Factory Default Config (vary from platforms)

- All platforms running Junos are shipped with a factory-default config.
- All factor-default config allow access using root account
- By default, the root account does not have a password
- *A root password must be configured before making any configuration changes*
- Faculty-default config also includes system logging
- *System logging tracks system events and writes those events to predefined log files.*
- the default hostname is ***Amnesiac***
- To return the device to factory-default config, use the command ***load factory-default***

Initial Config

Set root authentication

- ***set system root-authentication <topic>***
- commit

Set up SSH/telnet access,

- ***edit system services*** navigate
- ***set ssh <topic>***
- ***set telnet <topic>***
-
-

set up hostname, domain-name, name servers, time zone, login message

- ***edit system***
- ***set hostname <val>***
- ***set domain-name <val>***
- ***set name-server <val>***
- ***set time-zone <area>***
- ***set login message "hello world"***

set up date, cli idle timeout

- ***>set date <YYYYMMDDhhmm.ss>***
- ***>set cli idle-timeout <0-100,000 minutes>***

Login Classes

- A set of one or more permissions
- All users who can login to a Junos device must have a login class
- Allows you to define
    - access privilege on the device
    - commands that users can or cannot specify
    - session idle time

Predefined Login Classes

- super-user: all permissions
- operator: clear, network, reset, trace, and view permissions
- read-only: view permissions
- unauthorized: no permissions
- ***# set system login user admin class <predefined class>***

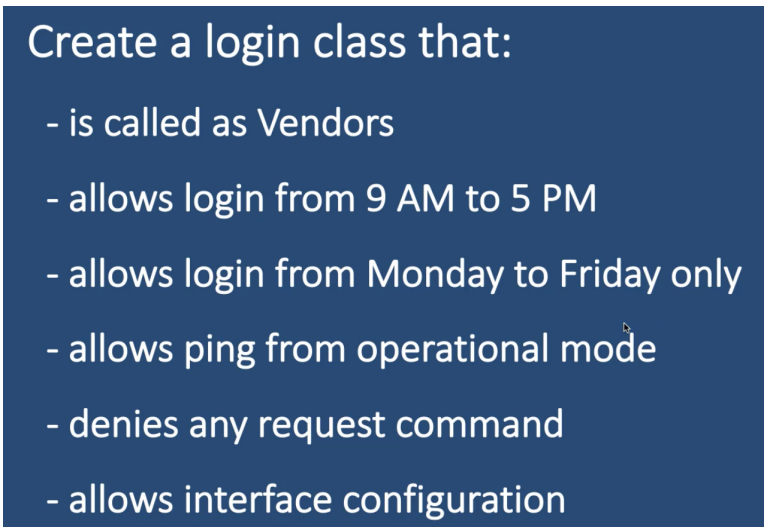
Customize Login Class

- **# edit system login**
- **# set class <name> <topic>**

```
shyam@SRX# set class DEMO ?
Possible completions:
  access-end           End time for remote access (hh:mm)
  access-start         Start time for remote access (hh:mm)
  allow-commands       Regular expression for commands to allow explicitly
+ allow-commands-regexps  Object path regular expressions to allow commands
  allow-configuration  Regular expression for configure to allow explicitly
+ allow-configuration-regexps  Object path regular expressions to allow
  allow-hidden-commands  Allow all hidden commands to be executed
+ allowed-days         Day(s) of week when access is allowed.
+ apply-groups         Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups
> cli
  configuration-breadcrumbs  Enable breadcrumbs during display of configuration
> confirm-commands     List of commands to be confirmed explicitly
  deny-commands        Regular expression for commands to deny explicitly
+ deny-commands-regexps  Object path regular expressions to deny commands
  deny-configuration   Regular expression for configure to deny explicitly
+ deny-configuration-regexps  Object path regular expressions to deny
  idle-timeout         Maximum idle time before logout (minutes)
  login-alarms         Display system alarms when logging in
  login-script         Execute this login-script when logging in
  login-tip            Display tip when logging in
> no-hidden-commands   Deny all hidden commands with exemptions
+ permissions          Set of permitted operation categories
  security-role        Common Criteria security role
  tenant               Tenant associated with this login
[edit system login]
```

- **# set class <name> <topic> permissions**

```
Possible completions:
  [                     Open a set of values
  access                Can view access configuration
  access-control        Can modify access configuration
  admin                 Can view user accounts
  admin-control         Can modify user accounts
  all                   All permission bits turned on
  clear                 Can clear learned network info
  configure             Can enter configuration mode
  control               Can modify any config
  field                 Can use field debug commands
  firewall              Can view firewall configuration
  firewall-control      Can modify firewall configuration
  floppy                Can read and write the floppy
  flow-tap              Can view flow-tap configuration
  flow-tap-control      Can modify flow-tap configuration
  flow-tap-operation    Can tap flows
  idp-profiler-operation  Can Profiler data
  interface             Can view interface configuration
  interface-control     Can modify interface configuration
  maintenance           Can become the super-user
  network               Can access the network
  pgcp-session-mirroring  Can view pgcp session mirroring configuration
  pgcp-session-mirroring-control  Can modify pgcp session mirroring configuration
  reset                 Can reset/restart interfaces and daemons
  rollback              Can rollback to previous configurations
  routing               Can view routing configuration
  routing-control       Can modify routing configuration
  secret                Can view secret statements
  secret-control        Can modify secret statements
  security              Can view security configuration
  security-control      Can modify security configuration
  shell                 Can start a local shell
  snmp                  Can view SNMP configuration
  snmp-control          Can modify SNMP configuration
  storage               Can view fibre channel storage protocol configuration
  storage-control       Can modify fibre channel storage protocol configuration
  system                Can view system configuration
  system-control        Can modify system configuration
  trace                 Can view trace file settings
  trace-control         Can modify trace file settings
  unified-edge          Can view unified edge configuration
  unified-edge-control  Can modify unified edge configuration
  view                  Can view current values and statistics
  view-configuration    Can view all configuration (not including secrets)
---(more 100%)---
```



- **edit system login**
- **edit class Vendors**
- **set access-start 09:00**
- **set access-end 17:00**
- **set allowed-days [monday tuesday wednesday thursday friday]**
- **set allow-commands ping**
- **set deny-commands request**
- **set permissions interface-control**
- **set permissions configure**

User Accounts

- provide a way for users to access the Junos device
- each user has a home directory on the device - **/var/home/username**
- users can access the device without accounts if RADIUS or TACACS+ servers have been configured (centralized user management services)

user account
- username: unique string, up to 64 characters in length, without spaces, colons, or commas
- user identifier: numeric identifier associated with username
- full name
- login class
- authentication method

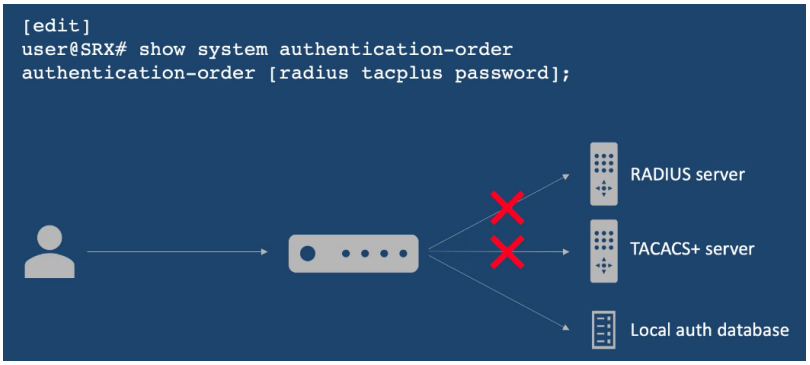
create user account command
- ***edit system login***
- ***set user <name> class <class type> authentication <type>***
- top commit

Authentication Methods

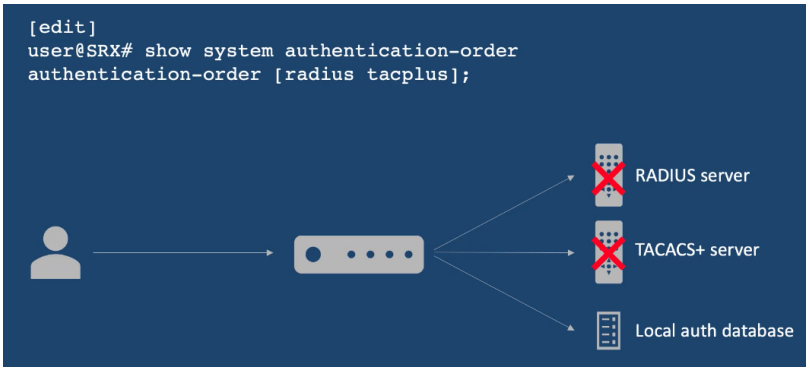
- local password authentication (configured on the Junos device)
- remote authentication Dial-In User Service (RADIUS)
- terminal access controller access control system plus (TACACS+)

RADIUS and TACACS+ are distributed client and server systems - the client runs on the Junos device, while the server runs on a remote host.

For each login attempt, Junos tries the authentication methods in order, until the password is accepted. If the previous authentication method failed to reply, or if the method rejected the login attempt, the next method is tried.



If not authentication method not respond



Intro Types of Interfaces

- Primarily used to connect a device to a network
- Some interfaces are also used to provide a service or a specific function for the system
- can be physical or logical

Types of interfaces

- Management interfaces
- Internal interfaces

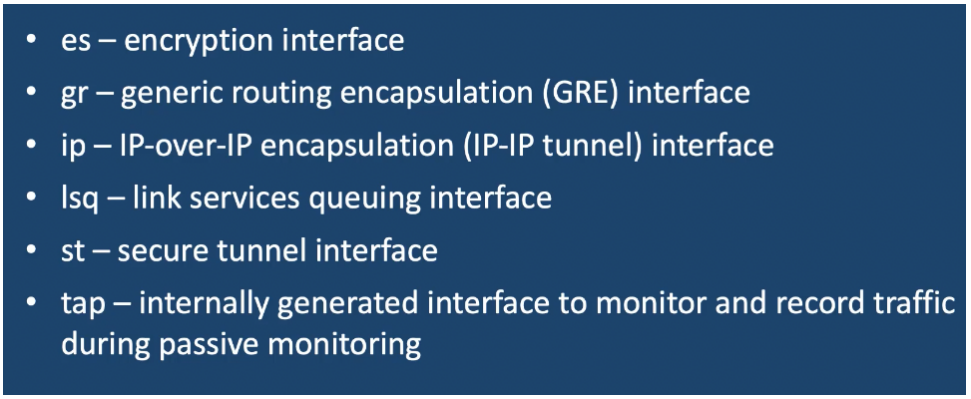
- Network interfaces
- Service interfaces
- Loopback interfaces

Management Interface
- dedicated interface used to connect the Junos device to a management network
- common designation include fxp0 and me0

Internal Interface
- Provide communication between the Routing Engine and the Packet Forwarding Engine
- Automatically configured when the device boots
- common designation include fxp1 and me0

Network Interface
- Provide physical connections to other devices
- Examples include Ethernet, SONET, Asynchronous Transfer Mode (ATM), TI, and DS3

Service Interface
- used to provide one or more traffic manipulating services such as encapsulation, encryption, tunneling, and link services
- service interfaces may be provided through a physical interface card or through software



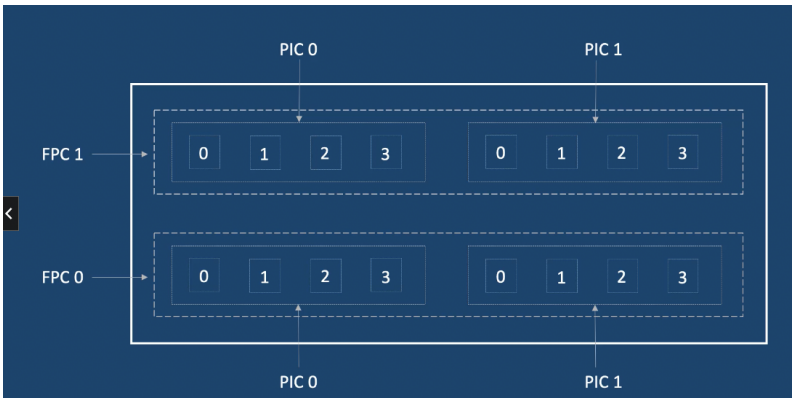
Loopback interface
- Traffic sent to the loopback interface is addressed to the same device
- uses the lo0 designation on all platforms
- used to identify the device and is the preferred method to determine if the device online

Interface Naming Convention

Most interfaces are name as **type - fpc/pic/port**
- fpc - flexible PIC concentrator - line card slot number
- pic - physical interface card - interface card slot number

- port - port number

Example: ge-1/0/1



- Some interfaces do not follow naming convention:
  - lo0 – loopback interface
  - ae – aggregated Ethernet interface
  - as – aggregated SONET interface
  - vlan – VLAN interface

Interface Properties

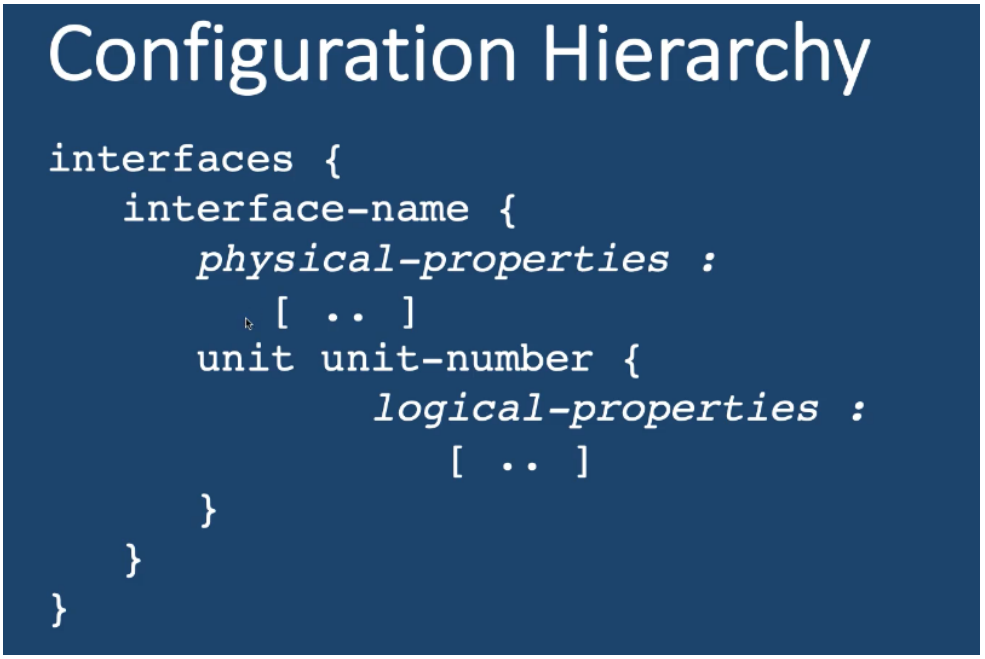
Physial Properties

- Mode - half duplex or full duplex
- Speed - link speed
- MTU - maximum transmission unit, varies from 256-9192 bytes
- Clock - interface clock sources, either internal or external
- Frame Check Sequence (FCS) - error detection scheme
- Encapsulation - types include PPP, Frame Relay, PPPoE

Logical Properties

- Protocol Family - inet, ient6, iso, mpls, ethernet-switching
- Address - e.g. IP address for inet family
- VLAN tagging
- Firewall filters or routing policies

unit keyboard used for logical interface



Interface Address Configuration

- Junos device can have more than one IP address on a single logical interface
- Issuing a second set command does not overwrite the previous address but rather adds an additional address under the logical unit
- To change an existing address use **rename** or **delete**
- ***rename address <ip> to address <ip>***

Preferred Address

- used when you have multiple IP addresses belonging to the same subnet on the same interface
- allows you to select which address will be used as the source address for packets sent to hosts on the directly connected subnet
- **By default, this is the numerically lowest address**

Primary Address

- used as the source address for broadcast and multicast packets
- **By default, this is the numerically lowest address**

Multiple Protocol Families

```
[edit]
user@SRX# show interfaces
ge-0/0/0 {
    unit 0 {
        family inet {
            address 10.1.1.1/24;
        }
        family inet6 {
            address 2001:db8::2/128;
        }
    }
}
```

Configuration Groups

- Common configuration snippets that can be applied to other parts of the configuration
- Create a group containing configuration statements and apply that to the rest of the configuration
- Ideal for grouping statements that are repeated in many places in the configuration

First configuration group take priority, we can override the value
show groups junos-defaults

edit groups band-config interfaces ge-0/0/1 unit <*>
set bandwidth 100

```
[edit]
root# show groups band-config
interfaces {
    ge-0/0/1 {
        unit <*> {
            bandwidth 100;
        }
    }
}

[edit]
```

set interfaces ge-0/0/1 apply-groups band-config
show interfaces ge-0/0/1 | display inheritance

// to specify a unit 5 not inherited from band-config
set interfaces ge-0/0/1 unit 5 apply-groups-except band-config

System Logs

- used to record system-wide, high-level operations, such as interfaces going up or down, or users logging in to or out of the device.
- logs are placed in files that are stored in the **/var/log** directory
- the primary syslog which is included in all factory default configurations is the **/var/log/messages file**
- Each system log message belongs to a **facility**
- A facility is a group of messages that are either generated by the same software process or concern a similar activity (such as authentication attempts)
- each message is also assigned a severity level that indicates how seriously the triggering event affects the device functions

Facility	Type of Event or Error
any	All messages from all facilities
authorization	Authentication and authorization attempts
change-log	Changes to the Junos configuration
daemon	Actions performed or errors encountered by system processes
firewall	Packet filtering actions performed by a firewall filter
interactive-commands	Commands issued at the Junos CLI
kernel	Actions performed or errors encountered by the Junos kernel
security	Security related events or errors
user	Actions performed or errors encountered by user processes

Value	Severity Level	Description
N/A	none	Disables logging of the associated facility
0	emergency	System panic or other condition that causes the device to stop functioning
1	alert	Conditions that require immediate correction, such as a corrupted system database
2	critical	Critical conditions
3	error	Error conditions that have less serious consequences
4	warning	Conditions that warrant monitoring
5	notice	Conditions that are not errors but might warrant special handling
6	info	Events or non-error conditions of interest
7	any	Includes all severity levels

Configuring Syslog

edit system syslog
set file cli-commands interactive-commands any
set file change-log change-log any
set file security security any
commit

```
root@SRX# show
file cli-commands {
    interactive-commands any;
}
file change-log {
    change-log any;
}
file security {
    security any;
}
```

annotate file cli-commands “/* Logs commands entered by users*/”

```
root@SRX# show
/* Logs commands entered by users */
file cli-commands {
    interactive-commands any;
}
file change-log {
    change-log any;
}
file security {
    security any;
}
```

> show log cli-commands

```
May  4 13:55:27  SRX mgd[5941]: UI_CMDLINE_READ_LINE: User 'root', command 'set file security security any '
May  4 13:55:30  SRX mgd[5941]: UI_CMDLINE_READ_LINE: User 'root', command 'show '
May  4 13:56:02  SRX mgd[5941]: UI_CMDLINE_READ_LINE: User 'root', command 'annotate file cli-commands "/* Logs commands entered by users */" '
May  4 13:56:04  SRX mgd[5941]: UI_CMDLINE_READ_LINE: User 'root', command 'show '
May  4 13:56:26  SRX mgd[5941]: UI_CMDLINE_READ_LINE: User 'root', command 'annotate file change-log "/* Logs all config changes */" '
May  4 13:56:40  SRX mgd[5941]: UI_CMDLINE_READ_LINE: User 'root', command 'annotate file security "/* Logs all security events */" '
May  4 13:56:42  SRX mgd[5941]: UI_CMDLINE_READ_LINE: User 'root', command 'show '
May  4 13:57:11  SRX mgd[5941]: UI_CMDLINE_READ_LINE: User 'root', command 'annotate file security "" '
May  4 13:57:14  SRX mgd[5941]: UI_CMDLINE_READ_LINE: User 'root', command 'show '
May  4 13:57:22  SRX mgd[5941]: UI_CMDLINE_READ_LINE: User 'root', command 'annotate file security "/* Logs all security events */" '
May  4 13:57:24  SRX mgd[5941]: UI_CMDLINE_READ_LINE: User 'root', command 'show '
May  4 13:58:24  SRX mgd[5941]: UI_CMDLINE_READ_LINE: User 'root', command 'set user * any emergency '
May  4 13:58:27  SRX mgd[5941]: UI_CMDLINE_READ_LINE: User 'root', command 'show '
May  4 13:58:34  SRX mgd[5941]: UI_CMDLINE_READ_LINE: User 'root', command 'commit '
```

> help syslog UI_CMDLINE_READ_LINE

```
root@SRX> help syslog UI_CMDLINE_READ_LINE
Name:          UI_CMDLINE_READ_LINE
Message:       User '<username>', command '<command>'
Help:          User entered command at CLI prompt
Description:   The indicated user typed the indicated command at the CLI prompt and pressed the Enter key, sending the command string to the management process (mgd).
Type:          Event: This message reports an event, not an error
Severity:      info
Facility:      LOG_AUTH
```

Syslog Entries

- timestamp - indicates when the message was logged
- name - configured system name
- process name or PID - name or ID of the process that generated the log entry
- message code - identifies nature and purpose of the message
- message text - provides additional information related to message code

Explicit Priority

To add a numeric priority value consisting of facility and severity level to syslog messages, add the `explicit-priority` statement

Before:

```
Apr 23 13:41:52 my-junos mgd[79821]: UI_CMDLINE_READ_LINE: User
'shyam', command 'set file cli-commands explicit-priority'
```

After:

```
Apr 23 13:42:19 my-junos mgd[79821]: %INTERACT-6-UI_CMDLINE_READ_LINE:
User 'shyam', command 'commit'
```

Archival

- When a log file called ***logfile*** is achieved, the file is closed, compressed, and its name is changed to ***logfile.0.gz***
- Logs are then written to a new file called logfile
- can be configured for all files or individual files

delete log file

```
root@SRX> file delete /var/log/cli-commands
```

clear log file

```
root@SRX> clear log change-log
```

Tracing

- Tracing allows you to track events that occur in the device - both normal operations and error conditions
- when enabled, a trace file is created that is used to store decoded protocol information received or sent by the routing engine.
- Tracing results are sent to a specific file stored in the /var/log dir or to a remote syslog server
- to avoid unnecessary resource consumption, tracing must be stopped when not needed

```
[edit]
root@SRX# set security policies traceoptions file policy.txt files 3

root@SRX# set security policies traceoptions flag ?
Possible completions:
  all                  Trace everything
  compilation          Policy compilation events
  configuration        Trace configuration events
  ipc                  Inter-process communication events
  lookup               Policy lookup events
  routing-socket       Trace routing socket events
  rules                Policy rules related events
[edit]
root@SRX# set security policies traceoptions flag all
```

trace for physical interface only
if in a specific interface, trace stored in messages no file option

```
root@SRX# set interfaces traceoptions file interface.txt size 10K

[edit]
root@SRX# set interfaces traceoptions flag ?
Possible completions:
  alert                Log DCD alert events
  all                  Enable all configuration logging
  bfd-events           Log BFD related events
  change-events        Log changes that produce configuration events
  config-states        Log the configuration state machine changes
  critical             Log DCD critical events
  debugging            Log DCD debug events
  emergency            Log DCD emergency events
  error                Log DCD error events
  gres-events          Log the events related to GRES
  informational        Log DCD informations
  japi                 Log DCD JAPI events
  kernel               Log configuration IPC messages to kernel
  kernel-detail        Log details of configuration messages to kernel
  lib-events           Log DCD library related events
  notice               Log DCD notification events
  reserved             Reserved DCD logs
  resource-usage       Log the resource usage for different states
  select-events        Log the events on select state machine
  verbose              Log DCD debug all events
  warning              Log DCD warning events
[edit]
root@SRX# set interfaces traceoptions flag all
```

Delete traceoptions

```
[edit]
root@SRX# show | match traceoptions | display set
set security policies traceoptions file policy.txt
set security policies traceoptions file files 3
set security policies traceoptions flag all
set interfaces traceoptions file interface.txt
set interfaces traceoptions file size 10k
set interfaces traceoptions flag all

[edit]
root@SRX# delete security policies traceoptions

[edit]
root@SRX# delete interfaces traceoptions
```

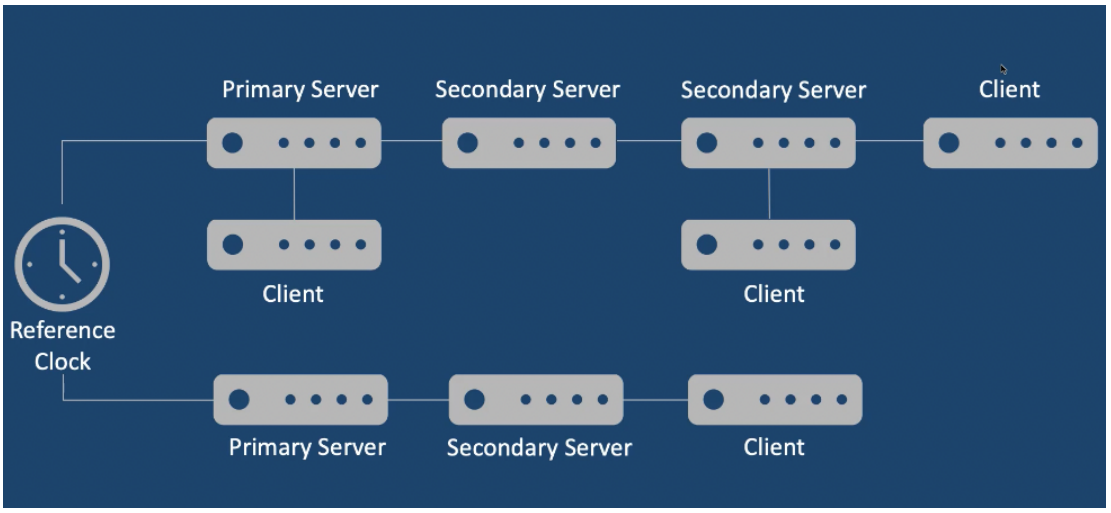
Network Time Protocol

- used to synchronize the clocks of routers and other hardware devices on the internet.
- debugging and troubleshooting is much easier when the timestamps in the log files of all the devices are synchronized
- Junos devices can be configured to act as an NTP client, a secondary NTP server, or a primary NTP server.

Primary NTP Servers
- Synchronized to a reference clock that is directly traceable to UTC
- These servers then re-distribute this time data downstream to other secondary NTP servers or NTP clients

Secondary NTP servers
- synchronized to a primary or secondary NTP server
- these servers then re-distribute this data downstream to other secondary NTP servers or NTP clients

NTP client
- synchronized to a primary or secondary NTP server
- do not redistribute time data to other servers



NTP Modes
Brodcast mode
- used to transmit time information to a specified broadcast or multicast address
- other device listen for time syn packets on these addresses

Client/Server mode
- with client mode, the local device synchronizes with the remote system, but the remote system can never be synchronized with the local device
- with server mode, the local device operates as an NTP server

Symmetric Active Mode
- the local device and the remote system can synchronized with each other

NTP
- if an NTP client drifts by more than 128 milliseconds, it tries to synchronize with the server
- to manually synchronize with a server use the command ***set date ntp***

NTP Boot Server vs NTP Server

- When an **NTP boot server** is configured, when the device boots, it immediately synchronizes with the boot server
- The device synchronizes with the boot server even if the NTP process is explicitly disbaled
- When an **NTP server** is configured, the device is synchronized with periodic updates

edit system ntp
set server pool.ntp.org

```
root@SRX> show system uptime
Current time: 2020-05-04 07:56:59 UTC
Time Source:  NTP CLOCK
System booted: 2020-05-04 07:26:40 UTC (00:30:19 ago)
Protocols started: 2020-05-04 07:29:36 UTC (00:27:23 ago)
Last configured: 2020-05-04 07:56:44 UTC (00:00:15 ago) by root
 7:56AM  up 30 mins, 1 users, load averages: 1.27, 1.30, 1.12

root@SRX> show ntp associations
   remote         refid           st t when poll reach   delay   offset  jitter
==============================================================================
 198.255.68.106   .STEP.          16 - 1100   64    0    0.000    0.000 4000.00

root@SRX> show ntp status
status=c035 sync_alarm, sync_unspec, 3 events, event_clock_reset,
version="ntpd 4.2.0-a Thu Mar 21 09:24:25  2019 (1)", processor="amd64",
system="FreeBSDJNPR-11.0-20190305.df99236_buil", leap=11, stratum=16,
precision=-23, rootdelay=0.000, rootdispersion=1.095, peer=0,
refid=STEP, reftime=00000000.00000000  Thu, Feb  7 2036  6:28:16.000,
poll=4, clock=e25a4987.02b04ec5  Mon, May  4 2020  7:57:59.010, state=3,
offset=0.000, frequency=0.000, jitter=0.000, stability=0.000
```

> set date ntp //mannual sync
> set date ntp <server>

SNMP

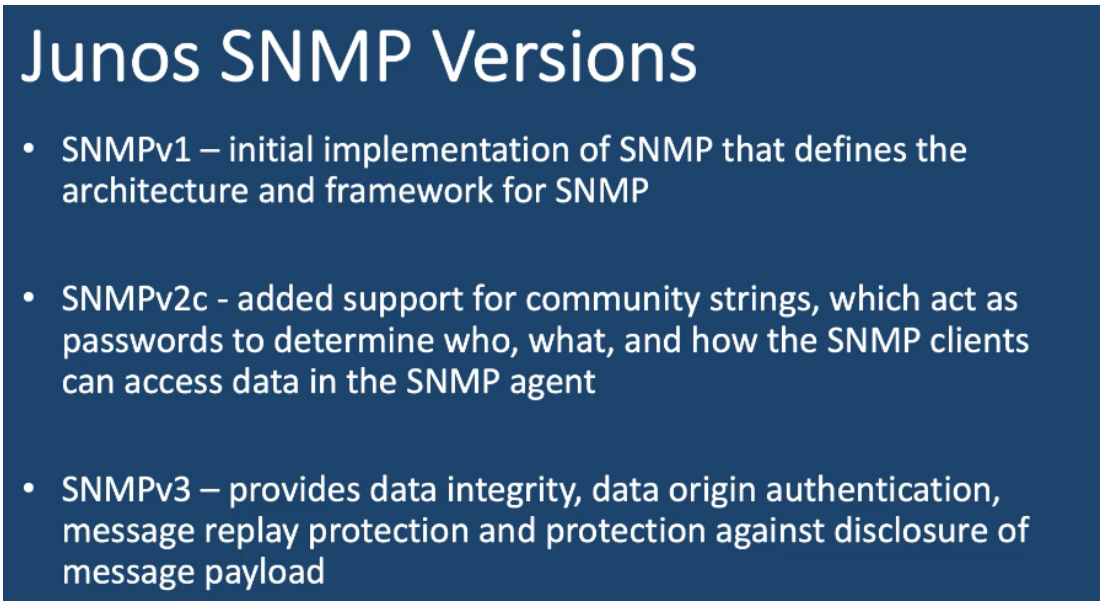
- SNMP enables the monitoring of network devices from a central location
- This is done using two entities
    - SNMP agent (process running on the Junos device)
    - Network management system (NMS) (server that monitor device)

SNMP agent

- exchanges network management information with SNMP manager software running on an NMS
- responds to requests for information and actions from the manager

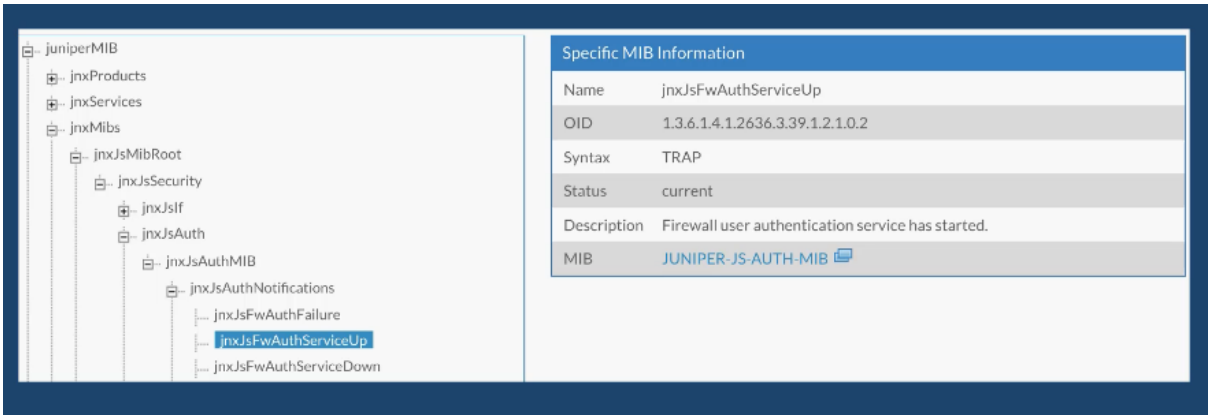
NMS

- collects information about network connectivity, activity, and events by polling managed devices



Management Information Base

- SNMP data is stored in a highly structured, hierarchical format
- The MIB structure is based on a tree structure, with related objects being grouped together
- Each object in the MID is associated with an object identifier (OID), which names the object
- The “leaf” in the tree structure is the actual managed object instance, which represents a resource, event, or activity that occurs on the device



- MIBs are either **standard** or **enterprise-specific**
- standard MIBs are defined by IETF
- Enterprise-specific MIBs are defined by a specific equipment manufacturer

SNMP Communication

- Get, GetBulk, and GetNext requests - manager requests information from the agent, the agent returns information in a GET response message
- Set requests - manager changes the value of an MIB object controlled by the agent; the agent indicates status in a Set response message
- Trap Notification - agent send traps to notify the manager of significant events that occur on the device.

SNMP Traps and Informs

- Junos devices can send notifications to SNMP managers when significant events occur on a network device, most often eros or failures
- SNMP notifications can be sent as traps or inform requests
- SNMP traps are unconfirmed notification
- SNMP informs are confirmed notification

```
root@SRX> show snmp mib walk jnxMibs
jnxBoxClass.0 = jnxProductLineVSRX.0
jnxBoxDescr.0 = Juniper VSRX Internet Router
jnxBoxSerialNo.0 = 1c762e5c9c2b
jnxBoxRevision.0
```

Configure SNMP for remote

> edit
edit snmp
set name “My Junos”
set contact “Shyam - xxx xxx x999”
set community myjunos authorization read-only
set community myjunos clients 10.0.10.100
commit

```
[edit snmp]
root@SRX# show
name "My Junos";
contact "Shyam - xxx xxx x999";
community myjunos {
    authorization read-only;
    clients {
        10.0.10.100/32;
    }
}
```

To access Junos device
$ snmpwalk -v 2c -c myjunos 10.0.10.254

Rescue Configuration

- user-defined, known-good configuration that is designed to restore connectivity in the event of configuration problems.
- if the active configuration is corrupted, the device **automatically** loads the rescue configuration file as the active configuration
- use > **request system configuration rescue** save to save a rescue config
- **> file list /config** to show the rescue config file **rescue.conf.gz**
- we can roll back by **rollback rescue**
- **request system configuration rescue delete** to delete

Backups

- Junos can backup the current configuration using FTP or SCP, periodically or after each commit
- If more than one archive site is specified, the system attempts to transfer the configuration file to the first archive site in the list, moving to the next site only if the transfer fails
- Once the configuration file is transferred to the remote storage device, a system log message is generated, confirming success or failure of the transfer

// every time we commit, the config backed up or archived to the archival site
edit system archival
set configuration transfer-on-commit
commit

// config archival site
set configuration archive-sites ftp://shaym@10.0.10.100 password “junos123”
commit
show

```
root@SRX# show
configuration {
    transfer-on-commit;
    archive-sites {
        "ftp://shyam@10.0.10.100" password "$9$bsY4ZHqfn/tqmBEcSeK4aJDqm"; ## SECRET-DATA
    }
}
```

> show log messages | match transfer

```
May 24 13:42:24  SRX pfed: ACCT_TRANSFER_FILE_FAILED:  upload_dir:1793 Error <65280> uploading file '/var/transfer/config/_20200524_122958_juniper.conf.gz'
May 24 13:44:24  SRX pfed: ACCT_TRANSFER_FILE_FAILED:  upload_dir:1793 Error <256> uploading file '/var/transfer/config/_20200524_122958_juniper.conf.gz'
May 24 14:35:59  SRX mgd[18661]: UI_CFG_AUDIT_SET: User 'root' set: [system archival configuration] <unconfigured> -> "transfer-on-commit"
May 24 14:35:59  SRX mgd[18661]: UI_CMDLINE_READ_LINE: User 'root', command 'set configuration transfer-on-commit '
May 24 14:36:44  SRX mgd[18661]: UI_CFG_AUDIT_SET: User 'root' set: [system archival configuration transfer-interval] <unconfigured> -> "1440"
May 24 14:36:44  SRX mgd[18661]: UI_CMDLINE_READ_LINE: User 'root', command 'set configuration transfer-interval 1440 '
May 24 14:37:00  SRX mgd[18661]: UI_CFG_AUDIT_SET: User 'root' set: [system archival configuration] <unconfigured> -> "transfer-on-commit"
May 24 14:37:00  SRX mgd[18661]: UI_CMDLINE_READ_LINE: User 'root', command 'set configuration transfer-on-commit '
May 24 14:38:47  SRX mgd[18894]: UI_CFG_AUDIT_SET: User 'root' set: [system archival configuration] <unconfigured> -> "transfer-on-commit"
May 24 14:38:47  SRX mgd[18894]: UI_CMDLINE_READ_LINE: User 'root', command 'set configuration transfer-on-commit '
May 24 14:40:33  SRX logger: transfer-file: Transferred /var/transfer/config/SRX_20200524_144420_juniper.conf.gz
May 24 14:40:36  SRX mgd[18894]: UI_CMDLINE_READ_LINE: User 'root', command 'show log messages | match transfer '
```