# Integrity Check of Candidate Config

This chapter describes how to perform integrity check of Candidate Config.

This chapter includes the following sections:



## About Candidate Config

Candidate config is a subset of the running-config which checks whether the Candidate config exists in the running-config without any additions or modifications or deletions.

To check the integrity of the candidate config, use the following commands:

- `show diff running-config`
- `show diff startup-config`

For more information on the CLIs, refer to Performing Integrity Check for Candidate Config, on page 7.

## Guidelines and Limitations for Candidate Config Integrity Check

Candidate config integrity check has the following guidelines and limitations:

- Beginning with Cisco NX-OS Release 10.2(3)F, Candidate config integrity check option is introduced on all Cisco Nexus switches.
- If you must perform an integrity check on a full running configuration as input instead of a partial config, then it is recommended not to use the **partial** keyword.
- The line numbers that are displayed in the generated running config do not match with the candidate config as they are internally generated one.
- If there is any difference between the configuration of running and candidate, then it is displayed inline as output.

- If the whole block of configuration in the candidate file is a new addition, it will be appended at the end of the generated running config.
- When the candidate config has an SNMP or an AAA user CLI with clear-text password, the SNMP user is seen as a diff even when the user is already configured.
- Beginning from Cisco NX-OS Release 10.4(3)F, you can also use polymorphic commands in candidate configuration to perform partial diff.
- EIGRP address family IPv4 configs are recommended to configure under the EIGRP address family hierarchy and not under the router mode hierarchy in the candidate file, before running a partial diff.
- If the target/candidate file has a default command (for example, `- log-neighbor-warnings;`) configured directly under the **router eigrp** mode and not one of its submodes, that is, **address-family ipv4 unicast** or **address-family ipv6 unicast**, then partial-diff shows + displayed in the output of the default command (for example, `+ log-neighbor-warnings`) in the diff.
- For noncase sensitive commands, if there is a letter case distinction between the commands in the running config and candidate-config files, then the output of **partial diff** displays both the commands due to the difference in letter case.
- Cleartext passwords are allowed in case of partial diff candidate CONFIG_FILE as the user database gets synced between SNMP and AAA (Security).
- Configuration profile, maintenance profile (mmode) and scheduler mode configurations are not supported.

### Guidelines and Limitations for Partial Diff of Default Commands for Multicast Components

The content of this section is applicable from Cisco NX-OS Release 10.4(3)F.

If the default commands of multicast components are present in the candidate CONFIG_FILE, they are seen in show diff as follows:

| Multicast Component | Default Commands in show diff |
|---|---|
| PIM | `ip access-list copp-system-p-acl-pim`<br>`10 permit pim any 224.0.0.0/24`<br>`20 permit udp any any eq pim-auto-rp`<br>`ip access-list copp-system-p-acl-pim-mdt-join`<br>`ip access-list copp-system-p-acl-pim-reg`<br>`10 permit pim any any` |
| PIM6 | `ipv6 access-list copp-system-p-acl-pim6`<br>`10 permit pim any ff02::d/128`<br>`20 permit udp any any eq pim-auto-rp`<br>`ipv6 access-list copp-system-p-acl-pim6-reg`<br>`10 permit pim any any` |
| IGMP | `ip access-list copp-system-p-acl-igmp`<br>`10 permit igmp any 224.0.0.0/3`<br>`class-map copp-system-p-class-normal-igmp` |
| MLD | `ipv6 access-list copp-system-p-acl-mld`<br>`10 permit icmp any any mld-query`<br>`20 permit icmp any any mld-report`<br>`30 permit icmp any any mld-reduction`<br>`40 permit icmp any any mldv2` |

### Guidelines and Limitations for show diff running-config *file_url* [unified] [partial ] [merged] Command

- When using the **unified**, **partial**, and **merged** option to review the differences for the following PBR commands, the diff outputs are as mentioned below:
  - **set ip next-hop**
  - **set ip default next-hop**
  - **set ip default vrf next-hop**
  - **set ipv6 next-hop**
  - **set ipv6 default next-hop**
  - **set ipv6 default vrf next-hop**

1. If the candidate next-hops are a subset of running next-hops (in the same order and sequence), and candidate additive flags are a subset of running flags, then the diff output is empty as shown in the following table:

| Candidate Config | Running Config | Partial Unified Merged Diff Output |
|---|---|---|
| `route-map rmap1 permit 10`<br>`set ip next-hop 1.1.1.1`<br>`2.2.2.2 load-share` | `route-map rmap1 permit 10`<br>`set ip next-hop 1.1.1.1`<br>`2.2.2.2 3.3.3.3 load-share`<br>`force-order` | <no-diff> |

2. If the candidate next-hops are a subset of running next-hops (in the same order and sequence), and the candidate has some extra additive flags which are not present in running config, then the diff output appends any additional flags present in the candidate config to the running config, similar to command line behavior as shown in the following table:

| Candidate Config | Running Config | Partial Unified Merged Diff Output |
|---|---|---|
| `route-map rmap1 permit 10`<br>`set ip next-hop 1.1.1.1`<br>`2.2.2.2 load-share`<br>`force-order` | `route-map rmap1 permit 10`<br>`set ip next-hop 1.1.1.1`<br>`2.2.2.2 3.3.3.3 load-share`<br>`drop-on-fail` | `route-map rmap1 permit 10`<br>`- set ip next-hop 1.1.1.1`<br>`2.2.2.2 3.3.3.3 load-share`<br>`drop-on-fail`<br>`+ set ip next-hop 1.1.1.1`<br>`2.2.2.2 3.3.3.3 load-share`<br>`force-order drop-on-fail` |

3. If candidate next-hops are not a subset of running next-hops (in the same order and sequence), and the candidate and running record can have any additive flag, then the diff output indicates this with a '–' for the running config record and a '+' for the candidate config record.

   This distinction is important, particularly when using with PBR commands, where the sequence of next-hops is critical. Even if the next-hops IP addresses are identical, their order affects functionality.

   For example, '1.1.1.1 2.2.2.2' is different from '2.2.2.2 1.1.1.1'.

**Important** If there is an additive flag in the running config that you wish to retain after merging with the candidate config, you must explicitly include that flag in the candidate config. This ensures that the needed flags are preserved in the final, merged configuration.

| Candidate Config | Running Config | Partial Unified Merged Diff Output |
|---|---|---|
| route-map rmap1 permit 10<br>set ip next-hop 1.1.1.1<br>2.2.2.2 load-share<br>drop-on-fail | route-map rmap1 permit 10<br>set ip next-hop 2.2.2.2<br>1.1.1.1 load-share<br>force-order | route-map rmap1 permit 10<br>- set ip next-hop 2.2.2.2<br>1.1.1.1 load-share<br>force-order<br>+ set ip next-hop 1.1.1.1<br>2.2.2.2 load-share<br>drop-on-fail |

- When **Partial Unified** or **Partial Unified Merged** option is used, all the PBR commands are mutually exclusive and cannot coexist within the same parent route-map. Therefore, if a candidate configuration specifies multiple mutually exclusive PBR commands under a single route-map, only the last command variant will be shown in the partial diff output.

  Example-1: In this example, the candidate configuration includes multiple PBR commands under a single route-map **rmap1**:

  ```
  route-map rmap1 permit 10
    set ip next-hop 1.1.1.1 2.2.2.2
    set ipv6 next-hop 3::3
    set ip next-hop verify-availability 4.4.4.4
    set ip next-hop verify-availability 5.5.5.5
    set ip vrf green next-hop 6.6.6.6
    set ip vrf blue next-hop 7.7.7.7 8.8.8.8
  ```

  Before the generation of the partial-diff output, the above candidate configuration is automatically converted to the following:

  ```
  route-map rmap1 permit 10
    set ip vrf green next-hop 6.6.6.6
    set ip vrf blue next-hop 7.7.7.7 8.8.8.8
  ```

  Example-2: In this example, the candidate configuration includes multiple 'set ip next-hop verify-availability' commands with different track IDs specified for the route-map **rmap2**. Since track IDs cannot be modified for the same next-hop, these commands are mutually exclusive:

  ```
  route-map rmap2 permit 10
    set ip next-hop verify-availability 1.1.1.1 track 1
    set ip next-hop verify-availability 2.2.2.2 track 20
    set ip next-hop verify-availability 2.2.2.2 track 30
    set ip next-hop verify-availability 2.2.2.2 track 40
    set ip next-hop verify-availability 3.3.3.3 track 3
  ```

  Before generating the partial-diff output, the system will automatically consolidate these commands by retaining only the last **set ip next-hop verify-availability** command for each next-hop IP address as shown below:

  ```
  route-map rmap2 permit 10
    set ip next-hop verify-availability 1.1.1.1 track 1
    set ip next-hop verify-availability 2.2.2.2 track 40
    set ip next-hop verify-availability 3.3.3.3 track 3
  ```

- When the **Partial Unified Merged** option is used, to review the differences for the **verify-availability** command variants, the track ID for a given next-hop is not modifiable.

  Therefore, if the candidate and running configurations contain the same next-hop but have different track IDs under the same parent route-map, the candidate record cannot simply be merged with the running record, as per command line behavior. Therefore, to apply the candidate record with different track ID for the same next-hop, the corresponding running config record must be removed first ( '–' for the running

configuration record in the diff) and then when the candidate record is merged, it will be appended at the end of the last record under the same parent route-map ('+' for the candidate config record).

The following table shows the sample candidate and running configuration with the **Partial Unified Merged** output for different use cases as mentioned below:

1. If the track ID is different for the same next-hop under candidate and running config, then the diff output is as shown in the following table:

| Candidate Config | Running Config | Partial Unified Merged Diff Output |
|---|---|---|
| route-map rmap1 permit 10<br>  set ip next-hop<br>verify-availability 1.1.1.1<br> track 1<br>  set ip next-hop<br>verify-availability 2.2.2.2<br> track 20<br>  set ip next-hop<br>verify-availability 3.3.3.3<br> track 3 load-share | route-map rmap1 permit 10<br>  set ip next-hop<br>verify-availability 1.1.1.1<br> track 1<br>  set ip next-hop<br>verify-availability 2.2.2.2<br> track 2<br>  set ip next-hop<br>verify-availability 3.3.3.3<br> track 3 load-share | route-map test permit 10<br>  set ip next-hop<br>verify-availability 1.1.1.1<br>track 1<br> - set ip next-hop<br>verify-availability 2.2.2.2<br>track 2<br>  set ip next-hop<br>verify-availability 3.3.3.3<br>track 3<br> + set ip next-hop<br>verify-availability 2.2.2.2<br>track 20 load-share |

2. If track ID is not present under candidate config but present in running config for the same next-hop, then the diff output is empty as shown in the following table:

| Candidate Config | Running Config | Partial Unified Merged Diff Output |
|---|---|---|
| route-map rmap1 permit 10<br>  set ip next-hop<br>verify-availability 1.1.1.1<br> track 1<br>  set ip next-hop<br>verify-availability 2.2.2.2<br><br>  set ip next-hop<br>verify-availability 3.3.3.3<br> track 3 | route-map rmap1 permit 10<br>  set ip next-hop<br>verify-availability 1.1.1.1<br> track 1<br>  set ip next-hop<br>verify-availability 2.2.2.2<br> track 2<br>  set ip next-hop<br>verify-availability 3.3.3.3<br> track 3 | no-diff |

3. If track ID is not present under running config but present in candidate config for the same next-hop, then the diff output is as shown in the following table:

| Candidate Config | Running Config | Partial Unified Merged Diff Output |
|---|---|---|
| route-map rmap1 permit 10<br>  set ip next-hop<br>verify-availability 1.1.1.1<br> track 1<br>  set ip next-hop<br>verify-availability 2.2.2.2<br> track 20<br>  set ip next-hop<br>verify-availability 3.3.3.3<br> track 3 | route-map rmap1 permit 10<br>  set ip next-hop<br>verify-availability 1.1.1.1<br> track 1<br>  set ip next-hop<br>verify-availability 2.2.2.2<br><br>  set ip next-hop<br>verify-availability 3.3.3.3<br> track 3 | route-map rmap1 permit 10<br>  set ip next-hop<br>verify-availability 1.1.1.1<br>track 1<br> - set ip next-hop<br>verify-availability 2.2.2.2<br>  set ip next-hop<br>verify-availability 3.3.3.3<br>track 3<br> + set ip next-hop<br>verify-availability 2.2.2.2<br>track 20 |

### Guidelines and Limitations for Partial Diff of RPM Commands

The content of this section is applicable from Cisco NX-OS Release 10.4(3)F.

When using the unified, partial, and merged option to review the differences for the following RPM commands, the diff outputs are as follows:

- In the candidate configuration, the RPM commands will undergo syntactic validation as reflected in the diff output. However, semantic validation will not be performed in the diff output. It is the user's responsibility to ensure that the commands in the candidate configuration are semantically accurate.

  If the command in the Candidate-config is semantically incorrect, the diff may incorrectly indicate that the command is executable, but in actual it may not.

- Ensure that you provide the sequence number mandatorily for the following commands in the Candidate-config file:
  - **ip prefix-list list-name seq** *seq* {**deny** | **permit**} *prefix*
  - **ipv6 prefix-list list-name seq** *seq* {**deny** | **permit**} *prefix*
  - **mac-list list-name seq** *seq* {**deny** | **permit**} *prefix*
  - **ip community-list** {**standard** | **expanded**} *list-name* seq *seq* {**deny** | **permit**} *expression*
  - **ip extcommunity-list** {**standard** | **expanded**}*list-name* seq *seq* {**deny** | **permit**} *expression*
  - **ip large-community-list** {**standard** | **expanded**} *list-name* seq *seq* {**deny** | **permit**} *expression*
  - **ip-as-path access-list** *list-name* seq *seq* {**deny** | **permit**} *expression*

- When the following commands include an expression string that has spaces enclosed in quotes within the Candidate-config, there will be no differences displayed in the diff output:
  - **ip community-list expanded** *list-name* seq *seq* {**deny** | **permit**} *expression*
  - **ip extcommunity-list expanded** *list-name* seq *seq* {**deny** | **permit**} *expression*
  - **ip large-community-list expanded** *list-name* seq *seq* {**deny** | **permit**} *expression*
  - **ip-as-path access-list** *list-name* seq *seq* {**deny** | **permit**} *expression*

| Candidate Config | Running Config | Partial Unified [Merged] Diff Output |
|---|---|---|
| `ip community-list expanded list_abc seq 10 permit "1:1 "` | `ip community-list expanded list_abc seq 10 permit "1:1"` | `no-diff` |
| `ip extcommunity-list expanded list_abc seq 10 permit "1:1  "` | `ip extcommunity-list expanded list_abc seq 10 permit "1:1"` | `no-diff` |
| `ip large-community-list expanded list_abc seq 10 permit "1:1:1   "` | `ip large-community-list expanded list_abc seq 10 permit "1:1:1"` | `no-diff` |
| `ip as-path access-list list_abc seq 10 permit "1 "` | `ip as-path access-list list_abc seq 10 permit "1"` | `no-diff` |

# Performing Integrity Check for Candidate Config

To perform the integrity check, use the following commands:

### Before you begin

**Note** Before performing the integrity check, ensure that the running config and the candidate config belong to the same image version.

### SUMMARY STEPS

1. **show diff running-config** *file_url* [**unified**] [**partial**] [**merged**]
2. **show diff startup-config** *file_url* [ **unified** ]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **show diff running-config** *file_url* [**unified**] [**partial**] [**merged**]<br>**Example:**<br>`switch# show diff running-config bootflash:candidate.cfg partial unified` | Displays the differences between the running and user given candidate config.<br>• *file_url*: File path to compare with.<br>• **unified**: Displays the difference between running and user configuration in unified format.<br>• **partial**: Enter **partial** only if user configuration file is partial and not a full configuration.<br>• **merged**: Enter **merged** only if sub-commands need to be merged instead of replace. |
| **Step 2** | **show diff startup-config** *file_url* [ **unified** ]<br>**Example:**<br>`switch# show diff startup-config bootflash:candidate.cfg unified` | Displays the differences between the startup and user given candidate config.<br>• *file_url*: File path to compare with.<br>• **unified**: Displays the difference between startup and user configuration in unified format. |

# Examples of Integrity Check

### No Difference Between Running and Candidate Config

```
switch# show diff running-config bootflash:base_running.cfg
switch#
```

### Difference Between Running and Candidate

```
switch# show diff running-config bootflash:modified-running.cfg unified
--- running-config
+++ User-config
@@ -32,11 +32,11 @@

interface Ethernet1/1
   mtu 9100
   link debounce time 0
   beacon
-  ip address 2.2.2.2/24
+  ip address 1.1.1.1/24
   no shutdown

interface Ethernet1/2

interface Ethernet1/3
switch#
```

### Difference Between Running and Partial Candidate

```
switch# show file bootflash:intf_vlan.cfg
interface Vlan101
  no shutdown
  no ip redirects
  ip address 1.1.2.1/24 secondary
  ip address 1.1.1.1/24
switch#
switch# show diff running-config bootflash:intf_vlan.cfg partial unified
--- running-config
+++ User-config
@@ -3897,10 +3883,14 @@
   mtu 9100
   ip access-group IPV4_EDGE in
   ip address 2.2.2.12/26 tag 54321

 interface Vlan101
+ no shutdown
+ no ip redirects
+ ip address 1.1.2.1/24 secondary
+ ip address 1.1.1.1/24

 interface Vlan102
   description Vlan102
   no shutdown
   mtu 9100
switch#
```

### Partial Configuration Diff Merged

```
switch# show file po.cfg
interface port-channel500
description po-123
switch#
switch# sh run int po500

!Command: show running-config interface port-channel500
!Running configuration last done at: Fri Sep 29 12:27:28 2023
!Time: Fri Sep 29 12:30:24 2023

version 10.4(2) Bios:version 07.69

interface port-channel500
```

```
  ip address 192.0.2.0/24
  ipv6 address 2001:DB8:0:ABCD::1/48

switch#

switch# show diff running-config po.cfg partial merged unified
--- running-config
+++ User-config
@@ -124,10 +110,11 @@
interface port-channel100
 interface port-channel500
   ip address 192.0.2.0/24
   ipv6 address 2001:DB8:0:ABCD::1/48
+ description po-123
 interface port-channel4096
 interface Ethernet1/1
switch#
```