

NASA hw3

Author: B09902011 陳可邦

NA

VLAN, access & trunk

- Gi/0/3 is an access port, therefore when it receive an untagged packet, it will add VLAN 307 tag on it.
 - Gi/0/4 is a trunk port, therefore it will try to match the VLAN ID of the packet with the Native VLAN ID the port, in this case it matches (VLAN 1), so it would be sent without .1q tag.
 - Gi/0/5 is a trunk port, therefore it will try to match the VLAN ID of the packet with the Native VLAN ID the port, in this case it does not match, so it will add VLAN 307 tag on it.
2. Packets sent from host A must have VLAN 424 header, and when Gi/0/1 gets it, the switch will strip the header, and send out the untagged packet from Gi/0/2.
3. If the admin wants to see what all of these untagged packets are doing, they can use native trunk to point it to an unused VLAN only the admin can see.

<https://www.pcwldd.com/tagged-untagged-and-native-vlans>

More on link aggregation

1. No. IEEE standard requires each link have identical speed, if you try to do link aggregation with two cables with different speed, most device will throw an error.

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

2. channel-group mode in LACP can not all be set to passive, or the port channel can not be set up. To fix this, set any of Gi1/0/1 and Gi1/0/2 to be `channel-group 1 mode active`.

Source: 上課簡報

Malicious User

1. L2 Switches only does switching based on MAC address (Layer 2), while L3 switches can handle IP headers and have routing tables, so it can create subnets in a LAN.

Routers can connect to WAN, and can support layer 3 features like NAT, firewall, etc. L3 switches can only do things inside a LAN, but is generally faster.

<https://community.fs.com/blog/layer-2-switch-vs-layer-3-switch-which-one-do-you-need.html>

<http://www.fiber-optic-equipment.com/layer-3-switch-vs-router-choose.html>

2. ARP table match an IP to a MAC address, MAC address table match an MAC address to a port on a switch.

<https://eeepage.info/arp-mac-tale>

3. Start at the core switch, use `show arp | include <IP>` to find which L2 switch it is on, and its MAC address. Then on the edge switch, use `show mac address-table | include <MAC>` to find which port the target is connected on.

Source: cisco documentations

Set up another Cisco switch

1. Serial communication means transferring 1 bit at a time continuously, as opposed to transferring multiple bits in parallel.

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

2. Pro: It's the only way to connect to a brand new machine

Con: You can not use them while you're not with the machine

<https://www.jannet.hk/zh-Hant/post/console-cable/>

3. If you have previously configured remote connection methods such as Telnet or SSH, you can use them, else you just simply can't do that.

<http://www.james-tw.com/cisco/cisco-she-ding-yuan-duan-lian-xian-telnet-ssh>

4. Stacking makes multiple switches act like one device with all the port in the stack. This enables you to expand bandwidth as much as possible, also providing link redundancy, can still work when one of the link brakes.

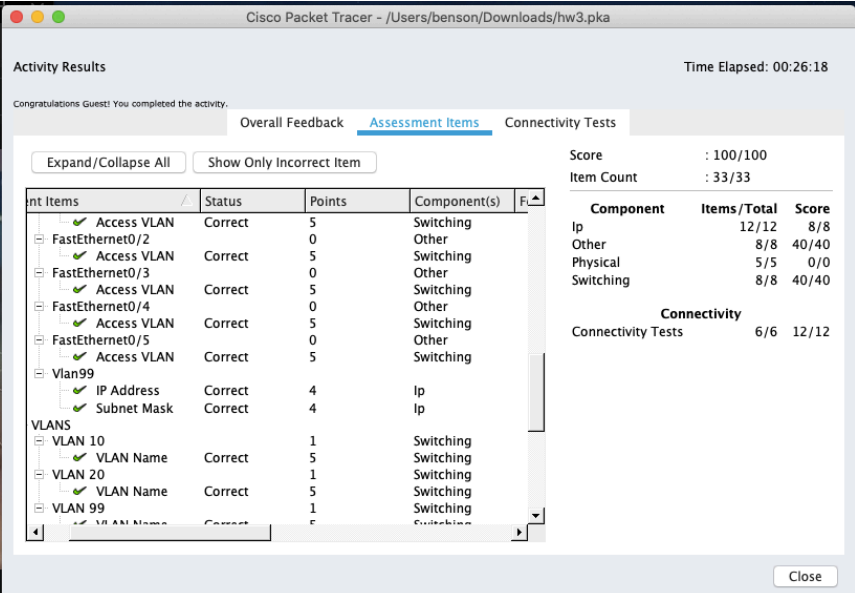
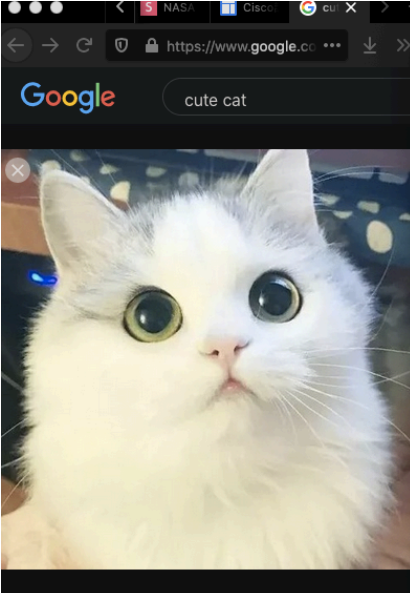
2 switches require 2 stack cable to work.

<https://community.fs.com/blog/switch-stacking-vs-trunking-vs-uplink-which-is-best-to-connect-switches.html>

Cisco Packet Tracer

```
enable
conf t
# 1
hostname CiscoLab
# 2
no ip domain-lookup
# 3
enable password CISCO
service password-encryption
# 4, 5, 6
int range fa0/1-2
switchport access vlan 10
int range fa0/3-4
switchport access vlan 20
int fa0/5
switchport access vlan 99
exit

line vty 0 4
password cisco
int vlan 99
ip address 192.168.99.1 255.255.255.0
no shutdown
exit
```



The screenshot shows the Cisco Packet Tracer interface with the 'Activity Results' window open. The window displays a congratulatory message and a table of assessment items. The table has columns for 'Item(s)', 'Status', 'Points', and 'Component(s)'. The items are categorized into 'Access VLAN', 'VLAN 99', and 'VLAN 10'. The 'Access VLAN' section shows 12 items, all 'Correct', with a total score of 8/8. The 'VLAN 99' section shows 2 items, both 'Correct', with a total score of 4/4. The 'VLAN 10' section shows 3 items, all 'Correct', with a total score of 12/12. The overall score is 100/100.

Item(s)	Status	Points	Component(s)
Access VLAN	Correct	5	Switching
FastEthernet0/2	Correct	0	Other
Access VLAN	Correct	5	Switching
FastEthernet0/3	Correct	0	Other
Access VLAN	Correct	5	Switching
FastEthernet0/4	Correct	0	Other
Access VLAN	Correct	5	Switching
FastEthernet0/5	Correct	0	Other
Access VLAN	Correct	5	Switching
Vlan99			
IP Address	Correct	4	Ip
Subnet Mask	Correct	4	Ip
VLAN 10			
VLAN Name	Correct	1	Switching
VLAN 20			
VLAN Name	Correct	1	Switching
VLAN 99			
VLAN Name	Correct	1	Switching

Score : 100/100
Item Count : 33/33

Component Items/Total Score
Ip 12/12 8/8
Other 8/8 40/40
Physical 5/5 0/0
Switching 8/8 40/40

Connectivity
Connectivity Tests 6/6 12/12

Bonus cat picture because why the hell not

SA

1

```
valid_lft forever preferred_lft forever
[nasa@localhost ~]$ ping 192.168.204.141
PING 192.168.204.141 (192.168.204.141) 56(84) bytes of data:
64 bytes from 192.168.204.141: icmp_seq=1 ttl=128 time=0.425 ms
64 bytes from 192.168.204.141: icmp_seq=2 ttl=128 time=1.11 ms
64 bytes from 192.168.204.141: icmp_seq=3 ttl=128 time=1.25 ms
64 bytes from 192.168.204.141: icmp_seq=4 ttl=128 time=1.19 ms
64 bytes from 192.168.204.141: icmp_seq=5 ttl=128 time=1.15 ms
64 bytes from 192.168.204.141: icmp_seq=6 ttl=128 time=1.14 ms
64 bytes from 192.168.204.141: icmp_seq=7 ttl=128 time=1.10 ms
^C
--- 192.168.204.141 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6016ms
rtt min/avg/max/mdev = 0.425/1.057/1.253/0.263 ms
[nasa@localhost ~]$ _
```

命令提示字元

```
連線特定 DNS 尾碼 . . . . . :
連結-本機 IPv6 位址 . . . . . : fe80::cd08:7fb0:244b:239b%17
IPv4 位址 . . . . . : 192.168.15.1
子網路遮罩 . . . . . : 255.255.255.0
預設閘道 . . . . . :

C:\Users\student>ping 192.168.15.128

Ping 192.168.15.128 (使用 32 位元組的資料):
回覆自 192.168.15.128: 位元組=32 時間<1ms TTL=64
回覆自 192.168.15.128: 位元組=32 時間<1ms TTL=64
回覆自 192.168.15.128: 位元組=32 時間<1ms TTL=64
回覆自 192.168.15.128: 位元組=32 時間<1ms TTL=64

192.168.15.128 的 Ping 統計資料:
    封包: 已傳送 = 4, 已收到 = 4, 已遺失 = 0 (0% 遺失),
    大約的來回時間 (毫秒):
        最小值 = 0ms, 最大值 = 0ms, 平均 = 0ms

C:\Users\student>
```

```
sudo yum install virt-install qemu-kvm libvirt -y
systemctl enable libvirtd
systemctl start libvirtd
```

2

1

NAT assigns the guest a subnet, and masks all traffic as if they come from the host.

Bridge network assigns a ip in the same subnet the host is in, outsider can see it along with the host.

<https://superuser.com/questions/227505/what-is-the-difference-between-nat-bridged-host-only-networking>

2

1. Edit `/etc/sysconfig/network-scripts/ifcfg-eth0`
 - comment out `BOOTPROTO`
 - Add `BRIDGE=br0`
2. Create `/etc/sysconfig/network-scripts/ifcfg-br0`
 - Add:

```
DEVICE=br0
BOOTPROTO=dhcp
ONBOOT=yes
TYPE=Bridge
```

3. `/etc/init.d/network restart`

https://www.linux-kvm.org/page/Networking#Public_Bridge

3

1. `mkdir -p /data/img`
2. `qemu-img create -f qcow2 /data/img/img.qcow2 10G`
3. Add to kickstart:

```
# Add before Anything with %
user --name="xiaoming" --password="XMishandsome" --groups=wheel
# Add at bottom
%post
#!/bin/sh
yum install epel-release sudo vim wget -y
%end
```

4. Run:

```
virt-install \
--name ILoveNASA \
--ram 2048 \
--vcpus=2 \
--nographics \
--network bridge=br0 \
--disk path=/data/img/img.qcow2,format=qcow2 \
--location http://centos.cs.nctu.edu.tw/7/os/x86_64/ \
--initrd-inject=/root/nasa.ks \
--extra-args="ks=file:/nasa.ks console=tty0 console=ttyS0 console=ttyS0,115200 serial"
```

<https://docs.centos.org/en-US/centos/install-guide/Kickstart2/>

<https://www.cyberciti.biz/faq/kvm-install-centos-redhat-using-kickstart-ks-cfg/>

4

1.

```
yum install openssh-clients openssh-server
systemctl enable sshd.service
systemctl start sshd.service
```

<https://www.cyberciti.biz/faq/centos-stop-start-restart-sshd-command/>

2.

```
[xiaoming@localhost ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 52:54:00:ba:7f:b2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.150.130/24 brd 192.168.150.255 scope global noprefixroute dynamic eth0
        valid_lft 1589sec preferred_lft 1589sec
    inet6 fe80::5054:ff:feba:7fb2/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[xiaoming@localhost ~]$ _
```

3. Press Ctrl+]

4.

```
[root@localhost ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master br0 state UP group default qlen 1000
    link/ether 00:0c:29:ba:0d:3b brd ff:ff:ff:ff:ff:ff
3: br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:0c:29:ba:0d:3b brd ff:ff:ff:ff:ff:ff
    inet 192.168.150.128/24 brd 192.168.150.255 scope global noprefixroute dynamic br0
        valid_lft 1098sec preferred_lft 1098sec
    inet6 fe80::20c:29ff:feba:d3b/64 scope link
        valid_lft forever preferred_lft forever
4: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 52:54:00:27:82:d2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
        valid_lft forever preferred_lft forever
5: virbr0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast master virbr0 state DOWN group default qlen 1000
    link/ether 52:54:00:27:82:d2 brd ff:ff:ff:ff:ff:ff
9: vnet0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master br0 state UNKNOWN group default qlen 1000
    link/ether fe:54:00:ba:7f:b2 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::fc54:ff:feba:7fb2/64 scope link
        valid_lft forever preferred_lft forever
[root@localhost ~]#
```

5.

```
[root@localhost ~]# ssh 192.168.150.130
The authenticity of host '192.168.150.130 (192.168.150.130)' can't be established.
ECDSA key fingerprint is SHA256:XB/0JSHMzu23yqbrq6rAcZXXPJ5rMY9w8tXCxqp32E.
ECDSA key fingerprint is MD5:73:26:96:20:ea:0b:3d:95:20:80:c0:77:3f:aa:54:b5.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.150.130' (ECDSA) to the list of known hosts.
root@192.168.150.130's password:
Last login: Sun Apr 11 00:51:32 2021
[root@localhost ~]# whoami
root
[root@localhost ~]#
```

5

1. `virsh suspend ILoveNASA`

2. `virt-clone --original ILoveNASA --name ILoveNASA-2 --autoclone`

3. `virsh resume ILoveNASA`

```
[root@localhost ~]# virsh list --all

```

	Id	Name	State
4.	4	ILoveNASA	running
	-	ILoveNASA-2	shut off

```
[root@localhost ~]# _
```

5. `virsh setvcpus ILoveNASA-2 1 --config`

```
[root@localhost ~]# virsh domiflist ILoveNASA
```

	Interface	Type	Source	Model	MAC
6.	vnet0	bridge	br0	virtio	52:54:00:ba:7f:b2

