JUNOS Cheat-Sheet

Quick Reference – www.cciezone.com

File System

Active	/config/juniper.conf.gz	
Rollbacks	n = 1-3	Stored in /config/juniper.conf.*n*.gz
	n = 4-49	Stored in /config/db/config/juniper.conf.*n*.gz
Rescue	/config/rescue.conf.gz	
JUNOS Images	Should be stored in /var/tmp for easy cleanup	

Interfaces – disabling & enabling

	IOS	JUNOS
Disable	`interface <name>` `shutdown`	`set interface <name> disable`
Enable	`interface <name>` `no shutdown`	`delete interface <name> disable`

HELP!

`help topic`	General topics
`help reference`	Syntax
`help syslog`	Lookup syslog msgs

System Maintenance

(all are operational-mode commands)

Upgrade	`request system software add`
Reboot	`request system reboot`
Shutdown	`request system power-off`

EZsetup

Login as root, run `ezsetup`

OR

Connect to ge-0/0/0, use DHCP and access 192.168.1.1 (web or telnet/SSH)

OR

Choose *Enter Ezsetup* from LCD screen

OR

Connect to me0 and access 192.168.2.1 (EX-series)

Rescue Configuration

There is no default rescue config - don't forget to create it!

Create	`request system configuration rescue save`

Rollback (apply/restore)	`[edit]`
	`rollback rescue`
	OR
	Press the config button for less than 5 seconds

Date/Time

Show	`show system uptime`
Set	`set date`
Set Timezone	`set system time-zone`
Set (NTP)	`set date ntp <IP>`
Show (NTP)	`show ntp associations`

Misc Device Config & Hardening

Set Root password	`set system root-authentication plain-text-password`
Enable SSH	`set system services ssh`
Disable Telnet	`delete system services telnet`
Set Hostname	`set system host-name <name>`

Juniper EX-series Cheat Sheet

Quick Reference – www.cciezone.com

The EX-series can be an NTP server!

Factory Default Configuration

- All ports are `family ethernet-switching`
- PoE is enabled on all PoE-capable ports
- LLDP and RSTP enabled
- Virtual chassis system ID is 0 (zero)
- `mastership-priority` of 128

Reset back to default `load factory-default`

STP and RTG

- Up to 64 MSTP instances are supported
- Configure under `[edit protocols]` hierarchy (stp, rstp and mstp)
- Use Redundant Trunk Groups (RTGs) to have a failover/ secondary link without the use of STP
  Up to 16 RTGs are supported per switch

```
show spanning-tree bridge
show spanning-tree interface
show spanning-tree statistics interface
show spanning-tree mstp configuration
```

```
[edit ethernet-switching-options]
redundant-trunk-group {
    group rtg10 {
        interface ge-0/0/3.0;
        interface ge-0/0/4.0;
    }
}
```

```
show redundant-trunk-group
```

Virtual Chassis System (VCS)

Each EX 4200 comes with a ½-meter VCB

Up to 10 (ten) EX 4200s can be stacked into a VCS

Pre-emption is enabled by default, highest priority wins

VCPs	Virtual Chassis Ports – form the backplane
VCB	Virtual Chassis Backplane cables – interconnects switches into a VCS
VCEPs	Virtual Chassis Extender Ports – uses fiber to interconnect remote switches Only supported on 10Gbps uplink module
VCCP	Virtual Chassis Control Protocol – used to exchange LSA-based discovery messages between PFEs in a VCS
VME	Virtual Management Ethernet interface – used to administer the switch stack
PFE	Packet Forwarding Engine 24-port EX 4200s have 2 PFEs 48-port EX 4200s have 3 PFEs

Configure a VME

```
request virtual-chassis vc-port set
    pic-slot <#> port <#>
```

LAGs and Trunks

- Up to 8 interfaces in a single LAG
- Max # LAGs:
  EX 3200 = 32 LAGs per switch
  EX 4200 = 64 LAGs per switch
  VCS = 128 LAGs per VCS
- Trunks do not have to have a native VLAN

VCS Commands

- `show chassis hardware`
- `show virtual-chassis status`
- `show virtual-chassis active-topology`
- `show virtual-chassis interfaces`
- `show virtual-chassis member-config`
- `show virtual-chassis protocol`

If me0 isn't configured as a L3 interface, it is automatically assigned to the mgmt VLAN

Remember that all ports by default are access ports

Configure a LAG

1. Set the number of ae interfaces
   `set chassis aggregated-devices ethernet device-count <#>`
2. Bind the physical interface to the ae interface
   `set interfaces <name> ether-options 802.3ad <ae_int>`
3. Set the ae interface properties (physical and logical)

Configure a Trunk

1. Set the port mode to trunk
   `set interfaces <name> unit <#> family ethernet-switching port-mode trunk`
2. Set the VLAN membership on the trunk
   `set interfaces <name> unit <#> family ethernet-switching vlan members <name(s)>`
3. Set the native VLAN (optional)
   `set interfaces <name> unit <#> family ethernet-switching native-vlan-id <name>`

Routed VLAN Interface (RVI)

Provides inter-VLAN routing. Like an SVI on IOS.

```
[edit interfaces]
vlan {
    unit 200 {
        family inet {
            address 10.1.1.1/24
        }
    }
}

[edit vlans]
test {
    vlan-id 200;
    l3-interface vlan.200;
}
```

The VLAN unit doesn't have to match the VLAN ID – best-practices recommend it

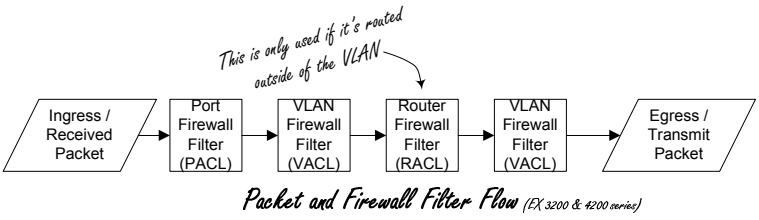
Ports can be:

L2 Configure `family ethernet-switching`

L3 Configure `family inet`

Juniper EX-series Cheat Sheet

Quick Reference – www.cciezone.com



Packet and Firewall Filter Flow (EX 3200 & 4200 series)

Guard against CAM attacks with MAC Limiting!!!

MAC Limiting protects the CAM:
Only allows statically-defined MAC addresses
OR
Limits the number of dynamically-learned MAC addresses

MAC Limiting actions:
`shutdown` (blocks data traffic & generates system log entry)
`drop` (drops the packet and generates a system log entry)
`log` (does not drop packet, but generates a system log entry)
`none` (do not do anything)

Configuration Example:

```
[edit ethernet-switching-options]
secure-access-port {
    interface ge-0/0/0.0 {
        allowed-mac [ 00:00:00:00:00:01 ];
    }
    interface ge-0/0/1.0 {
        mac-limit 2 action shutdown;
    }
}
```

DHCP Snooping

Mitigate rogue DHCP servers!

Default Port Trusts:
Access port = untrusted
Trunk port = trusted

Configuration Example:

```
[edit ethernet-switching-options]
secure-access-port {
    interface ge-0/0/0.0 {
        dhcp-trusted;
    }
    interface ge-0/0/1.0 {
        no-dhcp-trusted;
    }
    vlan test {
        examine-dhcp;
    }
}
```

DHCP Snooping Commands

```
show dhcp snooping binding
clear dhcp snooping binding
```

Helpful MAC Limiting Commands

Examine `show ethernet-switching table` to view the MAC table.

Use `clear ethernet-switching table interface <name>` to clear violations.

Look at `show log messages` for MAC Limiting violation messages.

Dynamic ARP Inspection (DAI)

- Relies on examining entries in the DHCP Snooping table, so requires DHCP Snooping
- Disabled on all VLANs by default
- It is enabled on a per-VLAN basis
- Any interface that is configured as a trusted interface for DHCP Snooping is also setup as a DAI trusted interface (bypasses ARP inspection)

Configuration Example:

```
[edit ethernet-switching-options]
secure-access-port {
    interface ge-0/0/0.0 {
        dhcp-trusted;
    }
    vlan test {
        arp-inspection;
        examine-dhcp;
    }
}
```

Monitoring Commands:

```
show dhcp snnoping bindings
show arp inspection statistics
```

802.1X

802.1X port modes:

`single` (default – only first host is authenticated, all other hosts piggy-back on the first supplicant)
`single-secure` (only permits a single supplicant, all others are denied)
`multiple` (permits access for multiple supplicant, each supplicant is authenticated individually)

802.1X Parameters & Options
Default Reauthentication Period: 3600 seconds
Range: 1 to 65,535 seconds

A Guest VLAN can be configured and is used when:
- When authentication fails
- When a client doesn't respond (have a supplicant)

MAC Static List is an authentication bypass for non-802.1X hosts.
MAC addresses are stored locally on the device.

Configuration Example:

```
[edit protocols dot1x authenticator]
interface {
    ge-0/0/0.0 {
        guest-vlan test-guest-vlan;
        reauthentication 3600;
        supplicant single-secure;
    }
    ge-0/0/3.0 {
        no-reauthentication;
    }
}
Static {
    00:00:00:00:00:01 {
        interface ge-0/0/0.0;
    }
    00:00:00:00:00:02;
}
```

Monitoring Commands:

```
show dot1x interface
Show dot1x static-mac-address
show dot1x authentication-failed-users
```

DHCP traceoptions are logged to /var/log/jsd by default

DHCP Server

Configuration Example:

```
[edit system services dhcp]
pool 10.0.0.0/24 {
    address-range low 10.0.0.1 high 10.0.0.200;
    exclude-address {
        10.0.0.1;
    }
    maximum-lease-time 86400;
    default-lease-time 86400;
    name-server {
        10.0.10.10;
    }
    router {
        10.0.0.254;
    }
}
```

Useful Commands:

```
show system services dhcp ?
clear system services dhcp conflict
```

DHCP/BOOTP Relay

Configuration Example:

```
[edit forwarding-options helpers bootp]
description "Main DHCP relay";
server 10.0.40.2;
maximum-hop-count 4;
minimum-wait-time 1;
interface {
    vlan.2 {
        no-listen;
    }
}
```

Juniper EX-series Cheat Sheet

Quick Reference – www.cciezone.com

Power over Ethernet (PoE)

- All switch ports are assigned to class 0 by default
- Modes:
  Static – max power for port is deducted from total power pool (only supports class 0)
  Dynamic – power budgeted from total power pool matches actual power consumed
  Class – max power class budget is deducted from the total power pool
- PoE Telemetries provide historical power usage for each powered device (PD)
  Disabled by default
  Default interval is 5 minutes (1 to 30 mins)
  Default duration is 1 hour (1 to 24 hrs)

Configuration Example:

```
[edit poe]
interface ge-0/0/0 {
    priority high;
    maximum-power 15.4;
    telemetries {
        interval 5;
        duration 1;
    }
}
interface ge-0/0/1 {
    telemetries {
        disable;
    }
}
```

Useful Commands:

```
show chassis hardware
show poe controller
show poe interface
```

Power Supplies

- Fully interchangeable between EX 3200 and 4200 series switches
- 320W, 600W and 930W capacities are available

Voice VLAN

- Configure CoS before enabling voice VLAN
- Use voice VLAN on ports with IP phones
- Use LLDP-MED to signal voice VLAN ID and 802.1p value to IP phone

Configuration Example:

```
[edit ethernet-switching-options]
voip {
    interface ge-0/0/0 {
        vlan test-voice;
        forwarding-class voice-ep;
    }
}
```

Useful Commands:

```
show vlans detail <name>
```

LLDP

LLDP Multicast Address: 01-80-C2-00-00-0E

- All mandatory LLDP TLVs are sent when LLDP is enabled
- All optional LLDP and LLDP-MED TLVs are enabled by default

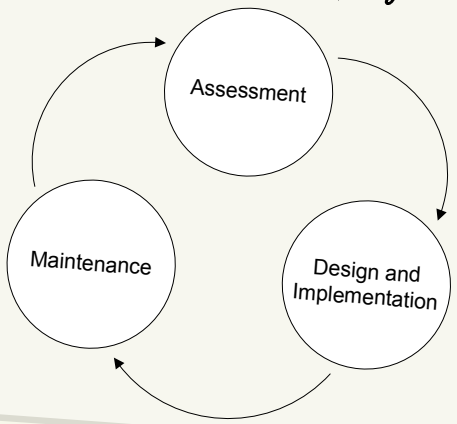
Configuration Example:

```
[edit protocols]
lldp {
    advertisement-interval 30;
    hold-multiplier 2;
    msgTxInterval 30;
    msgTxHold 4;
}
lldp-med;
```

Useful Commands:

```
show lldp statistics
show lldp detail
show lldp neighbors
show lldp local-info
```

Network Development Life Cycle



Juniper EX-series Cheat Sheet

Quick Reference – www.cciezone.com

EX 3200-series

- 24 to 48-ports
  - Basic model has 8 PoE ports
  - Up to 48 PoE ports are supported
- Does not support VCS
- Intended for access layer usage
- Supports redundant power supplies (one internal, one via RPS port)
- Field-replaceable PS and fan tray
- Uplink modules:
  - 4 x 1Gbps Ethernet (SFP)
  - 2 x 10Gbps Ethernet (XFP)
- Line-rate switching (non-blocking)

EX 4200-series

- 24 to 48-ports
  - Basic model has 8 PoE ports
  - Up to 48 PoE ports are supported
- Supports VCS (up to 10 switches in a VCS)
- Intended for distribution and access layer usage
- Redundant (both internal), hot-swappable PS
- Field-replaceable fan tray (3 fans – one can fail & not affect operations)
- Uplink modules:
  - 4 x 1Gbps Ethernet (SFP)
  - 2 x 10Gbps Ethernet (XFP)
- Line-rate switching (non-blocking)