IT Technology
Networking Assignments

Author
Per Dahlstrøm
pda@ucl.dk

Table of Contents

Hand in requirements:

All Hand ins must be done:

- On PeerGrade or on UCL LMS.
- Hand in only one .pdf file!
- on time!

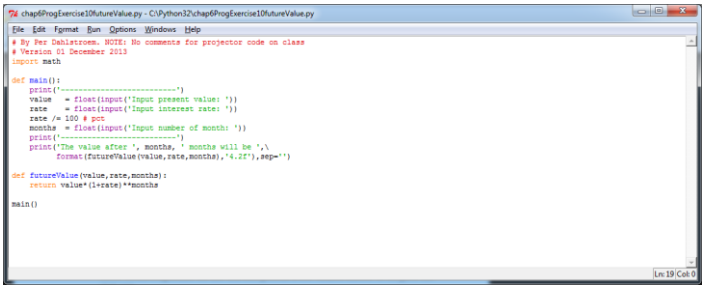
The .pdf file must be named: assXX your_first_name.pdf. Example: ass11 Per.pdf

All Hand ins must adhere to:

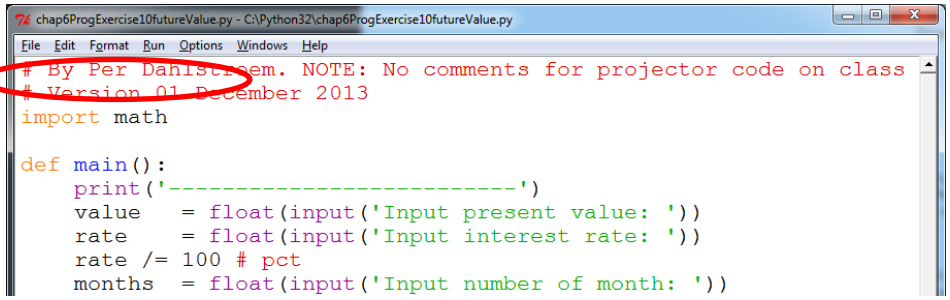
1. Use the stipulated documentation template.

2. Every screen shot must have 2 to 5 lines of explanation. Screen shots must be easily legible. The text in the shots must as a minimum be the same or correspond to the same size font as in the rest of the documentation. Every letter and number must be clearly legible when the page is displayed at an A4 paper corresponding size.

   NOT ACCETABLE:



   ACCETABLE:



3. Vital information in screen shots must be highlighted. E.g. by means of encircling as shown above, and the highlighted item must be explained in max 2 lines.

4. The author(s) name(s) must be specified in the file on the a cover page.

5. Pages must be numbered sequentially.

6. The exercise or item number convention in each assignment must be followed. I.e. if an assignment consists of e.g. sub questions 1, 2, 4, 6, and 8. Then the answers must be numbered likewise.

7. No copying from the internet is allowed. Describe in own words.

8. CLI commands and CLI output and configurations must be in font: Courier New, size 11 or 12.
   Example:

```
per@ubuntu:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data
From 192.222.10.4 icmp_seq=1 Destination Host Unreachable
From 192.222.10.4 icmp_seq=2 Destination Host Unreachable
```

Requirements in the assignments where program code is to be hand in:

1. Screen shot proof of execution with 2 to 5 line explanation to each screenshot. It must be a shot that shows the output from the programme and demonstrate both the correct execution of the programme and also situations where an error message to the user is produced.
   If the programme produces multiple results, a reasonable number of screen shots must be shown to prove the full functioning of the programme.

2. Handing in of Python code with syntax errors will not be accepted.
   You must spend the necessary time to find and correct syntax errors. This is a crucial activity in order to become a proficient programmer. In the beginning it is very time consuming, and only with practice, debugging time will be minimized.

3. Complex code snippets MUST be accompanied by a brief explanations.

4. Programs without comments will not be accepted. E.g.
   `# The cars "miles per gallon" is calculated`

5. Code must be copy pasted into the hand in and not be pasted in as a screen shot picture. Code must and will consequently be on white background.

6. Program code must be listed in color-coded format from e.g. Notepad++.
   The code font must be: `Courier New, size 10` and syntactically correctly indented.

7. It will not be accepted to have long lines that are auto wrapped. A long line must be logically split into easy readable multiline. Code must be show correctly indented. Normally landscape orientation of pages is the best solution to avoid auto wrapping and maintain the Python formatting when copied to e.g. Word.

   The example here below shows how the print statement can be split deliberately by the "\" sign:

   ACCEPTABLE:

```
print('The cars Miles-per-Gallon is: ', miles, '/', \
            gallons, ' = ', format(mpg,'.2f'), sep='')
```

NOT ACCEPTABLE:

```
print('The cars Miles-per-Gallon is: ', miles, '/', gallons, ' = ',
format(mpg,'.2f'), sep='')
```

Network troubleshooting

Please consult this GitLab repository for troubleshooting.

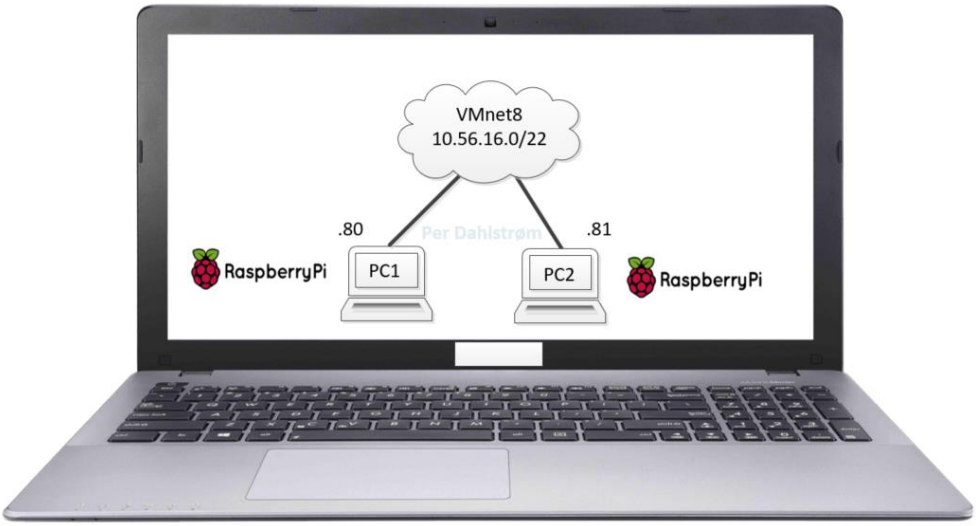
https://gitlab.com/PerPer/networking/blob/master/Trouble%20shooting/Network_Troubleshooting_Per_Dahlstroem_UCL.md

Assignment 1 Raspberry VM, IP and MAC addresses and ARP table.

Part1.

Learning goals.

- Install a Raspberry Pi Buster Operating system on a Virtual Machine VM in VMWW.
- Use ping to verify connectivity between network devices.
- Inspect the ARP table on a Linux box, here a Raspberry.
- Use Wireshark to confirm IP and MAC addresses.



Tasks.

1. Draw a network diagram with IP addresses and MAC addresses listed.
   Please note that as MAC addresses will only be learned later in this assignment, these will have to be added to the drawing when they have been learned.

2. Install a Raspberry Pi Buster Operating system on a Virtual Machine VM in VMWW.
   Connect it to VMnet8 set to NAT to give the Raspberry Pi Buster VM internet access.

3. Name the VM in VMWW: Raspberry_Buster_Base.

4. Install the networking software:

   - Before installing software on Linux do:
     - update (sudo apt update)
     - upgrade (sudo apt upgrade)

   - Install networking software from Linux repositories:

     - **wireshark (Ethernet capturing and monitoring GUI software.)**
     - **tcpdump (app to capture live TCP/IP packets on a network interface)**
     - **putty (Terminal program.)**
     - **net-tools arp, hostname, ifconfig, netstat, route).**
     - **bridge-utils (Utility to create and manage bridge devices.)**
     - **iproute2 (ip commands like: ip route)**

- **curl (curl is a command line tool to transfer data to or from a server.)**
- **ufw (Uncomplicated Firewall is a program for managing a netfilter firewall)**

5. Install nmcli Network Manager and uninstall dhcpcd on the the Raspberry_Buster_Base.

6. Clone the Raspberry_Buster_Base to create PC1 and PC2 and configure PC1 and PC2 with static IPs as shown in the illustration above.

7. Use ping to verify connectivity between network devices PC1 and PC2.
   Run Wireshark on PC1.
   Ping PC2 and the router in turn.
   Use the filter icmp as Wireshark Display filter.
   Find the source and destination IP addresses in the request packets and find the corresponding source and destination MAC addresses.
   Find the source and destination IP addresses in the reply packets and find the corresponding source and destination MAC addresses.

8. Compare the IP and MAC addresses found in Wireshark with the IP and MAC addresses found by the command

   $ ip addr

   Note that “inet” means IPV4 in the output from the ip addr command.

9. Draw up manually he ARP table from the findings in the items above. The ARP table maps IP addresses to MAC addresses, i.e. ARP resolves IPs to MAC addresses on a networking device. Here on the Raspberry Pi as a networking device.

Hand written ARP table layout suggestion:

Device name	IP address	MAC address
Gate Way or Router		
PC1		
PC2		

10. Use the ip neigh Linux command to inspect the ARP table on the Linux box PC1 and then on PC2.

    I.e. use the command:

    $ ip neigh

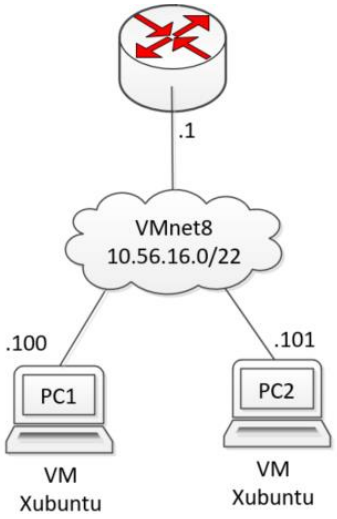
    or the old command:

    $ arp

    Comment on the output from these commands compared to the “hand written“ ARP table.

Hand in: Document all of the above items in a hand in.

Assignment 2 VMnet8, Network diagrams, Linux software, static IPs and traffic monitoring.



Introduction

The assignment will train the student in:

- setting up a network with two Linux Xubuntu hosts and internet access in VM Ware Workstation VMWW. The hosts will be interconnected and have internet access via one of VMWWs so called VMnets, i.e. VMnet8.
- drawing a network diagram.
- installing applications or programs or software from Linux repositories "on the internet" for configuring and troubleshooting networking on Linux devices, like a Xubuntu Virtual Machine. I.e. equipping a Linux Xubuntu base machine.
- configuring ethernet interfaces on Xubuntu Linux computers or devices.
- basic ethernet traffic monitoring in Wireshark.

Learning goals

The student can:

- Set up a VMnet8 in VMWare Workstation using Virtual Network Editor.
- Update and Upgrade a Linux OS.
- Pull and install software or applications from a Linux repository.
- Set static IP address on Linux hosts.
- Use PING to check connectivity between two hosts.
- Use Wireshark to monitor traffic between two hosts.
- Explain what a networking interface is.

Hand in

Hand in an assignment report that shows/explains:

1. An introduction.
2. A network diagram with IP addresses. (Layer 3 network diagram.)
3. How to set up VMnet8 in the Virtual Network Editor.
4. How to set static IP addresses on Xubuntu Linux hosts.
5. How to use PING to check connectivity between two hosts.

6. What the ping program is.
7. What a networking interface is.
8. How to use Wireshark to monitor traffic between two hosts.
9. How to update and upgrade a Linux OS.
10. What a Linux repository is and how to pull and install software from it.
11. Challenge: What a broadcast ping is and who will reply to it.
12. Conclusion on the learning goals.

Sources

1. See Weekly plan

Assignment 3 VMware Workstation and VM installation.

Introduction

This assignment is using the VM Ware Workstation hardware and network virtualisation management tool. From now on VM Ware Workstation is referred to as: VMWW.

Learning goals

After this assignment the student can:

- Install a hardware and network virtualisation management tool on a Lap Top host computer.
- Install a Linux host on the hardware and network emulation management tool.
- Superficially explain what a hardware emulator or Hypervisor is.

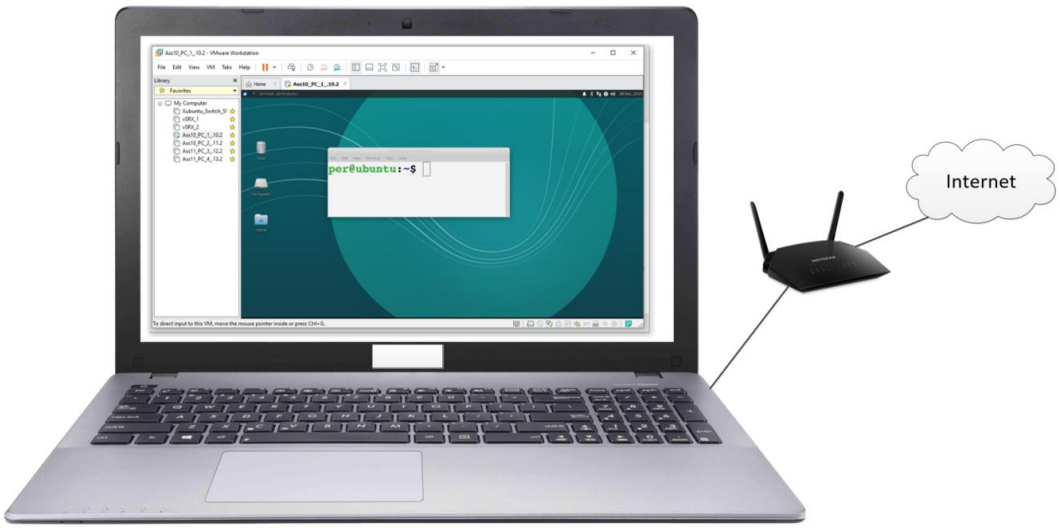
Tasks:

- Install VM Ware Workstation (VMWW) on a Lap Top host computer.
- Install a Xubuntu Linux Virtual Machine (VM) in VMWW.
- Connect the Linux VM to VMnet8 in VMWW.
    - VMnet8 will share the Lab Top hosts internet connection which means that the Linux VM should now have internet access via VMnet8.
- Run the default internet browser on Xubuntu to verify that this Xubuntu

Hand in

Hand in a lab report with:

1. A screen shot that shows that VMWW has been successfully installed.
2. Screen shots and an explanation on how to install a Xubuntu Linux computer Virtual Machine (VM) in VMWW.
3. A screen shot that shows that the installed VM has been successfully connected to VMnet8 and thus has internet access, i.e. a screen shot of a browser web page from the internet.
4. Explain in your own words in maximum 3 lines what a Hypervisor is.



Xubuntu VM in VMWW on a Laptop with internet connection.

Assignment 4 The Switch and the ARP and the tcpdump

Introduction

Above is shown an inexpensive simple layer 2, 4 port switch. Please note that the Switch and the ARP are actually not related topics. It is just convenient to talk about both in this assignment.

In this assignment is used the VMWare Workstation hardware and network emulation management tool.

Learning goals

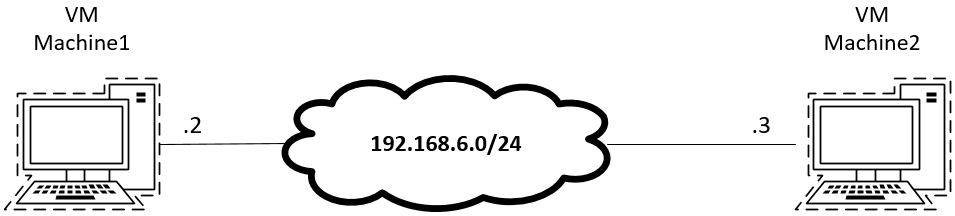
The student can:

- Set up a small network in VMWare Workstation including a stand alone Switch.
- Describe a Layer 2 switch. E.g. what is:
  - The functionality of a Layer 2 switch
  - Switch port
  - SAT - Source Address Table.
- Describe a hosts MAC table - Media Access Control table.
- Explain what the mechanics of ARP are.
- Use tcpdump to monitor traffic on interfaces and document ARP request/reply traffic.
- Optional/Challenge:
  - Describe other relevant Linux networking commands used in the context of this assignment.
  - Use Wireshark to display interesting traffic in the context of this assignment.
  - Make a Linux HUB. Prove that it works.

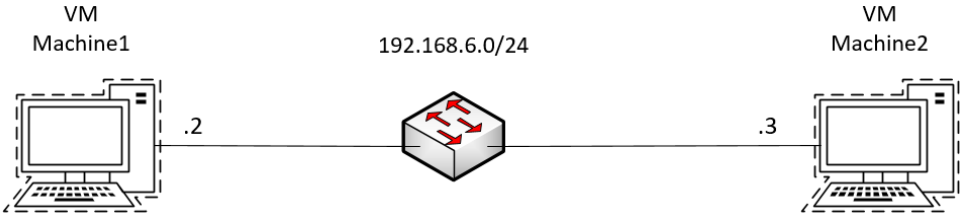
Topology

The network used to test the switch functionality is as follows:

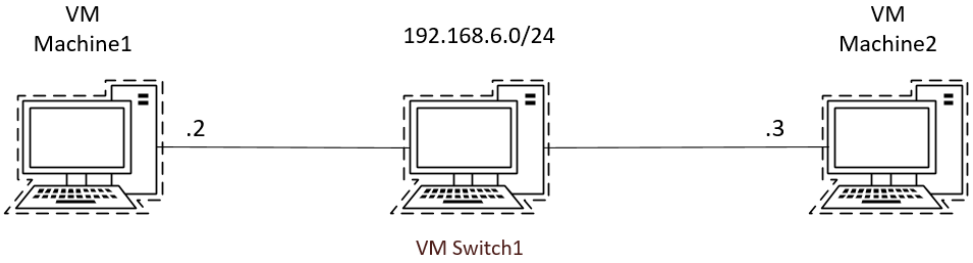
In principle, Machine 1 and 2 are interconnected on network 192.168.6.0 as shown here:



In this assignment a "physical" switch will constitute the intestines in the cloud:



The "physical" switch will be constituted by a Linux VM, VM Switch 1, set up to do switching:



To manage the switch efficiently some software must be installed on the machine:

- sudo apt install brctl or sudo apt install bridge-utils
- sudo apt install ifupdown

The easiest is to initially have VMnet8 attached before setting up the switch, and downloading the required software.

Hand in a lab report that shows/explains:

1. The Topology with one switch VM Switch 1 and the two hosts.
   Place relevant labels on the Topology. Remember to show what Workstation nets are used.
   It is also advisable to put the interface names in the diagram.

2. What brct1 is and how to configure the switch for switching/bridging.
   Commands
   a. sudo brctl showmacs br0
   b. brctl show
   c. sudo brctl stp br0 off (Switch STP off to not have STP traffic blurring the traffic)
   d. sudo brctl stp br0 on

3. How to set Ip addresses and Subnet masks on the two computers. Do not set a default gateway as there is no default gateway to receive traffic.

4. A TCPdump that shows a ping from one computer to the other.
   Commands:
   a. tcpdump –D
   b. tcpdump –i <interface name>
   c. tcpdump –n –i <interface name> (To only show IP addresses)

5. The host computers ARP tables with a maximum of 4 line explanation of the content of the ARP table. A screen shot that proves that the right MAC addresses are listed in the ARP tables. Possibly use the arp delete command and use tcpdump to show the arp requests.
   Commands
   a. man arp (Exit the manual by typing "q")
   b. arp
   c. arp –a
   d. arp –d <IP address> (Delete an ARP table entry)

6. The SAT table in the switch. Show the command to see the table. Explain what is in the table and how the table was populated.
   Commands:
   a. sudo brctl showmacs br0
   b. ifdown (Turn off an interface or bridge)
   c. ifup (Turn on an interface or bridge)

7. Extra.
   Add one or two more hosts and prove that the Switch
   a. floods out traffic as expected.
   b. separates traffic as expected.
   c. Make and test a Linux HUB. Prove that it works.
      Command:
      brctl setageing <bridgename> 0

Tips and trouble shooting

Sources

1. Internet sources

Assignment 5 The switch and STP

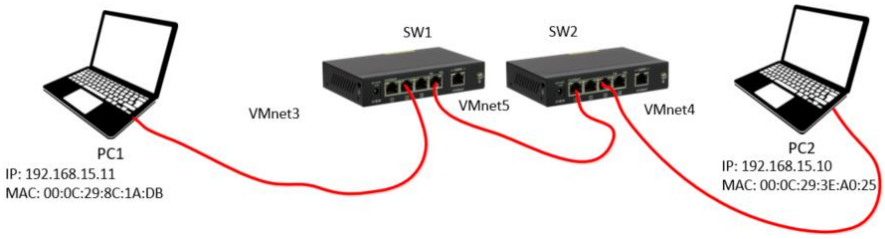
The assignment will train the student in network Layer 2 switching fundamentals when more than one switch is interconnected. If a switch loop is accidentally created, this can cause a broadcast storm, and in the assignment, it will be seen what problems this causes and how to prevent this.

Learning goals

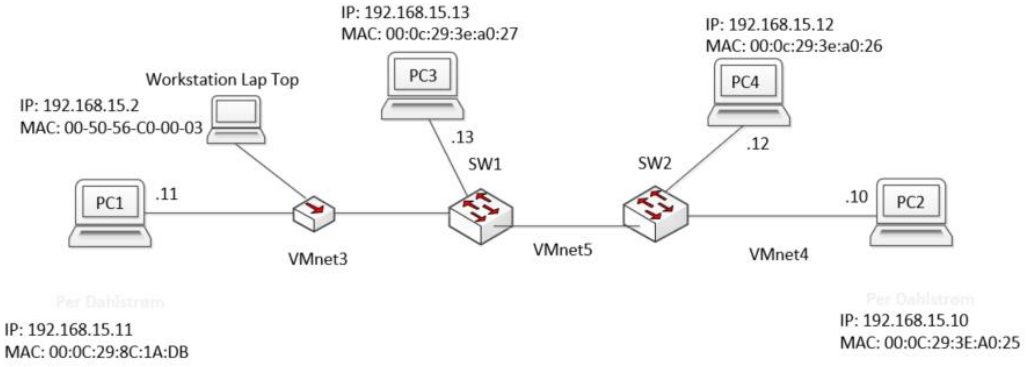
When this assignment is done you can:

- Describe the Spanning Tree Protocol STP.
- Switch on and off the STP on a Linux based switch.
- Set up a small network in VMware Workstation.
- Use TCP dump to monitor relevant network traffic.

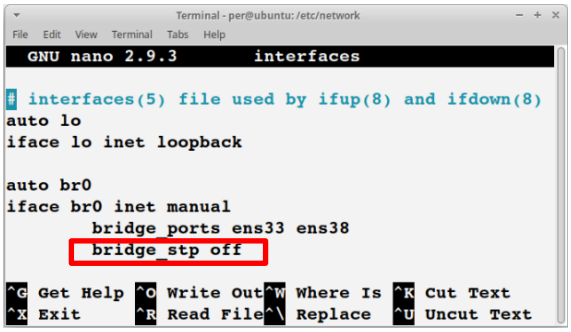
Set up a network with two switches that are interconnected.



Connect one or two PC hosts to each switch. Here below PC1 and PC3 are shown connected to SW1 as well as PC2 and PC4 to SW2.



Configure the switches with STP switched off. Only two switch ports in the shown config.



Hand in a lab report that shows/explains:

1. A network diagram both with and without a switch loop.

2. Prove that the Switch MAC table learning process is running. I.e. show that the MAC table in each SW has learned where the PC1 and PC2 devices MAC addresses are located. Do this with STP switched off. Omit the switchports own MAC addresses.

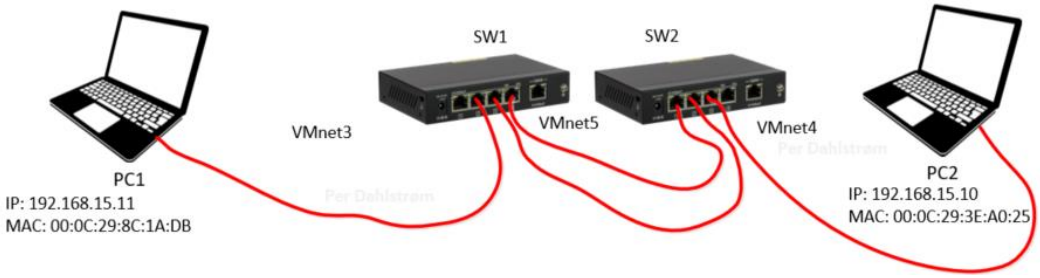
SW1 MAC Table:

Port	MAC
1	
2	
3	
4	

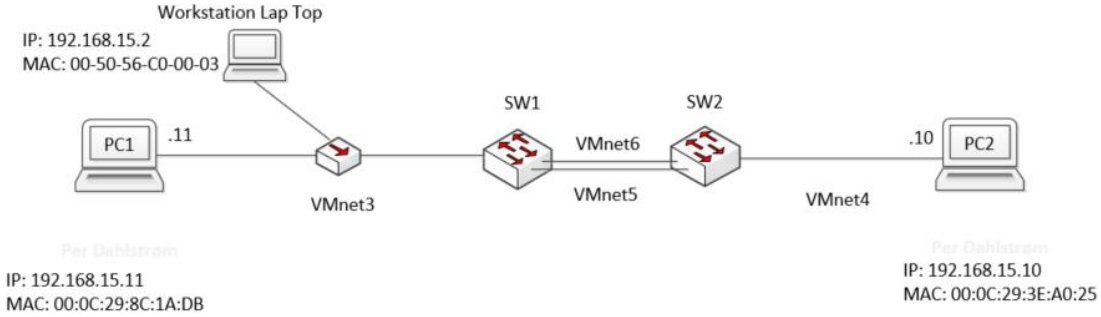
SW2 MAC Table:

Port	MAC
1	
2	
3	
4	

Now interconnect the two switches with one more connection, e.g. VMnet6. I.e. now two connections between the two switches.



3. Explain what will happen when this loop has now been created.



4. Use tcpdump to prove that there is a problem when there is a switch loop and STP is switched off.

5. Show that the switch loop problem is eliminated when STP is switched on.

6. Challenge: Tcpdump or Wireshark on SW1 and show some of the STP traffic. Comment on one or more STP traffic packets.

7. Explain superficially very brief what a switch loop is, why it occurs and what the symptoms in a network is. Remember the behaviour of the switch with flooding out frames. See the video, but only the first two minutes. https://www.youtube.com/watch?v=wOsbtA4Hx04

8. Challenge:
   Explain superficially very brief how the Spanning Tree Protocol STP prevents loops in a switch network.
   Explain why switch ports have MAC addresses.

Hint1: When the STP is off, thousands of packets will flow in the network and possibly block access to one or more devices in WMW Workstation due to CPU overload! Save essential work before testing with STP off! The computer might lock or crash! On an accessible switch SW1 or SW2 use **`sudo ifdown br0`** to stop the traffic.

Here, when the STP was off and packets rampant, and when pinging from PC1 to PC2 a duplicate ping was registered within 4 pings,:

```
per@ubuntu:~$ ping 192.168.15.10 -c 4
PING 192.168.15.10 (192.168.15.10) 56(84) bytes of data.
64 bytes from 192.168.15.10: icmp_seq=1 ttl=64 time=2041 ms
64 bytes from 192.168.15.10: icmp_seq=2 ttl=64 time=4203 ms
64 bytes from 192.168.15.10: icmp_seq=4 ttl=64 time=2206 ms
64 bytes from 192.168.15.10: icmp_seq=1 ttl=64 time=5286 ms (DUP!)
64 bytes from 192.168.15.10: icmp_seq=3 ttl=64 time=3254 ms

--- 192.168.15.10 ping statistics ---
4 packets transmitted, 4 received, +1 duplicates, 0% packet loss, time 3040ms
```

Hint2: The Switches do not have IP addresses. They communicate using the switch ports MAC addresses.

Assignment 6 Binary number system and IP addresses

Learning goals: The student can explain the binary number system and the connection between binary numbers and IP addresses.

1. Write the following decimal numbers in binary:
    a. 224
    b. 255
    c. 1234
    d. 10
    e. 0
    f. 1
    g. 252

2. Write the following dotted decimal notation Private IPV4 addresses in binary:

    a. 192.168.1.1
    b. 172.16.254.1
    c. 10.11.12.13
    d. 10.255.254.253
    e. 192.168.1.255

3. Write the following binary IP addresses in decimal:

    a. 11000000.10101000.00000001.00000001
    b. 10101100. 00011110.00011001.00000101

4. What is the binary equivalent of 242.168.94.124?

    a. 11110011 10101000 01011110 01111100
    b. 11110010 10101010 01011110 01111100
    c. 11110010 10101000 01011110 01111100
    d. 11110010 10101000 01010110 01111100

5. In dotted decimal notation, what is the equivalent of 11010101 01000010 01111111 11000010?

    a. 213.66.127.194
    b. 214.66.128.195
    c. 212.64.143.194
    d. 213.66.111.194

6. What represents the binary equivalence of 207?

    a. 11001111
    b. 11101011
    c. 11010111
    d. 11010101

Assignment 7 Subnetting

Learning goals: The student can explain the binary number system and the connection between binary numbers and IP addresses and subnet masks and sub netting.

1. By using a 28-bit subnet mask to segment the network block 108.12.5.0, how many usable hosts per subnet can be created?

    a. 10
    b. 14
    c. 12
    d. 16

2. Challenge: Given the IP address range 192.168.100.0 through 192.168.100.255, which network mask segments these addresses into 16 subnets?

    a. 255.255.255.224
    b. 255.255.255.240
    c. 255.255.255.248
    d. 255.255.255.252

3. What is the last or highest usable IP address in the 218.6.0.0/17 network?

    a. A. 218.6.125.254
    b. B. 218.6.126.254
    c. C. 218.6.127.254
    d. D. 218.6.128.254

4. How many host addresses are available in the /28 network?
    a. 6
    b. 14
    c. 28
    d. 30

5. What are the usable hosts on the 192.168.1.24/29 network?
    a. .24 through .48
    b. .24 through .32
    c. .25 through .30
    d. .35 through .31

6. If asked to use a 25-bit subnet mask to segment the network block 209.18.12.0. How many usable host addresses will there be per subnet?

    a. 2 hosts
    b. 120 hosts
    c. 126 hosts
    d. 255 hosts

Assignment 8 Sub netting

1. If asked to use a 30-bit subnet mask to segment the network block 108.12.5.0. How many usable host addresses will there be per subnet and how many subnets?

    a. 32 networks with 8 hosts
    b. 62 networks with 2 hosts
    c. 30 networks with 16 hosts
    d. 32 networks with 14 hosts

2. Which two statements are true regarding subnet masks:

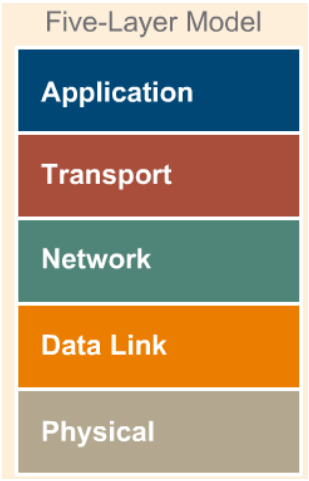
    a. The host portion of the subnet mask is by all 0s
    b. The network portion of the subnet mask is by all 0s
    c. The CIDR notation of 255.255.224.0 is /19
    d. The CIDR notation of 255.255.224.0 is /18

3. TBD

Assignment 9 Number systems

In the document, “Decimal Binary and Hexadecimal numbers.pdf” do exercise 1.3, items 1 and 2 and 3 and 9.

Assignment 10 Routing, one router, two subnets

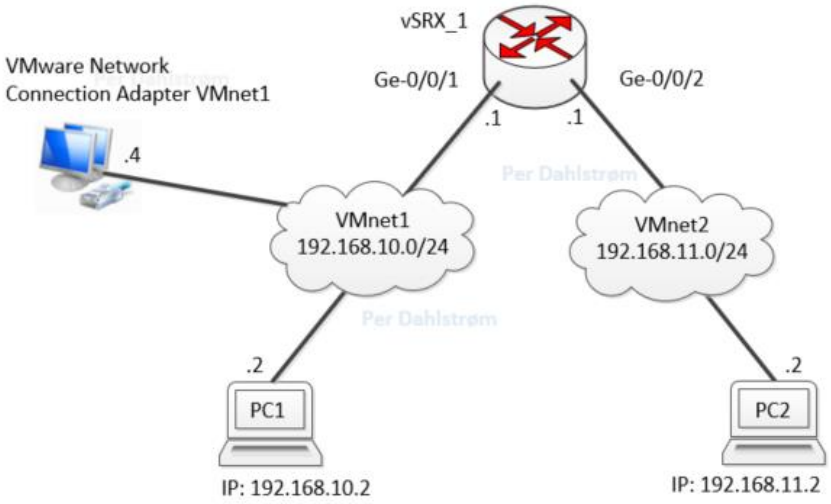


Learning objectives. After this assignment, the student can explain:

- What a router fundamentally is doing in a network.
- Fundamental routing. Static routes.
- Subnet. Not all the details.
- Default Gate Way.
- ARP and MAC addresses in routing.
- Broadcast domain.

Topology

Build the following network by means of VMware Workstation. Students are free to choose and experiment with other private IP address ranges for their subnets.



It is optional to have the "VMware Network Connection Adapter VMnet1" attached. Beware that this adapter can cause IP address conflict as it is set automatically by VMWW to noprmally be ".1"! Check and change the IP in windows of "VMware Network Connection Adapter VMnet1" if necessary.

Hand in

Please use the checklist for "Hand in requirements" in the beginning of this document before handing in.

1. A Networking diagram

2. Screenshots and description of how to "import" the vSRX router in VMware Workstation.

3. Very short description of how to configure the PCs.

4. One relevant screenshot and necessary descriptions of how to configure the vSRX router with static routes between the two shown subnets. Use copy/past from the Putty Terminal to past relevant CLI commands into the hand in, instead of screen shots.

5. Screenshots and descriptions of inter subnet PC pings to prove that the routing by the SRX between the two subnets is working.

6. Wireshark Screenshots and description to prove that the routing between the two subnets is working.
   Comment on MAC addresses and IP addresses, i.e. layer two and layer 3 "activity" seen in Wireshark.

7. Show on the Network diagram and describe how many Broadcast domains there are in the topology.

Challenge:

8. Add one more subnet. Show the network diagram for this. Document the addition of this extra subnet.

Configure DHCP on the SRX router for the two subnets

9. One relevant screenshots and description of how to configure the SRX router with DHCP for the two shown subnets. Use copy/past from the Putty Terminal to past relevant CLI commands into the hand in, instead of screen shots.
   Also show how to configure the PCs from DHCP.

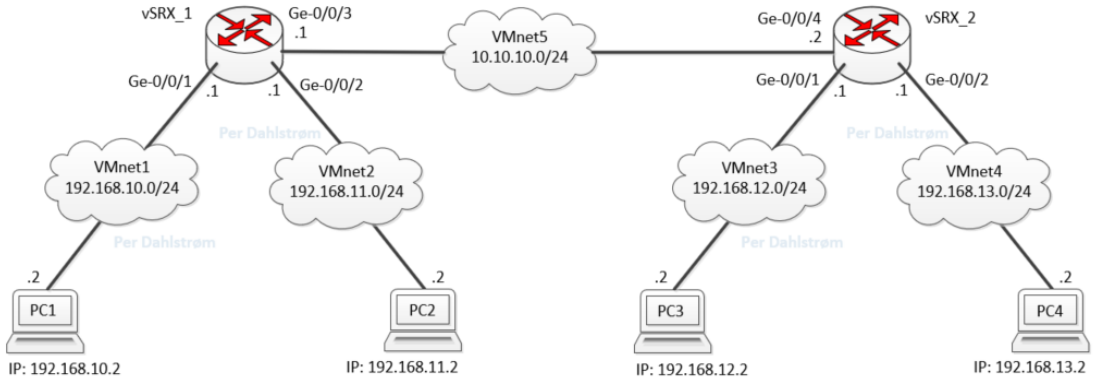
Assignment 11 Routing, two routers, five subnets

Learning objectives. After this assignment, the student can explain:

- Inter router routing
- Static routes
- Direct network
- Routing trouble shooting using ping and traceroute

Topology

By mean of VMware Workstation, build the following network complete with PCS on all subnets.



Hand in

Please use the checklist for hand in requirements in the beginning of this document before handing in.

1. A topology diagram.

2. One screenshot and a brief descriptions of how to set up vSRX_1 and vSRX_2 routers in VMware. Only include things that are different from assignment 10.

3. One screenshot and description of how to configure the PCs.

4. One screenshot, description, and commands on how to configure the vSRX_1 and vSRX_2 routers with static routes between relevant subnets.

5. Use Wireshark and run the ping command and show one screenshot/description that proves that the routing between subnets is working. Possibly comment on layer2 and layer3 addresses. If relevant: Show how ping was used for trouble shooting.

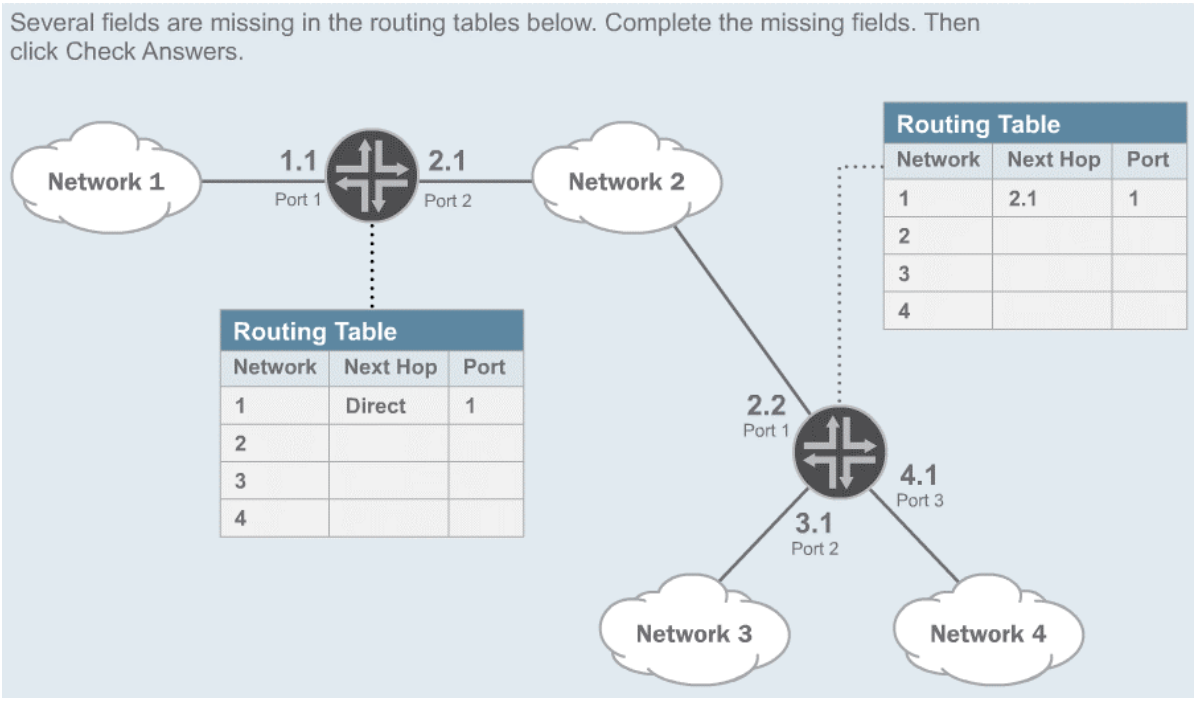
6. Run the traceroute command and show one screenshot/description that proves that the routing between subnets is working. If relevant, then show how traceroute was used for trouble shooting.

7. Describe and show on a/the topology diagram how many Broadcast domains there are in the topology. Challenge: Show some proof of broadcast domains. Hint: Broadcast ping.

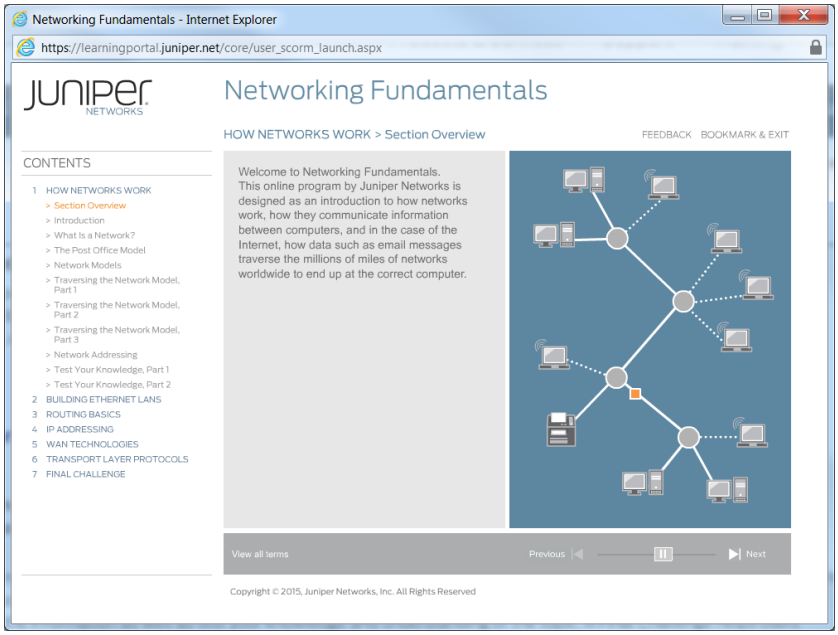
Assignment 12 Routing

This is an assignment from the Juniper Networking Fundamentals Videos in the Routing section.
Make sure to check your answer in the video before handing in on LMS. ☺
Link to the Video at the Juniper site: Networking Fundamentals – WBT

https://learningportal.juniper.net/juniper/user_activity_info.aspx?search=network+fundamentals



This is the start of the 5 hours course:
https://learningportal.juniper.net/core/user_scorm_launch.aspx



Assignment 13 Wireshark

This assignment will train basic Wireshark and HTTP understanding.

Use capture: 1_http.pcapng

1. How many packets are in this trace file?
2. What IP hosts are making a TCP connection in frames 1, 2, and 3?
3. What is the client IP and the server IP?
4. What HTTP command is sent in frame 4?
5. What is the length of the largest frame in this trace file?
6. What protocols are seen in the Protocol column?
7. What responses are sent by the HTTP server?
8. What port is the client on and what port is the server on?

Assignment 14 Wireshark

Wireshark the following traffic.

- DHCP
- ARP
- ICMP
- DNS
- ?

Match your findings with your understanding of the protocols. Investigate and describe what the various fields in the packages mean.

Assignment 15 Wireshark and Network Analysis

Draw a network diagram of the network you are currently on. Use Wireshark to investigate your traffic and try to extracting what your surroundings look like.

List what networking commands on the current system can be used to analyse the network you are on.

Assignment 15 Transport Layer TCP and Telnet

This assignment will train basic Wireshark, TCP and [1]Telnet.

The aim is to:

- see the establishment of a TCP connection by the three way hand shake and closing the connection by 4 way hand shake.
- experience the telnet program and protocol in action
- use Wireshark.

[2]Set static IP addresses on the computers to: 192.168.2.2 and 192.168.2.3
Set the subnet mask to 255.255.255.0. The subnet mask must be the same on the two machines.
Note that on windows 7 it can be tricky to set a static address and/or to keep the address. Micro Soft is largely ignoring the problem.
If the above doesn't work, try 10.10.10.2 and 10.10.10.4 Set the subnet mask to 255.0.0.0.(This seems to work with DNS 8.8.8.8 and 8.8.4.4. And default GW 10.10.10.1)

As a simple Socket/Telnet server written in Python will used, Python has to be installed:

1. Download and install Python 3.2. (The server might work with Python 3.3. and 3.4 also)
2. Download and install the Socket module.
3. Download the Telnet server program from Fronter.
4. Run the Telnet server.
5. Close the Telnet program.

Steps to perform:

1. Connect the patch cable between the two computers.
2. Set the static IPs and subnet mask on the two computers.
3. Make sure they are interconnected by mutually pinging each computer.
4. If ping fails, check the IPs with ipconfig.
   IP might be set to something like 169.254.224.68 which is the ?? address. This is a win 7 issue.
   Note that the subnet mask might be 255.255.0.0
5. Disable all other network cards except the LAN Card.
   It is now safe to switch off the firewall, which might prevent ping between the computers.
   Remember switching the firewall back on before enabling the NICs that connects to the internet.
6. Start wire shark on both machines and observe the pings in the form of ICMP packages.
7. If everything is fine.
   Run the Telnet server on one computer.
   Run the Telnet client on the other computer from the command prompt.

   telnet ip address port number. E.g: `telnet 192.168.2.3 9998`

[1] Telnet Protocol The TCP-IP Guide and SAMS Teach Yourself TCP IP in 24 Hours 4th Edition
[2] https://it.uoregon.edu/static-ip-win7

Hand in: A lab report for the executed work. E.g.

1. A network diagram.
2. Screenshots of Telnet terminal and the server terminal in action.
3. Screen shots of wiresharked connection establishment and closing.
4. Screen shots of wiresharked data send over the connection.
5. Sequence numbers?
6. Port numbers?
7. IP addresses?
8. Other interesting things?
9. PING?

Assignment 16 Different communication standards

Prepare one of the following subjects for a short presentation. The presentation should be a number of Power Point slides. The slides cannot contain text but should exclusively hold figures, drawings, pictures and screenshots etc.

Different communication standards:

- USB
- RS232
- RS485. How is it different from RS232?
- Profibus.
- Bluetooth.
- I2C
- CAN bus
- Other communication or bus system?

Ethernet things

- Hub
- Switch and Mirror port and Spanning Port.
- Bridge
- Router
- How does Ping work?
- How does Trace route work?

Assignment 17 VLANS with brctl

1. Show how to set up VLANs. Prove that it works or doesn't work with screenshots and descriptions. What does Wireshark show regarding the VLAN traffic?

https://www.linuxquestions.org/questions/linux-networking-3/vlan-tagging-through-a-bridge-to-a-vm-4175534283/

Assignment 17 The HUB

Learning goals

The student can:

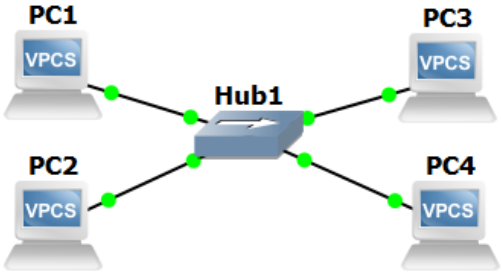
- Set up a small network in VMware Workstation
- Describe the difference between a Switch and a Hub

Set up a brctl implemented switch to act as a hub in order to test the hub functionality.

Hand in a lab report that shows/explains:

1. Set up a new network with a brctl hub and prove and explain that a Hub does not have the switch capabilities in terms of “separating” traffic.

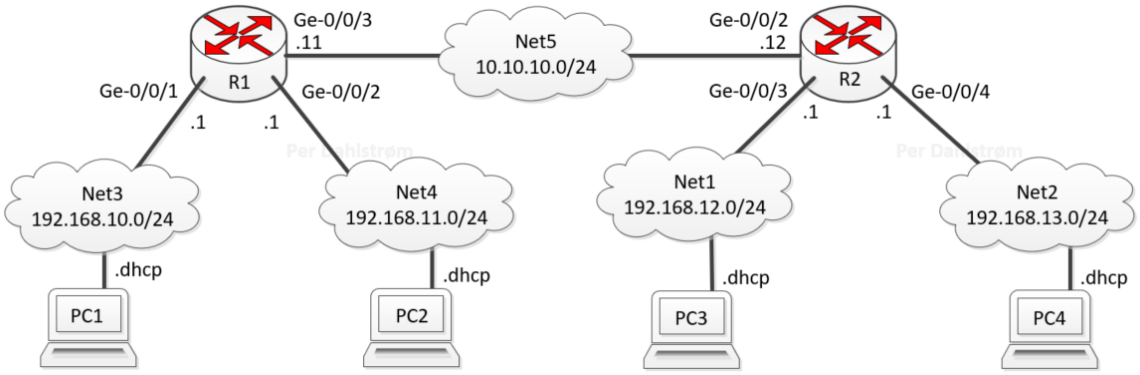
   Topology:



Assignment 18 DHCP service on router

Part 1: DHCP service.

By means of VMware Workstation, build the following network or something similar. Router R1 is with DHCP service for Net3 and Net4 and router R2 with DHCP service for Net1 and Net2. The routers are Juniper vSRXs



Make sure to:

- have tcpdump and Wireshark installed on the PC´s.
- [3]use the troubleshooting document for trouble shooting.
- check that all PCs can ping each other.

Hand in

Use the checklist for hand in requirements in the beginning of this document before handing in.

1. A topology diagram that shows where DHCP is applied and a brief explanation of where DHCP is applied in the topology.

2. One screenshot and configuration commands and description on how to configure:

    a. router R1 with DHCP service for Net3 and Net4.
    b. router R2 with DHCP service for Net1 and Net2.

    Put the configurations on GitLab and a working link to it in the hand in.

3. One screenshot and description of

    a. how to configure the PCs for DHCP
    b. screen shot of one of the PCs IPV4 settings received form the router DHCP service.

4. Explain briefly in 3 - 6 lines in your own words what [4]DORA is in the DHCP context.

---

[3] https://gitlab.com/PerPer/networking/blob/master/Troubleshooting/Network_Troubleshooting_Per_Dahlstroem_UCL.md

[4] https://www.juniper.net/documentation/en_US/junos/topics/topic-map/dhcp-for-routing-devices.html

5. Run Wireshark and show the DORA process.
   Comment on IP addresses, i.e. layer 3 addresses seen in Wireshark.

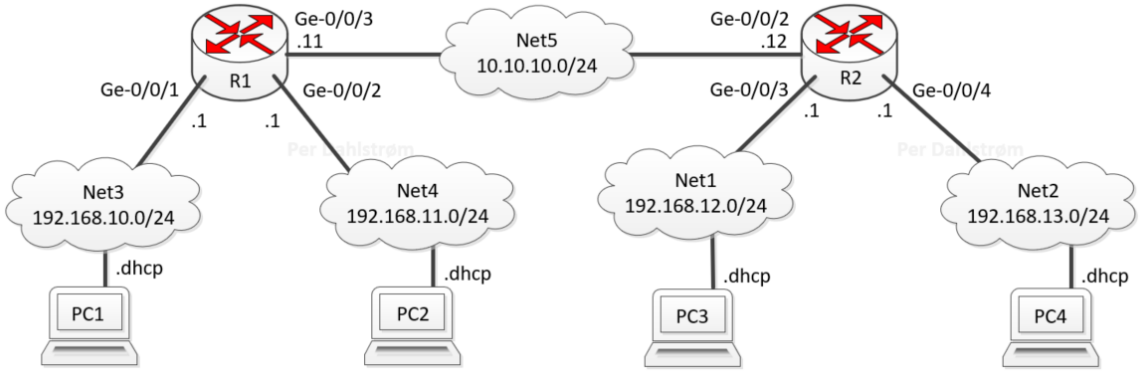
6. Explain briefly 3 lines maximum, what Transport layer 4 ports and protocol the DHCP client and server are using.

7. Show how ping and traceroute and Wireshark were used for possible troubleshooting.

Part 2: DHCP relay.

Now reconfigure R1 and R2 so that R1 is providing DHCP service for all four subnets Net1, Net2, Net3 and Net4 and R2 is acting as a DHCP relay for R1:

The diagram is unaltered repeated here for convenient reading:



Hand in

1. A topology diagram that shows where DHCP is applied and a brief explanation of where and how DHCP is applied in the topology.

2. One screenshot and configuration commands and description on how to configure:

   a. router R1 with DHCP service for Net1, Net2, Net3 and Net4.
   b. router R2 with DHCP relay service.

   Put the configurations on GitLab and a working link to it in the hand in.

3. One screenshot and description of

   a. screen shot of PC4s IPV4 settings received form the router DHCP service.

4. Show how ping and traceroute and Wireshark were used for possible troubleshooting.

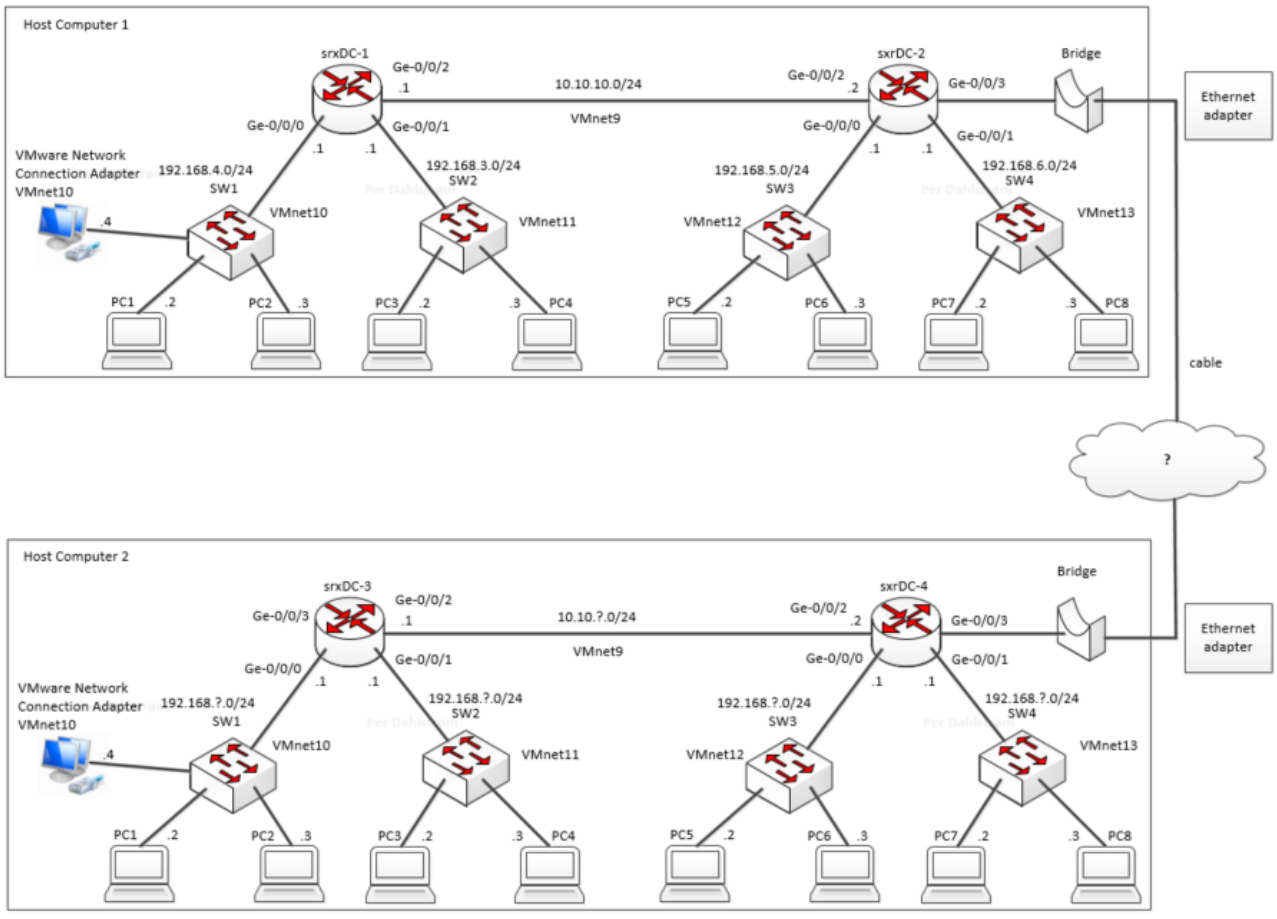
Assignment 19 Interconnecting between two VMW Workstations

Learning goals

The student can:

- Draw a [5]HLD, High Level Network Design
- Create a [6]LLD, Low Level Network Design.
- Use TCPdump and Wireshark and Junos monitor traffic to monitor relevant network traffic.
- Interconnect Virtualised networks via bridges and physical Ethernet adapters and cable.
- Explain and document all of the above.

By means of VMware Workstations on two computers Host Computer 1 and Host Computer 2, build the following networks complete with PCS on the subnets. Ultimately, all user hosts, PCs, should be able to ping each other.



By means of bridging, interconnect the network on Host Computer 1 and Host Computer 2 as shown in the diagram. Use Host Computer 1 and Host Computer 2 cabled Ethernet adapter ports for the interconnection. Some addresses are shown in the diagram with question marks and the bridged

[5] https://eal-it-technology.github.io/Network-design/hld.html
[6] https://eal-it-technology.github.io/Network-design/lld.html

network is also indicated with a question mark. This indicates that it has to be considered what subnet IP addresses should be used. DHCP can be used on the subnets.

Hand in

Use the checklist for hand in requirements in the beginning of this document before handing in.

Hint: Download the needed software like Wireshark and TCPdump to the PCs before connecting them to the routers, I.e. use VMnet8 with NAT initially to have internet access on the PCs.

1. One/two screenshots and descriptions of where the srxDC-x routers and host PCs are located on the VMware Workstations.

2. A HLD with brief explanation. Remember if DHCP is used.

3. A LLD with brief explanation. Remember if DHCP is used.

4. Show and describe how TCPdump and Wireshark and Junos monitor traffic was used for problem solving.

5. Demonstation of how TCPdump and Wireshark and Junos monitor traffic is used to monitor relevant network traffic.

6. Show and describe the configuration of Interconnect Virtualised networks via bridges and physical Ethernet adapters and cable.

7. Show that pings work for host PCs across Host Computer 1 and Host Computer 2 bridged cabled Ethernet adapter ports. In essence between all subnets.

8. Show at least 2 routers routing tables and explain very briefly the interesting parts.

9. Show one PCs routing table with **`ip route`**, and explain very briefly the relevant parts.

[7]Example LLD created in MS Excel for a part of the above shown network:

Device Name	Device type	Interface	Unit	ip address	Subnet Mask	VMW VMnet	IP Family	To device	To device IP Address	Comments
srxDC-1	**virtual-router Juniper SRX-240**	ge-0/0/0	0	192.168.4.1	/24	10	inet			USRLAN
		ge-0/0/1	0	192.168.3.1	/24	11	inet			PRODLAN
		ge-0/0/2	0	10.10.10.1	/24	9	inet	srxDC-2	10.10.10.2	
		ge-0/0/3								
		ge-0/0/4								
		ge-0/0/5								

[7] https://eal-it-technology.github.io/Network-design/lld.html

Assignment 20 Application layer protocol and TCP

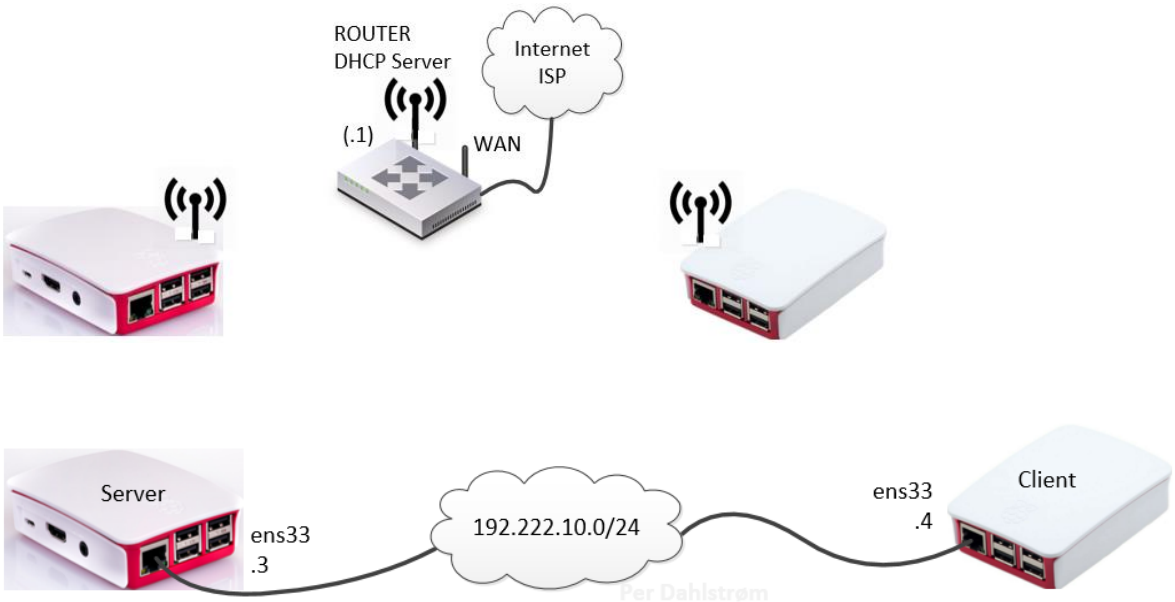
Learning goals

The student can:

- Explain what an application layer protocol is.
- Explain what a TCP port is.
- Explain what the TCP Three-way-hand shake is.
- Explain what a Python TCP Socket and a Python TCP Connection is.
- Document the TCP Three-way-hand shake by using WireShark and or TCPdump.
- Interconnect devices based on their IP address and Ports and transmit customised data between the devices.
- Modify a Python program to introduce a customised application layer protocol.

Explain and document all of the above.

Two devoices have to be interconnected via Ethernet and TCP/IP. The devices have to be physical devices like Raspberries. The interconnection can be wired or wireless. The initial system and programming can be done virtualised on VMware Workstation.



As shown in the illustration one device will act as a server and the other as a client. It is the client who initiates the communication between the devices.

In this assignment, the data send from the client to the server will/can be entered manually in the terminal.

The entered data simulates the readings from some sensors attached to the client device.

As the data that has to be send are picked up from various sensors, a data packet format has to be decided. Here is an example of what data could be picked up and have to be transmitted:

Parameter	Range	Resolution	Comment
Motor 1 position	0 – 259 decimal	1	
Motor 2 position	0 – 259 decimal	1	
Motor 1 speed	0 – 100%	1	
Motor 2 speed	0 – 100%	1	
Light sensor 1	20 – 60 decimal	1	
Light sensor 2	20 – 60 decimal	1	
Battery voltage	4 - 6	0,1	<4 is under voltage

A server and a client program are given. These programs have to be developed according to the here given specifications.

The programs Server program[8] and Client program[9] can be found at the links below or/and on the College LMS.

As the programs are now these are the outputs when executed. In this case both programs "connected" to IP 127.0.0.1. This has to be changed to the actual IPs used.

Client output:

```
Type sensor readings: 1234567812345678
Type sensor readings:
```

Server output:

```
Awaiting connection on IP:  127.0.0.1  Port:  65432
Connection from: ('127.0.0.1', 60902)
1231567812345649
```

The output from the server has to be changed to the format shown here below, when the transmitted data is as in the example above, namely "1231567812345649":

```
Light sensor 1        34
Light sensor 2        56
Battery voltage       4,9 volt
Motor 1 speed         78%
Motor 2 speed         12%
Motor 1 position      123
Motor 2 position      156
```

[8] https://github.com/perperperperper/realPythonTCPServer/blob/master/venv/Include/realPythonServ2.py
[9] https://github.com/perperperperper/realPythonTCPServer/blob/master/venv/Include/realPythonClient3.py

Hand in

Use the checklist for hand in requirements in the beginning of this document before handing in.

Hint: Download the needed software like Wireshark and TCPdump to devices, **`sudo apt install`**

1. A network diagram with brief explanation.

2. Show the TCP Three-way-hand shake in Wireshark. Give short explanation.

3. Illustrate graphically and explain the developed application layer protocol.

4. Show the client and server programs. Explain what was added to the programs.

5. Show and demonstrate the output from the two programs. Representative test runs must be shown and demonstrated to show that the programs are robust.

6. Optional:
   Develop the application layer protocol beyond the here give specifications.
   Illustrate graphically and explain the developed application layer protocol.

7. Optional:
   Make a GUI for the server program.

8. Optional:
   Put all source code in a GitHub repository and provide download links.

Assignment 21 Extended application layer protocol. Temperature sensor.

Learning goals

The student can:

- Explain what an application layer protocol is. Compared to assignment 20 the protocol here is more complex or extended.
- Explain how to store data in a Python data structure and how to present data.
- Modify a Python program to introduce a customised application layer protocol.

Explain and document all of the above.

Base version program:

The client and server programs from assignment 20 must be further developed so that the client creates 100 random temperature measurements and stores them in a list. When stored in the list the measurements are send to the server who stores the measurements in a list. After the server has stored the measurements in a list, the server prints out all values in a 10 columns by 10 rows table.

Optional: Timestamped measurement version:

The client and server programs from assignment 20 must be further developed so that the client creates 100 random temperature measurements and stores them in a list along with a time stamp. When stored in the list the measurements are send to the server who stores the measurements in a list. After the server has stored the measurements in the list, the server prints out all values in a nice way alongside their time stamps.

Optional: Graph plotting version:

The client and server programs from assignment 20 must be further developed so that the client creates 100 random temperature measurements and stores them in a list along with a time stamp. When stored in the list the measurements are send to the server who stores the measurements in a list. After the server has stored the measurements in the list, the server prints out all values in a nice way alongside their time stamps.

Hand in

Hint: Download the needed software like Wireshark and TCPdump to devices, `sudo apt install`

1. A network diagram with brief explanation.
2. Illustrate graphically and explain the developed application layer protocol.
3. Show and explain the output from the server program when client and server are executed.
4. Show in Wireshark that the transmitted data can be monitored in plain text.
5. Put the client code and the server code in appendixes.

Assignment 22 Synchronised transmission from client to server

Learning goals

The student can:

- Explain what it means to synchronise a client and a server for data transmission.
- Implement a simple synchronisation mechanism for continuous but discrete transmission of data between a server and a client.
- Consider what would be a suitable Python program solution to simulate temperature measurements.

Use case

A client device is doing measurements of its ambient temperature every second. An attached temperature sensor gauges the temperature. The client must send its ambient temperature very second to the server. The ambient temperature is in the range 0 to 100 degree Celsius.

It is a requirement to use TCP/IP socket for the communication.

Base version program:

- The server receives data every second and prints them to stdio, i.e. the console.

Optional: Timestamped measurement version:

- The server receives data every second with a time stamp and prints them to stdio, i.e. the console. The temperature is printed with the timestamped.

Optional: Graph plotting version:

- The server receives data every second and prints them to stdio, i.e. the console. The temperature is shown in a graph.

Hand in

Hint: Download the needed software like Wireshark and TCPdump to devices, **`sudo apt install`**
Hint: Use the time module on both server and client to achieve the synchronisation.

1. A network diagram with brief explanation.

2. Illustrate graphically and explain the developed application layer protocol. Focus on the synchronisation mechanism but of course also explain the data format in the transmitted messages. I.e. explain how the server and client synchronise so the temperature is send/received every second.

3. Show and explain the output from the server program when client and server are executed.

4. Show in Wireshark that the transmitted data can be monitored in plain text.

Put the client code and the server code in appendixes or on GitHub.

Assignment 23 TLS for socket communication.

Learning goals

The student can:

- Explain what it means to encrypt data and to do authentication.
- Explain what TLS means.
- Implement a TLS wrapper for the Python socket.

Building on either the program from assignment 20, 21 or 22, build a program that implements a TLS wrapper for the socket connection.

Use openssl to create a private key and a certificate. Source code for inspiration can be found here on GitLab[10].

Hand in

1. A network diagram with brief explanation.
2. Describe the aim of the software/program in 4 lines.
3. Illustrate graphically and explain the introduce TLS.
   Explain what it means to encrypt data and to do authentication.
4. Show how to create private key and server sertificate using openssl.
5. Show and explain the output from the server program when client and server are executed.
6. Show in Wireshark that the transmitted data cannot be monitored in plain text.
7. Optional: Show in Wireshark and explain the key and certificate exchange.

Put the client code and the server code in appendixes or on GitLab. Code must be accessible on GitLab by a link if gitLab is used.

[10] https://gitlab.com/PerPer/python-socket-tls

Assignment 24 Mini Networking project and Project Management

Learning goals

The student can:

- Apply acquired technical skills and combine these skills to produce a desired result.
- Manage a teamwork using an online project tool. Here GitLab will be required.
- Be a contributing part of a managed team.

The task here is for the team to define a project that incorporates the following technologies:

- Structured project management.
- Python
- Python socket
- TLS
- TCP or UDP
- Data logging
- Server/Client in a TCP connection.
- Data representation and data storing.

Work in a team of max. 4 person. The project is a short-term project and has focus on Project management.

Use GitLab boards for your project management. Please see these sources [11] [12].

Project layout:

Day1:

- Decide on project goal.
- Schedule meetings for the project period.
- Subdivide the project into subtasks.
- Put subtasks and meetings into your project management tool.
- Hand in in one document:
    - an overall requirements document or specifications document on PeerGrade where you use this template[13] for the requirements document.
      Note that the template is for a WebSite development. Where adequate, substitute the items that specifically deal with the WebSite with the actual items.
    - Your project plan showing:

[11] https://about.gitlab.com/2018/08/02/4-ways-to-use-gitlab-issue-boards/
[12] https://about.gitlab.com/product/issueboard/
[13] https://productcoalition.com/how-to-write-a-simple-yet-effective-requirements-document-bda5bf6623e0

Day2:

- Team members work on their subtasks.
- Update the project plan status.
- Status meeting with lecturer

Day3:

- Teammembers work on their subtasks.
- Update the project plan status.
- Presentation of achievements and project management lessons learned.

Assignment 25 Subnetting

Learning goals

The student can:

- Configure IP addresses on a small Network including subnet masks.
- Identify when IP addresses are on the same IP network and when they are not.

The task here is to set up a small test networks in VMWW:

1. Make a network with two hosts on a /28 network. Use private IP addresses. E.g. 192.168.168.?/28.

   Choose and complete the IP addresses for the two hosts. Configure the hosts in VNWW and prove that they can ping each other.

2. For two hosts, set the following IP addresses. Note that the subnet masks are different for the two hosts. It is normally not a good idea to have different subnet masks for networking devices who should communicate on the same IP network.

   1: 192.168.168.5/20
   2: 192.168.168.10/24

   Can the hosts ping each other?

   Explain in binary why the hosts can ping each other or why they cannot ping each other.

3. Challenge: Configure two hosts on the same logic IP network with the biggest possible subnet mask. I.e. the subnet mask with the highest possible number of ones in it that still allows for two hosts to have legal IP addresses on the network.

Handing in:

- Document the above-mentioned items.

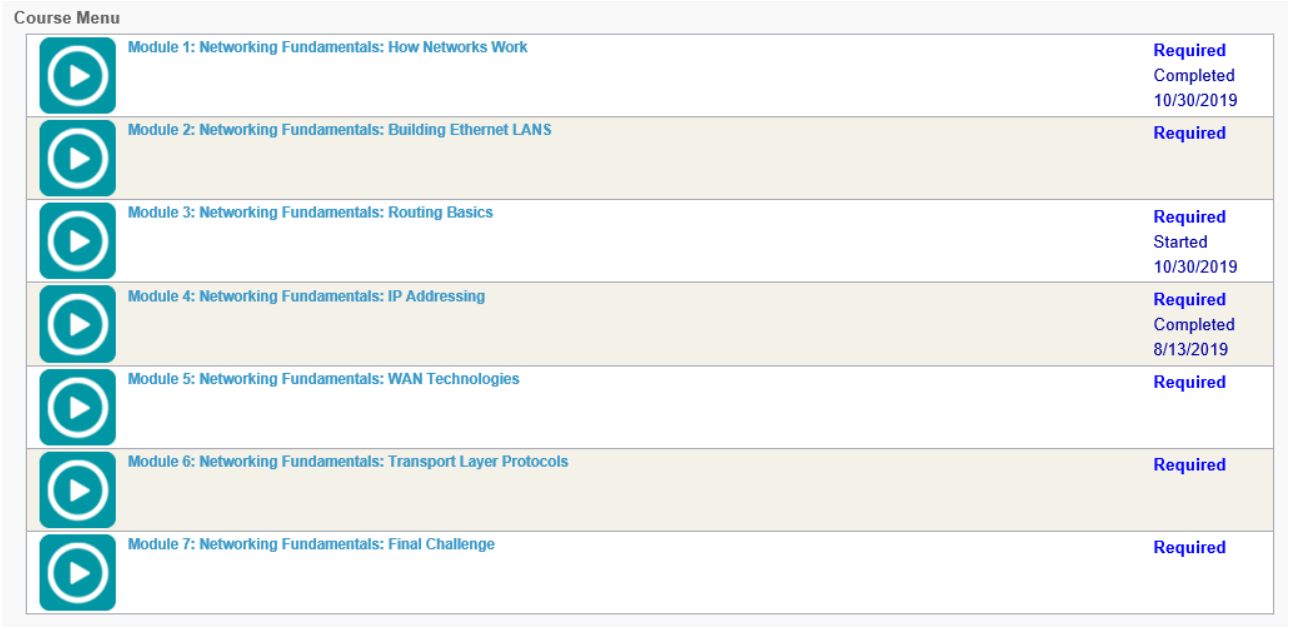
Assignment 26 Routing

This is an assignment from the Juniper Networking Fundamentals Videos in the Routing section. Make sure to check your answer in the video before handing in. ☺

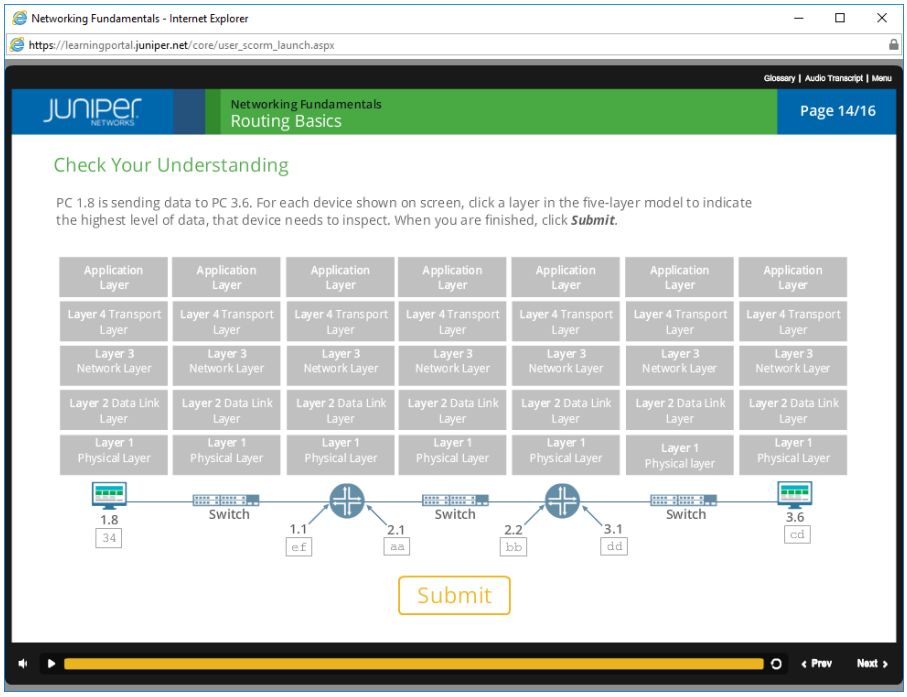
Link to the Video at the Juniper site: Networking Fundamentals – WBT

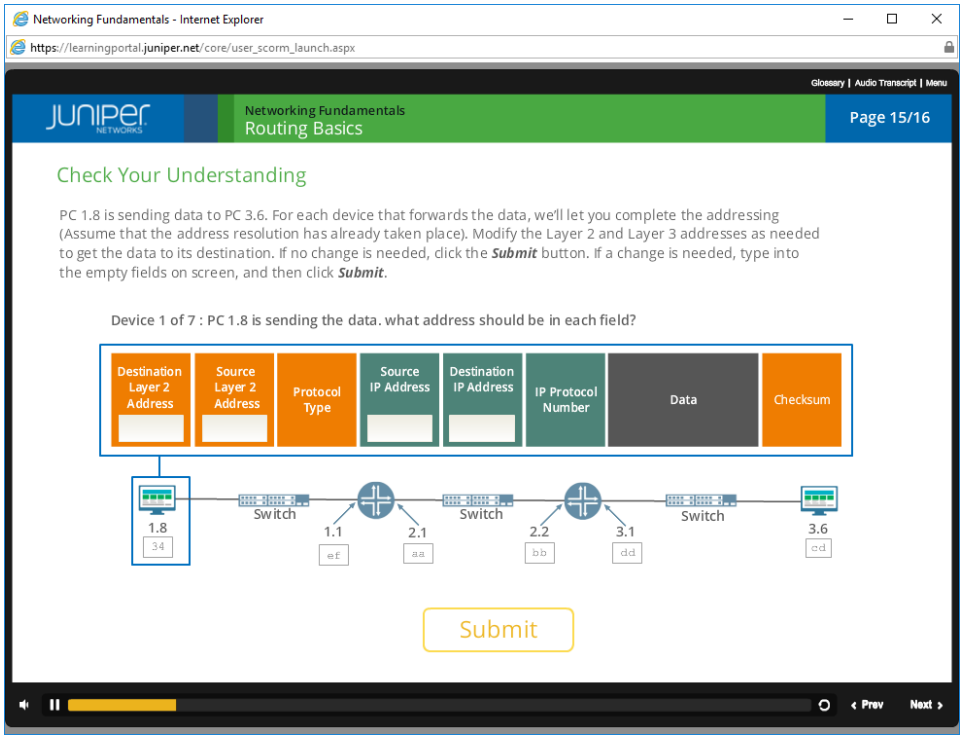
https://learningportal.juniper.net/juniper/user_activity_info.aspx?id=769

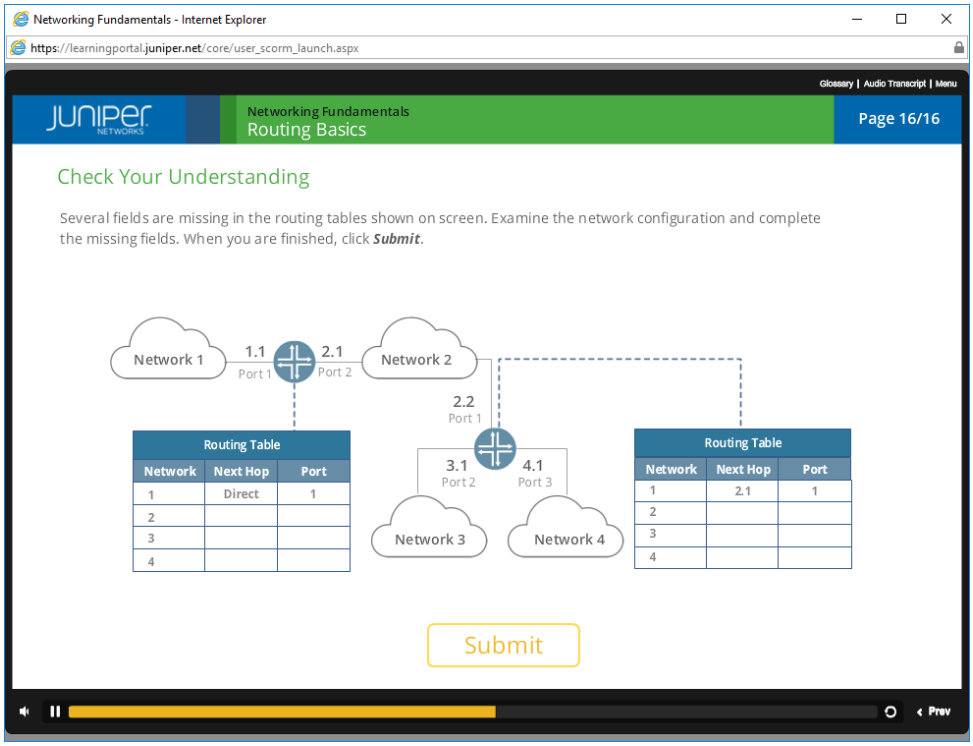
It will require you to register.



Hand in screen shots that prove that the three "Check Your Understanding" parts/questions in the Netwworking Fundamentals Routing Basics have been answered correctly. Only hand in when all is correct, i.e. keep training until it is all understood. ☺







It is recommended to do the whole course until the final Chalenge, i.e. Module 7 can be answrede correctly. ☺

Assignment 27 Routing on physical SRX240

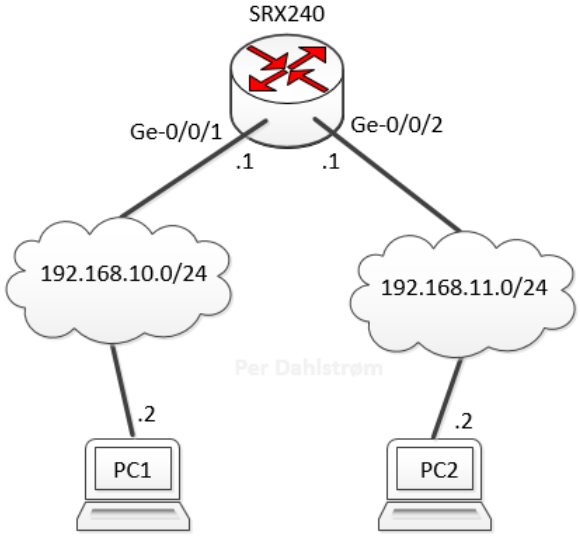
Learning objectives. After this assignment, the student can explain:

- What a physical router fundamentally is doing in networking.
- Fundamental routing. Static routes.

Topology

Build the following network using one of the physical SRX240 routers in the networking lab.

Use Physical devices as PC1 and PC2. E.g. Raspberry Pi´s.



Tasks:

1. First only connect your Laptops serial USB port to the SRXx-x console port via your table and patch panel 39.
2. Check your serial port number ComX in the Windows Device Manager and connect to the SRXx-x using Putty.
3. Load a base configuration:
   https://gitlab.com/PerPer/networking/blob/master/SRX%20configurations/SRX240BaseConfigV02.json
4. Use:
   SRXx-xx# **`load override terminal`**
   Copy and past with: Right click in the Putty terminal.
   Press: ctrl + d
   SRXx-xx# **`commit`**
5. The SRX is now ready for configuration.
   Note that only ge-0/0/1 has been configured in this base configuration. The rest must be configured now. This can be done in two different ways:

   a. In the SRX edit mode.
   b. Editing the base configuration file and upload it again.

6. Connect the table and patch cables to the SRX ge-0/0/1 and ge-0/0/2 and do the tests needed to check that the configuration in working as intended.

Hand in

Please use the checklist for "Hand in requirements" in the beginning of this document before handing in.

1. A Networking diagram. Remember all interface names.

2. Description of how to configure the PCs. E.g. the Raspberries.

3. One relevant screenshot and necessary descriptions of how to configure the SRX router with static routes between the two shown subnets. Use copy/past from the Putty Terminal to past relevant CLI commands into the hand in, instead of screen shots.

4. Describe briefly the Physical serial console connection to the router console port.

5. Screenshots and descriptions of inter subnet PC pings to prove that the routing by the SRX between the two subnets is working.

6. TCPdump or Wireshark screenshots with description to prove that the routing between the two subnets is working.
   Comment on MAC addresses and IP addresses, i.e. layer 2 and layer 3 "activity" seen in TCPdump.

7. Show on the Network diagram and describe how many Broadcast domains there are in the topology. Show a proof of this.

   Use: **`ping -b 192.168.10.255`** eller **`ping -b 255.255.255.255`**

   -b stands for broadcast.

Challenge:

Configure DHCP on the SRX router for the two subnets

8. One relevant screenshots and description of how to configure the SRX router with DHCP for the two shown subnets. Use copy/past from the Putty Terminal to past relevant CLI commands into the hand in, instead of screen shots.

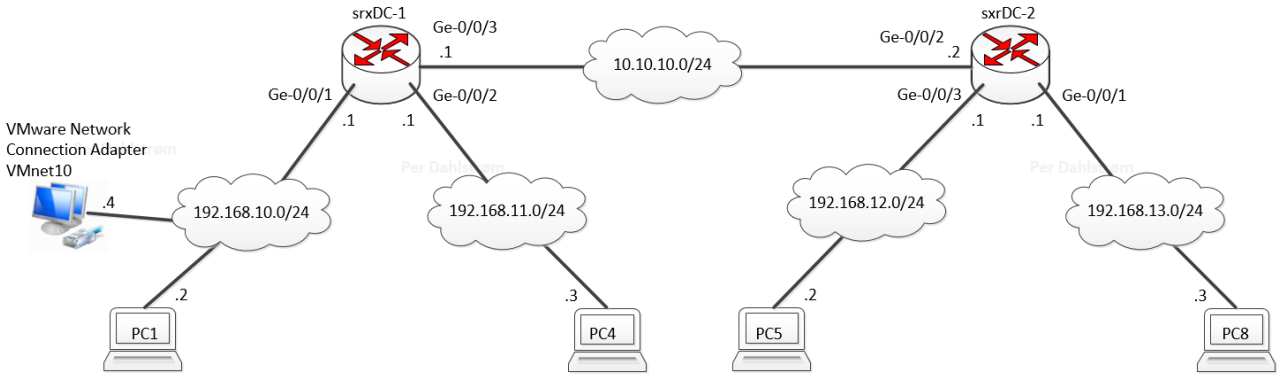
Assignment 28 Routing, two routers, five subnets on physical routers.

Learning objectives. (“Same" as ass. 11.) After this assignment, the student can explain:

- Inter router routing
- Static routes
- Direct network
- Routing trouble shooting using ping, tcpdump and traceroute

Topology

Build the following networks complete with Raspberry PIs as PCs on all subnets on physical routers SRX240.



Hand in

Use the checklist for hand in requirements in the beginning of this document before handing in.

1. A topology diagram.

2. One screenshot and description of how to configure the PCs.

3. One screenshot, description, and commands on how to configure the srxDC-1 and srxDC-2 routers with static routes between relevant subnets.

4. Show how ping was used for trouble shooting. Run the ping command and show one screenshot/description that proves that the routing between subnets is working.

5. Show how traceroute was used for trouble shooting. Run the traceroute command and show one screenshot/description that proves that the routing between subnets is working.

6. Describe and show on a topology diagram how many Broadcast domains there are in the topology. Challenge: Show a proof of this. Hint: Use ping 255.255.255.255.

7. Challenge: Install WireShark on one or more of the Raspberry PIs Linux hosts.
   Run Wireshark and show one screenshots/description that proves that the routing between all subnets is working. Comment on MAC addresses and IP addresses, i.e. layer two and layer 3 “activity” seen in Wireshark.

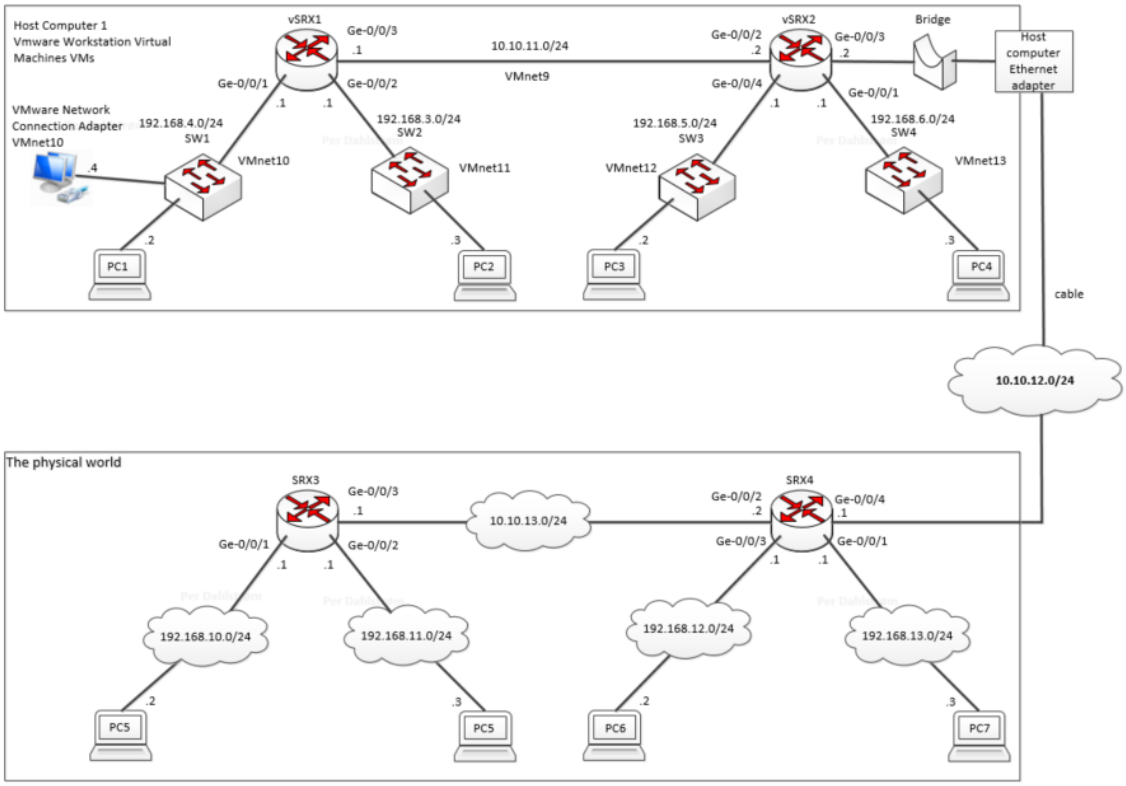
Assignment 29 Connecting VMW Workstation nets to physical nets

Learning goals (Originally assignment 19)

The student can:

- Draw a [14]HLD, High Level Network Design
- Create a [15]LLD, Low Level Network Design.
- Use TCPdump and Wireshark and Junos monitor traffic to monitor relevant network traffic.
- Interconnect Virtualised networks via bridges and physical Ethernet adapters and cable.
- Explain and document all of the above.

By means of VMware Workstations on a computer Host Computer 1 and physical routers, build the following networks complete with PCs on the subnets. Ultimately, all user hosts, PCs, should be able to ping each other. Use Raspberries for the Physical network.



By means of bridging, interconnect the network on Host Computer 1 with the physical router(s), as shown in the diagram. Use cabled Ethernet adapter port for the interconnection.

Hand in

Use the checklist for hand in requirements in the beginning of this document before handing in.

[14] https://eal-it-technology.github.io/Network-design/hld.html
[15] https://eal-it-technology.github.io/Network-design/lld.html

Hint: Download the needed software like Wireshark and TCPdump to the PCs before connecting them to the routers, I.e. use VMnet8 with NAT initially to have internet access on the PCs.

1. A working GitLab link to well organised router configurations.

2. A HLD with brief explanation.

3. A LLD with brief explanation.

4. Show and describe how TCPdump and Wireshark and Junos monitor traffic was used for problem solving.

5. Demonstation of how TCPdump and Wireshark and Junos monitor traffic is used to monitor relevant network traffic.

6. Show and describe the configuration of Interconnected Virtualised network via bridge and physical Ethernet adapters and cable.

7. Show that pings work for host PCs across Host Computer 1 and physical routers bridged cabled Ethernet adapter ports. In essence between all subnets.

8. Show at least a virtual and a physical routers routing tables and explain very briefly the interesting parts.

9. Show one or more PCs routing tables with **`route -n`**, and explain very briefly the relevant parts.

[16]Example LLD created in MS Excel for a part of the above shown network:

Device Name	Device type	Interface	Unit	ip address	Subnet Mask	VMWW VMnet	IP Family	To device	To device IP Address	Comments
srxDC-1	**virtual-router Juniper SRX-240**	ge-0/0/0	0	192.168.4.1	/24	10	inet			USRLAN
		ge-0/0/1	0	192.168.3.1	/24	11	inet			PRODLAN
		ge-0/0/2	0	10.10.10.1	/24	9	inet	srxDC-2	10.10.10.2	
		ge-0/0/3								
		ge-0/0/4								
		ge-0/0/5								

[16] https://eal-it-technology.github.io/Network-design/lld.html

Assignment 30 Source Nat and default route

Learning objectives:

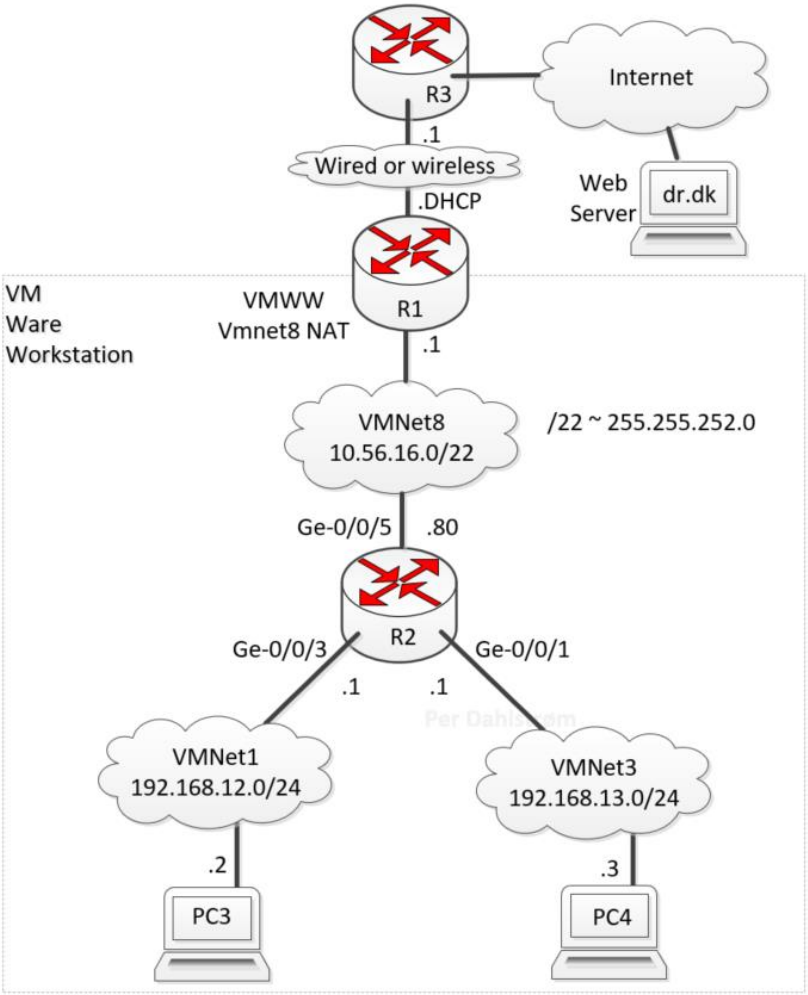
After this assignment, the student can explain:

- [17]Source Natting NAT and default route

The student can:

- Set up NAT and default route on a SRX Junos router.

Topology



[18]By means of VMware Workstation VMWW, build a network that allows Source Natting on a SRX router to be set up and tested. A network suggestion is shown above.

Before configuring Linux hosts PC3 and PC4, please install Wireshark.

[17] https://rtodto.net/juniper-srx-for-beginners/
[18] https://www.juniper.net/documentation/en_US/junos/topics/topic-map/nat-security-source-and-source-pool.html#id-example-configuring-source-nat-for-egress-interface-translation

Hand in

Use the checklist for hand in requirements in the beginning of this document before handing in.

1. A topology diagram with explanation.

2. Configure default route and NAT on the R2 according to the diagram. The router should provide internet access for all possible hosts on networks 192.168.12.0/24 and 192.168.13.0/24.
   Please note that the 10.56.16.0 is a /22 network and not a /24 network. I.e. the /22 network mask is 255.255.252.0.

3. Put the router configuration on GitLab and also the topology diagram. Post a working link here to the configuration and topology. It is obligatory to put relevant comments in the configuration.

4. Demonstrate how these programs were possibly used for trouble shooting:
   a. ping.
   b. traceroute.
   c. Wireshark.

5. Run Wireshark and the ping command on PC3 or PC4 and show one screenshots/description. Comment on MAC addresses and IP addresses.

6. [19]On the SRX run the command:

   ```
   # show security flow session nat [brief | extensive | summary]
   ```

   a. Only run ping 8.8.8.8 on PC3 and show the SRX output and explain it.
   b. Also run a web browser and browse to e.g. dr.dk and show the SRX output and explain it.

Here is an example output from PC3 web browser to dr.dk:

```
root@R2> show security flow session nat brief
Session ID: 11353, Policy name: internet-access/6, Timeout: 296, Valid
  In: 192.168.12.5/47610 --> 34.107.221.82/80;tcp, If: ge-0/0/3.0, Pkts: 8, Bytes: 636
  Out: 34.107.221.82/80 --> 10.56.16.80/1026;tcp, If: ge-0/0/5.0, Pkts: 6, Bytes: 464
```

[20]The originating or source IP is 192.168.12.2 port 47610 to destination IP 34.107.221.82 port 80. The source IP and port is then to the untrust zone, ge-0/0/5 swapped or translated to originate from 10.56.16.80 port 1026. The destination 34.107.221.82 port 80 is not altered. The source port numbers along with their IP addresses are stored by the SRX, for the SRX to remember what session a possible answer belongs to, i.e. who should receive the answer. This is source Port Address Translation or PAT.

Here is an example output from PC3 pinging 8.8.8.8 which is more tricky to dissect in Wireshark as ping is not using ports:

```
[edit]
root@R2# run show security flow session nat
```

[19] https://rtodto.net/srx-for-beginners-2/
[20] https://www.youtube.com/watch?v=qij5qpHcbBk&ab_channel=CertBros From (03:20) to (05:20)

```
Session ID: 8543, Policy name: internet-access/6, Timeout: 4, Valid
  In: 192.168.12.2/5 --> 8.8.8.8/15693;icmp, If: ge-0/0/3.0, Pkts: 1, Bytes: 84
  Out: 8.8.8.8/15693 --> 10.56.16.80/1162;icmp, If: ge-0/0/5.0, Pkts: 1, Bytes: 84
```

The originating or source IP is 192.168.12.2 port 5 to destination IP 8.8.8.8 port 15693. This is then to the untrust zone, ge-0/0/5 translated to originate from 10.56.16.80 port 1162 still to destination 8.8.8.8. The port numbers are added by the SRX, for the SRX to remember who should receive the possible answer. This is embedded in ICMP.

Assignment 31 IP V4 addresses

Learning objectives:

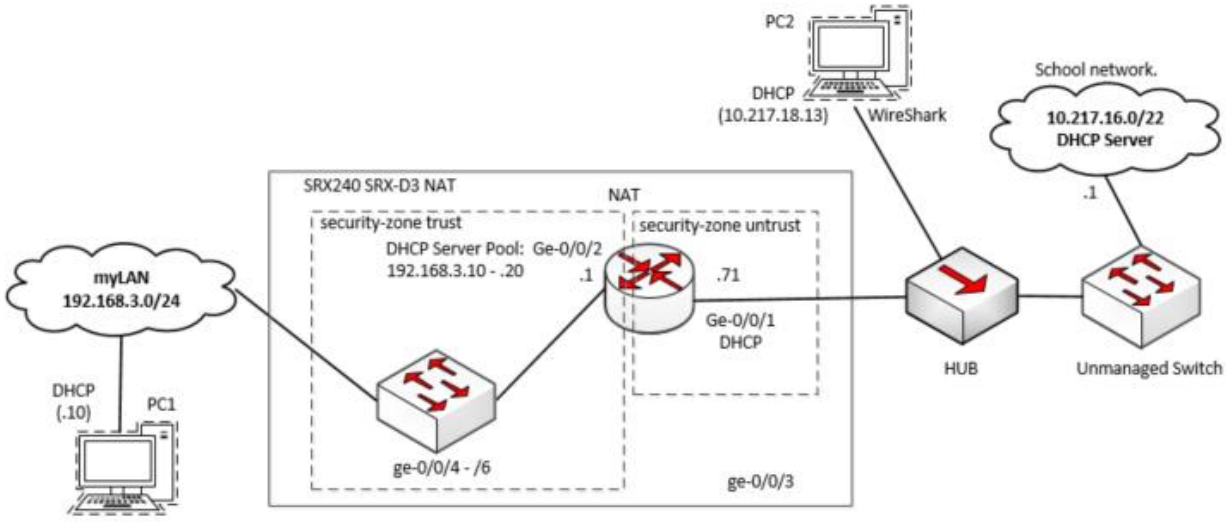
After this assignment, the student can explain:

- What an IP subnet mask is and what host IPs are possible on a given subnet.

The student can:

- List what host IPs are possible on a given subnet.

In the given network diagram shown below a sub network named School network is 10.217.16.0/22.



The SRX-D3 has from the School network DHCP server/service on interface ge-0/0/1 got the IP address 10.217.16.71/22.

PC2 has from the School network DHCP server/service got the IP address 10.217.18.13/22.

1. Show a proof of that SRX-D3 is on the correct sub network.
2. Show a proof of that PC2 is on the correct sub network.
3. Show how to calculate how many theoretically possible usable IPV4 addresses are available on the shown School network, and show the resulting number of IPs.
4. List all theoretically possible usable IPV4 addresses available on the shown School network. Do this in an abbreviated short form.
5. List all theoretically possible usable IPV4 addresses available on the shown myLAN. Do this in an abbreviated short form.

6. A laptop running Windows 10 is connected to the schools wired network has got the following from the DHCP server:

   Ethernet adapter Ethernet:
   Connection-specific DNS Suffix . : eal.local
     IPv4 Address. . . . . : 10.217.17.47
     Subnet Mask . . . . : 255.255.252.0
     Default Gateway . . . . : 10.217.16.1

   Prove that the computer is on the schools wired network 10.217.16.0/22

   Prove that the IPv4 Address 10.217.17.47 is on the right subnet.

7. TBD…

Assignment 32 Source nat on physical SRX

Learning objectives:

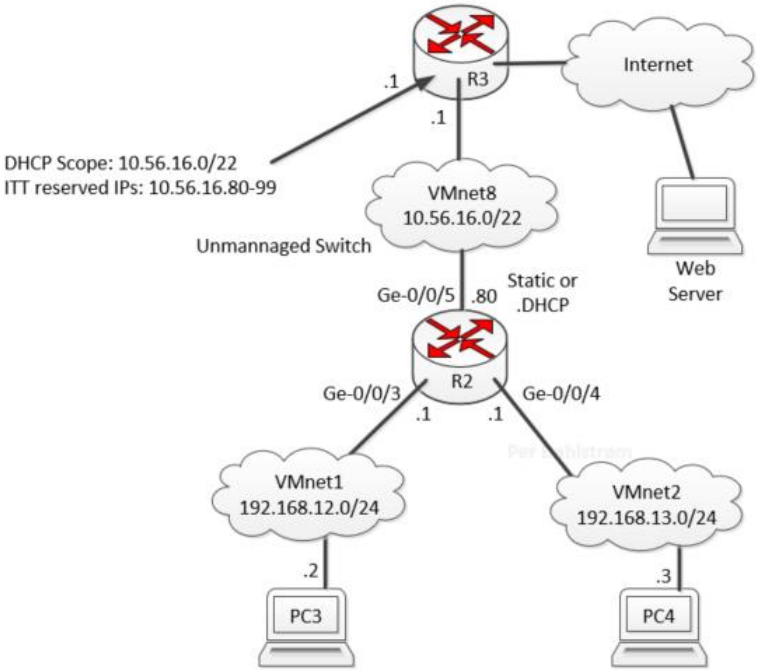
After this assignment, the student can explain:

- [21]Source Natting NAT and default route on a physical router

The student can:

- Set up NAT and default route on a SRX Junos physical router.

Topology



Build a network that allows [22]Source Natting on a SRX router to be set up and tested. A network suggestion is shown above.

For ge-0/0/5 check what IP range is free and can be used on this interface here:

https://gitlab.com/ucl-juniperlab/admin/-/blob/master/ips/dhcp_subnet.md

The IP on ge-0/0/5 has to be outside the DHCP scopes listed.

Before configuring Linux hosts PC3 and PC4, please install Wireshark.

[21] https://rtodto.net/juniper-srx-for-beginners/
[22] https://www.juniper.net/documentation/en_US/junos/topics/topic-map/nat-security-source-and-source-pool.html#id-example-configuring-source-nat-for-egress-interface-translation

Hand in

1. A topology diagram with explanation.

2. Configure default route and NAT on the R2 according to the diagram. The router should provide internet access for all possible hosts on networks 192.168.12.0/24 and 192.168.13.0/24.
   Please note that the 10.56.16.0 is a /22 network and not a /24 network. I.e. the /22 network mask is 255.255.252.0. NOTE the 252!

3. Put the router configuration on GitLab and also the topology diagram. Post a working link here to the configuration and topology. It is obligatory to put relevant comments in the configuration.

4. Demonstrate and explain how these programs can be used for troubleshooting:

   a. **ping**
   b. **traceroute**
   c. **Wireshark**

5. Run Wireshark and the ping command on PC3 or PC4 and show one screenshots/description. Comment on MAC addresses and IP addresses.

6. [23]On the SRX run the command:

   ```
   # show security flow session nat [brief | extensive | summary]
   ```

   a. Only run ping 8.8.8.8 on PC3 and show the SRX output and explain it.
   b. Also run a web browser and browse to e.g. dr.dk and show the SRX output and explain it.

Here is an example output from PC3 web browser to dr.dk:

```
root@R2> show security flow session nat brief
Session ID: 11353, Policy name: internet-access/6, Timeout: 296, Valid
  In: 192.168.12.5/47610 --> 34.107.221.82/80;tcp, If: ge-0/0/3.0, Pkts: 8, Bytes: 636
  Out: 34.107.221.82/80 --> 10.56.16.80/1026;tcp, If: ge-0/0/5.0, Pkts: 6, Bytes: 464
```

[24]The originating or source IP is 192.168.12.2 port 47610 to destination IP 34.107.221.82 port 80. The source IP and port is then to the untrust zone, ge-0/0/5 swapped or translated to originate from 10.56.16.80 port 1026. The destination 34.107.221.82 port 80 is not altered. The source port numbers along with their IP addresses are stored by the SRX, for the SRX to remember what session a possible answer belongs to, i.e. who should receive the answer. This is source Port Address Translation or PAT.

Here is an example output from PC3 pinging 8.8.8.8 which is more tricky to dissect in Wireshark as ping is not using ports:

```
[edit]
root@R2# run show security flow session nat
Session ID: 8543, Policy name: internet-access/6, Timeout: 4, Valid
```

[23] https://rtodto.net/srx-for-beginners-2/
[24] https://www.youtube.com/watch?v=qij5qpHcbBk&ab_channel=CertBros From (03:20) to (05:20)

```
In: 192.168.12.2/5 --> 8.8.8.8/15693;icmp, If: ge-0/0/3.0, Pkts: 1, Bytes: 84
Out: 8.8.8.8/15693 --> 10.56.16.80/1162;icmp, If: ge-0/0/5.0, Pkts: 1, Bytes: 84
```

The originating or source IP is 192.168.12.2 port 5 to destination IP 8.8.8.8 port 15693. This is then to the untrust zone, ge-0/0/5 translated to originate from 10.56.16.80 port 1162 still to destination 8.8.8.8. The port numbers are added by the SRX, for the SRX to remember who should receive the possible answer. This is embedded in ICMP.

Assignment 33 SRX destination nat

Learning objectives:

After this assignment, the student can explain:

- Destination Nat
- Trust and Untrust zones on a SRX router.
- WebServer access from the schools wired network.
- SOHO

The student can:

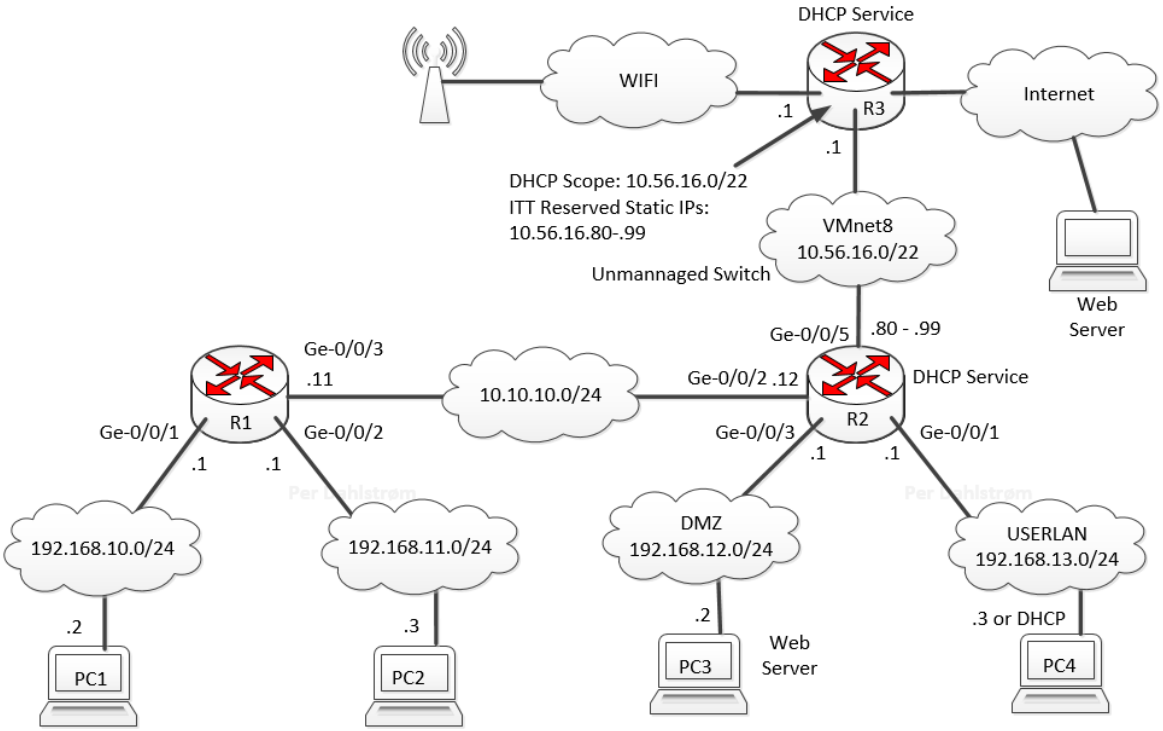
- Set up Destination Nat

Sources

[25]Juniper source on destination nat.

Topology and task

The network diagram below is a high-level diagram with some, but not all, details. Build the network in VMware Workstation. The task is to make the Web Server on PC3 reachable from the 10.56.16.0/22 network.



[25] https://www.juniper.net/documentation/en_US/junos12.1/topics/example/nat-security-destination-address-port-translation-configuring.html

Hand in

Use the checklist for hand in requirements in the beginning of this document before handing in.

Build the network in VMware Workstation.

1. A topology diagram with 10 lines of explanation. Show what interfaces are in trust, untrust and DMZ zones.

2. Briefly explain and show how to install the Webserver on PC3 which should be a Raspberry Pi or a Xubuntu.

3. Briefly explain what Destination NAT is. Maximum 5 lines.

4. Put the router configuration as a .json file and the topology diagram as a .pdf in the same folder on GitLab and put a link to the configuration and diagram in the hand in.

Assignment 34 SRX L2 switch and SOHO

Learning objectives:

After this assignment, the student can explain:

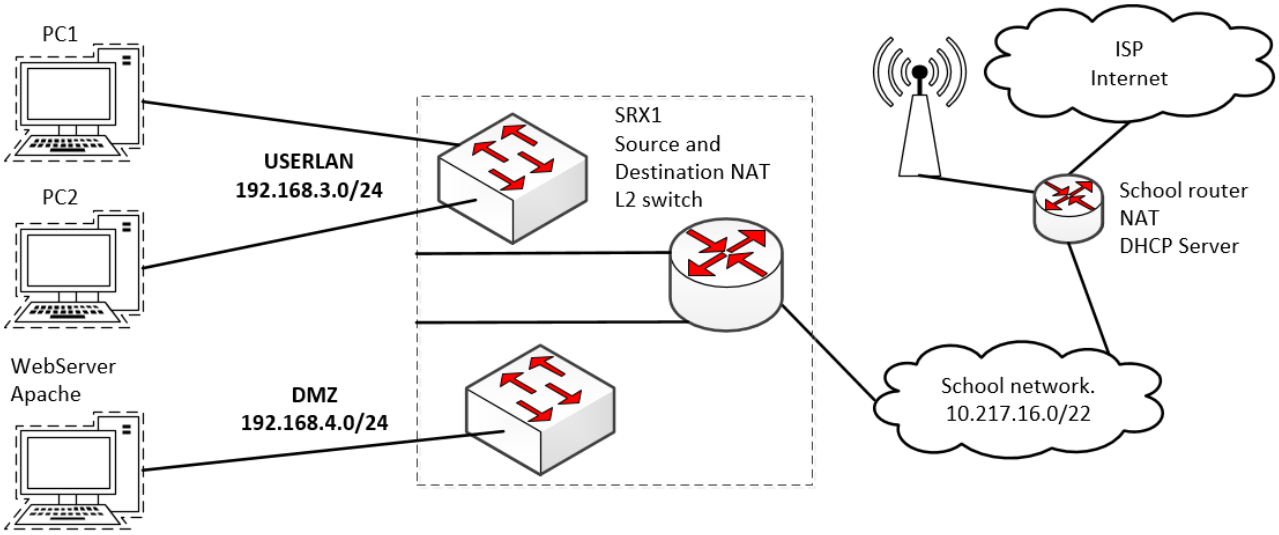
- One type of L2 switching on a SRX router

The student can:

- Set up one type of L2 switching on a SRX router
- In general, do basic configuration of SRX for SOHO use.

Topology

The network diagram below is a high-level diagram with few details.



See this juniper source[26] and this [27]O´reilly source in the Switching Configuration section.

Hand in

Use the checklist for hand in requirements in the beginning of this document before handing in.

1. A topology diagram with explanation. Show what interfaces are in trust, untrust and DMZ zones.

2. A Low Level Design.

3. A filled out test plan.

4. Put the router configuration as .json and the topology diagram as a .pdf in the same folder on GitLab and put a link to the configuration and diagram in the hand in.

[26] https://www.juniper.net/documentation/en_US/junos/topics/example/layer-2-switching-mode-security-configuring.html
[27] https://www.oreilly.com/library/view/juniper-srx-series/9781449339029/ch04.html

Assignment 35 SRX port mirroring

Learning objectives:

After this assignment, the student can explain:

- What port mirroring is and why it sometimes is necessary.

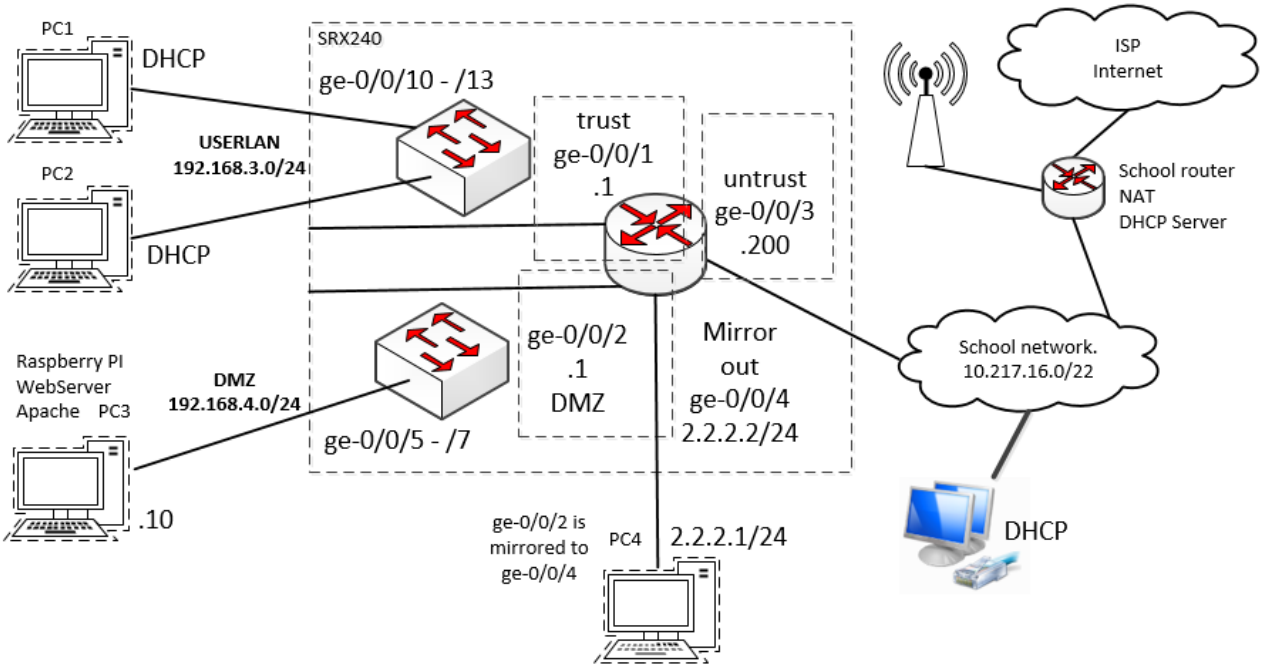
The student can:

- Set up one port mirroring on a SRX router
- Set up a networking device to do basic network traffic analysis on a mirror output port.
- Set up Wireshark as basic analysing tool for networking traffic.

Topology

The network diagram below is a high-level diagram with quite a few details. It is not required to follow the diagrams stated interfaces and addresses, but if this is not the case a new diagram must obviously illustrate the applied topology.

A copy of the traffic that that comes into or goes out of the ge-0/0/2 DMZ interface is sent to the monitoring PC4 from the ge-0/0/4 interface where it is captured and analysed.



Please consult this source[28] for instructions on how to set up a mirror port.

Hand in

1. A topology diagram with explanation. Show what interfaces are in trust, untrust and DMZ zones.

[28] https://kb.juniper.net/InfoCenter/index?page=content&id=KB21833&cat=SRX_240&actp=LIST

2. A Low Level Design.

3. Briefly explain and show how to install and run the monitoring PC4.

4. A filled out test plan.

5. Put the router configuration as .json and the topology diagram as a .pdf in the same folder on GitLab and put a link to the configuration and diagram in the hand in.

Assignment 36 SRX Simple VLANs

Learning objectives: Routing Traffic Between VLAN s

After this assignment, the student can explain:

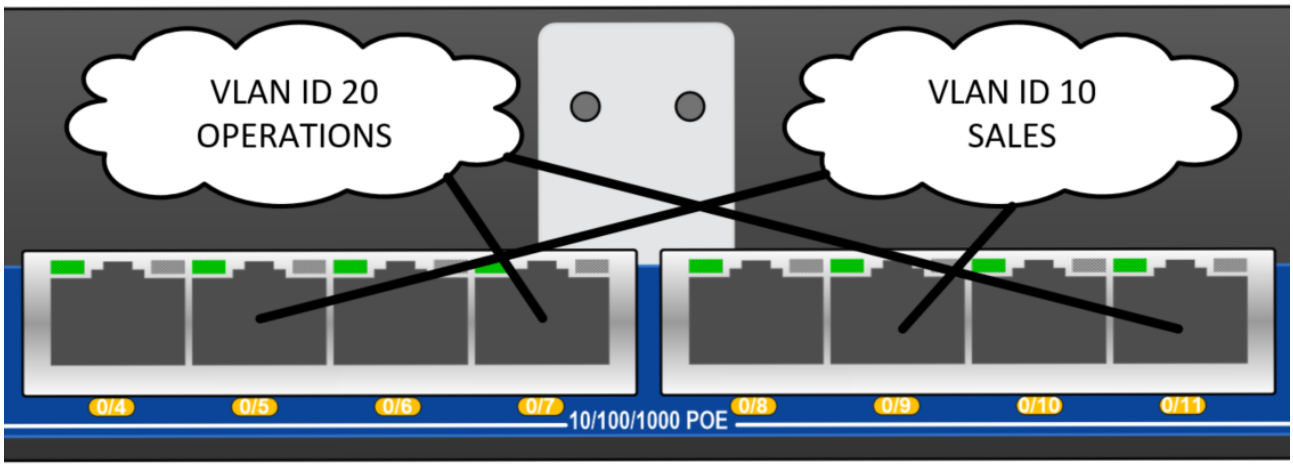
- What a VLAN is.

The student can:

- Set up simple VLANs on Juniper SRX router.
- Test simple VLANs on Juniper SRX router.

Topology

The network diagram below is a high-level diagram of the intended VLANs. The diagram is just a suggestion and minimum requirement. More interfaces and VLANs can be implemented and other names and VLAN IDs can be used. These changes must of course be thoroughly documented in the hand in.



Hand in

1. A HLD with explanation. The HLD must include devices used for testing and referenced in the testplan.

2. A Low Level Design. The LLD must reference the devices shown in the HLD.

3. A filled out test plan. The test plan must reference the devices shown in the HLD. All referenced devices must be uniquely and easily humanly identifiable. ☺

Put the router configuration as .json and the HLD as a .pdf in the same folder on GitLab and put a link to the configuration and diagram in the hand in.

Assignment 37 SRX Routing Traffic Between VLANs

Learning objectives:

After this assignment, the student can explain:

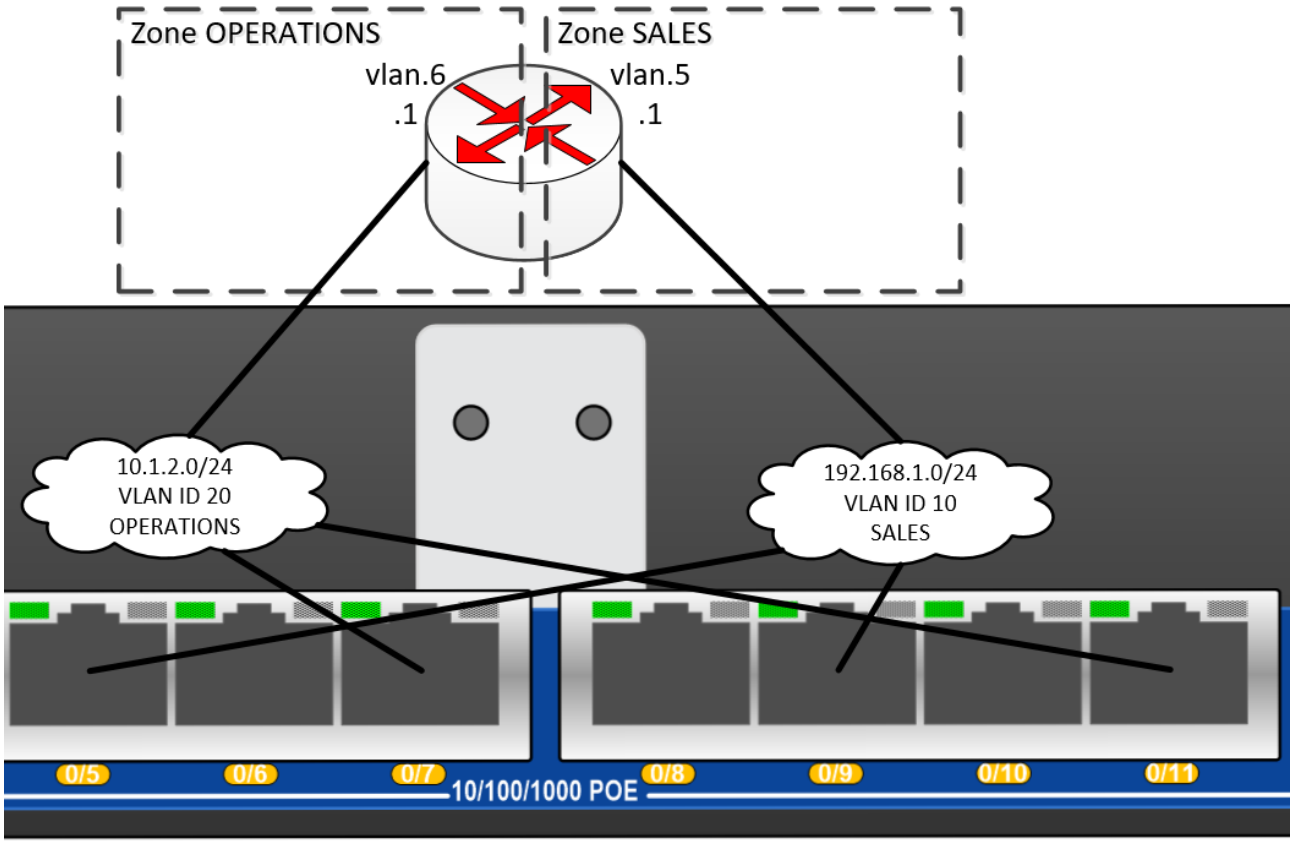
- What Routing Traffic Between VLANs means.

The student can:

- Set up simple VLANs on Juniper SRX router with Routing Traffic Between VLANs.
- Test simple VLANs on Juniper SRX router with Routing Between VLANs.

Topology

The HLD/Illustration below illustrates the possible zones that can be defined. The two virtual interfaces vlan.5 and vlan.6 have been assigned to the SALES and OPERATIONS zones respectively. The diagram is just a suggestion and minimum requirement. More interfaces and VLANs can be implemented and other names and VLAN IDs can be used. These changes must of course be thoroughly documented in the hand in.



Hand in

1. A HLD with explanation. The HLD must include devices used for testing and referenced in the test plan.

2. A Low Level Design. The LLD must reference the devices shown in the HLD.

3. Show and explain the routers routing table. Hint: **`show route terse`**

4. A filled out test plan. The test plan must reference the devices shown in the HLD. All referenced devices must be uniquely and easily humanly identifiable. ☺

5. Try out and explain the following commands:
    a. **`show ethernet-switching interfaces`**
    b. **`show ethernet-switching table`**
    c. **`show ethernet-switching mac-learning-log`**

Put the router configuration as .json and the HLD as a .pdf in the same folder on GitLab and put a link to the configuration and diagram in the hand in.

Assignment 38 SRX Tagged Interfaces and 802.1q trunk traffic

Learning objectives:

After this assignment, the student can explain:

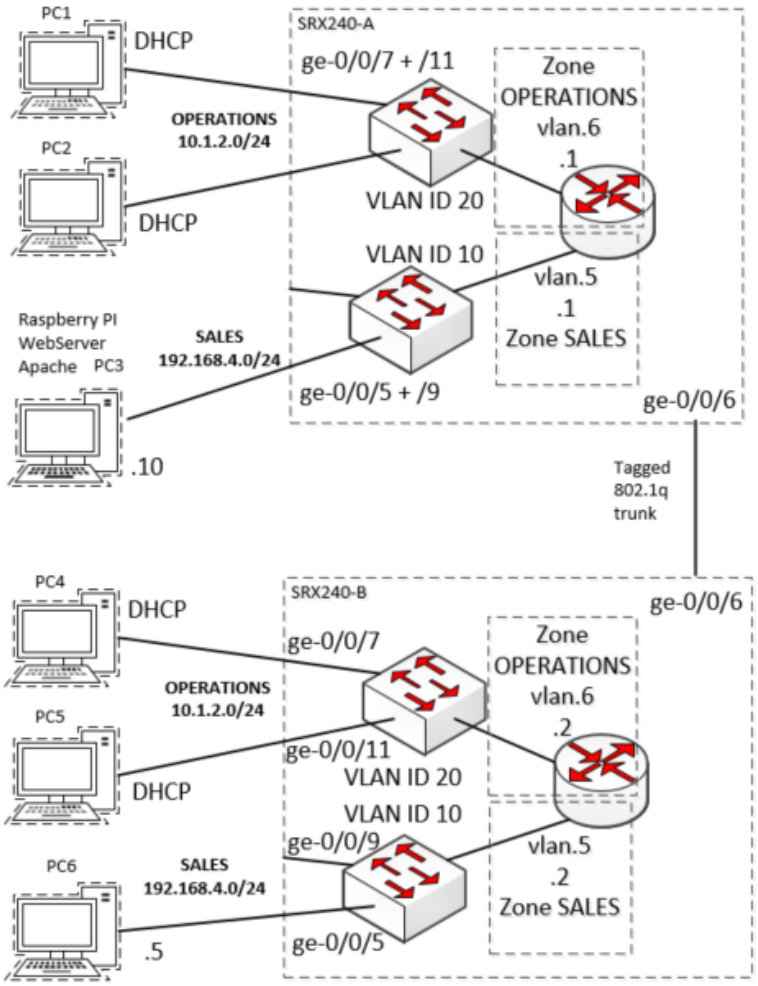
- What tagged and untagged Ethernet packets means.

The student can:

- Set up a working 802.1q trunk connection directly between two Junos networking devices.
- Test a 802.1q trunk connection between two Junos networking devices.

Topology

The HLD/Illustration below illustrates the possible interconnection between two SRX routers. VLANs can be implemented and other names and VLAN IDs can be used. These changes must of course be thoroughly documented in the hand in.



Hand in

1. A HLD with explanation. The HLD must include devices used for testing and referenced in the test plan.

2. An inventory of used devices. The bullet point list must facilitate replication of the achieved results.

3. A Low Level Design. The LLD must reference the devices shown in the HLD.

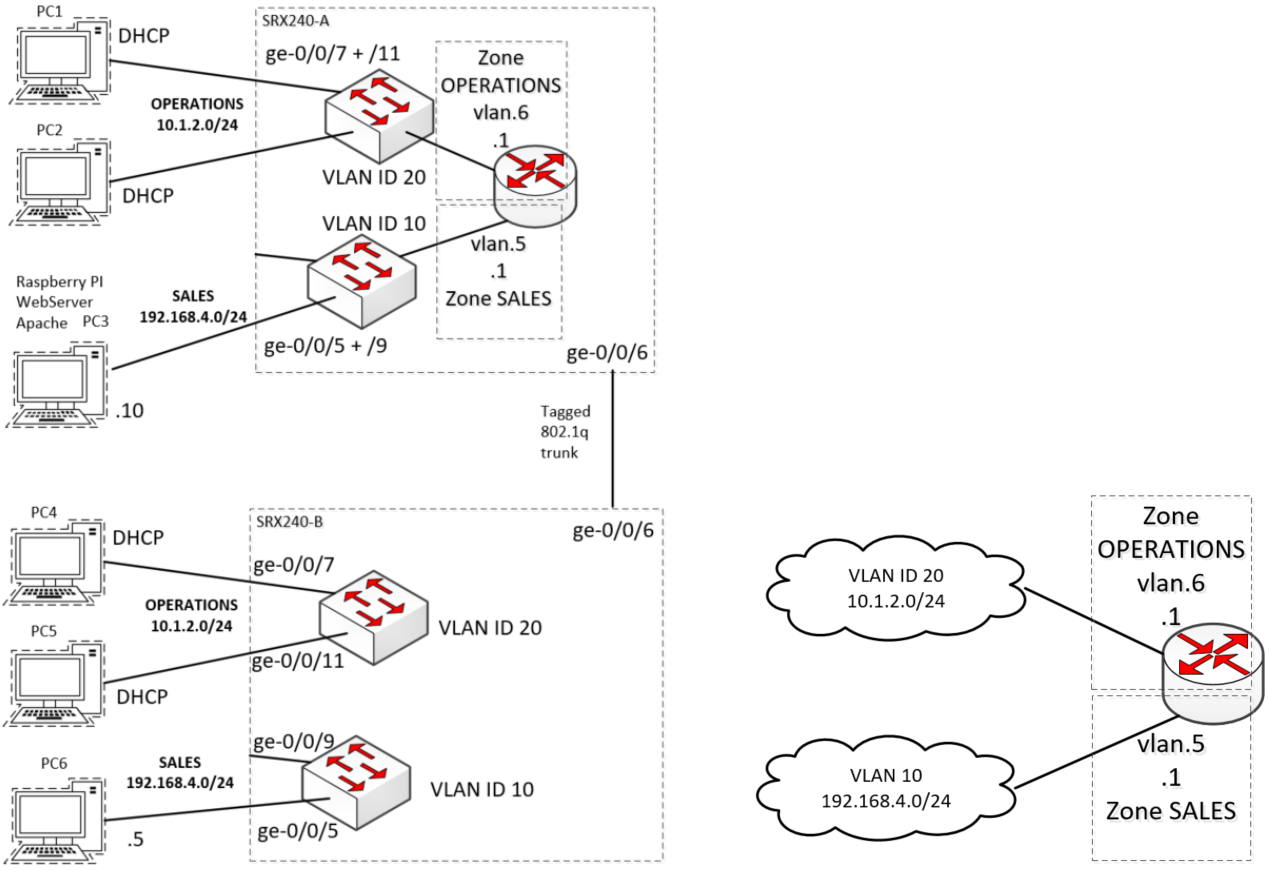
4. Show explicitly on the HLD diagram for all network connections where traffic is tagged and untagged.

5. Support the claim in item 2 by "gauging" on the wires e.g. by means of Wireshark, and show how it is seen that the traffic is tagged and not tagged.

6. A filled out test plan. The test plan must reference the devices shown in the HLD. All referenced devices must be uniquely and easily humanly identifiable. ☺

Put the router configurations as .json files and the HLD as a .pdf in the same folder on GitLab and put a link to the configurations and diagram in the hand in.

Here is an alternative topology/block diagram, which only holds one router functionality, which probably is how the network in most cases will have to be set up. On the right hand side is shown the layer 2 and layer 3 logic topology, which is important for a conceptual understanding. The hosts/PCs are omitted in this drawing. Students should complete the diagram with hosts.



Assignment 39 SRX Link Aggregation

Learning objectives:

After this assignment, the student can explain:

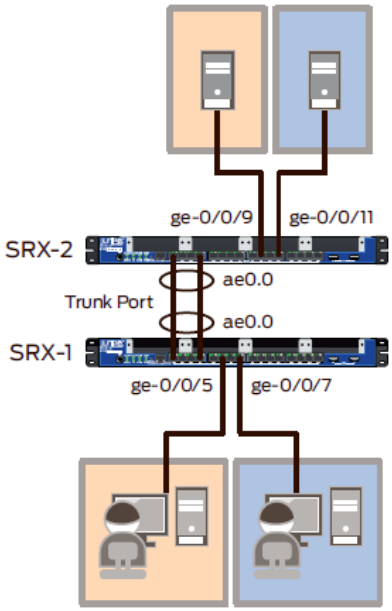
- What link aggregation means [29] + [30].
- What advantages link aggregation have over non aggregated links.

The student can:

- Set up a working link aggregated dot1q connection directly between two Junos networking devices.
- Test link aggregated dot1q connection between two Junos networking devices.

Topology

The HLD/Illustration below illustrates the possible interconnection between two SRX routers. VLANs can be implemented and other names and VLAN IDs can be used. These changes must of course be thoroughly documented in the hand in.



Hand in

1. A HLD with explanation. The HLD must include devices used for testing and referenced in the test plan.

2. An inventory of used devices. The bullet point list must facilitate replication of the achieved results.

3. A Low Level Design. The LLD must reference the devices shown in the HLD.

[29] https://www.juniper.net/documentation/en_US/junos/topics/concept/interfaces-lag-overview.html
[30] Juniper SRX Branch Router Switching.pdf page 11.

4. Show explicitly on the HLD diagram for all network connections where traffic is tagged and untagged.

5. Support the claim in item 4 by "gauging" on the wires e.g. by means of Wireshark, and show how it is seen that the traffic is tagged and not tagged.

6. A filled out test plan. The test plan must reference the devices shown in the HLD. All referenced devices must be uniquely and easily humanly identifiable. ☺
    a. Test that it doesn't matter which of the aggregated links is interrupted, the remaining links will uphold the interconnection.
    b. Test if switching cables matters.
    c. Test anything else relevant.

    Make very brief conclusions for each test.

7. Challenge:
    Give internet access to the "blue" vlan users.
    Document the system.

Put the router configurations as .json files and the HLD as a .pdf in the same folder on GitLab and put a link to the configurations and diagram in the hand in.

Assignment 40 Loop avoidance with RSTP

Learning objectives:

After this assignment, the student can explain[31]:

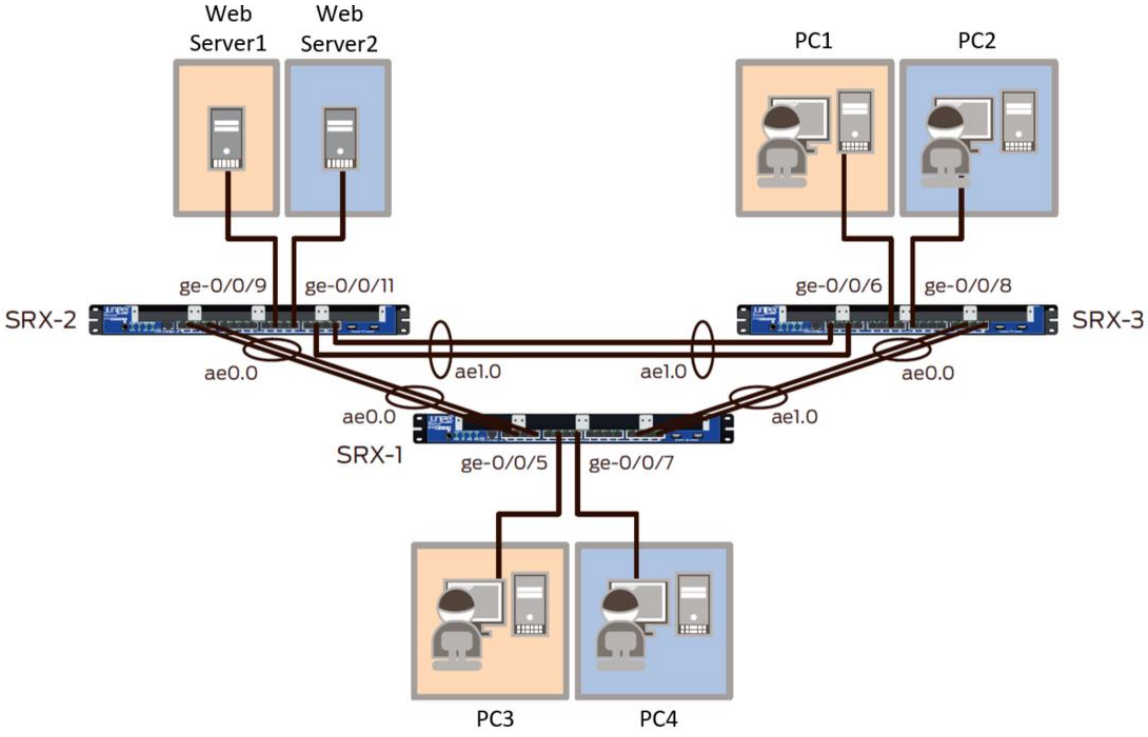
- What a closed loop is and what problems it can cause.
- What STP and RSTP and MSTP are.
- How STP alleviates the problems in loops..

The student can:

- Set up a number of layer two connections in a loop and demonstrate that a loop has problems.
- Implement and test that STP prevents loop problems.

Topology

The HLD/Illustration below illustrates the possible interconnection between three SRX´s. A web server must be introduced on at a minimum one vlan to test connectivity.



Hand in

1. A HLD with explanation. The HLD must include devices used for testing and referenced in the test plan.

2. An inventory of used devices. The bullet point list must facilitate replication of the achieved results.

[31]Juniper SRX Branch Router Switching.pdf pages 13, 14 and 15.

3. A Low Level Design. The LLD must reference the devices shown in the HLD.

4. Show and comment on Interfaces and routing tables in/on the SRX.

5. A filled out test plan. The test plan must reference the devices shown in the HLD. All referenced devices must be uniquely and easily humanly identifiable. ☺
    a. Test "connection" from e.g. PC3 to web server 1 without and with STP.
    b. Monitor the traffic on dot1q lines with STP off and on.
    c. Test that it doesn't matter which of the aggregated links is interrupted, the remaining links will uphold the interconnection.
    d. Test if switching cables matters.
    e. Test anything else relevant.

    Make very brief conclusions for each test.

6. Explain what "convergence time" means when using STP.

7. Challenge: Give internet access to the "blue" vlan users.

Put the router configurations as .json files and the HLD as a .pdf in the same folder on GitLab and put a link to the configurations and diagram in the hand in.

Assignment 41 RADIUS AAA server

Learning objectives: After this assignment, the student can explain:

- What AAA is.
- What a RADIUS server is[32]. (Remote Authentication Dial In User Service).
- Benefits of and when to use a Network Access Server NAS/Remote Access Server RAS.
- Optional: The use of a Relational Database with Radius authentication server

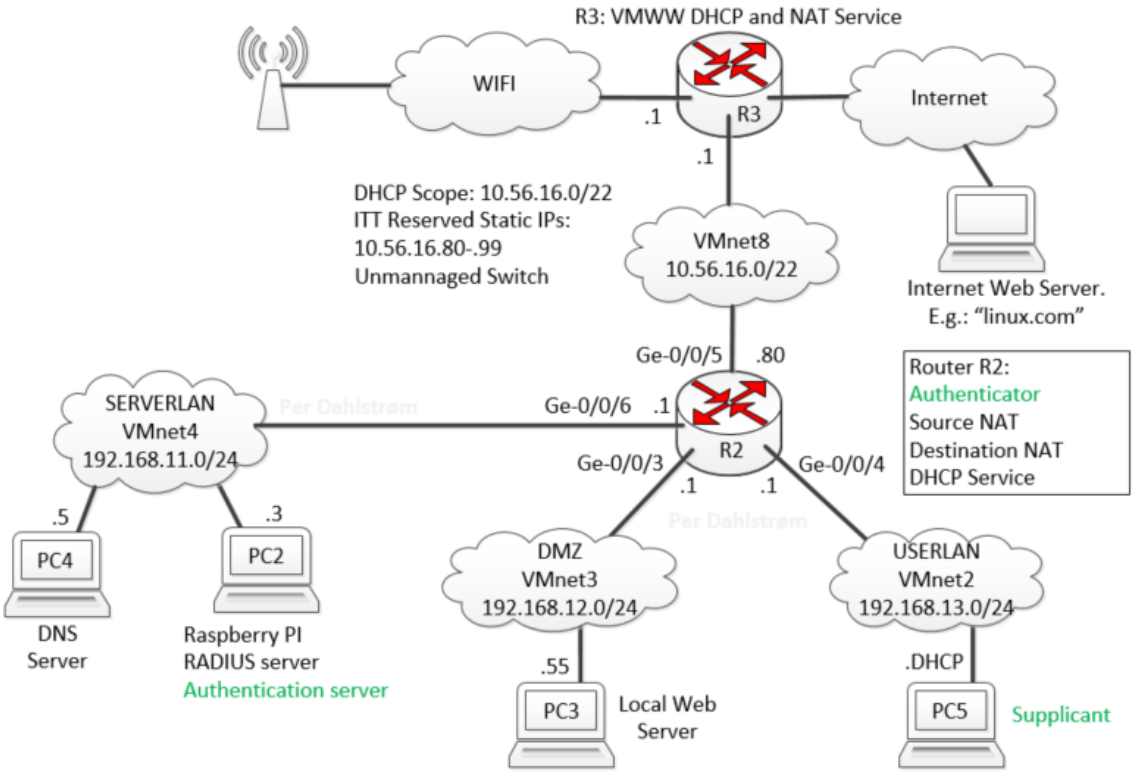
The student can:

- Set up a FreeRADIUS server on Linux and configure it for authentication.
- Set up e.g. a SRX240 for user authentication from a Radius server.
- Optional: Set up a Relational Database with Radius authentication server.
- Optional: Set up e.g. a SRX240 for 802.1X user authentication from a Radius server.

Task:

1. Set up a network with a [33]Radius server PC2 on e.g a Raspberry Pi and configure a[34] SRX R2 for authenticating the SSH user/suplicant of the SRX240 from the Radius server.
2. Set up a Relational Database with Radius authentication server PC2.
3. Set up a network with a Radius server on e.g a Raspberry Pi and configure a SRX for authenticating the PC5 user/suplicant onto the SERVERLAN (VLAN) from the Radius server.

Here is a setup suggestion:



[32] https://www.tutorialspoint.com/radius/index.htm
[33] https://wiki.freeradius.org/guide/Getting-Started
[34] https://kb.juniper.net/InfoCenter/index?page=content&id=KB16607&actp=METADATA

Hand in

1. One or two HLDs with explanation. The HLD must include devices used for testing and referenced in the optional test plan. HLD and Configurations must also be linked to on GitLab.

2. An inventory of used devices. The bullet point list must facilitate replication of the achieved results.

3. A Low Level Design. The LLD must reference the devices shown in the HLD.

4. Radius configuration with comments. Use FreeRADIUS for Linux.

5. SRX configuration with comments.

6. Optional: Show how to install and set up the SQLite database.

7. Optional: Demonstrate that users can be administered from or in the database.

8. Optional: Wireshark communication between Supplicant and Authenticator and between Authenticator and Authentication Server. Comment on the authentication relevant protocols observed. Where is 802.1x and RADIUS and others.

9. Optional: A filled out test plan. The test plan must reference the devices shown in the HLD. All referenced devices must be uniquely and easily humanly identifiable. ☺

Assignment 42 DNS server

Learning objectives: After this assignment, the student can explain:

- What DNS is.
- What a DNS server is.
- Benefits of and when to use a local DNS server.

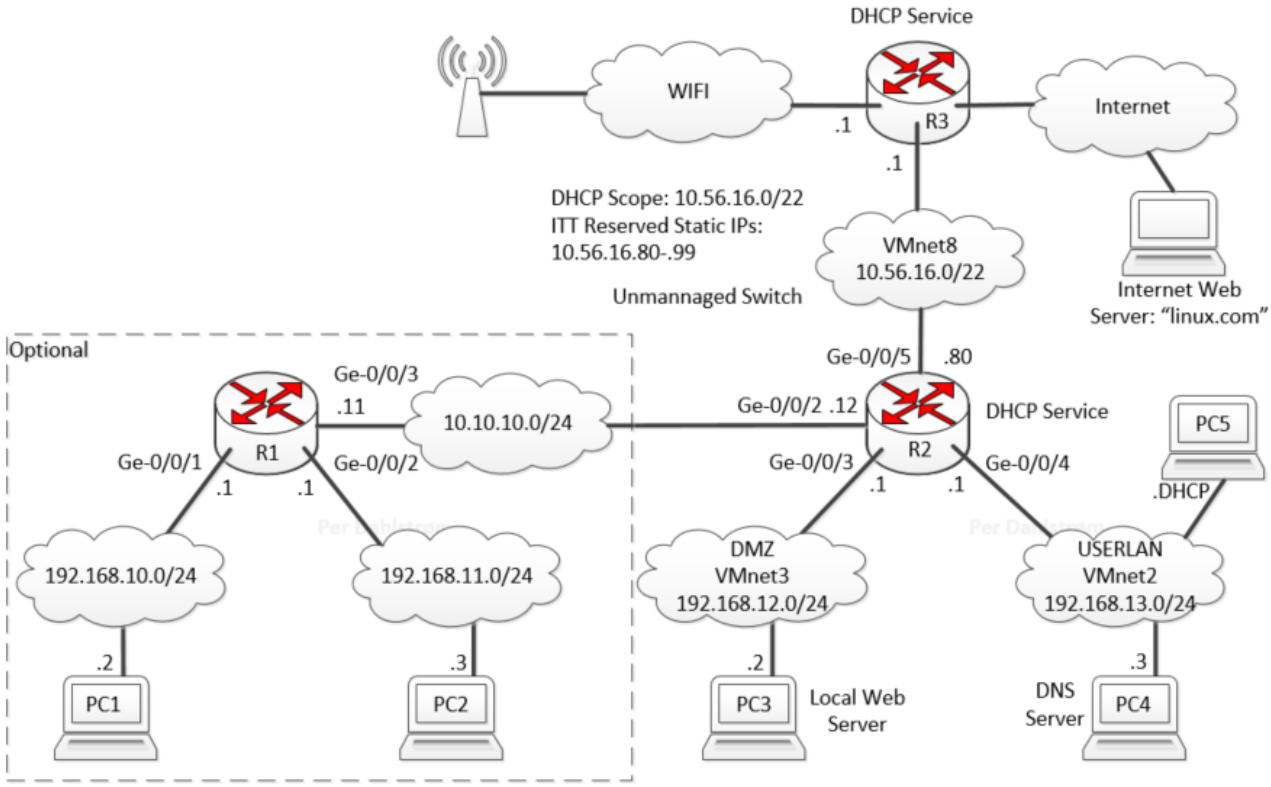
The student can:

- Set up a DNSmasq DNS server on Linux and configure it[35].
- Set up e.g. a SRX240 to do DHCP including the DNSmasq DNS server.

Task:

1. Set up a network with a DNSmasq DNS server on e.g a Raspberry Pi and configure a SRX with DHCP including handing out the IP of the DNS server.

Here is a setup suggestion:



Task continued:

All devices connected to USERLAN, like e.g. PC5, must receive DHCP from the SRX R2 and thus be informed by DHCP that the Raspberry Pi DNS server PC4 is the primary DNS server. Devices on USERLAN must be able to reach the Raspberry Pi Local Web Server PC3 Web Site "awesome.dk" by that domain name. Devices on the USERLAN must be able to reach e.g. the Web Site "linux.com" by that domain name on the internet.

[35] https://wiki.debian.org/HowTo/dnsmasq

Hint: Use the **`dig`**[36] command for testing.

Hand in

1. One HLDs with explanation. HLD and Configurations must also be linked to on GitLab.

2. An inventory of used devices and software. The bullet point list must facilitate replication of the achieved results.

3. DNSmasq[37] configuration with comments.

4. SRX configuration with comments only on DNS relevant part of configuration.
   Include a working link to the full configuration on GitLab.

5. DNS client's DNS relevant configuration. E.g. those clients on the USERLAN.

6. Wireshark DNS communication between DNS clients and server. Show different scenarios. E.g. local Web server access and remote Web server access.

[36] https://www.thegeekstuff.com/2012/02/dig-command-examples/
[37] https://wiki.debian.org/HowTo/dnsmasq

Assignment 43 Wireless Lan Controller WLC

Learning objectives: After this assignment, the student can explain:

- What a WLC is.
- What WiFi is and how it works.
- How to design a WiFi layout for a SOHO or SMB (Small to Medium sized Business.)
- Basics of central protocols used by WLCs and Access Points APs.

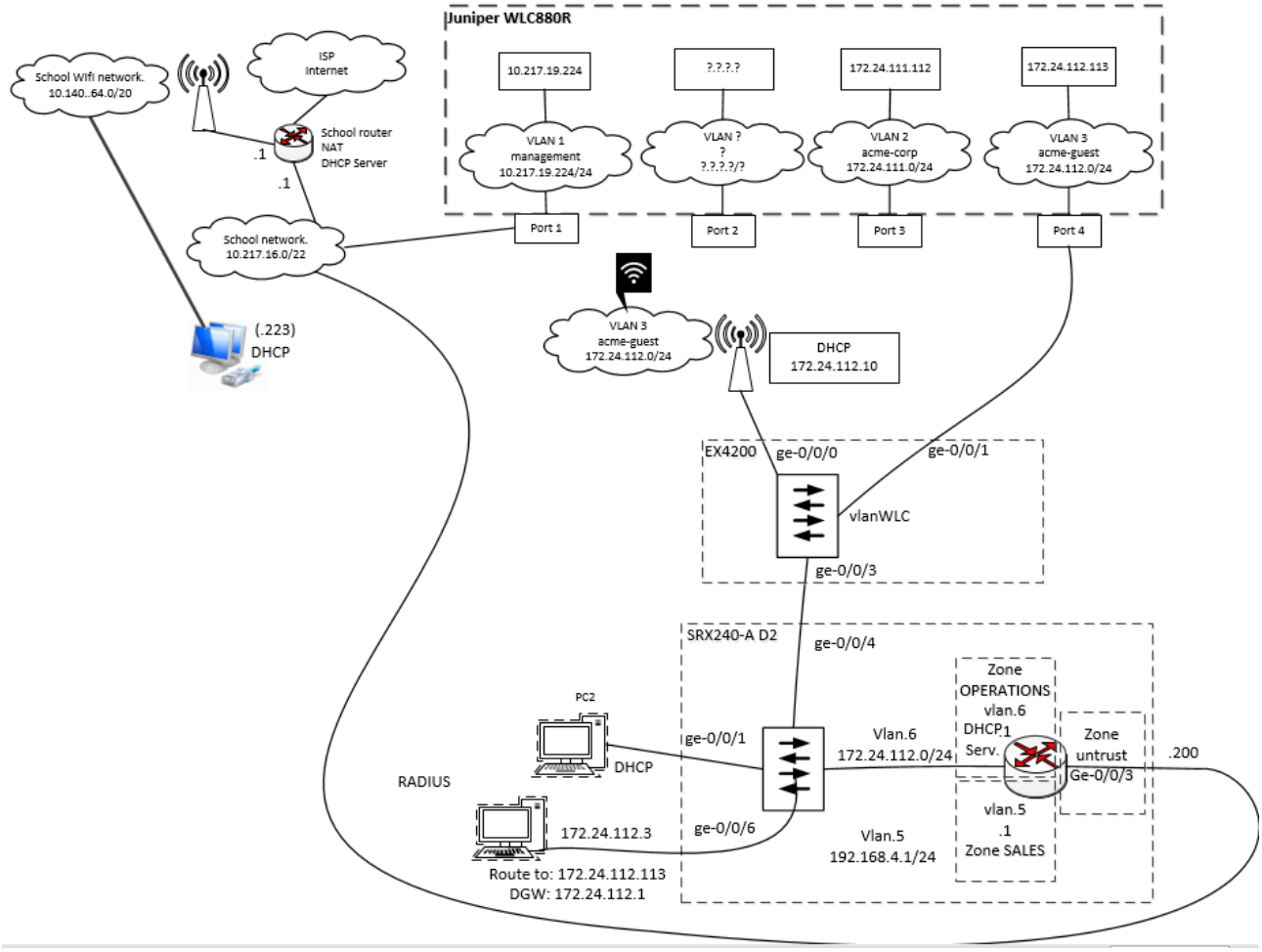
The student can:

- Set up a WLC and configure it with RADIUS user authentication of WiFi users.

Task:

1. Set up a WiFi network centrally administered by a WLC with a number of associated AP´s.
2. Set up RADIUS to authenticate WiFi users.
3. Optional: Ad user rights to RADIUS.

Here is shown a setup suggestion. The EX4200 is only there to provide POE as the SRX240 branch series does not provide it.



Hand in one PDF on Peer Grade

1. One HLDs with explanation. The HLD must include devices used for testing and referenced in the test plan. HLD and Configurations must also be linked to on GitLab.

2. An inventory of used devices. The bullet point list must facilitate replication of the achieved results.

3. A one page introduction to WiFi, WLC and WAPs.
   Suggestions:
   a. AP layout basics.
   b. AP frequencies and channels.
   c. The protocol(s) between WLC and Aps.

4. A Low Level Design. The LLD must reference the devices shown in the HLD.

5. A brief step by step guide to setting up a WLC and APs.

6. Filled out test plan.

7. Show by means of Wireshark and comment on the CAPWAP channel between the WLC and the AP´s.

8. A list of used sources or alternatively, the sources are put as footnotes where they are used for the first time in the text.

Assignment 44 OSPF and Virtual Routers on switch

Learning objectives: After this assignment, the student can explain:

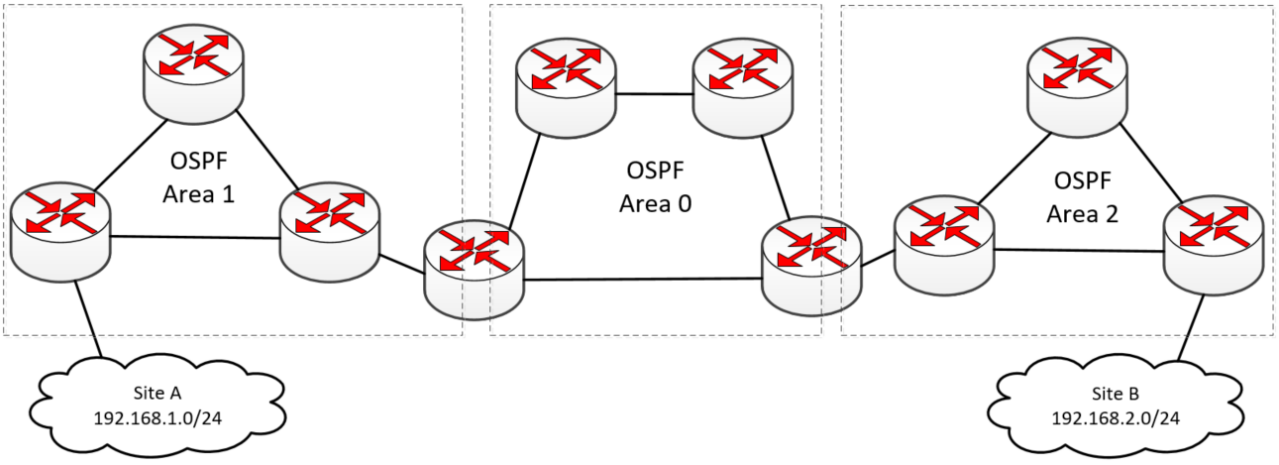
- What a Virtual Router VR is.
- When to use virtual routers.
- What OSPF is. [38]See this source on OSPF. And this on multi area OSPF[39].
- How to configure a basic OSPF network[40].

The student can:

- Configure Virtual Routers on EX4200 JunOS switch.
- Configure a basic OSPF network[41].

Task:

1. Set up an OSPF network. Area 0 must be constituted by virtual routers on an EX4200 switch. A WebSite on a server host on Site A must be reachable from client host on Site B.
2. Optional: Clients on Site A and Site B must have internet access.



Hand in one PDF on Peer Grade

1. One HLDs with explanation. The HLD must include devices used for testing and referenced in the test plan. HLD and Configurations must also be linked to on GitLab.

2. An inventory of used devices. The bullet point list must facilitate replication of the achieved results.

3. A Low Level Design. The LLD must reference the devices shown in the HLD.

4. A one page introduction to OSPF.

[38] https://www.youtube.com/watch?v=kfvJ8QVJscc&t=728s
[39] https://www.youtube.com/watch?v=PIMnj2oqYIo
[40] https://www.juniper.net/documentation/en_US/junos/topics/concept/ospf-configuration-overview.html
[41] https://www.juniper.net/documentation/en_US/junos/topics/concept/ospf-configuration-overview.html

5. A Low Level Design. The LLD must reference the devices shown in the HLD.

6. A brief step by step guide to setting up OSPF and clients according to the HLD.

7. Filled out test plan.

8. A list of used sources or alternatively, the sources are put as footnotes where they are used for the first time in the text.

9. Challenge:
   Site A and Site B both have the Network ID: 192.168.1.0/24

10. Challenge:
    Give internet access to both Site A and Site B.

Assignment 45 Virtual Private Network VPN

Learning objectives: After this assignment, the student can explain:

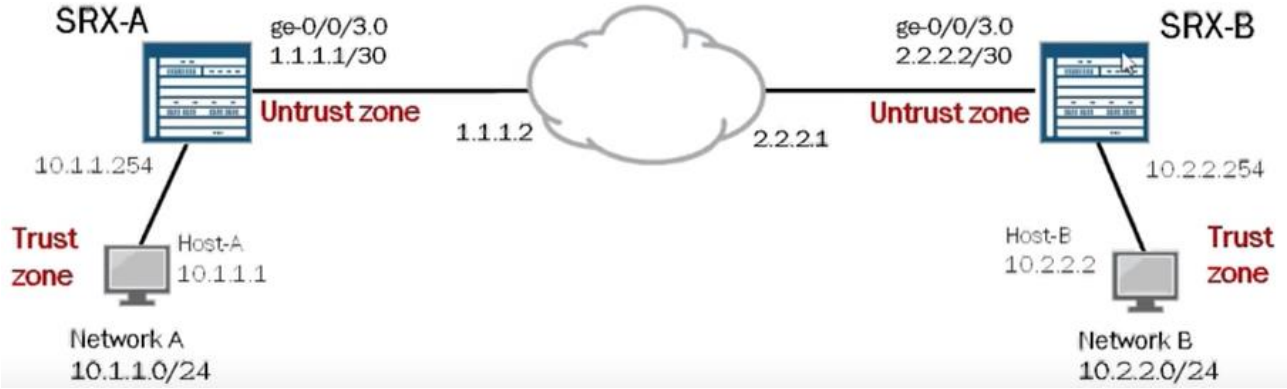
- What VPN is.
- What Routed VPN is.
- When to use Routed VPN.

The student can:

- [42]Set up a VPN between two sites.
- Challenge: Set up a VPN between three sites.

Task:

1. Set up a routed VPN.
   The topology here is a suggestion. It will take a bit of reworking for this assignment.
   As indicated two SRXés can be used for setting up this routed VPN.



Hand in one PDF on Peer Grade

1. One HLDs with explanation. The HLD must include devices used for testing and referenced in the test plan. HLD and Configurations must also be linked to on GitLab.

2. An inventory of used devices. The bullet point list must facilitate replication of the achieved results.

3. A Low Level Design. The LLD must reference the devices shown in the HLD.

4. A brief step by step guide to setting up routed VPN and clients according to the HLD.

5. Filled out test plan.

6. Show by means of Wireshark and comment on the VPN channel between the SRXés.

7. A list of used sources or alternatively, the sources are put as footnotes where they are used for the first time in the text.

[42] https://www.youtube.com/watch?v=4fhLZIbJ-ls

Assignment 46 Backup, disaster and recovery plan.

Learning objectives: After this assignment, the student can explain:

- Backup, disaster and recovery plan.

The student can:

- Work out a backup, disaster and recovery plan.
- Implement backup for a given network.
- Do a full disaster recovery of a given network.

Tasks

1. Elaborate a backup, disaster and recovery plan for a given network.
    - The plan must be detailed to such an extent that a peer class team will be able to do a disaster recovery of the given network.
2. Implement backup for a given network according to the plan in item 1.
3. Demonstrate a full disaster recovery according to the plan in item 1. for the given network.
4. It is compulsory as part of the backup setup to configure a ssh server to receive Junos SRX configurations and to configure the Junos SRX to do automated transmission of configuration on each commit to the ssh server.
    -

Hand in on PeerGrade:

1. The backup, disaster and recovery plan for a given network.
2. Notes and tips to the implementation of the backup according to the plan.
3. Notes and tips to a full disaster recovery of the given network.
4. Document how to set up a ssh server for Junos configurations and how to configure the SRX for backing up configuration on each commit.
   Document the backup is working.

Assignment 47 NTP server

Learning objectives: After this assignment, the student can explain:

- What NTP is.
- What a NTP server is.
- Benefits of and when to use a local NTP server.

The student can:

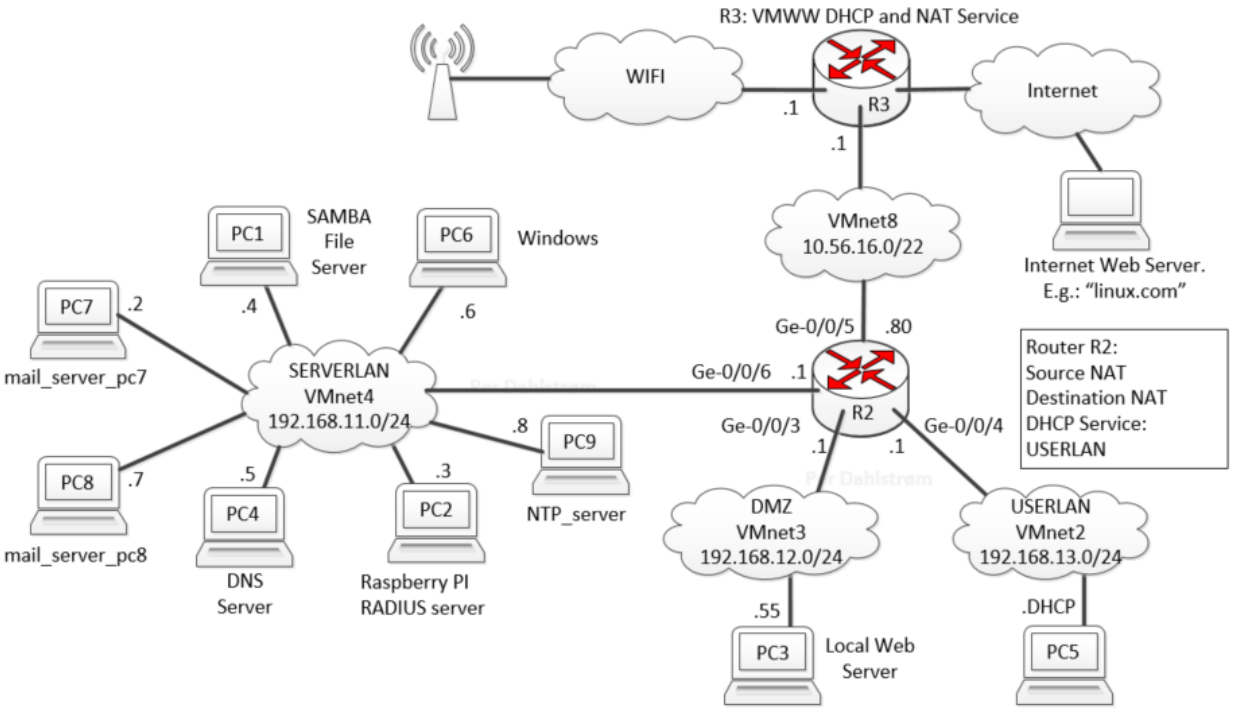
- Set up a NTP server on Linux and configure it[43].
- Set up e.g. a SRX240, Windows and Linux to do NTP.

Task:

Set up a network with a NTP server on e.g a Raspberry Pi and configure Windows, Linux and e.g. SRX240 as NTP clients.

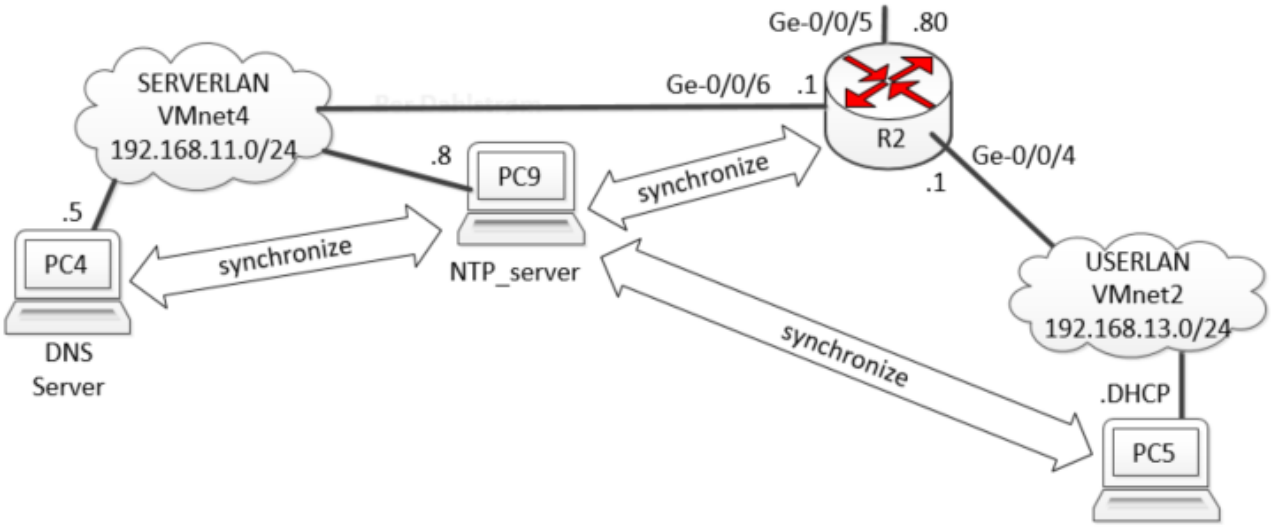
Here is a setup suggestion:

In the context of this assignment, PC9 is the NTP server, PC6 is a Windows NTP client, R2 and PC5 are NTP clients. In general, all local devices should be NTP clients.



[43] https://wiki.debian.org/HowTo/dnsmasq

And here is an extract of the diagram. The Windows PC is missing. Note that the Windows PC can also be the VMWW host Windows participating on VMnet4.



Task continued:

The NTP server needs continuous internet access, so source natting must be running on R2.

Hand in

1. One HLDs with explanation. HLD and Configurations must also be linked to on GitLab.
2. An inventory of used devices and software. The bullet point list must facilitate replication of the achieved results.
3. Proof that PC5 does synchronisation with the NTP PC9 server.
4. Proof that R2 does synchronisation with the NTP PC9 server.
5. Proof that Windows does synchronisation with the NTP PC9 server.
6. Wireshark NTP communication between NTP clients and server.

Assignment 48 SAMBA files sharing server

Learning objectives: After this assignment, the student can explain:

- At a high level, what the Server Message Block SMB protocol is and why it was created.
- What SAMBA is. A: It is a program that will run SMB on a Linux OS.
- Benefits of and when to use a local file sharing server.

The student can:

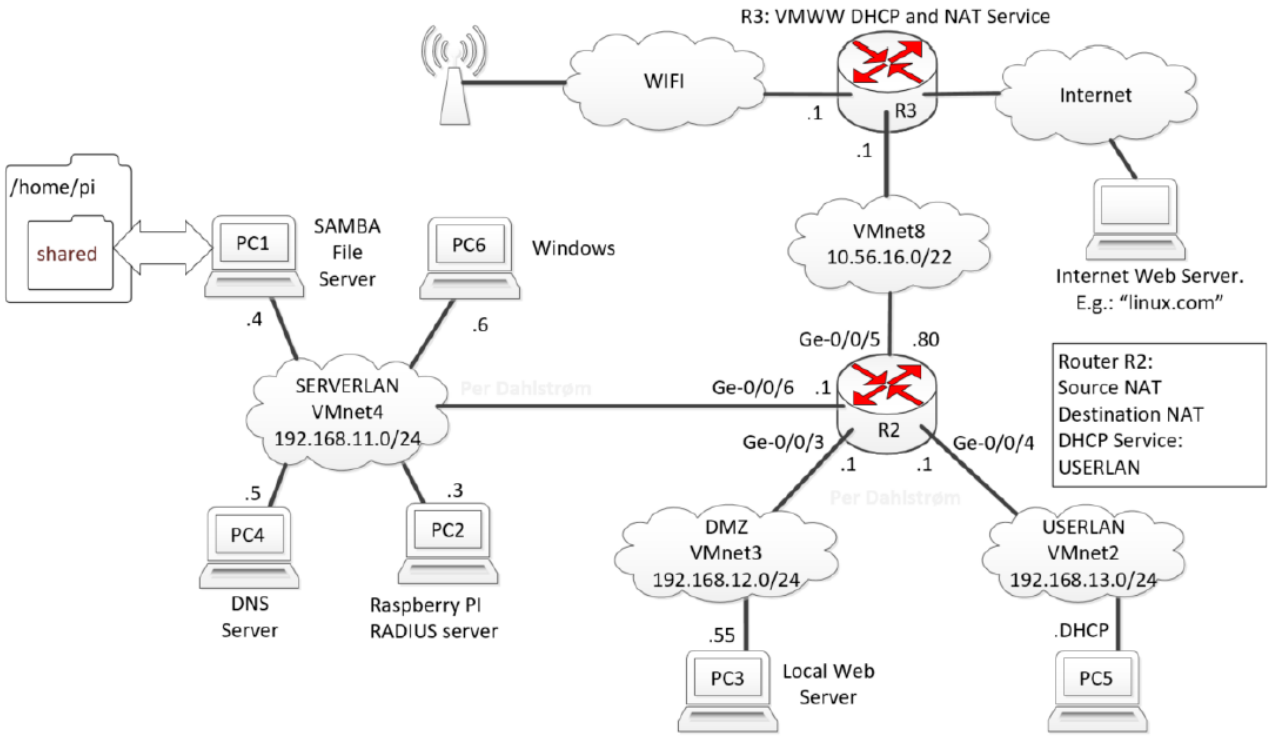
- Set up a SAMBA file sharing server on Linux and configure it[44].
- Set up e.g. a Windows and Linux clients to do access common files on a SAMBA file sharing server.

Task:

Set up a network with a SAMBA server on e.g a Raspberry Pi and configure a Windows device and a Linux device as file sharing clients.

Here is a setup suggestion:

In the context of this assignment, PC1 is the SAMBA server, PC6 is a Windows file sharing client, and PC5 is a Linux file sharing client. In general, all local devices could be SAMBA clients if they are capable of running SMB.



[44] https://pimylifeup.com/raspberry-pi-samba/

Task continued:

Routers R2 and R3 are configured to give local devices internet access. R3 is VMWWs build in router functionality, in this case for VMnet8, and thus a virtual router functionality configured through VMWWs network editor.

Hand in

1. One HLD with explanation. HLD and Configurations must also be linked to on GitLab.

2. An inventory of used devices and software. The bullet point list must facilitate replication of the achieved results.

3. Optional:
   Show how to configure:
   a. SAMBA server.
   b. Linux SMB client.
   c. Windows client.
   Please note that writing up how to do things will help remember later how it all was done and thus save time when it has to be repeated on another system.

4. Proof that PC5 can share files via the SAMBA server with PC6 and vice versa,

5. Wireshark SMB communication between SMB clients and server.

Please note that the PC numbers used here refer to the diagram and that they do not have to be the same in handed in documentation. They must match the handed in HLD.

Assignment 49 OSPF routing protocol

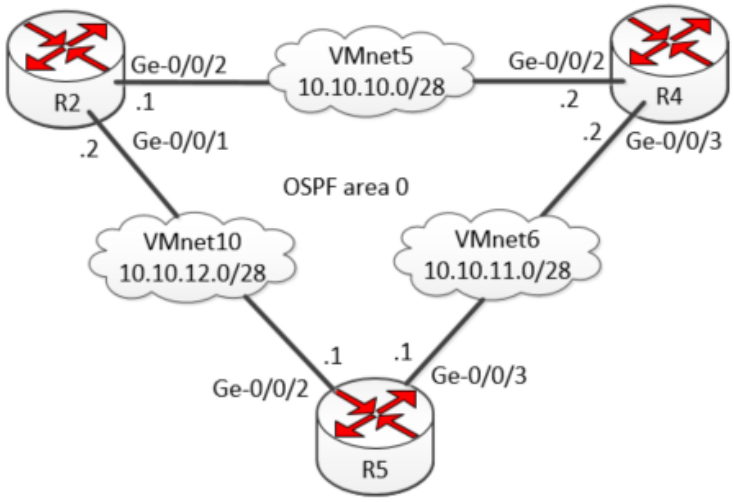
Learning objectives: After this assignment, the student can explain:

- At a high level, what the OSPF routing protocol is.
- Benefits of and when to use OSPF.

The student can:

- Set up OSPF in a multi router network
- Set up e.g. a Windows and Linux clients to communicate over the OSPF configured routers.

In the following network the three routers have to be configured with OSPF so that all three routers know all shown interfaces. In other words OSPF area 0 must include all shown interfaces. And again in other words. OSPF area 0 consists of all shown interfaces.



Hand in:

1. One HLD with explanation.
   HLD and Configurations must also be linked to on GitLab.

2. An inventory of used devices and software. The bullet point list must facilitate replication of the achieved results.

3. R2 routing table with explanation.

4. Show neighbours for all routers with explanation.

5. Proof that R5 can ping all interfaces on VMnet5,

Assignment 50 OSPF routing protocol Loopback interface

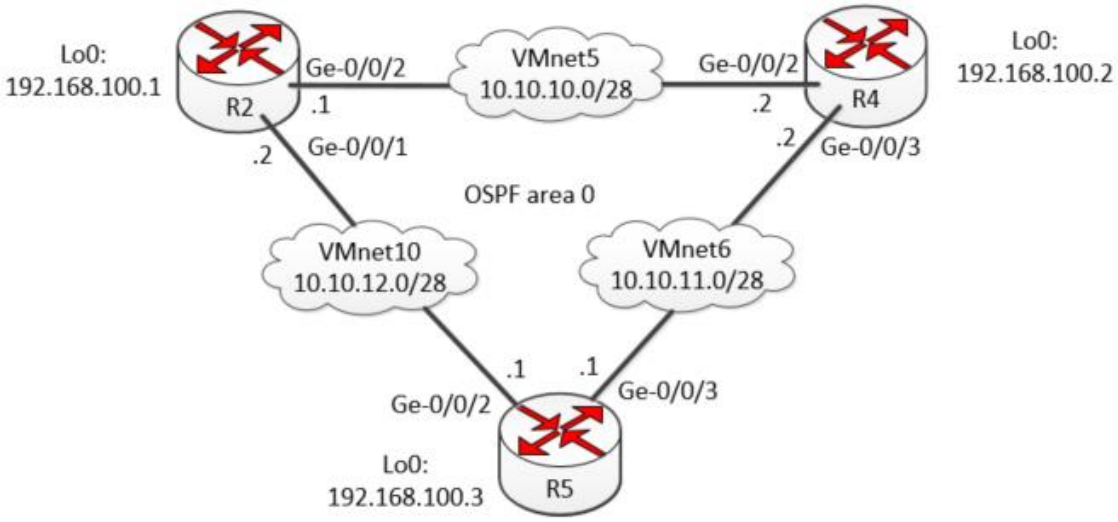
Learning objectives: After this assignment, the student can explain:

- At a high level, what a Junos router loop back interface is.
- Benefits of and when to use a Junos router loop back interface with OSPF.

The student can:

- Set up a Junos router loop back interface
- Demonstrate the use of a Junos router loop back interface in OSPF

In the following network the three routers have to be configured with OSPF and a Loopback interface so that all three routers know all shown interfaces. In other words, OSPF area 0 must include all shown interfaces. And again in other words. OSPF area 0 consists of all shown interfaces.



Hand in:

1. One HLD with explanation.
   HLD and Configurations must also be linked to on GitLab.

2. An inventory of used devices and software. The bullet point list must facilitate replication of the achieved results.

3. R4 routing table with explanation. Run: **`run show route protocol ospf`**

4. Run the **`run show ospf interface`** command on R4 and explain why and how the DR and BDR have been chosen to be what they are.

5. Proof that R5 can ping all interfaces on Router R2. Also the loopback interface.

Assignment 51 OSPF routing protocol and more subnets

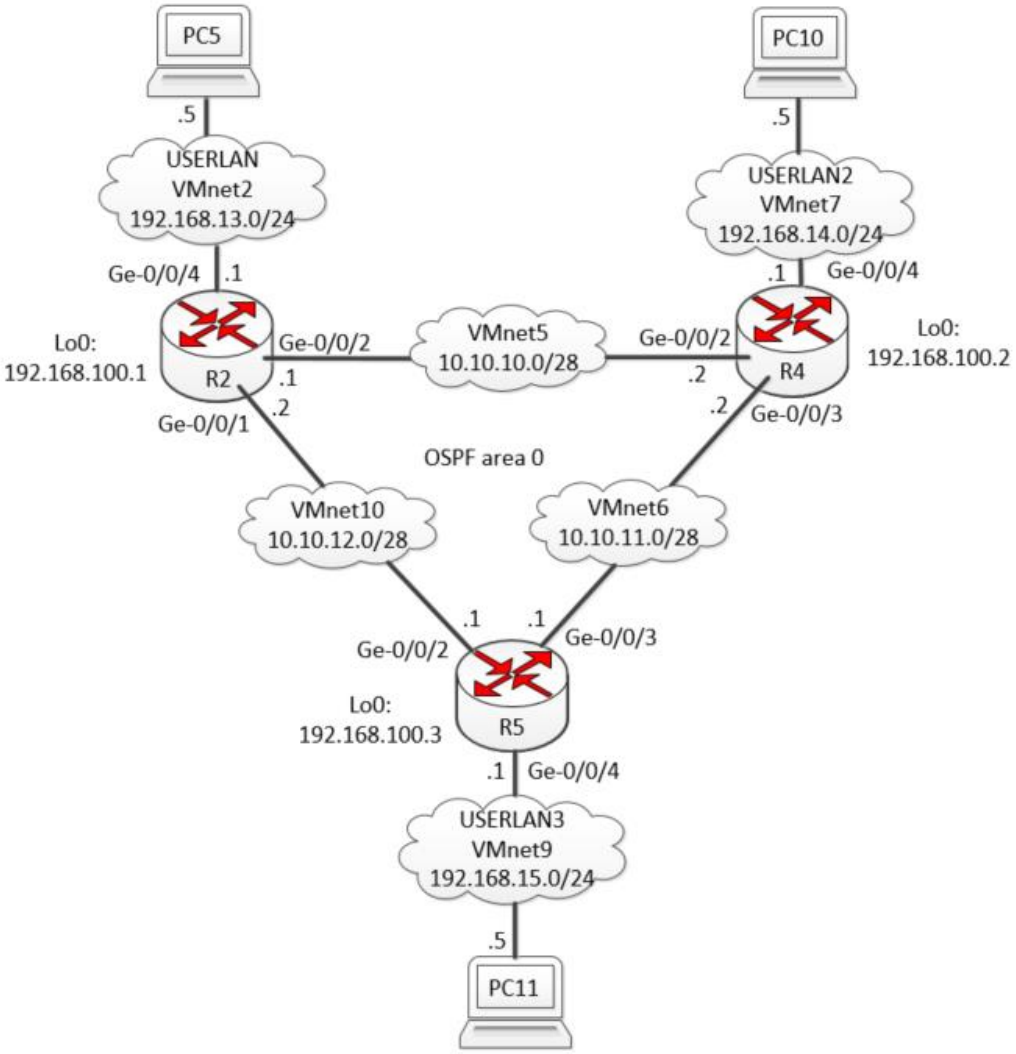
Learning objectives: After this assignment, the student can explain:

- At a high level, how to in cooperate more subnets in OSPF.

The student can:

- Set up a Junos router with OSPF and more subnets.
- Demonstrate the use of OSPF with more subnets.

In the following network the three routers have to be configured with OSPF and a Loopback interface so that all three routers know all shown interfaces. In other words, OSPF area 0 must include all shown interfaces. And again in other words. OSPF area 0 consists of all shown interfaces.



See next page for hand in.

Hand in:

1. One HLD with explanation.
   HLD and Configurations must also be linked to on GitLab.

2. An inventory of used devices and software. The bullet point list or table must facilitate replication of the achieved results.

3. R4 routing table with an explanation aimed at the USERLANs.
   Run: **`run show route terse`**

4. Proof that the PCs can ping each other.

5. Optional:
   Exclude the USERLANs from OSPF area 0 and instead use policy and export to inject the subnets into OSPF, to advertise the USERLANs in OSPF.

Assignment 52 OSPF routing protocol and default route

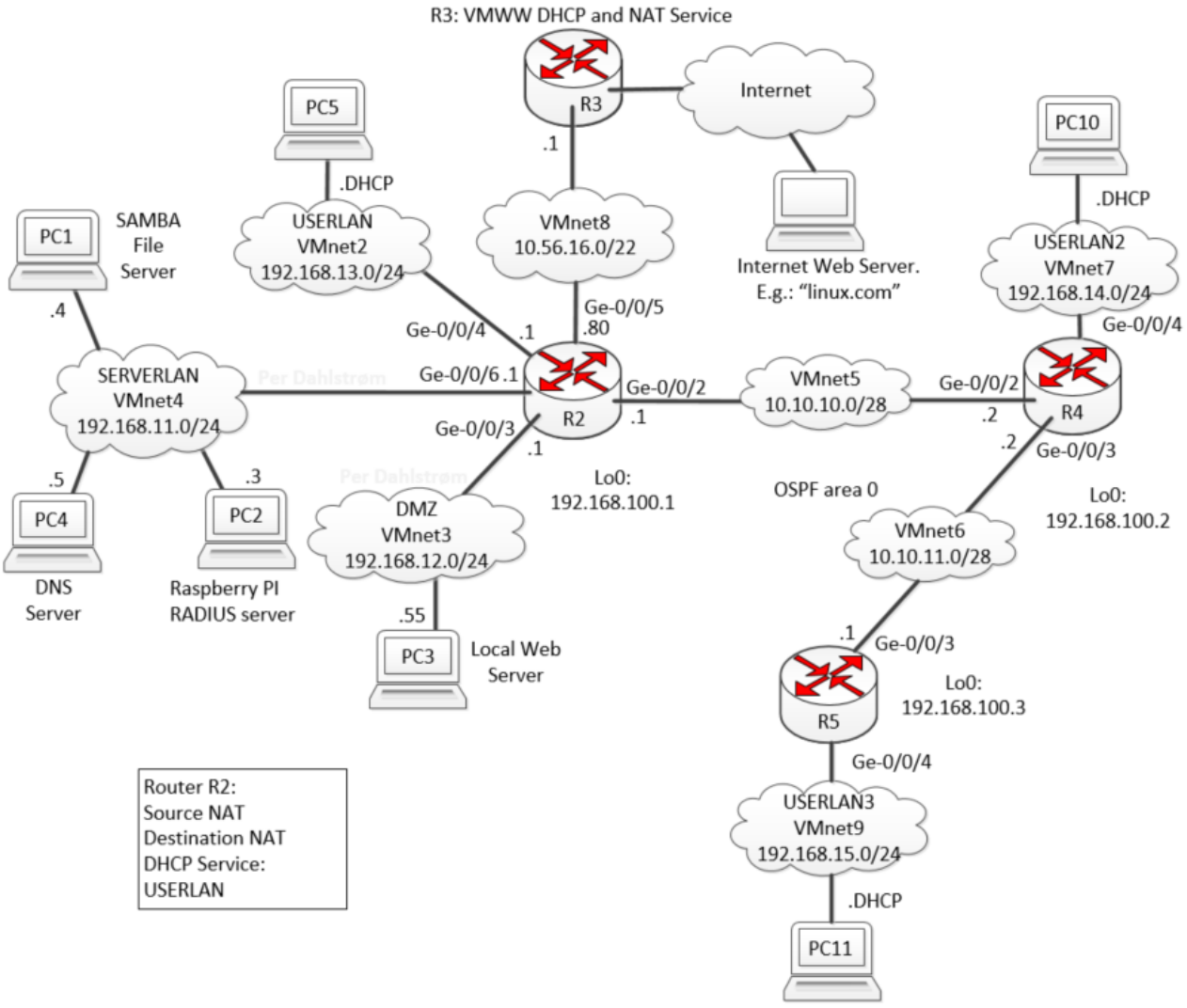
Learning objectives: After this assignment, the student can explain:

- At a high level, how to export default route to OSPF.

The student can:

- Set up a Junos router with OSPF and export default route.

In the following network the three routers R2, R4 and R5 have to be configured with OSPF and a loopback interface so that all three routers know all necessary interfaces. It should be possible for relevant clients to use e.g. the local DNS server PC4. Relevant subnets should have access to the internet. E.g. PC11 should be able to ping linux.com and also reach the local web server PC3 by its local domain name.



Task:

Create and document a network with a complexity similar to the shown network. Use OSPF.

Hand in

1. One HLD with explanation.
   HLD and Configurations must also be linked to on GitLab.

2. An inventory of used devices and software. The bullet point list or table must facilitate replication of the achieved results.

3. Necessary documentation that proves the functionality of the network.

Assignment 53 RaspberryPi as Virtual Machine and Web Server

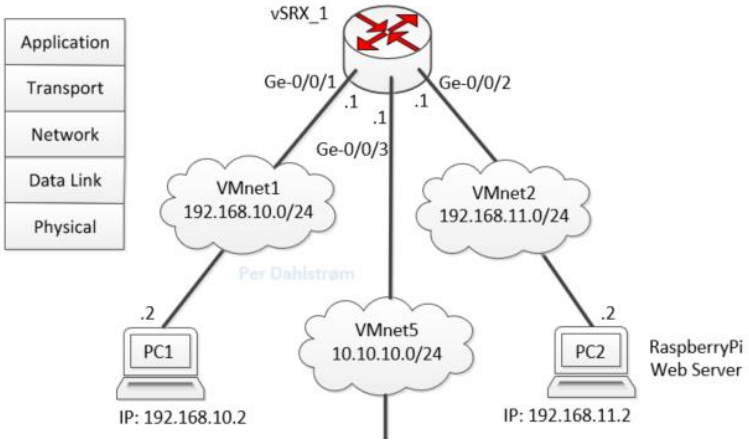
Learning objectives: After this assignment, the student can explain:

- How to create a RaspberryPi VM.
- What a RaspberryPi VM is and what the purpose of it is.
- What a Web Server is and what the HTTP application layer protocol is.
- Very fundamental what HTML is.
- How to make a basic dynamic web page by means of Python.

The student can:

- Set up a Raspberry Pi as a VM Virtual Machine and as a Web Server.

In the following network PC2 is a RaspberryPi with an installed Web Server. VMnet5 is not necessarily active.



Tasks:

- Get the RaspberryPi .iso file.
- Install the RaspberryPi on VMware Workstation.
- Configure the network settings on the Raspberry for the given network.
- Install necessary software. E.g. Wireshark.
- Install a Web Server on the RaspberryPi. E.g. nginx.
- Run and test the build in Python server: $ python3 -m http.server
- Create an .index test Web Page in HTML. Something very basic.
- Test that the Web Server is reachable from PC1.
- Document the tasks. See Hand in section here below.

Hand in

Produce and present necessary written documentation for each item:

1. One network diagram with explanation.
   Network diagram and Configuration(s) must also be linked to in a GitLab repository.

2. An inventory of used devices and software stating versions. The bullet point list or table must facilitate replication of the achieved results.

3. Documentation proof of a working Web server.

4. Wireshark HTTP traffic to and from the Web server with explanation and highlighting of the following layer information:

   a. Layer 2: Highlight source and destination MAC addresses.
   b. Layer 3: Highlight source and destination IP addresses.
   c. Layer 4: Highlight source and destination Ports.
   d. Layer 5: Highlight application layer data.

   Write two lines of commenting for each layer item.

5. Explain in two lines what the application layer HTTP protocol is. Make a drawing to support the explanation.

6. Show the Python Webserver .index page and show the resulting page in a browser.

Assignment 54 SRX security Address book, Zones and Policies

Learning objectives. After having worked with this assignment:

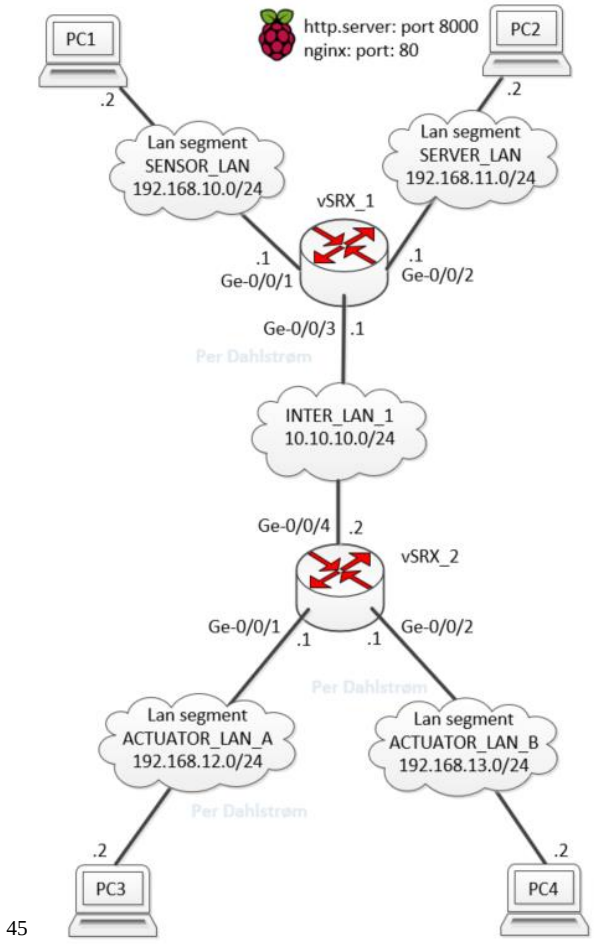
The student can at a basic level explain:

- SRX zones.
- SRX policies.
- SRX address book.
- SRX applications.

The student can at a basic level:

- Specify security requirements for a given simple network.
- List simple security specifications.
- Configure Junos SRX address book, zones, policies and applications.
- Elaborate a test plan and test simple security configurations accordingly.

This assignment is building on the network develop in assignment 11. The naming of subnets is different but the basic configurations of the two routers vSRX_1 and vSRX_2 are identical to those done in assignment 11. The assignment also builds on assignment 53, where a Raspberry Pi as a Web server was introduced. Here this Web Server on PC2 is also part of the assignment.



[45]

[45] 20S Network Drawing PDA V07.vsd

Tasks:

- Draw a network diagram.
- Build the network and make sure all PCs can intercommunicate.
- Implement the following security specification on one Zone on vSRX_1:
    - Security specifications:
        - PC1: Can Communicate all and fetch webpage from PC2.
        - PC2: Can Communicate all and fetch webpage from PC2.
        - PC3: Only communicate devices until 10.10.10.1.
        - PC4: Only communicate devices until 10.10.10.1 and fetch webpage from PC2.
    - A note on these specifications: Specifying and documenting network security is a huge topic and the above listed 4 lines are an extract and not really precise, but in this "exercise" context introducing basic security on a small network, they will do.
- Develop a test plan.
- Test that the specifications are full filled while filling out the test plan.
- Implement the security specifications by means of multiple zones on vSRX_1.
- Run the developed test plan again.

Hand in

Produce and present necessary written documentation for each item:

1. One network diagram with only one zone on vSRX_1 with explanation.
   Network diagram and Configuration(s) must also be linked to in a GitLab repository.

2. An inventory of used devices and software stating versions. The bullet point list or table must facilitate replication of the achieved results.

3. List of security specifications. Use the above stated specifications.

4. A filled-out test plan according to the specifications. See below.

5. Show and comment on the security part of the vSRX_1 configuration that implements the given security specifications by means of just one security zone.

6. One network diagram displaying the multiple zones on vSRX_1 with explanation.
   Network diagram and Configuration(s) must also be linked to in a GitLab repository

7. Show and comment on the security part of the vSRX_1 configuration that implements the given security specifications by means of multiple security zones.

Assignment is continued on next page.

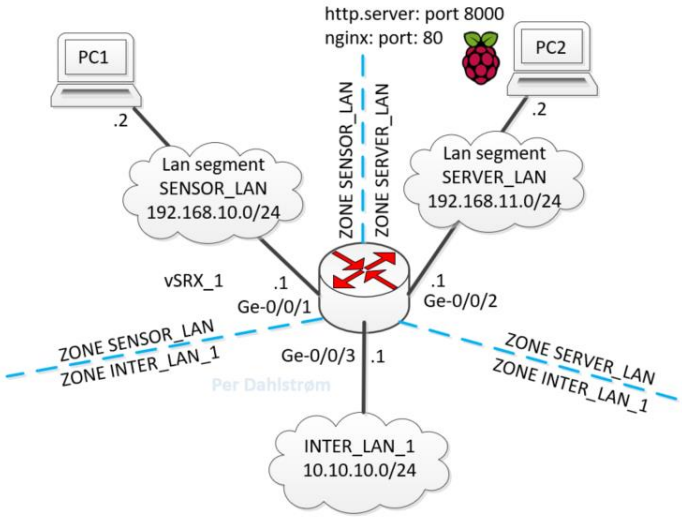
Here is an example or suggestion test table for the test plan:

	Can Ping: PC1	Can Ping: PC2	Can Ping: PC3	Can Ping: PC4	Can Fetch Web Page from PC2
PC1	ok	ok	ok	ok	ok
PC2	ok	ok	ok	ok	ok
PC3	error	ok	ok	ok	ok
PC4	ok	ok	ok	ok	error

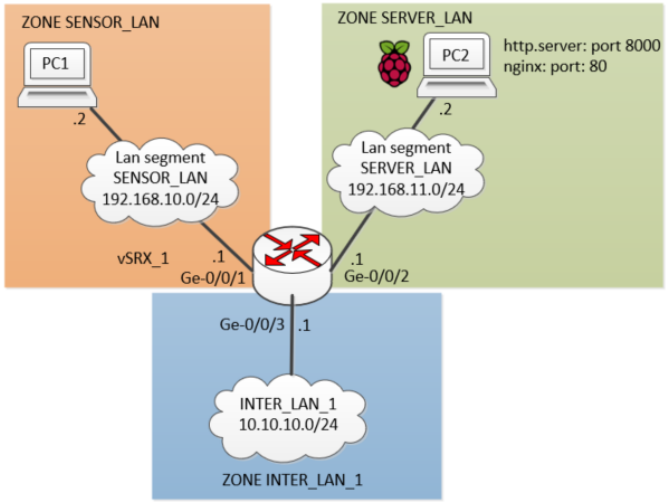
The left-hand side column lists the PCs as clients and the top horizontal list servers. I.e. the column PCs initiate the communication and are thus the clients.

A Green field means that this communication should be possible.
A Yellow field means that this communication should not possible.
A red text error is shown as it is possible for PC3 to ping PC1. This and example.
A red text error is shown as it is not possible for PC4 to fetch a web page from PC2.

Here is an example of how to illustrate interfaces in zones:



Or colours can be used:



Often Zones will also be documented in tables as many interfaces can be in the same zone.

Assignment 55 Basic MQTT devices on VMWW bridged network.

Learning objectives. After having worked with this assignment:

The student can at a basic level explain:

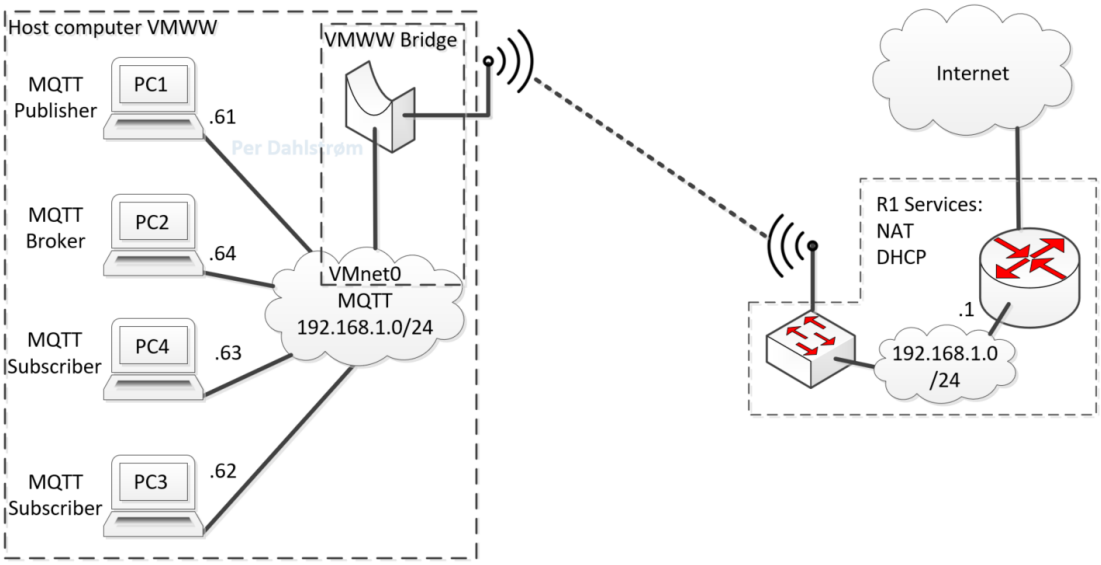
- How to set up MQTT broker, publisher and subscriber on Linux.
- What Bridge does in VMware Workstation.

The student can at a basic level:

- Set up a Bridged network in VMware Workstation.
- Set up a MQTT Broker on Linux. Use Mosquitto.
- Set up a MQTT Python Publisher on Linux
- Set up a MQTT Python Subscriber on Linux
- Verify that the Broker, Publisher and Subscriber can communicate via MQTT.

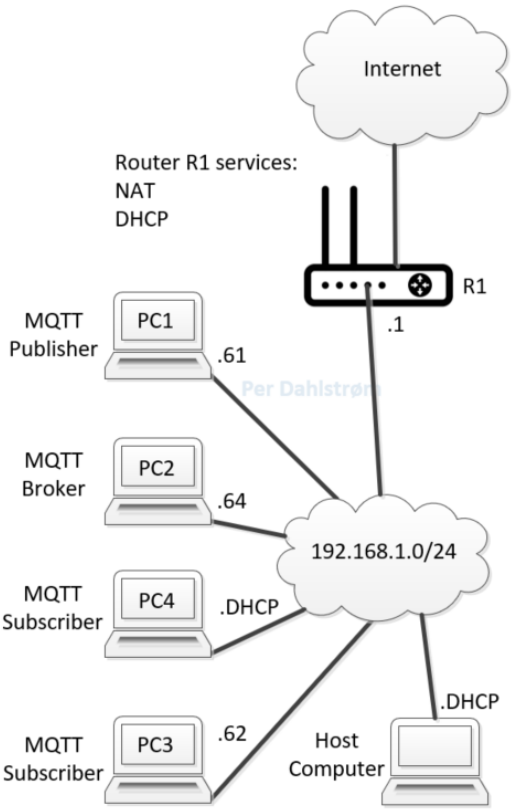
Please build the following network in VMware Workstation.

- PC1: MQTT Publisher. Python program as Publisher.
- PC2: MQTT Broker or server. Use mosquito.
- PC3 and PC4: MQTT Subscribers. Python program as Subscriber.



Use VMnet0 and set it to bridge to the host computers LAN, being it wireless or wired. Here a wireless LAN is illustrated. The router R1 dotted box symbolises the typical functionality of a home router. Note that PC1, 2, 3 and 4 are on the same network as the host computer, namely 192.168.1.0/24.

Conceptually the network has this design:



Tasks:

1. Draw a network diagram.

2. On workstation set VMnet0 to bridge to the host computer adapter that is connected to the network with the host computer default gateway on it. I.e. in most cases the homer router. Please note that the schools routers do NOT allow multiple IP from the same MAC address and this setup will thus not work on e.g. the schools wireless network.

3. Connect PC1, 2, 3 and 4 to VMnet0.

4. Set static IP addresses on PC1, 2, 3 and 4 according to the network diagram. Also set DNS server on PC1, 2, 3 and 4 to e.g. 8.8.8.8.

5. Verify that PCs have internet access.

6. Set up a MQTT Broker on Linux. Use mosquitto.

7. Set up a MQTT Python Publisher on Linux. Use a custom topic.

8. Set up a MQTT Python Subscriber on Linux.

9. Verify that the Broker, Publisher and Subscriber can communicate via MQTT.

Hand in:

1. The network diagram with comments.
2. MQTT Python Publisher program with comments.
3. MQTT Python Subscriber program with comments.
4. A screenshot showing a sample Publisher run.
5. A screenshot showing a sample Subscriber run. Proving that Subscriber can retrieve data from subscriber.

Assignment 56 Application layer protocol MQTT

Learning objectives. After having worked with this assignment:

The student can at a basic level explain:

- The term: Application layer protocol.
- How MQTT is an example of an Application layer protocol.
- Optional: How MQTT compares to HTTP.
- How to Wireshark MQTT.
- Optional: MQTT QoS.
- Optional: MQTT Retain.
- Optional: Clean Session.

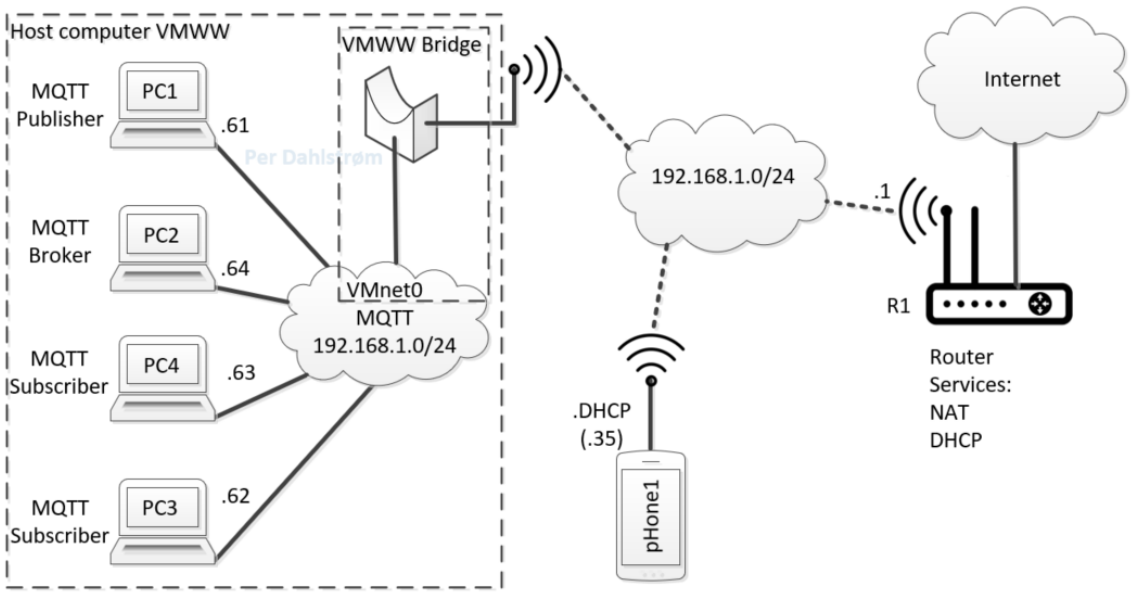
The student can at a basic level:

- Set up a MQTT app on a smartphone
- Capture and locate MQTT traffic in the capture.
    - To some very basic extend
        - analyse the MQTT traffic.
        - compare the traffic to the MQTT specification

Please build the following network in VMware Workstation.

- PC1: MQTT Publisher. Python program as Publisher.
- PC2: MQTT Broker or server. Use mosquito.
- PC3 and PC4: MQTT Subscribers. Python program as Subscriber.
- Phone1 is a smart phone with a MQTT application.

Use VMnet0 and set it to bridge to the host computer computers LAN, being it wireless or wired. Here a wireless LAN is illustrated. The router R1 dotted rectangle box symbolises the typical functionality of a home router. Note that PC1, 2, 3 and 4 are on the same network as the host computer, namely 192.168.1.0/24. Publishers and Subscribers can alternatively be on DHCP.



Tasks:

1. Draw a network diagram.

Do item 2 and 3 and 4 below with QoS set to 0 on all relevant clients.

2. Install a MQTT application like mqter or EasyMQTT for iPhone on a smartphone, and connect to the Broker or MQTT server on the network.

    a. On the smartphone app, publish to one or more topics.
    b. On the smartphone app, subscribe to one or more topics.
    c. Verify that PC1 can publish to "smartphone app" topics.
    d. Verify that PC3 and 4 can subscribe to "smartphone app" topics. I.e. receive values from the smart phone.

3. Run Wireshark on the Broker e.g. with capture filter: tcp port 1883.

    a. Show in Wireshark one publication transaction from PC1 to the broker. Comment on the transaction.
    b. For a/one MQTT CONNECT COMMAND in the transaction, comment on:
        i. MAC addresses.
        ii. IP addresses.
        iii. Ports.
        iv. MQTT protocol Flags:
            1. Message type
            2. QoS
            3. Clean Session
            4. Retain. (Trick question! 😊)
        v. Optional: MQTT keep alive value
        vi. Optional: MQTT Client ID

4. Run Wireshark on the Broker e.g. with capture filter: tcp port 1883.

    a. Show in Wireshark one publication transaction, from the smartphone app to the broker. Comment on the transaction.
    b. For a/one MQTT CONNECT COMMAND in the transaction, comment on:
        i. MAC addresses.
        ii. IP addresses.
        iii. Ports.
        iv. MQTT protocol Flags:
            1. Message type
            2. QoS
            3. Clean Session
            4. Retain. (Still a trick question! 😊)

5. Do item 3 above, now with QoS set to 1 and then with QoS set to 2.

Continued on next page.

6. Compare one MQTT message in a captured transaction to the MQTT standard paper. E.g. a "Connect Command" or "Connect Ack" or "Disconnect Ack" or "Publish Message" or a "Subscribe Command" or another message.
    a. Compare and comment on what is seen in Wireshark and in the MQTT st. paper.

7. Introduce an error on e.g. a client like in the PC1 publisher Python program.
   Do not use any Capture filter. Instead use a Display Filter to filter out the interesting packets.
    a. Describe and show how the error is introduced. I.e. describe and show if it is a:
        i. Networking error?
        ii. Programing error?
        iii. MQTT protocol error?
        iv. Or an other type of error or combination of more types.
    b. Show what the MQTT publish transaction now looks like in Wireshark.
    c. Explain what filter is used and why the filter is used.
    d. Comment on how the introduced error is identifiable in Wireshark or explain why it is not identifiable in Wireshark?

Hand in:

1. The network diagram with comments.

2. Document the fulfilment of each of the above listed tasks. Please organise your documentation in the same order as the task list If possible.

Assignment 57 SRX ipsec end to end VPN

[46]Doc.

[47]Doc.

[46] https://www.letsconfig.com/how-to-configure-site-to-site-policy-based-ipsec-vpn-on-juniper-srx/
[47] https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/topic-map/security-route-based-ipsec-vpns.html#id-understanding-route-based-ipsec-vpns

Assignment 58 SSH basics of the openSSH using only Server or Host keys.

Learning objectives. After having worked with this assignment:

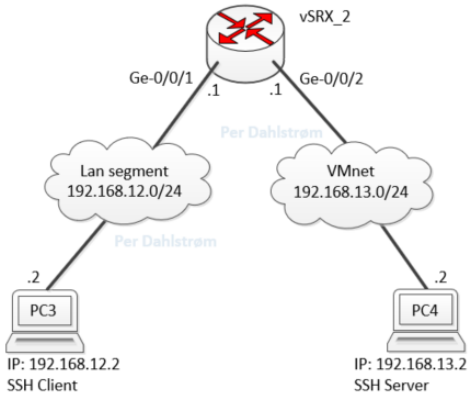
The student can at a basic level explain:

- What SSH is.
- What to use SSH for.
- What SSH host key pairs are.

The student can at a basic level:

- Set up a SSH client and server with host key pairs.

The following example network is referred to in the task descriptions. Note that the diagram does not show the VMWW host computer attached to the VMnet. This network layout can be used for the tasks below or another similar network can be used.



20S SSH School and Generic Network PDA V01.vsd

Tasks

1. Draw a network diagram with information relevant to the assignment. Include the VMWW host computer on the VMnet.

2. Installing openSSH on PC3 and PC4 which are two Linux machines.
    a. Install openSSH on PC3 and PC4.
    b. Log in from PC3 to PC4.
    c. In which directory does PC4 store the PC4 host public and private keys?
    d. In which directory does PC3 store the PC4 host public key?
    e. Nano into the public key files and compare the PC4 host public key on PC4 with the PC4 host public key now on PC3. It should be a copy of the one on PC4. Is that the case?

3. Wiresharking the ssh communication.
    a. Wireshark the communication between PC3 and PC4. Please use the ssh filter.
    b. Please comment on whether the communication is encrypted or not? In 3-5 lines explain what it means that communication is encrypted? A drawing or graphical representation can support the explanation.
    c. Please comment on why it is beneficial or not to have this communication encrypted?
    d. Highlight what ports are used on the transport layer for both server and client. Please comment on the port numbers. I.e. please tell in 2-3 lines where they come from?

4. Attaching the VMWW host computer:
    a. In VMWW Network Editor, configure the VMnet to include or attach the VMWW host computer to the VMnet.
    b. Please remember to indicate in the network diagram which number VMnet is being used and add the VMWW host computer to the diagram with relevant information.
    c. Check that the vSRX_2, VMWW host computer and PC4 can ping each other. Please check from all devices to the others.
    d. Optional as this is not related to SSH: Check if VMWW host computer and PC3 can ping each other. Please check in both directions. Please show what is observed and explain why this is happening.

5. Installing openSSH on the VMWW host computer:
    a. Install openSSH on the VMWW host computer.
    b. Log in from VMWW host computer to PC4.
    c. Optional: Log in from from PC4 to VMWW host computer.

6. Creating a new user karen on PC4.
    a. Create a new user karen on PC4. Use the **`adduser`** program for this.
    b. Log in to the new user from PC3.
    c. Log in to the new user from the VMWW host computer.

7. From PC3:
    a. SSH into vSRX_2 from PC3, using terminal command: **`username@ipaddress`**
    b. What user(s) are on the vSRX_2?

Hand in:

1. The network diagram with comments.

2. Document the fulfilment of each of the above listed tasks. Please organise your documentation in the same order as the task list If possible.

Assignment 59 SSH basics of the openSSH using client keys.

Learning objectives. After having worked with this assignment:

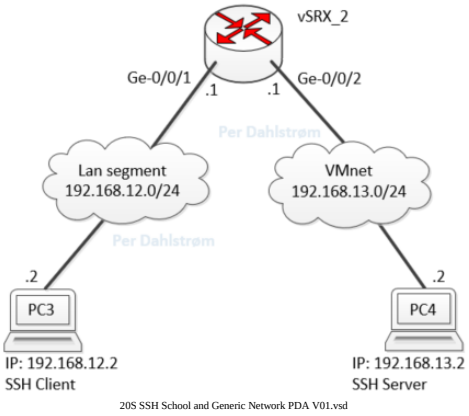
The student can at a basic level explain:

- What SSH client key pairs are.

The student can at a basic level:

- Set up a SSH client and server with client key pairs.

The following example network is referred to in the task descriptions. Note that the diagram does not show the VMWW host computer attached to the VMnet. This network layout can be used for the tasks below or another similar network can be used.



20S SSH School and Generic Network PDA V01.vsd

Tasks

1. Draw a network diagram with information relevant to the assignment. Include the VMWW host computer on the Vmnet.

2. Create a client key pair for a user on PC3 and copy the public key to the server PC4. Demonstrate that password free login is now possible from PC3 to PC4.

3. Create a new or another user on PC3 and also set up password free login to PC4 for this user.

4. Set up Putty for password free login to PC4.

5. Create a random text file on PC3 and also one on PC4.
   Demonstrate that the file can be copied from PC3 to PC4 using the Secure Copy program: scp

6. Create a new user on the router vSRX_2.
   First do login with only host or server keys.
   Then set up password free login and login to the router password free.

7. Optional:
   Junos can be configured to transmit its active configuration to a ssh server every time the user issues the commit command on a Junos box.
   Make Junos auto archive to a ssh server on commit

8. Optional:
   Demonstrate how to use Filezilla to copy files between clients and servers.

Hand in:

1. The network diagram with comments.

2. Document the fulfilment of each of the above listed tasks. Please organise your documentation in the same order as the task list If possible.

End of document.