

Networking

Contents

1	What it is	3
2	benefits of a network	3
2.1	guided wiring	4
2.2	unguided wiring	4
3	LAN vs WAN	4
4	IEEE 802.3	5
5	Protocols	6
5.1	OSI standard	6
5.2	good mnemonic for OSI	7
5.3	theory vs practice	7
5.4	horizontal vs vertical approach	7
6	ARP/RARP/DHCP	7
6.1	ARP Tables	8
6.2	Three-way-handshake	8
7	Networking Hardware	9
7.1	Routers	9
7.2	Modems	9
7.3	Hubs, bridges and switches	10
7.3.1	Hubs	10
7.3.2	Bridges	11
7.3.3	Switches	11
8	Cisco Packet Tracer	12
8.1	The step-by-step guide	13
8.1.1	expanding the network	33
9	Power over Ethernet	35
10	Network Topology	35
10.1	Star Topology	36
10.1.1	PROs	36
10.1.2	CONs	36

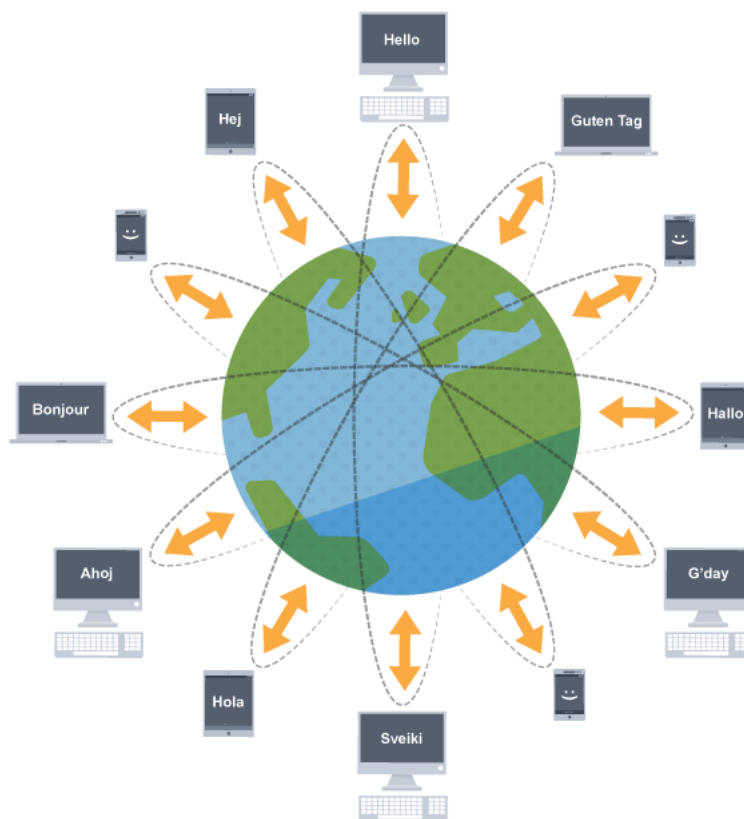
10.2	Ring Topology	37
10.2.1	PROs	37
10.2.2	CONs	37
11	Routing Protocols	38
11.1	Interior gateway protocols	38
11.1.1	link state routing protocols	38
11.1.2	distance vector routing protocols	39
11.2	Exterior gateway protocols	41
11.2.1	BGP	41

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 benefits of a network

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



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

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

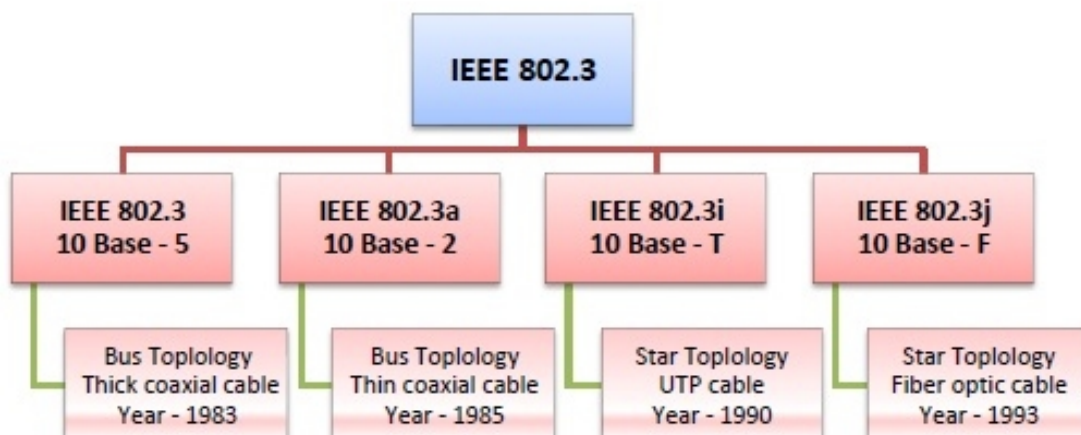
LAN, which stands for local area network, and WAN, which stands for wide area network, are two types of networks that allow connection between computers. As the naming conventions suggest, LANs are for smaller, more localized networking — in a home, business, school, etc. — while WANs cover larger areas, 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) sub-layer of the data link layer for wired Ethernet networks.

IEEE 802.3 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

7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

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.

5.2 good mnemonic for OSI

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 acknowledgment 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.

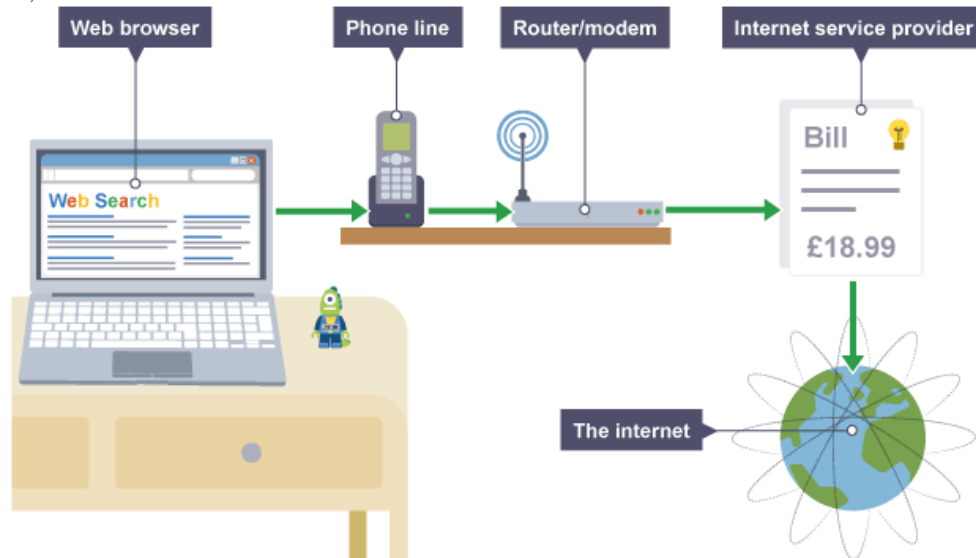
To send the message, it also requires Computer 2's MAC address. First, Computer 1 uses a cached ARP table to look up 192.168.0.55 for any existing records of Computer 2's MAC address (00:EB:24:B2:05:AC). If the MAC address is found, it sends an Ethernet frame containing the IP packet onto the link with 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



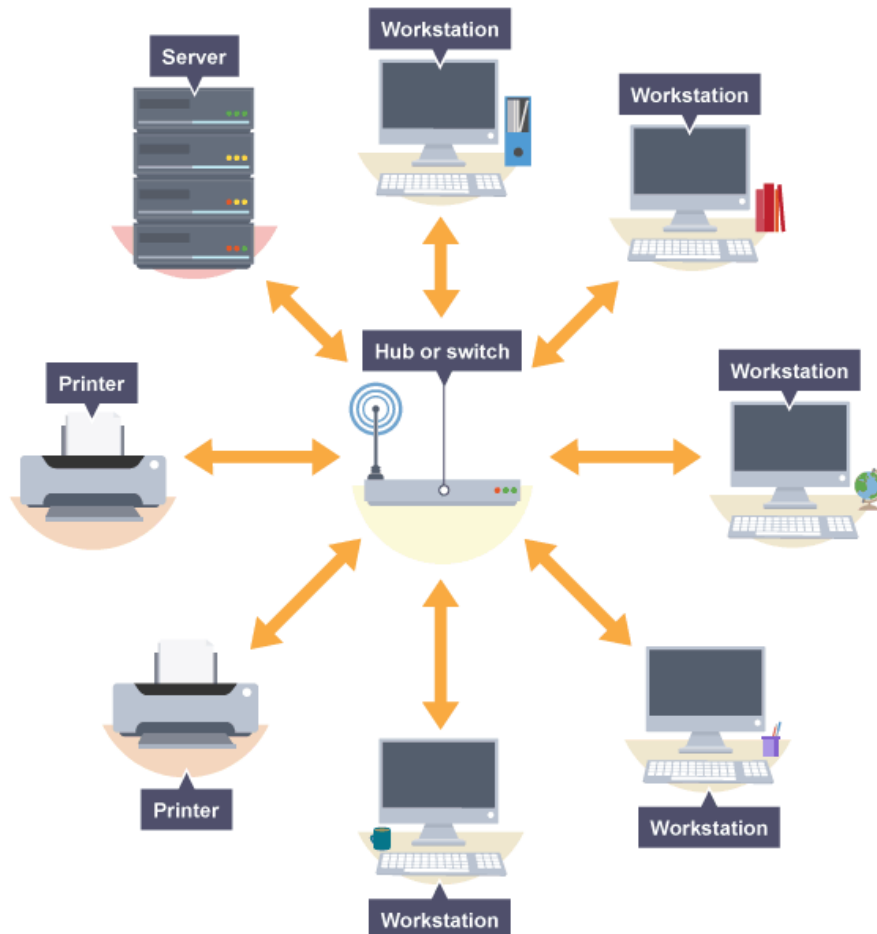
7.1 Routers

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.

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



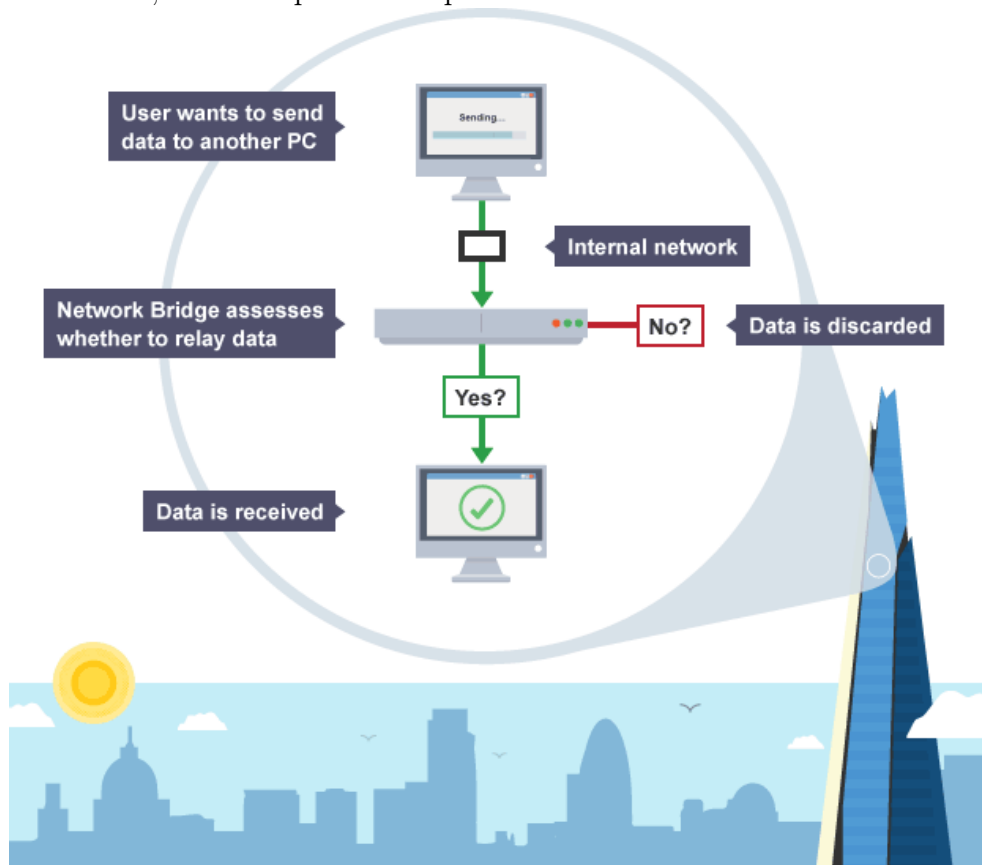
Hubs, bridges and switches allow multiple devices to connect to the router and they transfer data to all devices on a network. A router is a more complex device that usually includes the capability of hubs, bridges and switches.

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.

7.3.2 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.



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

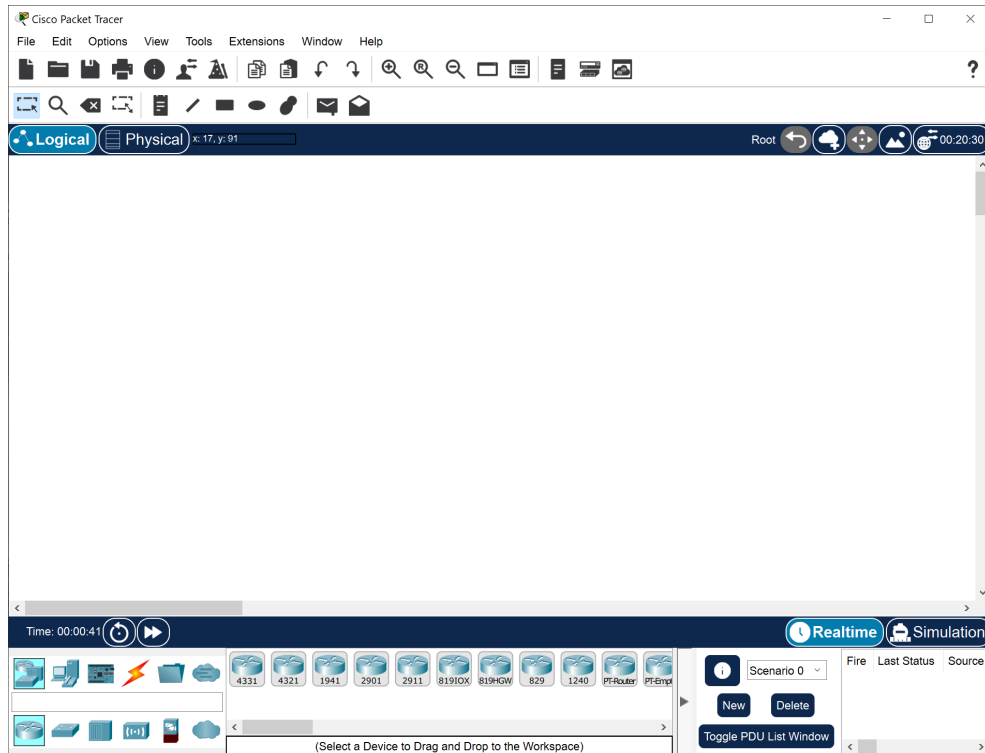
In this experiment we try to ping devices being set with 0 in the IP fields. Then we're gonna expand the network with more devices

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

²Bakni, 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.

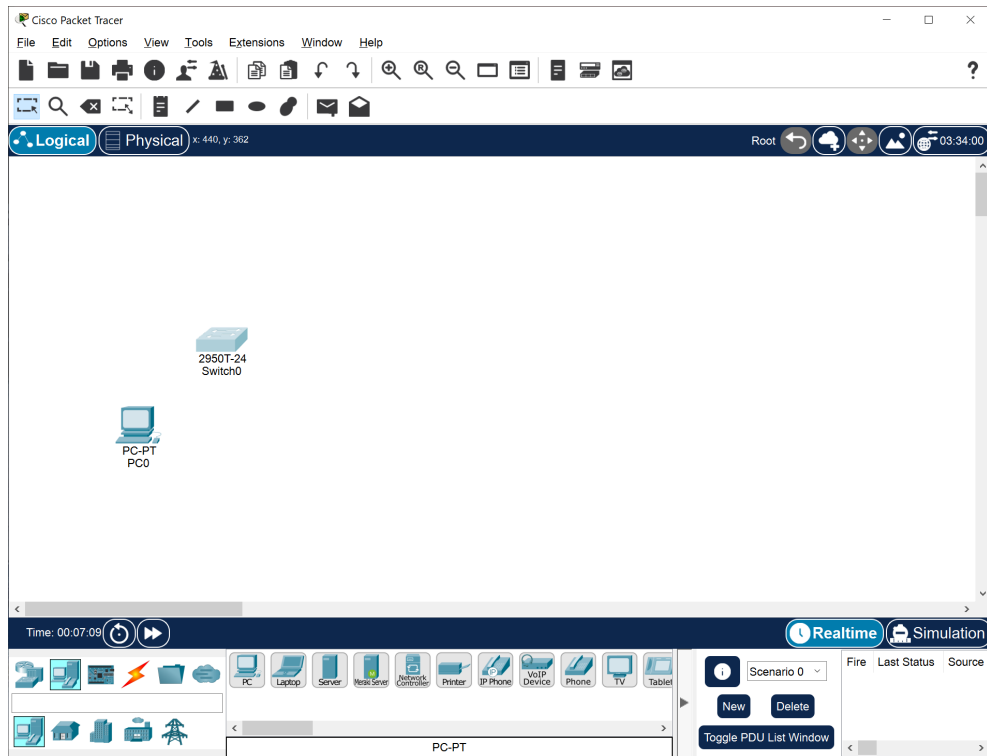
8.1 The step-by-step guide

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

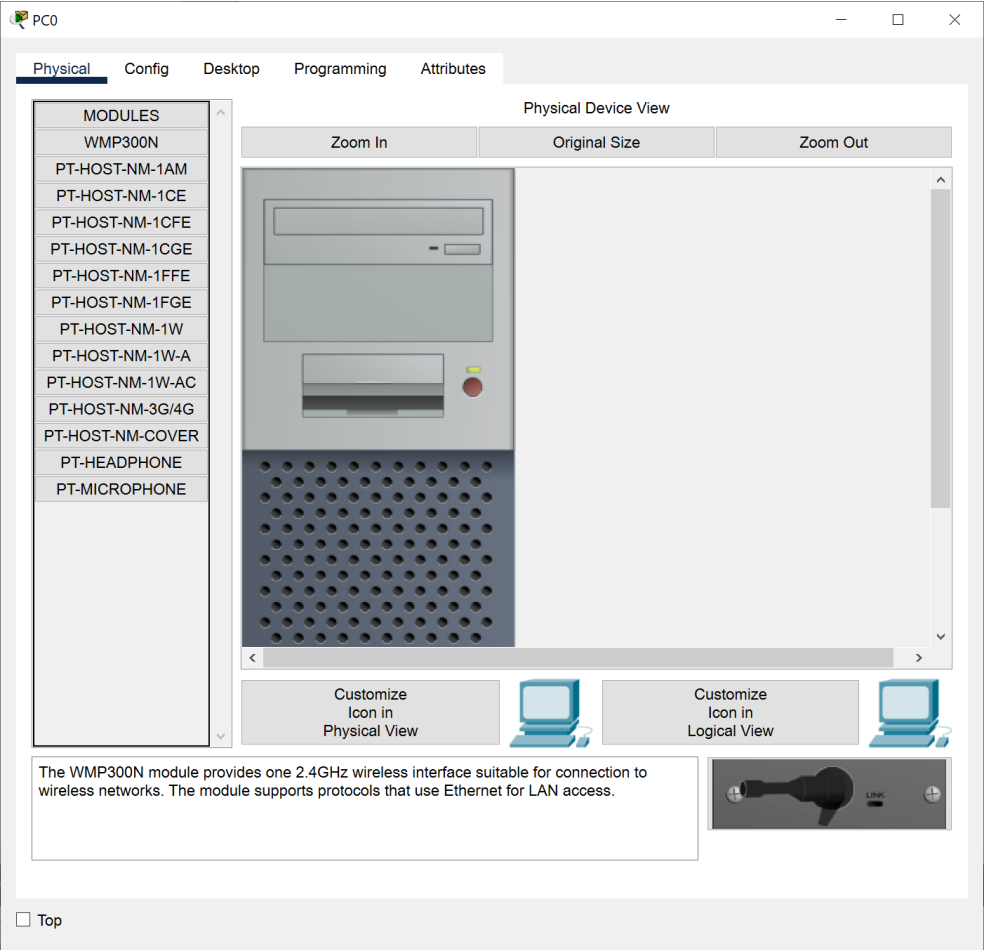


The screenshot shows the Cisco Packet Tracer application window. The title bar reads "Cisco Packet Tracer". The menu bar includes "File", "Edit", "Options", "View", "Tools", "Extensions", "Window", and "Help". The toolbar contains various icons for file operations, navigation, and simulation. The main workspace is titled "Physical" and shows a single device, "2950T-24 Switch0", placed on a light blue surface. The bottom status bar displays "Time: 00:04:37" and "Realtime" simulation mode. The bottom toolbar includes icons for different device types (routers, switches, servers, etc.) and buttons for "New", "Delete", and "Toggle PDU List Window".

And then we add a computer :



Now we click on the computer



And we move ourselves in the Config tab

The image shows a configuration window for a device named PC0. The window has a title bar with a PC icon and the text 'PC0'. Below the title bar are four tabs: 'Physical', 'Config' (which is selected and highlighted), 'Desktop', 'Programming', and 'Attributes'. On the left side of the 'Config' tab is a vertical sidebar with a tree view. The tree view has two main sections: 'GLOBAL' and 'INTERFACE'. Under 'GLOBAL' are 'Settings' and 'Algorithm Settings'. Under 'INTERFACE' are 'FastEthernet0' and 'Bluetooth'. The 'FastEthernet0' item is currently selected. The main area of the window displays the configuration for 'FastEthernet0' under the heading 'Global Settings'. It includes a 'Display Name' field with the value 'PC0' and an 'Interfaces' dropdown menu showing 'FastEthernet0'. Below these are two sections for 'Gateway/DNS' settings. The first section is for IPv4, with radio buttons for 'DHCP' and 'Static' (the 'Static' option is selected). It has input fields for 'Default Gateway' and 'DNS Server'. The second section is for IPv6, with radio buttons for 'Automatic' and 'Static' (the 'Static' option is selected). It also has input fields for 'Default Gateway' and 'DNS Server'. At the bottom left of the window is a checkbox labeled 'Top'.

PC0

Physical **Config** Desktop Programming Attributes

GLOBAL

- Settings
- Algorithm Settings

INTERFACE

- FastEthernet0
- Bluetooth

Global Settings

Display Name: PC0

Interfaces: FastEthernet0

Gateway/DNS IPv4

☐ DHCP

☒ Static

Default Gateway:

DNS Server:

Gateway/DNS IPv6

☐ Automatic

☒ Static

Default Gateway:

DNS Server:

☐ Top

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

The screenshot shows a configuration window for a PC0. The window has a title bar with a PC icon and the text "PC0". Below the title bar are four tabs: "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Config" tab is selected. On the left side of the "Config" tab is a sidebar with a tree view. The tree view has two main sections: "GLOBAL" and "INTERFACE". Under "GLOBAL" are "Settings" and "Algorithm Settings". Under "INTERFACE" are "FastEthernet0" (which is selected and highlighted in blue) and "Bluetooth". The main area of the window displays the configuration for "FastEthernet0". It includes fields for "Port Status" (checked "On"), "Bandwidth" (radio buttons for "100 Mbps", "10 Mbps", and "Auto", with "Auto" checked), "Duplex" (radio buttons for "Half Duplex", "Full Duplex", and "Auto", with "Auto" checked), and "MAC Address" (text field containing "00D0.BADE.C936"). Below these are two sections for IP configuration. The "IP Configuration" section has radio buttons for "DHCP" and "Static", with "Static" selected. It includes text fields for "IPv4 Address" and "Subnet Mask". The "IPv6 Configuration" section has radio buttons for "Automatic" and "Static", with "Static" selected. It includes a text field for "IPv6 Address" and a text field for "Link Local Address" containing "FE80::2D0:BAFF:FEDE:C936". At the bottom left of the window is a "Top" button with a small square icon.

PC0

Physical Config Desktop Programming Attributes

GLOBAL

- Settings
- Algorithm Settings

INTERFACE

- FastEthernet0
- Bluetooth

FastEthernet0

Port Status ☒ On

Bandwidth ☐ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☐ Full Duplex ☒ Auto

MAC Address 00D0.BADE.C936

IP Configuration

☐ DHCP

☒ Static

IPv4 Address

Subnet Mask

IPv6 Configuration

☐ Automatic

☒ Static

IPv6 Address

Link Local Address: FE80::2D0:BAFF:FEDE:C936

☐ Top

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

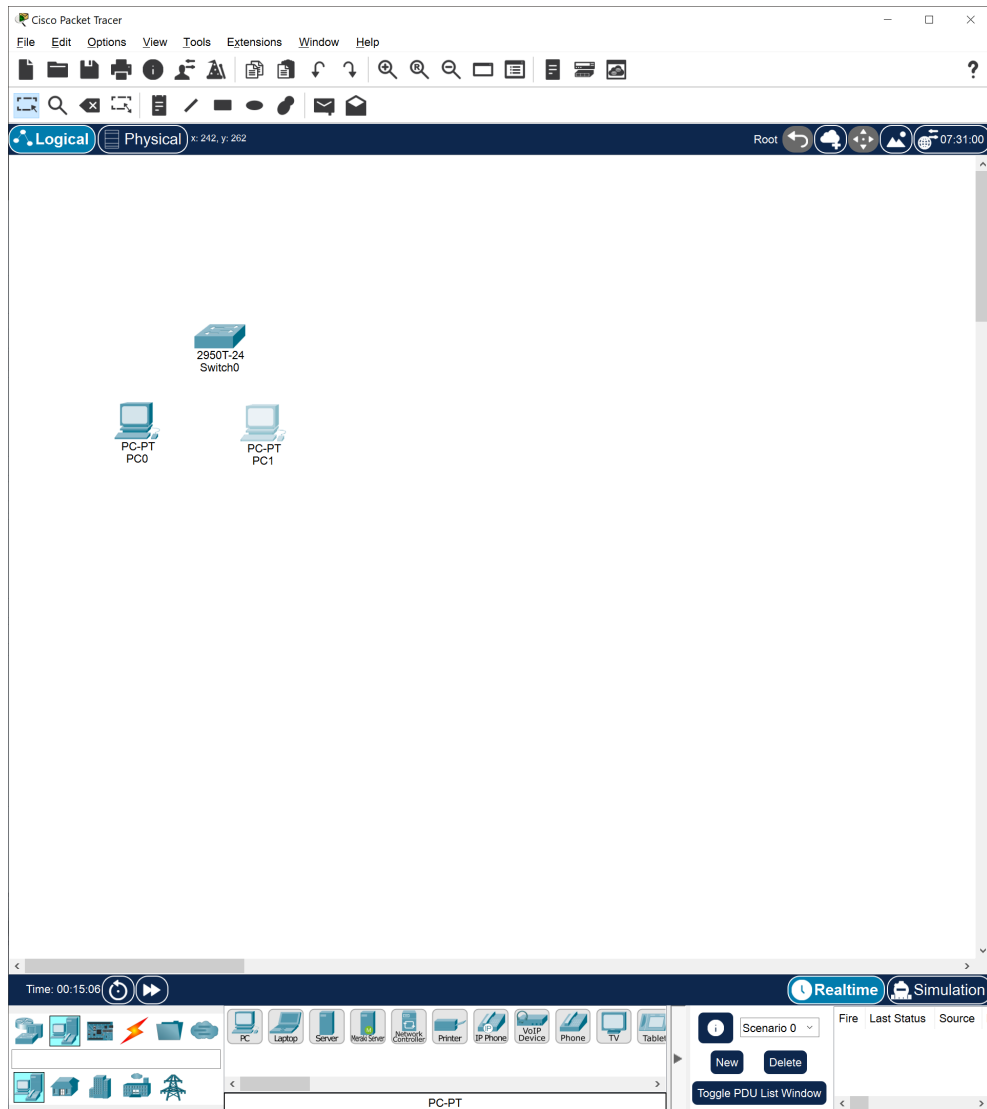
192.168.0.1

The screenshot shows a configuration window for a PC named PC0. The window has a sidebar on the left with a tree view containing 'GLOBAL' (expanded), 'Settings', 'Algorithm Settings', 'INTERFACE', 'FastEthernet0', and 'Bluetooth'. The main area is titled 'Global Settings' and contains the following fields:

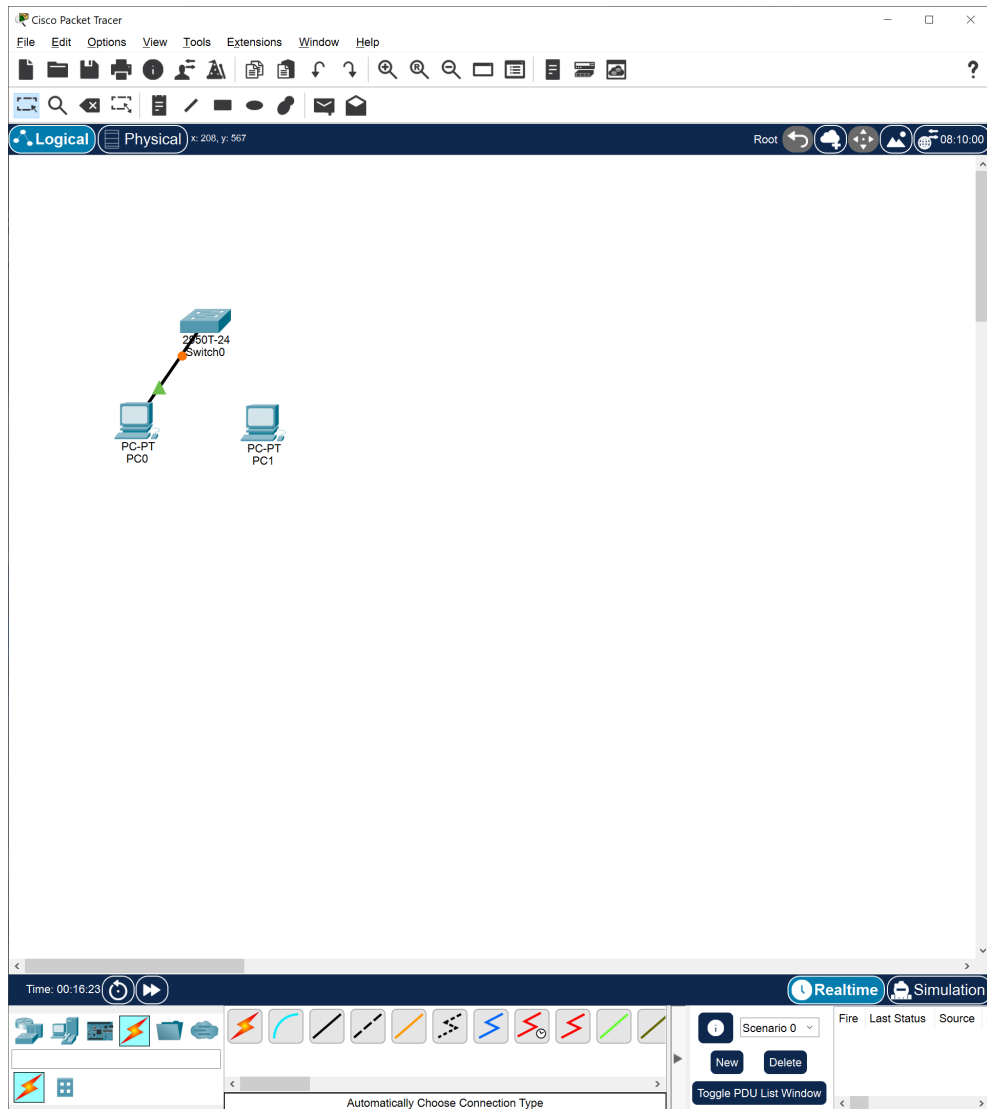
- Display Name:** PC0
- Interfaces:** FastEthernet0 (selected from a dropdown)
- Gateway/DNS IPv4:**
 - ☐ DHCP
 - ☒ Static
 - Default Gateway:** 192.168.0.1
 - DNS Server:** (empty field)
- Gateway/DNS IPv6:**
 - ☐ Automatic
 - ☒ Static
 - Default Gateway:** (empty field)
 - DNS Server:** (empty field)

At the bottom left of the window, there is a checkbox labeled 'Top'.

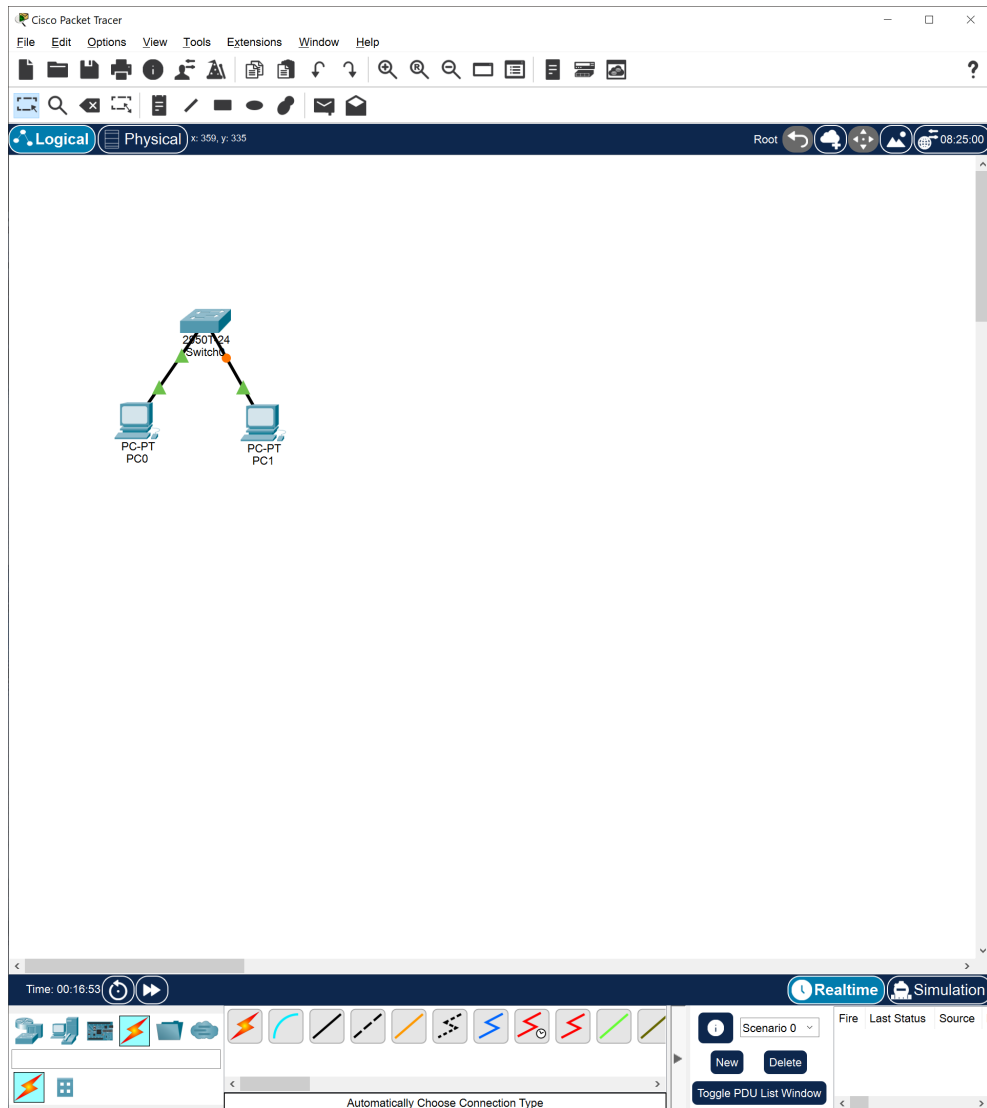
Now we add a new computer



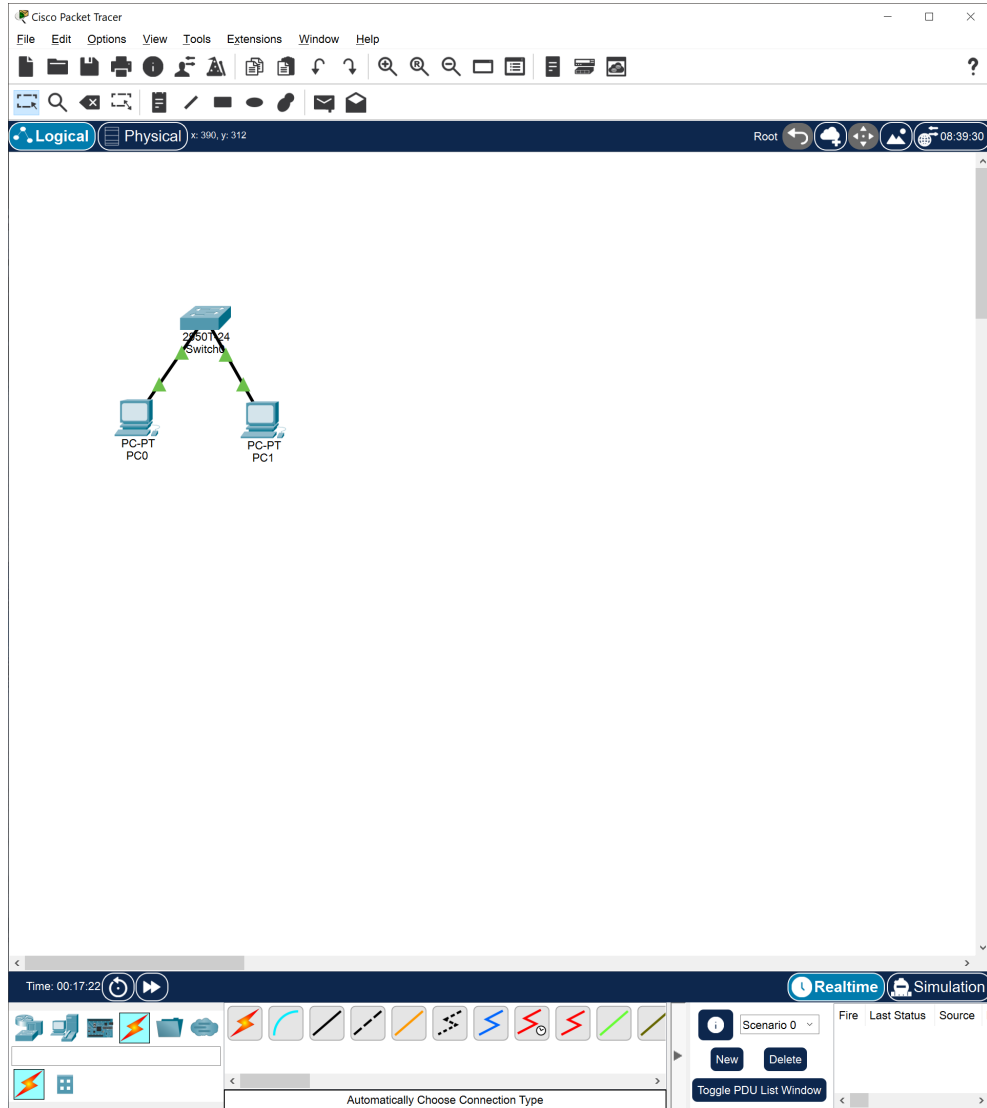
We link the switch to the first computer and wait for all lights to go green



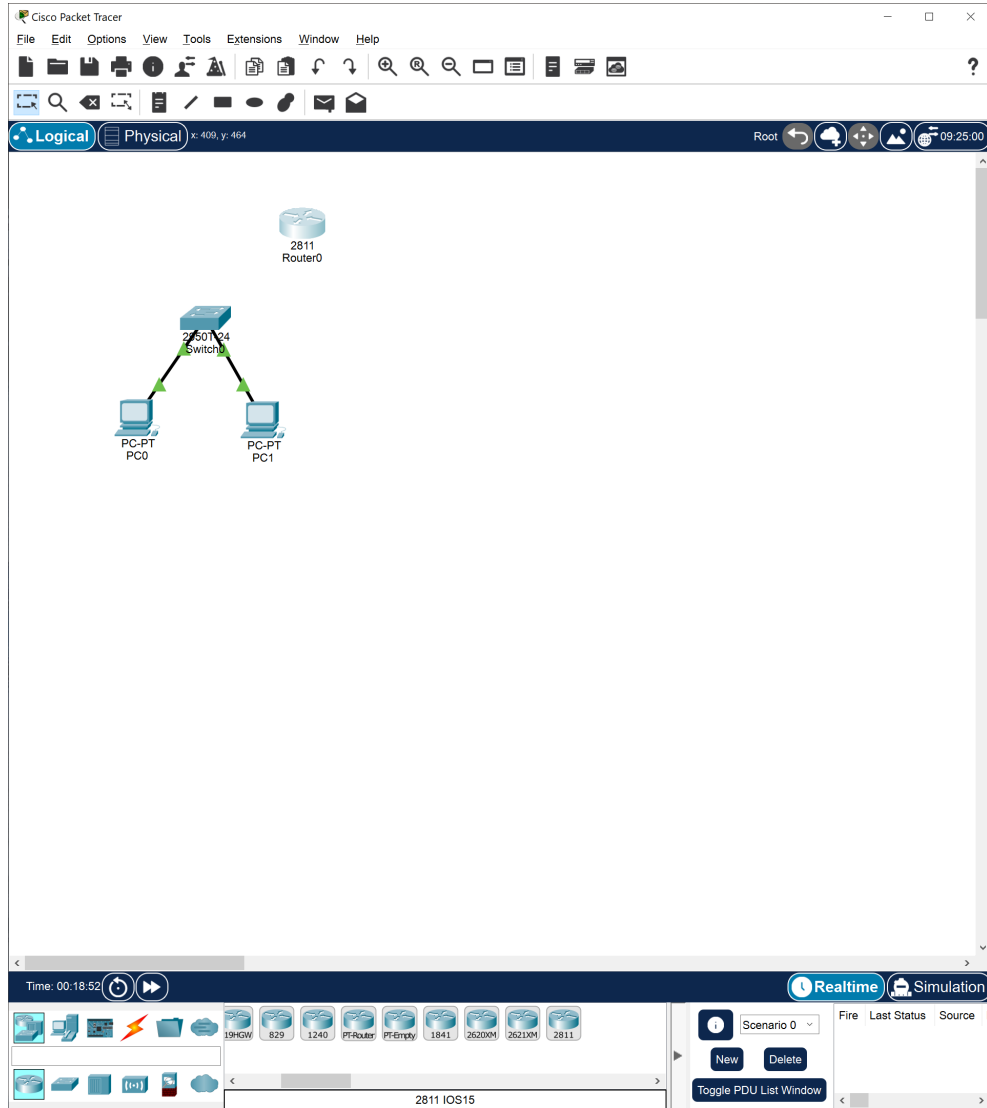
Link the switch to the second computer and wait for this link to go all green as well



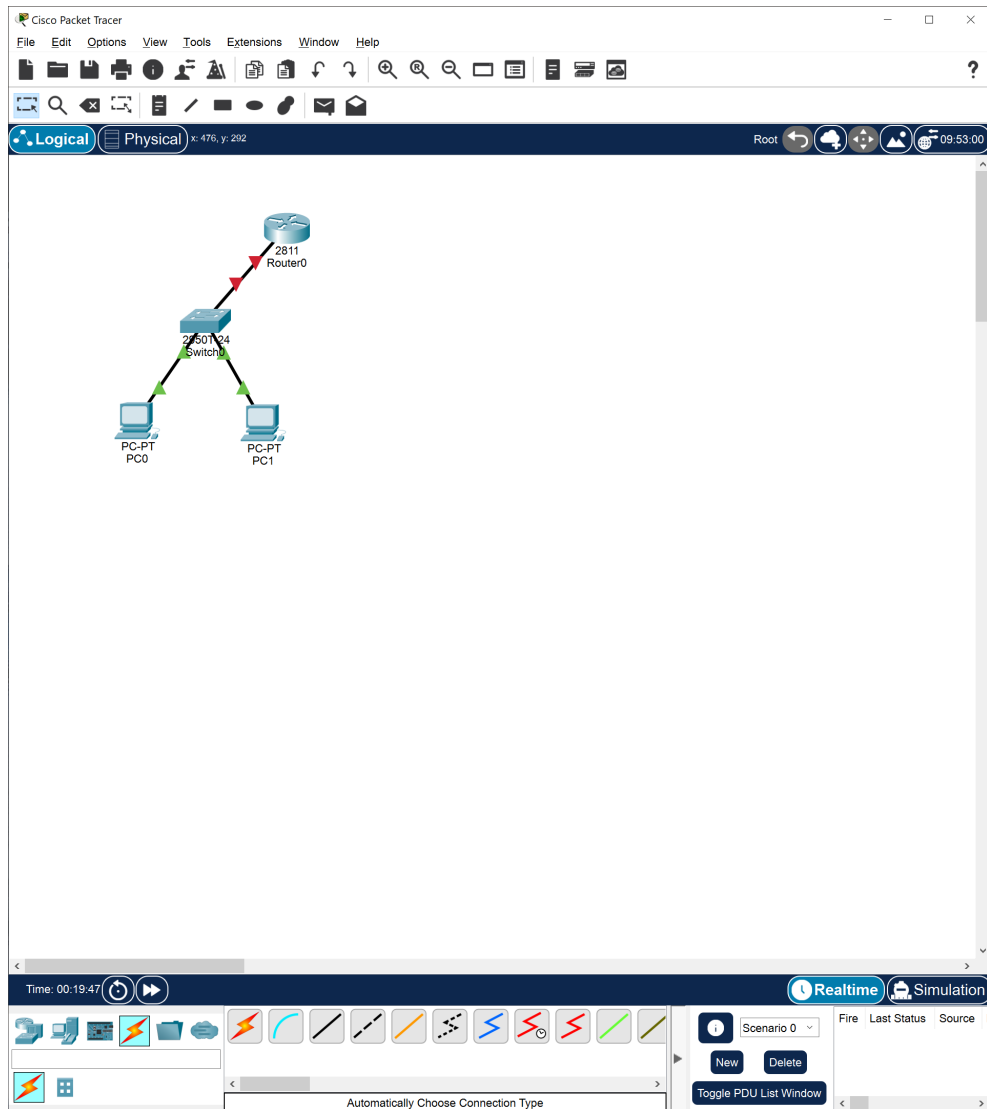
Now it's all green which makes us happy



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

The screenshot shows a window titled "Router0" with four tabs: "Physical", "Config", "CLI", and "Attributes". The "Config" tab is active, showing the configuration for "FastEthernet0/0". On the left is a sidebar with a tree view containing "GLOBAL" (with sub-items "Settings" and "Algorithm Settings"), "ROUTING" (with sub-items "Static" and "RIP"), "SWITCHING" (with sub-item "VLAN Database"), and "INTERFACE" (with sub-items "FastEthernet0/0" and "FastEthernet0/1"). The "FastEthernet0/0" interface is selected. The main configuration area for "FastEthernet0/0" includes: "Port Status" with an "On" checkbox; "Bandwidth" with radio buttons for "100 Mbps", "10 Mbps", and "Auto" (selected); "Duplex" with radio buttons for "Half Duplex", "Full Duplex", and "Auto" (selected); "MAC Address" with a text field containing "0060.7058.3901"; "IP Configuration" with fields for "IPv4 Address" and "Subnet Mask"; and "Tx Ring Limit" with a text field containing "10". Below the configuration area is a section titled "Equivalent IOS Commands" containing a text area with the following text:

```
--- System Configuration Dialog ---  
  
Would you like to enter the initial configuration dialog? [yes/no]:  
  
Press RETURN to get started!  
  
Router>enable  
Router#  
Router#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#  
Router(config)#  
Router(config)#interface FastEthernet0/0  
Router(config-if)#
```

 At the bottom left of the window is a "Top" button.

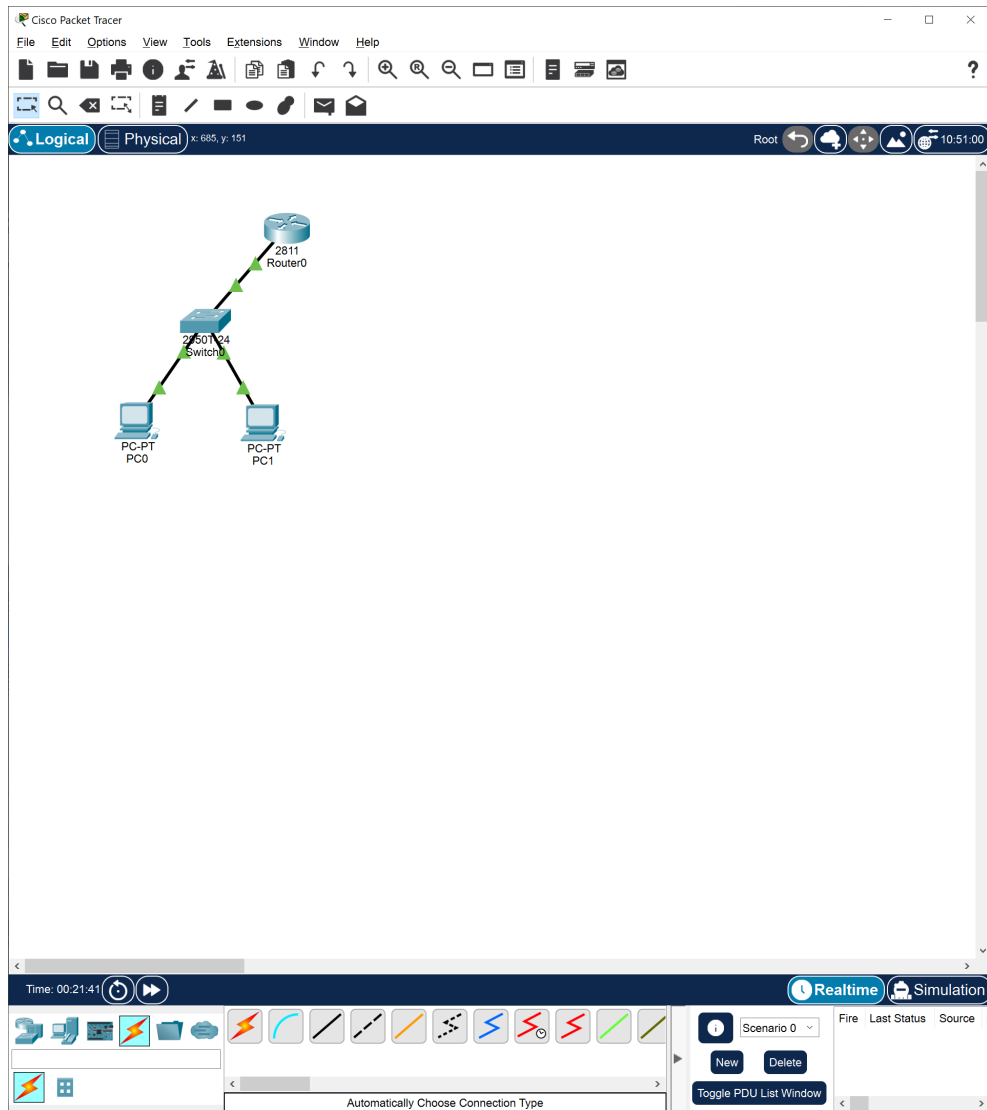
Once you click in the box a small tick will appear in it. This means the box is ticked and the function that box is proving is now being turned on

The screenshot shows the Router0 configuration window with the 'Config' tab selected. The left sidebar shows a tree view with categories: GLOBAL, ROUTING, SWITCHING, and INTERFACE. Under INTERFACE, 'FastEthernet0/0' is selected. The main area displays the configuration for 'FastEthernet0/0'. The 'Port Status' is set to 'On' (checked). 'Bandwidth' is set to 'Auto' (checked). 'Duplex' is set to 'Auto' (checked). The 'MAC Address' is '0060.7058.3901'. The 'Tx Ring Limit' is '10'. The 'IP Configuration' section has empty fields for 'IPv4 Address' and 'Subnet Mask'. Below the configuration area, there is a section titled 'Equivalent IOS Commands' with a text area containing the following commands:

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

At the bottom left, there is a 'Top' button.

as a result of ticking that box now you can see the link going green which means is enabled for data transmission



we only need to sort the **IP Configuration** out as well

The screenshot shows the configuration interface for Router0. The 'Config' tab is selected, and the 'FastEthernet0/0' interface is chosen from the left sidebar. The main configuration area for FastEthernet0/0 includes:

- Port Status:** ☒ On
- Bandwidth:** ☐ 100 Mbps ☐ 10 Mbps ☒ Auto
- Duplex:** ☐ Half Duplex ☒ Full Duplex ☒ Auto
- MAC Address:** 0060.7058.3901
- IP Configuration:**
 - IPv4 Address:
 - Subnet Mask:
- Tx Ring Limit:** 10

Below the configuration fields, the 'Equivalent IOS Commands' section displays the following commands:

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
```

At the bottom left, there is a 'Top' button.

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

$$255\text{values} - X\text{values}$$

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

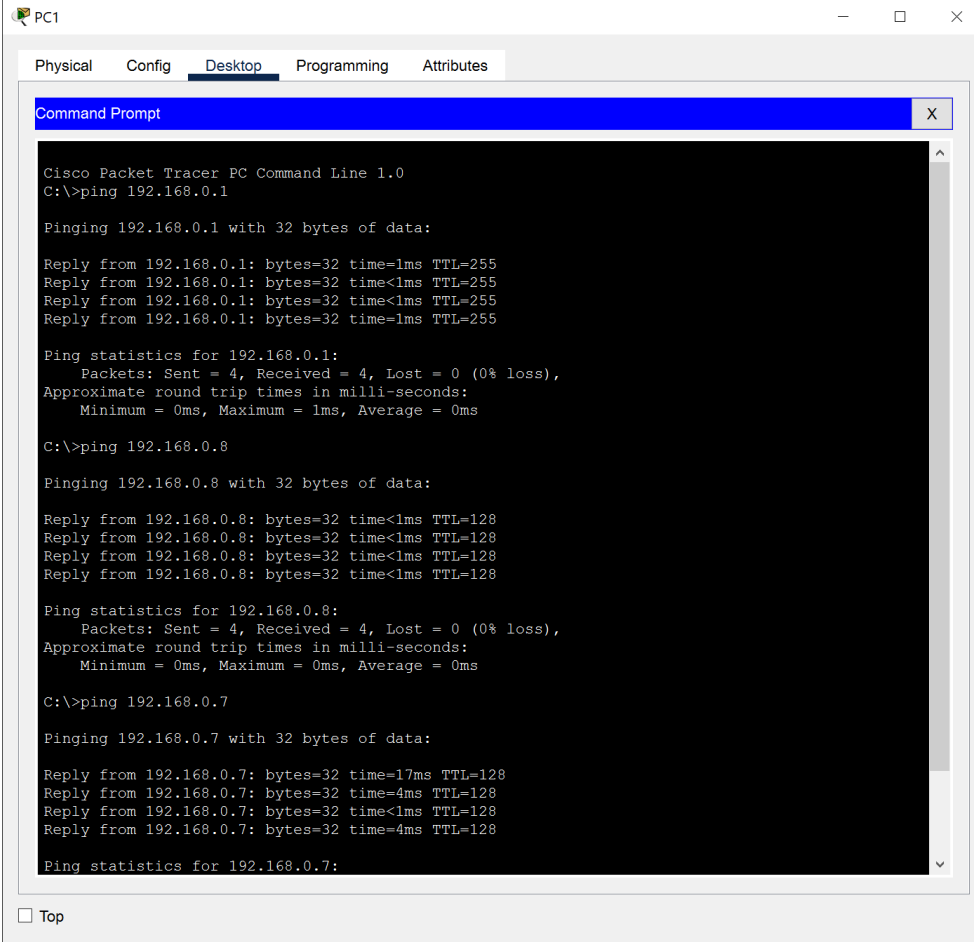
The screenshot shows a web-based configuration interface for a device named Router0. The 'Config' tab is active, and the 'INTERFACE' section is selected. The configuration for FastEthernet0/0 is displayed, showing the following settings:

- Port Status: ☒ On
- Bandwidth: ☐ 100 Mbps ☐ 10 Mbps ☒ Auto
- Duplex: ☐ Half Duplex ☒ Full Duplex ☒ Auto
- MAC Address: 0060.7058.3901
- IP Configuration:
 - IPv4 Address: 192.168.0.1
 - Subnet Mask: 255.255.255.0
- Tx Ring Limit: 10

Below the configuration, a section titled 'Equivalent IOS Commands' shows the following commands in a terminal window:

```
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#
```

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



The screenshot shows a Cisco Packet Tracer PC1 console window. The window has tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, showing a Command Prompt window. The Command Prompt displays the output of three ping commands: ping 192.168.0.1, ping 192.168.0.8, and ping 192.168.0.7. Each command shows four successful replies with 32 bytes of data, and the statistics indicate 0% loss.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.0.8

Pinging 192.168.0.8 with 32 bytes of data:

Reply from 192.168.0.8: bytes=32 time<1ms TTL=128
Reply from 192.168.0.8: bytes=32 time<1ms TTL=128
Reply from 192.168.0.8: bytes=32 time<1ms TTL=128
Reply from 192.168.0.8: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.0.7

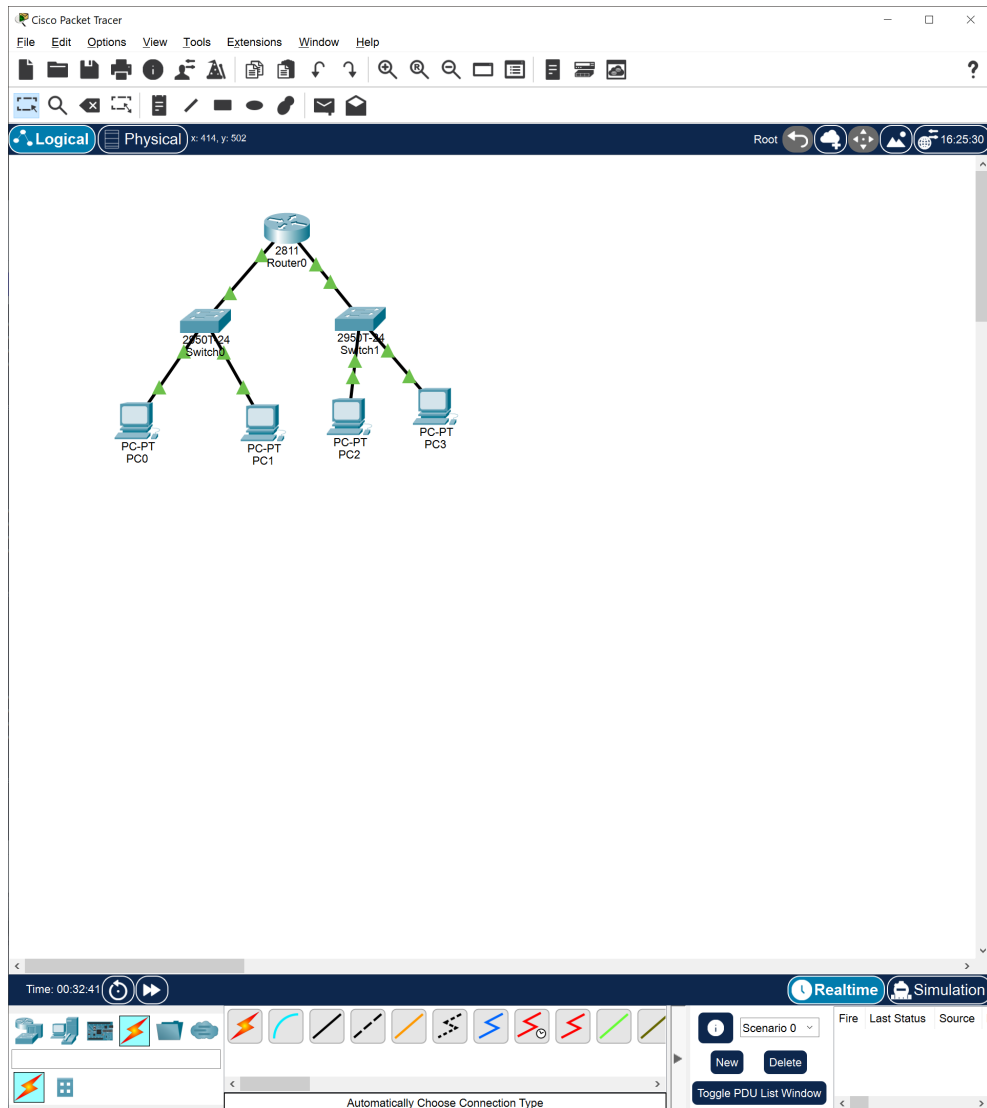
Pinging 192.168.0.7 with 32 bytes of data:

Reply from 192.168.0.7: bytes=32 time=17ms TTL=128
Reply from 192.168.0.7: bytes=32 time=4ms TTL=128
Reply from 192.168.0.7: bytes=32 time<1ms TTL=128
Reply from 192.168.0.7: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.0.7:
```

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

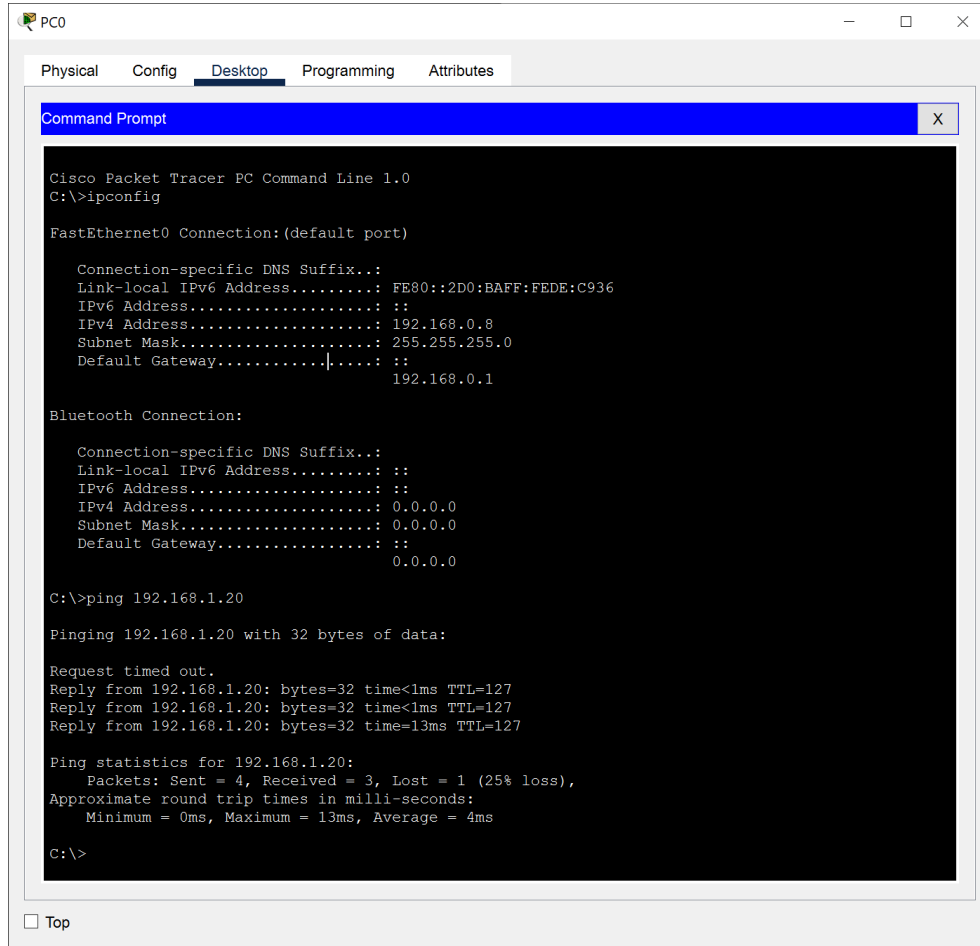
Let's add a printer with the following IP

192.168.1.20

The screenshot shows a window titled 'Printer1' with three tabs: 'Physical', 'Config', and 'Attributes'. The 'Config' tab is active. On the left, there is a sidebar with a tree view containing 'GLOBAL' and 'INTERFACE'. Under 'INTERFACE', 'FastEthernet0' is selected. The main area displays the configuration for 'FastEthernet0'. The 'Port Status' is 'On'. 'Bandwidth' is set to '100 Mbps' and 'Auto'. 'Duplex' is set to 'Full Duplex' and 'Auto'. The 'MAC Address' is '0004.9A90.BD99'. Under 'IP Configuration', 'Static' is selected. The 'IPv4 Address' is '192.168.1.20' and the 'Subnet Mask' is '255.255.255.0'. Under 'IPv6 Configuration', 'Static' is selected. The 'IPv6 Address' field is empty, and the 'Link Local Address' is 'FE80::204:9AFF:FE90:BD99'. A 'Top' button is at the bottom left.

FastEthernet0	
Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input checked="" type="radio"/> 100 Mbps <input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto
Duplex	<input type="radio"/> Half Duplex <input checked="" type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto
MAC Address	0004.9A90.BD99
IP Configuration	
<input type="radio"/> DHCP	
<input checked="" type="radio"/> Static	
IPv4 Address	192.168.1.20
Subnet Mask	255.255.255.0
IPv6 Configuration	
<input type="radio"/> Automatic	
<input checked="" type="radio"/> Static	
IPv6 Address	
Link Local Address:	FE80::204:9AFF:FE90:BD99

Let's ping the printer from PC0



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address.....: FE80::2D0:BAFF:FEDE:C936
    IPv6 Address.....: ::
    IPv4 Address.....: 192.168.0.8
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: ::
                                192.168.0.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address.....: ::
    IPv6 Address.....: ::
    IPv4 Address.....: 0.0.0.0
    Subnet Mask.....: 0.0.0.0
    Default Gateway.....: ::
                                0.0.0.0

C:\>ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.20: bytes=32 time<1ms TTL=127
Reply from 192.168.1.20: bytes=32 time<1ms TTL=127
Reply from 192.168.1.20: bytes=32 time=13ms TTL=127

Ping statistics for 192.168.1.20:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 4ms

C:\>
```

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

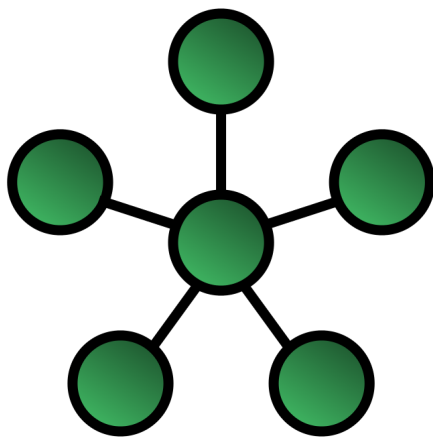
Network topology is the arrangement of the elements (links, nodes, etc.) of a communication network.

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

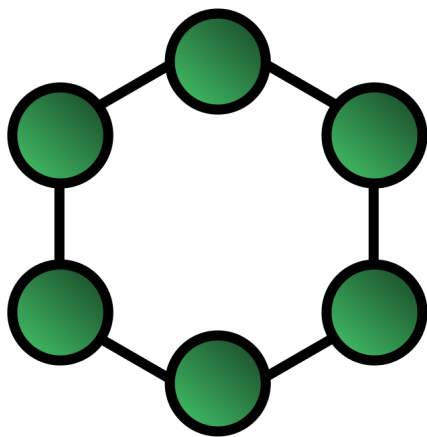
- simplicity of adding additional nodes
- is the easiest topology to design and implement

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

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

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

11.1 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.

11.1.1 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 rout-

ing 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.

11.1.2 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[1] 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.

11.2 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

11.2.1 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.[1] BGP is classified as a path-vector routing protocol,[2] 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).