CIS Benchmarks

CIS Cisco NX-OS Benchmark

v1.0.0 - 01-15-2021

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

Table of Contents

Overview

This document, Security Configuration Benchmark for Cisco IOS, provides prescriptive guidance for establishing a secure configuration posture for Cisco Devices running Cisco NX-OS.
The Cisco NX-OS is a data center class operating system designed for maximum scalability and application availability. The CLI interface for the NX-OS is very similar to Cisco IOS, so if you understand the Cisco IOS you can easily adapt to the Cisco NX-OS.
To obtain the complete benchmark and or the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Cisco NX-OS.

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit https://workbench.cisecurity.org/.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
Monospace font	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

- **Level 2**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Author
Rob Vandenbrink

Contributor
Darren Freidel
Rob Vandenbrink

Recommendations

1 Management Plane

Services, settings and data streams related to setting up and examining the static configuration of the firewall, and the authentication and authorization of firewall administrators. Examples of management plane services include: administrative device access (telnet, ssh, http, and https), SNMP, and security protocols like RADIUS and TACACS+.

1.1 Local Authentication, Authorization and Accounting (AAA) Rules

Rules in the Local authentication, authorization and accounting (AAA) configuration class enforce device access control, provide a mechanism for tracking configuration changes, and enforcing security policy.

1.1.1 Configure AAA Authentication - TACACS (Automated)

Profile Applicability:

- Level 1
- Level 2

Description:

TACACS+ is an authentication protocol that Cisco NX-OS devices can use for authentication of management users against a remote AAA server. These management users can access the Cisco NX-OS device through any protocol and use this back-end authentication. Using a central authentication store (such as Active Directory) ensures that all administrative actions are tied to named users, making the tracking of changes much easier. It also makes tracking compromised accounts and malicious activities much easier.

Rationale:

Central authentication is key as it minimizes the effort in managing named user accounts. Keeping local admin accounts opens the door to all the issues inherent in shared accounts, namely:

- Errors in implementation being done by generic admin accounts, which can then be denied by all.
- Shared credentials staying unchanged when administrative staff leave the organization or change roles.
- Giving malicious actors the ability to recover shared credentials from saved device backups

In many organizations TACACS+ is preferred over RADIUS when TACACS+ is supported by the AAA server and network device. This is because (with additional work) TACACS+ also supports command authorization, restricting specific users to the command set that they can use on the device. However, TACACS+ started as a Cisco centric protocol, so is not as widely supported by other vendors in comparison to RADIUS.

In addition, RADIUS use is much more widespread (primarily for secure wireless authentication), so is often already in place.

Finally, command authorization is a complex endeavor and is very rarely implemented because of that, so the main advantage of TACACS+ is very often not realized.

Impact:

Implementing TACACS+ (or any central authentication solution) ensures that only named users are allowed to gain an administrative session to the device. This allows:

- Tracking of all changes to named users
- Simplification of reconciling changes to a change management process
- Off-loading password change cycles and password complexity requirements to that central authentication store
- Simplification of removing admin access as administrators leave the organization or change their roles in the organization

Audit:

"Show running-config tacacs+" will show the basic TACACS+ configuration.

- The tacacs+ feature should be enabled
- Two or more TACACS+ servers should be defined
- Two or more TACACS+ servers should be in the TACACS+ server group

```
switch(config)#sho run tacacs

!Command: show running-config tacacs+
!Running configuration last done at: Mon Apr 13 05:14:30 2020
!Time: Mon Apr 13 05:14:35 2020

version 9.3(3) Bios:version
feature tacacs+

tacacs-server host 3.4.5.6 key 7 "vkqjcet"
tacacs-server host 4.5.6.7 key 7 "vkqjgtcjjnod"
aaa group server tacacs+ TACACSGROUP
    server 3.4.5.6
    server 4.5.6.7
```

for more detail, use "show run tacacs all"

```
switch(config)# show run tacacs all

!Command: show running-config tacacs+ all
!Running configuration last done at: Mon Apr 13 05:15:05 2020
!Time: Mon Apr 13 05:15:38 2020

version 9.3(3) Bios:version
feature tacacs+

no ip tacacs source-interface
tacacs-server test username test password 7 wawy idle-time 0
tacacs-server timeout 5
tacacs-server deadtime 0
tacacs-server host 3.4.5.6 key 7 "vkqjcet" port 49
```

```
tacacs-server host 4.5.6.7 key 7 "vkqjgtcjjnod" port 49
tacacs-server host 3.4.5.6 test username test password 7 wawy idle-time 0
tacacs-server host 4.5.6.7 test username test password 7 wawy idle-time 0
aaa group server tacacs+ TACACSGROUP
    server 3.4.5.6
    server 4.5.6.7
    use-vrf default
    no source-interface
```

Finally, verify that the aaa authentication list includes TACACS for both the default and console access:

```
# show run aaa

!Command: show running-config aaa
!Running configuration last done at: Mon Apr 13 05:15:05 2020
!Time: Mon Apr 13 05:16:11 2020

version 9.3(3) Bios:version
aaa authentication login default group TACACSGROUP local
aaa authentication login console group TACACSGROUP local
no aaa user default-role
login on-success log
```

Remediation:

First, enable TACACS+ in NX-OS

```
switch(config)#feature tacacs+
```

Next, define two or more TACACS+ servers:

```
switch(config)#tacacs-server host 3.4.5.6 key somekey
switch(config)#tacacs-server host 4.5.6.7 key someotherkey
```

define the aaa group for TACACS+:

```
switch(config)#aaa group server tacacs+ TACACSGROUP
    server 3.4.5.6
    server 4.5.6.7
```

Finally, create the aaa authentication list for both console and default access:

```
switch(config)#aaa authentication login default group TACACSGROUP local
switch(config)#aaa authentication login console group TACACSGROUP local
```

It is common to include "local" as the last entry in the list, to allow access to administer the device even if the RADIUS server is offline. Note that while this ensures access in the case of the device or the RADIUS server being offline, it also means that if an attacker can DOS the RADIUS Servers, they can authenticate locally as well.

Default Value:

By default TACACS+ is not implemented

References:

1. https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/nxos/commands/fund/show-running-config.html

CIS Controls:

Version 7

16.2 Configure Centralized Point of Authentication

Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

1.1.2 Configure AAA Authentication - RADIUS (Automated)

Profile Applicability:

- Level 1
- Level 2

Description:

RADIUS is an authentication protocol that Cisco NX-OS devices can use for authentication of management users against a remote AAA server. These management users can access the Cisco NX-OS device through any protocol and use this back-end authentication. Using a central authentication store (such as Active Directory) ensures that all administrative actions are tied to named users, making the tracking of changes much easier. It also makes tracking compromised accounts and malicious activities much easier.

Rationale:

Central authentication is key as it minimizes the effort in managing named user accounts. Keeping local admin accounts opens the door to all the issues inherent in shared accounts, namely:

- Errors in implementation being done by generic admin accounts, which can then be denied by all.
- Shared credentials staying unchanged when administrative staff leave the organization or change roles.
- Giving malicious actors the ability to recover shared credentials from saved device backups

RADIUS is the most widely used protocol for this purpose, since it is a requirement for secure wireless authentication (EAP-TLS). Just as important, RADIUS is much better supported by most non-Cisco vendors for back-end authentication.

Impact:

Implementing RADIUS (or any central authentication solution) ensures that only named users are allowed to gain an administrative session to the device. This allows:

- Tracking of all changes to named users
- Simplification of reconciling changes to a change management process
- Off-loading password change cycles and password complexity requirements to that central authentication store

- Simplification of removing admin access as administrators leave the organization or change their roles in the organization

Audit:

"show running-config radius" will show all radius definitions.
Two or more RADIUS servers must be defined, as well as the RADIUS server group:

```
switch(config)# sho running-config radius

!Command: show running-config radius
!Running configuration last done at: Mon Apr 13 05:02:06 2020
!Time: Mon Apr 13 05:07:21 2020

version 9.3(3) Bios:version
radius-server host 3.4.5.6 key 7 "vkqjcet" authentication accounting
radius-server host 4.5.6.7 key 7 "vkqjgtcjjnod" authentication accounting
aaa group server radius RADIUSGROUP
    server 3.4.5.6
    server 4.5.6.7
```

"Show running-config radius all" will give more detail if required:

```
switch# show run radius all

!Command: show running-config radius all
!Running configuration last done at: Mon Apr 13 05:02:06 2020
!Time: Mon Apr 13 05:10:12 2020

version 9.3(3) Bios:version
radius-server test username test password 7 wawy idle-time 0
radius-server timeout 5
radius-server retransmit 1
radius-server deadtime 0
radius-server host 3.4.5.6 key 7 "vkqjcet" auth-port 1812 acct-port 1813
authent
ication accounting timeout 5 retransmit 1
radius-server host 4.5.6.7 key 7 "vkqjgtcjjnod" auth-port 1812 acct-port 1813
au
thentication accounting timeout 5 retransmit 1
radius-server host 3.4.5.6 test username test password 7 wawy idle-time 0
radius-server host 4.5.6.7 test username test password 7 wawy idle-time 0
aaa group server radius radius
    server 3.4.5.6
    server 4.5.6.7
    deadtime 0
    use-vrf default
    no source-interface
aaa group server radius RADIUSGROUP
    server 3.4.5.6
    server 4.5.6.7
    deadtime 0
    use-vrf default
    no source-interface
```

```
no ip radius source-interface
```

"Show running-config aaa" will display the authentication lists. RADIUS should appear first in the authentication list for both default and console access:

```
switch# sho run aaa

!Command: show running-config aaa
!Running configuration last done at: Mon Apr 13 05:02:06 2020
!Time: Mon Apr 13 05:08:25 2020

version 9.3(3) Bios:version
aaa authentication login default group RADIUSGROUP local
aaa authentication login console group RADIUSGROUP local
no aaa user default-role
login on-success log
```

Remediation:

First define two or more RADIUS Servers

```
switch(config)#radius-server host 3.4.5.6 key somekey authentication
accounting
switch(config)#radius-server host 4.5.6.7 key someotherkey authentication
accounting
```

Then create an AAA group for RADIUS

```
switch(config)# aaa group server radius RADIUSGROUP
    server 3.4.5.6
    server 4.5.6.7
```

Finally, create the authentication lists in the correct order - to be effective the RADIUS group needs to appear first in the list. Both the default and console access should be secured in the same way:

```
switch(config)# aaa authentication login default group RADIUSGROUP local
switch(config)# aaa authentication login console group RADIUSGROUP local
```

It is common to include "local" as the last entry in the list, to allow access to administer the device even if the RADIUS server is offline. Note that while this ensures access in the case of the device or the RADIUS server being offline, it also means that if an attacker can DOS the RADIUS Servers, they can authenticate locally as well.

Default Value:

By default RADIUS is not implemented

References:

1. https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/nxos/commands/fund/show-running-config.html

CIS Controls:

Version 7

16.2 Configure Centralized Point of Authentication

Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

1.1.3 Configure AAA Authentication - Local SSH keys (Manual)

Profile Applicability:

- Level 1

Description:

Using the client's public key to authenticate their SSH sessions circumvents the need for using passwords for an administrative login to the switch.

Rationale:

This is primarily an ease-of-use feature. It means that the administrators don't need to remember or key in passwords. It also can be used to significantly improve the security of any scripts or API calls that might use SSH.

Impact:

There are pros and cons to this approach.

Pro:

- Scripts and API calls that use SSH no longer need to have credentials embedded in them. While this can be done securely (using password vaults for instance), all to often the credentials are in clear-text, in the code or in an input file.
- This is popular with network administrators, as they no longer need to key in passwords, or "grab" their password from a password manager application.
- It means that administrators can no longer configure easy to guess passwords.

Con:

- The private half of the PKI exchange (client side) can be available if the administrator's workstation or account is compromised
- An inventory of SSH hosts that use key based authentication needs to be maintained if this approach is used. This is so that if a key needs to be replaced or deleted, the list of hosts that need to be updated is easily accessed. This can be time sensitive if an administrator has left the organization, or if a laptop is lost or stolen. Even if this is just due to regular hardware replacement or a policy that expires keys at regular intervals, missing a device can be a "time bomb" that is often not found until the worst possible moment

Normally the best recommendation is to use a back-end authentication source (such as AD), with RADIUS or TACACS+ as the authentication protocol. The back end directory can then enforce whatever complexity or password change requirements are needed. In

particular if an administrator leaves the organization or changes departments, those situations can be managed by changing AD Group membership or by disabling the account in question.

Audit:

To list the status of one user account:

```
switch# sho user-account rvadmin
user:rvadmin
        this user account has no expiry date
        roles:network-operator network-admin
        ssh public key: ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK
3OiW4H7YyUyuA50rv7gsEPjhOBYmsi6PAVKui1nIf/DQhum+lJNqJP/eLowb7ubO+lVKRXFY/G+lJ
NIQ
W3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH3UD/vKyziEh5S4Tplx8=
```

To list all users that have SSH key authentication:

```
switch# sho run | i sshkey
username rvadmin sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK
3OiW4H7YyUyuA50rv7gsEPjhOBYmsi6PAVKui1nIf/DQhum+lJNqJP/eLowb7ubO+lVKRXFY/G+lJ
NIQ
W3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH3UD/vKyziEh5S4Tplx8=
```

Remediation:

- Create the client's SSH public and private keys. The keys must be in OpenSSH format for the NX-OS switch to interpret them correctly. Use either RSA or DSA algorithms, and be sure to specify enough bits for entropy (2048 minimum, more is of course better)
- Upload the client's SSH public key, and store it on the bootflash of the switch.
- Be sure that the file has a meaningful name, often the users's initials and the key algorithm (RSA or DSA) is in the filename. This makes it easier to remove or replace that file as keys are expired out, workstations migrate or administrators leave the organization.
- To enable key-based authentication for one local user (for instance, Davey Jones), enter the command:

```
switch(config)# username djadmin sshkey file bootflash:dj_rsa.pub
```

Alternatively, the ssh key can be defined in the username configuration line:

```
switch(config)# username djadmin sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK3OiW4H7YyUyuA50rv7gsEPjhOBYms
i6PAVKui1nIf/DQhum+lJNqJP/eLowb7ubO+lVKRXFY/G+lJNIQW3g9igG30c6k6+XVn+NjnI1B7i
hvpVh7dLddMOXwOnXHYshXmSiH3UD/vKyziEh5S4Tplx8=
```

The file based method is usually preferred, as they keys can be changed without modifying the configuration of the switch. Also, the keys are not stored in any archived copy of the configuration.
Note that the username and file name will vary depending on your organization's policies, procedures and standards

Default Value:

SSH keys are not created or defined by default.

1.2 Access Rules

Rules in the access class enforce controls for device administrative connections.

1.2.1 Ensure Idle Timeout for Login Sessions is set to 5 minutes (Automated)

Profile Applicability:

- Level 1
- Level 2

Description:

Verify device is configured to automatically disconnect sessions after a fixed idle time.

Rationale:

This prevents unauthorized users from misusing abandoned sessions. For example, if the network administrator leaves for the day and leaves a computer open with an enabled login session accessible. There is a trade-off here between security (shorter timeouts) and usability (longer timeouts). Review your local policies and operational needs to determine the best timeout value. In most cases, this should be no more than 10 minutes.

Impact:

Not having a timeout on idle sessions has several impacts:

- Unattended sessions on an unlocked administrative workstation are susceptible to passers-by entering commands
- If multiple sessions are exited by closing the session rather than logging out, the virtual sessions will remain active forever. When the maximum number of sessions is reached, additional administrative sessions will be denied.
- If a console session is left open by simply disconnecting the console or USB cable, that session will remain available and logged in, in the state it was abandoned in for the next person who connects.

While a short timeout is typically desired, this can be changed temporarily during long-running operations (scheduled NX-OS updates for instance).

Audit:

Perform the following to determine if the timeout is configured.
This command will audit both the timeout for SSH sessions:

```
switch# sho run | i idle
ssh idle-timeout 120
```

This command will audit the timeout for console sessions:

```
switch# sho run | section console
line console
  exec-timeout 120
```

Remediation:

Configure ssh and console timeouts to 120 seconds (2 minutes) to disconnect sessions after a fixed idle time.

```
switch(config)# ssh idle-timeout 120

switch(config) line console
switch(config-line)# exec-timeout 120
```

Default Value:

The default value for "exec-timeout" is 0 (disabled) for both the vty and console lines

References:

1. https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/fundamentals/521n11/b_5k_Fund_Config_521N11/b_5k_Fund_Config_521N11_chapter_0110.html

CIS Controls:

Version 6

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

1.2.2 Restrict Access to VTY Sessions (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

Restrict Management Access to trusted management stations and VLANs.

Rationale:

Exposing the management interface too broadly exposes that interface to MiTM (Monkey in the Middle) attacks as well as to credential stuffing attacks. The question "should your receptionist have access to your core switch?" usually illustrates the need for this if there are any disagreements.

Impact:

Not restricting access to the management interface has several risks:

- exposes your interface to credential stuffing attacks from commodity malware (such as Mirai)
- highlights your device as missing simple security remediations to even simple scans. This invites other attacks in addition to credential stuffing.

Audit:

Perform the following to determine if the ACL is set:
Verify that you see an access-class defined:

```
switch# sho run | section vty
```

Next, display the access-list to verify that it is appropriate for your organization:

```
switch# sho run <Access-Class name>
```

Remediation:

Create an access-list that defines the various trusted subnets and/or stations:

```
switch(config)# ip access-list ACL-MGT
switch(config-acl)# remark access-class ACL
```

```
switch(config-acl)# permit ip 192.168.12.0/24 any
switch(config-acl)# deny ip any any log
```

It is suggested that all ACLs are commented to help self-document the configuration.
The last line in the ACL should read `deny ip any any log` to record all attempts to reach the management interface from unauthorized stations.
Apply the Access-Class to the VTY interface:

```
switch(config)# line vty
switch(config-line)# access-class ACL-MGT in
```

Default Value:

No access-class is applied by default

CIS Controls:

Version 7

11.6 Use Dedicated Machines For All Network Administrative Tasks

Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.

11.7 Manage Network Infrastructure Through a Dedicated Network

Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

1.3 Password Rules

Rules in the password class enforce secure, local device authentication credentials.

1.3.1 Enable Password Complexity Requirements for Local Credentials (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

While configuring a back-end authentication store is the recommended configuration, at least one local administrative account must be configured. For this reason, ensuring a minimum bar for password strength for all local administrative accounts is important. Enabling this setting enforces passwords that conform to the following rules:

- At least eight characters long
- Does not contain many consecutive characters (such as "abcd")
- Does not contain many repeating characters (such as "aaabbb")
- Does not contain dictionary words
- Does not contain proper names
- Contains both uppercase and lowercase characters
- Contains numbers

Rationale:

While in ideal conditions local credentials won't be used, there are many scenarios (such as deployed on a purely public network or on an air gapped network) where this is the only option. Even if a back-end authentication source is used, if that service is not available the fall-back authentication is often to local credentials.

Impact:

Having a simple password (for instance, based on a dictionary word) for administrative credentials makes that account susceptible to credential stuffing attacks. Even if using a back-end credential store such as TACACS+ or RADIUS, an attacker can drill down to the local credentials by taking the back-end service offline.

Audit:

A simple "show" command audits the state of this setting:

```
switch# show password strength-check
Password strength check is enabled
```

Remediation:

A single command enables this:

```
switch(config)# password strength-check
```

Default Value:

Password strength checking is enabled by default. When enabled, this setting does not appear in the configuration. When enabled, the password strength settings are:

- At least eight characters long
- Does not contain many consecutive characters (such as "abcd")
- Does not contain many repeating characters (such as "aaabbb")
- Does not contain dictionary words
- Does not contain proper names
- Contains both uppercase and lowercase characters
- Contains numbers

Additional Information:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_0/nx-os/security/configuration/guide/sec_nx-os_config/sec_rbac.html#wp1314939

CIS Controls:

Version 7

4.4 Use Unique Passwords

Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

1.3.2 Configure Password Encryption (Manual)

Profile Applicability:

- Level 2

Description:

You can enable strong, reversible 128-bit Advanced Encryption Standard (AES) password encryption, also known as type-6 encryption. To start using type-6 encryption, you must enable the AES password encryption feature and configure a master encryption key, which is used to encrypt and decrypt passwords. After you enable AES password encryption and configure a master key, all existing and newly created clear-text passwords for supported applications (currently RADIUS and TACACS+) are stored in type-6 encrypted format, unless you disable type-6 password encryption. You can also configure Cisco NX-OS to convert all existing weakly encrypted passwords to type-6 encrypted passwords.

Rationale:

Encryption is a good way to protect data that will be used later. Encrypted data can later be decrypted to its original value. Although encrypting passwords protects them, typically, an application uses the same encryption key for storing all user passwords.

Impact:

Encryption of passwords is used to protect it from being sent over the wire cleartext. By applying encryption you are making it more difficult for an adversary to gain access to your device/network

Audit:

```
switch(config)# show encryption service stat
```

Remediation:

Configure a master key to be used with the AES password encryption feature. The key can contain between 16 and 32 alphanumeric characters

```
switch# key config-key ascii
New Master Key:
Retype Master Key:

switch(config)# feature password encryption aes
```

References:

1. https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/security/configuration/guide/b_Cisco_Nexus_7000_NX-OS_Security_Configuration_Guide__Release_5-x/b_Cisco_Nexus_7000_NX-OS_Security_Configuration_Guide__Release_5-x_chapter_010101.html

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.3.3 Set password lifetime, warning time and grace time for local credentials (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

NX-OS has commands to adjust the permitted lifetime of passphrases for local credentials, as well as the "warning time" before expiry and the "grace time" after expiry. If local credentials are in use, it is recommended that these be set to a value appropriate to the organization. Note that these timers cannot be set for the "admin" credential.

Rationale:

Impact:

If local credentials are in regular use, it is recommended that a reasonable (non default) value be set for the passphrase timer values.
The default of an infinite lifetime is of course not appropriate. Previous guidance of password changes on 30 or 60 day cycles however is also not appropriate if complex passwords are used and enforced. Some middle ground should be set - for instance, a password change cycle on a 6 or 12 month rotation is often easy to track.

This entire discussion illustrates clearly why it is most often advisable to use a back-end authentication source for credential storage. In an organization that has multiple switches and other infrastructure, setting a password rotation is a recipe that has the risk of missing or entirely forgetting the change date, or of missing one or more devices in the change procedure. Since password recovery after the grace period involves a reboot of the entire switch, this end result is undesirable in the extreme.

The best recommendation is to set a long, complex password for any local administrative accounts, then use a back-end authentication source, so that these local accounts are only used in the event that the back-end authentication source is not reachable.

Audit:

To show the passphrase timers set per-user:

```
switch# sho username <local userid> passphrase timevalues
Last passphrase change(Y-M-D):  2020-04-30
Passphrase lifetime:            99999 days after last passphrase change
Passphrase warning time starts: 14 days before passphrase lifetime
Passphrase Gracetime ends:       3 days after passphrase lifetime
```

To show the global defaults for passphrase timers:

```
switch# show userpassphrase timevalues
passphrase default warningtime (in days): 10
passphrase default gracetime (in days): 10
passphrase default lifetime (in days): 180
```

To show both the global defaults as well as the settings for all local users:

```
switch# sho run | i passphrase
username asdf passphrase  lifetime 99999 warntime 14 gracetime 3
username test passphrase  lifetime 180 warntime 10 gracetime 10
userpassphrase default-warntime 10
userpassphrase default-gracetime 10
userpassphrase default-lifetime 180
```

Remediation:

To set passphrase timers globally:

```
switch(config)# userpassphrase default-warntime <days>
switch(config)# userpassphrase default-gracetime <days>
switch(config)# userpassphrase default-lifetime <days>
```

example:

```
switch(config)# userpassphrase default-warntime 10
switch(config)# userpassphrase default-gracetime 10
switch(config)# userpassphrase default-lifetime 180
```

To set passphrase time values per-user:

```
switch(config)# username <userid> passphrase lifetime <days> warntime <time
in days> gradetime <time in days>
```

example

```
switch(config)# username test passphrase lifetime 180 warntime 10 gracetime
10
```

Default Value:

By default, the passphrase time values per-user are:

- Lifetime: 99999 (this value indicates no expiry, or an infinite lifetime)
- Gracetime: 3 days
- Warntime: 14 days

By default, there are no global default values set, they are assigned per local user as the local accounts are created.

By default the "admin" account does not have any associated timers, and these values cannot be set for this account.

CIS Controls:

Version 7

4.4 Use Unique Passwords

Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

1.3.4 Set password length for local credentials (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

Password length should be set to some value that makes compromising any captured hashed difficult. This generally means that the maximum value of 127 should never be changed, and that the minimum value, which defaults to 8, should always be increased. Typical values for minimum passphrase length of administrative users are generally 20 characters or longer (values of 30 or 32 are often seen).
A specific value is not recommended, since then a savvy attacker may start their attack with "only passwords of the exact length recommended in the CIS benchmark", which would reduce their attack time.

Rationale:

Passwords are stored in a non-reversible, hashed and salted format. If an attacker should "harvest" a password hash, it is of course hashed in a non-reversible format - however, it can be decoded using dictionary and/or brute-force attacks using tools such as hashcat or John the Ripper (JtR). The single best obstacle to an attack of this type is password length - the longer the password the more difficult it is to decode.
Since the default password hash schema on the NX-OS version 9 platform is MD5, it's recommended that the password length be set to (and enforced at) some longer value, for instance 24, 32 or even longer values. This may seem lengthy, until you consider that with modern hardware running through the entire namespace of 8 or 9 characters is often easily done in less than an hour.

This discussion actually illustrates why the best recommendation is to not use local credentials at all, but rather to use a back-end authentication source (using RADIUS or TACACS+). In this scenario, local administrative accounts are only used if the back-end authentication source is unavailable. This makes any compromised local credentials much harder to use, a successful attack would have to also take back end authentication sources offline (or make them otherwise unavailable).

Impact:

Not setting a maximum value leaves administrators with the freedom to set short passwords. If a stored configuration file is collected by an attacker (perhaps from a file share), this means that any password hashes in the stored configuration will be more likely to be "cracked", giving the attacker the unencrypted credential to the target switch.

Audit:

The "show userpassphrase length" command will display the minimum and maximum password length values.

```
switch# sho userpassphrase length
Minimum passphrase length : 20
Maximum passphrase length : 127
```

Alternatively, the single resulting configuration command can be displayed:

```
switch# sho run | i min-length
userpassphrase min-length 20 max-length 127
```

Remediation:

Passphrase length values can only be set globally, not per-local user

```
switch(config)# userpassphrase min-length <minimum passphrase length>
switch(config)# userpassphrase max-length <maximum passphrase length>
```

or in a single command:
userpassphrase min-length max-length
example:

```
switch(config)# userpassphrase min-length 20
switch(config)# userpassphrase max-length 127
```

Or in a single command:

```
switch(config)# userpassphrase min-length 20 max-length 127
```

Default Value:

The default minimum passphrase length is 8. This has possible values between 8 and 127. The default maximum passphrase length is 127. This has possible values between 80 and 127.

CIS Controls:

Version 7

4.4 Use Unique Passwords

Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

1.4 SNMP Rules

Simple Network Management Protocol (SNMP) provides a standards-based interface to manage and monitor network devices. This section provides guidance on the secure configuration of SNMP parameters.

1.4.1 If SNMPv2 is in use, use a Complex Community String (Manual)

Profile Applicability:

- Level 1

Description:

SNMP v2 while similar to v1 aside from adding support for 64 bit counters and the ability to use complex strings.

Rationale:

Utilizing complex strings with SNMPv2 is no different then using complex passwords. By using the complex string you are making it more difficult for an attacker to guess the string. Strings should not contain dictionary words or rely on "l33t-speak" spelling. Keep in mind that SNMPv2 is a clear-text protocol, so is subject to interception. This means that these strings are passed in clear-text during SNMPv2 operations, so can be "harvested" by a well-positioned attacker. Also SNMP results are susceptible to capture or modification in transit.

Audit:

```
switch(config)# sho snmp community
Community             Group / Access      context    acl_filter
_________             ______________      _______    __________
<SomeComplexString>   network-operator
```

Remediation:

```
switch(config)# snmp-server community <SomeComplexString> ro
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.4.2 If SNMPv2 is in use, set Restrictions on Access (Manual)

Profile Applicability:

- Level 1

Description:

NX-OS allows administrators to restrict SNMPv2 access to known management stations, usually servers with an NMS (Network Management System) installed. It is recommended that only known NMS servers have access to SNMPv2 functions on network infrastructure. While SNMP is not enabled by default on the NX-OS platform, historically the SNMP strings of "public" (for read-only access) and "private" (for read-write access) have been used. These well-known values should never be configured.

Rationale:

Since SNMPv2 is a clear-text UDP protocol, this combination means that even this precaution still exposes this traffic to spoofing, eavesdropping and in-flight modification attacks. It also means that the switch can be used as a DDOS amplification host if the NMS server's IP address is known.

For all of these reasons, the best recommendation is in fact to disable SNMPv2 and use SNMPv3. Proceed with this recommendation only if you must use SNMPv2 for some reason.

Impact:

If SNMPv2 is configured, not restricting access to SNMPv2 allows an attacker to launch a dictionary and/or a brute force attack to compromise the SNMPv2 community string. This would then give the attacker the ability to collect key information from the target switch, including it's version, interface status and configuration parameters.

Audit:

The "show snmp community" command will show all configured community strings and their applied ACLs:

```
switch(config)# sho snmp community
Community             Group / Access      context    acl_filter
_________             ______________      _______    __________
somecomplexstring     network-operator              ACL mapped: ipv4:ACL-
IPV4-SNMPv2
```

To show the exact and complete configuration commands, use "show running-configuration snmp":

```
switch# show run snmp

!Command: show running-config snmp
!Running configuration last done at: Thu Apr 30 21:47:03 2020
!Time: Thu Apr 30 21:48:48 2020

version 9.3(3) Bios:version
snmp-server community somecomplexstring group network-operator
snmp-server community somecomplexstring use-ipv4acl ACL-IPV4-SNMPv2
```

Finally, to show the ACL, use the "show access-list" command:

```
switch# show access-lists ACL-IPV4-SNMPv2

IP access list ACL-IPV4-SNMPv2
        10 permit udp 1.2.3.4/32 3.4.5.6/32 eq snmp
        20 permit udp 1.2.3.8/2 3.4.5.6/32 eq snmp
        30 deny ip any any log
```

Remediation:

Create the ACL:

```
switch(config)# ip access-list ACL-IPV4-SNMPv2
switch(config-acl)# permit udp 1.2.3.4/2 1.2.3.6/32 eq 161
switch(config-acl)# deny ip any any log
```

Then apply the ACL to the configured SNMP Community. The snmp-server community must be configured before applying the ACL.

```
switch(config)# snmp-server community <somecomplexstring> ro
switch(config)# snmp-server community <somecomplexstring> use-ipv4acl ACL-
IPV4-SNMPV2
```

For IPv6, the parameter "use-ipv6acl" would be used instead. Note that either an IPv4 OR an IPv6 ACL can be applied to a given SNMP community string, not both.
In releases prior to Cisco NX-OS Release 7.0(3)I4(1), this CLI command includes use-acl rather than use-ipv4acl.

Default Value:

By default SNMP is not configured on NX-OS platforms.

CIS Controls:

Version 7

4.6 Use of Dedicated Machines For All Administrative Tasks
Ensure administrators use a dedicated machine for all administrative tasks or tasks

requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

11.6 Use Dedicated Machines For All Network Administrative Tasks

Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.

11.7 Manage Network Infrastructure Through a Dedicated Network

Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

1.4.3 Configure SNMPv3 (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network.

Rationale:

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

Impact:

SNMPv3 provides security features such as:

- ***Message Integrity*** - Ensures that a packet has not be tampered with
- ***Authentication*** - Determines message is from a valid source
- ***Encryption*** - Scrambles the packet content to prevent being seen by unauthorized sources.

SNMPv2 does not provide any of these features, as SNMPv2 is a cleartext protocol that exposes the community string in each exchange of information.

Audit:

To audit the SNMPv3 configuration, use the "show run snmp" command.
Ensure that:
Ensure that SNMP version 3 is set
switch# sho run snmp | i version

```
version 9.3(3) Bios:version
snmp-server host 1.2.3.4 traps version 3 priv <SNMPv3_UserName>
```

Ensure that SNMPv3 encryption is enforced globally for all users:

```
switch# sho run snmp | i global
snmp-server globalEnforcePriv
```

Ensure that SNMP Users have appropriate access levels:

```
switch# sho run snmp | i user
snmp-server user SNMPv3_UserName network-admin auth sha
0x12624c4dcb90cffeb43a1177324f547d priv 0x12624c4dcb90cffeb43a1177324f547d
localizedkey
```

SNMP version 2 is NOT set - "show run snmp | i community" should not return any statements (failed audit shown below)

```
switch# sho run snmp | i community
snmp-server community asdf group network-operator
snmp-server community <SomeComplexString> group network-operator
snmp-server community asdfasdfasf group network-operator
```

Remediation:

Create SNMPv3 Users (and groups if needed). Ensure that SHA hashes are used rather than MD5. Also ensure that appropriate authorization levels are set ("network-admin" is shown below):

```
switch(config)#snmp-server user SNMPv3_UserName network-admin auth sha
0x12624c4dcb90cffeb43a1177324f547d priv 0x12624c4dcb90cffeb43a1177324f547d
localizedkey
```

To set SNMP to version 3, add the "version" parameter to the snmp-server command (note that SNMPv3 users and groups need to be configured first):

```
switch(config)# snmp-server host 1.2.3.4 traps version 3 priv
<SNMPv3_UserName>
```

To enforce encryption for all SNMPv3 Users. This can be done by individual user, but it's recommended to enforce it globally:

```
switch(config)# snmp-server globalEnforcePriv
```

Default Value:

Not configured

References:

1. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-3se/3850/snmp-xe-3se-3850-book/nm-snmp-snmpv3.html

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

1.4.4 Configure SNMP Traps (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

SNMP relies on an architecture which consists of a manager and an agent. SNMP Managers can be any machine on the network that is running SNMP to collect and process information from the devices on either the LAN or WAN.

Rationale:

Utilizing traps can alert the user of issues or compromises in advance. For example if the device is overheating or if an admin users account is being utilized during odd hours.

Audit:

```
switch# sho snmp traps
```

Remediation:

Examples of traps
All notifications

```
switch(config)##switch(config)#snmp-server enable traps
```

CISCO-AAA-SERVER-MIB

```
switch(config)#switch(config)#snmp-server enable traps aaa
```

ENITY-MIB, CISCO-ENTITY-FRU-CONTROL-MIB, CISCO-ENTITY-SENSOR-MIB

```
switch(config)#switch(config)#snmp-server enable traps entity
switch(config)#switch(config)#snmp-server enable traps entity fru
```

CISCO-LICENSE-MGR-MIB

```
switch(config)#switch(config)#snmp-server enable traps license
```

IF-MIB

```
switch(config)#switch(config)#snmp-server enable traps link
switch(config)#CISCO-PSM-MIB
switch(config)#switch(config)#snmp-server enable traps port-security
switch(config)#snmpv2-MIB
switch(config)#switch(config)#snmp-server enable traps switch(config)#snmp
switch(config)#switch(config)#snmp-server enable traps switch(config)#snmp
authentication
```

CISCO-FCC-MIB

```
switch(config)##switch(config)#snmp-server enable traps fcc
```

CISCO-DM-MIB

```
switch(config)#snmp-server enable traps fcdomain
```

CISCO-NS-MIB

```
switch(config)#snmp-server enable traps fcns
```

CISCO-FCS-MIB

```
switch(config)#snmp-server enable traps fcs discovery-complete
switch(config)#snmp-server enable traps fcs request-reject
```

CISCO-FDMI-MIB

```
switch(config)#snmp-server enable traps fdmi
```

CISCO-FSPF-MIB

```
switch(config)#snmp-server enable traps fspf
```

CISCO-PSM-MIB

```
switch(config)#snmp-server enable traps port-security
```

CISCO-RSCN-MIB

```
switch(config)#snmp-server enable traps rscn
switch(config)#snmp-server enable traps rscn els
switch(config)#snmp-server enable traps rscn ils
```

CISCO-ZS-MIB

```
switch(config)#snmp-server enable traps zone
switch(config)#snmp-server enable traps zone default-zone-behavior-change
switch(config)#snmp-server enable traps zone merge-failure
switch(config)#snmp-server enable traps zone merge-success
```

```
switch(config)#snmp-server enable traps zone request-reject
switch(config)#snmp-server enable traps zone unsupp-mem
```

Default Value:

Not configured

References:

1. https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/sm_snmp.html

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.4.5 Configure SNMP Source Interface for Traps (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

The administrator can configure SNMP to the interfaces source IP address for notifications

Rationale:

By using a source interface the administrator can ensure that the source IP of SNMP traps does not change as the network topology changes. For instance, if a link fails or is reconfigured, and a different IP address is now topologically "closer" to the SNMP trap server. There are a few typical candidates for an SNMP source IP address:

- A loopback address, as loopbacks are always up, and can then route over any transit interface.
- The MGMT 0 address, as that provides an out-of-band path to the SNMP server. SNMP traffic volume will not affect traffic volumes, and SNMP cannot be "starved" for bandwidth by production traffic. If the entire path is out-of-band, this also provides excellent protection from eavesdropping by malicious actors that may be on the "production data side" of the switch.
- A combination of the two (this is less common) - for instance a loopback address in the management VRF

Audit:

There are two typical commands to show the snmp source-interface configuration.
The first shows only the explicit definitions for traps and informs:

```
switch# sho snmp source-interface
----------------------------------------------------------------------
Notification                    source-interface
----------------------------------------------------------------------
trap                           mgmt0
inform                         mgmt0
----------------------------------------------------------------------
```

or, more completely, use the "show running-config snmp" command, and filter for the keyword "source":

```
switch# sho run snmp | i source
snmp-server source-interface traps mgmt0
snmp-server source-interface informs mgmt0
snmp-server host 1.2.3.4 source-interface loopback0
```

Remediation:

```
switch(config)# snmp-server host 1.2.3.4 source-interface mgmt 0
```

or

```
switch(config)# snmp-server host 1.2.3.4 source-interface loopback 0
```

SNMP Server traps or informs:

```
switch(config)# snmp-server source-interface traps loopback 0
switch(config)# snmp-server source-interface informs loopback 0
```

or

```
switch(config)# snmp-server source-interface traps mgmt 0
switch(config)# snmp-server source-interface informs mgmt 0
```

Default Value:

Not configured. By default SNMP traffic is sourced from the layer 3 interface that is topologically closest to the configured SNMP server

References:

1. https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/6-x/system_management/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_System_Management_Configuration_Guide/sm_9snmp.html#task_01A48123BA9B420A94E5780F5EF74C6E

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.4.6 Do not Configure a Read Write SNMP Community String (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

SNMP RW (Read-Write) access allows stations with Management access to both read and write SNMP MIB objects.

Rationale:

SNMP is typically used for monitoring specific operational characteristics of the switch. These tasks typically only require read access. Permitting RW (Read-Write) access permits SNMP to modify some SNMP values.

Impact:

Permitting SNMP RW Access not only allows "write" access to some SNMP MIB Objects, which allows a malicious attacker to modify some operational characterstics of the switch. By extension this access allows a malicious actor to collect the entire configuration of the device.

Audit:

The command "show run snmp | i community" will list all community strings, and which SNMP Groups each is in. The "show snmp groups" shows all SNMP groups, and what access they have. Ensure that only groups with RO access are used in any SNMPv2 deployment. The group "network-operator" is the most commonly seen read-only group.

```
switch# sho run snmp | i community
snmp-server community <SomeComplexString> group network-operator
```

This listing shows the SNMP groups on the switch by default:

```
CISNXOS9# sho snmp group

Role: aaa-db-admin
  Description: Predefined AAA DB admin, has no cli permissions. Allows
RESTful A
PI
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
```

```
  ------------------------------------------------------------------
  1       permit  read-write

Role: aaa-db-operator
  Description: Predefined AAA DB operator, has no cli permissions. Allows
RESTfu
l API
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read

Role: l3-db-admin
  Description: Predefined L3 DB admin, has no cli permissions. Allows RESTful
AP
I
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read-write

Role: l3-db-operator
  Description: Predefined L3 DB operator, has no cli permissions. Allows
RESTful
 API
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read

Role: network-admin
  Description: Predefined network admin role has access to all commands
  on the switch
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read-write

Role: network-operator
  Description: Predefined network operator role has access to all read
  commands on the switch
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read

Role: nxdb-admin
  Description: Predefined nxdb-admin role has no cli permissions.
  Allows json-rpc get and set.
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       deny    command

Role: nxdb-operator
  Description: Predefined nxdb-operator role has no cli permissions.
  Allows json-rpc get.
```

```
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       deny    command

Role: vdc-admin
  Description: Predefined vdc admin role has access to all commands within
  a VDC instance
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read-write

Role: vdc-operator
  Description: Predefined vdc operator role has access to all read commands
  within a VDC instance
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read

Role: dev-ops
  Description: Predefined system role for devops access. This role
  cannot be modified.
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  6       permit  command                         conf t ; username *
  5       permit  command                         attach module *
  4       permit  command                         slot *
  3       permit  command                         bcm module *
  2       permit  command                         run bash *
  1       permit  command                         python *

Role: priv-15
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read-write

Role: priv-14
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read-write

Role: priv-13
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
```

```
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-12
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-11
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-10
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-9
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-8
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-7
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-6
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-5
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-4
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
```

```
Role: priv-3
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-2
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-1
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-0
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ----------------------------------------------------------------------
  10      permit  command                         traceroute6 *
  9       permit  command                         traceroute *
  8       permit  command                         telnet6 *
  7       permit  command                         telnet *
  6       permit  command                         ping6 *
  5       permit  command                         ping *
  4       permit  command                         ssh6 *
  3       permit  command                         ssh *
  2       permit  command                         enable *
  1       permit  read
```

Remediation:

Only use RO groups for SNMPv2. The most common implementation is "network-operator", because if you use the legacy syntax:

```
switch(config)# snmp-server community <some complex string> ro
```

the switch will translate this to the new syntax, using "network-operator" group

```
switch(config)# snmp-server community <some complex string> group network-
operator
```

Default Value:

SNMP is not configured by default. The default SNMP Groups and permissions are:

```
switch# sho snmp group



Role: aaa-db-admin

  Description: Predefined AAA DB admin, has no cli permissions. Allows
RESTful A

PI

  ----------------------------------------------------------------

  Rule    Perm    Type        Scope               Entity

  ----------------------------------------------------------------

  1       permit  read-write



Role: aaa-db-operator

  Description: Predefined AAA DB operator, has no cli permissions. Allows
RESTfu

l API

  ----------------------------------------------------------------

  Rule    Perm    Type        Scope               Entity

  ----------------------------------------------------------------

  1       permit  read



Role: l3-db-admin

  Description: Predefined L3 DB admin, has no cli permissions. Allows RESTful
AP

I

  ----------------------------------------------------------------

  Rule    Perm    Type        Scope               Entity

  ----------------------------------------------------------------

  1       permit  read-write
```

```
Role: l3-db-operator

  Description: Predefined L3 DB operator, has no cli permissions. Allows
RESTful

 API

  ------------------------------------------------------------------

  Rule    Perm    Type        Scope               Entity

  ------------------------------------------------------------------

  1       permit  read


Role: network-admin

  Description: Predefined network admin role has access to all commands

  on the switch

  ------------------------------------------------------------------

  Rule    Perm    Type        Scope               Entity

  ------------------------------------------------------------------

  1       permit  read-write


Role: network-operator

  Description: Predefined network operator role has access to all read

  commands on the switch

  ------------------------------------------------------------------

  Rule    Perm    Type        Scope               Entity

  ------------------------------------------------------------------

  1       permit  read


Role: nxdb-admin

  Description: Predefined nxdb-admin role has no cli permissions.

  Allows json-rpc get and set.
```

```
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       deny    command

Role: nxdb-operator
  Description: Predefined nxdb-operator role has no cli permissions.
  Allows json-rpc get.
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       deny    command

Role: vdc-admin
  Description: Predefined vdc admin role has access to all commands within
  a VDC instance
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read-write

Role: vdc-operator
  Description: Predefined vdc operator role has access to all read commands
  within a VDC instance
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read
```

```
Role: dev-ops
  Description: Predefined system role for devops access. This role
  cannot be modified.
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  6       permit  command                         conf t ; username *
  5       permit  command                         attach module *
  4       permit  command                         slot *
  3       permit  command                         bcm module *
  2       permit  command                         run bash *
  1       permit  command                         python *

Role: priv-15
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read-write

Role: priv-14
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
```

```
  Vrf policy: permit (default)
  --------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  --------------------------------------------------------------------
  1       permit  read-write


Role: priv-13
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)


Role: priv-12
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)


Role: priv-11
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)


Role: priv-10
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
```

```
  Vrf policy: permit (default)


Role: priv-9
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)


Role: priv-8
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)


Role: priv-7
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)


Role: priv-6
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)


Role: priv-5
  Description: This is a system defined privilege role.
```

```
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-4
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-3
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-2
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-1
  Description: This is a system defined privilege role.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
```

```
Role: priv-0

  Description: This is a system defined privilege role.

  Vlan policy: permit (default)

  Interface policy: permit (default)

  Vrf policy: permit (default)

  ------------------------------------------------------------------

  Rule    Perm    Type        Scope               Entity

  ------------------------------------------------------------------

  10      permit  command                         traceroute6 *

  9       permit  command                         traceroute *

  8       permit  command                         telnet6 *

  7       permit  command                         telnet *

  6       permit  command                         ping6 *

  5       permit  command                         ping *

  4       permit  command                         ssh6 *

  3       permit  command                         ssh *

  2       permit  command                         enable *

  1       permit  read
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

1.5 Logging

1.5.1 Ensure Syslog Logging is configured (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

Logging should be configured such that: Logging level is set to a level sufficient for the target device Logs should be sent off the device to a syslog or trap server or servers Logs should be sourced from a consistent interface to ensure easy attribution of logs to the correct device Logging levels should be explicitly set to a level appropriate to the device.

Rationale:

Logging on any network device is always limited by how much storage can be set aside for logs. It's important for this reason to send all log entries to a central device that can collect and correlate all logs, either in a database or in flat text files. The key thing this approach contributes is central logs on a larger storage device (disk) Logging to an off-device target also makes clearing any incriminating logs more difficult for an attacker, or if an attempt is made to hide a mistake.
Logging off-device also ensures that any clearing of logs is also seen and can be alerted on. Sourcing all logs from a consistent interface ensures that log entries can be easily attributed to the correct device once they arrive at the log server. If a logging interface is not set, the source IP address of individual log entries can change as the network topology changes. This situation can make any subsequent log analysis more difficult.

Impact:

Because syslog traffic is not encrypted, it's recommended to ensure that the path the log traffic takes is not susceptible to any MiTM (Monkey in the Middle) attacks. Often this means assigning a dedicated management interface, which by default is in a separate VRF.

Audit:

To show the current logging server:

```
switch# sho logging server
Logging server:                 enabled
{1.2.3.4}
        server severity:        notifications
        server facility:        local7
```

```
        server VRF:             default
        server port:            514
```

To show the logging source interface:

```
CISNXOS9# sho logging source-interface
Logging source-interface :      enabled (Interface: mgmt0)
```

To show the logging level:

```
CISNXOS9# sho logging level

Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
aaa                     3                       3
acllog                  2                       2
aclmgr                  3                       3
aclqos                  5                       5
adbm                    2                       2
arp                     3                       3
auth                    0                       0
authpriv                3                       3
bootvar                 5                       5
callhome                2                       2
capability              2                       2
cdp                     2                       2
cert_enroll             2                       2
cfs                     3                       3
clis                    3                       3
clk_mgr                 2                       2
confcheck               2                       2
copp                    2                       2
cron                    3                       3
daemon                  3                       3
device_test             3                       3
dhclient                2                       2
dhcp_snoop              2                       2
diag_port_lb            2                       2
diagclient              2                       2
diagmgr                 2                       2
ecp                     5                       5
eltm                    2                       2
eth_port_channel        5                       5
ethpm                   5                       5
evmc                    5                       5
evms                    2                       2
feature-mgr             2                       2
fs-daemon               2                       2
ftp                     3                       3
ifmgr                   5                       5
igmp_1                  5                       5
interface-vlan          2                       2
ip                      3                       3
ipfib                   2                       2
ipqosmgr                4                       4
```

```
ipv6                    3                    3
kern                    3                    3
l2fm                    2                    2
l2pt                    3                    3
l3vm                    5                    5
lacp                    2                    2
licmgr                  6                    6
lldp                    2                    2
local0                  3                    3
local1                  3                    3
local2                  3                    3
local3                  3                    3
local4                  3                    3
local5                  3                    3
local6                  3                    3
local7                  3                    3
lpr                     3                    3
m2rib                   2                    2
m6rib                   5                    5
mail                    3                    3
mcm                     2                    2
mfdm                    2                    2
mmode                   2                    2
module                  5                    5
monitor                 3                    3
mrib                    5                    5
mvsh                    2                    2
news                    3                    3
ntp                     2                    2
otm                     3                    3
pfstat                  2                    2
pixm_gl                 4                    4
pixm_vl                 4                    4
platform                5                    5
plcmgr                  2                    2
plugin                  2                    2
port-profile            2                    2
radius                  3                    3
res_mgr                 5                    5
rpm                     5                    5
sal                     2                    2
scheduler               5                    5
securityd               3                    3
sflow                   2                    2
sksd                    3                    3
smm                     4                    4
snmpd                   2                    2
span                    3                    3
spm                     2                    2
stp                     3                    3
syslog                  3                    3
sysmgr                  3                    3
tamnw                   2                    2
telemetry               3                    3
template_manager        2                    2
u6rib                   5                    5
ufdm                    3                    3
```

```
urib                    5                       5
user                    3                       3
uucp                    3                       3
vdc_mgr                 6                       6
virtual-service         5                       5
vlan_mgr                2                       2
vshd                    5                       5
xbar                    5                       5
xmlma                   3                       3

0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
```

Remediation:

Configure a logging level and a syslog host:

```
switch(config)#logging server <server ip address or name>
switch(config)#logging level <service name> <logging level>
```

or

```
switch(config)#logging level all <logging level>
switch(config)#logging source-interface <interface name>
switch(config)#logging server <server ip address or name>
```

optionally:

```
switch(config)#logging server <server ip address or name>  vrf [management
vrf name]
switch(config)#logging source-interface <mgmt 0 or other dedicated management
interface>
```

Default Value:

By default syslog logging is not configured.

By default the source interface of all logs will be the interface in the "default" vrf that is topologically closest to the logging host, if defined.

By default, the logging levels (by service or feature) are shown below:

```
switch# sho logging level


Facility        Default Severity        Current Session Severity

--------        ----------------        ------------------------

aaa                     3                       3
```

acllog	2	2
aclmgr	3	3
aclqos	5	5
adbm	2	2
arp	3	3
auth	0	0
authpriv	3	3
bootvar	5	5
callhome	2	2
capability	2	2
cdp	2	2
cert_enroll	2	2
cfs	3	3
clis	3	3
clk_mgr	2	2
confcheck	2	2
copp	2	2
cron	3	3
daemon	3	3
device_test	3	3
dhclient	2	2
dhcp_snoop	2	2
diag_port_lb	2	2
diagclient	2	2
diagmgr	2	2
ecp	5	5
eltm	2	2
eth_port_channel	5	5

ethpm	5	5
evmc	5	5
evms	2	2
feature-mgr	2	2
fs-daemon	2	2
ftp	3	3
ifmgr	5	5
igmp_1	5	5
interface-vlan	2	2
ip	3	3
ipfib	2	2
ipqosmgr	4	4
ipv6	3	3
kern	3	3
l2fm	2	2
l2pt	3	3
l3vm	5	5
lacp	2	2
licmgr	6	6
lldp	2	2
local0	3	3
local1	3	3
local2	3	3
local3	3	3
local4	3	3
local5	3	3
local6	3	3
local7	3	3

lpr	3	3
m2rib	2	2
m6rib	5	5
mail	3	3
mcm	2	2
mfdm	2	2
mmode	2	2
module	5	5
monitor	3	3
mrib	5	5
mvsh	2	2
news	3	3
ntp	2	2
otm	3	3
pfstat	2	2
pixm_gl	4	4
pixm_vl	4	4
platform	5	5
plcmgr	2	2
plugin	2	2
port-profile	2	2
radius	3	3
res_mgr	5	5
rpm	5	5
sal	2	2
scheduler	5	5
securityd	3	3
sflow	2	2

```
sksd                    3                       3
smm                     4                       4
snmpd                   2                       2
span                    3                       3
spm                     2                       2
stp                     3                       3
syslog                  3                       3
sysmgr                  3                       3
tamnw                   2                       2
telemetry               3                       3
template_manager        2                       2
u6rib                   5                       5
ufdm                    3                       3
urib                    5                       5
user                    3                       3
uucp                    3                       3
vdc_mgr                 6                       6
virtual-service         5                       5
vlan_mgr                2                       2
vshd                    5                       5
xbar                    5                       5
xmlma                   3                       3


0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
```

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

1.5.2 Log all Successful and Failed Administrative Logins (Automated)

Profile Applicability:

- Level 1
- Level 2

Description:

By default failed logins are logged, but successful logins are not logged. This makes any configuration changes or successful malicious activity difficult to correctly attribute.

Rationale:

Logging of all device login attempts allows the security team to investigate all login attempts and successful logins as needed. In some organizations and for some switches, even successful logins will be configured to generate an alert that must be compared against authorized changes or assigned tickets. Without logging both successful and failed logins, several important components of any investigation may not be easily available for any subsequent investigation or analysis (userids, source IP addresses, login times and so on).

Impact:

Not logging successful logins means that unauthorized changes will be more difficult to attribute to the right person. It also means that otherwise suspicious logins (either because of the time of login, the source IP or other indicator) are not logged for further investigation. Logging successful logins means that any configuration errors that result in a service outage can also be attributed. Not logging unsuccessful logins means that brute force login attempts are not logged.

Audit:

```
switch# sho login on-failure log
aaa authentication login on-failure log is enabled

switch# show login on-successful log
aaa authentication login on-successful log is enabled
```

Note that login on-failure is set by default, so searching by command will not display all audit information:

```
switch# sho run | i "login on"
login on-success log
```

Remediation:

```
switch(config)# login on-failure log  ! set correctly by default
switch(config)# login on-success log
```

Note that login on-failure is set by default, so will not show in the configuration if properly set.

Default Value:

By default failed logins are logged and successful logins are not logged.

CIS Controls:

Version 7

4.9 Log and Alert on Unsuccessful Administrative Account Login

Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.

16.12 Monitor Attempts to Access Deactivated Accounts

Monitor attempts to access deactivated accounts through audit logging.

1.5.3 Configure Netflow on Strategic Ports (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

Netflow allows for detailed logging of transit traffic. For a Layer 3 Netflow configuration, this outlines several values identified as "keys": source and destination ports and protocols, source and destination IP addresses as well as traffic volumes in any combination. Sometimes QOS values (TOS bits only) is also used as a key. Each combination of Protocol, source port, destination port, source IP, destination IP is called a "tuple". The possible keys in a Layer 2 Tuple include source mac address, destination mac address, ethertype and vlan.

In most cases logging to this level is not recommended for all ports of an NX-OS device, with 10G or faster ports there is just too much data to log and process in a meaningful way, even with sampling (which is required).

However, for strategic ports (for instance, something facing a WAN link or traffic constrained server) this can be a good tool for troubleshooting. This sort of logging does take a fair amount of host resources, so if there is an upstream firewall or router, that device is often better suited to be a Netflow initiator, but if for instance the upstream device is owned by a carrier or a client, or is a host that needs this sort of telemetry, most NX-OS devices are certainly capable of providing Netflow telemetry.

On many NX-OS platforms only inbound Netflow is supported.

Rationale:

Impact:

If monitored graphically, often just a visual inspection of the netflow graphs will highlight anomalous traffic. For instance, a high volume exfiltration from a database server would show a spike of traffic from that database server to a host on the internet (which in most environments is not a normal pattern).

In many cases the netflow database can be queried directly, so anomalies can be queried for programmatically. However, coding "what is not normal" is not something that is easily

done in procedural languages. AI or ML frameworks such as TensorFlow may be helpful in this situation.

Audit:

To display the complete netflow configuration, use "show running-configuration netflow".
Ensure that valid values in the flow exporter, flow record, sampler and flow monitor sections.
Ensure that the flow monitor is applied to the correct interface (Layer 2 or Layer 3).
A Layer 3 example is shown:

```
switch# show run netflow
!Command: show running-config netflow
!Time: Mon Jan  4 13:48:45 2021

version 7.3(1)N1(1)
feature netflow

flow exporter FLOW-EXPORT
  destination 10.10.10.10
  transport udp 9996
  source mgmt0
  version 9
    option exporter-stats timeout 120
    option interface-table timeout 120
flow record FLOW-RECORD
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  collect routing source as
  collect routing destination as
  collect transport tcp flags
  collect counter bytes
  collect counter packets
sampler FLOWSAMPLER01
  mode 8 out-of 64
flow monitor FLOW-MONITOR
  record FLOW-RECORD
  exporter FLOW-EXPORT


interface Vlan9
  ip flow monitor FLOW-MONITOR input sampler FLOWSAMPLER01
```

To just show the existence of a the netflow sections in the configuration (the last line shows that it is applied to an interface, but not which interface):

```
switch# sho run netflow | i flow
feature netflow
flow exporter FLOW-EXPORT
flow record FLOW-RECORD
```

```
flow monitor FLOW-MONITOR
  ip flow monitor FLOW-MONITOR input sampler FLOWSAMPLER01
```

Remediation:

If needed, either Layer 3 or Layer 2 netflow can be configured.
Layer 3 IP and IPv6 flow monitors can be applied to VLANs, SVIs, Layer 3 routed interfaces or subinterfaces.
Layer 2 flow monitors can be applied to a physical interface or trunks
L3 netflow - typical application to a VLAN is shown
First, enable the netflow feature:

```
switch(config)#feature netflow
```

The flow record defines what data to record and export. Typical settings are shown, the important thing is that a valid flow record setting exists:

```
switch(config)# flow-record FLOW-RECORD
switch(config-flow-record)#  match ipv4 protocol
switch(config-flow-record)#  match ipv4 source address
switch(config-flow-record)#  match ipv4 destination address
switch(config-flow-record)#  match transport source-port
switch(config-flow-record)#  match transport destination-port
switch(config-flow-record)#  collect routing source as
switch(config-flow-record)#  collect routing destination as
switch(config-flow-record)#  collect transport tcp flags
switch(config-flow-record)#  collect counter bytes
switch(config-flow-record)#  collect counter packets
```

The flow exporter defines the destination and options around sent data. Again, the specific values are not important. The VRF can be specified in the "destination" line if needed.:

```
switch(config)# flow exporter FLOW-EXPORT
switch(config-flow-exporter)# transport udp 9996
switch(config-flow-exporter)# destination 10.10.10.10
switch(config-flow-exporter)# source mgmt 0
switch(config-flow-exporter)# version 9
switch(config-flow-exporter-version-9)# option exporter-stats timeout 120
switch(config-flow-exporter-version-9)# option interface-table timeout 120
```

The flow monitor "ties" the exporter and record together:

```
switch(config)# flow monitor FLOW-MONITOR
switch(config-flow-monitor)# exporter FLOW-EXPORT
switch(config-flow-monitor)#  record FLOW-RECORD
```

The sampling rate, "x packets out of y" can also be defined. Both should be a power of 2 (for instance, 8 out-of 64 is a valid combination)

```
switch(config)#sampler FLOWSAMPLER01
switch(config-flow-sampler)# mode 8 out-of 64
```

Finally, apply the monitor and optionally the sampler to a layer 3 interface:

```
switch(config-flow-monitor)# int vlan <interface number>
10GCORE01(config-if)# ip flow monitor FLOW-MONITOR input sampler
FLOWSAMPLER01
```

==========

**L2 netflow - typical application to physical interface shown **

Because if it's reliance on MAC Addresses, L2 netflow implementations are much less often used

```
switch(config)#feature netflow
```

The exporter configuration remains the same as L3:

```
switch(config)# flow exporter L2_FLOWEXPORTER01
switch(config-flow-exporter)# destination <netflow server ip> [use-vrf
management]
switch(config-flow-exporter)# transport udp <netflow port>
switch(config-flow-exporter)# source mgmt0
switch(config-flow-exporter)# version 9
```

The flow record reflects different (layer 2) tuple inputs:

```
switch(config)# flow record L2_FLOWRECORD01
switch(config-flow-record)#  match datalink ethertype
switch(config-flow-record)#  match datalink mac source-address
switch(config-flow-record)#  match datalink mac destination-address
switch(config-flow-record)#  match datalink vlan
```

The flow monitor remains similar:

```
switch(config)# flow monitor L2_FLOWMONITOR01
switch(config-flow-monitor)# record L2_FLOWRECORD01
switch(config-flow-monitor)# exporter L2_FLOWEXPORTER01
```

The flow sampler commands remain the same

```
switch(config)#sampler FLOWSAMPLER01
switch(config-flow-sampler)# mode <x> out-of <y>
```

Finally, apply the L2 definition to an L2 interface:

```
switch(config)# int Ethernet x/yy
switch(config-if)# layer2-switched flow monitor L2_FLOWMONITOR01 input
sampler FLOWSAMPLER01
```

Default Value:

Netflow is not defined by default.

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

1.5.4 Configure Logging Timestamps (Manual)

Profile Applicability:

- Level 1

Description:

Timestamps are incredibly important since they drive a number of important activities in our product. Most importantly, we use timestamps to filter data in your search results.

Rationale:

Using timestamps allow you to discover the timeframe of an incident.

Audit:

Using "show logging timestamp" is the reliable command to show this configuration setting, as it will show the default value of "seconds", which will not appear in the configuration:

```
switch# sho logging timestamp
Logging timestamp:              Seconds
```

Remediation:

Use the "logging timestampe" command to configure this setting. Note that if set to "seconds" (the default), this command will not appear in the configuration.

```
switch(config)# logging timestamp {microseconds | milliseconds | seconds}
```

Default Value:

By default logs are timestamped to the second, so the default value is "logging timestamp seconds".
This default value is not shown in the configuration.

CIS Controls:

Version 7

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

1.6 Time Services

1.6.1 Configure at least 3 external NTP Servers (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

Accurate time is a critical piece of security infrastructure. Without accurate time on all infrastructure, it is complex or even impossible to correlate events from multiple sources to get an accurate view of a security incident or technical issue. Using multiple sources gives redundancy in time sources. In most infrastructures, for efficiency only a small subset of devices (often a redundant pair of routers or switches) will use redundant external time sources. All other infrastructure will then synchronize time from them. This also means that any perimeter firewalls can be configured to limit NTP requests to the public internet to just those sources and destinations. The exception would of course be if the organization has an on-premise, internal atomic or GPS based network time source. Even in those situations an tiered NTP infrastructure is generally recommended on the internal network.

Rationale:

Accurate time is a critical piece of security infrastructure. Without accurate time on all infrastructure, it is complex or even impossible to correlate events from multiple sources to get an accurate view of a security incident or technical issue. Also, without accurate time authentication issues can arise. If an attacker can influence the NTP traffic, it is possible to "back-date" NTP responses to permit the use of older certificates, or "forward-date" NTP responses to invalidate any certificates in use on the device. Using multiple sources gives redundancy in time sources. If a management network is in use in the infrastructure, using the management VRF to source time can help to protect NTP response traffic from tampering. It is key to set an NTP source interface, so that any perimeter devices can be configured to permit NTP requests from those IP addresses, and to restrict NTP requests to a list of authorized IP addresses. Be sure that this is a "reliable" interface. In many cases this means using a loopback interface, so that any of several interfaces can be used to route the request to the NTP server. If a non-loopback interface is used, understand that if that interface is in a down state then NTP requests will not be sent.

Impact:

Accurate time is a critical piece of security infrastructure. Without accurate time on all infrastructure, it is complex or even impossible to correlate events from multiple sources to get an accurate view of a security incident or technical issue.

Audit:

The "show running-config ntp" command will list all configured NTP servers. Note that the IP addresses are for demonstrations purposes only, production configurations will likely vary.

```
switch(config)# sho run ntp

!Command: show running-config ntp !Running configuration last done at: Sat
Apr 25 10:40:55 2020 !Time: Sat Apr 25 10:41:01 2020

version 9.3(3) Bios:version ntp server 13.86.101.172 use-vrf management ntp
server 132.163.97.6 use-vrf management ntp server 132.246.11.231 use-vrf
management ntp source-interface loopback1

NTP default commands which are not explicitly configured can be displayed by
using the "show running-config ntp all" command.

switch(config)# sho running-config ntp all

!Command: show running-config ntp all !Running configuration last done at:
Sat Apr 25 11:31:43 2020 !Time: Sat Apr 25 11:33:44 2020

version 9.3(3) Bios:version ntp server 13.86.101.172 use-vrf management ntp
server 132.163.97.6 use-vrf management ntp server 132.246.11.231 use-vrf
management ntp source-interface loopback1 feature ntp no ntp allow private no
ntp allow control no ntp passive clock format 24-hours
```

Remediation:

If the default VRF is used (note that the IP addresses are for demonstrations purposes only, production configurations will likely vary):

```
switch(config)#ntp server 13.86.101.172 use-vrf default
switch(config)#ntp server 132.163.97.6 use-vrf default
switch(config)#ntp server 132.246.11.231 use-vrf default
switch(config)#ntp source-interface loopback1
```

If a management VRF is used:

```
switch(config)#ntp server 13.86.101.172 use-vrf management
switch(config)#ntp server 132.163.97.6 use-vrf management
switch(config)#ntp server 132.246.11.231 use-vrf management
switch(config)#ntp source-interface loopback1
```

Default Value:

NTP settings are not in the default confguration, they must be added. If a source VRF is not specified, the default VRF is used If a source interface is not specified, the interface that is topologically closest to the NTP service is used.

CIS Controls:

Version 7

6.1 Utilize Three Synchronized Time Sources

Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

1.6.2 Configure a Time Zone (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

Timezones are a source of contention in larger corporations. On one hand, if infrastructure is configured with time consistent with the local timezone, then it is simpler to co-relate end-user symptoms and logs on end-user equipment with logs from network equipment. On the other hand, in organizations that span multiple time zones, configuring local time can make it easy to mis-match log entries from gear in different time zones.

In some organizations, the solution is to post both local and UTC time in all log entries. In other organizations, all gear is configured for one timezone (either UTC or "head office time").

The important thing is to have a standard for time zone, and to configure it consistently across all hosts and infrastructure equipment.

Rationale:

Impact:

Not having a consistent time zone policy across all hosts and infrastructure means that when dealing with a security incident or technical issue, it becomes very easy to mis-match logs as affected hosts span multiple time zones.

Audit:

To show the current timezone, show the running configuration and filter for the word "timezone".

```
switch(config)# sho run | i timezone
clock timezone EST -5 0
```

Remediation:

To set the timezone, define the timezone name, the offset in hours, then the offset in seconds. The example below shows EST (Offset of -5 hours, zero seconds).

```
switch(config)# clock timezone EST -5 0
```

Default Value:

By default no time zone is configured.

CIS Controls:

Version 7

6.1 Utilize Three Synchronized Time Sources

Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

1.6.3 If a Local Time Zone is used, Configure Daylight Savings (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

If local time zones are configured on network infrastructure, it is important to also configure the time "shift" that occurs as a result of Daylight Savings Time.

Rationale:

Impact:

If local time zones are configured on network infrastructure, it is usually to simplify relating reported end-user issues back to local time entries in the logs. So if local time zones are configured and used in this manner, it becomes important to also configure the time "shift" that occurs as a result of Daylight Savings Time (or "summer-time" on the Cisco CLI)

Audit:

```
switch(config)# sho run | i summer-time
clock summer-time EDT 2 Sun Mar 02:00 1 Sun Nov 02:00 60
```

Remediation:

In most cases, just the name of the DST timezone name is sufficient. NX-OS assumes 1 hour offset, using the United States dates for DST.

```
switch(config)# clock summer-time <DST Timezone Name>
```

for example:

```
switch(config)# clock summer-time EDT
```

If a full definition of the change is needed, it can certainly be set:

```
switch(config)# clock summer-time <DST Timezone Name> <day1> <month1> <time1>
<day2> <month2> <time2> <offset in minutes>
```

where:

- day1, month1, time1 define the start of the DST period
- day2, month2, time2 define the end of the DST period

Default Value:

By default, summer-time (Daylight Savings Time) is not configured. If the summer-time start and stop dates are not specified, then the US standard dates are used: start = 2 Sun Mar 02:00 stop = 1 Sun Nov 02:00 60

CIS Controls:

Version 7

6.1 Utilize Three Synchronized Time Sources

Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

1.6.4 Configure NTP Authentication (Manual)

Profile Applicability:

- Level 2

Description:

By default, NTP is a clear text, unauthenticated protocol. However, it can be configured to authenticate time sources. NTP authentication is an upstream protocol only - authenticated clients have assurance that they are receiving correct time, that the ntp packets have not been tampered with.

Rationale:

Configuring authentication ensures that if the server key does not match the key configured on the NTP client, that the client will drop any NTP replies from that server. If multiple keys are configured,

Audit:

```
switch#show running-config ntp
!Running configuration last done at: Sat Apr 25 07:56:22 2020
!Time: Sat Apr 25 07:56:25 2020

version 9.3(3) Bios:version
ntp server 132.246.11.231 use-vrf management key 42
ntp source-interface loopback1
ntp authenticate
ntp authentication-key 42 md5 pu-slp-pwb 7
ntp trusted-key 42
```

Remediation:

```
switch(config)# ntp authenticate
switch(config)# ntp authentication-key 42 md5 my-ntp-key
switch(config)# ntp trusted-key 42
switch(config)# ntp server 132.246.11.231 use-vrf management key 42
```

Default Value:

By default NTP is not configured.
If NTP is configured, by default it is unauthenticated.

CIS Controls:

Version 7

6 Maintenance, Monitoring and Analysis of Audit Logs
Maintenance, Monitoring and Analysis of Audit Logs

1.7 Configure Banners

1.7.1 Configure an MOTD (Message of the day) Banner (Manual)

Profile Applicability:

- Level 1

Description:

An MOTD banner is displayed when a terminal connects, before a login occurs. This banner is useful for sending messages that affect all users (such as impending system shutdowns). This banner can also be used to notify unauthorized users of any penalties to accessing the device, or any logging that may be configured

Rationale:

Network banners are electronic messages that provide notice of legal rights to users of computer networks. From a legal standpoint, banners have four primary functions.

- Banners may be used to generate consent to real-time monitoring under Title III
- Banners may be used to generate consent to the retrieval of stored files and records pursuant to ECPA.
- in the case of government networks, banners may eliminate any Fourth Amendment "reasonable expectation of privacy" that government employees or other users might otherwise retain in their use of the government's network under O'Connor v. Ortega, 480 U.S. 709 (1987).
- In the case of a non-government network, banners may establish a system administrator's "common authority" to consent to a law enforcement search pursuant to United States v. Matlock, 415 U.S. 164 (1974)." (US Department of Justice APPENDIX A: Sample Network Banner Language)

Audit:

A simple filter will display the motd banner, show the running or saved configuration, with a "b" filter to "begin" the listing at the found string.

```
switch# sho run | b "banner motd"
banner motd ^
the MOTD Banner will be listed here.
^
```

Remediation:

Configure an MOTD banner as shown below. The delimiter character shown is a "^", but it can be any character can serve as a delimiter.

```
switch(config)# banner motd ^
> Enter MOTD Banner here.
> End this message with the same delimeter as above
> ^
switch(config)#
```

Default Value:

By default no MOTD banner is configured.

CIS Controls:

Version 7

17 Implement a Security Awareness and Training Program
Implement a Security Awareness and Training Program

1.7.2 Configure an EXEC Banner (Manual)

Profile Applicability:

- Level 1

Description:

The "exec banner" is displayed with an EXEC process is started. This occurs after login (if authentication is configured). Banners are normally configured for legal reasons, to ensure that any attackers are explicitly notified of the penalties involved in unauthorized access. Banners can also serve as a legal notice to authorized users of the equipment to notify them of any logging that may be configured. Finally, the exec banner (which is post-login) can often also hold asset-specific information, such as:

- The primary technical contacts for the equipment
- Location information - for instance the street address or rack number
- The purchase date
- The asset tag information for the device
- Any upstream circuit numbers
- Carrier or ISP support phone numbers
- Any other asset-specific information that may be important to the organisation

Rationale:

Configure an MOTD banner as shown below. The delimiter character shown is a "^", but it can be any character can serve as a delimiter.

Audit:

A simple filter will display the exec banner, show the running or saved configuration, with a "b" filter to "begin" the listing at the found string.

```
switch(config)# sho run | begin "banner exec"
banner exec ^
Enter your standard Banner text here.  End with the same delimeter as used
above
^
```

If the command does not return a result then the exec banner is not configured

Remediation:

Configure an EXEC banner as shown below. The delimiter character shown is a "^", but it can be any character can serve as a delimiter.

```
switch(config)# banner exec ^
> Enter your standard EXEC Banner text here.  End with the same delimiter as
used above
> ^
switch(config)#
```

Default Value:

By default no exec banner is configured.

CIS Controls:

Version 7

17 Implement a Security Awareness and Training Program
Implement a Security Awareness and Training Program

1.8 Other Services and Accesses

1.8.1 Disable Power on Auto Provisioning (POAP) (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

PowerOn Auto Provisioning (POAP) allows the switch to be auto-provisioned at the time of power-on. This can be extremely useful in a tightly controlled environment, with a solid "network as code" mindset and dev-ops procedures in place for network operations.

Rationale:

Impact:

Without solid procedures and a well-controlled environment, POAP provides a malicious actor the ability to compromise a switch as it is being deployed out of the box. This "day 0" approach to compromising gives the attacker control of the switch from the start - it can be difficult to detect that this has occurred, and may require physical access to gain control back.

Audit:

The "show boot" statement will show the status of POAP in both the running and saved configuration (successful audit criteria shown):

```
switch# sho boot
Current Boot Variables:
sup-1
NXOS variable = bootflash:/nxos.9.3.3.bin
Boot POAP Disabled

Boot Variables on next reload:
sup-1
NXOS variable = bootflash:/nxos.9.3.3.bin
Boot POAP Disabled
```

Alternatively, the command can be parsed from the running or startup config (failed audit criteria shown). Note that POAP is not enabled by default, and if disabled does not show in either the running or startup configuration:

```
switch# sho run | i poap
boot poap enable
switch# sho start | i poap
boot poap enable
```

Remediation:

To disable POAP, use the command:

```
switch(config)# no boot poap enable
```

Default Value:

POAP is not enabled by default. The "boot poap" configuration line does not show in the running or startup configuration if it is disabled, only if it is enabled.

References:

1. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-info-poap

1.8.2 Disable iPXE (Pre-boot eXecution Environment) (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

iPXE allows a NX-OS device to boot from the network, usually using HTTP.

Rationale:

This method allows the switch bootup image to be controlled centrally, often using DHCP services.

Impact:

The risks of using this boot method are obvious. First, DHCP is a broadcast request, so any host (including a malicious host) can provide the DHCP response - the first response "wins". This means that a malicious actor can control operating system being booted on the switch. In addition, the HTTP protocol is clear-text, so is susceptible to modification in transit by an attacker. This is a less likely attack however, as the NX-OS boot sequence has multiple checks in place to verify the validity of the OS, and all most succeed for the boot sequence to proceed.

Audit:

The "show boot order" command can be used to view if PXE is configured or not.
In this example, the running config has PXE configured (audit fail):

```
switch# sho boot order
Current Boot Order:
BootOrder = PXE boot first, follow by Bootflash if netboot failed

Boot Order on next reload:
BootOrder = PXE boot first, follow by Bootflash if netboot failed
```

This example shows the default - no boot order set, so the system boots from the bootflash image only (audit success):

```
CISNXOS9# show boot order
Current Boot Order:
BootOrder = Bootflash only
```

```
Boot Order on next reload:
Boot Order is not set. So, Bootflash is default
```

This example shows the values for a bootflash boot explicitly set (also audit success):

```
switch(config)# sho boot order
Current Boot Order:
BootOrder = Bootflash only

Boot Order on next reload:
BootOrder = Bootflash only
```

An easier programmatic audit would be to query the running or saved configuration directly, using:

```
switch# sho run | i "boot order"
boot order bootflash
```

An audit fail will include the keyword "pxe", and audit pass will not. So adding that:

```
switch# sho run | i "boot order" | grep pxe
```

A blank line indicates audit success, a returned line will include "pxe" so would indicate an audit failure.

Remediation:

Setting the boot order explicity to "bootflash" will remediate a PXE configured device.

```
switch(config)# boot order bootflash
```

You can also "no" the current boot order line to revert to the default setting. For instance, to remove the configuration line "boot order pxe bootflash" command, use

```
switch(config)# no boot order pxe bootflash
```

Default Value:

By default the boot order is "bootflash" only. This default configuration will not show in the configuration.

However, entering any valid "boot order" in the configuration will result it that order being explicit in the configuration, so entering "boot order bootflash" will result in that showing in the configuration.

1.9 Use Dedicated "mgmt" Interface and VRF for Administrative Functions (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

Vendors provisioning dedicated management interfaces is a widespread practice, and gives some significant security advantages when implementing:

- SSH access
- SNMP polling
- Syslog logging
- SNMP traps
- NTP requests

This practice facilitates implementation of segmented, access controlled Management VLANs or VRFs, which acts as a significant deterrent to attackers. It provides management access outside of the regular data plane operations. Also, if there is a routing or switching issue that might interfere with in-band access, the management interface is very often not affected by this and is still acceptable.

Rationale:

Administration via the mgmt interface bypasses the default routing and switching processing on the switch. This means that any routing issues or switching problems on the device itself will not affect access to the mgmt0 interface. Note however that in most cases the uplink from the mgmt0 interface is part of the larger switching infrastructure - this should be taken into account when architecting the overall network.

Impact:

Using the MGMT interface and a dedicated Management VRF ensures that production and management traffic can never interfere with each other.

More importantly, this provides a segregated path outside of the production data plane path for management traffic. This is important because often management traffic such as syslog, SNMPv2 and NTP are in clear text. Routing this traffic using the production data

paths gives a malicious actor the opportunity to intercept or modify this traffic, which facilitates several opportunities for reconnaissance or active attacks by modifying this data.

Audit:

Use the command "show running-config | i source-interface"
Ensure that (if configured) the source-interface is configured for snmp traps, snmp informs, ntp and logging.

```
switch# sho run  | i source-interface
snmp-server source-interface traps mgmt0
snmp-server source-interface informs mgmt0
snmp-server host 1.2.3.4 source-interface mgmt0
ntp source-interface mgmt0
logging source-interface mgmt0
```

Remediation:

First configure the mgmt0 interface:

```
switch(config)# interface mgmt0
switch(config-if)#   ip address 1.2.3.1/24
```

If needed, add the various routes needed for connectivity for the mgmt interface. Note that this can also be accomplished with a routing protocol implemented for the vrf "management"

```
ip route 5.6.7.8 255.255.255.0 1.2.3.254 vrf management
```

Then, configure the source-interface commands for each target protocol that is implemented:

```
switch(config)# snmp-server source-interface traps mgmt0
switch(config)# snmp-server source-interface informs mgmt0
switch(config)# snmp-server host 1.2.3.4 source-interface loopback0
switch(config)# ntp source-interface mgmt0
switch(config)# logging source-interface mgmt0
```

Default Value:

By default, the source-interface is not configured for any protocol. All protocols originate from the interface that is closest to it's target in the vrf "default".

CIS Controls:

Version 7

11.6 Use Dedicated Machines For All Network Administrative Tasks

Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.

11.7 Manage Network Infrastructure Through a Dedicated Network

Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

2 Control Plane

The control plane covers monitoring, route table updates, and generally the dynamic operation of the router. This includes services, settings, and data streams that support and document the operation, traffic handling, and dynamic status of the router. Examples of control plane services include: logging (e.g. Syslog), routing protocols, status protocols like CDP and HSRP, network topology protocols like STP, and traffic security control protocols like IKE. Network control protocols like ICMP, NTP, ARP, and IGMP directed to or sent by the router itself also fall into this area.

2.1 Global Service Rules

Rules in the global service class enforce server and service controls that protect against attacks or expose the device to exploitation.

2.1.1 Configure Control Plane Policing (Manual)

Profile Applicability:

- Level 1

Description:

Control Plane Policing is used to create a set of policies governing specific traffic. Normally this limits the volume and type of traffic that can be directed to the IP addresses on the device, as this traffic normally must be handled in process mode by the switch CPU. For instance, limiting the volume of ICMP traffic that can be sent to a device IP will both limit the CPU impact of that traffic and also limit the bandwidth that this traffic can take. With 10GB and faster interfaces available, both of these considerations are important.

Rationale:

You must configure control plane class maps for control plane policies.

You can classify traffic by matching packets based on existing ACLs. The permit and deny ACL keywords are ignored in the matching.

You can configure policies for IP version 4 (IPv4) and IP version 6 (IPv6) packets.

Impact:

Configuring Control Plane Policing both limits the impact of traffic (either diagnostic or malicious traffic) on the CPU and interfaces of the device. It also limits the impact of this traffic on available bandwidth - it can't restrict how much traffic is sent, but it certainly limits how much is processed, so by that limits the volume of reply traffic.
In many DOS attacks, ideally the attacker wants the volume of the reply traffic to exceed the traffic sent - getting the victim to "amplify" the attack is almost always a desired goal of the attacker. This DOS attack can then be directed to a third "victim" host by the use of spoofing, or the DOS attack may be just against the vulnerable device or host (in this case the NX-OS switch)

Audit:

To just show the COPP Policy applied:

```
switch# sho copp status
Last Config Operation: None
Last Config Operation Timestamp: None
Last Config Operation Status: None
Error Timestamp: 14:11:09 UTC May 11 2020
```

```
Error Occurred: TCAM region is not configured. Please configure TCAM region
and
retry the command (0x410400c5)
Policy-map attached to the control-plane: copp-system-p-policy-strict
```

or

```
switch# sho run | i copp
copp profile strict
```

To then show the policy itself (the default "strict" policy is shown):

```
switch# sho copp profile strict

ip access-list copp-system-p-acl-auto-rp
  permit ip any 224.0.1.39/32
  permit ip any 224.0.1.40/32
ip access-list copp-system-p-acl-bgp
  permit tcp any gt 1023 any eq bgp
  permit tcp any eq bgp any gt 1023
ipv6 access-list copp-system-p-acl-bgp6
  permit tcp any gt 1023 any eq bgp
  permit tcp any eq bgp any gt 1023
ip access-list copp-system-p-acl-dhcp
  permit udp any eq bootpc any
  permit udp any neq bootps any eq bootps
ip access-list copp-system-p-acl-dhcp-relay-response
  permit udp any eq bootps any
  permit udp any any eq bootpc
ipv6 access-list copp-system-p-acl-dhcp6
  permit udp any eq 546 any
  permit udp any any eq 547
ipv6 access-list copp-system-p-acl-dhcp6-relay-response
  permit udp any eq 547 any
  permit udp any any eq 546
ip access-list copp-system-p-acl-eigrp
  permit eigrp any any
ipv6 access-list copp-system-p-acl-eigrp6
  permit eigrp any any
ip access-list copp-system-p-acl-ftp
  permit tcp any any eq ftp-data
  permit tcp any any eq ftp
  permit tcp any eq ftp-data any
  permit tcp any eq ftp any
ip access-list copp-system-p-acl-hsrp
  permit udp any 224.0.0.0/24 eq 1985
ipv6 access-list copp-system-p-acl-hsrp6
  permit udp any ff02::66/128 eq 2029
ip access-list copp-system-p-acl-http
  permit tcp any eq 80 any
  permit tcp any any eq 80
ip access-list copp-system-p-acl-https
  permit tcp any eq 443 any
  permit tcp any any eq 443
ip access-list copp-system-p-acl-icmp
```

```
  permit icmp any any echo
  permit icmp any any echo-reply
ipv6 access-list copp-system-p-acl-icmp6
  permit icmp any any echo-request
  permit icmp any any echo-reply
ip access-list copp-system-p-acl-igmp
  permit igmp any 224.0.0.0/3
mac access-list copp-system-p-acl-mac-cdp-udld-vtp
  permit any 0100.0ccc.cccc 0000.0000.0000
mac access-list copp-system-p-acl-mac-cfsoe
  permit any 0180.c200.000e 0000.0000.0000 0x8843
  permit any 0180.c200.000e 0000.0000.0000
mac access-list copp-system-p-acl-mac-dot1x
  permit any 0180.c200.0003 0000.0000.0000 0x888e
mac access-list copp-system-p-acl-mac-fcoe
  permit any any 0x8906
  permit any any 0x8914
mac access-list copp-system-p-acl-mac-l2-tunnel
  permit any any 0x8840
mac access-list copp-system-p-acl-mac-l3-isis
  permit any 0180.c200.0015 0000.0000.0000
  permit any 0180.c200.0014 0000.0000.0000
  permit any 0900.2b00.0005 0000.0000.0000
  permit any 0900.2b00.0004 0000.0000.0000
mac access-list copp-system-p-acl-mac-lacp
  permit any 0180.c200.0002 0000.0000.0000 0x8809
mac access-list copp-system-p-acl-mac-lldp
  permit any 0180.c200.000e 0000.0000.0000 0x88cc
mac access-list copp-system-p-acl-mac-sdp-srp
  permit any 0180.c200.000e 0000.0000.0000 0x3401
mac access-list copp-system-p-acl-mac-stp
  permit any 0100.0ccc.cccd 0000.0000.0000
  permit any 0180.c200.0000 0000.0000.0000
mac access-list copp-system-p-acl-mac-undesirable
  permit any any
ipv6 access-list copp-system-p-acl-mld
  permit icmp any any mld-query
  permit icmp any any mld-report
  permit icmp any any mld-reduction
  permit icmp any any 143
ip access-list copp-system-p-acl-msdp
  permit tcp any gt 1023 any eq 639
  permit tcp any eq 639 any gt 1023
ipv6 access-list copp-system-p-acl-ndp
  permit icmp any any router-solicitation
  permit icmp any any router-advertisement
  permit icmp any any nd-ns
  permit icmp any any nd-na
ip access-list copp-system-p-acl-ntp
  permit udp any any eq ntp
  permit udp any eq ntp any
ipv6 access-list copp-system-p-acl-ntp6
  permit udp any any eq ntp
  permit udp any eq ntp any
ip access-list copp-system-p-acl-openflow
  permit tcp any eq 6653 any
ip access-list copp-system-p-acl-ospf
```

```
  permit ospf any any
ipv6 access-list copp-system-p-acl-ospf6
  permit ospf any any
ip access-list copp-system-p-acl-pim
  permit pim any 224.0.0.0/24
  permit udp any any eq 496
  permit ip any 224.0.0.13/32
ip access-list copp-system-p-acl-pim-mdt-join
  permit udp any 224.0.0.13/32
ip access-list copp-system-p-acl-pim-reg
  permit pim any any
ipv6 access-list copp-system-p-acl-pim6
  permit pim any ff02::d/128
  permit udp any any eq 496
ipv6 access-list copp-system-p-acl-pim6-reg
  permit pim any any
ip access-list copp-system-p-acl-ptp
  permit udp any 224.0.1.129/32 eq 319
  permit udp any 224.0.1.129/32 eq 320
mac access-list copp-system-p-acl-ptp-l2
  permit any any 0x88f7
ip access-list copp-system-p-acl-ptp-uc
  permit udp any any eq 319
  permit udp any any eq 320
ip access-list copp-system-p-acl-radius
  permit udp any any eq 1812
  permit udp any any eq 1813
  permit udp any any eq 1645
  permit udp any any eq 1646
  permit udp any eq 1812 any
  permit udp any eq 1813 any
  permit udp any eq 1645 any
  permit udp any eq 1646 any
ipv6 access-list copp-system-p-acl-radius6
  permit udp any any eq 1812
  permit udp any any eq 1813
  permit udp any any eq 1645
  permit udp any any eq 1646
  permit udp any eq 1812 any
  permit udp any eq 1813 any
  permit udp any eq 1645 any
  permit udp any eq 1646 any
ip access-list copp-system-p-acl-rip
  permit udp any 224.0.0.0/24 eq 520
ipv6 access-list copp-system-p-acl-rip6
  permit udp any ff02::9/64 eq 521
ip access-list copp-system-p-acl-sftp
  permit tcp any any eq 115
  permit tcp any eq 115 any
ip access-list copp-system-p-acl-snmp
  permit udp any any eq snmp
  permit udp any any eq snmptrap
  permit tcp any any eq snmp
  permit tcp any any eq snmptrap
ipv6 access-list copp-system-p-acl-snmp6
  permit udp any any eq snmp
  permit udp any any eq snmptrap
```

```
  permit tcp any any eq snmp
  permit tcp any any eq snmptrap
ip access-list copp-system-p-acl-ssh
  permit tcp any any eq ssh
  permit tcp any eq ssh any
ipv6 access-list copp-system-p-acl-ssh6
  permit tcp any any eq ssh
  permit tcp any eq ssh any
ip access-list copp-system-p-acl-tacacs
  permit tcp any any eq tacacs
  permit tcp any eq tacacs any
ipv6 access-list copp-system-p-acl-tacacs6
  permit tcp any any eq tacacs
  permit tcp any eq tacacs any
ip access-list copp-system-p-acl-telnet
  permit tcp any any eq telnet
  permit tcp any any eq 107
  permit tcp any eq telnet any
  permit tcp any eq 107 any
ipv6 access-list copp-system-p-acl-telnet6
  permit tcp any any eq telnet
  permit tcp any any eq 107
  permit tcp any eq telnet any
  permit tcp any eq 107 any
ip access-list copp-system-p-acl-tftp
  permit udp any any eq tftp
  permit udp any any eq 1758
  permit udp any eq tftp any
  permit udp any eq 1758 any
ipv6 access-list copp-system-p-acl-tftp6
  permit udp any any eq tftp
  permit udp any any eq 1758
  permit udp any eq tftp any
  permit udp any eq 1758 any
ip access-list copp-system-p-acl-traceroute
  permit icmp any any ttl-exceeded
  permit icmp any any port-unreachable
  permit udp any any range 33434 33534
ip access-list copp-system-p-acl-undesirable
  permit udp any any eq 1434
ip access-list copp-system-p-acl-vpc
  permit udp any any eq 3200
ip access-list copp-system-p-acl-vrrp
  permit ip any 224.0.0.18/32
ipv6 access-list copp-system-p-acl-vrrp6
  permit ipv6 any ff02::12/128

class-map type control-plane match-any copp-system-p-class-critical
  match access-group name copp-system-p-acl-bgp
  match access-group name copp-system-p-acl-rip
  match access-group name copp-system-p-acl-vpc
  match access-group name copp-system-p-acl-bgp6
  match access-group name copp-system-p-acl-ospf
  match access-group name copp-system-p-acl-rip6
  match access-group name copp-system-p-acl-eigrp
  match access-group name copp-system-p-acl-ospf6
  match access-group name copp-system-p-acl-eigrp6
```

```
  match access-group name copp-system-p-acl-auto-rp
  match access-group name copp-system-p-acl-mac-l3-isis
class-map type control-plane match-any copp-system-p-class-exception
  match exception ip option
  match exception ip icmp unreachable
  match exception ipv6 option
  match exception ipv6 icmp unreachable
class-map type control-plane match-any copp-system-p-class-exception-diag
  match exception ttl-failure
  match exception mtu-failure
class-map type control-plane match-any copp-system-p-class-fcoe
  match access-group name copp-system-p-acl-mac-fcoe
class-map type control-plane match-any copp-system-p-class-important
  match access-group name copp-system-p-acl-hsrp
  match access-group name copp-system-p-acl-vrrp
  match access-group name copp-system-p-acl-hsrp6
  match access-group name copp-system-p-acl-vrrp6
  match access-group name copp-system-p-acl-mac-lldp
class-map type control-plane match-any copp-system-p-class-l2-default
  match access-group name copp-system-p-acl-mac-undesirable
class-map type control-plane match-any copp-system-p-class-l2-unpoliced
  match access-group name copp-system-p-acl-mac-stp
  match access-group name copp-system-p-acl-mac-lacp
  match access-group name copp-system-p-acl-mac-cfsoe
  match access-group name copp-system-p-acl-mac-sdp-srp
  match access-group name copp-system-p-acl-mac-l2-tunnel
  match access-group name copp-system-p-acl-mac-cdp-udld-vtp
class-map type control-plane match-any copp-system-p-class-l3mc-data
  match exception multicast rpf-failure
  match exception multicast dest-miss
class-map type control-plane match-any copp-system-p-class-l3mcv6-data
  match exception multicast ipv6-rpf-failure
  match exception multicast ipv6-dest-miss
class-map type control-plane match-any copp-system-p-class-l3uc-data
  match exception glean
class-map type control-plane match-any copp-system-p-class-management
  match access-group name copp-system-p-acl-ftp
  match access-group name copp-system-p-acl-ntp
  match access-group name copp-system-p-acl-ssh
  match access-group name copp-system-p-acl-http
  match access-group name copp-system-p-acl-ntp6
  match access-group name copp-system-p-acl-sftp
  match access-group name copp-system-p-acl-snmp
  match access-group name copp-system-p-acl-ssh6
  match access-group name copp-system-p-acl-tftp
  match access-group name copp-system-p-acl-https
  match access-group name copp-system-p-acl-snmp6
  match access-group name copp-system-p-acl-tftp6
  match access-group name copp-system-p-acl-radius
  match access-group name copp-system-p-acl-tacacs
  match access-group name copp-system-p-acl-telnet
  match access-group name copp-system-p-acl-radius6
  match access-group name copp-system-p-acl-tacacs6
  match access-group name copp-system-p-acl-telnet6
class-map type control-plane match-any copp-system-p-class-monitoring
  match access-group name copp-system-p-acl-icmp
  match access-group name copp-system-p-acl-icmp6
```

```
  match access-group name copp-system-p-acl-traceroute
class-map type control-plane match-any copp-system-p-class-multicast-host
  match access-group name copp-system-p-acl-mld
class-map type control-plane match-any copp-system-p-class-multicast-router
  match access-group name copp-system-p-acl-pim
  match access-group name copp-system-p-acl-msdp
  match access-group name copp-system-p-acl-pim6
  match access-group name copp-system-p-acl-pim-reg
  match access-group name copp-system-p-acl-pim6-reg
  match access-group name copp-system-p-acl-pim-mdt-join
  match exception mvpn
class-map type control-plane match-any copp-system-p-class-nat-flow
  match exception nat-flow
class-map type control-plane match-any copp-system-p-class-ndp
  match access-group name copp-system-p-acl-ndp
class-map type control-plane match-any copp-system-p-class-normal
  match access-group name copp-system-p-acl-mac-dot1x
  match protocol arp
class-map type control-plane match-any copp-system-p-class-normal-dhcp
  match access-group name copp-system-p-acl-dhcp
  match access-group name copp-system-p-acl-dhcp6
class-map type control-plane match-any copp-system-p-class-normal-dhcp-relay-
res
ponse
  match access-group name copp-system-p-acl-dhcp-relay-response
  match access-group name copp-system-p-acl-dhcp6-relay-response
class-map type control-plane match-any copp-system-p-class-normal-igmp
  match access-group name copp-system-p-acl-igmp
class-map type control-plane match-any copp-system-p-class-openflow
  match access-group name copp-system-p-acl-openflow
class-map type control-plane match-any copp-system-p-class-redirect
  match access-group name copp-system-p-acl-ptp
  match access-group name copp-system-p-acl-ptp-l2
  match access-group name copp-system-p-acl-ptp-uc
class-map type control-plane match-any copp-system-p-class-undesirable
  match access-group name copp-system-p-acl-undesirable
  match exception multicast sg-rpf-failure
class-map type control-plane match-any copp-system-p-class-undesirablev6
  match exception multicast ipv6-sg-rpf-failure

policy-map type control-plane copp-system-p-policy-strict
  class copp-system-p-class-l3uc-data
    set cos 1
    police cir 250 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-critical
    set cos 7
    police cir 19000 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 3000 pps bc 256 packets conform transmit violate drop
  class copp-system-p-class-openflow
    set cos 5
    police cir 2000 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 3000 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-multicast-host
```

```
    set cos 1
    police cir 2000 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-l3mc-data
    set cos 1
    police cir 3000 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-normal
    set cos 1
    police cir 1500 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-ndp
    set cos 6
    police cir 1500 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 300 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 400 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-normal-igmp
    set cos 3
    police cir 6000 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-redirect
    set cos 1
    police cir 1500 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-exception
    set cos 1
    police cir 50 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-exception-diag
    set cos 1
    police cir 50 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 3000 pps bc 512000 packets conform transmit violate drop
  class copp-system-p-class-monitoring
    set cos 1
    police cir 300 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-l2-unpoliced
    set cos 7
    police cir 20000 pps bc 8192 packets conform transmit violate drop
  class copp-system-p-class-undesirable
    set cos 0
    police cir 15 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-fcoe
    set cos 6
    police cir 1500 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-nat-flow
    set cos 7
    police cir 100 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-l3mcv6-data
    set cos 1
    police cir 3000 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-undesirablev6
    set cos 0
    police cir 15 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-l2-default
    set cos 0
    police cir 50 pps bc 32 packets conform transmit violate drop
  class class-default
```

```
    set cos 0
    police cir 50 pps bc 32 packets conform transmit violate drop
```

To show all COPP Settings (note that the majority of this output will normally not be actively used):

```
switch(config)# # sho class-map type control-plane

    Class-map type control-plane match-any copp-system-p-class-critical
      match access-group name copp-system-p-acl-bgp
      match access-group name copp-system-p-acl-rip
      match access-group name copp-system-p-acl-vpc
      match access-group name copp-system-p-acl-bgp6
      match access-group name copp-system-p-acl-ospf
      match access-group name copp-system-p-acl-rip6
      match access-group name copp-system-p-acl-eigrp
      match access-group name copp-system-p-acl-ospf6
      match access-group name copp-system-p-acl-eigrp6
      match access-group name copp-system-p-acl-auto-rp
      match access-group name copp-system-p-acl-mac-l3-isis

    Class-map type control-plane match-any copp-system-p-class-exception
      match exception ip option
      match exception ip icmp unreachable
      match exception ipv6 option
      match exception ipv6 icmp unreachable

    Class-map type control-plane match-any copp-system-p-class-exception-diag
      match exception ttl-failure
      match exception mtu-failure

    Class-map type control-plane match-any copp-system-p-class-fcoe
      match access-group name copp-system-p-acl-mac-fcoe

    Class-map type control-plane match-any copp-system-p-class-important
      match access-group name copp-system-p-acl-hsrp
      match access-group name copp-system-p-acl-vrrp
      match access-group name copp-system-p-acl-hsrp6
      match access-group name copp-system-p-acl-vrrp6
      match access-group name copp-system-p-acl-mac-lldp

    Class-map type control-plane match-any copp-system-p-class-l2-default
      match access-group name copp-system-p-acl-mac-undesirable

    Class-map type control-plane match-any copp-system-p-class-l2-unpoliced
      match access-group name copp-system-p-acl-mac-stp
      match access-group name copp-system-p-acl-mac-lacp
      match access-group name copp-system-p-acl-mac-cfsoe
      match access-group name copp-system-p-acl-mac-sdp-srp
      match access-group name copp-system-p-acl-mac-l2-tunnel
      match access-group name copp-system-p-acl-mac-cdp-udld-vtp

    Class-map type control-plane match-any copp-system-p-class-l3mc-data
      match exception multicast rpf-failure
      match exception multicast dest-miss
```

```
    Class-map type control-plane match-any copp-system-p-class-l3mcv6-data
      match exception multicast ipv6-rpf-failure
      match exception multicast ipv6-dest-miss

    Class-map type control-plane match-any copp-system-p-class-l3uc-data
      match exception glean

    Class-map type control-plane match-any copp-system-p-class-management
      match access-group name copp-system-p-acl-ftp
      match access-group name copp-system-p-acl-ntp
      match access-group name copp-system-p-acl-ssh
      match access-group name copp-system-p-acl-http
      match access-group name copp-system-p-acl-ntp6
      match access-group name copp-system-p-acl-sftp
      match access-group name copp-system-p-acl-snmp
      match access-group name copp-system-p-acl-ssh6
      match access-group name copp-system-p-acl-tftp
      match access-group name copp-system-p-acl-https
      match access-group name copp-system-p-acl-snmp6
      match access-group name copp-system-p-acl-tftp6
      match access-group name copp-system-p-acl-radius
      match access-group name copp-system-p-acl-tacacs
      match access-group name copp-system-p-acl-telnet
      match access-group name copp-system-p-acl-radius6
      match access-group name copp-system-p-acl-tacacs6
      match access-group name copp-system-p-acl-telnet6

    Class-map type control-plane match-any copp-system-p-class-monitoring
      match access-group name copp-system-p-acl-icmp
      match access-group name copp-system-p-acl-icmp6
      match access-group name copp-system-p-acl-traceroute

    Class-map type control-plane match-any copp-system-p-class-multicast-host
      match access-group name copp-system-p-acl-mld

    Class-map type control-plane match-any copp-system-p-class-multicast-
router
      match access-group name copp-system-p-acl-pim
      match access-group name copp-system-p-acl-msdp
      match access-group name copp-system-p-acl-pim6
      match access-group name copp-system-p-acl-pim-reg
      match access-group name copp-system-p-acl-pim6-reg
      match access-group name copp-system-p-acl-pim-mdt-join
      match exception mvpn

    Class-map type control-plane match-any copp-system-p-class-nat-flow
      match exception nat-flow

    Class-map type control-plane match-any copp-system-p-class-ndp
      match access-group name copp-system-p-acl-ndp

    Class-map type control-plane match-any copp-system-p-class-normal
      match access-group name copp-system-p-acl-mac-dot1x
      match protocol arp

    Class-map type control-plane match-any copp-system-p-class-normal-dhcp
```

```
      match access-group name copp-system-p-acl-dhcp
      match access-group name copp-system-p-acl-dhcp6

    Class-map type control-plane match-any copp-system-p-class-normal-dhcp-
relay
-response
      match access-group name copp-system-p-acl-dhcp-relay-response
      match access-group name copp-system-p-acl-dhcp6-relay-response

    Class-map type control-plane match-any copp-system-p-class-normal-igmp
      match access-group name copp-system-p-acl-igmp

    Class-map type control-plane match-any copp-system-p-class-openflow
      match access-group name copp-system-p-acl-openflow

    Class-map type control-plane match-any copp-system-p-class-redirect
      match access-group name copp-system-p-acl-ptp
      match access-group name copp-system-p-acl-ptp-l2
      match access-group name copp-system-p-acl-ptp-uc

    Class-map type control-plane match-any copp-system-p-class-undesirable
      match access-group name copp-system-p-acl-undesirable
      match exception multicast sg-rpf-failure

    Class-map type control-plane match-any copp-system-p-class-undesirablev6
      match exception multicast ipv6-sg-rpf-failure
```

Remediation:

Normally the "strict" Control Plane Policing Policy is recommended. If additional protections are required for a specific situation, then this policy can be copied - the copy can then be modified and applied.
As noted in the command's response, applying a COPP Policy may disrupt other control traffic.

```
switch(config)# copp profile strict
This operation can cause disruption of control traffic. Proceed (y/n)?  [no]
y
switch(config)#
```

Default Value:

By default, the "strict" Control Plane Policing Policy is in place.

```
CISNXOS9# sho run | i copp

copp profile strict
```

The pre-configured COPP Policies that are available are:

- Strict—This policy is 1 rate and 2 color. This setting gives the NX-OS switch the best DOS protection of the 5 options available.
- Moderate—This policy is 1 rate and 2 color. The important class burst size is greater than the strict policy but less than the lenient policy.
- Lenient—This policy is 1 rate and 2 color. The important class burst size is greater than the moderate policy but less than the dense policy.
- Dense—This policy is 1 rate and 2 color. The policer CIR values are less than the strict policy.
- Skip—No control plane policy is applied. (Not Recommended)

References:

1. https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/6-x/security/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_Security_Configuration_Guide/b_Cisco_Nexus_9000_Series_NX-OS_Security_Configuration_Guide_chapter_010001.html#con_1060709

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

3 Data Plane

Services and settings related to the data passing through the router (as opposed to direct to it). The data plane is for everything not in control or management planes. Settings on a router concerned with the data plane include interface access lists, firewall functionality (e.g. CBAC), NAT, and IPSec. Settings for traffic-affecting services like unicast RPF verification and CAR/QoS also fall into this area.

3.1 Secure Routing Protocols

3.1.1 EIGRP

3.1.1.1 Configure EIGRP Authentication on all EIGRP Routing Devices (Manual)

Profile Applicability:

- Level 2

Description:

You can configure authentication between neighbors for EIGRP

Rationale:

You can configure EIGRP authentication for the EIGRP process or for individual interfaces. Interface EIGRP authentication configuration overrides the EIGRP process-level authentication configuration.

Because EIGRP is a multicast protocol, any device can advertise EIGRP capabilities and routes, and by default all connected EIGRP devices will honor those advertisements. This means that a malicious actor can advertise bogus routes to valid hosts or networks, allowing the interception and modification of traffic intended for those hosts or subnets.

For this reason it is important that EIGRP endpoints authenticate to each other, ensuring that only valid routers can participate in the exchange of routes.

Audit:

The "show running-configuration eigrp" command will show all of the EIGRP configuration, ensure that in the main EIGRP address-family section (whether that is ipv4 or ipv6) has both "authentication mode md5" set, and the appropriate key-chain assigned

```
switch(config-if)# sho run eigrp

!Command: show running-config eigrp
!Running configuration last done at: Wed May 20 14:39:55 2020
!Time: Wed May 20 14:48:11 2020

version 9.3(3) Bios:version
feature eigrp

router eigrp 10
  address-family ipv4 unicast
    passive-interface default
    authentication mode md5
    authentication key-chain <EIGRP key-chain name>
```

```
interface Vlan1
  no ip passive-interface eigrp 10
```

Remediation:

Ensure that you have enabled the EIGRP feature.
Ensure that all neighbors for an EIGRP process share the same authentication configuration, including the shared authentication key.
Create the key-chain for this authentication configuration. See the Cisco NX-OS Security Configuration Guide.
Ensure that you are in the correct VDC (or use the switchto vdc command)
Configure authentication:

```
switch(config)# router eigrp [instance-tag]
switch(config-router)# address-family {ipv4 | ipv6} unicast
switch(config-router)# authentication key-chain [key-chain]
switch(config-router)# authentication mode md5
```

Next assign the interface:

```
switch(config)# interface [interface-type slot/port]
switch(config-if)# router eigrp [instance-tag]
switch(config-if)# authentication key-chain eigrp [instance-tag key-chain]
switch(config-if)# authentication mode eigrp [instance-tag] md5
```

Every EIGRP routeable interface should be set to either passive-interface, or be configured with authentication keys.

Default Value:

EIGRP is not configured by default

If configured, EIGRP authentication is not configured by default.

By default, if configured, EIGRP both advertises on and listens on all interfaces that fall into the subnets defined in the "network" statements.

References:

1. https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_2/nx-os/unicast/configuration/guide/l3_cli_nxos/l3_eigrp.html#wp1075849

Additional Information:

For EIGRP environments only

CIS Controls:

Version 7

11.1 Maintain Standard Security Configurations for Network Devices

Maintain standard, documented security configuration standards for all authorized network devices.

3.1.1.2 Configure EIGRP Passive interfaces for interfaces that do not have peers (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

EIGRP both listens on and advertises on all interfaces that have IPs in subnets that are defined as "networks" in the EIGRP configuration.
Ensure that interfaces that do not "face" an EIGRP peer are set to passive.

Rationale:

If an interface is set to "passive", then EIGRP will not advertise out of that interface or listen on that interface for EIGRP neighbors. By default, all interfaces advertise via multicast to solicit EIGRP neighbors, and also listen for neighbor advertisements.

Impact:

If an interface is set to the default (ie - not passive), then an attacker can pose as an EIGRP peer, either to collect EIGRP information from advertisements or to inject bogus routes into the table. Bogus routes can then be used to DOS that subnet, or to intercept traffic to or from that subnet either to eavesdrop on conversations or to modify data in transit.

Quite often the goal of an attack of this type is to collect login credentials from a malicious copy of the target website.

Audit:

The "show running-config eigrp" command will list the entire EIGRP configuration. Passive interfaces are listed individually - in this example, interface VLAN 1 is passive

```
switch# sho run eigrp

!Command: show running-config eigrp
!Running configuration last done at: Wed May 20 14:13:17 2020
!Time: Wed May 20 14:17:22 2020

version 9.3(3) Bios:version
feature eigrp

router eigrp 10
```

```
  address-family ipv4 unicast
    authentication mode md5
    authentication key-chain <key-chain-name>

interface Vlan1
  ip passive-interface eigrp 10
```

Remediation:

If some IP interfaces have peers and some do not, set the ones with no peers to "passive"

```
switch(config-if)# int vlan 1
switch(config-if)# ip passive-interface eigrp <EIGRP process number>
```

Default Value:

By default, passive interfaces are not configured.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

3.1.1.3 Configure EIGRP log-adjacency-changes (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

Logging changes to the EIGRP peering relationships is recommended. This setting is enabled by default.

Rationale:

Any logged changes in a routing peer relationship will in the best case indicate a service issue due to standard operational issues (connectivity issues and so on) or in the worst case, could indicate malicious activity attempting to subvert the peering relationship and/or the routing table.

Impact:

Errors on adjacency relationships are a common early warning message in attacks on routers. If successful, a malicious actor can advertise bogus routes to valid hosts or networks, allowing the interception and modification of traffic intended for those hosts or subnets.

For this reason it is important that EIGRP endpoints alert on any interruptions in adjacency.

Audit:

By default EIGRP adjacency changes are logged, and this does not show in the configuration.
Audit pass (no output):

```
switch# sho run eigrp | i adjacency
```

Audit failure (logging is disabled, as shown in the output):

```
switch# sho run eigrp | i adjacency
  no log-adjacency-changes
```

Log entries of adjacency changes being formed and dropped are shown below. Logging servers and SIEMs should be configured to alert on the keyword "NBRCHANGE":

```
2020 May 22 18:47:32 switch %EIGRP-5-NBRCHANGE_DUAL:  eigrp-10 [3857]
(default-base) IP-EIGRP(0) 10: Neighbor 10.10.10.11 (Vlan1) is up: new
adjacency
2020 May 22 18:48:07 switch %EIGRP-5-NBRCHANGE_DUAL:  eigrp-10 [3857]
(default-base) IP-EIGRP(0) 10: Neighbor 10.10.10.11 (Vlan1) is down: holding
time expired
```

Remediation:

By default EIGRP adjacency changes are logged, and this does not show in the configuration.
If however it is disabled, it can be re-enabled as shown below.

```
switch(config)# router eigrp <eigrp process tag>
switch(config-router)# log-adjacency-changes
```

Default Value:

By default logging of eigrp adjacency changes is enabled.

CIS Controls:

Version 7

11.2 Document Traffic Configuration Rules

All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.

3.1.2 BGP

3.1.2.1 Configure BGP to Log Neighbor Changes (Manual)

Profile Applicability:

- Level 2
- Level 1

Description:

Logging changes to the BGP peering relationships is recommended. Any logged changes will in the best case indicate a service issue due to standard operational issues (connectivity issues and so on) or in the worst case, could indicate malicious activity attempting to subvert the peering relationship and/or the routing table.

Rationale:

Audit:

The "show running-config bgp" command will list out the full BGP configuration. For each BGP neighbor stanza, ensure that the "log-neighbor-changes" command is present.

```
switch# sho run bgp

!Command: show running-config bgp
!Running configuration last done at: Wed May 20 11:47:06 2020
!Time: Wed May 20 11:47:10 2020

version 9.3(3) Bios:version
feature bgp

router bgp 65520
  router-id 10.10.10.10
  neighbor 10.10.10.11
    remote-as 65521
    log-neighbor-changes
```

Logging events triggered by BGP sessions being established or dropped are shown below. The keyword "BGP-5-ADJCHANGE", or just "ADJCHANGE" should be configured in any logging or SIEM platform to generate an alert.

```
switch# sho logging | i ADJCHANGE
2020 May 20 11:54:18 CISNXOS9 %BGP-5-ADJCHANGE:  bgp- [7984] (default)
neighbor 10.10.10.11 Up
2020 May 20 13:08:15 CISNXOS9 %BGP-5-ADJCHANGE:  bgp- [7984] (default)
neighbor 10.10.10.11 Down - sent:  holdtimer expired error
```

Remediation:

In each "neigbor" stanza of the BGP configuration, add the command "log-neighbor-changes"

```
switch(config)# router bgp <asn>
switch(config-router)#   router-id <local ip, preferably a loopback>
switch(config-router)#   neighbor <neighbor ip address>
switch(config-router-neighbor)#     remote-as <neighbor asn>
switch(config-router-neighbor)#     log-neighbor-changes
```

In addition, the events below should be configured in any log or SIEM solution to generate an alert for investigation. A good keyword to alert on is "ADJCHANGE"

```
2020 May 20 11:54:18 CISNXOS9 %BGP-5-ADJCHANGE:  bgp- [7984] (default)
neighbor 10.10.10.11 Up
2020 May 20 13:08:15 CISNXOS9 %BGP-5-ADJCHANGE:  bgp- [7984] (default)
neighbor 10.10.10.11 Down - sent:  holdtimer expired error
```

Default Value:

Not enabled

References:

1. https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_2/nx-os/unicast/configuration/guide/l3_cli_nxos/l3_bgp.html

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

3.1.2.2 If Possible, Limit the BGP Routes Accepted from Peers (Manual)

Profile Applicability:

- Level 2

Description:

Once a BGP relationship is established, the BGP process will accept routes from any connected peers and consider those routes to be valid. For this reason, especially in ISP or other carrier situations, it is important that only routes that are valid for any particular peer are accepted for that peer.

Rationale:

Impact:

Without configuring route filtering, any route advertised by any BGP peer is considered valid. For this reason, especially in carrier or ISP situations it is important that route filtering be configured. Without filtering, a misconfigured or compromised peer can easily advertise entire subnets that should be routed elsewhere, either routing them to nul or receiving traffic to the compromised subnet for for interception or modification, then forwarding it on to it's final destination.

Audit:

"Show run bgp" will show a summary of the BGP configuration. In this case, we are looking for the inbound route-map statement (the last line in this example):

```
switch# sho run bgp

!Command: show running-config bgp
!Running configuration last done at: Tue May 19 17:08:35 2020
!Time: Tue May 19 17:14:14 2020

version 9.3(3) Bios:version
feature bgp

router bgp 65520
  router-id 10.10.10.10
  address-family ipv4 unicast
    network 10.10.10.0/24
  neighbor 10.10.10.11
    remote-as 65521
    address-family ipv4 unicast
      route-map route-map RM_BGP_PEERNAME_IN in
```

Showing the route-map displays the prefix list, which defines what subnets are permitted:

```
switch# sho route-map RM_BGP_PEERNAME_IN
route-map RM_BGP_PEERNAME_IN, permit, sequence 10
  Match clauses:
    ip address prefix-lists: PL_PEERNAME_PERMIT_SUBNETS
  Set clauses:
```

Finally, to display the prefixes:

```
switch# show ip prefix-list PL_PEERNAME_PERMIT_SUBNETS
ip prefix-list PL_PEERNAME_PERMIT_SUBNETS: 2 entries
   seq 5 permit 10.11.11.0/24
   seq 10 permit 10.11.12.0/24
```

Remediation:

First, define the subnets that will be permitted from the peer PEERNAME (use descriptive, self documenting names in NX-OS constructions where possible). Note that any subnets not listed as permitted are by default denied (there is an implicit "deny all" at the bottom of the list)

```
switch(config)# ip prefix-list PL_PEERNAME_PERMIT_SUBNETS description
Permitted Subnets from Peer PEERNAME
switch(config)# ip prefix-list PL_PEERNAME_PERMIT_SUBNETS permit
10.11.11.0/24
switch(config)# ip prefix-list PL_PEERNAME_PERMIT_SUBNETS permit
10.11.12.0/24
```

In this example above, only "permits" are defined. Deny lines are also allowed - refusing routes that are not accepted (for instance "bogon" or "martian" subnets), and may be more important in some situations, for example if this switch is accepting routes from the public internet. (note that this is not typical deployment scenario for an NX-OS switch)
Next, create the route-map, will will apply that list:

```
switch(config)# route-map RM_BGP_PEERNAME_IN permit 10
switch(config-route-map)#   match ip address prefix-list
PL_PEERNAME_PERMIT_SUBNETS
```

Finally, within the BGP configuration, apply that route-map to the BGP peer definition. Note that the "in" keyword denotes inbound (accepted) information.:

```
switch(config)# router bgp 65520
switch(config-router)#   router-id 10.10.10.10
switch(config-router)#   address-family ipv4 unicast
switch(config-router-af)#     network 10.10.10.0/24
switch(config-router-af)#   neighbor 10.10.10.11
switch(config-router-neighbor)#     remote-as 65521
switch(config-router-neighbor)#     address-family ipv4 unicast
switch(config-router-neighbor-af)#      route-map RM_BGP_PEERNAME_IN in
```

Default Value:

BGP filtering is not enabled by default. By default, all routes received from defined peers are accepted as valid.

References:

1. https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_2/nx-os/unicast/configuration/guide/l3_cli_nxos/l3_bgp.html

CIS Controls:

Version 7

11.1 Maintain Standard Security Configurations for Network Devices

Maintain standard, documented security configuration standards for all authorized network devices.

3.1.2.3 Configure BGP Authentication (Manual)

Profile Applicability:

- Level 2

Description:

BGP is a usually configured as a point-to-point / unicast protocol. Configuring authentication as part of the neighbor configuration adds an additional layer of security to the conversation.

Rationale:

Impact:

Configuring authentication adds an MD5 hash to the neighbor negotiation that occurs between two BGP peers. An authentication failure would indicate either a misconfiguration, or possibly an attacker mounting an impersonation attack, masquerading as the BGP peer (possibly by ARP cache poisoning attack) and attempting to then peer up with incorrect credentials.

Audit:

The "show running-confguration bgp" command will list the entire BGP configuration. Ensure that the "password" command is present in each neighbor stanza.

```
switch# sho run bgp

!Command: show running-config bgp
!Running configuration last done at: Wed May 20 13:52:03 2020
!Time: Wed May 20 13:54:17 2020

version 9.3(3) Bios:version
feature bgp

router bgp 65520
  router-id 10.10.10.10
  neighbor 10.10.10.11
    remote-as 65521
    log-neighbor-changes
    password 3 34a1d2277d4f4cc9e9fa97b9d4434019f46f16ae96bb54a3
    address-family ipv4 unicast
```

Remediation:

For each BGP neighbor, add the "password" command to the matching stanza, with a long and complex string. Note that the same password must be used on the matching peer. Different passwords should be used for each peer.

```
switch(config)# router bgp 65520
switch(config-router)# neigh 10.10.10.11
switch(config-router-neighbor)# password ?
  0     Specifies an UNENCRYPTED neighbor password will follow
  3     Specifies an 3DES ENCRYPTED neighbor password will follow
  7     Specifies a Cisco type 7  ENCRYPTED neighbor password will follow
  LINE  The UNENCRYPTED (cleartext) neighbor password

switch(config-router-neighbor)# password somelongcomplexstring
```

Default Value:

By default, BGP authentication is not enabled.

References:

1. https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_2/nx-os/unicast/configuration/guide/l3_cli_nxos/l3_advbgp.html#wp1066903

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

11.1 Maintain Standard Security Configurations for Network Devices

Maintain standard, documented security configuration standards for all authorized network devices.

3.1.3 OSPF

3.1.3.1 Set Interfaces with no Peers to Passive-Interface (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

By default, OSPF will advertise via multicast to solicit peers, and will listen for neighbor / peer advertisements on all OSPF configured interfaces.

Rationale:

If an interface is set to "passive", then EIGRP will not advertise out of that interface or listen on that interface for EIGRP neighbors. I will however still advertise the networks associated with that interface to peers on other interfaces. By default, all interfaces advertise via multicast to solicit OSPF neighbors, and also listen for neighbor advertisements.

Impact:

If an interface is set to the default (ie - not passive), then an attacker can pose as an OSPF peer, either to collect OSPF information from advertisements or to inject bogus routes into the table. Bogus routes can then be used to DOS that subnet, or to intercept traffic to or from that subnet either to eavesdrop on conversations or to modify data in transit.

Quite often the goal of an attack of this type is to collect login credentials from a malicious copy of the target website.

Audit:

The "show running-configuration ospf" command will list the complete OSPF configuration. For all interfaces that do not have facing peers, ensure that those interfaces have the "ip ospf passive-interface" set.
Every routeable interface should be set to either passive-interface, or be configured with authentication keys.

```
switch# sho running-config ospf

!Command: show running-config ospf
!Running configuration last done at: Wed May 20 14:24:49 2020
!Time: Wed May 20 14:26:46 2020
```

```
version 9.3(3) Bios:version
feature ospf

router ospf 10
  router-id 10.10.10.10

interface Vlan1
  ip ospf passive-interface
  ip router ospf 10 area 0.0.0.0
```

Remediation:

For each routeable interface, if there is no facing peer on that interface set that interface to passive with the "ip ospf passive-interface" configuration command.
Every routeable interface should be set to either passive-interface, or be configured with authentication keys.

```
switch(config)# int vlan 1
switch(config-if)# ip router ospf 10 area 0
switch(config-if)# ip ospf passive-interface
```

Default Value:

By default, passive interfaces are not configured - no OSPF configured interfaces are set to passive. This means that OSPF will advertise via multicast to solicit peers, and will listen for neighbor / peer advertisements on all OSPF configured interfaces.

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.1.3.2 Authenticate OSPF peers with MD5 authentication keys (Manual)

Profile Applicability:

- Level 2

Description:

If OSPF is configured, peers can be authenticated using keys. This is not configured by default. If configured, MD5 hashes are recommended as the authentication mechanism. MD5 is the best option for multi-vendor support, and is also the best cryptographic option available in the OSPF standard.

Rationale:

Impact:

Because OSPF is a multicast protocol, any device can advertise OSPF capabilities and routes, and by default all connected OSPF devices will honor those advertisements. This means that a malicious actor can advertise bogus routes to valid hosts or networks, allowing the interception and modification of traffic intended for those hosts or subnets.

For this reason it is important that OSPF endpoints authenticate to each other, ensuring that only valid routers can participate in the exchange of routes.

Audit:

The "show running-configuration ospf" lists the entire OSPF configuration. For all interfaces that face peers, ensure that these two commands are in place:

```
interface <interfacename>
   ip ospf authentication message-digest
   ip ospf authentication key-chain <OSPF Key-Chain name>
```

Each OSPF routeable interface should either have authentication configured or be configured as an OSPF passive interface.

```
switch(config-if)# sho run ospf

!Command: show running-config ospf
!Running configuration last done at: Wed May 20 14:39:55 2020
!Time: Wed May 20 14:43:02 2020

version 9.3(3) Bios:version
feature ospf
```

```
router ospf 10
  router-id 10.10.10.10

interface Vlan1
  ip ospf authentication message-digest
  ip ospf authentication key-chain OSPFKeyChain
  ip router ospf 10 area 0.0.0.0
```

Remediation:

For each OSPF routeable interface, set the message-digest authentication method, and assign the appropriate keychain.
Each OSPF routeable interface should either have authentication configured or be configured as an OSPF passive interface.

```
switch(config)# interface Vlan1
switch(config-int)# ip ospf authentication message-digest
switch(config-int)#  ip ospf authentication key-chain <OSPF Key Chain>
```

Default Value:

By default, OSPF authentication is not enabled by default.

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.1.3.3 Log OSPF Adjacency Changes (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

Logging changes to the BGP peering relationships is recommended.

Rationale:

Any logged changes in a routing peer relationship will in the best case indicate a service issue due to standard operational issues (connectivity issues and so on) or in the worst case, could indicate malicious activity attempting to subvert the peering relationship and/or the routing table.

Impact:

Errors on adjacency relationships are a common early warning message in attacks on routers. If successful, a malicious actor can advertise bogus routes to valid hosts or networks, allowing the interception and modification of traffic intended for those hosts or subnets.

For this reason it is important that OSPF endpoints alert on any interruptions in adjacency.

Audit:

The "show running-config OSPF" command will list out the full OSPF configuration. Ensure that the "log-adjacency-changes" command is present. It is globally applied to all adjacencies.

```
switch# sho run ospf | i log-adjacency
  log-adjacency-changes
```

Log entries for adjacencies being established are shown below. Configuring any syslog servers or SIEM to alert on the keyword 'ADJCHANGE" is recommended.

```
2020 May 22 10:34:28 CISNXOS9 %OSPF-5-ADJCHANGE:  ospf-10 [10184]  Nbr
10.10.10.11 on Vlan1 went EXSTART
2020 May 22 10:34:28 CISNXOS9 %OSPF-5-ADJCHANGE:  ospf-10 [10184]  Nbr
10.10.10.11 on Vlan1 went FULL
```

Log entries for adjacencies being dropped are shown below:

```
2020 May 22 10:32:04 CISNXOS9 %OSPF-5-ADJCHANGE:  ospf-10 [10184]  Nbr
10.10.10.11 on Vlan1 went DOWN
```

Remediation:

Enabling the logging of adjacencies is a single line in the OSPF process section. It is globally applied to all OSPF neighbors.

```
switch(config)# router ospf <Process tag>
switch(config-router)# log-adjacency-changes
```

Default Value:

By default changes in OSPF adjacencies are not logged.

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.1.4 Protocol Independent Routing Protections

Some routing protections are independent of the routing protocol, they are recommended in all cases, even if only static routes are configured.

3.1.4.1 If VLAN interfaces have IP addreses, configure anti spoofing / ingress filtering protections (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

If VLAN interfaces have IP addresses, it is important that anti-spoofing protections are in place, to prevent an attacker from spoofing an address that is illegal on that inbound interface.

Rationale:

If an attacker is allowed to "spoof" addresses to the point that packets are permitted to arrive on the incorrect interface, it becomes possible for an attacker to spoof their trust level from a network point of view, for instance to source "inside" addresses from an "outside" interface.

Impact:

The URPF feature uses the same tables as the routing protocol, so the CPU impact of configuring this feature is low. However, logging of high volume URPF attacks (or URPF misconfigurations) can result in:

- higher CPU impacts on the switch
- as higher network utilization on the path to the logging server
- higher disk utilization on the logging server
- higher cpu utilization on the logging server

Because of this, URPF events, especially in higher volumes should be configured to generate a high priority alert in your logging server or SIEM.

Audit:

The "show run ip" command will show all IP interfaces as well as their URPF settings.
All non-loopback interfaces that have IP addresses should have URPF configured (ip verify unicast source).

```
switch# sho run ip
```

```
!Command: show running-config ip
!Running configuration last done at: Sun May 17 13:32:08 2020
!Time: Sun May 17 13:36:49 2020

version 9.3(3) Bios:version
vrf context management
  ip route 0.0.0.0/0 10.17.8.2
  ip route 0.0.0.0/0 192.168.122.1

interface Vlan1
  ip address 10.10.10.10/24
  ip verify unicast source reachable-via rx
```

Remediation:

Apply the command "ip verify unicast source reachable-via rx" to all VLAN interfaces that have IP addresses. This forces the check to verify that the packet is arriving on the correct interface.
The command variant "ip verify unicast source reachable-via any" is not recommended, as it only filters for valid IP addresses. If the device has a default route, then this command variant has no affect.

```
switch(config)# interface Vlan X
switch(config-if)# ip verify unicast source reachable-via rx
```

Default Value:

By default, unicast reverse forwarding protections are not enabled

CIS Controls:

Version 7

6.8 Regularly Tune SIEM

On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.

11.2 Document Traffic Configuration Rules

All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.

3.1.4.2 Create and use a single Loopback Address for Routing Protocol Peering (Manual)

Profile Applicability:

- Level 2

Description:

The use of a loopback interface is recommended for use in all routing protocols. This recommendation describes the configuration of the loopback interface. Routing protocol specific configurations are described under the respective routing protocols.

Rationale:

Loopback interfaces are always up, and so are not dependent on physical interface link state issues (cabling or other link issues for instance). This means traffic sourced from a loopback interface can take any valid path to establish a routing relationship or to route traffic. Loopback interfaces by their nature cannot "flap" (toggle between up and down states). Depending on the error condition, most physical interfaces are susceptible to interface flapping.

Impact:

Using a loopback interface makes a routing device much less susceptible to intermittent or permanent interface failures.

Audit:

```
switch# sho ip int brief | i Lo
Lo0                  10.11.11.1      protocol-up/link-up/admin-up
```

Remediation:

Creating the loopback interface is a simple process. Addressing the loopback, in particular computing the subnet mask will vary by the organization and application. Often smaller subnets can be used for loopbacks, depending on how many potential peers are possible.

```
switch(config)# int loopback 0
switch(config-if)# ip address 10.11.11.1 255.255.255.252
```

In order to use the loopback interface (rather than the closest interface to the routing peer), it must be explicitly configured in the routing protocol. This is described in the recommendations for each respective routing protocol.

Default Value:

By default no loopback interfaces are created on NX-OS devices.

3.1.4.3 Use Unicast Routing Protocols Only (Manual)

Profile Applicability:

- Level 2

Description:

Unicast routing protocols describe the destination routing peers by IP address. Multicast and Broadcast based routing protocols will discover routing neighbors dynamically. Because of this discovery process, a malicious actor can much more easily establish a peering relationship and hijack the routing protocol.

Rationale:

While most routing protocols can be configured with authentication, multicast and broadcast routing protocols have an inherent weakness in their "trust" of any neighbor that advertises or will answer an advertisment.

Impact:

In multicast and broadcast routing protocols, the router (in this case the NX-OS device) will advertise its presence to all devices on a subnet, soliciting other routers using that same protocol. In that situation, an attacker can simply reply to those advertisements and establish a peering relationship. At that point the attacker can inject any route desired, so that traffic for that destination will route through the malicious router, putting the attacker in a "monkey in the middle" position, able to eavesdrop on or change any traffic to or from that destination, then forward it on. Tools such as scapy have well-established attack scripts for most broadcast or multicast routing protocols.

Audit:

In practice, this typically means "do not use RIP or EIGRP, OSPF in their default configuration, use unicast only"
In order to audit for this, check for the "multicast group" keyword for each configured routing protocol. Note that there is in some cases a "-" character in this keyword, also that the word "multicast" does not have consistent upper/lower case from protocol to protocol. For these reasons it is recommended to filter by the phrase "ulticast"

```
switch#show ip <routing protocol> | i ulticast
```

for instance:

```
switch# sho ip rip | i ulticast
RIP port 520, multicast-group 224.0.0.9
switch# sho ip eigrp | i ulticast
  IP proto: 88 Multicast group: 224.0.0.10
```

(note again the inconsistency in upper/lower case in the "multicast group" keywords)

Remediation:

Configure unicast routing only, for instance BGP.

3.1.4.4 Configure HSRP protections (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

HSRP is a valuable redundancy protocol, but like many protocols discussed in this document can be attacked and compromised. HSRP Authentication is recommended to protect against such attacks.

Rationale:

Impact:

By default, HSRP is a clear-text protocol that negotiates which of a number of routing peers host the logical "standby" IP address. Communication to negotiate this is via clear-text messages using the multicast address 224.0.0.2. By default, the protocol is authenticated in cleartext, with a passphrase of "cisco". In a two device HSRP pair, a tool such as SCAPY can be used to impersonate a third participant, advertising itself as an HSRP candidate at a higher priority value.

A successful attack of this type usually results in the malicious actor becoming the default gateway for that subnet, which puts the attacker in the position to inspect all traffic leaving the network, either for eavesdropping or for modifying traffic in transit. Return traffic will not usually be routed through the attacker (unless a second attack is mounted successfully to accomplish this), but intercepting sent traffic gives the attacker the ability to read credentials directly or modify the destination IP address (two common goals). Modifying the destination address allows the attacker to stand up a malicious copy of a target website (for instance, a bank site or paypal), where high value, encrypted credentials can be harvested.

Protecting HSRP with hashed credentials makes this type of attack much more difficult, the attacker must either reverse the hash, or otherwise mount a "pass the hash" attack on the HSRP hosts. Note however that this setting will not prevent all HSRP attacks - it will however make it much more likely that an attack will generate alerts in the log, giving the defending team a good indication that the attack occurred and should be investigated. Automated attacks are often simpler (for instance, may only try the default value), so those may be defeated.

Audit:

The "show running-config hsrp" shows all HSRP configurations. Ensure that MD5 authentication is configured for each HSRP configuration.

```
switch# sho run hsrp

!Command: show running-config hsrp
!Running configuration last done at: Wed May 20 17:24:20 2020
!Time: Wed May 20 17:25:33 2020

version 9.3(3) Bios:version
feature hsrp


interface Vlan1
  hsrp version 2
  hsrp 1
    authentication md5 key-chain HSRP-KEYCHAIN
    name HSRPVLAN1
    preempt
    priority 110
    ip 10.10.10.1
```

Remediation:

First, enable HSRP

```
switch(config)# feature hsrp
```

set the HSRP version to "2" to allow for MD5 encryption (per interface)

```
switch(config)# int vlan 1
switch(config-if)# hsrp version 2
```

Finally, configure the remainder of that interfaces HSRP setup. The key command is of course the "authentication md5" clause

```
switch(config-if)#   hsrp 1
switch(config-if-hsrp)#     authentication md5 key-chain <HSRP-KEYCHAIN>
switch(config-if-hsrp)#     name HSRPVLAN1
switch(config-if-hsrp)#     preempt
switch(config-if-hsrp)#     priority 110
switch(config-if-hsrp)#     ip 10.10.10.1
```

Default Value:

HSRP is not configured by default.

If configured, hashed authentication is not enabled by default (the cleartext value of "cisco" is used by default).

References:

1. https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/6-x/unicast/configuration/guide/l3_cli_nxos/l3_hsrp.html#47962

3.2 Basic Layer 3 Protections

3.2.1 IPv6 Specific Protections

3.2.1.1 Configure RA Guard (Manual)

Profile Applicability:

- Level 1

Description:

The IPv6 RA Guard feature provides support for allowing the network administrator to block or reject unwanted or rogue RA guard messages that arrive at the network device platform. RAs are used by devices to announce themselves on the link. The IPv6 RA Guard feature analyzes these RAs and filters out RAs that are sent by unauthorized devices. In host mode, all RA and router redirect messages are disallowed on the port. The RA guard feature compares configuration information on the Layer 2 (L2) device with the information found in the received RA frame. Once the L2 device has validated the content of the RA frame and router redirect frame against the configuration, it forwards the RA to its unicast or multicast destination. If the RA frame content is not validated, the RA is dropped.

Rationale:

Packets are classified into one of three DHCP type messages. If a packet arriving from DHCP server is a Relay Forward or a Relay Reply, only the device role is checked. In addition, IPv6 DHCP Guard doesn't apply the policy for a packet sent out by the local relay agent running on the switch.

Impact:

With RA Guard in it's default "not configured" state, a malicious actor can send IPv6 RA (Router Advertisement) packets, and present their station as a valid router. This places the attacker in a position where they can send specific traffic to a malicious site (usually to steal credentials). Also an attacker in this position can eavesdrop on or modify traffic in transit, before forwarding it on.

Audit:

Use the command "sho ipv6 nd raguard policy" to audit for this configuration. Ensure that a valid RA Guard Policy is applied to all routed VLANs, unless this causes some operational issue.

```
switch# sho ipv6 nd raguard policy

Policy RAGuardPol01 configuration:
  trusted-port
```

```
  device-role router
  hop-limit minimum 3
  managed-config-flag on
  other-config-flag on
  router-preference maximum high
Policy RAGuardPol01 is applied on the following targets:
Target               Type  Policy               Feature        Target range
vlan 10              VLAN  RAGuardPol01         RA guard       vlan all
```

Notes:
The parameters device-role, hop-limit, managed-config-flag, other-config-flag and router-preference describe various RA Guard checks, and are all optional. These will vary depending on your operational requirements. These statements are shown as examples only, the key audit parameter is that the RAGuard Policy is created and applied to the appropriate VLANs.

Remediation:

In the example below, the RA Guard policy is created, then applied to a VLAN.
Example

```
switch(config)# ipv6 nd raguard policy RAGuardPol01
switch(config-ra-guard)# device-role router
switch(config-ra-guard)# hop-limit minimum 3
switch(config-ra-guard)# managed-config-flag on
switch(config-ra-guard)# other-config-flag on
switch(config-ra-guard)# router-preference maximum high
switch(config-ra-guard)# trusted-port
```

Configuring RA Guard on an interface
Example
switch(config)#vlan configuration 10
switch(config-if) ipv6 nd raguard attach-policy RAGuardPol01

Default Value:

By default, RA Guard is not enabled:

```
switch# sho ipv6 nd raguard policy

RA guard feature not active
```

CIS Controls:

Version 7

11.1 Maintain Standard Security Configurations for Network Devices

Maintain standard, documented security configuration standards for all authorized network devices.

3.2.2 Disable ICMP Redirects on all Layer 3 Interfaces (Manual)

Profile Applicability:

- Level 1

Description:

A redirect packet basically informs the host that there is a better way to get to the destination host or network. This route is then cached on the (victim) host.

For instance, if the default gateway of a host is the NX-OS switch, and the victim host sends a packet to an internet or WAN IP, the NX-OS switch will inform the host that the firewall or WAN router will be a better path. If at some future time, if that firewall or WAN router should fail and trigger a routing change, the route to that failed device will persist in the victim host.

This scenario is only in play if the NX-OS device is the gateway for the victim host, and the Firewall or WAN router (or other next hop device) is also on the same subnet as the victim host. Also, if the next hop device handles its own failover (for instance, using HSRP), there is no routing change, so the "redirect" issue will not be a problem.

This situation is generally a problem only if the path to the destination is handled by a "next hop" mechanism, for instance by a routing protocol or a local route-map, and a backup path exists. In this situation, the route to the target will fail, the route will change to the backup path, and the victim will cache the old route for minutes or hours after the failure.

Rationale:

Audit:

```
switch# show running-config [layer 3 int]
```

For instance, this shows an audit success (redirects disabled)

```
CISNXOS9# sho run int vlan 9

!Command: show running-config interface Vlan9
!Running configuration last done at: Sun Jun 21 13:53:16 2020
!Time: Sun Jun 21 13:53:21 2020

version 9.3(3) Bios:version

interface Vlan9
```

```
  no ip redirects
  ip address 10.99.99.99/24
```

This shows an audit failure (no display, so the default of "redirects enabled" is active)

```
switch# sho run int vlan 9

!Command: show running-config interface Vlan9
!Running configuration last done at: Sun Jun 21 13:49:56 2020
!Time: Sun Jun 21 13:50:45 2020

version 9.3(3) Bios:version

interface Vlan9
  ip address 10.99.99.99/24
```

Remediation:

It is recommended that you perform this task on all Layer 3 Interfaces which have both a primary and a backup routed path to any destination. In particular, the next hop will need to be in the same subnet as the potential victim hosts.

The corollary to this is that if the network is architected such that all layer 3 egress paths are on dedicated or "point to point" segments (with no other hosts on those segments), then the ip redirect issue will never arise.

```
switch(config-if) no ip redirects
```

switch(config)#

Default Value:

IP redirects are enabled by default, and do not appear in the configuration. The desired value is "no ip redirects", which will appear in the configuration.

References:

1. https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/nx-os-software/213841-understanding-icmp-redirect-messages.html#anc17

CIS Controls:

Version 7

11.1 Maintain Standard Security Configurations for Network Devices
Maintain standard, documented security configuration standards for all authorized network devices.

3.2.3 Disable Proxy ARP on all Layer 3 Interfaces (Manual)

Profile Applicability:

- Level 1

Description:

Proxy ARP is the technique in which one host, usually a router, answers ARP requests intended for another machine on a different network segment (vlan or subnet). By faking its identity, the router accepts responsibility for routing packets to the real destination.

Rationale:

Audit:

Since Proxy ARP should be disabled on all routed interfaces, and if disabled it does not show in the configuration, any occurence of the keyword "proxy-arp" in the configuration is an audit failure for this check:

```
switch# Show running-config  | inc proxy-arp
```

More completely, an interface state can be viewed, filtering only for Proxy ARP settings (note that the case of the word "proxy" varies, so the "P" is removed from the filter):

```
switch# sho ip int vlan 1 | i roxy
  IP proxy ARP : disabled
  IP Local Proxy ARP : disabled
```

Or to quickly view the Proxy ARP status of all interfaces:

```
switch# sho ip int | i roxy
  IP proxy ARP : disabled
  IP Local Proxy ARP : disabled
  IP proxy ARP : disabled
  IP Local Proxy ARP : disabled
```

In these last two examples, the desired state is that all entries should be "disabled". The presence of the word "enabled" is an audit failure.

Remediation:

Proxy ARP is disabled on all interfaces by default, and that configuration does not appear in the running or saved configuration. Proxy ARP only appears in the configuration if it is enabled (which is not desired in most cases).
To disable this on an interface if it is enabled:

```
switch(config-if)# no ip proxy-arp
```

for instance:

```
switch(config)# int vlan 9
switch(config-if)# no ip proxy-arp
```

Default Value:

By default the Proxy ARP feature is disabled on all IP Interfaces. This desired and default setting does not appear in the configuration.

This default setting does not appear in the running or saved configurations.

CIS Controls:

Version 7

11.1 Maintain Standard Security Configurations for Network Devices

Maintain standard, documented security configuration standards for all authorized network devices.

3.2.4 Disable IP Directed Broadcasts on all Layer 3 Interfaces (Manual)

Profile Applicability:

- Level 1

Description:

An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for an IP subnet, but which originates from a node that is not itself a part of that destination subnet.

Rationale:

Directed broadcasts can be abused in several ways:

- a volumetric DOS attack against the NX-OS switch itself, the sent volume of data can be much larger than the received request
- a volumetric DOS attack against a third party (often called a "smurf attack")
- a single-packet reconnaissance of a local subnet

We recommend that you disable the ip directed-broadcast command on any interface where they are not required for some reason.

Audit:

```
switch# show running-config | beg [int or vlan]
```

Remediation:

```
switch(config-if)# no ip directed-broadcast
```

References:

1. https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/unicast/config/cisco_nexus7000_unicast_routing_config_guide_8x/configuring_ipv4.html#concept_e5q_4tt_cbb

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.3 Basic Layer 2 Protections

3.3.1 Configure DHCP Trust (Manual)

Profile Applicability:

- Level 1

Description:

You can configure whether DHCP snooping trusts traffic sources. An untrusted source may initiate traffic attacks or other hostile actions. To prevent such attacks, DHCP snooping filters messages from untrusted sources.

In an enterprise network, a trusted source is a device that is under your administrative control. These devices include the switches, routers, and servers in the network. Any device beyond the firewall or outside the network is an untrusted source. Generally, host ports are treated as untrusted sources.

Rationale:

In a service provider environment, any device that is not in the service provider network is an untrusted source (such as a customer switch). Host ports are untrusted sources.

In the Cisco NX-OS device, you indicate that a source is trusted by configuring the trust state of its connecting interface.

The default trust state of all interfaces is untrusted. You must configure DHCP server interfaces as trusted. You can also configure other interfaces as trusted if they connect to devices (such as switches or routers) inside your network. You usually do not configure host port interfaces as trusted.

Impact:

If DHCP Trust is not configured, all ports are trusted to provide DHCP services.

This situation enables a malicious attacker to provide incorrect DHCP information, for instance an attacker could:

- provide a malicious host IP as the default gateway, putting that host into a "Monkey in the Middle" position, able to intercept or modify traffic.
- Provide a malicious host as a proxy, via DHCP option 252 (commonly called a "WPAD attack"). This routes all browser traffic to that malicious host (for browsers that use the system setting for proxy)
- The final scenario is an end-user bringing in a rogue dhcp server in the form of an access point or switch that they've purchased themselves. The impact of this is

usually that the entire subnet will be DOS'd - normally impacted workstations will have a different subnet (192.168.0.0/24 ort 192.168.1.0/24), with the rogue device as the default gateway.

Configuring DHCP trust not only sends an alert to the log server or SIEM, it also puts the rogue DHCP port into ERR-DISABLE mode.

Audit:

```
switch(config)# show running-config dhcp
```

Remediation:

First, enable DHCP Snooping

```
switch(config)#ip dhcp snooping
```

Next, enable DHCP Snooping on target VLANs

```
switch(config)# ip dhcp snooping vlan 100,200,250-252
```

Configure Interface as Trusted

```
switch(config)# interface port-channel 5
switch(config)# ip dhcp snooping trust
```

On a distribution or access switch (for instance in a wiring closet or branch office), typically only the uplink ports are configured as trusted - the ports leading towards the DHCP server On a datacenter switch, especially with virtualization, usually multiple ports are candidates for where the DHCP servers may appear on, all possible ports that may have a DHCP server on them should be trusted.

Default Value:

Untrusted

References:

1. https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_1/nx-os/security/configuration/guide/sec_nx-os-cfg/sec_dhcpsnoop.html

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.3.2 Configure Storm Control (Manual)

Profile Applicability:

- Level 2
- Level 1

Description:

Traffic storm control (also called traffic suppression) allows you to monitor the levels of the incoming broadcast, multicast, and unicast traffic over a 3.9-millisecond interval. During this interval, the traffic level, which is a percentage of the total available bandwidth of the port, is compared with the traffic storm control level that you configured. When the ingress traffic reaches the traffic storm control level that is configured on the port, traffic storm control drops the traffic until the interval ends.

Rationale:

When the traffic exceeds the configured level, you can configure traffic storm control to perform the following optional corrective actions :

Shut down—When ingress traffic exceeds the traffic storm control level that is configured on a port, traffic storm control puts the port into the error-disabled state. To reenable this port, you can use either the shutdown and no shutdown options on the configured interface, or the error-disable detection and recovery feature. You are recommended to use the errdisable recovery cause storm-control command for error-disable detection and recovery along with the errdisable recovery interval command for defining the recovery interval. The interval can range between 30 and 65535 seconds.

Trap—You can configure traffic storm control to generate an SNMP trap when ingress traffic exceeds the configured traffic storm control level. The SNMP trap action is enabled by default. However, storm control traps are not rate-limited by default. You can control the number of traps generated per minute by using the snmp-server enable traps storm-control trap-rate command.

Impact:

This configuration is normally non-impactful - host network interfaces operating normally do not broadcast at the levels that are normally set in this command.

This command is primarily meant to protect the switch and more importantly other hosts in a broadcast domain (VLAN) from a network interface that is malfunctioning, either due to a hardware failure or a driver problem.

Note however that this protection can prevent some malicious activity, for instance VLAN wide DOS attacks, higher volume ARP Cache Poisoning attacks and CAM Table overflow attacks.

Audit:

The storm control levels and measurement methods will vary depending on normal traffic in your environment. Normally the action should be "shutdown", unless the values are in the process of being determined (in which case this is normally set to "trap"). If measuring in percent, remember that these are usually 10Gbps or faster interfaces.
The "show running-config interface" command will display the storm control parameters on one or several interfaces
To show for one interface:

```
switch# sho run interface e1/6

!Command: show running-config interface Ethernet1/6
!Running configuration last done at: Thu May 21 12:25:37 2020
!Time: Thu May 21 12:26:10 2020

version 9.3(3) Bios:version

interface Ethernet1/6
  storm-control broadcast level pps 1000
  storm-control multicast level pps 1000
  storm-control action shutdown
```

To show for all Ethernet interfaces:

```
switch# sho run interface e1/1 - 48
```

To show for all interfaces (which will then include port-channels):

```
switch# sho run interface
```

Remediation:

To set the broadcast limit in percent (multicast limit shown):

```
switch(config)# interface ethernet 1/1
switch(config)# storm-control multicast level 10
```

or to set in packets per second (broadcast limit shown)

```
switch(config)# storm-control broadcast level pps 8000
```

Configure to send SNMP trap if a broadcast limit is exceeded

```
switch(config-if)# storm-control action trap
```

or to place an interface into an ERR-DISABLE state if a broadcast limit is exceeded:

```
switch(config-if)# storm-control action disable
```

Default Value:

not enabled

References:

1. https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/6-x/security/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_Security_Configuration_Guide/b_Cisco_Nexus_9000_Series_NX-OS_Security_Configuration_Guide_chapter_010000.html

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.4 Discovery Protocols

3.4.1 Configure LLDP (Manual)

Profile Applicability:

- Level 1

Description:

LLDP is a discovery protocol that transmits information about the capabilities and current status of a device and its interfaces. LLDP devices use the protocol to solicit information only from other LLDP devices. You can use LLDP to discover and view information about many devices that are directly attached to the switch.

In many situations LLDP is required for normal operation (for instance for auto-provisioning, or for network configuration of VOIP handsets or Wireless Access Points).

LLDP advertises potentially sensitive information, including the current version of NX-OS. For this reason it is recommended that LLDP be disabled or restricted to receive-only on any link that links to equipment not owned by your organization.

In more sensitive environments, in particular in carrier or cloud services environments (where the majority of the endpoints are customer controlled hosts), it is recommended to disable LLDP entirely.

Rationale:

To permit the discovery of non-Cisco devices, the switch also supports the Link Layer Discovery Protocol (LLDP), a vendor-neutral device discovery protocol that is defined in the IEEE 802.1ab standard. LLDP allows network devices to advertise information about themselves to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other.

LLDP advertises potentially sensitive information, including the current version of NX-OS and exposed IP addresses. This information can be used by a malicious actor to identify which vulnerabilities exist on the device, and from there which exploits might be most effective to compromise it. For this reason, enabling LLDP is generally not recommended except for troubleshooting or network discovery purposes. In particular, any ports connected to service provider gear, or any system not owned by your organization should have LLDP explicitly disabled.

In more sensitive environments, disable LLDP globally.

Audit:

To show the global LLDP configuration

```
switch#  sho run lldp

!Command: show running-config lldp
!Running configuration last done at: Tue May 19 16:19:19 2020
!Time: Tue May 19 16:33:51 2020

version 9.3(3) Bios:version
feature lldp
```

To show the LLDP status for all interfaces:

```
switch# sho lldp all
Interface Information: Eth1/8 Enable (tx/rx/dcbx): Y/Y/Y
Interface Information: Eth1/7 Enable (tx/rx/dcbx): Y/Y/Y
Interface Information: Eth1/6 Enable (tx/rx/dcbx): Y/Y/Y
```

To show connected LLDP capable devices (neighbors):

```
switch# sho lldp neighbors
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID            Local Intf      Hold-time  Capability  Port ID
0050.56c0.0001       mgmt0           3601                   0050.56c0.0001
0050.56c0.0003       Eth1/1          3601                   0050.56c0.0003
```

In many environments, LLDP is required. For instance, LLDP send and receive is often required in workstation switches to facilitate the registration of VOIP telephones.

Remediation:

To enable the LLDP feature, then enable LLDP:

```
switch(config)# feature lldp
```

To disable LLDP globally:

```
switch(config)# no feature lldp
```

To disable LLDP on a specific interface - note that transmit and receive capabilities are controlled independently. While in many cases LLDP is not required at all, often only LLDP receive is needed for correct operation.:

```
switch(config)# int Ethernet x/y
switch(config-if)# no lldp transmit
switch(config-if)# no lldp receive
```

Default Value:

LLDP is not enabled by default. If the LLDP feature is enabled, the protocol is enabled for both send and receive on all interfaces by default.

References:

1. https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/system_management/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_System_Management_Configuration_Guide_7x/b_Cisco_Nexus_9000_Series_NX-OS_System_Management_Configuration_Guide_7x_chapter_010010.html

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.4.2 Configure CDP (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

The Cisco Discovery Protocol (CDP) is a media-independent and protocol-independent protocol that runs on all Cisco-manufactured equipment including routers, bridges, access and communication servers, and switches. You can use CDP to discover and view information about all the Cisco devices that are directly attached to the device.

Each device that you configure for CDP sends periodic advertisements to a multicast address. Each device advertises at least one address at which it can receive SNMP messages. The advertisements also contain hold-time information, which indicates the length of time that a receiving device should hold CDP information before removing it. You can configure the advertisement or refresh timer and the hold timer.

CDP advertises potentially sensitive information, including the current version of NX-OS. For this reason it is recommended that CDP be disabled on any link that links to equipment not owned by your organization. In more sensitive environments, in particular in carrier or cloud services environments (where the majority of the endpoints are customer controlled hosts), it is recommended to disable CDP entirely

Rationale:

CDP advertises potentially sensitive information, including the current version of NX-OS. This information can be used by a malicious actor to identify which vulnerabilities exist on the device, and from there which exploits might be most effective to compromise it. For this reason, enabling CDP is generally not recommended except for troubleshooting or network discovery purposes. In particular, any ports connected to service provider gear, or any system not owned by your organization should have CDP explicitly disabled.

In more sensitive environments, disable CDP globally.

Audit:

To show all CDP definitions, for all interfaces:

```
switch# sho cdp all
```

To show CDP status for any single interface:

```
switch# sho cdp interface Ethernet x/y
Ethernetx/y is up
    CDP disabled globally
    CDP enabled on interface
    Refresh time is 60 seconds
    Hold time is 180 seconds
```

Remediation:

Enabling CDP Globally

```
switch(config)# cdp enable
```

Enabling on one interface

```
switch(config)# int Ethernet x/y
switch(config-if)# cdp enable
```

To disable CDP globally:

```
switch(config-if)# no cdp enable
```

To disable CDP on one interface only:

```
switch(config)# int Ethernet x/y
switch(config-if)# no cdp enable
```

Default Value:

CDP is enabled by default, and is enabled on all interfaces by default.

References:

1. https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/system_management/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_System_Management_Configuration_Guide_7x/b_Cisco_Nexus_9000_Series_NX-OS_System_Management_Configuration_Guide_7x_chapter_0101.html

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.5 Fiber Channel / Fiber Channel over Ethernet

3.5.1 Basic Fiber Channel Configuration (Manual)

Profile Applicability:

- Level 2

Description:

Fibre Channel over Ethernet (FCoE) encapsulation allows a physical Ethernet cable to carry standard Fibre Channel traffic within Ethernet frames. In Cisco Nexus devices, an FCoE-capable physical Ethernet interface can carry traffic for one virtual Fibre Channel (vFC) interface. If FCoE functionality is not required, this functionality should be disabled. Note also that this is a licensed feature, so is not available without a purchased license.

Rationale:

Audit:

```
switch# sho interface fcoe
Ethernet1/1 is FCoE down
Ethernet1/2 is FCoE UP
Ethernet1/3 is FCoE down
Ethernet1/4 is FCoE down
```

Displays basic FCoE status

```
switch# sho fcoe
Global FCF details
        FCF-MAC is 8c:60:4f:a6:29:60
        FC-MAP is 0e:fc:00
        FCF Priority is 128
        FKA Advertisement period for FCF is 8 seconds
```

Displays full FCoE database:

```
switch# show fcoe database
```

Displays the FCoE settings for an interface or all interfaces.

```
switch# show interface [interface number] fcoe
```

Displays LLDP configuration.

```
switch# show lldp neighbors
```

Remediation:

Enable the FCoE feature globally on the switch:

```
switch(config)# feature fcoe
FC license checked out successfully

fc_plugin extracted successfully
FC plugin loaded successfully
FCoE manager enabled successfully
FC enabled on all modules successfully
Warning: Ensure class-fcoe is included in qos policy-maps of all types
```

Enable FCoE on a specific port (not required on all models):

```
switch(config)# interface ethernet x/y
switch(config-if)# fcoe mode on
```

set the priority flow mode on a specific port:

```
switch(config-if)# priority-flow-control mode auto
```

FCoE also requires the DCBX (Data Center Bridging Exchange) protocol, which is used to negotiate capabilities between the FCOE endpoints. DCBX is an extension of LLDP, and LLDP is enabled globally and on all interfaces by default.
If LLDP is disabled on any particular interface, it can be re-enabled as:

```
switch(config-if)# int Ethernet x/y
switch(config-if)# lldp transmit
switch(config-if)# lldp receive
```

Default Value:

The FCoE feature is not enabled by default. LLDP is enabled globally and on all interfaces by default, so if FCoE is enabled then DCBX is enabled by default

CIS Controls:

Version 7

11.1 Maintain Standard Security Configurations for Network Devices

Maintain standard, documented security configuration standards for all authorized network devices.

3.5.2 Configure FCoE Zoning (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

Cisco uses a construction called a "VSAN" (analagous to a VLAN) which is used to restrict access between hosts and SAN resources. In restrictive cases, a typical VSAN will include two entries for the two host FCoE interfaces, and two entries for the SAN Controller interfaces (usually an FCoE SAN will have at least two). In the most restrictive case, the FCOE infrastructure will be split into two fabrics, and zones can hold as few as 2 entries (one for the host and one for the SAN controller on that fabric).

Rationale:

Impact:

This configuration limits the reconnaissance available to a compromised or malicious host. Without configuring Zoning, a compromised host can collect the FCoE information from all other hosts in the same VSAN. It can then use that information to impersonate any of these hosts, and access their respective LUNs (unless some other control prevents that).

Note that in Virtualized environments and in most Cluster architectures, multiple hypervisor hosts will access the a common set of LUNs on the SAN. In these situations the VSAN can have significantly more members (all host interfaces as well as all target SAN controller interfaces), since the reconnaissance and impersonation risks are somewhat lessened - you would need a compromised hypervisor to attack another hypervisor. While this risk is non-zero, it is understood that hypervisors typically (hopefully) have more strict protections than many other physical hosts.

In addition, risk occurs if different server operating systems are in play. The most common issue is that if a Windows host can mount a volume that is partitioned for Linux or VMware ESXi, Windows will ask a logged in administrator for permission to "sign" that volume. If the administrator selects "Yes", then that volume will no longer be readable by the Linux or ESXi host(s).

At a minimum, hypervisors should not share a zone with other physical hosts. Physical hosts should not share zones with each other. Hosts with different operating systems or

incompatible filesystems should never share the same zone. In the best case, the "one host / one SAN controller / one zone" rule is the safest approach.

Audit:

```
switch# sho vsan 101
vsan 101 information
         name:HOST_X_SAN_Y  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:down

switch# sho vsan membership
vsan 1 interfaces:


vsan 100 interfaces:


vsan 101 interfaces:
    vfc1001           vfc1002

vsan 4079(evfp_isolated_vsan) interfaces:


vsan 4094(isolated_vsan) interfaces:

switch# sho int vfc 1001
vfc1001 is down (Administratively down)
    Bound MAC is 00:01:0b:00:00:02
    Hardware is Ethernet
    Port WWN is 23:e8:8c:60:4f:a6:29:bf
    Admin port mode is F, trunk mode is on
    snmp link state traps are enabled
    Port vsan is 101
    1 minute input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    1 minute output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      0 frames input, 0 bytes
        0 discards, 0 errors
      0 frames output, 0 bytes
        0 discards, 0 errors
    last clearing of "show interface" counters never


switch# sho fcoe database

------------------------------------------------------------------------------
--
INTERFACE       FCID            PORT NAME               MAC ADDRESS
------------------------------------------------------------------------------
--
```

Remediation:

Create a VSAN. Give it a meaningful name

```
switch(config-if)# vsan database
switch(config-vsan-db)# vsan 101
switch(config-vsan-db)# vsan 101 name HOST_X_SAN_Y
```

Create Virtual Fiber Channel Interfaces.

```
switch(config)# interface vfc 1001
switch(config-if)# bind mac-address 00:01:0b:00:00:02
switch(config-if)# int vfc 1002
switch(config-if)# bind mac-address 00:01:0b:00:00:08
switch(config)# int vfc 1003
switch(config-if)# bind interface e 1/4
```

Add VFC interfaces to the VSAN

```
switch(config-if)# vsan database
switch(config-vsan-db)# vsan 101 interface vfc 1001
switch(config-vsan-db)# vsan 101 interface vfc 1002
switch(config-vsan-db)# vsan 101 interface vfc 1003
```

Default Value:

By default, if FCoE is not enabled. If FCoE is enabled and configured, if a single VSAN is configured all FCoE devices have access to all other FCOE devices.

CIS Controls:

Version 7

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

4 Operations and Management

4.1 Configure Local Configuration Backup Schedule (Manual)

Profile Applicability:

- Level 1

Description:

Using the job scheduler function allows the user to automate backups. This ensures that regular backups are created.

Rationale:

Having current backups creates an environment where the user can roll back a config in the event of configuration failure. Additionally in the event of a compromise a recent backup can get the device back up to running condition in a small matter of time.

Audit:

```
switch(config)# sho scheduler job
```

Remediation:

```
switch(config)# scheduler job name [local backup]
switch(config-job)#copy running-config startup-config
```

Set up timetable for this backup.

```
switch(config)# scheduler schedule name [backups]
switch(config-schedule)# schedule name [backups]
switch(config-schedule)# time weekly [day 00:00]
```

Default Value:

not enabled

References:

1. https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/6-x/system_management/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_System_Management_Configuration_Guide/sm_8scheduler.html

CIS Controls:

Version 7

10.2 Perform Complete System Backups

Ensure that each of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.

11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes

Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.

4.2 Configure a Remote Backup Schedule (Manual)

Profile Applicability:

- Level 1

Description:

NX-OS can be configured to initiate remote backups using scheduled jobs. This recommendation can also be satisfied (and likely satisfied better) using a host based backup tool, using SSH or SCP.

Rationale:

Remote backups are preferred over local backups, as an attacker that has compromised a device also has full access to any locally stored files (which local backups are). In that situation, an attacker can modify or delete the stored backups, impeding any recovery or remediation efforts.

Impact:

A host-based backup solution is preferred over one implemented locally. Locally configured backups have several security issues. By protocol, they are:

- TFTP - cleartext, which is susceptible to interception or modification over the wire and the target filesystem allows unauthenticated writes (and usually unauthenticated reads)
- FTP or HTTP - cleartext, which is susceptible to interception or modification over the wire. Credentials are embedded in the job configuration
- HTTPS, SCP, SFTP: encrypted, but credentials are still embedded in the job configuration

Audit:

```
switch# sho scheduler config
```

Remediation:

Note that this first example job uses tftp for backups. The risk here is that the backup is sent in clear-text, so can be intercepted and/or modified in transit.

```
switch(config)# Scheduler job name [backup-cfg]
switch(config-job)copy running-config tftp://1.2.3.4/$(SWITCHNAME)-
cfg.$(TIMESTAMP) vrf management
```

This example job uses SCP. The risk here is that the credentials need to be embedded in the configuration, so can be recovered if the backup repository is compromised. As this is true for all local passwords, the risk may be deemed low in some organizations.

```
switch(config)# scheduler aaa-authentication username <username> password
<some complex password>

switch(config)# Scheduler job name <backup-cfg>
switch(config-job)copy running-config scp://1.2.3.4/$(SWITCHNAME)-
cfg.$(TIMESTAMP) vrf management
```

Whatever the protocol, set timetable for this backup

```
switch(config)# scheduler schedule name [backups]
switch(config-schedule)# schedule name [backups]
switch(config-schedule)# job name <backup-cfg>
switch(config-schedule)# time weekly [day 00:00]
```

While this can certainly work, if the backup server IP should ever change, the effort to fix this across multiple switches can be both error-prone and time-intensive. It is normally recommended to backup configurations from the backup server to the NX-OS switch over SSH or SCP, rather than from the switch to the host. As this config (host to switch) resides on the remote host, it cannot be audited from the switch.

CIS Controls:

Version 7

10.2 Perform Complete System Backups

Ensure that each of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.

11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes

Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.

4.3 Configure Alerts on all Configuration Changes (Manual)

Profile Applicability:

- Level 2

Description:

This is not easily implemented directly on the switch. Changes should ideally be backed up remotely, and a "diff" process to highlight any changes in successive configurations is a good process to implement.

Rationale:

Change Control processes are ubiquitous in the industry. Especially with a text-based configuration such as most network devices have, it is easy to extract the exact changes from one version of the saved or running configuration to the next. This can then be correlated back to the change control process, to see:

- Did any and all approved changes get executed?
- Did any unapproved changes get executed?
- Relating this back to the syslogs created by named user logins, did the change happen within the correct window?
- Also relating back to the syslogs created by named user logins, did the correct person make the change? (see the AAA section, and named administrative users)
- Is there a pattern of any one or more administrators making unapproved or outside of window changes?

Impact:

A formal change control process can manage conflicts in changes nicely, especially between disparate sections of the infrastructure. For instance, the situation where "a server upgrade failed because the firewall changes interrupted the VPN session" is much less likely to occur if all changes are reviewed in advance.

In addition, changes made without planning tend to result in the "testing in prod" scenario, ending up with a much higher ratio of service interruptions.

Audit:

This should be an automated process running on the host that is the repository for daily backups. An assessment should be made on that host.

Remediation:

This is not a process that typically runs on the switch, there is no on-switch remediation.

Default Value:

None.

CIS Controls:

Version 7

11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes
Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**Management Plane**		
1.1	**Local Authentication, Authorization and Accounting (AAA) Rules**		
1.1.1	Configure AAA Authentication - TACACS (Automated)	☐	☐
1.1.2	Configure AAA Authentication - RADIUS (Automated)	☐	☐
1.1.3	Configure AAA Authentication - Local SSH keys (Manual)	☐	☐
1.2	**Access Rules**		
1.2.1	Ensure Idle Timeout for Login Sessions is set to 5 minutes (Automated)	☐	☐
1.2.2	Restrict Access to VTY Sessions (Manual)	☐	☐
1.3	**Password Rules**		
1.3.1	Enable Password Complexity Requirements for Local Credentials (Manual)	☐	☐
1.3.2	Configure Password Encryption (Manual)	☐	☐
1.3.3	Set password lifetime, warning time and grace time for local credentials (Manual)	☐	☐
1.3.4	Set password length for local credentials (Manual)	☐	☐
1.4	**SNMP Rules**		
1.4.1	If SNMPv2 is in use, use a Complex Community String (Manual)	☐	☐
1.4.2	If SNMPv2 is in use, set Restrictions on Access (Manual)	☐	☐
1.4.3	Configure SNMPv3 (Manual)	☐	☐
1.4.4	Configure SNMP Traps (Manual)	☐	☐
1.4.5	Configure SNMP Source Interface for Traps (Manual)	☐	☐
1.4.6	Do not Configure a Read Write SNMP Community String (Manual)	☐	☐
1.5	**Logging**		
1.5.1	Ensure Syslog Logging is configured (Manual)	☐	☐
1.5.2	Log all Successful and Failed Administrative Logins (Automated)	☐	☐
1.5.3	Configure Netflow on Strategic Ports (Manual)	☐	☐
1.5.4	Configure Logging Timestamps (Manual)	☐	☐
1.6	**Time Services**		
1.6.1	Configure at least 3 external NTP Servers (Manual)	☐	☐
1.6.2	Configure a Time Zone (Manual)	☐	☐
1.6.3	If a Local Time Zone is used, Configure Daylight Savings (Manual)	☐	☐
1.6.4	Configure NTP Authentication (Manual)	☐	☐

1.7	**Configure Banners**		
1.7.1	Configure an MOTD (Message of the day) Banner (Manual)	☐	☐
1.7.2	Configure an EXEC Banner (Manual)	☐	☐
1.8	**Other Services and Accesses**		
1.8.1	Disable Power on Auto Provisioning (POAP) (Manual)	☐	☐
1.8.2	Disable iPXE (Pre-boot eXecution Environment) (Manual)	☐	☐
1.9	Use Dedicated "mgmt" Interface and VRF for Administrative Functions (Manual)	☐	☐
2	**Control Plane**		
2.1	**Global Service Rules**		
2.1.1	Configure Control Plane Policing (Manual)	☐	☐
3	**Data Plane**		
3.1	**Secure Routing Protocols**		
3.1.1	**EIGRP**		
3.1.1.1	Configure EIGRP Authentication on all EIGRP Routing Devices (Manual)	☐	☐
3.1.1.2	Configure EIGRP Passive interfaces for interfaces that do not have peers (Manual)	☐	☐
3.1.1.3	Configure EIGRP log-adjacency-changes (Manual)	☐	☐
3.1.2	**BGP**		
3.1.2.1	Configure BGP to Log Neighbor Changes (Manual)	☐	☐
3.1.2.2	If Possible, Limit the BGP Routes Accepted from Peers (Manual)	☐	☐
3.1.2.3	Configure BGP Authentication (Manual)	☐	☐
3.1.3	**OSPF**		
3.1.3.1	Set Interfaces with no Peers to Passive-Interface (Manual)	☐	☐
3.1.3.2	Authenticate OSPF peers with MD5 authentication keys (Manual)	☐	☐
3.1.3.3	Log OSPF Adjacency Changes (Manual)	☐	☐
3.1.4	**Protocol Independent Routing Protections**		
3.1.4.1	If VLAN interfaces have IP addreses, configure anti spoofing / ingress filtering protections (Manual)	☐	☐
3.1.4.2	Create and use a single Loopback Address for Routing Protocol Peering (Manual)	☐	☐
3.1.4.3	Use Unicast Routing Protocols Only (Manual)	☐	☐
3.1.4.4	Configure HSRP protections (Manual)	☐	☐
3.2	**Basic Layer 3 Protections**		
3.2.1	**IPv6 Specific Protections**		
3.2.1.1	Configure RA Guard (Manual)	☐	☐
3.2.2	Disable ICMP Redirects on all Layer 3 Interfaces (Manual)	☐	☐
3.2.3	Disable Proxy ARP on all Layer 3 Interfaces (Manual)	☐	☐
3.2.4	Disable IP Directed Broadcasts on all Layer 3 Interfaces (Manual)	☐	☐

3.3	**Basic Layer 2 Protections**		
3.3.1	Configure DHCP Trust (Manual)	☐	☐
3.3.2	Configure Storm Control (Manual)	☐	☐
3.4	**Discovery Protocols**		
3.4.1	Configure LLDP (Manual)	☐	☐
3.4.2	Configure CDP (Manual)	☐	☐
3.5	**Fiber Channel / Fiber Channel over Ethernet**		
3.5.1	Basic Fiber Channel Configuration (Manual)	☐	☐
3.5.2	Configure FCoE Zoning (Manual)	☐	☐
4	**Operations and Management**		
4.1	Configure Local Configuration Backup Schedule (Manual)	☐	☐
4.2	Configure a Remote Backup Schedule (Manual)	☐	☐
4.3	Configure Alerts on all Configuration Changes (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version