i

Network infrastructure

Exercises

Arttu Karhunen
n4924@student.jamk.fi

Syksy 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Exercise 1

Arttu Karhunen
n4924@student.jamk.fi

Exercise
Syyskuu 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

1 Task 1

Question:

Install Virtualbox to you machine from https://www.virtualbox.org... and install the Linux!

Answer:

Downloaded virtualbox from https://www.virtualbox.org/wiki/Downloads and CentOS from https://centos.org/download/.

then installed CentOS to virtualbox according to this instruction https://linuxhint.com/install_centos8_virtualbox/

I had problems connecting the server to network because I was at Dynamo using eduroam network (with my own laptop). Eduroam network didn’t allow me to ping to google.com. After some googling I figured to connect laptop to my mobilephones network and ping.

2 Task 2

Question:

Since you have some perfect Linux VM just installed, its the most perfect time make a clone of your VM. We need two Linux machines for these exercises. Instead of installing another, you can just make a copy from the existing one. Please note also: if you clone the VM with OpenSSH server installed, the server keeps its host key. Thus you really should regenerate new SSH server keys after new VM is deployed. Also remember that you just might hit situation where your VMs have same IP or MAC address or so

Answer:

After first VM was created I exported .ova file to my desktop and then imported it to virtualbox with different MAC address.

After cloning i changed both machines network settings from NAT to bridge and got them a different IP addresses.

Then I created new SSH keys to both machines with command:

```
ssh-keygen -t ed25519
```

3 Task 3

Since management of Linux machines is most often done through SSH, we do that as well in this course.

1. Login to your 1st Linux machine via SSH.

   I installed Putty to my desktop and connected it to my first Linux with its IP and port number 22.

2. Set up SSH keys so there is no need to type password (nor even username) when logging in

   I used Putty connection manager to connect to CentOS from my desktop.
   I configured auto login with this guide https://www.technlg.net/windows/putty-auto-login-ssh-keys/
   I used WinSCP to copy the ssh key to my desktop

3. Set up the sudo access right management so that you can use sudo instead of su.

   I used this command to add my user to sudoers

   Sudo usermod -aG wheel *username*

4 TASK 4

Install a VyOS virtual router to your Virtualbox. Name it e.g. VyOS-1Tips: - Use Linux / Debian64 for your Vyos virtual box machine type and version.- Vyos has default credentials: vyos/vyos- You can install vyos to the VM via install image-command from the VyOS cli. Before making any configurations to it, make a clone out of it to and name it e.g. to VyOS-2

Downloaded VyOS ISO-file from https://support.vyos.io/en/downloads/files/vyos-1-1-8-iso

Installed VyOS to Debian64

Then changed keyboard settings to Finland with:

```
sudo dpkg-reconfigure keyboard-configuration
```

Next created exported .ova file to my desktop and then imported it to virtualbox.

Exercise 2a

Arttu Karhunen
n4924@student.jamk.fi

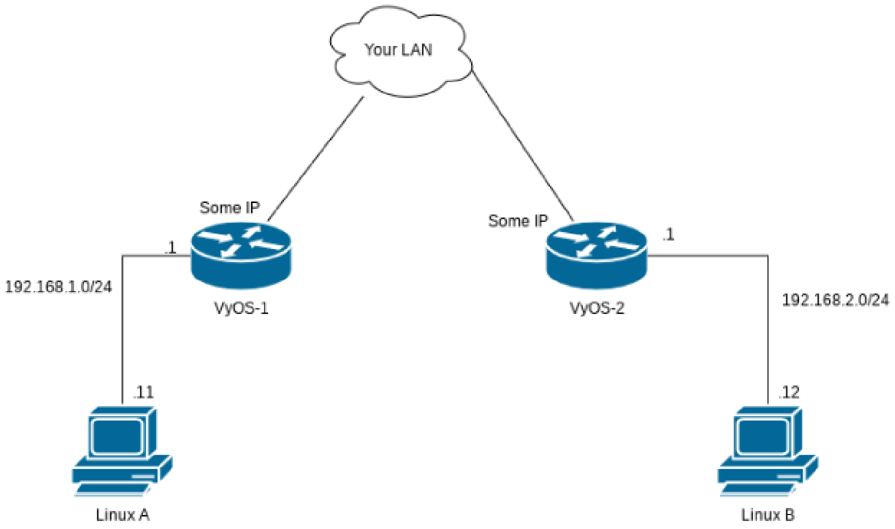
Exercise
Syyskuu 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Apply better network setup.Needed stuff: Your Linux VMs and VyOS machinesNotes: You might need this: https://wiki.vyos.net/wiki/User_Guide

5 TASK 1

Create a network setup from your Linux VMs and VyOS routers that matches the one depicted.Note: This is very poor network documentation image. Only meant for initial setup.From the virtualbox, the Vyos interface towards Your Lan can be either in bridged or in internal mode having some dedicated internal network assigned.The interconnections between a machine and its corresponding router should be done using Virtualbox internal networks. Thus VyOS-1 and VyOS-2 require two network interfaces. Verify that e.g. Linux A can ping VyOS-1 192.168.1.1 interface and likewise Linux B VyOS-2.



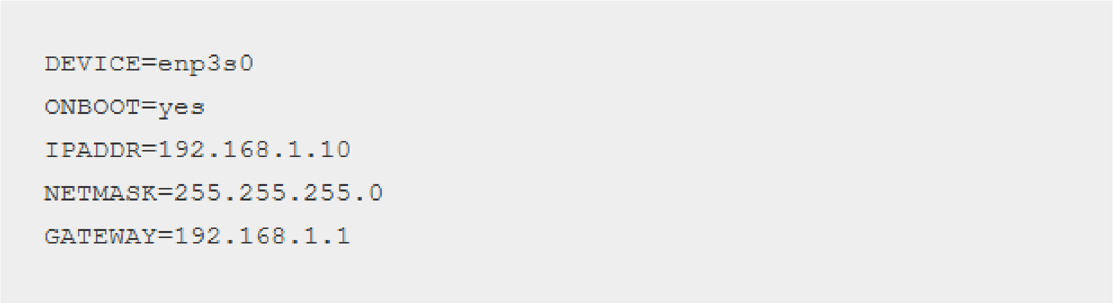
Task 1 execution:

At first I created both Vyos routers 2 network adapters eth0 and eth1 in virtualbox GUI. Eth0 was then configured as internatl network which is going to connect to the CentOS machine. Eth1 was configured as bridged so it’s in a same network as the desktop host machine.

Both virtual CentOS machines network adapters were configured as internal metwork

Next step I created IP addresses to the Vyos routers according to the https://wiki.vyos.net/wiki/User_Guide.

Then I added IP addresses, network mask and default gateway to CentOS /config/config.boot file.



```
DEVICE=enp3s0
ONBOOT=yes
IPADDR=192.168.1.10
NETMASK=255.255.255.0
GATEWAY=192.168.1.1
```

TASK 2

Add static routes to your network that all devices can ping each others. Tips: read https://wiki.vyos.net/wiki/User_GuideTASK 3:Document your work to your own exercise document

Task 2 execution:

I added static routes to both Vyos routers like this:

```
set protocols static route 0.0.0.0/0 next-hop <address>
```

where 0.0.0.0/0 is network where we are going to connect. In this case the internal network in other Vyos/CentOS. Address is the IP address of the other Vyos in the bridged network.

Then we had a connection from CentOS-1 to CentOS -2.

Exercise 2b

Arttu Karhunen
n4924@student.jamk.fi

Exercise
Syyskuu 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Goal: Better network diagrams

Needed stuff: ?

Notes: Be a Visionaire

6 TASK 1

From the previous exercise you created a network. Now it is the time to create network diagrams of it.

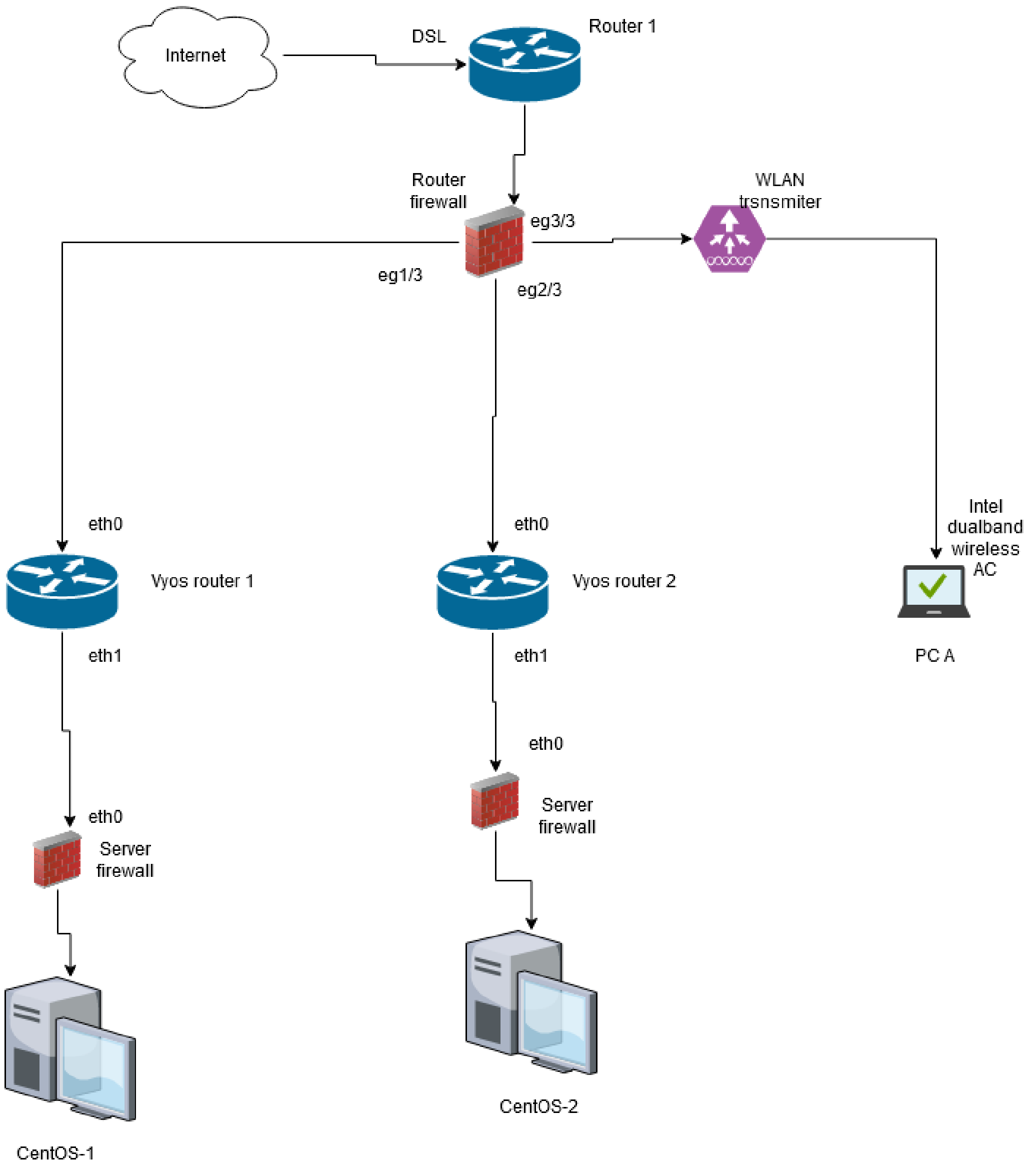
Consider the VyOS-1 and VyOS-2 routers to be in different physical location. Like you'd had two different sites.

Create two network diagrams of your current network:
- Physical setup
- Logical setup

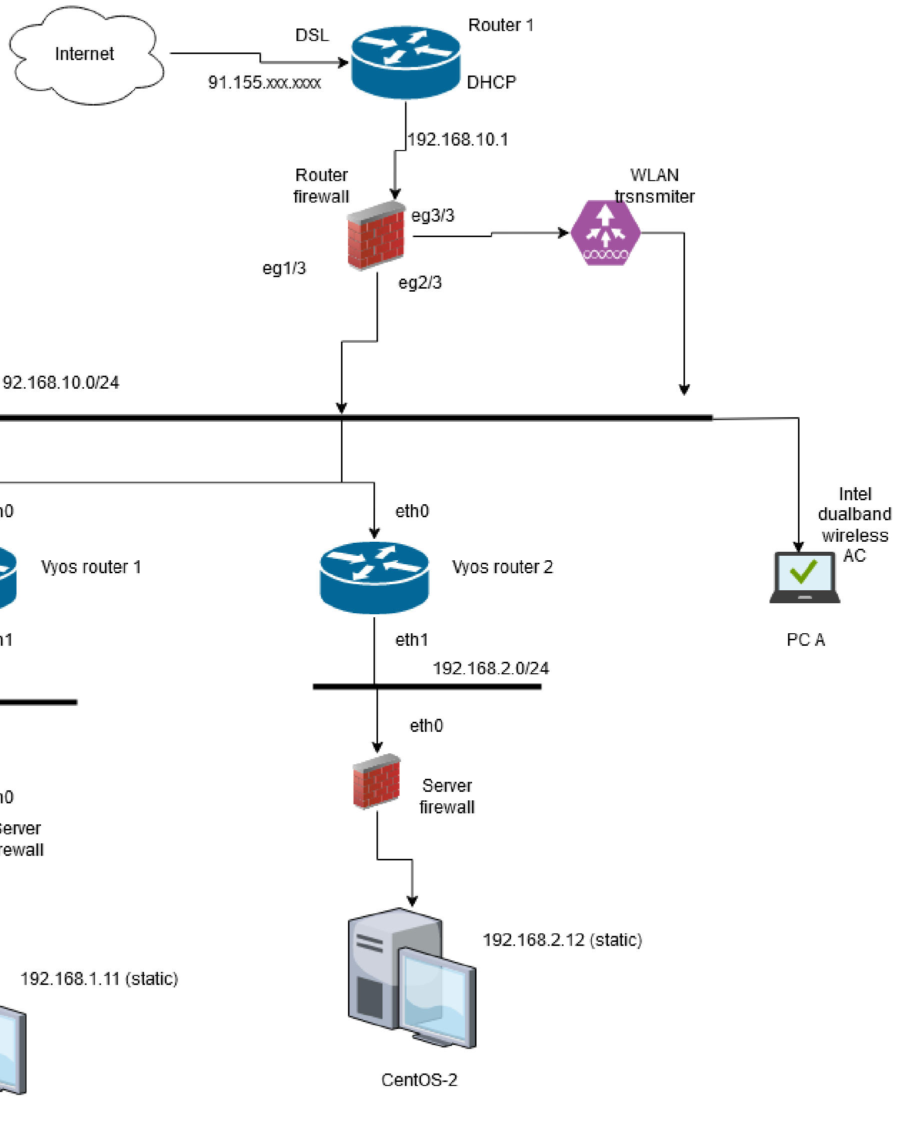
Two existing networks, 192.168.1.0/24, and 192.168.2.0/24 should be treated as workstation networks.

Note: Yes, we are running these exercises in virtualbox. Try to forget the virtualization and draw the physical diagram as it would be real world. Insert pictures from this task also to your exercise document please.

Physical network:



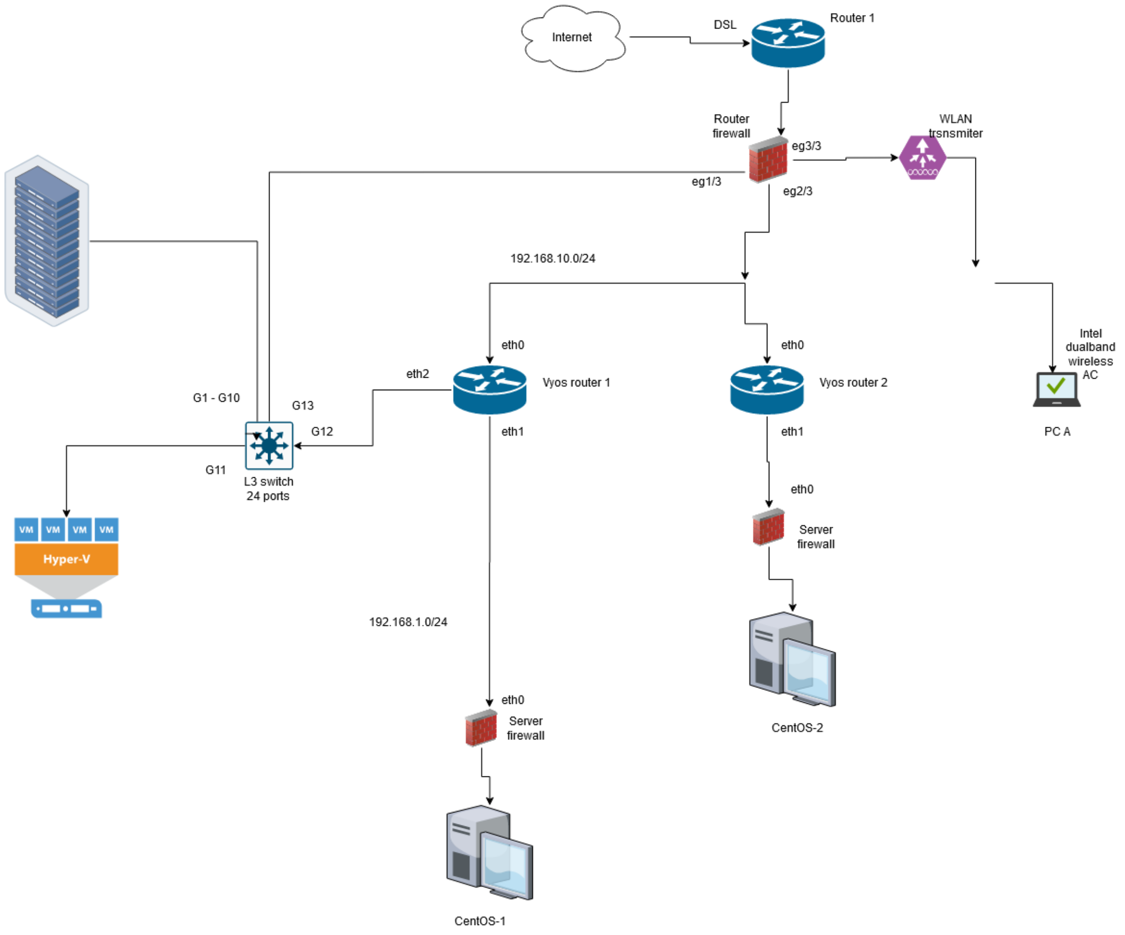
Logical network:



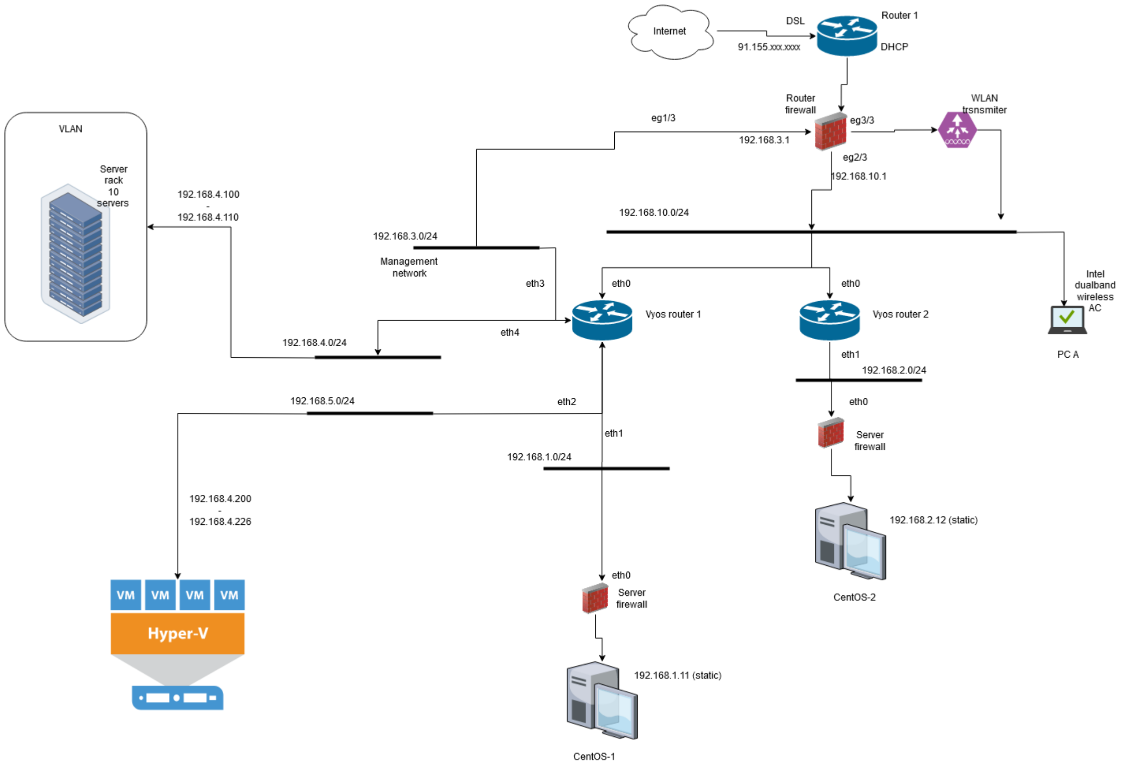
7 TASK 2

Now it is time to add some stuff into these documents. Make plans to your physical and logical pictures to include in the VyOS-1 site :
- separate management network for network devices (this case VyOS)
- VLAN for virtual machine servers running customer applications. Room for approx 20-30 VMs there.
- VLAN for servers running infrastructure services. Room for approx 10 machines.
You can pretty flexible decide the network layout as these aforementioned goals are met. Insert pictures from this task also to your exercise document please.

Physical network:



Logical network:



Exercise 3

BGP setup

Arttu Karhunen
n4924@student.jamk.fi

Exercise
Syyskuu 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Goal: Setup BGP between VyOS routers

8 TASK 1

Question:

Remove all static routes from the VyOS routers so the networks cannot reach each others!

Answer:

Removed all static routes from Vyos Routers with:

```
$ configure

$ delete protocol static route [network]

Commit

Save

Exit
```

Unable to ping another Vyos anymore.

9 TASK 2

Question:

Set up BGP between VyOS-1 and VyOS-2 Assume they are in separate AS. Thus use AS numbers e.g. 65001 and 65002 for them respectively. Once done, verify that Linux A and B can ping each others. Tips:
https://wiki.vyos.net/wiki/BGPhttps://docs.vyos.io/en/latest/routing/bgp.htmlRemember to bind the bgp to loopback interface as suggested here: http://www.powerfast.net/bgp/BGP_Nd45.html
Oh: REMEMBER: in VyOS configure mode use save to store your configs over reboot

Answer:

VyOS 1 Configuration:

```
set protocols bgp 65001 neighbor 192.168.10.123 ebgp-multihop '2'
set protocols bgp 65001 neighbor 192.168.10.123 update-source '192.168.10.177'
set protocols bgp 65001 neighbor 192.168.10.123 remote-as '65002'

set protocols bgp 65001 network '192.168.41.0/24'
set protocols bgp 65001 parameters router-id '192.168.10.177'
```

VyOS 2 Configuration:

```
set protocols bgp 65002 neighbor 192.168.10.177 ebgp-multihop '2'
set protocols bgp 65002 neighbor 192.168.10.177 update-source '192.168.10.123'
set protocols bgp 65001 neighbor 192.168.10.123 remote-as '65001'

set protocols bgp 65002 network '192.168.42.0/24'
set protocols bgp 65002 parameters router-id '192.168.10.123'
```

Then ping VyOS1 to VyOS2 and another way around.
Then ping from CentOS to another.

10 TASK 3

Prepend the AS path from 65001 towards 65002.

```
# set policy route-map setasp rule 10 action 'permit'

# set policy route-map setasp rule 10 set as-path 65002

# commit

# show policy route-map setasp rule 10 set

# set protocols bgp 65001 neighbor 192.168.10.123 route-map import setasp

# set protocols bgp 65001 neighbor 192.168.10.123 soft-reconfiguration inbound
```

11 TASK 4

Add MED of 100 for route updates from 65002 towards 65001.https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13759-37.htm

```
# set policy route-map setmed rule 1 action 'permit'

# set policy route-map setmed rule 1 set metric 100
Commit

# show policy route-map setmed rule 1 set

# set protocols bgp 65001 neighbor 192.168.10.123 route-map import setmed
# set protocols bgp 65001 neighbor 192.168.10.123 soft-reconfiguration inbound
```

Exercise 4

VPN

Arttu Karhunen
n4924@student.jamk.fi

Exercise
Syyskuu 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Goal: VPN between your VyoS routers

Needed stuff: Your setup

Notes: Decide is yours

12 TASK 1

Question:

First of all, remove all BGP stuff from your VyoS routers

Answer:

Delete protocols bgp

Delete policy route-map

13 TASK 2 (optional)

Question:

If you feel like: add NAT to your VyOS routers so the Linux machines behind can reach the Internet.

Answer:

VyOS1

```
Configure
set nat source rule 100 outbound-interface 'eth0'
set nat source rule 100 source address '192.168.41.0/24'
set nat source rule 100 translation address 'masquerade'
```

VyOS2

```
Configure
set nat source rule 100 outbound-interface 'eth0'
set nat source rule 100 source address '192.168.42.0/24'
set nat source rule 100 translation address 'masquerade'
```

14 TASK 3

Question:

Configure one of the next: IPsec OpenVPN WireguardVPN between your VyOS routers. Assume the connection between them is in public network and you wish to have them connected with each others using secure VPN mechanism.

Answer:

Configured IPsec IKEv1 with this example:

Vyos 1 local_IP: 192.168.10.177 (Bridged adapter)

Vyos 1 subnet: 192.168.41.0/24 (Centos network)

Vyos 2 local_IP: 192.168.10.123 (Bridged adapter)

Vyos 2 subnet: 192.168.42.0/24 (Centos network)

15 TASK 4

Question:

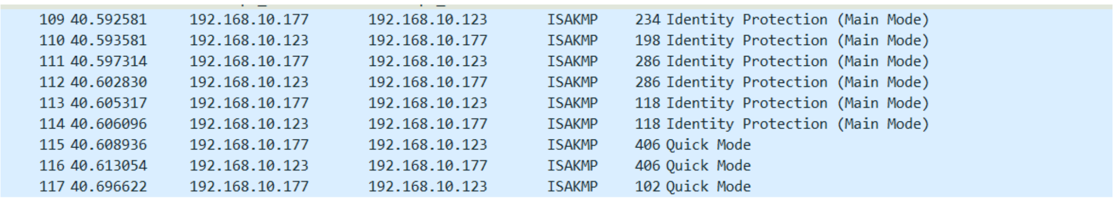
Verify the connectivity using Linux machines and try to capture VPN network traffic using Wireshark or some similar.

Answer:

To see the traffic between vyos routers I started VBoxManage nictrace for Vyos 1 router, which makes log files for all traffic in virtual machine.

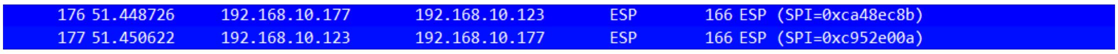
When VBoxManage was logging I openend vyos routers and centos machines. Then ping Centos 1 to Centos 2 machine.

Then opened log file in wireshark. First you can see ISAKMP packets which defines payloads for exchanging key generation and authentication data.



```
109 40.592581   192.168.10.177   192.168.10.123   ISAKMP   234 Identity Protection (Main Mode)
110 40.593581   192.168.10.123   192.168.10.177   ISAKMP   198 Identity Protection (Main Mode)
111 40.597314   192.168.10.177   192.168.10.123   ISAKMP   286 Identity Protection (Main Mode)
112 40.602830   192.168.10.123   192.168.10.177   ISAKMP   286 Identity Protection (Main Mode)
113 40.605317   192.168.10.177   192.168.10.123   ISAKMP   118 Identity Protection (Main Mode)
114 40.606096   192.168.10.123   192.168.10.177   ISAKMP   118 Identity Protection (Main Mode)
115 40.608936   192.168.10.177   192.168.10.123   ISAKMP   406 Quick Mode
116 40.613054   192.168.10.123   192.168.10.177   ISAKMP   406 Quick Mode
117 40.696622   192.168.10.177   192.168.10.123   ISAKMP   102 Quick Mode
```

Then can see as many ESP packets between VPN peers as there was ping messages sent between Centos machines.



```
176 51.448726   192.168.10.177   192.168.10.123   ESP   166 ESP (SPI=0xca48ec8b)
177 51.450622   192.168.10.123   192.168.10.177   ESP   166 ESP (SPI=0xc952e00a)
```

Exercise 5

Linux network setup and firewalling

Arttu Karhunen
n4924@student.jamk.fi

Exercise
Lokakuu 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Goal: Apply better network setup and a firewall

Needed stuff: Your Linux VM

Notes: This really changes the setup. Please see attachment1 on the next page.

16 TASK 1

Question:

Apply a network setup based on your plans in the exercise 2b. So create these three networks more.

Answer:

First need to create one more adapter to VyOS 1 router with these commands in windows cmd:

```
VBoxManage modifyvm VyOS_1 --nic5 intnet
VBoxManage modifyvm VyOS_1 --nictype5 82545EM
VBoxManage modifyvm VyOS_1 --macaddress5 auto
VBoxManage modifyvm VyOS_1 --cableconnected5 on
VBoxManage modifyvm VyOS_1 --intnet5 intnet2
```

Then change eth0 adapter to NAT from Vyos 1 and Vyos2.
Then change eth0 address in /config/config.boot to dhcp
Then ip addresses to three more adapters:

```
# Set interfaces ethernet eth2 address 192.168.50.1/24

# Set interfaces ethernet eth3 address 192.168.60.1/24

# Set interfaces ethernet eth4 address 192.168.70.1/24
```

17 TASK 2

Question:

Apply firewalling to your VyOS-1 and VyOS-2 routers. Deny all incoming connections from the outside. Also create firewall rules to limit the network traffic between the different networks.

Answer:

Same configurations to both VyOS routers except interfaces eth2,3 and 4 only in VyOS 1 router

First firewall rules for traffic coming for outside the subnet

```
# Set firewall name OUTSIDE-LOCAL default-action drop
# set firewall name OUTSIDE-IN default-action 'drop'

# Set interfaces ethernet eth0 firewall local name OUTSIDE-LOCAL
# Set interfaces ethernet eth0 firewall in name OUTSIDE-IN
```

Then firewall rules for limiting traffic between subnets

```
# Set interfaces ethernet eth1 firewall local name OUTSIDE-LOCAL
# Set interfaces ethernet eth2 firewall local name OUTSIDE-LOCAL
# Set interfaces ethernet eth3 firewall local name OUTSIDE-LOCAL
# Set interfaces ethernet eth4 firewall local name OUTSIDE-LOCAL
```

18 TASK 3

Question:

Add NAT to the VyOS-1 and VyOS-2 so that Linux machines have Internet connectivity.Tips: read https://wiki.vyos.net/wiki/User_Guide

Answer:

NAT for 192.168.41.0 subnet in VyOS 1 and 192.168.42.0 for VyOS 2

```
#set nat source rule 100 outbound-interface 'eth0'
#set nat source rule 100 source address '192.168.41.0/24'
#set nat source rule 100 translation address masquerade
```

19 TASK 4

Question:

Now once you’re finished with setting up the firewall and NAT. Change the interface that is connecting your VyOS routers together to “Bridged” mode from Virtualbox settings. Change the specific interface to fetch IP address using DHCP (or setup a static addressing and routing) so that the VyOS routers can reach the Internet → And also the Linux machines behind them.

Answer:

Changed NAT interfaces to bridged and IP addresses to dhcp in /config/config.boot

Then set firewall settings so CentOS machines can connect to internet.

```
# set firewall name OUTSIDE-IN rule 10 action 'accept'
# set firewall name OUTSIDE-IN rule 10 state established 'enable'
# set firewall name OUTSIDE-IN rule 10 state related 'enable'
```

```
# Set interfaces ethernet eth1 firewall out name OUTSIDE-IN
# Set interfaces ethernet eth2 firewall out name OUTSIDE-IN
# Set interfaces ethernet eth3 firewall out name OUTSIDE-IN
# Set interfaces ethernet eth4 firewall out name OUTSIDE-IN
```

20 TASK 5

Question:

Update the VPN setup endpoint IP addresses if necessary to have working tunnel. Verify connectivity between VMs and routers using ping and also towards the Internet using ping. For instance ping 62.78.96.149. To have fluent Internet connectivity and for instance yum to operate correctly: Remember that DNS nameservers must be specified to Linux machines.

Answer:

To get VPN tunnel working need to accept LAN to connect to VPN service:

```
# set firewall name OUTSIDE-LOCAL rule 20 action 'accept'
# set firewall name OUTSIDE-LOCAL rule 20 source address 192.168.10.0/24
```

Exercise 6

High availability

Arttu Karhunen
n4924@student.jamk.fi

Exercise
Lokakuu 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Goal: Insert another VyOS router next to your VyOS-2 and make them a HA pair

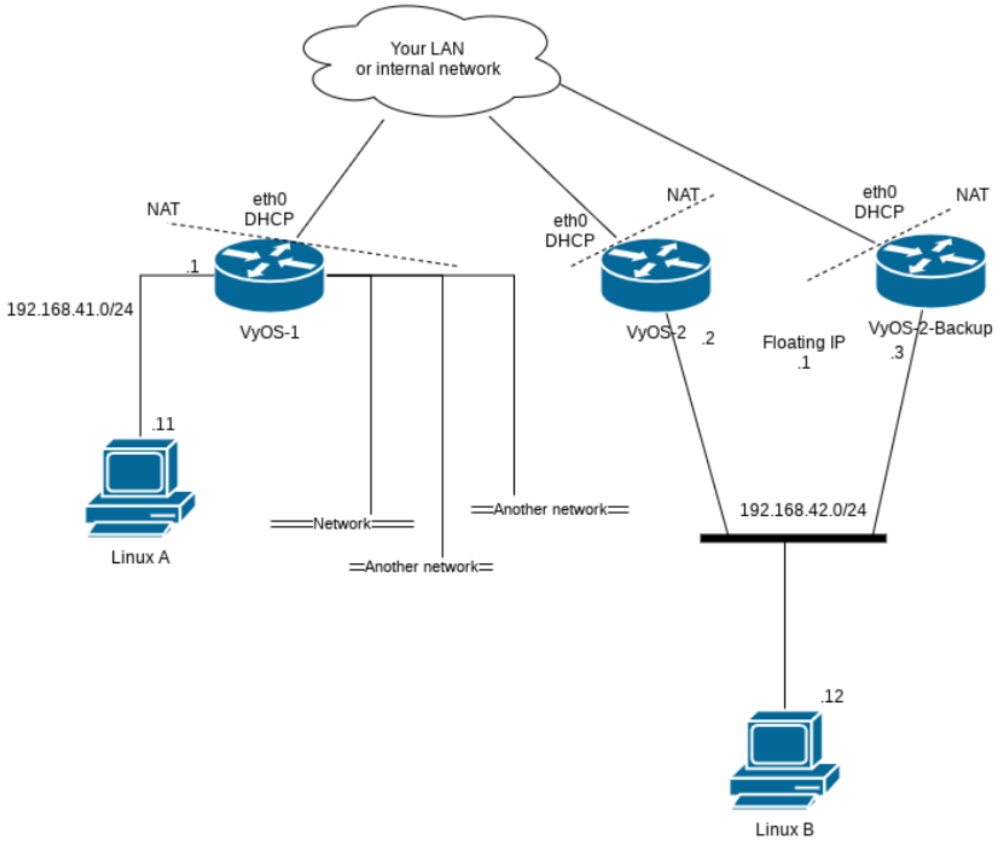
Needed stuff: Your environment

Notes: We’re using VyOS-2 since it has only one network behind. This way its simpler.

21 TASK 1

Question:

Clone your VyOS-2 router. Remember to create new MAC addresses.. re-configure IP addressing for the router so they do not overlap. For instance assign 192.168.42.2 and 192.168.42.3 to them. The 192.168.42.1 can then be used for floating IP for VRRP. Please see the attachment.



Answer:

Cloned the vyos 2 by exporting vm to desktop and installing with new mac addresses.

Still needed to manually change the mac addresses to /config/config.boot to get interfaces eth0 and eth1 as NAT and internal networks. Because VirtualBox generated them as adapters eth2 and eth3.

22 TASK 2

Question:

Configure high-availability, VRRP group, for your 192.168.42.0/24 network. Verify the connectivity using Centos Linux. Also check the MAC addresses with “arp” -command”

note that you might need net-tools package from the repository.

Additionally take a capture using e.g. tcpdump to show the VRRP network packets.

Answer:

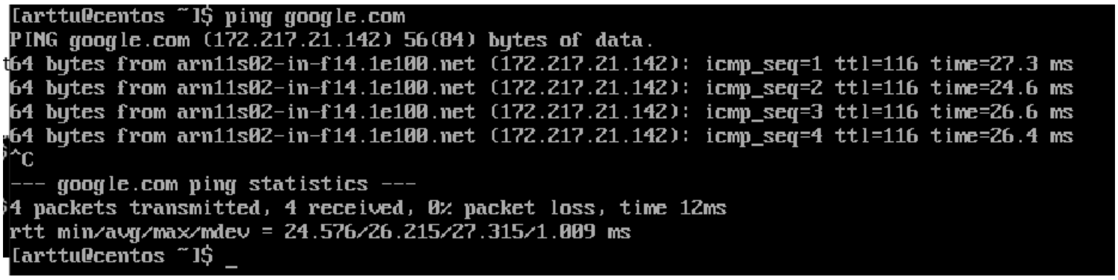
Primary router:

```
set interfaces ethernet eth0 vrrp vrrp-group 1 preempt true
set interfaces ethernet eth0 vrrp vrrp-group 1 priority 200
set interfaces ethernet eth0 vrrp vrrp-group 1 virtual-address 192.168.42.1/24
```

backup router:

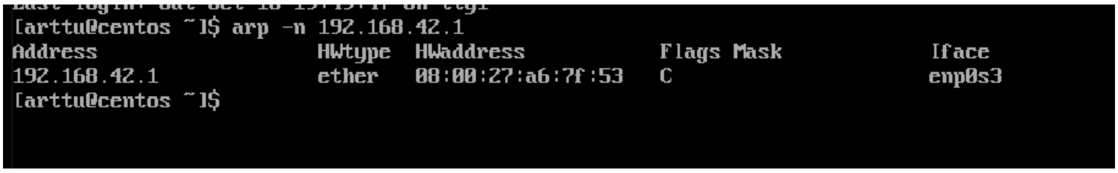
```
set interfaces ethernet eth0 vrrp vrrp-group 1 preempt true
set interfaces ethernet eth0 vrrp vrrp-group 1 priority 100
set interfaces ethernet eth0 vrrp vrrp-group 1 virtual-address 192.168.42.1/24
```

Checking connectivity with CentOS



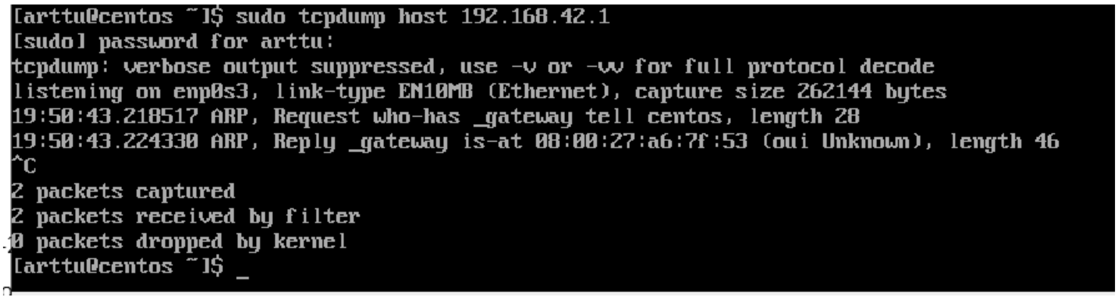
```
[arttu@centos ~]$ ping google.com
PING google.com (172.217.21.142) 56(84) bytes of data.
64 bytes from arn11s02-in-f14.1e100.net (172.217.21.142): icmp_seq=1 ttl=116 time=27.3 ms
64 bytes from arn11s02-in-f14.1e100.net (172.217.21.142): icmp_seq=2 ttl=116 time=24.6 ms
64 bytes from arn11s02-in-f14.1e100.net (172.217.21.142): icmp_seq=3 ttl=116 time=26.6 ms
64 bytes from arn11s02-in-f14.1e100.net (172.217.21.142): icmp_seq=4 ttl=116 time=26.4 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 12ms
rtt min/avg/max/mdev = 24.576/26.215/27.315/1.009 ms
[arttu@centos ~]$ _
```

Arp-table in CentOS:



```
[arttu@centos ~]$ arp -n 192.168.42.1
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.42.1             ether   08:00:27:a6:7f:53   C                     enp0s3
[arttu@centos ~]$
```

VRRP packets in tcpdump



```
[arttu@centos ~]$ sudo tcpdump host 192.168.42.1
[sudo] password for arttu:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
19:50:43.218517 ARP, Request who-has _gateway tell centos, length 28
19:50:43.224330 ARP, Reply _gateway is-at 08:00:27:a6:7f:53 (oui Unknown), length 46
^C
2 packets captured
2 packets received by filter
0 packets dropped by kernel
[arttu@centos ~]$ _
```

23 TASK 3

Question:

When the VyOS-2 router hosting IPSec faces problems and e.g. shuts down, traffic should change to the backup router in this network. Explain what happens to the VPN tunnel between sites? How could you resolve this issue? No need to resolve it though, but if you do: its highly appreciated.

Answer:

Tunnel between host router and client will break and so VPN connection will brake also. To get VPN working in backup router you could have separate ipsec tunnel between that router and the client. That connection could be addressed to same subnet as the primary router.

Exercise 7

Monitoring devices

Arttu Karhunen
n4924@student.jamk.fi

Exercise
Lokakuu 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Goal: Start to monitor your devices.

Needed stuff: Your environment

Notes: This requires some setup

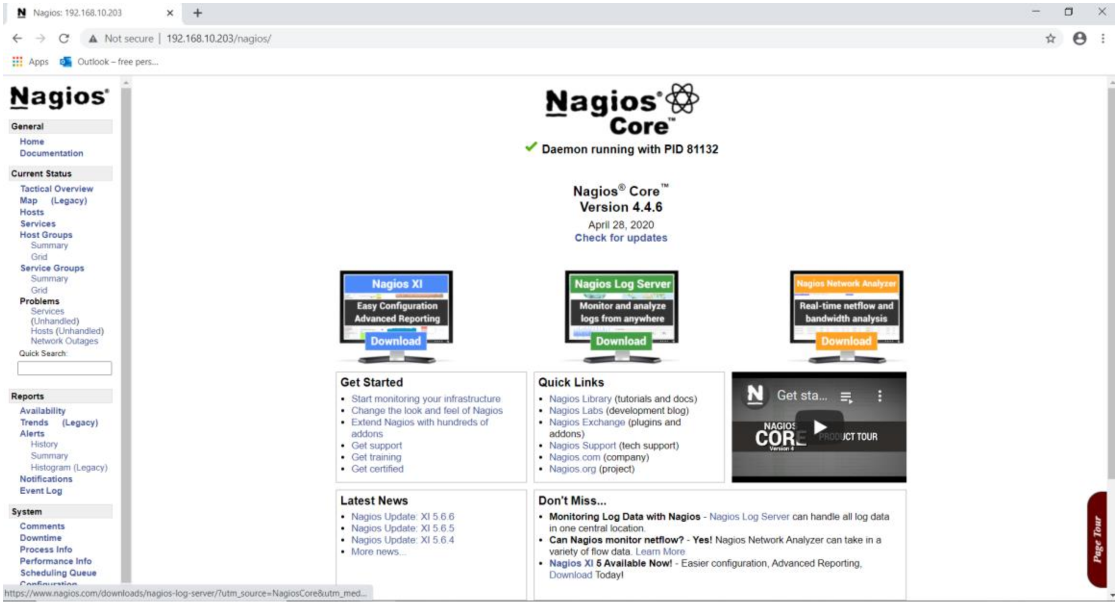
24 TASK 1

Question:

Set up either Nagios or Observium to a Centos Linux server. You can decide which one to use. Also using existing Linux machine is allowed, as long as you remember that in real life the network environment should be carefully considered and firewalled. This time its just fine to reduce the load from your machine and not to create a lot of new VMs. (like in this task we could have created new machine(monitoring machine) to new network(admin tools).Once done, add a screenshot to the document from it.

Answer:

Kuva nagios selain ikkunasta.



Daemon running with PID 81132

Nagios® Core™
Version 4.4.6
April 28, 2020
Check for updates

Get Started

- Start monitoring your infrastructure
- Change the look and feel of Nagios
- Extend Nagios with hundreds of addons
- Get support
- Get training
- Get certified

Quick Links

- Nagios Library (tutorials and docs)
- Nagios Labs (development blog)
- Nagios Exchange (plugins and addons)
- Nagios Support (tech support)
- Nagios.com (company)
- Nagios.org (project)

Latest News

- Nagios Update: XI 5.6.6
- Nagios Update: XI 5.6.5
- Nagios Update: XI 5.6.4
- More news...

Don't Miss...

- **Monitoring Log Data with Nagios** - Nagios Log Server can handle all log data in one central location.
- **Can Nagios monitor netflow? - Yes!** Nagios Network Analyzer can take in a variety of flow data. Learn More
- **Nagios XI 5 Available Now!** - Easier configuration, Advanced Reporting, Download Today!

25 TASK 2

Question:

Add both VyOS routers to the monitoring service.

Answer:

1.

Edit the main Nagios config file.

```
vi /usr/local/nagios/etc/nagios.cfg
```

Remove the leading pound (#) sign from the following line in the main configuration file:

```
#cfg_file=/usr/local/nagios/etc/objects/switch.cfg
```

Save the file and exit.

2.

This for both routers

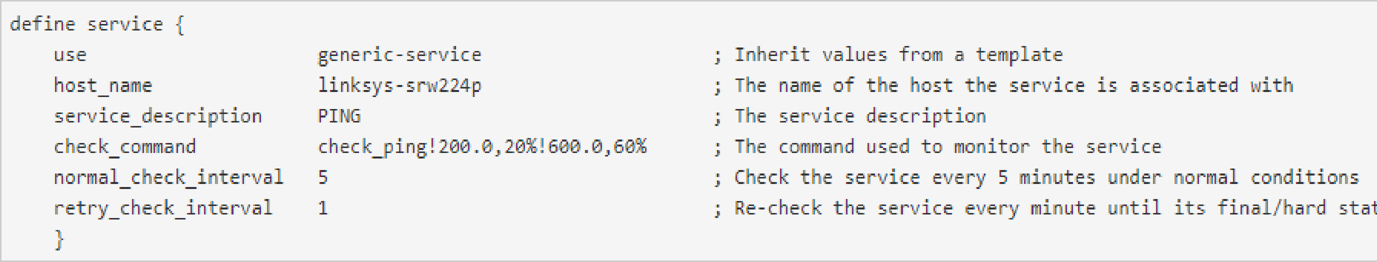
Open the switch.cfg file for editing.

```
vi /usr/local/nagios/etc/objects/switch.cfg
```

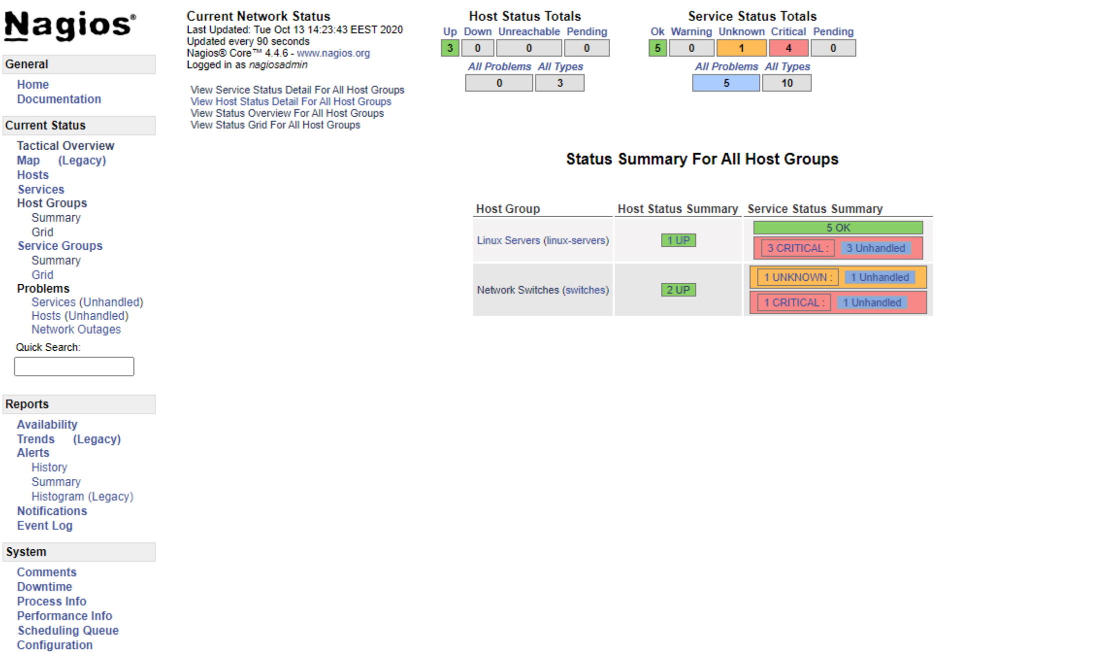
Add a new host definition for the switch that you're going to monitor. If this is the *first* switch you're monitoring, you can simply modify the sample host definition in switch.cfg. Change the host_name, alias, and address fields to appropriate values for the switch.

```
define host {
   use         generic-switch          ; Inherit default values from a template
   host_name   VyOS_1                             ; The name we're giving to this switch
   alias       VyOS_1 Switch           ; A longer name associated with the switch
   address     192.168.10.177          ; IP address of the switch
   hostgroups  allhosts,switches       ; Host groups this switch is associated with
}
```

Defining service



```
define service {
    use                     generic-service                 ; Inherit values from a template
    host_name               linksys-srw224p                 ; The name of the host the service is associated with
    service_description     PING                            ; The service description
    check_command           check_ping!200.0,20%!600.0,60%  ; The command used to monitor the service
    normal_check_interval   5                               ; Check the service every 5 minutes under normal conditions
    retry_check_interval    1                               ; Re-check the service every minute until its final/hard stat
    }
```



Current Network Status
Last Updated: Tue Oct 13 14:23:43 EEST 2020
Updated every 90 seconds
Nagios® Core™ 4.4.6 - www.nagios.org
Logged in as *nagiosadmin*

Host Status Totals

Up	Down	Unreachable	Pending
3	0	0	0

All Problems	*All Types*
0	3

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
5	0	1	4	0

All Problems	*All Types*
5	10

Status Summary For All Host Groups

Host Group	Host Status Summary	Service Status Summary
Linux Servers (linux-servers)	1 UP	5 OK 3 CRITICAL : 3 Unhandled
Network Switches (switches)	2 UP	1 UNKNOWN : 1 Unhandled 1 CRITICAL : 1 Unhandled

26 TASK 3

Question:

Add one Linux server to the monitoring service.

Answer:

First Install nrpe-plugins to remote linux server with dnf.

```
# dnf install epel-release
# dnf install nrpe
# dnf search nagios-plugins
```

I chosed plugins:

```
# dnf install nagios-plugins-nrpe
# dnf install nagios-plugins-load
# dnf install nagios-plugins-users
```

Then enable nrpe:

```
# systemctl enable --now nrpe
```

Then accept it in firewall:

```
# firewall-cmd --add-port=5666/tcp --permanent
# firewall-cmd –reload
```

Then check it listening the right port:

```
# netstat -at | egrep "nrpe|5666"
```

Then add allowed host to /etc/nagios/nrpe.cfg:

```
allowed_hosts=127.0.0.1,192.168.42.12
```

on the nagios server side:

Install nrpe plugins:

```
# wget
https://github.com/NagiosEnterprises/nrpe/releases/download/nrpe
-3.2.1/nrpe-3.2.1.tar.gz
```

Extract the NRPE source code tarball:

```
# tar xzf nrpe-3.2.1.tar.gz# cd nrpe-nrpe-3.2.1
```

Compile the NRPE addon:

```
# ./configure

# make check_nrpe
```

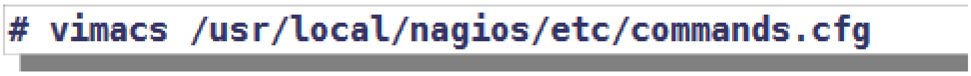
Install the NRPE plugin.

```
# make install-plugin
```

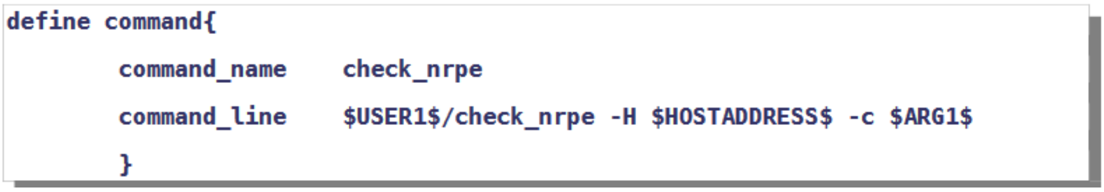
Then test connection:

```
#/usr/local/nagios/libexec/check_nrpe -H 192.168.42.12
```

Then add command definition to configure file:

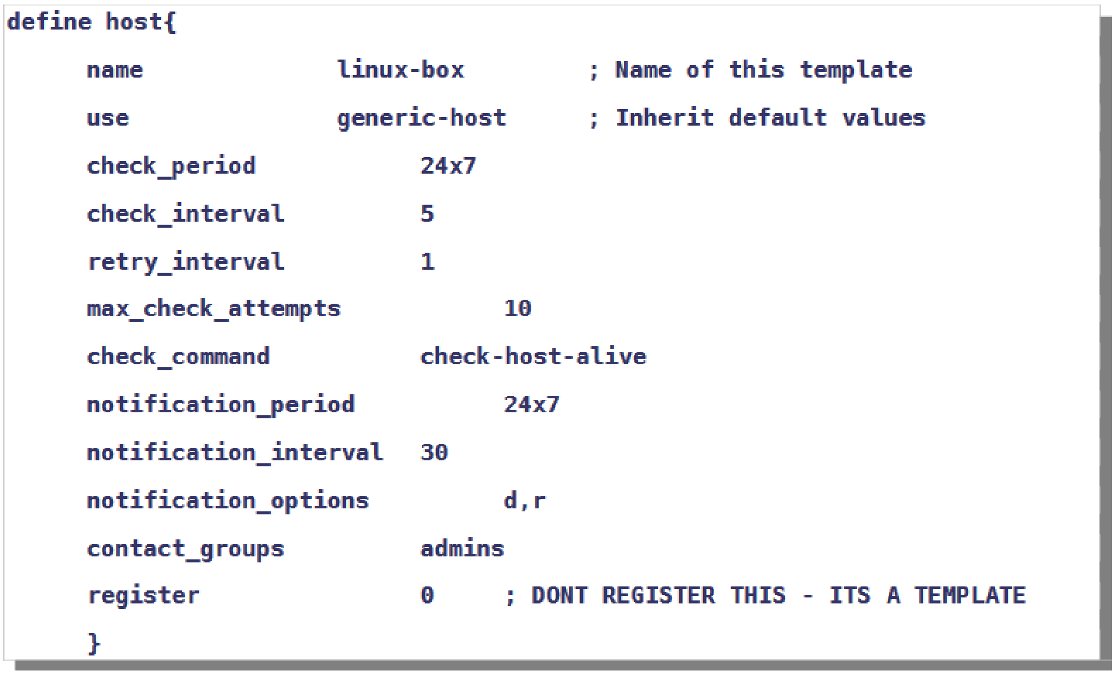


```
# vimacs /usr/local/nagios/etc/commands.cfg
```



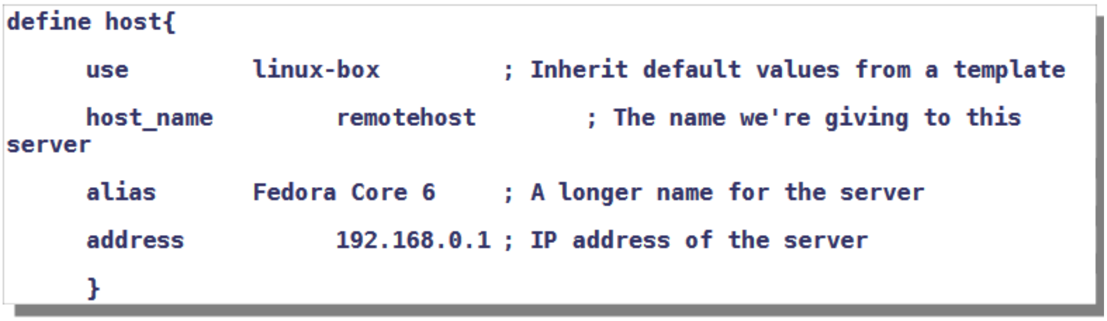
```
define command{
        command_name    check_nrpe
        command_line    $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$
        }
```

Then need to add template to host:



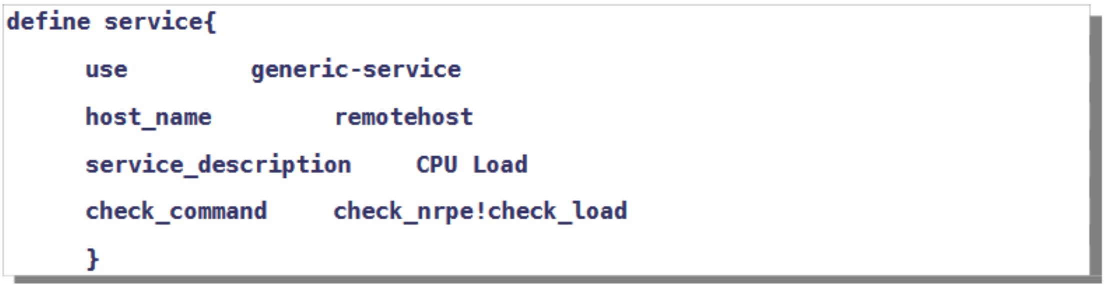
```
define host{
      name              linux-box        ; Name of this template
      use               generic-host     ; Inherit default values
      check_period            24x7
      check_interval          5
      retry_interval          1
      max_check_attempts            10
      check_command           check-host-alive
      notification_period           24x7
      notification_interval   30
      notification_options          d,r
      contact_groups          admins
      register                0     ; DONT REGISTER THIS - ITS A TEMPLATE
      }
```

Then make define new host:

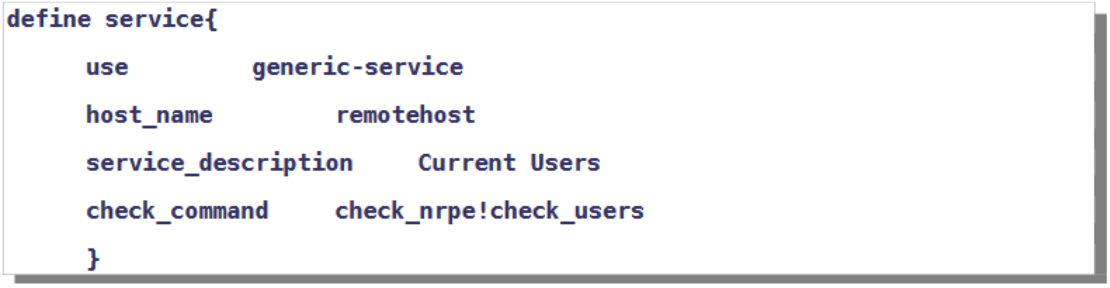


```
define host{
      use         linux-box         ; Inherit default values from a template
      host_name         remotehost        ; The name we're giving to this
server
      alias       Fedora Core 6     ; A longer name for the server
      address           192.168.0.1 ; IP address of the server
      }
```

And add services which I chose to remote server:



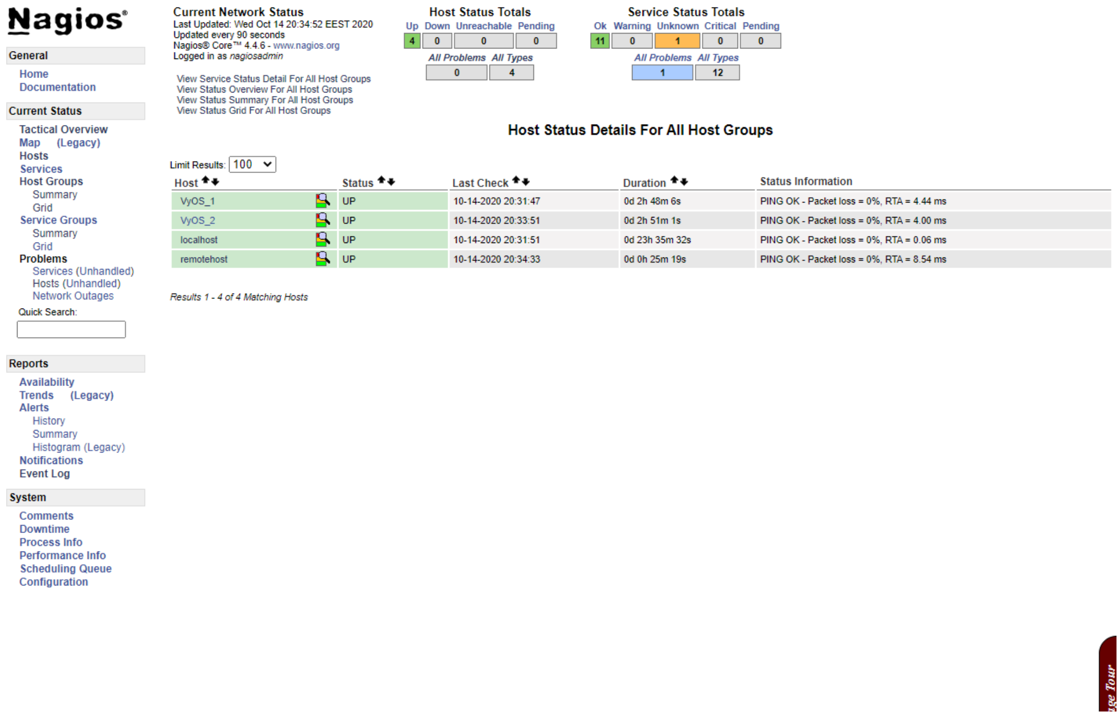
```
define service{
      use         generic-service
      host_name         remotehost
      service_description     CPU Load
      check_command     check_nrpe!check_load
      }
```



```
define service{
      use         generic-service
      host_name         remotehost
      service_description     Current Users
      check_command     check_nrpe!check_users
      }
```

Then restart nagios and nrpe

Now it can be monitored In nagios:



Current Network Status
Last Updated: Wed Oct 14 20:34:52 EEST 2020
Updated every 90 seconds
Nagios® Core™ 4.4.6 - www.nagios.org
Logged in as *nagiosadmin*

Host Status Totals

Up	Down	Unreachable	Pending
4	0	0	0

All Problems	All Types
0	4

Service Status Totals

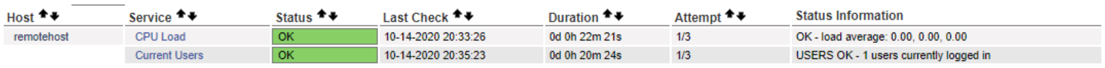
Ok	Warning	Unknown	Critical	Pending
11	0	1	0	0

All Problems	All Types
1	12

Host Status Details For All Host Groups

Host	Status	Last Check	Duration	Status Information
VyOS_1	UP	10-14-2020 20:31:47	0d 2h 48m 6s	PING OK - Packet loss = 0%, RTA = 4.44 ms
VyOS_2	UP	10-14-2020 20:33:51	0d 2h 51m 1s	PING OK - Packet loss = 0%, RTA = 4.00 ms
localhost	UP	10-14-2020 20:31:51	0d 23h 35m 32s	PING OK - Packet loss = 0%, RTA = 0.06 ms
remotehost	UP	10-14-2020 20:34:33	0d 0h 25m 19s	PING OK - Packet loss = 0%, RTA = 8.54 ms

Results 1 - 4 of 4 Matching Hosts



Host	Service	Status	Last Check	Duration	Attempt	Status Information
remotehost	CPU Load	OK	10-14-2020 20:33:26	0d 0h 22m 21s	1/3	OK - load average: 0.00, 0.00, 0.00
	Current Users	OK	10-14-2020 20:35:23	0d 0h 20m 24s	1/3	USERS OK - 1 users currently logged in

27 TASK 4

Question:

Generate some traffic between the Linux machines using e.g. iperf3, hping, ping or so. Watch whether you see this traffic in the monitoring software. Note that in some cases the monitoring software has some specific update time e.g. 5mins or so.

Answer:

I think you cant see traffic from nagios core monitoring software without some plugins example to alert from certain kind of traffic in network. But you can configure nagios to ping host devices to check they response correctly.

Exercise 8

SDN experiments

Arttu Karhunen
n4924@student.jamk.fi

Exercise
Lokakuu 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Goal: Find out how the SDN should work in a UBUNTU linux server.

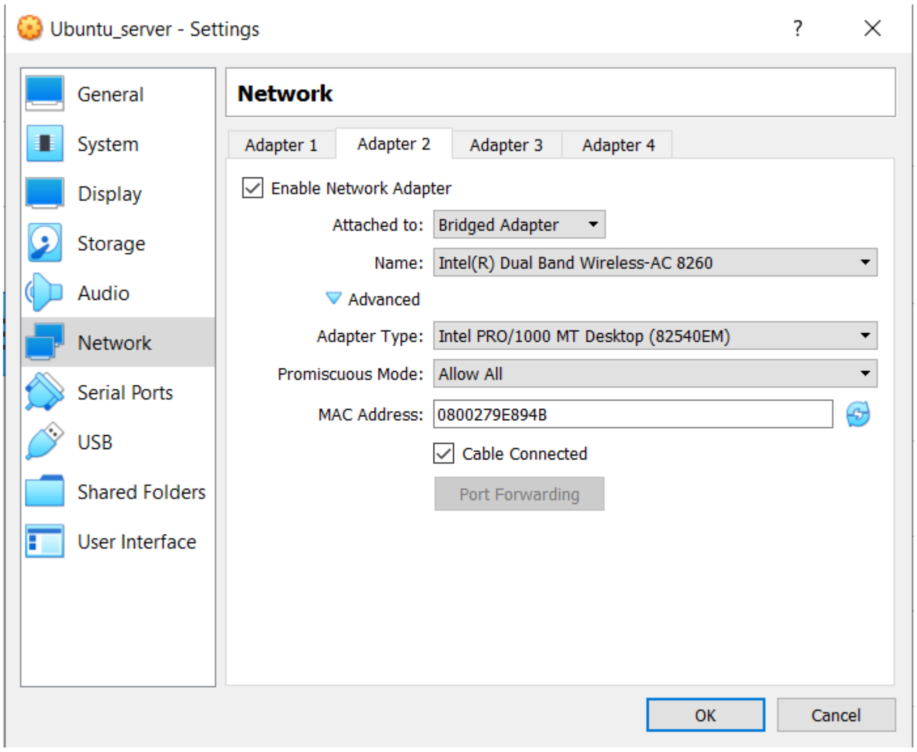
Needed stuff: Ubuntu Linux. Install one or grab one from the teacher.

Notes: Not anymore an easy task.

28 TASK 1

Question:

Add new network interface to a Linux server from Virtualbox. Note! Remember! You MUST set (from the Adapter 2) Advanced → Promiscuous mode: Allow All. This interface will be the one that gets connected to the openvswitch (OVS).
Answer:



Network

☑ Enable Network Adapter

Attached to: Bridged Adapter

Name: Intel(R) Dual Band Wireless-AC 8260

Advanced

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Allow All

MAC Address: 0800279E894B

☑ Cable Connected

29 TASK 2

Question:

Install openvswitch to the Linux server. (in ubuntu openvswitch-switch) You can freely choose the installation method. Once installed, create new bridge to the OVS,.. and connect the added physical network interface to the OVS. Note that you might need to turn the newly created NIC on via: root@ubuntu:~# ip link set enp0s8 up

You can check the openvswitch status with:[root@localhost student]# ovs-vsctl show

Answer:

Installing openswitch with apt and start open vSwitch daemon:

```
sudo apt install openvswitch-switch
sudo ovs-vswitchd
```

Creating new bridge to ovs:

```
ovs-vsctl add-br br0
ovs-vsctl add-port br0 enp0s8
```

30 TASK 3

Question:

Install Faucet SDN controller (https://faucet.nz) to your Linux server.

Answer:

Add the faucet official repo to our system:

```
# sudo apt-get install curl gnupg apt-transport-https lsb-release

# echo "deb https://packagecloud.io/faucetsdn/faucet/$(lsb_release -si | awk
'{print tolower($0)}')/ $(lsb_release -sc) main" | sudo tee
/etc/apt/sources.list.d/faucet.list

# curl -L https://packagecloud.io/faucetsdn/faucet/gpgkey | sudo apt-key add –

# sudo apt-get update
```

Install the faucet-all-in-one metapackage which will install all the correct dependencies.

```
# sudo apt-get install faucet-all-in-one
```

31 TASK 4

Question:

This is all at the moment. Next exercise will be about containers that will run in this Linux and utilize the OVS for their network. Further in next exercise the Faucet SDN controller shall start to manage the OVS.

Answer: 😊

Exercise 9

LXC/LXD installation and containers

Arttu Karhunen
n4924@student.jamk.fi

Exercise
Lokakuu 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Goal: Run LXC containers and use OVS for their networking

Needed stuff: EX8 Ubuntu

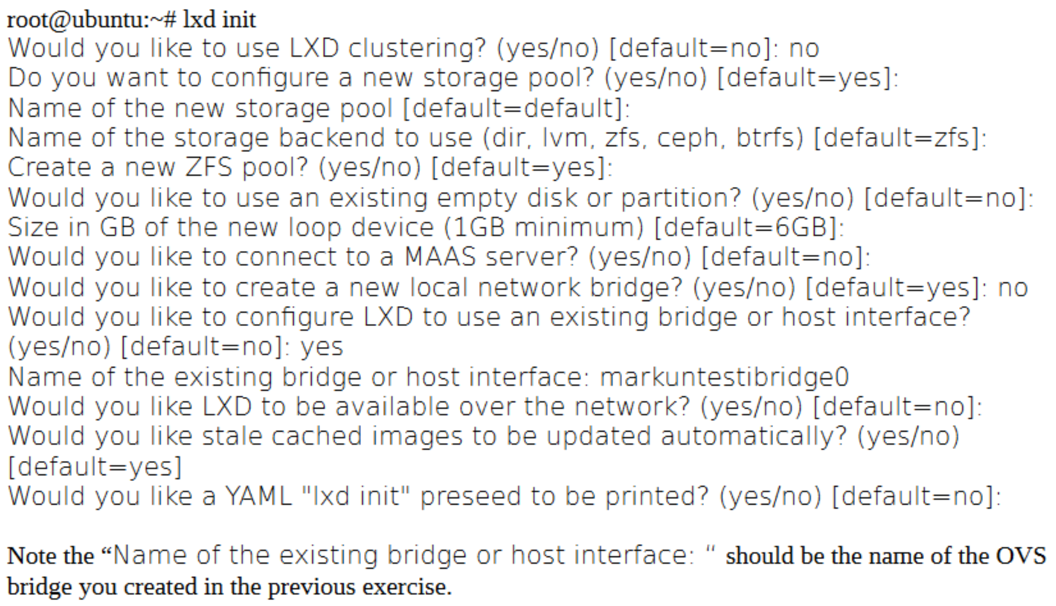
Notes: Complicated, yes

32 TASK 1

Question:

Install the LXD to your Ubuntu server.

Then run lxd init



```
root@ubuntu:~# lxd init
Would you like to use LXD clustering? (yes/no) [default=no]: no
Do you want to configure a new storage pool? (yes/no) [default=yes]:
Name of the new storage pool [default=default]:
Name of the storage backend to use (dir, lvm, zfs, ceph, btrfs) [default=zfs]:
Create a new ZFS pool? (yes/no) [default=yes]:
Would you like to use an existing empty disk or partition? (yes/no) [default=no]:
Size in GB of the new loop device (1GB minimum) [default=6GB]:
Would you like to connect to a MAAS server? (yes/no) [default=no]:
Would you like to create a new local network bridge? (yes/no) [default=yes]: no
Would you like to configure LXD to use an existing bridge or host interface?
(yes/no) [default=no]: yes
Name of the existing bridge or host interface: markuntestibridge0
Would you like LXD to be available over the network? (yes/no) [default=no]:
Would you like stale cached images to be updated automatically? (yes/no)
[default=yes]
Would you like a YAML "lxd init" preseed to be printed? (yes/no) [default=no]:
```

Note the “Name of the existing bridge or host interface: “ should be the name of the OVS bridge you created in the previous exercise.

Note the “Name of the existing bridge or host interface: “ should be the name of the OVS bridge you created in the previous exercise.

Answer:

First installed lxd:

# Sudo apt install lxd

Then run:

lxd init

And make configurations

33 TASK 2

Question:

The previous lxd init should have done the trick.. Still! For my best knowledge it creates “macvlan” style network interface for the containers → this does not work at all in this kind of setup.Thus the we use the “bridge” interface since it works.next: Either modify the default LXC profile, or create new LXC profile to:use your OVS virtual switch for the networking in as nictype: bridged.You can check the current profile via command lxc profile show default

Answer:

I created new profile file with text editor and added it to LXD:

Create profile file:

```
# nano profile
config: {}
description: ""
devices:
  eth0:
    name: eth0
    nictype: bridged
    parent: br0
    type: nic
  root:
    path: /
    pool: one
    type: disk
name: lxdprofile
used_by: []
```

add profile to LXD:

```
# lxc profile create lxdprofile
```

"Copy" the textfile to the new profile:

```
# cat lxdprofile | lxc profile edit lxdprofile
```

34 TASK 3

Question:

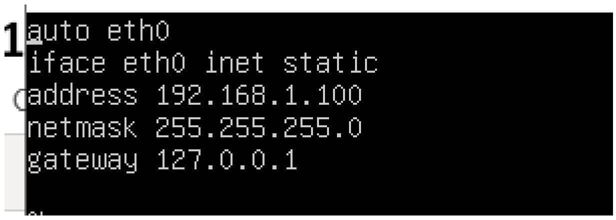
Once the LXC is properly configured, run your first container there.You can decide whatever distro to use. I used Alpine since it is rather small and has traditional network setup.For instance: lxc launch images:alpine/3.12 testalpineNote that this uses the default profile and if you set up another profile you must append -p profilename to the command.Learn to use commands:lxc listlxc exec testalpine ashAdd another container, add IP addresses for them and verify they can ping each others. (and also other parts of the network if you feel like that and your setup supports it)

Answer:

I made two containers. I used alpine distro and run it with:

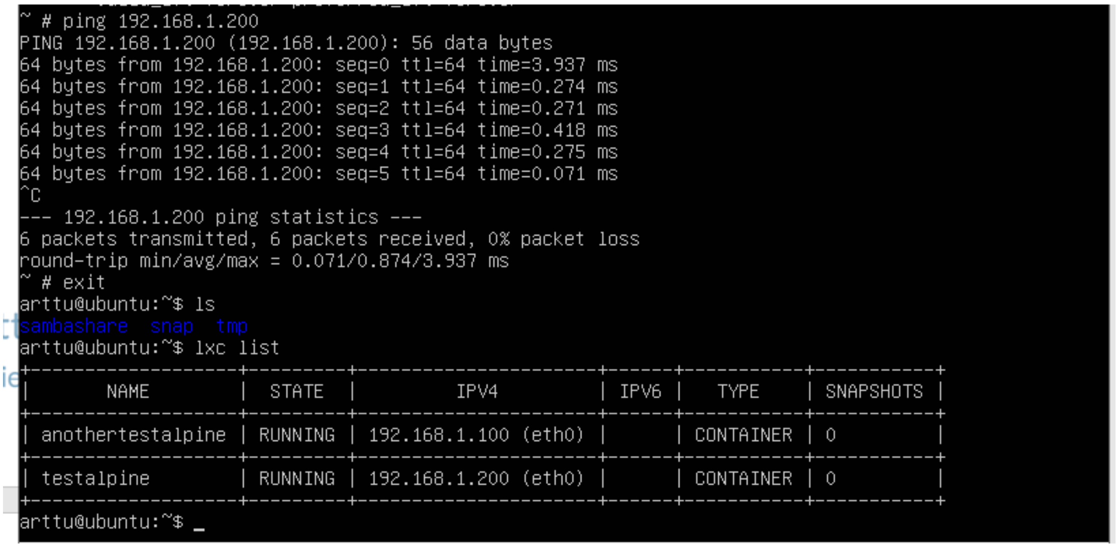
# lxc launch images:alpine/3.12 testalpine -p lxdprofile
# lxc launch images:alpine/3.12 anothertestalpine -p lxdprofile

Then added static IP addresses to both VM’s in /etc/network/interfaces and tested the connection between VM’s:



```
auto eth0
iface eth0 inet static
address 192.168.1.100
netmask 255.255.255.0
gateway 127.0.0.1
```

/etc/network/interfaces



```
~ # ping 192.168.1.200
PING 192.168.1.200 (192.168.1.200): 56 data bytes
64 bytes from 192.168.1.200: seq=0 ttl=64 time=3.937 ms
64 bytes from 192.168.1.200: seq=1 ttl=64 time=0.274 ms
64 bytes from 192.168.1.200: seq=2 ttl=64 time=0.271 ms
64 bytes from 192.168.1.200: seq=3 ttl=64 time=0.418 ms
64 bytes from 192.168.1.200: seq=4 ttl=64 time=0.275 ms
64 bytes from 192.168.1.200: seq=5 ttl=64 time=0.071 ms
^C
--- 192.168.1.200 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0.071/0.874/3.937 ms
~ # exit
arttu@ubuntu:~$ ls
sambashare  snap  tmp
arttu@ubuntu:~$ lxc list
+-------------------+---------+----------------------+------+-----------+-----------+
|       NAME        |  STATE  |         IPV4         | IPV6 |   TYPE    | SNAPSHOTS |
+-------------------+---------+----------------------+------+-----------+-----------+
| anothertestalpine | RUNNING | 192.168.1.100 (eth0) |      | CONTAINER | 0         |
+-------------------+---------+----------------------+------+-----------+-----------+
| testalpine        | RUNNING | 192.168.1.200 (eth0) |      | CONTAINER | 0         |
+-------------------+---------+----------------------+------+-----------+-----------+
arttu@ubuntu:~$ _
```

Ping between VM’s and lxc list

35 TASK 4

Question:

Finally, connect the openvswitch bridge that you created in the task2 to the Faucet. root@ubuntu:/home/student# ovs-vsctl set-controller Bridgename tcp:127.0.0.1:6653You can verify this again using the ovs-vsctl show command or from the Faucet logs. You need to modify only the /etc/faucet/faucet.yaml configurationFor this purpose you will need switch dp_id and interface numbers. They can be queried from the OVS using command:root@ubuntu:~# ovs-ofctl show <bridgename>Note that in real environments you really should carefully map the port and the container together, this case its not necessary since all the containers shall be in the same VLANThe gathered dpid: some VALUE needs the 0x in fron of the VALUE for the faucetNOTE: Apply configuration updatesroot@ubuntu:/home/student# pkill -HUP -f faucet.faucetThen verify via ovs-vsctl showthat the OVS bridge has connected state Controller "tcp:127.0.0.1:6653" is_connected: true.. and start to monitor faucet root@ubuntu:~# tail -f /var/log/faucet/faucet.log You should see that some switch has learned new mac address to be behind one port
Answer:

connect the openvswitch bridge to the Faucet:

# ovs-vsctl set-controller br0 tcp:127.0.0.1:6653

# ovs-ofctl show br0

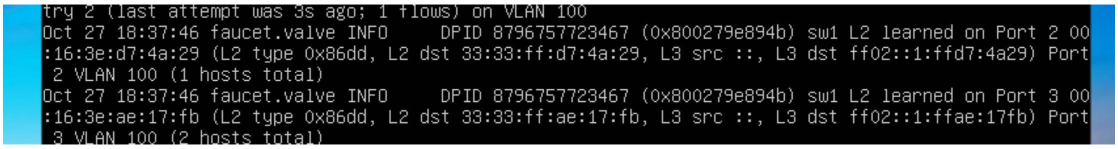
Dp id is 00000800279e894b and interfaces are 2 and 3 for containers

Added them to /etc/faucet/faucet.yaml and removed all other interfaces and switches, which were there by default

Then ran:

# pkill -HUP -f faucet.faucet

The log file shows that sw1 has learned the container mac addresses:



```
try 2 (last attempt was 3s ago; 1 flows) on VLAN 100
Oct 27 18:37:46 faucet.valve INFO     DPID 8796757723467 (0x800279e894b) sw1 L2 learned on Port 2 00
:16:3e:d7:4a:29 (L2 type 0x86dd, L2 dst 33:33:ff:d7:4a:29, L3 src ::, L3 dst ff02::1:ffd7:4a29) Port
 2 VLAN 100 (1 hosts total)
Oct 27 18:37:46 faucet.valve INFO     DPID 8796757723467 (0x800279e894b) sw1 L2 learned on Port 3 00
:16:3e:ae:17:fb (L2 type 0x86dd, L2 dst 33:33:ff:ae:17:fb, L3 src ::, L3 dst ff02::1:ffae:17fb) Port
 3 VLAN 100 (2 hosts total)
```

36 TASK 5

Done – phew, it was a setup.

Optional: Note that there is also Grafana that can be used to monitor Faucet. Check the https://docs.faucet.nz/en/latest/tutorials/first_time.html#configure-grafana

Exercise 10

Performance

Arttu Karhunen
n4924@student.jamk.fi

Exercise
Lokakuu 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Goal: Measure our network setup performance

Needed stuff: Your setup

Notes: THIS belongs to lesson 11 – You can do this before-hand already

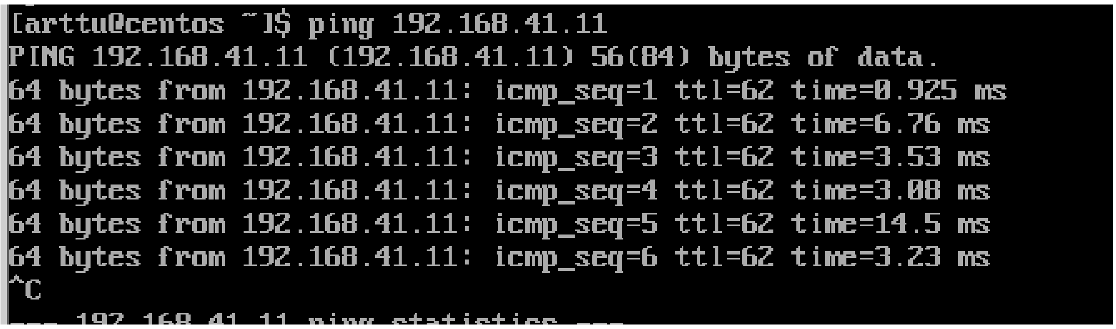
Notes2: remember to TURN on your MONITORING device that was set up in exercise 7

37 TASK 1

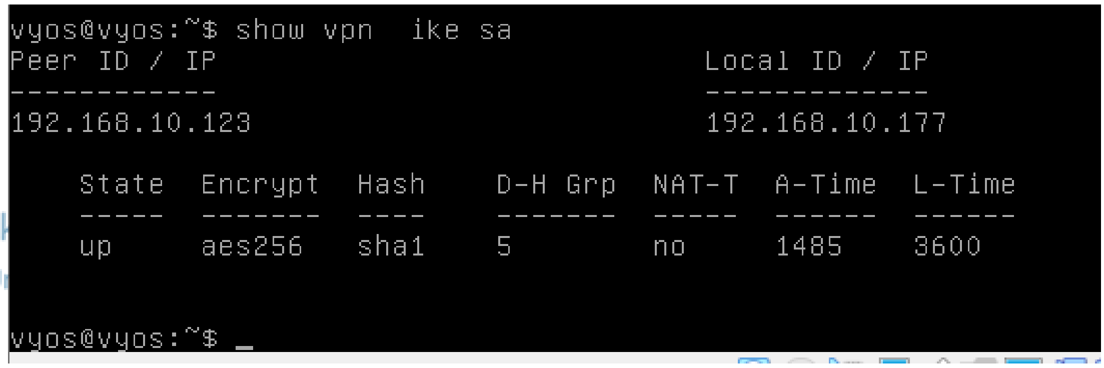
Question:

Measure the performance of the network setup created using your chosen VPN solution.

1. Verify that Linux clients behind routers can reach each others using ping and traffic goes through the VPN tunnel

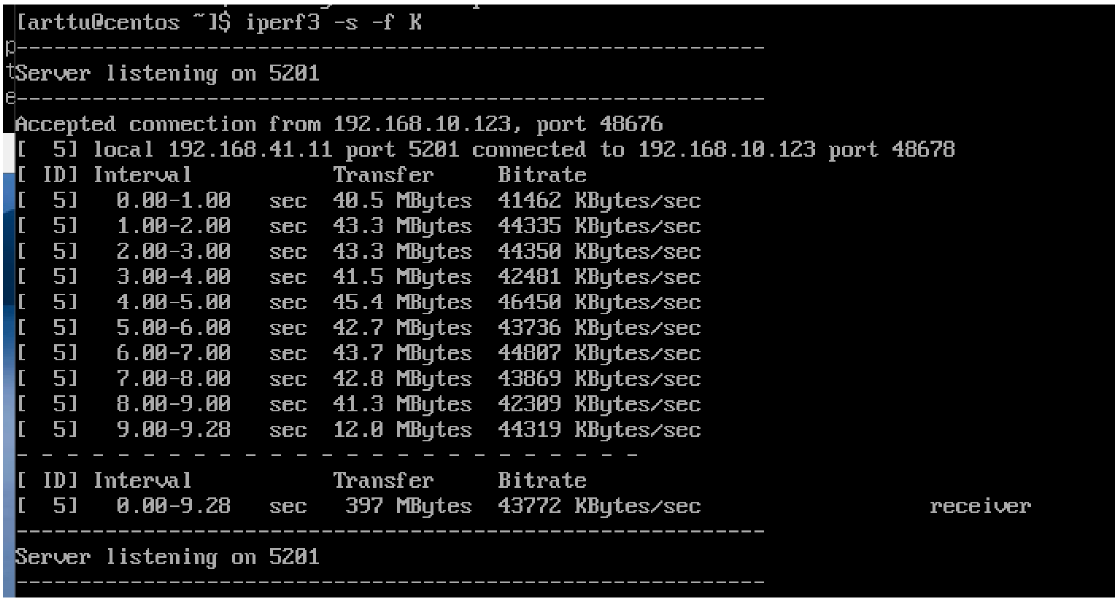


```
[arttu@centos ~]$ ping 192.168.41.11
PING 192.168.41.11 (192.168.41.11) 56(84) bytes of data.
64 bytes from 192.168.41.11: icmp_seq=1 ttl=62 time=0.925 ms
64 bytes from 192.168.41.11: icmp_seq=2 ttl=62 time=6.76 ms
64 bytes from 192.168.41.11: icmp_seq=3 ttl=62 time=3.53 ms
64 bytes from 192.168.41.11: icmp_seq=4 ttl=62 time=3.08 ms
64 bytes from 192.168.41.11: icmp_seq=5 ttl=62 time=14.5 ms
64 bytes from 192.168.41.11: icmp_seq=6 ttl=62 time=3.23 ms
^C
--- 192.168.41.11 ping statistics ---
```

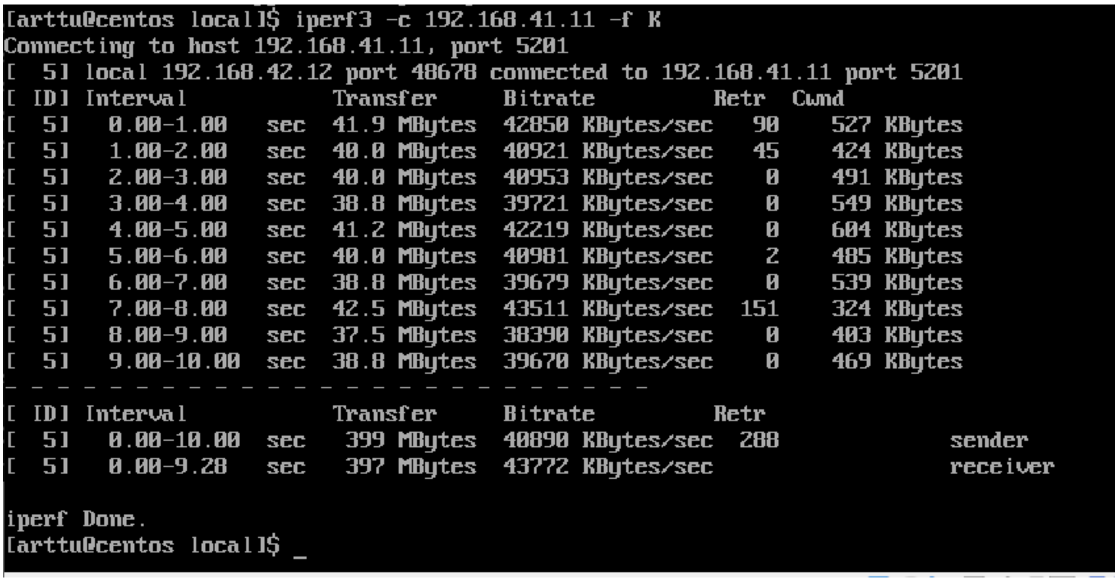


```
vyos@vyos:~$ show vpn  ike sa
Peer ID / IP                                Local ID / IP
------------                                -------------
192.168.10.123                              192.168.10.177

    State  Encrypt  Hash    D-H Grp  NAT-T  A-Time  L-Time
    -----  -------  ----    -------  -----  ------  ------
    up     aes256   sha1    5        no     1485    3600


vyos@vyos:~$ _
```

2. Use iperf3 tool to measure the TCP throughput between your devices

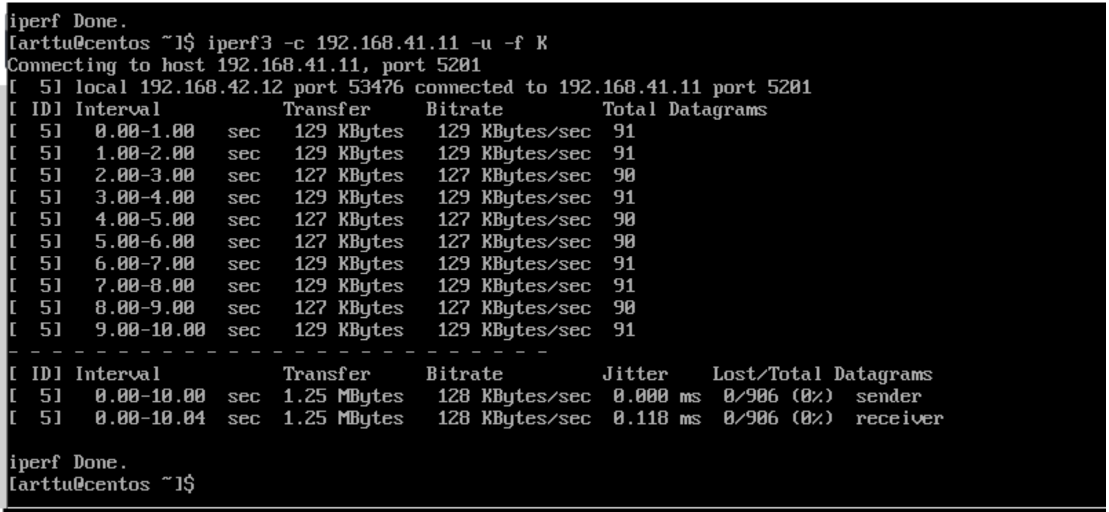


```
[arttu@centos ~]$ iperf3 -s -f K
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
Accepted connection from 192.168.10.123, port 48676
[  5] local 192.168.41.11 port 5201 connected to 192.168.10.123 port 48678
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-1.00   sec  40.5 MBytes  41462 KBytes/sec
[  5]   1.00-2.00   sec  43.3 MBytes  44335 KBytes/sec
[  5]   2.00-3.00   sec  43.3 MBytes  44350 KBytes/sec
[  5]   3.00-4.00   sec  41.5 MBytes  42481 KBytes/sec
[  5]   4.00-5.00   sec  45.4 MBytes  46450 KBytes/sec
[  5]   5.00-6.00   sec  42.7 MBytes  43736 KBytes/sec
[  5]   6.00-7.00   sec  43.7 MBytes  44807 KBytes/sec
[  5]   7.00-8.00   sec  42.8 MBytes  43869 KBytes/sec
[  5]   8.00-9.00   sec  41.3 MBytes  42309 KBytes/sec
[  5]   9.00-9.28   sec  12.0 MBytes  44319 KBytes/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-9.28   sec   397 MBytes  43772 KBytes/sec                  receiver
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
```

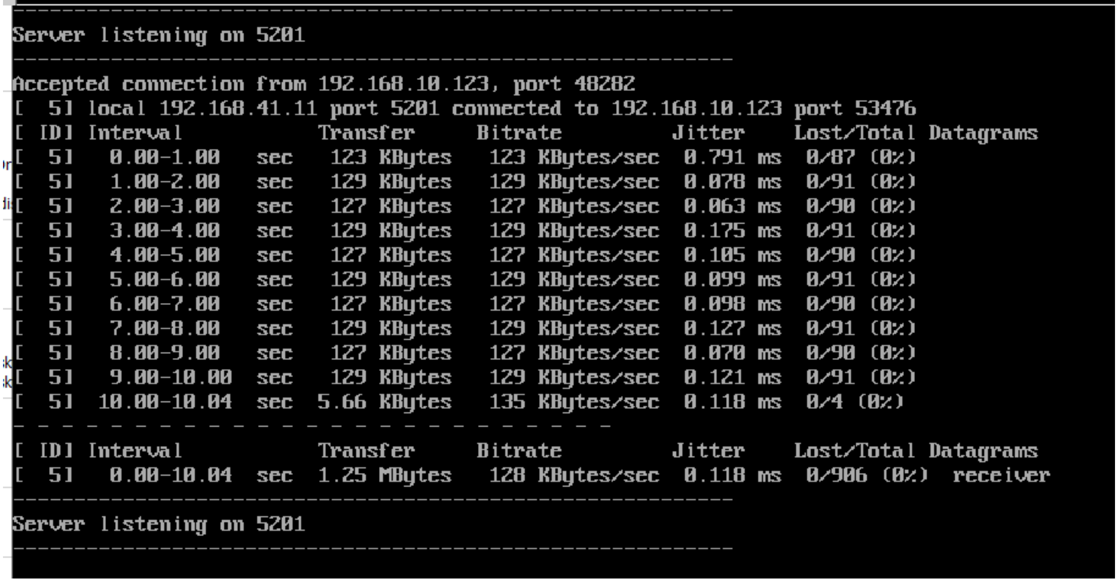


```
[arttu@centos local]$ iperf3 -c 192.168.41.11 -f K
Connecting to host 192.168.41.11, port 5201
[  5] local 192.168.42.12 port 48678 connected to 192.168.41.11 port 5201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.00   sec  41.9 MBytes  42850 KBytes/sec   90    527 KBytes
[  5]   1.00-2.00   sec  40.0 MBytes  40921 KBytes/sec   45    424 KBytes
[  5]   2.00-3.00   sec  40.0 MBytes  40953 KBytes/sec    0    491 KBytes
[  5]   3.00-4.00   sec  38.8 MBytes  39721 KBytes/sec    0    549 KBytes
[  5]   4.00-5.00   sec  41.2 MBytes  42219 KBytes/sec    0    604 KBytes
[  5]   5.00-6.00   sec  40.0 MBytes  40981 KBytes/sec    2    485 KBytes
[  5]   6.00-7.00   sec  38.8 MBytes  39679 KBytes/sec    0    539 KBytes
[  5]   7.00-8.00   sec  42.5 MBytes  43511 KBytes/sec  151    324 KBytes
[  5]   8.00-9.00   sec  37.5 MBytes  38390 KBytes/sec    0    403 KBytes
[  5]   9.00-10.00  sec  38.8 MBytes  39670 KBytes/sec    0    469 KBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Retr
[  5]   0.00-10.00  sec   399 MBytes  40890 KBytes/sec  288             sender
[  5]   0.00-9.28   sec   397 MBytes  43772 KBytes/sec                  receiver

iperf Done.
[arttu@centos local]$ _
```

2. Use iperf3 tool to measure the UDP throughput between your devices

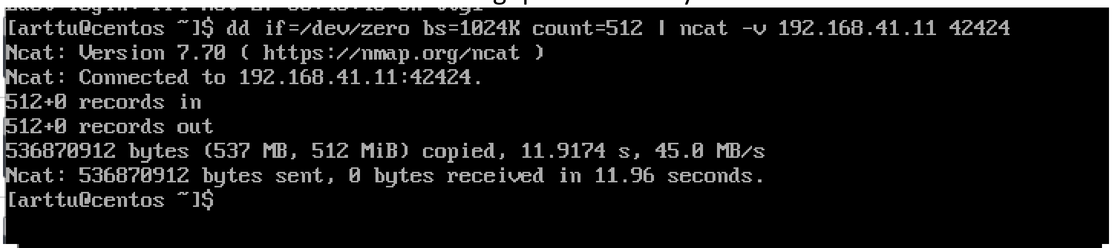


```
iperf Done.
[arttu@centos ~]$ iperf3 -c 192.168.41.11 -u -f K
Connecting to host 192.168.41.11, port 5201
[  5] local 192.168.42.12 port 53476 connected to 192.168.41.11 port 5201
[ ID] Interval           Transfer     Bitrate         Total Datagrams
[  5]   0.00-1.00   sec   129 KBytes   129 KBytes/sec  91
[  5]   1.00-2.00   sec   129 KBytes   129 KBytes/sec  91
[  5]   2.00-3.00   sec   127 KBytes   127 KBytes/sec  90
[  5]   3.00-4.00   sec   129 KBytes   129 KBytes/sec  91
[  5]   4.00-5.00   sec   127 KBytes   127 KBytes/sec  90
[  5]   5.00-6.00   sec   127 KBytes   127 KBytes/sec  90
[  5]   6.00-7.00   sec   129 KBytes   129 KBytes/sec  91
[  5]   7.00-8.00   sec   129 KBytes   129 KBytes/sec  91
[  5]   8.00-9.00   sec   127 KBytes   127 KBytes/sec  90
[  5]   9.00-10.00  sec   129 KBytes   129 KBytes/sec  91
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datagrams
[  5]   0.00-10.00  sec  1.25 MBytes   128 KBytes/sec  0.000 ms  0/906 (0%)  sender
[  5]   0.00-10.04  sec  1.25 MBytes   128 KBytes/sec  0.118 ms  0/906 (0%)  receiver

iperf Done.
[arttu@centos ~]$
```

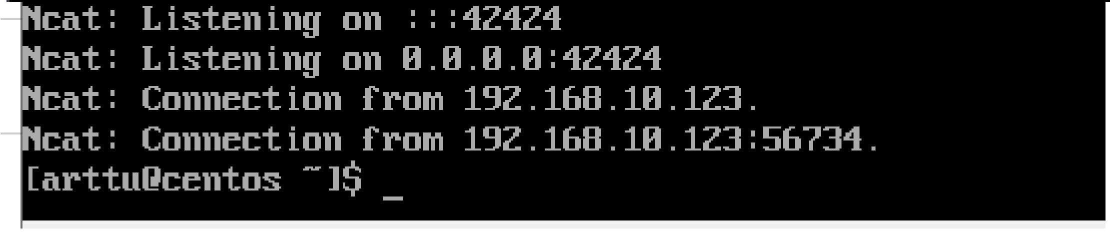


```
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
Accepted connection from 192.168.10.123, port 48282
[  5] local 192.168.41.11 port 5201 connected to 192.168.10.123 port 53476
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datagrams
[  5]   0.00-1.00   sec   123 KBytes   123 KBytes/sec  0.791 ms  0/87 (0%)
[  5]   1.00-2.00   sec   129 KBytes   129 KBytes/sec  0.078 ms  0/91 (0%)
[  5]   2.00-3.00   sec   127 KBytes   127 KBytes/sec  0.063 ms  0/90 (0%)
[  5]   3.00-4.00   sec   129 KBytes   129 KBytes/sec  0.175 ms  0/91 (0%)
[  5]   4.00-5.00   sec   127 KBytes   127 KBytes/sec  0.105 ms  0/90 (0%)
[  5]   5.00-6.00   sec   129 KBytes   129 KBytes/sec  0.099 ms  0/91 (0%)
[  5]   6.00-7.00   sec   127 KBytes   127 KBytes/sec  0.098 ms  0/90 (0%)
[  5]   7.00-8.00   sec   129 KBytes   129 KBytes/sec  0.127 ms  0/91 (0%)
[  5]   8.00-9.00   sec   127 KBytes   127 KBytes/sec  0.070 ms  0/90 (0%)
[  5]   9.00-10.00  sec   129 KBytes   129 KBytes/sec  0.121 ms  0/91 (0%)
[  5]  10.00-10.04  sec  5.66 KBytes   135 KBytes/sec  0.118 ms  0/4 (0%)
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datagrams
[  5]   0.00-10.04  sec  1.25 MBytes   128 KBytes/sec  0.118 ms  0/906 (0%)  receiver
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
```

3. Use netcat tool to measure the TCP throughput between your devices

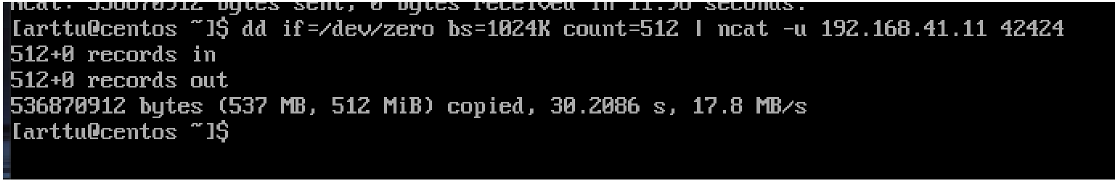


```
[arttu@centos ~]$ dd if=/dev/zero bs=1024K count=512 | ncat -v 192.168.41.11 42424
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 192.168.41.11:42424.
512+0 records in
512+0 records out
536870912 bytes (537 MB, 512 MiB) copied, 11.9174 s, 45.0 MB/s
Ncat: 536870912 bytes sent, 0 bytes received in 11.96 seconds.
[arttu@centos ~]$
```



```
Ncat: Listening on :::42424
Ncat: Listening on 0.0.0.0:42424
Ncat: Connection from 192.168.10.123.
Ncat: Connection from 192.168.10.123:56734.
[arttu@centos ~]$ _
```

4. Use netcat tool to measure the UDP throughput between your devices



```
[arttu@centos ~]$ dd if=/dev/zero bs=1024K count=512 | ncat -u 192.168.41.11 42424
512+0 records in
512+0 records out
536870912 bytes (537 MB, 512 MiB) copied, 30.2086 s, 17.8 MB/s
[arttu@centos ~]$
```

5. Evaluate the differences in results between netcat and iperf3 tools. Goal is to find whether some tool does not give correct answers.

TCP traffic seems qiute same with both tools. 43.7MB/s with iperf3 and 45,0MB/cd/s with natcat. In UDP traffic iperf shows much smaller speed because it only sends 128Kbytes in 1 second periods, so speed can't be more than 128KB/s. Netcat shows UDP speed up to 17.8MB/s.

TIPS for 4 and 5: Netcat is cool tool, on the one machine use: nc -v -n -l -p 42424 >/dev/null on the second machine generate traffic to the target using: dd if=/dev/zero bs=1024K count=512 | nc -v IP_TOISELLE_KONEELLE 42424 Remember that netcat uses also UDP via -u flag. Listen using: nc -n -l -u -p 42424 > /dev/null

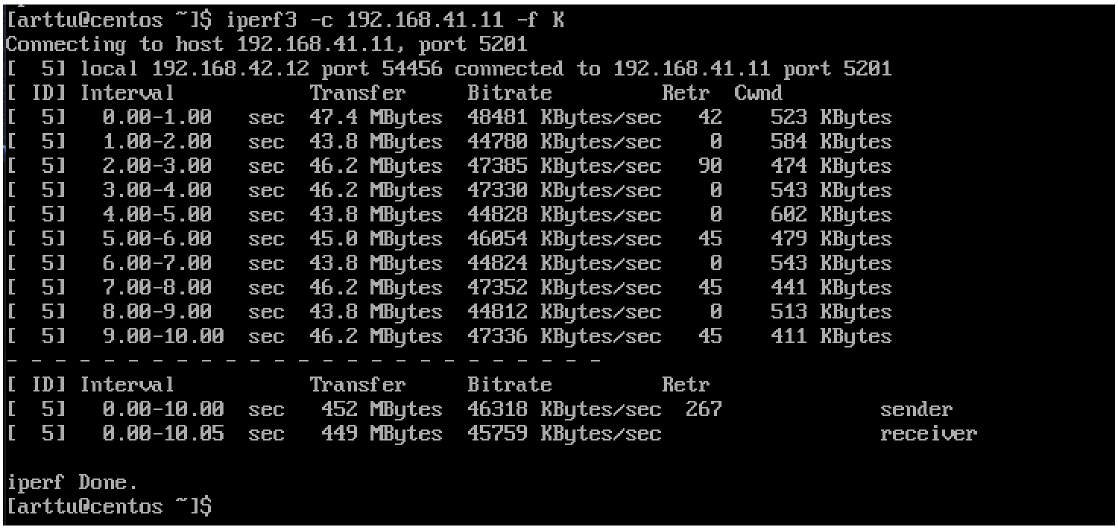
and generate traffic dd if=/dev/zero bs=1024K count=512 | nc -u IP_TOISELLE_KONEELLE 42424
Pro tip: Use bwm-ng to monitor network traffic as well in one machine
cont next page.

38 TASK 2:

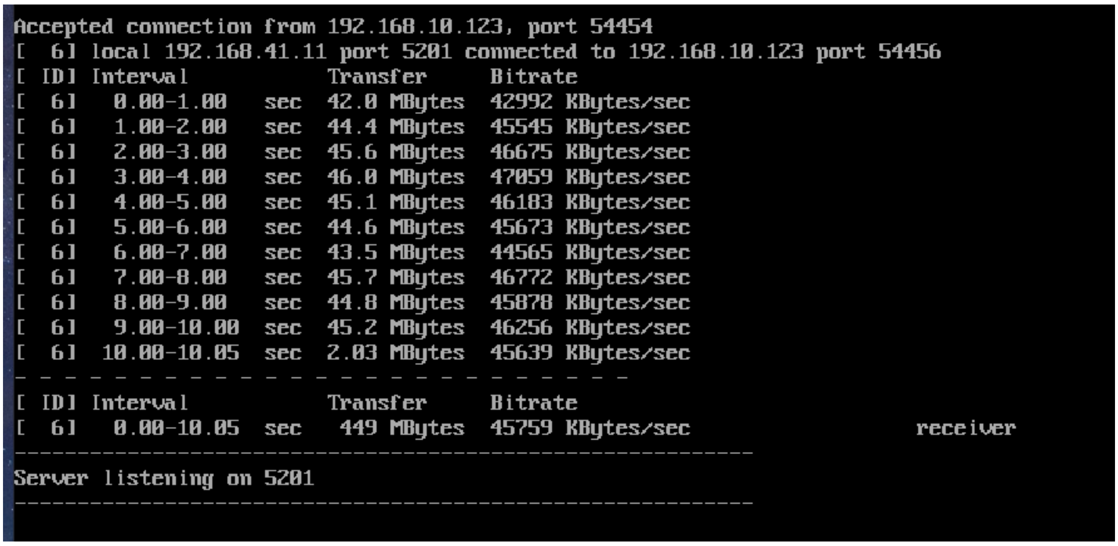
Disable VPN tunneling (no need to remove any configuration, just use disable for e.g. Wireguard) if necessary and/or use just insert static routes to the VyOS devices e.g. (oh.. please use the correct next-hops in your network) Vyos configs. e.g.:...interfaces { wireguard wg1 {disable... protocols { static { route 192.168.2.0/24 { next-hop 192.168.42.389 { } }Verify that traffic does not use VPN tunneling. Repeat measurements from the

TASK 1. So: do the 2,3,4 and 5 sections from the task 1: Measure using iperf3 and netcat. Idea is that we try to illustrate how VPN affects the bandwidth. Did you notice any differences between VPN and non-VPN solutions?

TCP with ipefr3

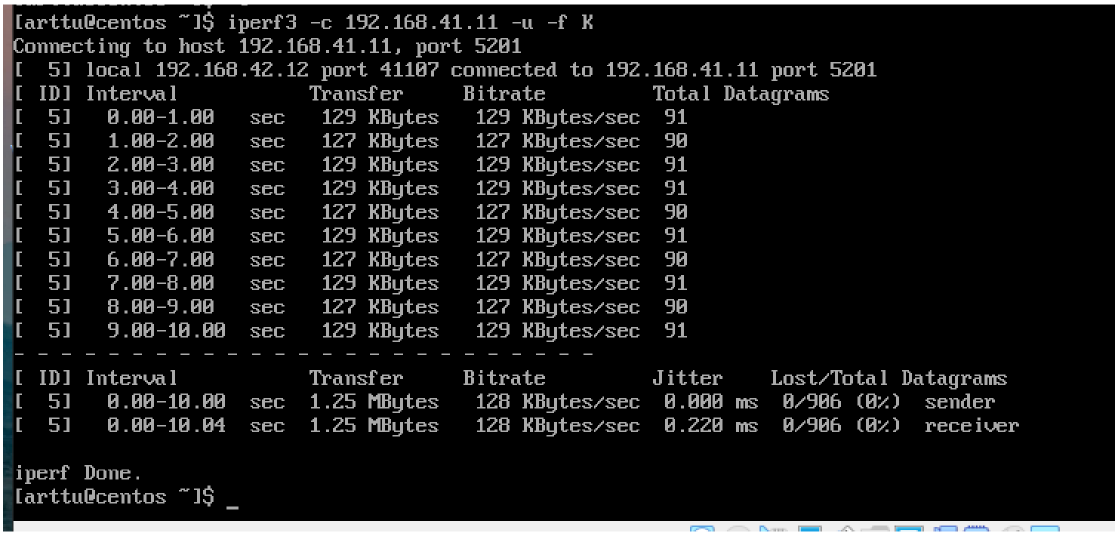


```
[arttu@centos ~]$ iperf3 -c 192.168.41.11 -f K
Connecting to host 192.168.41.11, port 5201
[  5] local 192.168.42.12 port 54456 connected to 192.168.41.11 port 5201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.00   sec  47.4 MBytes  48481 KBytes/sec   42    523 KBytes
[  5]   1.00-2.00   sec  43.8 MBytes  44780 KBytes/sec    0    584 KBytes
[  5]   2.00-3.00   sec  46.2 MBytes  47385 KBytes/sec   90    474 KBytes
[  5]   3.00-4.00   sec  46.2 MBytes  47330 KBytes/sec    0    543 KBytes
[  5]   4.00-5.00   sec  43.8 MBytes  44828 KBytes/sec    0    602 KBytes
[  5]   5.00-6.00   sec  45.0 MBytes  46054 KBytes/sec   45    479 KBytes
[  5]   6.00-7.00   sec  43.8 MBytes  44824 KBytes/sec    0    543 KBytes
[  5]   7.00-8.00   sec  46.2 MBytes  47352 KBytes/sec   45    441 KBytes
[  5]   8.00-9.00   sec  43.8 MBytes  44812 KBytes/sec    0    513 KBytes
[  5]   9.00-10.00  sec  46.2 MBytes  47336 KBytes/sec   45    411 KBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Retr
[  5]   0.00-10.00  sec   452 MBytes  46318 KBytes/sec  267             sender
[  5]   0.00-10.05  sec   449 MBytes  45759 KBytes/sec                  receiver

iperf Done.
[arttu@centos ~]$
```

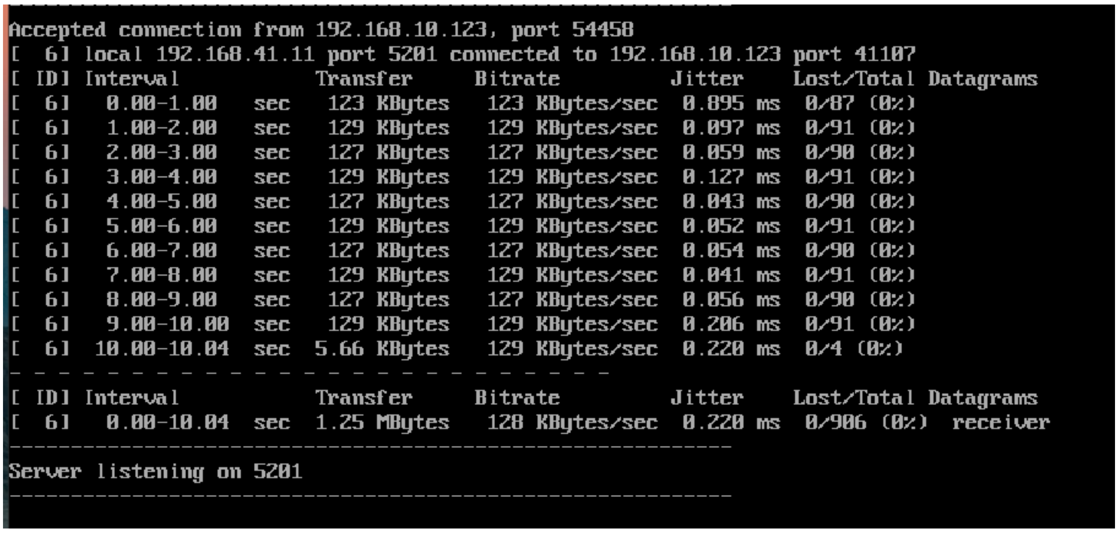


```
Accepted connection from 192.168.10.123, port 54454
[  6] local 192.168.41.11 port 5201 connected to 192.168.10.123 port 54456
[ ID] Interval           Transfer     Bitrate
[  6]   0.00-1.00   sec  42.0 MBytes  42992 KBytes/sec
[  6]   1.00-2.00   sec  44.4 MBytes  45545 KBytes/sec
[  6]   2.00-3.00   sec  45.6 MBytes  46675 KBytes/sec
[  6]   3.00-4.00   sec  46.0 MBytes  47059 KBytes/sec
[  6]   4.00-5.00   sec  45.1 MBytes  46183 KBytes/sec
[  6]   5.00-6.00   sec  44.6 MBytes  45673 KBytes/sec
[  6]   6.00-7.00   sec  43.5 MBytes  44565 KBytes/sec
[  6]   7.00-8.00   sec  45.7 MBytes  46772 KBytes/sec
[  6]   8.00-9.00   sec  44.8 MBytes  45878 KBytes/sec
[  6]   9.00-10.00  sec  45.2 MBytes  46256 KBytes/sec
[  6]  10.00-10.05  sec  2.03 MBytes  45639 KBytes/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate
[  6]   0.00-10.05  sec   449 MBytes  45759 KBytes/sec                  receiver
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
```

UDP with iperf3:

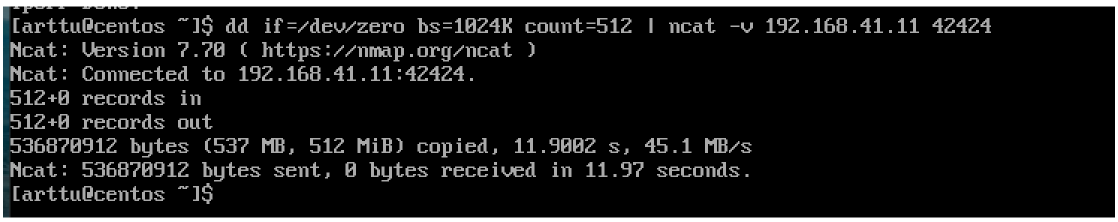


```
[arttu@centos ~]$ iperf3 -c 192.168.41.11 -u -f K
Connecting to host 192.168.41.11, port 5201
[  5] local 192.168.42.12 port 41107 connected to 192.168.41.11 port 5201
[ ID] Interval           Transfer     Bitrate         Total Datagrams
[  5]   0.00-1.00   sec   129 KBytes   129 KBytes/sec  91
[  5]   1.00-2.00   sec   127 KBytes   127 KBytes/sec  90
[  5]   2.00-3.00   sec   129 KBytes   129 KBytes/sec  91
[  5]   3.00-4.00   sec   129 KBytes   129 KBytes/sec  91
[  5]   4.00-5.00   sec   127 KBytes   127 KBytes/sec  90
[  5]   5.00-6.00   sec   129 KBytes   129 KBytes/sec  91
[  5]   6.00-7.00   sec   127 KBytes   127 KBytes/sec  90
[  5]   7.00-8.00   sec   129 KBytes   129 KBytes/sec  91
[  5]   8.00-9.00   sec   127 KBytes   127 KBytes/sec  90
[  5]   9.00-10.00  sec   129 KBytes   129 KBytes/sec  91
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datagrams
[  5]   0.00-10.00  sec  1.25 MBytes   128 KBytes/sec  0.000 ms  0/906 (0%)  sender
[  5]   0.00-10.04  sec  1.25 MBytes   128 KBytes/sec  0.220 ms  0/906 (0%)  receiver

iperf Done.
[arttu@centos ~]$ _
```



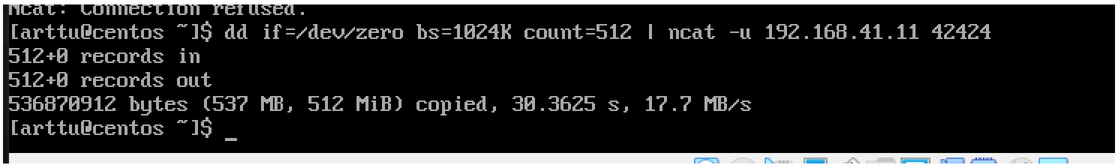
```
-----------------------------------------------------------
Accepted connection from 192.168.10.123, port 54458
[  6] local 192.168.41.11 port 5201 connected to 192.168.10.123 port 41107
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datagrams
[  6]   0.00-1.00   sec   123 KBytes   123 KBytes/sec  0.895 ms  0/87 (0%)
[  6]   1.00-2.00   sec   129 KBytes   129 KBytes/sec  0.097 ms  0/91 (0%)
[  6]   2.00-3.00   sec   127 KBytes   127 KBytes/sec  0.059 ms  0/90 (0%)
[  6]   3.00-4.00   sec   129 KBytes   129 KBytes/sec  0.127 ms  0/91 (0%)
[  6]   4.00-5.00   sec   127 KBytes   127 KBytes/sec  0.043 ms  0/90 (0%)
[  6]   5.00-6.00   sec   129 KBytes   129 KBytes/sec  0.052 ms  0/91 (0%)
[  6]   6.00-7.00   sec   127 KBytes   127 KBytes/sec  0.054 ms  0/90 (0%)
[  6]   7.00-8.00   sec   129 KBytes   129 KBytes/sec  0.041 ms  0/91 (0%)
[  6]   8.00-9.00   sec   127 KBytes   127 KBytes/sec  0.056 ms  0/90 (0%)
[  6]   9.00-10.00  sec   129 KBytes   129 KBytes/sec  0.206 ms  0/91 (0%)
[  6]  10.00-10.04  sec  5.66 KBytes   129 KBytes/sec  0.220 ms  0/4 (0%)
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datagrams
[  6]   0.00-10.04  sec  1.25 MBytes   128 KBytes/sec  0.220 ms  0/906 (0%)  receiver
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
```

TCP with netcat:



```
iperf Done.
[arttu@centos ~]$ dd if=/dev/zero bs=1024K count=512 | ncat -v 192.168.41.11 42424
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to 192.168.41.11:42424.
512+0 records in
512+0 records out
536870912 bytes (537 MB, 512 MiB) copied, 11.9002 s, 45.1 MB/s
Ncat: 536870912 bytes sent, 0 bytes received in 11.97 seconds.
[arttu@centos ~]$
```

UDP with netcat:



```
Ncat: Connection refused.
[arttu@centos ~]$ dd if=/dev/zero bs=1024K count=512 | ncat -u 192.168.41.11 42424
512+0 records in
512+0 records out
536870912 bytes (537 MB, 512 MiB) copied, 30.3625 s, 17.7 MB/s
[arttu@centos ~]$ _
```

Conclusion:

With these measurements there seems to be no significant difference between VPN and non-VPN connection. Only diiference was in iperf TCP traffic was 43MB/s vs 45MB/s which is not a very big difference.

39 TASK 3:

Did you notice these tests in your monitoring setup you set up in the ex7 ?

I did not have such monitoring tools configured to my nagios which could have showed bandwith etc.