Level 3 I.T Solutions
A Top Down Approach
ACL Brentwood

Daniele, Della Cioppa

daniele.dellacioppa@gmail.com

May 31, 2022

Contents

Part I

Networking

Chapter 1

The basics of Networks

In this article we spend some words to introduce the reader to the world of networking trying to cover all the most important aspects to the best of my knowledge. In the first chapter

1.1 What is a network?

A network is two or more computers (or other electronic devices) **connected** together, usually by cables(**guided**) or Wi-Fi(**unguided**).

1.1.1 Network benefits

1. sharing hardware, such as printers, computers, phones, tablets, scanners, etc...[1]

2. sharing software, allowing:

   - multiple users to run the same programs on different computers

   - data to be shared, so that other people can access shared work

   - you to access your data from any computer on the network

Networking is crucial if you want to use your computer to communicate. Without it you couldn't send an email, a text or an instant message and that would be so weird in 2022 isn't it?

We use a huge network on a daily basis and this is called the internet. Around 5 billion[2] people use the internet to share data, news and resources, amongst many other things.
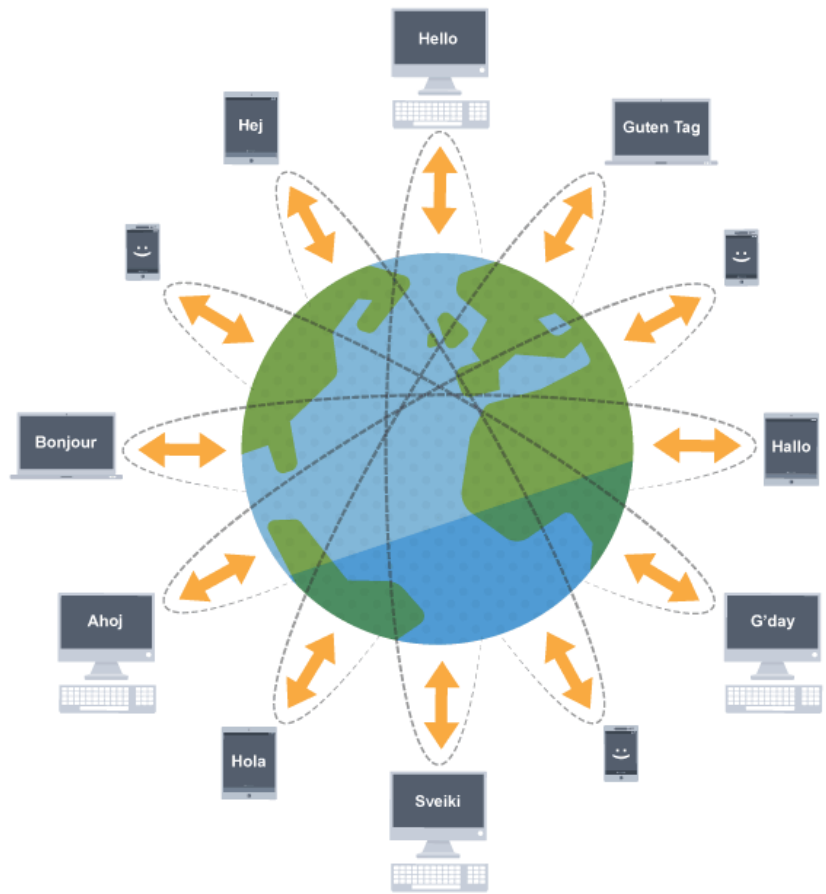

Figure 1.1: devices connected in the world

---

[1] All these pieces of hardware are usually addressed as **endpoints** as long as they have the ability to communicate effectively within a network

[2] Oberlo statistic.

1.1.2   GUIDED WIRING

Is quicker than unguided, it consists in physical wires. Optic Fiber is on the top of this list but can't be twisted or the light will bounce back. You can install an optic cable for a much longer distance and you won't get the same troubles you would get with copper cables for example. But no twisting or it'll bounce back!

1.1.3   UNGUIDED WIRING

The term wiring can be deceiving here as there are literally no wires involved to realize the connection. In Cantonese is probably much clearer (Figure 1.2).

Unguided wiring simply means Wi-Fi really. You can have a 2.4Ghz signal to reach longer distance but won't be nicely matched with a 5Ghz device. A 5Ghz device won't reach the same distance as a 2.4Ghz. Take a look how it's worded in Cantonese and you'll see a different etymological meaning from the English one[3] but still both words suggest the idea that no wires are involved.

FIGURE 1.2: Definition of WiFi in Historical Chinese commonly spoken in Hong Kong

The first character represents the concept of **not** having (mou^4). The second one (sin^3) is literally thread or line so that's why wiring to me is sort of misleading. If you ask a person :

Can you tell me what unguided wiring means?

Because of the word wiring one could start thinking about a particular kind of special fancy wire. But wires are the last thing you'll ever see in the case of **unguided wiring**

FIGURE 1.3: Cantonese characters in the WiFi word

1.2   LAN VS WAN

LAN, which stands for **local area network**, and WAN, which stands for **wide area network**, are two types of networks and `as the naming conventions suggest`, LANs are for more localized networking[4] while WANs cover larger areas, such as cities, and even allow computers in different nations to connect. LANs are typically faster and more secure than WANs, but WANs enable more widespread connectivity. Of course there are sort of exceptions like the NHS having a huge Local Area Network spread all over the country with local IP addresses starting in the first octet with 10 instead of 192, thus using a Class A Address rather than a Class C (more on this topic in the Section called **The Five IPv4 Classes**)
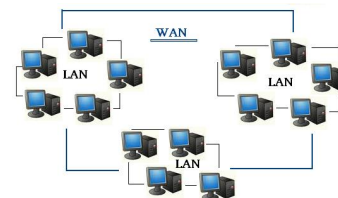
FIGURE 1.4: difference between WAN and LAN

---

[3] stands for Wireless Fidelity.It kept this name for a short time after the brand name was created by the Wi-Fi Alliance.

[4] in a home,business,school,etc.

Chapter 2

Standards and Protocols

Here we will discuss about protocols and standards

2.1   IEEE 802.3

IEEE 802.3 is a set of standards and protocols that define Ethernet-based networks. Ethernet technologies are primarily used in LANs, though they can also be used in WANs as well.

IEEE 802.3 defines the physical layer and the medium access control (MAC) sub-layer of the data link layer for wired Ethernet networks. The unique identifier of our computer's motherboard is actually adhering to a standard defined by IEEE 802.3. The psysical layer is the lowest layer identified in the TCP/IP protocol or the ISO/OSI protocol. The packets on the network before they finally go to destination they need to know which MAC address corresponds to the IP they hold already in the headers. In the next paragraph we'll explain the different cables in Figure 2.1.
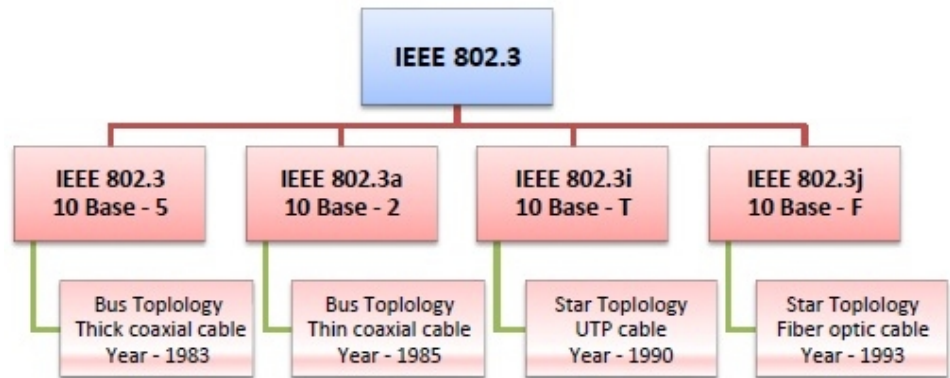
Figure 2.1: IEEE cable hierarchy

2.1.1   POPULAR VERSIONS

There are a number of versions of IEEE 802.3 protocol. The most popular ones are:

- IEEE 802.3: This was the original standard given for coaxial (10BASE-5). Here, 10 is the maximum throughput which means 10 Mbps and 5 refers to the maximum segment length of 500m. If it goes longer than 500m there's no guarantee it'll work

- IEEE 802.3a: This gave the standard for thin coax (10BASE-2), which is a thinner variety of coaxial cable. The 2 refers to the maximum segment length of about 200m (185m to be precise)

- IEEE 802.3j: This gave the standard for Ethernet over Fiber (10BASE-F) that uses fiber optic cables as medium of transmission

2.2 Protocols

Protocols are kind of rules defined in advance to make sure two or more devices know in advance what to expect if they send a particular message and what to expect in return

2.2.1 OSI Standard

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network. It was the first standard model for network communications, adopted by all major computer and telecommunication companies in the early 1980s

The modern Internet is not based on OSI, but on the simpler TCP/IP model. However, the OSI 7-layer model is still widely used, as it helps visualize and communicate how networks operate, and helps isolate and troubleshoot networking problems.

2.2.2 A good Mnemonic

One way to remember the OSI Layer is, as always, by using funny and silly stories but this time we won't be talking of italian clichés, mentioning videogames monsters or referencing Boris Johnson jumping from an airplane holding the British Flag (yes he did that as well) but we'll use this mnemonic insetead:

Please Do Not Throw Sausage and Pizza Away

It's obtained by looking at the 1st letter of each layer from the bottom

Figure 2.2: OSI Layer representation

2.2.3 Theory vs Practice

Even if The Transmission Control Protocol/Internet Protocol (TCP/IP) model came before the Open Systems Interconnection (OSI) model it is what is used in practice today, and it has only five layers:

- Application layer
- Transport layer
- Network access layer
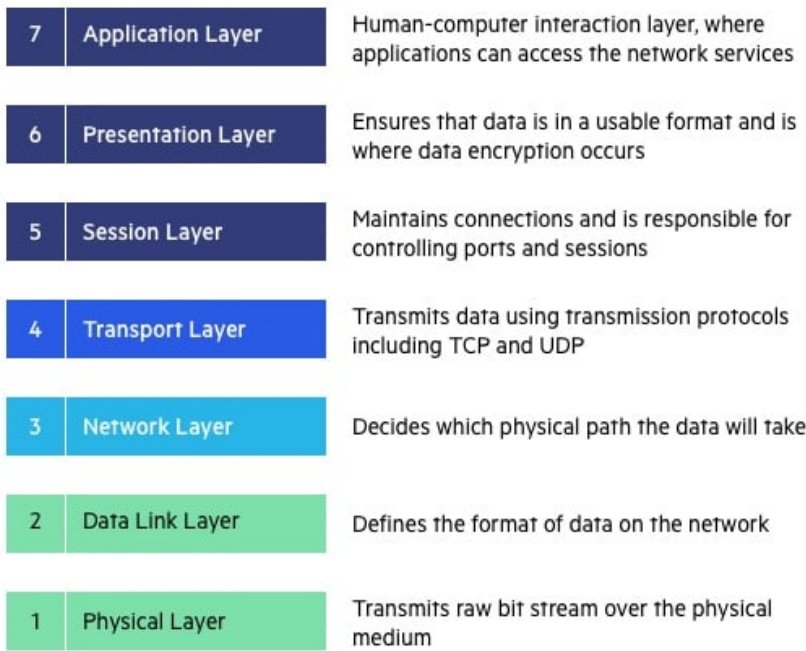- Network interface layer
- Hardware layer

It may look different from the OSI model, but some functions are just encompassed in a single layer which is **the application layer** corresponding to $Application^{OSI}$,$Presentation^{OSI}$ and $Session^{OSI}$.

CONNECTION-ORIENTED PROTOCOLS

Unlike UDP, TCP/IP is a **connection-oriented** protocol[1]. This means that before the client and server can start to send data to each other, they first need to handshake and establish a TCP connection. One end of the TCP connection is attached to the client socket and the other end is attached to a server socket. When creating the TCP connection, we associate it with the client socket address(IP address and port number). With the TCP connection established, when one side wants to send data to the other side, it just drops the data into the TCP connection via its socket. This is different from UDP, for which the server must attach a destination address to the packet before dropping it into the socket.

Now let's take a closer look at the interaction of client and server programs in TCP. The client has the job of initiating contact with the server. In order for the server to be able to react to the client's initial contact, the server has to be ready. This implies two things. First, as in the case of UDP, the TCP server must be running as a process before the client attempts to initiate contact. Second, the server program must have a special door, more precisely a special socket, that welcomes some initial contact from a client process running on an arbitrary host. Using our **house/door** analogy for a **process/socket**, we will sometimes refer to the client's initial contact as "knocking on the welcoming door."

With the server process running, the client process can initiate a TCP connection to the server. This is done in the client program by creating a TCP socket. When the client creates its TCP socket, it specifies the address of the welcoming socket in the server, namely, the IP address of the server host and the port number of the socket. After creating its socket, the client initiates a **three-way handshake** and establishes a TCP connection with the server. The three-way handshake, which takes place within the transport layer, is completely invisible to the client and server programs.

During the three-way handshake, the client process knocks on the welcoming door of the server process. When the server "hears" the knocking, it creates a new door, more precisely, a new socket that is dedicated to that particular client. In our example below, the welcoming door is a TCP socket object that we call serverSocket; the newly created socket dedicated to the client making the connection is called connectionSocket. People encountering TCP sockets for the first time sometimes confuse the welcoming socket (which is the initial point of contact for all clients wanting to communicate with the server), and each newly created server-side connection socket that is subsequently created for communicating with each client.

From the application's perspective, the client's socket and the server's connection socket are directly connected by a pipe. As shown in Figure 2.3, the client process can send arbitrary bytes into its socket, and TCP guarantees that the server pro-

FIGURE 2.3: The TCPServer process has two sockets

cess will receive (through the connection socket) each byte in the order sent. TCP thus provides a reliable service between the client and server processes. Furthermore, just as people can go in and out the same door, the client process not only sends bytes into but also receives bytes from its socket; similarly, the server process not only receives bytes from but also sends bytes into its connection socket.
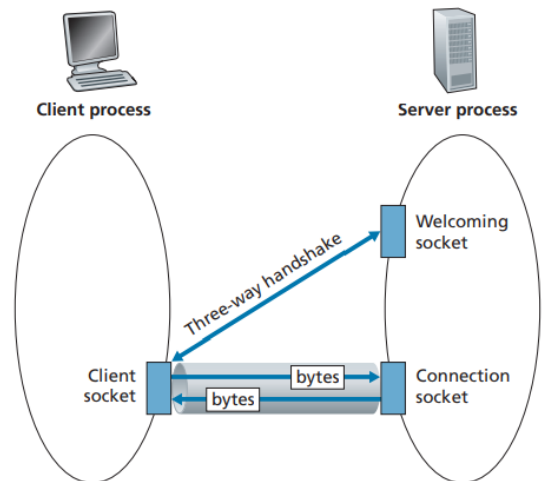
---

[1]James F. Kurose and Keith W. Ross Computer Networking A Top-Down Approach.

CONNECTIONLESS PROTOCOLS

UDP is a no-frills, lightweight transport protocol, providing minimal services. UDP is connectionless, so there is no handshaking before the two processes start to communicate. UDP provides an unreliable data transfer service, which means, when a process sends a message into a UDP socket, UDP provides no guarantee that the message will ever reach the receiving process. Furthermore, messages that do arrive at the receiving process may arrive out of order.

UDP does not include a congestion-control mechanism, so the sending side of UDP can pump data into the layer below (the network layer) at any rate it pleases. (Note, however, that the actual end-to-end throughput may be less than this rate due to the limited transmission capacity of intervening links or due to congestion).

HORIZONTAL VS VERTICAL APPROACH

In the OSI model,the layers communicate directly with each other, hence horizontal approch.
While in TCP/IP, each layer is traversed meaning data travels each layer, only then it is sent, hence vertical approch.

horizontal and vertical approaches
Quora.com

If someone can explain to me how to interpret the message Quora.com is trying to convey or in general which protocol is horizontal and which is vertical and most importantly what's horizontal and vertical definition, then I'd be all ears and ready to learn but until then it'll be a mistery that someone one day will solve **but that day is not today and it won't be me**. If a question like this comes out in the exam I'll just have a random guess

2.3   Switched Local Area Networks

Let's do now talk about Switched local networks.

Figure 2.4 shows a switched local network connect-
ing two servers, three departments and a router using
four switches. Since these switches operate at the link
layer (layer-2 if you recall Figure 2.2), they switch link-
layer frames (instead of network-layer datagrams[2]),
hence don't recognize network-layer addresses, thus
don't use routing algorithms like for example OSPF
to determine paths through the network of layer-2
switches. Rather than using IP addresses, we will soon
see that they use link-layer addresses to forward link-
layer frames through the network of switches. We shall
approach switched LANs by first covering linklayer ad-
dressing (Section 2.3.1). We then take a close look
to the famous Ethernet protocol (Section -.-.-). Once

FIGURE 2.4: An institutional network connected together by four switches

we've seen the link-layer addressing and Ethernet, we'll look at how link-layer switches operate (Section
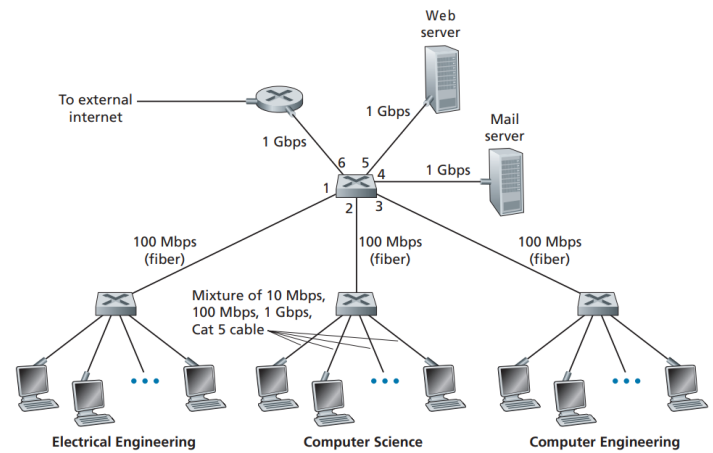-.-.-), and then see (Section -.-.-) how these switches are often used to build large-scale LANs.

2.3.1   Link-layer addressing and ARP

Hosts and routers have link-layer addresses. You might be asking, why in the world do we need to have
addresses at both the network and link layers? In addition to describing the syntax and function of the
link-layer addresses, in this section we hope to shed some light on why the two layers of addresses are
useful and, in fact, indispensable. We'll also cover the Address Resolution Protocol (ARP), which provides
a mechanism to translate IP addresses to link-layer addresses.

MAC Addresses

The truth is, hosts and routers don't have link-layer addresses but their adapters (their network interfaces)
do instead. A host or router with multiple network interfaces will thus have multiple link-layer addresses
associated with it, just as it would also have multiple IP addresses associated with it.
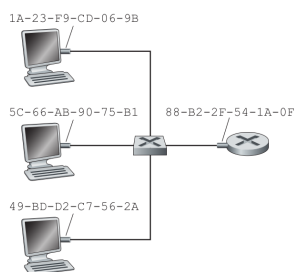

FIGURE 2.5: Each interface connected to a LAN has a unique MAC address

It's important to note, however, that link-layer switches do
not have link-layer addresses associated with their interfaces
that connect to hosts and routers.This is because the job of
the link-layer switch is to carry datagrams between hosts
and routers; a switch does this job transparently, that is,
without the host or router having to explicitly address the
frame to the intervening switch. This is illustrated in Figure
2.5. A linklayer address is variously called a **LAN address**,
a **physical address**, or a **MAC address**. Because MAC
address seems to be the most popular term, we'll henceforth
refer to link-layer addresses as MAC addresses. For most

LANs (including Ethernet and 802.11 wireless LANs), the MAC address is 6 bytes long, giving 2^{48} possible

---

[2]basic transfer unit associated with a packet-switched network structured in header and payload providing connectionless communication service

MAC addresses. As shown in Figure 2.5, these 6-byte addresses are typically expressed in HEX notation. Although MAC addresses were designed to be permanent, it is now possible to change an adapter's MAC address via software. For the rest of this section, however, we'll assume that an adapter's MAC address is fixed.

One MAC address is unique in the world altough adapters are manufactured in many countries by many companies. How does a company manufacturing adapters in Liechtenstein make sure that it is using different addresses from a company manufacturing adapters in Singapore? IEEE manages the MAC address space. In particular, when a company wants to manufacture adapters, it purchases a chunk of the address space consisting of 2^{24} addresses for a nominal fee. IEEE allocates the chunk of 2^{24} addresses by fixing the first 24 bits of a MAC address and letting the company create unique combinations of the last 24 bits for each adapter.

An adapter's MAC address has a flat structure (as opposed to a hierarchical structure) and doesn't change no matter where the adapter goes. A laptop with an Ethernet interface always has the same MAC address, no matter where the computer goes. A smartphone with an 802.11 interface always has the same MAC address, no matter where the smartphone goes. Recall that, in contrast, IP addresses have a hierarchical structure (that is, a network part and a host part), and a host's IP addresse needs to be changed when the host moves,for example the host is attached to another network. An adapter's MAC address is analogous to a person's National Insurance Number, which also has a flat addressing structure and which doesn't change no matter where the person goes. An IP address is analogous to a person's postal address, which is hierarchical and which must be changed whenever a person moves. Just as a person may find it useful to have both a postal address and a NIN, it is useful for a host and router interfaces to have both a network-layer address (IP) and a MAC address.

When an adapter wants to send a frame to some destination adapter, the sending adapter inserts the destination adapter's MAC address into the frame and then sends the frame into the LAN. As we will soon see (TO-DO), a switch occasionally broadcasts an incoming frame onto all of its interfaces. We'll see in Chapter - that 802.11 also broadcasts frames. Thus, an adapter may receive a frame that isn't addressed to it. Thus, when an adapter receives a frame, it will check to see whether the destination MAC address in the frame matches its own MAC address. If there is a match, the adapter extracts the enclosed datagram and passes the datagram up the protocol stack. If there isn't a match, the adapter discards the frame, without passing the network-layer datagram up. Thus, only the destination adapter will be interrupted when the frame is received.

However, sometimes a sending adapter <u>does</u> want all the other adapters on the LAN to receive and process the frame it is about to send. In this case, the sending adapter inserts a special MAC **broadcast address** into the destination address field of the frame. For LANs that use 6-byte addresses (such as Ethernet and 802.11), the broadcast address is a string of 48 consecutive 1s (that is, FF-FF-FF-FF-FF-FF in hexadecimal notation).

Address Resolution Protocol (ARP)

Because there are both network-layer addresses (for example, Internet IP addresses) and link-layer addresses (that is, MAC addresses), there is a need to translate between them. For the Internet, this is the job of the Address Resolution Protocol (ARP). To understand the need for a protocol such as ARP, consider the network shown in Figure 2.6. In this simple example, each host and router has a single IP address and single MAC address. As usual, IP addresses are shown in dotted-decimal

notation and MAC addresses are shown in hexadecimal notation. For the purposes of this discussion, we will assume in this section that the switch broadcasts all frames, which means, whenever a switch

receives a frame on one interface, it forwards the frame on all of its other interfaces. In the next section(?), we will provide a more accurate explanation of how switches operate.

Now suppose that the host with IP address 222.222.222.220 wants to send an IP datagram to host 222.222.222.222. In this example, both the source and destination are in the same subnet. To send a datagram, the source must give its adapter not only the IP datagram but also the MAC address for destination 222.222.222.222. The sending adapter will then construct a link-layer frame containing the destination's MAC address and send the frame into the LAN.

The important question addressed in this section is, How does the sending host determine the MAC address for the destination host with IP address 222.222.222.222? It uses ARP. An ARP module in the sending host takes any IP address on the same LAN as input, and returns the corresponding MAC

FIGURE 2.6: Each interface on a LAN has an IP address and a MAC address

address. In the example at hand, sending host 222.222.222.220 provides its ARP module the IP address 222.222.222.222, and the ARP module returns the corresponding MAC address 49-BD-D2-C7-56-2A. So we see that ARP resolves an IP address to a MAC address. In many ways it is analogous to DNS, which resolves host names to IP addresses. However, one important difference between the two resolvers is that DNS resolves host names for hosts anywhere in the Internet, whereas ARP resolves IP addresses only for hosts and router interfaces on the same subnet. If a node in California were to try to use ARP to resolve the IP address for a node in Mississippi, ARP would return with an error.

Now that we have explained what ARP does, let's look at how it works. Each host and router has an ARP table in its memory, which contains mappings of IP addresses to MAC addresses.

Figure 2.7 shows what an ARP table in host 222.222.222.220 might look like.

The ARP table also contains a time-to-live (TTL) value, which indicates when each mapping will be deleted from the table. Note that a table does not necessarily contain an entry for every host and router on the subnet; some may have never been entered into the table, and others may have expired. A typical expiration time for an entry is 20 minutes from when an entry is placed in an ARP table.

IP Address	MAC Address	TTL
222.222.222.221	88-B2-2F-54-1A-0F	13:45:00
222.222.222.223	5C-66-AB-90-75-B1	13:52:00

FIGURE 2.7: A possible ARP table in 222.222.222.220

Now suppose that host 222.222.222.220 wants to send a datagram that is IP-addressed to another host or router on that subnet. The sending host needs to obtain the MAC address of the destination given the IP address. This task is easy if the sender's ARP table has an entry for the destination node. But what if the ARP table doesn't cur- rently have an entry for the destination? In particular, suppose 222.222.222.220 wants to send a datagram to 222.222.222.222. In this case, the sender uses the ARP protocol to resolve the address. First, the sender constructs a special packet called an ARP packet. An ARP packet has several fields, including the sending and receiving IP and MAC addresses. Both ARP query and response packets have the same format. The pur- pose of the ARP query packet is to query all the other hosts and routers on the subnet to determine the MAC address corresponding to the IP address that is being resolved.

Returning to our example, 222.222.222.220 passes an ARP query packet to the adapter along with an indication that the adapter should send the packet to the MAC broadcast address, namely, FF-FF-FF-
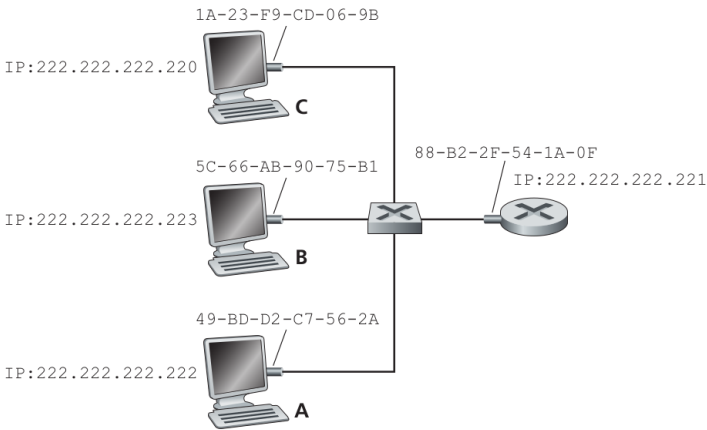
FF-FF-FF. The adapter encapsulates the ARP packet in a link-layer frame, uses the broadcast address for the frame's destination address, and transmits the frame into the subnet. Recalling our NIN/postal address analogy, an ARP query is equivalent to a person shouting out with a loudhailer in a small street in Walthamstow Central "What is the NIN of the person whose postal address is **35, Folkestone road E17 9SD**?" The frame containing the ARP query is received by all the other adapters on the subnet, and (because of the broadcast address) each adapter passes the ARP packet within the frame up to its ARP module. Each of these ARP modules checks to see if its IP address matches the destination IP address in the ARP packet. The one with a match sends back to the querying host a response ARP packet with the desired mapping. The querying host 222.222.222.220 can then update its ARP table and send its IP datagram, encapsulated in a link-layer frame whose destination MAC is that of the host or router responding to the earlier ARP query.

[arp -a] output on my linux shell On my machine for example the ARP table contains just two entries, one for the gateway, and one for the TV who's connected in the same WiFi. The LAN is obviously larger than that but my computer never had the need to send other machines a packet.

```
_gateway (192.168.0.1) at 24:a7:dc:31:5b:d1 [ether] on wlp3s0
TV (192.168.0.129) at cc:d3:c1:64:f9:f3 [ether] on wlp3s0
```

RARP and DHCP

RARP demands another computer (usually a server in the same LAN) to assign the demanding one with an IP which is essentially what DHCP is doing that's why RARP got obsolete

2.4 Networking Hardware

Computers need networking hardware in order to connect to each other. **Routers**, **hubs**, **switches** and **bridges** are all pieces of networking equipment that can perform slightly different tasks. A router can often incorporate hubs, switches and wireless access within the same hardware

2.4.1 Routers

A router can form a **LAN** by connecting devices within a building. It also makes it possible to connect different networks together.   Homes and businesses use a router to connect to the internet. A router can often incorporate a modem within the hardware.
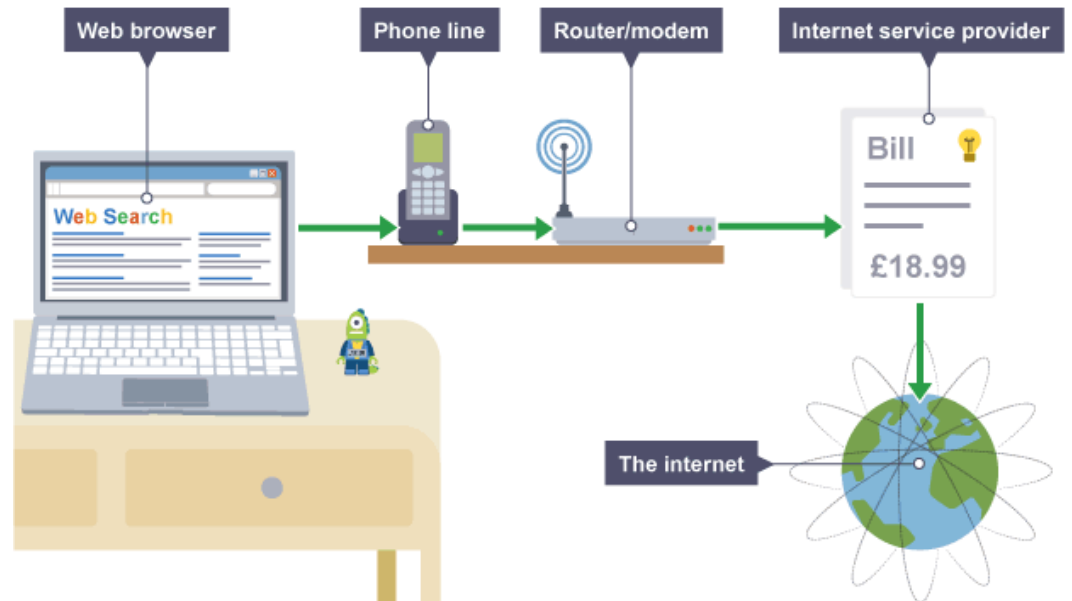
<p align="center"><small>FIGURE 2.8: Router connecting devices in a LAN over the Internet</small></p>

2.4.2 Modems

A **modem** enables a computer to connect to the internet over a telephone line.   A modem converts **digital** signals from a computer to analogue signals that are then sent down the telephone line. A modem on the other end converts the analogue signal back to a digital signal which another computer can understand.

2.4.3 Hubs, bridges and switches

Hubs, **bridges** and **switches** allow multiple devices to connect to the router and they transfer data to all devices on a network. A router is a more complex device that usually includes the capability of hubs, bridges and switches.

Hubs

A hub broadcasts data to all devices on a network. This can use a lot of **bandwidth** as it results in unnecessary data being sent - not all computers might need to receive the data. A hub would be useful to link up a few games consoles for a local multiplayer game using a wired LAN. A hub is a physical-layer device that acts on individual bits rather than frames.When a bit, representing a zero or a one, arrives from one interface, the hub simply recreates the bit, boosts its energy strength, and transmits the bit onto all the other interfaces. Thus, Ethernet with a hub-based star topology is also a broadcast LAN.

Whenever a hub receives a bit from one of its interfaces, it sends a copy out on all of its other interfaces. In particular, if a hub receives frames from two different interfaces at the same time, a collision occurs and the nodes that created the frames

FIGURE 2.9: devices connected together

must retransmit.At some point many hubs got replaced with switches which are "collision-less" but unlike routers, which operate up through layer 3, switches operates only up through layer 2.
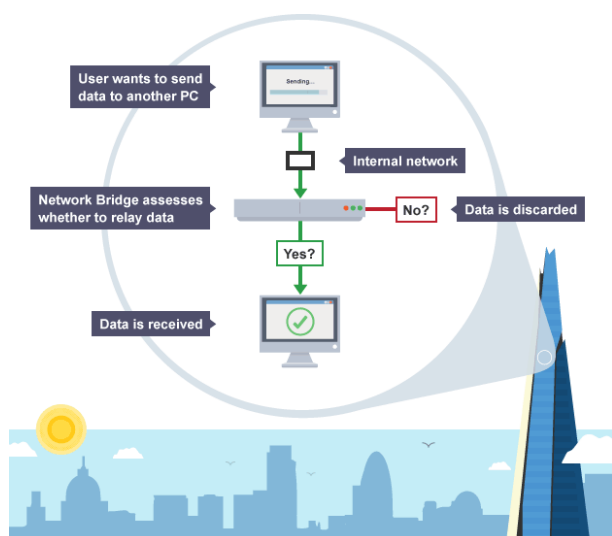

FIGURE 2.10: Bridge saving unnecessary data transfer

Bridges

A **bridge** is used to connect two separate LAN networks. A computer can act as a bridge through the **operating system**. A bridge looks for the receiving device before it sends the message. This means that it will not send a message if the receiving computer is not there. It will check to see if the receiver has already had the message. This can help save unnecessary data transfers, which improves the performance of a network.(see Figure 2.10)

Switches

A **switch** performs a similar role to a hub and a bridge but is more powerful. It stores the **MAC addresses** of devices on a network and filters **data packets** to see which devices have asked for them. This makes a switch more efficient when demand is high. If, for example, a game involved lots of data being passed between machines, then a switch could reduce the amount of **latency**

2.5   Cisco Packet Tracer

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit. The software is mainly focused towards Cisco Networking Academy students as an educational tool for helping them learn fundamental CCNA concepts. Previously students enrolled in a CCNA Academy program could freely download and use the tool free of charge for educational use.[3]

In this experiment we try to ping devices being set with 0 in the IP fields. Then we're gonna expand the network with more devices

- First nextwork has a 192.168.1.1 default gateway

- Second network has a 192.168.0.1 default gateway

---

[3]Bakni, Michel; Cardinale, Yudith; Moreno, Luis Manuel (June 2018). **An Approach to Evaluate Network Simulators: An Experience with Packet Tracer**.Revista Venezolana de Computación. 5: 29–36. ISSN 2244-7040.
Javid,Sheikh Raashid (May 2014). **Role of Packet Tracer in learning Computer Networks** (PDF). International Journal of Advanced Research in Computer and Communication Engineering. 3 (5): 6508–6511.

2.5.1   The step-by-step guide

Seregios[4] wants to create a network on Cisco Packet Tracer. The task is quite easy but he's got quite a few tasks to accomplish

The first he needs to do is opening Cisco Packet Tracer. The screen will be completely empty with no devices selected. On the right hand side of the bottom panel **Realtime** is being selected instead of **Simulation**
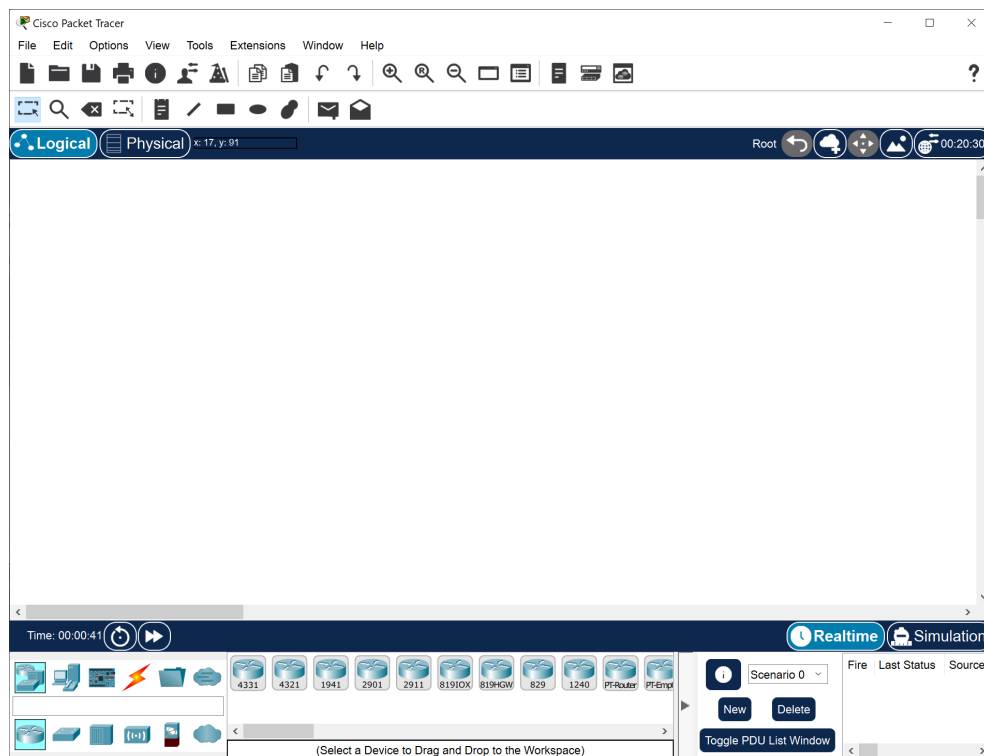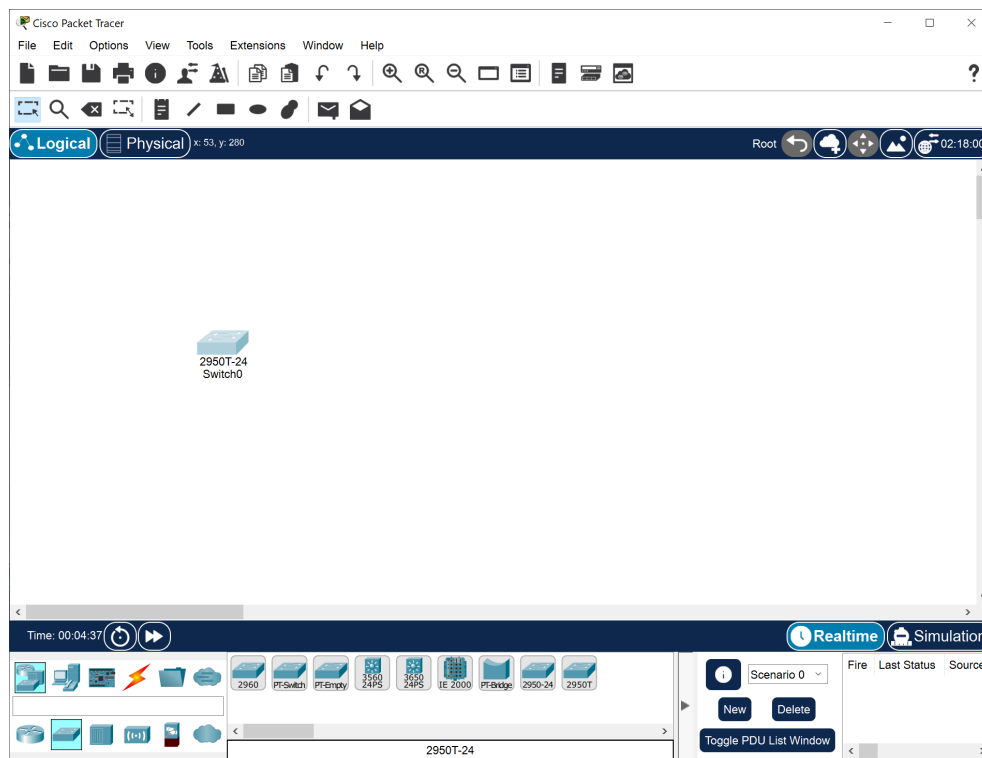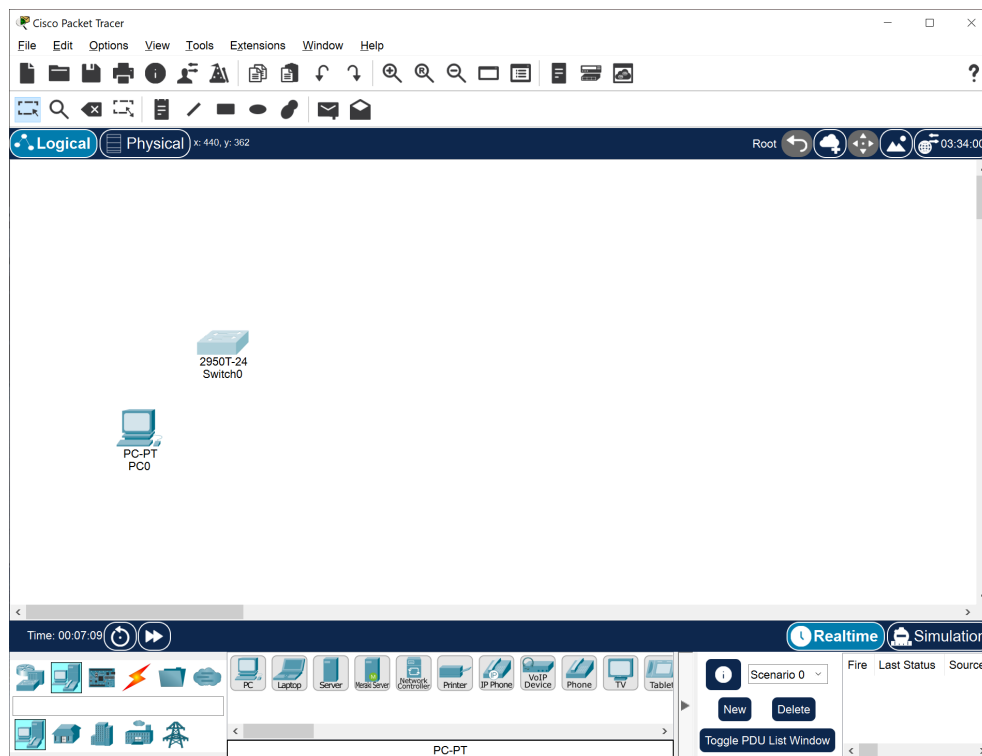

Figure 2.11: first screen he gets when he opens Cisco Packet Tracer

---

[4]Seregios is a Flying Wyvern introduced in Monster Hunter 4 Ultimate.

Now what he needs to do is to add a switch :

And then we add a computer :

Now we click on the computer
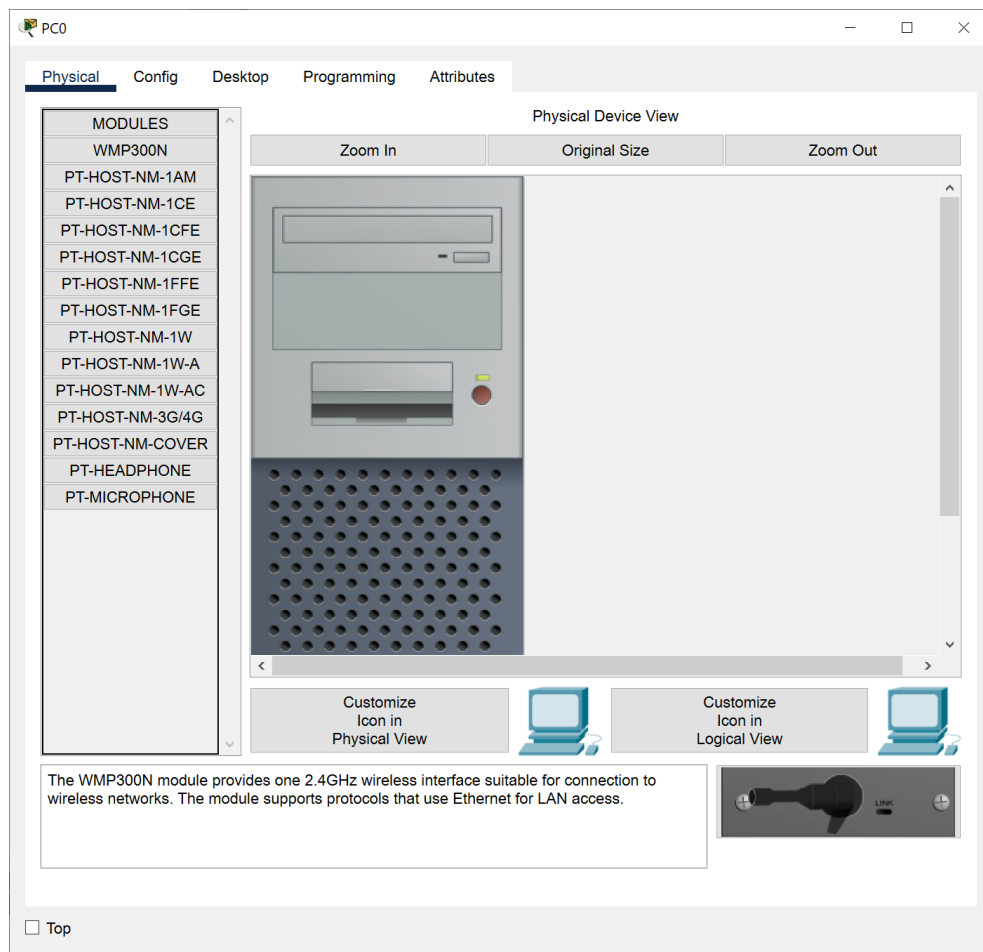
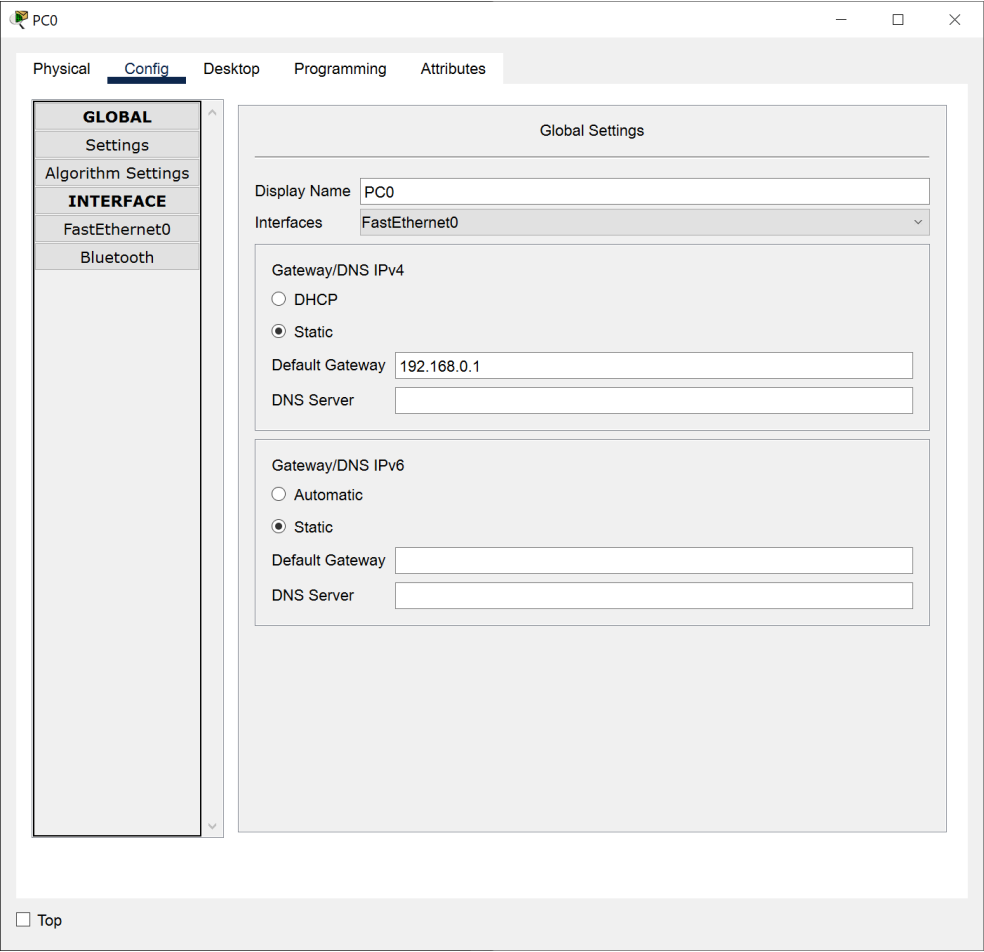And we move ourselves in the Config tab
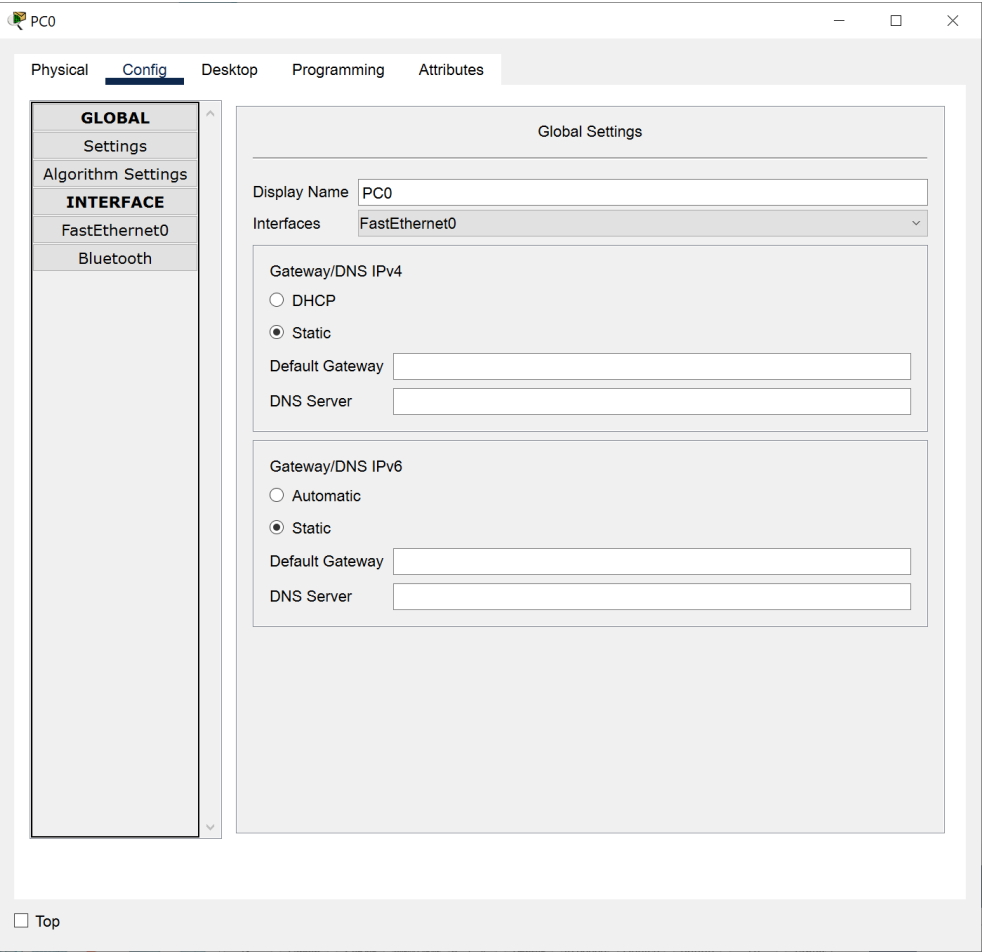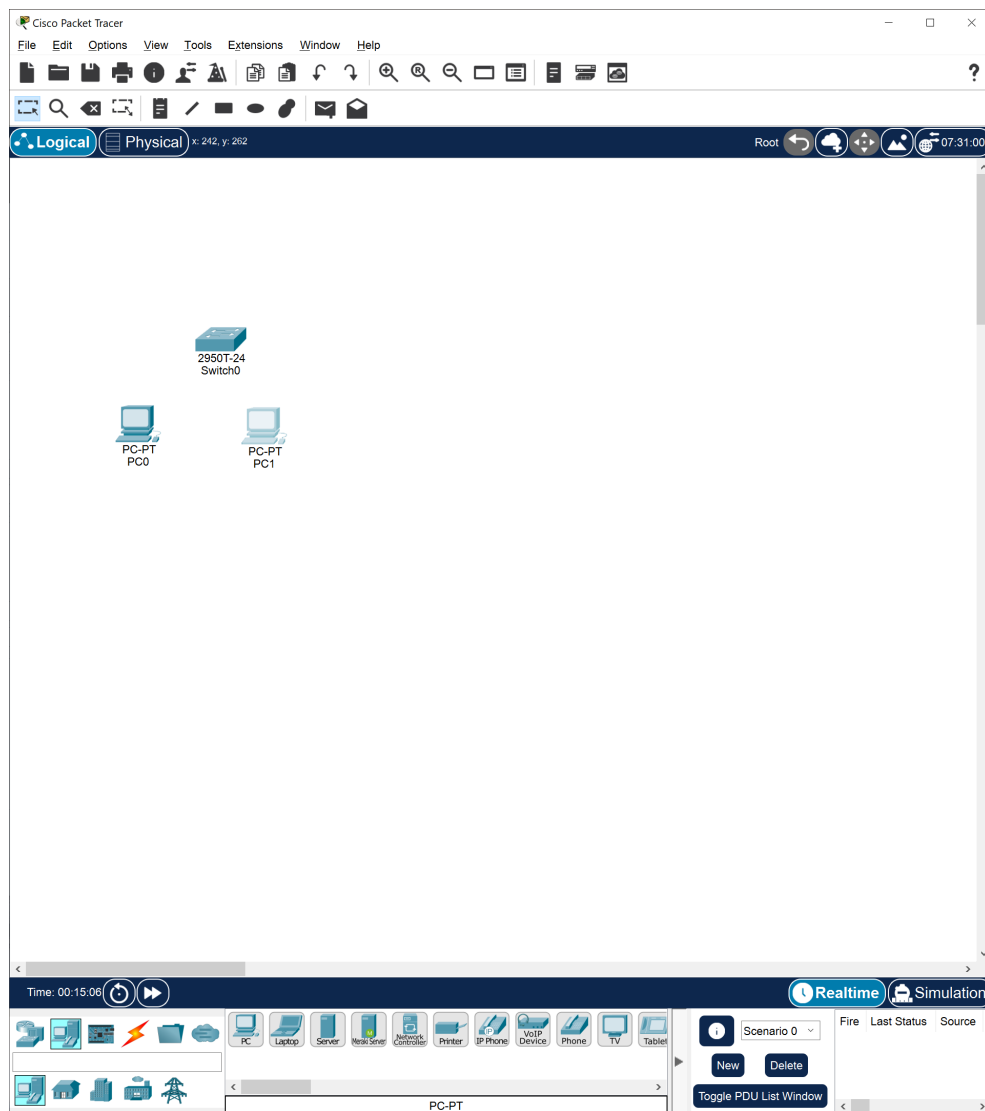
what we're gonna be looking later at is the IPV4 address
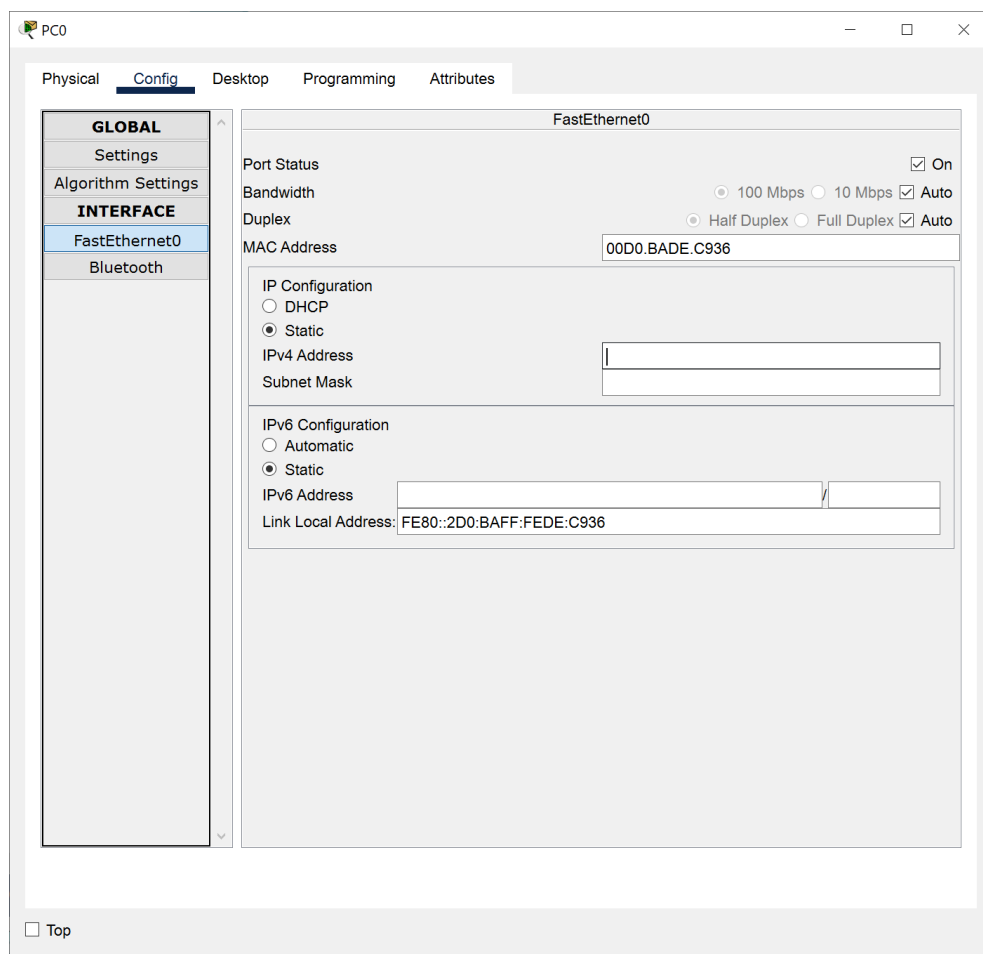
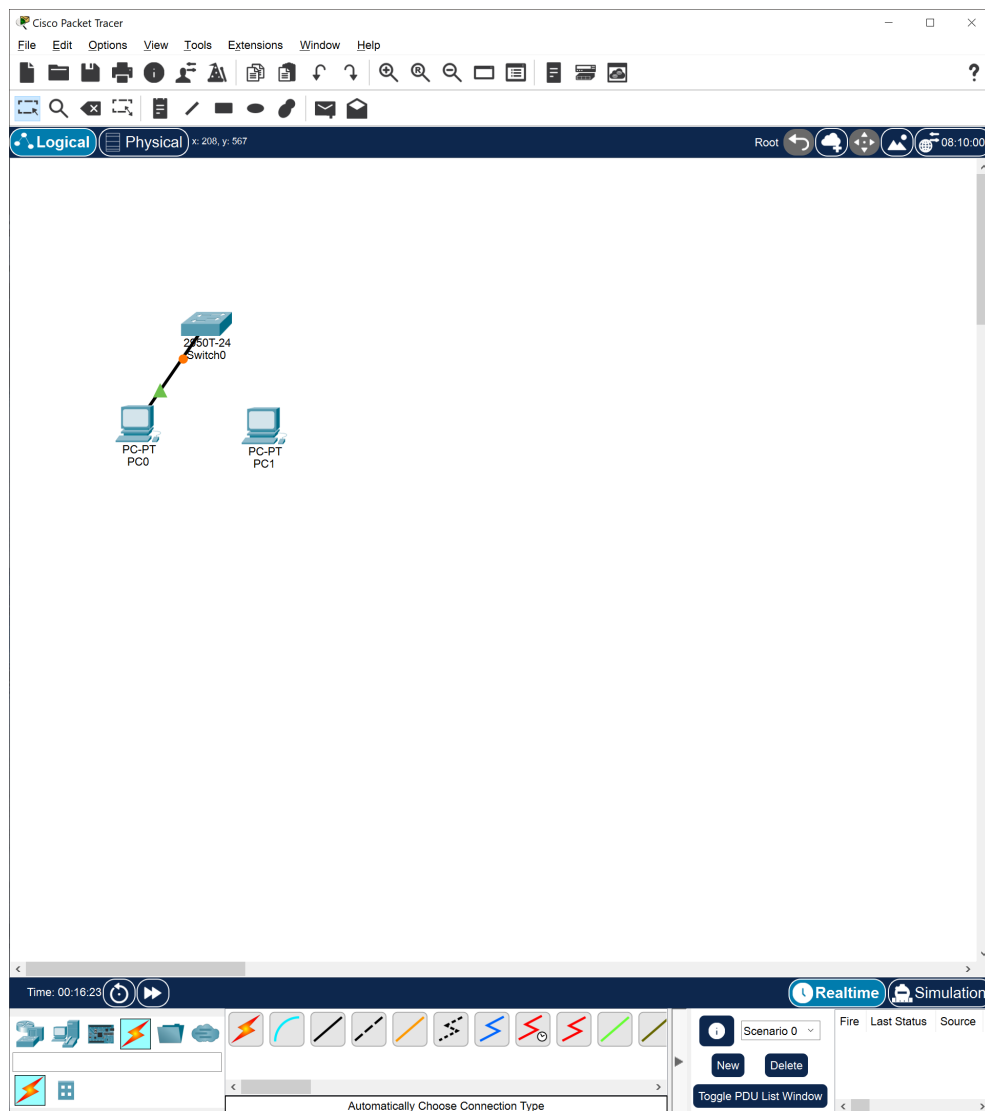in the meantime let's go in global and set the **IP Address** equal to this
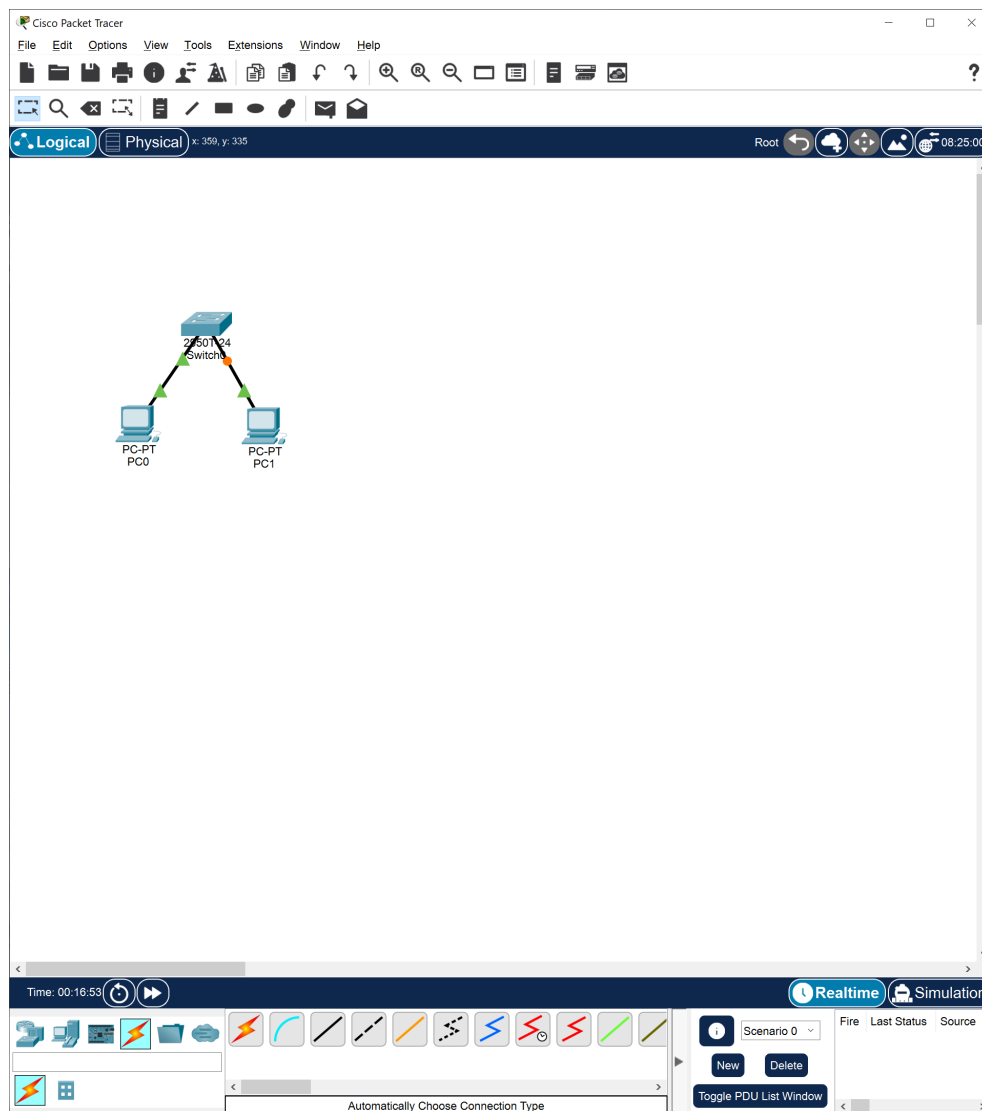
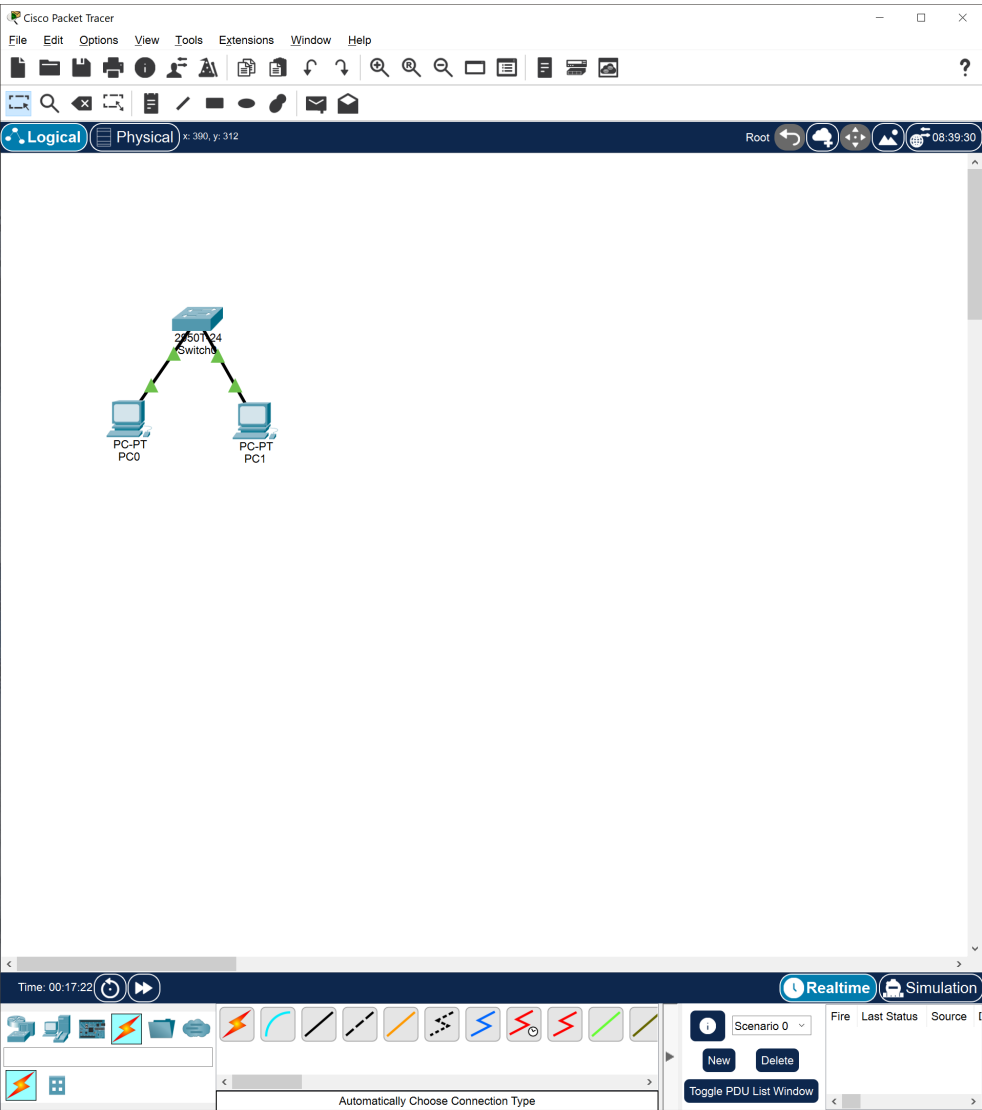$$192.168.0.1$$

Now we add a new computer

We link the switch to the first computer and wait for all lights to go green
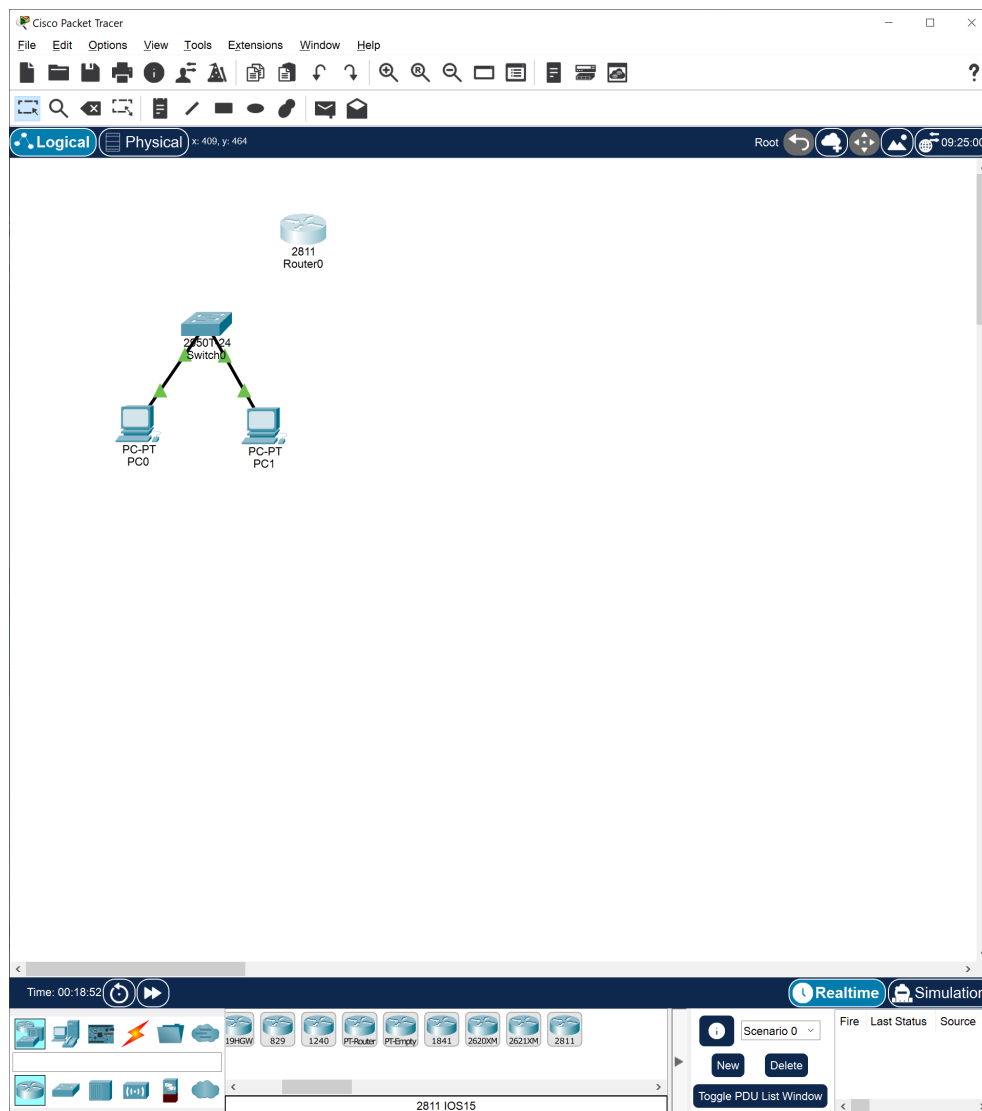
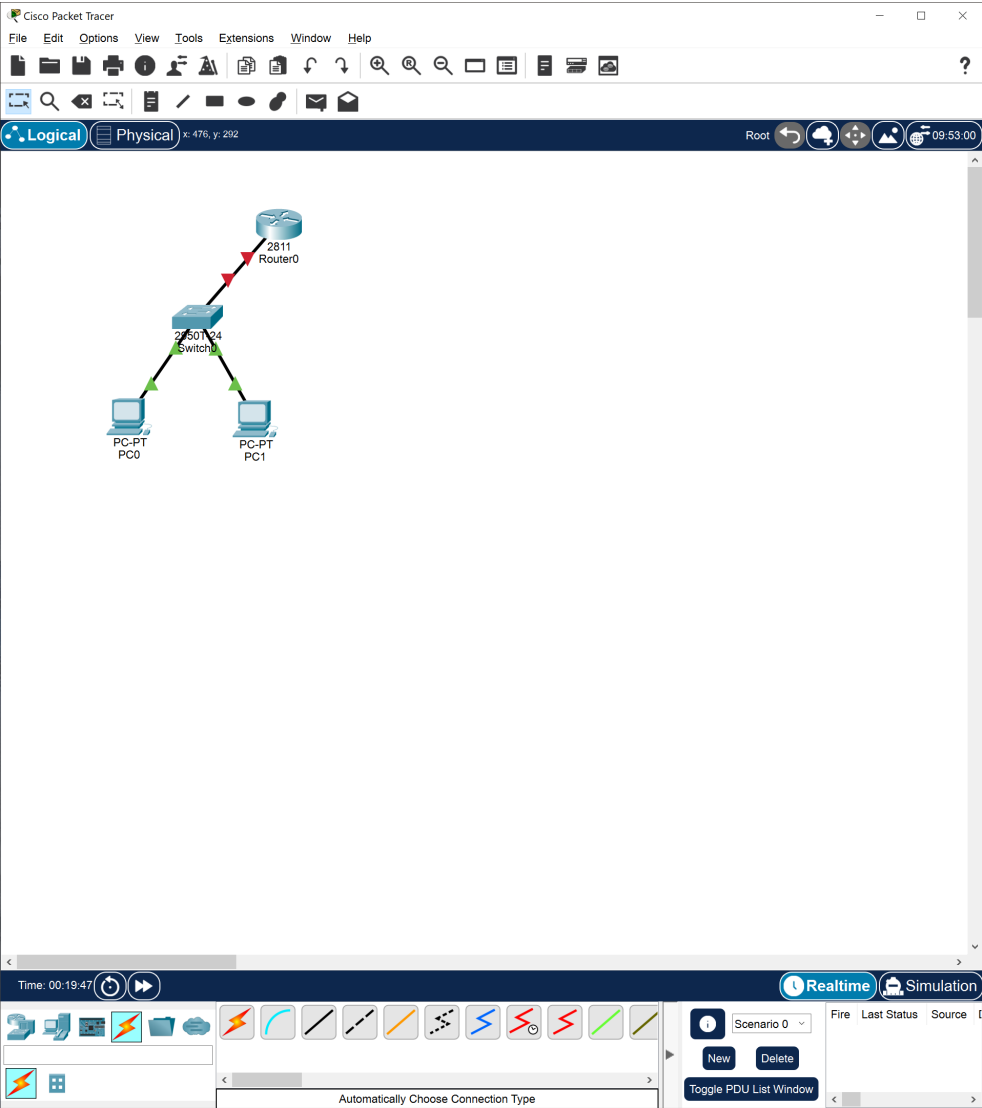Link the switch to the second computer and wait for this link to go all green as well

Now it's all green which makes us happy

Let's add a router

Let's link the router to the first computer

If you click on the router, in the config tab there is a box you need to check. That box will emulate the router being powered on

Once you click in the box a small tick will appear in it. This means the box is ticked and the function that box is proving is now being turned on

as a result of ticking that box now you can see the link going green wich means is enabled for data transmission
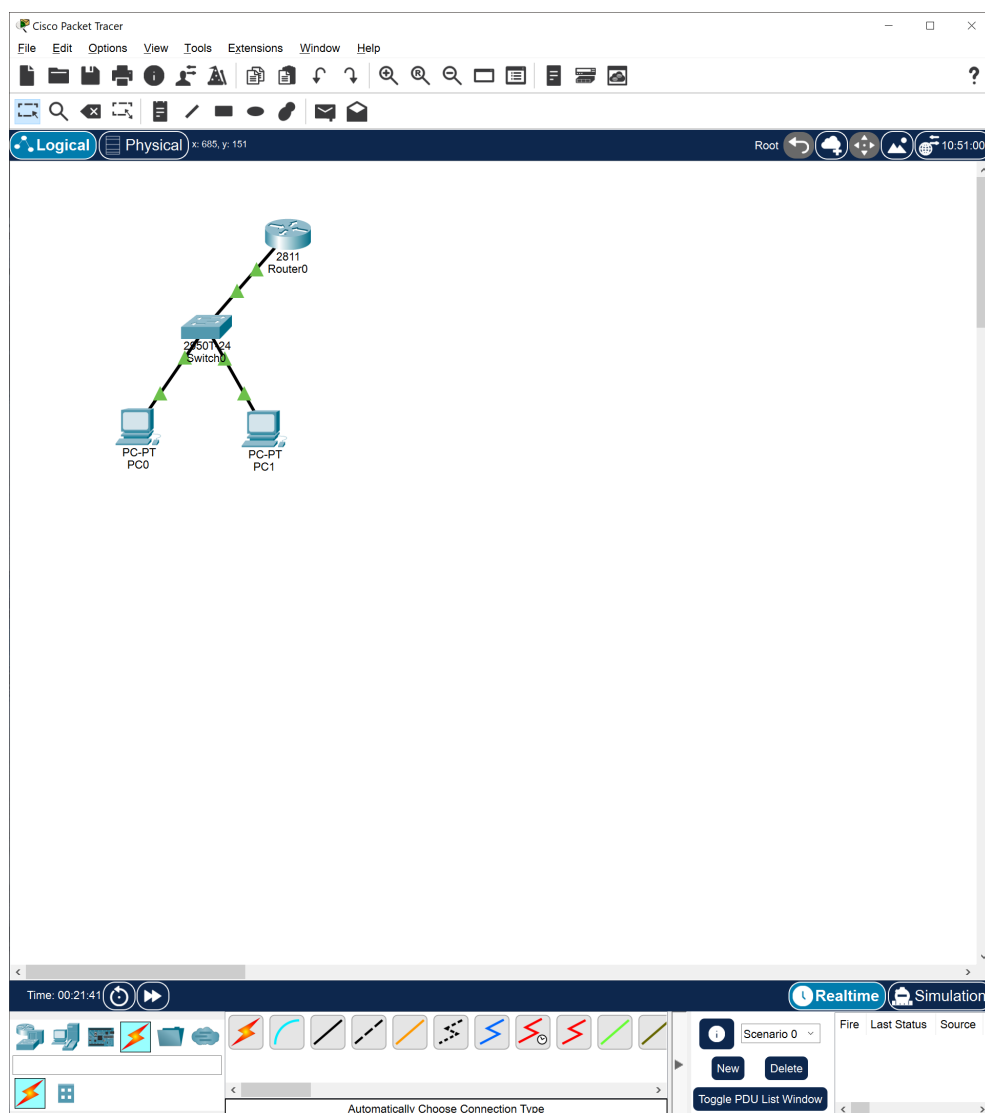
we only need to sort the **IP Configuration** out as well

Now, because the subnet mask indicates how many values can you actually use this means we can use

$$255 values - X values$$

where $\underline{X}$ is the number in a subnetmask like $\underline{Z.Y.W.X}$ which in the case of $\underline{255.255.255.0}$ will be

$$255 - 0$$

which returns 255 values but because we start counting from 0 we can go up to 254. In the following example you can see the value 0 being accepted as a valid value

Let's pick up PC1 console and ping all devices in the 192.168.0.1 network. The ping works

Let's create a copy of the subnetwork we have already. The gateway will be this time

$$192.168.1.1$$
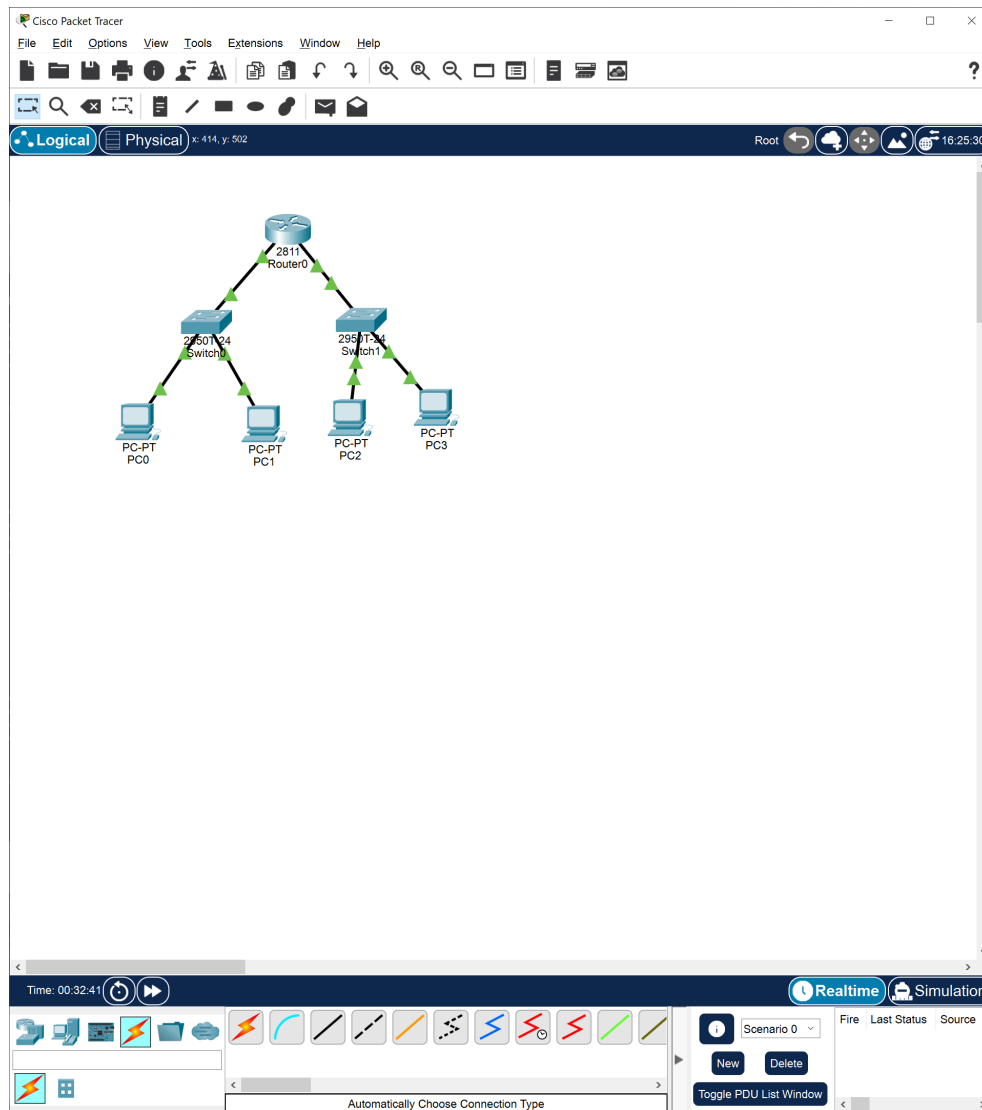
expanding the network

Let's add a printer with the following IP

$$192.168.1.20$$
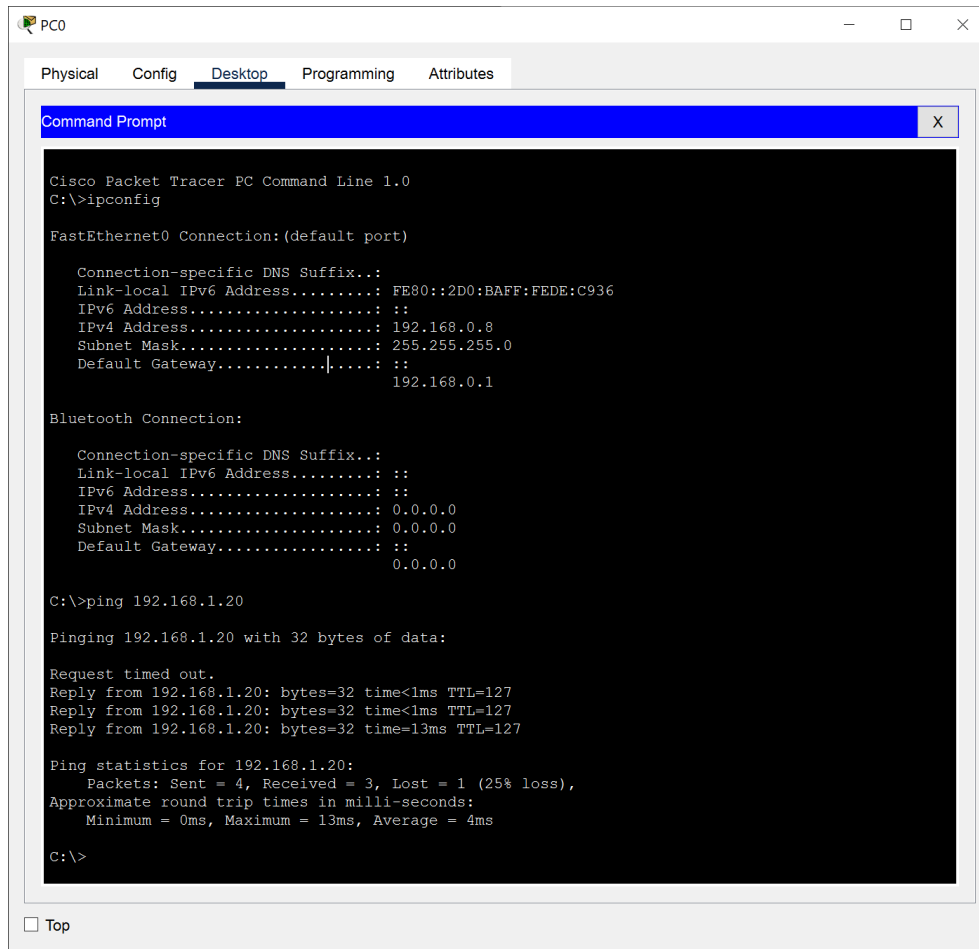
Let's ping the printer from PC0

We can safely assume the network is working

2.6   Power over Ethernet

Power over Ethernet is a technique for delivering DC power to devices over copper Ethernet cabling, eliminating the need for separate power supplies and outlets. While PoE doesn't add Ethernet data capabilities, it does offer expanded options for how and where Ethernet end devices can be placed.

2.7   Network Topology

Network topology is the arrangement of the elements (links, nodes, etc.) of a communication network.

Network topology is the structure of a network and may be depicted physically or logically. It is an application of graph theory wherein communicating devices are modeled as nodes and the connections between the devices are modeled as links or lines between the nodes. Physical topology is the placement of the various components of a network (e.g., device location and cable installation), while logical topology illustrates how data flows within a network. Distances between nodes, physical interconnections, transmission rates, or signal types may differ between two different networks, yet their logical topologies may be identical. A network's physical topology is a particular concern of the physical layer of the OSI model.

Examples of network topologies are found in local area networks (LAN), a common computer network installation. Any given node in the LAN has one or more physical links to other devices in the network; graphically mapping these links results in a geometric shape that can be used to describe the physical topology of the network. A wide variety of physical topologies have been used in LANs, including ring, bus, mesh and star. Conversely, mapping the data flow between the components determines the logical topology of the network. In comparison, Controller Area Networks, common in vehicles, are primarily distributed control system networks of one or more controllers interconnected with sensors and actuators over, invariably, a physical bus topology.

2.7.1   Star Topology

In star topology, every peripheral node (computer workstation or any other peripheral) is connected to a central node called a hub or switch. The hub is the server and the peripherals are the clients. The network does not necessarily have to resemble a star to be classified as a star network, but all of the peripheral nodes on the network must be connected to one central hub. All traffic that traverses the network passes through the central hub, which acts as a signal repeater.
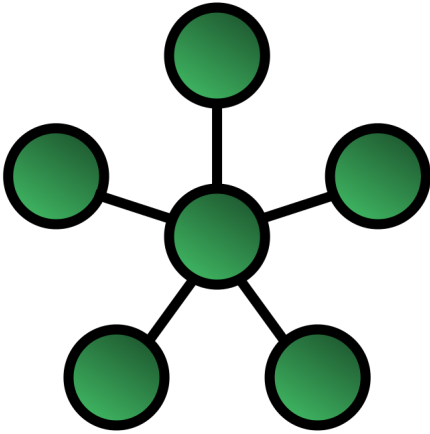
PROs

- simplicity of adding additional nodes

- is the easiest topology to design and implement

CONs

- the hub represents a single point of failure

- Since all peripheral communication must flow through the central hub, the aggregate central bandwidth forms a network bottleneck for large clusters

2.7.2   Ring Topology

A ring topology is a daisy chain in a closed loop. Data travels around the ring in one direction. When one node sends data to another, the data passes through each intermediate node on the ring until it reaches its destination. The intermediate nodes repeat (re transmit) the data to keep the signal strong.[5] Every node is a peer; there is no hierarchical relationship of clients and servers. If one node is unable to re transmit data, it severs communication between the nodes before and after it in the bus.
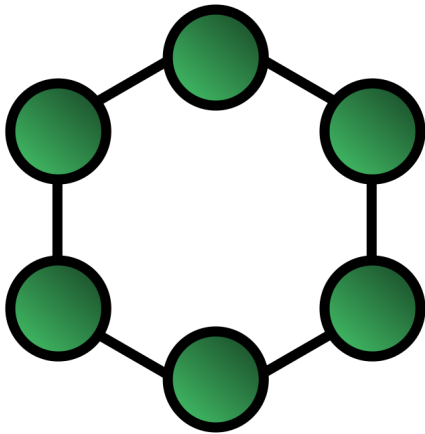
PROs

- When the load on the network increases, its performance is better than bus topology

- There is no need of network server to control the connectivity between workstations

CONs

- Aggregate network bandwidth is bottlenecked by the weakest link between two nodes

---

[5]Inc, S., (2002) . Networking Complete. Third Edition. San Francisco: Sybex

2.7.3   Ring Topology on Cisco Packet Tracer

This is a quick example of how can a Ring Topology look like on Cisco Packet Tracer. The links at the center have been added later on for testing purporses
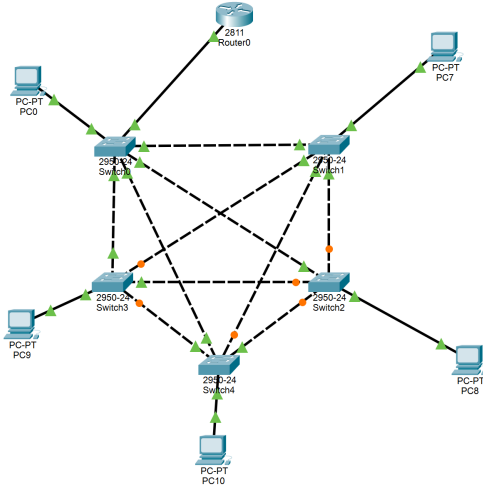
2.8   Routing Protocols

A routing protocol specifies how routers communicate with each other to distribute information that enables them to select routes between nodes on a computer network. Routers perform the traffic directing functions on the Internet; data packets are forwarded through the networks of the internet from router to router until they reach their destination computer. Routing algorithms determine the specific choice of route. Each router has a prior knowledge only of networks attached to it directly. A routing protocol shares this information first among immediate neighbors, and then throughout the network. This way, routers gain knowledge of the topology of the network. The ability of routing protocols to dynamically adjust to changing conditions such as disabled connections and components and route data around obstructions is what gives the Internet its fault tolerance and high availability.

The specific characteristics of routing protocols include the manner in which they avoid routing loops, the manner in which they select preferred routes, using information about hop costs, the time they require to reach routing convergence, their scalability, and other factors such as relay multiplexing and cloud access framework parameters. Certain additional characteristics such as multilayer interfacing may also be employed as a means of distributing uncompromised networking gateways to authorized ports. This has the added benefit of preventing issues with routing protocol loops.

Many routing protocols are defined in technical standards documents called RFCs

2.9   Interior gateway protocols

An interior gateway protocol (IGP) is a type of routing protocol used for exchanging routing table information between gateways (commonly routers) within an autonomous system (for example, a system of corporate local area networks). This routing information can then be used to route network-layer protocols like IP.

Interior gateway protocols can be divided into two categories: **distance-vector** routing protocols and **link-state** routing protocols.

2.9.1   link state routing protocols

Link-state routing protocols are one of the two main classes of routing protocols used in packet switching networks for computer communications, the other being distance-vector routing protocols. Examples of link-state routing protocols include Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS).

The link-state protocol is performed by every switching node in the network (i.e., nodes that are prepared to forward packets; in the Internet, these are called routers). The basic concept of link-state routing is that every node constructs a map of the connectivity to the network, in the form of a graph, showing which nodes are connected to which other nodes. Each node then independently calculates the next best logical path from it to every possible destination in the network. Each collection of best paths will then form each node's routing table.

This contrasts with distance-vector routing protocols, which work by having each node share its routing table with its neighbours, in a link-state protocol the only information passed between nodes is connectivity related. Link-state algorithms are sometimes characterized informally as each router, "telling the world about its neighbors."

OSPF

Open Shortest Path First (OSPF) is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing (LSR) algorithm and falls into the group of interior gateway protocols (IGPs), operating within a single autonomous system (AS).

OSPF gathers link state information from available routers and constructs a topology map of the network. The topology is presented as a routing table to the Internet Layer for routing packets by their destination IP address. OSPF supports Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6) networks and supports the Classless Inter-Domain Routing (CIDR) addressing model.

OSPF is widely used in large enterprise networks. IS-IS, another LSR-based protocol, is more common in large service provider networks.

Originally designed in the 1980s, OSPF is defined for IPv4 in protocol version 2 by RFC 2328 (1998).[1] The updates for IPv6 are specified as OSPF Version 3 in RFC 5340 (2008).[2] OSPF supports the Classless Inter-Domain Routing (CIDR) addressing model.

2.9.2   distance vector routing protocols

A distance-vector routing protocol in data networks determines the best route for data packets based on distance. Distance-vector routing protocols measure the distance by the number of routers a packet has to pass; one router counts as one hop. Some distance-vector protocols also take into account network latency and other factors that influence traffic on a given route. To determine the best route across a network, routers using a distance-vector protocol exchange information with one another, usually routing tables plus hop counts for destination networks and possibly other traffic information. Distance-vector routing protocols also require that a router inform its neighbours of network topology changes periodically.

Distance-vector routing protocols use the Bellman–Ford algorithm to calculate the best route. Another way of calculating the best route across a network is based on link cost, and is implemented through link-state routing protocols.

The term distance vector refers to the fact that the protocol manipulates vectors (arrays) of distances to other nodes in the network. The distance vector algorithm was the original ARPANET routing algorithm and was implemented more widely in local area networks with the Routing Information Protocol (RIP).

RIP

The Routing Information Protocol (RIP) is one of the oldest distance-vector routing protocols which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination. The largest number of hops allowed for RIP is 15, which limits the size of networks that RIP can support.

RIP implements the split horizon, route poisoning, and holddown mechanisms to prevent incorrect routing information from being propagated.

In RIPv1 routers broadcast updates with their routing table every 30 seconds. In the early deployments, routing tables were small enough that the traffic was not significant. As networks grew in size, however, it became evident there could be a massive traffic burst every 30 seconds, even if the routers had been initialized at random times.

In most networking environments, RIP is not the preferred choice of routing protocol, as its time to converge and scalability are poor compared to EIGRP, OSPF, or IS-IS. However, it is easy to configure, because RIP does not require any parameters, unlike other protocols.

RIP uses the User Datagram Protocol (UDP) as its transport protocol, and is assigned the reserved port number 520.

EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) is an advanced distance-vector routing protocol that is used on a computer network for automating routing decisions and configuration. The protocol was designed by Cisco Systems as a proprietary protocol, available only on Cisco routers. Functionality of EIGRP was converted to an open standard in 2013 and was published with informational status as RFC 7868 in 2016.

EIGRP is used on a router to share routes with other routers within the same autonomous system. Unlike other well known routing protocols, such as RIP, EIGRP only sends incremental updates, reducing the workload on the router and the amount of data that needs to be transmitted.

EIGRP replaced the Interior Gateway Routing Protocol (IGRP) in 1993. One of the major reasons for this was the change to classless IPv4 addresses in the Internet Protocol, which IGRP could not support.

2.10 Exterior gateway protocols

An exterior gateway protocol is a routing protocol used to exchange routing information between autonomous systems. This exchange is crucial for communications across the Internet. Notable exterior gateway protocols include Exterior Gateway Protocol (EGP), now obsolete, and Border Gateway Protocol (BGP)[6][7.5]:

---

[6] Hunt, Craig (2002). TCP/IP network administration (3 ed.). O'Reilly Media. ISBN 9781449391430. OCLC 52356435. Archived from the original on 1 July 2020. Retrieved 5 November 2021 – via Dokuz Eylül University.

2.10.1   BGP

Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet. BGP is classified as a path-vector routing protocol, and it makes routing decisions based on paths, network policies, or rule-sets configured by a network administrator.

BGP used for routing within an autonomous system is called Interior Border Gateway Protocol, Internal BGP (iBGP). In contrast, the Internet application of the protocol is called Exterior Border Gateway Protocol, External BGP (eBGP).

2.11   IoT

The **Internet of things** describes physical objects with sensors, processing ability, software, and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks.Internet of things has been considered a misnomer because devices do not need to be connected to the public internet, they only need to be connected to a network and be individually addressable.

2.12   IoT in Aviation

With the inclusion of digital technologies, the airline industry has now been able to deliver unique customer experiences, simplified underlying processes, and most importantly enhancing the productivity of the workforce. The next stride in leveraging IoT can lead to the exploration of newer dimensions in the aviation industry. Combining IoT with other technologies like AI and robotics would generate a number of opportunities related to service delivery improvement. Further, a smart IoT ecosystem can bring in all the required entities and assets together in the industry value chain and make it look like the new normal.

2.12.1   Existing Technologies in Aviation Industry

Digitized Security

Today, state-of-the-art technology is being developed for implementing advanced concepts such as "walk through security" to reduce the passenger waiting times. Biometrics are also being used for automating the verification processes, thus reducing the burden of staffing.

Security systems are increasingly becoming a major technology trend at the airport terminals as these are equipped with the latest security system for security purposes.

VR for Last-Minute Changes

A leading global aviation company has been testing a new way for its passengers to upgrade their tickets by allowing them premium seats using VR. The airline company allows passengers to upgrade at the last minute. The airline company said that the best way for understanding the benefits of a premium economy, that has extra legroom and seat pitch can be done virtualized using VR.

Biometrics

Biometrics are being potentially used by the aviation industry for some time now and is gaining a stronghold across this industry vertical. Some of the biggest airports across the world have invested in fingerprint and facial recognition technology. The aviation industry emphasizes on using facial recognition so that the passenger's face becomes the new passport. Also at various airports, biometric-based recognition is being implemented at the airport lounge entrance and integrating this technology with flight information display systems for serving the passengers with a higher degree of personalized information along with offers.

2.12.2   IoT Adoption Challenges

Following are some key challenges that are to be addressed for implementing IoT on a wide scale. These are inclusive of -

- Most of the airline companies operate on a global level spread across diversified geographical boundaries. Each of these geographies has its own cultural diversity as well as technological adaptability. A successfully implemented IoT needs to support these regional variations.

- The airline industry operates in a top-notched secure environment. Thus, security and privacy need to be the top priority for implementing IoT in the aviation industry. Privacy can also be seen as a critical issue whenever there is a deployment of advanced technologies such as facial recognition as an outcome of the large volume of passenger's private data.

2.12.3   Opportunities for IoT in Aviation

IoT offers a number of tremendous benefits to the aviation industry and its rippling effects include- reduced travel times, enhancing the comfort levels of passengers with better security levels. In order to fully realize the **IoT** opportunities, the businesses and governments need to coordinate with the same frequency for answering the political as well as business issues related to IoT.
This disruptive technology holds several benefits when it comes to the aviation industry -

- When sensors are embedded in connected objects, it can be used for controlling, monitoring and collecting accurate real-time data. Sensors have significantly improved over the past few years. Wireless can be a key driver behind the emergence of IoT devices that operate on Wi-Fi or a strong cellular network such as 5G. Using a low-power wide area network (LPWAN) could be used for enriching the performance of sensors that offer low bandwidth.

- Cloud Computing can be used for creating a common platform for handling and integrating data from several sources like- people, their processes and their systems (devices). Real-time data can be utilized for gaining purposeful insights from current market data ad then distribute this information to the customers in a very short span of time.

- The airport terminals can duplicate the underlying concept of **smart cities**, thereby, implementing advanced technologies besides improved methods for collecting data to mine out the meaningful real-time insights. The use of sensor data could be done for improving operations and cumulative passenger experience. Multiple data sets can be integrated, optimized and analyzed for developing smarter applications and services related to airports, aircraft, and passengers.

- Beacons offer tremendous scope for IoT gateways. These can be placed across the entire airport infrastructure for triggering notifications on the passenger's mobile as soon as he is in the beacon's range. These notifications could be related to time, flight status or even displaying an e-boarding pass on the passenger's mobile. This, in turn, provides the passenger with more accurate information every time. This can even help the airline crew for determining how far is the passenger from the airline in order to determine how long they need to wait before the actual take-off.

2.13   IPv6

Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion, and is intended to replace IPv4[7].

2.13.1   IPsec

Internet Protocol Security (IPsec) was originally developed for IPv6, but found widespread deployment first in IPv4, for which it was re-engineered. IPsec was a mandatory part of all IPv6 protocol implementations,[8] and Internet Key Exchange (IKE) was recommended, but with RFC 6434 the inclusion of IPsec in IPv6 implementations was downgraded to a recommendation because it was considered impractical to require full IPsec implementation for all types of devices that may use IPv6.

FIGURE 2.12: IPv6 8-bytes Format

However, as of RFC 4301 IPv6 protocol implementations that do implement IPsec need to implement IKEv2 and need to support a minimum set of cryptographic algorithms. This requirement will help to make IPsec implementations more interoperable between devices from different vendors. The IPsec Authentication Header (AH) and the Encapsulating Security Payload header (ESP) are implemented as IPv6 extension headers.[9]

2.13.2   Link-local address

In computer networking, a **link-local** address is a network address that is valid only for communications within the network segment or the broadcast domain that the host is connected to. Link-local addresses are most often assigned automatically with a process known as **stateless address autoconfiguration** or **link-local address autoconfiguration**,[10] also known as automatic private IP addressing (APIPA) or auto-IP.

---

[7]"FAQs". New Zealand IPv6 Task Force. Archived from the original on 29 January 2019. Retrieved 26 October 2015.

[8]S. Deering; R. Hinden (December 1998), Internet Protocol, Version 6 (IPv6) Specification, Internet Engineering Task Force (IETF), RFC 2

[9]Silvia Hagen (2014). IPv6 Essentials: Integrating IPv6 into Your IPv4 Network (3rd ed.). Sebastopol, CA: O'Reilly Media. p. 196. ISBN 978-1-4493-3526-7. OCLC 881832733.

[10]S. Cheshire; B. Aboba; E. Guttma (May 2005). Dynamic Configuration of IPv4 Link-Local Addresses. The Internet Society. doi:10.17487/RFC3927. RFC 3927.

In the Internet Protocol Version 6 (IPv6), the address block fe80::/10 has been reserved for link-local unicast addressing.[11][2.4] (IETF), RFC 2Of the 64 bits of a link-local addresses' network component, the most significant 10 bits (1111111010) correspond to the IANA-reserved "global routing prefix" for link-local addresses, while the "subnet ID" (the remaining 54 bits) is zero.[11][2.5.6]

10 bits	54 bits	64 bits
1111111010	000 ... 000	Interface ID

FIGURE 2.13: IPv6 8-bytes Format

Unlike IPv4, IPv6 requires a link-local address on every network interface on which the IPv6 protocol is enabled, even when routable addresses are also assigned.[11][2.8]

Consequently, IPv6 hosts usually have more than one IPv6 address assigned to each of their IPv6-enabled network interfaces. The link-local address is required for IPv6 sublayer operations of the Neighbor Discovery Protocol, as well as for some other IPv6-based protocols, such as DHCPv6.

When using an IPv6 link-local address to connect to a host, a zone index must be added to the address so that the packets can be sent out on the correct interface.

In IPv6, addresses may be assigned by stateless (automatic) or stateful (manual) mechanisms. Stateless address autoconfiguration is performed as a component of the Neighbor Discovery Protocol (NDP).[12] The address is formed from its routing prefix and a unique identifier for the network interface.

Through NDP routing prefix advertisements, a router or server host may announce configuration information to all link-attached interfaces which causes additional IP address assignment on the receiving interfaces for local or global routing purposes. This process is sometimes also considered stateless, as the prefix server does not receive or log any individual assignments to hosts. Uniqueness is guaranteed automatically by the address selection methodology. It may be MAC-address based,[12][1] or randomized.[13] Automatic duplicate address detection algorithms prevent assignment errors.

2.14   IPv4

Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP). It is one of the core protocols of standards-based internetworking methods in the Internet and other packet-switched networks.

IPv4 was the first version deployed for production on SATNET in 1982 and on the ARPANET in January 1983. It is still used to route most Internet traffic today,[14] even with the ongoing deployment of Internet Protocol version 6 (IPv6),[15] its successor.

IPv4 uses a 32-bit address space which provides 4,294,967,296 (2^{32}) unique addresses, but large blocks are reserved for special networking purposes.[16] [17]

2.14.1   conversion to binary

[11] R. Hinden; S. Deering (February 2006). IP Version 6 Addressing Architecture. IETF. doi:10.17487/RFC4291. RFC 4291. Updated by RFC 5952, RFC 6052, RFC 7136, RFC 7346, RFC 7371, RFC 8064.

[12] S. Thomson; T. Narten; T. Jinmei (September 2007). IPv6 Stateless Address Autoconfiguration. Network Working Group. doi:10.17487/RFC4862. RFC 4862. Obsoletes RFC 2462. Updated by RFC 7527.

[13] F. Gont; S. Krishnan; T. Narten; R. Draves (February 2021). Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6. IETF. doi:10.17487/RFC8981. ISSN 2070-1721. RFC 8981. Obsoletes RFC 4941.

[14] "BGP Analysis Reports". Retrieved 2013-01-09.

[15] "IPv6 – Google". www.google.com. Retrieved 2022-01-28.

[16] "IANA IPv4 Special-Purpose Address Registry". www.iana.org. Retrieved 2022-01-28.

[17] "RFC 5735 - Special Use IPv4 Addresses". datatracker.ietf.org. Retrieved 2022-01-28.

First a couple of words on the binary code first. A binary code is essentially text, computer processor low level instructions, or any other data using a two-symbol system. The two-symbol system used is often "0" and "1" from the **binary number system**. The binary code assigns a pattern of bits (aka binary digit), to each character, instruction, etc. For example, a binary string of eight bits can represent any of 256 possible values and can, therefore, represent a wide variety of different items. In computing and telecommunications, binary codes are used for various methods of encoding data, such as character strings, into bit strings.

FIGURE 2.14: IPv6 8-bytes Format

Let's now convert 192.168.2.7 into binary

Division by 2	Quotient	Remainder	Notes
192/2	96	0	This will be the 8th bit
96/2	48	0	The 7th bit
48/2	24	0	The 6th bit
24/2	12	0	The 5th bit
12/2	6	0	The 4th bit
6/2	3	0	The 3th bit
3/2	1	1	The 2nd bit
1/2	0	1	The 1st bit

2.15   binary to Hex

The hexadecimal system uses the number 16 as its base. As a $base^{16}$ numeral system, it uses 16 symbols. These are the 10 decimal digits

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9$$

and the first six letters of the English alphabet

$$A, B, C, D, E, F$$

which are representing the values 10, 11, 12, 13, 14 and 15. This is useful in mathematics and IT as a more friendly way to represent binary. Each hex digit represents four binary digits; therefore you could say hex is a language to write binary in an abbreviated form. Four binary digits make up half a byte. This means one byte can carry binary values from 0000 0000 to 1111 1111. In hex, these can be represented ranging from 00 to FF. In html programming, colors can be represented by a 6-digit hexadecimal number: FFFFFF represents white whereas 000000 represents black. Hex is more friendly in terms of possibility. It goes from 0 to 9 and then from A to F. It's The calculator has a **programmer** mode which allows you to use hex as well

2.16   IP config

Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, ipconfig displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters.

2.16.1   ipconfig/all

Displays the full TCP/IP configuration for all adapters. Adapters can represent physical interfaces, such as installed network adapters, or logical interfaces, such as dial-up connections.

2.16.2   ipconfig/displaydns

Displays the contents of the DNS client resolver cache, which includes both entries preloaded from the local Hosts file and any recently obtained resource records for name queries resolved by the computer. The DNS Client service uses this information to resolve frequently queried names quickly, before querying its configured DNS servers.

The fields in the output of /displaydns correspond to the fields of an actual DNS reply.

- In a DNS server's database, each piece of data is a "resource record".

- "Record name" is the name you query DNS for, and the records (addresses or something else) belong to that name.

- "Record type" is the type, displayed as a number - although more commonly they are referred to by their names, internally (in the DNS protocol) each has a number. Type 1 is "A" for "address", an IPv4 address. (IPv6 uses type 28, "AAAA", for an address four times as long.) "PTR", type 12, is a "pointer" to a hostname - most commonly used when mapping an IP address back to its name. "CNAME" is "canonical name".

- "Time To Live" is the time in seconds after which the cache entry must expire.

- "Data Length" appears to be the length in bytes - an IPv4 address is four bytes, IPv6 is sixteen bytes. For CNAME or PTR, Windows displays a static number (either 4 or 8, depending on your system) - this is actually the size of a memory address where the actual text is kept.

- The "answer" section of a DNS reply is the actual answer to the query, and "additional" contains information that will likely be needed to find the actual answer. For example, glue records.

- "<type> record" shows the actual value stored.

2.16.3   ipconfig/flushdns

Flushes and resets the contents of the DNS client resolver cache. During DNS troubleshooting, you can use this procedure to discard negative cache entries from the cache, as well as any other entries that have been added dynamically.

2.16.4   ipconfig/registerdns

Initiates manual dynamic registration for the DNS names and IP addresses that are configured at a computer. You can use this parameter to troubleshoot a failed DNS name registration or resolve a dynamic update problem between a client and the DNS server without rebooting the client computer. The DNS settings in the advanced properties of the TCP/IP protocol determine which names are registered in DNS.

2.16.5   ipconfig/flushdns-

By default, most operating systems will cache IP addresses and other Domain Name System (DNS) records in order to fulfill future requests more quickly.

For example, when I type in https://lonezscents.com/ in my browser's address bar for the first time, the browser has to ask DNS servers where to find the site. Once it has that information, the browser can store it in its local cache. Then, the next time I type in that website address, the browser will look for its DNS information in the local cache first and be able to find the site more quickly.

The problem is that sometimes dangerous IP addresses or corrupted results can be cached and need to be removed. The DNS cache can also impact your ability to connect to the internet or cause other issues. Whatever the reason, all major operating systems allow you to force the process of clearing this cache — or "flushing DNS."

what flush DNS does

Flushing DNS will clear any IP addresses or other DNS records from your cache. This can help resolve security, internet connectivity, and other issues.

It's important to understand that your DNS cache will clear itself out from time to time without your intervention. That's because the DNS cache — in addition to saving all information that's relevant to identifying and finding a website — also saves a component called TTL, or time to live. This specifies a period of time (in seconds) in which the DNS record for a site remains valid. Within this time period, any queries to the website are answered from the local cache without the help of the DNS server. Once the TTL expires, the entry will be removed from the cache.

However, there are reasons you may need to force a DNS flush rather than wait for the TTL of all the entries to expire. Let's take a look at why below.

why would you flush DNS

There's a few reasons you might need to flush your DNS cache. These reasons may have to do with security, technical problems, or data privacy. Let's briefly cover each one below.

- **You want to prevent DNS spoofing**. DNS spoofing — also known as DNS cache poisoning — is an attack in which bad actors gain access to your DNS cache and alter the information in order to redirect you to the wrong sites. In some cases, they will redirect you to a fraudulent website that resembles its intended destination so that you enter in sensitive information, like your online banking login information.

- **You're seeing a 404 error**. Let's say you've cached the DNS information of a site that's since moved to a new domain name or host. In that case, the DNS information on your computer may not get updated right away and you could end up seeing a 404 error or an outdated version of a site

when you try to visit. Although the information will eventually get updated in your DNS cache, you don't have to wait. You can clear DNS cache at any time.

- **You're having trouble accessing a website**. If you're having trouble getting a website to load, then you should try other steps first, like clearing your browser's temporary files and cookies and adjusting your browser settings to turn off pop-up blockers and allow sites to save and read cookies. But if you've exhausted your options, then you can flush DNS to reset your computer's connection to the internet.

- **You want to keep your search behavior private**. When you think of tracking user behavior on the internet, you probably think of cookies — but the DNS cache can reveal your search history as well. That's because the DNS cache is designed to act like a virtual address book, storing the information of the websites you visit regularly. To keep this information away from data collectors or bad actors on the web, it's a good idea to regularly flush your DNS cache.

Now that we understand what flushing your DNS cache means and why you'd want to, let's walk through how you can do it below.

2.17 DHCP

2.17.1 IPCONFIG renew and release

The host asks the router to drop the network configuration and make a new one

2.17.2 BYOD

Bring your own device

2.17.3 vulnerabilities in LAN

Poor configuration and Poor encryption

Poor configuration

Poor encryption

2.17.4 Fixed IP

So that someone doesn't just plug a device and gets an IP-address from DHCP. A device needs to be approved in order to receive an IP

2.18 dns root server

There are 13 important DNS root servers on the internet that store a complete database of domain names and their associated public IP addresses. These top-tier DNS servers are named A through M for the first 13 letters of the alphabet.Ten of these servers are in the US, one in London, one in Stockholm, and one in Japan

2.18.1   why 13 DNS servers

That's exactly how much we need with IPv4. The IP packet size is 2 bytes.

2.18.2   who manages

The Internet Assigned Numbers Authority (IANA) keeps this list of DNS root servers if you're interested. ICANN manages them as well by delegating to IANA. It stands for Internet Corporation for Assigned Names and Numbers.

2.19   The DNS Service

The DNS service is the practical implementation of the DNS System. The DNS service is what a server running DNS software offers - the ability to use and manage DNS settings. Today, the DNS service is a very popular offer, with almost every domain registrar company offering their own DNS service. The DNS service can be run on a separate server, which is effective if running a very large and popular website, and can also be run on a shared hosting server, which is sufficient in 90% of the cases.

- recursive = non-authoritative

- non-recursive = authoritative

2.20   The four DNS Servers to load a webpage

Once a DNS query is entered, it passes through a few different servers before resolution, without any end-user interaction.

2.20.1   DNS recursor

This is a server designed specifically to receive queries from client machines. It tracks down the DNS record and makes additional requests to meet the DNS queries from the client. The number of requests can be decreased with DNS caching when the requested resources are returned to the recursor early on in the lookup process.

2.20.2   Root name server

This server does the job of translating the human-friendly hostnames into computer-friendly IP addresses. The root server accepts the recursor's query and sends it to the TLD nameservers in the next stage, depending on the domain name seen in the query.

2.20.3   dns server

Top-Level Domain (TLD) nameserver
    The TLD nameservers are responsible for maintaining the information about the domain names. For example, they could contain information about websites ending in ".com" or ".org" or country-level domains like "www.example.com.uk", "www.example.com.us", and others. The TLD nameserver will take the query

from the root server and point it to the authoritative DNS nameserver associated with the query's particular domain.

2.20.4 Authoritative nameserver

In the last step, the authoritative DNS nameserver will return the IP address back to the DNS recursor that can relay it to the client. This authoritative DNS nameserver is the one at the bottom of the lookup process that holds the DNS records. Think of these as the last stop or the final authoritative source of truth in the process.

2.21 public dns

public dns

2.22 private dns

private dns

2.23 dns authentication

dns authentication

2.24 PING

Ping is a computer network administration software utility used to test the reachability of a host on an Internet Protocol (IP) network. It is available for virtually all operating systems that have networking capability, including most embedded network administration software

Ping measures the round-trip time for messages sent from the originating host to a destination computer that are echoed back to the source. The name comes from active sonar terminology that sends a pulse of sound and listens for the echo to detect objects under water.[1]

Ping operates by means of Internet Control Message Protocol (ICMP) packets. Pinging involves sending an ICMP echo request to the target host and waiting for an ICMP echo reply. The program reports errors, packet loss, and a statistical summary of the results, typically including the minimum, maximum, the mean round-trip times, and standard deviation of the mean.

The command-line options of the ping utility and its output vary between the numerous implementations. Options may include the size of the payload, count of tests, limits for the number of network hops (TTL) that probes traverse, interval between the requests and time to wait for a response. Many systems provide a companion utility ping6, for testing on Internet Protocol version 6 (IPv6) networks, which implement ICMPv6.

2.25 loopback

Loopback (also written loop-back) is the routing of electronic signals or digital data streams back to their source without intentional processing or modification. It is primarily a means of testing the communications

infrastructure.

There are many example applications. It may be a communication channel with only one communication endpoint. Any message transmitted by such a channel is immediately and only received by that same channel. In telecommunications, loopback devices perform transmission tests of access lines from the serving switching center, which usually does not require the assistance of personnel at the served terminal. Loop around is a method of testing between stations that are not necessarily adjacent, wherein two lines are used, with the test being done at one station and the two lines are interconnected at the distant station. A patch cable may also function as loopback, when applied manually or automatically, remotely or locally, facilitating a loop-back test.

Where a system (such as a modem) involves round-trip analog-to-digital processing, a distinction is made between analog loopback, where the analog signal is looped back directly, and digital loopback, where the signal is processed in the digital domain before being re-converted to an analog signal and returned to the source.

2.26 subnet

A subnetwork or subnet is a logical subdivision of an IP network.[1]:1,16 The practice of dividing a network into two or more networks is called subnetting.

Computers that belong to the same subnet are addressed with an identical most-significant bit-group in their IP addresses. This results in the logical division of an IP address into two fields: the network number or routing prefix and the rest field or host identifier. The rest field is an identifier for a specific host or network interface.

The routing prefix may be expressed in Classless Inter-Domain Routing (CIDR) notation written as the first address of a network, followed by a slash character (/), and ending with the bit-length of the prefix. For example, 198.51.100.0/24 is the prefix of the Internet Protocol version 4 network starting at the given address, having 24 bits allocated for the network prefix, and the remaining 8 bits reserved for host addressing. Addresses in the range 198.51.100.0 to 198.51.100.255 belong to this network, with 198.51.100.255 as the subnet broadcast address. The IPv6 address specification 2001:db8::/32 is a large address block with 296 addresses, having a 32-bit routing prefix.

For IPv4, a network may also be characterized by its subnet mask or netmask, which is the bitmask that, when applied by a bitwise AND operation to any IP address in the network, yields the routing prefix. Subnet masks are also expressed in dot-decimal notation like an IP address. For example, the prefix 198.51.100.0/24 would have the subnet mask 255.255.255.0.

Traffic is exchanged between subnetworks through routers when the routing prefixes of the source address and the destination address differ. A router serves as a logical or physical boundary between the subnets.

The benefits of subnetting an existing network vary with each deployment scenario. In the address allocation architecture of the Internet using CIDR and in large organizations, it is necessary to allocate address space efficiently. Subnetting may also enhance routing efficiency, or have advantages in network management when subnetworks are administratively controlled by different entities in a larger organization. Subnets may be arranged logically in a hierarchical architecture, partitioning an organization's network address space into a tree-like routing structure, or other structures such as meshes.

2.27   Broadcast address

A broadcast address is a network address used to transmit to all devices connected to a multiple-access communications network. A message sent to a broadcast address may be received by all network-attached hosts.

In contrast, a multicast address is used to address a specific group of devices, and a unicast address is used to address a single device.

For network layer communications, a broadcast address may be a specific IP address. At the data link layer on Ethernet networks, it is a specific MAC address

2.27.1   single Broadcast address

this is a consequence of having only one subnet, creating unnecessary traffic.

A task left is to create 2 subnets in the same local network

2.27.2   vlans

to make sure every subnet is isolated

2.28   Multicast

In computer networking, multicast is group communication[1] where data transmission is addressed to a group of destination computers simultaneously. Multicast can be one-to-many or many-to-many distribution.[2] Multicast should not be confused with physical layer point-to-multipoint communication.

Group communication may either be application layer multicast[1] or network-assisted multicast, where the latter makes it possible for the source to efficiently send to the group in a single transmission. Copies are automatically created in other network elements, such as routers, switches and cellular network base stations, but only to network segments that currently contain members of the group. Network assisted multicast may be implemented at the data link layer using one-to-many addressing and switching such as Ethernet multicast addressing, Asynchronous Transfer Mode (ATM), point-to-multipoint virtual circuits (P2MP)[3] or InfiniBand multicast. Network-assisted multicast may also be implemented at the Internet layer using IP multicast. In IP multicast the implementation of the multicast concept occurs at the IP routing level, where routers create optimal distribution paths for datagrams sent to a multicast destination address.

Multicast is often employed in Internet Protocol (IP) applications of streaming media, such as IPTV and multipoint videoconferencing.

IGMP

2.29   Unicast

In computer networking, unicast is a one-to-one transmission from one point in the network to another point; that is, one sender and one receiver, each identified by a network address.[18]

Unicast is in contrast to multicast and broadcast which are one-to-many transmissions.

---

[18]Godred Fairhurst "Unicast, Broadcast, and Multicast".

Internet Protocol unicast delivery methods such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are typically used.

2.30 The Five IPv4 Classes

In the IPv4 IP address space, there are five classes: A, B, C, D and E. Each class has a specific range of IP addresses (and ultimately dictates the number of devices you can have on your network). Primarily, class A, B, and C are used by the majority of devices on the Internet. Class D and class E are for special uses.

The list below shows the five available IP classes, along with the number of networks each can support and the maximum number of hosts (devices) that can be on each of those networks. The four octets that make up an IP address are conventionally represented by a.b.c.d - such as 127.10.20.30.

Additionally, information is also provided on private addresses and loop address (used for network troubleshooting).

2.30.1 Class A Public Private IP Address Range

Class A addresses are for networks with large number of total hosts. Class A allows for 126 networks by using the first octet for the network ID. The first bit in this octet, is always zero. The remaining seven bits in this octet complete the network ID. The 24 bits in the remaining three octets represent the hosts ID and allows for approximately 17 million hosts per network. Class A network number values begin at 1 and end at 127.

- Public IP Range: 1.0.0.0 to 127.0.0.0

- First octet value range from 1 to 127

- Private IP Range: 10.0.0.0 to 10.255.255.255

- Subnet Mask: 255.0.0.0 (8 bits)

- Number of Networks: 126

- Number of Hosts per Network: 16,777,214

2.30.2 Class B Public Private IP Address Range

Class B addresses are for medium to large sized networks. Class B allows for 16,384 networks by using the first two octets for the network ID. The first two bits in the first octet are always 1 0. The remaining six bits, together with the second octet, complete the network ID. The 16 bits in the third and fourth octet represent host ID and allows for approximately 65,000 hosts per network. Class B network number values begin at 128 and end at 191.

- Public IP Range: 128.0.0.0 to 191.255.0.0

- First octet value range from 128 to 191

- Private IP Range: 172.16.0.0 to 172.31.255.255

- Subnet Mask: 255.255.0.0 (16 bits)

- Number of Networks: 16,382

- Number of Hosts per Network: 65,534

2.30.3 Class C Public Private IP Address Range

Class C addresses are used in small local area networks (LANs). Class C allows for approximately 2 million networks by using the first three octets for the network ID. In a class C IP address, the first three bits of the first octet are always 1 1 0. And the remaining 21 bits of first three octets complete the network ID. The last octet (8 bits) represent the host ID and allows for 254 hosts per network. Class C network number values begins at 192 and end at 223.

- Public IP Range: 192.0.0.0 to 223.255.255.0

- First octet value range from 192 to 223

- Private IP Range: 192.168.0.0 to 192.168.255.255

- Special IP Range: 127.0.0.1 to 127.255.255.255

- Subnet Mask: 255.255.255.0 (24 bits)

- Number of Networks: 2,097,150

- Number of Hosts per Network: 254

2.30.4   Class D IP Address Range

Class D IP addresses are not allocated to hosts and are used for multicasting. Multicasting allows a single host to send a single stream of data to thousands of hosts across the Internet at the same time. It is often used for audio and video streaming, such as IP-based cable TV networks. Another example is the delivery of real-time stock market data from one source to many brokerage companies.

- Range: 224.0.0.0 to 239.255.255.255

- First octet value range from 224 to 239

- Number of Networks: N/A

- Number of Hosts per Network: Multicasting

2.30.5   Class E IP Address Class

Class E IP addresses are not allocated to hosts and are not available for general use. These are reserved for research purposes.

- Range: 240.0.0.0 to 255.255.255.255

- First octet value range from 240 to 255

- Number of Networks: N/A

- Number of Hosts per Network: Research/Reserved/Experimental