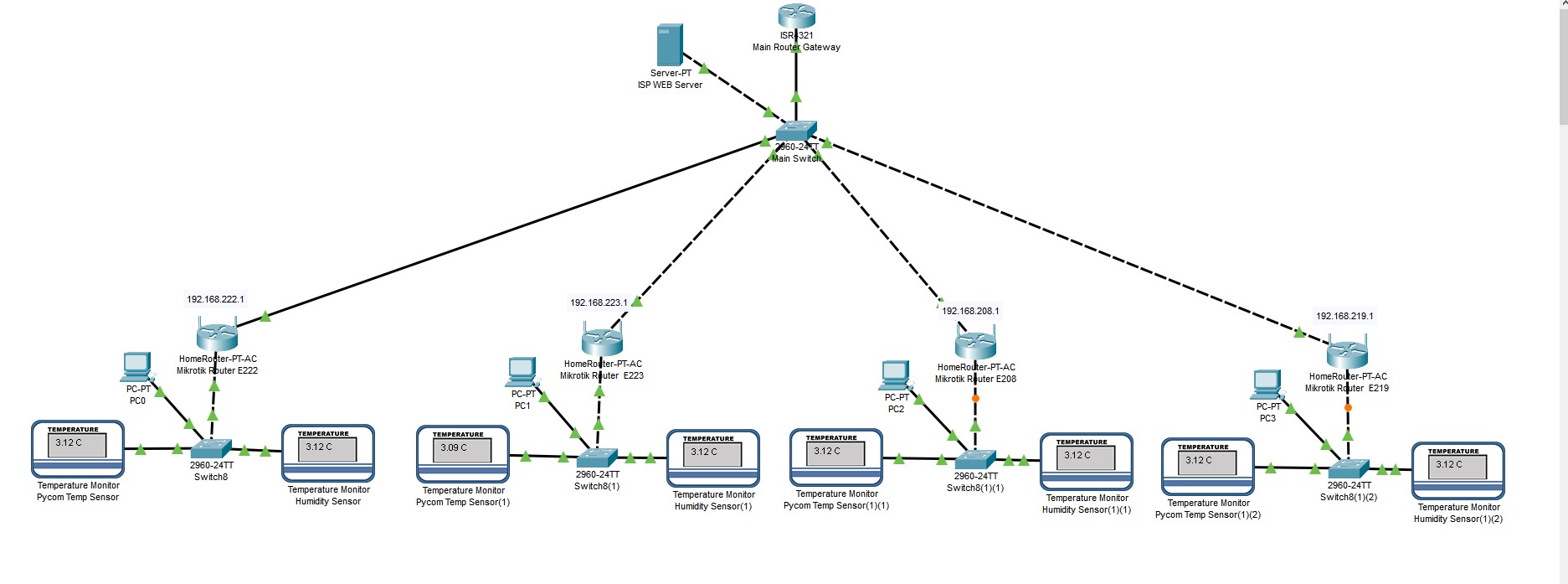
Network Documentation

# Design:

Below is the network design for each room.

# Network Materials needed:

The materials needed for this setup is below:

* 4x Mikrotik Devices (Wireless AP)
* 4x 2960 Switches
* 4x Computers
* Core Switch
* Core Server
* Core Router

# Installation:

For the installation of this network we will start room by room and work our way through each room. Before moving on to the next room ensuring that that room is tested and set up correctly. To ensure the network is all working correctly we would using tracerts and ping to ensure that the network is connecting from the router to its clients. On the clients computer we would also to a ipconfig /all to ensure that the DHCP server is giving out the correct address from the range that was set. This network would be installed over a weekend with our team to ensuring there is as little downtime for students and teachers as possible!

# Cyber Security Risk Management:

MikroTiks firewall is based on Stateful Filtering technology, this means it can be used to detect and blocks threats that use stealth scan, DoS attacks and SYN floods. Because of the available security options, unauthorized access can be prevented and monitored in real time.

MikroTiks Firewall is based around:

* IP address filtering
* Port protocol filtering
* Network interface filtering
* Source MAC address filtering
* TCP protocol option

Masquerading can be used to hide your private network behind one external address. With masquerade, clients using the internet will appear to the outside world as one IP address which is the address of the router. With this, all traffic will funnel through one safe and secure connection and external threats will have a lot more trouble breaking into your network.

The use of secure passwords for the administrator account, allowing the administrators static IP address connect to the router. Changing of the default connection port which will make it harder for the router to be breached and hacked.

## Wireless Routers Configuration:

Below is the router configuration we have set up for the rooms as seen in the diagram.

# oct/30/2020 12:54:49 by RouterOS 6.47.1

# software id = QC5U-WZLM

#

# model = RB952Ui-5ac2nD

# serial number = A0C60AD5AD01

/interface wireless

set [ find default-name=wlan1 ] band=2ghz-b/g/n disabled=no mode=ap-bridge \

ssid=Industry4

set [ find default-name=wlan2 ] band=5ghz-a/n/ac mode=ap-bridge ssid=\

Industry4-5G

/interface vlan

add interface=wlan1 name="Industry4.0 VLAN" vlan-id=40

/interface wireless security-profiles

set [ find default=yes ] authentication-types=wpa2-psk eap-methods="" mode=\

dynamic-keys supplicant-identity=MikroTik wpa2-pre-shared-key=Password1

/ip pool

add name=dhcp\_pool0 ranges=192.168.2.1-192.168.2.253

add name=dhcp\_pool1 ranges=192.168.222.1-192.168.222.253

/ip dhcp-server

add address-pool=dhcp\_pool0 disabled=no interface=ether2 name=dhcp1

add address-pool=dhcp\_pool1 disabled=no interface=wlan1 name=dhcp2

/interface ethernet switch vlan

add disabled=yes ports=ether5 switch=switch1 vlan-id=40

/ip address

add address=192.168.2.254/24 interface=ether2 network=192.168.2.0

add address=192.168.222.254/24 interface=wlan1 network=192.168.222.0

add address=192.168.100.254/24 interface="Industry4.0 VLAN" network=\

192.168.100.0

/ip dhcp-client

add disabled=no interface=ether1

/ip dhcp-server network

add address=192.168.2.0/24 gateway=192.168.2.254

add address=192.168.222.0/24 gateway=192.168.222.254

/ip dns

set allow-remote-requests=yes

/ip firewall nat

add action=masquerade chain=srcnat out-interface=ether1

/system clock

set time-zone-name=Australia/Melbourne

/system identity

set name=Industry\_4.0

By Harry O’Brien