

LAB MANUAL FOR JNCIA

Version 3.0

CONTENTS:

1. Routing Fundamental Labs

- 1.1. [Lab Exercise 1: Entering configuration mode on a router and exit](#)
- 1.2. [Lab Exercise 2: Setting host name](#)
- 1.3. [Lab Exercise 3: Setting routers domain name](#)
- 1.4. [Lab Exercise 4: Configure the root password \(Encrypted Password\)](#)
- 1.5. Lab Exercise 5: Configure a DNS name server
- 1.6. Lab Exercise 6: Configure a backup router
- 1.7. Lab Exercise 7: Router interface address configuration
- 1.8. Lab Exercise 8: Shut down an interface
- 1.9. Lab Exercise 9: Set interface description
- 1.10. Lab Exercise 10: Configuring encapsulation on a physical interface
- 1.11. Lab Exercise 11: Configuring No-keepalives
- 1.12. Lab Exercise 12: Set keepalive timers
- 1.13. Lab Exercise 13: Configuring management ethernet interface(fxp0)
- 1.14. Lab Exercise 14: Setting bandwidth on an interface
- 1.15. Lab Exercise 15: Setting the hold-time value on a physical interface
- 1.16. Lab Exercise 16: Setting the DTE clock rate
- 1.17. Lab Exercise 17: Basic gigabit ethernet configuration on a router
- 1.18. Lab Exercise 18: Configuring speed on sonet interface
- 1.19. Lab Exercise 19: Show chassis commands on J and M series routers

2. Static Routing Labs

- 2.1. [Lab Exercise 1: Configuring static routes](#)
- 2.2. [Lab Exercise 2: Ping Test](#)
- 2.3. Lab Exercise 3: Telnet
- 2.4. Lab Exercise 4: Traceroute

3. Policies Configuration Labs

- 3.1. [Lab Exercise 1: Routing policy lab 1](#)
- 3.2. Lab Exercise 2: Routing policy lab 2

4. RIP Configuration Labs

4.1. Lab Exercise 1: RIP configuration

5. Dynamic Routing Labs

5.1. Lab Exercise 1: Ping test by configuring RIP

5.2. Lab Exercise 2: Ping test by configuring OSPF with multiple areas

6. Show Commands Labs

6.1. Lab Exercise 1: Show commands lab

7. OSPF Labs

7.1. Lab Exercise 1: OSPF configuration

7.2. Lab Exercise 2: OSPF configuration and verification

8. BGP Labs

8.1 Lab Exercise: BGP configuration

9. MPLS Labs

9.1 Lab Exercise 1: Enabling MPLS family on the interface

9.2 Lab Exercise 2: Enabling MPLS protocol on the interface

9.3 Lab Exercise 3: Enabling LDP protocol on the interface

9.4 Lab Exercise 4: MPLS show commands

9.5 Lab Exercise 5: MPLS ping and traceroute

10. IPV6 Labs

10.1 Lab Exercise 1: Configuring IPv6 address on an interface in EUI-format

10.2 Lab Exercise 2: Configuring IPv6 address on an interface in general form

10.3 Lab Exercise 3: Ipv6 show commands

10.4 Lab Exercise 4: Configuring IPV6 static routes

10.5 Lab Exercise 5: Ping Test using IPV6

10.6 Lab Exercise 6: Traceroute on IPV6

11. Firewall Filter (ACL) Labs

11.1 Lab Exercise 1: Creating a Firewall filter

11.2 Lab Exercise 2: Applying firewall filter to an interface

11.3 Lab Exercise 3: View Firewall filter entries

11.4 Lab Exercise 4: Configuring and Verifying firewall filter Lab Scenario-1

12. Network Address Translation Labs

- 12.1 [Lab Exercise 1: Configuring Source NAT using Egress interface Address](#)
- 12.2 [Lab Exercise 2: Configuring Source NAT Translation pool](#)
- 12.3 Lab Exercise 3: Configuring Destination NAT pools
- 12.4 Lab Exercise 4: Creating Destination NAT rule set
- 12.5 Lab Exercise 5: Configuring Static NAT for single address translation
- 12.6 Lab Exercise 6: Configuring Source NAT using multiple rules Lab Scenario-1
- 12.7 Lab Exercise 7: Configuring Destination NAT using multiple rules

13. Exercises on DHCP

- 13.1 [Lab Exercise 1: Configuring juniper router as a DHCP Server](#)
- 13.2 Lab Exercise 2: DHCP client configuration
- 13.3 Lab Exercise 3: Assigning ip address to PC(computer) from DHCP server

14. Exercises on VPN

- 14.1 [Lab Exercise 1: Configuring Address Books and Address Sets](#)
- 14.2 [Lab Exercise 2: Configuring a security zone and bind the interfaces to the appropriate zones.](#)
- 14.3 Lab Exercise 3: Configuring host-inbound services for each interface in the zone
- 14.4 Lab Exercise 4: Configuring IKE Phase 1 Proposal
- 14.5 Lab Exercise 5: Configuring IKE Phase 1 Policy
- 14.6 Lab Exercise 6: Configuring IKE Phase 1 gateway and reference the IKE policy
- 14.7 Lab Exercise 7: Configuring IPSEC Phase 2 proposals
- 14.8 Lab Exercise 8: Configuring IPSEC Phase 2 policies and reference the IPSEC proposals
- 14.9 Lab Exercise 9: Configuring the IPSEC Phase 2 VPN tunnel and reference the IPSEC Phase 2 policy
- 14.10 Lab Exercise 10: Configuring Security Policies
- 14.11 Lab Exercise 11: Configuring and Verifying Policy based VPN
- 14.12 Lab Exercise 12: Configuring and Verifying Route based VPN

15. Basic Switch Labs

- 15.1. [Lab Exercise 1: Entering configuration mode on a switch and exit](#)
- 15.2. [Lab Exercise 2: Setting Hostname](#)
- 15.3. Lab Exercise 3: Set interface description
- 15.4. Lab Exercise 4: Shutdown an interface
- 15.5. Lab Exercise 5: Basic CLI commands
- 15.6. Lab Exercise 6: Configure bandwidth on an interface
- 15.7. Lab Exercise 7: Configuring ether-options on the gigabit ethernet switch interface
- 15.8. Lab Exercise 8: Configuring the management IP address on EX series switch

16. Lab Exercises on VLAN

- 16.1. [Lab Exercise 1: Define VLANs](#)
- 16.2. [Lab Exercise 2: Configure a port for membership in that VLAN](#)

- 16.3. Lab Exercise 3: Configuring an interface as a trunk port**
- 16.4. Lab Exercise 4: Configuring VLANs**
- 16.5. Lab Exercise 5: Configuring Routed VLAN interface (Inter-VLAN routing)**

17. Lab Exercises on Spanning tree protocol and VSTP

- 17.1. Lab Exercise 1: Configuring STP Timers**
- 17.2. Lab Exercise 2: Setting bridge priority on switch**
- 17.3. Lab Exercise 3: Configuring port priority**
- 17.4. Lab Exercise 4: Verifying STP_**
- 17.5. Lab Exercise 5: Enabling VSTP on all VLANs**
- 17.6. Lab Exercise 6: Enabling VSTP on a VLAN using a single VLAN-ID / VLAN-Name**

JUNOS Command Line Interface

The operating system software that powers the Juniper routers is called JUNOS. The software is modular and standards based. Another important feature of JUNOS is that the software is platform independent (within Juniper hardware systems, not to be confused with other vendor hardware), thus delivering the same scalability and security across several hardware platforms.

JUNOS CLI is a simple to use, text-based command interface. We give various commands on CLI for configuring, troubleshooting and monitoring the software.

JUNOS primarily supports two types of command modes.

- a) Operational Mode
- b) Configuration Mode

a) Operational Mode:

When we log in to the router and the CLI starts, we are at the top level of the CLI operational mode. In this mode, we enter the commands for

1. Controlling the CLI environment, and
2. Monitor and troubleshoot network connectivity, and
3. Initiating the Configuration Mode.

Frequently used commands in this mode include ping, show, traceroute, configure, etc.

b) Configuration Mode:

We use the Configuration mode for configuring the JUNOS software by creating a hierarchy of configuration statements. We enter the configuration mode by using the command "configure" as shown below:

```
user@host>configure
Entering configuration mode
[edit]
user@host#
```

Issuing the commands one at a time using CLI can configure a JUNOS™ router or alternately, we can configure by creating a text (ASCII) file that contains the statement hierarchy. Remember to activate the configuration by using the command "commit" on the router.

As shown in the above example, the generic configuration prompt is user@host#. Ofcourse, we can change the prompt by using appropriate command.

Statement Hierarchy:

We use the above configuration mode commands to create a statement hierarchy, and then configure the JUNOS software. The term "statement hierarchy" is used to define the sequence of commands used for configuring a particular feature (or features) of the router. An example statement hierarchy is given

below:

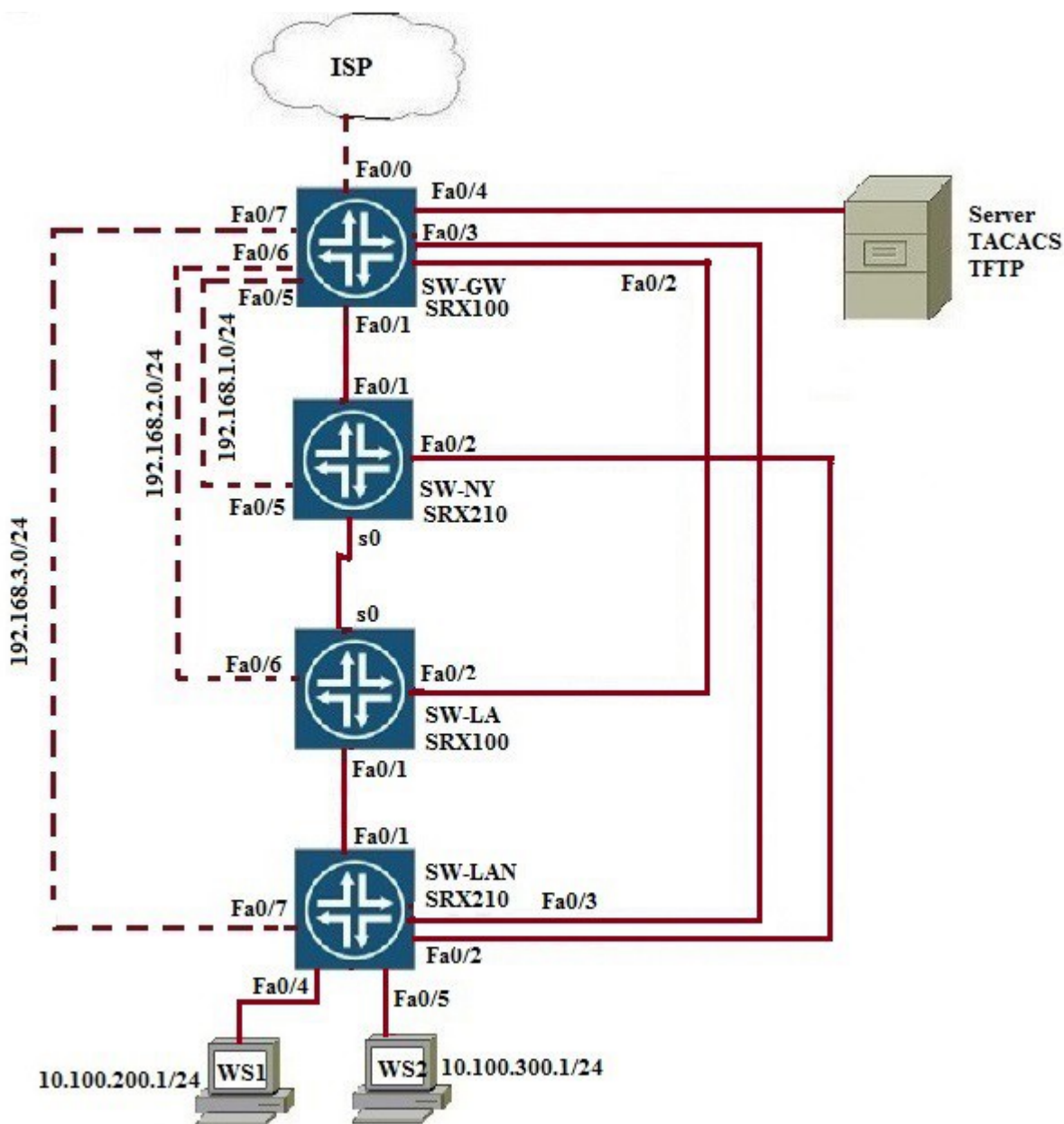
```
user@host>configure  
Entering configuration mode  
[edit] ----Top level  
user@host#edit protocols ospf  
[edit protocols ospf] ----protocols ospf hierarchy level  
user@host#
```

"set" commands are used to configure specific leaf statements.

Ex: user@host#set hello-interval 14

1. ROUTING FUNDAMENTAL LABS

Note: Please refer to the below default network Diagram for all the exercises given in this manual



1.1: Lab Exercise 1: Entering configuration mode on a Router, and exit

Description: A basic exercise, that shows how to enter configuration mode, and exit from the same.

Instructions:

1. Enter into configuration mode
2. Get back to the operational mode

```
anandsoft@SG100>configure
Entering configuration mode
[edit]
anandsoft@SG100#exit
anandsoft@SG100>
```

Explanation: The Junos OS CLI has two modes:

- **Operational mode** - This mode displays the current status of the device. In operational mode, you enter commands to monitor and troubleshoot the Junos OS, devices, and network connectivity. To enter the operational mode, type the CLI command. The character “>” identifies operational mode. For example, user@router>
- **Configuration mode** - A configuration for a device running on Junos OS is stored as a hierarchy of statements. In configuration mode, you enter these statements to define all properties of the Junos OS, including interfaces, general routing information, routing protocols, user access, and several system and hardware properties. You enter the configuration mode by issuing the configure command from the operational mode. The character “#” identifies configuration mode. For example, user@router#

[Back](#)

1.2: Lab Exercise 2: Setting Host Name

Description: Set the router host name.

Instructions:

1. Enter into configuration mode
2. Set hostname as juniper1

```
anandsoft@SG100>configure
[edit]
anandsoft@SG100#edit system
[edit system]
anandsoft@SG100#set host-name juniper1
[edit system]
user@juniper1#exit
[edit]
user@juniper1#commit
commit complete
[edit]
user@juniper1#show host-name
```

Explanation: The hostname of a device is its identification. A router or switch must have its identity established to be accessible on the network to other devices. That is perhaps the

most important reason to have a hostname, but a hostname has other purposes: Junos OS uses the configured hostname as part of the command prompt, to prepend log files and other accounting information, as well as in other places where knowing the device identity is useful. We recommend that the hostname be descriptive and memorable.

You can configure the hostname at the **[edit system]** hierarchy level

The output of show command after configuring hostname as “juniper1” is shown below.

```
anandsoft@SG100# show host-name
host-name juniper1;
[edit system]
```

You can also verify the same using the show command “show configuration” after committing the changes.

[Back](#)

1.3: Lab Exercise 3: Setting Routers Domain Name

Description: Set the router domain name.

Instructions:

1. Enter into configuration mode
2. Set domain name as mydomain.net.

```
anandsoft@SG100>configure
[edit]
anandsoft@SG100#edit system
[edit system]
anandsoft@SG100#set domain-name mydomain.net
[edit system]
anandsoft@SG100#exit
[edit]
anandsoft@SG100#commit
commit complete
[edit]
anandsoft@SG100#show domain-name
```

Explanation: Configure the name of the domain in which the router or switch is located. This is the default domain name that is appended to hostnames that are not fully qualified.

Below is the show output , where domain-name is configured as “mydomain.net”

```
[edit system]
anandsoft@SG100# show domain-name
domain-name mydomain.net;
```

[Back](#)

1.4: Lab Exercise 4: Configure the Root Password (Encrypted Password)

Description: This lab demonstrates configuring encrypted password on the router.

Instructions:

1. Enter into configuration mode
2. Move to the root-authentication hierarchy
3. Set the encrypted password as 24adr3e

```
anandsoft@SG100>configure
[edit]
anandsoft@SG100#edit system root-authentication
[edit system root-authentication]
anandsoft@SG100#set encrypted-password 24adr3e
[edit system root-authentication]
anandsoft@SG100#exit
[edit]
anandsoft@SG100#commit
commit complete
[edit]
anandsoft@SG100#show root-authentication encrypted-password
```

Explanation: The root user has complete privileges to operate and configure the Junos OS device, perform upgrades, and manage files in the file system. Initially, the root password is not defined on the Junos OS device. To ensure basic security, you must define the root password during initial configuration. If a root password is not defined, you cannot commit configuration settings on the device.

Below is show output where root-authentication password is set to “24adr3e”

```
anandsoft@SG100# show root-authentication encrypted-password
encrypted-password 24adr3e; ## SECRET-DATA
[edit system]
anandsoft@SG100#
```

[Back](#)

1.5: Lab Exercise 5: Configure a DNS Name Server

Not available in demo version

1.6: Lab Exercise 6: Configure a Backup Router

Not available in demo version

1.7: Lab Exercise 7: Router Interface Address Configuration

Not available in demo version

1.8: Lab Exercise 8: Shut down an Interface

Not available in demo version

1.9: Lab Exercise 9: Set Interface Description

Not available in demo version

1.10: Lab Exercise 10: Configuring the Encapsulation on a Physical Interface

Not available in demo version

1.11: Lab Exercise 11: Configuring No-Keepalives

Not available in demo version

1.12: Lab Exercise 12: Set Keepalive Timers

Not available in demo version

1.13: Lab Exercise 13: Configuring the Management Ethernet interface (fxp0)

Not available in demo version

1.14: Lab Exercise 14: Setting Bandwidth on an interface

Not available in demo version

1.15: Lab Exercise 15: Configuring the hold-time value on a physical interface to damp interface transitions

Not available in demo version

1.16: Lab Exercise 16: Configuring the DTE Clock Rate

Not available in demo version

1.17: Lab Exercise 17: Basic gigabit ethernet configuration on a router

Not available in demo version

1.18: Lab Exercise 18: Configuring speed on sonet interface

Not available in demo version

1.19: Lab Exercise 19: Show chassis commands on J and M-series routers

Not available in demo version

2. STATIC ROUTING LABS

2.1: Lab Exercise 1: Configuring Static Routes

Description: Configure static route 172.16.1.0 mask 255.255.255.0 with next hop address of 192.16.2.1.

Instructions:

1. Enter into Global Configuration Mode
2. Configure a static route to a destination sub-network (172.16.1.0) with 24-bit subnet mask and next hop IP address of 172.16.2.1.

```
anandsoft@SG100>configure
[edit]
anandsoft@SG100#edit routing-options
[edit routing-options]
anandsoft@SG100#edit static route 172.16.1.0/24
[edit routing-options static route 172.16.1.0/24]
anandsoft@SG100#set next-hop 172.16.2.1
[edit routing-options static route 172.16.1.0/24]
anandsoft@SG100#exit
[edit routing-options]
anandsoft@SG100#exit
[edit]
anandsoft@SG100#commit
commit complete
[edit]
anandsoft@SG100#show routing-options
anandsoft@SG100#exit
```

Explanation: Routes that are permanent fixtures in the routing and forwarding tables are often configured as static routes. These routes generally do not change, and often include only one or very few paths to the destination. To create a static route in the routing table,

you must, at minimum, define the route as static and associate a next-hop address with it. The static route in the routing table is inserted into the forwarding table when the next-hop address is reachable. All traffic destined for the static route is transmitted to the next-hop address for transit.

syntax: ip route prefix mask {address|interface} [distance]

prefix mask: is the ip route prefix and mask for the destination.

address|interface: Use either the next hop router ip or the local router outbound interface used to reach the destination.

distance: is the administrative distance and an optional parameter.

Below screenshot shows output of static route configuration.

```

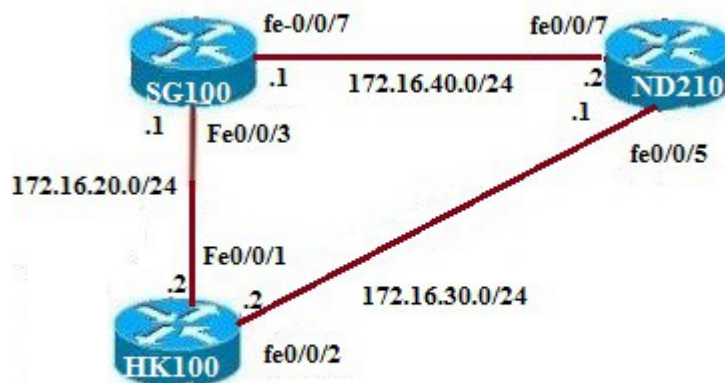
anandsoft@SG100# show routing-options
static {
  route 0.0.0.0/0 next-hop 192.168.0.1;
  route 172.16.1.0/24 next-hop 172.16.2.1;
}

```

[Back](#)

2.2: Lab Exercise 2: Ping test

Description: The purpose of this lab is to configure IP Address on all the devices and test for connectivity using ping command. Applicable network diagram is given below



Copyright © CertExams.com

Instructions:

1. Assign the IP address of all the devices as given below and commit the configurations

Device	Interface	IP Address	Mask

SG100	fe-0/0/7	172.16.40.1	255.255.255.0
	fe-0/0/3	172.16.20.1	255.255.255.0
ND210	fe-0/0/7	172.16.40.2	255.255.255.0
	fe-0/0/5	172.16.30.1	255.255.255.0
HK100	fe-0/0/1	172.16.20.2	255.255.255.0
	fe-0/0/2	172.16.30.2	255.255.255.0

2. From router SG100 issue a ping command to WS1 and WS2
3. Commands to be executed:

On SG100

```

anandsoft@SG100>configure
[edit]
anandsoft@SG100#edit interfaces fe-0/0/7
[edit interfaces fe-0/0/7]
anandsoft@SG100#edit unit 0 family inet
[edit interfaces fe-0/0/7 unit 0 family inet]
anandsoft@SG100#set address 172.16.40.1/24
[edit interfaces fe-0/0/7 unit 0 family inet]
anandsoft@SG100#exit
[edit interfaces fe-0/0/7]
anandsoft@SG100#exit
[edit]
anandsoft@SG100#edit interfaces fe-0/0/3
[edit interfaces fe-0/0/3]
anandsoft@SG100#edit unit 0 family inet
[edit interfaces fe-0/0/3 unit 0 family inet]
anandsoft@SG100#set address 172.16.20.1/24
[edit interfaces fe-0/0/3 unit 0 family inet]
anandsoft@SG100#exit
[edit interfaces fe-0/0/3]
anandsoft@SG100#exit
[edit]
anandsoft@SG100#set security zones security-zone trust host-inbound-traffic system-
services ping
[edit]
anandsoft@SG100#set security zones security-zone trust host-inbound-traffic system-
services telnet
[edit]
anandsoft@SG100#set security zones security-zone trust host-inbound-traffic system-
services ssh
[edit]

```

```
anandsoft@SG100#commit
commit complete
[edit]
anandsoft@SG100#
```

On ND210

```
anandsoft@ND210>configure
[edit]
anandsoft@ND210#edit interfaces fe-0/0/7
[edit interfaces fe-0/0/7]
anandsoft@ND210#edit unit 0 family inet
[edit interfaces fe-0/0/7 unit 0 family inet]
anandsoft@ND210#set address 172.16.10.2/24
[edit interfaces fe-0/0/7 unit 0 family inet]
anandsoft@ND210#exit
[edit interfaces fe-0/0/7]
anandsoft@ND210#exit
[edit]
anandsoft@ND210#edit interfaces fe-0/0/5
[edit interfaces fe-0/0/5]
anandsoft@ND210#edit unit 0 family inet
[edit interfaces fe-0/0/5 unit 0 family inet]
anandsoft@ND210#set address 172.16.30.1/24
[edit interfaces fe-0/0/5 unit 0 family inet]
anandsoft@ND210#exit
[edit interfaces fe-0/0/5]
anandsoft@ND210#exit
[edit]
anandsoft@ND210#set security zones security-zone trust host-inbound-traffic system-
services ping
[edit]
anandsoft@ND210#set security zones security-zone trust host-inbound-traffic system-
services telnet
[edit]
anandsoft@ND210#set security zones security-zone trust host-inbound-traffic system-
services ssh
[edit]
anandsoft@ND210#commit
commit complete
[edit]
anandsoft@ND210#
```

On HK100

```
anandsoft@HK100>configure
[edit]
anandsoft@HK100#edit interfaces fe-0/0/1
[edit interfaces fe-0/0/1]
anandsoft@HK100#edit unit 0 family inet
```

```
[edit interfaces fe-0/0/1 unit 0 family inet]
anandsoft@HK100#set address 172.16.20.2/24
[edit interfaces fe-0/0/1 unit 0 family inet]
anandsoft@HK100#exit
[edit interfaces fe-0/0/1]
anandsoft@HK100#exit
[edit]
anandsoft@HK100#edit interfaces fe-0/0/2
[edit interfaces fe-0/0/2]
anandsoft@HK100#edit unit 0 family inet
[edit interfaces fe-0/0/2 unit 0 family inet]
anandsoft@HK100#set address 172.16.30.2/24
[edit interfaces fe-0/0/2 unit 0 family inet]
anandsoft@HK100#exit
[edit interfaces fe-0/0/2]
anandsoft@HK100#exit
[edit]
anandsoft@HK100#set security zones security-zone trust host-inbound-traffic system-
services ping
[edit]
anandsoft@HK100#set security zones security-zone trust host-inbound-traffic system-
services telnet
[edit]
anandsoft@HK100#set security zones security-zone trust host-inbound-traffic system-
services ssh
[edit]
anandsoft@HK100#commit
commit complete
[edit]
anandsoft@HK100#
```

On SG100

```
anandsoft@SG100>ping 172.16.40.2
anandsoft@SG100>ping 172.16.20.2
```

[Back](#)

2.3: Lab Exercise 3: Telnet

Not available in demo version

2.4: Lab Exercise 4: Traceroute

Not available in demo version

3. POLICIES CONFIGURATION LABS

3.1: Lab Exercise 1: Routing Policy Lab 1

Description: Use this lab to configure the routing policy on router, by specifying the match condition to accept all rip routes, that is checked against the source address of the route advertised.

Instructions:

1. Enter into configuration mode.
2. Create a policy statement by name as same as riproutes.
3. Create a term under the policy created above by the name as AdvRip.
4. Create a match condition and specify to accept rip routes under the above term.

```
anandsoft@SG100>configure
[edit]
anandsoft@SG100#edit policy-options policy-statement riproutes
[edit policy-options policy-statement riproutes]
anandsoft@SG100#edit term AdvRip
[edit policy-options policy-statement riproutes term AdvRip]
anandsoft@SG100#edit from
[edit policy-options policy-statement riproutes term AdvRip from]
anandsoft@SG100#set protocol rip
[edit policy-options policy-statement riproutes term AdvRip from]
anandsoft@SG100#exit
[edit policy-options policy-statement riproutes term AdvRip]
anandsoft@SG100#edit then
[edit policy-options policy-statement riproutes term AdvRip then]
anandsoft@SG100#set accept
[edit policy-options policy-statement riproutes term AdvRip then]
anandsoft@SG100#exit
[edit policy-options policy-statement riproutes term AdvRip]
anandsoft@SG100#exit
[edit policy-options policy-statement riproutes]
anandsoft@SG100#exit
[edit]
anandsoft@SG100#commit
commit complete
[edit]
anandsoft@SG100#show policy-options
```

Explanation: Define a routing policy, including subroutine policies. A term is a named structure in which match conditions and actions are defined. Routing policies are made up of one or more terms. Each routing policy term is identified by a term name

Each term contains a set of match conditions and a set of actions:

- Match conditions are criteria that a route must match before the actions can be applied. If a route matches all criteria, one or more actions are applied to the route.
- Actions specify whether to accept or reject the route, control how a series of policies are evaluated, and manipulate the characteristics associated with a route.

show output of routing policy is given below

```
anandsoft@SG100> show policy-options
policy-statement riproutes {
  term Advrip {
    from protocol rip;
    then accept;
  }
}
```

3.2: Lab Exercise 2: Routing Policy Lab 2

Not available in demo version

4. RIP CONFIGURATION LAB

4.1: Lab Exercise 1: RIP Configuration

Description: Use this lab to configure the RIP on router, by applying an export and import policies at their respective hierarchical levels.

Instructions:

1. Enter into configuration mode.
2. Enable RIP routing on the router.
3. Create a group called neighborRouters apply an export policy riproutes to this group.
4. Specify the neighbor interface as ge-0/0/0 under the above created group and apply an import policy riproutes to this neighbor.

```
anandsoft@SG100>configure
[edit]
anandsoft@SG100#edit protocols rip
[edit protocols rip]
anandsoft@SG100#edit group neighborRouters
[edit protocols rip group neighborRouters]
anandsoft@SG100#set export riproutes
[edit protocols rip group neighborRouters]
anandsoft@SG100#edit neighbor ge-0/0/0
[edit protocols rip group neighborRouters neighbor ge-0/0/0]
anandsoft@SG100#set import riproutes
[edit protocols rip group neighborRouters neighbor ge-0/0/0]
anandsoft@SG100#exit
[edit protocols rip group neighborRouters]
anandsoft@SG100#exit
```

```
[edit protocols rip]
anandsoft@SG100#exit
[edit]
anandsoft@SG100#commit
commit complete
[edit]
anandsoft@SG100#show
```

Explanation: Apply a policy to routes being exported to the neighbors.

By default, RIP does not export routes it has learned to its neighbors. To enable RIP to export routes, apply one or more export policies.

To filter routes being imported by the local routing device from its neighbors, include the import statement, and list the names of one or more policies to be evaluated. If you specify more than one policy, they are evaluated in order (first to last) and the first matching policy is applied to the route. If no match is found, the local routing device does not import any routes.

Below screenshot shows import and export policy defined on RIP

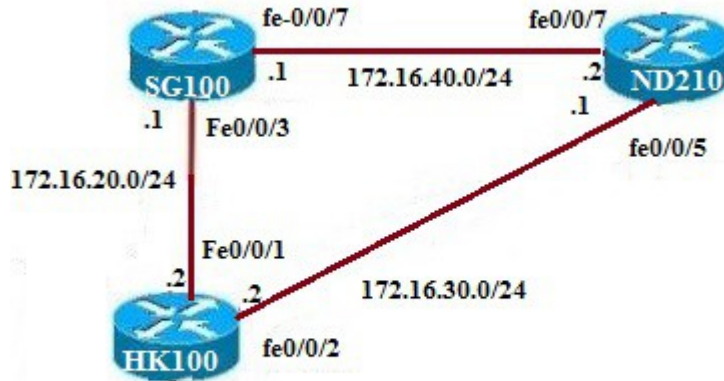
```
protocols <
  rip <
    group neighborRouters <
      export riproutes;
      neighbor ge-0/0/0.0 <
        import riproutes;
      >
    >
  >
```

[Back](#)

5. DYNAMIC ROUTING LABS

5.1: Lab Exercise 1: Ping test by configuring RIP

Description: The purpose of this lab is to configure RIP Routing and other required commands to advertise these rip routes on all the devices and test for ping command. Applicable network diagram is given below:



Copyright © CertExams.com

Instructions:

1. Assign the IP address of all the devices as given below

Device	Interface	IP Address	Mask
SG-100	fe-0/0/7	172.16.40.1	255.255.255.0
	fe-0/0/3	172.16.20.1	255.255.255.0
ND-210	fe-0/0/7	172.16.40.2	255.255.255.0
	fe-0/0/5	172.16.30.1	255.255.255.0
HK100	fe-0/0/1	172.16.20.2	255.255.255.0
	fe-0/0/2	172.16.30.2	255.255.255.0

2. Enable RIP routing on all the devices
3. Specify the policy to accept the rip routes on all the devices
4. Apply an import policy and an export policy (policy created above) on all the devices.
5. Issue “show rip neighbor” command on all the devices to view its neighbor information
6. From SG100 issue a ping command to ND210

On SG100:

```

anandsoft@SG100>configure
[edit]
anandsoft@SG100#edit interfaces fe-0/0/7 unit 0 family inet
[edit interfaces fe-0/0/7 unit 0 family inet]
anandsoft@SG100#set address 172.16.40.1/24

```

```

[edit interfaces fe-0/0/7 unit 0 family inet]
anandsoft@SG100#exit
[edit]
anandsoft@SG100#edit interfaces fe-0/0/3 unit 0 family inet
[edit interfaces fe-0/0/3 unit 0 family inet]
anandsoft@SG100#set address 172.16.20.2/24
[edit interfaces fe-0/0/3 unit 0 family inet]
anandsoft@SG100#exit
[edit]
anandsoft@SG100#edit policy-options policy-statement R1pol term R1term
[edit policy-options policy-statement R1pol term R1term]
anandsoft@SG100#edit from
[edit policy-options policy-statement R1pol term R1term from]
anandsoft@SG100#set protocol rip
[edit policy-options policy-statement R1pol term R1term from]
anandsoft@SG100#exit
[edit policy-options policy-statement R1pol term R1term]
anandsoft@SG100#edit then
[edit policy-options policy-statement R1pol term R1term then]
anandsoft@SG100#set accept
[edit policy-options policy-statement R1pol term R1term then]
anandsoft@SG100#exit
[edit policy-options policy-statement R1pol term R1term]
anandsoft@SG100#exit
[edit]
anandsoft@SG100#edit protocols rip group R1grp
[edit protocols rip group R1grp]
anandsoft@SG100#set export R1pol
[edit protocols rip group R1grp]
anandsoft@SG100#edit neighbor fe-0/0/7
[edit protocols rip group R1grp neighbor fe-0/0/7]
anandsoft@SG100#set import R1pol
[edit protocols rip group R1grp neighbor fe-0/0/7]
anandsoft@SG100#exit
[edit protocols rip group R1grp]
anandsoft@SG100#edit neighbor fe-0/0/3
[edit protocols rip group R1grp neighbor fe-0/0/3]
anandsoft@SG100#set import R1pol
[edit protocols rip group R1grp neighbor fe-0/0/3]
anandsoft@SG100#exit
[edit protocols rip group R1grp]
anandsoft@SG100#exit

[edit]
anandsoft@SG100#commit
commit complete
[edit]
anandsoft@SG100#exit
anandsoft@SG100>show rip neighbor

```

On ND210:

```
anandsoft@ND210>configure
[edit]
anandsoft@ND210#edit interfaces fe-0/0/7 unit 0 family inet
[edit interfaces fe-0/0/7 unit 0 family inet]
anandsoft@ND210#set address 172.16.40.2/24
[edit interfaces fe-0/0/7 unit 0 family inet]
anandsoft@ND210#exit
[edit]
anandsoft@ND210#edit interfaces fe-0/0/5 unit 0 family inet
[edit interfaces fe-0/0/5 unit 0 family inet]
anandsoft@ND210#set address 172.16.30.1/24
[edit interfaces fe-0/0/5 unit 0 family inet]
anandsoft@ND210#exit
[edit]
anandsoft@ND210#edit policy-options policy-statement R2pol term R2term
[edit policy-options policy-statement R2pol term R2term]
anandsoft@ND210#edit from
[edit policy-options policy-statement R2pol term R2term from]
anandsoft@ND210#set protocol rip
[edit policy-options policy-statement R2pol term R2term from]
anandsoft@ND210#exit
[edit policy-options policy-statement R2pol term R2term]
anandsoft@ND210#edit then
[edit policy-options policy-statement R2pol term R2term then]
anandsoft@ND210#set accept
[edit policy-options policy-statement R2pol term R2term then]
anandsoft@ND210#exit
[edit policy-options policy-statement R2pol term R2term]
anandsoft@ND210#exit
[edit]
anandsoft@ND210#edit protocols rip group R2grp
[edit protocols rip group R2grp]
anandsoft@ND210#set export R2pol
[edit protocols rip group R2grp]
anandsoft@ND210#edit neighbor fe-0/0/7
[edit protocols rip group R2grp neighbor fe-0/0/7]
anandsoft@ND210#set import R2pol
[edit protocols rip group R2grp neighbor fe-0/0/7]
anandsoft@ND210#exit
[edit protocols rip group R2grp]
anandsoft@ND210#edit neighbor fe-0/0/5
[edit protocols rip group R2grp neighbor fe-0/0/5]
anandsoft@ND210#set import R2pol
[edit protocols rip group R2grp neighbor fe-0/0/5]
anandsoft@ND210#exit
[edit protocols rip group R2grp]
anandsoft@ND210#exit
[edit]
```

```
anandsoft@ND210#commit
commit complete
[edit]
anandsoft@ND210#exit
anandsoft@ND210>show rip neighbor
```

On HK100

```
anandsoft@HK100>configure
[edit]
anandsoft@HK100#edit interfaces fe-0/0/1 unit 0 family inet
[edit interfaces fe-0/0/1 unit 0 family inet]
anandsoft@HK100#set address 172.16.20.2/24
[edit interfaces fe-0/0/1 unit 0 family inet]
anandsoft@HK100#exit
[edit]
anandsoft@HK100#edit interfaces fe-0/0/2 unit 0 family inet
[edit interfaces fe-0/0/2 unit 0 family inet]
anandsoft@HK100#set address 172.16.30.2/24
[edit interfaces fe-0/0/2 unit 0 family inet]
anandsoft@HK100#exit
[edit]
anandsoft@HK100#edit policy-options policy-statement R3pol term R3term
[edit policy-options policy-statement R3pol term R3term]
anandsoft@HK100#edit from
[edit policy-options policy-statement R3pol term R3term from]
anandsoft@HK100#set protocol rip
[edit policy-options policy-statement R3pol term R3term from]
anandsoft@HK100#exit
[edit policy-options policy-statement R3pol term R3term]
anandsoft@HK100#edit then
[edit policy-options policy-statement R3pol term R3term then]
anandsoft@HK100#set accept
[edit policy-options policy-statement R3pol term R3term then]
anandsoft@HK100#exit
[edit policy-options policy-statement R3pol term R3term]
anandsoft@HK100#exit
[edit]
anandsoft@HK100#edit protocols rip group R3grp
[edit protocols rip group R3grp]
anandsoft@HK100#set export R3pol
[edit protocols rip group R3grp]
anandsoft@HK100#edit neighbor fe-0/0/1
[edit protocols rip group R3grp neighbor fe-0/0/1]
anandsoft@HK100#set import R3pol
[edit protocols rip group R3grp neighbor fe-0/0/1]
anandsoft@HK100#exit
[edit protocols rip group R3grp]
anandsoft@HK100#edit neighbor fe-0/0/2
[edit protocols rip group R3grp neighbor fe-0/0/2]
```

```

anandsoft@HK100#set import R3pol
[edit protocols rip group R3grp neighbor fe-0/0/2]
anandsoft@HK100#exit
[edit protocols rip group R3grp]
anandsoft@HK100#exit
[edit]
anandsoft@HK100#commit
commit complete
[edit]
anandsoft@HK100#exit
anandsoft@HK100>show rip neighbor

```

“show rip neighbor” command output on SG100 is given below

```

anandsoft@SG100> show rip neighbor
Neighbor          Local   Source      Destination  Send  Receive  In
                  State  Address     Address      Mode  Mode     Met
                  -----
fe-0/0/3.0        Up     172.16.20.1  224.0.0.9    mcast both    1
fe-0/0/7.0        Up     172.16.40.1  224.0.0.9    mcast both    1
anandsoft@SG100> █

```

On SG100

```

anandsoft@SG100>ping 172.16.40.2
anandsoft@SG100>ping 172.16.20.2

```

[Back](#)

5.2: Lab Exercise 2: Ping test by configuring OSPF with multiple areas

Not available in demo version

6. SHOW COMMAND LAB

6.1: Lab Exercise 1: Show Commands

Description: This exercise demonstrates various basic show commands available.

Instructions:

1. Issue show version brief command.
2. Issue show cli command.
3. Issue show cli history command.

anandsoft@SG100>show version brief

anandsoft@SG100>show cli

anandsoft@SG100>show cli history

Explanation: Below fig. lists the output fields for the “show cli history” command. Output fields are listed in the approximate order in which they appear

```
anandsoft@SG100> show cli history
14:01:16 -- show version brief
14:02:06 -- show cli
14:02:53 -- show cli history
anandsoft@SG100> █
```

The “show cli” command displays configured CLI settings. Below screenshot is the output from “show cli” command

```
anandsoft@SG100> show cli
CLI complete-on-space set to on
CLI idle-timeout disabled
CLI restart-on-upgrade set to on
CLI screen-length set to 24
CLI screen-width set to 80
CLI terminal is 'xterm'
CLI is operating in enhanced mode
CLI timestamp disabled
CLI working directory is '/cf/var/home/anandsoft'
```

The “show version brief” command displays the hostname and version information about the software running on the router or switch.

```
anandsoft@SG100> show version brief
Hostname: SG100
Model: srx100h2
JUNOS Software Release [12.1X44-D35.5]
anandsoft@SG100>
```

[Back](#)

7. OSPF LABS

7.1: Lab Exercise 1: OSPF Configuration

Description: Use this lab to configure the OSPF on router with an area 0.

Instructions:

1. Enter into configuration mode.
2. Enable OSPF routing on the router.
3. Put the interfaces fe-0/0/6 and fe-0/0/7 under area 0

```
anandsoft@SG100>configure
[edit]
anandsoft@SG100#edit protocols ospf
[edit protocols ospf]
anandsoft@SG100#edit area 0
[edit protocols ospf area 0]
anandsoft@SG100#edit interface fe-0/0/6
[edit protocols ospf area 0 interface fe-0/0/6]
anandsoft@SG100#exit
[edit protocols ospf area 0]
anandsoft@SG100#edit interface fe-0/0/7
[edit protocols ospf area 0 interface fe-0/0/7]
anandsoft@SG100#exit
[edit protocols ospf area 0]
anandsoft@SG100#exit
[edit protocols ospf]
anandsoft@SG100#exit
[edit]
anandsoft@SG100#show
```

Explanation: To activate OSPF on a network, you must enable the OSPF protocol on all interfaces within the network on which OSPF traffic is to travel. To enable OSPF, you must configure one or more interfaces on the device within an OSPF area. Once the interfaces are configured, OSPF LSAs are transmitted on all OSPF-enabled interfaces, and the network topology is shared throughout the network.

Below screenshot is the show output of ospf configuration where interfaces fe-0/0/6 and fe--0/0/7 are assigned to area 0

```
protocols {
  ospf {
    area 0.0.0.0 {
      interface fe-0/0/6.0;
      interface fe-0/0/7.0;
    }
  }
}
```

[Back](#)

7.2: Lab Exercise 2: OSPF configuration and verification

Not available in demo version

8. BGP Labs

8.1: Lab Exercise 1: BGP Configuration

Note: This Lab is divided into 6 sections.

Section I: To configure the BGP peer sessions.

Description: This lab exercises demonstrates the configuring BGP peer sessions

Instructions:

1. Enter into configuration mode of device SG100
2. Move to interfaces hierarchy
3. Configure the ip address and description of the interface
4. Exit from the interfaces hierarchy

```
anandsoft@SG100>configure
[edit]
anandsoft@SG100#edit interfaces
[edit interfaces]
anandsoft@SG100#set fe-0/0/1 description to-A
[edit interfaces]
anandsoft@SG100#set fe-0/0/1 unit 0 family inet address 172.16.10.1/24
[edit interfaces]
anandsoft@SG100#set fe-0/0/2 description to-B
[edit interfaces]
anandsoft@SG100#set fe-0/0/2 unit 0 family inet address 10.100.100.2/24
[edit interfaces]
anandsoft@SG100#exit
[edit]
anandsoft@SG100#
```

[Back](#)

Section II: Setting the AS number

Not available in demo version

Section III: Create BGP group and add the External neighbor addresses

Not available in demo version

Section IV: Specify the AS number of the external AS.

Not available in demo version

Section V: Set the peer type to external BGP (EBGP)

Not available in demo version

Section VI: Setting the bgp hold-time

Not available in demo version

9. MPLS labs

9.1: Lab Exercise 1: Enabling MPLS family on the interface

Description: A basic exercise that shows how to enter configuration mode and exit from the same.

Instructions:

1. Enter into configuration mode
2. Enter the *[edit interfaces]* mode to configure MPLS.
3. Confirm the configuration by entering the show command from configuration mode

```
anandsoft@SG100>configure
[edit]
anandsoft@SG100#edit interfaces ge-0/0/0
[edit interfaces ge-0/0/0]
anandsoft@SG100#set unit 0 family mpls
[edit interfaces ge-0/0/0]
anandsoft@SG100#exit
[edit]
anandsoft@SG100#commit
commit complete
[edit]
anandsoft@SG100#show
```

Explanation: For MPLS to be activated, it is necessary to add the MPLS protocol family to the interfaces that will bear MPLS traffic. MPLS must also be configured under the *[edit protocols]* level of hierarchy as shown in the above example

Show command output is shown below where mpls is enabled on ge-0/0/0 interface

```
ge-0/0/0 <
  unit 0 <
    family inet <
      address 192.168.1.1/24;
    >
    family mpls;
  >
>
```

<Output omitted for brevity>

[Back](#)

9.2: Lab Exercise 2: Enabling MPLS protocol on the interface

Description: The lab exercise explains how to configure MPLS protocol on the interface.

Instructions:

1. Enter into configuration mode
2. Move to the protocols hierarchy
3. Enable the MPLS protocol on all or particular interface
4. Exit from the protocol hierarchy.
5. Confirm the configuration by entering the show command from configuration mode

```
anandsoft@SG100>configure
[edit]
anandsoft@SG100#edit protocols mpls
[edit protocols mpls]
anandsoft@SG100#set interface all
[edit protocols mpls]
anandsoft@SG100#exit
[edit]
anandsoft@SG100#commit
commit complete
[edit]
anandsoft@SG100#show
```

To enable the MPLS protocol on particular interface following command is used.

```
anandsoft@SG100>configure
[edit]
anandsoft@SG100#edit protocols mpls
[edit protocols mpls]
anandsoft@SG100#set interface ge-0/0/0
```

Explanation: Below show output shows MPLS protocol is enabled on all the interfaces of device SG100

```
protocols {  
  mpls {  
    interface all;  
  }  
}
```

<Output omitted for brevity>

[Back](#)

9.3: Lab Exercise 3: Enabling LDP protocol on the interface

Not available in demo version

9.4: Lab Exercise 4: MPLS show commands

Not available in demo version

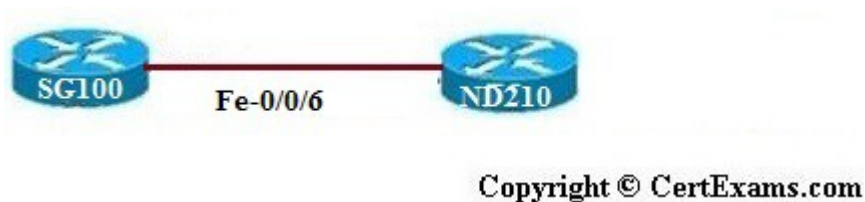
9.5: Lab exercise 5: MPLS ping and traceroute

Not available in demo version

10. IPV6 labs

Note: Please refer to the below network for the exercises 10.1, 10.2, 10.3 given in this section

Enabling IPV6: In junos ipv6 is enabled as soon as one interface is configured for ipv6



10.1: Lab Exercise 1: Configuring IPv6 address on an interface in EUI-format

Description: This lab exercise explains configuring ipv6 address on an interface in EUI-64 format

Instructions:

1. Enter into configuration mode
2. Enter the [edit interfaces] mode to configure the ipv6 address of fe-0/0/6 interface of SG100.
3. Confirm the configuration by entering the show command from configuration mode

On SG100

```
anandsoft@SG100>configure
[edit]
anandsoft@SG100#edit interfaces fe-0/0/6
[edit interfaces fe-0/0/6]
anandsoft@SG100#set unit 0 family inet6 address 3ffb:db8:1::/64 EUI-64
[edit interfaces fe-0/0/6]
anandsoft@SG100#exit
[edit]
anandsoft@SG100#show interfaces fe-0/0/6
```

Explanation: Below is screenshot from show output, ipv6 address configured in EUI format.

```
fe-0/0/6 {
  description fe-0/0/6;
  unit 0 {
    family inet {
      address 192.168.100.1/24;
    }
    family inet6 {
      address 3ffb:db8:1::/64 {
        eui-64;
      }
    }
  }
}
```

[Back](#)

10.2: Lab Exercise 2: Configuring IPv6 address on an interface in general form

Description: This lab exercise explains steps required to configure ipv6 address on an interface in general form.

Instructions:

1. Enter into configuration mode
2. Enter the [edit interfaces] mode to configure the ipv6 address of fe-0/0/6 interface of SG100
3. Confirm the configuration by entering the show command from configuration mode

On SG100

```
anandsoft@SG100>configure
[edit]
anandsoft@SG100#edit interfaces fe-0/0/6
[edit interfaces fe-0/0/1]
anandsoft@SG100#set unit 0 family inet6 address 2001:db8:1::1/64
[edit interfaces fe-0/0/1]
anandsoft@SG100#exit
[edit]
anandsoft@SG100#show
```

Explanation: Below is the screenshot from show output, ipv6 configured in general form.

```
fe-0/0/6 {
  description fe-0/0/6;
  unit 0 {
    family inet {
      address 192.168.100.1/24;
    }
    family inet6 {
      address 3ffb:db8:1::/64 {
        eui-64;
      }
      address 2001:db8:1::1/64;
    }
  }
}
```


10.3: Lab Exercise 3: IPV6 show commands

Not available in demo version

10.4: Lab Exercise 4: Configuring ipv6 static routes

Not available in demo version

10.5: Lab Exercise 5: Ping Test using IPV6

Not available in demo version

10.6: Lab Exercise 6: Traceroute on IPV6

Not available in demo version

11. Firewall Filter (ACL) Labs

Firewall filters enables to control packets transiting the device to a network destination as well as packets destined for and sent by the device. You can configure a firewall filter to perform specified actions on packets of a particular protocol family, including fragmented packets, that match specified conditions based on Layer3 or Layer4 packet header fields.

Stateless and Stateful Firewall Filters

A stateless firewall filter, also known as an *access control list (ACL)*, does not statefully inspect traffic. Instead, it evaluates packet contents statically and does not keep track of the state of network connections. Stateless firewalls watch network traffic, and restrict or block packets based on source and destination addresses or other static values. They are not 'aware' of traffic patterns or data flows. - See more at:

In contrast, a *stateful firewall filter* uses connection state information derived from other applications and past communications in the data flow to make dynamic control decisions. Stateful firewalls can watch traffic streams from end to end. They are aware of communication paths and can implement various IP Security (IPsec) functions such as tunnels and encryption. In technical terms, this means that stateful firewalls can tell what stage a TCP connection is in (open, open sent, synchronized, synchronization acknowledge or established), it can tell if the MTU has changed, whether packets have fragmented etc.

Stateless firewalls are typically faster and perform better under heavier traffic loads. Stateful firewalls are better at identifying unauthorized and forged communications.

The command to configure a firewall filter is made at the [edit firewall family inet] hierarchy level

```

filter filter-name {
    term term-name {
        from {
            match-conditions;
        }
        then {
            action;
        }
    }
}

```

where filter-name is the name of the filter, term-name is the name of the filter term, match-conditions is the condition that the incoming packets must match for the action to be applied, and action is the steps to take for packets that match the filter condition.

Note: Please refer to the default network diagram for the exercises 19.1, 19.2, 19.3 given in this section

11.1: Lab Exercise 1: Creating a Firewall filter

Description: The lab exercise helps to get familiar with configuring juniper firewall filter

Instructions:

1. Enter into configuration mode
2. Enter into firewall filter mode by creating a filter with name filter1
3. Configure the match-condition that permit traffic from address 192.168.10.5, and block all other traffic by creating a term by name term1.
4. Create term by name term2 that blocks only the single IP address 196.145.25.5
5. Create a term by name term3 that allows traffic from any ip address.

```

anandsoft@SG100>configure
[edit]
anandsoft@SG100#edit firewall family inet filter filter1
[edit firewall family inet filter filter1]
anandsoft@SG100#set term term1 from source-address 192.168.10.5/24
[edit firewall family inet filter filter1]
anandsoft@SG100#set term term1 then accept
[edit firewall family inet filter filter1]
anandsoft@SG100#set term term2 from source-address 196.145.25.5/24

```

```
[edit firewall family inet filter filter1]
anandsoft@SG100#set term term2 then reject
[edit firewall family inet filter filter1]
anandsoft@SG100#set term term3 then accept
[edit firewall family inet filter filter1]
anandsoft@SG100#exit
[edit]
anandsoft@SG100#show
```

Explanation: In this example firewall configured with filter name filter1 consists three terms term1, term2 and term3 with required from and then match conditions as shown in the below output.

```
firewall <
  family inet <
    filter filter1 <
      term term1 <
        from <
          source-address <
            192.168.10.5/24;
          >
        >
        then accept;
      >
      term term2 <
        from <
          source-address <
            196.145.25.5/24;
          >
        >
        then <
          reject;
        >
      >
      term term3 <
        then accept;
      >
    >
  >
>
```

<Output omitted for brevity>

[Back](#)

11.2: Lab Exercise 2: Applying firewall filter to an interface

Description: The lab exercise explains assigning incoming and outgoing traffic to an interface

Instructions:

1. Enter into configuration mode
2. Create firewall filter filter1
3. Apply the match condition that permit traffic from any source to any destination
4. Exit from filter mode
5. Enter into interface mode and apply the filter to fe-0/0/7 interface of SG100
6. Confirm the configuration by entering the show command from configuration mode

```

anandsoft@SG100>configure
[edit]
anandsoft@SG100#edit firewall family inet filter filter1
[edit firewall family inet filter filter1]
anandsoft@SG100#set term term1 then accept
[edit firewall family inet filter filter1]
anandsoft@SG100#exit
[edit]
anandsoft@SG100#edit interfaces fe-0/0/7 unit 0 family inet
[edit interfaces fe-0/0/7 unit 0 family inet]
anandsoft@SG100#set filter input filter1
[edit interfaces fe-0/0/7 unit 0 family inet]
anandsoft@SG100#exit
[edit]
anandsoft@SG100#show

```

Explanation: For a firewall filter to work, you must apply it to at least one interface. To do this, include the filter statement when configuring a logical interface at the [edit interfaces] hierarchy level:

```
[edit interfaces]
```

```
anandsoft@SG100#set interface-name unit logical-unit-number family family-name filter (input |
output) filter-name
```

In the input statement, specify a firewall filter to be evaluated when packets are received on the interface. Input filters applied to a loopback interface affect only traffic destined for the Routing Engine. In the output statement, specify a filter to be evaluated when packets exit the interface. In the below show output firewall filter is applied to interface fe-0/0/7

```

fe-0/0/7 <
  unit 0 <
    family inet <
      filter <
        input filter1;
      >
    >
  >
>

```

<Output omitted for brevity>

[Back](#)

11.3: Lab Exercise 3: View Firewall filter entries

Not available in demo version

11.4: Lab Exercise 4: Configuring and Verifying firewall filter Lab Scenario-1

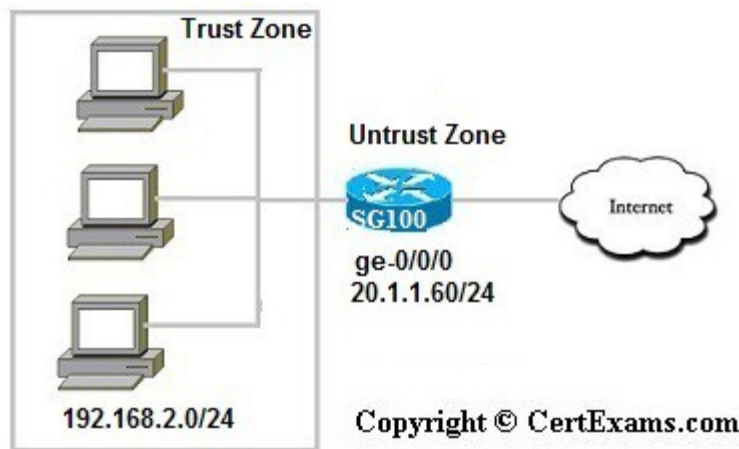
Not available in demo version

12. Network Address Translation Labs

There are 3 kinds of NAT for junos devices. Source NAT, Destination NAT and Static NAT.

- 1. Source NAT:** Changing the source IP address of a packet coming from the trust(inside) network to the untrust(outside) network.
- 2. Destination NAT:** Changing the destination ip address of a packets coming from untrust(outside) network to trust(inside) network.
- 3. Static NAT:** Static NAT defines a one-to-one mapping from one IP subnet to another IP subnet. The mapping includes destination IP address translation in one direction and source IP address translation in the reverse direction. From the NAT device, the original destination address is virtual host ip address while the mapped to address is the real host ip address.

12.1: Lab Exercise 1: Configuring Source NAT using Egress interface Address



Description: The lab exercise explains Source NAT rule set rs1 with a rule r1 to match any packet from the trust zone to the untrust zone. For matching packets, the source address is translated to the IP address of the egress interface.

Instructions:

1. Enter into configuration mode
2. Enter into source NAT hierarchy mode
3. Create Source NAT rule set rs1 with a rule r1 to match any packet from the trust zone to the untrust zone. For matching packets, the source address is translated to the IP address of the egress interface. That is ge-0/0/0 interface ip address

Original Source IP	Translated Source IP
192.168.2.0/24	20.1.1.60/24(Interface IP)

On SG100

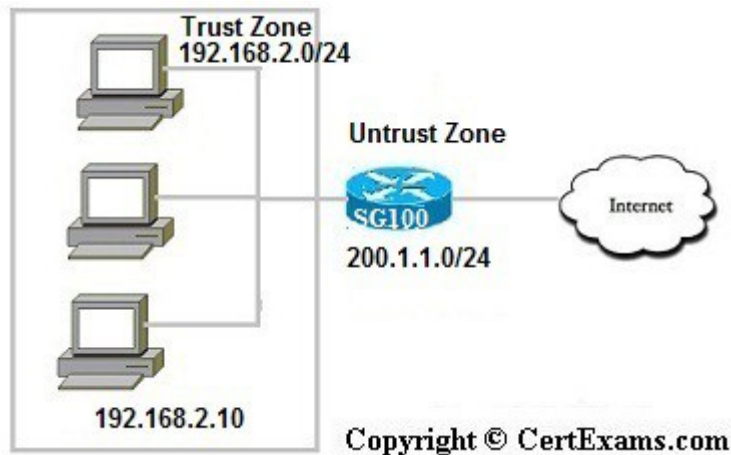
```
anandsoft@SG100>configure
[edit]
anandsoft@SG100# edit security nat source rule-set rs1
[edit security nat source rule-set rs1]
anandsoft@SG100#set from zone trust
[edit security nat source rule-set rs1]
anandsoft@SG100#set to zone untrust
[edit security nat source rule-set rs1]
anandsoft@SG100# set rule r1 match source-address 192.168.2.0/24
[edit security nat source rule-set rs1]
anandsoft@SG100# set rule r1 match destination-address 0.0.0.0/0
[edit security nat source rule-set rs1]
anandsoft@SG100# set rule r1 then source-nat interface
[edit security nat source rule-set rs1]
anandsoft@SG100#exit
[edit]
anandsoft@SG100#show
```

Explanation: Below screenshot is source-nat configuration hierarchy output.

```
nat <
  source <
    rule-set trust-to-untrust <
      from zone trust;
      to zone untrust;
      rule source-nat-rule <
        match <
          source-address 0.0.0.0/0;
        >
        then <
          source-nat <
            interface;
          >
        >
      >
    >
  >
  rule-set rs1 <
    from zone trust;
    to zone untrust;
    rule r1 <
      match <
        source-address 192.168.2.0/24;
        destination-address 0.0.0.0/0;
      >
      then <
        source-nat <
          interface;
        >
      >
    >
  >
  >
  >
  >
  >
```

[Back](#)

12.2: Lab Exercise 2: Configuring Source NAT Translation pool



Description: The lab exercise explains configuring address pools for source NAT.

Instructions:

1. Enter into configuration mode
2. Create a source NAT pool with name pool1
3. Configure a rule that matches packets and translates the source address to an address in the source NAT pool. That is all traffic from trust zone to untrust zone is translated to the source ip pool pool1
4. Issue “show security nat source summary” command to view the source nat summary details

Original Source IP	Translated Source IP
192.168.2.10 to 192.168.2.30	200.1.1.10 to 200.1.1.30

On SG100

```
anandsoft@SG100>configure
[edit]
anandsoft@SG100#edit security nat source
[edit security nat source]
anandsoft@SG100#set pool pool1 address 200.1.1.10/24 to 200.1.1.30/24
[edit security nat source]
anandsoft@SG100#set rule-set trust-to-untrust from zone trust
[edit security nat source]
anandsoft@SG100#set rule-set trust-to-untrust to zone untrust
[edit security nat source]
anandsoft@SG100# set rule-set trust-to-untrust rule r1 match source-address
192.168.2.0/24
[edit security nat source]
anandsoft@SG100# set rule-set trust-to-untrust rule r1 match destination-address 0.0.0.0/0
```



```

[edit security nat source]
anandsoft@SG100#set rule-set trust-to-untrust rule r1 then source-nat pool pool1
[edit security nat source]
anandsoft@SG100#exit
[edit]
anandsoft@SG100#show
[edit]
anandsoft@SG100#commit
commit complete
[edit]
anandsoft@SG100#exit
anandsoft@SG100>show security nat source summary

```

Explanation: The “show security nat source summary” displays summary of the source NAT information. Number of source nat pools, name of source address pool, IP address or IP address range for the pool, Name of the routing instance, whether Port Address Translation (PAT) is enabled (yes or no), Number of source NAT rules, Number of ports assigned to the pool, Maximum number of NAT or PAT transactions done at any given time. Show output is as shown below

```

nat <
  source <
    pool pool1 <
      address <
        200.1.1.10/24 to 200.1.1.30/24;
      >
    >
  rule-set trust-to-untrust <
    from zone trust;
    to zone untrust;
    rule source-nat-rule <
      match <
        source-address 0.0.0.0/0;
      >
      then <
        source-nat <
          interface;
        >
      >
    >
  rule r1 <
    match <
      source-address 192.168.2.0/24;
      destination-address 0.0.0.0/0;
    >
    then <
      source-nat <
        pool <
          pool1;
        >
      >
    >
  >
>

```

```

anandsoft@SG100> show security nat source summary
Total port number usage for port translation pool: 1354752
Maximum port number for port translation pool: 67108864
Total pools: 1
Pool Name           Address Range           Routing Instance          PAT   Total Address
pool1                200.1.1.10-200.1.1.30  default                yes   21

Total rules: 2
Rule name           Rule set           From           To           Action
source-nat-rule    trust-to-untrust  trust          untrust      interface
r1                  trust-to-untrust  trust          untrust      pool1

anandsoft@SG100> █

```

[Back](#)

12.3: Lab Exercise 3: Configuring Destination NAT pools

Not available in demo version

12.4: Lab Exercise 4: Creating Destination NAT rule set

Not available in demo version

12.5: Lab Exercise 5: Configuring Static NAT for single address translation

Not available in demo version

12.6: Lab Exercise 6: Configuring Source NAT using multiple rules Lab Scenario-1

Not available in demo version

12.7: Lab Exercise 7: Configuring Destination NAT using multiple rules

Not available in demo version

12. Exercises on DHCP

13.1: Lab Exercise 1: Configuring juniper router as a DHCP Server

Description: This lab exercise demonstrates the required commands for DHCP Server configuration on a juniper router.



Copyright © CertExams.com

Instructions:

1. Enter into configuration mode of device SG100
2. Configure the dhcp server
3. Specify the low and high ip address pool range
4. Configure default and maximum lease-time
5. Configure the domain-name used by client
6. Configure DNS Server IP address
7. Configure the default-router address
8. Confirm the configuration by entering the show command from configuration mode

On SG100

```
anandsoft@SG100>configure
[edit]
anandsoft@SG100#edit system services dhcp
[edit system services dhcp]
anandsoft@SG100#set pool 10.100.100.0/24 address-range low 10.100.100.1
[edit system services dhcp]
anandsoft@SG100#set pool 10.100.100.0/24 address-range high 10.100.100.50
[edit system services dhcp]
anandsoft@SG100#set pool 10.100.100.0/24 domain-name xyz.com
[edit system services dhcp]
anandsoft@SG100#set pool 10.100.100.0/24 name-server 10.100.100.3
[edit system services dhcp]
anandsoft@SG100#set pool 10.100.100.0/24 router 10.100.100.2
[edit system services dhcp]
```

```

anandsoft@SG100#set pool 10.100.100.0/24 default-lease-time 1309300
[edit system services dhcp]
anandsoft@SG100#set pool 10.100.100.0/24 maximum-lease-time 2429300
[edit system services dhcp]
anandsoft@SG100#exit
[edit]
anandsoft@SG100#show
[edit]
anandsoft@SG100>show system services dhcp pool
[edit]

```

Explanation: In this example, you configure the device as a DHCP server. You specify the IP address pool as 10.100.100.0/24 and from a low range of 10.100.100.1 to a high range of 10.100.100.50. You set the maximum-lease-time to 2429300. Then you specify the DNS server IP address as 10.100.100.3 and default-router as 10.100.100.2 and default-lease-time as 1309300 and domain-name as xyz.com. Below is the show output of the device configured as dhcp server and also configure an interface with an IP address on which the DHCP server will be reachable in this example it's configured as 10.100.100.2/24

```

pool 10.100.100.0/24 <
  address-range low 10.100.100.1 high 10.100.100.50;
  maximum-lease-time 2429300;
  default-lease-time 1309300;
  domain-name xyz.com;
  name-server <
    10.100.100.3;
  >
  router <
    10.100.100.2;
  >
  >
  propagate-settings fe-0/0/0.0;
>

```

```

anandsoft@SG100> show system services dhcp pool
Pool name      Low address    High address    Excluded addresses
10.100.100.0/24  10.100.100.1  10.100.100.50  10.100.100.2
192.168.1.0/24  192.168.1.2   192.168.1.254
anandsoft@SG100>

```

[Back](#)

13.2: Lab Exercise 2: DHCP client configuration



Copyright © CertExams.com

Description : This lab exercise demonstrates DHCP client configuration i.e, Configuring an interface on the router to use DHCP to acquire its IP address.

Instructions:

1. Before proceeding with the DHCP client configuration, make sure that DHCP server is configured as shown in the previous lab exercise.
2. Enter into configuration mode of device SG100
3. For the security zone (for example, untrust) to which the interface is bound, specify DHCP as a host-inbound service.
4. Enter into configuration mode of ND210 and specify the interface (ge-0/0/0) on which to enable the DHCP client.
5. On ND210 issue “show system services dhcp client” command to view information about DHCP Client

On SG100

```
anandsoft@SG100>configure
[edit]
anandsoft@SG100#set security zones security-zone untrust interfaces fe-0/0/7 host-
inbound-traffic system-services dhcp
[edit]
anandsoft@SG100#commit
[edit]
commit complete
anandsoft@SG100#exit
[edit]
```

On ND210

```
anandsoft@ND210>configure
[edit]
anandsoft@ND210#set interfaces fe-0/0/7 unit 0 family inet dhcp
[edit]
anandsoft@ND210#commit
[edit]
```

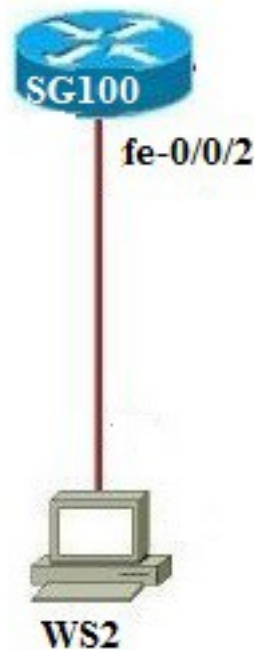
```
commit complete
anandsoft@ND210#exit
[edit]
anandsoft@ND210>show system services dhcp client
```

Explanation: To obtain an IP address from dhcp server you will need to enable DHCP client on the interface, and also as a host inbound service on the interface on the security zone.

[Back](#)

13.3: Lab Exercise 3: Assigning ip address to PC(computer) from DHCP server

Description: The lab exercise explains dynamically assigning ip address to computers via DHCP server.



Copyright © CertExams.com

Instructions:

1. Connect to SG100 and configure the IP address of 10.100.100.2/24 on the fe-0/0/2 interface and also configure the SG100 as DHCP server

```
anandsoft@SG100>configure
[edit]
anandsoft@SG100#set interfaces fe-0/0/2 unit 0 family inet address 10.100.100.2/24
```

```
[edit]
anandsoft@SG100#edit system services dhcp
[edit system services dhcp]
anandsoft@SG100#set pool 10.100.100.0/24 address-range low 10.100.100.1
[edit system services dhcp]
anandsoft@SG100#set pool 10.100.100.0/24 address-range high 10.100.100.50
[edit system services dhcp]
anandsoft@SG100#set pool 10.100.100.0/24 domain-name xyz.com
[edit system services dhcp]
anandsoft@SG100#set pool 10.100.100.0/24 name-server 10.100.100.3
[edit system services dhcp]
anandsoft@SG100#set pool 10.100.100.0 router 10.100.100.2
[edit system services dhcp]
anandsoft@SG100#exit
[edit]
```

Assign DHCP as an allowed inbound service for the interface fe-0/0/2 to enable DHCP.

```
anandsoft@SG100#set security zones security-zone untrust interfaces fe-0/0/2 host-
inbound-traffic system-services dhcp
```

```
anandsoft@SG100#commit
commit complete
anandsoft@SG100#exit
anandsoft@SG100>show system services dhcp pool
```

Obtain ip address automatically from DHCP server for PC1

```
WS2>ip dhcp
WS2>show ip
```

<http://www.jpudasaini.com.np/2015/09/juniper-dhcp-server-configuration.html>

<http://www.jaredlog.com/?p=2085>

[Back](#)

14. Exercises on VPN

14.1 Lab Exercise 1: Configuring Address Books and Address Sets

Description: Address book entries include addresses of hosts and subnets whose traffic is either allowed, blocked, encrypted, or user-authenticated. These addresses can be any combination of IPv4 addresses, IPv6 addresses, wildcard addresses, or Domain Name System (DNS) names.

Lab Exercise helps to configure address book and address sets in juniper router.

Instructions:

1. Create an address book and define addresses in it.
2. Create address sets.
3. Attach the address book to a security zone.

On Device SG100

```
anandsoft@SG100>configure
Entering into Configuration Mode
[edit]
anandsoft@SG100#edit security address-book
[edit security address-book]
anandsoft@SG100#set bldg1 address bldg1_a1 192.168.1.0/24
[edit security address-book]
anandsoft@SG100#set bldg1 address bldg1_a2 192.168.2.0/24
[edit security address-book]
anandsoft@SG100#set bldg1 address bldg1_a3 192.168.3.0/24
[edit security address-book]
anandsoft@SG100#set bldg1 address bldg1_a4 192.168.4.0/24
[edit security address-book]

anandsoft@SG100#set bldg2 address bldg2_a1 172.16.1.0/24
[edit security address-book]
anandsoft@SG100#set bldg2 address bldg2_a2 172.16.2.0/24
[edit security address-book]
anandsoft@SG100#set bldg2 address bldg2_a3 172.16.3.0/24
[edit security address-book]
anandsoft@SG100#set bldg2 address bldg2_a4 172.16.4.0/24
[edit security address-book]
anandsoft@SG100#exit
[edit]
anandsoft@SG100#edit security address-book bldg1
[edit security address-book bldg1]
anandsoft@SG100#set address-set set1 address bldg1_a1
[edit security address-book bldg1]
anandsoft@SG100#set address-set set1 address bldg1_a2
[edit security address-book bldg1]
anandsoft@SG100#set address-set set2 address bldg1_a3
```



```
[edit security address-book bldg1]
anandsoft@SG100#set address-set set2 address bldg1_a4
[edit security address-book bldg1]
anandsoft@SG100#set attach zone trust
[edit security address-book bldg1]
anandsoft@SG100#exit
[edit security address-book]
anandsoft@SG100#exit
[edit]

anandsoft@SG100#edit security address-book bldg2
[edit security address-book bldg2]
anandsoft@SG100#set address-set set1 address bldg2_a1
[edit security address-book bldg2]
anandsoft@SG100#set address-set set1 address bldg2_a2
[edit security address-book bldg2]
anandsoft@SG100#set address-set set2 address bldg2_a3
[edit security address-book bldg2]
anandsoft@SG100#set address-set set2 address bldg2_a4
[edit security address-book bldg2]
anandsoft@SG100#set attach zone trust
[edit security address-book bldg2]
anandsoft@SG100#exit
[edit security address-book]
anandsoft@SG100#exit
[edit]
anandsoft@SG100#show
[edit]
```

Below is the show output of the address-book configuration on device SG100

```

security <
  address-book <
    bldg1 <
      address bldg1_a1 192.168.1.0/24;
      address bldg1_a2 192.168.2.0/24;
      address bldg1_a3 192.168.3.0/24;
      address bldg1_a4 192.168.4.0/24;
      address-set set1 <
        address bldg1_a1;
        address bldg1_a2;
      >
      address-set set2 <
        address bldg1_a3;
        address bldg1_a4;
      >
      attach <
        zone trust;
      >
    >
  >
  bldg2 <
    address bldg2_a1 172.16.1.0/24;
    address bldg2_a2 172.16.2.0/24;
    address bldg2_a3 172.16.3.0/24;
    address bldg2_a4 172.16.4.0/24;
    address-set set1 <
      address bldg2_a1;
      address bldg2_a2;
    >
    address-set set2 <
      address bldg2_a3;
      address bldg2_a4;
    >
    attach <
      zone untrust;
    >
  >
>

```

References:

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-address-books-sets.html#id-understanding-address-books

[Back](#)

14.2 Lab Exercise 2: Configuring a security zone and bind the interfaces to the appropriate zones

Description: A security zone is a collection of one or more network segments requiring the regulation of inbound and outbound traffic through policies. Security zones are logical entities to which one or more interfaces are bound. You can define multiple security zones as per your network requirements.

Lab Exercise explains to configure security zones and binding interfaces to appropriate zones

Instructions:

1. Assign interfaces to the security zones

anandsoft@SG100>configure

[edit]

anandsoft@SG100#set security zones security-zone trust interfaces ge-0/0/0

[\[edit\]](#)

[anandsoft@SG100#set security zones security-zone untrust interfaces ge-0/0/1](mailto:anandsoft@SG100#set%20security%20zones%20security-zone%20untrust%20interfaces%20ge-0/0/1)

[\[edit\]](#)

Ref:

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-zone-configuration.html

[Back](#)

14.3 Lab Exercise 3: Configuring host-inbound services for each interface in the zone

Not available in demo version

14.4 Lab Exercise 4: Configuring IKE Phase 1 Proposal

Not available in demo version

14.5 Lab Exercise 5: Configuring IKE Phase 1 Policy

Not available in demo version

14.6 Lab Exercise 6: Configuring IKE Phase 1 gateway and reference the IKE policy

Not available in demo version

14.7 Lab Exercise 7: Configuring IPSEC Phase 2 proposals

Not available in demo version

14.8 Lab Exercise 8: Configuring IPSEC Phase 2 policies and reference the IPSEC proposals

Not available in demo version

14.9 Lab Exercise 9: Configuring the IPSEC Phase 2 VPN tunnel and reference the IPSEC Phase 2 policy

Not available in demo version

14.10 Lab Exercise 10: Configuring Security Policies

Not available in demo version

14.11 Lab Exercise 11: Configuring and Verifying Policy based VPN

Not available in demo version

14.12 Lab Exercise 12: Configuring and Verifying Route based VPN

Not available in demo version

15. Basic Switch Labs

15.1: Lab Exercise 1: Entering configuration mode on a switch and exit

Description: A basic exercise that shows how to enter configuration mode and exit from the same.

Instructions

1. Enter into configuration mode
2. Get back to the operational mode

```
anandsoft@SG100>configure
[edit]
anandsoft@SG100#exit
anandsoft@SG1001>
```

[Back](#)

15.2: Lab Exercise 2: Setting Hostname

Description: Set the switch hostname as SG100.

Instructions

1. Enter into configuration mode
2. Set hostname as “SG100”

```
anandsoft@SG100>configure
[edit]
anandsoft@SG100#edit system
[edit system]
anandsoft@SG100#set host-name SG100
[edit system]
anandsoft@SG100#exit
[edit]
```

Explanation: The hostname of a device is its identification. A router or switch must have its identity established to be accessible on the network to other devices. That is perhaps the most important reason to have a hostname, but a hostname has other purposes: Junos OS uses the configured hostname as part of the command prompt, to prepend log files and other accounting information, as well as in other places where knowing the device identity is useful. We recommend that the hostname be descriptive and memorable.

You can configure the hostname at the **[edit system]** hierarchy level

[Back](#)

15.3: Lab Exercise 3: Set interface description

Not available in demo version

15.4: Lab Exercise 4: Shutdown an interface

Not available in demo version

15.5: Lab Exercise 5: Basic CLI commands

Not available in demo version

15.6: Lab Exercise 6: Configure bandwidth on an interface

Not available in demo version

15.7: Lab Exercise 7: Configuring ether-options on the gigabit ethernet switch interface

Not available in demo version

15.8: Lab Exercise 8: Configuring the management IP address on EX series switch

Not available in demo version

16. Lab Exercises on VLAN

16.1: Lab Exercise 1: Define VLANs

Description: This exercise demonstrates the commands required to create VLANs on the switch.

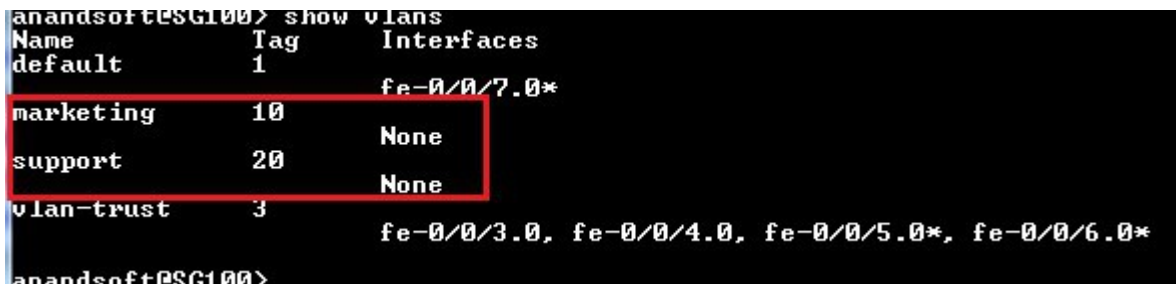
Instructions

1. Create VLAN 10 and 20 by using the command syntax “set vlans <vlan-name> vlan-id <vlan-id-number>”
2. Verify the same using show vlans command

```
anandsoft@SG100>configure
[edit]
anandsoft@SG100#set vlans marketing vlan-id 10
[edit]
anandsoft@SG100#set vlans support vlan-id 20
[edit]
anandsoft@SG100#commit
[edit]
anandsoft@SG100#exit
anandsoft@SG100>show vlans
```

Explanation: To configure a VLAN create the VLAN by setting the unique VLAN name and configuring the VLAN ID. The following “show vlans” command output displays the created vlans.

Below screenshot shows output from “show vlans” command after configuring vlan 10 and 20



```
anandsoft@SG100> show vlans
Name      Tag      Interfaces
default   1        fe-0/0/7.0*
marketing  10       None
support   20       None
vlan-trust 3        fe-0/0/3.0, fe-0/0/4.0, fe-0/0/5.0*, fe-0/0/6.0*
anandsoft@SG100>
```

[Back](#)

16.2: Lab Exercise 2: Configure a port for membership in that VLAN

Description: This exercise demonstrates the commands required to configure a port as a member of the VLAN.

Instructions

1. Create VLAN by configuring the VLAN
2. Configure the interface port to be a member of the created VLAN
3. Verify using show command

```
anandsoft@SG100>configure
[edit]
anandsoft@SG100#set vlans marketing vlan-id 10
[edit]
anandsoft@SG100#set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members
marketing
[edit]
anandsoft@SG100#commit
[edit]
anandsoft@SG100#exit
anandsoft@SG100>show vlans
```

Explanation: Assign an interface to the VLAN by specifying the logical interface (with the unit statement) and specifying the VLAN name as the member. The following “show vlans” command displays assigned interface to vlan member. You can observe from the output where ge-0/0/1 interface is a member of vlan-name “marketing”.

[Back](#)

16.3: Lab Exercise 3: Configuring an interface as a trunk port

Not available in demo version

16.4: Lab Exercise 4: Configuring VLANs

Not available in demo version

16.5: Lab Exercise 5: Configuring Routed VLAN interface (Inter-VLAN routing)

Not available in demo version

[Back](#)

17. Lab Exercises on Spanning tree protocol and VSTP

17.1: Lab Exercise 1: Configuring STP Timers

Description: This lab exercise demonstrates configuring spanning-tree protocol timers.

Instructions:

1. Enter into configuration mode on SG100
2. Use the command “set stp hello-time/forward-time/max-age <value>” to configure the various STP timers on the switch
3. Verify the configuration using show configuration command.

```
anandsoft@SG100>configure
```



```
[edit]
anandsoft@SG100#edit protocols
[edit protocols]
anandsoft@SG100#set stp forward-delay 20
[edit protocols]
anandsoft@SG100#set stp hello-time 5
[edit protocols]
anandsoft@SG100#set stp max-age 30
[edit protocols]
anandsoft@SG100#exit
[edit]
anandsoft@SG100#commit
[edit]
anandsoft@SG100#exit
anandsoft@SG100>show configuration
```

Explanation:

- I. Hello-Time: Determines how often the switch broadcasts hello messages to other switches.
- ii. Forward-Time: Determines how long each of the listening and learning states last before the interface begins forwarding.
- iii. Max-Age: Determines the amount of time the switch stores protocol information received on an interface.

Below screenshot is output from “show configuration” command after configuring STP timers.

```

protocols <
  mpls <
    interface fe-0/0/1.0;
  >
  bgp <
    group external-peers <
      type external;
      hold-time 190;
      peer-as 22;
      neighbor 172.16.10.2;
      neighbor 10.100.100.1;
    >
  >
  ospf <
    area 0.0.0.0 <
      interface fe-0/0/1.0;
      interface fe-0/0/2.0;
    >
  >
  ldp <
    interface fe-0/0/1.0;
    interface fe-0/0/2.0;
    interface all;
  >
  lldp <
    advertisement-interval 30;
    hold-multiplier 4;
    interface all;
  >
  stp <
    max-age 30;
    hello-time 5;
    forward-delay 20;
  >
>

```

Output omitted for brevity>

[Back](#)

17.2: Lab Exercise 2: Setting bridge priority on switch

Description: This exercise demonstrates the command required to configure switch priority of a VLAN.

Instructions:

1. Enter into configuration mode on SG100
2. Issue the command "bridge-priority <priority-value> to configure the switch priority of a VLAN.

```

anandsoft@SG100>show spanning-tree interface
anandsoft@SG100>configure
[edit]
anandsoft@SG100#edit protocols
[edit protocols]
anandsoft@SG100#set stp bridge-priority 12288
[edit protocols]
anandsoft@SG100#exit
[edit]
anandsoft@SG100#show

```

[\[edit\]](#)

Explanation: The switch priority can be configured thus making it more likely to be chosen as the root switch. Priority range is 0 to 61440 in increments of 4096, default is 32768.

show output screenshot is shown below

```
stp <
  bridge-priority 12k;
  max-age 30;
  hello-time 5;
  forward-delay 20;
>
<Output omitted for brevity>
```

The “show spanning-tree interface” command output is shown below

```
anandsoft@ESG100> show spanning-tree interface
Spanning tree interface parameters for instance 0
Interface      Port ID      Designated      Designated      Port      State  Role
                port ID      port ID         bridge ID      Cost
fe-0/0/5.0     128:518     128:518     32768.40a6772e5608  2000000  FWD   DESG
fe-0/0/6.0     128:519     128:519     32768.40a6772e5608  2000000  FWD   DESG
fe-0/0/7.0     128:520     128:520     32768.40a6772e5608  2000000  FWD   DESG
anandsoft@ESG100>
```

[Back](#)

17.3: Lab Exercise 3: Configuring port priority

Not available in demo version

17.4: Lab Exercise 4: Verifying STP

Not available in demo version

17.5: Lab Exercise 5: Enabling VSTP on all VLANs

Not available in demo version

17.6: Lab Exercise 6: Enabling VSTP on a VLAN using a single VLAN-ID / VLAN-Name

Not available in demo version