

Creating a Virtual Private Network (VPN)

Purpose of Creating VPNs
How to Create a VPN
Troubleshooting Tools
Local Hostname Resolution



Creating a Virtual Private Network (VPN)

Purpose of Creating VPNs
How to Create a VPN
Troubleshooting Tools
Local Hostname Resolution



Virtual Private Networks (VPNs)

For the remainder of this course, we will focus on networking using our VMs. This lab (**lab6**) will focus on setting up a **Virtual Private Network** (VPN), connecting our VMs and c7host machine to the VPN, and configuring our VPN to make more convenient to use, troubleshoot and protect.

Lab7 will focus on configuring **SSH** and using a **firewall** (via iptables command) to making access to your VPN more secure.

Lab8 will focus on configuring mobile connections (eg. wireless "hot-spots" or random wired access locations) via **DHCP** to automatically assign an IP address.

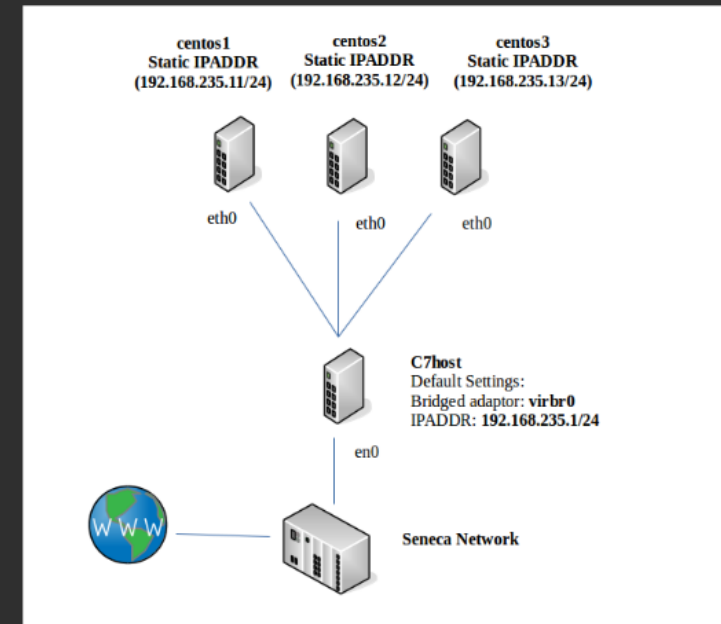


Virtual Private Networks (VPNs)

There are several reasons for creating VPNs:

The main reason is to **safely connect servers together** (i.e. to **safely limit but allow the sharing of information** among computer network users).

This allows for a secure connection of computers yet controlling access to and monitoring (protecting) access to permitted users (discussed later in lab7).



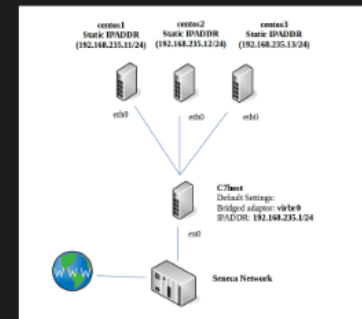
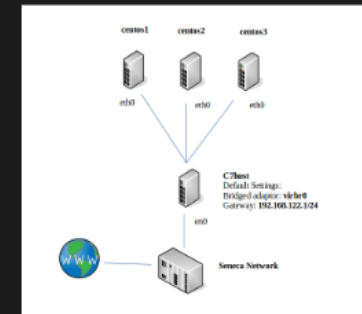
Virtual Private Networks (VPNs)

When your **c7host** machine was created in lab1, your machine was assigned a IPADDR by **DHCP**.

In lab2, when you created your VMs (i.e. **centos1**, **centos2**, and **centos3**) they have been assigned an IPADDR via **DHCP**. In order to create a Virtual Private Network, a few things need to be setup:

- Create a **subnet** to allow VMs to use c7host as a **DNS proxy server** to Seneca's router to be able to have VMs connect to the Internet
- Configure each VM to have each of their own **permanent Static IP Address** (not via DHCP) to connect to the subnet.

Double-click on the above image to show the existing setup from lab2, and then click on the below image to show the proposed VPN setup for lab6.



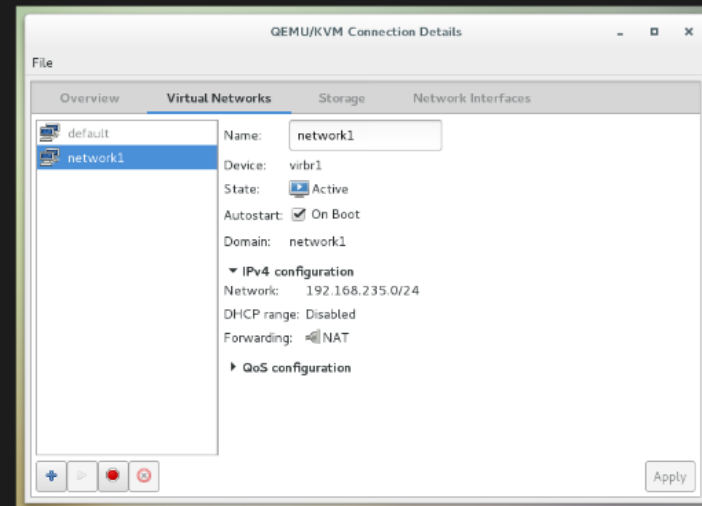
Setup a VPN

We need to re-configure the Virtual Network settings for our **Virtual Machine Manager**.

In the Virtual Machine Manager dialog box, select **Edit-> Connection Details**.

In the Connection Details dialog box, select the **Virtual Networks** tab.

Then we click the stop our default network, turn-off the dynamic (default) network connection, and add a new subnet labelled **network1**, with a new network IPADDR: **192.168.235.0/24**, **disable DHCP on start-up**, and setup **forwarding via NAT**.

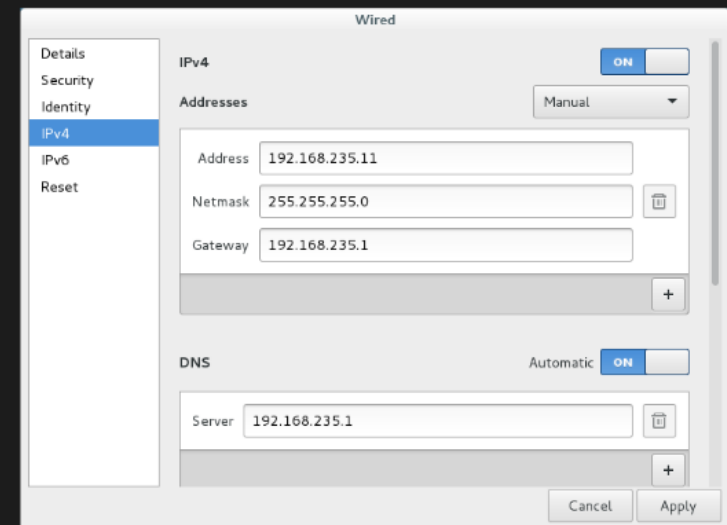


Setup a VPN

Next, you would need to setup the network configuration for **each VM** manually (as opposed to DHCP) including the following information:

IPADDR
NETMASK
GATEWAY
DNS Server

For your **centos1** VM, you will learn how to setup the network configuration graphically. Double-click on the diagram to view full-screen.



Setup a VPN

For the **centos2** and **centos3** VMs, since they are command-line only, you have two ways to configure the network connection:

- **Temporary connection** using **ifconfig**, **route**, and **nameserver** commands (can also edit `/etc/resolv.conf` file). This does NOT keep settings when restarting machine. CLI only machines require installation of **net-tools**
- **Persistent (permanent) connection** by editing the `/etc/sysconfig/network-scripts/ifcfg-eth0` file.

Double-click on the image to view the typical settings for the `ifcfg-eth0` file. All VMs in OPS335 course will be command-line - FYI.

```
[root@centos2 ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
# Generated by dracut initrd
NAME="eth0"
HWADDR="52:54:00:a6:8e:ca"
ONBOOT=yes
UUID="acb299a8-dd4b-4c21-bec1-121fdc87435b"
IPV6INIT=no
BOOTPROTO=static
TYPE=Ethernet
IPADDR=192.168.235.12
NETMASK=255.255.255.0
GATEWAY=192.168.235.1
DNS1=192.168.235.1
[root@centos2 ~]# _
```


Network Troubleshooting Tools

Sometimes you need to **troubleshoot** when a network connection is NOT working. The following Linux utilities are considered very useful for network troubleshooting:

ping - Sends ICMP packets to confirm transmission and receipt of packets

ifconfig (ip) - Either command provides IPADDR, netmask, MACADDR, etc
The ip command is newer (eg **ip address**, **ip route**, etc.)

arp - Stands for **Address Resolution Protocol** to resolve **IPADDR** to a **MACADDR** (physical machine via network interface).

netstat - Stands for Network Statistic. Useful for analyzing network traffic
Common options are: **-nautp**



Local Hostname Resolution

You are probably tired of remembering your VM's IP Addresses that you are required to enter in previous lab-checking scripts (labs 2 - 5).

You can refer to your VMs as names as opposed to IPADDR using **Local Hostname Resolution**. Simply edit the **/etc/hosts** file as root for each machine (including ALL VMs and your host machine):

```
192.168.235.1 c7host  
192.168.235.11 centos1  
192.168.235.12 centos2  
192.168.235.13 centos3
```

After you do this procedure, you can use the server's **name** as opposed to IPADDR. Local Hostname Resolution is useful for small networks, but large networks require a **DNS server** to be installed and run to efficiently resolve hostnames to IPADDR (you will learn how to do this in OPS335).

Creating a Virtual Private Network (VPN)

Purpose of Creating VPNs
How to Create a VPN
Troubleshooting Tools
Local Hostname Resolution

