Aalto University
School of Science
and Technology

ELEC-E7330 Laboratory Course in Internet Technologies

27 – IPv4 Routing

Student edition

Oskari Simola & Antti Aro
Zhong Yunqiu, 8.8.2008
Matias Elo & Antti Kajander, 6.8.2010
Tahir Jemal, 15.8.2018

Contents

This laboratory work includes 16 questions. The total number of points is 62.

Answer the following questions shortly but **clearly**. You can answer in Finnish/Swedish or in English. It is also a good idea to examine the laboratory assignments and Juniper J2320 IPv4 HowTo beforehand. There is only 5 hours work time on your lab turn.

1 Preliminary exercises (10 points)

P1 (2 points)
Consider a network presented in Figure 1. OSPF version 2 is used. There is a little trick that needs to be done in order to get full connectivity through the network, when the areas are defined as presented. Find out what that trick is.
Hint: See RFC 2328 [1] section *3. Splitting the AS into Areas*.

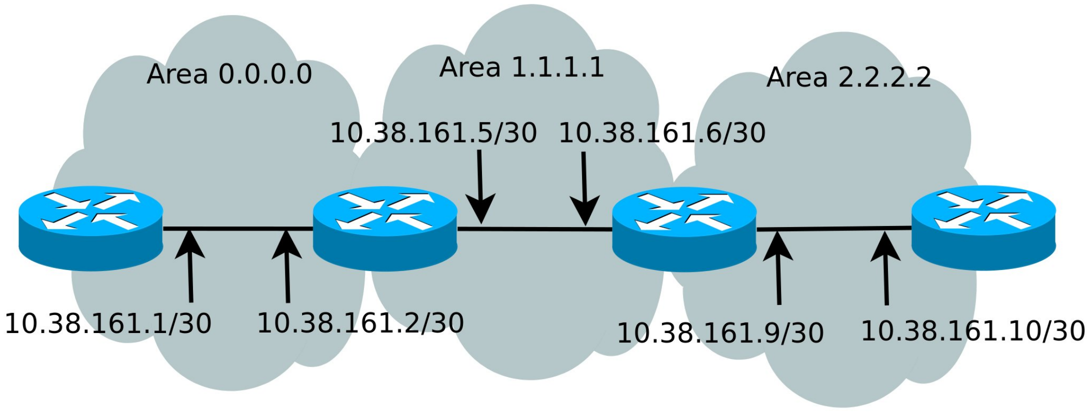


Figure 1: OSPF Network

P2 (4 points)
Explain the main differences between RIP and OSPF routing protocols.

P3 (4 points)
Plan the IP address allocation for the network used in this laboratory work. The network topology is presented in Appendix A. In Appendix B there is a screenshot from the IP address checking system. See 2.1.1 for more information.

*Note: It's possible, but **not necessary**, to use RFC 3021 Point-to-Point addressing for all IPv4 Point-to-Point Links except for the gateway link.*

2 Laboratory exercises (52 points)

2.1 Work description

This work is about IPv4 routing. You will get familiar with IPv4 addressing and configuring IPv4 routers. Both RIP and OSPF protocols are used. In addition,you can use *tcpdump [man <command to look up> in linux terminal]* to capture traffic and make packet analysis. However, this work is only a very basic lesson about how to configure IPv4 networks.

You have to assign IPv4 addresses and configure the network as follows:

- The entire network uses RIP
- The entire network uses OSPF
- Both RIP and OSPF are used

2.1.1 Environment

The work environment consists of six Juniper logical systems (vMX) and two virtual client PCs running Ubuntu 14.04.1 LTS, which are used to test the network. Juniper routers are using JUNOS 18.1R2.5 software. In addition there is a gateway, which is pre-configured. Routers (logical systems) are named according to Finnish cities: Oulu, Vaasa, Lappeenranta, Tampere, Turku and Helsinki.Domain name for this labwork is ipv4.lab and name server 10.38.0.1. Two LANs are connected to the routers, one in Helsinki and the other in Oulu. Network topology can be seen in Appendix A. The default gateway is connected to Turku's Gigabit Ethernet 0/0/25 interface and its address is set to 10.38.161.1/30(group 1) and 10.38.171.1/30(group 2) . All interfaces of the routers and PCs are connected inside vMX. Your assistant configures the topology for you.

2.1.2 Group 1

You need to configure IP addresses for selected router interfaces. You must also assign a loopback address for every router. The address space is only 10.38.161.0 – 10.38.161.65. There are 13 computers connected to the LAN in Helsinki and 4 computers connected to the LAN in Oulu. You really have to think carefully how to set the IP addresses for the interfaces. Client PCs use DHCP for obtaining their IP addresses so you have to configure DHCP Servers to Helsinki and Oulu.

Network information:

Address space:	10.38.161.0 – 10.38.161.65
Domain name:	ipv4.lab
Default gateway:	10.38.161.1/30
Name server:	10.38.0.1

The vMX fxp0 interface is preconfigured and used only for Junos router management. All the router configurations can be done using SSH connection **Username and password** for the vMX instance,for the workstations, and for the logical systems (routers) are shown in the table below.

Table 1: SSH management interfaces for routers and workstations(vmx1)

Name	IP address	SSH command	Password
vMX instance (vmx1)	10.255.4.200	lab@10.255.4.200	eeeeee
Junos core router	10.255.4.201	root@10.255.4.201	JunosJ
Helsinki	————	helsinki@10.255.4.201	Student
Lappeenranta	————	lappeenranta@10.255.4.201	Student
Tampere	————	tampere@10.255.4.201	Student
Turku	————	turku@10.255.4.201	Student
Oulu	————	oulu@10.255.4.201	Student
Vaasa	————	oulu@10.255.4.201	Student
Helsinki Lan (LAN1)	10.255.4.205	lab@10.255.4.205	Student
Oulu Lan (LAN2)	10.255.4.206	lab@10.255.4.206	Student

2.1.3 Group 2

You need to configure IP addresses for selected router interfaces. You must also assign a loopback address for every router. The address space is only 10.38.171.0 – 10.38.171.65. There are 13 computers connected to the LAN in Helsinki and 4 computers connected to the LAN in Oulu. You really have to think carefully how to set the IP addresses for the interfaces. Client PCs use DHCP for obtaining their IP addresses so you have to configure DHCP Servers to Helsinki and Oulu.

Network information:

Address space:	10.38.171.0 – 10.38.171.65
Domain name:	ipv4.lab
Default gateway:	10.38.171.1/30
Name server:	10.38.0.1

The vMX fxp0 interface is preconfigured and used only for Junos router management. All the router configurations can be done using SSH connection **Username and password** for the vMX instance,for the workstations, and for the logical systems (routers) are shown in the table below.

Table 2: SSH management interfaces for routers and workstations(vmx2)

Name	IP address	SSH command	Password
vMX instance (vmx2)	10.255.4.210	lab@10.255.4.210	eeeeee
Junos core router	10.255.4.211	root@10.255.4.211	JunosJ
Helsinki	————	helsinki@10.255.4.211	Student
Lappeenranta	————	lappeenranta@10.255.4.211	Student
Tampere	————	tampere@10.255.4.211	Student
Turku	————	turku@10.255.4.201	Student
Oulu	————	oulu@10.255.4.201	Student
Vaasa	————	oulu@10.255.4.201	Student
Helsinki Lan (LAN1)	10.255.4.215	lab@10.255.4.215	Student
Oulu Lan (LAN2)	10.255.4.216	lab@10.255.4.216	Student

2.1.4 IP Addresses

IP addresses must be bound to the routers' *logical interfaces*. Depending on the router, you have to configure 3 – 5 interfaces. The *physical interfaces* (Ethernet ports) used in this lab work are named *ge-0/0/1*, *ge-0/0/2*, *ge-0/0/3* etc . In addition there is a "physical" loopback interface lo0. Each physical interface can have multiple logical interfaces, but in this lab work only one (unit 0) is used. Some of the routers don't use all available interfaces.

You have to issue `commit` command to make configuration changes active. You don't have to reboot routers, IP addresses are in use immediately.

2.1.5 Routing

RIP or OSPF routing can be modified by giving the following commands in *configuration mode*

```
[edit]
root@router#
edit protocols rip
edit protocols ospf
```

When you have given the `commit` command, routing process will start automatically. You can check routing tables in *operational mode* by using `show route` command.

There is no tutorial about routing protocols RIP and OSPF included in this document. Almost any book concerning basic IPv4 routing is enough to cope with this exercise. RFC 2328 [1] presents OSPF version 2 in detail and RFC 2453 [2] is about RIP version 2. As mentioned, the purpose of this work is not to teach the protocol details. You must still have the basic knowledge of these protocols. For example TKK's course S-38.2121 Routing in Communication Networks gives the required theory for this work.

2.1.6 Capturing Packets

When you want to capture packets with *tcpdump [man <command to look up> in linux terminal]* (on eth interfaces or bridges), you can issues the command *sudo brctcl show* on the terminal of the vMX to list the available bridges. Table 3 below shows the link bridges, so they can be helpful for troubleshooting.

You are not allowed to do any changes to the topology by changing, removing, connecting cables or doing anything similar. If this happens, your IPv4 lab work is failed this time. It is also recommended, that you go through RIP and OSPF and get familiar with the Juniper IPv4 HowTo in advance. Otherwise this laboratory exercise may be impossible to do in five hours.

Table 3: Bridde interfaces

Bridge name	City link
bridge_1	Oulu <-> Vaasa
bridge_2	Oulu <-> Lappeenranta
bridge_4	Vaasa <-> Tampere
bridge_5	Tampere <-> Lappeenranta
bridge_6	Lappeenranta <-> Helsinki
bridge_7	Tampere <-> Helsinki
bridge_8	Turku <-> Tampere
bridge_9	Turku <-> Helsinki
link_turkuGW	Turku <-> GW
link_lan1	Helsinki <-> LAN1
link_lan2	Oulu <-> LAN2

For example, *sudo tcpdump -i bridge_1* will capture traffic on the bridge_1 interface.

2.2 Exercises in the laboratory

You will have to answer to the questions marked with Q in you final report, so it is useful to take notes during the lab work.

2.2.1 IPv4 Checker

Q1 (1 point)
In the lab you first have to validate your IP addresses with IPv4 Checker, which creates the DNS zone **ipv4.lab** and reverse zone for 10.38.161.0/24 or 10.38.171.0/24. Go to `http://admin.noc.lab/ipv4checker/`. Fill in the WWW form shown in Appendix B. You can hit the TAB key twice to move the cursor to the next row. This validates your IP addresses. If they are valid, DNS zones are created. Why is it useful to have a name server in this lab work?

2.2.2 Setting the IP Addresses and DHCP servers

Q2 (2 points)
After your IP table has been successfully validated, carefully set the IP addresses according to your plan for each router interface. Test that the links are up by `ping`ing.

You also have to configure a DHCP server to Helsinki and Oulu LANs and a default gateway to Turku.

Can you ping from Helsinki to the loopback address of Turku? Why is it so?

2.2.3 RIP Routing

Q3 (2 points)
Configure the whole network to use RIP according to the instructions of the Juniper manual. Make router Turku to advertise the default route. When you are done, test the network by `ping`ing from *LAN1* to *LAN2*. Check also the route from *LAN1* to *LAN2* with `tracert` command and write it down. The configuration files from Turku and Lappeenranta have to be included in your final report. You can use for example `scp`, webmail or a USB flash drive to transfer these files.

Q4 (3 points)
Now, call the assistant to show you how to use *tcpdump* if you need it. Start packet capturing according to the assistant's instructions. Capture data from Helsinki ge-0/0/18 and ge-0/0/19.

Start `ping`ing from *LAN1* to *lo0* of Oulu.

Disable Lappeenranta ge-0/0/14 interface.

How long does it take until the packets reach Oulu again? What is the route now? Measure the time between route changes using the timestamps or a clock. After you're done, save your captures.

Q5 (2 points)
Keep the `ping` running, start a new capture and enable the disabled link again. How much time does it take before the previous route is used again? You can use the packet capture timestamps to get time between the route changes or you can use the traditional clock method.

End the packet capture and save the results.

2.2.4 OSPF Routing

Q6 (3 points)
Disable RIP routing on each router and configure the whole network according to the instructions of the Juniper HowTo to use OSPF.

OSPF enables metric manipulation much easier than RIP. The small numbers beside the links in Appendix A are link costs. Default cost for Gigabit Ethernet links is 1.

Remember that virtual link carries traffic over a transit area. Ask the assistant if you don't know where to place the virtual links. Remember to make router in Turku advertise the default route.

After you have configured OSPF to every router according to the Appendix A, test that you are able to ping from *LAN1* to *lo0* of Oulu.

Area 0.0.0.0

- Turku – Helsinki
- Turku – Tampere
- Helsinki – Tampere

Area 1.1.1.1

- Helsinki – Lappeenranta
- Lappeenranta – Tampere
- Tampere – Vaasa

Area 2.2.2.2

- Vaasa – Oulu
- Lappeenranta – Oulu

Q7 (4 points)
Use `tracert` to check that the shortest path from *LAN1* to *LAN2* is Helsinki – Turku – Tampere – Vaasa – Oulu. The configuration files from Turku and Lappeenranta have to be included in your final report.

Now, capture traffic from Helsinki ge-0/0/20 and ge-0/0/19 interfaces. Ping from *LAN1* to *lo0* of Oulu.

(a) At first, disable interface Vaasa ge-0/0/7 (now the traffic should go through Helsinki – Lappeenranta – Oulu). How long does it take until packets go through again?
(b) Enable Vaasa ge-0/0/7 interface and wait until the packets go via Vaasa again. How much time does it take before the previous route is used again?
(c) Now disable both Vaasa's interfaces. How long does it now take before the traffic goes via Helsinki – Lappeenranta – Oulu?

Enable the interfaces in Vaasa again.

2.2.5 OSPF Authentication

Q8 (2 points)

(a) First configure Lappeenranta ge-0/0/14 with OSPF authentication in area 2.2.2.2 with the password **comnet** according to the instructions of the Juniper manual. Trace route from *LAN2* to the interface ge-0/0/16 of Lappeenranta and examine the OSPF neighbor information with the command `show ospf neighbor`. Can *LAN2* reach Lappeenranta via ge-0/0/14?
(b) Then configure Oulu ge-0/0/2, ge-0/0/3 and Vaasa ge-0/0/6 with OSPF authentication in area 2.2.2.2 with the same password. Trace route from *LAN2* to the interface ge-0/0/16 of Lappeenranta again. What is happening now? Verify the OSPF neighbor information of Lappeenranta.

2.2.6 Both RIP and OSPF used in the network

Q9 (3 points)
This exercise should be quite easy, if you have coped with last two exercises.

(a) Configure the network in such way, that routers Turku and Helsinki only use OSPF and routers Vaasa and Oulu only use RIP. Lappeenranta and Tampere use both RIP and OSPF. The configuration file from Lappeenranta has to be included in your final report. In OSPF areas can be either *0.0.0.0* or *1.1.1.1*. You don't need to change them from the previous section. When you redistribute routing information from OSPF to RIP, put 1 to the default-metric value. Don't change link costs of OSPF compared to the previous section. Test that you are able to `ping` from *LAN1* to *LAN2*.

(b) Ping from *LAN1* to Oulu's *lo0* again and capture packets from Oulu ge-0/0/2 and ge-0/0/3 interfaces. Disable interface ge-0/0/14 from Lappeenranta. How long does it take before the traffic goes via Vaasa? Enable the interface again. How much time does it take before the previous route is used again?

2.2.7 Restoring the initial settings

The assistant will restore basic settings for each router.

Remember to take a copy of every file needed for the final report. Then delete all files you have created during the assignment from the workstation.

3 Final report

In your final report answer to the questions presented during the assignment (marked with Q) and to the additional final questions (marked with F).

F1 (2 points)
Present your final version of the IP address allocation. Explain how you ended up with it.

F2 (4 points)
In what kinds of situations are routing loops possible when RIP is used? Are there any situations in which OSPF can create routing loops?

F3 (4 points)
Study the routing messages you captured in the lab and present an analysis about them. Don't include complete captures to the report, but explain what kind of messages RIP and OSPF send. Also explain how routing protocols behaved when a link got broken.

F4 (20 points)
Present your final report in the form of *Final report model for IPv4 routing* in Noppa. (https://noppa.tkk.fi/noppa/kurssi/s-38.2131/materiaali/final_report_model_for_ipv4_routing.pdf)

Remember to add your configuration files from the different scenarios to your final report.

Points and Grade

The grade should be given according to the next table:

Preliminary report: 10 pts.
Final report: 23 + 30 = 52 pts
Total: 62 pts.

Grades	
Points	Grade
0...30	0
31...36	1
37...42	2
43...48	3
49...55	4
56...62	5

However, the grade must be zero (0) if any of the following conditions is true:

- Less than 50% of preliminary exercises are right.
- The student has failed to pass tasks in the laboratory.

References

[1] J. Moy, Ascend Communications, Inc. RFC 2328 - OSPF Version 2. http://tools.ietf.org/html/rfc2328, April 1998.

[2] G. Malkin, Bay Networks. RFC 2453 - RIP Version 2. http://tools.ietf.org/html/rfc2453, November 1998.

Appendix A

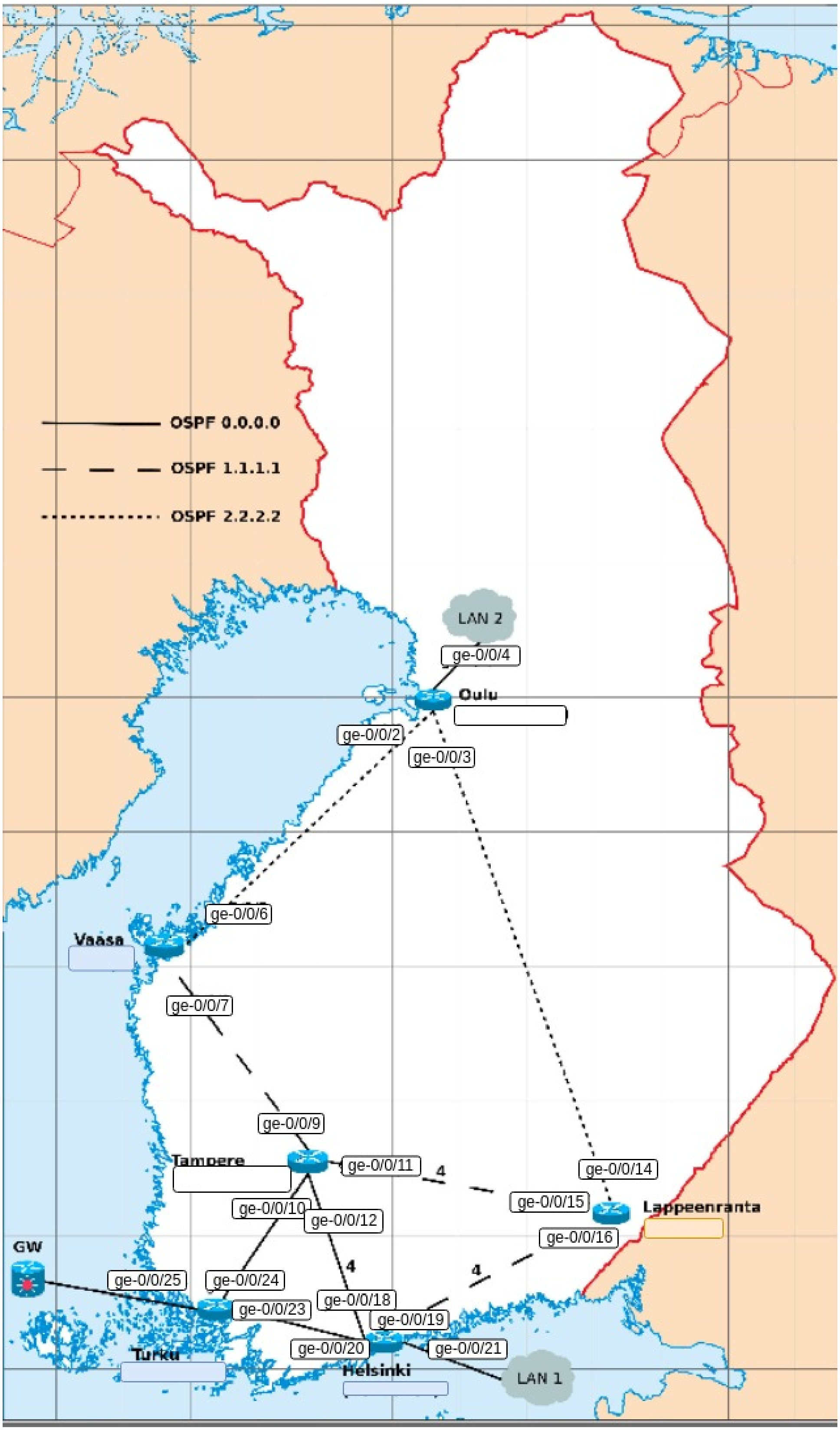
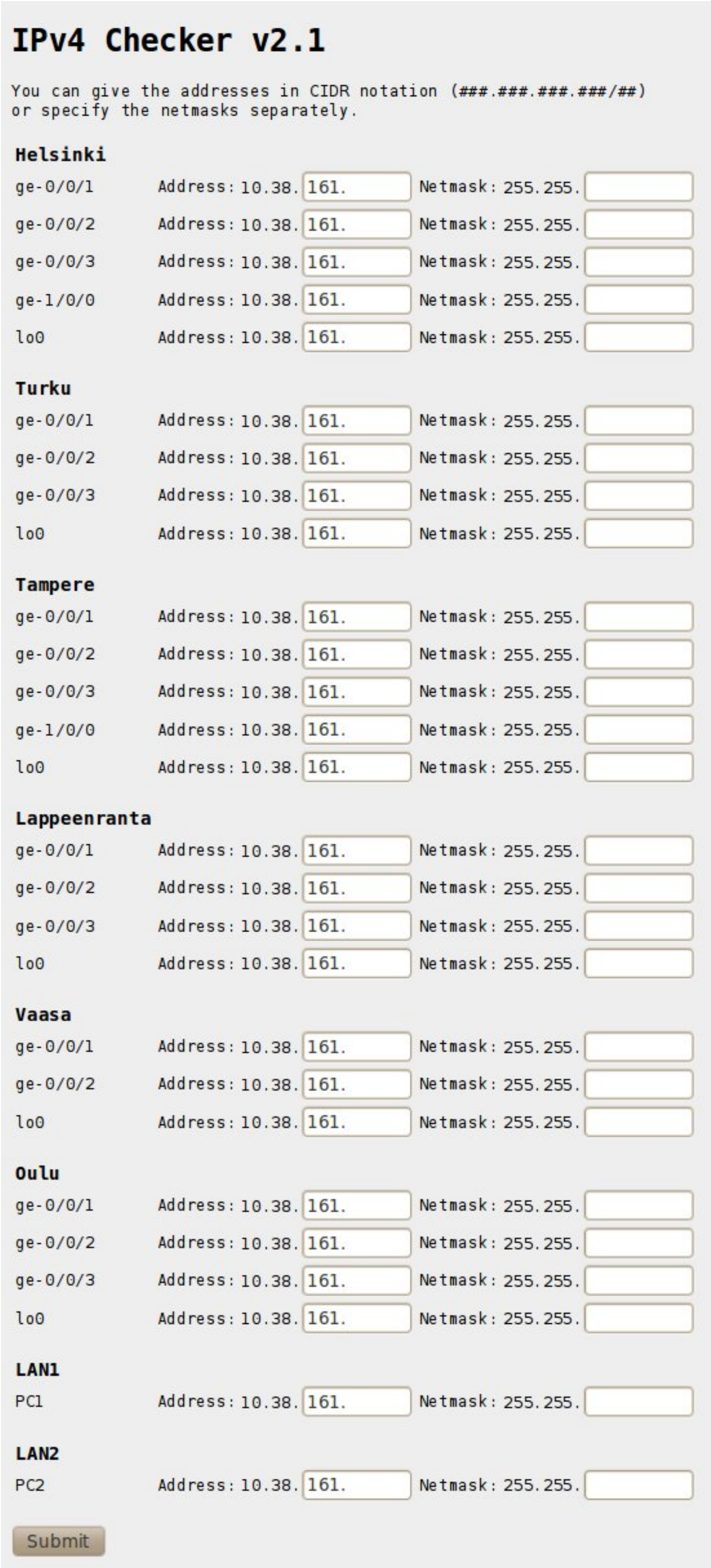


Figure 2: Network topology

Appendix B



IPv4 Checker v2.1

You can give the addresses in CIDR notation (###.###.###.###/##)
or specify the netmasks separately.

Helsinki

ge-0/0/1	Address: 10.38. 161.	Netmask: 255.255.
ge-0/0/2	Address: 10.38. 161.	Netmask: 255.255.
ge-0/0/3	Address: 10.38. 161.	Netmask: 255.255.
ge-1/0/0	Address: 10.38. 161.	Netmask: 255.255.
lo0	Address: 10.38. 161.	Netmask: 255.255.

Turku

ge-0/0/1	Address: 10.38. 161.	Netmask: 255.255.
ge-0/0/2	Address: 10.38. 161.	Netmask: 255.255.
ge-0/0/3	Address: 10.38. 161.	Netmask: 255.255.
lo0	Address: 10.38. 161.	Netmask: 255.255.

Tampere

ge-0/0/1	Address: 10.38. 161.	Netmask: 255.255.
ge-0/0/2	Address: 10.38. 161.	Netmask: 255.255.
ge-0/0/3	Address: 10.38. 161.	Netmask: 255.255.
ge-1/0/0	Address: 10.38. 161.	Netmask: 255.255.
lo0	Address: 10.38. 161.	Netmask: 255.255.

Lappeenranta

ge-0/0/1	Address: 10.38. 161.	Netmask: 255.255.
ge-0/0/2	Address: 10.38. 161.	Netmask: 255.255.
ge-0/0/3	Address: 10.38. 161.	Netmask: 255.255.
lo0	Address: 10.38. 161.	Netmask: 255.255.

Vaasa

ge-0/0/1	Address: 10.38. 161.	Netmask: 255.255.
ge-0/0/2	Address: 10.38. 161.	Netmask: 255.255.
lo0	Address: 10.38. 161.	Netmask: 255.255.

Oulu

ge-0/0/1	Address: 10.38. 161.	Netmask: 255.255.
ge-0/0/2	Address: 10.38. 161.	Netmask: 255.255.
ge-0/0/3	Address: 10.38. 161.	Netmask: 255.255.
lo0	Address: 10.38. 161.	Netmask: 255.255.

LAN1

PC1	Address: 10.38. 161.	Netmask: 255.255.

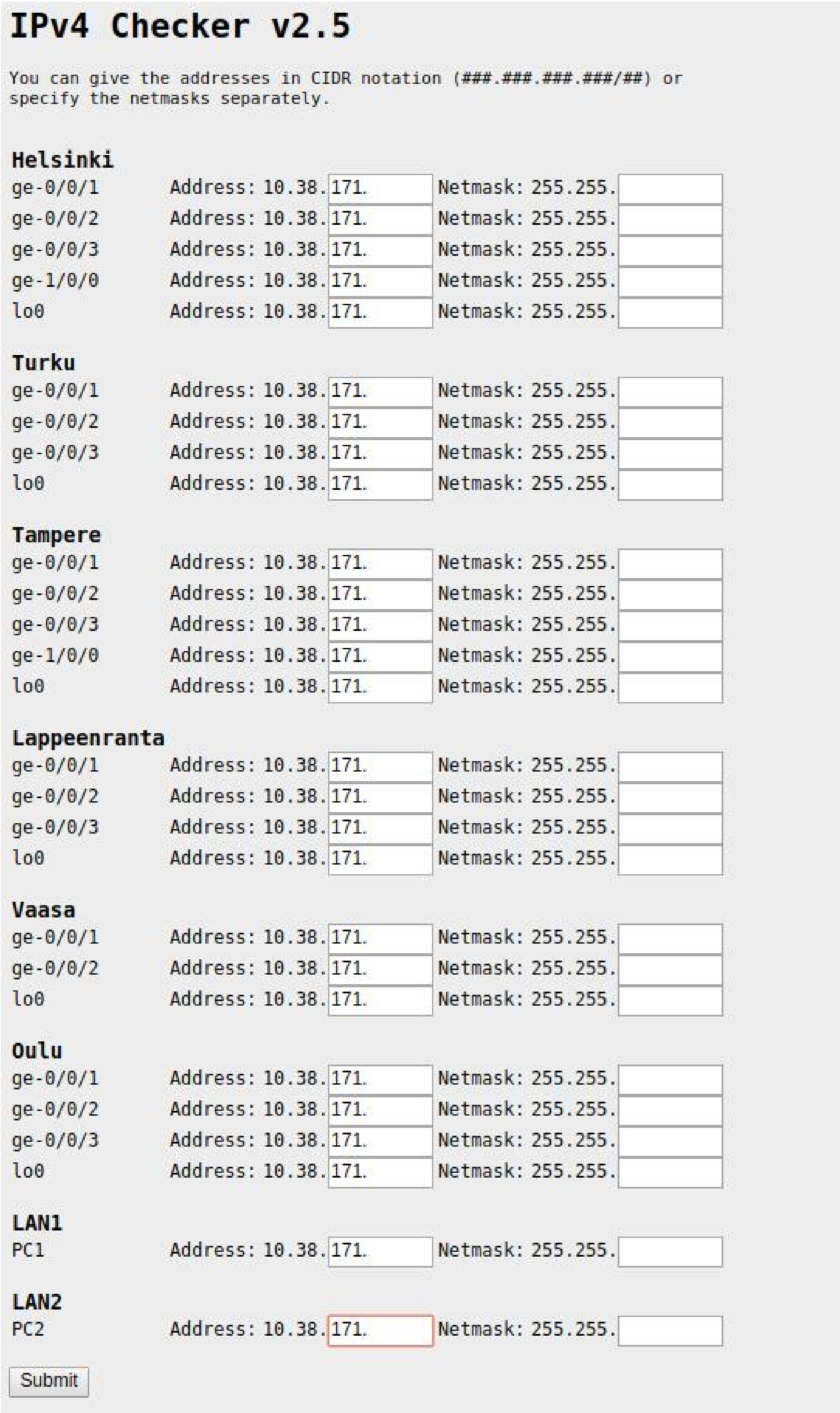
LAN2

PC2	Address: 10.38. 161.	Netmask: 255.255.

Submit

Figure 3: Group 1 IP checker

Appendix C



IPv4 Checker v2.5

You can give the addresses in CIDR notation (###.###.###.###/##) or specify the netmasks separately.

Helsinki

ge-0/0/1	Address: 10.38.171.	Netmask: 255.255.
ge-0/0/2	Address: 10.38.171.	Netmask: 255.255.
ge-0/0/3	Address: 10.38.171.	Netmask: 255.255.
ge-1/0/0	Address: 10.38.171.	Netmask: 255.255.
lo0	Address: 10.38.171.	Netmask: 255.255.

Turku

ge-0/0/1	Address: 10.38.171.	Netmask: 255.255.
ge-0/0/2	Address: 10.38.171.	Netmask: 255.255.
ge-0/0/3	Address: 10.38.171.	Netmask: 255.255.
lo0	Address: 10.38.171.	Netmask: 255.255.

Tampere

ge-0/0/1	Address: 10.38.171.	Netmask: 255.255.
ge-0/0/2	Address: 10.38.171.	Netmask: 255.255.
ge-0/0/3	Address: 10.38.171.	Netmask: 255.255.
ge-1/0/0	Address: 10.38.171.	Netmask: 255.255.
lo0	Address: 10.38.171.	Netmask: 255.255.

Lappeenranta

ge-0/0/1	Address: 10.38.171.	Netmask: 255.255.
ge-0/0/2	Address: 10.38.171.	Netmask: 255.255.
ge-0/0/3	Address: 10.38.171.	Netmask: 255.255.
lo0	Address: 10.38.171.	Netmask: 255.255.

Vaasa

ge-0/0/1	Address: 10.38.171.	Netmask: 255.255.
ge-0/0/2	Address: 10.38.171.	Netmask: 255.255.
lo0	Address: 10.38.171.	Netmask: 255.255.

Oulu

ge-0/0/1	Address: 10.38.171.	Netmask: 255.255.
ge-0/0/2	Address: 10.38.171.	Netmask: 255.255.
ge-0/0/3	Address: 10.38.171.	Netmask: 255.255.
lo0	Address: 10.38.171.	Netmask: 255.255.

LAN1

PC1	Address: 10.38.171.	Netmask: 255.255.

LAN2

PC2	Address: 10.38.171.	Netmask: 255.255.

Submit

Figure 4: Group 2 IP checker