<table>
<thead>
<tr>
<th>Agenda</th>
<th>Description</th>
<th>Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Firmware Distribution</td>
<td>All platforms</td>
</tr>
<tr>
<td>2</td>
<td>Log Buffer Notification</td>
<td>Feature specific, check platform</td>
</tr>
<tr>
<td>3</td>
<td>Admin Access to the log file</td>
<td>6200,6300,6400</td>
</tr>
<tr>
<td>4</td>
<td>Locked out Users</td>
<td>All platforms</td>
</tr>
<tr>
<td>5</td>
<td>Prefer statement on NTP Server</td>
<td>All platforms</td>
</tr>
<tr>
<td>6</td>
<td>IPv6 RA Guard (without ND Guard)</td>
<td>8325</td>
</tr>
<tr>
<td>7</td>
<td>‘sh ip ospf interface’ improvement</td>
<td>All ospv2 platforms</td>
</tr>
<tr>
<td>8</td>
<td>‘sh spanning tree’ improvement</td>
<td>All platforms</td>
</tr>
<tr>
<td>9</td>
<td>‘sh mac-address’ improvement</td>
<td>All platforms</td>
</tr>
</tbody>
</table>
Usability
Firmware Distribution - REST
All switch platforms
Firmware Site Distribution - REST

AO-CX Firmware site distribution feature supports a switch and image to be used as a local image distributor.

Supported by any CX Switch with 10.09 or later

Uses the same existing Firmware REST API

No cross-family image distribution between switches

Process is to

• Upgrade switch image slot in a switch (optionally reboot)
• Then use the switch image as a local image distributor
Example

1. Central triggers an upgrade request on the desired switch
2. Switch updates its firmware image via the target image server
3. Central can now leverage the Switch as the distribution server

The Central functionality to provide the orchestration will be present in the next release
(*anticipated release 2.5.5)
Usability

Log Buffer notification - Notify when logs exceed threshold
Problem Statement

Some features inadvertently fill the partition with logs in the /var/log directory and when the log-buffer ‘wraps’, the older logs are overwritten with no user warning or notification.

A method is required to ensure that the Network Administrator has the option of copying log files prior to the overwrite and is notified via rmon traps and an event log raised whenever the log buffer or var/log directory size exceeds its threshold limit.
Solution Overview

Generate an event log as well as a rmon trap whenever the log buffers exceeds its limit.

Log buffer notification supported below log buffers
- Event logs
- Auth logs
- Audit logs
- Security logs (Applicable to 6200, 6300 and 6400 platforms).

Platform support [event log/audit/auth log]
4100i, 6100, 6200, 6300, 6400, 8320, 8325, 8360, 8400

Security log platform support - new
6200/6300/6400
Design detail

Log buffer monitoring:

The log buffer is split into manageable ‘chunks’.
The size and the number of ‘chunks’ may vary based on the platform.
Whenever one chunk is full, it will be archived and a new chunk is created for storing new logs.
When the max limit for the last chunk number is reached, the chunk is archived & the oldest chunk will be deleted.
The log buffer almost full event and snmp RMON trap is raised whenever the number of chunks reaches one less than the max limit.
User can collect the needed logs before they get rotated.
The log buffer overwritten event and snmp RMON trap is raised whenever the max limit is hit resulting in rotating the oldest chuck.
Uses the logrotate functionality to notify log-mgmtd, whenever log buffers are reaching to their threshold and about to rotate/wrapped.
The log-mgmtd will trigger the event/trap notification as appropriate.
Example – 6300 platform

Log Buffer chunks of 16mb each
When 5 chunks are consumed, a log buffer almost full event with snmp RMON trap is triggered

1. When one chunk is full, it is archived and a new chunk is created.
2. When 5 chunks (80 mb) is consumed, the log buffer almost full event and snmp RMON trap is triggered.
3. When 6 chunks are consumed, the log buffer full event and snmp RMON trap is triggered.
4. When the max limit is reached on the number of chunks, the oldest chunk is deleted.
5. The log buffer almost full event and snmp RMON trap is raised whenever the number of chunks reaches one less than the max limit.
Example Log threshold CLI

Log Buffer chunks of 16mb each – 6300 (chunk size will vary for each platform)
% values indicates the log buffer chunk is full

Syntax:

[no] log-threshold { event-log | security-log | audit-log | auth-log } <15 | 30 | 50 | 70 | 90 | 100>

Default threshold-limit: 90

*Avoid changing the default threshold higher than 90%
Example Log threshold rotation

Whenever one chunk is full, it will be archived and a new chunk is created for storing the new logs.

When we hit the max limit for the number of chunks, the oldest chunk will be deleted.
Log archive and retrieval

- Start shell from cli prompt
- Shell commands
- Rotated audit log file ‘chunk1’
- Allow apps that are network namespace unaware to be run outside of the default network namespace
- Run SFTP commands to destination host server
Commands

switch(config)# log-threshold event-log 30
switch(config)# log-threshold auth-log 50
switch(config)# log-threshold audit-log 70
switch(config)# log-threshold security-log 50
switch(config)# no log-threshold event-log
switch(config)# no log-threshold auth-log
switch(config)# no log-threshold audit-log
switch(config)# no log-threshold security-log

‘no log-threshold’ command restores the log default value
### Platform storage capacity

<table>
<thead>
<tr>
<th>Platform</th>
<th>Flash size/type</th>
</tr>
</thead>
<tbody>
<tr>
<td>6100</td>
<td>16GB eMMC</td>
</tr>
<tr>
<td>6200</td>
<td>16GB eMMC</td>
</tr>
<tr>
<td>4100i</td>
<td>32GB eMMC</td>
</tr>
<tr>
<td>6300</td>
<td>32GB eMMC</td>
</tr>
<tr>
<td>6400</td>
<td>32GB eMMC</td>
</tr>
<tr>
<td>8360</td>
<td>32GB eMMC</td>
</tr>
<tr>
<td>8320</td>
<td>64GB SSD</td>
</tr>
<tr>
<td>8325</td>
<td>64GB SSD</td>
</tr>
<tr>
<td>8400</td>
<td>100GB SSD</td>
</tr>
<tr>
<td>10000</td>
<td>64GB SSD</td>
</tr>
</tbody>
</table>

*eMMC = embedded multimedia card  
SSD = solid state drive  
*SSD will be considerably faster when transferring data compared to an eMMC storage device*
Summary

All platforms have 6 ‘chunks’ for event, auth and Security logs
All platforms have 2 ‘chunks’ for audit logs
The size of the platform ‘chunk’ will vary depending on platform, some platforms are ‘lightweight’.
Usability

Admin access to the logfile (security log) 6200/6300/6400
Admin Access to the security logfile – 6200,6300,6400 series

A new log file is available for security logging as part of the security logging framework

The security logging is a framework to log events generated by daemons, process and plugins running within the switch software which are of a sensitive nature or related to authentication and authorisation.

The Security logging framework captures these generated security-logs into a secure file.

A local user group can be given privileges for viewing and copying the security logs to a remote location.

This privilege can only be granted by members of the ‘administrators’ user group.

The group that obtains the security permission behaves like a security user group or security auditor group.

Although members of the ‘administrators’ group can grant this privilege, they themselves are not permitted to execute the commands.
Security User and built in groups

A security user is a user having access to only security log related commands and no other access on the switch.

Administrators are advised to configure a user group permitting only security log commands.

A security user can be created to similar to a local-user and can be given privilege to execute security-log related commands which are not available to any built-in-users.

It is advised that when such a security-user group is created no other commands apart from the security related commands are added to the group.

The 3 default built in roles: Administrators, operators, auditors are not permitted to execute the following CLI commands:

- `show security-logs`
- `clear security-logs`
- `copy security-logs`

Only a local user-group created and permitted to execute these commands by the users of the ‘administrators’ group have the required privilege.
Creating a security user group and user

user-group security-audit
20 permit cli command "clear security-logs*"
30 permit cli command "show security-logs*"
40 permit cli command "copy security-logs*"

*The assignment user groups and cli permissions are not new. The security-log and association events to the security-user is new

local user assignment to group membership security-audit

Security commands assigned to user group
### sh security-logs

- **-a**  Display event logs from previous and current boots
- **-c**  Display event logs for specified event category
- **-d**  Display event logs for specified daemon
- **-n**  Display the specified number of event logs
- **-r**  Display event logs in reverse order (most recent first)
- **-s**  Display event logs as per specified severity

#### 6200-BLDG02-F1# sh security-logs

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alert</td>
<td>Display logs with severity 'alert(6)' and above</td>
</tr>
<tr>
<td>crit</td>
<td>Display logs with severity 'critical(5)' and above</td>
</tr>
<tr>
<td>debug</td>
<td>Display logs with all severities</td>
</tr>
<tr>
<td>emerg</td>
<td>Display logs with severity 'emergency(7)' only</td>
</tr>
<tr>
<td>err</td>
<td>Display logs with severity 'error(4)' and above</td>
</tr>
<tr>
<td>info</td>
<td>Display logs with severity 'info(1)' and above</td>
</tr>
<tr>
<td>notice</td>
<td>Display logs with severity 'notice(2)' and above</td>
</tr>
<tr>
<td>warn</td>
<td>Display logs with severity 'warning(3)' and above</td>
</tr>
</tbody>
</table>

Users assigned to security-user group only have access to the assigned security cli commands.
Security-log commands access

6200-BLDG02-F1# sh security-logs
Permission denied. User cannot execute this command.

6200-BLDG02-F1# sh running-config
Cannot execute command. Command not allowed.

Users with admin privileges cannot access the security commands that are specific to users assigned to the security-group.

Users with security-group privileges cannot access other commands only the allocated [security] commands.

user-group security-audit
20 permit cli command "clear security-logs*"
30 permit cli command "show security-logs*"
40 permit cli command "copy security-logs*"
Summary

```
sh security-logs
clear security-logs [separate logfile]
copy security-log sftp://root@10.80.2.118/securelog vrf mgmt
copy security-log scp://root@10.80.2.118/securelog vrf mgmt
copy security-log tftp://root@10.80.2.118/securelog vrf mgmt
```

3 new commands

Security user group is supported with AAA configurations and standard RBAC features with Radius and Tacacs

The security user role is not ‘in built’ and has to be configured

Security user roles are created by the user-group administrators

Administrators cannot execute the associated security log commands (x3)

Only assigned users to the security-group can access the security log commands (the recommendation is to restrict to the security related commands only – and no other commands)
## EVENT-IDs Security logging - 1

<table>
<thead>
<tr>
<th>Event Name</th>
<th>ID</th>
<th>Description</th>
<th>Severity</th>
<th>Event Catagory</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERFACE_LINK_MACSEC_PFC_INCOMPAT</td>
<td>408</td>
<td>Log when interface is down due to incompatible MACsec and PFC configuration</td>
<td>LOG_WARN</td>
<td>INTERFACE</td>
</tr>
<tr>
<td>AAA_CONFIG</td>
<td>2301</td>
<td>Logs AAA Authentication/Authorization/Accounting/fail-through</td>
<td>LOG_INFO</td>
<td>AAA</td>
</tr>
<tr>
<td>TACACS</td>
<td>2302</td>
<td>Logs TACACS+ server update, server group update and global default update</td>
<td>LOG_INFO</td>
<td>AAA</td>
</tr>
<tr>
<td>RADIUS</td>
<td>2303</td>
<td>Logs RADIUS server update, server group update and global default update</td>
<td>LOG_INFO</td>
<td>AAA</td>
</tr>
<tr>
<td>RADIUS_TRACKING</td>
<td>2304</td>
<td>Logs changes in RADIUS server reachability status</td>
<td>LOG_INFO</td>
<td>AAA</td>
</tr>
<tr>
<td>TACACS_TRACKING</td>
<td>2305</td>
<td>Logs changes in TACACS server reachability status</td>
<td>LOG_INFO</td>
<td>AAA</td>
</tr>
<tr>
<td>RADIUS_SERVER_ROUTE_REACHABILITY</td>
<td>2306</td>
<td>Logs changes in RADIUS server route reachability status</td>
<td>LOG_INFO</td>
<td>AAA</td>
</tr>
<tr>
<td>SELFTEST_BEGIN</td>
<td>4501</td>
<td>logs the start of selftest on a particular subsystem</td>
<td>LOG_INFO</td>
<td>SELFTEST</td>
</tr>
<tr>
<td>SELFTEST_END</td>
<td>4502</td>
<td>logs the completion of selftest on a particular subsystem</td>
<td>LOG_INFO</td>
<td>SELFTEST</td>
</tr>
<tr>
<td>CARD_SELFTEST_FAILURE</td>
<td>4503</td>
<td>logs the selftest failure of a particular subsystem</td>
<td>LOG_ERR</td>
<td>SELFTEST</td>
</tr>
<tr>
<td>PORT_SELFTEST_FAILURE</td>
<td>4504</td>
<td>logs the port selftest failure on a given subsystem</td>
<td>LOG_ERR</td>
<td>SELFTEST</td>
</tr>
<tr>
<td>AUTZ_FAILURE</td>
<td>4506</td>
<td>logs a failed authorization attempt of a user via REST</td>
<td>LOG_ERR</td>
<td>SELFTEST</td>
</tr>
</tbody>
</table>
## EVENT-IDs Security logging -2

<table>
<thead>
<tr>
<th>Event Name</th>
<th>ID</th>
<th>Description</th>
<th>Severity</th>
<th>Event Catagory</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTZ_SUCCESS</td>
<td>4607</td>
<td>logs a successful authorization attempt of a user via REST</td>
<td>LOG_INFO</td>
<td>RESTD</td>
</tr>
<tr>
<td>AUTZ_ALLOWED</td>
<td>4608</td>
<td>logs an allowed authorization attempt of a user via REST</td>
<td>LOG_INFO</td>
<td>RESTD</td>
</tr>
<tr>
<td>USER_PASSWORD_CHANGE_SUCCESS</td>
<td>4611</td>
<td>logs a successful password change for a user via REST</td>
<td>LOG_INFO</td>
<td>RESTD</td>
</tr>
<tr>
<td>USER_PASSWORD_CHANGE_FAILURE</td>
<td>4612</td>
<td>logs an unsuccessful password change for a user via REST</td>
<td>LOG_WARN</td>
<td>RESTD</td>
</tr>
<tr>
<td>USER_PASSWD_CHANGE</td>
<td>4703</td>
<td>Logs a message when a user changes his/her password</td>
<td>LOG_INFO</td>
<td>USER-MGMT</td>
</tr>
<tr>
<td>USER_PASSWD_CHANGE_FAIL</td>
<td>4704</td>
<td>Logs a message when a user fails to change his/her password</td>
<td>LOG_ERR</td>
<td>USER-MGMT</td>
</tr>
<tr>
<td>PASSWD_EXPORT</td>
<td>4705</td>
<td>Logs a message when a user sets export password</td>
<td>LOG_INFO</td>
<td>USER-MGMT</td>
</tr>
<tr>
<td>NO_PASSWD_EXPORT</td>
<td>4706</td>
<td>Logs a message when a user restores default export password</td>
<td>LOG_INFO</td>
<td>USER-MGMT</td>
</tr>
<tr>
<td>DEFAULT_EXP_PASSWD_USED</td>
<td>6501</td>
<td>Warns the user that export password file was corrupted and default passwd was used instead.</td>
<td>LOG_WARN</td>
<td>CREDMGR</td>
</tr>
<tr>
<td>CHASSIS_SECRET_CORRUPTED</td>
<td>6502</td>
<td>Warns the user that the chassis secret has been corrupted.</td>
<td>LOG_ALERT</td>
<td>CREDMGR</td>
</tr>
<tr>
<td>SS_CERT_CREATED</td>
<td>6504</td>
<td>Logs a message when the self-signed cert is created by credmgr.</td>
<td>LOG_INFO</td>
<td>CREDMGR</td>
</tr>
<tr>
<td>SVOS_ADMIN_PW_CHANGED</td>
<td>6505</td>
<td>Logs a message when a user changes admin password from ServiceOS</td>
<td>LOG_INFO</td>
<td>CREDMGR</td>
</tr>
</tbody>
</table>
## EVENT-IDs Security logging -3

<table>
<thead>
<tr>
<th>Event Name</th>
<th>ID</th>
<th>Description</th>
<th>Severity</th>
<th>Event Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTH_KEY_CREATED</td>
<td>6506</td>
<td>Logs a message when SSH authorized keys are added for a user</td>
<td>LOG_INFO</td>
<td>CREDMGR</td>
</tr>
<tr>
<td>AUTH_KEY_FAILED</td>
<td>6507</td>
<td>Logs a message after a failure to write SSH authorized keys for a user</td>
<td>LOG_ERR</td>
<td>CREDMGR</td>
</tr>
<tr>
<td>AUTH_KEY_DELETED</td>
<td>6508</td>
<td>Logs a message after deleting SSH authorized keys for a user</td>
<td>LOG_INFO</td>
<td>CREDMGR</td>
</tr>
<tr>
<td>AUTH_KEY_INVALID</td>
<td>6509</td>
<td>Logs a message when SSH authorized key fails validation check</td>
<td>LOG_ERR</td>
<td>CREDMGR</td>
</tr>
<tr>
<td>ACL_LOG_STATS</td>
<td>1000</td>
<td>ACL log statistics</td>
<td>LOG_INFO</td>
<td>ACL</td>
</tr>
<tr>
<td>ACL_APPLICATION_FAILURE</td>
<td>1000</td>
<td>ACL application failure</td>
<td>LOG_ERR</td>
<td>ACL</td>
</tr>
</tbody>
</table>
Usability
locked out users
All platforms
locked out users

Login attempts can be limited with two new authentication commands impacting ssh vty access and console access.

```
6200-BLDG02-F1(config)# aaa authentication
   allow-fail-through   Allow AAA fail-through
   console-login-attempts Limit user console failed login attempts
   limit-login-attempts  Limit user failed login attempts
   login                 Switch login
   port-access           Configure Port Based Network Access.
```

```
6200-BLDG02-F1(config)# aaa authentication limit-login-attempts 5 lockout-time 60
```

```
6200-BLDG02-F1(config)# aaa authentication console-login-attempts 5 console-lockout-time 60
```

**Values**

- `login-attempts <1-10>` Max retries
- `lockout-time <1-360>` [seconds] Timeout
- `max lockout hr`
Locked out user example

6200-BLDG02-F1# sh user-list

<table>
<thead>
<tr>
<th>USER</th>
<th>GROUP</th>
</tr>
</thead>
<tbody>
<tr>
<td>contractor</td>
<td>administrators</td>
</tr>
<tr>
<td>security-user</td>
<td>security-audit</td>
</tr>
</tbody>
</table>

6200-BLDG02-F1# sh authentication locked-out-users

<table>
<thead>
<tr>
<th>USER</th>
<th>GROUP</th>
</tr>
</thead>
<tbody>
<tr>
<td>contractor</td>
<td>administrators</td>
</tr>
</tbody>
</table>
### Summary

<table>
<thead>
<tr>
<th></th>
<th>console-login-attempts</th>
<th>limit-login-attempts</th>
<th>console</th>
<th>SSH, REST &amp; Telnet</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scenario 1</strong></td>
<td>Enabled</td>
<td>Disabled</td>
<td>User locked out when configured limit-login threshold is exceeded</td>
<td>The locked out user can still access the switch through SSH, REST and Telnet interface</td>
</tr>
<tr>
<td><strong>Scenario 2</strong></td>
<td>Disabled</td>
<td>Enabled</td>
<td>The locked out user can access the switch through the console login</td>
<td>User is locked out of SSH, REST and Telnet when configured limit-login threshold is exceeded</td>
</tr>
<tr>
<td><strong>Scenario 3</strong></td>
<td>Enabled</td>
<td>Enabled</td>
<td>User will be locked Out from all interfaces when limit-login threshold is exceeded</td>
<td>User is locked out of all interfaces when limit-login threshold is exceeded</td>
</tr>
</tbody>
</table>
Caveats

If remote authentication using RADIUS/TACACS+ is configured on any channel (eg: ssh, https-server, console, telnet, default) then the console login attempts and lockout feature cannot be configured.

If console login attempts and lockout is configured, then remote authentication using RADIUS/TACACS+ cannot be configured on any channel.

Console login attempts configuration is only applied to console channel (not applied to SSH, TELNET and REST).

No timestamp available
Usability

Prefer statement on a NTP server
IPv4 IPv6
All AOS-CX switch platforms
NTP Server preference

BLDG01-AGG02(config)# ntp server time2.google.com
  burst  NTP Association use burst mode
  iburst  NTP Association use iburst mode
  key-id  NTP Key ID
  maxpoll  NTP maximum poll time to use configuration
  minpoll  NTP minimum poll time to use configuration
  prefer  NTP Association preference configuration
  version  NTP Association version configuration

ntp server 10.80.2.219 iburst prefer
ntp server time.google.com
ntp server time1.google.com
ntp enable

ip dns domain-name tmelab.net
ip dns server-address 10.80.2.219

Note when using multiple servers with the same stratum setting a preferred server is recommended.

Setting a preferred server, NTP will attempt to keep the preferred server the primary NTP connection.

If a preferred server is not manually set and NTP is enabled the configured server with the lowest stratum will automatically be set as the preferred server.

Prefer selection of servers with same stratum (if not manually selected) may change on reboot or reconfiguration.

Supported with IPv4 and IPv6 addressing
Summary & Caveats

IPv4 & IPv6 NTP services are supported.

If no manual preference is configured, an ‘auto’ preference is applied based on the configured server with the lowest stratum. This will automatically be set as the preferred server.

**A manual preferred server is highly recommended, especially when using multiple servers with the same stratum setting**

DHCP options can be used to configure up to 2 NTP servers

AOS-CX switches 4100i, 6100, 6200, 6300, 6400v1, v2 & 10000 using DHCP option (42) after the ‘erase all zeroize’ command.

1. DHCP uses the OBM port to get its Ip addresses and at the same time receive the DHCP NTP server detail
2. NTP is set to use the default VRF and using this method cannot access the NTP server to mark it as ‘preferred’
3. Work around is to use the mgmt. vrf for NTP ‘ntp vrf mgmt’
4. After connectivity via the mgmt. VRF, the default VRF can be used.
5. Does not impact 8400 & 8325 series
Usability
IPv6 RA guard without ND guard
AOS-CX 8325 Series
IPv6 RA Guard

Routers periodically multicast Router Advertisement (RA) messages to announce their availability and convey information to neighboring nodes that enable them to be automatically configured on the network.

Hosts listen for RA messages for IPv6 address autoconfiguration and discovery of link-local addresses of the neighboring routers, and can also send a Router Solicitation (RS) message to request immediate advertisements.

RA messages are unsecured, which makes them susceptible to attacks on the network that involve the spoofing (or forging) of link-layer addresses.

RA guard can be applied to filter router advertisements, either block or permit RAs based on trust or untrusted ports.

The RA guard feature is now available on the 8325 series platform.
**IPv6 RA Guard – Configuration notes**

**ND Snooping**

The ND snooping feature is used in Layer 2 switching networks. It learns the source MAC addresses, source IPv6 addresses, input interfaces, VLANs of arriving ND messages and data packets to build the ND snooping table. ND snooping entries can be used by ND detection to prevent spoofing attacks. ND detection processes the ND messages received on ND trusted and untrusted interfaces.

**RA Guard**

RA guard is applied to a VLAN.

ND-Snooping must enabled at a global level and at the desired VLAN level.

When enabled, ingress RA (Router Advertisement) and RR (Router Redirect) packets are blocked and dropped on untrusted ports.

RA/RR packets are forwarded if received on trusted ports.
IPv6 RA Guard feature - 8325 series

SwitchA

SwitchB

SwitchC

2001:DB8:0:1::/64

Trusted port

Untrusted port

2001:DB8:0:1::/64
RA guard applied to a VLAN

SERV-AGG02(config)# nd-snooping enable
SERV-AGG02(config)# vlan 101
SERV-AGG02(config-vlan-101)# nd-snooping ra-guard log

SERV-AGG02(config)# interface 1/1/5
SERV-AGG02(config-if)# no routing
SERV-AGG02(config-if)# vlan access 101
SERV-AGG02(config-if)# nd-snooping trust

*nd-snooping trust [interface/lag]

*nd-snooping trust [interface/lag]
Ingressing RA (Route Advertisements) RR (Router Redirect) packets are blocked/dropped on untrusted ports

nd-snooping enabled globally
nd-snooping with ra-guard

*nd-snooping trust [interface/lag]
Useful commands

SERV-AGG02# sh nd-snooping

  statistics  Show ND Snooping statistics
  vlan        Show ND Snooping configuration for the specific VLAN
  vsx-peer    Displays VSX peer switch information

SERV-AGG02# sh nd-snooping vlan 101

  ND Snooping Information
  ------------------------
  ND Snooping : Enabled
  MAC Address Check : Enabled
  RA Guard     : Enabled
  PORT        TRUST
---------- ------
  lag69    No
  lag256   No
  1/1/5    Yes
Usability

sh ip ospf interface
All platform support for OSPFv2
OSPF Passive interface

Either in the ospf context or per interface

```
router ospf 1
  router-id 10.69.253.4

interface 1/1/1
  no shutdown
  ip mtu 9192
  ip address 10.69.0.17/31
  ip ospf 1 area 0.0.0.0
  no ip ospf passive
  ip ospf network point-to-point
```

SwitchA

OSPF start-up sequence

SwitchB

Init - Ospf hello packets
Exstart - Peer relationship established
Exchange - Dbase synchronization
Loading - Link state updates between peers
Full – fully functional neighbor adjacency

Switch C in Init state

Switch C
VTEP2# sh ip ospf interface

Codes: DR - Designated router  BDR - Backup Designated router

Interface 1/1/49 is up, line protocol is up

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF</td>
<td>default</td>
</tr>
<tr>
<td>IP Address</td>
<td>192.168.2.3/31</td>
</tr>
<tr>
<td>Status</td>
<td>Up</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>10 sec</td>
</tr>
<tr>
<td>Transit Delay</td>
<td>1 sec</td>
</tr>
<tr>
<td>BFD</td>
<td>Disabled</td>
</tr>
<tr>
<td>Cost Configured</td>
<td>NA</td>
</tr>
<tr>
<td>State/Type</td>
<td>Point-to-point</td>
</tr>
<tr>
<td>DR</td>
<td>No</td>
</tr>
<tr>
<td>Link LSAs</td>
<td>0</td>
</tr>
<tr>
<td>Authentication</td>
<td>No</td>
</tr>
<tr>
<td>Passive</td>
<td>No</td>
</tr>
</tbody>
</table>

Process : 1  
Area : 0.0.0.0  
Network Type : Point-to-point  
Dead Interval : 40 sec  
Retransmit Interval : 5 sec  
Link Speed : 100000 Mbps  
Cost Calculated : 1  
Router Priority : n/a  
BDR : No  
Checksum Sum : 0
Usability

sh spanning-tree
All switch platforms
sh spanning-tree

6405-BLDG03# sh spanning-tree

Spanning tree status      : Enabled Protocol: MSTP

MST0

Root ID    Priority : 32768
MAC-Address: 90:20:c2:dc:47:00
This bridge is the root
Hello time(in seconds): 2  Max Age(in seconds): 20
Forward Delay(in seconds): 15

Bridge ID Priority : 32768
MAC-Address: 90:20:c2:dc:47:00
Hello time(in seconds): 2  Max Age(in seconds): 20
Forward Delay(in seconds): 15

Port         Role           State      Cost           Priority   Type             BPDU-Tx     BPDU-Rx   TCN-Tx   TCN-Rx
------------ ----------- -------------- ----------- --------- -------------- ---------- ---------- ---------- ----------
1/3/1 Disabled     Down  20000          128        P2P          0          0          0          0          
1/3/3 Disabled     Down  20000          128        P2P          0          0          0          0          
1/3/4 Disabled     Down  20000          128        P2P          0          0          0          0          

From Disabled/Blocking
To Disabled/Down
Usability
Show mac-address improvement
All switch platforms
show mac-address table port - adding Interface for port alias

Prior to 10.09

SwitchB# sh mac-address-table
  address  Show a specific MAC address
  count    Number of MAC addresses
  detail   Show Layer 2 MAC address table detail information
  dynamic  Show learnt MAC addresses
  hsc      Show MAC addresses learnt by the Hardware Switch Controller
  port     Show MAC addresses learnt on port
  static   Show static MAC address information
  vlan     Show MAC addresses learnt on VLANs
  vsx-peer Displays VSX peer switch information

'Sh mac-address-table port' command will be deprecated

SwitchB# sh mac-address-table port 1/1/1
  MAC age-time   : 300 seconds
  Number of MAC addresses : 1
  MAC Address    VLAN  Type  Port
  -------------------------------
  00:50:56:8e:fb:12  30    dynamic  1/1/1

10.09

SwitchA# sh mac-address-table
  address  Show a specific MAC address
  count    Number of MAC addresses
  detail   Show Layer 2 MAC address table detail information
  dynamic  Show learnt MAC addresses
  hsc      Show MAC addresses learnt by the Hardware Switch Controller
  interface Show MAC addresses learnt on interface
  port     Show MAC addresses learnt on port
  static   Show static MAC address information
  vlan     Show MAC addresses learnt on VLANs
  vsx-peer Displays VSX peer switch information

Replaced with 'sh mac-address-table interface' command

SwitchA# sh mac-address-table interface 1/1/1
  MAC age-time   : 300 seconds
  Number of MAC addresses : 1
  MAC Address    VLAN  Type  Interface
  -------------------------------
  00:50:56:8e:62:1d  20    dynamic  1/1/1
Thank you

Contact information