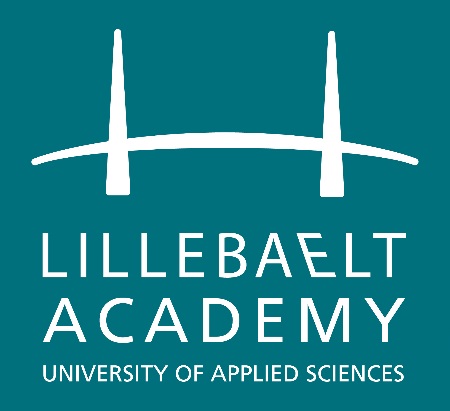
**IT Technology**

**Project Network report**



LILLEBAELT ACADEMY

UNIVERSITY OF APPLIED SCIENCE

Author

Michal Skorczewski

Martin Grønholdt

1st June 2017

**Table of Contents**

[1 Introduction 3](#_Toc484091486)

[1.1 Introduction 3](#_Toc484091487)

[1.2 Project Plan 3](#_Toc484091488)

[1.3 Responibilities 3](#_Toc484091489)

[2 Ethernet L2 & L3 Switching 3](#_Toc484091490)

[2.1 VLAN Implementation 3](#_Toc484091491)

[2.2 VLAN Trunking 3](#_Toc484091492)

[2.3 VLAN L3-Interface 3](#_Toc484091493)

[2.4 Virtual Routers 3](#_Toc484091494)

[2.5 Rthernet OAM 3](#_Toc484091495)

[2.6 Troubleshooting & Monitoring 3](#_Toc484091496)

[3 Intermediate Routing 3](#_Toc484091497)

[3.1 Ipv6 3](#_Toc484091498)

[3.2 OSPF 3](#_Toc484091499)

[3.3 IS-IS 3](#_Toc484091500)

[3.4 Route Re-Distribution (OSPF/IS-IS) 3](#_Toc484091501)

[3.5 BGP 3](#_Toc484091502)

[3.6 Route Re-Distribution (BGP/OSPF) 3](#_Toc484091503)

[4 Security 4](#_Toc484091504)

[4.1 Routing Policies 4](#_Toc484091505)

[4.2 Route Redistribution 4](#_Toc484091506)

[4.3 RE/PFE 4](#_Toc484091507)

[4.4 Firewall Filters 4](#_Toc484091508)

[4.5 CoS 4](#_Toc484091509)

[5 Conclusion 4](#_Toc484091510)

# Introduction

## Introduction

## Project Plan

|  |  |  |  |
| --- | --- | --- | --- |
| Task Name | Duration | Start | Finish |
| **Project Network 2. Semester** | **31.14 days?** | **Mon 1/9/17** | **Mon 5/8/17** |
| **Stage-1: Ethernet L2 & L3 Switching** | **9 days** | **Mon 1/9/17** | **Tue 2/14/17** |
| VLAN Implementation | 1 day | Mon 1/9/17 | Tue 1/10/17 |
| Vlan Trunking (802.1q) | 1 day | Tue 1/10/17 | Mon 1/16/17 |
| VLAN L3-Interface | 1 day | Mon 1/16/17 | Tue 1/17/17 |
| Virtual Routers (SRX & EX) | 2 days | Tue 1/17/17 | Tue 1/24/17 |
| Ethernet OAM | 1 day | Tue 1/24/17 | Mon 1/30/17 |
| Troubleshooting & Monitoring | 1 day | Mon 1/30/17 | Tue 1/31/17 |
| **Stage-2: Intermediate Routing** | **15 days** | **Tue 1/31/17** | **Mon 4/3/17** |
| IPv6 | 2 days | Tue 1/31/17 | Tue 2/14/17 |
| OSPF | 2 days | Tue 2/14/17 | Tue 2/21/17 |
| IS-IS | 2 days | Tue 2/21/17 | Tue 2/28/17 |
| Route Re-Distribution (OSPF/IS-IS) | 3 days | Tue 2/28/17 | Tue 3/7/17 |
| BGP (iBGP & eBGP w. OSPF) | 3 days | Tue 3/7/17 | Mon 3/20/17 |
| Route Redistribution (BGP/OSPF) | 3 days | Tue 3/21/17 | Mon 4/3/17 |
| **Stage-3: Security** | **12 days** | **Mon 4/3/17** | **Tue 5/16/17** |
| Routing Policies | 2 days | Mon 4/3/17 | Mon 4/10/17 |
| Route Redistribution | 2 days | Mon 4/10/17 | Mon 4/17/17 |
| RE/PFE | 2 days | Mon 4/17/17 | Tue 4/25/17 |
| Firewall Filters | 3 days | Tue 4/25/17 | Mon 5/8/17 |
| CoS | 3 days | Mon 5/8/17 | Tue 5/16/17 |
| **Finalize Report** | 4 days | Tue 5/16/17 | Mon 6/5/17 |
| ***Project End/Hand-in*** | 0 days | Mon 6/5/17 | Mon 6/5/17 |

## Responibilities

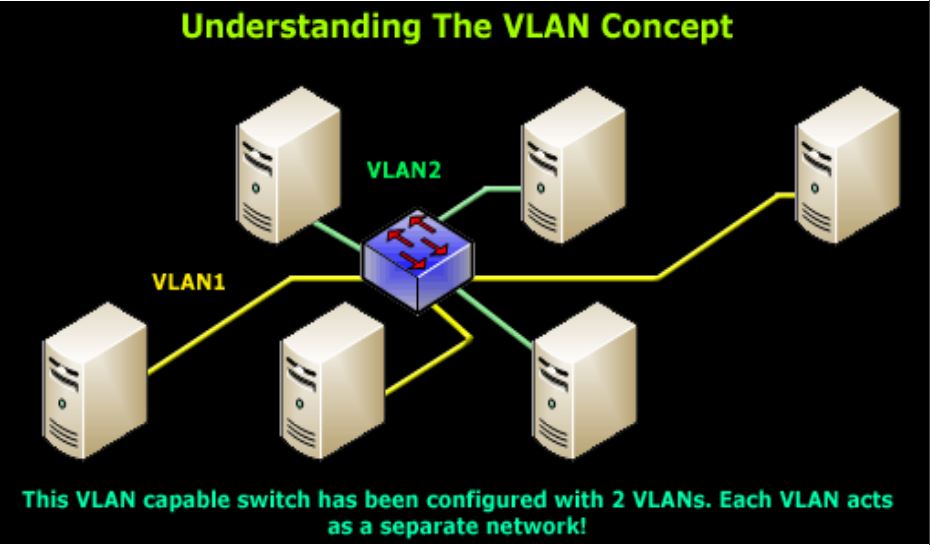
|  |  |
| --- | --- |
| Vlan Implementation | Michal Skorczewski |
| Vlan Trunking (802.1q) | Michal Skorczewski |
| Vlan L3- Interface | Michal Skorczewski |
| Vurtual Routers | Michal Skorczewski |
| Ethernet OAM | Michal Skorczewski |
| Troubleshooting & Monitoring | Michal Skorczewski |
|  |  |
| Ipv6 | Martin Gronholdt |
| OSPF | Martin Gronholdt |
| IS-IS | Martin Gronholdt |
| Route Re-distribution OSPF/IS-IS | Martin Gronholdt |
| BGP | Michal Skorczewski |
| Router Redistribution BGP/OSPF | Michal Skorczewski |
|  |  |
| Routing Policies | Michal Skorczewski |
| Route Redistribution | Martin Gronholdt |
| RE/PFE | Michal Skorczewski |
| Firewall Filters | Martin Gronholdt |
| CoS | Michal Skorczewski |

# Ethernet L2 & L3 Switching

Ethernet LANs were originally designed for small networks that primarly carried text, over years the type of data carried by LANs grew to include voice, graphics, and video. This complex data, when combined with the speed of transmission became too much of a load for the original Ehernet LAN design, packet collisions were slowing down larger LANs. The IEEE 802.1D-2004 standard helped evolve LANs to cope with the higher data and transmission requirements by defining the concept of bridging.

* Bridging divides a single physical LAN (now broadcast domain) into two or more virtual LANs
* By default, system on one VLAN don’t see the traffic associated with systems on other VLANs on the same network

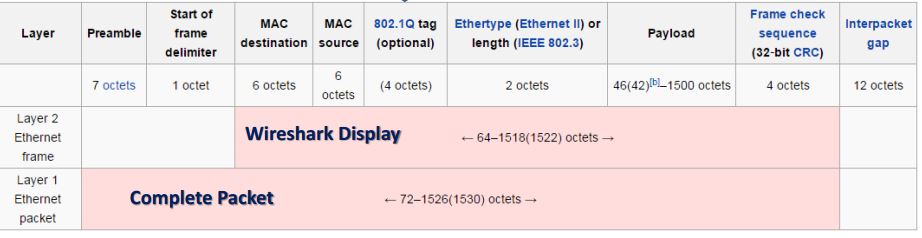
IEEE 802.1Q is the standard defining VLANs. Each VLAN is identified by a unique 802.1Q ID, only IDs 1 through 4094 can be assigned to VLANs during configuration, IDs 0 and 4095 are reserved by Junos OS and cannot be assigned.



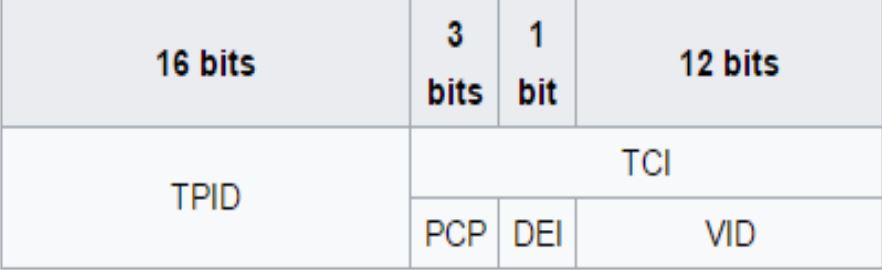
Ethernet packets includes:

* Tag protocol identifier
* EtherType field, which identidies the protocol being transported. When a device within a VLAN generates a packet, this field includes a value of 0x8100, which indicates that the packet is a VLAN-tagged packet.
* The packet also has a VLAN ID field that includes the unique 802.1Q ID, which identifies the VLAN to which the packet belongs

The Ethernet Frame + 802.1q Tag



The “layer 1 Ethernet Packet” is what is transmitted over the wire, bit-by-bit.  
The “layer 2 Ethernet Frame” is the display on monitor interface.



The 802.1q tag:

Tag protocol ID (TPID): a 16 bit field set ro a value of 0x8100

Tag control information (TCI)

* Priority code point (PCP): 3 bit field which refers to the IEEE 802.1p class of service and maps to the frame priority
* Drop eligible indicatior (DEI): 1 bit field, may be used separately or in conjunction with PCP to indicate frames eligible to be dropped in the presence of congestion
* VLAN identifier (VID) a 12 bit field specifying the VLAN to which the frame belongs

## VLAN Implementation

Step 1: Create a layer 2 vlan

*set vlans <vlan-name> vlan-id <vlan-id>*

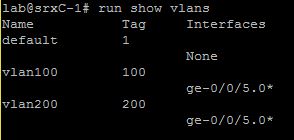
Step 2: Create a logical layer 3 VLAN interface:

*set interfaces vlan unit <unit> family inet address <ip address/mask>*

Step 3: Link the layer 2 VLAN to the layer 3 VLAN interface:

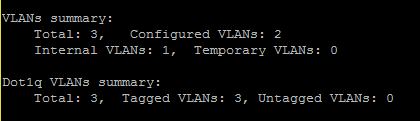
*set vlans <vlan-name> l3-interface vlan.<unit mentioned above>*

The result in project after implementing vlans can be displayed using command: *show vlans.*



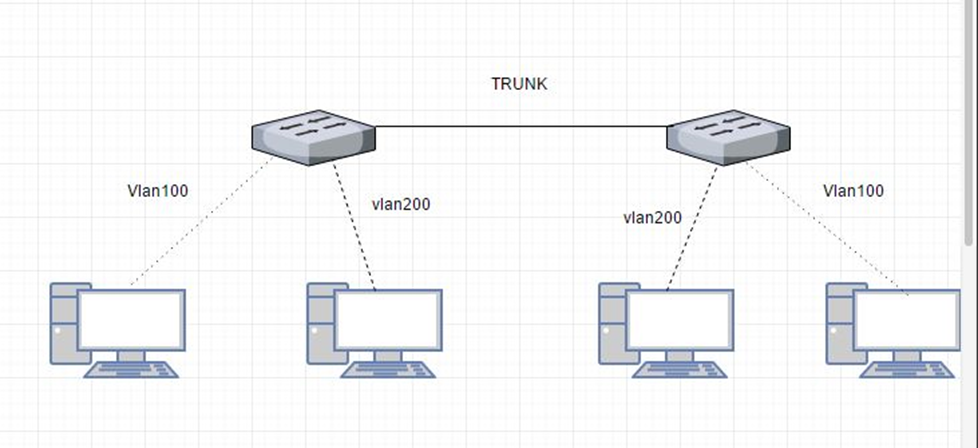
Other command that can be used to display configured vlans is: *show vlans summary.*

In the display, untagged and tagged vlans are shown.



## VLAN Trunking

Trunk mode interfaces are used to connect switches to one another. Traffic sent between switches can then consist of packets from multiple VLANs, with those packets multiplexed so they can be sent over the same physical connection.



The trunk interface is a switched interface, have to have a corresponding interface on a second switch.

QUICK CONFIGURATION:

*set interfaces <interface> unit <unit number> family ethernet-switching port-mode access vlan members <vlan-name>*

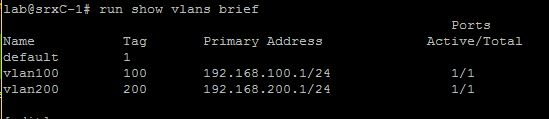
Only VLANs named in members <vlan-name> have access over the Trunk.

## VLAN L3-Interface

In order to configure the switch to perform L3 switching it is necessary to assign VLAN interface to VLAN using command:

*Set vlans <vlan name> l3-interface vlan.<vlan number>*

This is how it looks when the VLAN is implemented with L3 interface.



## Virtual Routers

In Junos Software, a virtual router is a routing instance type. It is a collection of routing tables, interfaces and routing option settings. Routing instance virtual router can act like a normal router, with policies and routing options. It allows to isolate traffic without using multiple routing devices to segment network.

To establish a virtual router it is necessary to follow few steps.

* Create a virtual router
* Assign an interface to a virtual router
* Assign an interface to a zone

It is possible to assign other routing option to virtual router.

To share routes in more than one routing instance it is optional to select physical or logical connection.

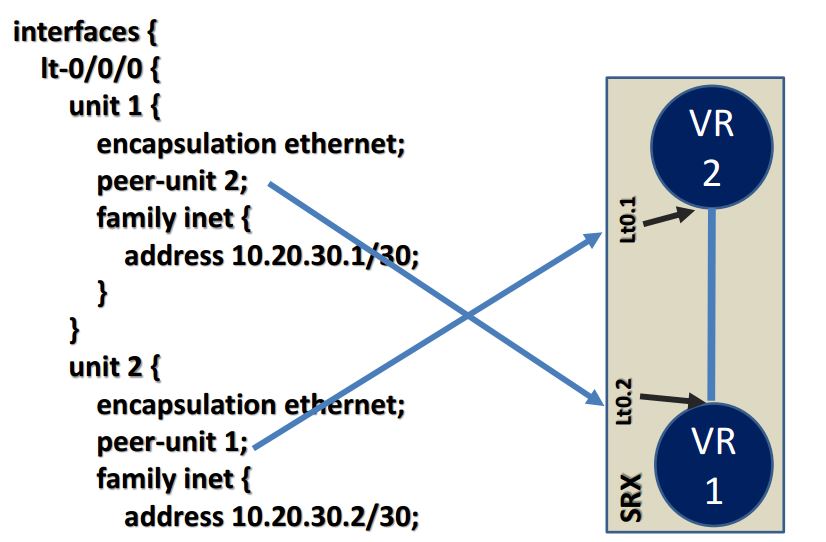
Physical connection is a normal interface (for example ge-0/0/0 or so-0/0/0) it can be established using cables or VMNets in VMware.

Logical Tunnels (lt0 interfaces) can be used only on SRX Juniper devices.

To connect two routing instances with a logical connection logical tunnel interface should be configured for each instance. Then, it is mandatory to configure a peer relationship between the logical tunnel interfaces, thus creating a point-to-point connection. To create a point-to-point connection logical tunnel has to configured using the lt-fpc/pic/port format.

Each logical tunnel interface should be configured with a proper encapsulation type.

It is important to configure only one peer unit for each logical interface. (Unit 0 cannot peer with both unit 1 and unit 2.)



## Rthernet OAM

Ethernet Operations, Administration, and Maintenance

Ethernet OAM is a set of tools that network manager use to know the way how Ethernet links are working. Ethernet OAM should:

* Rely only on the media access control (MAC) address or virtual local area network (VLAN) identifier for troubleshooting
* Work independently of the actual Ethernet transport and function over physical Ethernet ports, or a virtual service such as pseudowire, and so on.
* Isolate faults over a flat (or single operator) network architecture or a nested or hierarchical (or multi-provider) networks.

## Troubleshooting & Monitoring

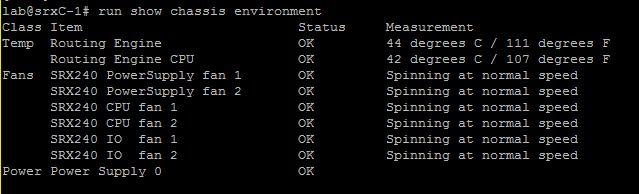
**Troubleshooting**

Juniper SRX device provides set of commands that can be used for troubleshooting. Mostly it is giving an opportunity to view log files, environment of router and alarms.

Few troubleshooting commands:

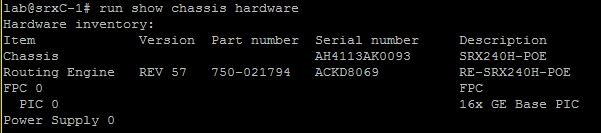
* show chassis environment

Command above allows to display temperatures, fans and power supply on SRX device.



* show chassis hardware

Using command above causes display hardware informations like serial numbers, part numbers and version.



* show chassis alarms

This command is used for displaying information about alarms in real time.

alarms

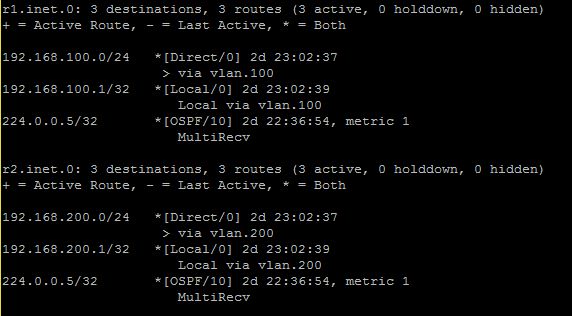
Troubleshooting commands above were used on Juniper SRXC-1 in schools lab.

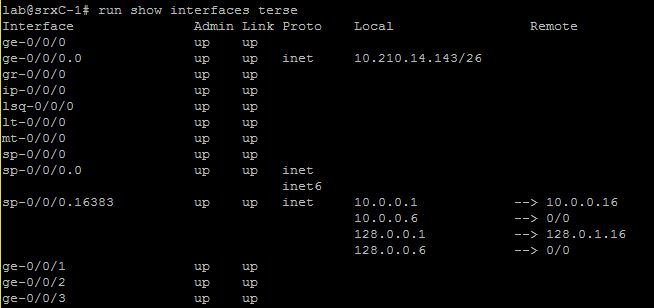
**Monitoring**

Except troubleshooting Juniper gives command to monitor interfaces, traffic and routes on device.

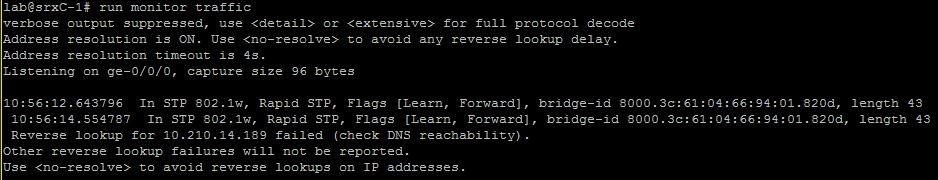
Most common command for monitoring routes in router is: *show route.*

Where next-hops, routes, preferences and protocols.



*show interfaces terse* allows to see admin and link state of interfaces as well as protocol its using and addresses.

In Juniper Devices it is possible to monitor traffic inside the router, using *monitor traffic.*



# Intermediate Routing

## Ipv6

## OSPF (all of configurations are located in Appendix)

### OSPF

OSPF is short for Open Shortest Path First and is the name of a routing protocol. OSPF is an interior gateway protocol which means that it is used to exchange routing information within an autonomous system. IOSPF Version 2 was defined in RFC2328 in 1998 and Version 3 in RFC5340 in 2008. Version 3 is an update to support IPv6.

OSPF forms IP datagrams directly and packages them using protocol number 89 and implements its own transport layer error detection and correction functions. OSPF uses multicast addressing for distributing routing information within a broadcast domain.

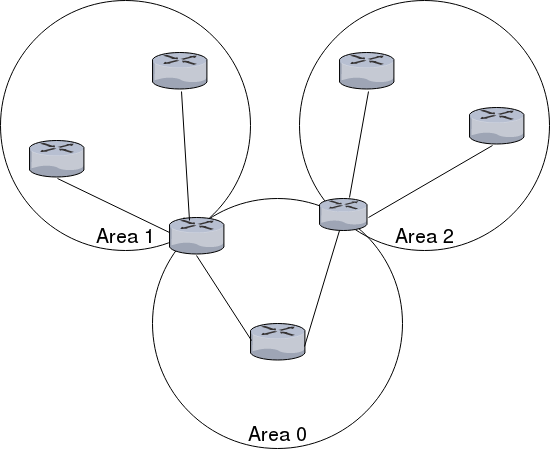
Routers running OSPF communicate with neighbouring routers on connected interfaces to establish the state of connections:

* **Down:** Initial state of the connection indicating that no resent communication has been received.
* **Init:** A HELLO packet has been received from a neighbour but the routers have not established two-way communication.
* **Exchange:** The router is sending its link state database to the neighbour in database description packets. Each packet has a sequence number that is explicitly acknowledged.
* **Loading:** The router requests the most recent link-state advertisements from its neighbor discovered in the Exchange state.
* **Full:** The end state when all adjacent routers has reached the Full state and the link state database of o the neighbours are fully synchronized.

### OSPF areas

Areas in OSPF are used to administratively group networks and host in an AS together, areas are identified by 32-bit numbers. The topology of an area is unknown outside that area

An example of a network split into areas are shown in Illustration 1. The routers fully inside the areas (circles) are called internal routers, these are all connected to devices inside the same area. The routers on the borders between to areas are called area border routers or ABRs. Area 0 has a special role as the backbone area that distributes routes between areas. All ABRs are connected to the backbone, and the backbone area most be contiguous, if not physically, by using virtual links. The backbone has no ABRs and the routers in area 1 has to go through area 0 to talk to routers in area 2. It is the backbones job to redistribute routing information between the other areas.

  
Illustration 1: OSPF areas

### Designated Router

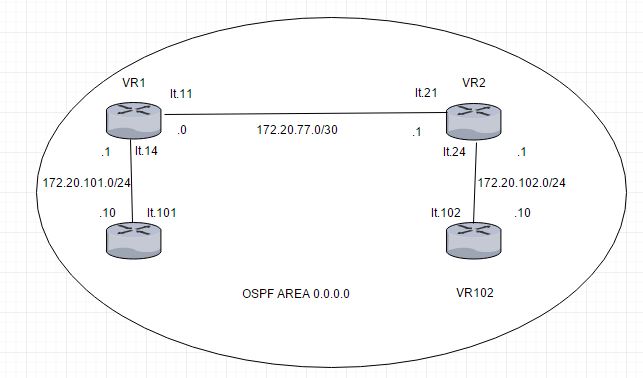
To not load down the network with routing traffic in large networks OSPF uses designated routers. Routers in the same network sends their link state information to the designated router. The designated router send the link advertisements on behalf of the network and participates in synchronising the link state database by establishing adjacencies. The designated router is found through election.

* The router priorities are evaluated and the router with the highest priority is selected as the designated router.
* If there is more than one router with the same priority, the one with the highest router identifier is chosen.
* If the no router ids are configured the election will go by the IP address of the first interface that comes online. This is usually the loopback interface.
* If nothing of the above, the first hardware interface with an IP address will be used for the election.

By default routing devices has a priority of 128. The priorities work like this:

* 0: the router will not e considered in the election.
* 1: the router has the least chance of being elected.

### Quick configuration example

  
Illustration 2: Network diagram og the OSPF example configuration.

The above diagram illustrates an example configuration of virtual router to use OSPF. Connection between the virtual routers are connected using logical tunnels.

This is the routing instance designated “VR1” in the illustration above:

routing-instances {

gangstin {

The logical tunnel interfaces and loopback interface are set up according to the illustration above.

instance-type virtual-router;

interface lt-0/0/0.11;

interface lt-0/0/0.14;

interface lo0.1;

Next comes the actual OSPF configuration. This configuration includes all interfaces in area 0, the backbone area.

protocols {

ospf {

area 0.0.0.0 {

interface lt-0/0/0.11;

interface lt-0/0/0.14;

interface lo0.1;

}

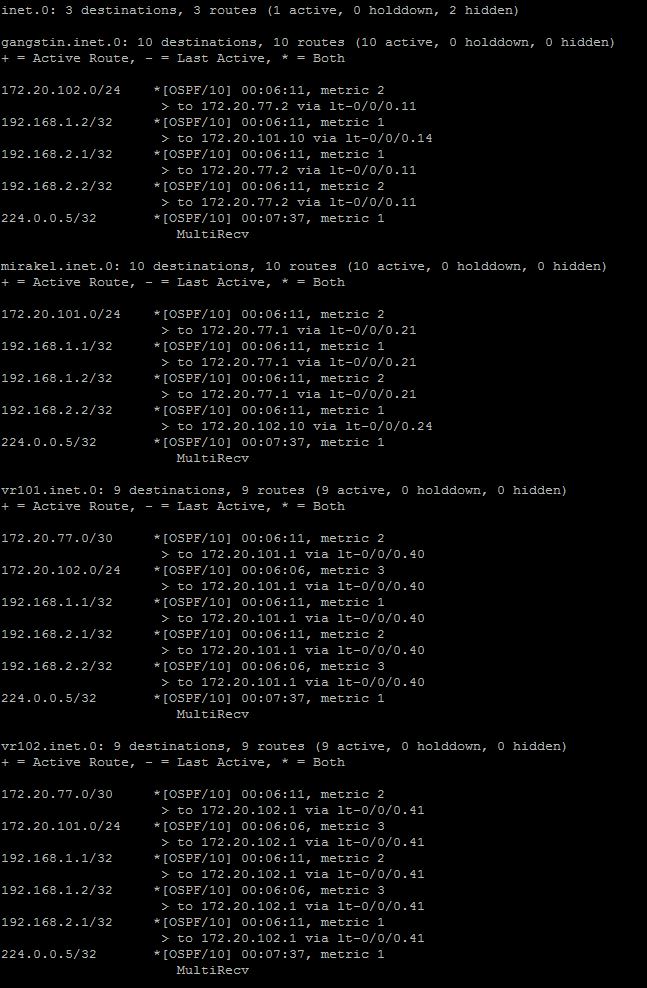
}

}

}

}

This configuration is mirrored on each virtual router, except of course the interfaces change according to the digram above.



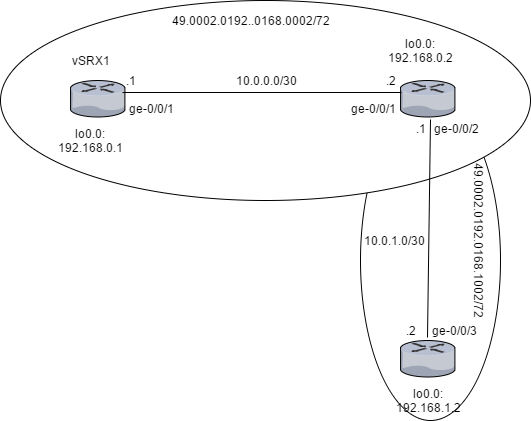
### Sources:

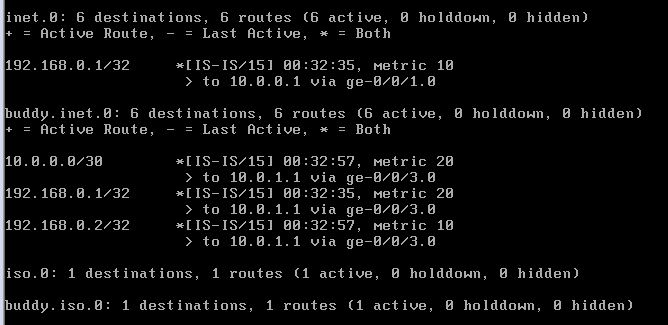
Wikipedia - Open Shortest Path First - <https://en.wikipedia.org/wiki/Open_Shortest_Path_First>

Juniper website - Understanding OSPF Areas - <https://www.juniper.net/documentation/en_US/junos/topics/concept/ospf-routing-understanding-ospf-areas-overview.html>

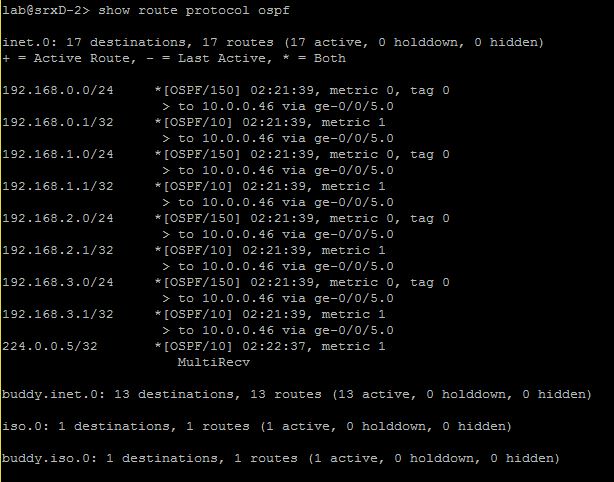
EAL - OSPF/Open Shortest Path First presentation

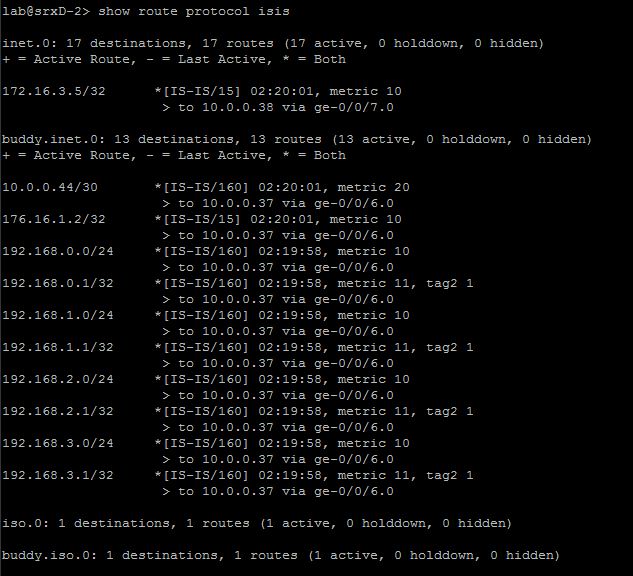
## IS-IS





## Route Re-Distribution (OSPF/IS-IS)

****

****

## BGP

## Route Re-Distribution (BGP/OSPF)

# Security

## Routing Policies

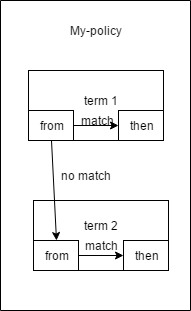
Routing Policy (all of configurations are located in Appendix)

Routing Policy allows user to control the flow of routing information between the routing protocols and the routing tables and between the routing tables and the forwarding table. Routing policy allows you to control which routes the routing protocols store in and retrieve from the routing table.

Routing policy was used because:

* It was not an intention to import all routes into routing table. Routes were specified by proper match criteria in terms.
* According to route redistribution It was intended to transfer active routes learned from another routing protocol (BGP/OSPF, IS-IS/OSPF)

Routing Policy Flow:



Number of terms in routing policy is equal or bigger than 0, the software evaluates terms until it reaches a terminating action or end policy. Names of policies and terms are defined by user.

Each term contains “from” and “then” statement. The first describe match condition(s) and the second one describe action that is taken if a “from” statement is matched.

Match criteria that was used in project:

* from protocol direct
* from protocol ospf
* route-filters (192.168.0.0/22 longer; 10.0.0.44/30 exact; 10.0.0.36/30 exact)

“from” statement describes match conditions

Match types used in project: longer, exact.

* Exact match the specified prefix and mask exactly (10.0.0.36/30 exact)
* Longer match routes that have longer masks (192.168.0.0/22 longer)

Actions

“then” statement describes the actions to take if a “from” statement is matched.

Just one terminating action was used in project, it was “accept”

Implementing Routing Policy.

Defined routing policy is always located under the [edit policy-options] hierarchy on Juniper Device. (configuration in Appendix)

Quick set-up:

[edit policy-options]

set policy-options policy statement ospf-isis term 1 from protocol ospf

set policy-options policy statement ospf-isis term 1 from route-filter 192.168.0.0/22 longer

set policy-options policy statement ospf-isis term 1 then accept

|  |  |
| --- | --- |
| policy-options { |  |
|  | policy-statement ospf-isis { |
|  | term 1 { |
|  | from { |
|  | protocol ospf; |
|  | route-filter 192.168.0.0/22 longer; |
|  | } |
|  | then accept; |
|  | } |
|  | } |

Applied routing policies as import or export policies can be found at different hierarchy levels (for example under routing-instances or protocols)

[edit protocols]

set isis export ospf-isis

set isis interface ge-0/0/7.0

set isis interface lo0.0

|  |  |
| --- | --- |
| protocols { |  |
|  | isis { |
|  | export [ ospf-isis send-direct-to-isis-neighbors ]; |
|  | interface ge-0/0/7.0; |
|  | interface lo0.0; |
|  | } |

Sources:

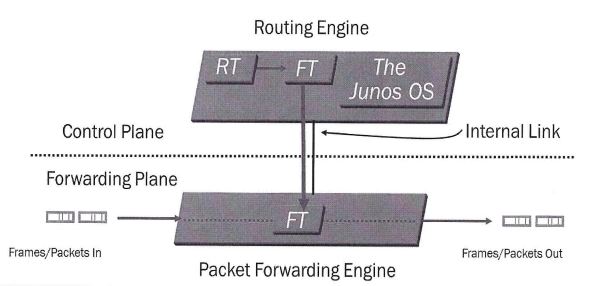
Routing Policy presentation

https://www.juniper.net/documentation/en\_US/junos/information-products/pathway-pages/config-guide-policy/config-guide-policy.html

## Route Redistribution

## RE/PFE

All platform running the JunosOS share a common design goal: clean separation of control and forwarding functions.



Routing Engine is located in control plane, it is the brain of the Juniper Device, responsible for performing protocol updates and system management, it runs various deamons that reside inside a protected memory environment. The Routing Engine maintains the routing tables, bridging table and forwarding table and conntects to the Packet Forwarding Engine through an internal link. The RE provides the CLI in addition to the J-Web GUI.

The Packet Forwarding Engine is responsible for forwarding transit traffic through the device. In many Juniper platforms the PFE uses application-specific integrated circuits (ASICs) for increased performance.

The PFE receives the layer 2 and layer 3 forwarding table (FT) from Routing Engine. FT updates are a high priority for the Junos OS kernel and are performed incrementally. It implements various services such as policing, stateless firewall filtering, and class of service

Transit Traffic consists of all traffic that enters an ingress network port, is compared against the forwarding table entries, and is forwarded out an egress network port toward its destination.

Exception Traffic does not pass through the local device but rather requires some form of special handling. Examples of exception traffic:

* Packets addressed to the chassis (telnet, pings traceroutes)
* Traffic that requires the generation of ICMP messages

Exception traffic is rare-limited on the internal link to protect the RE from potential DoS attacks

Source: Introduction to the Junos Operating System – Student Guide Revision V-15.a

## Firewall Filters

## CoS

# Conclusion

Sources:

Vlan presentation from Peter

<http://searchnetworking.techtarget.com/definition/virtual-LAN>

<https://kb.juniper.net/InfoCenter/index?page=content&id=KB11000>

<https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/l3-interface-bridging.html>

<https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/bridging-vrf-qfx-series-cli.html>

<https://kb.juniper.net/InfoCenter/index?page=content&id=KB21260>

https://www.juniper.net/documentation/en\_US/junos12.3/topics/concept/layer-2-802-1ag-ethernet-oam-overview-mx-solutions.html