


Learning About Networking Using Cisco Packet Tracer

Cisco Packet Tracer is a network simulation and design tool used to learn networking concepts. You can download the software at [Cisco Packet Tracer - Networking Simulation Tool \(netacad.com\)](https://www.netacad.com).

We will be running the program via a Virtual Machine. Make sure you have

installed [Virtual Box](#)  on your computer and then download the following machine appliance file:

<https://drive.google.com/file/d/1WNQNbtIsiRyFoHjMeQmcZXuVQvCpLH1M/view?usp=sharing>

Start **Virtual Box** and then click **File**→**Import Appliance**

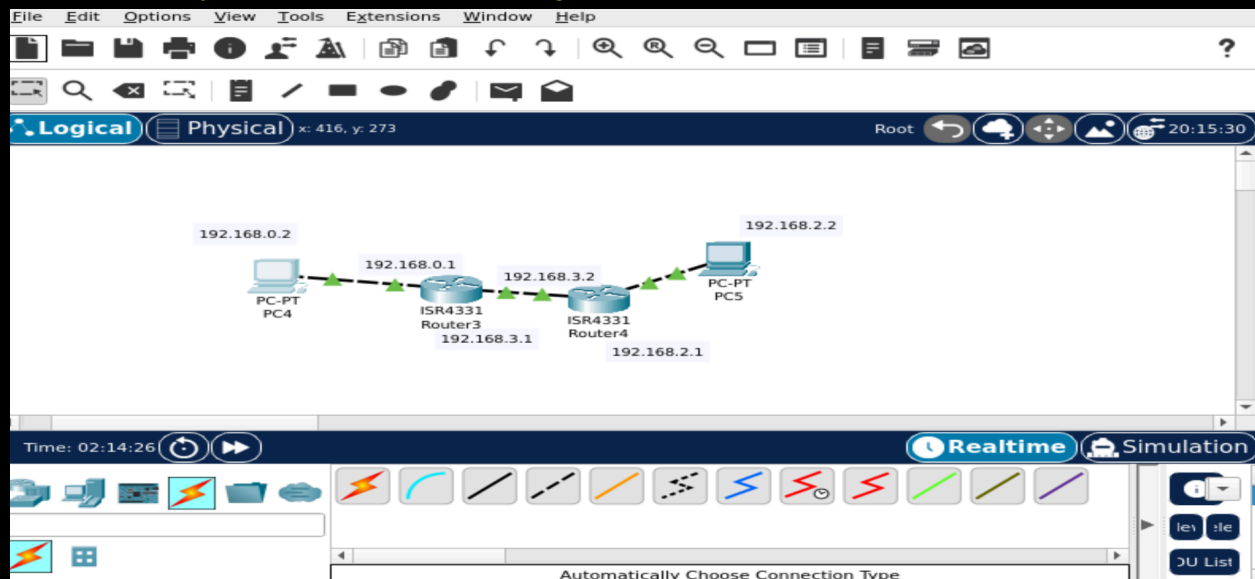
Select the file and follow all default settings.

Once the machine is set up, start it and then click on the **Start** button in **Bodhi Linux**, go to **Applications**→**Other**→**Cisco Packet Tracer(CPT)**.



You could also use the [iso file](#) made with Bodhi Linux and CPT.

Start CPT and you should see the following:




The middle of the screen is where we can design our networks and test them. There are many, many features available of which we will only be using a few.

Before we begin using CPT we need to learn about a variety of networking concepts first.


 Open the slide [Intro to Networking](#) and complete it with your teacher.


 Open the doc [What is An IP Address](#). Read and complete the questions at the end.

 Open the slide [Building Network Cables](#) and complete it with your teacher.

 Open the slide [What are slide Routers, Hubs and Switches](#) and complete it with your teacher.

 Open the slide [What is a Mac Address](#) and complete it with your teacher.

 Open the slide [What is DNS and DHCP](#) and read through it and complete the QnE at the end.

 Open and read through and complete all the work on the [Router Networking](#) handout.

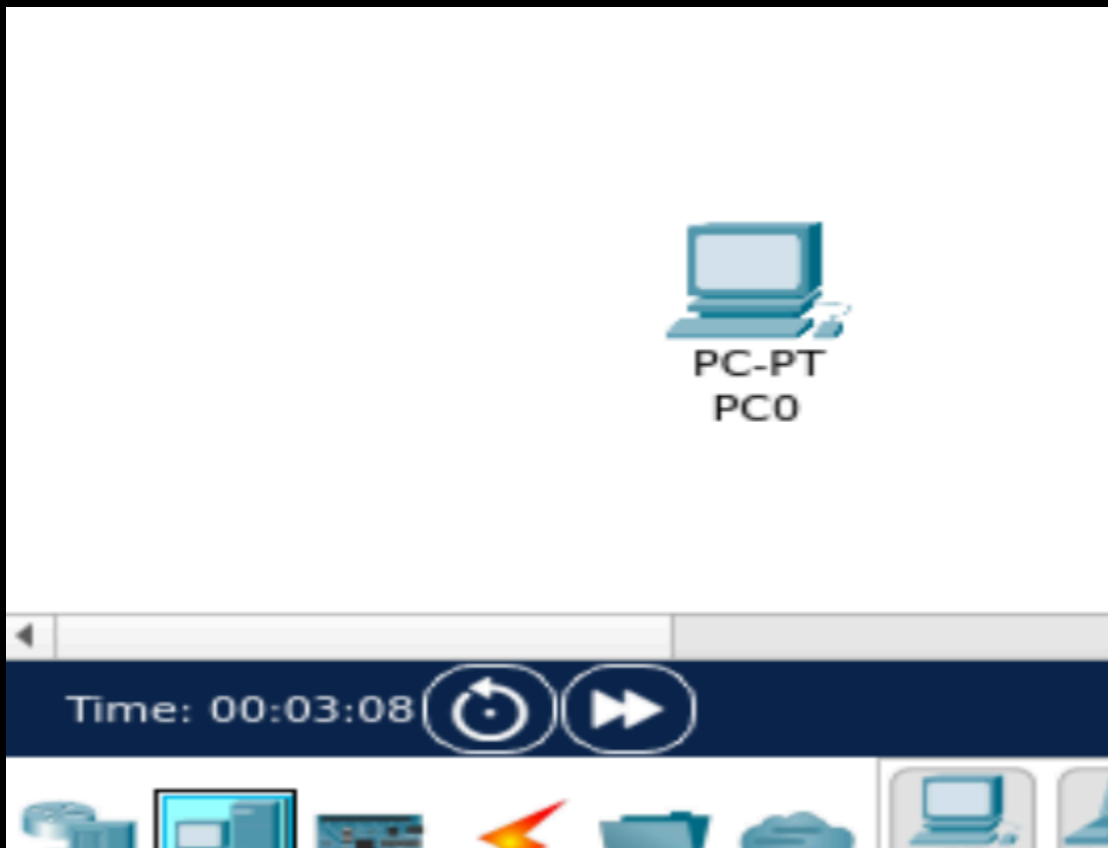
^ Do not do

IP Addresses

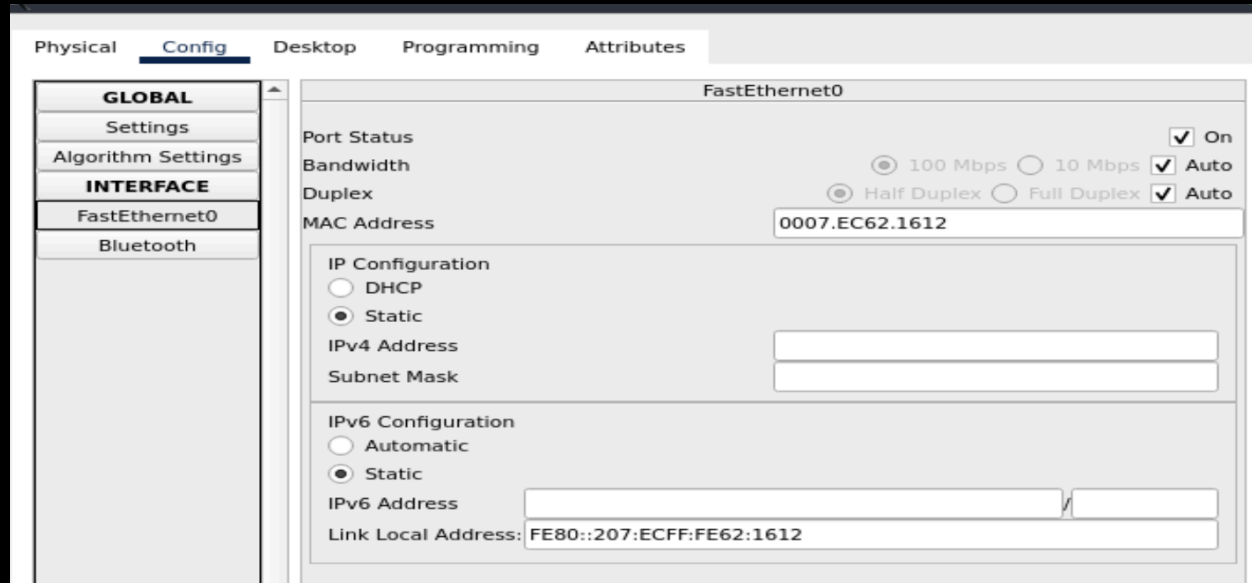
Every device connected to the internet has an **IP address**. This is a 4 number address between 0 and 255 that identifies that device on the network. Let's add a device to our network in **CPT**. All the available devices are listed by clicking on the bottom left icon at the bottom left corner of the CPT program:



To the right of this icon is a computer. Click and drag the computer onto the screen.

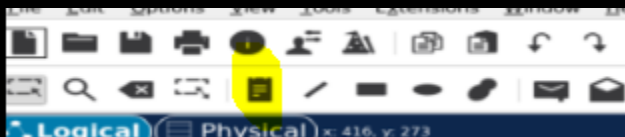


To see or set the IP address of this computer, double click it, then click on the **Config** tab and then click on the **FastEthernet0** box from the selections provided:

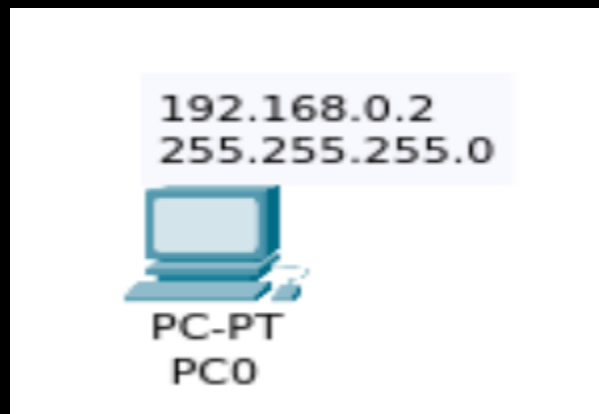


You should see the above. Note that the IPv4 address is empty which means that this PC has not yet been assigned an IP address. You can assign the PC an address or you can have a program do it for you. For now we will assign IP addresses **statically** or **manually**. Make sure the **Static** option is selected. Also make sure the **Port Status** is **On**. In the IPv4 address box type **192.168.0.2** and in the **Subnet Mask** type **255.255.255.0**. Leave the settings screen and then mouse hover over the PC. You should see the IP address set for the only **NIC(network interface card)** on that PC.

A good habit is to label the PC with text indicating its IP address and subnet mask info. On the toolbar above the design window click on the **Place Note**



icon and then click above the PC and then type in the **IP** and **Subnet Mask** info.



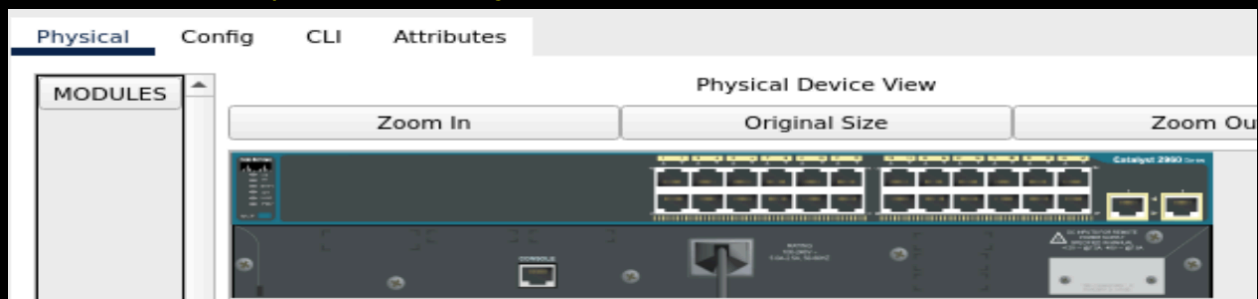
Double click the PC, select the **Config** tab and change its **Display Name** on the main dialog box that appears. Change it to '**PCLeft**'.



Normally when we connect PCs in a network we use a **Switch**. A Switch is a network device that connects all the devices on one network together. Each device on a network is referred to as a **Node**. Click on the **All Network** devices icon (bottom left) and then find the Switch and add it to your network.



Before we go on we should have a good idea of how this Switch looks in real life. Double click it and then make sure you are in the **Physical** tab.





You'll see the back of the Switch with a large number of **RJ-45 ethernet ports**. In this case there are 24 of them to allow for up to 24 Nodes to be connected to a network.

Below is a real life image of this Switch:

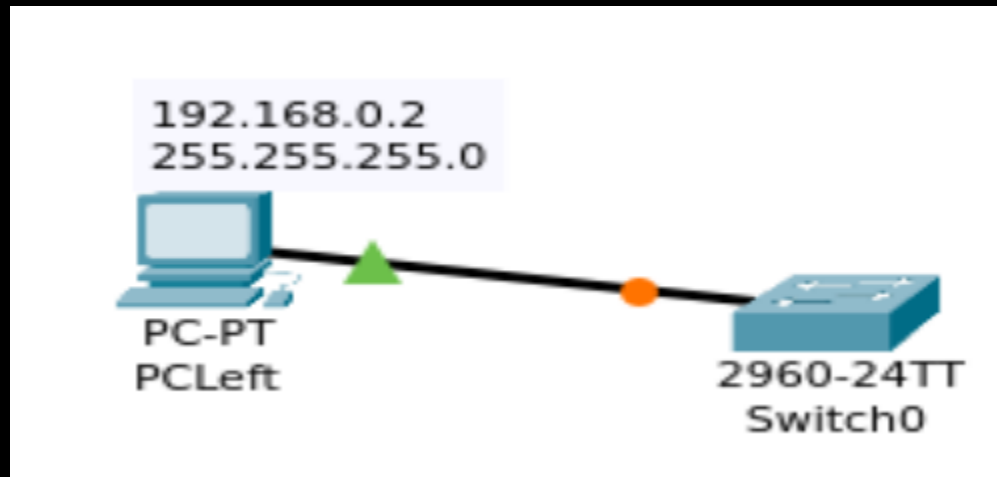


We connect devices to the Switch using an **ethernet cable**



or more specifically a **Straight Through** ethernet cable. To connect devices with cables in **CPT** click the **Connections** icon  and then select the same icon from the list of connections (this will automatically pick the right cable...although you could do it manually by picking a **Straight Through** cable ).

Once selected, click on the PC and drag the cable to the Switch. You should see this:



The green triangle indicates that the connection is good and data can pass through it between the devices.

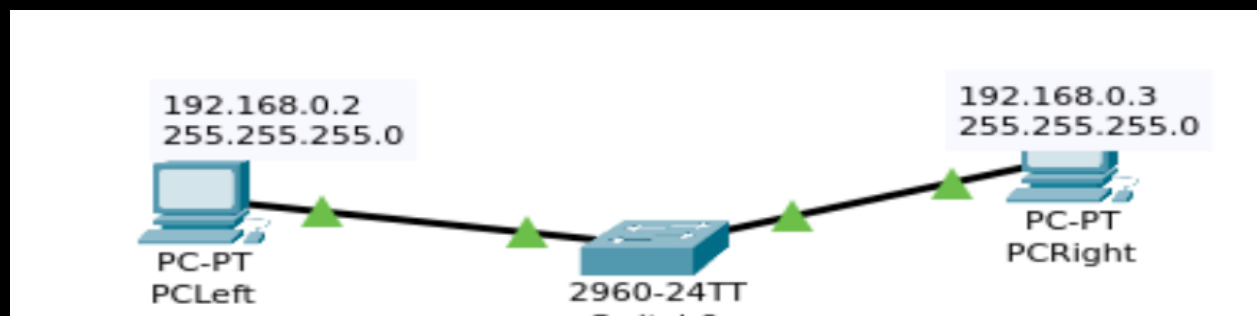
Connect a second PC on the right side of the Switch with the following info:

Name: PCRight

IP Address: 192.168.0.3

Subnet Mask: 255.255.255.0

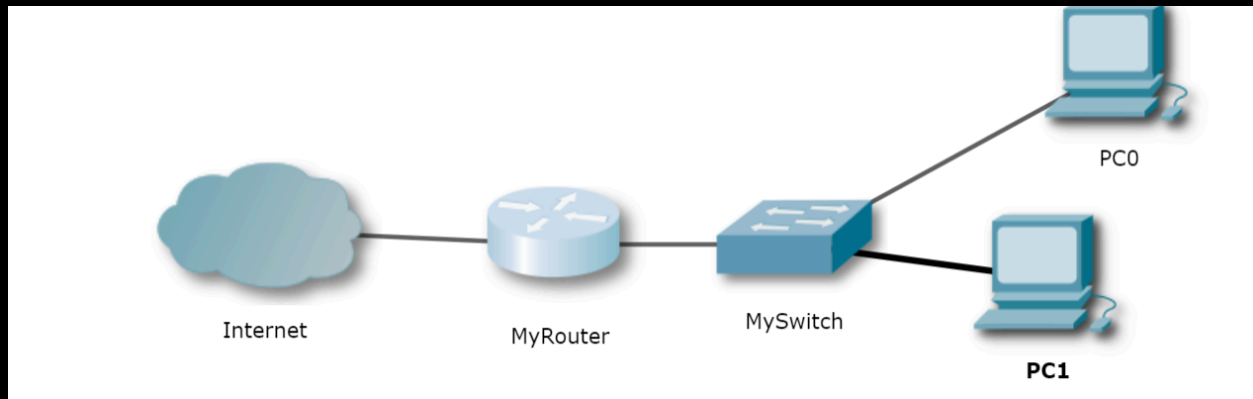
Port: On



Note all the green triangles, which means we have a good connection on all endpoints between all connecting devices.

Do some research and learn how to use the ping command in the windows console to test the connection between these computers. To access the command prompt in either of these computers click the computer, select **Desktop** from the tabs and then **Windows Console**. Enter the ping command in this window to test the connection between one computer and the other.

A **Router** is the device that allows all the devices on one network to connect to devices on another network. In essence, a **Router** is the **Gateway** to another network. In this diagram the other network is the **Internet**.



The first thing when setting up a local network (LAN or local area network) is to configure the router. Oftentimes the router comes pre configured with its own IP address. Normally the router has 2 interfaces 1. For the connection to the internal network (connected to the LAN ports) and 2. For the connection to the internet or other network (connected to the WAN port). Most routers have an internal IP of 192.168.0.1 while the internet facing IP interface is assigned from the ISP(internet service provider) provider.

Add a router to your network by clicking on the **Network Devices** icon again and then add the first Router in the list (the 4331 Router):



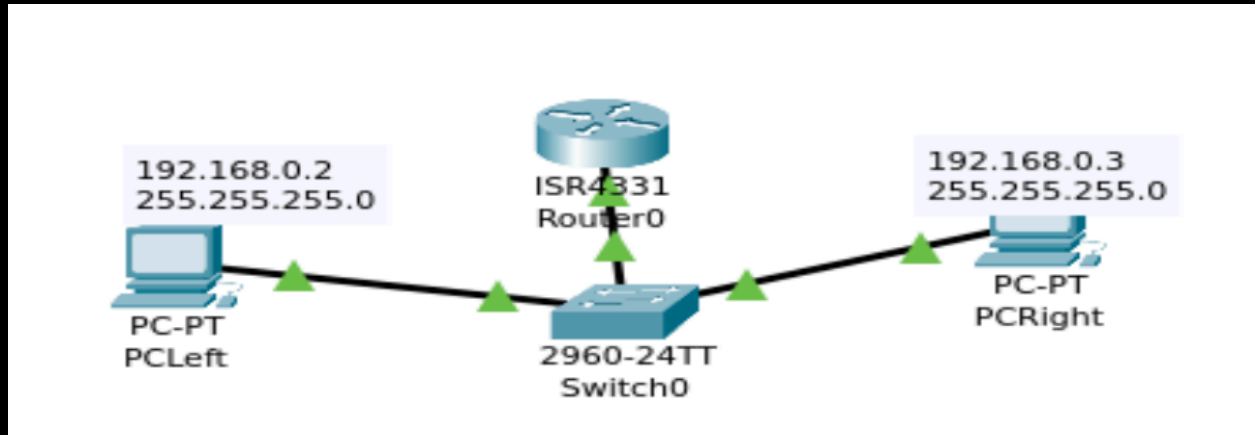
Embed a screenshot of the physical look of the Router below:



You should notice that there are far fewer ports on the Router because its role is simply to connect 2 separate networks together.

Connect the **Router** to the **Switch**. Double click the Router and select the **Config** tab. Go to the **Interfaces** section and notice the three **GigaBitEthernet** ports. Each port can be connected to the **Switch** of a different network.

Click on **GigabitEthernet0/0/0** and set its IP to **192.168.0.1** and **Subnet Mask** to **255.255.255.0**. And make sure the **Port Status** is **On**.



You should notice all triangles are green meaning we have a viable network!

Add a text note to the router showing its IP address and subnet mask:

Save the current network. Embed a screenshot of it here:



Computers that are connected to a **Router** can be automatically assigned an IP address via **DHCP (Dynamic Host Configuration Protocol)** or can be manually assigned. We will manually assign our PCs their IP addresses. In order for the PCs to be on the same network as the **Router** they have to have the same network address. The **Subnet Mask** is used to identify the portion of the IP address that is the **Network Address**. Since our Router had an IP address of 192.168.0.1 and a Subnet Mask of 255.255.255.0 it is considered to be on the 192.168.0.0 network and for any device to communicate with it they need to be on the same network.

Question:

Look at the following image. Assuming both computers have a subnet mask of 255.255.255.0. What is each computer's host address and what is the network address both are on?

PCLeft

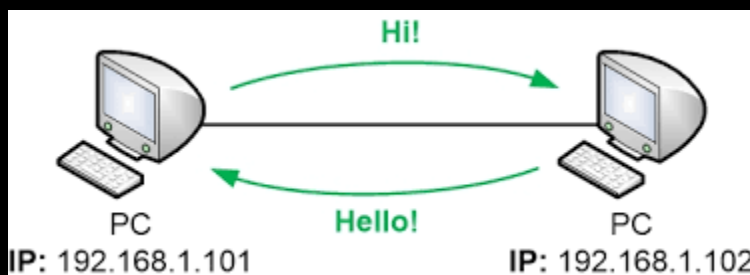
Network address: 192.168.1.0

Host address: 101

PCRight

Network address: 192.168.1.0

Host address: 102



Exercise:

Create a new network with 3 PCs, a switch and a router. The network address is 192.168.2.0. Give the PCs and router each a unique **Host** address. The **Host** address is normally the last

number in the IP address and must range between 1 and 255 (1 is often used for the router). Do not use 0 for the host address as this is reserved for the network address.

What are the host addresses of the following:

PC1:192.168.2.1

PC2:192.168.2.2

PC3:192.168.2.3

Router0:192.168.2.4

What is the Network address for all 3: 192.168.2.0

Fully label the network and embed a screenshot here. Make sure to save a copy of the network file:



Network Host and Broadcast Addresses

An IP address is made up of 4 numbers, each between 0 and 255. Because of this only 1 byte or 8 bits are needed to represent each number. This is why it's referred to as a **4 octet number**. Octet meaning 8. IP addresses should really be viewed in their binary form to understand the role of binary numbers in their designations.

Here's an example IP address and its subnet mask:

192.168.0.1= 11000000.10101000.00000000.00000001

255.255.255.0= 11111111. 11111111. 11111111 .00000000

The **Subnet Mask** tells the network device what network address it's a part of and what part of it refers to its unique address i.e. **Host Address**. The 1s in the Subnet Mask designate the Network Address portion of the IP address. The 0s designate the Host portion.

192.168.0.1= 11000000.10101000.00000000.00000001

255.255.255.0= 11111111. 11111111. 11111111. 00000000

Exercise: Determine the Network and Host Addresses of the following IP Address Subnet Mask pairs:

124.248.127.114 255.255.255.0 Network: 124.248.127.0 Host: 0.0.0.114

252.0.163.175 255.255.0.0 Network: 252.0.0.0 Host: 0.0.163.175

83.184.109.10 255.255.255.0 Network: 83.184.109.0 Host: 0.0.0.10

171.11.22.137 255.255.0.0 Network: 171.11.0.0 Host: 0.0.22.137

44.100.23.19 255.0.0.0 Network: 44.0.0.0 Host: 0.100.23.19

153.94.9.132 255.255.255.0 Network: 153.94.9.0 Host: 0.0.0.132

166.78.52.207 255.255.0.0 Network: 166.78.0.0 Host: 0.0.52.207

239.19.133.158 255.0.0.0 Network: 239.0.0.0 Host: 0.19.133.158

39.157.145.174 255.255.255.0 Network: 39.157.145.0 Host: 0.0.0.174

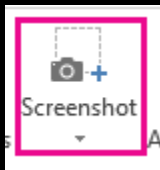
194.28.65.81 255.0.0.0 Network: 194.0.0.0 Host: 0.28.65.81

Question: If an IP address is 192.168.0.1 and the Subnet Mask is 255.255.255.0, how many possible host addresses are there?

Answer: Remember, each IP address octet can range from 0 to 255. Usually, but not always, 0 is reserved for the network address and 255 is reserved for the **Broadcast address**. The Broadcast address is used to send a packet of data to all hosts on the same network address. So, technically that leaves 254 hosts with addresses that range between 1 and 254! In our last network, you should have assigned 4 different host addresses. Three of them were assigned to the 3 PCs and 1 to the router (they should have been any number between 1 and 254). That leaves us with 251 more possible devices to attach to this network!

Exercise: In this exercise we will use some common **Windows Console commands** to test our network. Load your original network you made with PCLeft and PCRight. To bring up the console for a PC device just click or double click it and select the **Desktop** tab and then click on the **Command Prompt** button. Do this for PCLeft and type in the console/terminal window the following:

ping 192.168.0.3. Take a screenshot and embed it below:

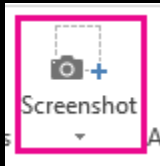


What you should notice is that PCRight which is located at 192.168.0.3 replies. To ping a host computer means to send packets of data to it in the hope it will respond. In the output PCLeft sends 32 bytes worth of data to PCRight and gets 4 replies indicating that it received them! This means that the two hosts are successfully connected to each other on the same network. This means we can set up apps to communicate between these computers i.e. LAN game , servers, chats etc.

Insert below 3 URLs to videos describing the network ping command:

1. <https://youtu.be/llicPE38O-s?si=-iGdkMvNRieb9pfA>
2. <https://youtu.be/tVOHTjf94M8?si=tN6Pcq58Q47ugGdQ>
3. <https://youtu.be/KYmtMBsuA50?si=nX-QrOCk2iUdgWvj>

Exercise: Try pinging 192.168.0.15 from PCLeft. Embed a screenshot of the response:



Obviously this time there was no response as there is no device with that IP address on the same network!

Exercise : Try pinging PCLeft from PCRight. Explain what happens. Embed a screenshot of the response:



IPCONFIG

You just learned how to use the ping command to determine if another host was reachable on the network. If it was, then it meant that the other device is reachable from the device that sent the ping. Another command is often used to determine information about the current device on the network. Enter the command **ipconfig** into **PCLeft** and hit enter in the console and embed a screenshot below:



Note the information listed. You'll see the device's IP address and its Subnet Mask. There's more but we'll get to that later.

Now add the option **/all** to the command i.e. **ipconfig /all**. Embed a screenshot below:



What additional information do you see?

The additional information is DHCP info

What is another name often used for the **Physical Address**?

MAC Address

In what format is the physical address represented?

Hex

What is a **DNS server**?

A Domain Name System/Server is a server that assigns Domain names (text based addresses) to IP addresses for ease

What is a **DHCP server**?

A DHCP server assigns dynamic IP addresses to computers in a network

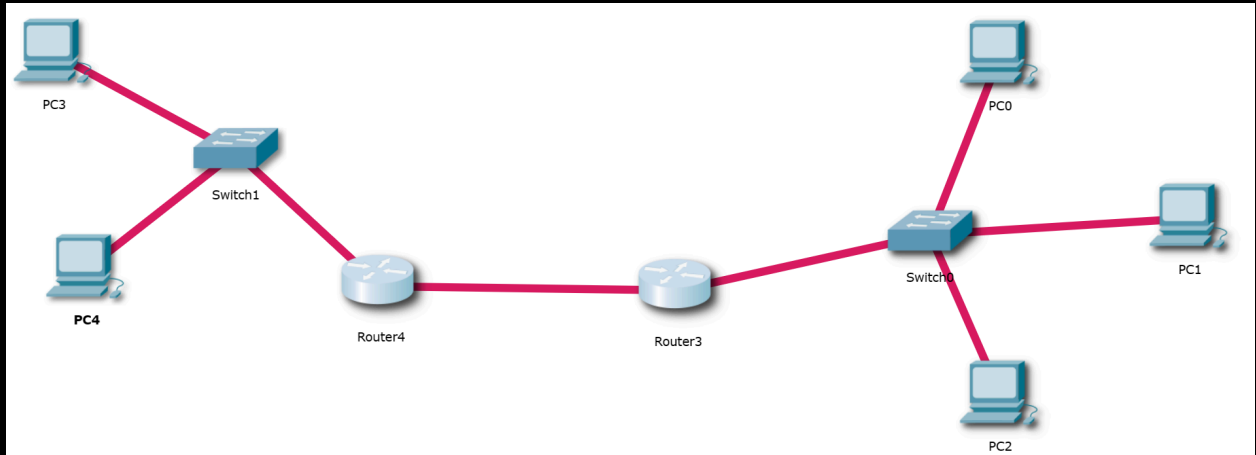
Why does your computer need the address of these servers?

To know where to get the information from

Questions and Exercises:

1. What is a WAN? Wide area network - connects different LANs together like internet
2. What is a LAN? Local area network - connect small PCs in small areas like homes
3. What is the difference between a WAN and a LAN? WAN covers a wider area and connects LANs
4. How does the internet relate to the LAN and the WAN? Internet is a WAN and WAN connects LANs
5. What is another name for gateway? Router
6. How is a switch different from a gateway? A switch connects computers together, while a router connects different devices

7. What is a network packet? A unit of data sent on a network
8. What is a protocol? Rules that state how data should be used (sent, received, etc)
9. What is the protocol of the internet? TCP/IP (Transmission Control Protocol/Internet Protocol)
10. Create a new network with 3 PCs and attempt to ping PC1 and PC2 from PC0. What happens and why? If there is a problem, fix it and try again. They replied because they all have the same network address and are connected to the same network,
11. What happens when you ping your network address 255 from PC0? Why do you get replies from several different host addresses? What devices are assigned these host addresses? There is a reply from every computer on the network. This is the broadcast number.
12. Create a new network that looks as follows:



13. Configure the left side of the network to be on network address 192.168.0.0 and the right side to be on 192.168.2.0
14. Ping PC4 from PC3. What happens and why? We got a response because they share a network address and are both connected to the switch
15. Ping PC0 from PC4. What happens and why? There is a reply because both PCs are connected to their respective switches, sharing a network address, and are connected to their individual routers which are connected together.

Switches and Routers Review

A Switch is a device used to connect all devices in the same network. A Router is a device used to connect other networks to each other. You will always have a Router in between networks. Each port in a Switch can be connected to a network device or node in the same network. Switches use the **MAC** address of the device they are connected to help identify each device.

Exercise:

Open the following network:

https://drive.google.com/file/d/10xEjwGdh9be_q92O3OPHmWtESPjecoF/view?usp=sharing

Find the network address by looking at the IP address of one of the PCs and then using its console ping its broadcast address to find the IP addresses of all the PCs. Embed a screenshot here:



Determine how many ports the Switch has by selecting the Switch. Go to the Config tab and then to Interfaces. How many Ethernet ports are there?

24 FastEthernet and 2 GigabitEthernet

Switches keep track of all the devices connected to them by recording their **MAC** addresses.

Exercise:

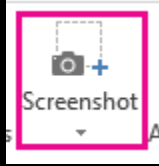
To see the table of MAC addresses do the following:

1. From one of the PCs send a broadcast ping command.
2. Enter the Switch CLI console window via the CLI tab. In the console type the following:

```
enable
```

```
show mac-address-table
```

Embed a screenshot of the output:



Now select PC0 and find its MAC address by selecting the Config tab and then go to INTERFACE and select the FastEthernet0 bar. What port is PC0 connected to on the Switch?

Fa0/2 or Port 2

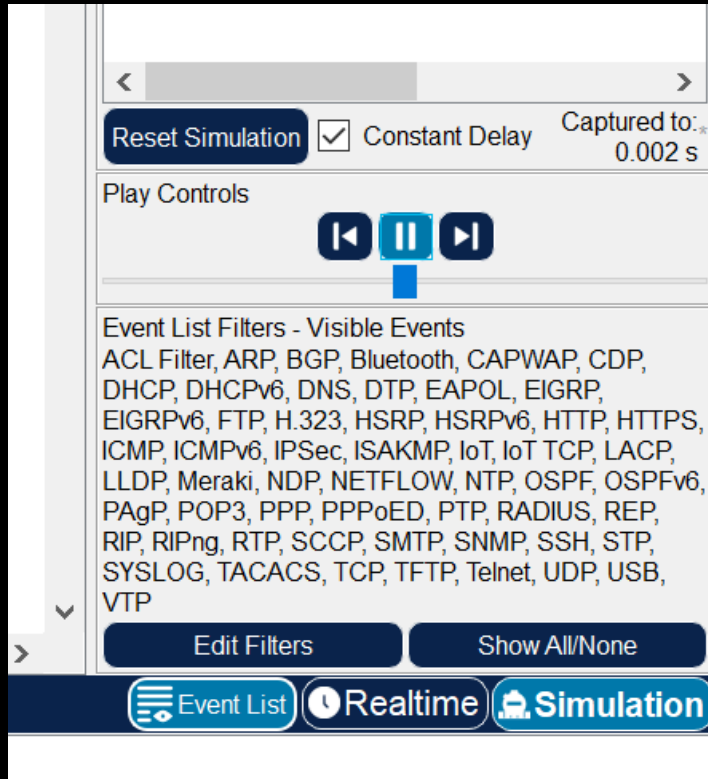
All data packets sent from one device to another in a network have the MAC address of the sending device and the destination device. The Switch checks which port is connected to which MAC address and then knows where to send the packet i.e. via which port. Hubs, another network device, don't do this and simply send a copy of the packet through all of their ports hoping that the destination device will be one of the receivers to get it. As a result of this, Hubs are much more inefficient at dealing with network traffic and are not good for large busy networks.

Exercise:

Create a new network with 1 hub in the center and 4 PCs connected to it. Give each PC an address on the same network. Embed a screen of your network here:



On the toolbar at the top look for the **mail** looking icon and press it. Then click on any PC and then on any other. Next click on the **Simulation** button at the bottom right corner of the screen and then click the play button that appears.



Watch what happens to the packet of data meant to be sent to only one of the other PCs.

Describe what happens?

The packets are sent to all other PCs, however only the two that were not supposed to be sent the packets are sent with an X. As well, the starting PC received the packet back.

Do the exact same thing but replace the Hub with a Switch. Describe what happens? Embed a screenshot here:

The package is only sent to PC 1 and then is sent back to PC 0.

Routers are responsible for routing data across different networks using IP addresses. Switches use MAC addresses to know where to send data inside the same network.xcc

Review Exercise:

Identify the network and host portions of the following IP addresses. The first has been done for you.

IP address	Subnet mask	Network address	Host ID
192.168.1.105	255.255.255.0	192.168.1.0	105
192.168.10.6	255.255.255.0	192.168.10.0	6

172.16.32.25	255.255.0.0	172.16.0.0	32.25
10.80.1.10	255.0.0.0	10.0.0.0	80.1.10

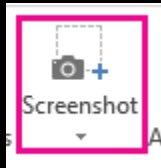
In which of the following are the source and destination devices on the same local network, and which are on different networks? The first has been done for you.

Source: IP address and subnet mask	Destination: IP address and subnet mask	Same local network or different networks?
192.168.1.105 255.255.255.0	192.168.1.250 255.255.255.0	Same: both have network address 192.168.1.0
192.168.10.6 255.255.255.0	192.168.10.252 255.255.255.0	Same network
192.16.32.25 255.255.0.0	192.168.31.32 255.255.255.0	Different network
10.80.1.10 255.255.0.0	10.80.2.26 255.255.0.0	Same network

Open the following network:

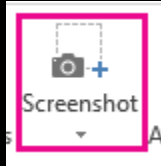
<https://drive.google.com/file/d/1kkzAyhanegS3digYs55i4YZDHNYI6hgY/view?usp=sharing>

Attempt to ping PC4 from PC5. What happens? Why? Embed a screenshot of the response you get.



You get the expected reply because both PCs are on the same network address of 192.168.8.0.

Now try and ping PC6 and PC7 from PC4 or PC5. What happens? Why? Embed a screenshot of the response here:



PC6 and PC7 are on a different network address 192.168.2.x and so it can not be reached by PC4 or PC5 which are in the network address 192.168.0.x.

Check Router0 and its Interface information. How many interfaces have been configured?

One has been configured (GigabitEthernet0/0)

Check Router1 and its Interface information. How many interfaces have been configured?

One has been configured (GigabitEthernet0/1)

In order for Router0 to communicate with Router1 and then in turn with the devices in Router1, Router1 needs to have its interfaces configured properly i.e. the port connecting to Router0 and the port connecting to Switch1. We'll discuss how to do this when we talk about **Routing**.

Dynamic Configuration

By now you should understand that all devices connected to a network need an IP address. So far we have been manually assigning these values but in real life that would be a tedious task, especially considering that devices connect and disconnect from different networks all the time. This can be done automatically or dynamically through something called **DHCP** or **dynamic host configuration protocol**.

Most routers have a //DHCP server built into them. This is a program that will automatically determine what the best IP address is that should be assigned to a device that connects to it.

Exercise: Open the following network:

<https://drive.google.com/file/d/17nbVeE7jhs38UMM0-T1r1iBDgu0ZnHtW/view?usp=sharing>

Open any PCs console and type

ipconfig /all

Does it have an IP address? How about a Subnet mask? What does this mean about its ability to communicate with any device on the network? Embed a screenshot of the response here:

NO it does not have an Ip address, nor a subnet mask. This means it cannot connect to any devices.



Since the PC has no IP address nor Subnet mask this means it will not be part of the local network and will therefore not have access to any device or service on that network.

Click on any PC and then select the Config tab and then the Settings bar. Under the Gateway/DNSIPv4 box select DHCP. Now we have to connect it to a DHCP server. To do this, click the End Devices icon



And then find from the displayed list a Server and add it to the network. Connect the server to Switch0. Click on the Server, go to Config, then under the Gateway/DNS box select Static and enter the IP of Router0. Select the FastEthernet0 bar and under IP Configuration select Static and then enter the IP Address 192.168.0.2 and Subnet Mask 255.255.255.0. Next click on the Services tab and go to the DHCP bar and turn the service on. Set the Default Gateway to Router0's address. For start IP addresses we'll start assigning them at 192.168.0.3 (we already used 192.168.0.1 for Router0 and 192.168.0.2 for the Server. Set the Maximum Number of Users to 254. Click the Save button.]

Select any PC on the network attached to the Server and enter its console. Type:

ipconfig /renew

ipconfig /all

What do you notice has happened?

The PCs now have been assigned IP addresses!!!!

Add a new PC to the switch. Repeat the console commands.

What happened?

The new PC was assigned an IP address

DHCP has automatically assigned IP addresses to all our new devices connected to the network. It's no longer necessary to manually assign them each time we connect a new device.

Identify the two correct statements in the list below.

IP addresses starting 192.168.0.0 are private addresses and are commonly used in home networks. **Correct**

ISP stands for Internet Secret Protocol and is used to deliver packets to private addresses. **Wrong!!! It stands for Internet System Protocol**

Devices can never have the same IP address, even on different home networks. **Wrong again bucko**

ISP is an abbreviation for internet service provider. **Correct you are awesome!!!**

NAT(Network Address Translation)

NAT is used to allow local network devices with internal IP addresses to communicate with devices in other private local networks with possibly the same IP address.

This works because the router has a public and a private IP address. When the internal device with a private IP address sends a data packet to the internet the router substitutes its public IP address with the private one so it essentially does the communicating for the internal private IP address device. When the internet device sends back a response the router knows to which private device to send the data to.

Identify the one correct statement in the list below.

NAT is an acronym for network address transmission. **WRONG! ITS TRANSLATION**

A typical home gateway router can carry out network address translation (NAT).

Ding! right

If you want to use NAT on a typical home network, you will need to buy an additional computer to carry out network address translation. **WRONG**

An ISP may send out thousands of similar home gateways to its customers. Can they all be given the same LAN IP address?

No they can't, as LAN IP addresses cannot match if they are all connected to the same ISP

WIFI

A gateway can be configured as a wifi access point. This essentially allows devices to connect to it wirelessly as if it were connected to it with wires. In order for a device to connect to the gateway the gateway will need to have an **SSID (service set identifier)** that will be broadcast so that users can select it from a set of potential wireless networks to connect to. Security is important so at a minimum the **WPA2 Personal** should be selected which requires the user to know a password or passphrase or sometimes called a pre-shared key).

Some years ago, home gateways were often delivered with the same default SSID and passphrase/key, accompanied by instructions on how to change these. Nowadays,

there is usually a label displaying a complicated passphrase/key attached to the gateway. Which is better?

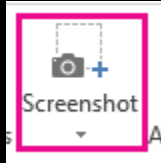
The modern version is better, as most people are lazy and will not change their default password, making their network not secure!!!

DNS(Domain Name System)

The DNS is used to convert between human readable addresses and numeric IP addresses. There are DNS servers on the internet that perform this operation.

For example www.google.com might be 172.217.18.196. It's easier for us to remember the former and have a computer convert it to the latter for actual use.

In your personal computer terminal window type **ipconfig /all** or **ifconfig -a** on a Mac or Linux. Look for the DNS server info. Embed a screenshot here:



Exercise:

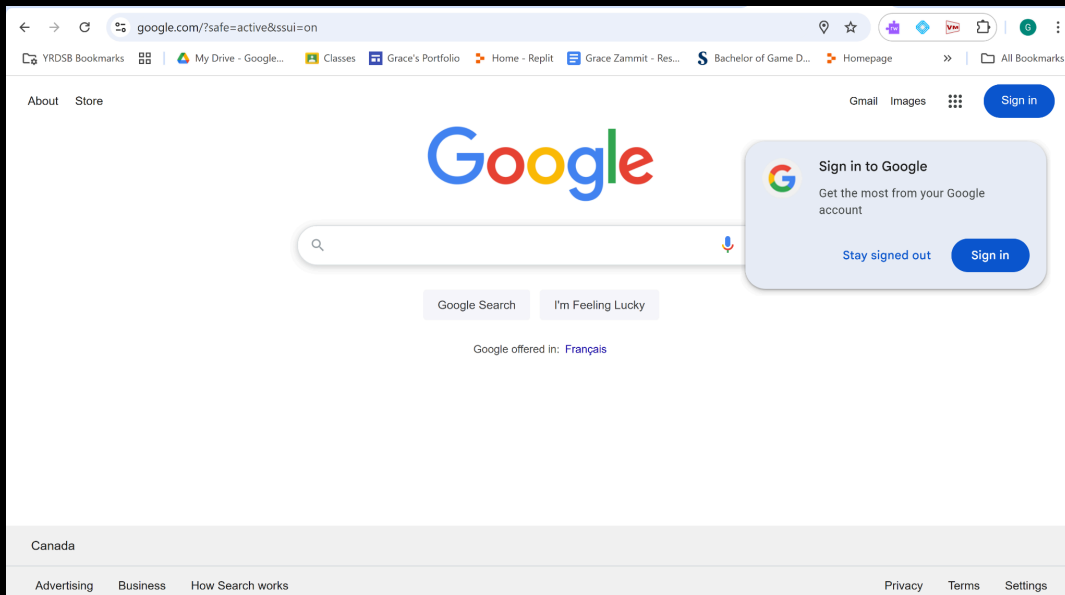
Go to [Online nslookup — Find DNS records](https://www.online-nlookup.com/)

Type in www.google.com and click the button.

What is the IP address of the web server hosting google's homepage?

74.125.130.106

Open your browser and type the IP address in the address bar and hit Enter. What happens and why? Embed a screenshot here:



Classless Inter-Domain Routing (CIDR)

A system to allow for the efficient assignment of network addresses.

Let's look at the following address using CIDR:

192.168.2.0/24

The 24 means that the first 24 most significant bits are used for the address of the network and the remaining are used for the hosts:

192.168.2.0=11000000.10101000.00000010.00000000

11000000.10101000.00000010.00000000

11111111. 11111111. 11111111 .00000000 =/24 multiply to get the network address

11000000.10101000.00000010.00000000=192.168.0.0

Note that because we have the last 8 bits reserved for Hosts that means we can have 2^8 hosts or 256. However as mentioned much earlier we reserve 0 for the network portion of the address and 255 for broadcasts. That really leaves us with 254 possible hosts on this network.

Question:

Express the following in CIDR notation:

IP address: 192.168.100.0

Subnet Mask: 255.255.0.0

192.168.100.0/16

What is the size of the host portion of the following IP address expressed in CIDR:

192.168.10.0/24?

8 bits

If you needed a network with 512 addresses what would the CIDR notation be for your network?

192.168.0.0/23

We can borrow from the most significant bits of the host portion of an address to create subnetworks i.e. networks separate from but connected to the main network address.

For example let's say we have a network address of 192.168.0.1/23. This means that 9 bits are reserved for all hosts on this network:

192.168.0.1/23=11000000.10101000.00000000.00000001

11000000. 10101000.00000000.00000001

11111111 .11111111. 11111110 .00000000 x

11000000.10101000.00000000.00000000

192 168 0 0

The network address is 192.168.0.0.

The first host on this network can be:

11000000. 10101000.00000000.00000001=192.168.0.1

The next one is:

11000000. 10101000.00000000.00000010=192.168.0.2

Then:

11000000. 10101000.00000000.00000011=192.168.0.3

Then:

11000000. 10101000.00000000.00000100=192.168.0.4

All the way up to:

11000000. 10101000.00000000.1.11111111=192.168.1.255

If we wanted to create subnets/subnetworks then we borrow bits from the most significant set of bits in the host. For example let say we borrow the 2 most significant host bits:

11000000.10101000.00000000.0.00000000

This means we can have 2^2 subnets and 2^7 hosts on each subnet. The subnet addresses would be as follows:

11000000.10101000.00000000.0.00000000=192.168.0.0

11000000.10101000.00000000.0.10000000=192.168.0.128

11000000.10101000.00000000.1.00000000=192.168.1.0

11000000.10101000.00000000.1.10000000=192.168.1.128

The first host on the first subnet would be:

11000000.10101000.00000000.0.00000001=192.168.0.1

The second:

11000000.10101000.00000000.0.00000010=192.168.0.2

And so on until the last one:

11000000.10101000.00000000.0.11111111=192.168.0.127 (broadcast)

The first host on the second subnet would be:

11000000.10101000.00000000.0.10000001=192.168.0.129

The second:

11000000.10101000.00000000.0.10000010=192.168.0.130

And so until the last one at:

11000000.10101000.00000000.0.11111111=192.168.0.255 (broadcast)

The first host on the third subnet would be:

11000000.10101000.00000000.1.00000001=192.168.1.1

The second:

11000000.10101000.00000000.1.00000010=192.168.1.2

And so until the last one at:

11000000.10101000.00000000.1.01111111=192.168.1.127(broadcast)

The first host on the last subnet would be:

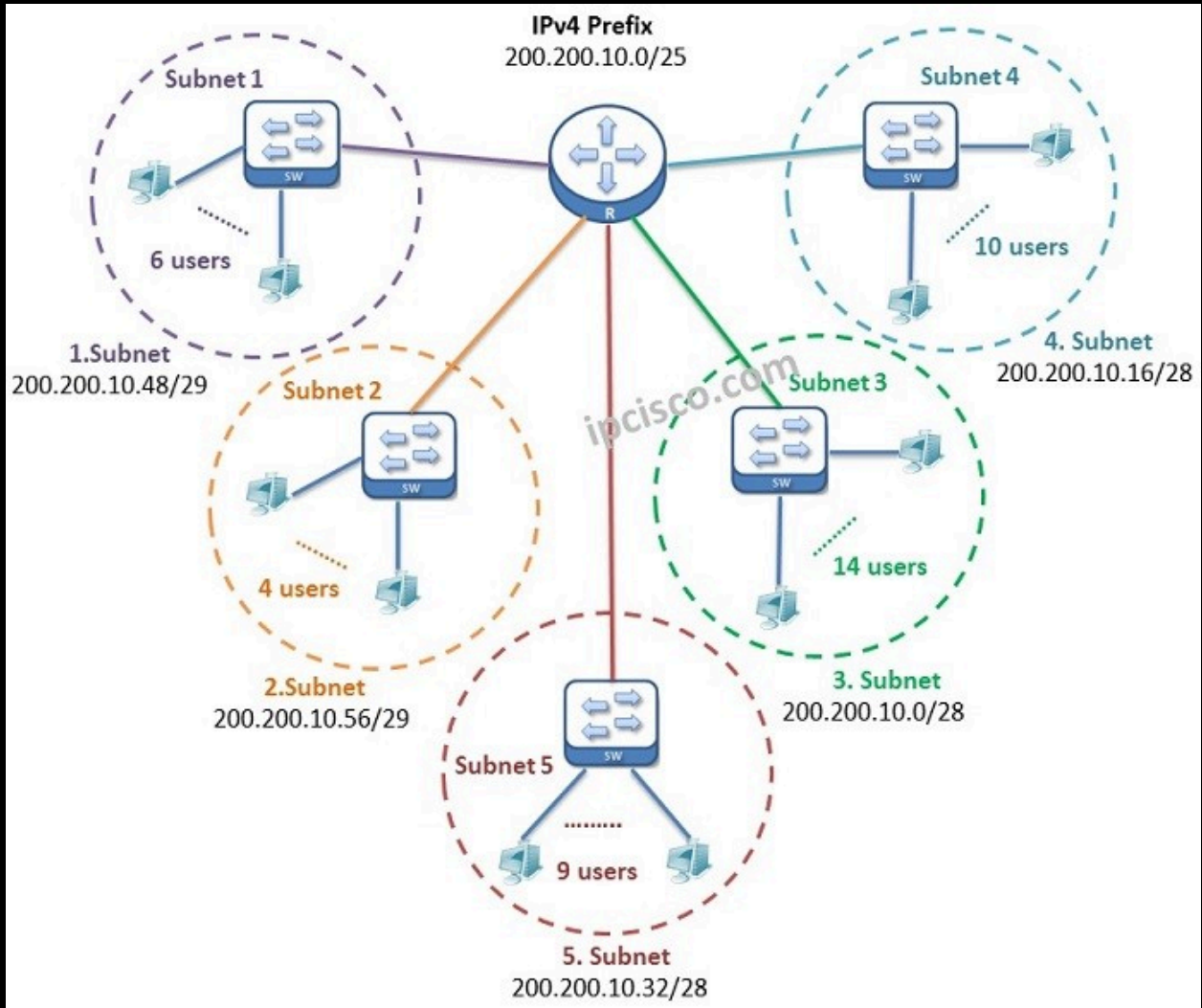
11000000.10101000.00000000.1.10000001=192.168.1.1

The second:

11000000.10101000.00000000.1.10000010=192.168.1.2

And so until the last one at:

11000000.10101000.00000000.1.11111111=192.168.1.255(broadcast)



Exercise:

Open the network

https://drive.google.com/file/d/1uO_vipJpcl36dSmElgP_qE2mxCxzj0Go/view?usp=sharing

Try a data packet send simulation from PC1 to PC0. What happens?

The PC send the packet to the switch which send it to all PCs however the other PCs all get an X and reject them, other than PC0

Try a data packet send simulation from PC0 to PC1. What happens?

The PC send the packet to the switch which send it to all PCs however the other PCs all get an X and reject them, other than PC1

Try a data packet send simulation from PC4 to PC5. What happens?

The packet is only sent to PC 5

Try a data packet send simulation from PC5 to PC4. What happens?

The packet is only sent to PC 4

Try a data packet send simulation from PC0 to PC4. What happens? How is the path the data packet sends from PC0 to PC4 different from the path it takes to get to PC1? Why is it different?

The switch sends out a broadcast to all the computers to collect the MAC addresses to fill out its information table.

Now try and send a data packet from PC4 or PC5 to each other and then to any of the other 4 computers. What's the difference and why?

The packet has to go through the router before it talks to any of the other computers

Tracing the Route

Open the following network:

https://drive.google.com/file/d/1kEoxcJeSWwNVIYv-Ft3sAM_Mk6T5Tds3/view?usp=sharing

Try pinging PC6 and PC7 from either PC4 or PC5. What happens?

PC6 replies to PC4

What is the IP address of Router0?

192.168.0.1

What is the IP address of Router1?

192.168.2.1

What is the IP address of PC6?

192.168.2.2

From the windows console of PC4 write the following command:

tracert 192.168.2.2

Embed a screenshot of your results here and explain it:



Tracert will trace the path that the IP takes to get to the destination

Try performing a tracert from PC7 to PC5. Explain the results.

The trace goes first to the router1, then router0, then PC5.

To perform a trace from a Cisco router to a device use the **traceroute** command in place of **tracert**. Select Router0. Enter the CLI tab. Enter the **exit** command and hit enter until your prompt looks like **Router>**. Enter the command **traceroute 192.168.2.2**. Embed the results as a screenshot below and explain the difference between it and the results you got when you performed the command from PC4:



This command shows the path data takes to get to the router

Now try a trace from any PC to 127.0.0.1 (loopback address). What happens and why?

The trace only shows the loopback address as it is only looping the current computer path (which is none since it's just one computer)

Routing

Open the network

<https://drive.google.com/file/d/1AEIDF4rdCuvyqPYt0CDmLuDbUdHMewNH/view?usp=sharing>

Try pinging PC1 from PC0 and then PC0 from PC1. Try pinging PC3 from PC2 and PC2 from PC3. What happens? Why?

PC1 replies, and so does PC1. Same with the others. This is because they are all connected on the same network.

Now try pinging PC2 from PC0 and PC0 from PC2. What happens? Why?

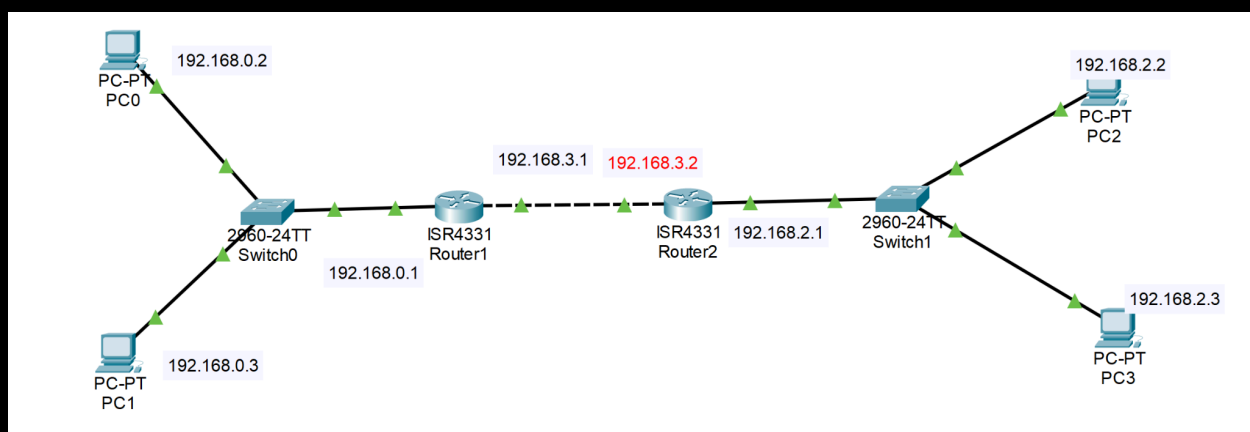
There is no reply, as the two LAN networks cannot communicate.

In order for one network to communicate with another network we have to tell them how. Do the following:

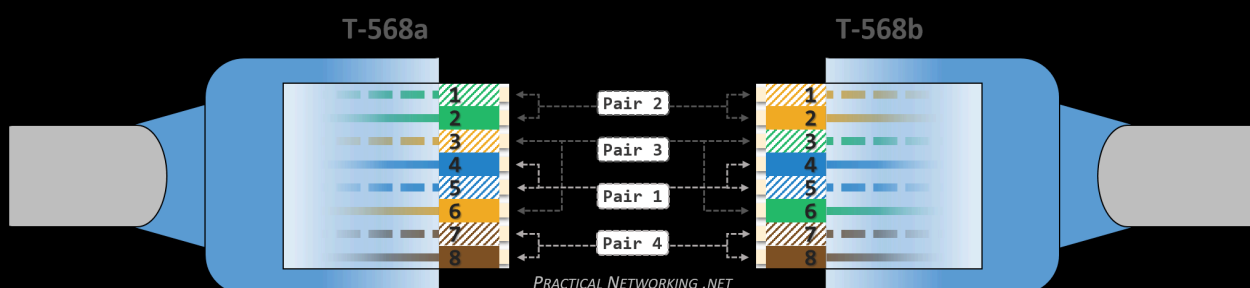
1. Select Router 1, go to Config and then select the Static bar from the ROUTING section. In the network box we add the network IP address we want this router to be able to communicate with i.e. 192.168.2.0 255.255.255.0. To get to this network our router has to send its messages to the router connected to that network. The address of the next router is 192.168.3.2. Click the Add button.
2. Select Router 2, go to Config and then select the Static bar from the ROUTING section. In the network box we add the network IP address we want this router to be able to communicate with i.e. 192.168.0.0 255.255.255.0. To get to this network our router has to send its messages to the router connected to that network. The address of the next router is 192.168.3.1. Click the Add button.
3. Enter each PC and set their Gateway address.

Now try and ping PC2 from PC0. PC2 from PC1. PC1 from PC2 and PC1 from PC3.

Note that in order for the routes to be successful all connecting interfaces must be part of the same network address:



Note that the two interfaces connecting the routers must also be part of their own network (192.168.3.0). Also note the dashed wire between routers. This normally represents a **crossover** cable. A **crossover** cable is normally used to **connect similar devices** i.e. router to router. A **crossover** cable uses different wiring configurations on both ends. A normal **straight through** cable has similar configurations on both ends and is used to **connect dissimilar devices** i.e. router to switch. The solid lines represent straight through cables.



Exercise:

Open the network

<https://drive.google.com/file/d/1yeC3X23GigJuZiVtMEX-owkZZ1wH5N77/view?usp=sharing>

Try pinging PC2 and PC3 from PC0 and PC1. Now try pinging PC0 and PC1 from PC2 and PC3. Try using the simulation option to send data packets from one side of the network to the other. The static routing should have been set up correctly to allow data packets to travel from the left and right networks to each other. Make modifications to the network so that the two top networks can communicate with the bottom one. Add labels next to each interface identifying its IP address.

Dynamic Routing

This is sometimes referred to as RIP (Routing Information Protocol) and is used to get routers to learn their own routes instead of you adding them in manually. The downside to using RIP is that networks can take time to do this and it can slow down the network.

The way this works is to simply inform the router what networks they are connected to. All routers in the network should be set up with RIP once you decide to use this method.

Exercise:

Open the network:

https://drive.google.com/file/d/18BL1nOS8DI_Cn0188QwbHXdkB5vJ3aqi/view?usp=sharing

Look at the routing information for Router0. Note that the static routing tables have been removed. Inspect the RIP and notice the two networks added on either side of the router. Set up the RIP for the other two routers and then test connectivity between all PCs.

Complete the attached worksheets:

<https://drive.google.com/file/d/1gkF1ZnGIAMOHJhDpLcK8BSeLsNe7WdTc/view?usp=sharing>

https://docs.google.com/document/d/11oZH2qxEpm4mvjlkI98bD5LmdkYq1_cnSz_YAFSdaUQ/edit?usp=sharing~