**Personal Specialisation Project**

Mohammed Nasser Alshukaili.

ICT, Fontys University of Applied Sciences.

Cyber Security, Semester 4.

2022

Contents

[**SCOPE** 3](#_Toc124111234)

[**Main Question** 3](#_Toc124111243)

[Sub Questions 3](#_Toc124111244)

[**My Plan** 4](#_Toc124111245)

[**Results** 5](#_Toc124111246)

[What network fundamentals do I need to take the exam? 5](#_Toc124111247)

[How networks can be accessed? 26](#_Toc124111248)

[What is IP address and what does it offer? 39](#_Toc124111249)

[What security skills do I need to pass the exam? 42](#_Toc124111250)

[What is automation and programming in the CCNA? 45](#_Toc124111251)

[**Personal Reflection** 46](#_Toc124111252)

[**References** 47](#_Toc124111253)

# **SCOPE**

The aim of this research is to study the CCNA subjects to prepare myself to become a network engineer. The scope of this research is to examine the modern networking technologies and their implementation in the context of the Cisco Certified Network Associate certificate (CCNA). The research will also include some practical exercises to set up home networks. The research will be conducted using a combination of online trainings and resources, such as itpro.tv, YouTube, CCNA articles, and online interviews with CCNA experts.

# **Main Question**

**How can Cisco Certified Network Associate (CCNA) certificate prepare me to become a network engineer?**

## Sub Questions

1. What network fundamentals do I need to take the exam?
2. How networks can be accessed?
3. What is IP address and what does it offer?
4. What security skills do I need to pass the exam?
5. What is Automation and Programming in the CCNA?

# **My Plan**

In this research, I will be using the DOT framework to answer my questions. (<https://ictresearchmethods.nl/Methods>)

DOT framework consists of 5 strategies:

1. Library
2. Field
3. Lab
4. Showroom
5. Workshop

Each strategy offers several methods.

Here is my plan for this research:

Table

Description automatically generated

# **Results**

After browsing Cisco website, I found the content of the CCNA exam. Therefore, I will be relying on that website to study step-by-step for the exam. ([­­­­­­](https://learningnetwork.cisco.com/s/ccna-exam-topics)).

From the website above, here is the content of the current CCNA version:

Graphical user interface, text, application, email

Description automatically generated

## What network fundamentals do I need to take the exam?

**Network Fundamentals**

#### **Network Topologies**

There are many types that people used to design networks. Some of them are:

* Bus Topology
* Ring Topology
* Star Topology

#### Bus Topology

The internet started with 2 devices that were connected using the same cable, this is called Bus Topology. It can handle more than 2 devices as long as they are connected to the same cable.

A picture containing text, sign

Description automatically generated

This design shows that the 3 devices can talk to each other because they use the same cable.

This design is outdated and not used nowadays.

#### Ring Topology

A picture containing text

Description automatically generated

Ring topology is creating a circle with the devices that are connected with each other.

Advantages:

* Network Management: devices can be replaced/removed from the network without shutting it down.
* Cost: Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.
* Reliable: It is a more reliable network because the communication system is not dependent on the single host computer.

Disadvantages:

* Difficult troubleshooting.
* Delay

#### Star Topology

This design is the most used design these days. The shared device is in the middle, and a cable is going out from it to each device.

Advantages:

* Efficient troubleshooting: troubleshooting is easier than the other designs.
* Easily expandable: more devices can be easily connected to the centered device using its own cable.

Disadvantages:

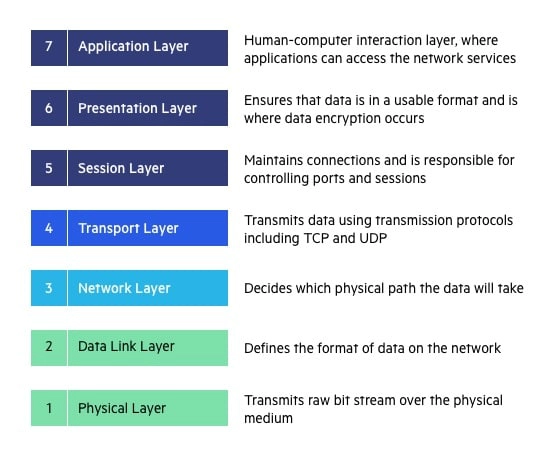
* A Central point of failure.
* So many cables.

(*Computer Network Topologies - Javatpoint, n.d.)*.

#### **OSI MODEL**

The Open Systems Interconnection (OSI) is the model that is being used by the modern devices to communicate to other devices on the internet.

The OSI model consists of 7 layers that share the steps of encapsulation/decapsulation.



([*https://www.imperva.com/learn/application-security/osi-model/#:~:text=The%20Open%20Systems%20Interconnection%20(OSI,companies%20in%20the%20early%201980s*)](https://www.imperva.com/learn/application-security/osi-model/#:~:text=The%20Open%20Systems%20Interconnection%20(OSI,companies%20in%20the%20early%201980s)).

Let’s start from the top:

**Layer 7 – Application Layer:**

This layer is where the end-user interacts with a software. Such as, HTTP/S for when visiting a website as in our scenario.

**Layer 6 – Presentation Layer:**

This layer is responsible for encoding, encrypting, and compressing the data that is being sent and received.

**Layer 5 – Presentation Layer:**

It ensures to create communication channels (sessions) to allow the devices to talk to each other. It also ensures that these channels are not being interrupted.

**Layer 4 – Transport Layer:**

This layer turns the data into ordered segments to make sure the data is in the correct order.

It also ensures that the specific segment has been received to send the next one. If a segment was not received, the layer would send it again.

**Layer 3 – Network Layer:**

Network layer breaking up the segments into network packets. Also, it routes the packets to the best path towards the destination.

**Layer 2 – Data Link Layer:**

This layer receives the network packets and turn them into frames, then it sends them to the destination using the Media Access Control to route the frames.

**Layer 1 – Physical Layer:**

It takes care of the physical cables and how the devices are connected and talking to each other.

#### **TCP/UDP**

TCP requires 2 devices to be connected for them to send packets, therefore TCP is considered connection-based protocol. The following are some of the services that the TCP protocol brings:

* The server ensure that the client received the packets, if not, the server will keep sending the same packet until it is received.
* It uses three-way-handshake to establish a connection.
* Ordered packets
* Reliable

UDP, on the other hand, doesn’t require a connection between the receiver and the sender, therefore, people call it “connectionless”. The UDP has many pros, such as:

* Smaller packets
* Less bandwidth
* Fast

(BasuMallick, 2022).

##### TCP

Let’s talk about how TCP works.

Scenario 1:

Let’s assume that I am on my PC, and I want to access git.fhict.nl.

I open google and I type:

Graphical user interface, text, application

Description automatically generated

It will send me to the git page that I asked for. However, I want to discuss what happens behind the scenes that led to showing the page.

After pressing Enter, a PDU information that consists of 7 layers will be sent to the destination server. What is inside the 7 layers?

**Layer 7:**

Layer 7 will tell the server that I sent HTTPs request, this helps the server to route me to the web page.

The PDU will look like this after this layer:

Graphical user interface, application

Description automatically generated

This means that application layer completed its data, and the other layers are waiting.

**Layer 4:**

Transport layer is where the port information is stored. As we are requesting a web page, layer 4 will carry TCP as header + the port that we are connecting to:

Graphical user interface, text

Description automatically generated

Now this is called a segment.

**Layer 3:**

The network layer carries the information about the source IP address and the destination IP address.

Text

Description automatically generated

Now this packet has all the previous information PLUS the IP addresses.

**Layer 2:**

Layer 2 will take all the information before and add the MAC addresses. After adding the Layer 2 header and trailer, it will be called “Frame”.

Text

Description automatically generated

Now all these information are stored in one “envelope” this letter is ready to be sent using the Ethernet cable which we cover in the next layer.

Layer 1:

Physical layer is the connection cable that will take all the previous information and send them to the internet.

After the message is received by the destination, then it will **decapsulate** the letter to reveal the layers information.

The web server will **decapsulate** the layers just to find out that they carry information for the server itself. The server will find its MAC address in layer 2, its IP address in layer 3, port TCP in layer 4, and HTTPs in layer 7, then it will send back the web page. (NetworkChuck, 2020a)

#### Subnetting

Subnetting is the strategy used to create separate networks inside one network.

When you have one network and 100 employees, you would not want all the employees to be in the same network. Therefore, network engineers divide that one network into many sub-networks.

Then, a sub network can be given to several employees that share the same job like marketing, business, and information technology.

**Subnet masks:**

*CLASS A:* 255.0.0.0 (Number of hosts possible: 255\*255\*255 = 16581375)

*CLASS B:* 255.255.0.0. (Number of hosts possible: 255\*255 = 65025)

*CLASS C:* 255.255.255.0 (Number of hosts possible = 255)

Why subnetting is important?

* It helps to reduce the traffic by splitting the network into many.
* It helps to divide the hosts as wanted.
* It helps employees to work from home without needing to connect to the open network.

(Techopedia, 2017).

Let’s understand subnetting by answering some questions:

**What is the broadcast address for 223.209.177.136/29?**

The broadcast is the last IP address for a specific network. The question gives us a single IP in that network. How do we know how many hosts are in that network to find the last IP?

Subnet mask can help us here.

Subnet mask = 29 = (29 1s then the rest are zeros) = 11111111.11111111.11111111.11111000

= 255.255.255.248

Text

Description automatically generated

What is the network ID for 221.230.76.99/27 ?

Network ID is the first IP in a network.

First, we need to figure out the number of hosts possible in this network.

/27 = 11111111.11111111.11111111.11100000

Hosts = 2 to the power of 5 = 32.

Text

Description automatically generated

**You have 209.51.44.0/24, you need to subnet into 5 networks. What is your new subnet mask?**

/24 = 11111111.11111111.11111111.00000000

This equals 2 to the power of zero = 1 network possible.

I need 5 networks. Therefore, I need to borrow from the host portion. If I borrow only one zero, it will give me 2 to the power of 1 = 2 networks.

If I borrow 2 zeros, it will give me 2 to the power of 2 networks = 4 networks, still not enough.

If I borrow 3, it will give me 2 to the power of 3 = 8 networks possible.

Text

Description automatically generated

(ITProTV, 2022)

#### **Cisco Packet Tracer**

I will be using Cisco Packet Tracer to practice my networking skills and understand how online devices communicate behind the scenes.

Cisco Packet Tracer can be downloaded from here:

<https://www.netacad.com/courses/packet-tracer>

Once you open the application, you will find a dashboard that helps you with simulating a network.

Graphical user interface, application

Description automatically generated

Let me start with creating a simple network that consists of 2 PCs and one switch.

Chart

Description automatically generated

Now the 2 PCs are connected to the same switch. However, they can not talk to each other yet due to the fact they do not have IP addresses yet.

Let me configure each PC to have its own IP address.

**PC0**

Graphical user interface, text, application, email

Description automatically generated

**PC1**

Graphical user interface, text, application, email

Description automatically generated

Now that the 2 end points have IP addresses, let me try to ping one device to another:

Graphical user interface, application

Description automatically generated

On the PC0 device, I am trying to ping PC1. So far there is no response because I need to resume the simulation.

After forwarding the message,

Diagram

Description automatically generated with low confidence

There is an envelope going from PC0 to the switch that carries the information for the ping.

Let me see what is inside that message:

Graphical user interface, text, application

Description automatically generated

The switch operates on layer 2, this is why it can only see the MAC address of the source and destination.

After forwarding the message from the switch to the final destination, PC1 can open all the layers messages as it is the final destination.

Graphical user interface, text, application, email

Description automatically generated

**Router CLI**

Router CLI modes:

* **user EXEC mode**

This is the initial startup mode. It uses the greater than sign to differ from other modes.

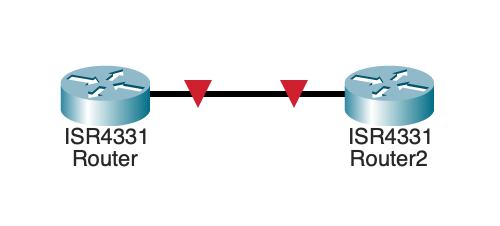
* **privileged EXEC mode**

This is the system administrator mode. It allows to read router files, change operating parameters, and router can be rebooted.

* **global configuration mode**

Used to modify system-wide configuration parameters, such as routing tables and algorithms.

**Router hostname**

****

Above, we can see 2 connected routers, let me use the command line interface to rename both routers.

Graphical user interface, application

Description automatically generated

Notice that it is currently in the user EXEC mode. I need to be in the global configuration mode to be able to rename the device.

Text

Description automatically generated

enable command takes me to the privileged EXEC mode. I still need the global configuration mode.

Text

Description automatically generated with medium confidence

configure terminal command takes me to the global configuration mode.

Now that I am in the correct mode, I can rename the device name by using the following command:

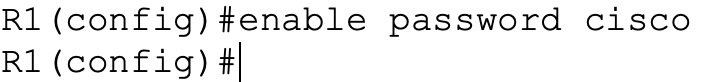
Text

Description automatically generated with medium confidence

R1 was renamed successfully. Now I can do the same steps to rename the second router.

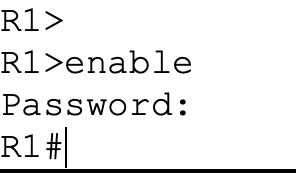
**Router password**

Setting a password for the router can help us to secure the system configuration from being changed by intruders. This will require the unauthorized people to enter the correct password to be able to enter the privileged mode.



This command creates a password for R1. The password is “cisco”.

Now when I try to enter the privileged mode, I get asked for this password.



We can show the configuration file using the command show run

Text

Description automatically generated

And to encrypt the password, we use this command:

****

show run :

Text

Description automatically generated with medium confidence

“cisco” password is now stored encrypted.

enable secret cisco works like password but secret is prioritized over password.

After reloading the router, I noticed that all the configuration that I added disappeared. Why?

Because router does not save the configurations by itself, I need to add another command to copy the running-config which I modified, to the startup-config.



With this command I saved the changes to the startup-config, now when I reload the router, I should be able to find the modified configuration.

**VLANS**

VLANS can help us to isolate devices from other devices in the same network. It also allows us to create more than one LAN in the same network, this helps to divide devices depending on their purpose in the network.

Timeline

Description automatically generated

This is a simple network that share the same Layer3 devices. Devices can ping between each other successfully.

Let’s assume that PC1 and PC3 are in the business department, and PC2 with PC4 are in security department. How can we create 2 VLANS each one for one department?

This can be done using the 2 switches.

First, assign PC1 to vlan 1 using Switch 1:

PC1 is in the F0/2 port.

Text

Description automatically generated

Next, assign PC2 to vlan 2:

PC2 is in the F0/3 port.

Text

Description automatically generated

vlan 1 is already created in every switch, therefore it did not mention anything about creating vlan 1 like it did when creating vlan 2.

Assign PC3 to vlan 1:

PC3 is in the F0/2 port.

Text

Description automatically generated

Assign PC4 to vlan 2:

PC4 is in the F0/3 port.

Text

Description automatically generated

PC1 & PC3 are assigned to vlan 1 and should be able to ping between each other.

PC2 & PC4 are assigned to vlan 2 and should be able to ping between each other.

Let’s ping:

PC1 to PC3 (succeed)

PC2 to PC4 (failed). Why? They are in the same vlan, they should be able to ping.

Because F0/1 port in both switches are assigned to the native vlan which is vlan 1 by default.

In order to share information between switches and allow them to pass connections with multiple vlans, we must configure the F0/1 port that connects them as Trunk.

Text

Description automatically generated with medium confidence

Next, assign F0/1 port in switch 2 to trunk as well.

Chart

Description automatically generated

Now both vlans should be able to communicate.

Conclusion

This sub question helped me to investigate in the foundation of the internet. It explained to me how the OSI model works and how useful can it be to a network engineer. It also introduced to me the concept of subnetting and how to divide one network to multiple smaller networks. Finally, I used Cisco Packet Tracer to practice the things I learned by creating networks and VLANS.

## How networks can be accessed?

**Network Access**

#### **VLAN**

What is VLAN?

A virtual LAN is a logical concept that connects devices that share the same purpose together. Then, the devices that are in the same VLAN are in a different sub-network that other devices. Grouping them helps to isolate the traffic for each sub-network.

Why is VLAN important?

Network engineers tend to use VLANS for some of the following reasons:

* To strengthen the security
* To reduce the unnecessary traffic
* To improve performance
* Easier to administrate

**Security**

VLANS can help with improving the security by controlling which devices have access to other devices. Administrators can strict the connections between these devices, and only allow the devices that need each other to send data between them

**Reduce unnecessary traffic**

Dividing the devices into VLANS means that marketing devices does not know anything about the traffic that business devices are sending and receiving. This improves the flow of the traffic in the network as each sub-network can only have access to what it needs.

**Improve performance**

Less traffic leads to better performance. VLANS reduce the number of other devices that keep sending broadcast.

Engineers can also prioritize traffic against another. For instance, VLANS that consists of voice over IP can prioritize this traffic to improve the performance, and isolate other devices on a different VLAN.

**Administration**

Grouping devices that share the same purpose can help with administrating them. Network engineers can them navigate to one VLAN and start administrating.

(Slattery & Burke, 2022)

How to create VLANS?

End-point devices that are connected to the same switch can be divided into multiple VLANS. For instance, in a small company, marketing, business, security devices are connected to the same switch, this causes unnecessary traffic for the different sections. Creating VLANS can be by specifying the ports to a unique VLAN.

Diagram

Description automatically generated

This picture illustrates that one switch can create more than one VLAN. Each color represents a VLAN that consists of the devices that are connected to that color.

What happens if we want to add a device that is connected to another switch to a VLAN in this switch?

**Trunk**

Trunk is connecting a switch to another switch via a physical cable. This will allow all the devices that are connected to one switch communicate with devices that are connected with the other switch.

Diagram

Description automatically generated

Now a single VLAN can be created for each color.

Let me apply this in a practice lab.

Diagram

Description automatically generated

Cisco IP Phone is connected to NYCORE2 switch. I want to create 2 VLANS in that switch, one for voice, and one for data.

Text

Description automatically generated

Here are the commands that I would need to create VLANS in a switch. Now that I created 2 VLANS (Voice and Data) and they are both active, notice that I did not assign any ports for these VLANS.

With the following commands, I can assign specific ports to the 2 VLANS that I created earlier.

Text

Description automatically generated

As you can see, Voice and Data VLANS are now connected to the same port.

(ITProTV, 2022)

#### **Switch**

What is a switch?

Switches are used in networks to connect to devices physically using ethernet cables. It can have many connected devices, and it allows them to communicate by forwarding data packets from source to destination. Diagram

Description automatically generated with medium confidence

Here is a simple network that consists of 3 end points, and a switch that allows them to communicate.

Most switches are using layer 2 to communicate, meaning that it needs to know the source MAC address and the destination MAC address in order to work properly.

How does it know which device is the source MAC address and which is the destination MAC address?

Switches are not smart enough to know this from the first time, they keep learning until they get to the point where they do their job perfectly.

Let me simulate a data packet from PC to PC1

PC terminal:



After pressing enter:

Diagram

Description automatically generated

You can see that there is an envelope coming from PC going to the switch

**A picture containing chart

Description automatically generated**

The switch received the envelope that carries that ICMP data from the source MAC address to the destination MAC address.

Since this is the first time for the switch to work on this network, it only knows the source MAC address after receiving the message from a specific port. It still does not know the destination MAC address.

Diagram

Description automatically generated

It forwards the packet to all the connected ports except for the source port. Simply, the switch is discovering in which port does is MAC address located.

Both devices will receive an ICMP packet, but only the device with the same MAC address that is inside the envelope will reply.

Chart

Description automatically generated

The red X indicates that it received a packet that it was not meant for it. Therefore, it will just drop and ignore the packet.

On the other hand, PC1 will reply to the switch telling it that I am the device with that MAC address.

Diagram

Description automatically generated

Switches only need to do this on the first time. Thanks to the Content Addressable Memory (CAM) table.

Content Addressable Memory (CAM) table:

It stores each connected port with its MAC address.

|  |  |
| --- | --- |
| **MAC address** | **Port** |
| Computer A's MAC address | 1 |
| Computer B's MAC address | 2 |
| Computer C's MAC address | 3 |

If it is the first time for a switch in a network, this table would look like this:

|  |  |
| --- | --- |
| **MAC address** | **Port** |
| ? | ? |
| ? | ? |
| ? | ? |

It needs to start learning which port is what MAC address.

Let me build the CAM for our scenario:

First, the CAM table looked like this:

|  |  |
| --- | --- |
| **MAC address** | **Port** |
| ? | ? |
| ? | ? |
| ? | ? |

Then I sent an ICMP packet from PC to PC1

Once After receiving the message from PC, it adds the source port and MAC address to the table.

|  |  |
| --- | --- |
| **MAC address** | **Port** |
| 0000.0CE3.2C73 | 1 |
| ? | ? |
| ? | ? |

Now since the CAM table does not know in which port lives the destination MAC address, it forwards the packet to all the connected port except for the source port (flooding). After that the device with the correct MAC address (unknown unicast) will respond and the switch will update the CAM table to look like this:

|  |  |
| --- | --- |
| **MAC address** | **Port** |
| 0000.0CE3.2C73 | 1 |
| 0060.3E5E.5A4E | 2 |
| ? | ? |

It keeps update this table until it has all the network information that it needs.

(Cloudflare, 2022).

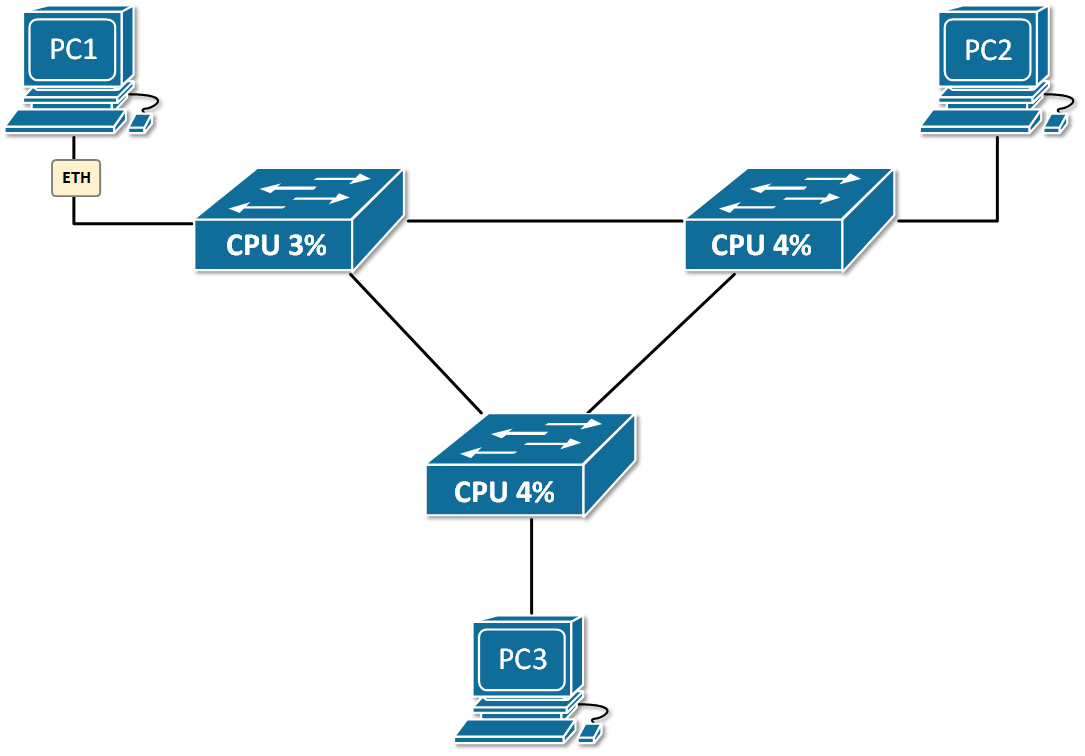
The previous process works fine for a simple network. However, modern technology is expected to serve everything with no delay and no problems as this is an integral part in the CIA triad. Therefore, networks are required to have redundancy to keep serving clients.

Redundancy in networks means that the network is not relying on one single cable, there should be plan B and C to avoid any disconnection.

One of redundancy solutions is to use more than one cable to connect switches, meaning that whenever a cable disconnects for any reason, there are alternatives that ensure to continue working properly. However, this solution comes with its drawbacks.

When having more than one switch in a network, switches will keep forwarding the same broadcast to each other, creating an infinite loop of the same packet, this is called Ethernet Loop, Layer 2 Loop, or Broadcast Storm.

Next GIF illustrates a big problem with switches (Layer 2 loop):



*(*[*https://www.networkacademy.io/sites/default/files/inline-images/Broadcast%20Domain.gif*](https://www.networkacademy.io/sites/default/files/inline-images/Broadcast%20Domain.gif)*)*

(*LAN Switching With Redundant Links*, 2022)

Problems that appear when using redundant networks:

* Broadcast Storm (Layer 2 loop)

Switches keep forwarding the same packet to each other in an infinite loop.

* Unstable MAC address table

Switches keep updating the MAC address table because they keep getting the same packet from different ports.

* Duplicate frames

Just like the switches, the destination device will keep receiving the same packet infinitely.

(CertBros, 2017).

How did network engineers overcome this problem? (STP)

**Spanning Tree Protocol (STP)**

STP is a layer 2 network protocol used to prevent loops when exchanging data between switches in networks that contains redundant paths.

Usually, switches forward data through all the connected ports. STP fixed this problem by following certain rules by all the switches.

STP chooses for the switches which ports to block and forward.

These are only 2 states that STP uses, the states are:

1. Disabled

The port does not forward data nor listen to it.

1. Blocking

The port does not forward any data. However, it listens to the received Bridge protocol data unit (BPDU).

1. Listening

The port discards packets that are forwarded by another port. it just receives BPDUs and redirects them to the switch for processing.

1. Learning

The port discards packets that are forwarded by another port. It processes the received BPDU and start updating the MAC address table.

1. Forwarding

The port forwards the packets to all the connected ports. It listens and learns, meaning that it updates the MAC address table as well.

(Sheldon, 2021).

How STP works?

STP follows the following steps in each network:

1. Elect a Root Bridge

Root bridges have the authority to control all the other switches in the network. They have all their ports in forwarding state (FWD).

1. Put Root Bridge ports in a Forwarding state

Root bridges have the priority to forward the packets to other switches/devices.

1. Each non-root switch should choose its Root port

Non-root switches are all the other switches except the Root Bridge. They should choose a port that can Forward data which is the Root port.

1. Other links choose a Designated port

Non-root ports can also Forward packets, but it needs to have some conditions.

1. All other ports are put in Blocking state.

This is why frames only get received once.

How STP selects which switch is the root bridge?

The criteria are (in order):

1. The lowest bridge priority. (Normal is 32768)
2. The lowest MAC address.
3. The lowest cost (Closer path to root)
4. The lowest number of the port.

(CertBros, 2017).

#### **Wireless Lan Controller (WLC)**

The growing demand for internet requires networks to have more than one access point in each building. Managing and configuring all these access points can consume more money and time. Therefore, Wireless Lan Controller comes to settle this bottleneck by taking care of managing and controlling different access points in one device.

Home networks do not need to consider having a WLC. However, medium-big companies tend to have multiple access points inside their building, this is the perfect time to consider implementing a Wireless Lan Controller (Worton, 2021).

#### **Wireless Security Protocols**

Wired networks can secure the network by hiding the network cables from reach to harden it for hackers to gain access, hackers would need to dig behind the walls to find the cables that will connect them to the network which is very rare to happen.

Wired networks can be easily secured. On the other hand, how about the wireless networks? Hackers can get to the network even from outside the building.

Let me talk about the different wireless security protocols.

* Wired equivalent Privacy (Web)

This is the oldest Wi-Fi security protocol. WEP encrypts the data coming from and going to the access point using a static key. Any device that is connected to that network has access to that key. Therefore, it can decrypt the data.

WEP only supports 64-bit or 128-bit encryption key sizes, making it easier to decrypt. WEP uses only the hexadecimal characters which only allow for numbers 0-9 and from A-F (Ghimiray, 2022).

* Wi-Fi Protected Access (WPA)

Tech companies collaborated to improve the security of Wi-Fi access as the WEP failed to do so. They came up with a solution to encrypt every packet with a unique key.

Once again, hackers found the pattern used to encrypt the data which explains that this method was not safe anymore.

* Wi-Fi Protected Access 2 (WPA2)

This protocol is still being used on most networks today. Rather than it only encrypts the data, the user must be authenticated too to connect to the network.

* Wi-Fi Protected Access 3 (WPA3)

This is used to protect the user when connecting to public networks in public spaces.

(ITProTV, 2022).

Conclusion

To sum up, security is an integral part in creating networks, because bad people can easily reach your network. Also, to create a network, people need to learn how VLANS work, and how to use the Command Line Interface (CLI) to configure devices within a network. People also need to learn how to implement the best suitable methods depending on the purpose of their network and how to troubleshoot them. I tried to attach advantages and disadvantages for many used methods, this helps to choose the best option.

## What is IP address and what does it offer?

#### **Packet Forwarding**

A picture containing chart

Description automatically generated

In this example, when we want to send a packet from PC1 to PC2, what does PC1 need in order to send the message? Does it need destination MAC address, or destination IP address?

The sender machine initializes a frame header that looks like this:

Src: IP | MAC

Dst: IP | MAC

It will use the sender machine IP and MAC addresses in the source section of the frame header, and It will add the IP address of the destination machine. However, it does not know the MAC address of the destination because they are not in the same network.

How would it label the frame header if it does not know the destination MAC address?

It will simply put the MAC address of the default gateway in that network.

After that, the frame will go from the sender to the default gateway which is Router0.

Router0 will never change any of the IP addresses, it will change the source MAC address to its own MAC address, and the destination MAC address to Router1 MAC address.

Router1 still does not have the PC2 in the same network. Therefore, it will change the MAC address to its own, and the destination MAC to Router2 MAC, then it will forward the frame to it.

With this process, different networks can talk to each other. (ITProTV, 2022).

#### **Network Address Translation (NAT)**

NAT stands for Network Address Translation. It is the process of translating private IP addresses that want to go outside to the internet, to a public IP address.

**How it works?**

Assume there is a PC in a private network that has the IP address of: 192.168.10.10

When it asks an online server to send something, the server will not be able to send the data to the same device because it does not know whose IP address is 192.168.10.10. Therefore, NAT will switch the private IP address to the public IP address before going out to the server, with this, now the server can return data to the same public IP.

**NAT TYPES**

1. **Static NAT**

One private IP address gets assigned the public IP address, meaning that only one device can communicate with the public internet.

1. **Dynamic NAT**

Instead of choosing the same IP address, NAT will choose the IP address randomly.

1. **PAT**

PAT stands for Port Address Translation. All the private IP addresses get assigned to the same public IP address when communicating to the outer world.

4 billion IP addresses are not enough to cover all the online devices in the world. It seemed enough when IPv4 was launched in the 1970s. However, the modern world is trying to make every product as smart as possible which consumes all the possible IP addresses. NAT came to overcome this problem, 100 online devices in a single house with private IP addresses can use only one public IP address. (*Network Address Translation Definition | How NAT Works | Computer Networks | CompTIA*, 2022).

#### **Syslog**

Syslog is a protocol used to analyze the traffic happening on a connected device.

There are 3 layers to syslog:

1. **Transport layer**

It sends the message over the network

1. **Application layer**

It enables the message to be routed, interpreted, and stored.

1. **Content layer**

It contains the actual data, including timestamps, facility codes, and severity levels.

(Sumo Logic, Inc., 2021).

In research from Sumo Logic, Inc. “To identify the source of a message, syslog uses a numeric facility code, or simply a “facility,” generated by the originator of the message. These codes originated in Unix systems and aren’t obvious based on their values. The list below correlates the message code with its facility.

0: kernel messages

1: user-level messages

2: mail system

3: system daemons

4: security/authorization messages

5: messages generated internally by syslog

6: line printer subsystem

7: network news subsystem

8: UUCP subsystem

9: clock daemon

10: security/authorization messages

11: FTP daemon

12: NTP subsystem

13: log audit

14: log alert

15: clock daemon”

(2021).

**Syslog message levels**

Syslog message is presented with a numeric number that indicates the danger of the message.

* 0 – Emergency (The highest)
* 1 – Alert
* 2 – Critical
* 3 – Error
* 4 – Warning
* 5 – Notice
* 6 – Informational
* 7 – Debug (The lowest)

(Sumo Logic, Inc., 2021).

#### **OSPF (Open Shortest Path First)**

When a device tries to communicate with another online device from a different network, it sends the data to the gateway that will take the responsibility on delivering the message to the correct router. The gateway uses a router protocol called OSPF to find the best path for the packets to reach the destination.

OSPF replaced Routing Information Protocol (RIP).

Routers store all the routing data in the routing table, and whenever there is a change in one router’s routing table, it broadcasts it to all other OSPF hosts in the network. Where RIP sends the entire table to all hosts every 30 seconds (Burke, 2015).

## What security skills do I need to pass the exam?

#### **Key Security Concepts**

When companies use the internet, they are exposed to millions of users every day, this can be a good thing and a bad thing at the same time. Using the internet to brand companies can bring an enormous number of customers. However, not all users want the good for a specific company. Some users would want to damage the company for many reasons. Therefore, implementing and strengthen the security of the usage of the internet has become an integral part for all companies.

The purpose of network security is to prevent the bad guys from damaging anything owned by the company. Firewalls, detection tools, and other devices can help with controlling the network security.

In research from GeeksforGeeks “Key Security Concepts:

Asset: Anything of value to a company is considered an asset. If you are aware of the assets you are trying to protect, their value, their location, and their vulnerabilities, you will be more effective in how much time, effort, and money you invest in protecting those assets. You can make decisions.

Vulnerability: A security flaw in the hardware, software, or configuration of a device or process is called a “vulnerability.” Parties responsible for remediating such vulnerabilities should conduct vulnerability testing on a regular basis.

Risk: The likelihood of being targeted by a particular attack, the likelihood of a successful attack, and overall exposure to a particular threat are all referred to as ‘risk’. As you can see, there is risk where there is both vulnerability and danger.

Threat: A particular type of attack source and means is called a “threat”. A threat analysis is performed to determine how best to protect your system against a particular threat or class of threats.

Exploit: An exploit is a method or tool used by an attacker to exploit a vulnerability and damage a target system.

Countermeasures: Countermeasures are protections that reduce possible risks. Countermeasures reduce the likelihood that an attacker can exploit a risk by reducing or eliminating the vulnerability.”

(2022).

#### **Virtual Private Network (VPN)**

VPN is a service that provides a safe, encrypted connection. It provides more privacy for users. It can be used to hide the geographical location, which makes it efficient for people who want to stay fully anonymous.

VPN is great for people who work from home. It creates a secure tunnel between the employee from home and to the work network.

**VPN Protocols**

VPN protocols provide security to devices when the connected network cannot provide it. Several protocols can be used to securely encrypt the data including:

* IP Security (IPsec)
* Secure Sockets Layer (SSL) and Transport Layer Security (TLS)
* Point-to-Point Tunneling Protocol (PPTP)
* Layer 2 Tunneling Protocol (L2TP)
* OpenVPN

Here are some of the benefits for VPN:

* Users can hide their IP
* Provides secure encrypted connection
* Bypass geo-blocked content

On the other hand, there are some challenges for VPN as well:

* Not all devices support VPN
* Trusted VPNs are more likely to be the paid ones
* VPN slows down the internet speed

#### **Security Onion**

Security onion is an open-source platform for Network Security Monitoring (NSM). It gathers threat hunting tools such as Playbook, Suricata, Kibana, Elasticsearch, Logstach, Zeek, and Wazuh.

It has been downloaded by over 2 million and is being used by security teams around the world to monitor and defend their assets (*About — Security Onion 2.3 Documentation*, 2021).

**Security Onion Console**

Security Onion Console is the first thing you see when you successfully log into the dashboard.

It includes Alerts section that show the alerts coming from the NIDS(Suricata) and HIDS(Wazuh).

A screenshot of a computer

Description automatically generated

**Dashboards & Hunts** visualize the threats and specify which service created the alert.

Alerts, Dashboard, and Hunts are places to go through all the alerts. Once the user finds something unusual and deserves to be analyzed, they will send the alert to **Cases**.

**Cases** is the case management interface that consists of the threats that were escalated. Other analysts can collaborate to overcome the issue.

**CyberChef**

CyberChef allows to decode, decompress, and analyze artifacts.

**Playbook**

Playbook allows to create a Detection Playbook. These plays are self-contained and describe the different aspects around the alerts.

Users can select which alerts they want to see depending on group by option

Graphical user interface, text, application

Description automatically generated

Conclusion

In conclusion, to configure a network, network engineers implement methods that help the packets to choose the best route for production efficiency. They also need to configure the routers/switches to deal with the packet depending on what is it exactly. I also discussed VPN because it is getting more popular these days.

## What is automation and programming in the CCNA?

#### **Automation**

Network automation is the process of automating networks to reduce the human-to-machine interactions.

Automation saves time by providing Zero Touch Provisioning (ZTP) to configure networks automatically without having to do it manually. While the traditional networking, configuring networks is done by using SSH to the command line for one device at a time which can be time consuming.

There are multiple ways to automate networks, such as Python scripts, Cisco DNA Center (Dan, 2022).

#### **API**

What is API?

Application Programming Interface (API) is software that connects between information user and information provider. For instance, when a user inputs a ZIP code in a map application, that is considered a user input, it needs a software that sends this input to the information provider (Backend) and return a response (*What Is a REST API?*, 2022).

#### **JSON**

JavaScript Object Notation (JSON) is a format that represent structured data following the JavaScript object’s syntax. It is most used to transmit data in web applications.

JSON structures its data like the following example:

{

“name”: “Mohammed”,

“age”: 22,

“active”: true,

“birthYear”: 2000,

}

It depends on the data that needs to be represented. However, I provided a basic JSON object (*Working With JSON - Learn Web Development | MDN*, 2022).

# **Personal Reflection**

This research helped me to understand so many networking concepts that I always wanted to know about. I did not come from a networking background, once I studied networking stuff this semester, I decided that this is what I want to spend so much time learning. All I knew about networking was IP address and TCP/UDP protocols. However, this project gave me a better insight about how the internet works. The usage of DOT framework helped me to cover the sub questions with good understandings. Cisco Packet Tracer helped me to apply my networking skills into something more realistic and practical. My future plan is to read books about the CCNA to finalize the steps toward taking the exam.

# **References**

* BasuMallick, C. (2022, April 18). *TCP vs. UDP: Understanding 10 Key Differences*. <https://www.spiceworks.com/tech/networking/articles/tcp-vs-udp/>
* *Computer Network Topologies - javatpoint*. (n.d.). www.javatpoint.com. <https://www.javatpoint.com/computer-network-topologies>
* NetworkChuck. (2020a, August 6). *REAL LIFE example!! (TCP/IP and OSI layers) // FREE CCNA // EP 4*. YouTube. https://www.youtube.com/watch?v=3kfO61Mensg
* Techopedia. (2017, July 18). Subnetting. Techopedia.com. <https://www.techopedia.com/definition/28328/subnetting>
* ITProTV. (2022). <https://app.itpro.tv/login/?redirect_to=%2Fcourse%2Fcisco-ccna-200-301-2022%2Fperforming-class-c-ipv4-subnetting>
* Slattery, T., & Burke, J. (2022, June 3). *VLAN (virtual LAN)*. Networking. <https://www.techtarget.com/searchnetworking/definition/virtual-LAN>
* *Cisco Packet Tracer*. (2022, June 17). Networking Academy. <https://www.netacad.com/courses/packet-tracer>
* *What is the network layer? | network vs. internet layer - cloudflare*. (2022). Retrieved December 20, 2022, from <https://www.cloudflare.com/learning/network-layer/what-is-the-network-layer/>
* *LAN Switching with Redundant Links*. (2022). NetworkAcademy.io. <https://www.networkacademy.io/ccna/ethernet/an-switching-redundant-links>
* CertBros. (2017, August 29). *Spanning Tree Protocol Explained | Step by Step*. YouTube. <https://www.youtube.com/watch?v=japdEY1UKe4>
* Sheldon, R. (2021, August 9). *Spanning Tree Protocol (STP)*. Networking. <https://www.techtarget.com/searchnetworking/definition/spanning-tree-protocol>
* *Wireless LAN Controller (Wireless AC) Explained | FS Community*. (2021). Knowledge. <https://community.fs.com/blog/wireless-lan-controller-explained.html>
* Ghimiray, D. (2022, December 20). Wi-Fi Security: WEP vs WPA or WPA2. Retrieved December 21, 2022, from <https://www.avast.com/c-wep-vs-wpa-or-wpa2>
* *Network Address Translation Definition | How NAT Works | Computer Networks | CompTIA*. (2022). Default. <https://www.comptia.org/content/guides/what-is-network-address-translation>
* Sumo Logic, Inc. (2021, October 14). *What is syslog?* Sumo Logic. <https://www.sumologic.com/syslog/>
* Burke, J. (2015, May 29). *OSPF (Open Shortest Path First)*. Networking. <https://www.techtarget.com/searchnetworking/definition/OSPF-Open-Shortest-Path-First>
* GeeksforGeeks. (2022, December 20). *Key Security Concepts*. <https://www.geeksforgeeks.org/key-security-concepts/>
* *What is a REST API?* (n.d.). <https://www.redhat.com/en/topics/api/what-is-a-rest-api>
* *Working with JSON - Learn web development | MDN*. (2022, September 25). <https://developer.mozilla.org/en-US/docs/Learn/JavaScript/Objects/JSON>
* Dan. (2022, December 18). *What is Network Automation and why we need it?* Study CCNA. Retrieved January 7, 2023, from <https://study-ccna.com/network-automation-overview/>
* *Methods - ICT research methods*. (2020). <https://ictresearchmethods.nl/Methods>
* *About — Security Onion 2.3 documentation*. (2021). <https://docs.securityonion.net/en/2.3/about.html>