# CSG1105 Workshop Three

## 1 Introduction

This week we are going to explore aspects of Ethernet, a commonly used Network Access Layer protocol.

## 2 Exercise: Finding Your MAC Address

### 2.1 Windows

- Open a command prompt
- Issue the command `ipconfig /all`
- Find your active adapter and look for "Physical Address"
- Note the address for future reference. It will be something like: `34-48-ED-A3-22-BA`

### 2.2 OS X

- From the Applications->Utilities folder, run the terminal App
- Issue the command `ifconfig`
- There will be a field called **ether** followed by the MAC address Note the address for future reference. It will be something like: `34-48-ED-A3-22-BA`

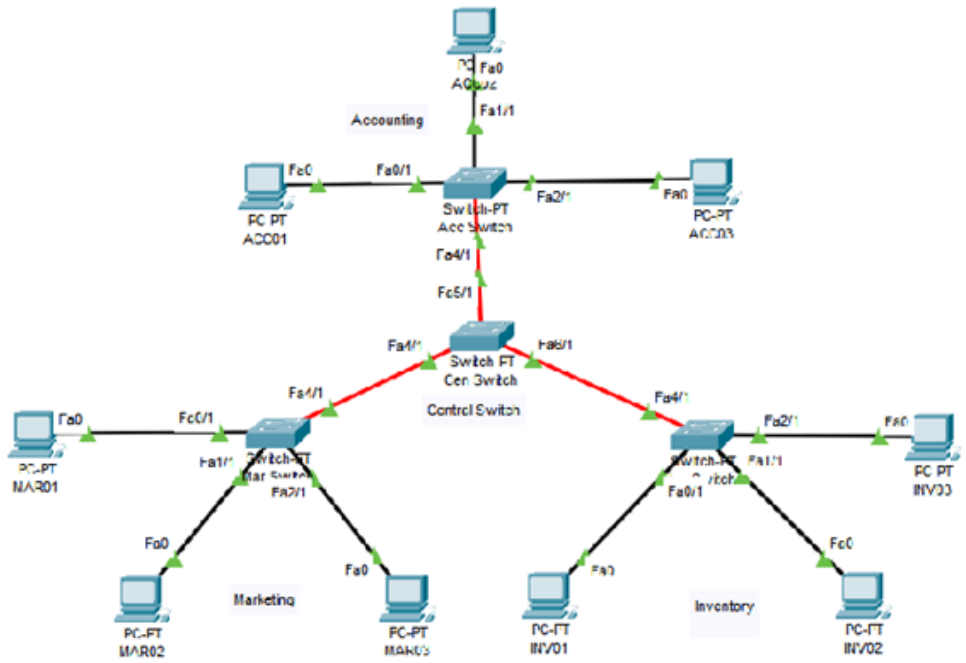
### 2.3 Exercise: Switching

Switches use the source MAC address of a frame (see Module 3 lecture) to build the **MAC Address Table**. The source MAC address is recorded against the ingress port of the switch. The MAC Address Table is used by the switch to direct an incoming frame to the correct egress port by examining the destination MAC address in the frame and using it to direct the frame.
In this exercise, we will be using the CISCO Packet Tracer tool to model a small network. **Please see the separate instructions for creating a CISCO One Identity Account require to use Packet Tracer.**

### 2.4 The following network is a model in CISCO Packet Tracer

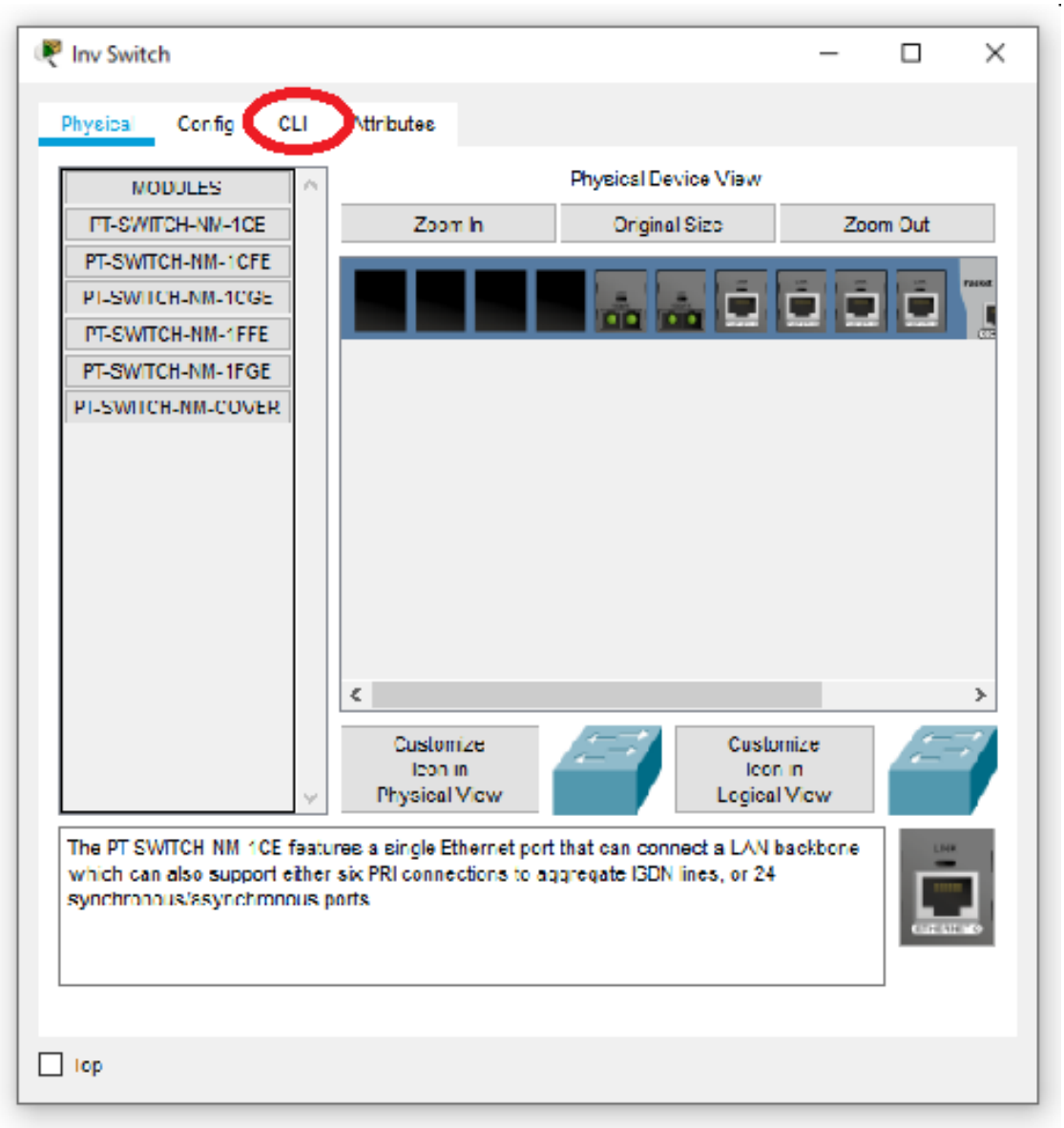
We have a simple fully switched network, with a central switch connecting three peripheral switches using optic fibre. Each of the ports on each switch is identified with a code Fa, indi-

cating Fast Ethernet and a number identifying the connection e.g. Fa4/1. Every interface, both on the switches and on the PCs, has a MAC address.

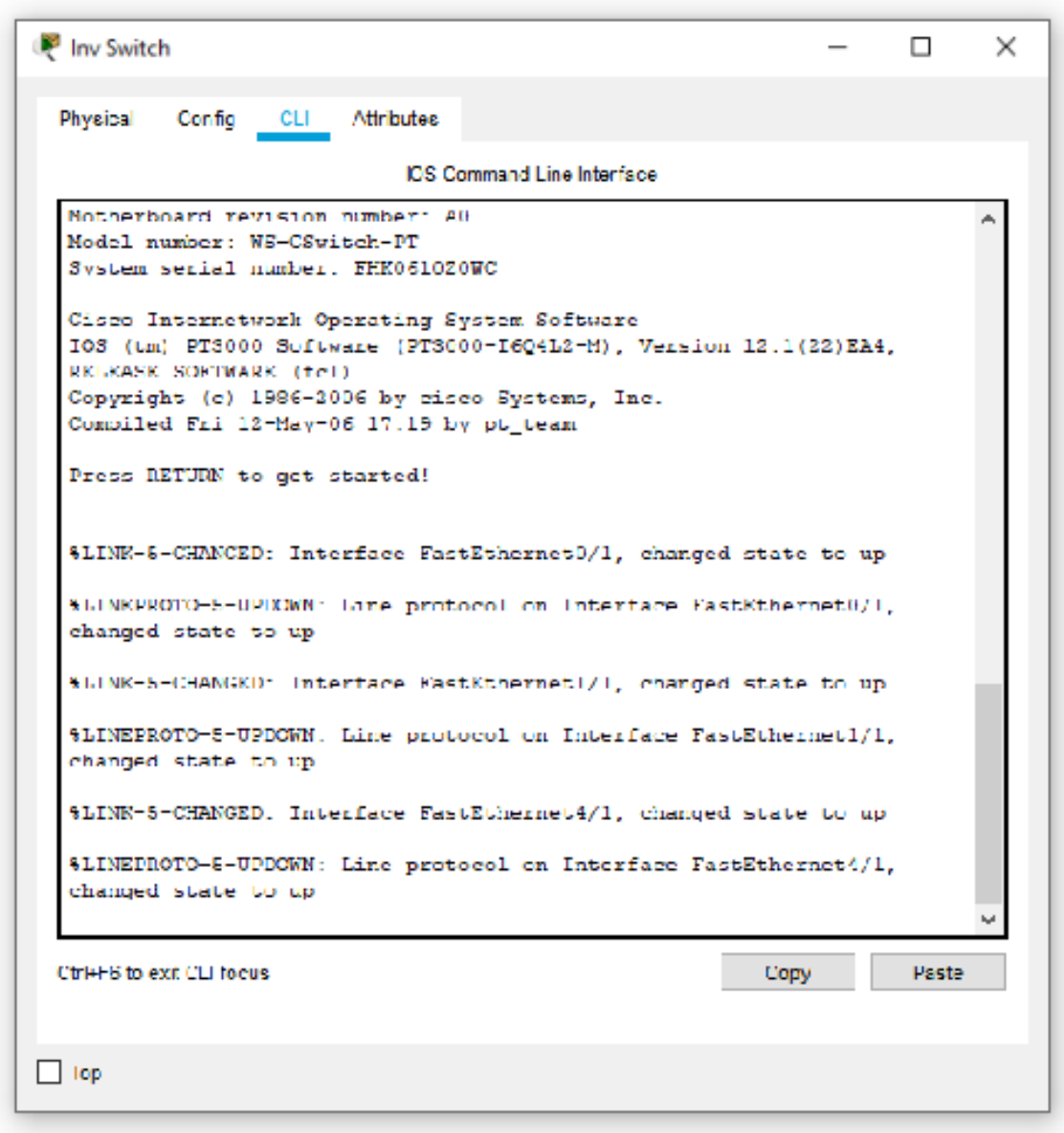



When the switches are powered on, they exchange status information, resulting in the MAC addresses of the interfaces being recorded in the MAC Address table of each switch.

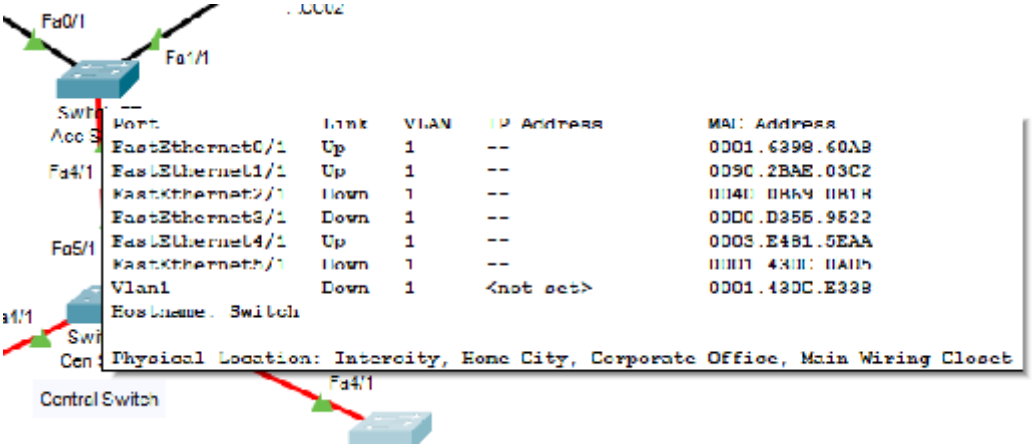
1. Run CISCO Packet Tracer
2. Load the SwitchedNetwork.pkt file
3. You should see a network matching the diagram
4. Each of the PCs has been allocated an IP address in the 192.168.0.0 network
5. Click on one of the switches




6. A window will open giving details of the switch. Click on the **CLI** tab




7. Click in the terminal window and press "Enter" (most commands will require you to press "enter")
8. The terminal will display a **Switch>** prompt
9. At this prompt, type `enable`. The prompt will change to **#Switch** indicating you're logged in as an administrator (There would normally be a password)
10. Type `show mac-address-table`
11. this will display the MAC address of any ports on connected switches
12. Repeat this for all switches
13. Hovering the cursor over a device in the main model will show the MAC addresses of all interfaces. Use this to confirm that the MAC address(es) in the MAC Address Table are those on the connected switches.




**Central switch - before ping**

```
 Vlan Mac Address Type Ports
-- ------ ---- ---

1 0003.e481.5eaa DYNAMIC Fa5/1 MAC of Fa4/1 on Acc Sw
1 0030.f2c8.8033 DYNAMIC Fa4/1 MAC of Fa4/1 on Mar Sw
1  00d0.971d.3b1b DYNAMIC Fa6/1MAC of Fa4/1 on Inv Sw
```

**Marketing switch - before ping**

```
 Vlan Mac Address Type Ports
-- ------ ---- ---

1 00d0.589d.7eea DYNAMIC Fa4/1 MAC of Fa4/1 on Cen Sw
```

**Accounting switch - before ping**

```
 Vlan Mac Address Type Ports
-- ------ ---- ---

1 0060.5ce8.30a8 DYNAMIC Fa4/1 MAC of Fa5/1 on Acc
```

This table is generated dynamically by recording the Source MAC address of a frame received against the Port that it was received on. This may then be used to direct frames to the port that is associated with the MAC address in the destination field of a subsequent frame. Multiple MAC addresses may be associated with a port in a tiered network.
The tables are not static and are updated in three ways:

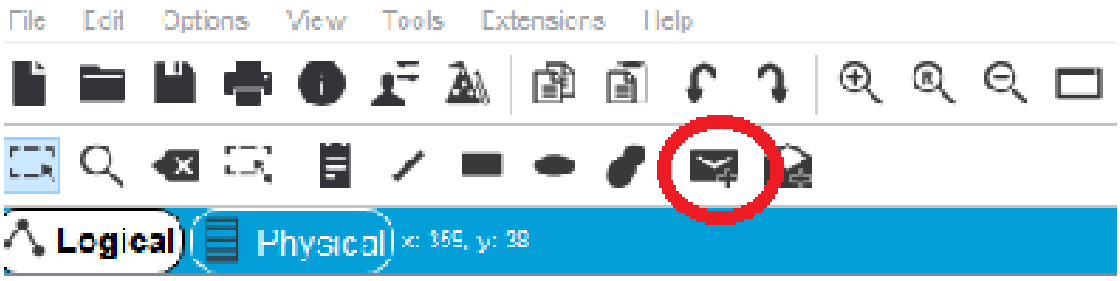
1. When an entry is created, a timer is started. If the time expires without the MAC being seen again, the entry is dropped from the table

2. When new source MAC addresses are seen arriving at a port, they are recorded against that port.
3. On advanced managed switches, an administrator may add a static entry

### *2.4.1 MAC Tables after Pings*

The `ping` command that a remote host is 1) Up and 2) how much delay exists between you and the host. We will use ping to generate traffic between hosts. You can look at the MAC address tables before and after the ping to see how they have altered. In Packet Tracer, there is a GUI for sending pings between hosts.

1. In the menu bar there is an envelope icon.




2. Click on the envelope icon, then Click
   a) On a source PC and
   b) On a destination PC
3. This will send a ping between the source and destination PCs
4. Re-examine the MAC address tables of all the switches

**Central switch - after ping**

```
Ping from PC MAR02 to PC ACC03
MAC of MAR002 0001.639b.d60e
MAC of ACC003 000c.8522.5333

Vlan Mac Address Type Ports
-- ------ ---- ---
1 0001.639b.d60e DYNAMIC Fa4/1(link to Mar Switch)
1 0003.e481.5eaa DYNAMIC Fa5/1
1 000c.8522.5333 DYNAMIC Fa5/1(link to Acc Switch)
1 0030.f2c8.8033 DYNAMIC Fa4/1
1 00d0.971d.3b1b DYNAMIC Fa6/1
```

**Marketing switch - after ping**

```
 Vlan Mac Address Type Ports
-- ------ ---- ---
1 0001.639b.d60e DYNAMIC Fa1/1(link to MARO2)
1  000c.8522.5333 DYNAMIC Fa4/1(link to central switch)
1 00d0.589d.7eea DYNAMIC Fa4/1
```

**Accounting switch - after ping**

```
Vlan Mac Address Type Ports
—- ———— ——— ——
1 0001.639b.d60e DYNAMIC  Fa4/1(link to central switch)
1 000c.8522.5333 DYNAMIC  Fa2/1(link to ACC02)
1 0060.5ce8.30a8 DYNAMIC  Fa4/1
```

# 3 ARP - Address Resolution Protocol

The ARP protocol is used to determine the MAC address associated with an IP as the MAC address is needed to deliver the frame containing a packet. In this exercise, we will briefly use Wireshark to examine ARP packets.

## 3.1 Exercise - Viewing ARP packets with Wireshark

1. Using instructions from Workshop Two, start Wireshark capturing packets
2. Ask a colleague in the class the IP of their PC (on campus only, if you're working elsewhere, skip this step unless you have two devices available on the same subnet)
3. Open a command prompt and issue the command `ping 192.168.0.1` (substitute the appropriate IP)
4. Stop the Wireshark capture
5. Filter for ARP packets and find your request and the response from the second machine
6. Examine the MAC and IP in both the request and the response. What do you notice about these values?