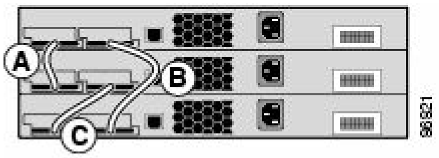
Network Administration/System Administration (NTU CSIE, Spring 2019) Homework #3

Network Administration

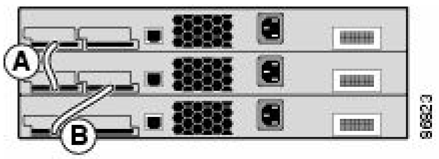
1. Set up another Cisco Switch (11%)

1. 好處是如果是用網路設定，如果改到一些跟我目前的連線有關係的設定，就會一直斷線再重連，甚至有時候設定完就再也連不上了，RS232則不太有這個問題，壞處是我們一定要從那台 switch 拉線出來做設定，在某些環境顯的很麻煩。
2. 有些 switch 提供從網路端 access 的服務，不然就是去買一條 RS232 的線。
3. Plain text is: No_TypE_7
   Reference: http://www.ifm.net.nz/cookbooks/passwordcracker.html
4. 可以只連接一台 switch 進行管理，避免一直切換的麻煩。
   線路看起來比較乾淨整潔，壞掉換新的也比較方便。
   Reference: https://en.wikipedia.org/wiki/Stackable_switch
   https://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/71925-cat3750-create-switch-stks.html
5. 兩條，根據文件

   Full Bandwidth Connection

   Half Bandwidth Connection

   Reference:
   https://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/71925-cat3750-create-switch-stks.html

2. Cisco Packet Tracer (14%)

Set the hostname of the switch to ”CiscoLab”

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname CiscoLab
```

Reference:
https://www.cisco.com/c/en/us/support/docs/switches/catalyst-6000-series-switches/10581-6.html

Disable domain name lookup in CLI

```
CiscoLab#ping google.com
Translating "google.com"...domain server (255.255.255.255)
% Unrecognized host or address or protocol not running.

CiscoLab(config)#no ip domain-lookup

CiscoLab#ping google.com
Translating "google.com"
% Unrecognized host or address or protocol not running.
```

Reference:
https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/n5k/commands/ip-domain-lookup.html

Set enable password to ”CISCO” and encrypt it

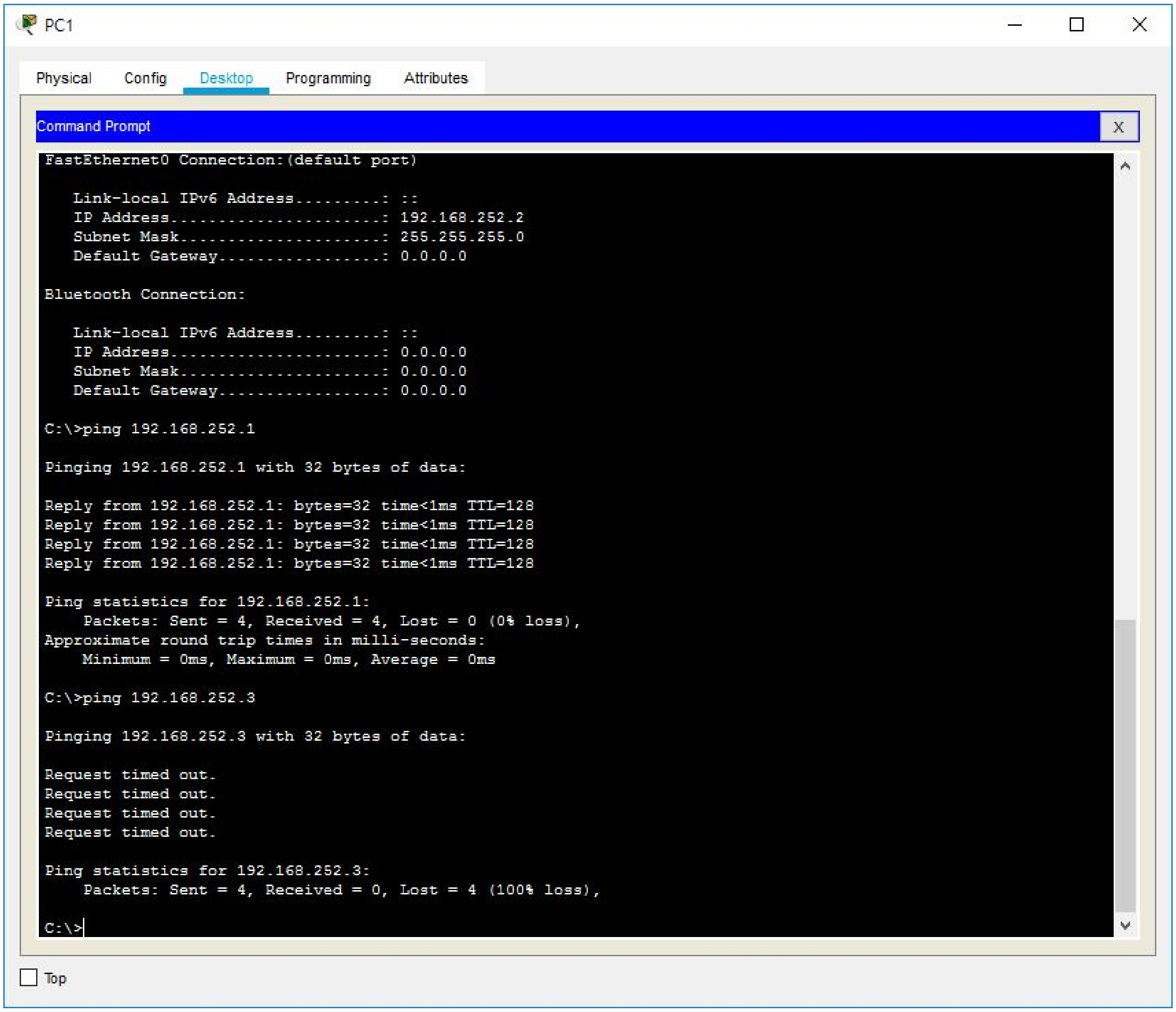
```
CiscoLab(config)#enable password CISCO # wrong method
CiscoLab(config)#no enable password    # cancel password
CiscoLab(config)#enable secret CISCO

CiscoLab#show running-config
enable secret 5 $1$mERr$NJdjwh5wX8Ia/X8aC4RIu.
```

Reference:
https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfpass.html

Create VLANs 10, 20, 99. Assign PC0 and PC1 to VLAN10 and assign PC2 and PC3 to VLAN20 so that PCs in different. VLANs cannot ping each other

```
CiscoLab(config)#interface Fa0/1
CiscoLab(config-if)#switchport mode access
CiscoLab(config-if)#switchport access vlan 10
CiscoLab(config)#interface Fa0/2
CiscoLab(config-if)#switchport mode access
CiscoLab(config-if)#switchport access vlan 10
```

```
CiscoLab(config)#interface Fa0/3
CiscoLab(config-if)#switchport mode access
CiscoLab(config-if)#switchport access vlan 20
CiscoLab(config)#interface Fa0/4
CiscoLab(config-if)#switchport mode access
CiscoLab(config-if)#switchport access vlan 20
```



```
FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: ::
   IP Address......................: 192.168.252.2
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 0.0.0.0

Bluetooth Connection:

   Link-local IPv6 Address.........: ::
   IP Address......................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: 0.0.0.0

C:\>ping 192.168.252.1

Pinging 192.168.252.1 with 32 bytes of data:

Reply from 192.168.252.1: bytes=32 time<1ms TTL=128
Reply from 192.168.252.1: bytes=32 time<1ms TTL=128
Reply from 192.168.252.1: bytes=32 time<1ms TTL=128
Reply from 192.168.252.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.252.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.252.3

Pinging 192.168.252.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.252.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Assign Admin to VLAN99 and Admin should be able to access the switch by telneting 192.168.99.1

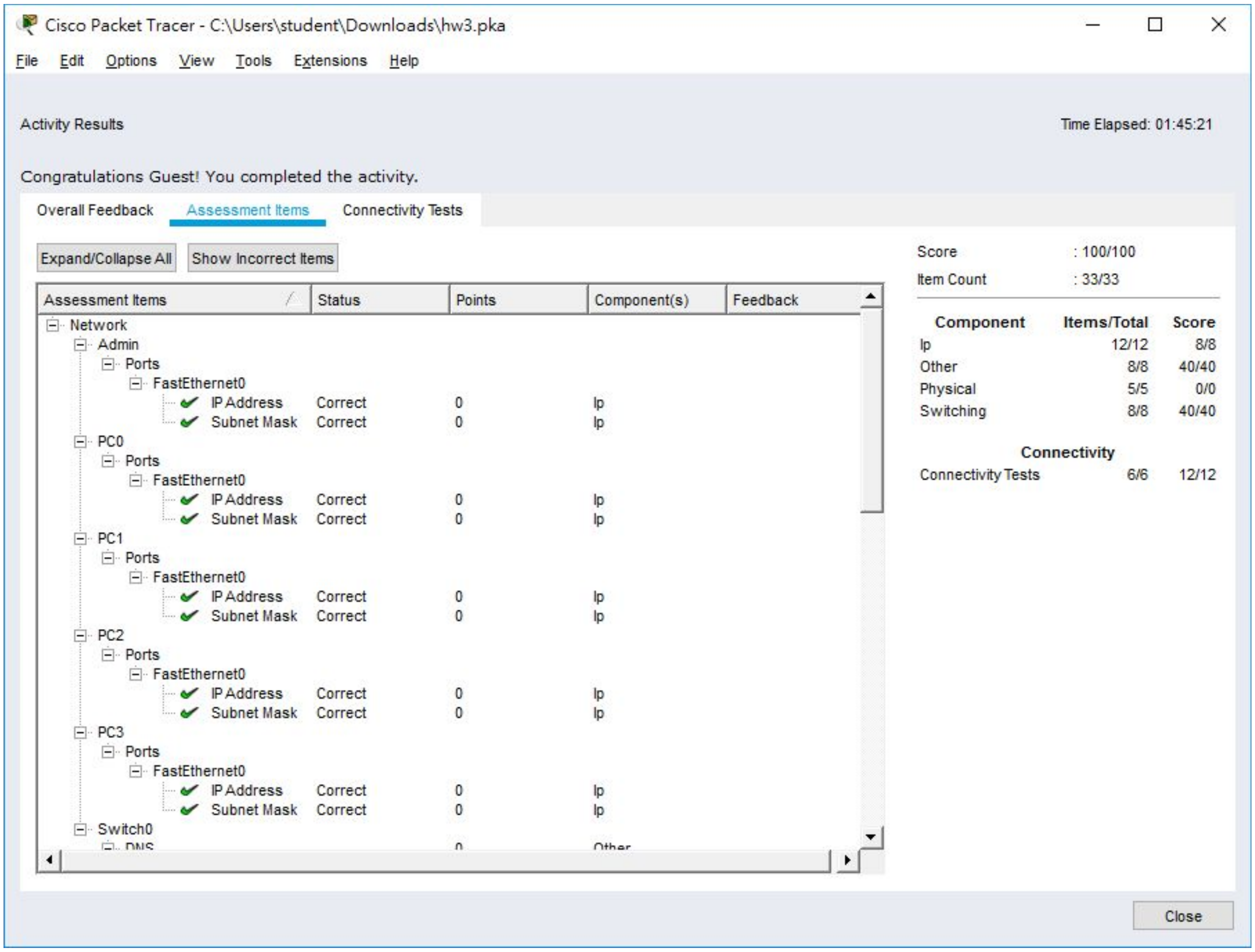
```
CiscoLab(config)#interface Fa0/5
CiscoLab(config-if)#switchport mode access
CiscoLab(config-if)#switchport access vlan 99
CiscoLab(config)#interface vlan 99
CiscoLab(config-if)#ip address 192.168.99.1 255.255.255.0
CiscoLab(config-if)#no shutdown
```

Reference:
http://www.omnisecu.com/cisco-certified-network-associate-ccna/what-is-management-vlan-and-how-to-configure-management-vlan.php

Set the telnet login password to ”cisco” on VTY 0 to 4

```
CiscoLab(config)#line vty 0 4
CiscoLab(config-line)#password cisco
CiscoLab(config-line)#login
CiscoLab(config)#service password-encryption # encode password (not useful)

CiscoLab#show running-config
line vty 0 4
password 7 0822455D0A16
```

Reference:
https://www.netadmin.com.tw/article_content.aspx?sn=1205070002&jump=5



Activity Results

Time Elapsed: 01:45:21

Congratulations Guest! You completed the activity.

Assessment Items	Status	Points	Component(s)	Feedback
Network				
Admin				
Ports				
FastEthernet0				
✓ IP Address	Correct	0	Ip	
✓ Subnet Mask	Correct	0	Ip	
PC0				
Ports				
FastEthernet0				
✓ IP Address	Correct	0	Ip	
✓ Subnet Mask	Correct	0	Ip	
PC1				
Ports				
FastEthernet0				
✓ IP Address	Correct	0	Ip	
✓ Subnet Mask	Correct	0	Ip	
PC2				
Ports				
FastEthernet0				
✓ IP Address	Correct	0	Ip	
✓ Subnet Mask	Correct	0	Ip	
PC3				
Ports				
FastEthernet0				
✓ IP Address	Correct	0	Ip	
✓ Subnet Mask	Correct	0	Ip	
Switch0				
DNS		0	Other	

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

3. Malicious User (6%)

CISCO 有提供好用的 traceroute [Traceroute Utility]

```
Router# traceroute mac ip {source_ip_address | source_hostname}
{destination_ip_address | destination_hostname} [detail]
```

```
Traceroute mac ip 140.112.30.254 140.112.30.250 detail
```

Reference:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/l2trace.html
https://www.ciscozine.com/how-to-trace-mac-address/

4. More on Link Aggregation (8%)

1. (3%)
   根據 Catalyst 2960 and 2960-S Switches Software Configuration Guide
   The LACP is defined in IEEE 802.3ad and enables Cisco switches to manage Ethernet channels between switches that conform to the IEEE 802.3ad protocol. LACP facilitates the automatic creation of EtherChannels by exchanging LACP packets between Ethernet ports.
   這邊使用 IEEE802.3ad 進行 link aggregation，然後根據 wiki
   However, all the IEEE standard requires is that each link be full duplex and all of them have an identical speed (10, 100, 1,000 or 10,000 Mbit/s).
   所以是不行的
   Reference:
   https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_58_se/configuration/guide/2960scg/swethchl.html#75052
   https://en.wikipedia.org/wiki/Link_aggregation#Same_link_speed

2. (5%)
   根據 Cisco Nexus 1000V Interface Configuration Guide

   - A port in **active** mode can form a port channel with another port in **passive** mode.
   - A port in **passive** mode cannot form a port channel with another port that is also in **passive** mode, because neither port will initiate negotiation.

   所以把一台 switch 的 channel -group 1 mode passive 改成 active 就可以了

   Reference:
   https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus1000/sw/4_0/interface/configuration/guide/n1000v_interface/if_5portchannel.html

5. The Evil VLAN, Access, and Trunk (11%)

1. (3%)
   Access mode 的 interface 只能接受一個 vlan，所以往 Gi 1/0/2 的 packet 不會有 802.1q 的 header。
   Reference:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/AccessTrunk.html#33020

2. (4%)
   Gi 1/0/3： 加上 307 tag
   Gi 1/0/4： drop
   Gi 1/0/5： 加上 307 tag
   Reference:
   https://community.extremenetworks.com/extremeswitching-exos-223284/does-switch-drop-untagged-frames-on-tagged-only-port-6591980
3. (4%) 當兩台 switch 之間存在不懂 802.1q的裝置，native vlan 可以避免整個網路失效
   Reference:
   https://www.jannet.hk/zh-Hant/post/virtual-lan-vlan/
   https://community.cisco.com/t5/switching/why-native-vlan-exists-on-a-trunk/td-p/1363872
   http://allenhua.pixnet.net/blog/post/3376178-native-vlan-on-cisco-device
   https://learningnetwork.cisco.com/message/58076#58076

System Administration

1. Install a VM host running CentOS 7 (10%)

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

2. Create a Virtual Machine (guest) on VM host (18%)

1.

```
sudo mkdir -p /data/img
```

2.

```
qemu-img create [--object objectdef] [-q] [-f fmt] [-b
backing_file] [-F backing_fmt] [-u] [-o options] filename[size]
```

Reference:
https://qemu.weilnetz.de/doc/qemu-doc.html#qemu_005fimg_005finvocation

```
sudo qemu-img create -f qcow2 nasa-img.qcow2 10G
```

3.

```
sudo yum install pykickstart # for checking script syntax
ksvalidator *.ks
```

```
$ diff anaconda-ks.cfg anaconda-ks-origin.cfg

5d4
< repo --name=epel
--baseurl=http://download.fedoraproject.org/pub/epel/6/x86_64/
7,8c6,7
< # Use text install
< text
---
> # Use graphical install
> graphical
32,35d30
< # custom user
< group --name=wheel
< user --name=meow --groups=wheel
--password='$6$mlCOcI8BccngJ65n$KxUlStzFcojQIejtU0I5iZUzugcciMwmFj6VrWX76If
SuUC1TXRLsVfjLEdoF5YF3MaUyYQhKsDrsYSpAyR2D1' --iscrypted
<
40,44d34
< epel-release
< vim
< openssh-server
< sudo
< wget
```

4. 我用 `nmtui` create 一個 bridge 叫做 `virbr1`
   然後去編輯 /etc/sysconfig/network-script/ifcfg-ens33 最後加上 `BRIDGE=virbr1`
   之後重啟 `network.service`
5. Warning KVM acceleration not available, using ‘qemu’
   Go to VM > setting > processors check virtualization engine

```
virt-install \
--name nasa \
--memory 2048 \ # 如果太少會出現 No space left on device
--disk /data/img/nasa-img.qcow2,format=qcow2 \
--cpu host \
--vcpus 1 \
--nographics \
--network bridge=virbr0 \
--location http://centos.cs.nctu.edu.tw/7/os/x86_64/ \
--initrd-inject anaconda-ks.cfg
```

```
--extra-args="inst.ks=file:/anaconda-ks.cfg console=ttyS0"
```

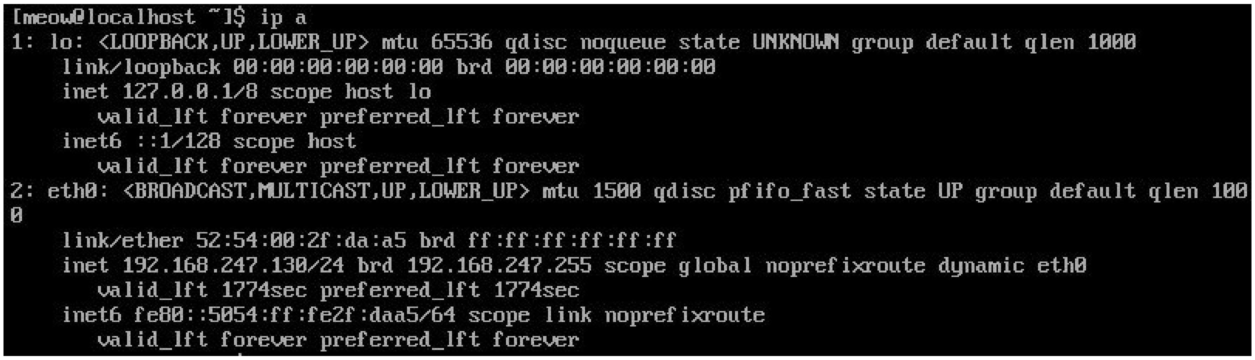
Reference:
B07902123
https://access.redhat.com/documentation/zh-tw/red_hat_enterprise_linux/7/html/installation_guide/sect-kickstart-howto
virt-install
https://lists.fedoraproject.org/archives/list/test@lists.fedoraproject.org/thread/PWID5JWUYQZEOYKZKDATMOSWBJITKMZE/
https://www.mankier.com/1/virt-install
https://blog.gtwang.org/linux/kvm-qemu-virt-install-command-tutorial/
https://anaconda-installer.readthedocs.io/en/latest/boot-options.html
https://unix.stackexchange.com/questions/207090/install-vm-from-command-line-with-virt-install
http://blog.leifmadsen.com/blog/2016/12/16/creating-virtual-machines-in-libvirt-with-virt-install/
https://github.com/lzap/pwkickstart
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/virtualization_deployment_and_administration_guide/sect-guest_virtual_machine_installation_overview-creating_guests_with_virt_install
https://serverfault.com/questions/257962/kvm-guest-installed-from-console-but-how-to-get-to-the-guests-console
Bridge
https://www.itzgeek.com/how-tos/mini-howtos/create-a-network-bridge-on-centos-7-rhel-7.html
https://www.tuxfixer.com/install-and-configure-kvm-qemu-on-centos-7-rhel-7-bridge-vhost-network-interface/

3. Enter Guest (5%)

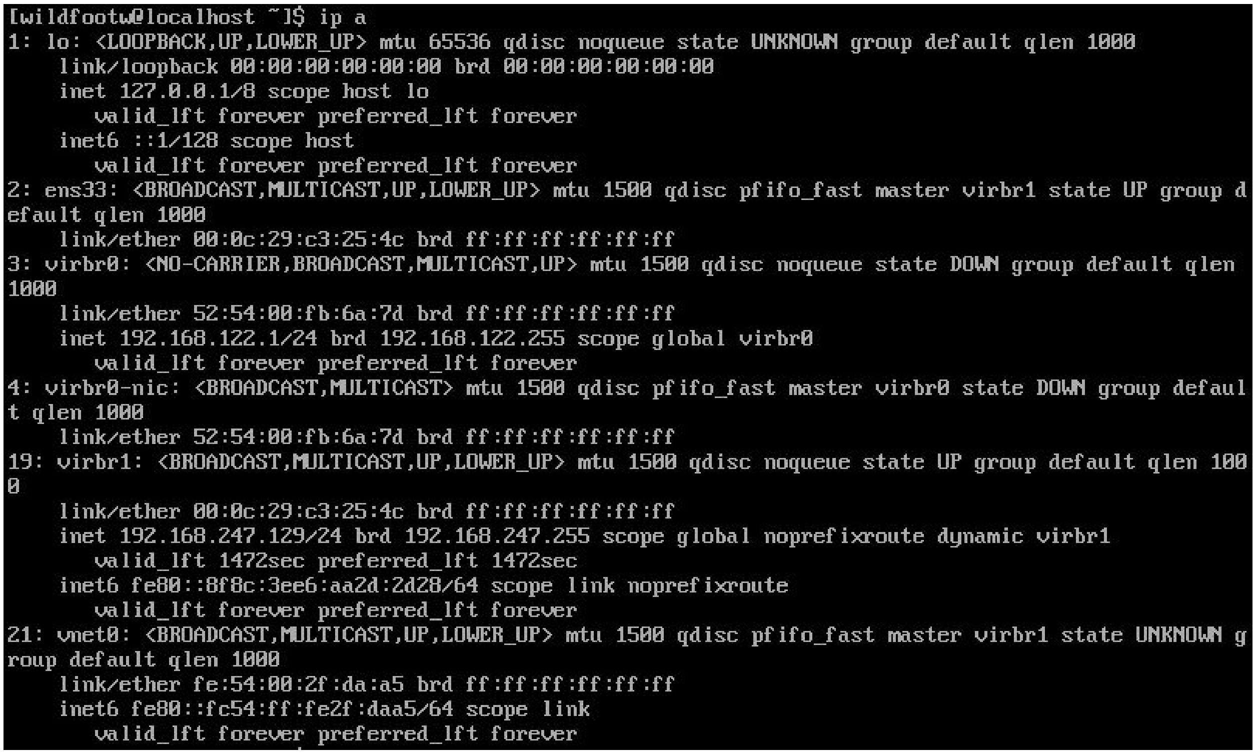
1. Command

```
sudo virsh console nasa
```

2. Screenshot



```
[meow@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 100
0
    link/ether 52:54:00:2f:da:a5 brd ff:ff:ff:ff:ff:ff
    inet 192.168.247.130/24 brd 192.168.247.255 scope global noprefixroute dynamic eth0
       valid_lft 1774sec preferred_lft 1774sec
    inet6 fe80::5054:ff:fe2f:daa5/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

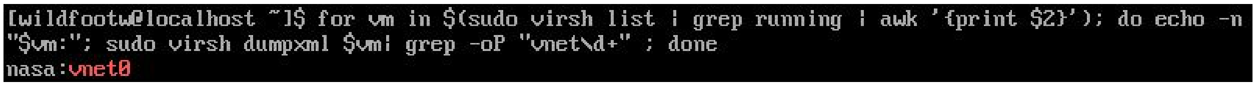


```
[wildfootw@localhost ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master virbr1 state UP group d
efault qlen 1000
    link/ether 00:0c:29:c3:25:4c brd ff:ff:ff:ff:ff:ff
3: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen
1000
    link/ether 52:54:00:fb:6a:7d 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
4: virbr0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast master virbr0 state DOWN group defaul
t qlen 1000
    link/ether 52:54:00:fb:6a:7d brd ff:ff:ff:ff:ff:ff
19: virbr1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 100
0
    link/ether 00:0c:29:c3:25:4c brd ff:ff:ff:ff:ff:ff
    inet 192.168.247.129/24 brd 192.168.247.255 scope global noprefixroute dynamic virbr1
       valid_lft 1472sec preferred_lft 1472sec
    inet6 fe80::8f8c:3ee6:aa2d:2d28/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
21: vnet0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master virbr1 state UNKNOWN g
roup default qlen 1000
    link/ether fe:54:00:2f:da:a5 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::fc54:ff:fe2f:daa5/64 scope link
       valid_lft forever preferred_lft forever
```

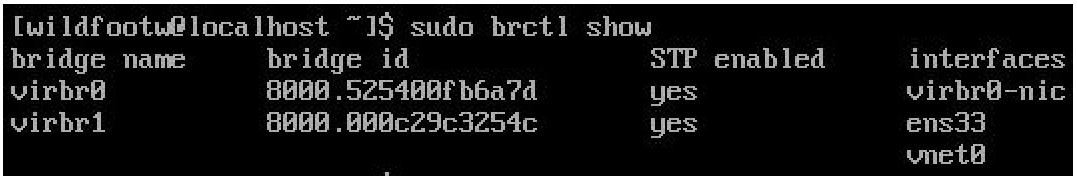
Reference:
https://ravada.readthedocs.io/en/latest/docs/config_console.html

4. Manage the VM from VM host (5%)

```
virsh list --all        # show all virtual machine

virsh destroy [name]    # stop virtual machine
virsh undefine [name]   # delete virtual machine

virsh edit [name]       # edit MACHINE'S XML CONFIGURATION SETTINGS

# show network interfaces of a VM
for vm in $(virsh list | grep running | awk '{print $2}'); do
    echo -n "$vm:"; virsh dumpxml $vm| grep -oP "vnet\d+" ;
done

brctl show
```



```
[wildfootw@localhost ~]$ for vm in $(sudo virsh list | grep running | awk '{print $2}'); do echo -n
"$vm:"; sudo virsh dumpxml $vm| grep -oP "vnet\d+" ; done
nasa:vnet0
```



```
[wildfootw@localhost ~]$ sudo brctl show
bridge name     bridge id               STP enabled     interfaces
virbr0          8000.525400fb6a7d       yes             virbr0-nic
virbr1          8000.000c29c3254c       yes             ens33
                                                        vnet0
```

Reference:
https://www.cyberciti.biz/faq/linux-list-a-kvm-vm-guest-using-virsh-command/
https://www.cyberciti.biz/faq/howto-linux-delete-a-running-vm-guest-on-kvm/
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/virtualization_deployment_and_administration_guide/sect-managing_guest_virtual_machines_with_virsh-editing_a_guest_virtual_machines_configuration_file
https://serverfault.com/questions/396105/is-there-a-way-to-determine-which-virtual-interface-belongs-to-a-virtual-machine
https://www.cyberciti.biz/faq/linux-command-to-display-network-bridge-name/

5. Back up without stopping guest VM (12%)

```
# for Error: Operation not supported: live disk snapshot not supported with this QEMU binary
sudo yum -y install centos-release-qemu-ev qemu-kvm-ev
Sudo yum update
sudo virsh shutdown nasa
sudo virsh start nasa

sudo virsh domblklist nasa
sudo virsh snapshot-create-as --domain nasa --diskspec vda,file=/data/img/overlay1.qcow2 --disk-only --atomic

sudo mkdir /bc-img
sudo cp /data/img/nasa-img.qcow2 /bc-img/nasa_backup.qcow2

sudo virsh blockcommit nasa vda --active --verbose --pivot
```

Reference:
https://wiki.libvirt.org/page/Live-disk-backup-with-active-blockcommit