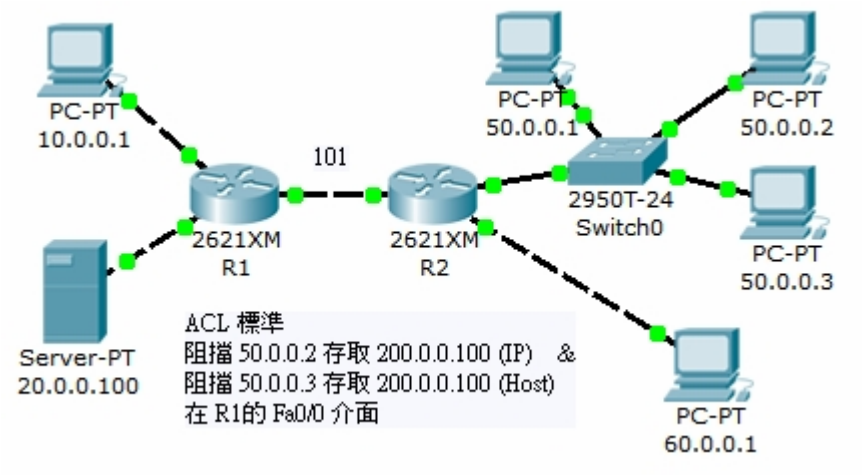
a. Please show your assign ip address list in the table.

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

Access Control List **(ACL)** is a schema that control the packet flow to filter or restrict the network use by certain users or devices. ACL can be created for specific network protocol and applied to certain interface. When we use ACLs, we are defining the permission list for each processed packet from networks. Packet that doesn't match the permission list will be automatically blocked by the default setting "deny all traffic".



There are three types of ACLs: Standard IP ACLs, Extended IP ACLs and Named ACLs. Standard ACL identifies the destination IP address (Note: not source address) of OSPF routes for redistribution. Standard ACL can't be applied to interfaces to control the network traffic.

Reference:

https://blog.xuite.net/tolarku/blog/38160949-%5BCCNA%5D+Cisco+Router+%E5%AD%98%E5%8F%96%E6%8E%A7%E5%88%B6+-+ACL+-+Standard

c. What are the 'RIPv2' and 'OSPF?

Routing Information Protocol version2 **(RIPv2)** is a routing protocol commonly used for network routing. It is a kind of interior gateway protocol that it routes the packets within a single autonomous system (AS), for example, LAN. RIPv2 protocol sends routing information among the computers on the LAN. When a PC receives RIPv2 routing information that includes changes to an entry, it will update its routing table to renew the new routing.

Open Shortest Path First **(OSPF)** is another routing protocol usually comparing to RIPv2. It is a linking state protocol. A link can be considered an interface on the router, and the state of the link is a description of that interface and of its relationship to its neighboring routers. All these linking states constitute a link-state database. OSPF protocol uses linking state algorithm (Dijkstra Algorithm) to calculate the shortest path to all known routing destinations. Following is the difference between RIP and OSPF

Features	RIP		OSPF
	Version 1	Version 2	
Algorithm	Bellman-Ford		Dijkstra
Path Selection	Hop based		Shortest Path
Routing	Classful	Classless	Classless
Transmission	Broadcast	Multicast	Multicast
Administrative Distance	120		*110*
Hop Count Limitation	15		No Limitation
Authentication	No	MD5	MD5
Protocol	UDP		IP
Convergence Time	RIP>OSPF		

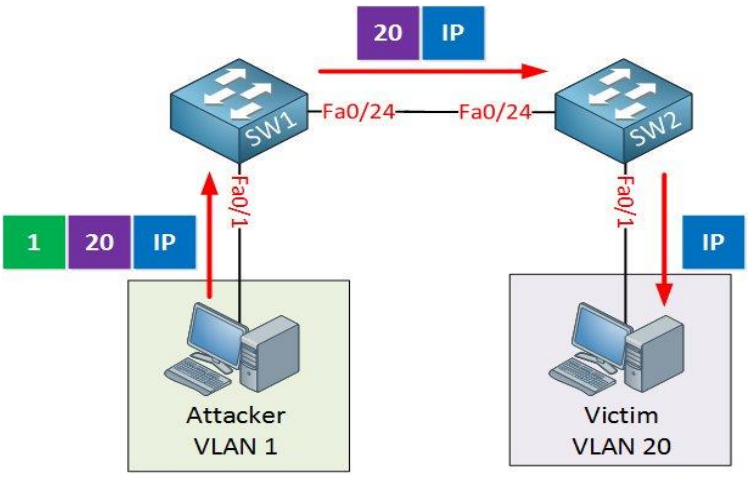
Reference:

https://www.netadmin.com.tw/article_content.aspx?sn=1004160020

http://resources.intenseschool.com/rip-vs-ospf-which-is-better-for-your-network/

d. What is the VLAN hopping?

VLAN hopping is an attacking method to the network resources on a VLAN. The basic concept of VLAN hopping attacks is that a malicious host on a VLAN try to illegally access other VLANs. There are two general methods of VLAN hopping: 1. switch spoofing and 2. double tagging. Both attack methods can be mitigated by the proper configuration of switch port.

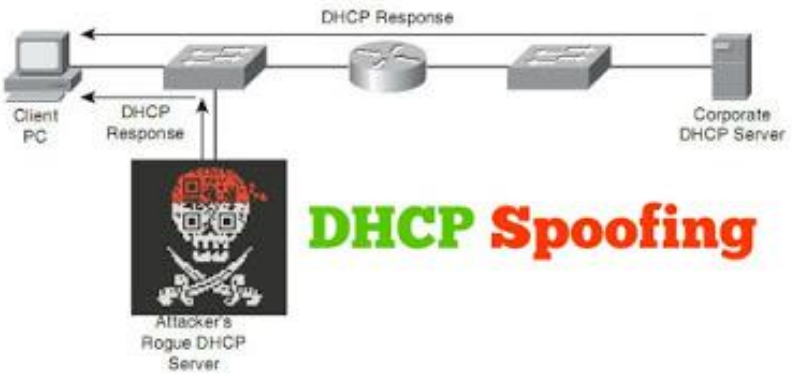


Reference:

https://en.wikipedia.org/wiki/VLAN_hopping

e. What is the DHCP spoofing?

DHCP spoofing is a network attack that the attacker listens for victim's DHCP requests and answers them with fake DHCP response before the authorized DHCP response sends to the clients. The fake DHCP Response may give a malicious IP address as the client's default gateway. All the traffic sent from victim clients will go through the attacker's computer, so the attacker may eavesdrop the network packets or do "man-in-the-middle" attacks.

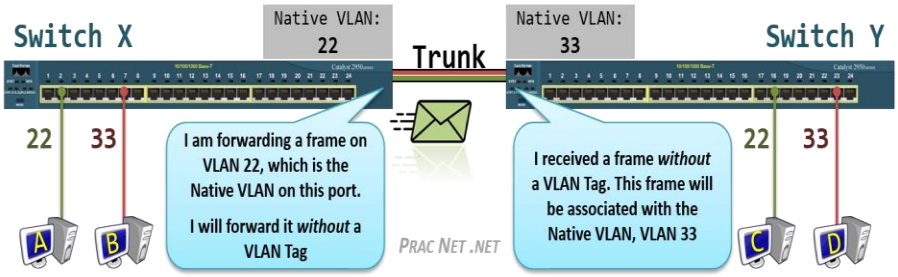


Reference:

http://ccnp300-115.blogspot.com/2016/08/dhcp-snooping.html

f. Please describe the security implications of a native VLAN.

First, let me explain what is a native VLAN. It's part of the VLAN interface that untagged traffic received on a trunk port will be forward into. Assume you have a trunk port including VLANs 10, 20, and 30. VLAN 10 is by default set as the native VLAN. Any packet received on that port with specific tag will be forwarded into the corresponding VLAN. In contrast, any packet that has no tag will be put into VLAN 10 since it is the native VLAN.



As to the implications of native VLANs, I found a basic rule on the internet *"You should never use the default VLAN either because VLAN hopping is much more easily accomplished from the default VLAN."* Besides, we can also use a Native VLAN that is outside of the range permitted for the customer and tag the native VLAN in the cloud.

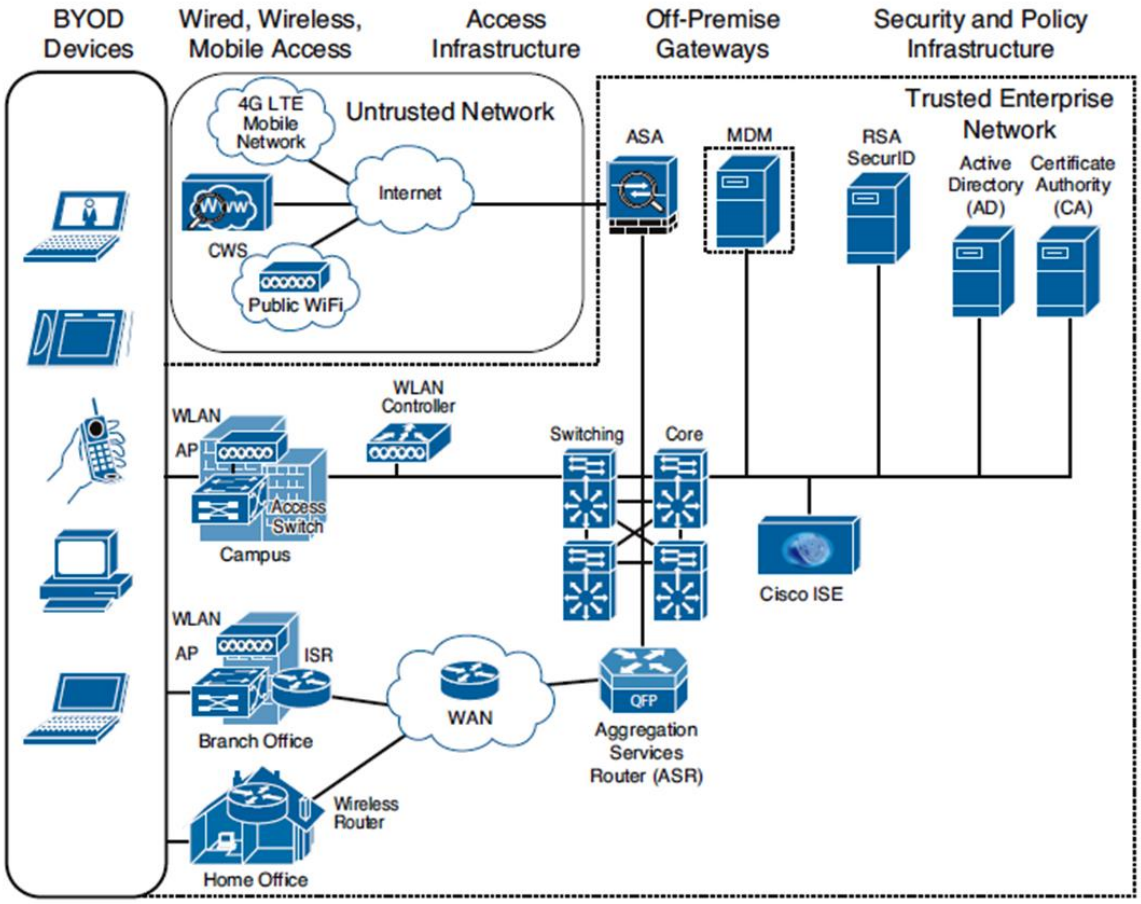
Reference:

https://networkengineering.stackexchange.com/questions/32737/why-should-the-native-vlan-never-be-used

g. Please describe the BYOD architecture framework.

BYOD refers to as “Bring Your Own Device”. It means the employees can bring their own computing devices, for example, smart phones and laptops to work with them instead of using company-supplied devices.

Now, employees usually use their own laptops and mobile devices while working. A BYOD policy designed to control the use of such devices is important in terms of mitigating BYOD's information security risks. BYOD may boost employees’ productivity and morale; however, it may cause some problems regarding to security issues. Because BYOD devices aren't strictly controlled by an organization, it may increase the risk of company data breaches.



Example: High-Level BYOD Solution Architecture

Reference:

https://www.moigetech.co.ke/index.php/tech-news-and-info/148-byod-architecture-framework

https://www.techopedia.com/definition/29070/bring-your-own-device-byod

h. Please list 10 important commands you use in this assignment and describe the reason what is the main purpose to use them.

> enable **// also known as “en”, switch to the privileged mode**

configure terminal **// the first step to configure the CLI**

hostname twroc@cisco **// to set the user host name**

enable password nihao **// set the VTY password as 'nihao'**

// After separate the VLAN, we grant the access right of that VLAN

interface range fastEthernet0/1-8

switchport mode access

switchport access vlan 10

no shutdown **// bring the interface up**

router ospf processID **// use the OSPF protocol as routing method**

access-list [number] permit/deny IP address **// the beginning setting of the ACLs**

show running-config **// to check the configuration is correct or not**

i. Please list all the commands you use in this assignment.