NASA-HW3

B07902117 陳漱宇

Network Administration

1.Set up another Cisco Switch

(1)
advantage: Its design is easy. It just need three pin to finish full duplex communication, and the three pins are one for sending, one for receiving, and one pin for connecting to ground.
disadvantage: RS232 has slow speed of data transmission. The highest transmission speed of RS232 is roughly 20 kbit/s only.

Reference:
https://www.twblogs.net/a/5b7e795b2b7177683857937e
http://ind.ntou.edu.tw/~optp/VB%20CLASS/OPVB10%20RS232.pdf

(2)
We can use USB console line to replace RS232 console line.

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

(3)
password:No_TypE_7
(Using online cisco type 7 password decryption website)
(Its password is type 7)

Reference:
https://community.cisco.com/t5/switching/set-username-password-on-cisco-3750-switch/td-p/2084980
http://smalleaf.blogspot.com/2011/05/cisco-routerswitch.html
http://ibeast.com/tools/CiscoPassword/index.asp

(4)

The advantages of stacking compared with trunk are higher speed and higher density of ports.
(The concept of switch stacking is to connect multiple switchs and let them become one switch logically)

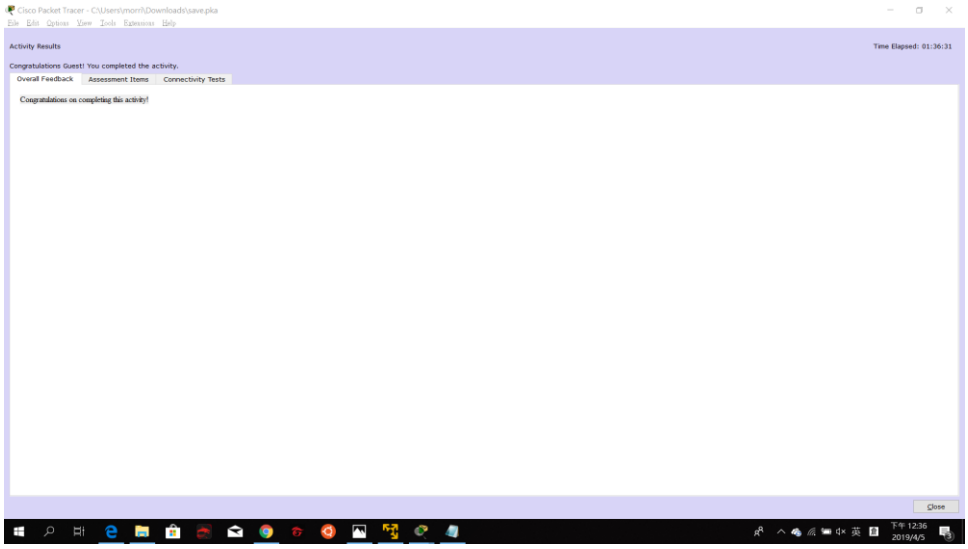
Reference:
http://www.fiberopticshare.com/switch-stacking-vs-trunking-whats-difference.html?fbclid=IwAR1CulM2T9h5HSuEVhkXff7qRBGuJ3DukMbSunlB_Xb_LN7KGZV627hIhGc
https://ithelp.ithome.com.tw/questions/10043752

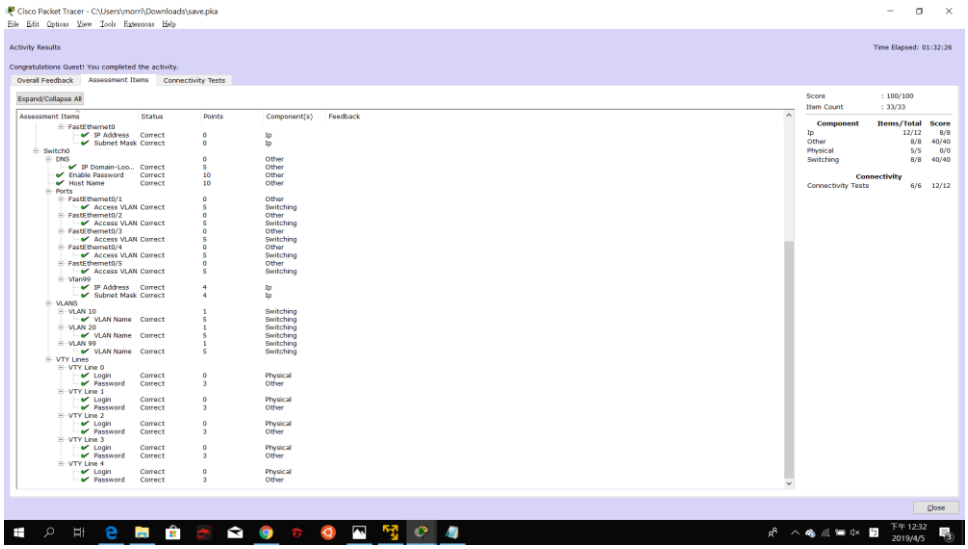
(5)
We need two cables to achieve full functionally of stacking.

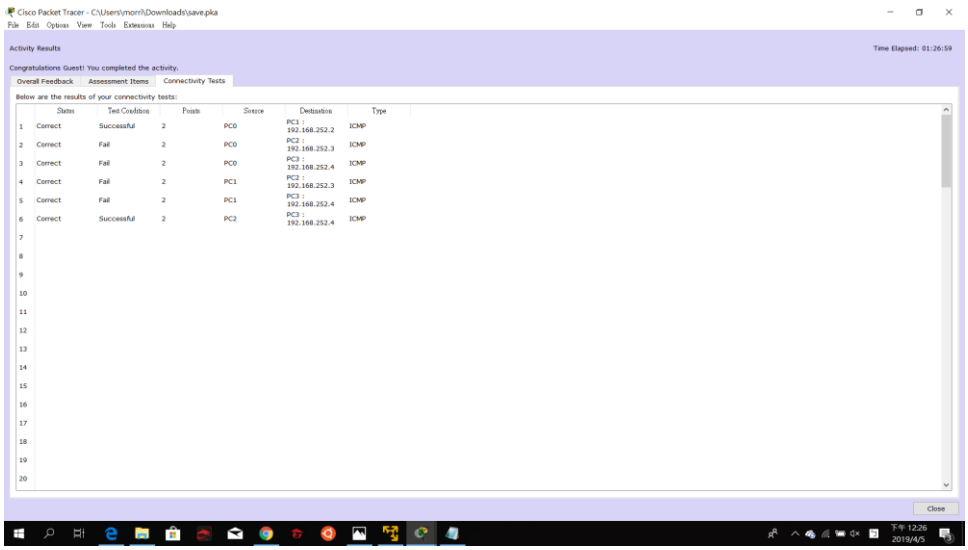
Reference:
https://community.cisco.com/t5/routing/number-of-stack-cables-for-two-3650/td-p/3179794?fbclid=IwAR30ULTtrfnXMsdEdJUOS7puT2tECD0e71d4MBxl2o3xn9PMRcXsV3cDbts

2. Cisco Packet Tracer

Screenshots of my check result:







Reference:
https://study-ccna.com/configure-an-ip-address-on-a-switch/
https://slides.com/b04902011/deck#/5/2

3. Malicious User

We can use Addrss Resolution Protocal(ARP) to achieve the goal. ARP is that we throw a query package to all the devices by using boardcast, and then the the device in the destination ip will send back a packet within its MAC address.
We can first use command "show ip arp" to get the hardware address, and then use "show mac-address-table address" to get the vlan and destination port.

Reference:
https://www.jannet.hk/zh-Hant/post/address-resolution-protocol-arp/
https://zh.wikipedia.org/wiki/%E5%9C%B0%E5%9D%80%E8%A7%A3%E6%9E%90%E5%8D%8F%E8%AE%AE
http://eportfolio.lib.ksu.edu.tw/~4970Q007/blog?node=000100016
https://networkengineering.stackexchange.com/questions/596/how-to-find-the-port-a-device-is-connected-to-based-on-ip-on-a-cisco-catalyst?fbclid=IwAR0a8bS0OwLFiZJ5ALwM64n9oYNrgTRYHnqm5kYoHnFmRsKeTnX9iv936yI

4. More on Link Aggregation

(1)
No. Because when implementing link aggregation, it only allows several same speed cables to do link aggregation. So Cat.6 UTP cable(support 1Gbps bandwidth) and Cat.5 UTP cable(support 100 Mbps bandwidth) cannot do so.

(2)
The wrong configuration is that both interfaces channel-group 1 mode is passive. It should be at least one interface is active so that port-channel can be work normally.

Reference:
http://linux.vbird.org/linux_enterprise/0110network.php#hardware_port
https://www.jannet.hk/zh-Hant/post/etherchannel-pagp-lacp/

5. The Evil VLAN, Access, and Trunk

(1)
The difference in 802.1q header between the two output packets from distinct source ports is that if it still has vlan tag. Generally speaking, trunk port is to connect the devices such as switch or router while access port is to connect edge device such as users' PC. And for trunk port, typically is the connection between switchs, it needs to ensure the package sent correctly according to vlan, so it will give or keep the vlan tag of the package(tagged). In contrast, for access port, it already knows which device is the destination, so it will take off the vlan tag of the package(untagged) and then send to the destination.

Reference:
https://www.itread01.com/articles/1476186610.html
https://ithelp.ithome.com.tw/questions/10102431
https://tw.answers.yahoo.com/question/index?qid=20100129000015KK03238

(2)
For port Gi1/0/3, when receiving an untagged package, it will put its PVID 307 in the package and then send it out.
For port Gi1/0/4, it is both possible for tagging 307 or 511, depends on which vlan is primary.
For port Gi1/0/5, because the native vlan is vlan 307, so it will tag 511 in the package and then send it out.
(Native vlan is the default vlan, all packages with no tag will be send to this vlan)

Reference:
https://weihanit.wordpress.com/2017/07/27/switch%E4%B8%89%E7%A8%AEport%E6%A8%A1%E5%BC%8Faccess%E3%80%81hybrid%E3%80%81trunk%E8%A1%8C%E7%82%BA%E6%A8%A1%E5%BC%8F/
https://www.itread01.com/articles/1476186610.html?fbclid=IwAR2e1SwGECVVhlZl6vZ7eqKgRkShWtqKfO7FZNt1FKsHO2WUMVw8vy_Ea0w
https://weihanit.wordpress.com/2017/07/27/switch%E4%B8%89%E7%A8%AEport%E6%A8%A1%E5%BC%8Faccess%E3%80%81hybrid%E3%80%81trunk%E8%A1%8C%E7%82%BA%E6%A8%A1%E5%BC%8F/

(3)
If the vlan of the port is same as the native vlan. It is possible to get Double Tag Attack, that is, if there is a attacking package got double tagged(the destination vlan wrapped with the native vlan), after switch receive a package with tagging native vlan, switch will take off the native tag and then the destination vlan will be exposed. And then the attacking will be send to the destination. To avoid it, we can configure the native vlan to make it
different from the vlan of the port , so the tag of the package will not be taken off.

Reference:
https://www.jannet.hk/zh-Hant/post/virtual-lan-vlan/?fbclid=IwAR1hlOVrUGecFu_AwIpM8kUoKsyKiUrR-Qm1juQnrHLkGy2-

R7lDLvmqm-w#native
https://www.jannet.hk/zh-Hant/post/virtual-lan-vlan-attack/#hopping

System Administration

1. Install a VM host running CentOS 7

yum install virt-install
yum insatll gemu-kvm
yum install libvirt
yum install systemd
systemctl start libvirtd
systemctl status libvirtd
systemctl enable libvirtd

Reference:
https://doc.opensuse.org/documentation/leap/virtualization/html/book.virt/cha.libvirt.overview.html

2. Create a Virtual Machine (guest) on VM host

mkdir /data
mkdir /data/img
cd /data/img
qemu-img create -f qcow2 quest_image 10G
(create a 10G QCOW2 image named quest_image)
touch kickstart
vi kickstart
(
user --name=meow --groups=wheel --iscrypted --password=6vIb1NqqmWyiDwi3o$0vOc/TpM4lG8nhDBVUuNHceOrNdTQfLt78v3EmyVuQLS6/DOdiU4iV3IK6o73n8vM6EdFdjZz04RlK6koUJxK
(add an user named meow to wheel group and its password is meow(use pwkickstart to encrypt))

repo --name=epel --baseurl=
http://download.fedoraproject.org/pub/epel/6/x86_64/
%packages
epel-release
vim
openssh-server
sudo
wget

%end
(download packages)
)
sudo virt-install --name=nasa --ram=4096 --vcpus=1 --disk=/data/img/quest_image.qcow2 -w bridge=virbr0 -v --nographics --location 'http://centos.cs.nctu.edu.tw/7/os/x86_64/' --os-type linux --initrd-inject=/kickstart --extra-args "ks=file:/kickstart console=ttyS0"
(create a new vm named nasa, its memory is 4GB, it has one CPU, it use quest_image.qcow2 as its image , it use bridge virbr0 to connect to net , add --nographic to see the process, --loction shows where the os it should download,--os-type linux shows its os type is linuxm ks=file:/kickstart shows where the kickstart file is, and because my kickstart file is on local, so the parameter –initrd-inject is needed, console ttyS0 indicates that I want to use text console)

Reference:
https://newtoypia.blogspot.com/2015/03/qcow2.html
https://access.redhat.com/documentation/zh-tw/red_hat_enterprise_linux/7/html/installation_guide/sect-kickstart-syntax
https://www.golinuxhub.com/2018/01/how-to-create-user-normal-and-root.html
https://access.redhat.com/documentation/zh-tw/red_hat_enterprise_linux/7/html/installation_guide/sect-kickstart-syntax#sect-kickstart-packages
https://bugzilla.redhat.com/show_bug.cgi?id=1416216
https://www.itread01.com/content/1537444649.html
http://www.zerodev.it/automating-centos-netinstall-with-kickstart-and-remastering.html?fbclid=IwAR1-

776moXcINYyAd_2LdEXC6rdIb73vARxgXHWETF19v9qKZL0jchsIs7I

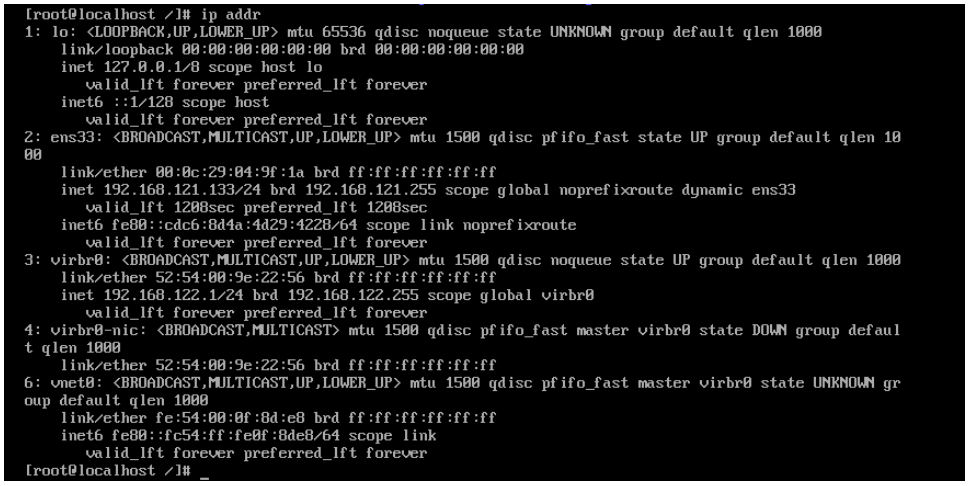
B07902001 徐維謙

B07902031 黃永雯

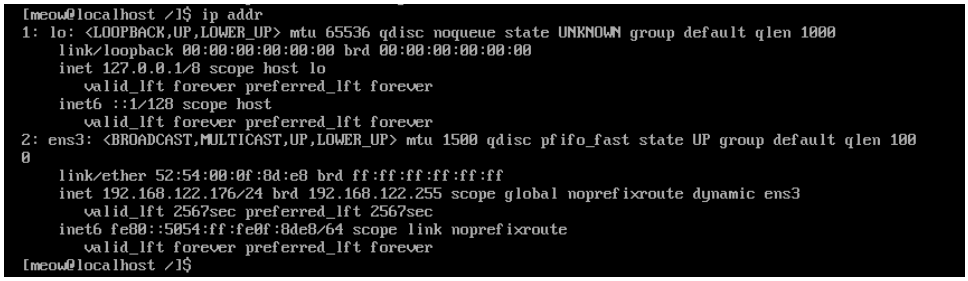
3. Enter Guest

The command I use to enter guest vm is “virsh console nasa”

ip addr for host



ip addr for guest



From the screenshoes aboved, we can know that the guest vm’s IP is given from DHCP server of the host, and they are in the same sub-net.

Reference:
https://www.cnblogs.com/tanghuimin0713/p/4534275.html
https://dotblogs.com.tw/law1009/2011/12/30/63911

4. Manage the VM from VM host

(1)
virsh start nasa
(start guest vm nasa)
virsh list --all
(list all the guest vm)

```
[root@localhost /]# virsh list --all
 Id    Name                           State
----------------------------------------------------
 2     nasa                           running
```

virsh shutdown nasa
(shutdown guest vm nasa)
virsh list --all

```
[root@localhost /]# virsh list --all
 Id    Name                           State
----------------------------------------------------
 -     nasa                           shut off
```

(2)
virsh shutdown nasa
virsh undefine nasa
(remove guest vm nasa)

```
[root@localhost /]# virsh shutdown nasa
Domain nasa is being shutdown

[root@localhost /]# virsh undefine nasa
Domain nasa has been undefined
```

(3)
virsh edit nasa

(4)
virsh domiflist nasa

```
[root@localhost /]# virsh domiflist
error: command 'domiflist' requires <domain> option
[root@localhost /]# virsh domiflist nasa
Interface  Type       Source     Model       MAC
-------------------------------------------------------
vnet0      bridge     virbr0     rtl8139     52:54:00:0f:8d:e8

[root@localhost /]# _
```

(5)

virsh domifstat nasa vnet0

```
[root@localhost /]# virsh domifstat nasa vnet0
vnet0 rx_bytes 184954
vnet0 rx_packets 3515
vnet0 rx_errs 0
vnet0 rx_drop 0
vnet0 tx_bytes 3678
vnet0 tx_packets 29
vnet0 tx_errs 0
vnet0 tx_drop 0

[root@localhost /]# _
```

Reference:

https://jerry2yang.wordpress.com/2011/11/24/%E4%BF%AE%E6%94%B9%E8%99%9B%E6%93%AC%E6%A9%9Fkvmqemu%E7%A1%AC%E9%AB%94%E8%A8%AD%E5%AE%9A-with-virsh-management-user-interface/

https://godleon.github.io/blog/KVM/KVM-libvirt-network/

https://www.cyberciti.biz/faq/howto-linux-delete-a-running-vm-guest-on-kvm/

B07902031 黃永雯

5. Back up without stopping guest VM

yum install -y centos-release-qemu-ev

yum install -y qemu-kvm-ev

yum install -y qemu-kvm-rhev

(for centos 7, its version of qemu is too old)

virsh snapshot-create-as nasa "backup" ,snapshot=external,file=/data/img/backup_overlay --disk-only –atomic

(use command “snapshot-create-as“ to create a snapshot, and the parameters snapshot=external and --disk-only indicate that the snapshot should be external and disk-only)

virsh domblklist nasa

```
[root@localhost bc-img]# virsh domblklist nasa
Target     Source
------------------------------------------------
hda        /data/img/quest_image.backup
```

cd /
mkdir /bc-img
cd /bc-img
cp /data/img/quest_image /bc-img
cp quest_image nasa_backup.qcow2
rm quest_image
virsh blockcommit nasa hda --verbose --pivot --active
(use command “virsh blockcommit” to merge the overlay file back to the base image)

```
[root@localhost bc-img]# virsh start nasa
Domain nasa started

[root@localhost bc-img]# virsh blockcommit nasa hda --verbose --pivot --active
Block commit: [100 %]
Successfully pivoted
```

virsh domblklist nasa

```
[root@localhost bc-img]# virsh blockcommit nasa hda --verbose --pivot --active
Block commit: [100 %]
Successfully pivoted
[root@localhost bc-img]# virsh domblklist nasa
Target     Source
------------------------------------------------
hda        /data/img/quest_image
```

Reference:
https://www.itread01.com/content/1540983869.html
https://wiki.libvirt.org/page/Live-merge-an-entire-disk-image-chain-including-current-active-disk

B07902031 黃永雯