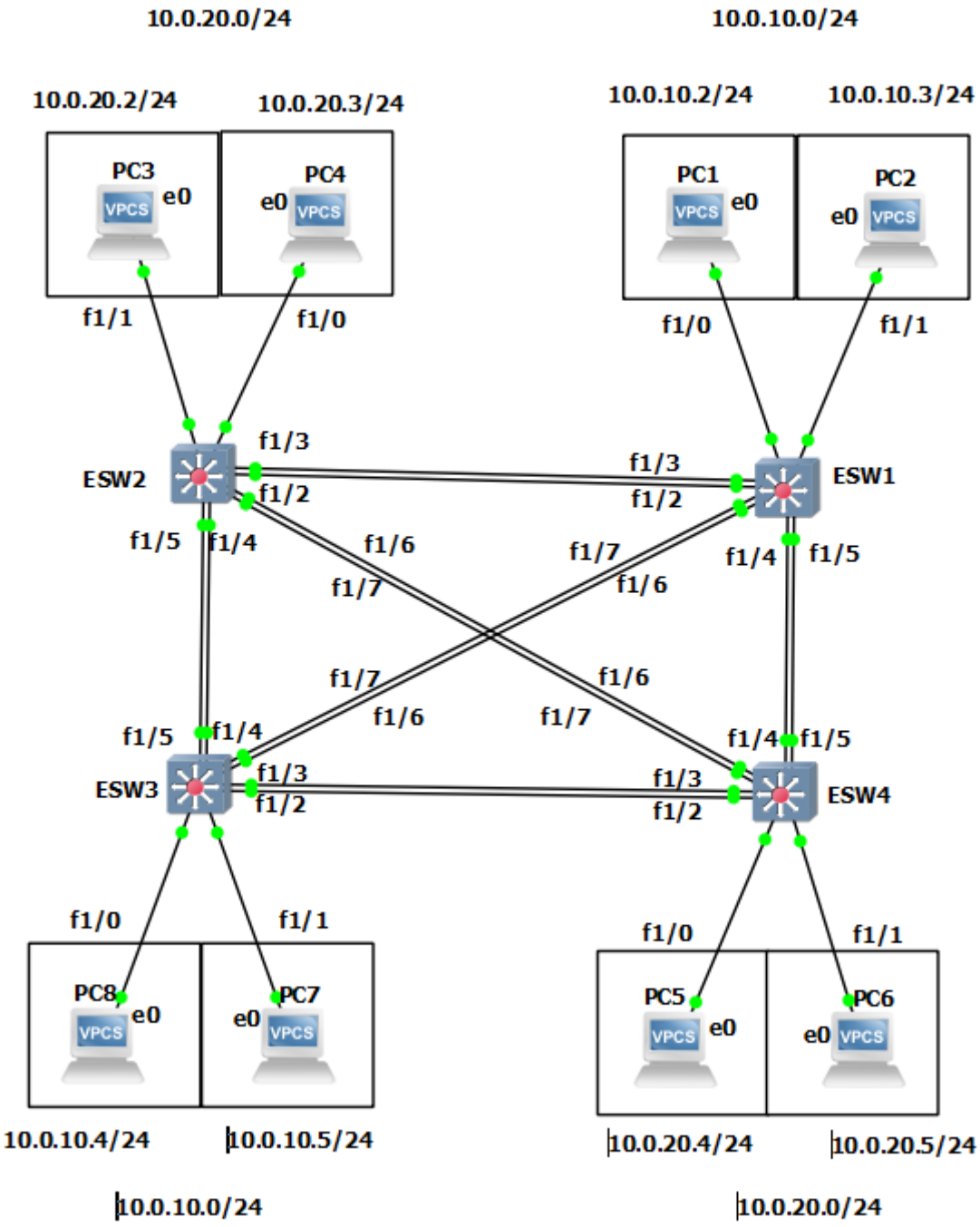
IT-C 247 Lab 4 - Switching Part 1

Practical Lab - Switches and VLANs

Introduction

In this lab, you'll be constructing a mesh topology with 4 switches and 2 VPCs connected to each switch, segmenting them into two different IP subnets and VLANs. This will provide hands-on experience with VLANs, port channeling, and Link Aggregation Control Protocol (LACP).

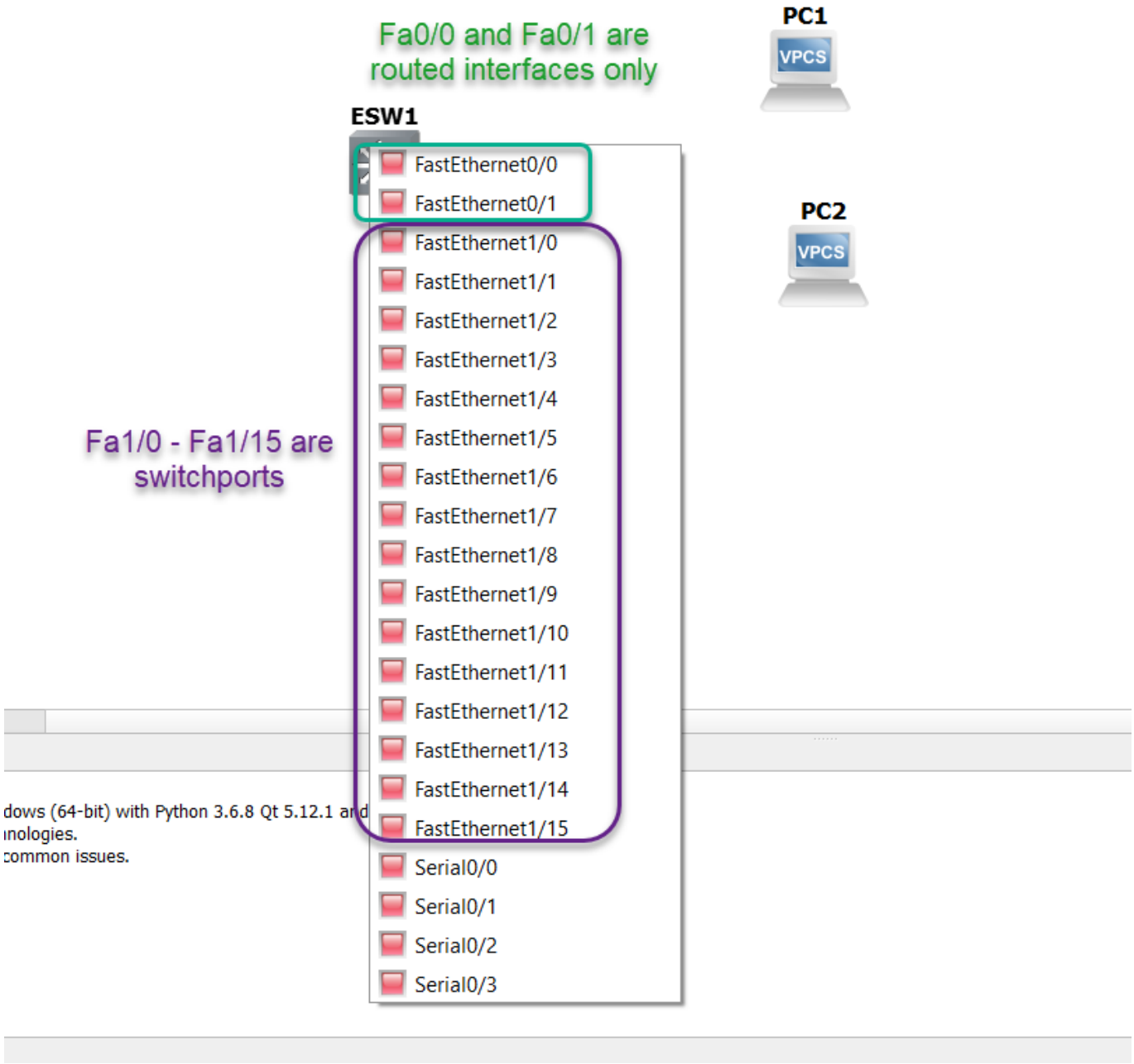
Your task will be to recreate the following network topology in GNS3:



Lab setup

Switch vs Router Modules

A quick refresher on switch/router modules in GNS3 is illustrated below:



Modules are structured as follows:

- f0/# -> these are routing interfaces
- f1/# -> these are switchport interfaces

General

Helpful commands for viewing interfaces, their respective mode, and their respective VLAN if configured:

```
show int status
show int summary
```

VLANs aren't saving in VLAN DB

Commands for troubleshooting VLANs not being created in the VLAN database:

```
show vlan-switch
show ip int brie
```

Cisco Extended Vlan not allowed in Current VTP mode

To extend the default VLAN range of 1 - 1000 to the full 1 - 4096 range, use:

```
vtp mode transparent
```

Setup VPC's

For the VPCs, use the following commands:

```
VPC1> ip 10.0.10.1/24
VPC2> ip 10.0.10.2/24
```

... and so on, until all VPCs are set up with the appropriate IP addresses.

Setup Switches

1. Drag 4 Ethernet Switch devices onto the GNS3 workspace.
2. Connect 2 VPCS (Virtual PC Simulator) devices to each switch.

Ensure you use the NM-16ESW module (denoted by f1/#) for host connections.

To configure the switches:

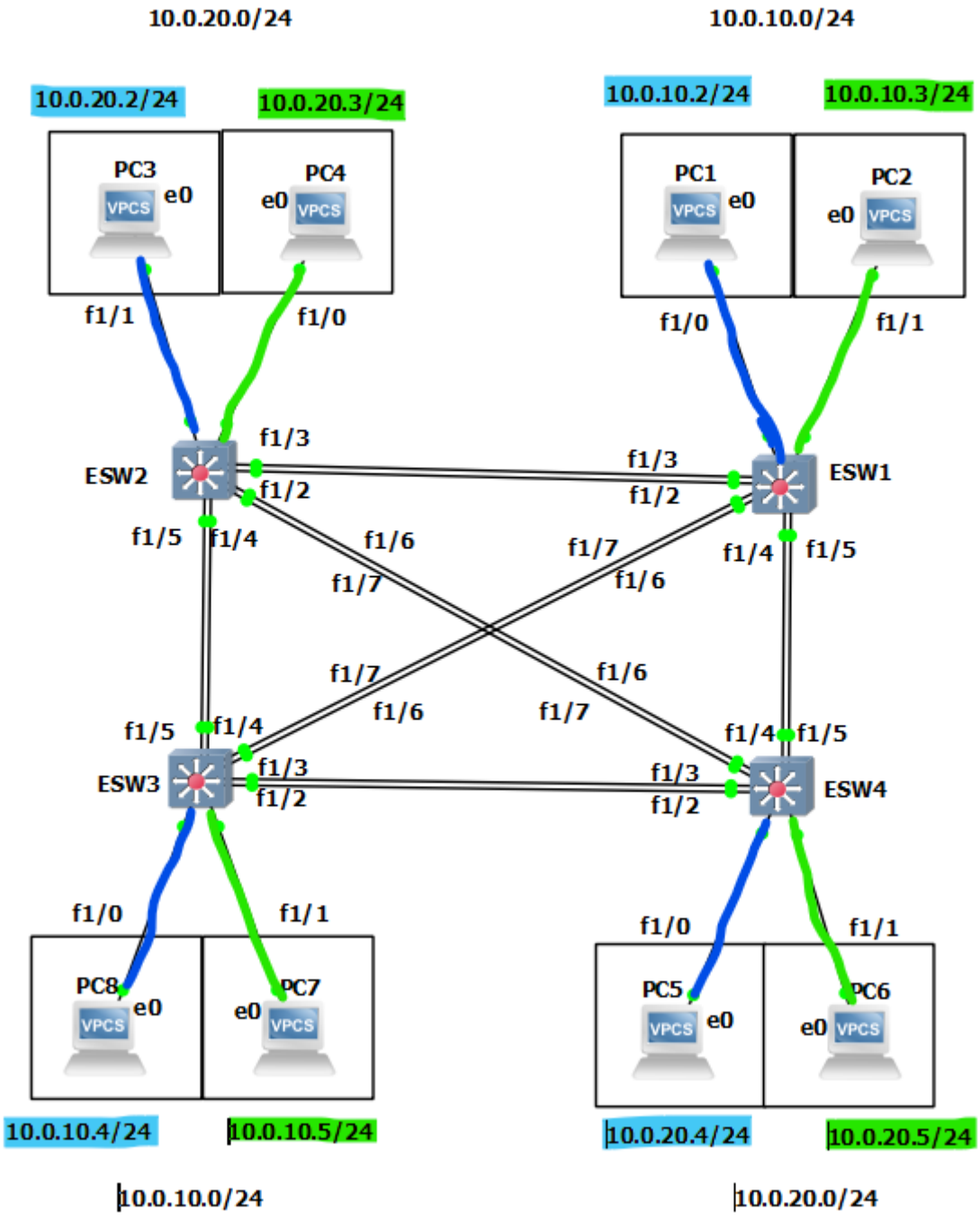
```
Switch> enable
Switch# configure terminal
Switch(config)# interface f1/0
Switch(config-if)# switchport mode access
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# do copy run start
Switch(config)# exit
Switch# write
```

Adjust the interface (`f1/0`) for your connection. Repeat for each interface.

At this point you will be able to ping between VPCs connected to the same switch. You should get the following response. If not go back and re-configure your switch

```
PC1> ping 10.0.10.3/24
84 bytes from 10.0.10.3 icmp_seq=1 ttl=64 time=0.555 ms
84 bytes from 10.0.10.3 icmp_seq=2 ttl=64 time=0.839 ms
```

Configure VLANs



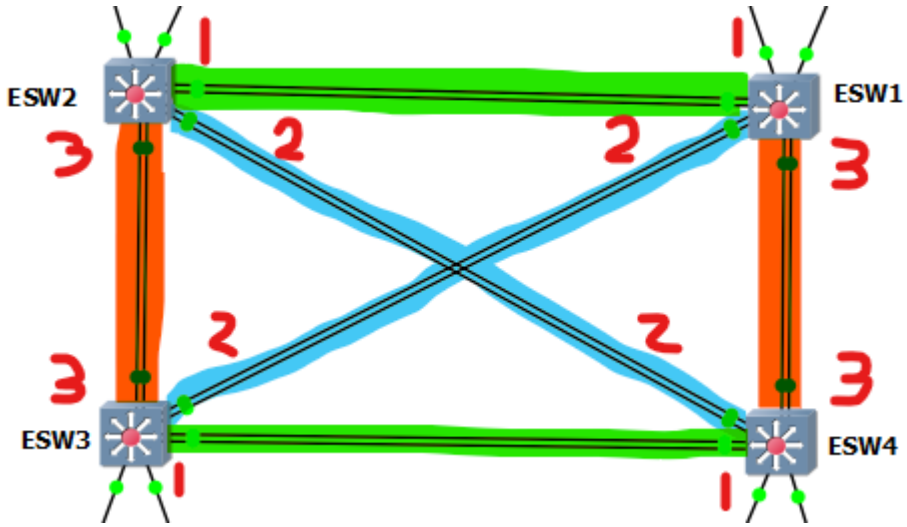
Example set up for VLANs 10 and 20 for our two subnets.

```
Switch> enable
Switch# vlan database
Switch(vlan)# vlan 10
Switch(vlan)# vlan 20
Switch(vlan)# exit
```

```
Switch# configure terminal
Switch(config)# interface f1/0
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit
Switch(config)# interface f1/1
Switch(config-if)# switchport access vlan 20
Switch(config-if)# exit
Switch(config)# do copy run start
Switch(config)# exit
Switch# write
```

Adjust the `interfaces` and `VLANs` assignments accordingly.

Setup Mesh Topology and LACP



- Green - Port channel 1
- Blue - Port channel 2
- Orange - Port channel 3

For the mesh topology, each switch needs to be interconnected with every other switch. While connecting these switches, use the `switchport mode trunk` command and specify VLANs 10 and 20 to be allowed on the trunk.

```
Switch> enable
Switch# configure terminal
Switch(config)# interface range f1/2 - 7
Switch(config-if-range)# switchport mode trunk
Switch(config-if-range)# switchport trunk allowed vlan add 10,20
Switch(config-if-range)# no shutdown
Switch(config-if-range)# exit
```

For Link Aggregation with LACP, you'll set both sides to be `on`.

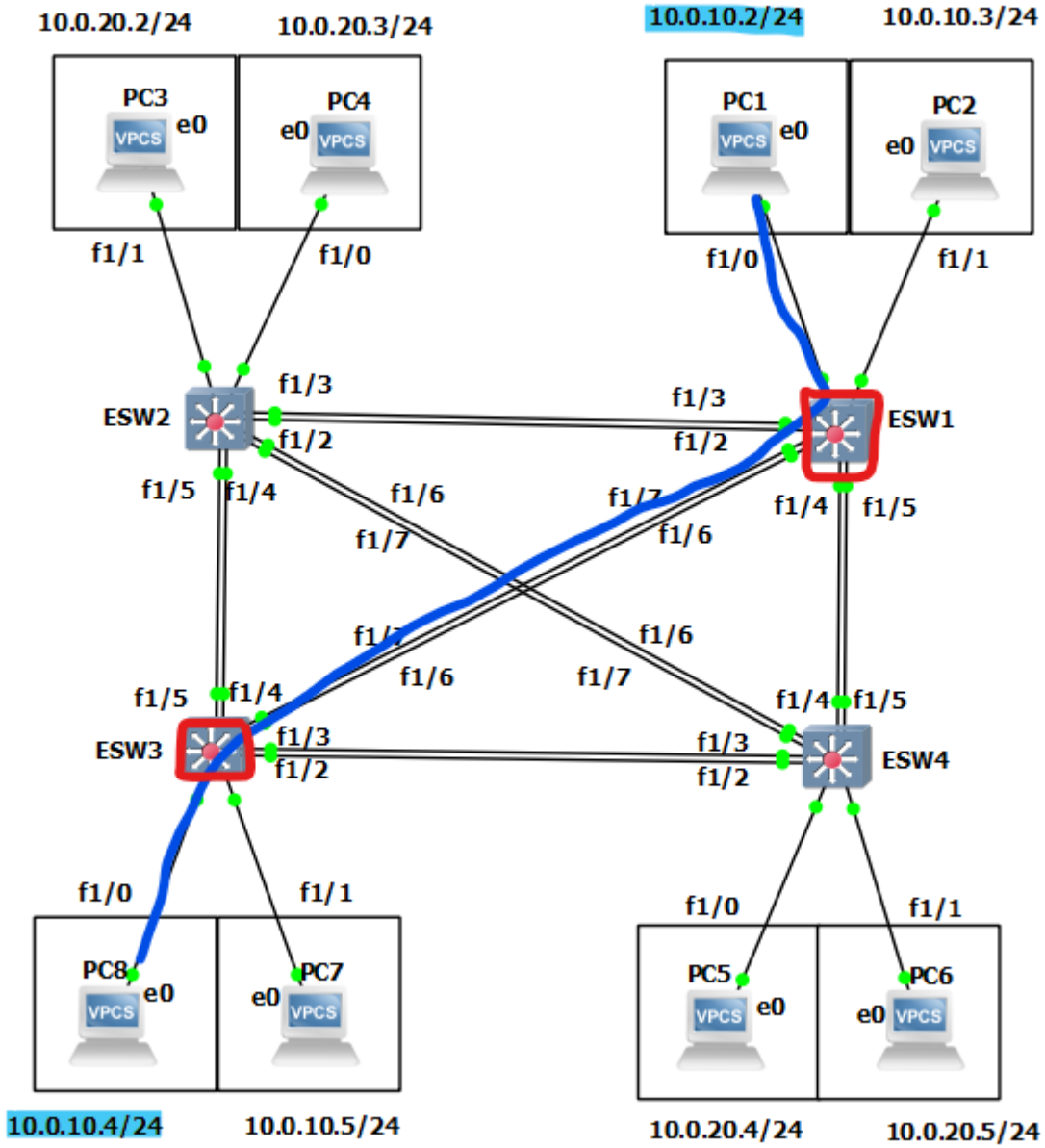
```
Switch(config)# interface range f1/2 - 3
Switch(config-if-range)# channel-group 1 mode on
Switch(config-if-range)# exit
Switch(config)# interface Port-channel 1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 10,20
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# do copy run start
Switch(config)# exit
Switch# write
```

On the other switch:

```
Switch> enable
Switch# configure terminal
Switch(config)# interface range f1/2 - 3
Switch(config-if-range)# switchport mode trunk
Switch(config-if-range)# switchport trunk allowed vlan add 10,20
Switch(config-if-range)# channel-group 1 mode on
Switch(config-if-range)# exit
Switch(config)# interface Port-channel 1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 10,20
Switch(config-if)# exit
Switch(config)# do copy run start
Switch(config)# exit
Switch# write
```

Repeat the above instructions for each pair of switches and do so according to the diagram.

In the following example if you have a pair of configured you should be able to ping as so:



Ping Response

```
PC1> ping 10.0.10.4
84 bytes from 10.0.10.4 icmp_seq=1 ttl=64 time=0.917 ms
84 bytes from 10.0.10.4 icmp_seq=2 ttl=64 time=0.997 ms
84 bytes from 10.0.10.4 icmp_seq=3 ttl=64 time=1.347 ms
84 bytes from 10.0.10.4 icmp_seq=4 ttl=64 time=1.387 ms
84 bytes from 10.0.10.4 icmp_seq=5 ttl=64 time=1.064 ms
```

VLAN Security - Dangers of VLAN 1

Virtual Local Area Networks (VLANs) are used to segment a local network into multiple distinct broadcast domains. Each VLAN is identified by a unique number (VLAN ID). When switches first come out of the box and are powered on, all ports are a member of a default VLAN, which is typically VLAN 1.

Why is VLAN 1 Potentially Dangerous?

1. **Default VLAN**: Since VLAN 1 is the default VLAN, all ports on a switch belong to it unless explicitly configured otherwise. This means that any device connected to a port that has not been specifically assigned to another VLAN will automatically be a part of VLAN 1.

2. **Management VLAN**: Many times, network administrators use VLAN 1 as the management VLAN, where switch management interfaces are assigned. If an attacker gains access to VLAN 1, they may potentially gain access to management functions of the switch.

3. **Cannot be Deleted**: VLAN 1 cannot be removed from a switch, and all unused ports are typically members of VLAN 1 by default. This provides an opportunity for attackers to exploit these unused ports.

4. **VLAN Hopping Attacks**: This is a primary concern with VLAN 1. In a VLAN hopping attack, a malicious user can send packets to or receive packets from a VLAN that the attacker's port is not natively a part of. One of the methods to perform VLAN hopping is by taking advantage of the default configuration of VLAN 1. If an attacker can access a port on VLAN 1, they might be able to exploit it to hop onto other VLANs.

Preventative Measures:

1. **Assign All Ports to Specific VLANs**: Even if a port is not in use, it should be assigned to a specific "dummy" VLAN that is not used for any network operations. This ensures that even if someone connects a device to an unused port, they won't have access to VLAN 1 or any other operational VLAN.

2. **Disable Unused Ports**: If a port is not in use, it's a good practice to disable it. This reduces the chances of unauthorized devices being connected to the switch.

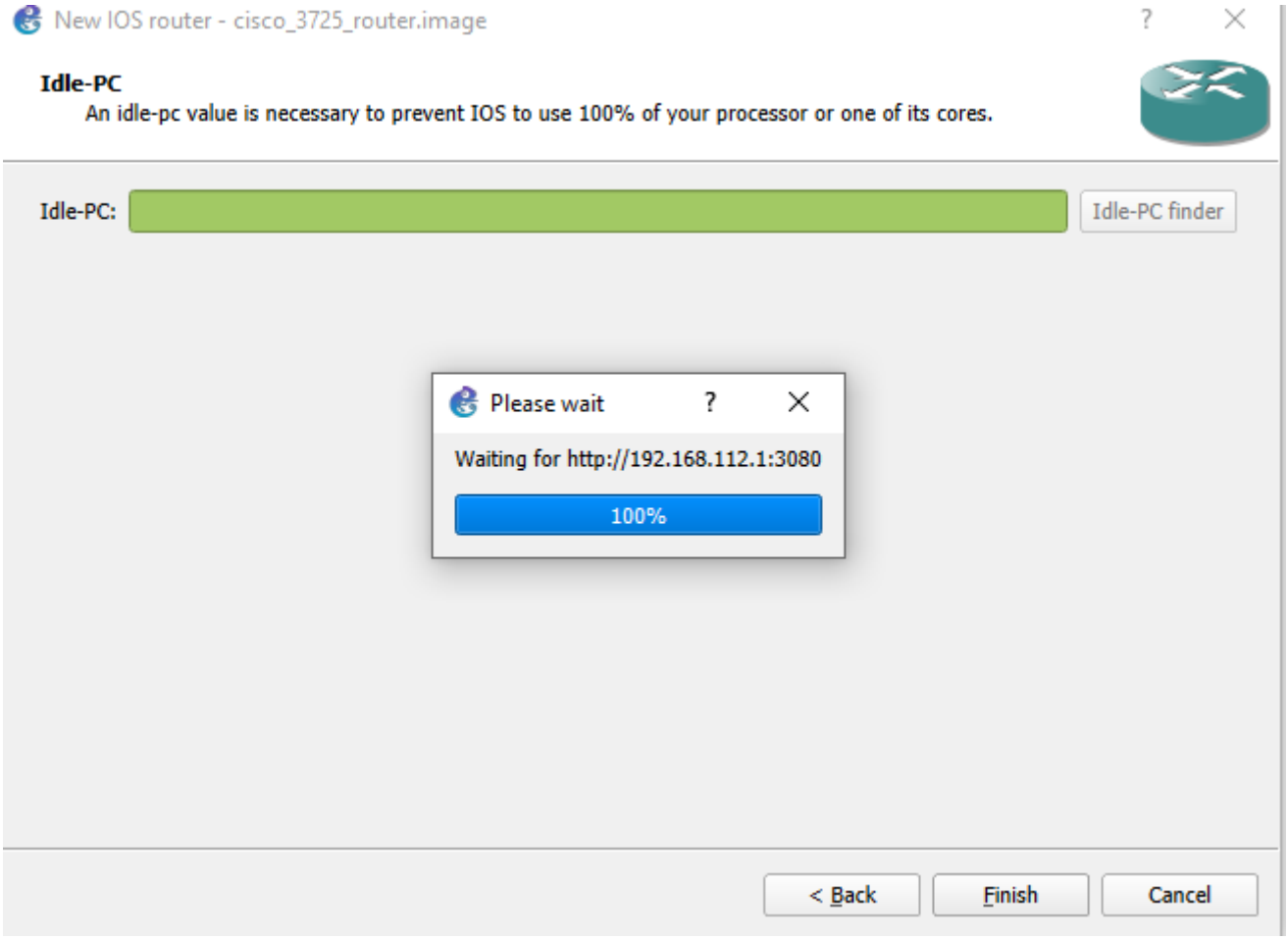
3. **Use a Different VLAN for Management**: Instead of using VLAN 1 for switch management, use a different, non-default VLAN. This way, even if someone gains access to VLAN 1, they won't have access to the management functions of the switch.

4. **Secure Trunk Ports**: Ensure that trunk ports, which carry traffic for multiple VLANs, are securely configured. Explicitly define which VLANs are allowed on the trunk and do not rely on the default "all" setting.

In summary, while VLAN 1 serves as a default and often a management VLAN, its widespread use and default behaviors make it a potential security risk. Best practices recommend avoiding its use for data or management traffic and ensuring that all ports are explicitly configured, leaving no port in its default state.

Final Note on All GNS3 Devices

Reminder: Set Idle-PC on each device to manage CPU usage.



Pass-off

For the lab pass-off, ensure:

1. Four switches are set up in a mesh topology.
2. Each switch has two VPCs connected.
3. VPCs are segmented into two IP subnets and VLANs (10.0.10.0/24 for VLAN 10 and 10.0.20.0/24 for VLAN 20).
4. LACP is set up between switches.
5. A screenshot of your network
6. A screenshot of your "show vlan brief" output confirms no interfaces are on VLAN 1.
7. A screenshot of a successful ping test that confirms connectivity across the network

Credit

All image credits to the GNS3 Software.

Lab by Nathan Moser, with thanks to Bryan Wood for the foundational lab concepts and structure.