

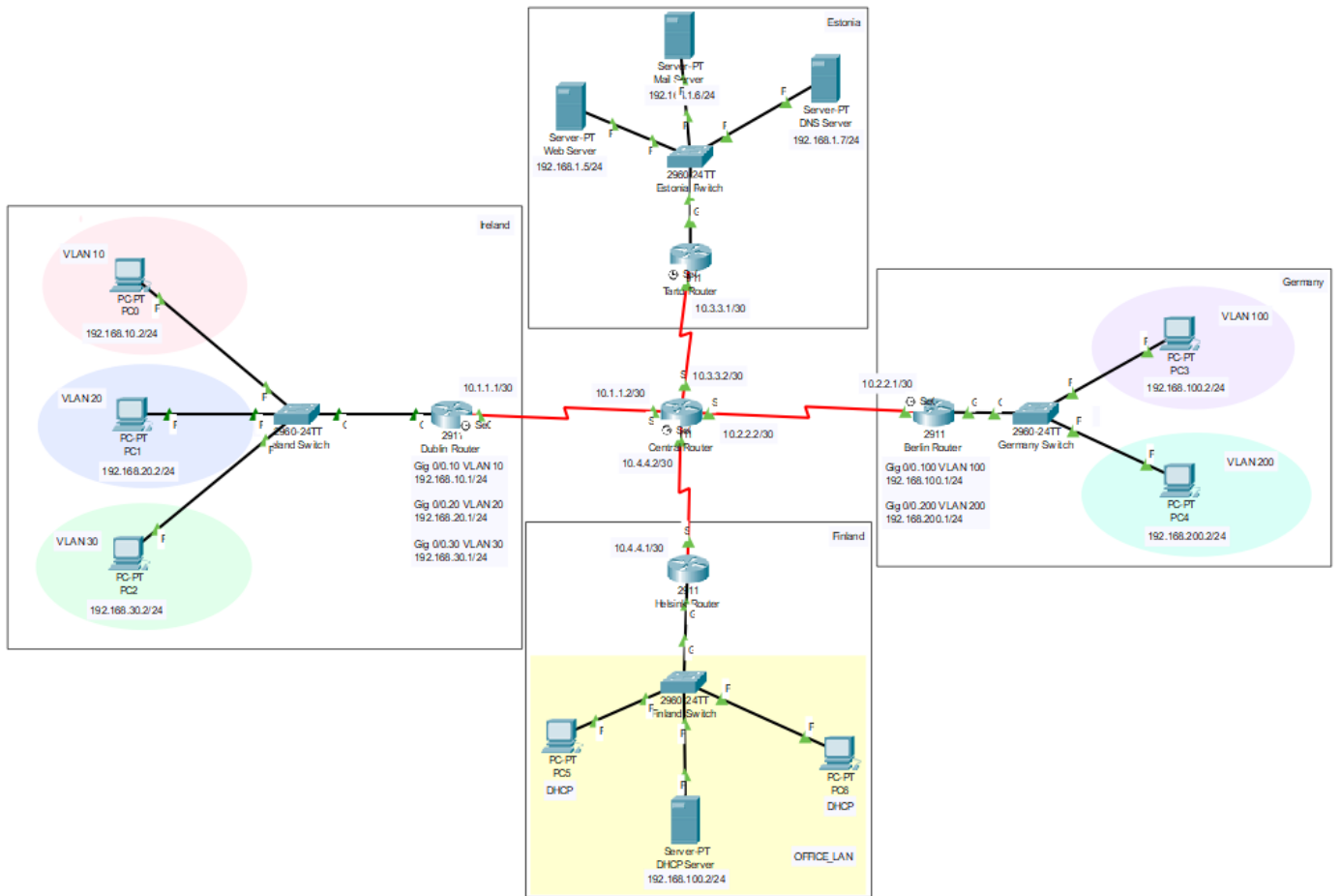
COM 5335 : NETWORK SECURITY ASSIGNMENT#3

108064535 陳文遠 WEN-YUAN CHEN (Chris)

A. Show my assign IP address and other information list in the following table.

- The device information under each VLAN

Devices	Interface	IP / Mask	Gateway	VLAN
PC0 (Ireland)	NIC	192.168.10.2/24	192.168.10.1	10
PC1 (Ireland)		192.168.20.2/24	192.168.20.1	20
PC2 (Ireland)		192.168.30.2/24	192.168.30.1	30
PC3 (Germany)	NIC	192.168.100.2/24	192.168.100.1	100
PC4 (Germany)		192.168.200.2/24	192.168.200.1	200
PC5 (Finland)	NIC	DHCP	192.168.100.1	N/A
PC6 (Finland)				
DHCP Server (Finland)	NIC	192.168.100.2/24	192.168.100.1	
Web Server (Estonia)	NIC	192.168.1.5/24	192.168.1.1	N/A
Mail Server (Estonia)		192.168.1.6/24		
DNS Server (Estonia)		192.168.1.7/24		
Dublin Router (Ireland)	G0/0.10	192.168.10.1/24	N/A	N/A
	G0/0.20	192.168.20.1/24		
	G0/0.30	192.168.30.1/24		
	S0/0/0	10.1.1.1/30		
Berlin Router (Germany)	G0/0.100	192.168.100.1/24	N/A	N/A
	G0/0.200	192.168.200.1/24		
	S0/0/0	10.2.2.1/30		
Tartu Router (Estonia)	G0/0	192.168.1.1/24	N/A	N/A
	S0/0/0	10.3.3.1/30		
Helsinki Router (Finland)	G0/0	192.168.100.1/24	N/A	N/A
	S0/0/0	10.4.4.1/30		
Central Router (Our company)	S0/0/0	10.1.1.2/30	N/A	N/A
	S0/0/1	10.2.2.2/30		
	S0/1/0	10.3.3.2/30		
	S0/1/1	10.4.4.2/30		







B. What are the purposes of Configure the Standard Access Control List?

Cisco provides basic traffic filtering capabilities with Access Control List (ACL). Access Control List can be configured for all routed network protocols (such as IP and so on) to filter those protocols' packets as the packets pass through a router.

C. What are the “RIPv2” and “OSPF”?

1. RIPv2

Routing Information Protocol (RIP) is suitable for small network environments and low reliability network. It can let router dynamically appropriate the variety of network by continuously exchanging information. In this protocol, routers exchange information with neighboring routers every 30 seconds to dynamically build routing tables. RIPv2 is a modified version of RIPv1, it improves the following points on the basis of RIPv1.



-  Supports Route Tag. It has flexible routing control according to Tag in routing strategy.
-  The packet carries mask information and supports route aggregation and CIDR.
-  Only RIPv2 devices can receive protocol messages, which reduces resource consumption.
-  Supports verification of protocol messages to enhance security.

2. OSPF

Open shortest Path First (OSPF) is a routing protocol based on IP protocol. Compare to RIP, it's more suitable for large network environments. It takes Dijkstra's algorithm to calculate the shortest path tree. Also, OSPF offers the concept of 「Area」, a network can be consisted of a single area or multiple areas. Among them, area 0 is called Backbone Area, this area is the core of the whole OSPF network and directly connected with other areas.

D. What is the VLAN hopping?

VLAN hopping is a kind of computer security exploit, it's a method of attacking the network resources on VLAN. This attack's basic concept is for an attacking host on a VLAN to gain access to traffic on other VLANs that would normally not be accessible. There are two primary method of VLAN hopping : 「 Switched Spoofing 」 and 「 Double Tagging 」 .

-  **Switched Spoofing** : Attacker masquerades as a switch to spoof the legal one and create a checkpoint between them. Once the trunk link be created, attacker will can access all the information from arbitrary VLAN.
-  **Double Tagging** : Attacker add or modify tags on Ethernet frames, allowing packets to be transmitted over any VLAN, this kind of technology is called Double Tagging.

There are three conditions of forming VLAN hopping :

1. Attacker must connect to a switch's Access Port.
2. The switch turns on 802.1Q Trunk.
3. The Trunk must treat the attacker's Access VLAN as its Native VLAN.

There are two solutions of VLAN hopping :

1. Set up native VLAN of trunk as a useless VLAN.
2. Force switch set up VLAN Tag on all of packets.

E. What is the DHCP spoofing?

DHCP spoofing is a kind of DDOS. It could let DHCP server has no assignable DHCP address. As a result, the normal devices in this network cannot obtain dynamic IP address. At the same time, hackers also can impersonate as a DHCP server and allocate a modified DNS server address to lead you to a fake website.

There three solutions of DHCP spoofing :

1. Enable DHCP snooping on switch port.
2. Show request rate.
3. Limit the amount of MAC address on switch port.

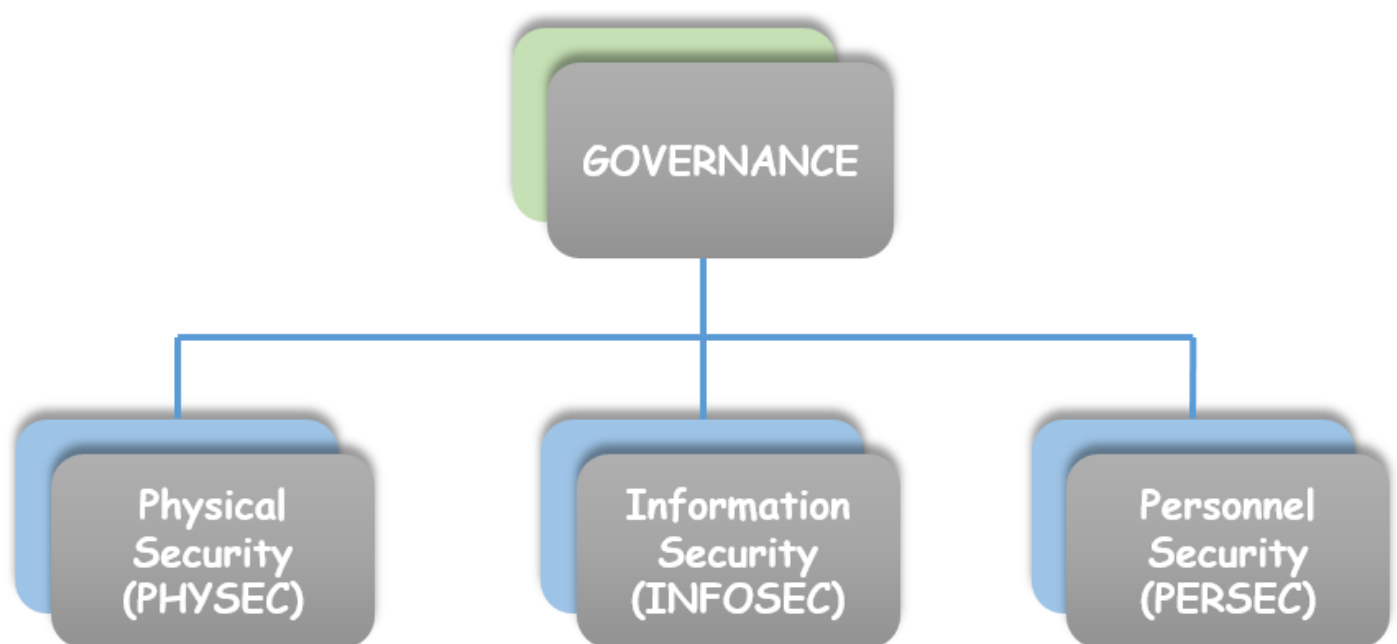
F. Describe the security implications of a native VLAN.

We should never use the default VLAN either because VLAN hopping is much more easily accomplished from the default VLAN. But what we have to remember that the security risk is more to do with VLAN 1 (default VLAN) being set as a native VLAN. We should change the native VLAN from VLAN 1 to a new VLAN we create. The native VLAN is used for a lot of management data such as DTP, VTP and CDP frames and also BPDU's for spanning tree.

If we are using VLAN 1 as our native VLAN, we have all the ports that we haven't configured to be part of this VLAN. So if an attacker connects to a port that is not used and not configured, he(he) has straight away access to our management VLAN and can read and inject packets that could allow VLAN hopping or capture packets we don't want him/her to see.

G. Describe the one of the network security architecture/framework. I take PSR framework as an example.

NZISM Protective Security Requirements (PSR) Framework is New Zealand's national technical security policy, and it describes baseline and minimum mandatory security standards for government departments and agencies. It forms an important part of the New Zealand Security Intelligence Service's Protective Security Requirements (PSR) framework, which sets out the Government's expectations for managing personnel, information and physical security. The following figure is a simplified framework of PSR.



H. List 10 important commands I use in this assignment and describe the reason what is the main purpose to use them.

1. **copy running-config startup-config**

After you do any change in your device, please use this command to write your records into device memory. If you haven't do this command before you shutdown your device, you will lose all records.

2. **VLAN 10**

Used to create our own VLAN rather than using default VLAN.

3. **switchport access vlan 10 & switchport mode access**

Put the specific interface into VLAN 10.

4. **show vlan brief**

Show up all VLAN configurations of specific device.

5. **interface gigabitEthernet 0/0.10**

Create a new sub-interface for VLAN 10.

6. **encapsulation dot1Q 10**

To enable IEEE 802.1Q encapsulation of traffic on a specified subinterface, use the encapsulation dot1Q command. To disable encapsulation, use no form of this command.

7. **router ospf 1**

Enter ospf routing protocol configuration.

8. **network 192.168.10.0 0.0.0.255 area 0**

Add new IP address into ospf routing protocol area 0.

9. **password XXX & login**

Set up password and activate.

10. **line vty 0 4**

Configure the incoming vty lines on router.

I. List all the commands I use in this assignment.

- Configure within the **Ireland Switch**

```
> enable
# configure terminal
(config)# VLAN 10
(config)# VLAN 20
(config)# VLAN 30
(config)# interface fastEthernet 0/1
(config-if)# switchport access vlan 10
(config-if)# switchport mode access
(config)# interface fastEthernet 0/2
(config-if)# switchport access vlan 20
(config-if)# switchport mode access
(config)# interface fastEthernet 0/3
(config-if)# switchport access vlan 30
(config-if)# switchport mode access
(config-if)# end
# show vlan brief
(config)# interface gigabitEthernet 0/1
(config-if)# no shutdown
(config-if)# switchport mode trunk
# show run
# copy running-config startup-config
```

- Configure within the **Dublin Router**

```
> enable
# configure terminal
(config)# interface gigabitEthernet 0/0
(config-if)# no shutdown
(config)# interface gigabitEthernet 0/0.10
(config-subif)# encapsulation dot1Q 10
(config-subif)# ip address 192.168.10.1 255.255.255.0
(config)# interface gigabitEthernet 0/0.20
(config-subif)# encapsulation dot1Q 20
(config-subif)# ip address 192.168.20.1 255.255.255.0
(config)# interface gigabitEthernet 0/0.30
(config-subif)# encapsulation dot1Q 30
(config-subif)# ip address 192.168.30.1 255.255.255.0
# show run
# show ip route
```

```
(config)# line console 0
(config-line)# password ireland@cisco
(config-line)# login
(config)# enable password ireland@cisco
(config)# line vty 0 4
(config-line)# password ciscocisco
(config-line)# login
(config)# router ospf 1
(config-router)# network 192.168.10.0 0.0.0.255 area 0
(config-router)# network 192.168.20.0 0.0.0.255 area 0
(config-router)# network 192.168.30.0 0.0.0.255 area 0
(config-router)# network 10.1.1.0 0.0.0.3 area 0
# copy running-config startup-config
```

- Configure within the **Germany Switch**

```
> enable
# configure terminal
(config)# VLAN 100
(config)# VLAN 200
(config)# interface fastEthernet 0/1
(config-if)# switchport access vlan 100
(config-if)# switchport mode access
(config)# interface fastEthernet 0/2
(config-if)# switchport access vlan 200
(config-if)# switchport mode access
(config-if)# end
# show vlan brief
(config)# interface gigabitEthernet 0/1
(config-if)# no shutdown
(config-if)# switchport mode trunk
# show run
# copy running-config startup-config
```

- Configure within the **Berlin Router**

```
> enable
# configure terminal
(config)# interface gigabitEthernet 0/0
(config-if)# no shutdown
(config)# interface gigabitEthernet 0/0.100
(config-subif)# encapsulation dot1Q 100
(config-subif)# ip address 192.168.100.1 255.255.255.0
(config)# interface gigabitEthernet 0/0.200
```



```
(config-subif)# encapsulation dot1Q 200
(config-subif)# ip address 192.168.200.1 255.255.255.0
# show run
# show ip route
(config)# line console 0
(config-line)# password germany@cisco
(config-line)# login
(config)# enable password germany@cisco
(config)# line vty 0 4
(config-line)# password ciscocisco
(config-line)# login
(config)# router ospf 1
(config-router)# network 192.168.100.0 0.0.0.255 area 0
(config-router)# network 192.168.200.0 0.0.0.255 area 0
(config-router)# network 10.2.2.0 0.0.0.3 area 0
# copy running-config startup-config
```

- Configure within the **Tartu Router**

```
> enable
# configure terminal
(config)# line console 0
(config-line)# password tartu@cisco
(config-line)# login
(config)# enable password tartu@cisco
(config)# line vty 0 4
(config-line)# password ciscocisco
(config-line)# login
(config)# router ospf 1
(config-router)# network 192.168.1.0 0.0.0.255 area 0
(config-router)# network 10.3.3.0 0.0.0.3 area 0
# copy running-config startup-config
```

- Configure within the **Helsinki Router**

```
> enable
# configure terminal
(config)# line console 0
(config-line)# password finland@cisco
(config-line)# login
(config)# enable password finland@cisco
(config)# line vty 0 4
(config-line)# password ciscocisco
(config-line)# login
```

```
(config)# router ospf 1
(config-router)# network 192.168.100.0 0.0.0.255 area 0
(config-router)# network 10.4.4.0 0.0.0.3 area 0
# copy running-config startup-config
```

- Configure within the Central Router

```
> enable
# configure terminal
(config)# router ospf 1
(config-router)# network 10.1.1.0 0.0.0.3 area 0
(config-router)# network 10.2.2.0 0.0.0.3 area 0
(config-router)# network 10.3.3.0 0.0.0.3 area 0
(config-router)# network 10.4.4.0 0.0.0.3 area 0
# copy running-config startup-config
```