Creating and Hardening a Small Business Network

Created by Logan Reed

Introduction

This lab will walk you through how to configure and secure a small business network through Cisco Packet Tracer and discuss the reasoning behind each action taken, as well as discuss options available outside of Cisco Packet Tracer's abilities. Cisco Packet Tracer is an application designed to simulate network building without needing physical hardware besides the device you downloaded the application on. Within Cisco Packet Tracer you will create and secure an ASA, DHCP server, Web server, WAP, multiple switches, and endpoint user computers. Before you get started here are a few terms you should be aware of if you aren't already:

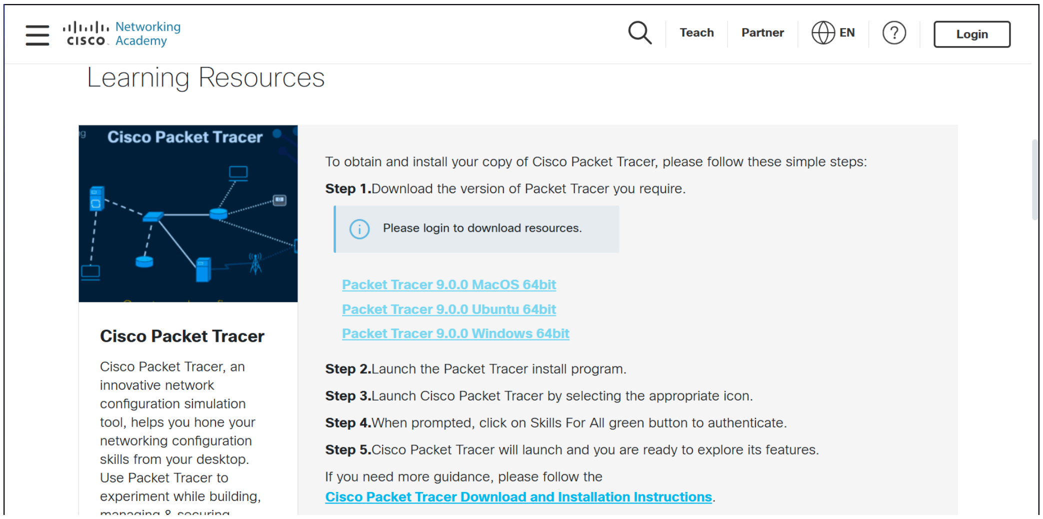
- **IP Address:** A unique numerical label for devices on a network to help with communication and connectivity between them. You can think of them as home addresses but for computers.
- **Subnet:** A subnet is a network inside a network. Subnets are used to separate segments of the full network. You can think of them as cities for computers.
- **VLAN:** VLAN stands for Virtual Local Area Network and is similar to a subnet. VLANs separate a physical network into multiple virtual networks. Unlike a subnet, each VLAN acts as its own network.
- **ASA:** ASA stands for Adaptive Security Appliance which is specific to Cisco. It combines multiple networking and security devices into one. We will be using it for a router and a firewall.
- **DHCP and WEB Server:** A DHCP server automatically provides IP addresses to devices so that you don't need to manually enter them. A WEB server holds the company's website.

- **WAP:** WAP stands for Wireless Access Point and is how wireless devices like phones and laptops can connect to a network through Wi-Fi.
- **Switch:** A switch is a device that acts as a central connection point to connect many different wired connections together.

To start off you can download Cisco Packet Tracer from this link:

https://www.netacad.com/resources/lab-downloads?courseLang=en-US

You will need to create an account to download resources from their site and then Cisco Packet Tracer will require you to sign into that account when you open it.



Learning Resources

Cisco Packet Tracer

Cisco Packet Tracer, an innovative network configuration simulation tool, helps you hone your networking configuration skills from your desktop. Use Packet Tracer to experiment while building, managing & securing

To obtain and install your copy of Cisco Packet Tracer, please follow these simple steps:

Step 1. Download the version of Packet Tracer you require.

Please login to download resources.

Packet Tracer 9.0.0 MacOS 64bit
Packet Tracer 9.0.0 Ubuntu 64bit
Packet Tracer 9.0.0 Windows 64bit

Step 2. Launch the Packet Tracer install program.

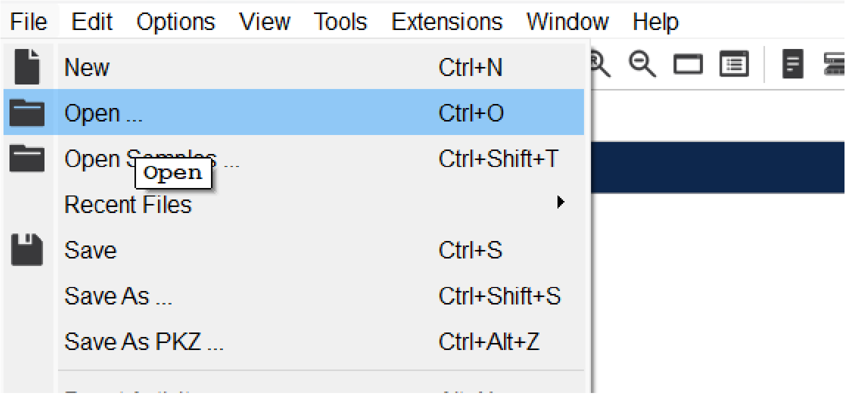
Step 3. Launch Cisco Packet Tracer by selecting the appropriate icon.

Step 4. When prompted, click on Skills For All green button to authenticate.

Step 5. Cisco Packet Tracer will launch and you are ready to explore its features.

If you need more guidance, please follow the Cisco Packet Tracer Download and Installation Instructions.

Next you need to download and open the "Starting Network" file provided in the Github through Cisco Packet Tracer by clicking on "file" and then "open" on the top left of the page.

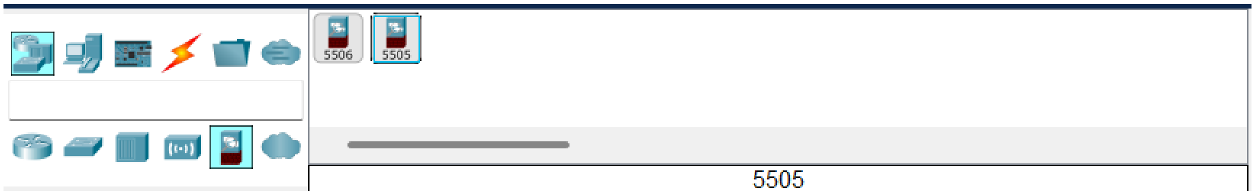


This starting network uses a pre configured router to serve as the "internet" to connect your network to and protect from.

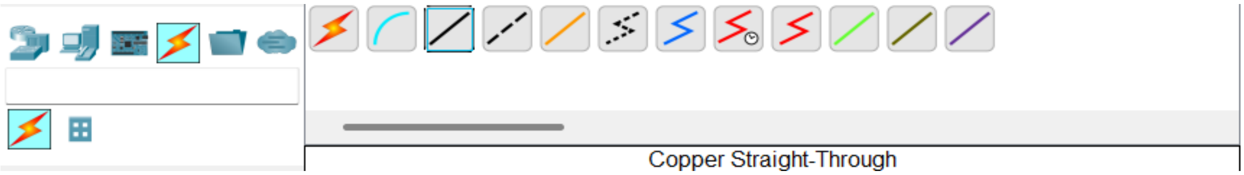
Warning: You should complete each section in this lab completely and save in between each one before closing the program since if you don't you could possibly lose massive amounts of progress. To save your network click on "File" on the upper left and then click on "Save". You will also be asked if you want to save your work upon exiting the program.

Placing and Connecting a ASA

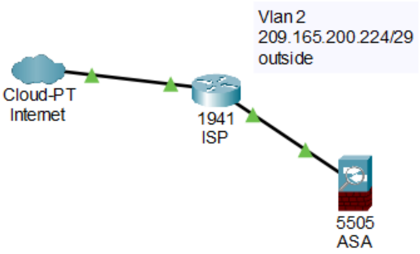
The first thing to configure is the ASA, which will serve as the router and firewall of our network. It will filter outside traffic and provide connectivity between the internet and your inside network. This device is located on the bottom left in Network Devices >> Security >> 5505:



Just click on it, then click on a spot near the router labeled "ISP", which acts as your internet service provider's connection. Click on the name "ASA0" below the device you just placed and rename it to just ASA. You should then grab a Copper Straight-Through wire on the bottom left in Connections >> Copper Straight-Through:



Click on the ASA you put down with the wire connection and a list of connection points should appear. Click on Ethernet0/0 then click on the ISP router and connect the wire to GigabitEthernet0/1. This should connect a wire between the two devices:



Configuring VLANs

Now that you have connected the ASA to the ISP router you should make different VLANs for each network the ASA will be connecting. You'll notice there is a note about VLAN 2 for the outside network. This makes it easier to keep track of what type of network it is compared to yours. Other than "outside" there will be "dmz" or "demilitarized zone" and "inside" as types of networks the ASA will be dealing with. Click on the ASA device and then click on the "CLI" tab at the top of the window that pops up. CLI stands for Command Line Interface and normally you would need another computer to modify the ASA like this, but the simulation lets us enter it without one. Here you can enter commands to configure the ASA.

Before we get started with the VLAN we need to rename the ASA terminal, define the company website "company.com", and create a "secret" which is an encrypted password stored on the ASA that the terminal asks for any time you enter the "enable mode" which allows you to view the current configuration and enter the "configuration mode" which is where you make advanced changes. Upon opening the CLI enter the following commands (Green text are comments made about what the command is doing and not part of the command. Blue test will be the command itself):

```
ciscoasa> enable
        Entering enable mode
Password:
        Since there is no password set yet just press "enter"
ciscoasa# conf t
        Entering configuration mode
ciscoasa(config)# hostname MainASA
        Renaming the terminal
MainASA(config)# enable password Cisco123
        ASA encrypts any password and the "enable secret" command does not exist like
        in the other devices we will be configuring later
MainASA(config)# domain-name company.com
        This defines the company website we will be using and creating later
```

Now that the initial configuration of the ASA is done we can begin with VLAN 2, which is for the “outside” network. From the configuration terminal we will enter the VLAN’s, rename it to “outside”, set it’s security level, and enter the IP address of the device it is connecting to:

```
MainASA(config)# int VLAN 2
```

Entering VLAN interface

```
MainASA(config-if)# nameif outside
```

Naming the VLAN

```
MainASA(config-if)# ip add 209.165.200.226 255.255.255.248
```

IP address of the port connecting to the ISP router we connected to and it’s subnet mask

```
MainASA(config-if)# security-level 0
```

Setting the security level which is the level of trust we have of this network, 0 being none and 100 be complete trust

We also need to establish a “static route” which establishes a specific route that any traffic heading out of the network that the destination is unknown to our ASA will go through:

```
MainASA(config-if)# route outside 0.0.0.0 0.0.0.0 209.165.200.225
```

This command routes any unknown traffic (0.0.0.0) to the “outside” network (209.165.200.225)

Next we will configure VLAN 1 which goes to our “inside” network which we trust much more than the “outside” network. We will do the same steps as the last VLAN with slight changes and without a static route:

```
MainASA(config)# int VLAN 1
MainASA(config-if)# nameif inside
MainASA(config-if)# ip add 192.168.1.1 255.255.255.0
MainASA(config-if)# security-level 100
MainASA(config-if)# exit
```

Exits back out of the interface to configuration mode

Finally we can configure VLAN 3 which goes to the “dmz” network which is where our company WEB server is located. This server requires some amount of trust since it is ours but it is still not in our internal network. This VLAN will require switching a port from VLAN 2 to VLAN 3 because the first two VLANs were automatically created with assigned ports:

```
MainASA(config)# int VLAN 3
MainASA(config-if)# ip add 192.168.2.1 255.255.255.0
MainASA(config-if)# no forward interface vlan 1
        Prevents VLAN 1 from initiating connections with VLAN 3 but still allows
        network traffic
MainASA(config-if)# nameif dmz
        Automatically makes security level 0
MainASA(config-if)# security-level 50
MainASA(config-if)# int e0/2
        Enter ethernet port 0/2’s interface
MainASA(config-if)# switchport access vlan 3
        Switch port’s access to VLAN 3
MainASA(config-if)# exit
```

Now that our VLANs are set up we can create specific rules for what kind of traffic can be sent to and from the higher security VLANs in the next section. Before we do that though we should save our configurations. With cisco devices there are two different types of configurations: “running configuration” and “starting configuration”. Running configuration is the current configuration of the device and starting configuration is the configuration for whenever the device is powered on. The running configuration gets deleted when the device is turned off and restarts with the starting configuration. In order to prevent our work from getting deleted we need to copy the running configuration to the starting configuration like this:

```
MainASA(config)# exit
MainASA# copy run start
        Press enter after entering this command to finish the save
```

Filtering Network Traffic

The ASA can act as a firewall as well as a router. In this section we will be configuring the ACLs (Access Control Lists) of the VLANs we configured in the last section, which firewalls use to filter out unauthorized network traffic. Before we can filter traffic though we need to set up Network Address Translation (NAT) which translates private IP addresses into a public IP address. We will set this up for traffic between the inside and outside networks as well as the traffic between the dmz and outside networks:

```
MainASA> enable
Password:
        Enter "Cisco123" which is our password from the previous section
MainASA# conf t
MainASA(config)# object network inside-net
MainASA(config-network-object)# subnet 192.168.1.0 255.255.255.0
        Enables NAT for the inside network
MainASA(config-network-object)# nat (inside,outside) dynamic interface
        Maps NAT between inside and outside networks
MainASA(config-network-object)# end Exits all the way to configure mode
MainASA# conf t
MainASA(config)# object network dmz-network
MainASA(config-network-object)# host 192.168.2.3
MainASA(config-network-object)# nat (dmz,outside) static 209.165.200.227
        Maps NAT between dmz and outside networks
MainASA(config-network-object)# end
```

The reason we don’t do this between the dmz and inside networks is because they both have private IP addresses that can find their way to each other. NAT would just needlessly complicate the connection between the two.

Now we can continue and create an ACL between the outside network and dmz network to only allow ICMP and TCP traffic. ICMP or Internet Control Message Protocol sends pings which we will use for testing to see if addresses can be reached and TCP or Transmission Control Protocol actually sends data and establishes connection with places in the outside network. Since the connection between a WEB server (dmz network) and the internet (outside internet) doesn't commonly require anything outside of this we would only want to allow these two protocols from getting through and nothing else. This can help prevent some DDoS (Distributed Denial of Service) attacks by blocking the malicious traffic. By entering the following commands we create and apply the ACL to the outside network:

```
MainASA# conf t
MainASA(config)# access-list OUTSIDE-DMZ permit icmp any host 192.168.2.3
        Allowing ICMP in ACL
MainASA(config)# access-list OUTSIDE-DMZ permit tcp any host 192.168.2.3 eq 80
        Allowing TCP in ACL
MainASA(config)# access-group OUTSIDE-DMZ in interface outside
        Applying the ACL list to the outside network port
```

Now normally the ASA firewall does not inspect and filter ICMP packets like we want it to so we will have to look at the default inspection policy (the packets the ASA inspects by default) and add ICMP to it. We can do this by creating a new class to copy the default inspection policy's configuration and then create a new policy to add the copy and ICMP inspection to and apply. This is complicated in text format but the commands actually do this step by step. First we create and copy the default inspection list to a class:

```
MainASA(config)# class-map inspection_default
        Creating new class of traffic inspection named "inspection_default"
MainASA(config-cmap)# match default-inspection-traffic
        Copying default inspection class to our new class
MainASA(config-cmap)# exit
```

Next we create and add the previously made class to a inspection policy:

```
MainASA(config)# policy-map global_policy
        Creating a new inspection policy called “global_policy”
MainASA(config-pmap)# class inspection_default
        Adding class into inspection policy
MainASA(config-pmap-c)# inspect icmp
        Adding inspection of icmp into inspection policy
MainASA(config-pmap-c)# exit
```

Then we apply the new inspection policy as the one we use:

```
MainASA(config)# service-policy global_policy global
        Making new policy the new inspection policy
```

ICMP packets will now be inspected by the ASA firewall along with TCP which was a part of the default inspection policy. We are all done configuring the ASA to work as both a router and a firewall, but before we move onto the next section we should turn off any unused ports:

```
MainASA(config)# int e0/3
MainASA(config-if)# shutdown
        Enters and turns off port Ethernet0/3
MainASA(config-if)# int e0/4
MainASA(config-if)# shutdown
MainASA(config-if)# int e0/5
MainASA(config-if)# shutdown
MainASA(config-if)# int e0/6
MainASA(config-if)# shutdown
MainASA(config-if)# int e0/7
MainASA(config-if)# shutdown
MainASA(config-if)# exit
MainASA(config)# no dhcpd enable inside
        Disable the ASA’s built in DHCP server to prevent collisions later
```

Turning off unused ports is a good way of preventing malicious persons from plugging into the router and accessing the network unauthorized.

The ASA is the most complex with configurations and everything else after this will be easier. In the next section we will be setting up the WEB server holding our company website in the dmz network that we have been talking about and the IP address “192.168.2.3” that has been showing up will be the IP address of the WEB server. After that we will start making our internal network with switches, a DHCP server, a WAP, and computers. Before we move onto the next section let's save our configuration with these commands:

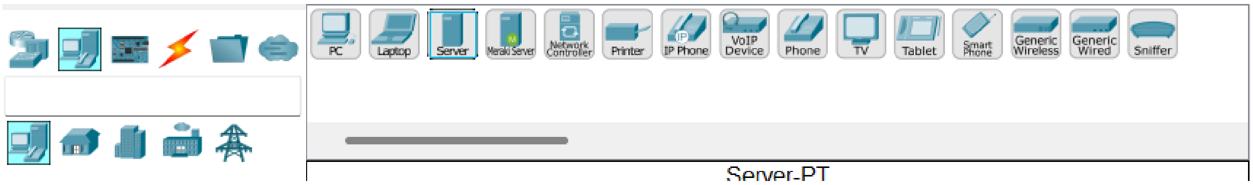
```
MainASA(config)# exit
MainASA# copy run start
```

Press enter after entering this command to finish the save

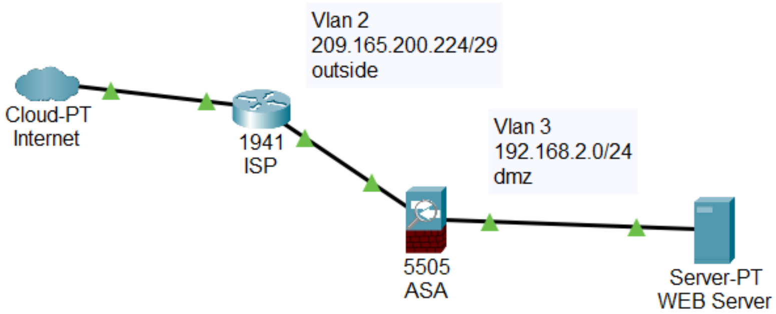
We should also save our network by clicking “File” in the top left of the home window and then clicking “Save”.

Connecting and Configuring the WEB Server

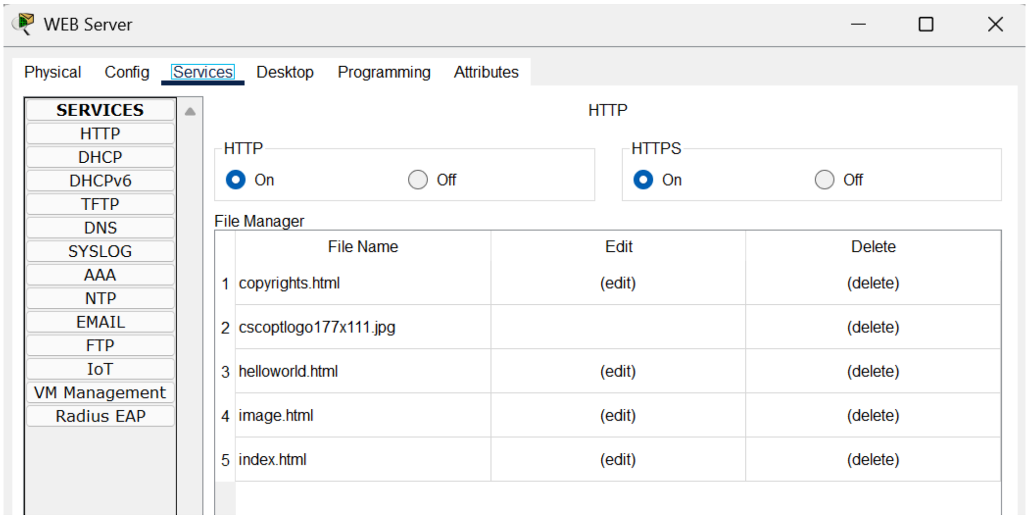
In this section we will be connecting the WEB server that holds the company’s website. It is a very simple configuration. On top of that we will disable any unused services that are also on the server to help secure it. There is no CLI with this device so we will have to use the Cisco UI. First let's grab the server from End Devices >> Server-PT at the bottom left of the window.



Place the server somewhere to the right of the ASA and connect it using the Copper Straight-Through wire using the Ethernet0/2 port on the ASA and the FastEthernet0/0 port on the server. Rename the server from “Server0” to “WEB Server” and place a note between the two devices to remind us what network it is. You can place a note by pressing “n” on your keyboard and clicking on the place you want it. The note should contain the vlan (Vlan 3) , the network address (192.168.2.0/24) and the type of network (dmz). Your network should look something like this:



Now clicking on the server will bring up a UI that we can use to configure it. Clicking on the tab labeled “Services” brings up the list of available services. We should disable all services except “HTTP” and “HTTPS” as they are not used on this server.



HTTP

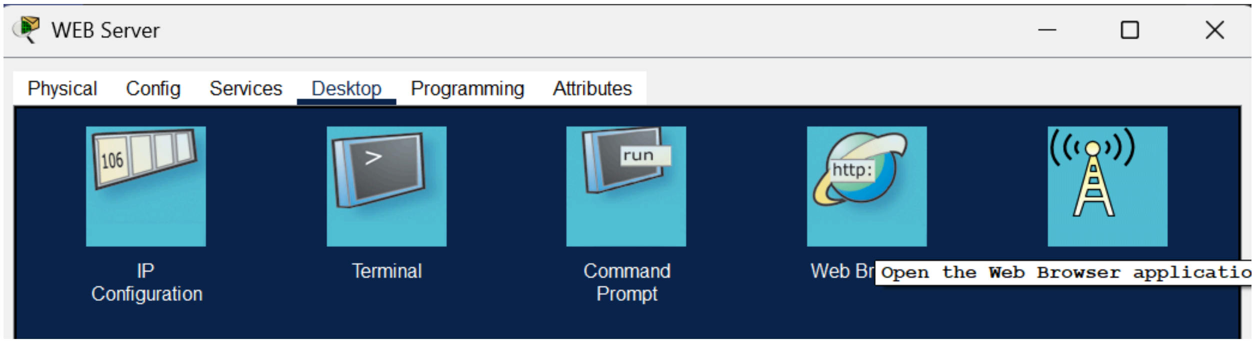
HTTP ● On ○ Off

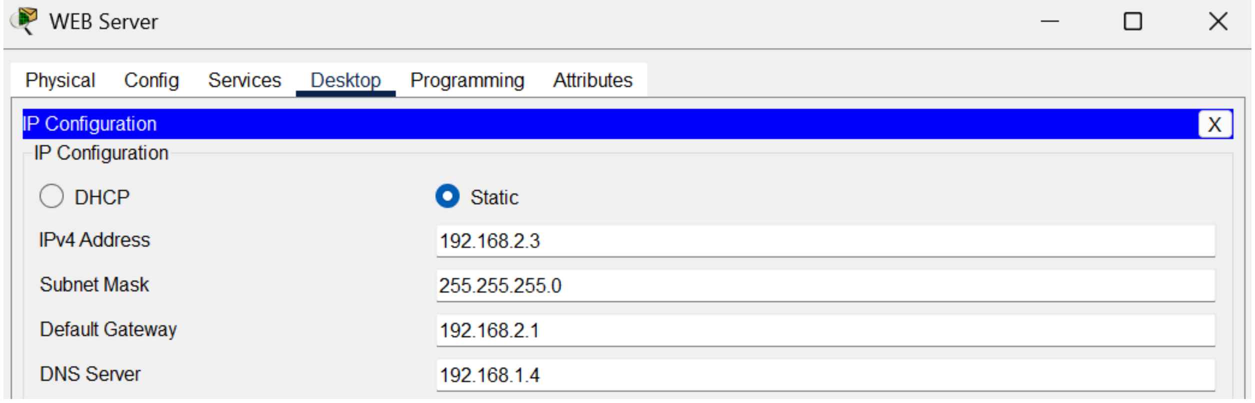
HTTPS ● On ○ Off

File Manager

	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo177x111.jpg		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)

Now we need to configure the IP address in the WEB server by clicking on the “Desktop” tab and then click on the “IP Configuration” box to start configuring the IP address, default gateway, and subnet.





IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.2.3

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1

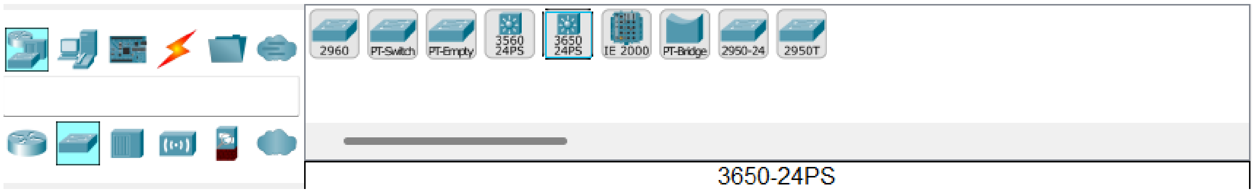
DNS Server: 192.168.1.4

If a computer were to put the IP address into the url bar of a web browser it would bring up the contents of the WEB server, but if we use a DNS server, which we will do in the next section, then just putting “company.com” into the url bar will also bring up the contents of the WEB server.

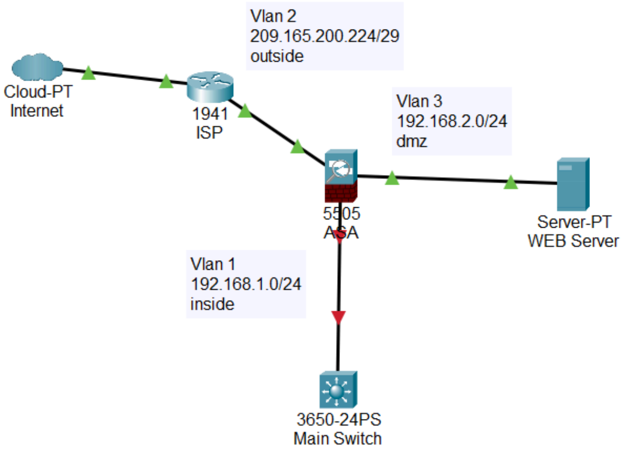
Since the WEB server doesn’t have a CLI it saves automatically and we don’t have to do any extra commands. We should still save the network though before we go onto the next section by clicking “File” and “Save” at the top left.

Connecting and Configuring the Main Switch and DHCP Server

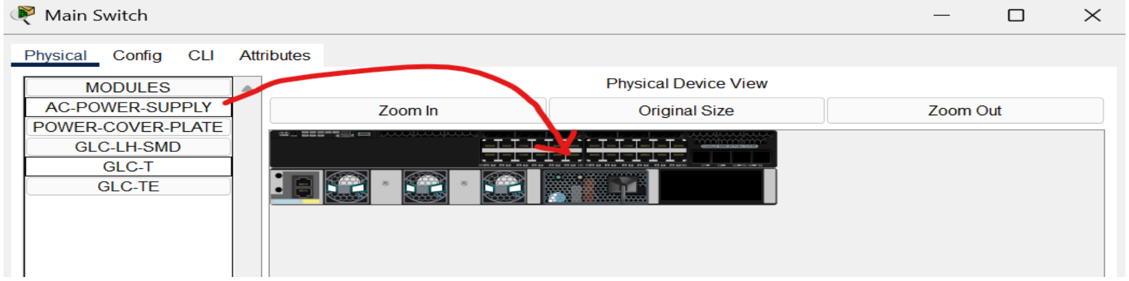
Before we can configure the DHCP server we need to connect a switch that will connect all our major network devices in the internal network that includes a WAP, several switches, ASA, and the DHCP server. The switch we will use is found in Network Devices >> Switches >> 3650-24PS.



Place it below the ASA, rename it to "Main Switch", and use a Copper Straight-Through wire to connect it from the Ethernet0/1 port on the ASA to the GigabitEthernet1/0/1 port on the switch. You may also want to place another note to remind yourself this is the inside network by noting the VLAN (Vlan 1), network address (192.168.1.0/24), and the type (inside). Your network should look similar to this:



You'll notice that the triangles are red instead of green which means there is no connection between these two devices at all. This is because the switch does not come with a pre-installed power supply for this model. By clicking onto the switch and bringing up it's window we should already be on the "Physical" tab where is we click and drag the module "AC-POWER-SUPPLY" to an empty slot on the model of a switch to the right of the module list we can provide this power:

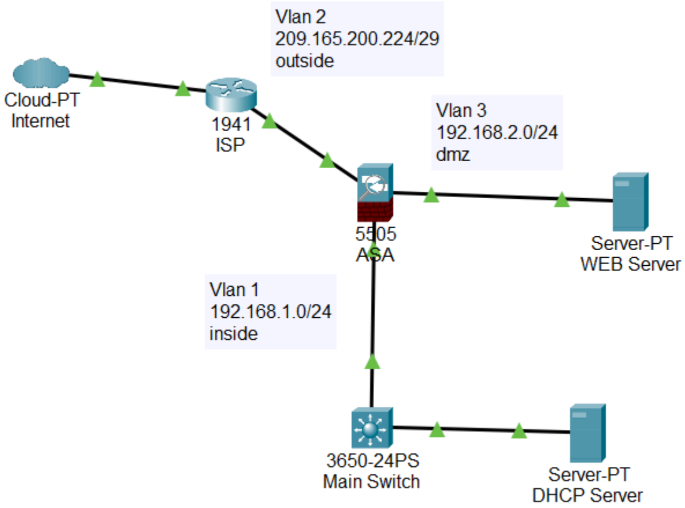


The switch should automatically turn on and connect to the ASA allowing us to continue with our configurations.

While we are messing with the Main Switch we should turn off any ports we will not be using and put an encrypted password on the terminal by going to the "CLI" tab in the Main Switch's window and typing the following commands (The switch will ask if you want to enter the initial configuration dialog which we reply to with "no"):

```
Switch> enable
Switch# conf t
Switch(config)# hostname MainSwitch
MainSwitch(config)# enable secret Cisco123
MainSwitch(config)# int range Gig1/0/12-24
        Entering a range of similar port interfaces
MainSwitch(config-if-range)# shutdown
        Shutting down every port we entered
MainSwitch(config-if-range)# int range Gig1/1/1-4
MainSwitch(config-if-range)# shutdown
MainSwitch(config-if-range)# end
        Going back to enable mode
MainSwitch# copy run start
```

Now that we have the Main Switch connected we can connect the DHCP server to the switch so it can provide any devices connecting to the network with an automatically assigned IP address so we don't have to enter one into every device ourselves. Inside the DHCP server we will configure a DNS server which will allow us to use the web address of "company.com" for our WEB server. Similar to the WEB server we need to grab the device located at End Devices >> Server-PT and place it somewhere to the right of our new Main Switch. We should rename it "DHCP Server" and using a Copper Straight-Through wire connect the GigabitEthernet1/0/2 port on the Main Switch to the Ethernet0 port on the server so that your new network should look like this:

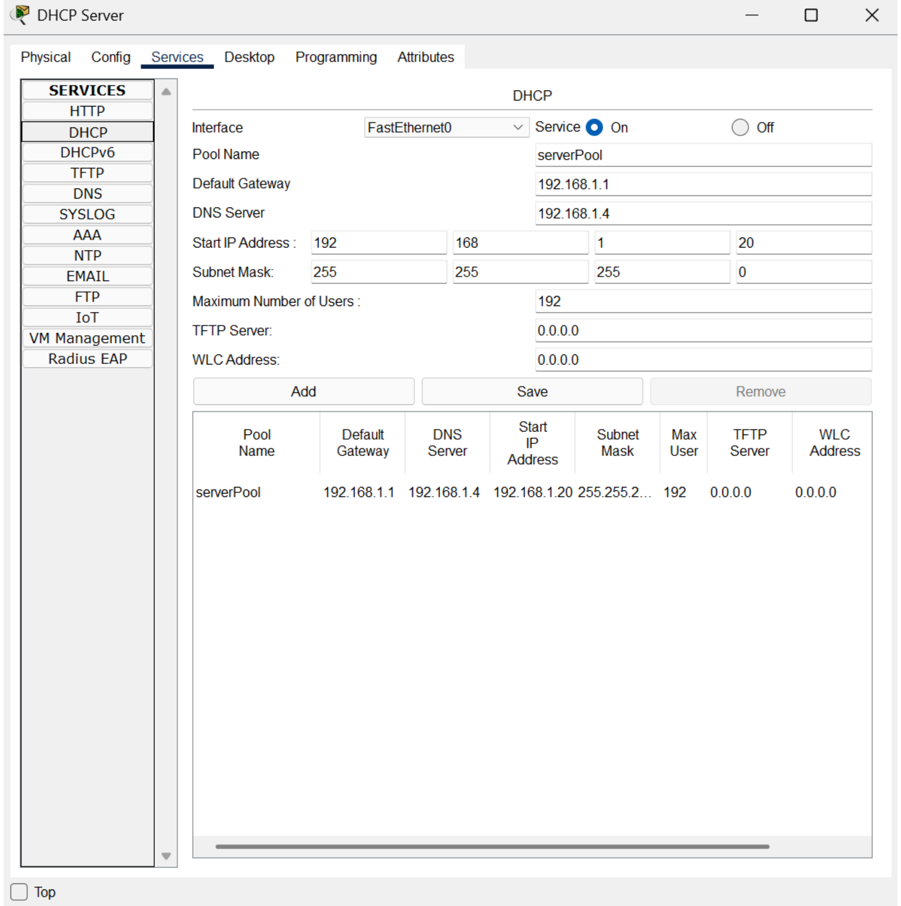


Similar to the WEB server we should start with disabling all services and enabling the "DHCP" (not DHCPv6) and "DNS" services since these are the only two we will be using and configuring. To configure the DHCP service we need to modify the existing IP address pool by clicking on the "serverPool" pool in the pool list and make the following changes:

1. Default Gateway: 192.168.1.1
2. DNS Server: 192.168.1.4
3. Starting Address: 192.168.1.20
4. Subnet Mask: 255.255.255.0
5. Max Number of Users: 192

Then click the "save" button above the list of pools in the center of the window. The default gateway is the IP address of the port we assigned to VLAN 1 for our internal network on the

ASA. The DNS server address is the same IP address as this device since we will also be configuring the DNS server here. The starting address is the first address that will be automatically assigned to a device using DHCP and the max users is how many more IP addresses can be assigned. Now anytime a new device is set up that uses DHCP to get it's IP address it will be sent an available IP address in the range of 192.168.1.20 to 192.168.1.212. The DHCP service should look like this now:

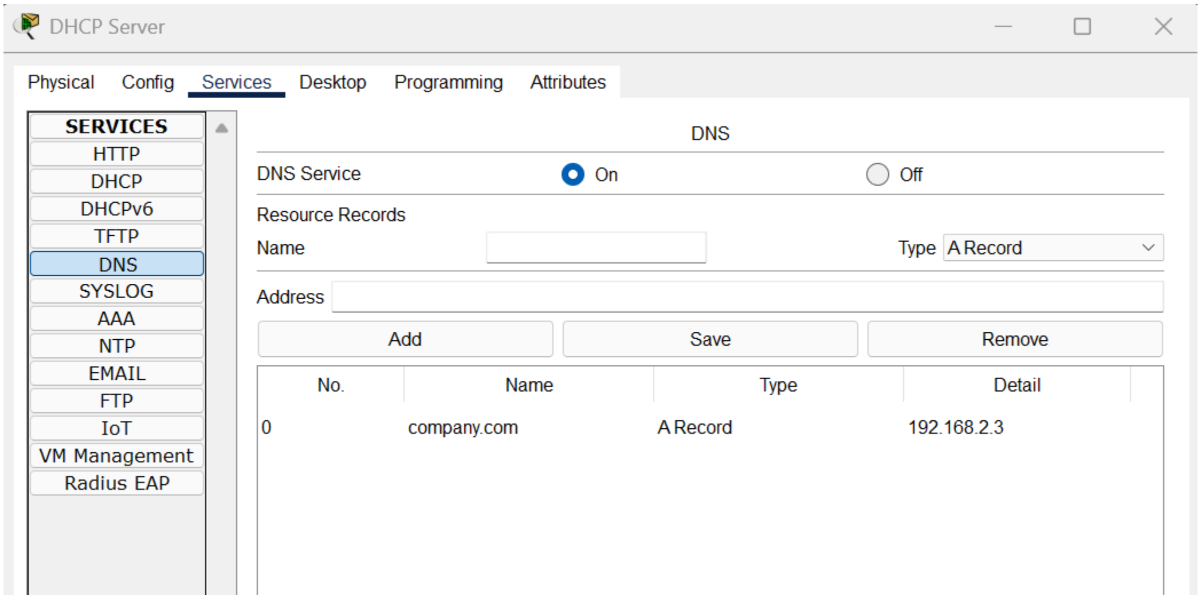


DHCP

Interface	FastEthernet0	Service ● On ○ Off		
Pool Name	serverPool			
Default Gateway	192.168.1.1			
DNS Server	192.168.1.4			
Start IP Address :	192	168	1	20
Subnet Mask:	255	255	255	0
Maximum Number of Users :	192			
TFTP Server:	0.0.0.0			
WLC Address:	0.0.0.0			

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168.1.1	192.168.1.4	192.168.1.20	255.255.2...	192	0.0.0.0	0.0.0.0

To configure our DNS server we need to click on the DNS service and type in the name (company.com) of the website, IP address of the WEB server (192.168.2.3) and then click the “Add” button. This should add “company.com” to the list below confirming that we have assigned the website name to the WEB server containing our company website so it looks like this:



DNS

DNS Service ● On ○ Off

Resource Records

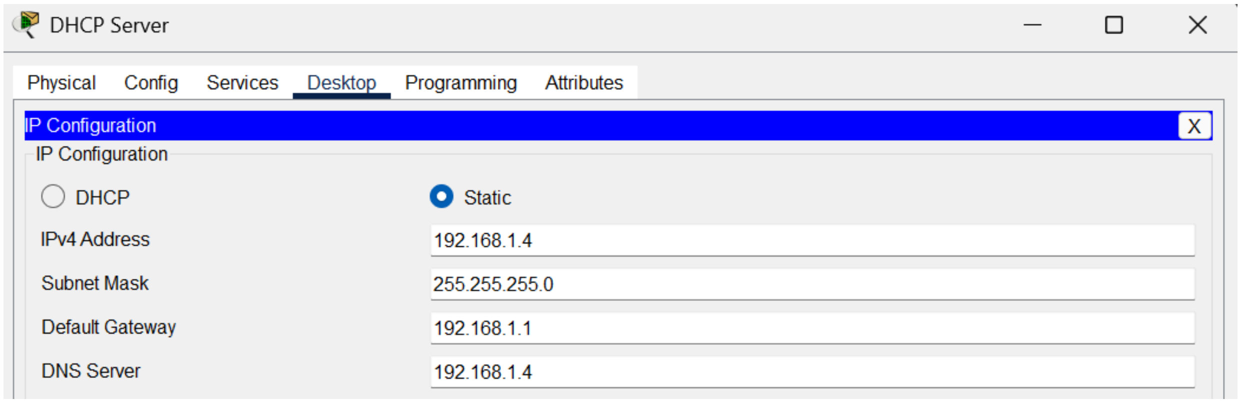
Name

Type A Record

Address

No.	Name	Type	Detail
0	company.com	A Record	192.168.2.3

All we need to do now is change the actual IP configuration of the DHCP server by going to the “Desktop” tab and clicking on the “IP Configuration” box like we did with the WEB server and type in the IP address (192.168.1.4), subnet mask (255.255.255.0), Default gateway (192.168.1.1), and DNS server (192.168.1.4).



IP Configuration

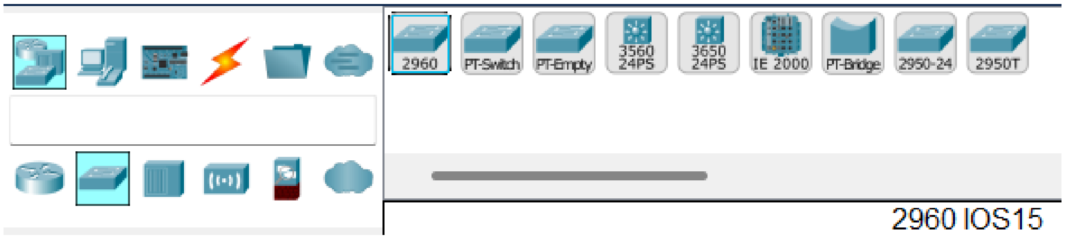
○ DHCP ● Static

IPv4 Address	192.168.1.4
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	192.168.1.4

Make sure to save your network before moving onto the next section which will be setting up several switches and a WAP.

Connecting and Configuring Branch Switches and WAP

Our next task is to connect and configure several switches that belong to three different branches within our network and a WAP so that wireless devices can connect to our network as well. First we will grab a switch from Network Devices >> Switches >> 2960:



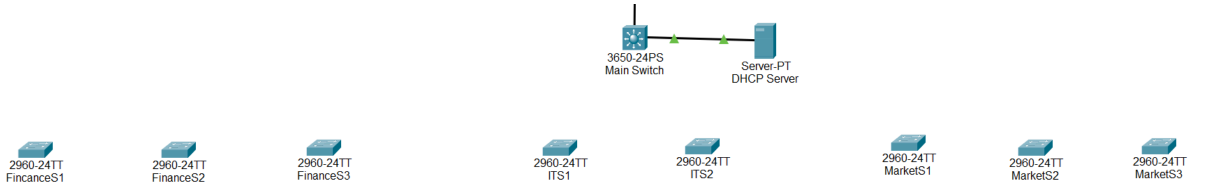
Place the switch into the network and enter its CLI to modify it. Once you get into the CLI enter the following commands to set up the hostname and password for the switch:

```
Switch> enable
Switch# conf t
Switch(config)# hostname BranchSwitch
BranchSwitch(config)# enable secret Cisco123
```

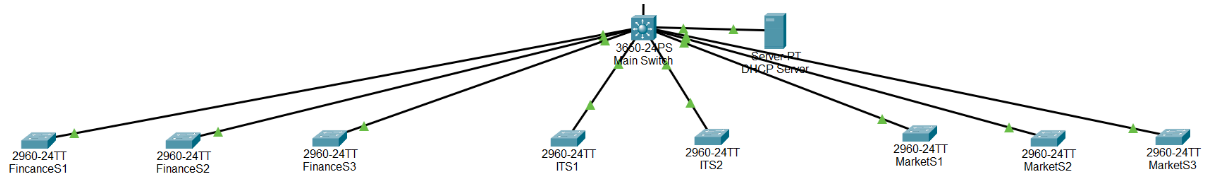
Next we will disable any interfaces we will not be using with these switches and save the configuration:

```
BranchSwitch(config)# int range Fa0/13-24
BranchSwitch(config-if-range)# shutdown
BranchSwitch(config-if-range)# exit
BranchSwitch(config)# int Gig0/2
BranchSwitch(config-if)# shutdown
BranchSwitch(config-if)# exit
BranchSwitch(config)# exit
BranchSwitch# copy run start
```

Now we have a template switch to use for every other switch we will be using for the different branches in the network. You can copy the switch exactly by clicking on the switch and pressing ctrl + c. Then you can paste it by pressing ctrl + v and drag the copies away from the original. You’re going to want to copy the switch 7 times making a total of 8 switches, and you want to put three in a group below the main switch and to the left naming them FinanceS1 to FinanceS3. Then you want to put another three in a group below the main switch and to the right naming them MarketS1 to MarketS3. In between the two groups put a group of two below the main switch naming them ITS1 and ITS2. Spread the groups out to make sure there is enough room to connect many computers to each switch. Your network should look like similar to this:

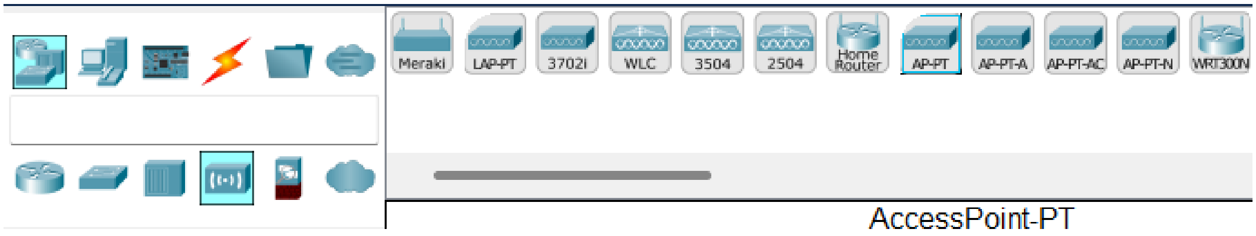


Connect a copper straight through wire from each switch's GigabitEthernet0/1 port to the GigabitEthernet1/0/3 through GigabitEthernet1/0/10 ports in the main switch so that your network looks like this:

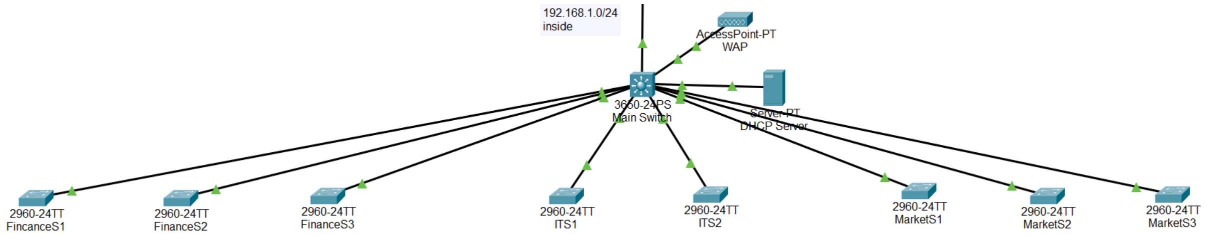


Now the switches are ready to have all the PCs connected to them in the next section.

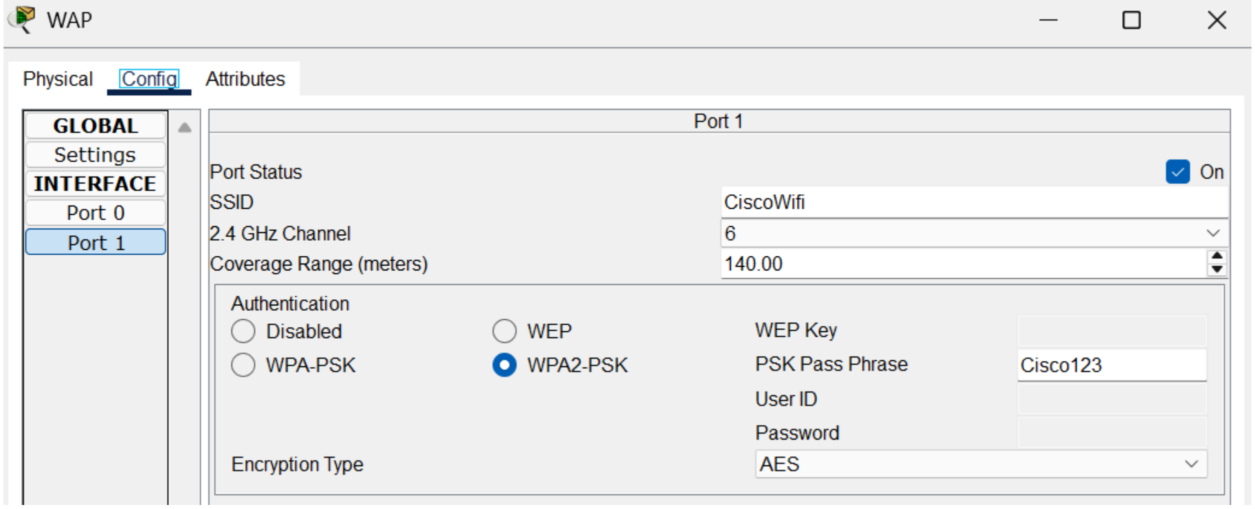
Next we will set up a Wireless Access Point (WAP) so that mobile devices like laptops and phones can connect to the network as well. We can do this by grabbing a WAP from Network Devices >> Wireless Devices >> AP-PT:



Place the WAP to the right of the main switch and rename it to WAP. Connect a copper straight-through wire to the Port 0 connection on the WAP to the GigabitEthernet1/0/11 port on the main switch. Your network should look like this:



Then you can modify the WAP by clicking on it to bring up its setup window, clicking on the Config tab, and clicking on Port 1. This brings up all the settings we can change for the WAPs Wi-Fi connection. In these settings we want to change the SSID (The display name of the Wi-Fi connection) to "CiscoWifi". We also want to change the authentication type to "WPA2-PSK", which is the best authentication security available on this WAP. This makes it so that anyone connecting to the Wi-Fi needs to put in a passphrase which we will change to "Cisco123". The new settings should look like this:



Port 1

Port Status	☑ On
SSID	CiscoWifi
2.4 GHz Channel	6
Coverage Range (meters)	140.00

Authentication

○ Disabled ○ WEP
○ WPA-PSK ● WPA2-PSK

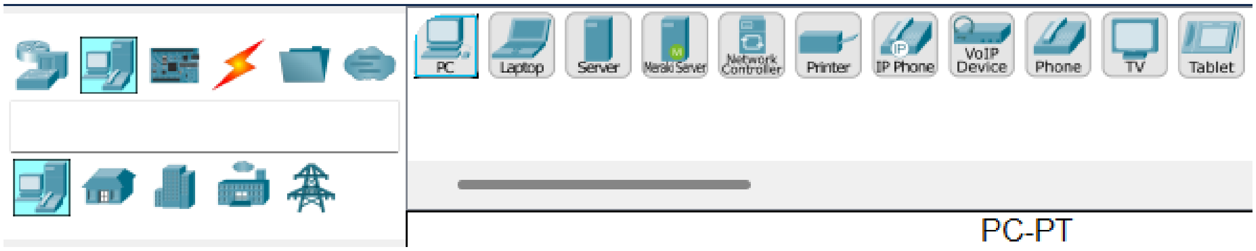
WEP Key	
PSK Pass Phrase	Cisco123
User ID	
Password	
Encryption Type	AES

Now anytime someone tries to connect to the network via Wi-Fi they do so through this WAP using the password. Devices connecting through the Wi-Fi will also automatically get an IP address from the DHCP server.

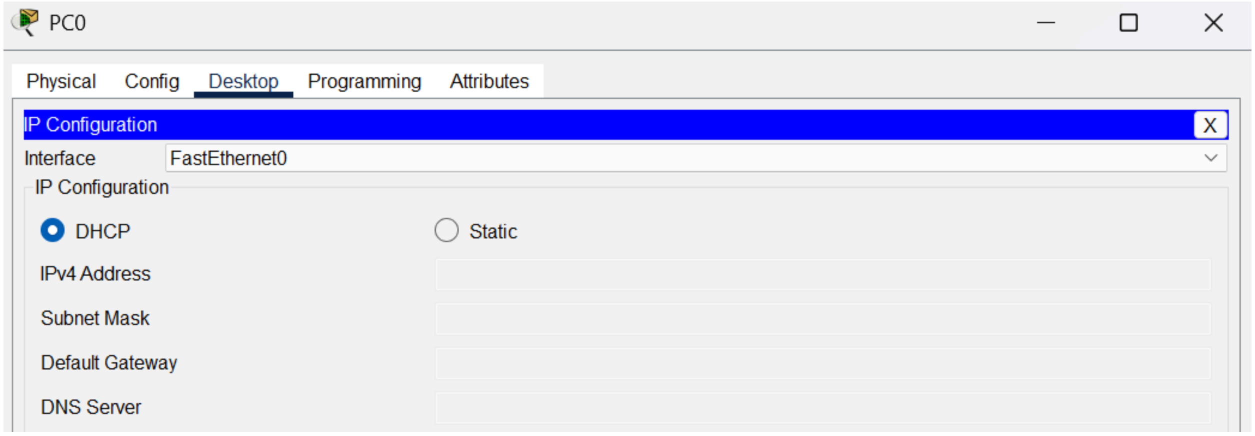
Connecting and Configuring Desktop PCs to Branch Switches

This next section can be really repetitive if you don't use copy and paste. We will be setting up 96 PCs, 12 for each branch switch. This will also cause your screen to become cluttered depending on how well you spread out the branch switches and how you decided to place your PCs in the network.

Before we get into copy and pasting we need to make our template first. To do this you need to grab a PC from End Devices >> End Devices >> PC.



Place it in the network and click on it to bring up the modification window. Click on the Desktop tab at the top of the window and click IP Configuration. Here we will simply check off the DHCP option to change it from manual.



PC0

Physical Config Desktop Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

● DHCP ○ Static

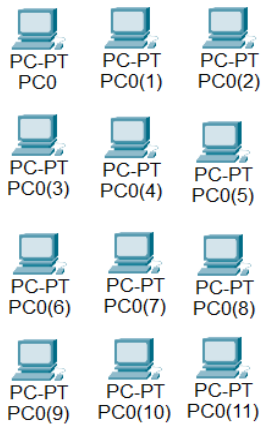
IPv4 Address

Subnet Mask

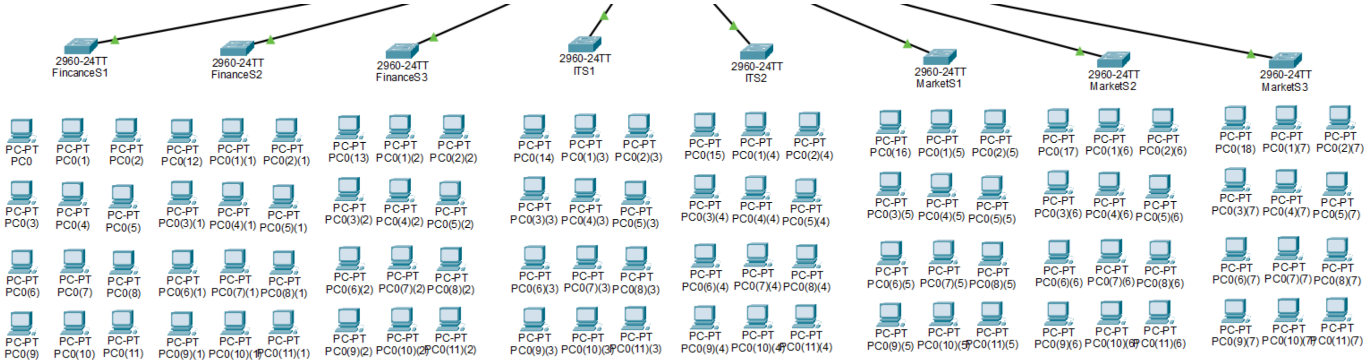
Default Gateway

DNS Server

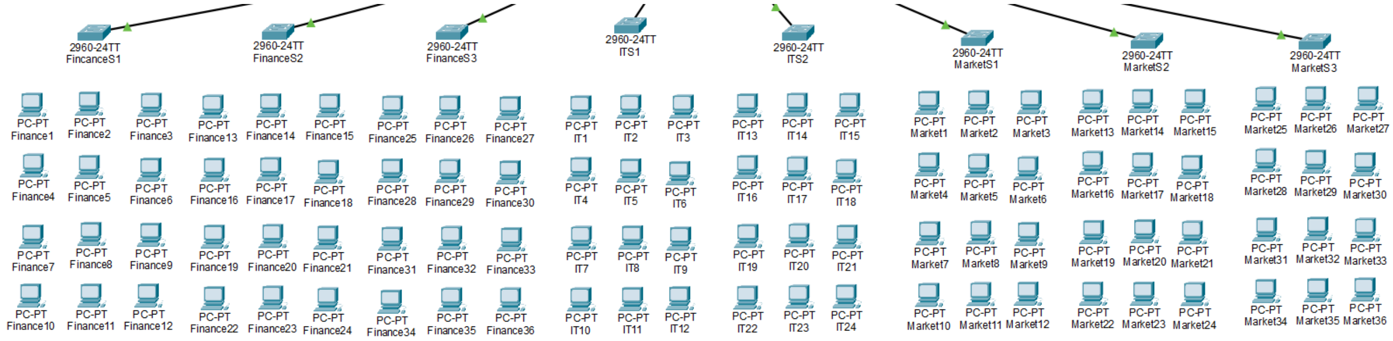
The rest of our network should now take care of connecting this PC to the rest of the network and we have our template PC. To copy and paste it we can do the strategy of pressing ctrl+c and ctrl+v over and over or we can make a shape with the computers and copy them as a group. First we need to get multiple computers to make the shape by pressing ctrl+c and then ctrl+v 11 times so we get 12 PCs. Then move the computers into a shape all in one group with decent space between each of them. For my network I chose this shape and will be using it for the rest of this section:



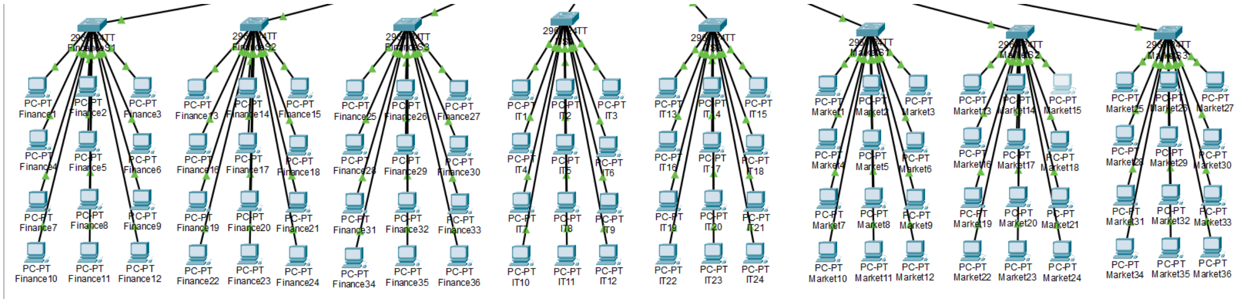
Now that we have a shape you can draw a box around it to select multiple devices by holding the left mouse button and dragging the mouse over them. Then pressing ctrl+c will copy the shape and all the device settings. We can move the PCs as a group now and they will stay in that shape, but if you unselect the group you will have to draw the box again or move every PC by itself. For this reason only copy one group at a time. Place your initial group at the first Branch Switch wherever you want then copy it once and move the new group to the next Branch Switch. Repeat this until you have a group next to each Branch Switch like this:



Feel free to move devices however you want to make the network less crowded. You probably also noticed that the PC names don't make a lot of sense. You don't have to rename them, but in my network I will to make it easier to follow along:



Now that we have all the PCs configured we can connect them to the switches with a copper straight-through cable. Since we disabled the later half of the ports (FastEthernet0/13 - FastEthernet0/24) on the Branch Switches we can only connect 12 PCs to each one and only with the first half of the ports (FastEthernet0/1 - FastEthernet0/12). For example, to connect the PCs Finance1 through Finance12 we will connect a copper straight-through wire to the FastEthernet0/1 port on Finance1 and connect it to the FastEthernet0/1 port on FinanceS1, then connect another wire to the FastEthernet0/1 port on Finance2 and connect it to the FastEthernet0/2 port on FinanceS1. Once you get done with this first switch you connect the next group of Finance PCs (Finance13 - Finance24) to FinanceS2's first half ports (FastEthernet0/1 - FastEthernet0/12). To speed things up if you hold the ctrl button while connecting the wires you won't have to reselect the wire after every PC.



Once you are done you can test your network by clicking on a random PC and making sure it got an IP address from our DHCP server by going back to the IP Configuration section. The IP address should start with 192.168.1 and then have a number from our DHCP pool. Then you can go to the Command Prompt section under the Desktop tab and ping other computers, switches, router, or even the whole network. Run a few of these test pings here and they should all be successful:

- ping 192.168.1.255 (This pings the whole network)
- ping 192.168.2.3 (This ping the WEB server)
- ping 209.165.200.225 (This pings a valid external device)

You can also test an invalid device “ping 192.168.3.20” to see what a failed ping looks like. If everything is successful then congrats! You have put together a working network with security. You can mess with a few settings or have fun with the visual pinging feature that network packet tracer has by pressing “p” and clicking the source and destination devices. You will then be able to see it go through the network and back.