Networking

Daniele, Della Cioppa
daniele.dellacioppa@gmail.com

May 12, 2022

Contents

1 What it is

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

2 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

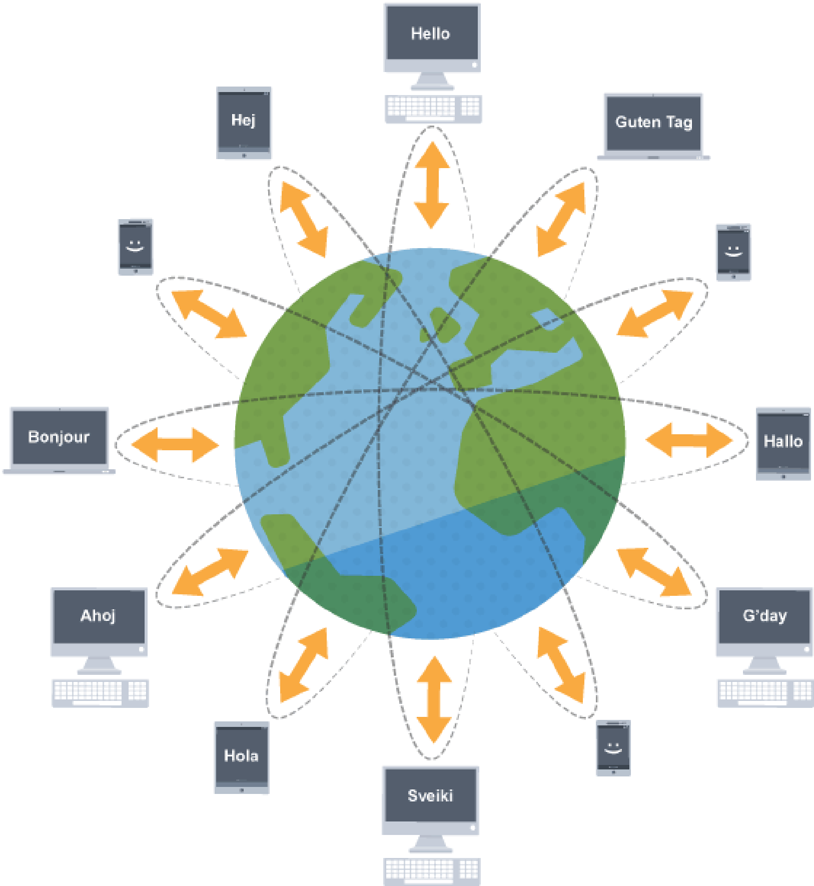


FIGURE 1: devices connected in the world

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

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

2.1 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. You can install a optic cable for a much longer distance and you won't get the same troubles you would get with copper cables for example

2.2 unguided wiring

This is Wi-Fi essentially. You can have a 2.4Ghz signal to reach longer distance but won't be nicely matched with a 5Ghz device

3 LAN vs WAN

LAN, which stands for local area network, and WAN, which stands for wide area network, are two types of networks that allow connection between computers. As the naming conventions suggest, LANs are for smaller, more localized networking — in a home, business, school, etc. — 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

4 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) sublayer of the data link layer for wired Ethernet networks.

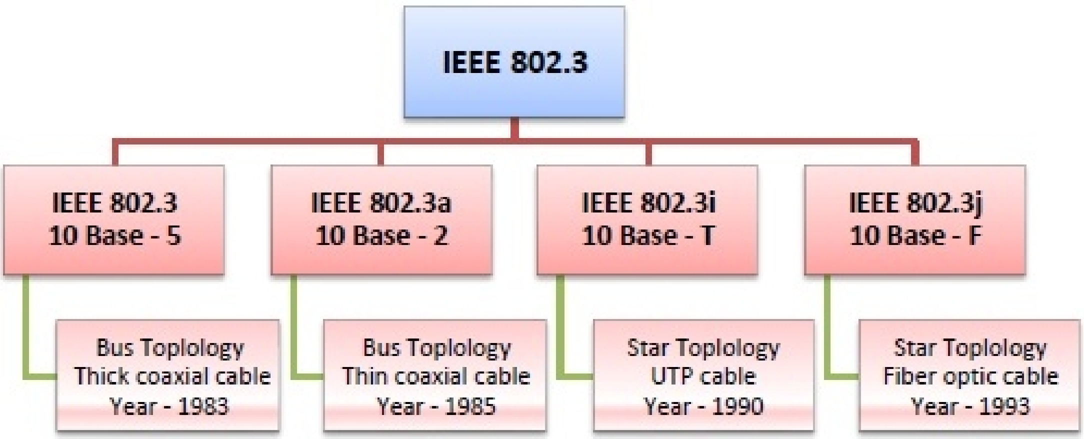


Figure 2: IEEE hierarchy

4.1 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 10BASE-5. It used a thick single coaxial cable into which a connection can be tapped by drilling into the cable to the core. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and 5 refers to the maximum segment length of 500m

- IEEE 802.3a: This gave the standard for thin coax (10BASE-2), which is a thinner variety where the segments of coaxial cables are connected by BNC connectors. The 2 refers to the maximum segment length of about 200m (185m to be precise)
- IEEE 802.3i: This gave the standard for twisted pair (10BASE-T) that uses unshielded twisted pair (UTP) copper wires as physical layer medium. The further variations were given by IEEE 802.3u for 100BASE-TX, 100BASE-T4 and 100BASE-FX
- IEEE 802.3j: This gave the standard for Ethernet over Fiber (10BASE-F) that uses fiber optic cables as medium of transmission

5 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

5.1 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.

OSI was introduced in 1983 by representatives of the major computer and telecom companies, and was adopted by ISO as an international standard in 1984.

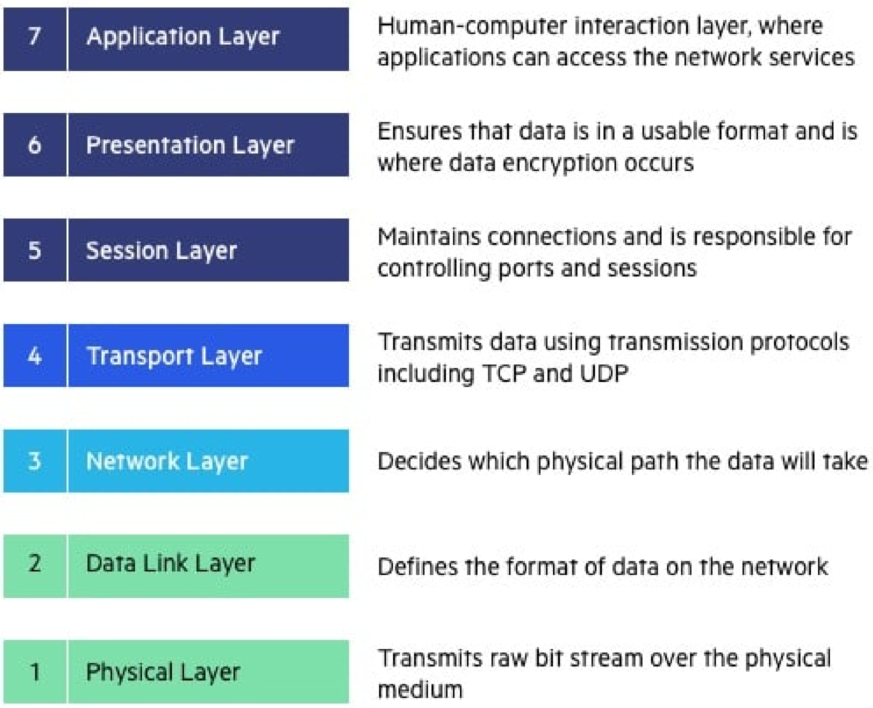


Figure 3: OSI Layer representation

5.2 A good Mnemonic

Every layer of the OSI model can be remembered with the mnemonic : Please Do Not Throw Sausage and Pizza Away

5.3 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

This may look drastically different from the OSI model, primarily because some functions are encompassed in a single layer: the application layer. In TCP/IP, this provides users with the physical standards, transport functions, network interface, and internetworking functions that correspond with the first three layers of the OSI model. In other words, in the TCP/IP model, these services are all done in the application layer.

TCP/IP is connection and connectionless

5.4 horizontal vs vertical approach

There's a debate on which one is vertical and which is horizontal so that point won't be discussed in this documents

6 ARP/RARP/DHCP

Address Resolution Protocol translates MAC addresses into IPs so that from the network layer we can communicate over the internet with IPs while RARP demands another computer (usually a server) to assign the demanding one with an IP which is essentially what DHCP is doing that's why RARP got obsolete

6.1 ARP Tables

These are used from every component in a network to know which MAC address the packet needs to point at On this machine for example all it needs to know is which is the MAC address of the gateway, and the TV who's connected in the same WiFi

```
_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
```

6.2 Three-way-handshake

This is when the client sends the ARP request to the server. The server does an aknowledgment and answers with an ARP reply saying both its MAC and its IP. It all happens like this :

When Computer 1 wants to talk to Computer 2 in a local area network by Ethernet cables and network switches, with no intervening gateways or routers. Computer 1 has a packet to send to Computer 2. Through DNS, it determines that Computer 2 has the IP address 192.168.0.55.

To send the message, it also requires Computer 2's MAC address. First, Computer 1 uses a cached ARP table to look up 192.168.0.55 for any existing records of Computer 2's MAC address (00:EB:24:B2:05:AC). If the MAC address is found, it sends an Ethernet frame containing the IP packet onto the link with the destination address 00:EB:24:B2:05:AC. If the cache did not produce a result for 192.168.0.55, Computer 1 has to send a broadcast ARP request message (destination FF:FF:FF:FF:FF:FF MAC address), which is accepted by all computers on the local network, requesting an answer for 192.168.0.55.

Computer 2 responds with an ARP response message containing its MAC and IP addresses. As part of fielding the request, Computer 2 may insert an entry for Computer 1 into its ARP table for future use.

Computer 1 receives and caches the response information in its ARP table and can now send the packet

7 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

7.1 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.

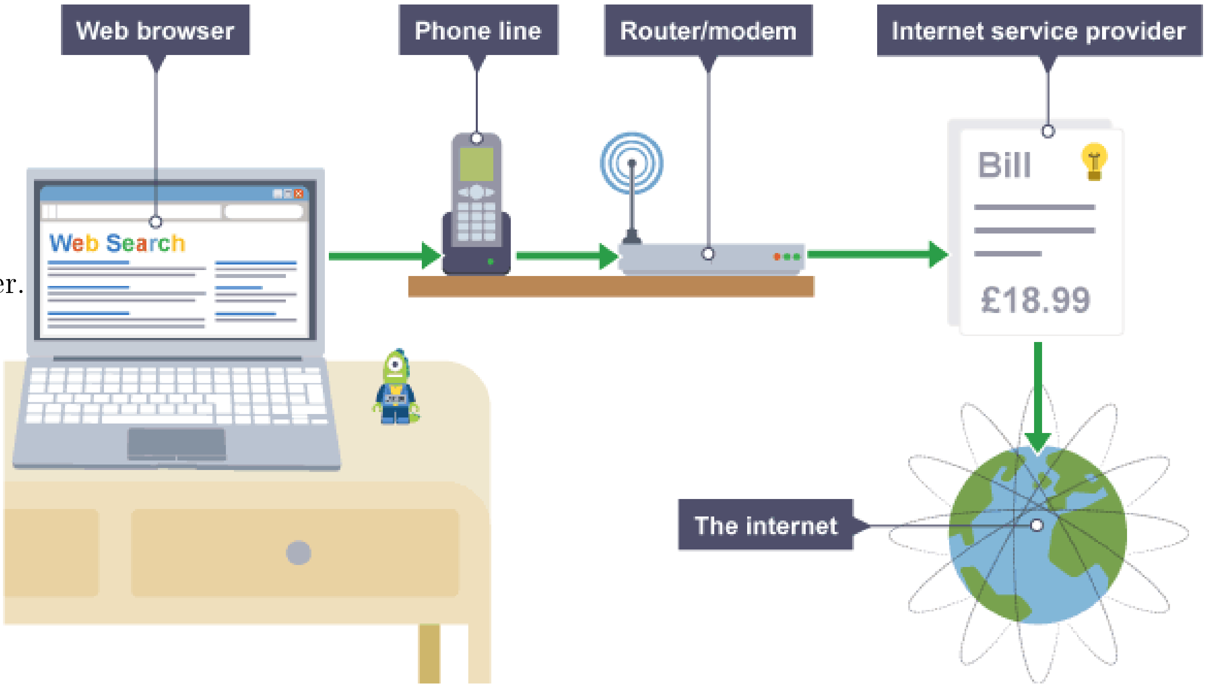


Figure 4: Router connecting devices in a LAN over the Internet

7.2 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.

7.3 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.

7.3.1 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.

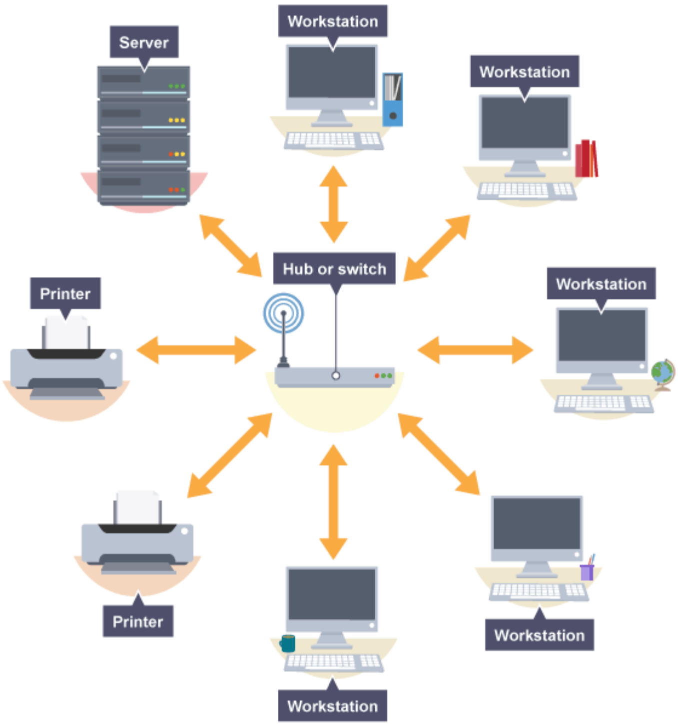


Figure 5: devices connected together

7.3.2 Bridges

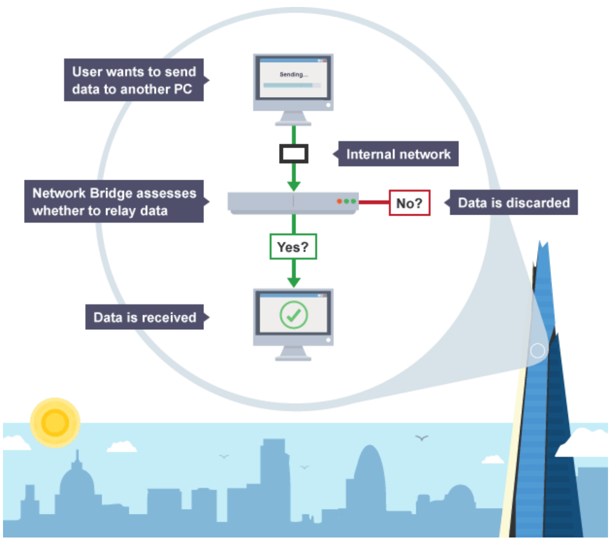


Figure 6: Bridge saving unnecessary data transfer

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 6)

7.3.3 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**

8 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.[2]

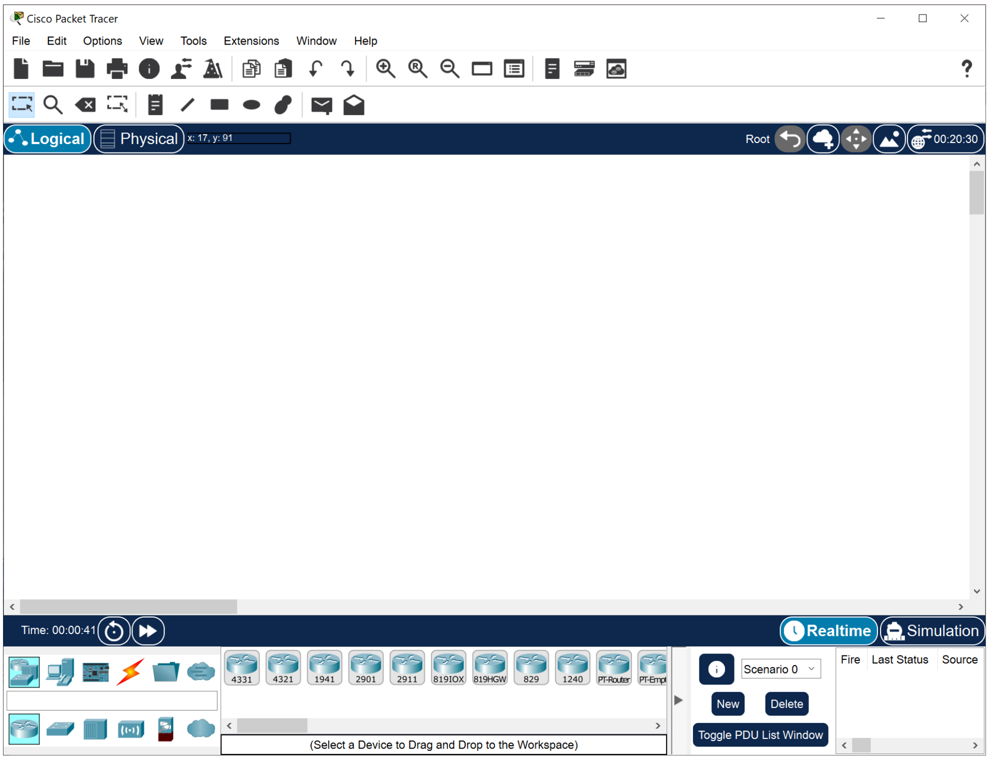
In this experiment we try to ping devices being set with 0 in the IP fields. Then we're gonna expand the network with more devices

- First nextwork has a 192.168.1.1 default gateway
- Second network has a 192.168.0.1 default gateway

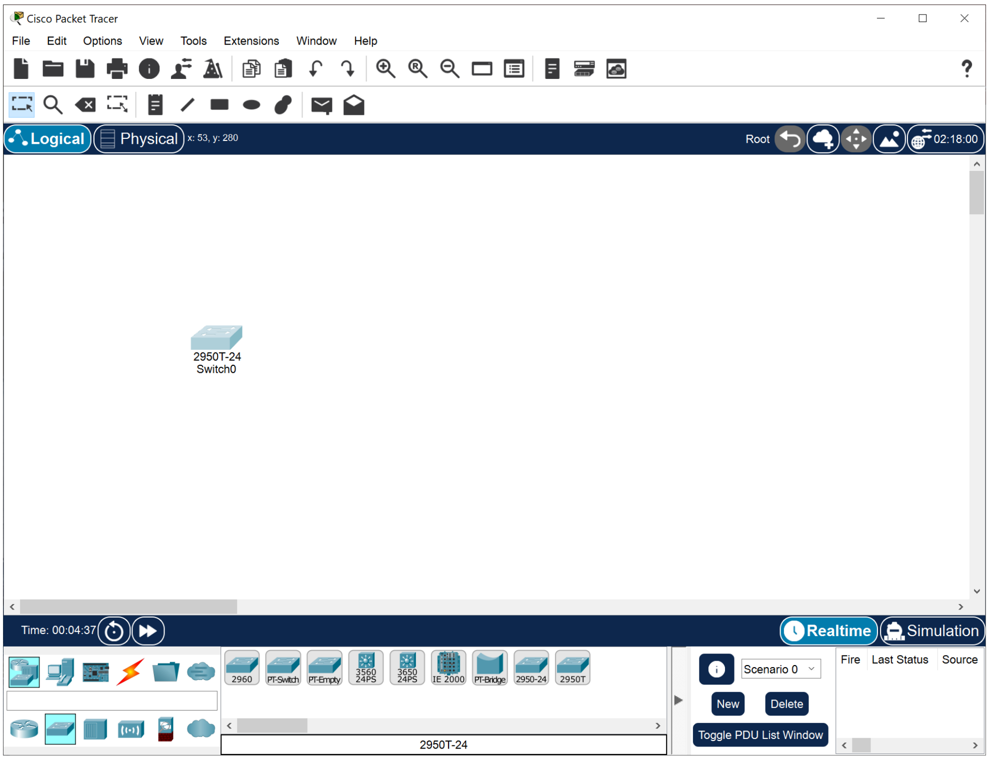
[2]Bakni, Michel; Cardinale, Yudith; Moreno, Luis Manuel (June 2018). **An Approach to Evaluate Network Simulators: An Experience with Packet Tracer**.Revista Venezolana de Computación. 5: 29–36. ISSN 2244-7040.
Javid,Sheikh Raashid (May 2014). **Role of Packet Tracer in learning Computer Networks**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

8.1 The step-by-step guide

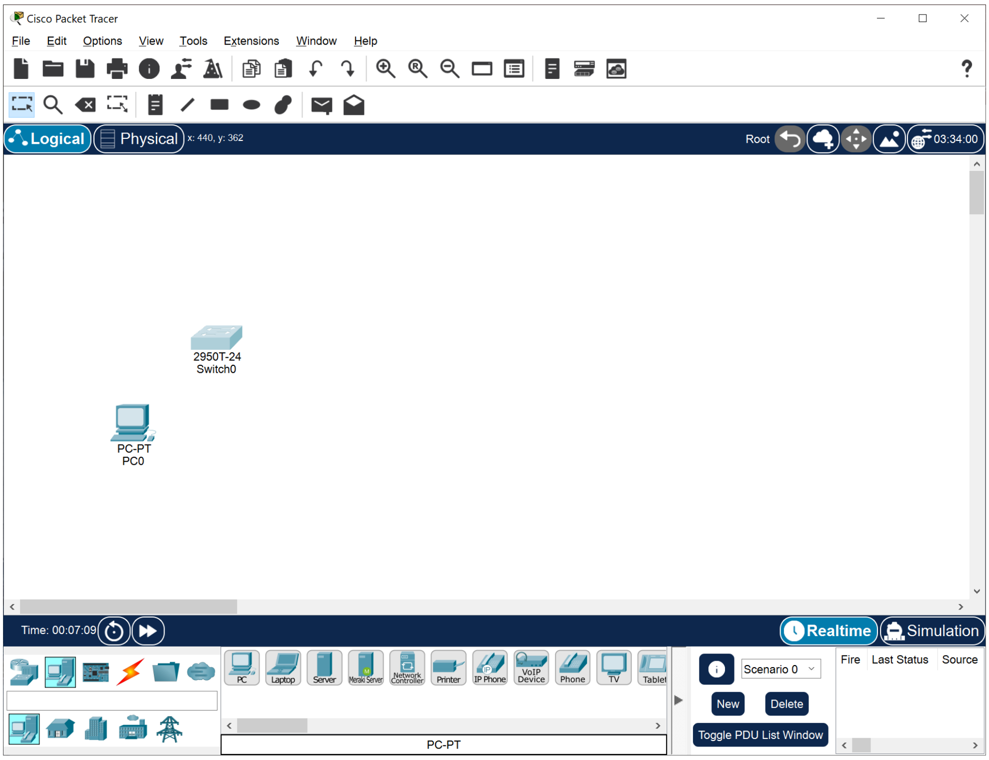
The following picture shows what we've got when we open Cisco Packet Tracer :



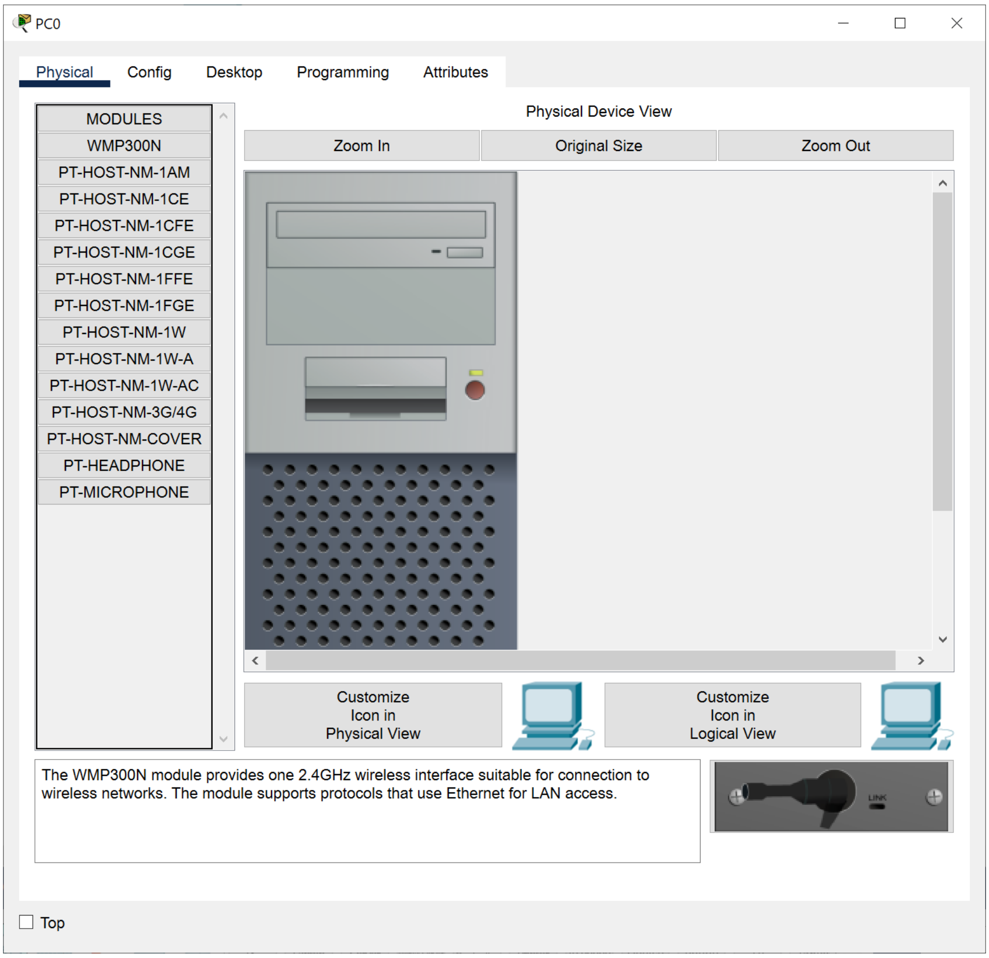
Now what we need to do is to add a switch :



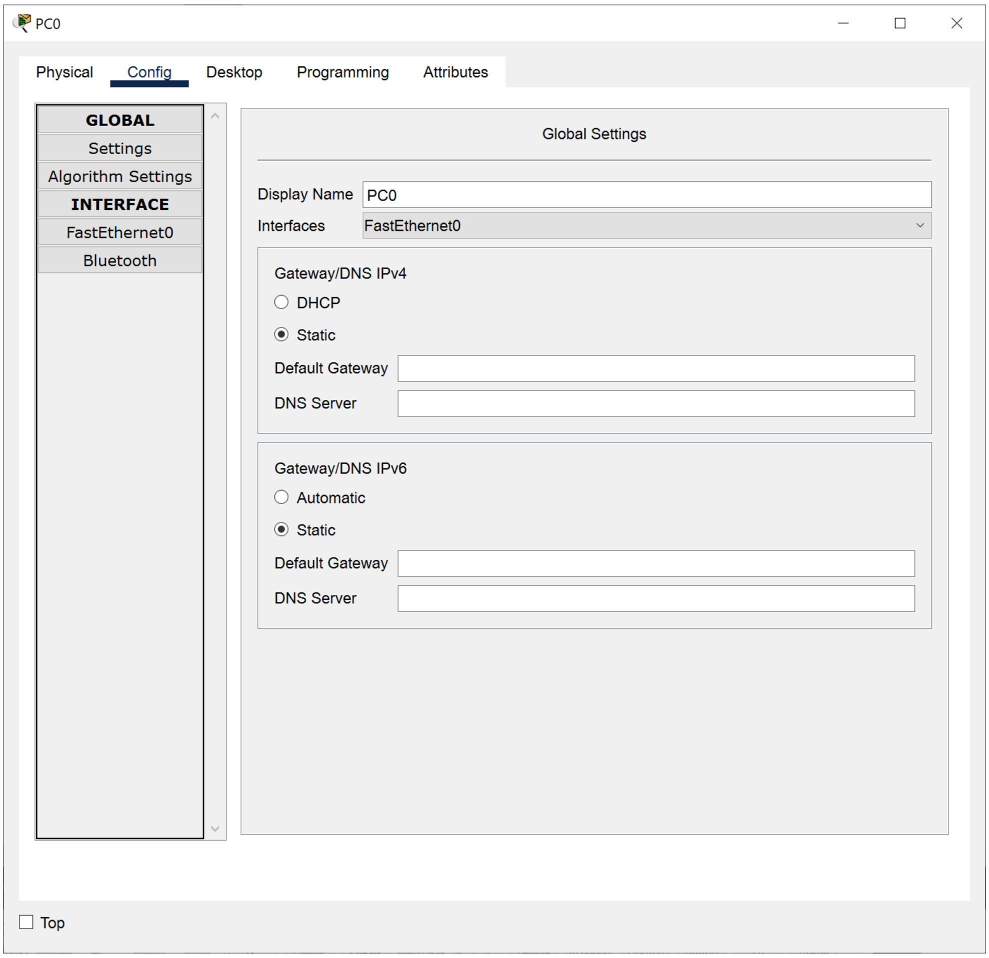
And then we add a computer :



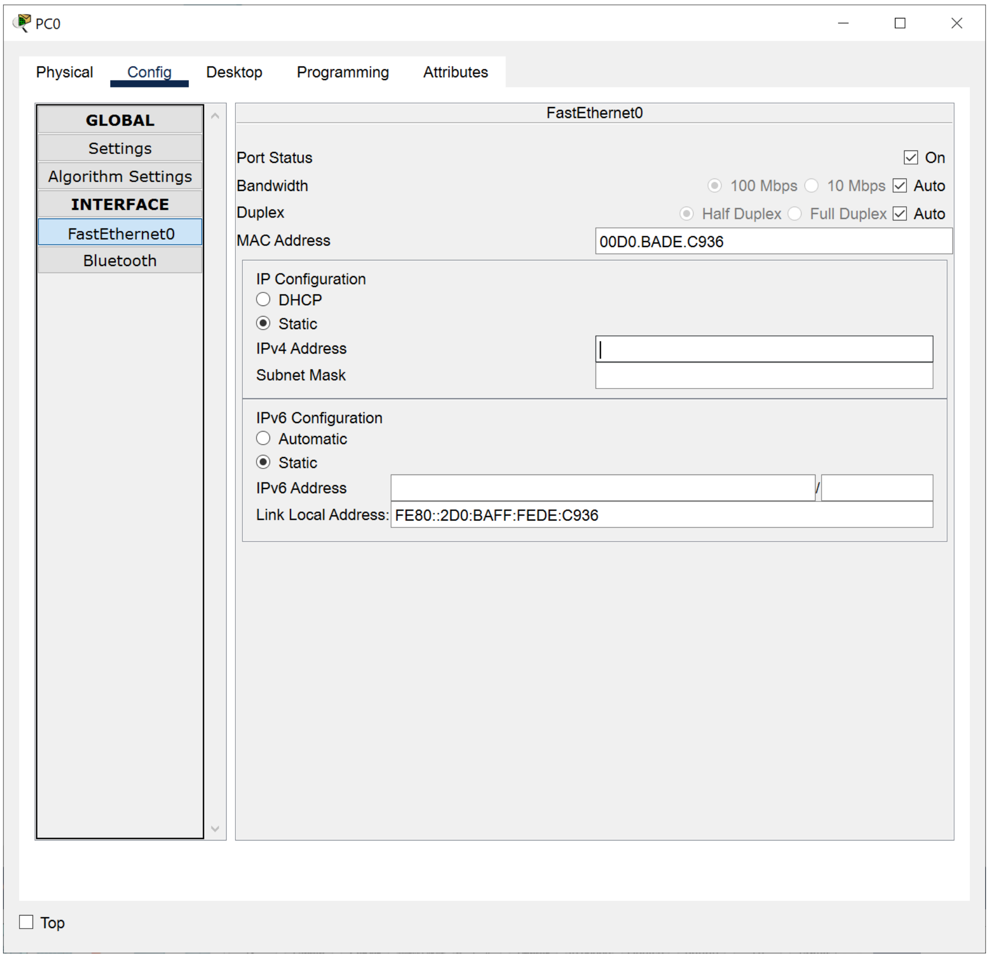
Now we click on the computer



And we move ourselves in the Config tab

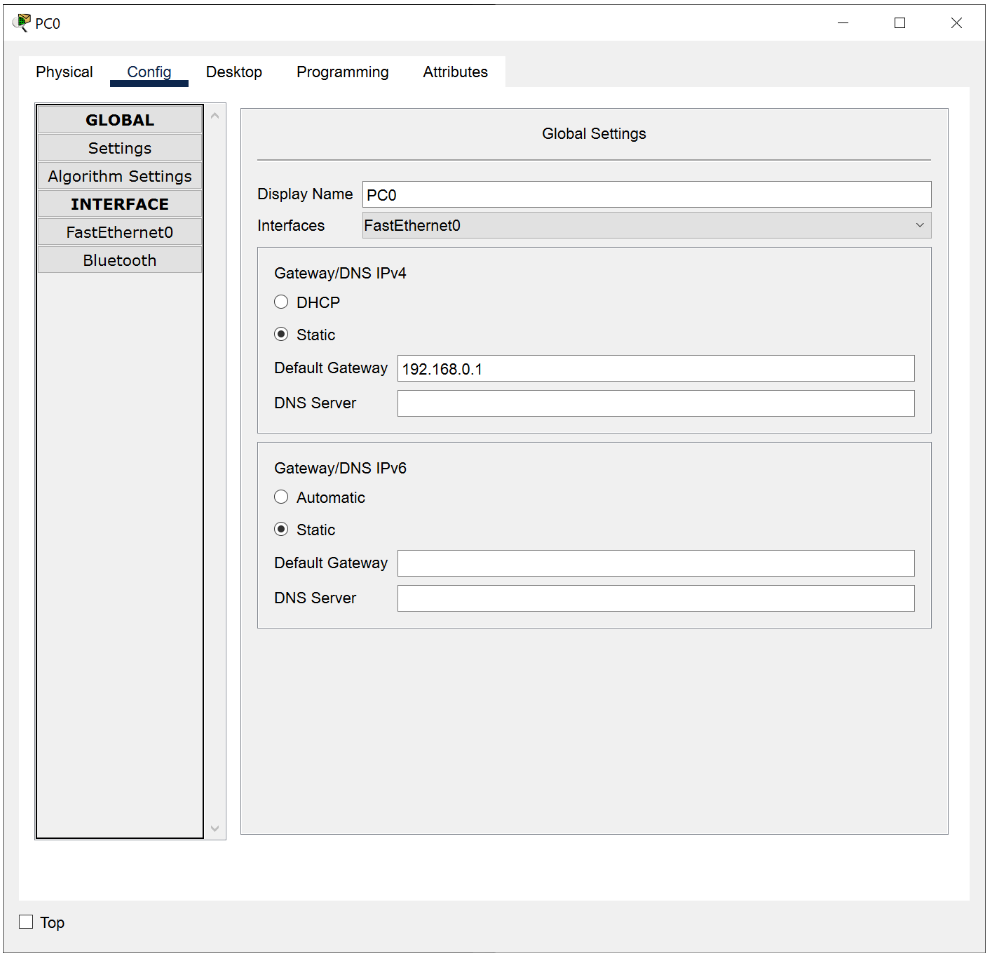


what we're gonna be looking later at is the IPV4 address

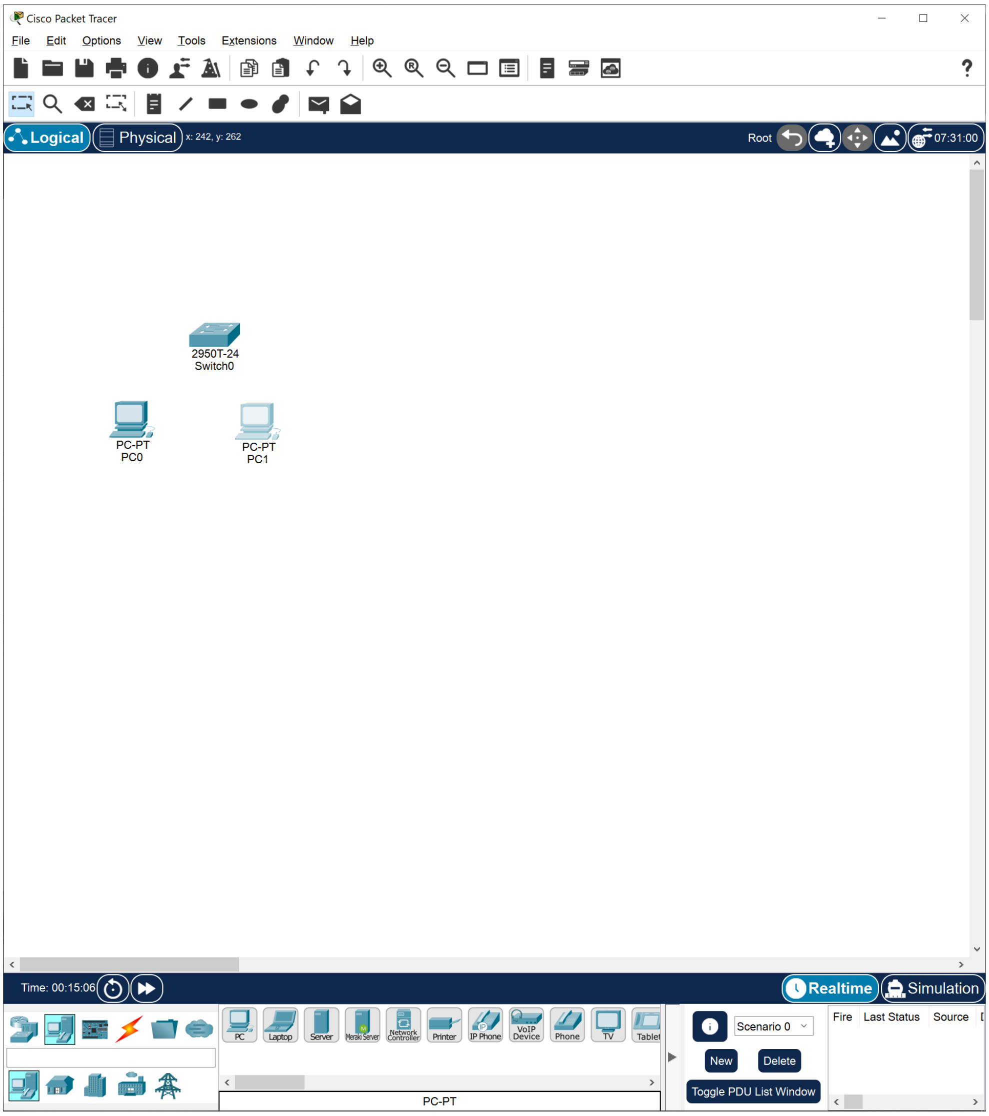


in the meantime let's go in global and set the **IP Address** equal to this

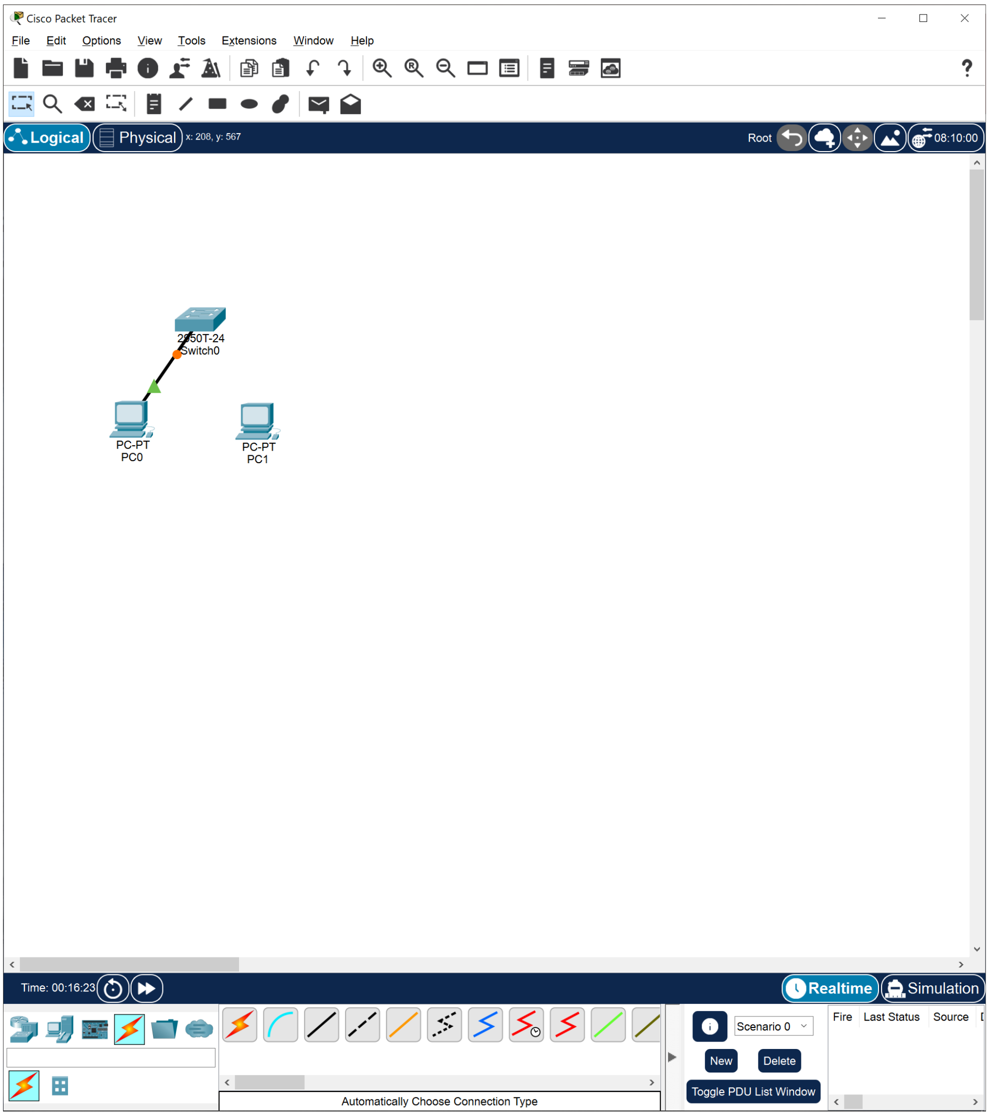
$$192.168.0.1$$



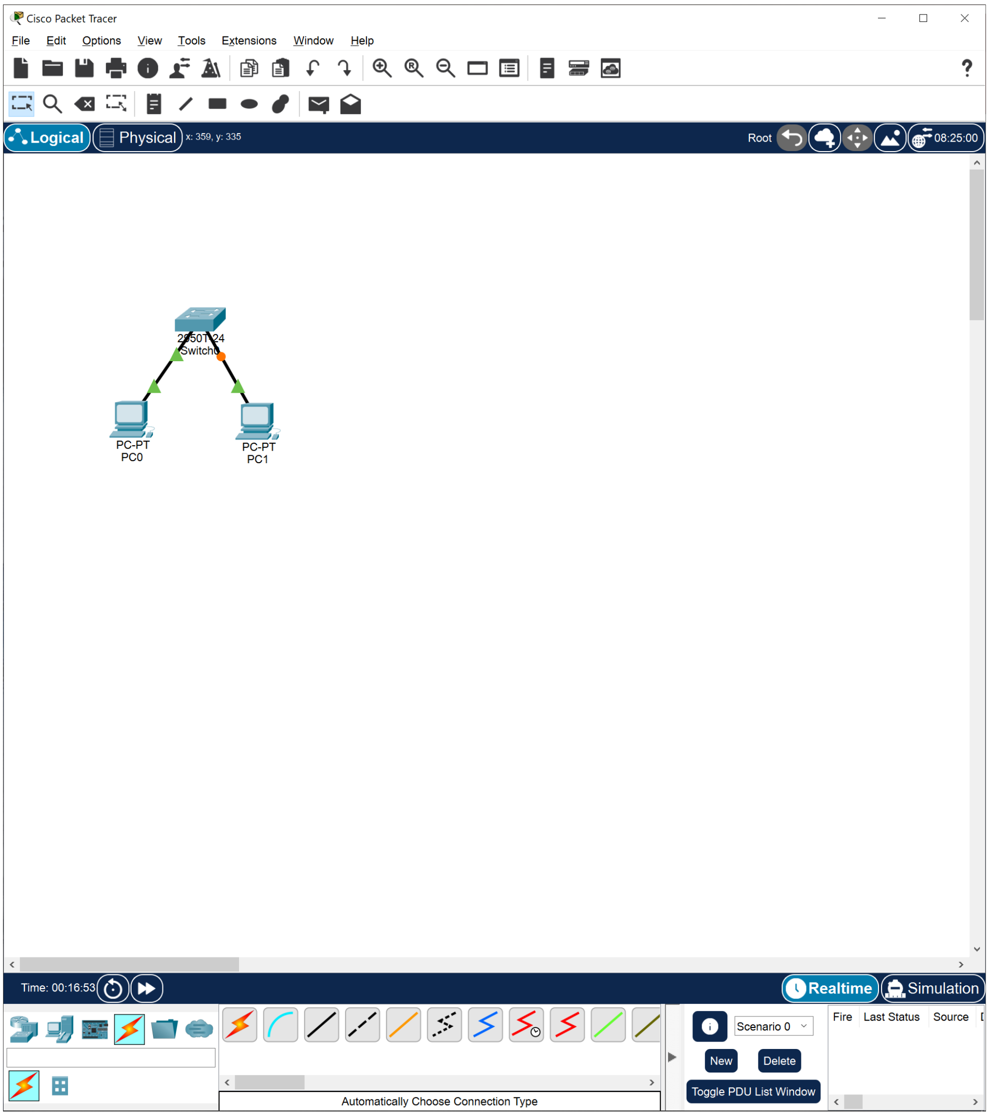
Now we add a new computer



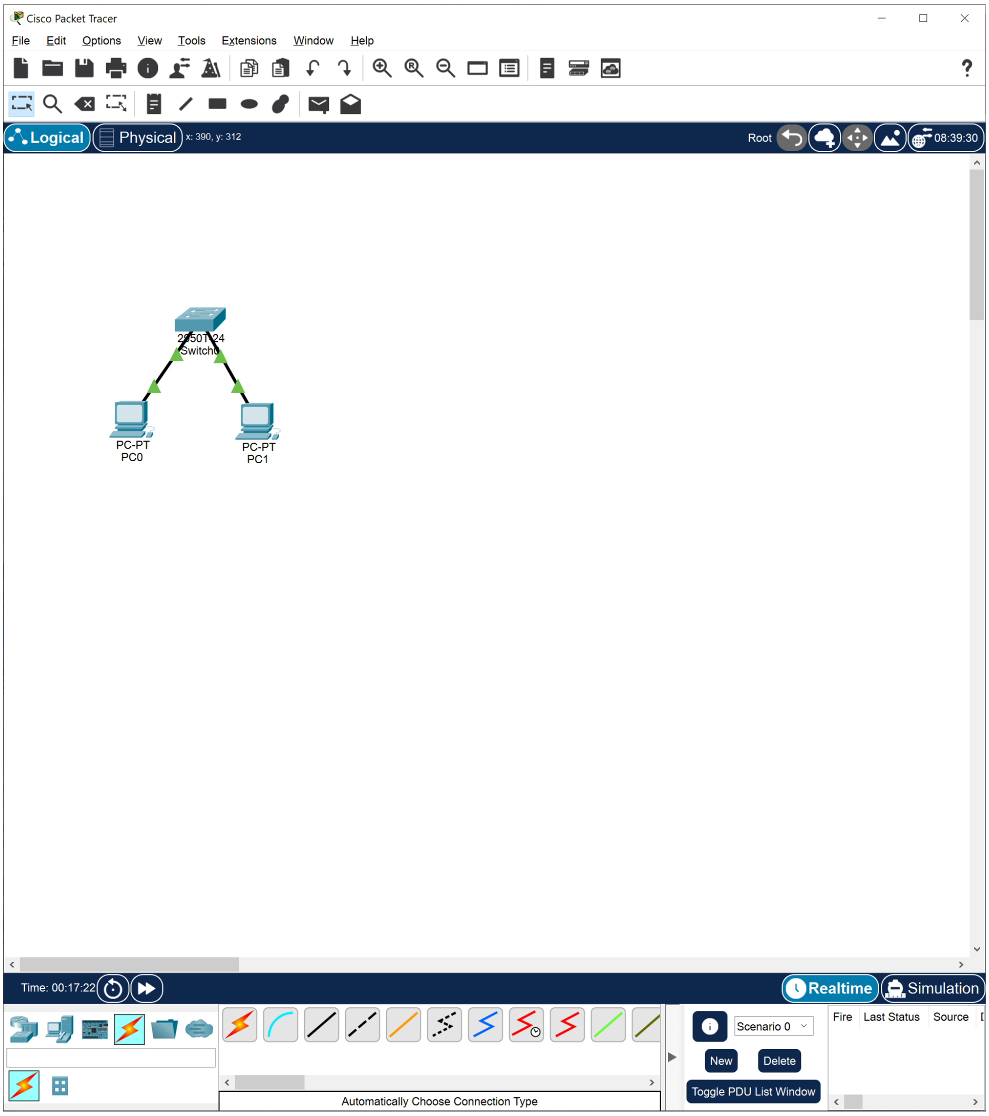
We link the switch to the first computer and wait for all lights to go green



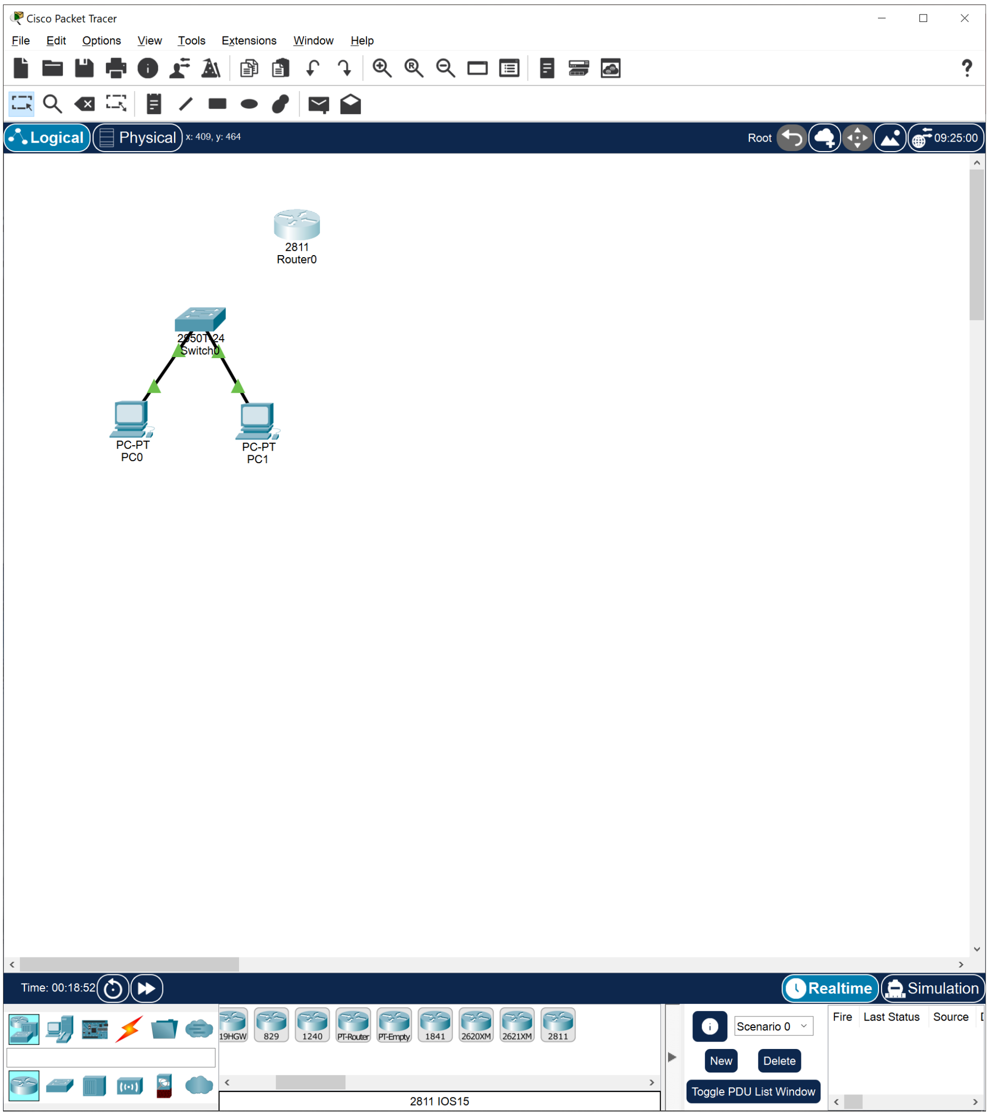
Link the switch to the second computer and wait for this link to go all green as well



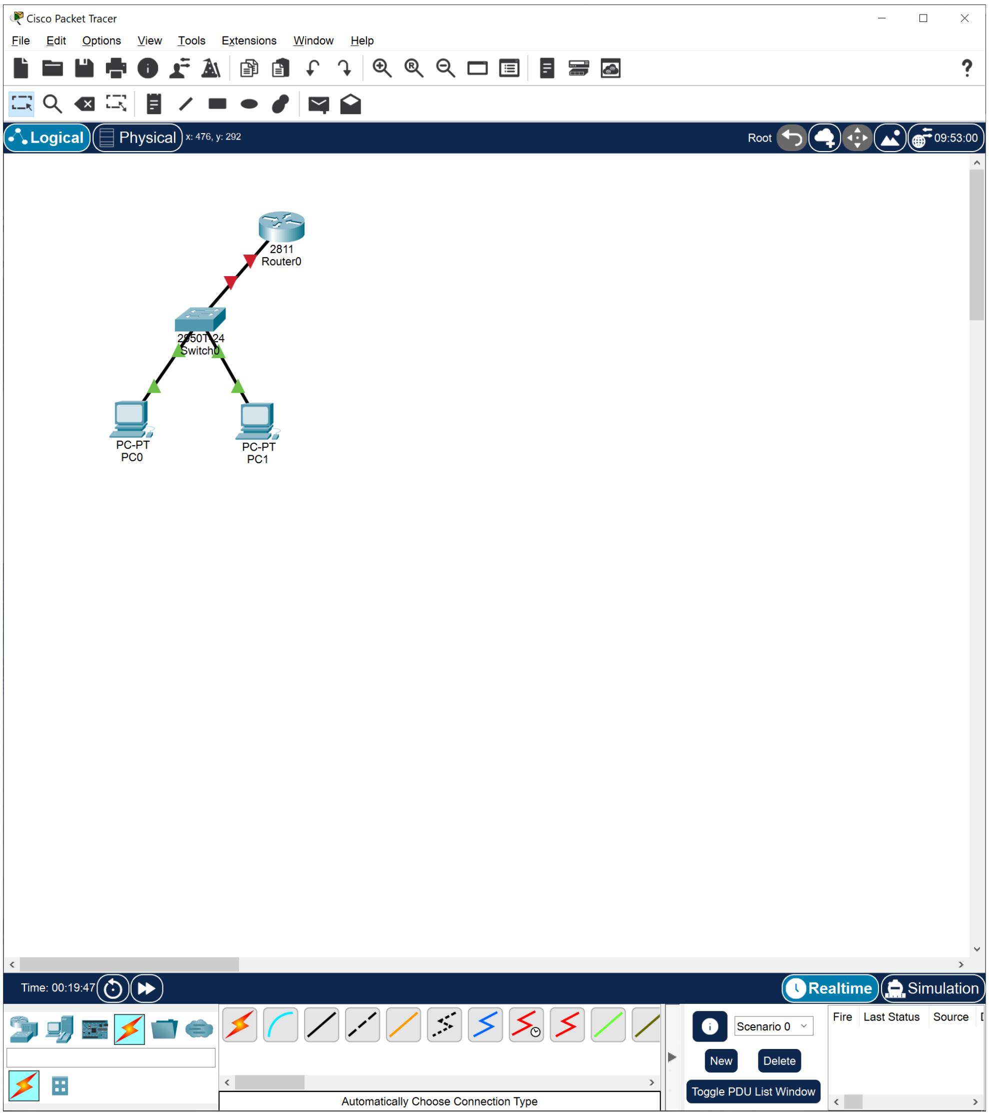
Now it’s all green which makes us happy



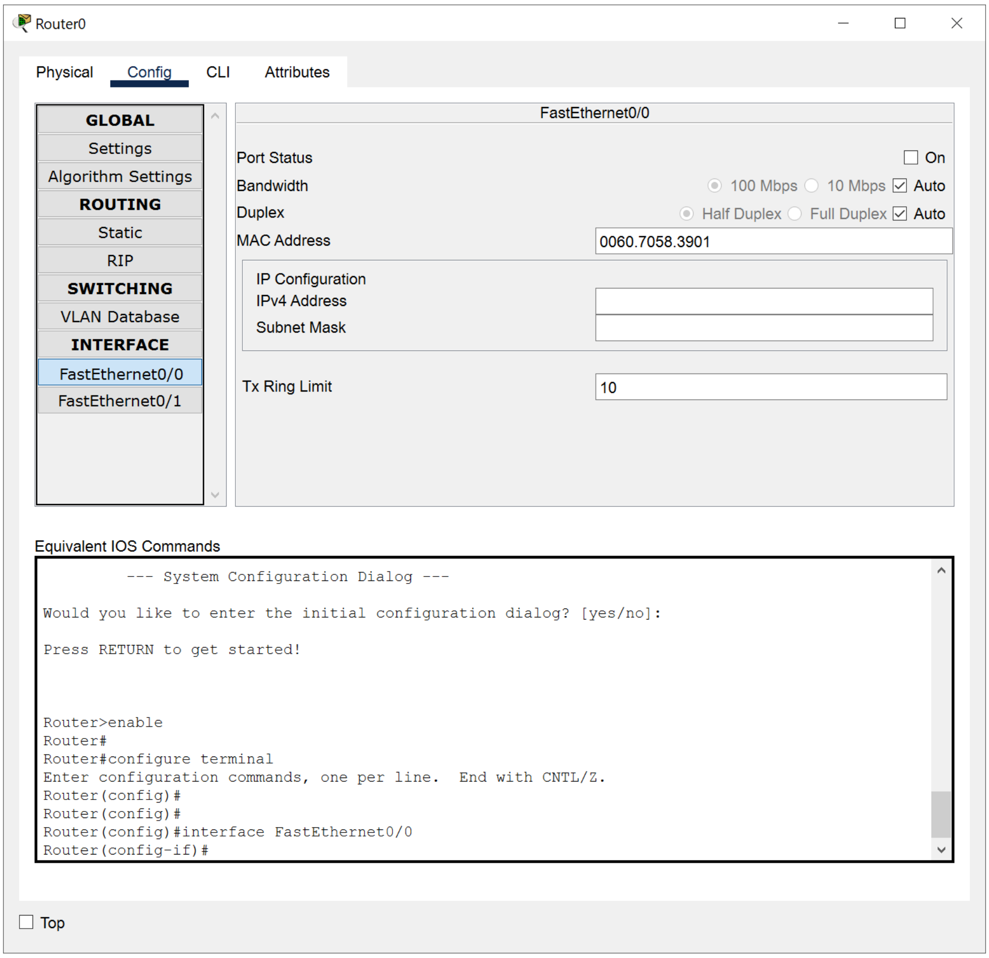
Let's add a router



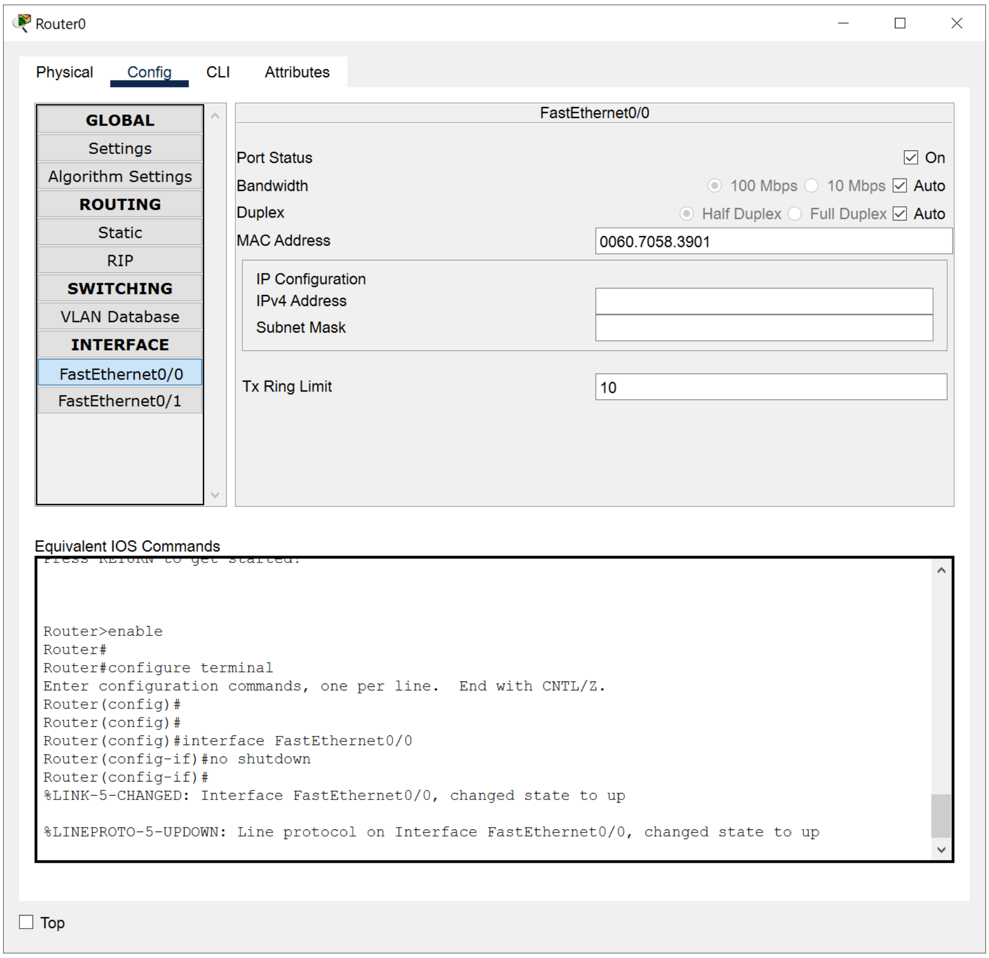
Let’s link the router to the first computer



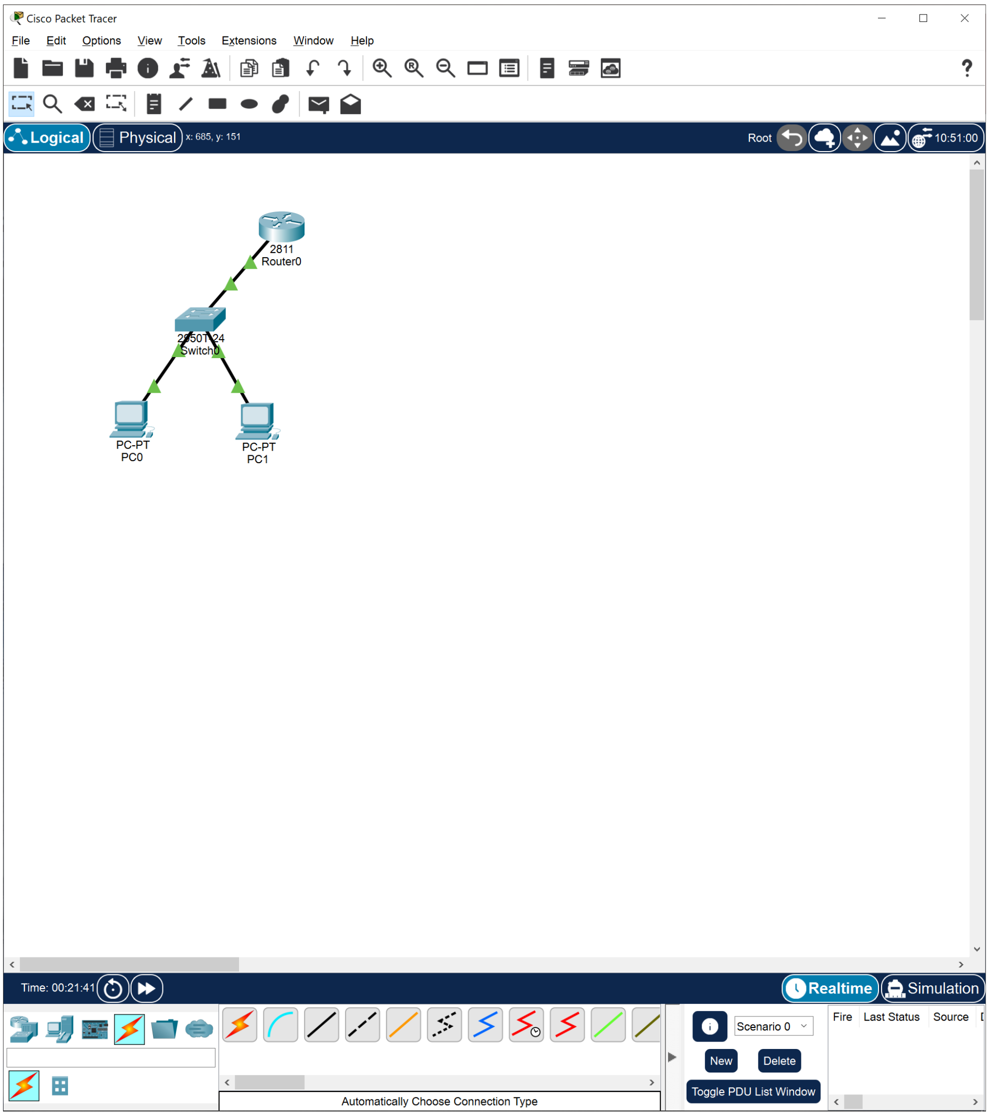
If you click on the router, in the config tab there is a box you need to check. That box will emulate the router being powered on



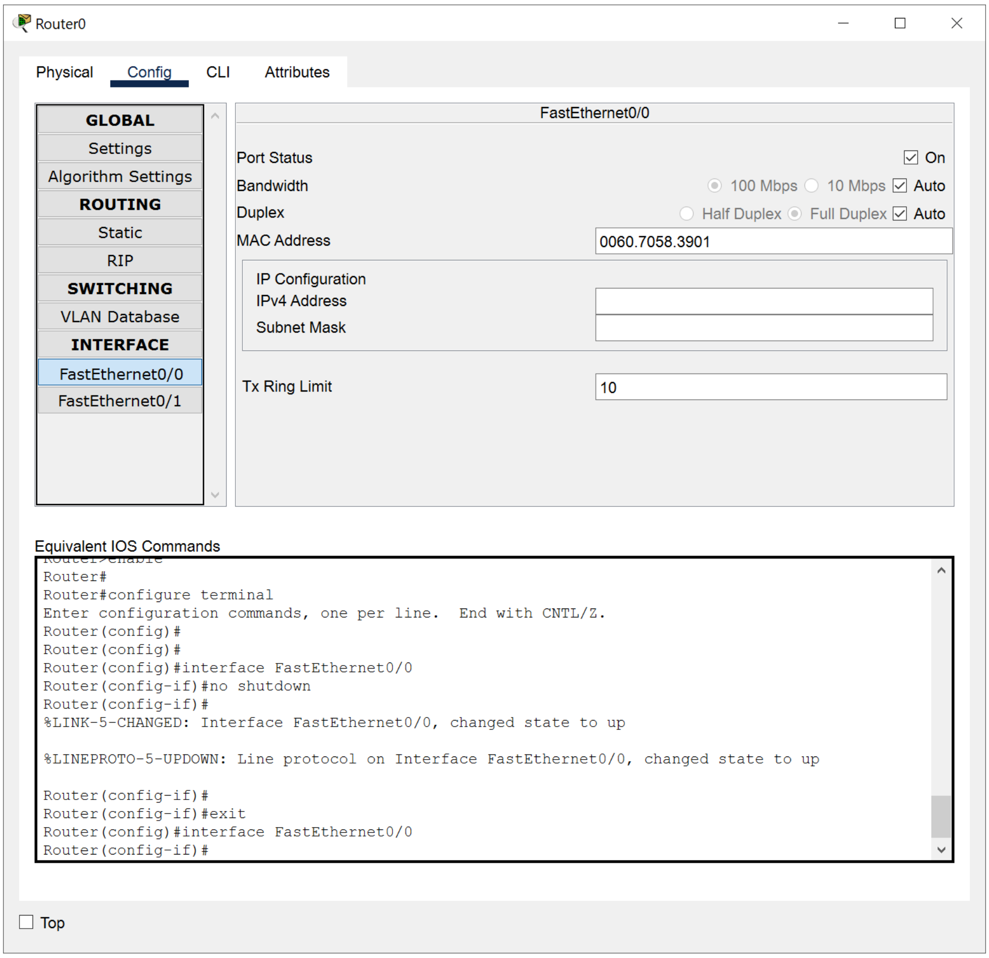
Once you click in the box a small tick will appear in it. This means the box is ticked and the function that box is proving is now being turned on



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



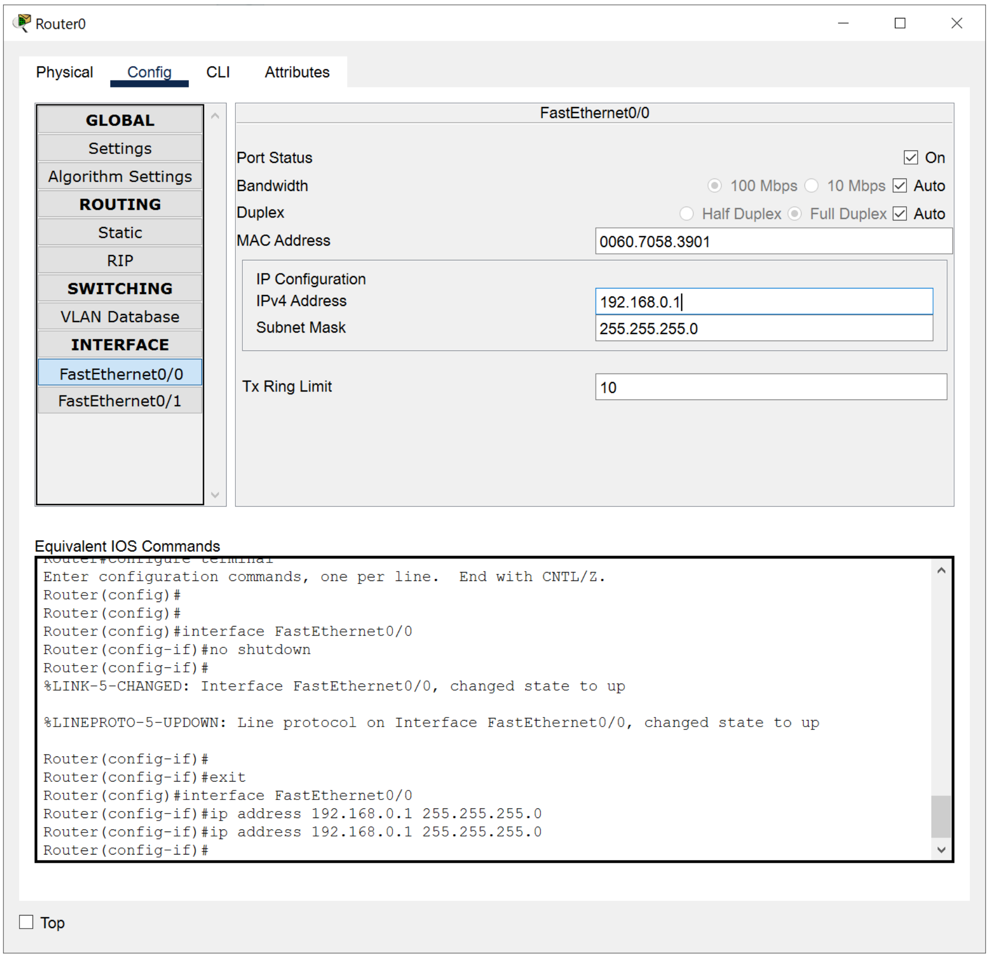
Now, because the subnet mask indicates how many values can you actually use this means we can use

$$255values - Xvalues$$

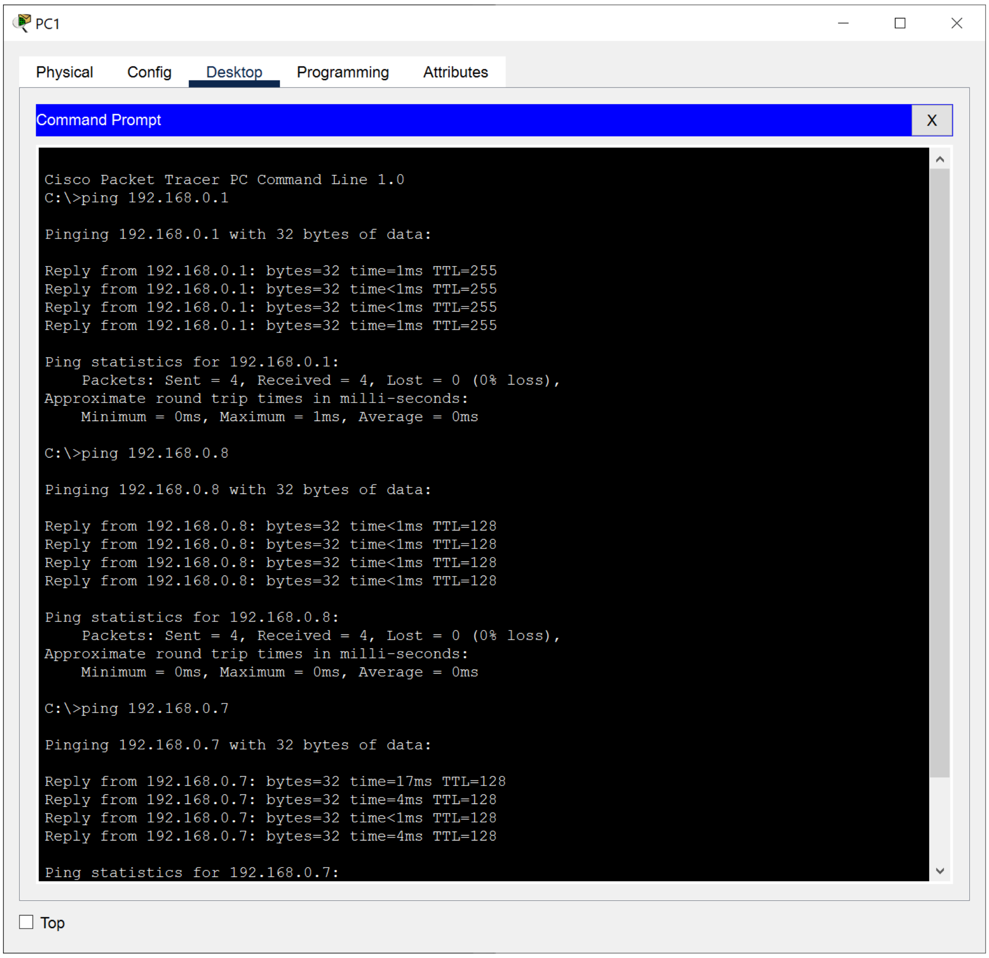
where X is the number in a subnetmask like $Z.Y.W.X$ which in the case of *255.255.255.0* will be

$$255 - 0$$

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

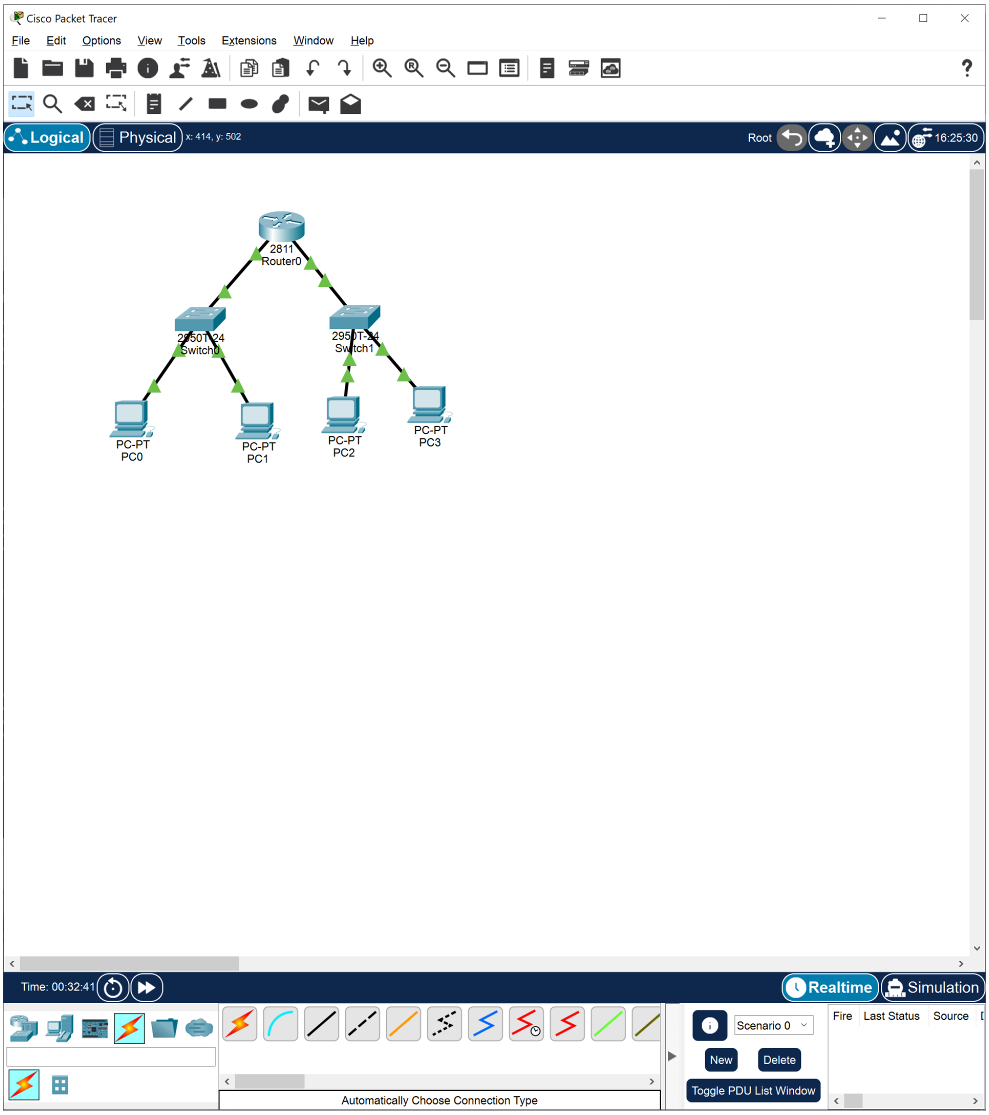


Let's pick up PC1 console and ping all devices in the 192.168.0.1 network. The ping works



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

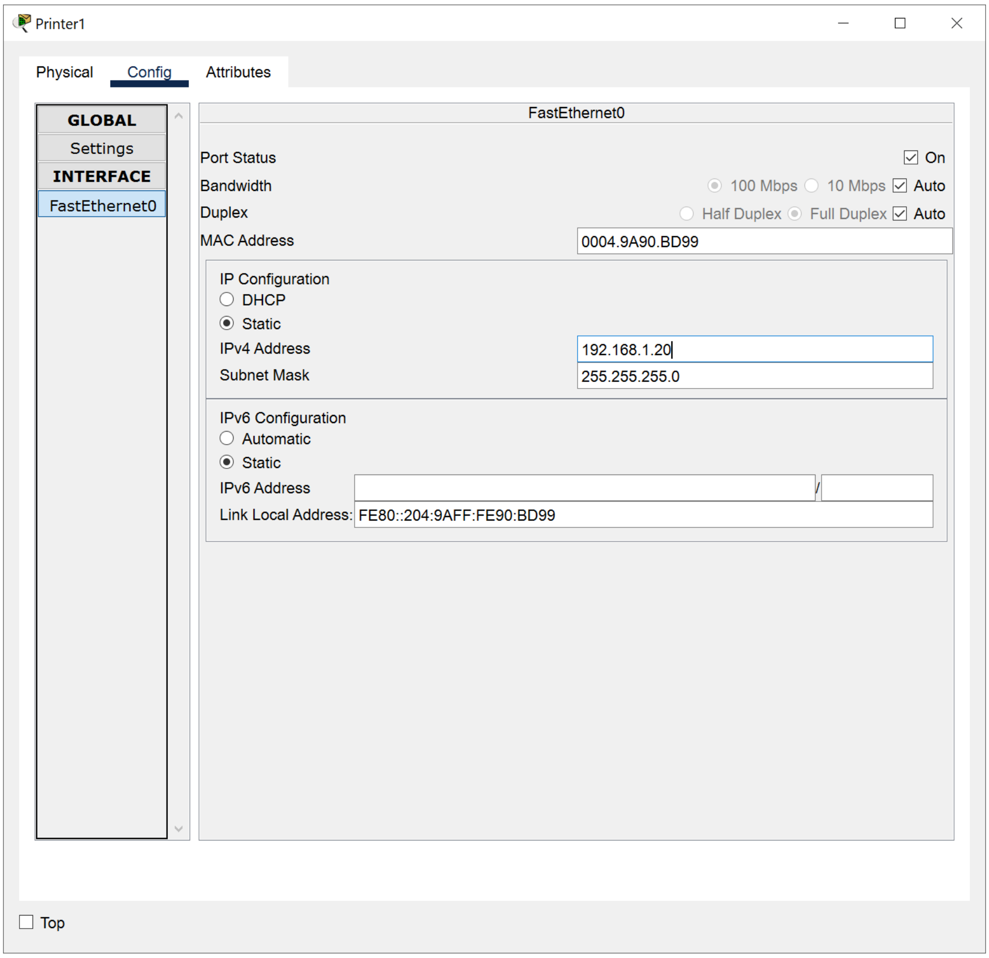
192.168.1.1



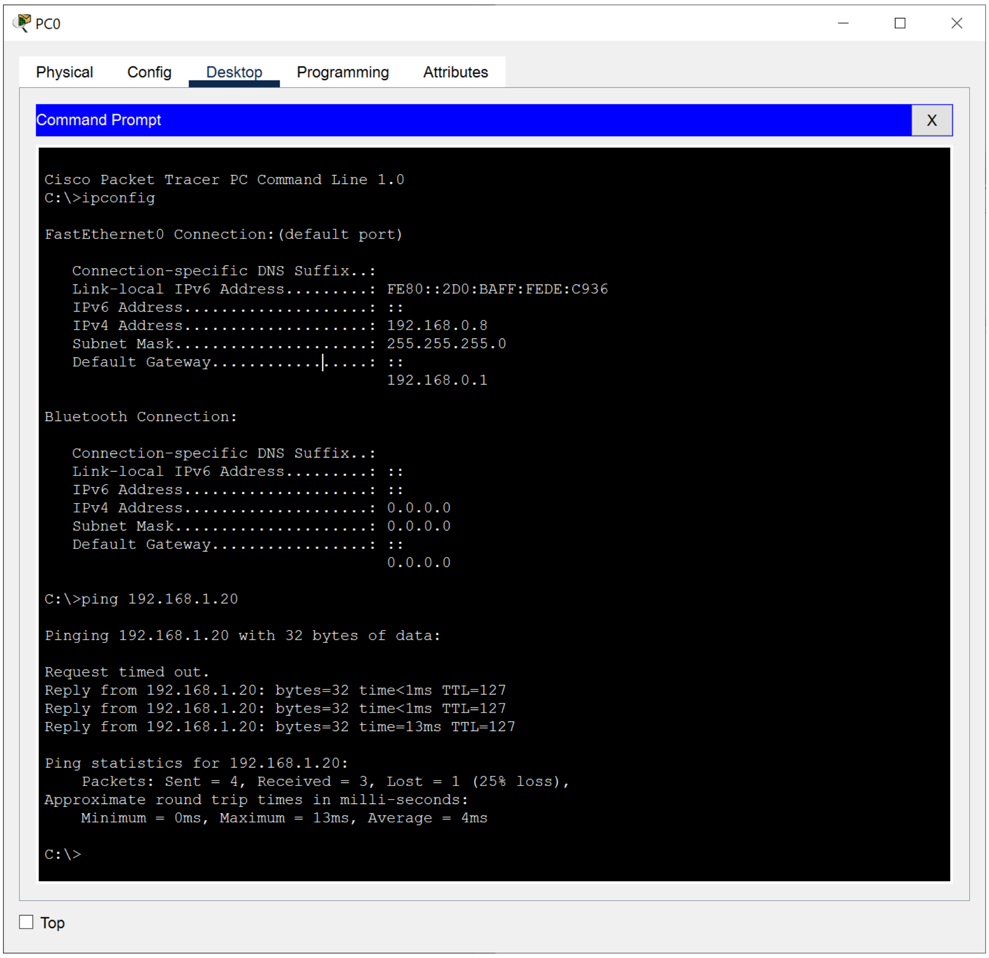
8.1.1 expanding the network

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

9 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.

10 Network Topology

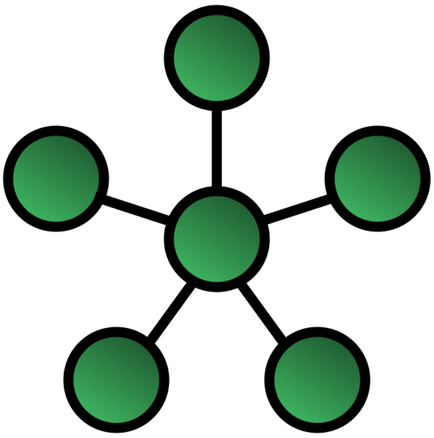
Network topology is the arrangement of the elements (links, nodes, etc.) of a communication network.

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.

10.1 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.



10.1.1 PROs

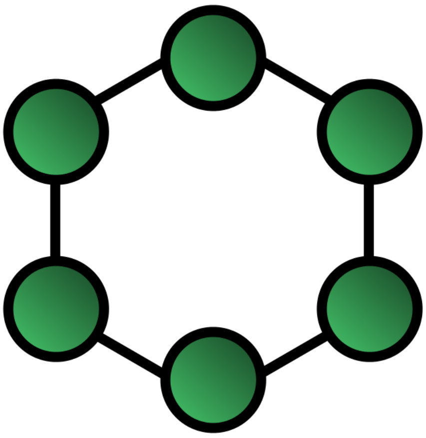
- simplicity of adding additional nodes
- is the easiest topology to design and implement

10.1.2 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

10.2 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.[3] 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.



10.2.1 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

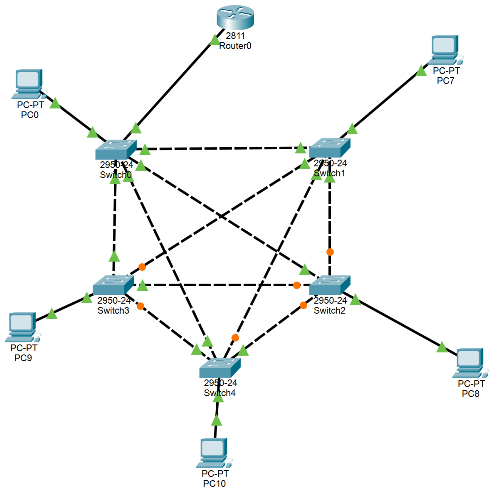
10.2.2 CONs

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

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

10.3 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 purposes



11 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

12 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.

12.1 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."

12.1.1 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.

12.2 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).

12.2.1 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.

12.2.2 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.

13 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).[1]:188–189

13.1 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).

14 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.

15 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.

15.1 Existing Technologies in Aviation Industry

15.1.1 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.

15.1.2 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.

15.1.3 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.

15.2 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.

15.3 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.

16 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[4].

16.1 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,[5] 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.

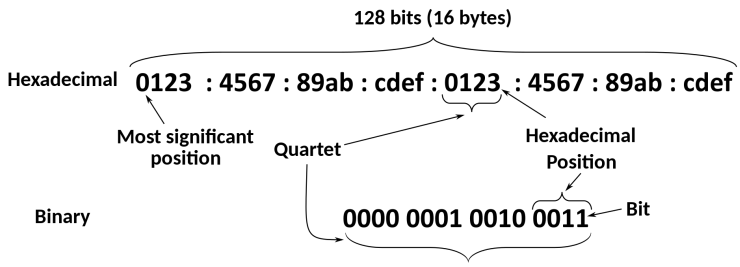


Figure 7: IPv6 8-bytes Format

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.[6]

16.2 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**,[7] also known as automatic private IP addressing (APIPA) or auto-IP.

In the Internet Protocol Version 6 (IPv6), the address block fe80::/10 has been reserved for link-local unicast addressing.[5][0] Of 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.[2]:2.5.6

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

Figure 8: 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.[2]:2.8 Consequently, IPv6 hosts usually have

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

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

[6]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.

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).[5] 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,[5] or randomized.[6] Automatic duplicate address detection algorithms prevent assignment errors.

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