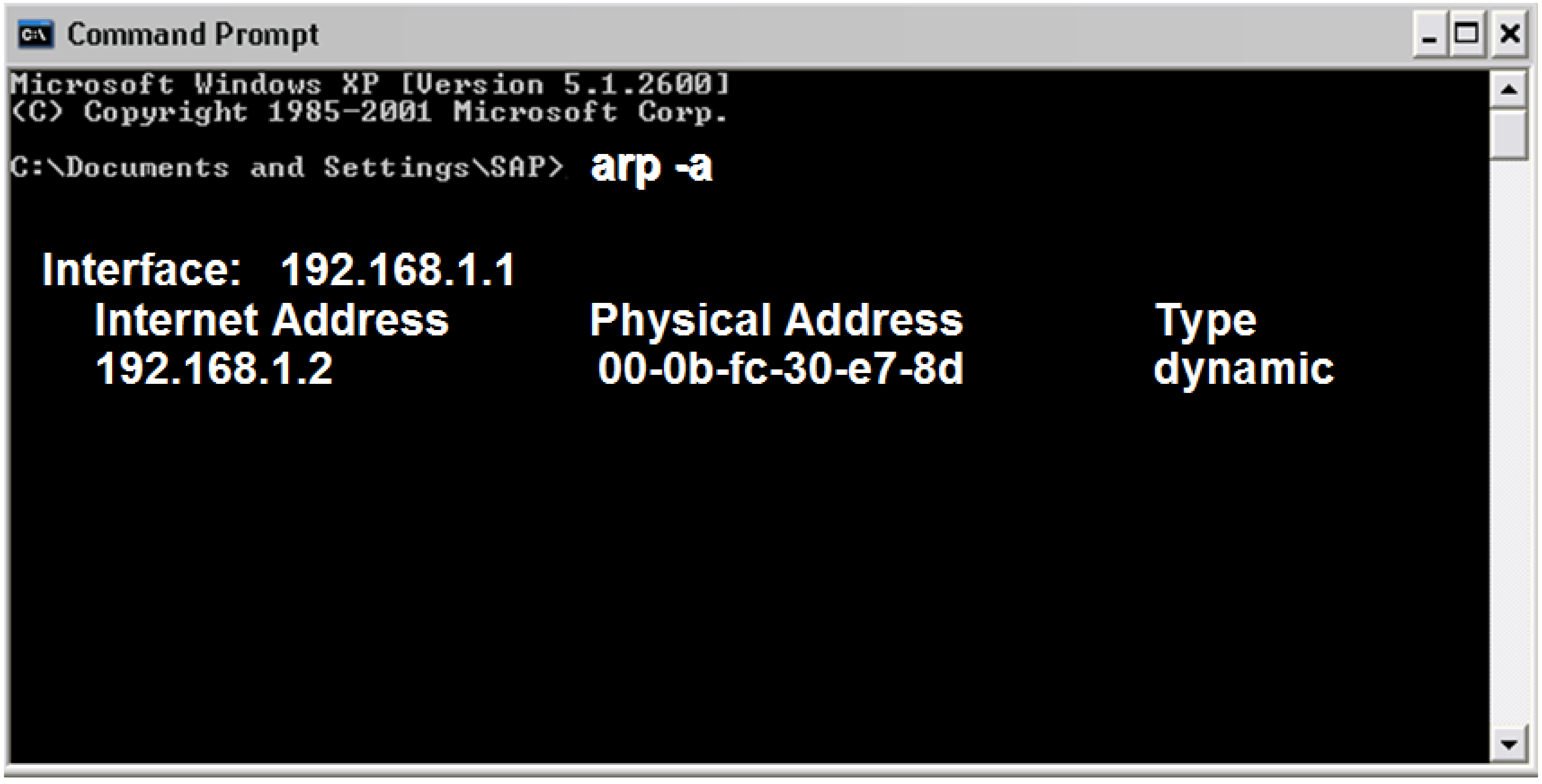
**Example of the nslookup utility**

Our last utility is called **ARP**. And as you might recall from an earlier lesson, ARP is used to resolve IP addresses to MAC addresses. In order for a computer to communicate with another computer, it needs to know the MAC address of that computer. So the first thing that the computer does is check its ARP cache to see whether it already has the MAC address for that computer. In fact, we can check this ourselves at a command prompt by using the ARP utility, by typing 'arp -a'. And as you can see in the output below, it has no entries at all.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\SAP> arp -a

  No ARP Entries Found
```

So, since there are no entries, if a computer wants to communicate with another computer, it will ask that computer, with the corresponding IP address, for its MAC address. Then once it has the MAC address it will store this information in the ARP cache. So let's do the same commands as before, and now you can see that the IP address and matching MAC address has been added to the ARP cache (below).

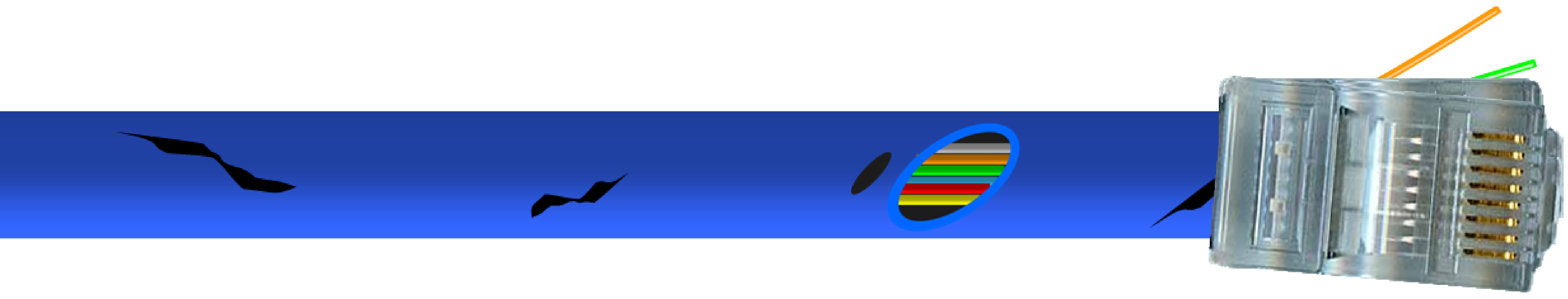


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\SAP> arp -a

  Interface:   192.168.1.1
     Internet Address          Physical Address          Type
     192.168.1.2                00-0b-fc-30-e7-8d         dynamic
```

So the ARP utility is a good way to manually check which IP address is associated with a certain MAC address.

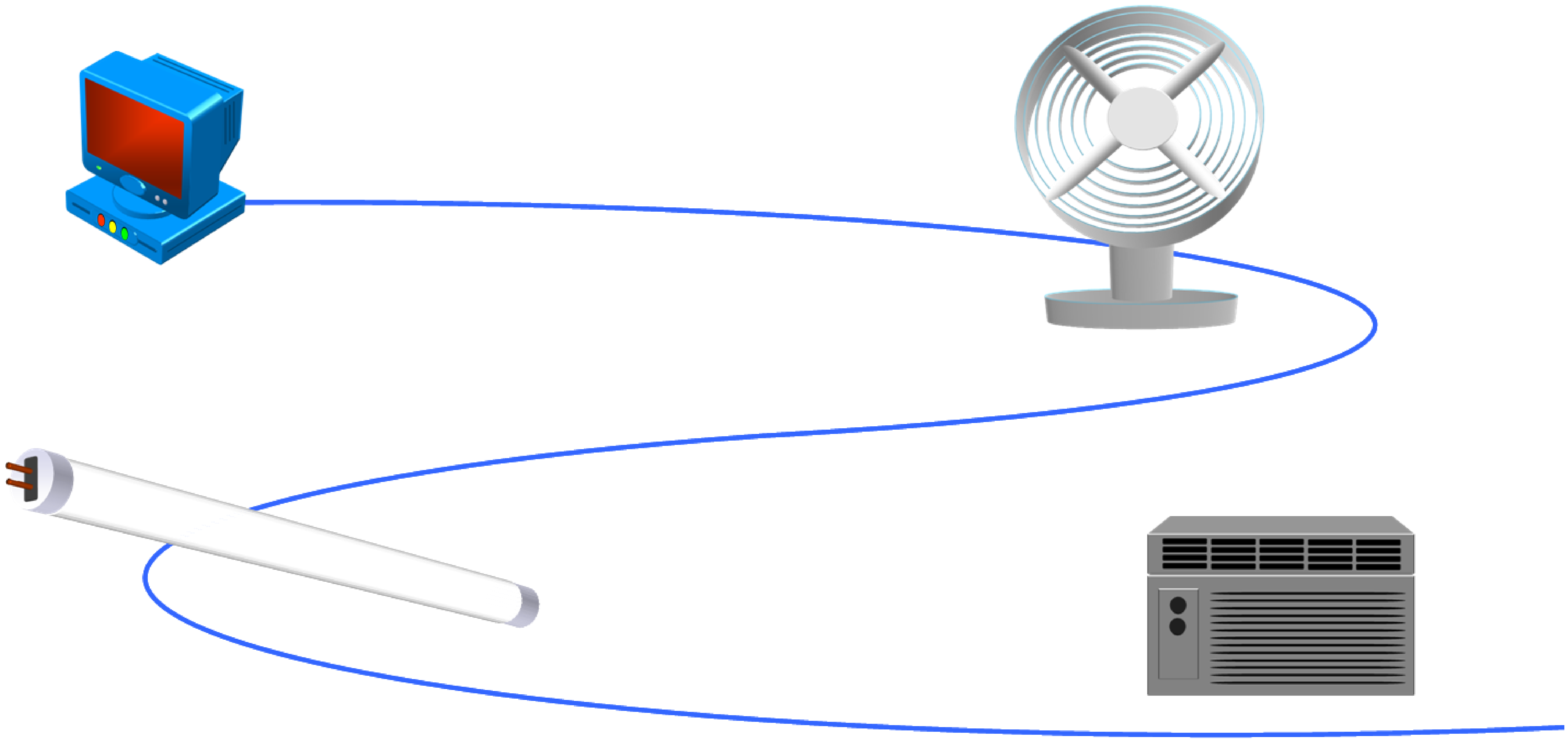
# Networking Issues

As far as the way a network is designed, there are two types: wired and wireless.  Networks don't have to use one or the other solely, but they can also be combined.  In fact, if you have a wireless network, at some point there is also a wired connection.  Most businesses today use a combination of wired and wireless networks.  So it's important to understand as a network administrator how to diagnose problems related to wired and wireless issues.  And one of those problems is media, and in a wired network, this involves copper cables.  Over time, cables can be worn out or damaged and that's when shorts can happen.



**Damaged cable**

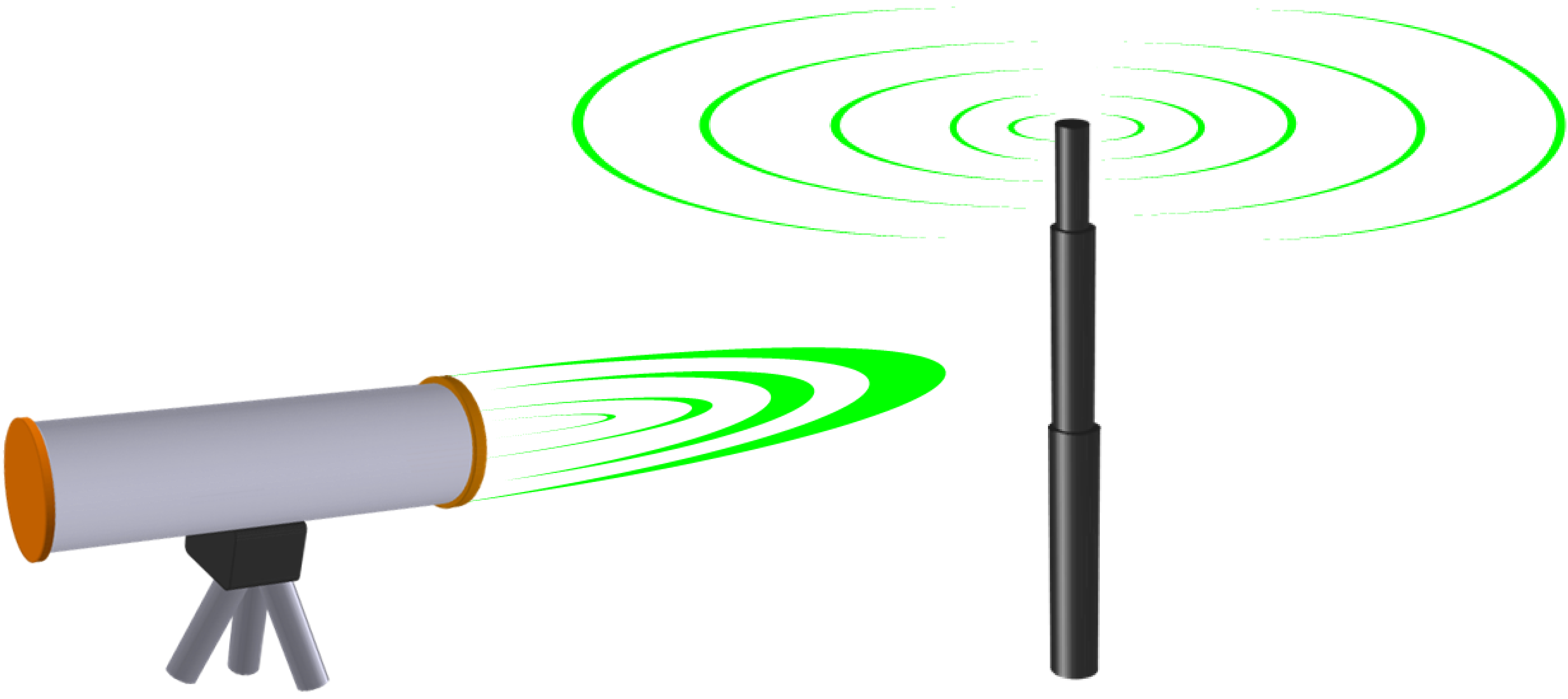
It's also important to remember to use the right type of cable depending on what kind of network you're using.  For example, if you are using copper cabling, it's important to recognize the environment around the cable.  This is because certain electronic equipment such as fans, fluorescent lights, or air conditioners, can interfere with the copper media and therefore alter or reduce the strength of the signal, which is known as **attenuation**.



**Fans, fluorescent lights, and air conditioners can alter the strength of a signal.**

Another factor is the length of the cable.  If the cable exceeds the maximum recommended length, then this could also cause a problem.  Or, if you are using the wrong type of cable.  For example, if you are using a crossover cable when you should be using a straight cable.

Antennas are a factor that affects a wireless signal. Since wireless devices operate using radio waves, the antenna is a big factor that can determine the range and speed of a signal.  One type of antenna is the **omni-directional antenna** and this happens to be the most common type as well.  This type of antenna transmits a signal in all directions.  So every wireless device in all directions can pick up the signal as long as they're in range.  Another type of antenna is the **directional antenna**.  This type directs the signal in one direction, and that direction is wherever you point the antenna to.



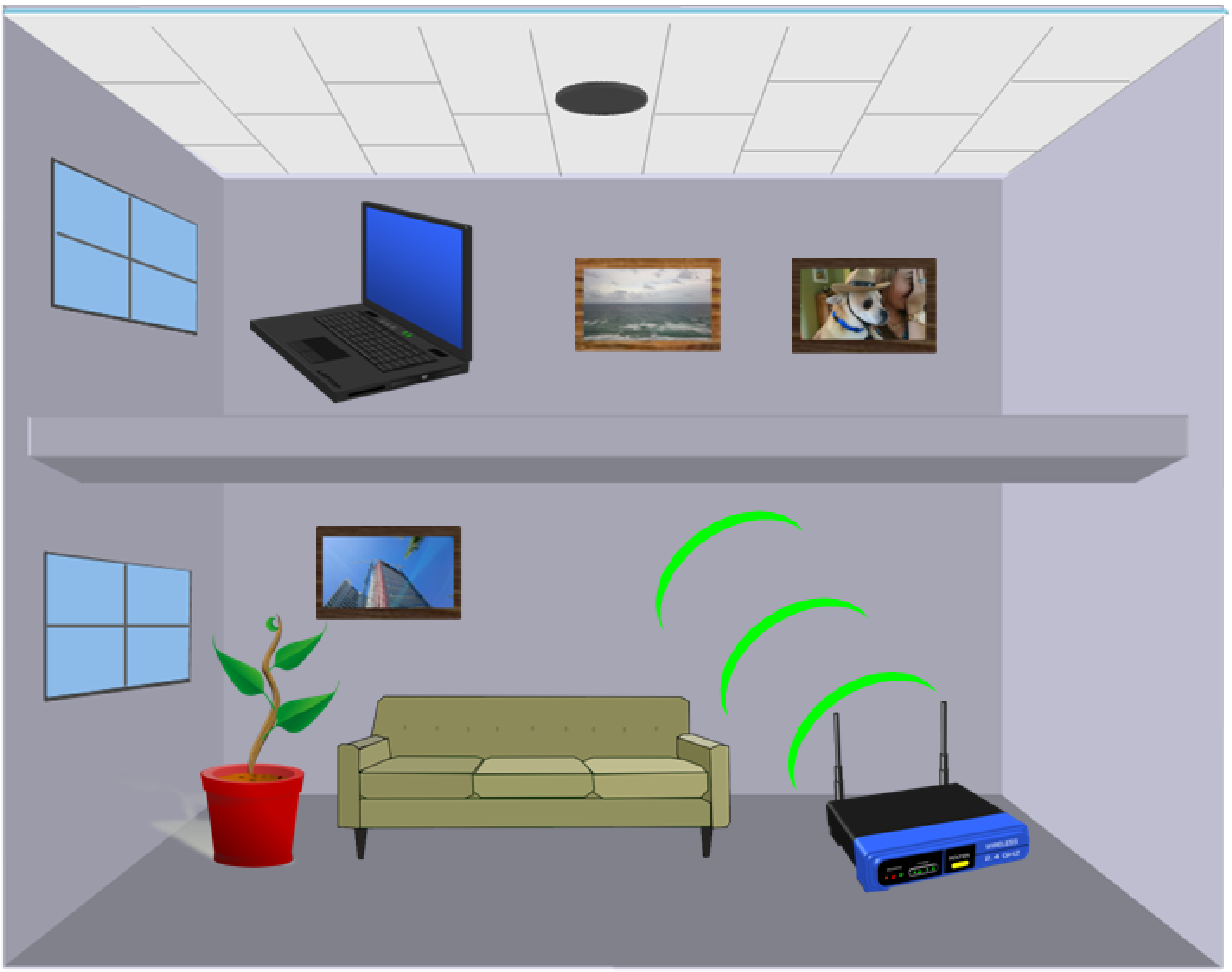
**Directional antenna** **Omni-directional antenna**

Another problem that can happen in a wireless environment is **interference**.  Microwave ovens can cause interference.  And certain wireless devices can also, such as cell phones and bluetooth devices, such as wireless keyboards and mice.  The waves that are produced by these devices can alter the signal of a wireless network.

**Cordless phone**

A cordless phone is another device that can interfere with a wireless network.  This is because a lot of cordless phones operate at the same frequency as wireless routers, which is at 2.4 GHz.  In fact, I had a situation one time where one of my customers was complaining that every time her phone rings, she would lose internet connection on her laptop.  This is because her cordless phone and her wireless router we're using the same wireless channel. So, to quickly resolve this issue, I just logged into the router's configuration page and changed the channel on her wireless signal, which quickly solved the problem.

The structure of a building is another factor that can affect a wireless signal.  Depending upon the structure of the building, like concrete walls, window film, and metal studs, these can all affect wireless signals.  So, in this case, you may have to consider where you are placing your wireless router to avoid these kinds of structural interference issues.  You may have to test out certain areas in your home or office to make sure that all your devices can use your wireless network.



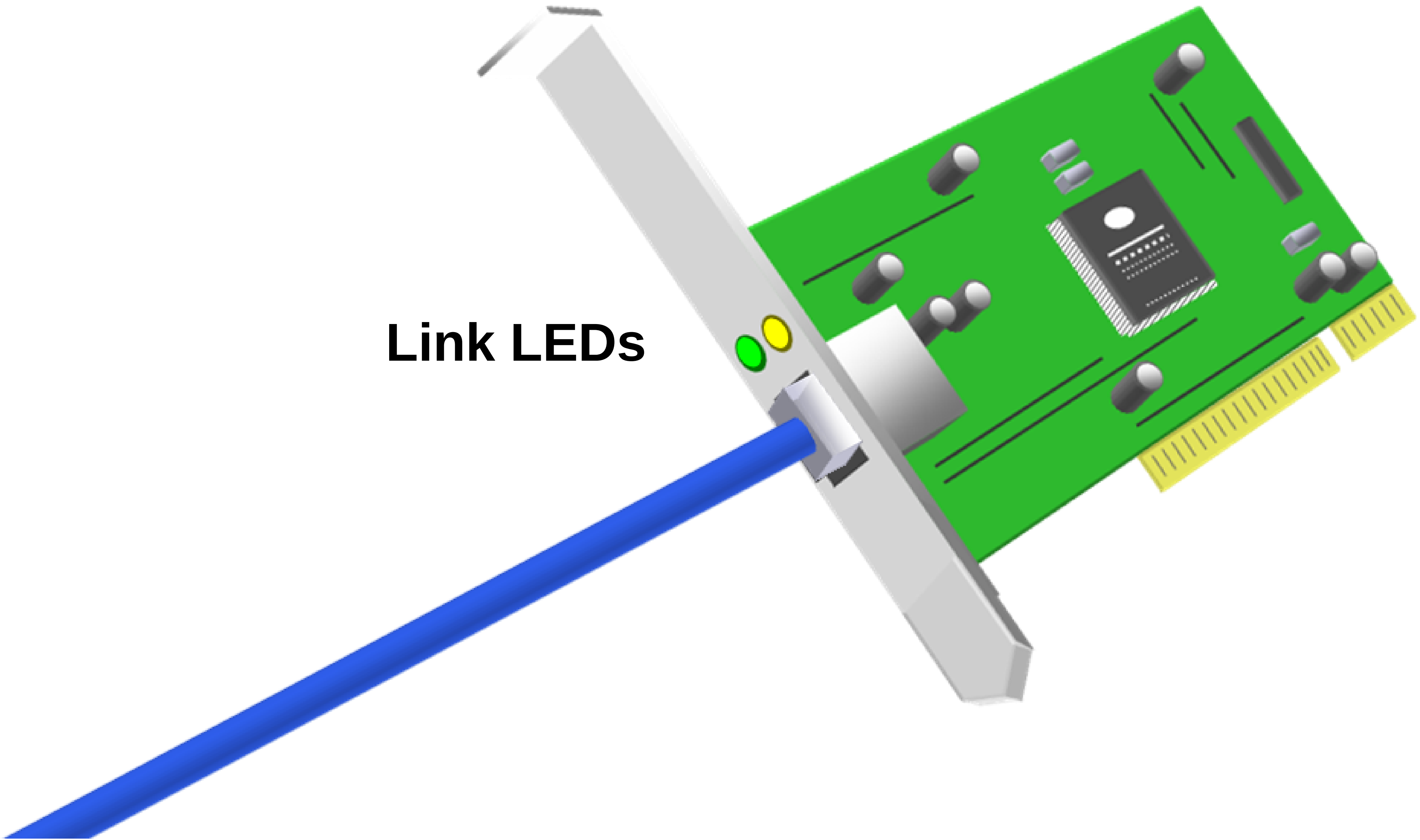
**Building structure can affect a wireless signal.**

Another factor that could cause issues in a wireless environment is using the **wrong encryption**.  Using the wrong encryption could prevent certain wireless devices from joining your network.  For example, let's say that a wireless router was using a modern wireless encryption method such as WPA2.  Now, this would be no problem for modern laptops joining the network, but for older laptops that can only use WEP or WPA, well then those laptops wouldn't be able to join the wireless network because the router is using a modern encryption method that the older laptops cannot recognize.

Similar issues can happen in fiber-optic networks as well, such as signal loss or attenuation.  Other factors include using the wrong type of cable, wavelength mismatches, fiber type mismatches, dirty connectors, connector mismatches, bending the cable too much, and exceeding the cable length limitations.

Problems can also happen if there was a **DNS issue**. And as we discussed earlier, DNS resolves domain names to IP addresses.  The main impact that this service would have on a network if DNS was not working properly, is basically accessing web pages using domain names.  For example, yahoo.com would be resolved to an IP address by a DNS server.  But if a DNS server was not present, you would not be able to access the yahoo website using the domain name yahoo.com.  You would only be able to access the yahoo website by typing in the IP address instead.

**Link LEDs** are very simple indicators that are used to tell us basic information about a network device.  For example, on a network interface card.  If you were to plug in a network cable, you would notice that the green LED turns on.  The green LED is called the link light and this indicates that there is a successful network connection.



However, if the LED does not light up after a cable is plugged in, then this indicates a problem, such as a bad cable or something simple like maybe the computer is turned off.  The blinking yellow LED, on the other hand, indicates that there is network activity happening. Whether the blink rate is fast or slow, this indicates normal operation.

Another issue, and probably the most obvious to check, is physical **connectivity**.  Is your computer connected to the network?  If it is, is the link LED on the network card turned on?  Or, is the cable that you are using good?  So, if you do not see the link LED and you know that the cable is good, then you might want to check the switch.  Is the switch turned on?  Are there any LEDs on the switch?  You might also want to check if the network cable is loose on either the NIC or on the switch.

# Troubleshooting Steps

There are certain procedures for solving network problems and here are some of the steps to do that.  So the first step is:

- **Identify the symptoms and potential causes.**

This step is where you gather information about the problem, such as what exactly is the problem, when did the problem occur, were there any specific error messages, and does it happen all the time or intermittently.  By gathering as much information as possible in the beginning it'll greatly enhance the diagnosing process and ultimately fixing the problem a lot faster.

The next step is to:

- **Identify the affected area**

A good question to ask would be, is the problem isolated at one particular location or is it spread across several locations?  For example, let's say that everyone on a LAN cannot access the network.  So one of the first places to look would be the switch, because we all know that all computers connect to this single device and if this device was not working properly, it would affect everyone.  Or what if the problem was isolated at one particular computer?  Then, in this case, we would not check the switch, but a good place to start, is to check the cable and connection for that particular computer.  When this step is done correctly it will dramatically cut down on the diagnosing process and save a lot of time.

So after you identify the affect area, the next step is to:

- **Establish what has changed.**

Problems don't occur at random. They happen for a reason. So the next questions to ask are: Did anything change just prior to the problem happening? Was there any hardware removed or added? Was there any software installed or uninstalled? Or did the user download anything?

- **Select the most probable cause.**

Try to keep this step simple. Always look for the simple and the obvious solutions before digging deeper. For example, checking if the computer or device is even turned on. Check to see if the cables are plugged in and check the simple LEDs. You'll be amazed how the simplest solutions will fix most network problems.

- **Implement an action plan and solution, including potential effects.**

This step is the cautious phase. So before taking any action to solve the problem, you must know what effect this will have on the network. For instance, if you were to take a device offline, how will this affect the rest of the network? Another question you should consider is, will doing this action affect everyone else or will it be isolated in one area?

- **Test the result.**

This step is where you actually take action to solve the problem. This is where you would know if your plan of action has solved the problem or not.

- **Identify the results and effects of the solution.**

Has your plan of action solved the problem or not?  If it has, what effect did it have on everyone else?  Do the results show a temporary fix or a permanent one?

- **Document the solution and process.**

This step is a very important one.  Now that the problem is solved, it's very important to document the problem and the solution so that if it ever happens again, you and everyone else will know not only how to solve the problem as fast as possible, but also to take preventive measures so that the problem will never happen again.  So the things to include in the documentation are:

- The problem itself.
- What actually caused the problem.
- How did you fix the problem.

By following all these steps carefully, you can be assured to diagnose and solve problems effectively as a network administrator.