



**FACULTY OF SCIENCE AND TECHNOLOGY**

**COURSEWORK FOR BSC (HONS) INFORMATION TECHNOLOGY (NETWORKING / CNS); YEAR 2,3**

**ACADEMIC SESSION DEC 2018; SEMESTER 4,8**

**NET3207: Network Management**

**DEADLINE: 10 December 2023 5:00pm**

Student Name	Student ID
Suhail Dorasamy	20020574
Nidal Bencheikh Lehocine	19097617
Elena Khoo Sze Kay	21012570
Dharshaan A/L Segaran	20029997
Tasha Hong Ruen Lin	21017561
Abdul Rahman Fedda	18112920

**INSTRUCTIONS TO CANDIDATES**

This assignment will contribute 20%+10% to your final grade.

- This coursework is a group assignment (5 students per group).

**IMPORTANT**

~~The University requires students to adhere to submission deadlines for any form of assessment.~~

Penalties are applied in relation to unauthorized late submission of work.

Courseworks must be submitted on their due dates. If a coursework is submitted after its due date, the following penalty will be imposed:

- ONE day late : 5 % deducted from the total marks awarded.
- TWO days late : 10 % deducted from the total marks awarded.
- THREE : 15% deducted from the total marks awarded.
- 1 week more days late : Assignment will not be marked and 0% will be awarded.

**Lecturer's Remark** (Use additional sheet if required)

I..... (Name) .....std. ID received the assignment and read the comments..... (Signature/date)

**Academic Honesty Acknowledgement**

"I Suhail, Nidal, Elena, Dharshaan, Tasha, & Abdul (student name). verify that this paper contains entirely my own work. I have not consulted with any outside person or materials other than what was specified (an interviewee, for example) in the assignment or the syllabus requirements. Further, I have not copied or inadvertently copied ideas, sentences, or paragraphs from another student. I realize the penalties (*refer to page 16, 5.5, Appendix 2, page 44 of the student handbook diploma and undergraduate programme*) for any kind of copying or collaboration on any assignment."

***Suhail, Nidal, Elena, Dharshaan, Tasha, & Abdul / 6 December 2024***

(Student's signature / Date)

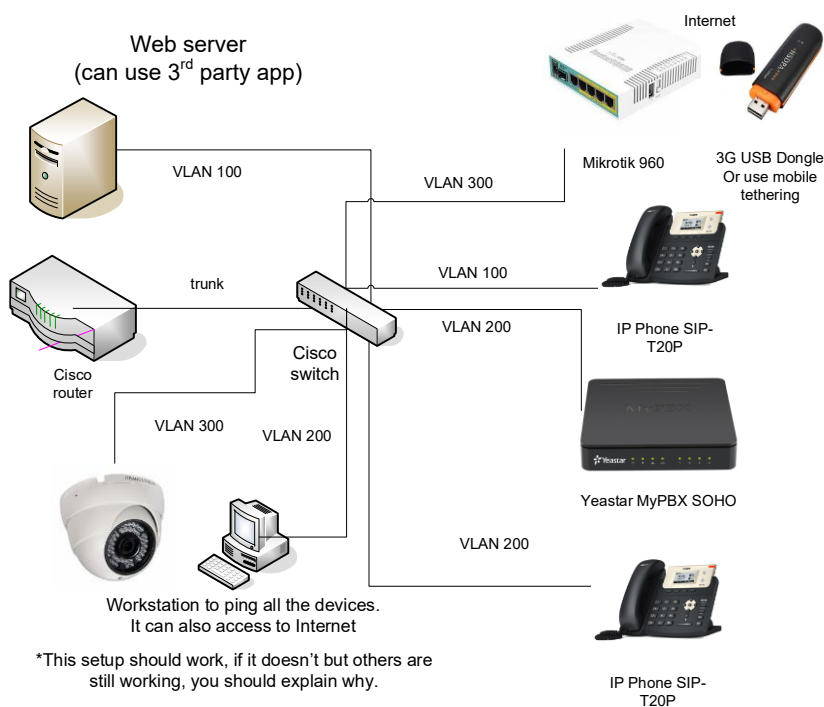
## Table of Contents

Overview .....	4
PBX Server & IP Phones .....	6
Overview .....	6
Implementation Details.....	6
Preparation for configuration .....	6
PBX Network Configuration .....	7
Create and configure extensions .....	9
IP Phone Registration .....	11
Configuration Challenges and Workarounds .....	14
Router.....	15
Overview .....	15
Implementation Details.....	18
DHCP Provisioning .....	18
Auto Start.....	21
Configuration Challenges and Workarounds .....	22
Switch .....	23
Overview .....	23
Implementation Details.....	23
Configuration Challenges and Workarounds .....	28
CCTV .....	29
Overview .....	29
Implementation Details.....	29
MikroTik Router .....	37
Overview .....	37
Implementation Details.....	37
Configuration Challenges and Workarounds .....	43
Web Server.....	45
Overview .....	45
Implementation Details.....	45
Configuration Challenges and Workarounds .....	49
VLAN and Trunk Features.....	49
Overview .....	49
Implementation Details.....	50
Configuration Challenges and Workarounds .....	51
Lessons Learnt.....	52

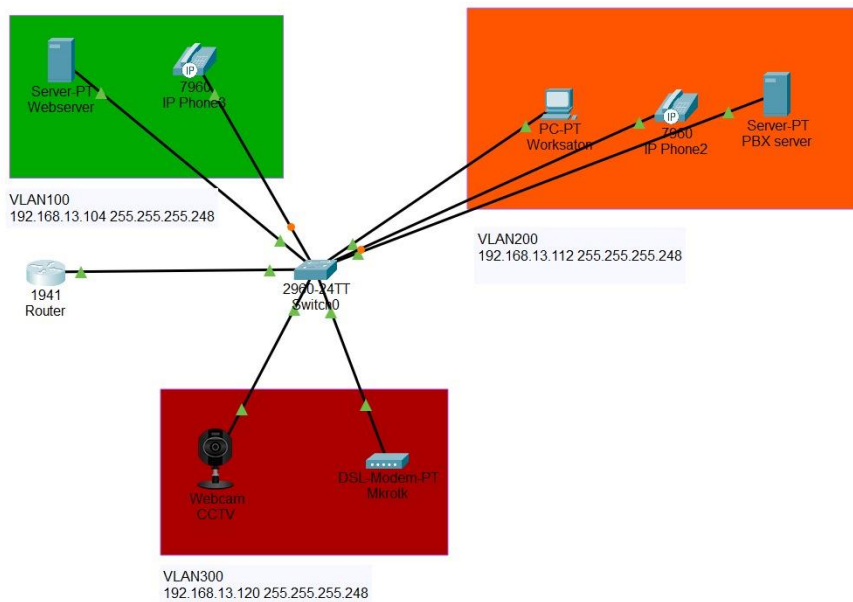
## **APPENDIX A**

### Overview

In this assignment, our group consisting of 6 members was given the task to configure a Local Area Network (LAN) which includes multiple VLANs and network components. The setup includes a Mikrotik router with internet access through a 3G USB dongle, a workstation, IP phones which are connected to a PBX server and a web server which can be hosted by a third party. Along with this, configurations of the VLANs to segment the network: VLAN 100 for the web server, VLAN 200 for the IP phones and the PBX server while VLAN 300 is for the CCTV and the Mikrotik router. The establishment of a trunk link between the Cisco router and switch to allow inter-VLAN communications is also done to ensure that the workstation would be able to ping all devices, access the internet and reach the web server. The network topology can be illustrated in Figure 1 below, outlining the structure of this assignment.



**Figure 1: Network Topology**



**Figure 2: Group 13's Network VLANs and subnets**

The devices required for this assignment include:

- 1 Cisco Catalyst 2960 Plus Switch
- 1 Cisco Router
- 1 Yeastar MyPBX SOHO Server
- 2 YeaLink SIP-T20P IP Phones
- 1 Mikrotik 960
- 1 3G USB Dongle
- 1 PC
- 1 CCTV Grandstream
- 1 3G LTE USB Dongle
- RJ-45 Ethernet Cables

## PBX Server & IP Phones

### Overview

PBX server, which stands for Private Branch eXchange, is a hardware system which manages the switching of incoming and outgoing phone calls between users on local lines such as a business location and a telephone network. This allows the PBX server to split a single phone line into different private lines which are identified by extensions which are usually assigned as 3- or 4-digit numbers.

A PBX system has a few main call processing duties which include establishing connections between phone sets of 2 users, disconnecting a connection following users' requirements, and maintaining connections if the user requires. A PBX server relies on a physical hardware box. This device is normally installed, stored and maintained typically on every employee's desk in the office. The phone lines are connected straight to the box and the box routes the calls to each desk via extension set in the office. This assignment requires the use and configurations to be done on a Yeastar MyPBX SOHO Server.



**Figure 3: Yeastar MyPBX SOHO Server**

### Implementation Details

#### *Preparation for configuration*

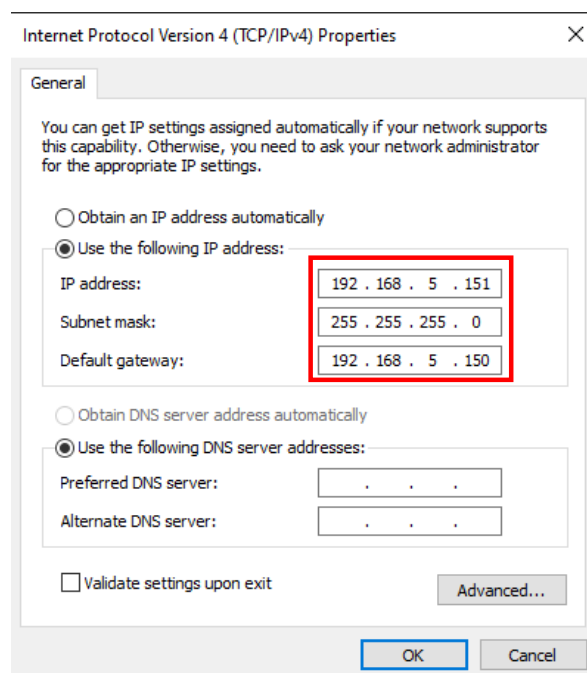
To begin the configuration of our devices, ensure that the PBX server and IP phones are powered on. Due to the possibility of other groups configurations still being present on the devices, factory reset them before adding the new configurations.

For the PBX server, press and hold on the reset button, located at the back of the device near the LAN and power port, until the indicator lights on the front of the device flash orange. To reset the IP phones, navigate to the advanced settings menu using the phones keypad. Once in the advanced settings menu, navigate down to the factory reset option and confirm our choice to factory reset the device. The phones will now reset themselves.

During this reset process, connect the devices to the network using ethernet cables. While the IP phones can be connected to the switch at this stage, our PBX server must first have its network settings configured by directly connecting it to our workstations LAN port.

### *PBX Network Configuration*

After the device has been reset, begin to configure its network settings so that it has a static IP address which will be used by the IP phones for auto provisioning and by the workstation to access the PBX server for further configuration and monitoring. After connecting the PBX server's LAN port to the workstation ethernet port using an ethernet cable, configure the workstation's IP address so that it is on the same network as the server's default IP address. This is necessary as we will use the server's IP address to access its configuration menu later. The server's default IP address is '192.168.5.150/24' so we change our workstation's IP address to be '192.168.5.151'. We also change the workstation's default gateway to be the server's IP address to assist it in finding the web GUI later.



**Figure 4: Changing workstation IP address**

Once the correct static IP address has been assigned to the workstation, access the PBX server's GUI web interface using a web browser. To do this, simply enter the default IP address of the PBX server. If the connection is successful, the web interface will load, allowing access to the PBX server's settings and features. At the login screen, use the default credentials provided: the default username is “admin”, and the default password is “password”. After entering these details, click the "Login" button to proceed to the main dashboard of the PBX server's GUI.

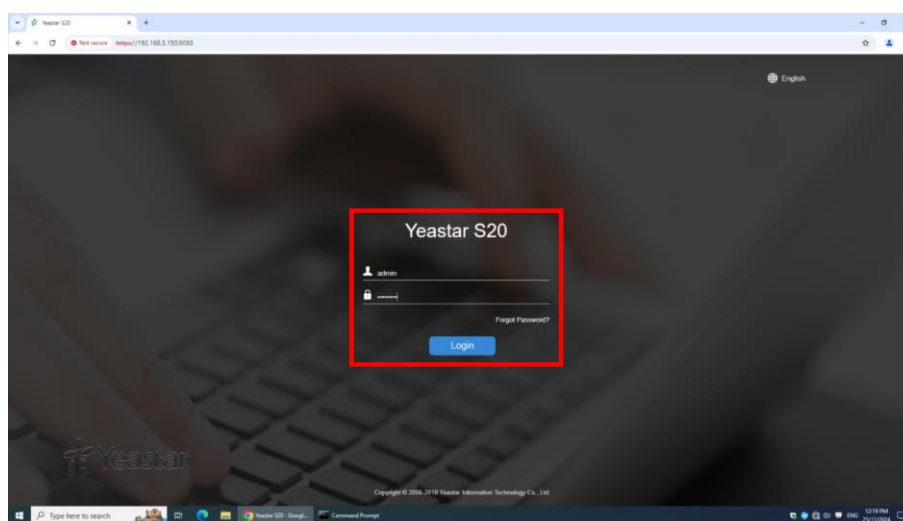


Figure 5: PBX web GUI login page

Next, navigate to “System > Network Preferences > LAN Settings” within the PBX server's web interface to modify the server's subnet configuration. In the LAN Settings, update the IP address of the PBX server to align with VLAN 200's DHCP pool, setting it to “192.168.13.116”.

Following this, the server's default gateway is also to be the configured router sub interface for VLAN 200, 192.168.13.113. After making these adjustments, click “Save” to confirm the changes and then reboot the PBX server. This step was necessary to apply the new configurations and ensure that the PBX server operated with the correct network settings.



The screenshot shows the 'Basic Settings' tab for the PBX configuration. The 'LAN' section is highlighted with a red box, indicating the network configuration. The 'WAN' section is also visible but not highlighted.

Section	Field	Value
LAN	IP Address	192.168.13.116
	Subnet Mask	255.255.255.248
	Gateway	192.168.13.113
	Preferred DNS Server	8.8.8.8
	Alternative DNS Server	
WAN	IP Address	
	Subnet Mask	
	Gateway	

**Figure 6: PBX network configuration**

Now that the PBX server's network configuration is completed, it is possible to connect both the PBX server and the workstation to the switch to continue the configuration and registration of the IP phones. The workstation's IPv4 settings should be changed so that it can automatically obtain an IP address from our configured router, without this change it would not be able to communicate with the PBX server or any other devices on our network.

### *Create and configure extensions*

After ensuring that the workstation is in VLAN 200, revisit the PBX web interface by entering its updated IP address in a web browser. Once the interface loads, navigate to "PBX > FXS/VoIP Extensions". It is important to ensure that any pre-existing extensions are deleted.

The screenshot shows the 'Extensions' tab in the PBX configuration. The table below is empty, indicating no items are defined.

Extension	Name	Type	Port	Edit	Delete
No items defined.					

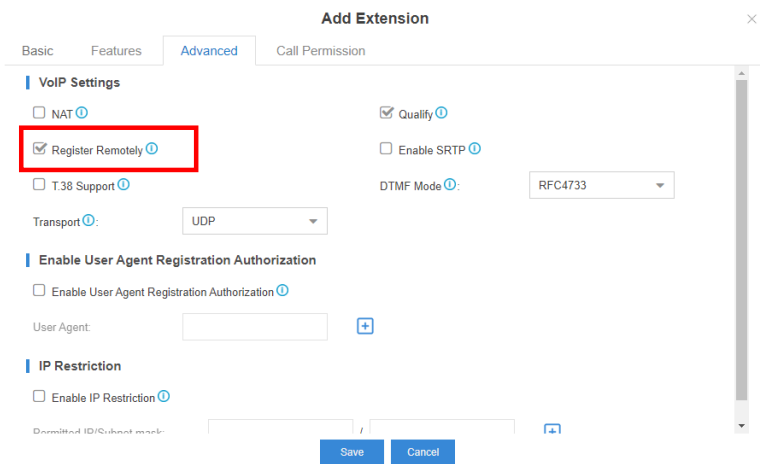
**Figure 7: Delete pre-existing extensions**

Next, add two new extensions for the two IP phones. For setup, use the extension number 1001 and 1002. Since the two IP phones are in different VLANs, VLAN 100 and VLAN 200, additional configuration is required to enable seamless communication between them. To allow both phones to call and ring each other across the VLANs, navigate to “VoIP Settings” and check the “Register Remotely” option.

The image displays two screenshots of the "Add Extension" configuration window, showing the "General" tab. The top screenshot shows the full form with the following values: Type: SIP, Extension: 101, Registration Name: 101, Concurrent Registrations: 2, Caller ID: 101, Caller ID name: Suhail, and Registration Password: [masked]. The bottom screenshot is identical but has a red box highlighting the Extension, Registration Name, and Concurrent Registrations fields.

Field	Value
Type	SIP
Extension	101
Registration Name	101
Concurrent Registrations	2
Caller ID	101
Caller ID name	Suhail
Registration Password	[masked]

Figure 8: Create new extension



**Add Extension**

Basic Features **Advanced** Call Permission

**VoIP Settings**

☐ NAT [?](#)

☒ **Register Remotely** [?](#)

☐ T.38 Support [?](#)

Transport [?](#): UDP

☒ Qualify [?](#)

☐ Enable SRTP [?](#)

DTMF Mode [?](#): RFC4733

**Enable User Agent Registration Authorization**

☐ Enable User Agent Registration Authorization [?](#)

User Agent:  [+](#)

**IP Restriction**

☐ Enable IP Restriction [?](#)

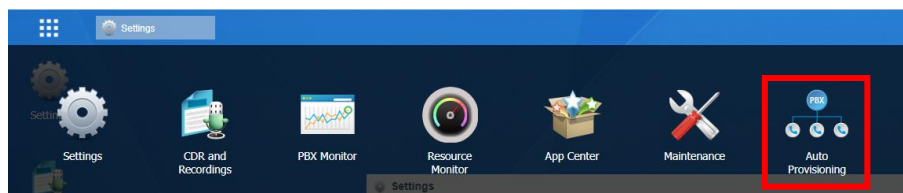
Disallowed IP/Subnet mask:  [+](#)

Save Cancel

**Figure 9: Select register remotely for newly created extension**

### IP Phone Registration

After creating the extensions for the IP phones, assign each extension to its respective IP phone. This was done by navigating to “PBX > Extensions > Auto Provisioning” in the PBX web interface.



**Figure 10: Auto provisioning in PBX web GUI**

Here click “Scan”, and the PBX server should automatically find the IP phone that is within the same VLAN as the server. Then assign extension 1001 to Line 1 of this phone. For the phone that is in a different VLAN, VLAN 100, it is necessary to manually register this phone using its MAC address which can be found on the label on the back of the phone. Extension 1002 is registered to Line 2 of this phone.

To ensure that the IP phones are correctly registered it is important to add the IP address of the PBX server under the auto provisioning option on each IP phone. To do this navigate settings > advanced settings > auto provisioning. Here type out the IP address of our server.

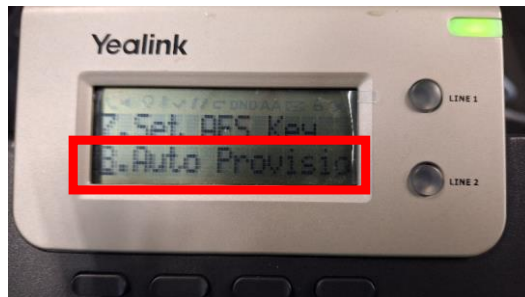


Figure 11: Auto provisioning setting

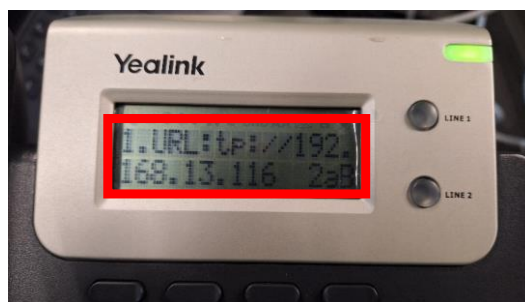


Figure 12: Entering IP address of PBX server

Then reboot the IP phones, and it should now be successfully registered with the correct extensions. The status of each phone should also be viewable on the web GUI.

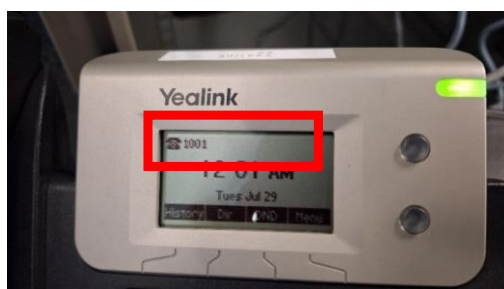
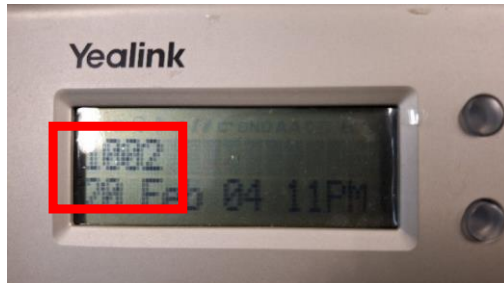


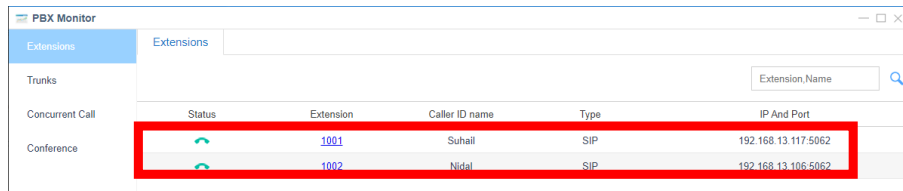
Figure 13: IP phone 1 registered successfully



**Figure 14: IP phone 2 registered successfully**



**Figure 15: IP phones in call with each other**



Status	Extension	Caller ID name	Type	IP And Port
Available	1001	Suhail	SIP	192.168.13.117:5062
Available	1002	Nidal	SIP	192.168.13.106:5062

Figure 16: IP phones status (Available)



Status	Extension	Caller ID name	Type	IP And Port
In call	1001	Suhail	SIP	192.168.13.117:5062
In call	1002	Nidal	SIP	192.168.13.106:5062

Figure 17: IP phone status (In call)

## Configuration Challenges and Workarounds

When setting up the PBX server and two IP phones, I ran into an issue with one of the IP phones that was placed in VLAN100, which was different from the VLAN where the PBX server was located. The phone wouldn't automatically receive its assigned extension or register with the PBX server, likely due to the VLAN setup causing some communication problems. To get it working, I had to manually reboot the phone and unplug its Ethernet cable during the reboot. This process made sure it could properly connect and register with the server.

**Commented [SD1]:** Potential points:  
 - IP phone in VLAN100 required manual reboot + unplugging the ethernet cable during reboot in order for it to receive the extension and be registered.

# Router

## Overview

A router is a type of connective device that connects two or more packet-switched networks or subnetworks. There are two functions which are the primary functions of having a router. It works to manage traffic between the networks by forwarding data packets to the IP addresses that are intended to, and also to allow multiple devices to use the same connection. The data is sent from one network to another by ensuring the best path is chosen for the data packet to reach its destination. There are many types of routers whereby each works differently suited to different network needs and environments. The types of routers include Wireless Routers, Wired Routers, Core Routers, EdgeRouters, Virtual Routers, and Distribution Routers.



**Figure 18: Cisco Router**

A router has multiple components in it which makes it a functionally reliable and offers high availability. The components are categorised in to two parts; External Components and Internal Components. Internal components of a router consists of Central Processing Unit (CPU), Read Only Memory (ROM), Flash, Non-Volatile RAM (NVRAM), Random Access Memory (RAM), Interfaces/ ports. The external components on the other hand consists of WAN Port, LAN Port, and Admin Port.

The CPU is an important component of a router. It is responsible for managing its internal operations. It processes algorithms, such as Dijkstra or DUAL, to ensure efficient routing decisions. The CPU communicates with the router's hardware through IRQs, interprets

configuration files, and processes data packets. Additionally, it oversees and regulates all of the router's interfaces. Similar to a computer's BIOS chip, a router contains a component that stores the bootstrap program, essential for loading its operating system. In Cisco router, this operating system, known as Cisco IOS, is stored in a separate component called Flash. Flash memory stores the router's operating system and retains its data even when the router is powered off or restarted. Upon startup, the operating system is loaded from flash memory into RAM for operation. Non-volatile random-access memory (NVRAM) retains data even after the router is powered off. It stores the router's startup configuration, making it a permanent memory for saving configurations.

To preserve changes through a reboot, the running-config must be saved as a startup-config in NVRAM. Unlike ROM, which contains fixed, unchangeable data, NVRAM allows modifications. When powered on, the router retrieves its initial configuration from NVRAM. The function of RAM is just like a PC RAM. It is used to store and retrieve data temporarily. As volatile memory, it requires constant power and all stored data is lost when the router is powered off or restarted. Upon startup, the router loads its configuration file and IOS into RAM. Temporary configurations like running-config are stored by RAM. It can be viewed by using the command *show running-config*. To save these configurations permanently, they must be written to NVRAM using the *write* command.

Routers have many interfaces for wired connections like Ethernet, Fast Ethernet, Gigabit Ethernet, or Serial. Each interface is uniquely identified by a name and number in the router's configuration. Interfaces can also be assigned to VLANs or sub-interfaces to manage and segment network traffic.

The external components of a router consist of its ports, categorized into LAN ports, WAN ports, and Admin ports. The WAN port connects the router to a Wide Area Network (WAN), typically the Internet. The LAN port links the router to the Local Area Network (LAN), often through a switch. The admin port is used for configuring or managing the router, usually via HyperTerminal or similar applications. These external ports enable the router to interact with various networks and facilitate its administration.







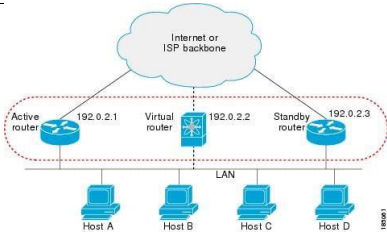
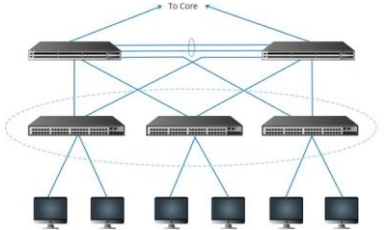
Image Of Router	Router Name
	Wireless Router
	Wired Router
	Core Router
	EdgeRouter
	Virtual Router
	Distribution Router

Table 1: Types of routers

## Implementation Details

### DHCP Provisioning

To successfully provision DHCP on a router, the basic configurations must be done. The basic configuration begins with *enable configure terminal*. By doing so, it switches the router to give full administrative access. It puts the router in global configuration mode, which allows the user to make any changes system-wide, which also includes setting up interfaces, DHCP pools and also routing. After that, a unique hostname is assigned which can be useful for environment with multiple routers. It will make it easy to identify the router in a setting where there are multiple routers.

Configuring passwords is another crucial step as only selected few which are also known as privileged users to access the router. After that is the configuration of the interface and VLAN trunking. This step is crucial for environments where many VLANs are used. Routing between the different VLANs is required. This step can be done by creating a sub interface for VLAN100 and then configure the sub interface to tag traffic with VLAN ID 100 using the 802.1Q protocol. An IP address is then assigned to the sub interface, whereby it acts as the default gateway for devices in VLAN 100. This step is repeated for the other VLANs, making sure each VLAN has a unique sub interface, VLAN ID and gateway IP.

The next step is to enable the DHCP service. DHCP service makes sure that the router is ready to take up the role of a DHCP server. The DHCP server is enabled by default, but the command *service dhcp* ensures that it is explicitly active if it happened to be disabled previously. DHCP also allows the router to assign IP addresses dynamically to devices in each VLAN. Next step is to exclude the addresses from DHCP allocation. The command *ip dhcp excluded-address* is used to prevent specific IP addresses from being assigned dynamically by the DHCP server. The reserved IPs are mostly used for critical devices such as default gateways, servers, or printers that require static IPs. The last step is to save the configuration with the command *write memory*.

```

ip dhcp excluded-address 192.168.13.105
ip dhcp excluded-address 192.168.13.113
ip dhcp excluded-address 192.168.13.121
!
ip dhcp pool VLAN100
network 192.168.13.104 255.255.255.248
default-router 192.168.13.105
dns-server 8.8.8.8
!
ip dhcp pool VLAN200
network 192.168.13.112 255.255.255.248
default-router 192.168.13.113
dns-server 8.8.8.8
!
ip dhcp pool VLAN300
network 192.168.13.120 255.255.255.248
default-router 192.168.13.121
dns-server 8.8.8.8

```

**Figure 19: Excluded address and DHCP pool for each VLAN**

This configuration shows the DHCP provisioning for three different VLANs which are VLAN100, VLAN200, and VLAN300. The excluded addresses listed are 192.168.13.105, 192.168.13.113, and 192.168.13.121. These excluded addresses are usually reserved for default gateways or other critical network devices like servers and printers. This step is crucial to ensure that the IPs are not assigned to client devices by accident. It also avoids conflicts with static IP configurations.

A DHCP pool named VLAN100 was created. The function of pool is to act as a logical group of settings used to assign IP addresses dynamically to devices in VLAN100. The network which is 192.168.104/29 with subnet mask 255.255.255.248 offers 6 usable IP addresses from 192.168.13.105 to 192.168.13.110.

The broadcast address, which is 192.168.13.111, is also reserved. The default gateway for devices in VLAN100 is set to 192.168.13.105. This allows the IP to correspond to the router's sub interface for VLAN100. Google's public DNS server is set at 8.8.8.8 to resolve domain names to IP addresses. This step is repeated for both VLAN200 and VLAN300.

In a nutshell, DHCP provisioning works by assigning dynamic IP addresses where a device in any set VLAN, (100, 200, 300) can connect to the network. Following up, DHCP is requested to the router. The router will then respond with any available IP address from the corresponding VLAN's DHCP pool together with the default gateway and DNS server.

The IPs that are excluded will not be assigned to any clients. It ensures that those IP addresses are reserved for routing purposes. And then, all VLANs will use the same DNS server, which is 8.8.8.8, for name resolution. However, the VLANs will have different and unique subnets and gateways, which maintains the logical separation of traffic.

VLAN	SUBNET	USABLE IPs	DEFAULT GATEWAY	BROADCAST ADDRESS
VLAN100	192.168.13.104/29	192.168.13.106–110	192.168.13.105	192.168.13.111
VLAN200	192.168.13.112/29	192.168.13.114–118	192.168.13.113	192.168.13.119
VLAN300	192.168.13.120/29	192.168.13.122–126	192.168.13.121	192.168.13.127

**Table 2: Network table**

```
interface GigabitEthernet0/0
  no ip address
  duplex auto
  speed auto
!
interface GigabitEthernet0/0.100
  encapsulation dot1Q 100
  ip address 192.168.13.105 255.255.255.248
!
interface GigabitEthernet0/0.200
  encapsulation dot1Q 200
  ip address 192.168.13.113 255.255.255.248
!
interface GigabitEthernet0/0.300
  encapsulation dot1Q 300
  ip address 192.168.13.121 255.255.255.248
!
```

**Figure 20: Configuration for router sub-interfaces**

The purpose of VLANs in a network is to be divided into smaller and isolated sub-networks. As proven, VLANs provide high security and reduce broadcast traffic, however, they cannot communicate with each other directly. Inter-VLAN routing enables communication between different VLANs. Router-on-a-Stick is a technique that uses a single physical interface on the router with sub interfaces configured for each VLAN. Each sub interface is a gateway for its respective VLAN.

**Interfaces GigabitEthernet0/0** show the physical interface which connects the router to the switch. Any IP addresses are removed from the interface as it will act as a parent interface for sub interfaces via the command **no ip address**, **duplex auto** and **speed auto** configure the interface to negotiate the appropriate speed and duplex settings. It ensures compatibility with switches that are connected to it.

The sub interface configuration is important as it handles all the traffic for VLAN100 and makes sure the devices in that VLAN are able to communicate with other VLANs via the router. VLAN200 sub interface enables the router to manage the traffic for VLAN200 and accommodate communication with other VLANs. As for VLAN300 sub interface, it routes the traffic to VLAN300 and enables communication with devices in other VLANs.

Trunking works by connecting the physical interface which is the GigabitEthernet0/0 to the switch, which serves as a trunk link. Trunk links are links that carry multiple traffic for multiple VLANs. It tags packets with VLAN IDs by using 802.1Q encapsulation protocol. The sub interfaces on the router are then configured to handle the traffic for a specific VLAN. Tagging of outgoing packets with appropriate VLAN ID is done and it expects incoming packets to have the corresponding tag. Each sub interface is then assigned an IP address. It serves as the default gateway for devices in that VLAN. Lastly, when a device in VLAN100 sends a packet to a device in VLAN200, the packet is then sent to the router via the trunk link. The router then identifies the VLAN based on the tag. After that, it forwards the packet to the appropriate sub interface. The router then routes the packet to the sub interface corresponding to VLAN200 and forwards it back to the switch.

## Auto Start

```
Router#copy running-config start
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Figure 21: To save configurations of router

By running the command “*copy-running-config startup-config*”, the router running configuration can be saved. Upon the router configuration, it is always important to save the settings, so that the configuration is always backed up. In case of router shutdown or reboot, due to any reason, the configurations will not be saved to the latest amendment. The command “*running-config*” has all the router settings stored in volatile RAM, which are lost when the devices lose power. To ensure there is no data loss, these configurations are required to be saved to “*startup-config*” in non-volatile NVRAM, making sure that they are persistent even when there are power outages.

### Configuration Challenges and Workarounds

There were no major challenges faced during the configuration of the router. The only challenge of note was to determine the correct IP address and subnet masks to use within our network to ensure that all 3 of our VLANs would be able to use 192.168.13.x IP addresses.

**Commented [SD2]:** Potential points:  
- IP phone in VLAN100 required manual reboot + unplugging the ethernet cable during reboot in order for it to receive the extension and be registered.

## Switch

### Overview

A network switch is a device used for interconnecting devices in the LAN. The switch forwards data packets to the device intended to receive it based on their physical addresses (MAC addresses). Network switches often operate on the OSI layer 2 or 3 (data link or network layer). Most layer 2 switches use the destination MAC address whereas layer 3 switches use destination IP addresses to forward data. Layer 2 switches are more common and use Ethernet cables to connect devices to the network. A MAC address is a permanent ID used for each piece of hardware and does not change. This assignment requires performing configurations on the Cisco Catalyst 2960 Plus Series switch. The following implementation details section will showcase the process of configuring the Cisco switch to trunk links, access ports, and VLANs while being able to start automatically after rebooting. The following implementation details document how the switch was configured to create VLANs and modify the access ports and trunk ports for all devices on the network topology.



Figure 21: Cisco Catalyst 2960 Plus Switch

### Implementation Details

#### Initial Configurations

Firstly, console it into the switch using the console port at the back of the switch.



Figure 22: Console port of switch

Once connected, go over to the putty terminal and initialize the switch, the most important step is to delete the previous configurations. To do that, enable the switch and use the “show flash” command and look for the vlan.dat file, delete it using the “delete vlan.dat” command. Next, is to erase any saved configurations, this is done using the “erase startup-config” this will ensure and clean switch ready to be configured. Reload once this is done and perform router configurations.

Commented [NB3]: ADD SCREENSHOT FOR THE RESET

```
Switch>en
Switch#show flash

Directory of flash:/

   2  -rw-    1736  Mar 1 1993 01:02:25 +00:00  config.text.renamed
   3  -rw-    1400  Mar 1 1993 00:12:55 +00:00  express_setup.debug
   4  -rw-    2291  Mar 2 1993 05:54:59 +00:00  startup-config
   5  drwx     192  Mar 1 1993 00:07:28 +00:00  c2960-lanbasek9-mz.150-2.SE8
   6  -rw-     736  Mar 1 1993 00:03:45 +00:00  vlan.dat
591  drwx      64  Mar 1 1993 00:11:44 +00:00  dc_profile_dir
590  -rw-    1919  Mar 1 1993 01:02:25 +00:00  private-config.text.renamed
592  -rw-     1730  Mar 1 1993 00:01:05 +00:00  config.text.old2
593  -rw-   17432  Mar 1 1993 01:54:59 +00:00  multiple-fs
594  -rw-     4608  Mar 1 1993 05:39:09 +00:00  startup-cofig

65544192 bytes total (49477120 bytes free)
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
Switch#delete start
Switch#delete start-
Switch#delete startup
Switch#delete startup-config
Delete filename [startup-config]?
Delete flash:/startup-config? [confirm]
```

Figure 23 – Commands to delete previously made VLANs and startup configs

```
Switch#reload
Proceed with reload? [confirm]

*Mar 1 00:35:38.532: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload command.
```

Figure 24: Reloading switch after deleting previous configuration

After configuring the router, connect the devices to the switch using the switch ports. Switch ports are layer 2 (data link) interfaces with the purpose of carrying layer 2 traffic. For switch ports, individual ports are allowed to carry a single VLAN traffic. Devices connected to the switch ports are assigned the VLAN 1 by default. VLAN 1 cannot be deleted since it is often relied on by the management traffic. There are 2 forms of ports in a VLAN environment, access ports and trunk ports. Similarly, access ports carry only one VLAN traffic of the VLAN they are assigned to. Trunk ports carry more than one VLAN traffic. Trunk ports are often used in exchanging traffic from multiple VLANs to the other devices connected. The table below shows how each device is connected to the switch and the VLANs each device uses.



Port number	Device	VLAN
f0/1	Web Server	100
f0/2	IP Phone 1	100
f0/3	IP Phone 2	200
f0/4	PBX Server	200
f0/5	Workstation	200
f0/6	CCTV	300
f0/7	MikroTik	300
F0/24 - G0/0	Trunk link	

Once the devices are connected to the ports, establish a connection to the switch. The following configurations are done in the switch's CLI on the application PuTTY.

Following this, enable the switch's privileged EXEC mode.

## VLAN Configurations

Once the switch is reloaded, enter the global configuration mode using "configure terminal" and create 3 VLANs (vlan100, vlan200, and vlan300). After all 3 VLANs are created, run the command "exit" to go back to the global configuration mode.

```
Switch(config)#vlan 100
Switch(config-vlan)#name Vlan100
Switch(config-vlan)#vlan 200
Switch(config-vlan)#name Vlan200
Switch(config-vlan)#vlan 300
Switch(config-vlan)#name Vlan300
Switch(config-vlan)#exit
```

Figure 25: VLAN Configuration Table in Network Switch

## VLAN Interfaces and Descriptions

Devices connected to the switch ports should be assigned to the created VLANs according to the topology and table below. In our network topology, the trunk link is not assigned a VLAN.

Port number	Device	VLAN
f0/1	Web Server	100
f0/2	IP Phone 1	100
f0/3	IP Phone 2	200
f0/4	PBX Server	200
f0/5	Workstation	200
f0/6	CCTV	300
f0/7	MikroTik	300

**Table 3: Switch port to device/VLAN table**

Enter the privileged EXEC mode and then the global configuration mode using “configure terminal”. Enter each interface according to the table above using the command “interface F0/x” replace the “x” with the port number. Add a description for each interface so they can be easily recognized during reference. Enable the interfaces using the “no shutdown” command. To configure interfaces to run in the access mode, use the command “switchport mode access” and then for each device allocate their respective VLANs using “switchport access vlan” followed by their VLAN ID. Lastly, exit the interface configuration mode using the “exit” command. Repeat this for every device on the network topology except the trunk link.

```
Switch(config)#interface F0/1
Switch(config-if)#description Web server
Switch(config-if)#no shutdown
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 100
Switch(config-if)#exit
Switch(config)#
Switch(config)#
Switch(config)#interface F0/2
Switch(config-if)#description Phone 100
Switch(config-if)#no shutdown
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 100
Switch(config-if)#exit
Switch(config)#
Switch(config)#
Switch(config)#interface F0/3
Switch(config-if)#description Phone 2
Switch(config-if)#no shutdown
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 200
Switch(config-if)#exit
Switch(config)#
Switch(config)#
Switch(config)#interface F0/4
Switch(config-if)#description PBX server
Switch(config-if)#no shutdown
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 200
Switch(config-if)#exit
Switch(config)#
Switch(config)#
Switch(config)#interface F0/5
Switch(config-if)#description Workstation
Switch(config-if)#no shutdown
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 200
Switch(config-if)#exit
```

Figure 266: Configuration for interfaces F0/1-F0/5

```
Switch(config)#interface F0/6
Switch(config-if)#description CCTV
Switch(config-if)#no shutdown
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 300
Switch(config-if)#exit
Switch(config)#
Switch(config)#interface F0/7
Switch(config-if)#description MikroTik
Switch(config-if)#no shutdown
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 300
Switch(config-if)#exit
```

Figure 27: VLAN Configuration for interfaces F0/6-F0/7

## VLAN TRUNKING:

Trunk ports allow traffic from multiple VLANs to be routed between network devices such as routers and switches on one link. This is done by encapsulating the packets with unique VLAN tags.

For the trunk link between the switch and the router, configure the port f0/24. These configurations are done to allow devices on the different VLANs to communicate with the router, this allows the router to assign ip addresses to the devices based on their respective VLANs. Proceed by giving the interface the description “Trunk link” to make it easier to differentiate devices between each interface. Use the command “no shutdown” to enable the physical interference link. Following this, use the “switchport mode trunk” command in the switch configurations to configure the port to carry traffic for the multiple VLANs.

```
Switch(config)#interface F0/24
Switch(config-if)#description Trunk link
Switch(config-if)#no shutdown
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
```

Figure 28: Configuration of Trunk Link on Interface F0/24

## Auto-start

Finally, save the running configuration file by using the command “copy running-config startup-config” to ensure the configurations are saved and will run upon reboot.

```
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Figure 29: Configurations to copy running and startup configs

## Configuration Challenges and Workarounds

The problems during the switch configuration were not many. The most important problem was the reset of the switch to default settings, which was easy to do but needed to start with clean configurations. Since the configuration followed the standard way of configuration and each step was checked, after the resetting, the setup of the VLANs went on without any hitches. Thus, the network switch was ready to be used with its VLANs appropriately set.

Commented [NB4]: ADD A SCREENSHOT FOR THE COPY RUN START COMMAND

## CCTV

### Overview

A CCTV Camera also known as Closed Circuit Television Camera is a type of surveillance camera which transmits video footage to a closed audience meaning only specific people who are authorized can access and view them. There are various types of CCTV cameras some are analog cameras which is an older system as well as a digital cctv camera also known as IP camera which can be accessed remotely over the internet. The CCTV cameras capture the footage using the camera lens and the captured data gets transmitted via a cable or wirelessly to a device which is used to monitor the camera feed.



**Figure 30: CCTV Camera**

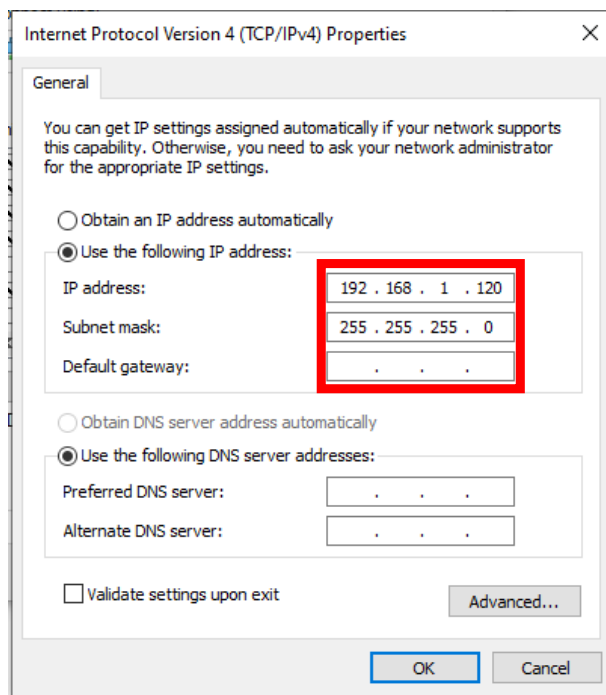
### Implementation Details

To begin our implementation of the CCTV camera, power on the device and connect it via ethernet cable to our workstation's ethernet port; to initially configure the camera, it must be directly connected to the workstation, it will later be connected to the network switch.

Now that it is connected and powered, download the "gs\_search" tool from grandstream's official website. Grandstream being the manufacturer of the CCTV camera. This tool will search our workstations local network for any grandstream devices (i.e our camera) and tell us its IP and mac address. Using this information, access the device's web GUI to configure it.

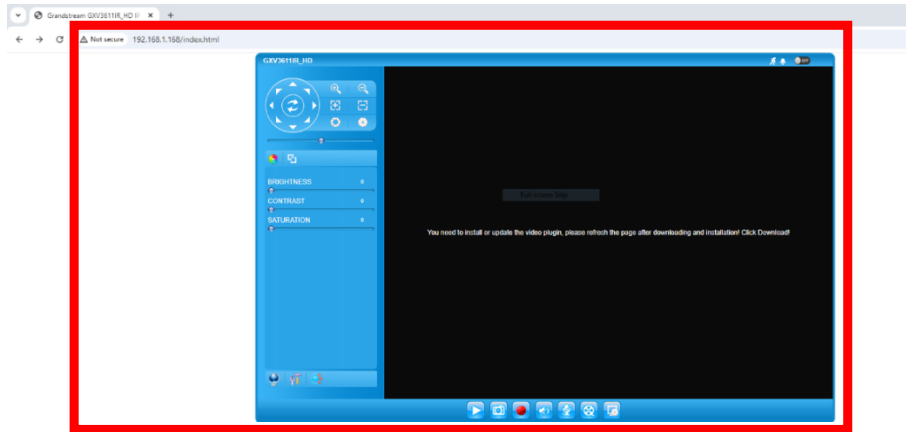
After using the tool, the device's IP address was '192.168.1.168'. Before searching up this IP in the web browser, we first need to configure our workstation's IP address to be within the same network as the camera.

As shown below change our workstation's IP address to '192.168.1.120'.



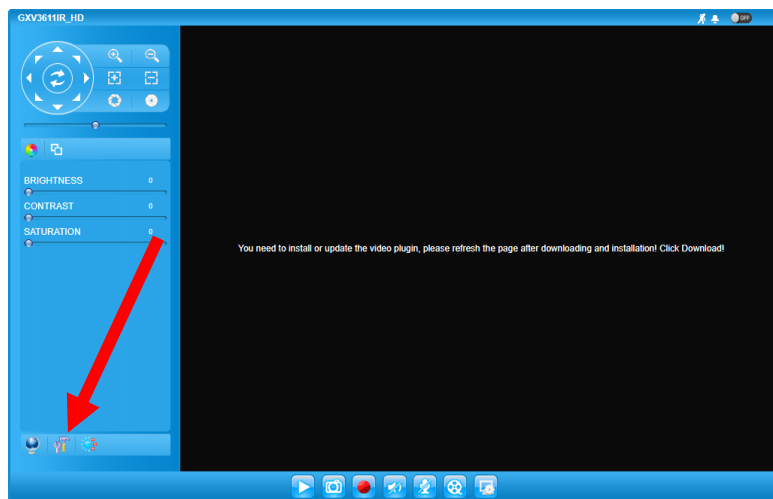
**Figure 31: Workstation IP address change**

Once that is completed, move on to accessing the camera's web GUI by typing in the previously mentioned IP address into our web browser's search bar.

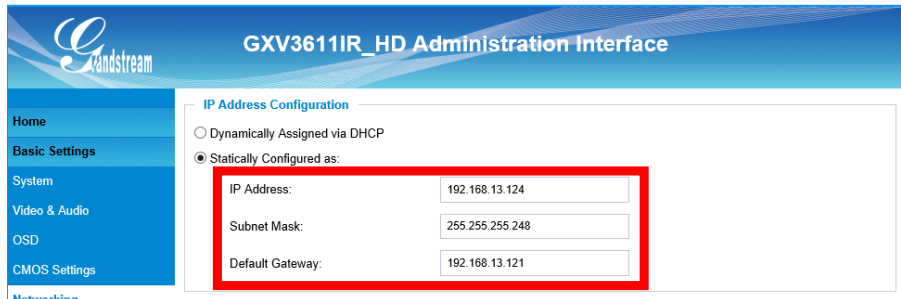


**Figure 32: CCTV camera web GUI**

Now begin configuring the camera's network settings so that it will have a static IP address within the network address range of VLAN 300. Navigate to 'settings > Basic Settings > Networking > IP Address Configuration'. Here set the IP address to "statically configured as:" and set the IP address in the fields below.

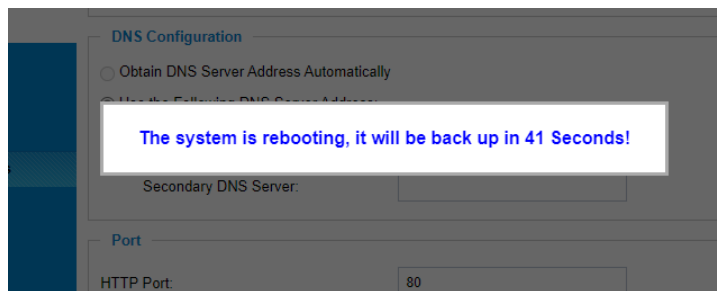


**Figure 33: Access CCTV settings**



**Figure 34: Setting static IP for camera**

Once the network settings for the camera is configured, save the changes and allow the camera to reboot.

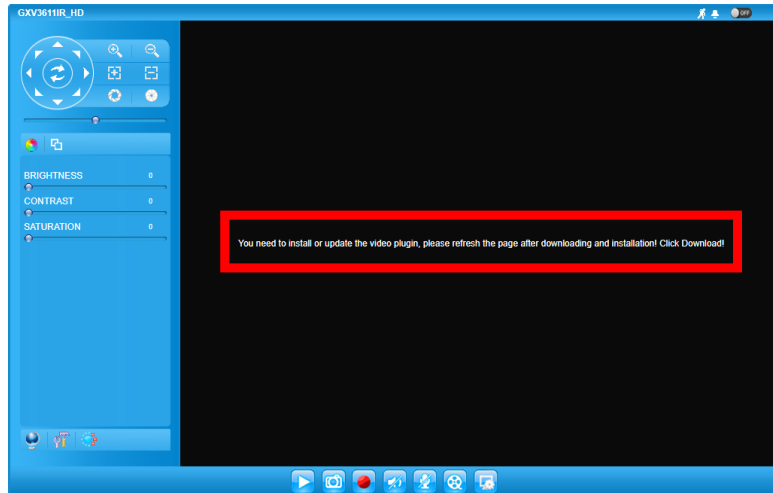


**Figure 35: CCTV rebooting**

After rebooting, proceed to connect the camera to our network via the switch and attempt to access it again via our workstation. The workstation will also be reconnected to the network and receive an IP address via DHCP from the router.

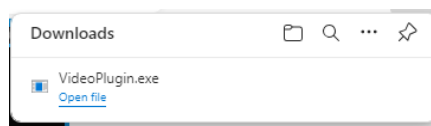


If the configuration is successful, access the web GUI using the new static IP address that was set for the camera.

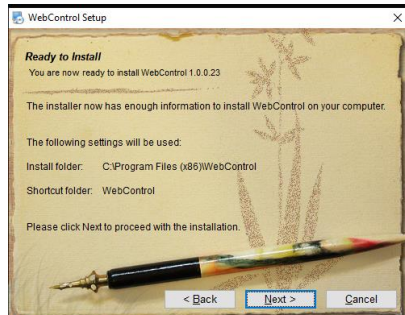


**Figure 36: Web GUI after updating camera network settings**

Now download the video plugin required to receive video output from the camera. This is done by clicking the white text that is present in the main window of the web GUI. Once downloaded, run the executable file and follow the installation prompts to install the video plugin. Once successfully installed, proceed to the final step of the CCTV camera's configuration.



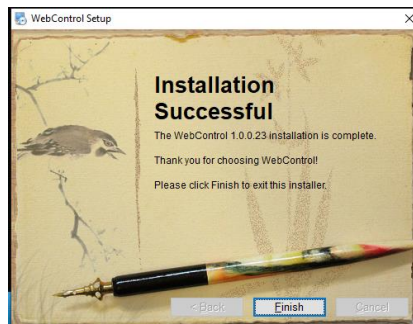
**Figure 37: Web GUI after updating camera network settings**



**Figure 38: Video plugin installation 1**



**Figure 39: Video plugin installation 2**



**Figure 40: Video plugin installation complete**

Lastly, Internet Explorer compatibility options must be enabled. Without completing this step, the web browser will not display any video output from the camera. This is done by going to the settings in Internet Explorer and typing "Internet Explorer" in the search bar to find Internet Explorer Mode (IE Mode). Enable the IE compatibility and add the CCTV camera GUI URL to the trusted sites.

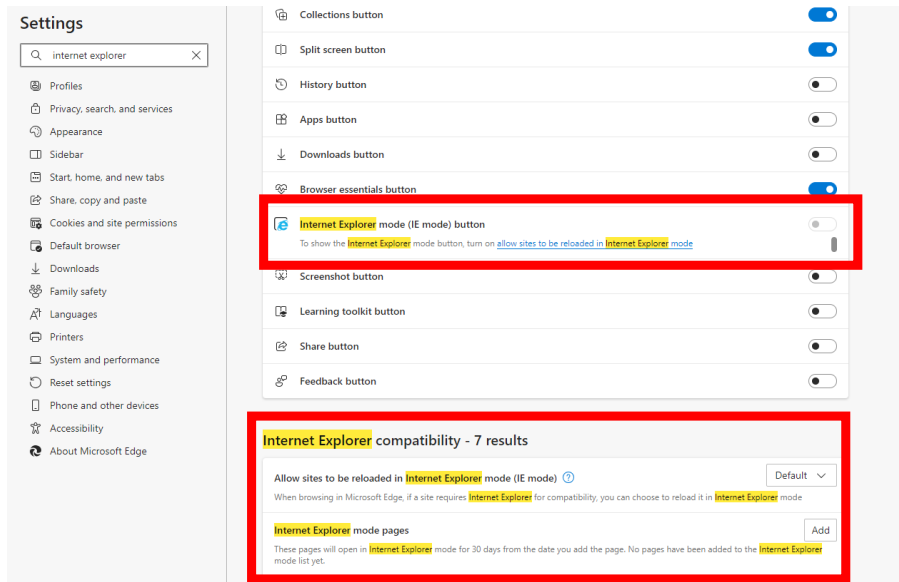


Figure 41: Searching for internet explorer compatibility mode

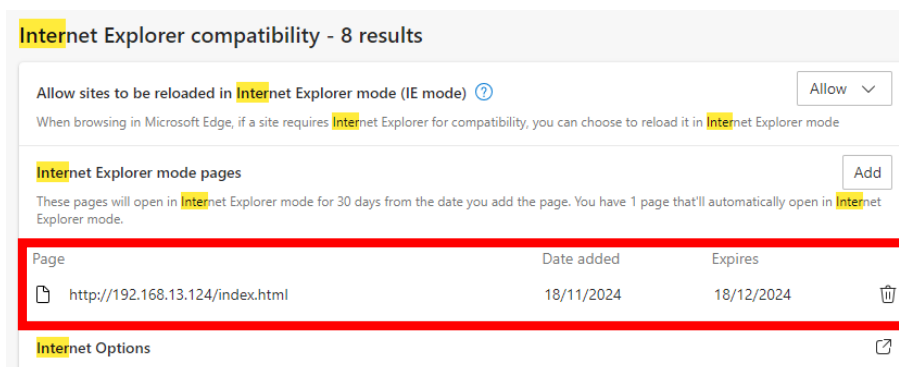


Figure 42: Adding web GUI url to list of trusted sites.

After the site has been added, return to the web GUI and refresh the page. Once the page loads, video output from the camera should now be presented.



Figure 43: Successfully receiving video output from camera

## MikroTik Router

### Overview

Mikrotik routers are developed by the company MikroTik which mostly develops routers and wireless ISP systems used in providing Internet connectivity. In our network topology, these devices operate similarly to a router and provide an Internet connection to the other devices. It is also used in managing traffic, bandwidth management, firewall security, and supports the bridging between other VLANs. A 3G USB dongle is connected to the MikroTik router to provide an internet access source.

### Implementation Details

#### Setup of MikroTik and USB Dongle

First step is to cable the mikrotik to be in the same vlan as the workstation, that makes it vlan200. This is so that the workstation is able to connect to the router using the winbox tool.

#### Download WinBox Application

As configurations are done using programs, download the application WinBox using the following links.

<https://mikrotik.com/download>

#### Scan and Establish Connection

Start up the WinBox program and click on the “Neighbors” tab. If the MikroTik router is not found, click “Refresh”. Click on the MikroTik router enter the MikroTik’s setup interface. The connect to will be loaded by default. For login use the default “admin” and leave the password blank. Once this is done, click the “Connect” button.

Commented [NB5]: ADD SCREENSHOT OF THE TAB

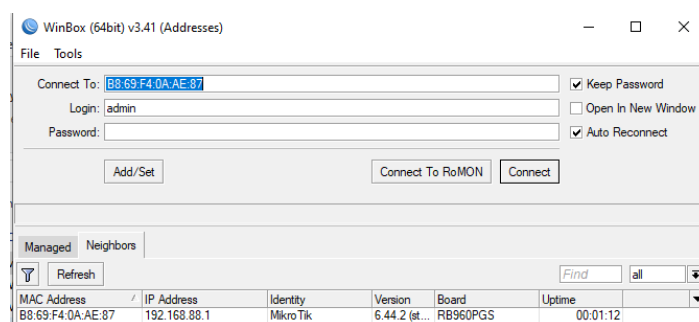
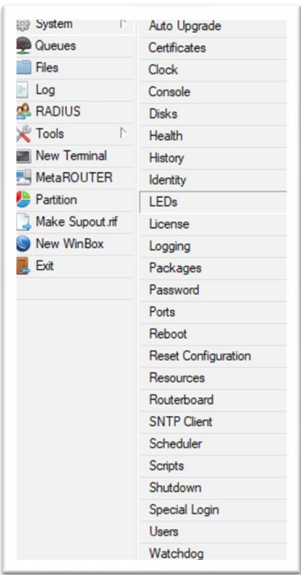


Figure 44: WinBox interface for connecting to a MikroTik router



Figure 45: To reset mikrotik router and delete previous configuration

Once connected reset the mikrotik router and delete the default configuration.

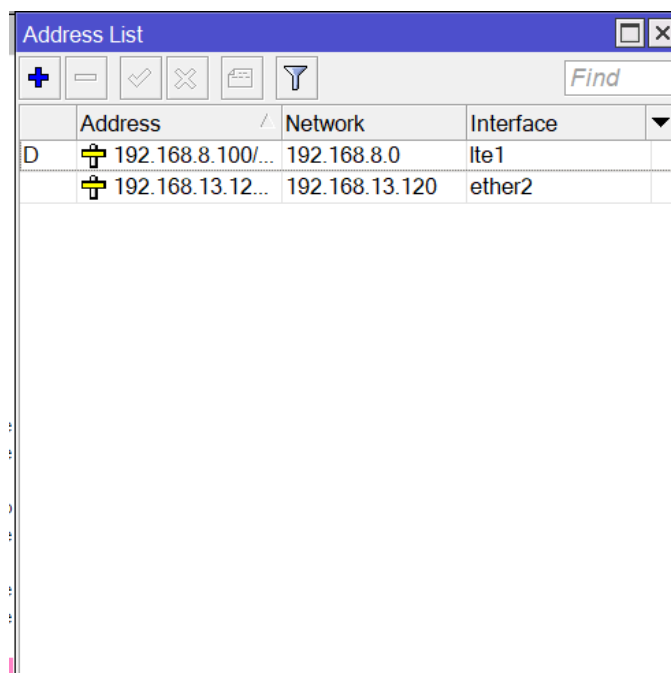


**Figure 46: To reset the MikroTik router configuration**

### Assign IP address

Once this is done, hover over the “IP” section and click on “Addresses”. The opened address list will display the USB dongle’s IP address with the interface “lte1”.

To add another address, click the “+” button and fill in the gateway address, network, and interface for the MikroTik router. This router was assigned the static ip “192.168.13.125” and the gateway “192.168.13.121”, the router was connected through port number 2 so assign the interface to be “ether2” as that’s the port that will be responsible for routing the traffic to the other vlans.



	Address	Network	Interface
D	192.168.8.100/...	192.168.8.0	lte1
	192.168.13.12...	192.168.13.120	ether2

**Figure 47: Address List Configuration in MikroTik Router Interface**

### Configure NAT

After the address list is configured, configure the Network Address Translation (NAT) for the MikroTik router. NAT is used to enable devices on the network to access the Internet by

translating their private IP addresses into a public IP address. In our network topology, NAT enables communications between the local networks and the Internet.

For this configuration, hover over “IP” and click on “Firewall”. In the opened firewall window, click “NAT” tab followed by the “+” sign. In the “General” tab, set the output interface to “lte1”, the USB dongle’s interface in the address list. This makes it so all data packets will be transmitted out of the MikroTik router using the “lte1” interface.

The screenshot shows the 'NAT Rule' configuration window in a MikroTik router. The 'General' tab is selected, displaying various configuration fields. The 'Chain' is set to 'srcnat'. The 'Out. Interface' is set to 'lte1'. The 'Status' at the bottom left is 'enabled'. On the right side, there are several action buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters.

**Figure 48: NAT Rule Configuration in MikroTik Router**

Next, click the “Action” tab and set the action to “masquerade”. This action allows the private network to be represented by the address from the public interface. Click the “OK” button and the new NAT rule will be displayed on the list.

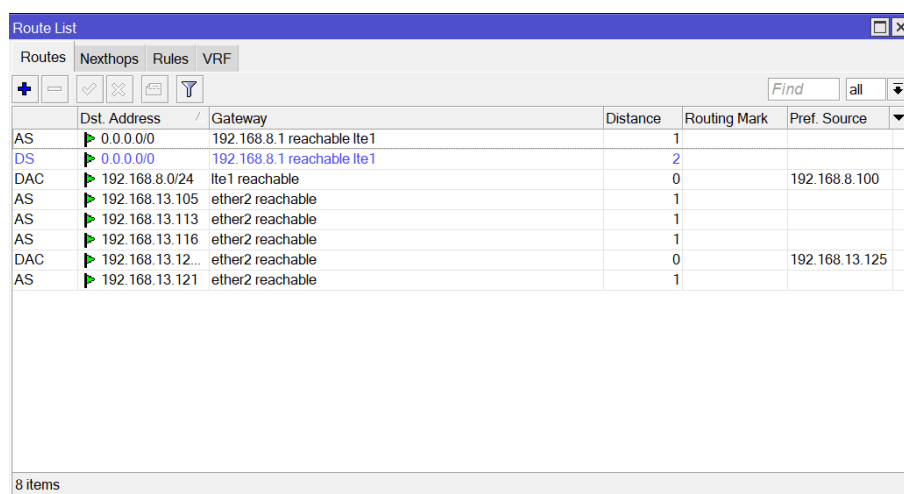
### **Configure Individual Routes to VLANs100/200**



For enabling data packets to be transmitted from different VLANs to the MikroTik and vice-versa, it is necessary to configure individual routes for the other VLANs. Since the MikroTik router resides in VLAN300, the remaining configurations are for VLANs 100 and 200.

To do this, hover over the “IP” section and click “Routes”. Within the “Route List”, Click the “+” button in the “Routes” tab. Configure the destination addresses to for VLAN100 and VLAN200. To route to VLAN100, add its gateway ip as the destination address “192.168.13.105” as for VLAN200 use the ip “192.168.13.113”, and use “ether2” as the gateway. The MikroTik router is connected to the other VLANs connected to the switch using the “ether2” gateway, click the “OK” button.

Alongside the routes for VLAN100 and VLAN200, configure a dedicated route using the default address “0.0.0.0/0” and the USB dongle gateway “192.168.8.0”. Set the “Distance” value to 2, this determines the number of hops the data can pass through while travelling from source to destination. Click “OK” once done. The figure below shows all the configured routes on the route list.



The screenshot shows the 'Route List' window in MikroTik WinBox. It has tabs for 'Routes', 'Next hops', 'Rules', and 'VRF'. The 'Routes' tab is active, showing a list of routes with columns for Dst. Address, Gateway, Distance, Routing Mark, and Pref. Source. The routes are as follows:

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	0.0.0.0/0	192.168.8.1 reachable lte1	1		
DS	0.0.0.0/0	192.168.8.1 reachable lte1	2		
DAC	192.168.8.0/24	lte1 reachable	0		192.168.8.100
AS	192.168.13.105	ether2 reachable	1		
AS	192.168.13.113	ether2 reachable	1		
AS	192.168.13.116	ether2 reachable	1		
DAC	192.168.13.12...	ether2 reachable	0		192.168.13.125
AS	192.168.13.121	ether2 reachable	1		

At the bottom of the window, it indicates '8 items'.

Figure 49: Route List Configuration in MikroTik Router

## Configuration Route Pointing to MikroTik

After configuring the WinBox, proceed by configuring the CISCO router. These configurations are done to direct unknown IP addresses to the MikroTik router. Start with entering the command “ip route” followed by the default IP (0.0.0.0 0.0.0.0) and MikroTik router IP

(192.168.13.125) in the CISCO router CLI. In the CLI, it should look like “Router (config) #ip route 0.0.0.0 0.0.0.0 192.168.13.125”. this command ensure that the router knows where to route the traffic.

## Internet Connectivity Test on Workstation

At this step, test the connectivity to the Internet by connecting to the MikroTik router and pinging the dns servers of google.com and test them if the internet is being router to the other VLANs.

Ping the connection between the MikroTik router and each VLAN on the switch.

```
Terminal <1>
[admin@MikroTik] > ping 192.168.13.105
  SEQ HOST                                SIZE TTL TIME  STATUS
    0 192.168.13.105                      56 255 0ms
    1 192.168.13.105                      56 255 0ms
    2 192.168.13.105                      56 255 0ms
    3 192.168.13.105                      56 255 0ms
sent=4 received=4 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms

[admin@MikroTik] > ping 192.168.13.113
  SEQ HOST                                SIZE TTL TIME  STATUS
    0 192.168.13.113                      56 255 0ms
    1 192.168.13.113                      56 255 0ms
    2 192.168.13.113                      56 255 0ms
    3 192.168.13.113                      56 255 0ms
sent=4 received=4 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms

[admin@MikroTik] > ping 192.168.13.121
  SEQ HOST                                SIZE TTL TIME  STATUS
    0 192.168.13.121                      56 255 0ms
    1 192.168.13.121                      56 255 0ms
    2 192.168.13.121                      56 255 0ms
    3 192.168.13.121                      56 255 0ms
sent=4 received=4 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

Figure 50: Ping Test Results for Network Connectivity in MikroTik Terminal

Test pinging the Google DNS server (8.8.8.8)

```
[admin@MikroTik] > ping 8.8.8.8
  SEQ HOST                                SIZE TTL TIME  STATUS
    0 8.8.8.8                             56 115 39ms
    1 8.8.8.8                             56 115 26ms
    2 8.8.8.8                             56 115 37ms
```

Figure 51: Ping Test to Google DNS (8.8.8.8) from MikroTik Terminal

Finally, test the Internet connectivity on the workstation PC by going on a web browser and searching for any websites. The following figures demonstrate searching for YouTube and Netflix while connected to the Internet.

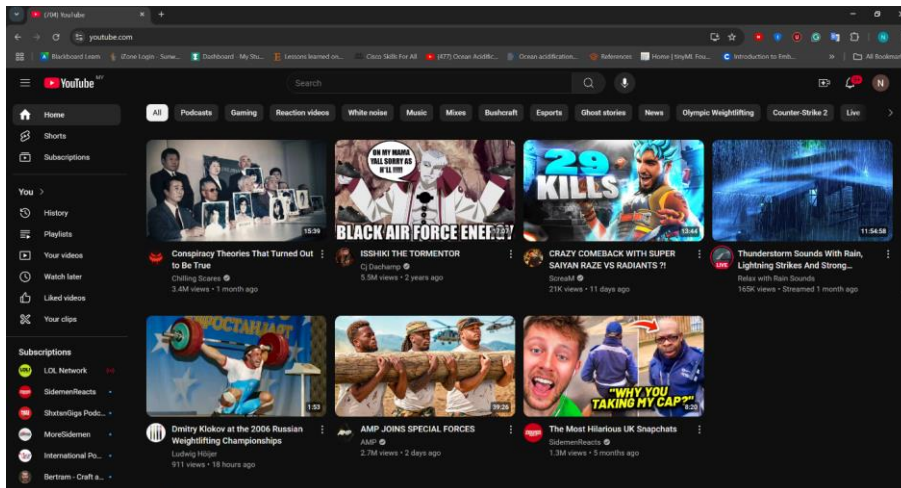


Figure 52: YouTube Homepage Display in a Web Browser

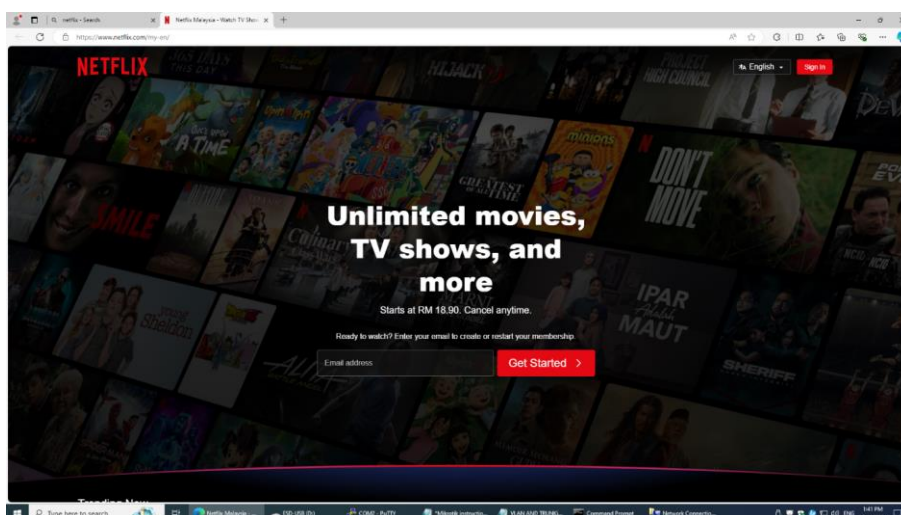


Figure 53: Netflix Homepage Display in a Web Browser

## Configuration Challenges and Workarounds

The mikrotik proved to be the most challenging, during the early trials the routes seemed to be working but when trying to access the internet from the workstation it was to avail. After resetting the router a couple of times, we noticed that there was a pop-up page that comes up after resetting which we never read and always closed straight away. After reading it showed

**Commented [NB6]:** Will add on Monday after testing the routing

that the router assigns its own Ip to the router which made it impossible to change and it gave a button to remove the configuration so that we have a blank slate to work on and that fixed the issue we were having. After removing it we were able to receive internet access from the mikrotik when in the same vlan.

## Web Server

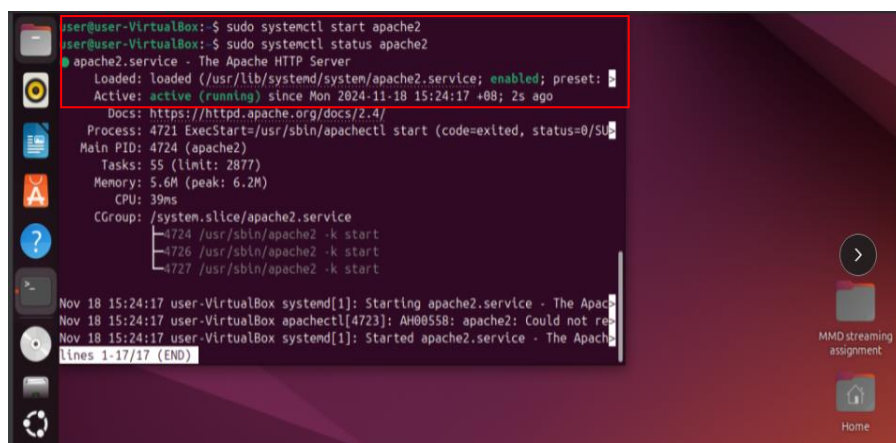
### Overview

A web server is a specialized system that plays a crucial role in hosting and delivering a website's content, such as images, text, videos, and other multimedia files. It operates by utilizing communication protocols like HyperText Transfer Protocol (HTTP) to process and respond to user requests efficiently. When someone accesses a website, the web server retrieves the requested resources and displays them to the user through their browser. Beyond serving content, web servers are also responsible for managing incoming traffic, ensuring that the website remains functional even under heavy loads. By distributing requests and controlling access, web servers help prevent the site from becoming overwhelmed, guaranteeing that users can interact with the website smoothly and reliably. For this assignment, the web server will be hosted on the open-source web server software, Ubuntu Apache. The implementation details will cover the process of configuring the web server to ensure that the websites can be accessed from all workstations in the network.

### Implementation Details

#### Ubuntu Startup

First, launch the Ubuntu Open Source Server. Enter the command **sudo systemctl start apache2**, which is used to start the Apache2 web server service on the system. Next, use the command **sudo systemctl status apache2** to verify the status of the Apache2 service. This command provides detailed information about whether the service is running or inactive.



```
user@user-VirtualBox:~$ sudo systemctl start apache2
user@user-VirtualBox:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: 
   Active: active (running) since Mon 2024-11-18 15:24:17 +08; 2s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 4721 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SU
 Main PID: 4724 (apache2)
    Tasks: 55 (limit: 2877)
   Memory: 5.6M (peak: 6.2M)
      CPU: 39ms
   CGroup: /system.slice/apache2.service
           └─4724 /usr/sbin/apache2 -k start
             4726 /usr/sbin/apache2 -k start
             4727 /usr/sbin/apache2 -k start

Nov 18 15:24:17 user-VirtualBox systemd[1]: Starting apache2.service - The Apac
Nov 18 15:24:17 user-VirtualBox apachectl[4723]: AH00558: apache2: Could not re
Nov 18 15:24:17 user-VirtualBox systemd[1]: Started apache2.service - The Apach
lines 1-17/17 (END)
```

Figure 54: Apache2 Service Management in Ubuntu Terminal

The output shown confirms that the Apache2 service is currently **active (running)** and has been successfully initiated. Additionally, the logs provide further information, such as the service's process ID (PID 4721) and details on memory usage.

## Website Setup

Next, create two html files, these two files will host the websites. These files will then be placed in the “var/www/html” folder. This folder is used by the apache server to host the websites.

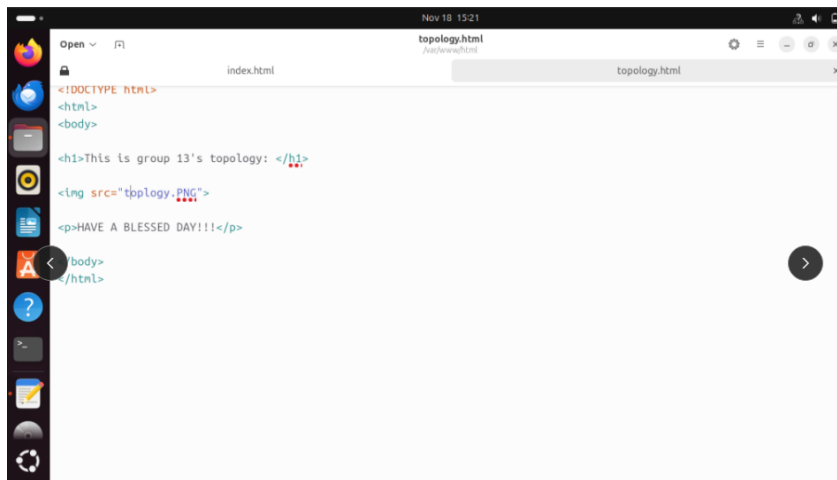


Figure 55: HTML File Displaying Group 13's Topology

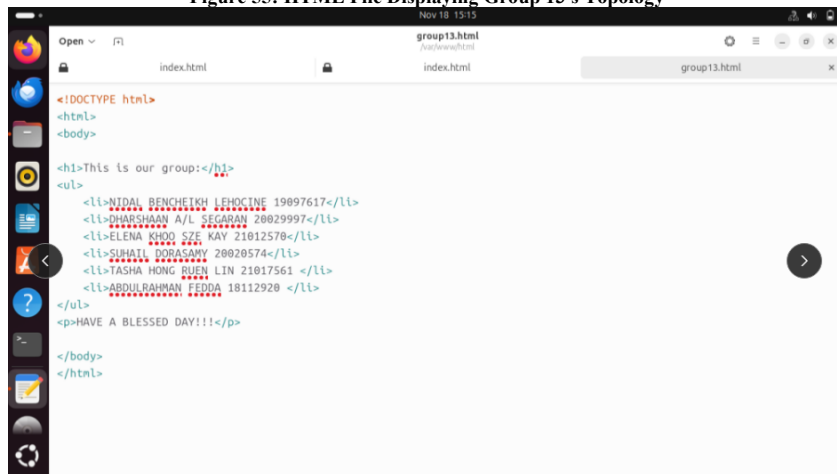


Figure 56: HTML File Displaying Group 13's Information

## Change Ubuntu Settings

Commented [NB7]: ADD SCREENSHOT TO SHOW IP IN THE UBUNTU

Change the Ubuntu Settings in the server machine, this allows the virtual machine to receive an Ip address.

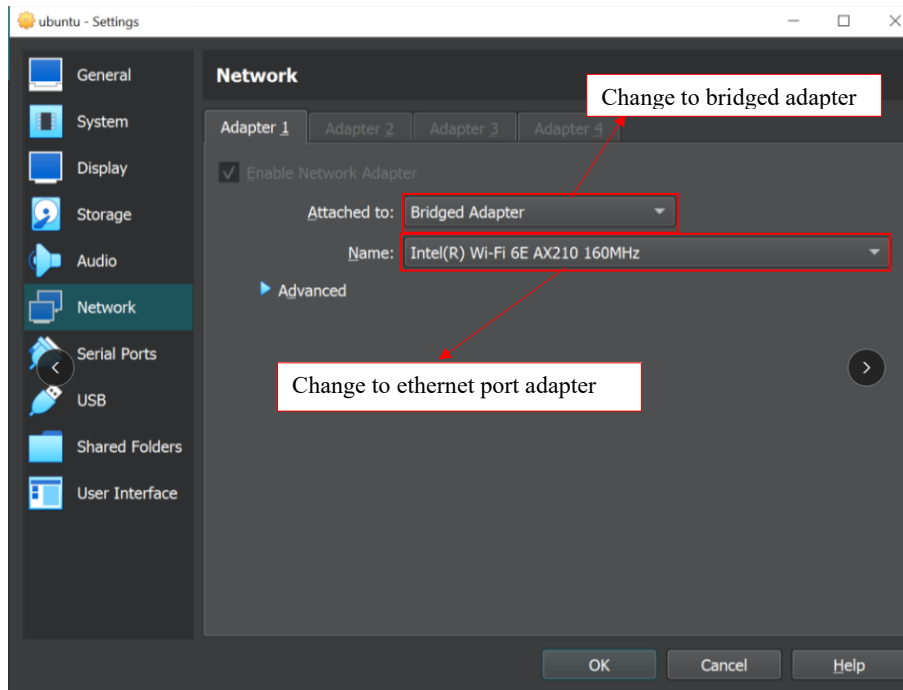
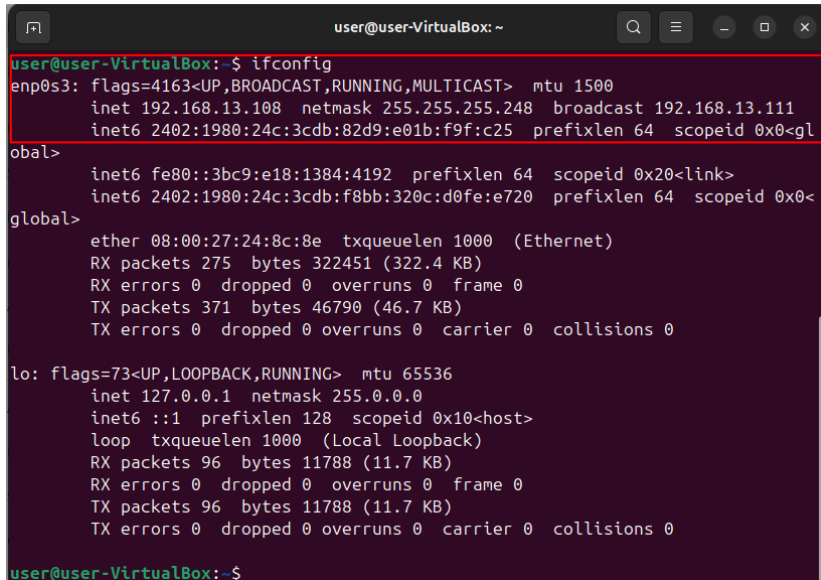


Figure 57: Network Adapter Configuration in VirtualBox Settings

Once that's done go to the terminal and type in the command "**ifconfig**" this command will show the ip address assigned to the webserver.

### Get IP address of the Web Server

In the next step of the assignment, the web server is configured within VLAN 100. The website's IP address will automatically correspond to the IP address assigned to the workstation hosting the server. To ensure the correct IP address for the website, it is essential to verify that the webserver is properly connected to a network switch port that is assigned to **VLAN 100**. To determine the IP address assigned to the workstation by the router's DHCP server, open the Command Prompt and use the command **ipconfig**. This command will display the network configuration details, including the IP address currently assigned to the webserver. The retrieved IP address will be crucial, as it will also be used to access the webpage through the other vlans.



```
user@user-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.13.108 netmask 255.255.255.248 broadcast 192.168.13.111
inet6 2402:1980:24c:3cdb:82d9:e01b:f9f:c25 prefixlen 64 scopeid 0x0<gl
obal>
inet6 fe80::3bc9:e18:1384:4192 prefixlen 64 scopeid 0x20<link>
inet6 2402:1980:24c:3cdb:f8bb:320c:d0fe:e720 prefixlen 64 scopeid 0x0<
global>
ether 08:00:27:24:8c:8e txqueuelen 1000 (Ethernet)
RX packets 275 bytes 322451 (322.4 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 371 bytes 46790 (46.7 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 96 bytes 11788 (11.7 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 96 bytes 11788 (11.7 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

user@user-VirtualBox:~$
```

Figure 58: ifconfig command in Virtual Box terminal

### Test the website from workstation (Different VLAN)

Next, a web browser was opened on the workstation located in VLAN200. The IP address of the web server was entered along with the specific file names, such as “192.168.13.109/group13.html” and “192.168.13.109/topology.html”. This action successfully displayed the previously created web pages on the client’s browser, confirming that the web server was properly configured and accessible across VLANs.

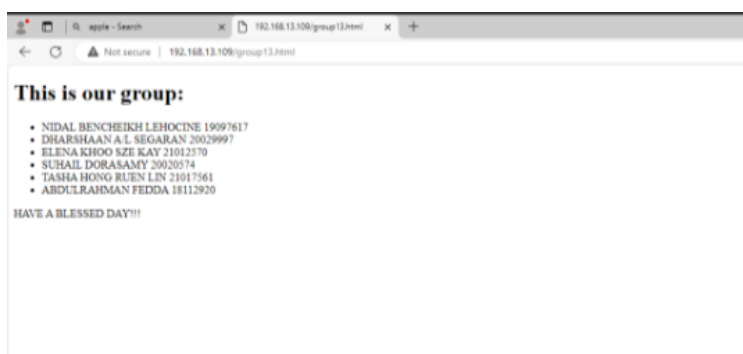
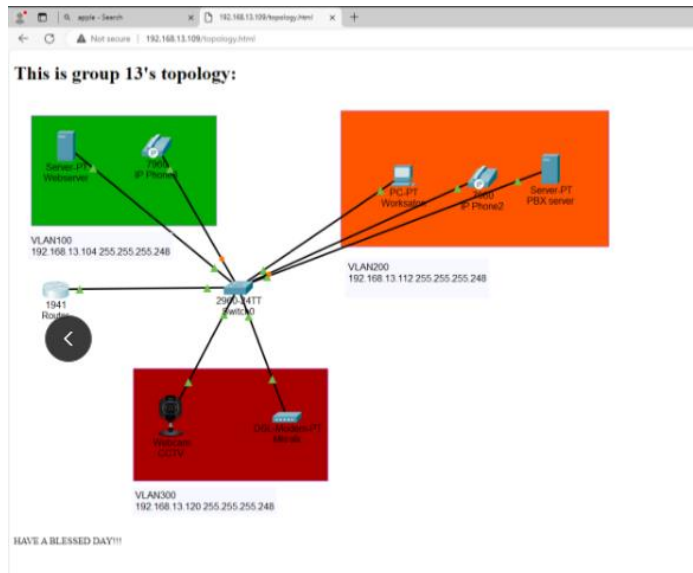


Figure 59 : HTML Webpage Listing Group Members Displayed in a Browser





**Figure 60: Group 13's Network Topology Visualization in a Web Browser**

## Configuration Challenges and Workarounds

Setting up the web server was rather smooth and did not raise significant problems. The web server is set up on an Ubuntu virtual machine, where appropriate packages had to be installed and configured- apache2. Once the server started, it could access without any problems. It went very smoothly, and nothing needed any technical troubleshooting.

## VLAN and Trunk Features

### Overview

VLAN trunking is an Ethernet technology used in creating a single link between the switches to support as many VLANs required by the network topology. VLAN trunking also separates VLAN traffic ensuring they do not interfere with one another.

VLAN (Virtual Local Area Network) is a custom network created from one or more LANs while allows a group of devices from multiple networks to be combined into a single network. Trunk links are physical links between switches and routers and are used in allowing traffic from different VLANs to pass through. Unlike access ports, trunk ports carry traffic for every

VLAN to allow the switch to exchange the VLAN traffic. This traffic is separated by tagging each frame with an identifier during transmission.

## Implementation Details

For this assignment, as the port f0/24 is used to connect the router and switches together. To enable trunking between these 2 devices, use the command “switchport mode trunk”. This makes it so ports on trunk mode will tag their frames during transmission. The Ethernet interface in the CISCO router is configured as 802.1Q trunk and connected on the switch using a trunk port.

```
Switch(config)#interface F0/24
Switch(config-if)#description Trunk link
Switch(config-if)#no shutdown
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
```

Figure 61: Configurations to setup trunk link on switch

Configurations for the router interface include creating sub-interfaces for each VLAN. These sub-interfaces are virtually created meaning they only exist in the software. Each sub-interface is specifically assigned to the VLANs so the router knows which traffic belongs to which VLAN. Every sub-interface is shared by the same physical Ethernet. The VLAN tagged using 802.1Q ensures the traffic is separately routed.

First of all, the physical interface g0/0/0 is activated by the use of the no shutdown command that initializes it. On the same physical interface g0/0/0, three sub-interfaces for VLANs 100, 200, and 300 are created.

The encapsulation dot1Q command is used in each of the sub-interfaces, including the VLAN ID number, 100, 200, or 300, in which 802.1Q Trunking is attained. This process ensures that the router will be able to distinguish between the VLANs properly by tagging the frames with their appropriate VLAN IDs. Then, each sub-interface is assigned a unique IP address within the associated subnet, such as 192.168.13.105 for VLAN 100, 192.168.13.113 for VLAN 200, and 192.168.13.121 for VLAN 300, with the inclusion of a subnet mask of 255.255.255.248.

Commented [NB8]: Add caption

Those sub-interfaces also provide default gateways for devices in each VLAN and enable internal traffic within the VLANs and outside. Such a structure will also allow for the proper segmentation of network traffic and routing between VLANs, while 802.1Q tagging will ensure efficient handling of VLAN-specific traffic over a single physical link.

For this assignment, verify the configurations of VLANs and inter-VLAN routing by verifying the connectivity works for hosts in different VLANs and default gateways. This can be done by pinging all devices in the network topology using workstations, use different VLANs to create calls between the 2 IP phones, access the Internet from the MikroTik router using the workstation, and access websites hosted on the web server using the workstation.

```
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/0.100
encapsulation dot1Q 100
ip address 192.168.13.105 255.255.255.248
!
interface GigabitEthernet0/0.200
encapsulation dot1Q 200
ip address 192.168.13.113 255.255.255.248
!
interface GigabitEthernet0/0.300
encapsulation dot1Q 300
ip address 192.168.13.121 255.255.255.248
!
```

Figure 62: Configurations to setup trunk links on router

## Configuration Challenges and Workarounds

Similar to the switch and webserver, we had no problems regarding the trunking and VLAN setup, creating the sub-interfaces and 802.1 encapsulation ran smoothly and did not require any additional troubleshooting.

## Lessons Learnt

This network management assignment was a rewarding experience that taught us valuable lessons about both technical and collaborative aspects of working on a complex project. One of the biggest takeaways was the importance of **teamwork and collaboration**. Each team member brought their unique skills and perspectives, and by working together and dividing tasks effectively, we were able to overcome challenges and meet our goals. Strong communication played a key role in keeping everyone aligned and productive.

We also learned how essential it is to **think outside the box** when faced with unexpected problems. For instance, when VLAN communication issues arose, or device-specific configurations didn't go as planned, we had to step back, analyze the situation creatively, and come up with innovative solutions. This reminded us that being adaptable and open-minded is just as critical as technical expertise.

Another important lesson was the value of **applying niche solutions**. We often relied on specialized tools, like MikroTik's WinBox application and Grandstream's gs\_search tool, to tackle unique device requirements. At the same time, we frequently turned to online forums, blogs, and other resources to find potential solutions for problems we couldn't immediately resolve. Trying out these ideas, adapting them to fit our setup, and learning from the results was a valuable part of the process. It reinforced how useful it can be to draw on the experiences and knowledge of a wider community when working on technical projects.

We also came to appreciate the importance of **persistence and systematic troubleshooting**. Whether it was fixing NAT issues on the MikroTik router or manually addressing VLAN mismatches, we learned the value of tackling challenges step by step and staying patient until we found the right solution. This process not only resolved issues but also deepened our understanding of how these systems work.

Lastly, we saw firsthand how critical **clear documentation and integration skills** are. Keeping a detailed record of our configurations made it easier to troubleshoot and ensured that our network setup was consistent and replicable. Successfully integrating diverse components—like VLANs, routers, switches, IP phones, and web servers—also gave us a deeper appreciation for how interconnected networks operate.

Overall, this assignment was not just about building a network—it was about growing as a team and as individuals. We gained practical technical skills, honed our problem-solving abilities, and learned the importance of collaboration, adaptability, and learning from experience.

#### Self-reflection:

##### 1. Suhail Dorasamy

Reflecting on this assignment, I realize how much I've grown and learned throughout the process. Collaborating with my team to set up and manage a Local Area Network (LAN) was not only a technical challenge but also a valuable opportunity to enhance my skills and gain insight into the practical application of networking concepts.

One of the most rewarding aspects of this experience was developing my technical expertise. Initially, tasks like setting up VLANs and ensuring seamless functionality seemed daunting, but they ultimately strengthened my understanding of network segmentation and inter-VLAN communication. Working hands-on with devices such as PBX servers, IP phones, switches, and routers made the theoretical knowledge from class feel tangible and relevant.

This project was about much more than just network configuration; it emphasized the importance of persistence, teamwork, and learning through trial and error. I'm proud of what our team achieved and grateful for the lessons this experience taught me. It has boosted my confidence in my abilities and provided a clearer vision of how I can apply these skills in the future.

##### 2. Nidal Bencheikh Lehocine

Prior to this assignment, my experience with networking was limited to working with routers and switches on Cisco Packet Tracer. I had never encountered IP phones, PBX servers, or Mikrotik routers before. Transitioning from a virtual environment to working with these devices in real life was both challenging and rewarding. It provided me with invaluable hands-on skills that could not be fully grasped through simulation alone.

Learning to route internet access from a dongle to different VLANs and linking two separate phones from different VLANs was particularly difficult at first due to my limited knowledge. However, by relying on my troubleshooting skills and my teammates' help, I was able to overcome these challenges, significantly broadening my understanding of networking devices and configurations.

Additionally, applying the skills I had previously learned on Packet Tracer after such a long time added a sense of achievement. It was fulfilling to see my past efforts pay off in a real-world context, whether configuring a switch or hosting a web server.

This assignment has helped me learn new skills that can be applied into the professional field as well as honing my existing skills.

3. Elena Khoo Sze Kay

I gained a lot of valuable insights through this assignment. Transitioning from configuring devices online to doing so physically was a completely different experience. This project required us to work on various devices, and my specific role involved configuring the CCTV system with support from my teammates. Initially, it was challenging as I had never configured a CCTV before, but with their guidance and assistance, I managed to learn and complete the task. Additionally, I developed an understanding of how to configure other devices, which significantly broadened my knowledge of device configurations. Although the assignment was difficult, I am grateful for the opportunity to engage in a hands-on project.

4. Dharshaan A/L Segaran

As all this while, we only learned about switches and routers virtually, this assignment required us to physically work with these devices. It was interesting as learning about it from a book and working with it in real life was very different. My part required me to work with the router. My friends were very helpful as they guided and taught me how to work with a router. I learned so much about auto-start, routing, gateway and many more. Although my part was just the router, my friends still explained other parts like PBX Server, CCTV, switch and other things thoroughly which enabled me to expand my understanding and knowledge on these devices. It was definitely an assignment that made me learn a lot about working with physical devices.

5. Tasha Hong Ruen Lin

In this assignment, I learnt about configuring devices, such as IP phones and CCTV, and how to connect them all together to create a network topology. In my part of the assignment, I learnt more about the switch and how to configure it to create virtual LANs for access and trunk ports. Overall, this assignment helped me learn more about how different devices must be configured so they can connect with other devices in a network topology. This assignment also gave me the opportunity to learn more about devices such as IP phones, CCTV camera, MikroTik router, PBX server, switch, and router.

6. Abdul Rahman Fedda

This assignment has been very educational, I was able to put my knowledge that I learnt from previous subjects where we configured networks on CISCO packet tracer and use it in a real-life scenario. This assignment has allowed me to learn much more about network configurations and I watched my groupmates configure their devices I was able to learn from their work as well, I had to configure the web server which was not too difficult as it only required the configuration of 2 web pages and then switching on apache and making sure it was running.





	Auto-start	1		
<b>Switch</b>	Access port	5		
	Description	3		
	VLAN	6		
	Justification	5		
Trunking & Internet	Configuration	5		
	Integration	10		
	Internet	10		
Documentation	Clear screenshots with informative discussion; standardized format; well-written	5		
Professionalism	All components (including additional feature(s)) are integrated and workable without errors	5		
Demonstration/ Presentation	Presentation skills; teamwork; ability to handle questions and answer them correctly	Total individual marks = 10		
	Member 1 (Suhail)	20		
	Member 2 (Nidal)	20		
	Member 3 (Elena)	20		
	Member 4 (Dharshaan)	20		
	Member 5 (Tasha)	20		
	Member 6 (Abdul)	20		

Note: non-performing and absent members will be marked zero.