HPE Aruba Networking Central On-Premises

3.0.4.3

CLI Reference Guide

Copyright Information

© Copyright 2026 Hewlett Packard Enterprise Development LP.

Open Source Code

This product includes code licensed under certain open source licenses which require source compliance. The corresponding source for these components is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, please check if the code is available in the HPE Software Center at https://myenterpriselicense.hpe.com/cwp-ui/software but, if not, send a written request for specific software version and product for which you want the open source code. Along with the request, please send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
WW Corporate Headquarters
1701 E Mossy Oaks Rd, Spring, TX 77389
United States of America

Revision History

The following table lists the revisions of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

What's New in HPE Aruba Networking

Following lists the updates to the HPE Aruba Networking Central On-Premises CLI:

- What's New in HPE Aruba Networking Central On-Premises 3.0.3.0

About this Guide

This guide describes the HPE Aruba Networking Central On-Premises commands. The commands in this guide are listed numerically.

The following information is provided for each command:

- Command Syntax—The complete syntax of the command.
- Description—A brief description of the command, including usage guidelines, prerequisites, prohibitions, and related commands.
- Example—An example of how to execute the command.
- Command History—The version of HPE Aruba Networking Central On-Premises in which the command was first introduced, including the modification history.

HPE Aruba Networking Central On-Premises Command Line Interface

The command-line interface features allows you to install, setup, manage, and troubleshoot HPE Aruba Networking Central On-Premises deployments. The CLI is accessed through a console or through a Secure Shell (SSH) session from a remote management console or workstation.

Accessing the HPE Aruba Networking Central On-Premises CLI

The following procedure describes how to access the SSH and start executing CLI commands:

1. From a secure shell (SSH) client, open an SSH connection.
2. Login as copadmin.
3. When prompted, enter the copadmin password.

   A list of commands is displayed.

For example:

```
login as: copadmin
admin@10.22.150.92 password:
Last login: Wed Aug  7 05:43:22 2019 from 10.20.15.180
```

Syntax

Enter option [0 - <option number>] : <enter option>

For example:

```
1. System
2. File Operations
3. Show
...
```

```
0. exit
...
Enter option [ 0 - 9 ]:
```

Common Command Options

The following common command options are used to:

- **0 – Exit**—Use this command option to exit the SSH connection.
- **b – Back**—Use this command option to go back to the previous menu.
- **m - Main menu**—Use this command option to go to the main menu.

Password Recovery

The password recovery system helps to create a new password for the **copadmin** user. If you forget the password, login to the console with the user, **coprecovery**, and the following options are displayed to generate the recovery key.

- **Generate Recovery Key**—The recovery key is generated and stored in an encrypted .asc file. You can either copy it or use the SCP command to copy the file. Once the key is copied to the local server, contact customer support to decrypt the recovery key to get a new password.
- **SCP Recovery Key**—The recovery key is generated and an SCP command is used to copy the file to a local server. Once the key is copied to the local server, contact customer support to decrypt the recovery key to get a new password.
- **Activate Recovery secret** —The secret key is provided and verified by the customer support. A reset option is used to rest the password in all nodes.
- **Retrieve "core" Password**—HPE Aruba Networking does not recommend using **core** user access. The customer support will decode the secret file provided by the user to provide access to the core user.

Main Menu Options

When you login to the HPE Aruba Networking Central On-Premises via the main set of commands are displayed. Using the main menu command options, you can perform various other actions as described in the table.

```
1. System
2. File Operations
3. Show
4. System Configuration
5. Advanced
6. Security
7. Support
8. Temporary Root Shell
9. Authentication
10. Certificate configuration
11. Search commands
==================================
0. exit

Enter option [ 0 - 11 ]:
```

Typographic Conventions

The following conventions are used throughout this manual to emphasize important concepts:

Table 2: *Text Conventions*

Type Style	Description
Italics	This style is used to emphasize important terms and to mark the titles of books.
Boldface	This style is used to emphasize command names and parameter options when mentioned in the text.
`Commands`	This fixed-width font depicts command syntax and examples of commands and command output.
`<angle brackets>`	In the command syntax, text within angle brackets represents items that you should replace with information appropriate to your specific situation. For example: ping <ipaddr> In this example, you would type “ping” at the system prompt exactly as shown, followed by the IP address of the system to which ICMP echo packets are to be sent. Do not type the angle brackets.
`[square brackets]`	In the command syntax, items enclosed in brackets are optional. Do not type the brackets.
`{Item_A|Item_B}`	In the command examples, single items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.
`{ap-name <ap-name>}|{ipaddr <ip-addr>}`	Two items within curled braces indicate that both parameters must be entered together. If two or more sets of curled braces are separated by a vertical bar, like in the example to the left, enter only one choice Do not type the braces or bars.

Specifying Addresses and Identifiers in Commands

This section describes addresses and other identifiers that you can reference in CLI commands.

Table 3: *Addresses and Identifiers*

Address or Identifier	Description
IP address	For any command that requires an IP address to specify a network entity, use IPv4 network address format in the conventional dotted decimal notation (for example, 10.4.1.258).
Netmask address	For subnet addresses, specify a netmask in dotted decimal notation (for example, 255.255.255.0).
MAC address	For any command that requires a device's hardware address, use the hexadecimal format (for example, 00:05:4e:50:14:aa).
SSID	A unique character string (sometimes referred to as a network name), consisting of not more than 32 characters. The SSID is case-sensitive (for example, WLAN-01).
BSSID	This entry is the unique hard-wireless MAC address of the AP. A unique BSSID applies to each frequency— 802.11a and 802.11g— used from the AP. Use the same format as that of a MAC address.
ESSID	The unique logical name of a wireless network. If the ESSID includes spaces, you must enclose the name in quotation marks.

Terminology Change

As part of advancing HPE's commitment to racial justice, we are taking a much-needed step in overhauling HPE engineering terminology to reflect our belief system of diversity and inclusion. Some legacy products and publications may continue to include terminology that seemingly evokes bias against specific groups of people. Such content is not representative of our HPE culture and moving forward, Aruba will replace racially insensitive terms and instead use the following new language:

Usage	Old Language	New Language
Campus Access Points + Controllers	Master-Slave	Conductor-Member
Instant Access Points	Master-Slave	Conductor-Member
Switch Stack	Master-Slave	Conductor-Member
Wireless LAN Controller	Mobility Master	Mobility Conductor
Firewall Configuration	Blacklist, Whitelist	Denylist, Allowlist
Types of Hackers	Black Hat, White Hat	Unethical, Ethical

Contacting Support

Table 4: *Contact Information*

Main Site	arubanetworks.com
Support Site	https://networkingsupport.hpe.com/home
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free)
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	lms.arubanetworks.com
End-of-life Information	https://networkingsupport.hpe.com/end-of-life
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins/ Email: aruba-sirt@hpe.com

System

```
1 System
```

Description

This command reboots and resets the system.

Hierarchy Level

```
1 System
   1-1 Reboot Systems
      1-1-1 Cluster Reboot
      1-1-2 Current Node Reboot
      1-2 Shutdown Systems
   1-3 Factory Reset
```

Enter the command option **1** from the main menu to reboot, shutdown, or reset the system to factory settings.

Main Menu Options

```
1. System
2. File Operations
3. Show
4. System Configuration
5. Advanced
6. Security
7. Support
8. Temporary Root Shell
9. Authentication
10. Certificate configuration
11. Search commands
===================================
0. exit

Enter option [ 0 - 11 ]: 1

============================
```

From the previous menu option, select **1** to display System options.

```
1. Reboot
2. Shutdown
3. Factory Reset
============================
b. back
m. main menu
0. exit
Enter option [0-3]:
```

Related Commands

Command	Description
Reboot System	Reboots the system.
Shutdown System	Shutdowns the system.
Factory Reset	Resets the system to its factory settings.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Reboot System

```
1 System
   1 Reboot
```

Description

Enter the command option **1** from the System menu to reboot the system.

System Options

```
1. Reboot
2. Shutdown
3. Factory Reset
============================
b. back
m. main menu
0. exit
Enter option [0-3]: 1
```

From the Show menu options, select **1** to confirm system reboot.

```
Are you sure you want to reboot the node (Y/N) :
```

In case of multi-node system reboot the following options are displayed:

```
This is a multi-cluster, please choose a reboot option -
1. Cluster Reboot
2. Current Node Reboot
```

Related Commands

Command	Description
Cluster Reboot	Performs wide reboot for all the nodes in the cluster.
Current Node Reboot	Performs reboot for only the current node in the cluster.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Cluster Reboot

```
1 System
   1 Reboot
      1 Cluster Reboot
```

Description

Enter the command option **1** from the Reboot menu to perform a cluster wide reboot. This option is displayed only in case of multi-node cluster.

System Options

```
1. Reboot
2. Shutdown
3. Factory Reset
============================
b. back
m. main menu
0. exit
Enter option [0-3]: 3
```

From the System menu options, select **1** to display the reboot options.

```
Are you sure you want to reboot the node (Y/N) :
```

In case of multi-node system reboot the following options are displayed:

```
This is a multi-cluster, please choose a reboot option -
1. Cluster Reboot
2. Current Node Reboot
Enter option [1 - 2]: 1
```

From the multi-node system reboot menu options, select **1** to reboot the cluster node.

```
Are you sure you want to reboot the cluster (Y/N): Y
Triggering reboot on 10.x.x.x.x
Executing node reboot...
Shutdown scheduled. Node will reboot after 1 minute.
Triggering reboot on 10.x.x.x.x
Executing node reboot...
Shutdown scheduled. Node will reboot after 1 minute.
Triggering reboot on 10.x.x.x.x
Executing node reboot...
Shutdown scheduled. Node will reboot after 1 minute.
Press [Enter] key to continue...
```

Related Commands

Command	Description
Current Node Reboot	Performs wide reboot for all the nodes in the cluster.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Current Node Reboot

```
1 System
   1 Reboot
      2 Current Node Reboot
```

Description

Enter the command option **2** from the Reboot menu to perform a system reboot of the current node. This option is displayed only in case of multi-node cluster.

System Options

```
1. Reboot
2. Shutdown
3. Factory Reset
============================
b. back
m. main menu
0. exit
Enter option [0-3]: 3
```

From the System menu options, select **1** to display the reboot options.

```
Are you sure you want to reboot the node (Y/N) :
```

In case of multi-node system reboot the following options are displayed:

```
This is a multi-cluster, please choose a reboot option -
1. Cluster Reboot
2. Current Node Reboot
Enter option [1 - 2]: 2
```

From the multi-node system reboot menu options, select **2** to reboot the current node.

```
Are you sure you want to reboot the cluster (Y/N): Y
Reboot job 'platform-config-node-mgmt-job-00swg under progress...
..
System will reboot in 1 minute.
Press [Enter] key to continue... Connection to 10.xx.xxx.xxx closed by
remote host.
Connection to 10.xx.xxx.xxx closed.
```

Related Commands

Command	Description
Cluster Reboot	Performs reboot for only the current node in the cluster.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Shutdown System

```
1 System
   2 Shutdown
```

Description

Enter the command option **2** from the System menu to shutdown the system.

System Options

```
1. Reboot
2. Shutdown
3. Factory Reset
============================
b. back
m. main menu
0. exit
Enter option [0-3]: 2
```

From the Show menu options, select **2** to schedule a system shutdown.

```
Executing shutdown...
Shutdown scheduled. Node will shutdown after 1 minute.

                                                    2-21 06:46:38
Press [Enter] key to continue...
```

Related Commands

Command	Description
Reboot System	Reboots the system.
Factory Reset	Resets the system to its factory settings.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Factory Reset

```
1 System
   3 Factory Reset
```

Description

Enter the command option **3** from the System menu to reset the system to its factory settings. Currently, it is a complete data reset.

System Options

```
1. Reboot
2. Shutdown
3. Factory Reset
============================
b. back
m. main menu
0. exit
Enter option [0-3]: 3
```

From the Show menu options, select **3** to initiate system factory reset..

```
Error: Please run the reset command from physical or remote console (ILO)
Are you sure you want to reboot the node (Y/N) :
Press [Enter] key to continue...
```

Related Commands

Command	Description
Reboot System	Reboots the system.
Shutdown System	Shutdowns the system.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

File Operations

```
2 File Operations
```

Description

This command uploads a file to the host.

Hierarchy Level

```
2 File Operations
   2-1 Upload via SCP
   2-2 Upload via SFTP
   2-3 Upload via HTTP/HTTPS
   2-4 Download File from COP
   2-5 Delete File
```

Enter option **2** from the main menu to upload a file to the host.

Main Menu Options

```
1. System
2. File Operations
3. Show
4. System Configuration
5. Advanced
6. Security
7. Support
8. Temporary Root Shell
9. Authentication
10. Certificate configuration
11. Search commands
==================================
0. exit

Enter option [ 0 - 11 ]: 2

============================
```

From the main menu options, select **2** to display File Operations options.

```
1. Upload via (SCP)
2. Upload via (SFTP)
3. Upload via (HTTP/HTTPS)
4. Download File from COP
5. Delete file
=========================
b. back
m. main menu
0. exit
Enter option [0-5]:
```

Related Commands

Command	Description
Upload via (SCP)	Uploads a file to the host over SCP.
Upload via (SFTP)	Uploads a file to the host over SFTP.
Upload via HTTP/HTTPS	Uploads a file to the host over HTTP or HTTPS.
Download File from COP	Downloads a file that is saved on the host.
Delete File	Deletes the files that was uploaded by the upload file command.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Upload via (SCP)

```
2 File Operations
   1 Upload via SCP
```

Description

Enter the command option **1** from the File Operations menu to upload a file to the host over SCP.

File Operation Options

```
1. Upload via (SCP)
2. Upload via (SFTP)
3. Upload via (HTTP/HTTPS)
4. Download File from COP
5. Delete file
==========================
b. back
m. main menu
0. exit
Enter option [0-5]: 1
```

From the file operations options, select **1** to upload a file to the host over SCP.

```
This will scp a file from the remote server to COP server
Enter remote hostname and path (username@hostname:<filepath>):
auto@10.xx.xxx.xx:/home/auto/packages.txt


Copying auto@10.xx.xxx.xx:/home/auto/packages.txt to COP server
auto@10.xx.xxx.xx's password:
packages.txt
                                              100% 3555    4.4MB/s    00:00

Press [Enter] key to continue...
```

The Upload via SCP command includes the following information.

Parameter	Description
SCP	Location of the file in a server.

Related Commands

Command	Description
Upload via (SFTP)	Uploads a file to the host over SFTP.
Upload via HTTP/HTTPS	Uploads a file to the host over HTTP or HTTPS.

Command	Description
Download File from COP	Downloads a file that is saved on the host.
Delete File	Deletes the files that was uploaded by the upload file command.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Upload via (SFTP)

```
2 File Operations
   2 Upload via SFTP
```

Description

Enter the command option **2** from the File Operations menu to upload a file to the host over SFTP.

File Operations Options

```
1. Upload via (SCP)
2. Upload via (SFTP)
3. Upload via (HTTP/HTTPS)
4. Download File from COP
5. Delete file
==========================
b. back
m. main menu
0. exit
Enter option [0-5]: 2
```

From the file operations options, select **2** to upload a file to the host over SFTP.

```
This will scp a file from the remote server to COP server
Enter remote hostname and path (username@hostname:<filepath>):
auto10.xx.xxx.xx:/home/auto/inst_packages.txt


Copying auto@10.xx.xxx.xx:/home/auto/inst_packages.txt to COP server

auto@10.10.xx.xxx.xx's password:
Connected to 10.10.xx.xxx.xx.
Fetching /home/auto/inst_packages.txt to
/var/airwave/appliance/localdisk/inst_
packages.txt
/home/auto/inst_packages.txt
                                          100% 1583      127.9KB/s
00:00


Press [Enter] key to continue...
```

The Upload via SFTP command includes the following information.

Parameter	Description
SFTP	Location of the file in a server.

Related Commands

Command	Description
Upload via (SCP)	Uploads a file to the host over SCP.
Upload via HTTP/HTTPS	Uploads a file to the host over HTTP or HTTPS.
Download File from COP	Downloads a file that is saved on the host.
Delete File	Deletes the files that was uploaded by the upload file command.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Upload via HTTP/HTTPS

```
2 File Operations
   3 Upload via HTTP/HTTPS
```

Description

Enter the command option **3** from the File Operations menu to upload a file to the host over HTTP or HTTPS.

File Operations Options

```
1. Upload via (SCP)
2. Upload via (SFTP)
3. Upload via (HTTP/HTTPS)
4. Download File from COP
5. Delete file
==========================
b. back
m. main menu
0. exit
Enter option [0-5]: 3
```

From the file operations options, select **3** to upload a file to the host over HTTP or HTTPS.

```
This will copy a file from the url to COP server
Enter full url path for file : http://10.xx.xxx.xx/a.html
a.html                                  100%

[=============================================================================
==>]
391.90M 106MB/s            in 3.7s
Upload file successful.
Press [Enter] key to continue...
```

Related Commands

Command	Description
Upload via (SCP)	Uploads a file to the host over SCP.
Upload via (SFTP)	Uploads a file to the host over SFTP.
Download File from COP	Downloads a file that is saved on the host.
Delete File	Deletes the files that was uploaded by the upload file command.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Download File from COP

```
2 File Operations
   4 Download file from cop
```

Description

Enter the command option **4** from the File Operations menu to download a file that is saved on the host.

File Operations Options

```
1. Upload via (SCP)
2. Upload via (SFTP)
3. Upload via (HTTP/HTTPS)
4. Download File from COP
5. Delete file
==========================
b. back
m. main menu
0. exit
Enter option [0-5]: 4
```

From the file operations options, select **4** to upload a file to download a file that is saved on the host.

```
! Files present under the directory !
cop_setup_logs inst_packages.txt packages.txt sftp.txt
Enter the file name to copy from COP server to the remote server:
packages.txt
This will scp packages.txt from localdisk to the remote server
Enter remote hostname and path (username@hostname:<filepath>):
auto@10.xx.xxx.xx:/home/auto

Copying localdisk files to auto@10.xx.xxx.xx:/home/auto
The authenticity of host '10.xx.xxx.xx (10.xx.xxx.xx)' can't be established.
RSA key fingerprint is SHA256:e9KqvWRV5YQhrPLoJQMiKFKKWVx7ZWz2T34oF31WvpU.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.xx.xxx.xx' (RSA) to the list of known hosts.
auto@10.xx.xxx.xx's password:
packages.txt
                                      100% 3555     2.9MB/s    00:00
Press [Enter] key to continue...
```

Related Commands

Command	Description
Upload via (SCP)	Uploads a file to the host over SCP.
Upload via (SFTP)	Uploads a file to the host over SFTP.

Command	Description
Upload via HTTP/HTTPS	Uploads a file to the host over HTTP or HTTPS.
Delete File	Deletes the files that was uploaded by the upload file command.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Delete File

```
2 File Operations
   5 Delete File
```

Description

Enter the command option **5** from the File Operations menu to delete the files that was uploaded by the upload file command.

File Operations Options

```
1. Upload via (SCP)
2. Upload via (SFTP)
3. Upload via (HTTP/HTTPS)
4. Download File from COP
5. Delete file
==========================
b. back
m. main menu
0. exit
Enter option [0-5]: 5
```

From the file operations options, select **5** to upload a file to download a file that is saved on the host.

```
! Files present under the directory !
cop_setup_logs inst_packages.txt packages.txt sftp.txt
Enter file/directory to delete:
packages.txt
Deleting file /var/airwave/appliance/localdisk/packages.txt
Are you sure you want to delete this file(Y/N):
Y File /
var/airwave/appliance/localdisk/packages.txt deleted
Press [Enter] key to continue...
```

Related Commands

Command	Description
Upload via (SCP)	Uploads a file to the host over SCP.
Upload via (SFTP)	Uploads a file to the host over SFTP.
Upload via HTTP/HTTPS	Uploads a file to the host over HTTP or HTTPS.
Download File from COP	Downloads a file that is saved on the host.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Show

```
3 Show
```

Description

The show commands are used to view or display the settings or parameters configured.

Hierarchy Level

```
3 Show
   3-1 Version
   3-2 List Files
   3-3 Backup-Restore Status
   3-4 Configuration
      3-4-1 Network-config/Cluster-info
      3-4-2 NTP/Timezone Info
      3-4-3 Show ILO IP Configuration
   3-5 System
      3-5-1 Memory Usage
      3-5-2 Uptime
   3-6 User Sessions
   3-7 Show Clock
   3-8 App Status
   3-9 Cluster Status
```

Enter the command option **3** from the main menu to view all the show commands supported.

Main Menu Options

```
1. System
2. File Operations
3. Show
4. System Configuration
5. Advanced
6. Security
7. Support
8. Temporary Root Shell
9. Authentication
10. Certificate configuration
11. Search commands
===================================
0. exit

Enter option [ 0 - 11 ]: 3

============================
```

From the main menu options, select **3** to display the Show options.

```
1. Version (Detail)
2. List Files
3. Backup-Restore Status
4. Configuration
5. System
```

```
6. User Sessions
7. Clock
8. App Status
9. Cluster Status
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 9 ]:
```

Related Commands

Command	Description
Version	Displays the version details of the Aruba Central On-Premises deployment.
List Files	Displays the total number of files in the pod.
Backup-Restore Status	Display the backup and restore status of the pod.
Configuration	Display the updated network settings, cluster details, NTP/Timezone information.
System	Display system information like usage of memory, activate information, and uptime.
User Sessions	Displays the list of user sessions.
Show Clock	Displays the date, week, month, time details.
App Status	Pod status of any Aruba Central On-Premises application.
Cluster Status	Displays the cluster details for Aruba Central On-Premises.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Version

```
3 Show
   1 Version (Detail)
```

Description

Enter command option **1** from the Show commands menu to display the version (Detail).

The Version (Detail) command includes the following information.

Parameter	Description
`Cop Version`	Version of the COP software installed.
`Build`	Version of the COP build.
`ISO Installed`	Status of the ISO installation.
`Setup Cluster`	Status of the setup cluster.

Show Options

```
1. Version (Detail)
2. List Files
3. Backup-Restore Status
4. Configuration
5. System
6. User Sessions
7. Clock
8. App Status
9. Cluster Status
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 9 ]: 1
```

From the Show options, select **1** to display the version details.

```
COP Version: 2.5.6.0
Build: 10.0.0-GA01.xxx
ISO Installed: Ok
COP Software Installed: Ok
Setup Cluster: Ok
Pulling ILO details. Please wait.
HPE Smart Array P408i-a SR Gen10: "4.11"
iLO 5: "2.18 Jun 22 2021"
System ROM: "U32 v2.34 (04/08/2020)"
Press [Enter] key to continue...
```

Related Commands

Command	Description
List Files	Displays the total number of files in the pod.
Backup-Restore Status	Display the backup and restore status of the pod.
Configuration	Display the updated network settings, cluster details, NTP/Timezone information.
System	Display system information like usage of memory, activate information, and uptime.
User Sessions	Displays the list of user sessions.
Show Clock	Displays the date, week, month, time details.
App Status	Pod status of any Aruba Central On-Premises application.
Cluster Status	Displays the cluster details for Aruba Central On-Premises.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

List Files

```
3 Show
   2 List Files
```

Description

Enter command option **2** from the Show commands menu to display the total number of files.

Show Options

```
1. Version (Detail)
2. List Files
3. Backup-Restore Status
4. Configuration
5. System
6. User Sessions
7. Clock
8. App Status
9. Cluster Status
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 9 ]: 2
```

From the previous menu option, select **2** to display the list files.

```
total 4
drwxr-xr-x 2 root root 4096 Jan 3 16:29 cop_setup_logs
Press [Enter] key to continue...
```

Related Commands

Command	Description
Version	Displays the total number of files in the pod.
Backup-Restore Status	Display the backup and restore status of the pod.
Configuration	Display the updated network settings, cluster details, NTP/Timezone information.
System	Display system information like usage of memory, activate information, and uptime.
User Sessions	Displays the list of user sessions.
Show Clock	Displays the date, week, month, time details.
App Status	Pod status of any Aruba Central On-Premises application.
Cluster Status	Displays the cluster details for Aruba Central On-Premises.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Backup-Restore Status

```
3 Show
   3 Backup-Restore Status
```

Description

Enter command option **3** from the Show commands menu to display the backup and restore status.

Show Options

```
1. Version (Detail)
2. List Files
3. Backup-Restore Status
4. Configuration
5. System
6. User Sessions
7. Clock
8. App Status
9. Cluster Status
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 9 ]: 3
```

From the previous menu option, select **3** to display the display the backup and restore status.

```
################################
backup/restore status
################################
Operation             : Backup
status                : Completed
error_message         : None
start_time            : 2022-12-13 04:22:00 UTC
ended_time            : 2022-12-13 08:36:58 UTC


Task status
---------------------
PostgreSQL            : success
Cassandra             : success
Elasticsearch         : success
Elasticsearch Aggregation   : success
Minio                 : success


Please [Enter] key to continue...




{"details": [
Aruba Central On-Premises 2.5.5.0 | User Guide 98
{ "
```

```
message": "
Postgres backup success",
"status": "success"
},
{ "
message": "
Cassandra backup success",
"status": "success"
},
{ "
message": "
Elasticsearch backup success",
"status": "success"
},
{ "
message": "
Minio backup success",
"status": "success"
},
{ "
message": "
Tar creation success",
"status": "success"
},
{ "
message": "
Transferring the backup to repository success",
"status": "success"
} ],
"endedOn": "Wed, 26 Jun 2019 12:52:29 GMT",
"operation": "Backup",
"startedOn": "Wed, 26 Jun 2019 11:59:43 GMT",
"status": "Completed"
}
```


Related Commands

Command	Description
Version	Displays the total number of files in the pod.
List Files	Displays the total number of files in the pod.
Configuration	Display the updated network settings, cluster details, NTP/Timezone information.
System	Display system information like usage of memory, activate information, and uptime.
User Sessions	Displays the list of user sessions.
Show Clock	Displays the date, week, month, time details.
App Status	Pod status of any Aruba Central On-Premises application.
Cluster Status	Displays the cluster details for Aruba Central On-Premises.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Configuration

```
3 Show
   4 Configuration
```

Description

Enter command option **4** from the Show commands menu to display the updated network settings, HPE Aruba Networking Central On-Premises cluster details, and NTP/Timezone information.

Show Options

```
1. Version (Detail)
2. List Files
3. Backup-Restore Status
4. Configuration
5. System
6. User Sessions
7. Clock
8. App Status
9. Cluster Status
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 9 ]: 4
```

From the Show menu options, select **4** to display the available configuration options.

```
1. Network-config/Cluster-info
2. NTP/Timezone Info
3. Show ILO IP Configuration
Enter option [ 0 - 3 ]:
```

Related Commands

Command	Description
Network-config/Cluster-info	Displays the network configuration and cluster information.
NTP/Timezone Info	Displays the NTP/Timezone information.
Show ILO IP Configuration	Displays the ILO IP configuration details.
Show Disk Status	Displays the disk status.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Network-config/Cluster-info

```
3 Show
   4 Configuration
      1 Network-config/Cluster-info
```

Description

Enter command option **1** from the Configuration menu to view the network configuration and cluster information.

Parameter	Description
`Hostname`	Location of the file in a server.
`IP Address`	IP address of the cluster.
`Subnet Mask`	Defines the subnet mask for Local; Local, L3; and Distributed, L3 DHCP scopes. The subnet mask and the network determine the size of subnet.
`Gateway`	IP address of the default gateway.
`DNS`	IP address of the DNS server.
`Secondary DNS`	IP address of the secondary DNS server in the network.
`Timezone`	Shows the current timezone.
`Cluster IP`	IP address of the cluster.
`Cluster FQDN`	Complete address of the cluster.
`Pod CIDR`	IP prefix for all the pods in the cluster.
`Router ID`	ID of the router.
`Cluster Node Count`	Number of nodes in the cluster.
`Cluster Node List`	Details of the node in the cluster. It displays the node name, status, roles assigned, age, and the installed version.

Show Options

```
1. Version (Detail)
2. List Files
3. Backup-Restore Status
4. Configuration
5. System
6. User Sessions
7. Clock
8. App Status
9. Cluster Status
```

```
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 9 ]: 4
```

From the Show menu options, select **4** to display the configuration options.

Configuration Options

```
1. Network-config/Cluster-info
2. NTP/Timezone Info
3. Show ILO IP Configuration
Enter option [ 0 - 3 ]: 1
```

From the Configuration menu options, select **1** to display the network configuration and cluster information.

```
Updated Network Settings
------------------------
Hostname                    : nodexxx.arubaxxx.com
IP Address                  : 10.xx.xxx.xx
Subnet Mask                 : 255.xxx.xxx.x
Gateway                     : 10.xx.xxx.xx
DNS                         : 10.xx.xxx.xx
Secondary DNS               : 10.xx.xxx.xx
Timezone                    : UTC
COP Cluster Details
-----------------------
Cluster IP          : 10.xx.xxx.xx
Cluster FQDN        : nodexxx.arubaxxx.com
Pod CIDR            : 172.xx.x.x/xx
Service CIDR        : 10.x.x.x/xx
Router ID           : 27
Time Zone           : UTC
Cluster Node Count : 3
Cluster Node List  :
NAME            STATUS   ROLES    AGE   VERSION
10.xx.xxx.xx    Ready    master   8h    v1.14.5
10.xx.xxx.xx    Ready    master   8h    v1.14.5
10.xx.xxx.xx    Ready    master   8h    v1.14.5
```

Related Commands

Command	Description
NTP/Timezone Info	Displays the timezone information of the NTP server.
Show ILO IP Configuration	Displays the ILO IP configuration details.
Show Disk Status	Displays the Disk status details.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

NTP/Timezone Info

```
3 Show
   4 Configuration
      2 NTP/Timezone Info
```

Description

Enter command option **2** from the Configuration menu to view the NTP/Timezone information.

Show Options

```
1. Version (Detail)
2. List Files
3. Backup-Restore Status
4. Configuration
5. System
6. User Sessions
7. Clock
8. App Status
9. Cluster Status
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 9 ]: 4
```

From the Show menu options, select **4** to display the configuration options.

Configuration Options

```
1. Network-config/Cluster-info
2. NTP/Timezone Info
3. Show ILO IP Configuration
Enter option [ 0 - 3 ]: 2
```

From the previous menu option, select **2** to display the display the NTP/Timezone information.

```
210 Number of sources = 2
MS Name/IP address         Stratum Poll Reach LastRx Last sample

===============================================================================
===
^* 10.xx.xxx.xx                4   6   377    57  -5116us[-5083us] +/-
65ms
^+ 10.xx.xxx.xx                 4   7   377    38  +6096us[+6096us] +/-
74ms
############################
TimeZone Info
############################
Etc/UTC

Press [Enter] key to continue...
```

Related Commands

Command	Description
Network-config/Cluster-info	Displays the the network configuration and cluster information.
Show ILO IP Configuration	Displays the ILO IP configuration details.
Show Disk Status	Displays the Disk status details.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Show ILO IP Configuration

```
3 Show
   4 Configuration
      3 Show ILO IP Configuration
```

Description

Enter command option **3** from the Configuration menu to view the ILO IP configuration details.

This option is not available for HPE Aruba Networking Central On-Premises Non-Appliance installation.

Parameter	Description
`Hostname`	Location of the file in a server.
`DHCPv4`	Status of the DHCP server.
`IPv4 Address`	IP address of the ILO server.
`Subnet Mask`	Defines the subnet mask for Local; Local, L3; and Distributed, L3 DHCP scopes. The subnet mask and the network determine the size of subnet.
`Gateway`	IP address of the default gateway.
`Primary DNS`	IP address of the primary DNS server.
`Secondary DNS`	IP address of the secondary DNS server.

Show Options

```
1. Version (Detail)
2. List Files
3. Backup-Restore Status
4. Configuration
5. System
6. User Sessions
7. Clock
8. App Status
9. Cluster Status
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 9 ]: 4
```

From the Show menu options, select **4** to display the configuration options.

Configuration Options

```
1. Network-config/Cluster-info
2. NTP/Timezone Info
3. Show ILO IP Configuration
Enter option [ 0 - 3 ]: 3
```

From the previous menu option, select **3** to display the display the ILO IP configuration details.

```
Enter option [ 0 - 3 ]:  3
Ethernet Management Interface '1'
DHCPv4: Disabled
HostName     : ILOxxxxxxxxxx
IPv4 Address : 10.xx.xxx.xx
Subnet Mask  : 255.xxx.xxx.x
Gateway      : 10.xx.xxx.x
Primary   DNS: 2001::1
Secondary DNS: 10.xx.xx.xx
```

Related Commands

Command	Description
NTP/Timezone Info	Displays the timezone information of the NTP server.
Network-config/Cluster-info	Displays the the network configuration and cluster information.
Show Disk Status	Displays the Disk status details.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Show Disk Status

```
3 Show
   4 Configuration
      4 Disk Status
```

Description

Enter command option **4** from the Configuration menu to view the disk status details.

Parameter	Description
Hostname	Location of the file in a server.
DHCPv4	Status of the DHCP server.
IPv4 Address	IP address of the ILO server.
Subnet Mask	Defines the subnet mask for Local; Local, L3; and Distributed, L3 DHCP scopes. The subnet mask and the network determine the size of subnet.
Gateway	IP address of the default gateway.
Primary DNS	IP address of the primary DNS server.
Secondary DNS	IP address of the secondary DNS server.

Show Options

```
1. Version (Detail)
2. List Files
3. Backup-Restore Status
4. Configuration
5. System
6. User Sessions
7. Clock
8. App Status
9. Cluster Status
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 9 ]: 4
```

From the Show menu options, select **4** to display the configuration options.

Configuration Options

```
1. Network-config/Cluster-info
2. NTP/Timezone Info
3. Show ILO IP Configuration
```

```
Enter option [ 0 - 3 ]: 4
```

From the previous menu option, select **4** to display the display the ILO IP configuration details.

```
Enter option [ 0 - 3 ]:  3 Enter option [ 0 - 4 ]:  4

SN  NODE                                        RAID    ONLINE/TOTAL
-----------------------------------------------------------------
1)  cnx-onprem-upgrade-144-75.arubacorp.net     RAID0        4/4
2)  cnx-onprem-upgrade-144-76.arubacorp.net     RAID0        4/4
3)  cnxop-install-node1.arubacorp.net     RAID0        4/4
4)  cnxop-install-node2.arubacorp.net     RAID0        4/4
5)  cop-node-144.149.arubacorp.net     RAID6        5/5
6)  cop2-5n-upgrade-n4.arubacorp.net     RAID0        4/4
7)  cop2-5n-upgrade-n5.arubacorp.net     RAID6        6/6

8) Exit

To see node specific disk details, Choose an option [1-8]:
```

Related Commands

Command	Description
NTP/Timezone Info	Displays the timezone information of the NTP server.
Network-config/Cluster-info	Displays the the network configuration and cluster information.
Show ILO IP Configuration	Displays the ILO IP configuration details.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.1.0	Command introduced.

System

```
3 Show
   5 System
```

Description

Enter command option **5** from the Show commands menu to display system information like usage of memory, system information, and so on.

Show Options

```
1. Version (Detail)
2. List Files
3. Backup-Restore Status
4. Configuration
5. System
6. User Sessions
7. Clock
8. App Status
9. Cluster Status
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 9 ]: 5
```

From the previous menu option, select **5** to display the system information options.

```
1. Memory/Hard disk/CPU Usage
2. Uptime
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 2 ]:
```

Related Commands

Command	Description
Memory/Hard disk/CPU Usage	Displays the usage of memory, hard disk, and CPU information.
Uptime	Displays the uptime duration of a HPE Aruba Networking Central On-Premises pod.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Memory/Hard disk/CPU Usage

```
3 Show
   5 System
      1 Memory Usage
```

Description

Enter the command option **1** from the System menu to view the usage of memory, hard disk, and CPU information.

Show Options

```
1. Version (Detail)
2. List Files
3. Backup-Restore Status
4. Configuration
5. System
6. User Sessions
7. Clock
8. App Status
9. Cluster Status
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 9 ]: 5
```

From the Show menu options, select **5** to display the system information options.

System Options

```
1. Memory/Hard disk/CPU Usage
2. Uptime
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 2 ]: 1
```

From the System menu options, select **1** to display the usage of memory, hard disk, and CPU information.

```
############################
Memory Usage
############################
total          used        free      shared     buff/cache   available
Mem:           503G        183G        241G        135M         79G
320G
Swap:            0B          0B          0B
############################
Hardisk Usage
############################
Filesystem      Size  Used Avail Use% Mounted on
```

```
udev            252G     0  252G   0% /dev
tmpfs            51G   33M   51G   1% /run
/dev/sda4        15G  5.3G  9.0G  37% /
tmpfs           252G     0  252G   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           252G     0  252G   0% /sys/fs/cgroup

/dev/sda3       465M   64M  373M  15% /boot
/dev/sda5        15G   41M   15G   1% /secondary
/dev/sda2       241M   512  241M   1% /boot/efi
/dev/sda6       3.5T  982G  2.3T  30% /data
tmpfs            51G     0   51G   0% /run/user/1003
tmpfs            51G     0   51G   0% /run/user/1001
############################
CPU Usage
############################
%Cpu(s): 23.0 us,  5.3 sy,  0.0 ni, 70.5 id,  0.3 wa,  0.0 hi,  0.9
si,  0.0 st
Architecture:        x86_64
CPU op-mode(s):      32-bit, 64-bit
Byte Order:          Little Endian
CPU(s):              80
On-line CPU(s) list: 0-79
Thread(s) per core:  2
Core(s) per socket:  20
Socket(s):           2
NUMA node(s):        2
Vendor ID:           GenuineIntel
CPU family:          6
Model:               85
Model name:          Intel(R) Xeon(R) Gold 6138 CPU @ 2.00GHz
Stepping:            4
CPU MHz:             2700.005
CPU max MHz:         3700.0000
CPU min MHz:         1000.0000
BogoMIPS:            4000.00
Virtualization:      VT-x
L1d cache:           32K
L1i cache:           32K
L2 cache:            1024K
L3 cache:            28160K
NUMA node0 CPU(s):   0-19,40-59
NUMA node1 CPU(s):   20-39,60-79
Flags:               fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge
mca cmov pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall
nx pdpe1gb rdtscp lm constant_tsc art arch_perfmon pebs bts rep_good nopl
xtopology nons
top_tsc cpuid aperfmperf pni pclmulqdq dtes64 monitor ds_cpl vmx smx est tm2
ssse3 sdbg fma cx16 xtpr pdcm pcid dca sse4_1 sse4_2 x2apic movbe popcnt
tsc_deadline_timer aes xsave avx f16c rdrand lahf_lm abm 3dnowprefetch
cpuid_fault epb
cat_l3 cdp_l3 invpcid_single pti intel_ppin ssbd mba ibrs ibpb stibp tpr_
shadow vnmi flexpriority ept vpid fsgsbase tsc_adjust bmi1 hle avx2 smep
bmi2 erms invpcid rtm cqm mpx rdt_a avx512f avx512dq rdseed adx smap
clflushopt clwb intel_
pt avx512cd avx512bw avx512vl xsaveopt xsavec xgetbv1 xsaves cqm_llc cqm_
occup_llc cqm_mbm_total cqm_mbm_local dtherm ida arat pln pts hwp
hwp_act_window hwp_pkg_req pku ospke md_clear flush_l1d arch_capabilities

Press [Enter] key to continue...
```

Related Commands

Command	Description
Uptime	Displays the uptime duration of a HPE Aruba Networking Central On-Premises pod.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Uptime

```
3 Show
   5 System
      2 Uptime
```

Description

Enter the command option **2** from the System menu to view the uptime duration of a HPE Aruba Networking Central On-Premises pod.

Show Options

```
1. Version (Detail)
2. List Files
3. Backup-Restore Status
4. Configuration
5. System
6. User Sessions
7. Clock
8. App Status
9. Cluster Status
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 9 ]: 5
```

From the Show menu options, select **5** to display the system information options.

System Options

```
1. Memory/Hard disk/CPU Usage
2. Uptime
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 2 ]: 2
```

From the System menu option, select **2** to display the display the uptime duration.

```
############################
uptime
############################
17:35:06 up 2 days,  3:11,  3 users,  load average: 24.54, 26.08, 26.89

Press [Enter] key to continue...
```

Related Commands

Command	Description
Memory/Hard disk/CPU Usage	Displays the memory, hard disk, and CPU usage information.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

User Sessions

```
3 Show
   6 User Sessions
```

Description

Enter command option **6** from the Show commands menu to display the list of user sessions.

Show Options

```
1. Version (Detail)
2. List Files
3. Backup-Restore Status
4. Configuration
5. System
6. User Sessions
7. Clock
8. App Status
9. Cluster Status
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 9 ]: 6
```

From the previous menu option, select **6** to display the list of user sessions.

```
############################
List of user sessions
############################
copadmin pts/0 2020-07-27 05:26 01:17 51432 (10.xx.xxx.xx)
ineedshell pts/1 2020-07-27 05:02 01:42 3261 (10.xx.xxx.xx)
cop_shell pts/2 2020-07-27 05:30 01:10 54299 (10.xx.xxx.xx)
copadmin pts/3 2020-07-27 05:54 . 76741 (10.xxx.xxx.xxx)
ineedshell pts/4 2020-07-27 06:05 00:39 47373 (10.xx.xxx.xxx)
ineedshell pts/5 2020-07-27 06:11 00:32 36861 (10.xx.xxx.xxx)
ineedshell pts/6 2020-07-27 06:42 00:02 68881 (10.xx.xxx.xx)
```

Related Commands

Command	Description
Version	Displays the version details of the Aruba Central On-Premises deployment.
List Files	Displays the total number of files in the pod.
Backup-Restore Status	Display the backup and restore status of the pod.
Configuration	Display the updated network settings, cluster details, NTP/Timezone information.

Command	Description
System	Display system information like usage of memory, activate information, and uptime.
Show Clock	Displays the date, week, month, time details.
App Status	Pod status of any Aruba Central On-Premises application.
Cluster Status	Displays the cluster details for Aruba Central On-Premises.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Show Clock

```
3 Show
   7 Clock
```

Description

Enter command option **7** from the Show commands menu to display the date, week, month, and time details.

Show Options

```
1. Version (Detail)
2. List Files
3. Backup-Restore Status
4. Configuration
5. System
6. User Sessions
7. Clock
8. App Status
9. Cluster Status
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 9 ]: 7
```

From the previous menu option, select **7** to display the date, week, month, and time details.

```
Thu Aug 8 03:35:50 UTC 2022
```

Related Commands

Command	Description
Version	Displays the version details of the Aruba Central On-Premises deployment.
List Files	Displays the total number of files in the pod.
Backup-Restore Status	Display the backup and restore status of the pod.
Configuration	Display the updated network settings, cluster details, NTP/Timezone information.
System	Display system information like usage of memory, activate information, and uptime.
User Sessions	Displays the list of user sessions.
App Status	Pod status of any Aruba Central On-Premises application.
Cluster Status	Displays the cluster details for Aruba Central On-Premises.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

App Status

```
3 Show
   8 App Status
```

Description

Enter command option **8** from the Show commands menu to provide the pod status of any HPE Aruba Networking Central On-Premises application.

Show Options

```
1. Version (Detail)
2. List Files
3. Backup-Restore Status
4. Configuration
5. System
6. User Sessions
7. Clock
8. App Status
9. Cluster Status
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 9 ]: 8
```

From the previous menu option, select **8** to display the pod status.

```
Enter the application name, to list all apps press Enter key:central
Enter the application name, to list all apps press Enter key:central
acp-system central-grafana-dashboard-7c845956dc-92xgj
1/1 Running
7h42m 172.xx.x.xxx 10.xx.xxx.xx <none> <none>
1
central acp-ae-rapids-api-deployment-b8d794d49-4sxck
1/1 Running 0 7h30m 172.xx.x.xxx 10.xx.xxx.xx <none>
<none>
central acp-ae-rapids-bootstrap-deployment-789f85cbbd-dtjsb
1/1 Running 0 7h38m 172.xx.x.xxx 1 10.xx.xxx.xx <none>
central acp-ae-rapids-deployment-588b4989b5-kc58v
1/1 Running 0 7h38m 172.xx.x.xxx  10.xx.xxx.xx <none>
<none
central acp-ae-rapids-deployment-588b4989b5-q7mw8
1/1 Running 0 7h38m 172.xx.x.xxx  10.xx.xxx.xx <none>
<none
central acp-ae-rapids-deployment-588b4989b5-q7mw8
1/1 Running 0 7h38m 172.xx.x.xxx  10.xx.xxx.xx <none>
<none
central acp-ae-rapids-deployment-588b4989b5-xx5ks
1/1 Running 0 7h38m 172.xx.x.xxx  10.xx.xxx.xx <none>
central acp-device-visibility-deployment-5f97648f6f-nxq28
1/1 Running 0 7h42m 172.xx.x.xxx  10.xx.xxx.xx <none>
<none>
central acp-device-visibility-deployment-5f97648f6f-nxq28
1/1 Running 0 7h42m 172.xx.x.xxx  10.xx.xxx.xx <none>
<none>
```

```
central admin-api-deployment-7d4f4984f7-9wq5h
1/1 Running 0 7h37m 172.xx.x.xxx 172.xx.x.xxx 10.xx.xxx.xx <none>
<none>
```

Related Commands

Command	Description
Version	Displays the version details of the Aruba Central On-Premises deployment.
List Files	Displays the total number of files in the pod.
Backup-Restore Status	Display the backup and restore status of the pod.
Configuration	Display the updated network settings, cluster details, NTP/Timezone information.
System	Display system information like usage of memory, activate information, and uptime.
User Sessions	Displays the list of user sessions.
Show Clock	Displays the date, week, month, time details.
Cluster Status	Displays the cluster details for Aruba Central On-Premises.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Cluster Status

```
3 Show
   9 Cluster Status
```

Description

Enter command option **9** from the Show commands menu to display the HPE Aruba Networking Central On-Premises cluster details.

Parameter	Description
`Cluster IP`	IP address of the cluster.
`Cluster FQDN`	FQDN of the cluster.
`Pod CIDR`	IP prefix for all the pods in the cluster.
`Service CIDR`	IP address range for the services.
`Router ID`	ID of the router.
`Time Zone`	Shows the current timezone.
`Cluster Node Count`	Number of nodes in the cluster.
`Cluster Node List`	List of nodes in the cluster.

Show Options

```
1. Version (Detail)
2. List Files
3. Backup-Restore Status
4. Configuration
5. System
6. User Sessions
7. Clock
8. App Status
9. Cluster Status
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 9 ]: 9
```

From the previous menu option, select **9** to display the cluster status.

```
COP Cluster Details
----------------------
Cluster IP : 10.xx.xxx.xx
Cluster FQDN : nodexxxx.arubxxx.com
Pod CIDR : 172.xx.x.x/xx
Service CIDR : 10.x.x.x/xx
Router ID : 27
```

```
Time Zone : UTC
Cluster Node Count : 3
Cluster Node List :
NAME STATUS ROLES AGE VERSION
10.xx.xxx.xx Ready master 8h v1.14.5
10.xx.xxx.xx Ready master 8h v1.14.5
```

Related Commands

Command	Description
Version	Displays the version details of the Aruba Central On-Premises deployment.
List Files	Displays the total number of files in the pod.
Backup-Restore Status	Display the backup and restore status of the pod.
Configuration	Display the updated network settings, cluster details, NTP/Timezone information.
System	Display system information like usage of memory, activate information, and uptime.
User Sessions	Displays the list of user sessions.
Show Clock	Displays the date, week, month, time details.
App Status	Pod status of any Aruba Central On-Premises application.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

System Configuration

```
4 System Configuration
```

Description

The System Configuration commands are used to configure system parameters like network setup, cluster setup, timezone setup, upgrade the setup, offline upgrade, and Datacenter Redundancy or perform a complete factory reset.

Hierarchy Level

```
4 System Config
   4-1 Upgrade
     4-1-1 Upload
       4-1-1-1 Select Signature and Installation File
       4-1-1-2 Upload Signature and Installation File via SCP
       4-1-1-3 Upload Signature and Installation File via SFTP
     4-1-2 Upgrade
     4-1-3 Proceed
   4-2 Network Setup
     4-2-1 Permanent
     4-2-2 Temporary
     4-2-3 Switch Network Interface
     4-2-4 Network link Aggregation
       4-2-4-1 Enable Network link Aggregation
       4-2-4-2 Disable Network link Aggregation
       4-2-4-3 Status of Network link Aggregation
   4-3 Proxy Setup
     4-3-1 Add Proxy
     4-3-2 Delete Proxy
     4-3-3 Get Proxy
   4-4 Setup Timezone
   4-5 Setup NTP
   4-6 Node Setup
      4-6-1 Add Node
      4-6-2 Replace Node
      4-6-3 Status
   4-7 Airgap
      4-7-1 Enable Airgap
      4-7-2 Disable Airgap
      4-7-3 Status
   4-8 Datacenter Redundancy
      4-8-1 Show Datacenter Redundancy Status
      4-8-2 Configure Datacenter Redundancy
        4-8-2-1 Show Config
        4-8-2-2 Show Datacenter Redundancy Pairing Key
        4-8-2-3 Configure
        4-8-2-4 Enable Redundancy
        4-8-2-5 Disable Redundancy
      4-8-3 Auto Failover
        4-8-3-1 Disable Auto Failover
        4-8-3-2 Enable Auto Failover
      4-8-4 Restore Frequency
      4-8-5 Time to Failover
      4-8-6 Initiate Switchover
      4-8-7 Remove Datacenter Redundancy Configuration
   4-9 Upgrade ILO using Service Pack
      4-9-1 Trigger ILO Upgrade Service Pack
```

```
   4-9-2 Check ILO Service Pack version
   4-9-3 Reset ILO Security Encryption After Service Pack
4-10 Autorecovery Maintenance Window
   4-10-1 Update current window
      4-10-1-1 Anytime (Recommended - reboots automatically while preserving HA)
      4-10-1-2 Set Window (set a day and time for reboots)
      4-10-1-3 Never (Not recommended - system will never reboot)
   4-10-2 Exit
4-11 HPE Networking Support Portal Authentication
```

Enter the command option **4** from the main menu to view all the system configuration options.

Main Menu Options

```
1. System
2. File Operations
3. Show
4. System Configuration
5. Advanced
6. Security
7. Support
8. Temporary Root Shell
9. Authentication
10. Certificate configuration
11. Search commands
==================================
0. exit

Enter option [ 0 - 11 ]: 4

============================
```

From the main menu options, select **4** to display the system configuration options.

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Time
5. Setup NTP
6. Node Setup
7. Airgap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]:
```

Related Commands

Command	Description
Upgrade	Upgrades the HPE Aruba Networking Central On-Premises system for either an online user or an offline user.
Network Setup	Sets up a network permanently or temporarily. It also enables users to switch interface.
Proxy Setup	Adds deletes, or gets the proxy URL.
Setup Timezone	Sets up the timezone.
Setup NTP	Sets up the NTP server.
Node Setup	Sets up a node cluster.
Airgap	Enables or disables Airgap mode for upgrade. Enabling Airgap allows you to upgrade the HPE Aruba Networking Central On-Premises setup offline without any internet access.
Disaster Recovery	Handles upgrade for Datacenter Redundancy in HPE Aruba Networking Central On-Premises network.
Upgrade ILO using ServicePack	Handles the System Configuration menu to upgrade the ILO service pack to keep the system updated with the latest ILO and firmware version.
Autorecovery Maintenance Window	Handles the System Configuration menu to set the auto-recovery maintenance windows.
HPE Networking Support Portal Authentication	Handles the System Configuration menu to log in with your HPE Networking Support Portal (NSP) credentials.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Upgrade

```
4 System Configuration
   1 Upgrade
```

Description

Enter command option **1** from the System Configuration commands menu to upgrade the system for either an online user or an offline user.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 1
```

From the System Configuration options, select **1** to display the available upgrade options for an online or offline user.

Upgrade Options

```
1. Upload Package
2. Upgrade Status
3. Proceed With Upgrade
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 3 ]:
```

Related Commands

Command	Description
Software Download	Uploads and selects the upgrade packages, signature file and upgrade file for offline update.
Upgrade Status	Displays the upgrade status.

Command	Description
Proceed With Upgrade	Enables to proceed with HPE Aruba Networking Central On-Premises upgrade.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Software Download

```
4 System Configuration
   1 Upgrade
      1 Software Download
```

Description

Enter command option **1** from the Upgrade commands menu to download and select the upgrade packages for offline update. The upgrade package includes the signature file and the upgrade file.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 1
```

From the System Configuration options, select **1** to display the available upgrade options for an online or offline user.

Upgrade Options

```
1. Software Download
2. Upgrade Status
3. Proceed With Upgrade
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 3 ]: 1
```

From the Upgrade options, select **1** to display available options to upload packages for offline update.

Upload Package Options

```
1. Software Download
2. Upgrade Status
```

```
3. Proceed With Upgrade
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 3 ]: 1
Enter the Protocol(SCP/SFTP):
```

Related Commands

Command	Description
Upgrade Status	Displays the upgrade status.
Proceed With Upgrade	Enables to proceed with HPE Aruba Networking Central On-Premises upgrade.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 2.5.x	Command introduced.

Upgrade Status

```
4 System Configuration
   1 Upgrade
      2 Upgrade Status
```

Description

Enter command option **2** from the Upgrade commands menu to know upgrade status.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 1
```

From the System Configuration options, select **1** to upgrade the system for an online or offline user.

Options

```
1. Upload Package
2. Upgrade Status
3. Proceed With Upgrade
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 3 ]: 2
```

From the System Configuration options, select **2** to upgrade status.

```
Enter option [ 0 - 3 ]: 2
COP Server Status
--------------------------------------------------------------------------------
----
Current Version                             : 2.5.7.0
Latest Version                              : 2.5.7.0
Online Customer                             : false
```

```
Upgrade Status                                : UPGRADE_NOT_STARTED
Upgrade Available                             : true
Sign File Transfer Completion Percentage      : 100
Upg Pkg File Transfer Completion Percentage : 100
Pkg Sign Validate Completion Percentage       : 100
Extract Completion Percentage                 : 100
Upgrade Stage Completion Percentage           : 0
-------------------------------------------------------------------------
----

       -
Last Sign File Transfer Status                : SUCCESS
Last Sign File Transfer Message               :
Last Sign File Transfer Time                  : 2023-07-26 06:10:50
Last Upg Pkg File Transfer Status             : SUCCESS
Last Upg Pkg File Transfer Message            :
Last Upg pkg File Transfer Time               : 2023-07-26 06:10:54
Last Pkg Sign Validate Status                 : SUCCESS
Last Pkg Sign Validate Message                :
Last Pkg Sign Validate Time                   : 2023-07-26 06:21:05
Last Extract Status                           : SUCCESS
Last Extract Message                          :
Last Extract  Time                            : 2023-07-26 11:14:34
Last Upgrade Status                           : SUCCESS
Last Upgrade Message                          :
Last Upgrade Time                             : 2023-07-21 09:58:55
-------------------------------------------------------------------------
----

       -
Press [Enter] key to continue
```

Related Commands

Command	Description
Software Download	Uploads and selects the upgrade packages, signature file and upgrade file for offline update.
Proceed With Upgrade	Enables to proceed with HPE Aruba Networking Central On-Premises upgrade.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 2.5.x	Command introduced.

Proceed With Upgrade

```
4 System Configuration
   1 Upgrade
      3 Proceed With Upgrade
```

Description

Enter command option **3** from the Upgrade commands menu to proceed with upgrade if there is any new HPE Aruba Networking Central On-Premises version available.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 1
```

From the System Configuration options, select **1** to upgrade the system for an online or offline user.

Options

```
1. Upload Package
2. Upgrade Status
3. Proceed With Upgrade
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 3 ]: 3
```

From the System Configuration options, select **3** to proceed with upgrade.

```
Enter option [ 0 - 3 ]: 3
Please confirm to start the upgrade to 2.5.7.0 version (Y/N):
```

Related Commands

Command	Description
Software Download	Uploads and selects the upgrade packages, signature file and upgrade file for offline update.
Upgrade Status	Displays the upgrade status.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 2.5.x	Command introduced.

Network Setup

```
4 System Configuration
   2 Network Setup
```

Description

Prerequisite

Ensure the DNS servers, both primary and secondary configured on HPE Aruba Networking Central On-Premises resolves the following FQDNs:

- central-<FQDN>
- sso-<FQDN>
- apigw-<FQDN>
- ccs-user-api-<FQDN>

Additionally, the DNS servers must also resolve the public and private DNS namespaces required by the organization.

Enter command option **2** from the System Configuration commands menu to setup a network permanently or temporarily. It also enables users to switch network interface and create network link aggregation in case of any breakage in the network.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 2
```

From the System Configuration options, select **2** to display the available Network Setup options.

Network Setup Options

```
1. Permanent (Network settings)
2. Temporary (Network settings)
3. Switch Network Interface
4. Network Link Aggregation Setup
====================================
```

```
b. back
m. main menu
0. exit

Enter option [ 0 - 4 ]:
```

Related Commands

Command	Description
Permanent (Network settings)	Sets up the permanent network settings.
Temporary (Network settings)	Sets up the temporary network settings.
Switch Network Interface	Enables user to switch interfaces.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Permanent (Network settings)

```
4 System Configuration
   2 Network Setup
      1 Permanent (Network settings)
```

Description

Enter command option **1** from the Network Setup commands menu to setup the permanent network settings.

HPE Aruba Networking Central On-Premises now requires the FQDNs to be resolved on both the primary and secondary DNS servers. When a valid FQDN is entered, it is resolved with the configured DNS server. But, when an invalid FQDN is entered, it is not resolved with the configured DNS servers. The maximum number of re-attempts is two and consequently, you need to re-enter the network settings again. However, during the re-attempt, the data provided earlier is defaulted for ease of re-entering the settings.

Parameter	Description
`Hostname`	Location of the file in the server..
`IP Address`	IP address of the cluster.
`Interface`	Connected interface.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 1
```

From the System Configuration options, select **2** to display the available Network Setup options.

Network Setup Options

```
1. Permanent (Network settings)
2. Temporary (Network settings)
3. Switch Network Interface
```

```
4. Network Link Aggregation Setup
==================================
b. back
m. main menu
0. exit

Enter option [ 0 - 4 ]:
```

From the Network Setup options, select **1** to display the permanent network setting options.

```
Network Settings
To list available interfaces, enter 'list'
Enter interface name [eno1]: eno1
Enter IP Address [10.xx.xxx.xx]: 10.xx.xxx.xx
Enter Subnet mask [255.xxx.xxx.x]: 255.xxx.xxx.x
Enter Gateway [10.xx.xxx.xxx ]: 10.xx.xxx.xxx
Enter DNS [10.xx.xxx.xx]: 10.xx.xxx.xx
Secondary DNS is optional. Press ENTER to proceed
Enter Secondary DNS [10.xx.xxx.xx]: 10.xx.xxx.xx
Network settings exist; will be reset to new value
Enter COP Hostname/FQDN [cop-xxx-xx.xxxx.arubaxxx.cloud.hpe.com]: cop-xxx-
xx.xxxx.arubaxxx.cloud.hpe.com
To list timezones, enter 'list'
Enter timezone [Etc/UTC]: Etc/UTC
============================ Updated Network Settings
============================
Hostname                    : cop-xxx-xx.xxxx.arubaxxx.cloud.hpe.com
IP Address                  : 10.xx.xxx.xx
Subnet Mask                 : 255.xxx.xxx.x
Gateway                     : 10.xx.xxx.xxx
DNS                         : 10.xx.xxx.xxx
Secondary DNS               : 10.xx.xxx.xxx
Timezone                    : Etc/UTC
================================================================================
====
Starting setup wizard container.
Starting the nginx container.
Press [Enter] key to continue...
```

Related Commands

Command	Description
Temporary (Network settings)	Sets up the temporary network settings.
Switch Network Interface	Enable users to switch interfaces.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Temporary (Network settings)

```
4 System Configuration
   2 Network Setup
      2 Temporary (Network settings)
```

Description

Enter command option **2** from the Network Setup commands menu to setup the temporary network settings.

Parameter	Description
`Hostname`	Location of the file in the server..
`IP Address`	IP address of the cluster.
`Interface`	Connected interface.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 1
```

From the System Configuration options, select **2** to display the available Network Setup options.

Network Setup Options

```
1. Permanent (Network settings)
2. Temporary (Network settings)
3. Switch Network Interface
4. Network Link Aggregation Setup
==================================
b. back
m. main menu
0. exit

Enter option [ 0 - 4 ]:
```

From the Network Setup options, select **2** to display the temporary network setting options.

```
Network Settings


Hostname   : ccs-xxx.arubaxxx.com
IP Address : 10.xx.xxx.xxx
Interface  : eno1

Enter Subnet mask : 255.xxx.xxx.0
Enter Gateway : 10.xx.xxx.xxx
Enter DNS : 10.xx.xxx.xxx

Secondary DNS is optional. Press ENTER to proceed
Enter Secondary DNS : 10.xx.xxx.xxx

Network settings exist; will be reset to new value
To list timezones, enter 'list'
Enter timezone : UTC

============================ Updated Network Settings
============================

Hostname                    : ccs-1n-cophost.arubathena.com
IP Address                  : 10.xx.xxx.xx
Subnet Mask                 : 255.xxx.xxx.x
Gateway                     : 10.xx.xxx.xxx
DNS                         : 10.xx.xxx.xxx
Secondary DNS               : 10.xx.xxx.xxx
Timezone                    : UTC


================================================================================
====

Press [Enter] key to continue...
```

Related Commands

Command	Description
Permanent (Network settings)	Sets up the permanent network settings.
Switch Network Interface	Enable users to switch interfaces.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Switch Network Interface

```
4 System Configuration
   2 Network Setup
      3 Switch Network Interface
```

Description

Enter command option **3** from the Network Setup commands menu to switch interfaces.

- You cannot switch interface from HPE Aruba Networking Central On-Premises CLI to a port slower than 10 Gbps.
- If all nodes are not connected to interfaces with same speed, any addition or replacement of nodes might fail.

Parameter	Description
`Current Interface`	Current connected interface.
`IP Address`	IP address of the cluster.
`Subnet Mask`	Defines the subnet mask for Local; Local, L3; and Distributed, L3 DHCP scopes. The subnet mask and the network determine the size of subnet.
`Gateway`	IP address of the default gateway.
`DNS`	IP address of the DNS server.
`Secondary DNS`	IP address of the secondary DNS server in the network.
`FQDN`	Status of the upgrade in percentage.
`Network Interface`	Connected interface after the network settings are applied.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
```

```
0. exit
Enter option [ 0 - 10 ]: 1
```

From the System Configuration options, select **2** to display the available Network Setup options.

Network Setup Options

```
1. Permanent (Network settings)
2. Temporary (Network settings)
3. Switch Network Interface
4. Network Link Aggregation Setup
====================================
b. back
m. main menu
0. exit

Enter option [ 0 - 4 ]:
```

From the Network Setup options, select **3** to display the switch network interface options.

```
The network interface currently configured is: eno1
Please capture and note down current network configurations for interface,
IP Address, Subnet mask and Gateway before
proceeding further.

Current Network Settings
-------------------------
Current Interface          : eno1
IP Address                 : 10.xx.xxx.xx
Subnet Mask                : 255.xxx.xxx.x
Gateway                    : 10.xx.xxx.xxx
DNS                        : 10.xx.xxx.xxx
Secondary DNS              : 10.xx.xxx.xxx
FQDN                       : copxxxxxx.arubxxx.com

Enter new interface name:
Enter valid interface name: lisst
Enter valid interface name: ens1f0
Configuring the ens1f0 network interface
Interface is up...moving on

Network Settings Being Applied
------------------------------
Network Interface          : ens1f0
IP Address                 : 10.xx.xxx.xx
Subnet Mask                : 255.xxx.xxx.x
Gateway                    : 10.xx.xxx.xxx
DNS                        : 10.xx.xxx.xxx
Secondary DNS              : 10.xx.xxx.xxx
FQDN                       : copxxxxx.arubaxxxx.com

Network settings exist: will be reset to a new value
9f83d89df0f5
Kubernets is up...moving up
deployment.apps/coredns scaled
deployment.apps/coredns scaled
1
```

```
OK
pod "platform-config-platform-uwsgi-deployment-86dc68d4d6" deleted
updating cache, please wait
Interface is updated to ens1f0

Press [Enter] key to continue...
```

Related Commands

Command	Description
Permanent (Network settings)	Sets up the permanent network settings.
Temporary (Network settings)	Sets up the temporary network settings.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Network Link Aggregation

```
4 System Configuration
   2 Network Setup
      4 Network Link Aggregation
```

Description

Prerequisite

Before enabling bonding or LACP from HPE Aruba Networking Central On-Premises side, physically two ports of switch should be connected to two ports of the server (ILO/COP box) using 10G fiber ethernet cables.

Enter command option **4** from the Network Setup commands menu to enable network link aggregation in case of any network breakage.

- Network Link Aggregation(LAG) can be enabled and disabled per node basis only from the ILO console.
- In order for LAG to work end to end, LAG should be enabled or disabled from switch as well as COP side.
- Switching interface is not allowed when LAG is enabled.
- Link Aggregation (LAG) setting will be available only when the cluster setup is completed.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 1
```

From the System Configuration options, select **2** to display the available Network Setup options.

Network Setup Options

```
1. Permanent (Network settings)
2. Temporary (Network settings)
3. Switch Network Interface
```

```
4. Network Link Aggregation Setup
==================================
b. back
m. main menu
0. exit

Enter option [ 0 - 4 ]: 4
```

From the Network Setup options, select **4** to display the network link aggregation options.

Network Link Aggregation Options

```
1. Enable Network Link Aggregation
2. Disable Network Link Aggregation
3. Check status of Network Link Aggregation


================================================================================
====
b. back
m. main menu
0. exit

Enter option [ 0 - 3 ]:
```

Related Commands

Command	Description
Enable Network Link Aggregation	Enables network link aggregation setup.
Disable Network Link Aggregation	Disables network link aggregation setup.
Check Status of Network Link Aggregation	Checks the link network aggregation status in the network.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Enable Network Link Aggregation

```
4 System Configuration
   2 Network Setup
      4 Network Link Aggregation
         1 Enable Network Link Aggregation
```

Description

Enter command option **1** from the Network Link Aggregation Setup commands menu to enable network link aggregation setup.

While enabling network link aggregation (LAG) configuration, it should be first enabled on the COP side, and then it should be enabled on the switch where HPE Aruba Networking Central On-Premises interfaces are connected.

Parameter	Description
`Hostname`	Current connected interface.
`IP Address`	IP address of the cluster.
`Interface`	Connected interface
`Subnet`	Defines the network IP address.
`Gateway`	IP address of the default gateway.
`DNS`	IP address of the DNS server.
`Secondary DNS`	IP address of the secondary DNS server in the network.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 1
```

From the System Configuration options, select **2** to display the available Network Setup options.

Network Setup Options

```
1. Permanent (Network settings)
2. Temporary (Network settings)
3. Switch Network Interface
4. Network Link Aggregation Setup
====================================
b. back
m. main menu
0. exit

Enter option [ 0 - 4 ]: 4
```

From the Network Setup options, select **4** to display the network link aggregation options.

Network Link Aggregation Options

```
1. Enable Network Link Aggregation
2. Disable Network Link Aggregation
3. Check status of Network Link Aggregation


================================================================================
====
b. back
m. main menu
0. exit

Enter option [ 0 - 3 ]:
```

From the Network Link Aggregation options, select **1** to display the enable network link aggregation options.

```
Enter option [ 0 - 3 ]: 1

Network settings exist; will be reset to new value

Network Settings

Hostname       : cop-3node-xxx-xxxx.xxxx.xxxx.arubaxxx.com
IP Address     : 10.xx.xxx.xxx
Interface      : ens1f0
Subnet         : 255.xxx.xxx.x
Gateway        : 10.xx.xxx.xxx
DNS            : 10.xx.xxx.xxx
Secondary DNS  : 10.xx.xxx.xxx

To list available interface, enter 'list'
Enter second interface name for bonding:  ens1f1
8c9a1f7dc7d0
Kubernetes is up...  moving on
Network Link Aggregation Enabled
Press [Enter] key to continue...._
```

Related Commands

Command	Description
Disable Network Link Aggregation	Disables network link aggregation setup.
Check Status of Network Link Aggregation	Checks the network link aggregation status.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Disable Network Link Aggregation

```
4 System Configuration
   2 Network Setup
      4 Network Link Aggregation
         2 Disable Network Link Aggregation
```

Description

Enter command option **2** from the Network Link Aggregation Setup commands menu to disable network link aggregation setup.

While disabling network link aggregation (LAG) configuration , it should be first disabled on the switch side, and then on the COP side, otherwise the node will not be reachable.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 2
```

From the System Configuration options, select **2** to display the available Network Setup options.

Network Setup Options

```
1. Permanent (Network settings)
2. Temporary (Network settings)
3. Switch Network Interface
4. Network Link Aggregation Setup
====================================
b. back
m. main menu
0. exit

Enter option [ 0 - 4 ]: 4
```

From the Network Setup options, select **4** to display the network link aggregation options.

Network Link Aggregation Options

```
1. Enable Network Link Aggregation
2. Disable Network Link Aggregation
3. Check status of Network Link Aggregation


================================================================================
====
b. back
m. main menu
0. exit

Enter option [ 0 - 3 ]: 2
```

From the Network Link Aggregation options, select **2** to display the disable network link aggregation options.

```
This operation will disable Network Link Aggregation on this Node
10.xx.xxx.xxx
Do you want to proceed? (Y/N) ? Y
Disabling Network Link Aggregation
8c9a1f7dc7d0
Kubernetes is up...  moving on
Network Link Aggregation disabled
Press [Enter] key to continue...._
```

Related Commands

Command	Description
Enable Network Link Aggregation	Enables network link aggregation setup.
Check Status of Network Link Aggregation	Checks the network link aggregation status.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Check Status of Network Link Aggregation

```
4 System Configuration
   2 Network Setup
      4 Network Link Aggregation
         3 Check Status of Network Link Aggregation
```

Description

Enter command option **3** from the Network Link Aggregation Setup commands menu to check the network link aggregation status. During the status check a list of all the active ports is displayed.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 2
```

From the System Configuration options, select **2** to display the available Network Setup options.

Network Setup Options

```
1. Permanent (Network settings)
2. Temporary (Network settings)
3. Switch Network Interface
4. Network Link Aggregation Setup
====================================
b. back
m. main menu
0. exit

Enter option [ 0 - 4 ]: 4
```

From the Network Setup options, select **4** to display the network link aggregation options.

Network Link Aggregation Options

```
1. Enable Network Link Aggregation
2. Disable Network Link Aggregation
3. Check status of Network Link Aggregation


================================================================================
====
b. back
m. main menu
0. exit

Enter option [ 0 - 3 ]: 3
```

From the Network Link Aggregation options, select **3** to check the status of network link aggregation options.

```
Network Link Aggregation is enabled on 10.xx.xxx.xxx
Interface Details: \n
Interface:  ens1f0  ::  Status:  Running
Interface:  ens1f1  ::  Status:  Down
Network Link Aggregation not enabled on 10.xx.xxx.xxx
Network Link Aggregation not enabled on 10.xx.xxx.xxx
Press [Enter] key to continue....
```

Related Commands

Command	Description
Enable Network Link Aggregation	Enables network link aggregation setup.
Disable Network Link Aggregation	Disables network link aggregation setup.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Proxy Setup

```
4 System Configuration
   3 Proxy Setup
```

Description

Enter command option **3** from the System Configuration menu to add, delete, or get proxy URL.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 3
```

From the System Configuration options, select **3** to display the available Network Setup options.

Proxy Setup Options

```
1. Add Proxy
2. Delete Proxy
3. Get Proxy
Enter option [ 0 - 3 ]:
```

Related Commands

Command	Description
Add Proxy	Adds a proxy URL.
Delete Proxy	Deletes a proxy URL.
Get Proxy	Enables users to get the details of a proxy URL.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Add Proxy

```
4 System Configuration
   3 Proxy Setup
      1 Add Proxy
```

Description

Enter command option **1** from the Proxy Setup commands menu to add a proxy URL.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 3
```

From the System Configuration options, select **3** to display the available Network Setup options.

Proxy Setup Options

```
1. Add Proxy
2. Delete Proxy
3. Get Proxy
Enter option [ 0 - 3 ]: 1
```

From the Proxy Setup options, select **1** to add proxy options.

```
Enter option [ 0 - 3 ]: 1
Enter the proxy url:
Enter Port:
Enter username(optional):
Enter password(optional):
Enter option [ 0 - 3 ]: 1
Enter the proxy url: www.techxxx.com
Enter port: 98
Enter username(optional):
Enter password(optional):
```

Related Commands

Command	Description
Delete Proxy	Deletes a proxy URL.
Get Proxy	Displays details about the proxy URL.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Delete Proxy

```
4 System Configuration
   3 Proxy Setup
      2 Delete Proxy
```

Description

Enter command option **2** from the Proxy Setup commands menu to delete a proxy URL.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 3
```

From the System Configuration options, select **3** to display the available Network Setup options.

Proxy Setup Options

```
1. Add Proxy
2. Delete Proxy
3. Get Proxy
Enter option [ 0 - 3 ]: 2
```

From the Proxy Setup options, select **2** to delete proxy options.

```
Proxy deleted
Press [Enter] key to continue...
```

Related Commands

Command	Description
Add Proxy	Adds a proxy URL.
Get Proxy	Displays details about the proxy URL.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Get Proxy

```
4 System Configuration
   3 Proxy Setup
      3 Get Proxy
```

Description

Enter command option **3** from the Proxy Setup menu to get the details of a proxy.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 3
```

From the System Configuration options, select **3** to display the available Network Setup options.

Proxy Setup Options

```
1. Add Proxy
2. Delete Proxy
3. Get Proxy
Enter option [ 0 - 3 ]: 1
```

From the Proxy Setup options, select **3** to get proxy options.

```
Enter option [ 0 - 3 ]: 3

  "url": "10.xx.xxx.xxx",
  "username": "admin",
  "password": "",
  "port": "3128"
```

Related Commands

Command	Description
Add Proxy	Adds a proxy URL.
Delete Proxy	Deleted a proxy URL.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Setup Timezone

```
4 System Configuration
   4 Setup Timezone
```

Description

Enter command option **4** from the System Configuration menu to setup a timezone.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 4
```

From the System Configuration options, select **4** to display the Setup Timezone options.

Setup Timezone Options

```
To list timezones, enter 'list'
Enter timezone [UTC]: GMT
Setting TimeZone for other nodes in this cluster...
configmap/airwave-config patched (no change)
Press [Enter] key to continue....
```

Related Commands

Command	Description
Upgrade	Upgrades the HPE Aruba Networking Central On-Premises system for either an online user or an offline user.
Network Setup	Sets up a network permanently or temporarily. It also enables users to switch interface.
Proxy Setup	Adds deletes, or gets the proxy URL.
Setup NTP	Sets up the NTP server.
Node Setup	Sets up a node cluster.

Command	Description
Airgap	Enables or disables Airgap mode for upgrade. Enabling Airgap allows you to upgrade the HPE Aruba Networking Central On-Premises setup offline without any internet access.
Disaster Recovery	Handles upgrade for Datacenter Redundancy in HPE Aruba Networking Central On-Premises network.
Upgrade ILO using ServicePack	Handles the System Configuration menu to upgrade the ILO service pack to keep the system updated with the latest ILO and firmware version.
Autorecovery Maintenance Window	Handles the System Configuration menu to set the auto-recovery maintenance windows.
HPE Networking Support Portal Authentication	Handles the System Configuration menu to log in with your HPE Networking Support Portal (NSP) credentials.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Setup NTP

```
4 System Configuration
   5 Setup NTP
```

Description

Enter command option **5** from the System Configuration menu to setup NTP.

All the nodes in a multi-cluster must synchronize to the same NTP server. Run the command `NTP/Timezone info` to verify if all the nodes are synchronized with the same NTP server. To run the `NTP/Timezone info`, enter command option **2** from the `show configuration` menu.

You also have an option to authenticate the NTP server by using the secure key.

- If you are using iLO when configuring NTP servers and require the secure key to authenticate the NTP server, you must either use the WebUI or CLI to copy the NTP server key. The copy and paste operation is not supported on the iLO console. Logon to the CLI with iLO credentials and use the VSP command to get the secure key.
- If the `Setup NTP` command is executed after the cluster is configured, then the modified details of NTP server is updated to the cluster. If cluster is not configured, then the modified NTP server details is updated only to the node.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 5
```

From the System Configuration options, select **5** to display the Setup NTP options.

Setup NTP Options

```
Enter primary NTP server : 10.xx.xxx.xxx
Enter secondary NTP server (Optional) :10.xx.xxx.xxx
Enter tertiary NTP server (Optional):
Is NTP Authentication required (y/n) :
n
Configuring NTP for node : 10.xx.xxx.xx
FIPS mode initialized
```

```
10.xx.xxx.xxx  NTP configured on node 10.xx.xxx.xxx
10.xx.xxx.xxx  NTP configured on node 10.xx.xxx.xx
FIPS mode initialized
NTP is configured node : 10.xx.xxx.xx
Press [Enter] key to continue...
```

Related Commands

Command	Description
Upgrade	Upgrades the HPE Aruba Networking Central On-Premises system for either an online user or an offline user.
Network Setup	Sets up a network permanently or temporarily. It also enables users to switch interface.
Proxy Setup	Adds deletes, or gets the proxy URL.
Setup Timezone	Sets up the timezone.
Node Setup	Sets up a node cluster.
Airgap	Enables or disables Airgap mode for upgrade. Enabling Airgap allows you to upgrade the HPE Aruba Networking Central On-Premises setup offline without any internet access.
Disaster Recovery	Handles upgrade for Datacenter Redundancy in HPE Aruba Networking Central On-Premises network.
Upgrade ILO using ServicePack	Handles the System Configuration menu to upgrade the ILO service pack to keep the system updated with the latest ILO and firmware version.
Autorecovery Maintenance Window	Handles the System Configuration menu to set the auto-recovery maintenance windows.
HPE Networking Support Portal Authentication	Handles the System Configuration menu to log in with your HPE Networking Support Portal (NSP) credentials.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Node Setup

```
4 System Configuration
   6 Node Setup
```

Description

Enter command option **6** from the System Configuration menu to setup a node.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 6
```

From the System Configuration options, select **6** to display the Node Setup options.

Node Setup Options

```
1. Add node
2. Replace node
3. Status
===================================
b. back
m. main menu
0. exit
Enter option [ 0 - 3 ]:
```

Related Commands

Command	Description
Add Node	Adds IP addresses to the cluster.
Replace Node	Replaces an existing node ip with another in the cluster.
Status	Displays the system operation details.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Add Node

```
4 System Configuration
   6 Node Setup
      1 Add Node
```

Description

Enter command option **1** from the Node Setup menu to add IP addresses to the cluster.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 6
```

From the System Configuration options, select **6** to display the Node Setup options.

Node Setup Options

```
1. Add node
2. Replace node
3. Status
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 3 ]: 1
```

From the Node Setup options, select **1** to display add node options.

```
Are you sure you want to Add the nodes (Y/N):
Enter node ip(s) to be added to the cluster separated by spaces:
```

Related Commands

Command	Description
Replace Node	Replaces an existing node ip with another in the cluster.
Status	Displays the system operation details..

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Replace Node

```
4 System Configuration
   6 Node Setup
      2 Replace Node
```

Description

Enter command option **2** from the Node Setup menu to replace an existing node ip with another in the cluster.

When replacing a node in the cluster, if the user uses the same IP address of the previous node, ensure that the previous node is down.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 6
```

From the System Configuration options, select **6** to display the Node Setup options.

Node Setup Options

```
1. Add node
2. Replace node
3. Status
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 3 ]: 2
```

From the Node Setup options, select **2** to display replace node options.

```
Enter existing node ip to be replaced from the cluster:
Enter new node ip:
```

Related Commands

Command	Description
Add Node	Adds IP addresses to the cluster.
Status	Displays the system operation details..

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Status

```
4 System Configuration
   6 Node Setup
      3 Status
```

Description

Enter command option **3** from the Node Setup menu to view the system operation details.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 6
```

From the System Configuration options, select **6** to display the Node Setup options.

Node Setup Options

```
1. Add node
2. Replace node
3. Status
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 3 ]: 3
```

From the Node Setup options, select **3** to display the status of node setup.

```
Active system operation details
-----------------------------------------
operation type: Replace node
operation state: SUCCESS
start time: Wed Nov 23 15:30:03 UTC 2022
end time: Wed Nov 23 15:45:04 UTC 2022
operation data: Old node - 10.xx.xxx.xxx,  New node - 10.xx.xxx.xxx, Execute
node - 10.xx.xxx.xxx, Job name - platform
- config-node-mgmt-job-gm6z9
-----------------------------------------
```

Related Commands

Command	Description
Add Node	Adds IP addresses to the cluster.
Replace Node	Replaces an existing node ip with another in the cluster.

Command History

Releas	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Airgap

```
4 System Configuration
   7 Airgap
```

Description

Enter command option **7** from the System Configuration menu to enable or disable Airgap mode for offline upgrade. Enabling Airgap allows you to upgrade the HPE Aruba Networking Central On-Premises setup offline without any internet access.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 7
```

From the System Configuration options, select **7** to display the Airgap options.

Airgap Options

```
1. Enable Airgap
2. Disable Airgap
3. Status
====================================
b. back
m. main menu
0. exit
```

Related Commands

Command	Description
Enable Airgap	Enables Airgap mode.
Disable Airgap	Disables Airgap mode.
Status	Checks the Airgap mode status in the network.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Enable Airgap

```
4 System Configuration
   7 Airgap
      1 Enable Airgap
```

Description

Enter command option **1** from the Airgap menu to enable airgap mode for offline upgrade.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 7
```

From the System Configuration options, select **7** to display the Airgap options.

Airgap Options

```
1. Enable Airgap
2. Disable Airgap
3. Status
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 8 ]: 1
```

From the System Configuration options, select **1** to enable Airgap options.

```
Changing of Airgap mode requires restart of services and is recommended ONLY
in maintenance window.Do you want to continue?(Y/N):
```

Related Commands

Command	Description
Disable Airgap	Disables the Airgap mode.
Status	Checks the Airgap mode status.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Disable Airgap

```
4 System Configuration
   7 Airgap
      2 Disable Airgap
```

Description

Enter command option **2** from the Airgap menu to disable the airgap mode.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 7
```

From the System Configuration options, select **7** to display the Airgap options.

Airgap Options

```
1. Enable Airgap
2. Disable Airgap
3. Status
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 8 ]: 2
```

From the System Configuration options, select **2** to disable Airgap options.

```
Airgap is already disabled.
Press [Enter] key to continue...
```

Related Commands

Command	Description
Enable Airgap	Enables the Airgap mode.
Status	Checks the Airgap mode status.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Status

```
4 System Configuration
   7 Airgap
      3 Status
```

Description

Enter command option **3** from the Airgap menu to see the status of the airgap mode.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using ServicePack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 7
```

From the System Configuration options, select **7** to display the Airgap options.

Airgap Options

```
1. Enable Airgap
2. Disable Airgap
3. Status
====================================
b. back
m. main menu
0. exit


Enter option [ 0 - 8 ]: 3
```

From the System Configuration options, select **3** to status of Airgap.

```
Airgap is disabled.
Press [Enter] key to continue...
```

Related Commands

Command	Description
Enable Airgap	Enables the Airgap mode.
Disable Airgap	Disables the Airgap mode.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Disaster Recovery

```
4 System Configuration
   8 Disaster Recovery
```

Description

Enter command option **8** from the System Configuration menu to handle upgrade for Disaster Recovery in HPE Aruba Networking Central On-Premises network.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Disaster Recovery
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 8
```

From the System Configuration options, select **8** to display the Disaster Recovery options.

Disaster Recovery Options

```
1. Show Disaster Recovery Status
2. Show Disaster Recovery Config
3. Disable Disaster Recovery Feature
4. Manual Failover
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 7 ]:
```

Related Commands

Command	Description
Show Disaster Recovery Status	Displays the overall status and infra sync status of the cluster.
Show Disaster Recovery Config	Displays the configuration details.
Disable Disaster Recovery Feature	Disables the disaster recovery feature.
Manual Failover	Enables to trigger a manual failover.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Show Disaster Recovery Status

```
4 System Configuration
   8 Disaster Recovery
      1 Show Disaster Recovery Status
```

Description

Enter command option **1** from the Disaster Recovery commands to display the Disaster Recovery status of the primary cluster.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Disaster Recovery
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 8
```

From the System Configuration options, select **8** to display the Disaster Recovery options.

Show Disaster Recovery Status Options

```
1. Overall Status
2. Infra Sync Status
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 7 ]: 1
```

From the Show Disaster Recovery Status options, select **1** to display the Overall status.

```
Enter option [ 0 - 2 ]:  1

Overall Sync Status            : SUCCESS

Last Successful Sync At        : Tue May 26 09:02:29 AM UTC 2026

Last Synced At                 : Tue May 26 10:03:07 AM UTC 2026

---------------------------------
Current Cluster Status
```

```
-----------------------------------
FQDN                            : central-xxx-xxx-3node.xxxxxxxxxx.xxxxx

Cluster Role                    : PRIMARY

Cluster Status                  : HEALTHY

Heartbeat Status                : SUCCESSFUL

Heartbeat Failed Count          : 0

Last Heartbeat Received At      : Tue May 26 10:07:04 AM UTC 2026

Failover Status                 : NOT_AVAILABLE

Last Failover Time              :

-----------------------------------
Peer Cluster Status
-----------------------------------
FQDN                            : central-xxx-xxx-3node.xxxxxxxxxx.xxxxx

Cluster Role                    : SECONDARY

Cluster Status                  : HEALTHY

Heartbeat Status                : SUCCESSFUL

Heartbeat Failed Count          : 0

Last Heartbeat Received At      : Tue May 26 10:07:18 AM UTC 2026

Failover Status                 : NOT_AVAILABLE

Last Failover Time              :

Press [Enter] key to continue...
```

From the Show Disaster Recovery Status options, select **2** to display the Infra Sync status.

```
Enter option [ 0 - 2 ]:  2
Infra           Sync Start Time                   Sync Completion Time
 Sync Duration  Sync Status   Last Sync Success Time            Failure
Reason
--------------- --------------------------------- --------------------------
------- -------------- ------------- -------------------------------- -----
-------------------------------------------
ArangoDB        Tue May 26 10:02:23 AM UTC 2026   Tue May 26 10:02:27 AM UTC
2026   3s             SUCCESS       Tue May 26 10:02:27 AM UTC 2026   NA
Cassandra       Tue May 26 09:02:38 AM UTC 2026   Tue May 26 09:04:23 AM UTC
2026   1m 44s         SUCCESS       Tue May 26 09:04:23 AM UTC 2026   NA
CockroachDB     Tue May 26 10:02:31 AM UTC 2026   Tue May 26 10:03:07 AM UTC
2026   36s            SUCCESS       Tue May 26 10:03:07 AM UTC 2026   NA
APISIX          Tue May 26 09:02:29 AM UTC 2026   Tue May 26 09:02:29 AM UTC
2026   0s             SUCCESS       Tue May 26 09:02:29 AM UTC 2026   NA
KMS Data        Tue May 26 07:02:27 AM UTC 2026   Tue May 26 07:02:28 AM UTC
2026   0s             SUCCESS       Tue May 26 07:02:28 AM UTC 2026   NA
Kafka           NA                                Tue May 26 10:12:04 AM UTC
2026   NA             SUCCESS       Tue May 26 10:12:04 AM UTC 2026   NA
```

```
MinIO           Tue May 26 09:02:48 AM UTC 2026   Tue May 26 09:17:01 AM UTC
2026   14m 12s         SUCCESS       Tue May 26 09:17:01 AM UTC 2026   NA
PostgreSQL      Tue May 26 09:02:29 AM UTC 2026   Tue May 26 09:10:07 AM UTC
2026   7m 37s          SUCCESS       Tue May 26 09:10:07 AM UTC 2026   NA
Redis           Tue May 26 10:02:23 AM UTC 2026   Tue May 26 10:02:25 AM UTC
2026   1s              SUCCESS       Tue May 26 10:02:25 AM UTC 2026   NA
Vault           Tue May 26 09:02:38 AM UTC 2026   Tue May 26 09:14:45 AM UTC
2026   12m 7s          SUCCESS       Tue May 26 09:14:45 AM UTC 2026   NA
Press [Enter] key to continue...
```

Related Commands

Command	Description
Show Disaster Recovery Status	CLI options available for the Disaster Recovery feature.
Show Disaster Recovery Config	Displays the configuration details.
Disable Disaster Recovery Feature	Disables the disaster recovery feature.
Manual Failover	Enables to trigger a manual failover.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Show Disaster Recovery Config

```
4 System Configuration
   8 Disaster Recovery
      2 Show Disaster Recovery Config
```

Description

Enter command option **2** from the Disaster Recovery options to view the configuration.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Disaster Recovery
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 8
```

From the Disaster Recovery options, select **2** to view the configuration status.

```
Enter option [ 0 - 4 ]:  2

Time to Failover (Minutes)              :   240

Automatic Failover                      :   Disabled

-----------------------------------
Current Cluster configuration
-----------------------------------
FQDN                                    :   central-xxx-xxx-
3node.xxxxxxxx.xxx

version                                 :   3.0.3.0

Preferred Role                          :   PRIMARY

Node Count                              :   3

-----------------------------------
Peer Cluster configuration
-----------------------------------
FQDN                                    :   central-xxx-xxx-
3node.xxxxxxxx.xxx

version                                 :   3.0.3.0
```

```
Preferred Role                          :   SECONDARY

Node Count                              :   3

Press [Enter] key to continue...
```

Related Commands

Command	Description
Show Disaster Recovery Config	CLI options available for the Disaster Recovery feature.
Show Disaster Recovery Status	Displays the overall status and infra sync status of the cluster.
Disable Disaster Recovery Feature	Disables the disaster recovery feature.
Manual Failover	Enables to trigger a manual failover.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Disable Disaster Recovery Feature

```
4 System Configuration
   8 Disaster Recovery
        3 Disable Disaster Recovery Feature
```

Description

Enter option **3** from the Disaster Recovery command to disable disaster recovery. You can also disable Disaster Recovery from the HPE Aruba Networking Central On-Premises WebUI.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Disaster Recovery
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 8
```

From the System Configuration options, select **8** to display the Disaster Recovery options.

Disaster Recovery Options

```
1. Show Disaster Recovery Status
2. Show Disaster Recovery Config
3. Disable Disaster Recovery Feature
4. Manual Failover
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 7 ]: 2
```

From the Disaster Recovery options, select **3** to disable the Disaster Recovery.

```
Enter option [ 0 - 4 ]:  3
Changing the Recovery mode may impact services. It is recommended to change
the mode during a maintenance window. Do you want to proceed?(Y/N):
```

Enter Y to confirm and disable the DR.

After DR is successfully disabled, the secondary cluster transitions to a fully active state.

NOTE

The scaling up of services on the secondary cluster may take approximately 20–30 minutes to complete.

Related Commands

Command	Description
Disable Disaster Recovery Feature	CLI options available for the Disaster Recovery feature.
Show Disaster Recovery Status	Displays the overall status and infra sync status of the cluster.
Show Disaster Recovery Config	Displays the configuration details.
Manual Failover	Enables to trigger a manual failover.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Manual Failover

```
4 System Configuration
   8 Disaster Recovery
        4 Manual Failover
```

Description

Enter option **4** from the Disaster Recovery command to initiate a manual failover.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Disaster Recovery
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 8
```

From the Disaster Recovery options, select **4** to trigger a failover.

```
Enter option [ 0 - 4 ]:  4
Warning: Failover will be initiated. Devices may disconnect and come up on
the new primary. Do you want to continue (Y/N)?
```

Enter Y to confirm and trigger a failover.

Related Commands

Command	Description
Manual Failover	CLI options available for the Disaster Recovery feature.
Show Disaster Recovery Status	Displays the overall status and infra sync status of the cluster.
Show Disaster Recovery Config	Displays the configuration details.
Disable Disaster Recovery Feature	Disables the disaster recovery feature.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Upgrade ILO using ServicePack

```
4 System Configuration
   9 Upgrade ILO using ServicePack
```

Description

Enter command option **9** from the System Configuration menu to upgrade the ILO service pack to keep the system updated with the latest ILO and firmware version.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance Window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 9
```

From the System Configuration options, select **9** to Upgrade the ILO using Service Pack.

Upgrade ILO using Service Pack Options

```
1. Trigger ILO upgrade using ServicePack
2. Check ILO ServicePack version
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 2 ]:
```

Related Commands

Command	Description
Trigger ILO upgrade ServicePack	Triggers the upgrade of the service pack from the ILO console.
Check ILO ServicePack version	Checks the version of the service pack.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Trigger ILO upgrade ServicePack

```
4 System Configuration
   9 Upgrade ILO using ServicePack
      1 Trigger ILO upgrade using ServicePack
```

Prerequisite

- Download new ILO Service Pack from HPE Support Portal, HPE Support Center.
- Download custom patched Service Pack by HPE from, SPP Custom Download.

HPE Aruba Networking Central On-Premises supports "2022.09.01.00" or higher service pack versions.

- For a fast and simultaneous installation of the SP ISO image, host the SP ISO image on the webserver for example, apache which is used to mount the ISO from ILO virtual disk option.

Description

Enter command option **1** from the Upgrade ILO using Service Pack commands to upgrade the Service Pack. Before upgrading the service pack, the system checks if there is any node down, replace node is in process, or add node is in process.

This menu 4-9-1, can only be triggered from a physical or remote ILO console. If you trigger it from the COP console it displays an error.

Admins must login to the ILO console after ILO goes to showdown mode and reset the ILO using the Service Pack downloaded from the HPE Support Portal.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance Window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 9
```

From the System Configuration options, select **9** to Upgrade the ILO using Service Pack.

Upgrade ILO using Service Pack Options

```
1. Trigger ILO upgrade using ServicePack
2. Check ILO ServicePack version
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 2 ]: 1
```

From the Upgrade ILO using Service Pack options, select **1** to Trigger the ILO upgrade using Service Pack.

```
Error: Please run ServicePack upgrade from physical or remote console (ILO)
Press [Enter] key to continue...
```

Related Commands

Command	Description
Check ILO ServicePack version	Checks the version of the service pack.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Check ILO ServicePack version

```
4 System Configuration
   9 Upgrade ILO using ServicePack
      2 Check ILO ServicePack version
```

Description

Enter command option **2** from the Upgrade ILO using Service Pack commands to check the service pack version that is applied.

HPE Aruba Networking Central On-Premises supports "2022.09.01.00" or higher service pack versions.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance Window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 9
```

From the System Configuration options, select **9** to Upgrade the ILO using Service Pack.

Upgrade ILO using Service Pack Options

```
1. Trigger ILO upgrade using ServicePack
2. Check ILO ServicePack version
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 2 ]: 2
```

From the Upgrade ILO using Service Pack options, select **2** to check the ILO Service Pack versions.

```
Installed : RAID: "6.22" ;ILO5: "3.00 Dec 14 2023" ; ROM:"U32 v2.90
(07/20/2023)" ; NIC:"11.1.5"
Firmware Version on ILO 10.xx.xxx.xx: Installed : RAID: "6.22" ; ILO5: "3.00
Dec 14 2023" ; ROM:"U32 v2.90 (07/20/2023)" ; NIC:"11.1.1"
Press [Enter] key to continue...
```

Related Commands

Command	Description
Trigger ILO upgrade ServicePack	Triggers the upgrade of the service pack from the ILO console.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Autorecovery Maintenance Window

```
4 System Configuration
   10 Autorecovery Maintenance Window
```

Description

Enter command option **10** from the System Configuration menu to set the auto-recovery maintenance windows.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance Window
11. HPE Networking Support Portal Authentication
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 10
```

From the System Configuration options, select **10** to set the auto-recovery maintenance windows.

.

Autorecovery Maintenance Options

```
Current Maintenance window is set to ANYTIME

1. Update current window
2. Exit
Choose an option [1-2]:
```

Related Commands

Command	Description
Update current window	Updates the setting of the auto recovery maintenance window.
Exit	Exits the auto recovery setting without any change.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Update current window

```
4 System Configuration
   10 Autorecovery Maintenance Window
     1 Update current window
```

Description

Enter command option **1** from the Autorecovery Maintenance menu to update the current auto recovery maintenance window.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 10
```

From the System Configuration options, select **10** to set the auto-recovery maintenance windows.
.

Autorecovery Maintenance Options

```
Current Maintenance window is set to ANYTIME

1. Update current window
2. Exit
Choose an option [1-2]: 1
```

From the Autorecovery maintenance options, select **1** to update the auto recovery maintenance window settings.

```
Select Maintenance window type :-
1. Anytime (Recommended - reboots automatically while preserving HA)

2. Set Window (set a day and time for reboots)
3. Never (not recommended - system will never reboot)
Enter choice [1-3]:
```

Related Commands

Command	Description
Exit	Exits the auto recovery setting without any change.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Anytime (Recommended - reboots automatically while preserving HA)

```
4 System Configuration
   10 Autorecovery Maintenance Window
     1 Update current window
      1 Anytime (Recommended - reboots automatically while preserving HA)
```

Description

Enter command option **1** from the Update Current Window menu to set the auto recovery option to anytime automatically.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance Window
11. HPE Networking Support Portal Authentication
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 10
```

From the System Configuration options, select **10** to set the auto-recovery maintenance windows.

Autorecovery Maintenance Options

```
Current Maintenance window is set to ANYTIME

1. Update current window
2. Exit
Choose an option [1-2]: 1
```

From the Autorecovery maintenance options, select **1** to update the auto recovery maintenance window settings.

Next Options

```
Select Maintenance window type :-
1. Anytime (Recommended - reboots automatically while preserving HA)

2. Set Window (set a day and time for reboots)
3. Never (not recommended - system will never reboot)
```

```
Enter choice [1-3]: 1
```

From the previous option, select **1** to update the auto recovery maintenance window to anytime. It is recommended to trigger reboot automatically while preserving High Availability (HA).

```
Autorecovery maintenance window set to ANYTIME

Press [Enter] key to continue...
```

Related Commands

Command	Description
Set Window (set a day and time for reboots)	Enables to set up auto recovery of the current window to a specific date and time.
Never (Not recommended - system will never reboot)	Enables you to disable auto recovery of the current window.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Set Window (set a day and time for reboots)

```
4 System Configuration
   10 Autorecovery Maintenance Window
     1 Update current window
      2 Set Window (set a day and time for reboots)
```

Description

Enter command option **2** from the Update Current Window menu to set the auto recovery option to a specific day and time.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance Window
11. HPE Networking Support Portal Authentication
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 10
```

From the System Configuration options, select **10** to set the auto-recovery maintenance windows.

Autorecovery Maintenance Options

```
Current Maintenance window is set to ANYTIME

1. Update current window
2. Exit
Choose an option [1-2]: 1
```

From the Autorecovery maintenance options, select **1** to update the auto recovery maintenance window settings.

Next Options

```
Select Maintenance window type :-
1. Anytime (Recommended - reboots automatically while preserving HA)

2. Set Window (set a day and time for reboots)
3. Never (not recommended - system will never reboot)
Enter choice [1-3]: 2
```

From the previous options, select **2** to set the auto recovery maintenance window to a specific day and time.

```
Choose a day of the week to run maintenance[1-7]:-

1. Sunday
2. Monday
3. Tuesday
4. Wednesday
5. Thursday
6. Friday
7. Saturday
Enter choice [1-7]: 2
```

Select the required option from the list from the weekdays displayed.

```
Enter time for Maintenance window:-
Enter time [1-12 hrs]: 2
Enter time [0-59 min]: 34
Choose Meridem(AM/PM) of time:-
1. AM
2. PM
Select Meridem [1-2]:1
```

Enter the required time stamp to start the auto recovery maintenance window.

```
Maintenance window will start at Monday 02:34 AM GMT
Do you want to confirm the change(Y/N)?
```

Related Commands

Command	Description
Anytime (Recommended - reboots automatically while preserving HA)	Enables to set auto recovery of the current window anytime automatically.
Never (Not recommended - system will never reboot)	Enables you to disable auto recovery of the current window.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Never (Not recommended - system will never reboot)

```
4 System Configuration
   10 Autorecovery Maintenance Window
     1 Update current window
      3 Never (Not recommended - system will never reboot)
```

Description

Enter command option **3** from the Update Current Window menu to disable auto recovery of the current window.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance Window
11. HPE Networking Support Portal Authentication
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 10
```

From the System Configuration options, select **10** to set the auto-recovery maintenance windows.

Autorecovery Maintenance Options

```
Current Maintenance window is set to ANYTIME

1. Update current window
2. Exit
Choose an option [1-2]: 1
```

From the Autorecovery maintenance options, select **1** to update the auto recovery maintenance window settings.

Next Options

```
Select Maintenance window type :-
1. Anytime (Recommended - reboots automatically while preserving HA)

2. Set Window (set a day and time for reboots)
3. Never (not recommended - system will never reboot)
Enter choice [1-3]: 3
```

From the previous options, select **3** to set the auto recovery maintenance window to never reboot the system.

```
Autorecovery maintenance window set to NEVER (Not recommended)
Press [Enter] key to continue...
```

Related Commands

Command	Description
Anytime (Recommended - reboots automatically while preserving HA)	Enables to set auto recovery of the current window anytime automatically.
Set Window (set a day and time for reboots)	Enables to set up auto recovery of the current window to a specific date and time.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0.8	Command introduced.

Exit

```
4 System Configuration
   10 Autorecovery Maintenance Window
     2 Exit
```

Description

Enter command option **2** from the Autorecovery Maintenance menu to exit the auto recovery settings of the current window.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 10
```

From the System Configuration options, select **10** to set the auto-recovery maintenance windows.
.

Autorecovery Maintenance Options

```
Current Maintenance window is set to ANYTIME

1. Update current window
2. Exit
Choose an option [1-2]: 2
```

From the Autorecovery maintenance options, select **2** to exit the auto recovery maintenance window settings.

```
No changes made! Exiting.
Press [Enter] key to continue...
```

Related Commands

Command	Description
Update current window	Updates the setting of the auto recovery maintenance window.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

HPE Networking Support Portal Authentication

```
4 System Configuration
   11 HPE Networking Support Portal Authentication
```

Description

Enter command option **11** from the System Configuration menu to log in with your HPE Networking Support Portal (NSP) credentials.

Parameter	Description
`Username`	Username for your NSP account.
`Password`	Password for your NSP account.

System Configuration Options

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Air Gap
8. Datacenter Redundancy
9. Upgrade ILO using Service Pack
10. Autorecovery Maintenance window
11. HPE Networking Support Portal Authentication
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 10 ]: 11
```

From the System Configuration options, select **11** to log in with your NSP credentials.

Related Commands

Command	Description
Upgrade	Upgrades the HPE Aruba Networking Central On-Premises system for either an online user or an offline user.
Network Setup	Sets up a network permanently or temporarily. It also enables users to switch interface.
Proxy Setup	Adds deletes, or gets the proxy URL.
Setup Timezone	Sets up the timezone.
Setup NTP	Sets up the NTP server.

Command	Description
Node Setup	Sets up a node cluster.
Airgap	Enables or disables Airgap mode for upgrade. Enabling Airgap allows you to upgrade the HPE Aruba Networking Central On-Premises setup offline without any internet access.
Disaster Recovery	Handles upgrade for Datacenter Redundancy in HPE Aruba Networking Central On-Premises network.
Upgrade ILO using ServicePack	Handles the System Configuration menu to upgrade the ILO service pack to keep the system updated with the latest ILO and firmware version.
Autorecovery Maintenance Window	Handles the System Configuration menu to set the auto-recovery maintenance windows.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Advanced

```
5 Advanced
```

Description

Enter the command option **5** from the main menu to access the advanced options.

Hierarchy Level

```
5 Advanced
   5-1 Test Connectivity
      5-1-1 Ping
      5-1-2 Dependent Servers Reachability
   5-2 NsLookup
   5-3 Configure ILO IP
   5-4 Enable or Disable NOPASSWORD for copadmin
      5-4-1 Enable NOPASSWORD
      5-4-2 Disable NOPASSWORDs
   5-5 IPsec Management
      5-4-1 Initiate IPsec
      5-4-2 Enable IPsec
      5-4-3 Disable IPsec
      5-4-4 IPsec Status
      5-4-5 Reset IPsec clusterwide
   5-6 Troubleshooting Cluster
   5-7 Test Bandwidth
```

Enter the command option **5** from the main menu to view all the advanced commands supported.

Main Menu Options

```
1. System
2. File Operations
3. Show
4. System Configuration
5. Advanced
6. Security
7. Support
8. Temporary Root Shell
9. Authentication
10. Certificate configuration
11. Search commands
===================================
0. exit

Enter option [ 0 - 11 ]: 5

============================
```

From the previous menu option, select **5** to display the Advanced options.

```
1. Test Connectivity
2. NsLookup
3. Configure ILO IP
4. Enable or Disable NOPASSWORD for copadmin
```

```
5. IPsec Management
6. Troubleshoot Cluster
7. Test Bandwidth
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 5 ]:
```

Related Commands

Command	Description
Test Connectivity	Tests the connectivity status.
NsLookup	Queries the DNS records.
Configure ILO IP	Configures the ILO IP.
Enable or Disable NOPASSWORD for Copadmin	Enables or disables NOPASSWORD for copadmin
IPsec Management	IPsec Management
Troubleshooting Cluster	Troubleshooting Cluster
Test Bandwidth	Test Bandwidth

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.3.0	Command introduced.

Test Connectivity

```
5 Advanced
   1 Test Connectivity
```

Description

Enter the command option **1** from the Advanced commands menu to test connectivity.

Advanced Options

```
1. Test Connectivity
2. NsLookup
3. Configure ILO IP
4. Enable or Disable NOPASSWORD for copadmin
5. IPsec Management
6. Troubleshoot Cluster
7. Test Bandwidth
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 5 ]: 1
```

From the Advanced menu options, select **1** to display the test connectivity options:

```
1. Ping
2. Dependent Servers Reachability
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 2 ]:
```

Related Commands

Command	Description
Ping	Enables to ping the host.
Dependent Servers Reachability	Enables to check dependent servers reachability.

Command HistoryCommand History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced

Ping

```
5 Advanced
   1 Test Connectivity
      1 Ping
```

Descriptions

Enter command option **1** from the Test Connectivity commands menu to ping the host. Enter the IP address and hostname to start the ping.

Advanced Options

```
1. Test Connectivity
2. NsLookup
3. Configure ILO IP
4. Enable or Disable NOPASSWORD for copadmin
5. IPsec Management
6. Troubleshoot Cluster
7. Test Bandwidth
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 5 ]: 1
```

From the Advanced menu options, select **1** to display the test connectivity options.

```
1. Ping
2. Dependent Servers Reachability
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 2 ]: 1
```

From the Test Connectivity menu options, select **1** to ping the host.

```
Enter the IP address and hostname to ping:
```

Related Commands

Command	Description
Dependent Servers Reachability	Enables to check reachability of dependent servers.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Dependent Servers Reachability

```
5 Advanced
   1 Test Connectivity
      2 Dependent Servers Reachability
```

Descriptions

Enter command option **2** from the Test Connectivity commands menu to check the reachability of the dependent servers.

Advanced Options

```
1. Test Connectivity
2. NsLookup
3. Configure ILO IP
4. Enable or Disable NOPASSWORD for copadmin
5. IPsec Management
6. Troubleshoot Cluster
7. Test Bandwidth
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 5 ]: 1
```

From the Advanced menu options, select **1** to display the test connectivity options.

```
1. Ping
2. Dependent Servers Reachability
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 2 ]: 2
```

From the Test Connectivity menu options, select **2** to display the dependent search reachability.

```
Connecting to coreupdate(coreupdate.central.arubanetworks.com) ...
Connection to coreupdate (coreupdate.central.arubanetworks.com) successful.
Connecting to coreupdate(coreupdate-prod.central.arubanetworks.com) ...
Connection to coreupdate (coreupdate-prod.central.arubanetworks.com)
successful.
Connecting to quay(quay.io) ...
Connection to quay  (quay.io) successful.
Connecting to nexus(nexus2.airwave.com) ...
Connection to nexus(nexus2.airwave.com) successful.
----- All dependent HTTP(S) servers are reachable -----
DNS resolution successful for all dependent servers.
Press [Enter] key to continue...
```

Related Commands

Command	Description
Ping	Enables to ping the host.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

NsLookup

```
5 Advanced
   2 NsLookup
```

Description

Enter the command option **2** from the Advanced commands menu to query the DNS records for a given domain name.

Advanced Options

```
1. Test Connectivity
2. NsLookup
3. Configure ILO IP
4. Enable or Disable NOPASSWORD for copadmin
5. IPsec Management
6. Troubleshoot Cluster
7. Test Bandwidth
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 5 ]: 2
```

From the previous menu options, select **2** for the NsLookup operation.

```
Enter the hostname or IP Address for NS Lookup:
```

Related Commands

Command	Description
Test Connectivity	Tests the connectivity status.
Toggle CDN	Toggles the CDN.
Configure ILO IP	Configures the ILO IP.
Enable or Disable NOPASSWORD for Copadmin	Enables or disables NOPASSWORD for copdamin.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Configure ILO IP

```
5 Advanced
   3 Configure ILO IP
```

Description

Enter the command option **3** from the Advanced commands menu to configure the ILO IP address.

Advanced Options

```
1. Test Connectivity
2. NsLookup
3. Configure ILO IP
4. Enable or Disable NOPASSWORD for copadmin
5. IPsec Management
6. Troubleshoot Cluster
7. Test Bandwidth
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 5 ]: 3
```

From the previous menu options, select **3** to configure the ILO IP address.

Related Commands

Command	Description
Test Connectivity	Tests the connectivity status.
NsLookup	Queries the DNS record.
Toggle CDN	Enables to toggle the CDN.
Enable or Disable NOPASSWORD for Copadmin	Enable or disable NOPASSWORD for copdamin

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Enable or Disable NOPASSWORD for Copadmin

```
5 Advanced
   4 Enable or Disable NOPASSWORD for copadmin
```

Description

Enter the command option **5** from the Advanced commands menu to enable or disable the **NOPASSWORD** option for the copadmin.

Advanced Options

```
1. Test Connectivity
2. NsLookup
3. Configure ILO IP
4. Enable or Disable NOPASSWORD for copadmin
5. IPsec Management
6. Troubleshoot Cluster
7. Test Bandwidths
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 5 ]: 4
```

From the previous menu options, select **4** to display the **Enable or Disable NOPASSWORD for copadmin** options.

```
1. Enable NOPASSWORD
2. Disable NOPASSWORD
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 2 ]:
```

Related Commands

Command	Description
Enable NOPASSWORD for Copadmin	Enables the **NOPASSWORD** option for the copadmin.
Disable NOPASSWORD for Copadmin	Disables the **NOPASSWORD** option for the copadmin.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 2.5.x	Command introduced.

Enable NOPASSWORD for Copadmin

```
5 Advanced
   4 Enable or Disable NOPASSWORD for copadmin
      1 Enable NOPASSWORD
```

Descriptions

Enter command option **1** from the Enable or Disable NOPASSWORD for copadmin commands menu to enable the **NOPASSWORD** option for the copadmin.

Advanced Options

```
1. Test Connectivity
2. NsLookup
3. Configure ILO IP
4. Enable or Disable NOPASSWORD for copadmin
5. IPsec Management
6. Troubleshoot Cluster
7. Test Bandwidths
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 5 ]: 5
```

From the previous menu options, select **4** to display the **Enable or Disable NOPASSWORD for copadmin** options.

Enable or Disable NOPASSWORD for copadmin Options

```
1. Enable NOPASSWORD
2. Disable NOPASSWORD
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 2 ]: 1
```

From the previous menu, enter **1** to enable the **NOPASSWORD** option for copadmin.

```
Are you sure you want to proceed (y/n)?:
```

Related Commands

Command	Description
Disable NOPASSWORD for Copadmin	Disables the **NOPASSWORD** option for the copadmin.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 2.5.x	Command introduced.

Disable NOPASSWORD for Copadmin

```
5 Advanced
   4 Enable or Disable NOPASSWORD for copadmin
      2 Disable NOPASSWORDs
```

Descriptions

Enter command option **2** from the Enable or Disable NOPASSWORD for copadmin commands menu to enable the **NOPASSWORD** option for the copadmin.

Advanced Options

```
1. Test Connectivity
2. NsLookup
3. Configure ILO IP
4. Enable or Disable NOPASSWORD for copadmin
5. IPsec Management
6. Troubleshoot Cluster
7. Test Bandwidths
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 5 ]: 4
```

From the previous menu options, select **4** to display the **Enable or Disable NOPASSWORD for copadmin** options.

Enable or Disable NOPASSWORD for copadmin Options

```
1. Enable NOPASSWORD
2. Disable NOPASSWORD
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 2 ]: 2
```

From the previous menu, enter **2** to disable the **NOPASSWORD** option for copadmin.

```
Are you sure you want to proceed (y/n)?:
```

Related Commands

Command	Description
Enable NOPASSWORD for Copadmin	Enables the NOPASSWORD option for the copadmin.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 2.5.x	Command introduced.

IPsec Management

```
5 Advanced
   5 IPsec Management
```

Description

Enter the command option **5** from the Advanced commands menu to view the IPsec Management.

Advanced Options

```
1. Test Connectivity
2. NsLookup
3. Configure ILO IP
4. Enable or Disable NOPASSWORD for copadmin
5. IPsec Management
6. Troubleshoot Cluster
7. Test Bandwidth
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 5 ]: 5
```

From the previous menu options, select **5** to display the **IPsec Management** options:

```
1. Initiate IPsec
2. Enable IPsec
3. Disable IPsec
4. IPsec status
5. Reset IPsec clusterwide
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 3 ]:
```

Related Commands

Command	Description
Initiate IPsec	Initiate IPsec
Enable IPsec	Enable IPsec

Command	Description
Disable IPsec	Disable IPsec
IPsec Status	IPsec status
Reset IPsec Clusterwide	Reset IPsec clusterwide

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.4.0	Command introduced

Initiate IPsec

```
5 Advanced
   5 IPsec Management
      1 Initiate IPsec
```

Description

Enter the command option **5** from the Advanced commands menu to view the IPsec Management.

Advanced Options

```
1. Test Connectivity
2. NsLookup
3. Configure ILO IP
4. Enable or Disable NOPASSWORD for copadmin
5. IPsec Management
6. Troubleshoot Cluster
7. Test Bandwidth
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 5 ]: 5
```

From the previous menu options, select **5** to display the **IPsec Management** options:

Initiate IPsec Option

```
1. Initiate IPsec
2. Enable IPsec
3. Disable IPsec
4. IPsec status
5. Reset IPsec clusterwide
====================================
```

```
b. back
m. main menu
0. exit
Enter option [ 0 - 3 ]:1
```

From the previous menu, enter **1** to initiate IPsec for the first time in the cluster. Initiate IPsec operation includes certificate creation, copying certificated to all available nodes and bringing up IPsec tunnel between different nodes in a full mesh topology. By default IPsec is in a disabled state.

Related Commands

Command	Description
Enable IPsec	Enable IPsec
Disable IPsec	Disable IPsec
IPsec Status	IPsec status
Reset IPsec Clusterwide	Reset IPsec clusterwide

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.4.0	Command introduced

Enable IPsec

```
5 Advanced
   5 IPsec Management
      2 Enable IPsec
```

Description

Enter the command option **5** from the Advanced commands menu to view the IPsec Management.

Advanced Options

```
1. Test Connectivity
2. NsLookup
3. Configure ILO IP
4. Enable or Disable NOPASSWORD for copadmin
5. IPsec Management
6. Troubleshoot Cluster
7. Test Bandwidth
==================================
b. back
```

```
m. main menu
0. exit
Enter option [ 0 - 5 ]: 5
```

From the previous menu options, select **5** to display the **IPsec Management** options:

Enable IPsec Option

```
1. Initiate IPsec
2. Enable IPsec
3. Disable IPsec
4. IPsec status
5. Reset IPsec clusterwide
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 3 ]:2
```

From the previous menu, select **2** to enable IPsec. When IPsec is enabled for the first time, its status changes to **Enabled**. Use this option only if IPsec has been disabled using Option 3.

Related Commands

Command	Description
Initiate IPsec	Initiate IPsec
Disable IPsec	Disable IPsec
IPsec Status	IPsec status
Reset IPsec Clusterwide	Reset IPsec clusterwide

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.4.0	Command introduced

Disable IPsec

```
5 Advanced
   5 IPsec Management
      3 Disable IPsec
```

Description

Enter the command option **5** from the Advanced commands menu to view the IPsec Management.

Advanced Options

```
1. Test Connectivity
2. NsLookup
3. Configure ILO IP
4. Enable or Disable NOPASSWORD for copadmin
5. IPsec Management
6. Troubleshoot Cluster
7. Test Bandwidth
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 5 ]: 5
```

From the previous menu options, select **5** to display the **IPsec Management** options:

Disable IPsec Option

```
1. Initiate IPsec
2. Enable IPsec
3. Disable IPsec
4. IPsec status
5. Reset IPsec clusterwide
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 3 ]:2
```

From the previous menu, enter **3** to disable IPsec.

Related Commands

Command	Description
Initiate IPsec	Initiate IPsec
Enable IPsec	Enable IPsec
IPsec Status	IPsec status
Reset IPsec Clusterwide	Reset IPsec clusterwide

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.4.0	Command introduced

IPsec Status

```
5 Advanced
   5 IPsec Management
      4 IPsec Status
```

Description

Enter the command option **5** from the Advanced commands menu to view the IPsec Management.

Advanced Options

```
1. Test Connectivity
2. NsLookup
3. Configure ILO IP
4. Enable or Disable NOPASSWORD for copadmin
5. IPsec Management
6. Troubleshoot Cluster
7. Test Bandwidth
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 5 ]: 5
```

From the previous menu options, select **5** to display the **IPsec Management** options:

IPsec Status Option

```
1. Initiate IPsec
2. Enable IPsec
3. Disable IPsec
4. IPsec status
5. Reset IPsec clusterwide
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 3 ]:4
```

From the previous menu, enter **4** to view the current status of IPsec in the cluster. The IPsec status tables display the following information related to the tunnels created between the nodes.

Parameter	Description
Node	Name assigned to the node
IP	IP address of the node
Role	Role assigned to the node such as Backup and VIP
Service	Service status of the node
Tunnels	List down all the expected tunnels created between the nodes
Status	Current status of the tunnels

Parameter	Description
Estimated Time	Displays the time duration for which the tunnel has been connected.

Related Commands

Command	Description
Initiate IPsec	Initiate IPsec
Enable IPsec	Enable IPsec
Disable IPsec	Disable IPsec
Reset IPsec Clusterwide	Reset IPsec Clusterwide

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.4.0	Command introduced

Reset IPsec Clusterwide

```
5 Advanced
   5 IPsec Management
      5 Reset IPsec clusterwide
```

Description

Enter the command option **5** from the Advanced commands menu to view the IPsec Management.

Advanced Options

```
1. Test Connectivity
2. NsLookup
3. Configure ILO IP
4. Enable or Disable NOPASSWORD for copadmin
5. IPsec Management
6. Troubleshoot Cluster
7. Test Bandwidth
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 5 ]: 5
```

From the previous menu options, select **5** to display the **IPsec Management** options:

Reset IPsec Clusterwide Option

```
1. Initiate IPsec
2. Enable IPsec
3. Disable IPsec
4. IPsec status
5. Reset IPsec clusterwide
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 3 ]:5
```

From the previous menu, enter 5 to reset the IPsec configuration for all the clusters. All the tunnels and certificates are removed.

Related Commands

Command	Description
Initiate IPsec	Initiate IPsec
Enable IPsec	Enable IPsec
Disable IPsec	Disable IPsec
IPsec Status	IPsec status

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.4.0	Command introduced

Troubleshooting Cluster

```
5 Advanced
   6 Troubleshooting Cluster
```

Description

Enter the command option **6** from the Advanced commands menu to view the Troubleshooting Cluster.

Advanced Options

```
1. Test Connectivity
2. NsLookup
3. Configure ILO IP
4. Enable or Disable NOPASSWORD for copadmin
5. IPsec Management
6. Troubleshoot Cluster
```

```
7. Test Bandwidth
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 5 ]: 6
```

From the previous menu options, select **6** to display the **Troubleshooting Cluster** options:

Related Commands

Command	Description

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced

Test Bandwidth

```
5 Advanced
   7 Test Bandwidth
```

Description

Enter the command option **7** from the Advanced commands menu to Test Bandwidth.

Advanced Options

```
1. Test Connectivity
2. NsLookup
3. Configure ILO IP
4. Enable or Disable NOPASSWORD for copadmin
5. IPsec Management
6. Troubleshoot Cluster
7. Test Bandwidth
==================================
b. back
```

```
m. main menu
0. exit
Enter option [ 0 - 5 ]: 7
```

From the previous menu options, select **7** to display the **Test Bandwidth** options:

Related Commands

Command	Description

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced

Security

```
6 Security
```

Description

Enter the command option **6** from the main menu to access the security options.

Hierarchy Level

```
6 Security
   6-1 Reset Password GUI
   6-2 Reset Password CLI
   6-3 Reset debug apps password
   6-4 Reset ILO Administrator Password
```

Enter the command option **6** from the main menu to view all the security commands supported.

Main Menu Options

```
1. System
2. File Operations
3. Show
4. System Configuration
5. Advanced
6. Security
7. Support
8. Temporary Root Shell
9. Authentication
10. Certificate configuration
11. Search commands
==================================
0. exit

Enter option [ 0 - 11 ]: 6

============================
```

From the previous menu option, select **6** to display Security options.

```
1. Reset Password GUI
2. Reset Password CLI
3. Reset debug apps password
4. Reset ILO Administrator Password
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 4 ]:
```

Related Commands

Command	Description
Reset GUI Admin Password	Resets the GUI admin user password.
Reset CLI Admin Password	Resets the CLI admin user password.
Reset Debug Apps Password	Resets the debug apps password.
Reset ILO Administrator Password	Resets the ILO admin user password.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Reset GUI Admin Password

```
6 Security
   1 Reset Password GUI
```

Description

Enter the command option **1** from the Security commands menu to reset the GUI admin password.

Security Options

```
1. Reset Password GUI
2. Reset Password CLI
3. Reset debug apps password
4. Reset ILO Administrator Password
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 4 ]: 1
```

From the previous menu options, select **1** to display the GUI to reset the password.

```
Do you want to reset GUI admin user password(y/n) :
```

Table 5: *Password Requirements*

Requirement	Description
Password length	The minimum number of alphanumeric characters required for a password is **14**. Range: 14 - 48 (combination of alphabets, numbers, and special characters).
Password character	Password should contain at least **5** unique characters. The password should not contain the strings of username in any form. Password must not contain more than two identical characters consecutively.
Upper Case characters	Use a minimum of 1 uppercase alphabet in password. Alphabets **A** to **Z**.
Lower Case characters	Use a minimum of 1 lowercase alphabet in password. Alphabets **a** to **z**.
Numbers	Use a minimum of 1 digit (number) in password. Numbers **0** - **9**.
Special characters	Use a minimum of 5 special character in password. Supported special characters are **~**, **!**, **@**, **#**, **$**, **%**, **^**, **&**, *****, **(**, **)**, **<**, **>**, **{**, **}**, **;**, **:**, **.** and **,**.

Related Commands

Command	Description
Reset CLI Admin Password	Resets the copadmin user password.
Reset Debug Apps Password	Resets the debug apps password.
Reset ILO Administrator Password	Resets the ILO admin user password.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced

Reset CLI Admin Password

```
6 Security
   2 Reset Password CLI
```

Description

Enter the command option **2** from the Security commands menu to reset the copadmin password.

Security Options

```
1. Reset Password GUI
2. Reset Password CLI
3. Reset debug apps password
4. Reset ILO Administrator Password
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 4 ]: 2
```

From the previous menu options, select **2** to display the CLI to reset the password.

```
Do you want to reset GUI copadmin password(y/n) :
```

Table 6: *Password Requirements*

Requirement	Description
Password length	The minimum number of alphanumeric characters required for a password is **14**. Range: 14 - 48 (combination of alphabets, numbers, and special characters).
Password character	Password should contain at least **5** unique characters. The password should not contain the strings of username in any form. Password must not contain more than two identical characters consecutively.
Upper Case characters	Use a minimum of 1 uppercase alphabet in password. Alphabets **A** to **Z**.
Lower Case characters	Use a minimum of 1 lowercase alphabet in password. Alphabets **a** to **z**.
Numbers	Use a minimum of 1 digit (number) in password. Numbers **0** - **9**.
Special characters	Use a minimum of 5 special character in password. Supported special characters are **~**, **!**, **@**, **#**, **$**, **%**, **^**, **&**, *****, **(**, **)**, **<**, **>**, **{**, **}**, **;**, **:**, **.** and **,**.

Related Commands

Command	Description
Reset GUI Admin Password	Resets the GUI admin user password.
Reset Debug Apps Password	Resets the debug apps password.
Reset ILO Administrator Password	Resets the ILO admin user password.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Reset Debug Apps Password

```
6 Security
   3 Reset debug apps password
```

Description

Enter the command option **3** from the Security commands menu to reset the debug apps password.

Security Options

```
1. Reset Password GUI
2. Reset Password CLI
3. Reset debug apps password
4. Reset ILO Administrator Password
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 4 ]: 3
```

From the previous menu options, select **3** to reset the debug apps password.

```
Do you want to reset debug apps password(y/n) :
```

Related Commands

Command	Description
Reset GUI Admin Password	Resets the GUI admin user password.
Reset CLI Admin Password	Resets the copadmin user password.
Reset ILO Administrator Password	Resets the ILO admin user password.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced

Reset ILO Administrator Password

```
6 Security
   4 Reset ILO Administrator Password
```

Description

Enter the command option **4** from the Security commands menu to reset the ILO administrator password.

Security Options

```
1. Reset Password GUI
2. Reset Password CLI
3. Reset debug apps password
4. Reset ILO Administrator Password
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 4 ]: 4
```

From the previous menu options, select **4** to rest the ILO administrator password.

```
Please enter current password for ILO Administrator account :
```

Related Commands

Command	Description
Reset GUI Admin Password	Resets the GUI admin user password.
Reset CLI Admin Password	Resets the CLI admin user password.
Reset Debug Apps Password	Resets the debug apps password.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Support

```
7 Support
```

Description

Enter the command option **7** from the main menu to start or stop the support connection, collect logs, and restart a particular application.

Hierarchy Level

```
7 Support
   7-1 Support Connection
      7-1-1 Start Support Connection
      7-1-2 Stop Support Connection
      7-1-3 Restart Support Connection
      7-1-4 Support Connection Support
      7-1-5 Upload Support Connection File
      7-1-6 Add Support User Support
      7-1-7 Delete Support User copsupport
      7-1-8 Show Contents of copsupport.gpg
   7-2 Collect COP Cluster Logs
      7-2-1 Collect Basic Cluster info while Collecting Logs
      7-2-2 Collect Advance Cluster info while Collecting Logs
   7-3 Log Snapshot Operations
      7-3-1 Generates Snapshots for a Category
      7-3-2 Generate System Operation Logs
      7-3-3 Generate Pod Logs
      7-3-4 Generate Node Snapshots
      7-3-5 Download Logs Snapshots
      7-3-6 Delete Logs Snapshots
      7-3-7 Download Upgrade Reports
   7-4 Download COP Setup Logs
   7-5 Restart Application
   7-6 System Operations Lock Management
      7-6-1 Lock Status
      7-6-2 Release Lock
      7-6-3 Update Lock Settings
   7-7 Reset allowed management subnet
   7-8 Logging Tool Management
      7-8-1 Show Logging Framework Status
      7-8-2 Cleanup Logging Framework
```

Main Menu Options

```
 1. System
 2. File Operations
 3. Show
 4. System Configuration
 5. Advanced
 6. Security
 7. Support
 8. Temporary Root Shell
 9. Authentication
 10. Certificate configuration
 11. Search commands
```

```
==================================
0. exit

Enter option [ 0 - 11 ]: 7
```

From the previous menu option, select **7** to display Support options.

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
7. Reset allowed management subnet
8. Logging Tool Management
============================
b. back
m. main menu
0. exit
Enter option [0-8]:
```

Related Commands

Command	Description
Support Connection	Supports the connection.
Collect COP Cluster Logs	Collects all logs.
Log Snapshot Operations	Logs the snapshot operations.
Download COP Setup Logs	Downloads the COP setup logs.
Restart Application	Restarts the application.
System Operations Lock Management	Operates the lock management system.
Reset allowed management subnet	Creates Reset Allowed Management Subnet.
Logging Tool Management	Helps in Logging Tool Management

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Support Connection

```
7 Support
   1 Support Connection
```

Description

Enter the command option **1**from the Support commands menu to start, stop, restart the support connection from remote TAC access or check the status of the support connection and upload the support connection file.

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
7. Reset allowed management subnet
8. Logging Tool Management
============================
b. back
m. main menu
0. exit
Enter option [0-8]: 1
```

From the **Support** options, select **1** to display the Support Connections options.

```
1. Start Support Connection
2. Stop Support Connection
3. Restart Support Connection
4. Support Connection Status
5. Upload Support Connection File
6. Add Support User 'copsupport'
7. Delete Support User 'copsupport'
8. Show contents of copsupport.gpg
===================================
b. back
m. main menu
0. exit
Enter option [ 0 - 8 ]:
```

Related Commands

Command	Description
Start Support Connection	Starts the support connection.
Stop Support Connection	Stops the support connection.
Restart Support Connection	Restarts the support connection.

Command	Description
Support Connection Status	Supports the connection status.
Upload Support Connection File	Uploads the support connection file.
Add Support User copsupport	Adds the support user cop support.
Delete Support User copsupport	Deletes the support user cop support.
Show contents of copsupport.gpg	Shows the contents of cop support.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Start Support Connection

```
7 Support
   1 Support Connection
     1 Start Support Connection
```

Description

Enter the command option **1** from the Support Connection commands menu to start a support connection.

The following command includes the following information.

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
============================
b. back
m. main menu
0. exit
Enter option [0-7]: 1
```

Support Connections Options

From the **Support** options, select **1** to display the Support Connections options

```
1. Start Support Connection
2. Stop Support Connection
3. Restart Support Connection
4. Support Connection Status
5. Upload Support Connection File
6. Add Support User 'copsupport'
7. Delete Support User 'copsupport'
8. Show contents of copsupport.gpg
===================================
b. back
m. main menu
0. exit
Enter option [ 0 - 8 ]: 1
```

From the previous menu, enter **1** to start a support connection.

```
{
"support_connection_status": "running",
"active_from": "Tue Jul 18 07:14:10 UTC 2023",
"connection": "active"
}
Press [Enter] key to continue...
```

Related Commands

Command	Description
Stop Support Connection	Stops the support connection.
Restart Support Connection	Restarts the support connection.
Support Connection Status	Supports the connection status.
Upload Support Connection File	Uploads the support connection file.
Add Support User copsupport	Adds the support user cop support.
Delete Support User copsupport	Deletes the support user cop support.
Show contents of copsupport.gpg	Shows the contents of cop support.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Stop Support Connection

```
7 Support
   1 Support Connection
     2 Stop Support Connection
```

Description

Enter the command option **2** from the Support Connection commands menu to stop a support connection.

The following command includes the following information.

Support Options

```
Enter option [0-11]: 7
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
============================
b. back
m. main menu
0. exit
Enter option [0-7]: 1
```

Support Connections Options

From the **Support** options, select **1** to display the Support Connections options

```
1. Start Support Connection
2. Stop Support Connection
3. Restart Support Connection
4. Support Connection Status
5. Upload Support Connection File
6. Add Support User 'copsupport'
7. Delete Support User 'copsupport'
8. Show contents of copsupport.gpg
===================================
b. back
m. main menu
0. exit
Enter option [ 0 - 8 ]: 2
```

From the previous menu, enter **2** to stop a support connection.

```
{
"support_connection_status": "stopped"
}
Press [Enter] key to continue...
```

Related Commands

Command	Description
Start Support Connection	Starts the support connection.
Restart Support Connection	Restarts the support connection.
Support Connection Status	Supports the connection status.
Upload Support Connection File	Uploads the support connection file.
Add Support User copsupport	Adds the support user cop support.
Delete Support User copsupport	Deletes the support user cop support.
Show contents of copsupport.gpg	Shows the contents of cop support.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Restart Support Connection

```
7 Support
   1 Support Connection
     3 Restart Support Connection
```

Description

Enter the command option **3** from the Support Connection commands menu to restart a support connection

The following command includes the following information.

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
============================
b. back
m. main menu
0. exit
Enter option [0-7]:1
```

Support Connections Options

From the **Support** options, select **1** to display the Support Connections options

```
1. Start Support Connection
2. Stop Support Connection
3. Restart Support Connection
4. Support Connection Status
5. Upload Support Connection File
6. Add Support User 'copsupport'
7. Delete Support User 'copsupport'
8. Show contents of copsupport.gpg
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 8 ]: 3
```

From the previous menu, enter **3** to restart a support connection.

```
{
"support_connection_status": "stopped"
}
Press [Enter] key to continue...
```

Related Commands

Command	Description
Start Support Connection	Starts the support connection.
Stop Support Connection	Stops the support connection.
Support Connection Status	Supports the connection status.
Upload Support Connection File	Uploads the support connection file.
Add Support User copsupport	Adds the support user cop support.
Delete Support User copsupport	Deletes the support user cop support.
Show contents of copsupport.gpg	Shows the contents of cop support.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Support Connection Status

```
7 Support
   1 Support Connection
     4 Support Connection Status
```

Description

Enter the command option **4** from the Support Connection commands menu to check the status of the support connection.

The following command includes the following information.

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
============================
b. back
m. main menu
0. exit
Enter option [0-7]:1
```

Support Connections Options

From the **Support** options, select **1** to display the Support Connections options

```
Enter option [ 0 - 7 ]: 1
1. Start Support Connection
2. Stop Support Connection
3. Restart Support Connection
4. Support Connection Status
5. Upload Support Connection File
6. Add Support User 'copsupport'
7. Delete Support User 'copsupport'
8. Show contents of copsupport.gpg
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 8 ]: 4
```

From the previous menu, enter **4** to check the status of a support connection.

```
{
"support_connection_status": "running",
"active_from": "Tue Jul 18 07:40:00 UTC 2023",
"connection": "active",
"node": "10.xx.xxx.xxx"
}
Press [Enter] key to continue...
```

```
{
"support_connection_status": "stopped"
}
Press [Enter] key to continue...
```

Related Commands

Command	Description
Start Support Connection	Starts the support connection.
Stop Support Connection	Stops the support connection.
Restart Support Connection	Restarts the support connection.
Upload Support Connection File	Uploads the support connection file.
Add Support User copsupport	Adds the support user cop support.
Delete Support User copsupport	Deletes the support user cop support.
Show contents of copsupport.gpg	Shows the contents of cop support.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Upload Support Connection File

```
7 Support
   1 Support Connection
     5 Upload Support Connection File
```

Description

Enter the command option **5** from the Support Connection commands menu to upload a support connection file.

The following command includes the following information.

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
============================
b. back
m. main menu
0. exit
Enter option [0-7]:1
```

Support Connections Options

From the **Support** options, select **1** to display the Support Connections options

```
1. Start Support Connection
2. Stop Support Connection
3. Restart Support Connection
4. Support Connection Status
5. Upload Support Connection File
6. Add Support User 'copsupport'
7. Delete Support User 'copsupport'
8. Show contents of copsupport.gpg
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 8 ]: 5
```

From the previous menu, enter **5** to upload a support connection file.

```
This will scp a file from the remote server to cop server
Enter remote hostname and path (username@hostname:<filepath>):
auto@10.xx.xxx.xx:/home/auto/support_connection.tar
Copying auto@10.xx.xxx.xx:/home/auto/support_connection.tar to COP server
auto@10.xx.xxx.xx's password:
Connected to 10.xx.xxx.xx.
Fetching /home/auto/isupport_connection.tar to
/var/airwave/appliance/localdisk/support_connection.tar
```

```
/home/auto/support_connection.tar 100% 1988  127.9MB/s   00:00
Press [Enter] key to continue...
```

Related Commands

Command	Description
Start Support Connection	Starts the support connection.
Stop Support Connection	Stops the support connection.
Restart Support Connection	Restarts the support connection.
Support Connection Status	Supports the connection status.
Add Support User copsupport	Adds the support user cop support.
Delete Support User copsupport	Deletes the support user cop support.
Show contents of copsupport.gpg	Shows the contents of cop support.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Add Support User copsupport

```
7 Support
   1 Support Connection
     6 Add Support User 'copsupport'
```

Description

Enter the command option **6** from the Support Connection commands menu to add support connection for user copsupport.

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
============================
b. back
m. main menu
0. exit
Enter option [0-7]:1
```

Support Connections Options

From the **Support** options, select **1** to display the Support Connections options.

```
1. Start Support Connection
2. Stop Support Connection
3. Restart Support Connection
4. Support Connection Status
5. Upload Support Connection File
6. Add Support User 'copsupport'
7. Delete Support User 'copsupport'
8. Show contents of copsupport.gpg
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 8 ]: 6
```

From the previous menu, enter **6** to add support for the user copsupport.

```
copsupport user account expires on: Mar 10, 2022 8 10:48:17
-----BEGIN PGP MESSAGE-----
hQIMA0wNcZIn82zzAQ//bj0kS7h2s2wMJWX0JlYcfX053lFjWUa2XqHJ5xKk1OP7
jzvVRw+yFApKy5R0DP1RbXnifLHFGGxZx+x40H592agTehIqrI3L5put4Ewi/uK2
RZg9znigDmTe8jKTNWIbrN80VBpTz4QXaArD+4yhAJ80JFhFyFij9fWz1dSCwIUj
oej3JpKtDzVNmRZqANje8HeF62Y6WYWXFFn8VrzBPaasIPk1KQU5MZEKXtZyB3zD
nmi3IyM5rF/+uqFniR7vYlQfYXwySB17ToPKvjbO4tvEt5WWwfXeEg+DczdNkdIz
EpxXwgoby958Le0xCgcV8efbRtGCkxrtks37pPMAGJlVc0qtSJ/74DZc/BHD0WrZ
r4euZjWD/F1Eaxq56nMUHal0jzyLVj5w7DP5Rhj9mnCYl+jsy6ZTIbxpfDzembUF
```

```
LwTbVdjrbq79Ib+RFSHMUwFCv9CPGMjMmCJokYpdL82wksdJyOaWwF4AclmA19sU
IuyUtwiXb5bZqwCM0N3+mVQhaUqti0Xu4K5K5E8kSje3QOAyUz0ogS9axGkJQUWx
FpthJUF8ZKwH/tHU07K/So5LhahMcIa+qnCxycUC1X9G5R9EhvpGzEEQrUwy59lp
zCz9w4M0ON/QwNh4IVssnZMTW6WLUv0r9fHEjnJAj/toIsRAVbKSAMgzXKNiwc/S
dQEKZuFfFlPufJW4BWIoAn5PeThJQOrNlKxocI+e3H7eUKMZVof38MACsl6DJdy+
RCVrl4Wie3Ek/i2jXawz9QhBQza5c6BhdnjWqhQ+U9swEB0REnUbTqlaVhTXNVnW
qMGdxD77nPuKKJuTluTONXJLdsF0KA==
=gWUQ
-----END PGP MESSAGE-----
Press [Enter] key to continue...
```

Related Commands

Command	Description
Start Support Connection	Starts the support connection.
Stop Support Connection	Stops the support connection.
Restart Support Connection	Restarts the support connection.
Support Connection Status	Supports the connection status.
Upload Support Connection File	Uploads the support connection file.
Delete Support User copsupport	Deletes the support user cop support.
Show contents of copsupport.gpg	Shows the contents of cop support.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Delete Support User copsupport

```
7 Support
   1 Support Connection
     7 Delete Support User 'copsupport'
```

Description

Enter the command option **7** from the Support Connection commands menu to delete support connection for the user copsupport.

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
============================
b. back
m. main menu
0. exit
Enter option [0-7]:1
```

Support Connections Options

From the **Support** options, select **1** to display the Support Connections options

```
1. Start Support Connection
2. Stop Support Connection
3. Restart Support Connection
4. Support Connection Status
5. Upload Support Connection File
6. Add Support User 'copsupport'
7. Delete Support User 'copsupport'
8. Show contents of copsupport.gpg
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 8 ]: 7
```

From the previous menu, enter **7** to delete support connection for the user copsupport.

```
Are you sure you want to delete support user 'copsupport' (Y/N)y
Removing user `copsupport' ...
Done.
Support user 'copsupport' deleted successfully.
Press [Enter] key to continue...
```

Related Commands

Command	Description
Start Support Connection	Starts the support connection.
Stop Support Connection	Stops the support connection.
Restart Support Connection	Restarts the support connection.
Support Connection Status	Supports the connection status.
Upload Support Connection File	Uploads the support connection file.
Add Support User copsupport	Adds the support user cop support.
Show contents of copsupport.gpg	Shows the contents of cop support.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Show contents of copsupport.gpg

```
7 Support
   1 Support Connection
     8 Show contents of copsupport.gpg
```

Description

Enter the command option **8** from the Support Connection commands menu to show the contents of copsupport.gpg file.

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
============================
b. back
m. main menu
0. exit
Enter option [0-7]:1
```

Support Connections Options

From the **Support** options, select **1** to display the Support Connections options

```
1. Start Support Connection
2. Stop Support Connection
3. Restart Support Connection
4. Support Connection Status
5. Upload Support Connection File
6. Add Support User 'copsupport'
7. Delete Support User 'copsupport'
8. Show contents of copsupport.gpg
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 8 ]: 8
```

From the previous menu, enter **8** to show the contents of copsupport.gpg file.

```
-----BEGIN PGP MESSAGE-----
hQIMA0wNcZIn82zzARAAmuLy9Jure2AHc9/oSKXc0OEZ9ZW35O6r+mvWFk98zrMz
V1IW4wocFj1KhcpfMnMZ0O/nBY0oZIb1CK6CpLnaxFAM+T6NLv7Kroz6wqKfVSt8
pjsrmSh3eyfmMK9FlIkU3u2LglB9xUxMFGqjgvqTqcieqwzWFG5LmK1ALUWsUMoE
4PsWTTdVO+gRGkx17hsa7c9US0iVFaeOQJBdfCnOgP3rfqJzoVhbnL3JEnJSZrYs
R/sBIB47LNyw+E0i5ei8mbZ6S3rlWOCexxqFIdmyw+S52xrDPcACW/oqcnW31ubh
u6jD4JqSZqavaf+QZKM80/I0r9N0jAXMExCkOT0TQX3mmg5K5pFgo38j5hnifXTN
O+3rAcjRAgWhu1Nq3+1qpdG0esBCYPGdVs5f2mOej+cNBIsfg+RTemejOa71IeVf
R4/NWpMJa0STYk3/qSybEXjLiYxwwwsJILiqjfE5TVKOcAJhoUVyTH/8t9l4zn+/
```

```
qASXne52ocPaa4lxI3SxKGKz159cYcQxlXsJh+CS6RudZaAh8m/WKtWi2g2SqGhk
UsnJXttG5ruFnbFQPk1DdUSPnSzy4SZaBnwC0fvwkbQNUhTuYJmgQEQe8M9on5su
swhivSLvWYZTg6EYTlRveMRjh/iMbsDqp/ylsKH21jLQf9QA+tBM8yuPTmgAjPPS
dQH6+RPsiSlhdjkWnH6ZItIwX1WB1DpZaBjjx/PTTG+7Wi5XerA+8v1liJJOo6X/
yIdMnqlrGrQALRO/xPAXJUc4pQxXIDgHpWTQd3VWlCX5oSl2tPIiUAeq5iDds3vS
5KgqEvskPIeY9BJyMWa+LX2sx175HQ==
=t1Xn
-----END PGP MESSAGE-----
Press [Enter] key to continue...
```

Related Commands

Command	Description
Start Support Connection	Starts the support connection.
Stop Support Connection	Stops the support connection.
Restart Support Connection	Restarts the support connection.
Support Connection Status	Supports the connection status.
Upload Support Connection File	Uploads the support connection file.
Add Support User copsupport	Adds the support user cop support.
Delete Support User copsupport	Deletes the support user cop support.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Collect COP Cluster Logs

```
7 Support
   2 Collect COP Cluster Logs
```

Description

Enter the command option **2** from the Support commands menu to collect the log files into a tar.gz file.

Support Options

```
Enter option [0-11]: 7
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
7. Reset allowed management subnet
8. Logging Tool Management
============================
b. back
m. main menu
0. exit
Enter option [0-8]: 2
```

From the **Support** options, select **2** to display the collect logs options.

```
1. Collect basic cluster info while collecting logs
2. Collect advance cluster info while collecting logs
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 2 ]:
```

Related Commands

Command	Description
Collect Basic Cluster Info while collecting Logs	Collects Basic Cluster Info while collecting Logs
Collect advance cluster info while collecting logs	Collect Advance Cluster Info while collecting Logs

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Collect Basic Cluster Info while collecting Logs

```
7 Support
2 Collect COP Cluster Logs
1 Collect basic cluster info while collecting logs
```

Description

Enter the command option **1** from the Support commands menu to collect the basic cluster info of the log files into a tar.gz file.

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
============================
b. back
m. main menu
0. exit
Enter option [0-7]: 2
```

Collect COP Cluster Logs

From the **Support** options, select **2** to select **2** to display the collect logs options.

```
1. Collect basic cluster info while collecting logs
2. Collect advance cluster info while collecting logs
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 2 ]: 1
```

From the previous menu, enter **1** to collect the basic cluster info of the log files into a tar.gz file.

```
cluster_log_collection...
Collecting all logs from Elasticsearch takes around 1-3 hours.
It can be also collected from "Log Snapshot Operations" by selecting all as
category.
Do you want to collect logs from Elasticsearch(Y/N):
```

Related Commands

Command	Description
Collect advance cluster info while collecting logs	Collect Advance Cluster Info while collecting Logs

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Collect advance cluster info while collecting logs

```
7 Support
2 Collect COP Cluster Logs
2 Collect advance cluster info while collecting logs
```

Description

Enter the command option **2** from the Support commands menu to collect the advance cluster info of the log files into a tar.gz file.

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
============================
b. back
m. main menu
0. exit
Enter option [0-7]: 2
```

Collect COP Cluster Logs

From the **Support** options, select **2** to select **2** to display the collect logs options.

```
1. Collect basic cluster info while collecting logs
2. Collect advance cluster info while collecting logs
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 2 ]: 2
```

From the previous menu, enter **2** to collect the advance cluster info of the log files into a tar.gz file.

```
cluster_log_collection...
Collecting all logs from Elasticsearch takes around 1-3 hours.
It can be also collected from "Log Snapshot Operations" by selecting all as
category.
Do you want to collect logs from Elasticsearch(Y/N):
```

Related Commands

Command	Description
Collect Basic Cluster Info while collecting Logs	Collects Basic Cluster Info while collecting Logs

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Log Snapshot Operations

```
7 Support
   3 Log Snapshot Operations
```

Description

Enter the command option **3** from the Support commands menu to generate and download snapshots for a category or node, generate logs for various pods, delete snapshots, and download upgrade reports.

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
7. Reset allowed management subnet
8. Logging Tool Management
============================
b. back
m. main menu
0. exit
Enter option [0-8]: 3
```

From the **Support** options, select **3** to generate and download snapshots for a category or node, generate logs for various pods, delete snapshots, and download upgrade reports.

```
1. Generate Snapshots for a Category
2. Generate System Operation Logs
3. Generate Pod Logs
4. Generate Node Snapshot
5. Download Logs/Snapshots
6. Delete Logs/Snapshots
7. Download Upgrade Reports
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 7 ]:
```

Related Commands

Command	Description
Generate Snapshots for a Category	Generates Snapshots for a category.
Generate System Operation Logs	Generates system operation logs.
Generate Pod Logs	Generates pod logs.

Command	Description
Generate Node Snapshot	Generates node snapshots.
Download Logs/Snapshots	Downloads log/snapshots.
Delete Logs/Snapshots	Deletes log/snapshots.
Download Upgrade Reports	Downloads upgrade reports.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Generate Snapshots for a Category

```
7 Support
   3 Log Snapshot Operations
     1 Generate Snapshots for a Category
```

Description

Enter the command option **1**from the Log Snapshot Operations commands menu to collect log snapshots of specific categories (kube. nginx, alert, infra, syslog, and system).

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
============================
b. back
m. main menu
0. exit
Enter option [0-7]:3
```

From the **Support** options, select **3** to display the **Log Snapshot** options.

Log Snapshot Options

```
1. Generate Snapshots for a Category
2. Generate System Operation Logs
3. Generate Pod Logs
4. Generate Node Snapshot
5. Download Logs/Snapshots
6. Delete Logs/Snapshots
7. Download Upgrade Reports
===================================
b. back
m. main menu
0. exit
Enter option [ 0 - 7 ]: 1
```

From the previous menu, enter **1** to generate log snapshots of specific categories (kube. nginx, alert, infra, syslog, and system).

```
Enter a category to create the snapshot [kube nginx alert infra syslog
system all]... alert
Enter the time range for snapshot creation [3h, 1d, 1w, 1M, 3M]... 1w
{ "status": "Accepted", "snapshotId": "alert-snap-7d-1644406412" }
Press [Enter] key to continue...
```

Related Commands

Command	Description
Generate System Operation Logs	Generates system operation logs.
Generate Pod Logs	Generates pod logs.
Generate Node Snapshot	Generates node snapshots.
Download Logs/Snapshots	Downloads log/snapshots.
Delete Logs/Snapshots	Deletes log/snapshots.
Download Upgrade Reports	Downloads upgrade reports.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Generate System Operation Logs

```
7 Support
   3 Log Snapshot Operations
     2 Generate System Operation Logs
```

Description

Enter the command option **2**from the Log Snapshot Operations commands menu to collect system operation logs.

The following command includes the following information.

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
============================
b. back
m. main menu
0. exit
Enter option [0-7]:3
```

From the **Support** options, select **3** to display the **Log Snapshot** options.

Log Snapshot Options

```
1. Generate Snapshots for a Category
2. Generate System Operation Logs
3. Generate Pod Logs
4. Generate Node Snapshot
5. Download Logs/Snapshots
6. Delete Logs/Snapshots
7. Download Upgrade Reports
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 7 ]: 2
```

From the previous menu, enter **2** to collect system operation logs.

```
Enter a category to create the snapshot [upgrade backuprestore migration]...
migration
% Total    % Received % Xferd  Average Speed   Time    Time     Time
Current
Dload  Upload   Total   Spent    Left  Speed
100   105  100   105    0     0    652      0 --:--:-- --:--:-- --:--:--
660
{ "status": "Accepted", "snapshotId": "migration-plain-1m-1644910302",
```

```
"category": "migration" }
Press [Enter] key to continue...
```

Related Commands

Command	Description
Generate Snapshots for a Category	Generates Snapshots for a category.
Generate Pod Logs	Generates pod logs.
Generate Node Snapshot	Generates node snapshots.
Download Logs/Snapshots	Downloads log/snapshots.
Delete Logs/Snapshots	Deletes log/snapshots.
Download Upgrade Reports	Downloads upgrade reports.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Generate Pod Logs

```
7 Support
   3 Log Snapshot Operations
     3 Generate Pod Logs
```

Description

Enter the command option **3** from the Log Snapshot Operations commands menu to collect pod logs.

The following command includes the following information.

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
============================
b. back
m. main menu
0. exit
Enter option [0-7]:3
```

From the **Support** options, select **3** to display the **Log Snapshot** options.

Log Snapshot Options

```
1. Generate Snapshots for a Category
2. Generate System Operation Logs
3. Generate Pod Logs
4. Generate Node Snapshot
5. Download Logs/Snapshots
6. Delete Logs/Snapshots
7. Download Upgrade Reports
===================================
b. back
m. main menu
0. exit
Enter option [ 0 - 7 ]: 3
```

From the previous menu, enter **3** to collect pod logs.

```
Enter a pod name to generate logs... postgres-cluster-0
{ "status": "Accepted", "snapshotId": "postgres-cluster-0-1m-1644410009",
"category": "pod" }
Press [Enter] key to continue...
```

Related Commands

Command	Description
Generate Snapshots for a Category	Generates Snapshots for a category.
Generate System Operation Logs	Generates system operation logs.
Generate Node Snapshot	Generates node snapshots.
Download Logs/Snapshots	Downloads log/snapshots.
Delete Logs/Snapshots	Deletes log/snapshots.
Download Upgrade Reports	Downloads upgrade reports.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Generate Node Snapshot

```
7 Support
   3 Log Snapshot Operations
     4 Generate Node Snapshot
```

Description

Enter the command option **4**from the Log Snapshot Operations commands menu to collect log snapshots for specific nodes.

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
============================
b. back
m. main menu
0. exit
Enter option [0-7]:3
```

From the **Support** options, select **3** to display the **Log Snapshot** options.

Log Snapshot Options

```
1. Generate Snapshots for a Category
2. Generate System Operation Logs
3. Generate Pod Logs
4. Generate Node Snapshot
5. Download Logs/Snapshots
6. Delete Logs/Snapshots
7. Download Upgrade Reports
===================================
b. back
m. main menu
0. exit
Enter option [ 0 - 7 ]: 4
```

From the previous menu, enter **4** collect log snapshots for specific nodes.

```
Enter node to generate logs [10.22.154.57]... 10.xx.xxx.xx
{ "status": "Accepted", "snapshotId": "10.xx.xxx.xx-snap-1m-1644410130" }
Press [Enter] key to continue...
```

Related Commands

Command	Description
Generate Snapshots for a Category	Generates Snapshots for a category.
Generate System Operation Logs	Generates system operation logs.
Generate Pod Logs	Generates pod logs.
Download Logs/Snapshots	Downloads log/snapshots.
Delete Logs/Snapshots	Deletes log/snapshots.
Download Upgrade Reports	Downloads upgrade reports.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Download Logs/Snapshots

```
7 Support
   3 Log Snapshot Operations
     5 Download Logs/Snapshots
```

Description

Enter the command option **5**from the Log Snapshot Operations commands menu to download the log snapshot file.

The following command includes the following information.

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
============================
b. back
m. main menu
0. exit
Enter option [0-7]:3
```

From the **Support** options, select **3** to display the **Log Snapshot** options.

Log Snapshot Options

```
1. Generate Snapshots for a Category
2. Generate System Operation Logs
3. Generate Pod Logs
4. Generate Node Snapshot
5. Download Logs/Snapshots
6. Delete Logs/Snapshots
7. Download Upgrade Reports
===================================
b. back
m. main menu
0. exit
Enter option [ 0 - 7 ]: 5
```

From the previous menu, enter **5** to download the log snapshot file.

```
List of available snapshots and their status
-------------------------------------------------------------
create time           snapshot name                      status
-------------------------------------------------------------
2022-02-08 11:12:35, "all-snap-7d-1644318755": "in_progress"
-------------------------------------------------------------
Select a name to be downloaded (without quotes)...
```

Related Commands

Command	Description
Generate Snapshots for a Category	Generates Snapshots for a category.
Generate System Operation Logs	Generates system operation logs.
Generate Pod Logs	Generates pod logs.
Generate Node Snapshot	Generates node snapshots.
Delete Logs/Snapshots	Deletes log/snapshots.
Download Upgrade Reports	Downloads upgrade reports.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Delete Logs/Snapshots

```
7 Support
   3 Log Snapshot Operations
     6 Delete Logs/Snapshots
```

Description

Enter the command option **6**from the Log Snapshot Operations commands menu to delete log snapshots.

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
============================
b. back
m. main menu
0. exit
Enter option [0-7]:3
```

From the **Support** options, select **3** to display the **Log Snapshot** options.

Log Snapshot Options

```
1. Generate Snapshots for a Category
2. Generate System Operation Logs
3. Generate Pod Logs
4. Generate Node Snapshot
5. Download Logs/Snapshots
6. Delete Logs/Snapshots
7. Download Upgrade Reports
===================================
b. back
m. main menu
0. exit
Enter option [ 0 - 7 ]: 6
```

From the previous menu, enter **6** to delete the log snapshots.

```
List of available snapshots and their status
-----------------------------------------------------------------
create time           snapshot name                       status
-----------------------------------------------------------------
2022-02-08 11:12:35, "all-snap-7d-1644318755": "in_progress"
-----------------------------------------------------------------
Select a name to be deleted (without quotes)...
```

Related Commands

Command	Description
Generate Snapshots for a Category	Generates Snapshots for a category.
Generate System Operation Logs	Generates system operation logs.
Generate Pod Logs	Generates pod logs.
Generate Node Snapshot	Generates node snapshots.
Download Logs/Snapshots	Downloads log/snapshots.
Download Upgrade Reports	Downloads upgrade reports.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Download Upgrade Reports

```
7 Support
   3 Log Snapshot Operations
     7 Download Upgrade Reports
```

Description

Enter the command option **7**from the Log Snapshot Operations commands menu to download upgrade reports.

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
============================
b. back
m. main menu
0. exit
Enter option [0-7]:3
```

From the **Support** options, select **3** to display the **Log Snapshot** options.

Log Snapshot Options

```
1. Generate Snapshots for a Category
2. Generate System Operation Logs
3. Generate Pod Logs
4. Generate Node Snapshot
5. Download Logs/Snapshots
6. Delete Logs/Snapshots
7. Download Upgrade Reports
===================================
b. back
m. main menu
0. exit
Enter option [ 0 - 7 ]: 7
```

From the previous menu, enter **7** to download the upgrade reports.

```
Added `minio` successfully.
mc: Configuration written to `/home/copadmin/.mc/config.json`. Please update
your access credentials.
mc: Successfully created `/home/copadmin/.mc/share`.
mc: Initialized share uploads `/home/copadmin/.mc/share/uploads.json` file.
mc: Initialized share downloads `/home/copadmin/.mc/share/downloads.json`
file.
mc: <ERROR> Unable to validate source minio/deployment/
Press [Enter] key to continue...
```

Related Commands

Command	Description
Generate Snapshots for a Category	Generates Snapshots for a category.
Generate System Operation Logs	Generates system operation logs.
Generate Pod Logs	Generates pod logs.
Generate Node Snapshot	Generates node snapshots.
Download Logs/Snapshots	Downloads log/snapshots.
Delete Logs/Snapshots	Deletes log/snapshots.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Download COP Setup Logs

```
7 Support
4 Download COP Setup Logs
```

Description

Enter the command option**4**from the Support commands menu to download the HPE Aruba Networking Central On-Premises setup logs.

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
7. Reset allowed management subnet
8. Logging Tool Management
============================
b. back
m. main menu
0. exit
Enter option [0-8]: 4
```

From the **Support** options, select **4** to download the HPE Aruba Networking Central On-Premises setup logs.

```
################################################################################
####
SCP would be used to copy the logs to a remote host

################################################################################
####
Enter remote hostname and path (username@hostname:<filepath>):
```

Related Commands

Command	Description
Support Connection	Supports the connection.
Collect COP Cluster Logs	Collects all logs.
Log Snapshot Operations	Logs the snapshot operations.
Restart Application	Restarts the application.
System Operations Lock Management	Operates the lock management system.

Command	Description
Reset allowed management subnet	Creates Reset Allowed Management Subnet.
Logging Tool Management	Helps in Logging Tool Management

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Restart Application

```
7 Support
5 Restart Application
```

Description

Enter the command option**5** from the Support commands menu to restart applications.

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
7. Reset allowed management subnet
8. Logging Tool Management
============================
b. back
m. main menu
0. exit
Enter option [0-8]: 5
```

From the **Support** options, select **5** to restart applications.

```
Enter an application name to restart:
```

Related Commands

Command	Description
Support Connection	Supports the connection.
Collect COP Cluster Logs	Collects all logs.
Log Snapshot Operations	Logs the snapshot operations.
Download COP Setup Logs	Downloads the COP setup logs.
System Operations Lock Management	Operates the lock management system.
Reset allowed management subnet	Creates Reset Allowed Management Subnet.
Logging Tool Management	Helps in Logging Tool Management

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

System Operations Lock Management

```
7 Support
   6 System Operations Lock Management
```

Description

Enter the command option **6**from the Support commands menu to manage the system operations lock management.

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
7. Reset allowed management subnet
8. Logging Tool Management
============================
b. back
m. main menu
0. exit
Enter option [0-8]: 6
```

From the **Support** options, select **6** to display the system operations lock management options.

```
1. Lock status
2. Release Lock
3. Update Lock Setting
===================================
b. back
m. main menu
0. exit
Enter option [ 0 - 3 ]:
```

Command	Description
Lock Status	Locks the status.
Release Lock	Releases the lock.
Update Lock Setting	Updates the lock settings.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Lock Status

```
7 Support
   6 System Operations Lock Management
     1 Lock Status
```

Description

Enter the command option **1**from the System Operations Lock Management commands menu to lock the status of the system operation.

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
============================
b. back
m. main menu
0. exit
Enter option [0-7]: 6
```

From the **Support** options, select **6** to display the system operations lock management options.

```
1. Lock status
2. Release Lock
3. Update Lock Setting
===================================
b. back
m. main menu
0. exit
Enter option [0-7]: 1
```

From the previous menu, enter **1** to lock the status of the system operation.

```
No system operation is active currently
Press [Enter] key to continue...
```

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Release Lock

```
7 Support
   6 System Operations Lock Management
     2 Release Lock
```

Description

Enter the command option **2** from the System Operations Lock Management commands menu to release the lock of the system operation.

Support Options

```
Enter option [0-11]: 7
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
============================
b. back
m. main menu
0. exit
Enter option [0-7]: 6
```

From the **Support** options, select **6** to display the system operations lock management options.

```
1. Lock status
2. Release Lock
3. Update Lock Setting
===================================
b. back
m. main menu
0. exit
Enter option [ 0 - 3 ]: 2
```

From the previous menu, enter **2** to release the lock of the system operation.

```
1. Upgrade
2. Backup
3. Restore
4. Migration
5. Add node
6. Replace node
7. Reboot node
=====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 7 ]:
```

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Update Lock Setting

```
7 Support
   6 System Operations Lock Management
     3 Update Lock Setting
```

Description

Enter the command option **3**from the System Operations Lock Management commands menu to update the lock settings.

The following command includes the following information.

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
============================
b. back
m. main menu
0. exit
Enter option [0-7]: 6
```

From the **Support** options, select **6** to display the system operations lock management options.

```
1. Lock status
2. Release Lock
3. Update Lock Setting
===================================
b. back
m. main menu
0. exit
Enter option [ 0 - 3 ]: 3
```

From the previous menu, enter **3** to update the lock settings.

```
1. on
2. off
===================================
b. back
m. main menu
0. exit
Enter option [ 0 - 2 ]:
```

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Reset allowed management subnet

```
7 Support
   7 Reset Allowed Management Subnet
```

Description

Enter the command option **7**from the Support commands menu to reset the system management subnet.

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
7. Reset allowed management subnet
8. Logging Tool Management
============================
b. back
m. main menu
0. exit
Enter option [0-8]: 7
```

From the **Support** options, select **7** to display the system operations lock management options.

```
Resetting the default subnet...
ingress.networking.k8s.io/allowed-subnet-config-created
configmap/allowed-subnet-configmap created
Press [Enter] key to continue...
```

Related Commands

Command	Description
Support Connection	Supports the connection.
Collect COP Cluster Logs	Collects all logs.
Log Snapshot Operations	Logs the snapshot operations.
Download COP Setup Logs	Downloads the COP setup logs.
Restart Application	Restarts the application.
System Operations Lock Management	Operates the lock management system.
Logging Tool Management	Helps in Logging Tool Management

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.1.0	Command introduced.

Logging Tool Management

```
7 Support
   8 Logging Tool Management
```

Description

Enter the command option **8**from the Support commands menu to manage the logging tool. It enables to display or cleanup the logging framework.

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
7. Reset allowed management subnet
8. Logging Tool Management
============================
b. back
m. main menu
0. exit
Enter option [0-8]: 8
```

From the **Support** options, select **8** to display the system operations lock management options.

```
1. Show Logging Framework Status
2. Cleanup Logging Framework
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 2 ]:
```

Related Commands

Command	Description
Show Logging Framework Status	Displays the logging framework status.
Cleanup Logging Framework	Cleans up the logs.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.1.0	Command introduced.

Show Logging Framework Status

```
7 Support
   8 Logging Tool Management
      2 Show Logging Framework Status
```

Description

Enter the command option **1**from the Logging Tool Management commands menu to display the logging framework status.

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
7. Reset allowed management subnet
8. Logging Tool Management
============================
b. back
m. main menu
0. exit
Enter option [0-8]: 8
```

From the **Support** options, select **8** to display the system operations lock management options.

```
1. Show Logging Framework Status
2. Cleanup Logging Framework
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 2 ]: 1
```

From the **Logging Tool Management** options, select **1** to display the logging framework status.

```
Starting to collect logging info
Checking pods related to logging and app
acp-system  fluent-bit-logging-86c72 0/1   CreateContainerError     3 (143d
ago)   205d  172.23.247.178  cop-node-152-56.arubacorp.ne  <none>   <none>
25.04.01-2
p.net   <none>           <none>           25.04.01-2
acp-system   fluent-bit-logging-dn25w     1/1   Running   3 (144d ago)
205d    172.23.159.81    cop-node-152-57.arubacorp.net   <none>  <none>

25.04.01-2
acp-system   fluent-bit-logging-w6d95     1/1   Running    2 (144d ago) 205d
   172.23.13.130    cop-node-152-58.arubacorp.net   <none>  <none>
25.04.01-2
gravity  app-security-fw-logging-graphql-service-8454589ddc-6btmq  0/2
Terminating 0 144d    172.23.247.131 cop-node-152-56.arubacorp.net <none>
<none>
```

```
25.04.01-2
infra-system       opensearch-logging-0   0/1   Terminating    1 205d
172.23.249.55    cop-node-152-56.arubacorp.net   <none>   <none>
25.04.01-2
infra-system       opensearch-logging-1    1/1    Running   0   144d
172.23.159.230   cop-node-152-57.arubacorp.net    <none> <none>   25.04.01-2
infra-system       opensearch-logging-2   1/1    Running   1 (144d ago 144d
172.23.13.164    cop-node-152-58.arubacorp.net   <none>   <none>
25.04.01-2
/var/airwave/appliance/bin/ampcli/collect_opensearch_logging_info.sh: line
10: kubectl: command not found
Execution completed
Press [Enter] key to continue...

==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 2 ]: 1
```

Related Commands

Command	Description
Cleanup Logging Framework	Cleans up the logs.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.1.0	Command introduced.

Cleanup Logging Framework

```
7 Support
   8 Logging Tool Management
      2 Cleanup Logging Framework
```

Description

Enter the command option **2**from the Logging Tool Management commands menu to perform a cleanup of the logging framework.

Support Options

```
1. Support Connection
2. Collect All Logs
3. Log Snapshot Operations
4. Download COP Setup Logs
5. Restart Application
6. System Operations Lock Management
7. Reset allowed management subnet
8. Logging Tool Management
============================
b. back
m. main menu
0. exit
Enter option [0-8]: 8
```

From the **Support** options, select **8** to display the system operations lock management options.

```
1. Show Logging Framework Status
2. Cleanup Logging Framework
==================================
b. back
m. main menu
0. exit
Enter option [ 0 - 2 ]: 2
```

From the **Logging Tool Management** options, select **2** to cleanup the logging framework.

```
Cleaning up the Logging framework removes the logs. Do you want to continue?
(Y/N):
```

Related Commands

Command	Description
Show Logging Framework Status	Displays the logging framework status.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.1.0	Command introduced.

Temporary Root Shell

```
8 Temporary Root Shell
```

Description

Enter the command option **8**from the main menu to create a temporary user, cop_shell with a random password and the system encrypts this password. Provide this key to the customer support. The customer support will then be able to access the Aruba Central On-Premises SSH using the username, cop_shell for 2 days from the date of creation.

Use this option to get access to the Shell for a limited period of time for checking pods, collecting logs, or for executing other CLI commands. This is useful if you want to troubleshoot or debug an issue.

Hierarchy Level

```
8 Temporary Root Shell
```

Enter the command option **8** from the main menu to view the temporary root shell command.

Main Menu Options

```
1. System
2. File Operations
3. Show
4. System Configuration
5. Advanced
6. Security
7. Support
8. Temporary Root Shell
9. Authentication
10. Certificate configuration
11. Search commands
====================================
0. exit

Enter option [ 0 - 11 ]:8

============================
```

From the previous menu option, select **8** to display Temporary Root Shell options.

```
This will reset the previous COP root shell's pwd. proceed? (y/n): y
cop_shell user account expires on: Jul 20, 2023 12:06:45 UTC
-----BEGIN PGP MESSAGE-----
hQIMA0wNcZIn82zzAQ//d6XBLE+z4yEEORRo+sCTX92tnJA/A+EpsOI9RRoT1u9J
WcXyXs2WvEQ8xALdgIpJ/SE3IfU+9rRrhubqtyN48jEVDjSJ4xkIXxD6Bkc+TU72
Qg8dr+kiLU5Vm9e5c2e0lsybVyOf1LBPrnd09LgoVmFdioi+zv5AHrohQD8XhDz6
QejHqGHizfu45kKogCtrLVOu4ZXrp7JsjBJ29TJuEqy6Gr8TLO5cqIAQpnbu/EP4
ESqhuOVE5bxke+MoKsRZDPuB0DpPoCCeKxPwCMjUmB2Lnp38Xo6N0vrmQXU3Wuwc
EhDa/RNfPl+eoFh9+dGY3MLnlcIDuVcnmut6niDQ+N8CyrrREgq0laZ2PoX7fV0Z
RkQ8m4GmkYjq4Lo9C74AccwwLg0AzT+Vr8aUdDdSbZlkQQkAP5XYudG7Nfs566kw
me2yh6G27P7JzJ8P/gviEf2aROiHW+LgvAQISdV53RT00lDbSpf6lui/K4uixdd6
1AsDo1he1y7XhQ/wp5iznhsLV1DCxHF1jjqBqvkiBQK1oTxdfoHhyV/UPPc+qJcv
vS7/GtV1opKg7p0H0SgE6kM7+5x/MkVp3CyfJYj2tW/ZvmClPtyjgDQ39ENYuJuB
```

```
gUx2Sezaf/6K267YIOywGd7ytVBF1D/0Xjcw3WCqQ6NV6ifwm/CL76xliqalcLTS
cwGgBWAZ0wfq6Q/pvhgws0lvFuUpvFPgD+VaWyc0guNPTw2Wa0QfzNDU4GCiQl2y
aXOVciH/TH733kwwuSL59eFifHxPM9ds7FkXctEooInlKY+fcdlrqt1+xMl0fOgP
bCqXv/flDYQdioUQqsJ21lHQkuU=
=uinz
-----END PGP MESSAGE-----
Press [Enter] key to continue...
```

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Authentication

```
9 Authentication
```

Description

Enter the command option **9** from the main menu to authenticate the SSH public keys required to connect to the HPE Aruba Networking Central On-Premises server.

```
9 Authentication
   9-1 Display public key
   9-2 Add public key to COP
   9-3 List all public key added COP
```

Enter the command option **9** from the main menu to view all the authentication commands supported.

Hierarchy Level

```
9 Authentication
   9-1 Display public key
   9-2 Add public key to COP
   9-3 List all public key added to COP
```

Main Menu Options

```
1. System
2. File Operations
3. Show
4. System Configuration
5. Advanced
6. Security
7. Support
8. Temporary Root Shell
9. Authentication
10. Certificate configuration
11. Search commands
==================================
0. exit

Enter option [ 0 - 11 ]: 9
```

From the main menu options, select **9** to display the Authentication options.

```
1. Display public key
2. Add public key to COP
3. List all public key added to COP
==================================
b. back
m. main menu
0. exit

Enter option [ 0 - 3 ]:
```

Related Commands

Command	Description
Display public key	Display SSH public key of the administrator of the HPE Aruba Networking Central On-Premises server.
Add public key to COP	Adds the SSH public key to the HPE Aruba Networking Central On-Premises server.
List all public key added COP	Lists all the SSH public key added to the HPE Aruba Networking Central On-Premises server.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Display public key

```
9 Authentication
   1 Display public key
```

Description

Enter the command option **1** from the Authentication commands menu to display SSH public key of the administrator of the HPE Aruba Networking Central On-Premises server. This is used to establish public key based SSH connection from the HPE Aruba Networking Central On-Premises server to an external SSH server.

Authentication Options

```
1. Display public key
2. Add public key to COP
3. List all public key added to COP
====================================
b. back
m. main menu
0. exit

Enter option [ 0 - 3 ]: 1
```

From the previous menu options, select **1** to display the public key details.

```
Public key for COP
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCgvtkfzXgG4AbaLsoJrdqbtdegGQ/NojIYZUDNQuYdNDXZ
m/Ti885MLzwuqJbv8GOlOd8vEor+YcQtJcWCjaBz7gZ2ZKUfC8qHyoErA1TnY52b1a+

djSLg05xnZSwMYmbsGW+146U2BgYsrcILltsWzoq8RZCNqZ2So6CiwjBLx6LGXQaszXePLm1Vkpu
VKE17SXmyGFEzYuq/p4VmE5u45s71PsqV/wIcuvHvMjdZg9YBP1MOHNDpFclvjujZ/6tG8X55

DAhszcwW30xjIQTEHBN0wHdSkLIaW4S9xq6xuw47Ez3lLGSpgB+fAclc34jL00lPHINVdUX2SY6l
o93r core@cop-156-209.arubathena.com
Press [Enter] key to continue...
```

Related Commands

Command	Description
Add public key to COP	Adds the SSH public key to the HPE Aruba Networking Central On-Premises server.
List all public key added COP	Lists all the SSH public key added to the HPE Aruba Networking Central On-Premises server.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Add public key to COP

```
9 Authentication
   2 Add public key to COP
```

Description

Enter the command option **2** from the Authentication commands menu to add the SSH public key to the HPE Aruba Networking Central On-Premises server.

Authentication Options

```
1. Display public key
2. Add public key to COP
3. List all public key added to COP
====================================
b. back
m. main menu
0. exit

Enter option [ 0 - 3 ]: 2
```

From the previous menu options, select **2** to add the public key to HPE Aruba Networking Central On-Premises.

```
Enter key in SSH format:
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDkg8xcD5bhfBX/SztxI4cME1IYs0+i7if28MXSHjmlwThl
mKVSJEkk+YuqeY8fq7seD2OuTP0snanQ4BbMdophZmJhR/Fx6Z9rDyAYRw+Uu7ViC0o

t6WbQ3ilDiEihWIYTOYrAmLMHx8Div4tHWBJ4sjI940Sr5bMpgEMczrl9TOSoHWLc1re1Y6UfTBN
KHST0Nyfrnor1QgoUyiD6sN0KZXvmp+8EGe8thq4wpNcbq/OJmndP5J40j05OSXLJCchvwgM5ZH

K3ifd5KwNtj6JkZw9KHOVvIsvnzbe8kA7rcTITn1C/XYOWpUUSX/TbhkXgSa/z7negg9YzXuqjgf
kx core@cop-dev-jenkins1.arubathena.com
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDkg8xcD5bhfBX/SztxI4cME1IYs0+i7if28MXSHjmlwThl
mKVSJEkk+YuqeY8fq7seD2OuTP0snanQ4BbMdophZmJhR/Fx6Z9rDyAYRw+Uu7ViC0

ot6WbQ3ilDiEihWIYTOYrAmLMHx8Div4tHWBJ4sjI940Sr5bMpgEMczrl9TOSoHWLc1re1Y6UfTB
NKHST0Nyfrnor1QgoUyiD6sN0KZXvmp+8EGe8thq4wpNcbq/OJmndP5J40j05OSXLJCchvwgM5

ZHK3ifd5KwNtj6JkZw9KHOVvIsvnzbe8kA7rcTITn1C/XYOWpUUSX/TbhkXgSa/z7negg9YzXuqj
gfkx core@cop-dev-jenkins1.arubathena.com
Adding keys to authorized user
Add keys to node : 10.xx.xxx.xx
authorized_keys
                                      100% 1234     2.7MB/s   00:00
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDkg8xcD5bhfBX/SztxI4cME1IYs0+i7if28MXSHjmlwThl
mKVSJEkk+YuqeY8fq7seD2OuTP0snanQ4BbMdophZmJhR/Fx6Z9rDyAYRw+Uu7Vi

C0ot6WbQ3ilDiEihWIYTOYrAmLMHx8Div4tHWBJ4sjI940Sr5bMpgEMczrl9TOSoHWLc1re1Y6Uf
TBNKHST0Nyfrnor1QgoUyiD6sN0KZXvmp+8EGe8thq4wpNcbq/OJmndP5J40j05OSXLJCchvwg
```

```
M5ZHK3ifd5KwNtj6JkZw9KHOVvIsvnzbe8kA7rcTITn1C/XYOWpUUSX/TbhkXgSa/z7negg9YzXu
qjgfkx core@cop-dev-jenkins1.arubathena.com
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC02/Bp28axKaL8COmDl1OVxAygmcXd/s97cDxOcej5JT57
LvpDLfBqU4neyIZOTj+bWZxqnYcEpqd7p8tx8dWFgl0ap2GcENoO2YUlLMSUqW7JnCo

HfkOV2xLvS3AU9MN3qj+uXfRGt4u7N02jbIuMWcdy/xU1YkWAKTnc89zGuf50ujn+s0hQR8XVZFP
IcxQyql5AJw1w4rKk1q26TkFZYE1YNOpbWZSwV9nCW79bki7tzBhVqPwQPUSon40R9fjrLV3Rl

Nh5kEXg5xwRfKmIdpdWu+VPSaKDXsusgX1FVI9J9w07R27Trxiai8+d4FlRf07W7fIhb9AQhtWOG
hf5 auto@slave-ui-p3
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDkg8xcD5bhfBX/SztxI4cME1IYs0+i7if28MXSHjmlwThl
mKVSJEkk+YuqeY8fq7seD2OuTP0snanQ4BbMdophZmJhR/Fx6Z9rDyAYRw+Uu7Vi

C0ot6WbQ3ilDiEihWIYTOYrAmLMHx8Div4tHWBJ4sjI940Sr5bMpgEMczrl9TOSoHWLc1re1Y6Uf
TBNKHST0Nyfrnor1QgoUyiD6sN0KZXvmp+8EGe8thq4wpNcbq/OJmndP5J40j05OSXLJCchvwg

M5ZHK3ifd5KwNtj6JkZw9KHOVvIsvnzbe8kA7rcTITn1C/XYOWpUUSX/TbhkXgSa/z7negg9YzXu
qjgfkx core@cop-dev-jenkins1.arubathena.com
Copying keys to user : copadmin
Copying keys to node : 10.xx.xxx.xx
Press [Enter] key to continue...
```

Related Commands

Command	Description
Display public key	Display SSH public key of the administrator of the HPE Aruba Networking Central On-Premises server.
List all public key added COP	Lists all the SSH public key added to the HPE Aruba Networking Central On-Premises server.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

List all public key added COP

```
9 Authentication
   3 List all public key added to COP
```

Description

Enter the command option **3** from the Authentication commands menu to list all the SSH public key added to the HPE Aruba Networking Central On-Premises server.

Authentication Options

```
1. Display public key
2. Add public key to COP
3. List all public key added to COP
====================================
b. back
m. main menu
0. exit

Enter option [ 0 - 3 ]: 3
```

From the previous menu options, select **3** to list all the SSH public keys added to the HPE Aruba Networking Central On-Premises server.

```
Local IP is - 10.22.156.209
Generating device cert for - 10.xx.xxx.xx
—
```

Related Commands

Command	Description
Display public key	Display SSH public key of the administrator of the HPE Aruba Networking Central On-Premises server.
Add public key to COP	Adds the SSH public key to the HPE Aruba Networking Central On-Premises server.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Certificate Configuration

```
10 Certificate Configuration
```

Description

This command allows the user to display the Root certificate and generate the device certificate. Enter the command option **10** from the main menu to generate the device certificate.

Hierarchy Level

```
10 Certificate configuration
   10-1 Disable client cert strict check
   10-2 Generate device cert
   10-3 Disable client cert strict check for devices
   10-4 Apply default certificates to Web UI And API Gateway
   10-5 Enable SHA1 for devices
   10-6 Disable SHA1 for devices
```

Main Menu Options

```
1. System
2. File Operations
3. Show
4. System Configuration
5. Advanced
6. Security
7. Support
8. Temporary Root Shell
9. Authentication
10. Certificate configuration
11. Search commands
==================================
0. exit

Enter option [ 0 - 11 ]: 10
```

From the previous menu option, select **10** to display Certificate configuration options.

```
1. Disable client cert strict check
2. Generate device cert
3. Disable client cert strict check for devices.
4. Apply default certificates to Web UI And API Gateway
5. Enable SHA1 for devices
6. Disable SHA1 for devices

============================
b. back
m. main menu
0. exit
Enter option [0-6]:
```

Related Commands

Command	Description
Disable client cert strict check	Disables the client certificate check.
Generate device cert	Generates the device certificate.
Disable client cert strict check for devices	Disables the client certificate for devices.
Apply default certificates to Web UI And API Gateway	Applies the wildcard certificate and login to COP directly.
Enable SHA1 for devices	Enables SHA1 for devices.
Disable SHA1 for devices	Disables SHA1 for devices.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Disable client cert strict check

```
10 Certificate Configuration
   1 Disable client cert strict check
```

Description

Enter the command option **1** from the Certificate Configuration menu to disable the client certificate check.

After disabling strict mode from the Command Line Interface (CLI), you must wait for 5 to 10 minutes until the system reaches a stable state.

The Disable client cert strict check command includes the following information.

Certificate Configuration Options

```
1. Disable client cert strict check
2. Generate device cert
3. Disable client cert strict check for devices.
4. Apply default certificates to Web UI And API Gateway
5. Enable SHA1 for devices
6. Disable SHA1 for devices

============================
b. back
m. main menu
0. exit
Enter option [0-6]: 1
```

From the Certificate Configuration options, select **1** to disable client cert strict check.

```
Strict client cert is already disabled
Press [Enter] key to continue...
```

Related Commands

Command	Description
Generate device cert	Generates the device certificate.
Disable client cert strict check for devices	Disables the client certificate for devices.
Apply default certificates to Web UI And API Gateway	Applies the wildcard certificate and login to COP directly.
Enable SHA1 for devices	Enables SHA1 for devices.
Disable SHA1 for devices	Disables SHA1 for devices.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Generate device cert

```
10 Certificate Configuration
   2 Generate device cert
```

Description

Enter the command option **2** from the Certificate Configuration menu to generate the device certificate.

Certificate Configuration Options

```
1. Disable client cert strict check
2. Generate device cert
3. Disable client cert strict check for devices.
4. Apply default certificates to Web UI And API Gateway
5. Enable SHA1 for devices
6. Disable SHA1 for devices

============================
b. back
m. main menu
0. exit
Enter option [0-6]: 2
```

From the Certificate Configuration options, select **2** to generate device cert.

Generate Device Cert Options

```
1. Generate local device certificate
2. LDevID Certificate Management
==================================
b. back
m. main menu
0. exit

Enter option [ 0 - 2 ]: 2
```

From the previous menu option, select **2** to generate the LDevID certificate for devices.

```
1. View LDevID Certificate Details
2. System LDevID Readiness Check
3. Provision LDevID Certificate
4. Delete LDevID Certificate
5. View LDevID Renewal Schedule
6. Manage LDevID Renewal Schedule
==================================
b. back
m. main menu
0. exit

Enter option [ 0 - 6 ]:  1
```

The following output displays the detailed information about the LDevID Certificate:

```
============================================================
  LDevID Certificate Details
============================================================
  Overall Status           : [OK]    ACTIVE
  Certificate Name         : LDevID Cert
  Certificate Type         : LDEVID_CERT
  Category                 : Device Certificate

------------------------------------------------------------
  Node: cop-node-129-130.arubacorp.net
------------------------------------------------------------
  Common Name (CN)         : S4P01A
  Country (C)              : US
  State (ST)               : N/A
  Locality (L)             : N/A
  Organization (O)         : Hewlett Packard Enterprise Development
  Org Unit (OU)            : HPE ANW

  Issuer CN                : Aruba Management CA 100
  Issuer C                 : US
  Issuer O                 : Hewlett Packard Enterprise Development
  Issuer OU                : Aruba

  Valid From               : Jun 09, 2026 10:44:30 UTC
  Valid Till               : Dec 31, 9999 23:59:59 UTC
  Serial Number            : 630005623795357718218085528051779757340
  Version                  : N/A

------------------------------------------------------------
  Node: cop-node-129-131.arubacorp.net
------------------------------------------------------------
  Common Name (CN)         : S4P01A
  Country (C)              : US
  State (ST)               : N/A
  Locality (L)             : N/A
  Organization (O)         : Hewlett Packard Enterprise Development
  Org Unit (OU)            : HPE ANW

  Issuer CN                : Aruba Management CA 100
  Issuer C                 : US
  Issuer O                 : Hewlett Packard Enterprise Development
  Issuer OU                : Aruba

  Valid From               : Jun 09, 2026 10:59:38 UTC
  Valid Till               : Dec 31, 9999 23:59:59 UTC
  Serial Number            : 571471884505683433785288433476538082602
  Version                  : N/A

------------------------------------------------------------
  Node: cop-node-129-132.arubacorp.net
------------------------------------------------------------
  Common Name (CN)         : S4P01A
  Country (C)              : US
  State (ST)               : N/A
  Locality (L)             : N/A
  Organization (O)         : Hewlett Packard Enterprise Development
  Org Unit (OU)            : HPE ANW

  Issuer CN                : Aruba Management CA 100
  Issuer C                 : US
  Issuer O                 : Hewlett Packard Enterprise Development
```

```
  Issuer OU                : Aruba

  Valid From               : Jun 09, 2026 11:05:46 UTC
  Valid Till               : Dec 31, 9999 23:59:59 UTC
  Serial Number            : 570691084990621485714023390600298651028
  Version                  : N/A

Press [Enter] key to continue...
```

Related Commands

Command	Description
Disable client cert strict check	Disables the client certificate check.
Disable client cert strict check for devices	Disables the client certificate for devices.
Apply default certificates to Web UI And API Gateway	Applies the wildcard certificate and login to COP directly.
Enable SHA1 for devices	Enables SHA1 for devices.
Disable SHA1 for devices	Disables SHA1 for devices.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Disable client cert strict check for devices

```
10 Certificate Configuration
   3 Disable client cert strict check for devices
```

Description

Enter the command option **3** from the Certificate Configuration menu to disable the client certificate for devices.

Certificate Configuration Options

```
1. Disable client cert strict check
2. Generate device cert
3. Disable client cert strict check for devices.
4. Apply default certificates to Web UI And API Gateway
5. Enable SHA1 for devices.
6. Disable SHA1 for devices

============================
b. back
m. main menu
0. exit
Enter option [0-6]: 3
```

From the Certificate Configuration options, select **3** to disable client cert strict check.

```
Disabling client strict check for devices.
Successfully updated client cert strict check for devices.
Restarting a few components for the updated strict cert check to take
effect. This may take a few minutes.
Press [Enter] key to continue...
```

Related Commands

Command	Description
Disable client cert strict check	Disables the client certificate check.
Generate device cert	Generates the device certificate.
Apply default certificates to Web UI And API Gateway	Applies the wildcard certificate and login to COP directly.
Enable SHA1 for devices	Enables SHA1 for devices.
Disable SHA1 for devices	Disables SHA1 for devices.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Apply default certificates to Web UI And API Gateway

```
10 Certificate configuration
   4 Apply default certificates to Web UI And API Gateway
```

Description

Enter the command option **4** to apply the wildcard certificate and login to HPE Aruba Networking Central On-Premises directly.

Certificate Configuration Options

```
1. Disable client cert strict check
2. Generate device cert
3. Disable client cert strict check for devices.
4. Apply default certificates to Web UI And API Gateway
5. Enable SHA1 for devices
6. Disable SHA1 for devices

============================
b. back
m. main menu
0. exit
Enter option [0-6]: 4
```

From the previous menu option, select **4** toApply default certificates to Web UI And API Gateway options.

```
Generating and applying default UI and GW certificates...
Are you sure you want to generate and apply default certificate for UI and
API Gateway? (Y/N): Y
Generating default certificates for UI And API GW services.
Cluster details is : vip - 10.xx.xxx.xxx, public ip - 10.xx.xxx.xxx, fqdn -
cop-3n-cap-cx.arubaxxx.com
-----BEGIN CERTIFICATE-----
MIIFsTCCA5mgAwIBAgIUS2RKkgKVAvEbWRM9Ya5VTBgxUuswDQYJKoZIhvcNAQEL
BQAwZzELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAkNBMRIwEAYDVQQHDAlTdW5ueXZh
bGUxEDAOBgNVBAoMB0FpcndhdmUxJTAjBgNVBAMMHGNvcC0zbi1jYXAtY3guYXJ1
YmF0aGVuYS5jb20wIBcNMjMwNzA3MDkwNzU1WhgPMjA1MDExMjIwOTA3NTVaMGcx
CzAJBgNVBAYTAlVTMQswCQYDVQQIDAJDQTESMBAGA1UEBwwJU3Vubnl2YWxlMRAw
DgYDVQQKDAdBaXJ3YXZlMSUwIwYDVQQDDBxjb3AtM24tY2FwLWN4LmFydWJhdGhl
bmEuY29tMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAtLrbSWC6OEf3
8RPsIy2Emi1D07jR6sgDv67D3ozvKXld1/dDoTw1/uluf/zgGa5rOU5v6+tLocO5
TOdedtyUflsq89kpkeF3UDO1Vbu+dSkOI5ZS84eUwewQ8a5oVjCwYfmbgThqwDgF
2jdUb4udYhEGKRCtlNJdDa5Chd4HEfqGsRWJzLNbWQfHFNIayCqbg/PFnqKU65u9
iV4Df/jWnh/2eJP/ZtcknPfwtoScGHypc6XvsMOUQTNf0JCOTCkxbvlqu7QqNbwB
7IfYnsNPuOw/rmPkm6Dt3TKDxkg5ajDjy6m21GIgAUSvmNO47/SdrvXhBBowYfRG
EWednb6if+Cm+bfX1+5Eeg1sSGDukNkxExZUpN8rrqX1gG3iGxA/zEJuBj50OVHJ
/TSx68C080LvrgnfoAmnMV8JnmSAVEJcRtGR5YOM0FKcBlkME8dlj/RgRx9b+HbW
M4GL8nmHdQc4yaM8T4dPs/ko6ESdRXe677Egk4AHiwA9UgQJbM1Rp2snQj8djDGQ
980WxoJayJkm7R+6NVh26mzXM3mjtXqFl6aFf60TcKVJzFg1KTYPb4nWDShkUqTR
voy2dxc+nP4ZISlXWBdK1KNqH5tNjfcAYWkKAFZSN4uXw5OgjeWBjv/l2hXG6l0Q
Sy8w0H249RQ6w/2SPSN/LGbrONyjlaUCAwEAAaNTMFEwHQYDVR0OBBYEFDSW9Su2
grmExanvvUNaJblA1MXFMB8GA1UdIwQYMBaAFDSW9Su2grmExanvvUNaJblA1MXF
MA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQELBQADggIBAA7/7G9wBvnZkdM6
S6BcEGlgOrlqu024FN7K10MFoEXnh4WfUwnfaplykvh1ogYmMXYbWXJ7zVrDGFs8
```

```
FiHhMjVTCRfjfvFPqaMMErPTIxH2/6UKAn5m2+6AWaGnxkwlQDwrXPorDj8chvBc
K8mutI5nNZIlQWQ7iT/CZy4EPBVC8m6SpP3yRXD6fpt3IE75yAvV+duTsyuqRUjl
F6rSsLW2F/BzJsywvGTZdVxICE9q363mTkMDJSb0PKMoRK4HQMVoq6zle/Im79s+
0X5B+chBmDsPu/4QCgr7xeqc07lKW2F5Q2FKlQICBiL7InmOAzeQz9vFzzb6KW6L
OB/pluF3uvoPFPnG57k3ft6YAGBzQh9xft6VDSmZ60p4hREVON0Vh0m3JKpdwdJd
43GmmMxbFItQcBQ2/HjbvDJhcdXUOoeJdHiAgQ/kfm2iyemkR+DbQWQKuO9vffT6
eLvVb1LiVh+/GyJg5yV+Jx6Z5OgfyyN8Md+Qqf+/oAEowtH9Tlzq9hMUMoNfvcBE
QCVS9riUT+diimJfVu57wOUkUKZ7xpWb8xJByQV1aU5AGUJYvCvtJwgC1+3sdSVw
zhCRzd3C3J4hm6ETpKr8ZV5GtWk0btFvAbiYDspqJh4UBGjtuonUJExw4yYWGN2R
O3G847Z4tubO+zaXCkmyN4joDTDd
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIIJKgIBAAKCAgEAtLrbSWC6OEf38RPsIy2Emi1D07jR6sgDv67D3ozvKXld1/dD
oTw1/uluf/zgGa5rOU5v6+tLocO5TOdedtyUflsq89kpkeF3UDO1Vbu+dSkOI5ZS
84eUwewQ8a5oVjCwYfmbgThqwDgF2jdUb4udYhEGKRCtlNJdDa5Chd4HEfqGsRWJ
zLNbWQfHFNIayCqbg/PFnqKU65u9iV4Df/jWnh/2eJP/ZtcknPfwtoScGHypc6Xv
sMOUQTNf0JCOTCkxbvlqu7QqNbwB7IfYnsNPuOw/rmPkm6Dt3TKDxkg5ajDjy6m2
1GIgAUSvmNO47/SdrvXhBBowYfRGEWednb6if+Cm+bfX1+5Eeg1sSGDukNkxExZU
pN8rrqX1gG3iGxA/zEJuBj50OVHJ/TSx68C080LvrgnfoAmnMV8JnmSAVEJcRtGR
5YOM0FKcBlkME8dlj/RgRx9b+HbWM4GL8nmHdQc4yaM8T4dPs/ko6ESdRXe677Eg
k4AHiwA9UgQJbM1Rp2snQj8djDGQ980WxoJayJkm7R+6NVh26mzXM3mjtXqFl6aF
f60TcKVJzFg1KTYPb4nWDShkUqTRvoy2dxc+nP4ZISlXWBdK1KNqH5tNjfcAYWkK
AFZSN4uXw5OgjeWBjv/l2hXG6l0QSy8w0H249RQ6w/2SPSN/LGbrONyjlaUCAwEA
AQKCAgEAp+ulq7vvyjM0MA5urRCxz/6WsrVadWZ59TOQUctou4REqVDYyYqEMOD7
BngSUEo63ff/DZiFoTuVg9rFbnLslapnckIn2Z8/mIkyxwG1qG4I8Q/O6u7iTHvm
EmgWEV8TwzSEQ8ADj6194o7eKPXzuRZQPv98CHacdwWeUXtF3nKDiy2T51oOWd5c
HwBIWgsci7GHwCkXbQI7TNLJNbIi1rCj9Myt1QO4xQ+p3CvCTQ4m84kN95MAwMPX
FpX5YNI1WALuJJD1Vw/kSby+jGS0QgFf+cxesCsKVyeEQEsC7aOXQ7fgY9z4F7WV
4c12W51QlStncsRSh/DK2YkIbXSezdpMsvBEkvBQgys422AdtjK7jjDQcSOr32/J
WZ2MaFHAhFdYqvIGTP02I8lbFgKxYctJyZ4GKQ1Bmq73hRCflM3kxE6ZdQC6qlcj
ySMzppl5zTCEgV6bK160LSaBZGhIHy3zHOo4nsB6LKj8xnTnAUNyZiOkvAmbojZO
fXobjvZVzjipinFXyI9xCoIT2QRPUXuniYhSRIEDR1rP2IbFksEq1GBwALCp746R
f8mObXsnTOJYrW+MaDQvDC8g7jHw0o66jCxbPhGMXx1INKQvZGmz3oqZp2+EFmd3
zgR9VEqFXP2CCcTSLOiOYzdTaY+RkKa++iZdvPrA8GA25pgiddECggEBANrYRYxc
WZ9NuQfShKqyyhfd20/xdiQULWpQ0LoYfctMVqgV6isnzn80hD0sqjCtfTl7mtag
nSf/LcTwSTQKoKl3nG2ulnXddjXrfHkCranWC9Z8uwSwdcUb/m37p1TiwhVANSV8
djsPZ23YLlSuGNuF2ltnY2V/Aic7YFiVBjy3ZXJP1PwDsYImVpH8xeui1gQteVs9
KnT7G8614QOw404QOnQhMNPNNXtlo8HVoP0ul+dewOPTRLBdSoopdQXl4brVbSJR
K+VYA8tUD4WdIdJwJLhwHyLelWd3ZU/qmSB37XG0y9xRy1oNuYsGt/8dN+DGvaIM
sGI8/4j5m/CaxhMCggEBANNp+84Ed+oVQvcfE3gbsoGMhnEVD5pLihArP1I5wbxP
6JiGE6feUqAe6S/Cmx7jo7mXxeDC6H+jPQdHvyI2ncNU9T5pud0aYIuWJu4gMdg0
/2PSfLzMDyw4yXSRear0rmmt3k+MLxeCnn7MNqAu+//uevdWEmVEmJR1vpQGVMPO
WnaqLUvWF4f5h5KFf4l7gD/x8m5jU45xVCq0N+m9PJhDbcxHi/l3mpiXQ0vVGfcs
HRBOTMErmcQggLskgPiUbbTKAXS4vRE61rkUQV9pyjo420+eXHZRFXi9E5BL7H8b
ZDrV5T8+H5a/Ue68Oo12DVByWzEgmifdnYRUs6U3DGcCggEBANGkTnOYYC5wKSlq
LLbNETXtzNL3T6JeRedLxbgQECl5VqYsYCe5OWK4L1ne+KYq/APd+cVTFVmkZPb8
7FNTPvc44vxbPD1qynv6u0G9JBnHN43f7NQgKqGJIKHBalmx5BSxbngbk7MeHYmn
hzKNmLhqsHPRRfGLysdEZRZWpCPz19W6ziAhdaFlEpdFG2CQnA5idZfGr25iww+x
Qf3kLMuyVhy7UugC9BHimw3rlQ4U3WXCamuVDn8Yz3gtILJmtmfhXmt6cN+CAhh8
zWXE0gqibTrWBa3EpkD4qm/1H31wBWFgvc2v+WqqLS0WYZqdJdNI745WM33YSz6v
RwglbEsCggEBAMuB5ABG0N+mI9YaNfWSQ9zs1qWYLnLKcFZsKwIN0u5gxXe86MLZ
AhRcbP+qhwPPAVWwQazAMmpbSm3tpJFcnbTf3Ut9Hos1zuXPXh4vI4wKSCVhAu4C
SEC7UUFCoCnuas4TrkJIoTQyajuIfLTpRW7xs7DPS9nrlCykwxVems35n59G5V9w
8SnVC6oBk+lV1vi3ADU+q7ocYXbSEFiR7vhrQBA6dwVnGov0X7VppxsFfdyqYrw4
KkZfO0vqMbQXvRsgsRIYmvcw+m0ikGM2RJKTFJmpyTujhdW5vFFUpI0eYvc32vtr
46CK/mWfD4YIs3xS+HFr/riNXgl6N4u8V9UCggEAD+MnL/vM/Z1EBQzcEjIq4ZWk
GYsCbeFF4f4Zm1m8ZfpZQ2rPGCR6OaSlEdh3Zs2Gto/3SrqdWxl7esqnr5uUBKA4
b+ndoX+2B6JShu0pooA3o8TIHOh0bTJTHO0ei9YMtBh92AgRtdkszWjcrstHOFnt
3oD0MGPjo9byYK56AzkaEIKuJrZKXmFCD2HbiTdA93I6/gxzpr/GC3GRq4WNPzRP
mHdMuVajsESfquwMKH9wLGb5UxHuwLYc3ePQrpBlKqMklhJDFNNOpekozBKNbndP
+t8xdBLszcAmmOdQnWOKF2JevTTaffePG+NG8TBwA1acDT8lDgKySZtWS7S7rA==
```

```
-----END RSA PRIVATE KEY-----
Refreshing API certificate store...
Response :
ERROR : Refreshing API certificate store failed.
Press [Enter] key to continue...
```

Related Commands

Command	Description
Disable client cert strict check	Disables the client certificate check.
Generate device cert	Generates the device certificate.
Disable client cert strict check for devices	Disables the client certificate for devices.
Enable SHA1 for devices	Enables SHA1 for devices.
Disable SHA1 for devices	Disables SHA1 for devices.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

Enable SHA1 for devices

```
10 Certificate configuration
   5 Enable SHA1 for devices
```

Description

Enter the command option **5** to enable SHA1 for devices.

Certificate Configuration Options

```
1. Disable client cert strict check
2. Generate device cert
3. Disable client cert strict check for devices.
4. Apply default certificates to Web UI And API Gateway
5. Enable SHA1 for devices
6. Disable SHA1 for devices

============================
b. back
m. main menu
0. exit
Enter option [0-6]: 5
```

From the previous menu option, select **5** to enable SHA1 for devices.

```
=== NGINX ConfigMap SSL Ciphers Patcher ===
ConfigMap: nginx-device-configuration
Namespace: ingress-nginx
Action: enable_sha1

Applying SHA1-compatible SSL ciphers configuration (for legacy support)...
WARNING: This configuration allows SHA1 and should only be used for legacy
compatibility!
Are you sure you want to enable SHA1-compatible SSL ciphers? (y/N): Y
configmap/nginx-device-configuration patched
Successfully applied SHA1-compatible SSL ciphers configuration
Applied ciphers:
DEFAULT@SECLEVEL=0:!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!SRP:!DSS:!RC4

=== Operation completed ===
Press [Enter] key to continue...
```

Related Commands

Command	Description
Disable client cert strict check	Disables the client certificate check.
Generate device cert	Generates the device certificate.
Disable client cert strict check for devices	Disables the client certificate for devices.

Command	Description
Apply default certificates to Web UI And API Gateway	Applies the wildcard certificate and login to COP directly.
Disable SHA1 for devices	Disables SHA1 for devices.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.1.0	Command introduced.

Disable SHA1 for devices

```
10 Certificate configuration
   6 Disable SHA1 for devices
```

Description

Enter the command option **6** to disable SHA1 for devices.

Certificate Configuration Options

```
1. Disable client cert strict check
2. Generate device cert
3. Disable client cert strict check for devices.
4. Apply default certificates to Web UI And API Gateway
5. Enable SHA1 for devices
6. Disable SHA1 for devices

============================
b. back
m. main menu
0. exit
Enter option [0-6]: 6
```

From the previous menu option, select **6** to disable SHA1 for devices.

```
=== NGINX ConfigMap SSL Ciphers Patcher ===
ConfigMap: nginx-device-configuration
Namespace: ingress-nginx
Action: disable_sha1
Applying secure SSL ciphers configuration (disabling SHA1)...
configmap/nginx-device-configuration patched
Successfully applied secure SSL ciphers configuration (SHA1 disabled)
Applied ciphers: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-
AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-
ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA384:DHE-RSA-AES128-SHA256:DHE-RSA-
AES256-SHA256:AES256-GCM-SHA384:AES128-GCM-SHA256:AES256-SHA256:AES128-
SHA256
=== Operation completed ===
Press [Enter] key to continue...
```

Related Commands

Command	Description
Disable client cert strict check	Disables the client certificate check.
Generate device cert	Generates the device certificate.
Disable client cert strict check for devices	Disables the client certificate for devices.

Command	Description
Apply default certificates to Web UI And API Gateway	Applies the wildcard certificate and login to COP directly.
Enable SHA1 for devices	Enables SHA1 for devices.

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.1.0	Command introduced.

Search commands

```
11 Search commands
```

Description

This command allows the user to search the commands.

Enter the command option **11** from the main menu to display the list of commands or search a particular command.

Hierarchy Level

```
11 Search Commands
```

Main Menu Options

```
1. System
2. File Operations
3. Show
4. System Configuration
5. Advanced
6. Security
7. Support
8. Temporary Root Shell
9. Authentication
10. Certificate configuration
11. Search commands
==================================
0. exit

Enter option [ 0 - 11 ]: 11
```

From the main menu option, select **11** to display the Search commands options.

```
Enter the text to get the list of available command options (case
insensitive) :
                1) System -> Reboot
1) System -> Reboot
2) System -> Shutdown
3) System -> Factory Reset
4) File Operations -> Upload via (SCP)
5) File Operations -> Upload via (SFTP)
6) File Operations -> Upload via (HTTP/HTTPS)
7) File Operations -> Download File from COP
8) File Operations -> Delete file
9) Show -> Version (Detail)
10) Show -> List Files
11) Show -> Backup-Restore Status
12) Show -> Configuration -> Network-config/Cluster-info
13) Show -> Configuration -> NTP/Timezone Info
14) Show -> Configuration -> Show ILO IP Configuration
15) Show -> System -> Memory/Hard disk/CPU Usage
16) Show -> System -> Uptime
17) Show -> User Sessions
18) Show -> Clock
19) Show -> App Status
```

```
20) Show -> Cluster Status
21) System Configuration -> Upgrade
22) System Configuration -> Network Setup -> Permanent (Network settings)
23) System Configuration -> Network Setup -> Temporary (Network settings)
24) System Configuration -> Network Setup -> Switch Network Interface
25) System Configuration -> Network Setup -> Network Link Aggregation Setup
-> Enable Network Link Aggregation
26) System Configuration -> Network Setup -> Network Link Aggregation Setup
-> Disable Network Link Aggregation
27) System Configuration -> Network Setup -> Network Link Aggregation Setup
-> Check status of Network Link Aggregation
28) System Configuration -> Proxy Setup -> Add Proxy
29) System Configuration -> Proxy Setup -> Delete Proxy
30) System Configuration -> Proxy Setup -> Get Proxy
31) System Configuration -> Setup Timezone
32) System Configuration -> Setup NTP
33) System Configuration -> Node Setup -> Add node
34) System Configuration -> Node Setup -> Replace node
35) System Configuration -> Node Setup -> Status
36) System Configuration -> Air Gap -> Enable Airgap
37) System Configuration -> Air Gap -> Disable Airgap
38) System Configuration -> Air Gap -> Status
39) System Configuration -> Datacenter Redundancy -> Show Datacenter
Redundancy Status
40) System Configuration -> Datacenter Redundancy -> Configure Datacenter
Redundancy  -> Show Config
41) System Configuration -> Datacenter Redundancy -> Configure Datacenter
Redundancy  -> Show Datacenter Redundancy Pairing Key
42) System Configuration -> Datacenter Redundancy -> Configure Datacenter
Redundancy  -> Configure
43) System Configuration -> Datacenter Redundancy -> Configure Datacenter
Redundancy  -> Enable Redundancy
44) System Configuration -> Datacenter Redundancy -> Configure Datacenter
Redundancy  -> Disable Redundancy
45) System Configuration -> Datacenter Redundancy -> Automatic Failover ->
Disable
46) System Configuration -> Datacenter Redundancy -> Automatic Failover ->
Enable
47) System Configuration -> Datacenter Redundancy -> Restore Frequency
48) System Configuration -> Datacenter Redundancy -> Time to Failover
49) System Configuration -> Datacenter Redundancy -> Initiate Switchover
50) System Configuration -> Datacenter Redundancy -> Remove Datacenter
Redundancy Configuration
51) Advanced -> Test Connectivity -> Ping
52) Advanced -> Test Connectivity -> Dependent Servers Reachability
53) Advanced -> NsLookup
54) Advanced -> Toggle CDN -> Enable CDN
55) Advanced -> Toggle CDN -> Disable CDN
56) Advanced -> Toggle CDN -> Show CDN status
57) Advanced -> Configure ILO IP
58) Advanced -> Enable or Disable NOPASSWORD for copadmin -> Enable
NOPASSWORD
59) Advanced -> Enable or Disable NOPASSWORD for copadmin -> Disable
NOPASSWORD
60) Security -> Reset Password GUI
61) Security -> Reset Password CLI
62) Security -> Reset debug apps password
63) Security -> Reset ILO Administrator Password
64) Support -> Support Connection -> Start Support Connection
65) Support -> Support Connection -> Stop Support Connection
66) Support -> Support Connection -> Restart Support Connection
```

```
67) Support -> Support Connection -> Support Connection Status
68) Support -> Support Connection -> Upload Support Connection File
69) Support -> Support Connection -> Add Support User 'copsupport'
70) Support -> Support Connection -> Delete Support User 'copsupport'
71) Support -> Support Connection -> Show contents of copsupport.gpg
72) Support -> Collect COP Cluster logs -> Collect basic cluster info while
collecting logs
73) Support -> Collect COP Cluster logs -> Collect advance cluster info
while collecting logs
74) Support -> Log Snapshot Operations -> Generate Snapshots for a Category
75) Support -> Log Snapshot Operations -> Generate System Operation Logs
76) Support -> Log Snapshot Operations -> Generate Pod Logs
77) Support -> Log Snapshot Operations -> Generate Node Snapshot
78) Support -> Log Snapshot Operations -> Download Logs/Snapshots
79) Support -> Log Snapshot Operations -> Delete Logs/Snapshots
80) Support -> Log Snapshot Operations -> Download Upgrade Reports
81) Support -> Download COP Setup Logs
82) Support -> Restart Application
83) Support -> System Operations Lock Management -> Lock status
84) Support -> System Operations Lock Management -> Release Lock -> Upgrade
85) Support -> System Operations Lock Management -> Release Lock -> Backup
86) Support -> System Operations Lock Management -> Release Lock -> Restore
87) Support -> System Operations Lock Management -> Release Lock ->
Migration
88) Support -> System Operations Lock Management -> Release Lock -> Add node
89) Support -> System Operations Lock Management -> Release Lock -> Replace
node
90) Support -> System Operations Lock Management -> Release Lock -> Reboot
node
91) Support -> System Operations Lock Management -> Update Lock Setting ->
on
92) Support -> System Operations Lock Management -> Update Lock Setting ->
off
93) Support -> Reset allowed management subnet
94) Support -> Logging Tool Management -> Show Logging Framework Status
95) Support -> Logging Tool Management -> Cleanup Logging Framework
96) Temporary Root Shell
97) Authentication -> Display public key
98) Authentication -> Add public key to COP
99) Authentication -> List all public key added COP
100) Certificate configuration -> Enable client cert strict check
101) Certificate configuration -> Disable client cert strict check
102) Certificate configuration -> Generate device cert
103) Certificate configuration -> Disable client cert strict check for
devices.
104) Certificate configuration -> Apply default certificates to Web UI And
API Gateway
105) Certificate configuration -> Show Root CA Cert
106) Search commands
```

Command History

Release	Modification
HPE Aruba Networking Central On-Premises 3.0.0.0	Command introduced.

What's New in HPE Aruba Networking Central On-Premises 3.0.3.0

This section lists the commands introduced, modified, or deprecated in HPE Aruba Networking Central On-Premises 3.0.1.0

New Commands in HPE Aruba Networking Central On-Premises 3.0.3.0

The following commands were introduced in HPE Aruba Networking Central On-Premises 3.0.3.0:

Command	Description
`4-8 Disaster Recovery`	This command is introduced for the Disaster Recovery feature. It consists of the following options: ▪Show Disaster Recovery Status ▪Show Disaster Recovery Config ▪Disable Disaster Recovery Feature ▪Manual Failver

Appendix B - Glossary of Terms

The following is the list of terminologies used in this guide.

3DES

Triple Data Encryption Standard. 3DES is a symmetric-key block cipher that applies the DES cipher algorithm three times to each data block.

3G

Third Generation of Wireless Mobile Telecommunications Technology. See W-CDMA.

3GPP

Third Generation Partnership Project. 3GPP is a collaborative project aimed at developing globally acceptable specifications for third generation mobile systems.

4G

Fourth Generation of Wireless Mobile Telecommunications Technology. See LTE.

802.11

802.11 is an evolving family of specifications for wireless LANs developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). 802.11 standards use the Ethernet protocol and Carrier Sense Multiple Access with collision avoidance (CSMA/CA) for path sharing.

802.11 bSec

802.11 bSec is an alternative to 802.11i. The difference between bSec and standard 802.11i is that bSec implements Suite B algorithms wherever possible. Notably, Advanced Encryption Standard-Counter with CBC-MAC is replaced by Advanced Encryption Standard - Galois/Counter Mode, and the Key Derivation Function (KDF) of 802.11i is upgraded to support SHA-256 and SHA-384.

802.11a

802.11a provides specifications for wireless systems. Networks using 802.11a operate at radio frequencies in the 5 GHz band. The specification uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM) that is especially well suited to use in office settings. The maximum data transfer rate is 54 Mbps.

802.11ac

802.11ac is a wireless networking standard in the 802.11 family that provides high-throughput WLANs on the 5 GHz band.

802.11b

802.11b is a WLAN standard often called Wi-Fi and is backward compatible with 802.11. Instead of the Phase-Shift Keying (PSK) modulation method used in 802.11 standards, 802.11b uses Complementary Code Keying (CCK) that allows higher data speeds and makes it less susceptible to multipath-propagation interference. 802.11b operates in the 2.4 GHz band and the maximum data transfer rate is 11 Mbps.

802.11d

802.11d is a wireless network communications specification for use in countries where systems using other standards in the 802.11 family are not allowed to operate. Configuration can be fine-tuned at the Media Access Control (MAC) layer level to comply with the rules of the country or district in which the network is to be used. Rules are subject to variation and include allowed frequencies, allowed power levels, and allowed signal bandwidth. 802.11d facilitates global roaming.

802.11e

802.11e is an enhancement to the 802.11a and 802.11b specifications that enhances the 802.11 Media Access Control layer with a coordinated Time Division Multiple Access (TDMA) construct. It adds error-correcting mechanisms for delay-sensitive applications such as voice and video. The 802.11e specification provides seamless interoperability between business, home, and public environments such as airports and hotels, and offers all subscribers high-speed Internet access with full-motion video, high-fidelity audio, and VoIP.

802.11g

802.11g offers transmission over relatively short distances at up to 54 Mbps, compared with the 11 Mbps theoretical maximum of 802.11b standard. 802.11g employs Orthogonal Frequency Division Multiplexing (OFDM), the modulation scheme used in 802.11a, to obtain higher data speed. Computers or terminals set up for 802.11g can fall back to speed of 11 Mbps, so that 802.11b and 802.11g devices can be compatible within a single network.

802.11h

802.11h is intended to resolve interference issues introduced by the use of 802.11a in some locations, particularly with military Radar systems and medical devices. Dynamic Frequency Selection (DFS) detects the presence of other devices on a channel and automatically switches the network to another channel if and when such signals are detected. Transmit Power Control (TPC) reduces the radio frequency (RF) output power of each network transmitter to a level that minimizes the risk of interference.

802.11i

802.11i provides improved encryption for networks that use 802.11a, 802.11b, and 802.11g standards. It requires new encryption key protocols, known as Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).

802.11j

802.11j is a proposed addition to the 802.11 family of standards that incorporates Japanese regulatory extensions to 802.11a; the main intent is to add channels in the radio frequency (RF) band of 4.9 GHz to 5.0 GHz.

802.11k

802.11k is an IEEE standard that enables APs and client devices to discover the best available radio resources for seamless BSS transition in a WLAN.

802.11m

802.11m is an Initiative to perform editorial maintenance, corrections, improvements, clarifications, and interpretations relevant to documentation for 802.11 family specifications.

802.11n

802.11n is a wireless networking standard to improve network throughput over the two previous standards, 802.11a and 802.11g. With 802.11n, there will be a significant increase in the maximum raw data rate from 54 Mbps to 600 Mbps with the use of four spatial streams at a channel width of 40 MHz.

802.11r

802.11r is an IEEE standard for enabling seamless BSS transitions in a WLAN. 802.11r standard is also referred to as Fast BSS transition.

802.11u

802.11u is an amendment to the IEEE 802.11 WLAN standards for connection to external networks using common wireless devices such as smartphones and tablet PCs. The 802.11u protocol provides wireless clients with a streamlined mechanism to discover and authenticate to suitable networks, and allows mobile users to roam between partner networks without additional authentication. An 802.11u-capable device supports the Passpoint technology from the Wi-Fi Alliance Hotspot 2.0 R2 Specification that simplifies and automates access to public Wi-Fi.

802.11v

802.11v is an IEEE standard that allows client devices to exchange information about the network topology and RF environment. This information is used for assigning best available radio resources for the client devices to provide seamless connectivity.

802.1Q

802.1Q is an IEEE standard that enables the use of VLANs on an Ethernet network. 802.1Q supports VLAN tagging.

802.1X

802.1X is an IEEE standard for port-based network access control designed to enhance 802.11 WLAN security. 802.1X provides an authentication framework that allows a user to be authenticated by a central authority.

802.3af

802.3af is an IEEE standard for Power over Ethernet (PoE) version that supplies up to 15.4W of DC power. See PoE.

802.3at

802.3at is an IEEE standard for PoE version that supplies up to 25.5W of DC power. See PoE+.

A-MPDU

Aggregate MAC Protocol Data Unit. A-MPDU is a method of frame aggregation, where several MPDUs are combined into a single frame for transmission.

A-MSDU

Aggregate MAC Service Data Unit. A-MSDU is a structure containing multiple MSDUs, transported within a single (unfragmented) data MAC MPDU.

AAA

Authentication, Authorization, and Accounting. AAA is a security framework to authenticate users, authorize the type of access based on user credentials, and record authentication events and information about the network access and network resource consumption.

ABR

Area Border Router. ABR is used for establishing connection between the backbone networks and the Open Shortest Path First (OSPF) areas. ABR is located near the border of one or more OSPF areas.

AC

Access Category. As per the IEEE 802.11e standards, AC refers to various levels of traffic prioritization in Enhanced Distributed Channel Access (EDCA) operation mode. The WLAN applications prioritize traffic based on the Background, Best Effort, Video, and Voice access categories. AC can also refer to Alternating Current, a form of electric energy that flows when the appliances are plugged to a wall socket.

ACC

Advanced Cellular Coexistence. The ACC feature in APs enable WLANs to perform at peak efficiency by minimizing interference from 3G/4G/LTE networks, distributed antenna systems, and commercial small cell/femtocell equipment.

Access-Accept

Response from the RADIUS server indicating successful authentication and containing authorization information.

Access-Reject

Response from RADIUS server indicating that a user is not authorized.

Access-Request

RADIUS packet sent to a RADIUS server requesting authorization.

Accounting-Request

RADIUS packet type sent to a RADIUS server containing accounting summary information.

Accounting-Response

RADIUS packet sent by the RADIUS server to acknowledge receipt of an Accounting-Request.

ACE

Access Control Entry. ACE is an element in an ACL that includes access control information.

ACI

Adjacent Channel Interference. ACI refers to interference or interruptions detected on a broadcasting channel, caused by too much power on an adjacent channel in the spectrum.

ACL

Access Control List. ACL is a common way of restricting certain types of traffic on a physical port.

Active Directory

Microsoft Active Directory. The directory server that stores information about a variety of things, such as organizations, sites, systems, users, shares, and other network objects or components. It also provides authentication and authorization mechanisms, and a framework within which related services can be deployed.

ActiveSync

Mobile data synchronization app developed by Microsoft that allows a mobile device to be synchronized with either a desktop or a server running compatible software products.

ad hoc network

An ad hoc network is a network composed of individual devices communicating with each other directly. Many ad hoc networks are Local Area Networks (LANs) where computers or other devices are enabled to send data directly to one another rather than going through a centralized access point.

ADO

Active X Data Objects is a part of Microsoft Data Access Components (MDACs) that enables client applications to access data sources through an (Object Linking and Embedding Database) OLE DB provider. ADO supports key features for building client-server and Web-based applications.

ADP

Aruba Discovery Protocol. ADP is an Aruba proprietary Layer 2 protocol. It is used by the APs to obtain the IP address of the TFTP server from which it downloads the AP boot image.

AES

Advanced Encryption Standard. AES is an encryption standard used for encrypting and protecting electronic data. The AES encrypts and decrypts data in blocks of 128 bits (16 bytes), and can use keys of 128 bits, 192 bits, and 256 bits.

AIFSN

Arbitrary Inter-frame Space Number. AIFSN is set by the AP in beacon frames and probe responses. AIFS is a method of prioritizing a particular category of traffic over the other, for example prioritizing voice or video messages over email.

AirGroup

The application that allows the end users to register their personal mobile devices on a local network and define a group of friends or associates who are allowed to share them. AirGroup is primarily designed for colleges and other institutions. AirGroup uses zero configuration networking to allow Apple mobile devices, such as the AirPrint wireless printer service and the AirPlay mirroring service, to communicate over a complex access network topology.

AirWave Management Client

AirWave Management Client is a Windows software utility that enables client devices (such as a laptop) to act as passive RF sensors and augments the AirWave RAPIDS module.

ALE

Analytics and Location Engine. ALE gives visibility into everything the wireless network knows. This enables customers and partners to gain a wealth of information about the people on their premises.

This can be very important for many different verticals and use cases. ALE includes a location engine that calculates associated and unassociated device location periodically using context streams, including RSSI readings, from WLAN controllers or Instant clusters.

ALG

Application Layer Gateway. ALG is a security component that manages application layer protocols such as SIP, FTP and so on.

AM

Air Monitor. AM is a mode of operation supported on wireless APs. When an AP operates in the Air Monitor mode, it enhances the wireless networks by collecting statistics, monitoring traffic, detecting intrusions, enforcing security policies, balancing wireless traffic load, self-healing coverage gaps, and more. However, clients cannot connect to APs operating in the AM mode.

AMON

Advanced Monitoring. AMON is used in Aruba WLAN deployments for improved network management, monitoring and diagnostic capabilities.

AMP

AirWave Management Platform. AMP is a network management system for configuring, monitoring, and upgrading wired and wireless devices on your network.

ANQP

Access Network Query Protocol. ANQP is a query and a response protocol for Wi-Fi hotspot services. ANQP includes information Elements (IEs) that can be sent from the AP to the client to identify the AP network and service provider. The IEs typically include information about the domain name of the AP operator, the IP addresses available at the AP, and information about potential roaming partners accessible through the AP. If the client responds with a request for a specific IE, the AP will send a Generic Advertisement Service (GAS) response frame with the configured ANQP IE information.

ANSI

American National Standards Institute. It refers to the ANSI compliance standards for products, systems, services, and processes.

API

Application Programming Interface. Refers to a set of functions, procedures, protocols, and tools that enable users to build application software.

app

Short form for application. It generally refers to the application that is downloaded and used on mobile devices.

ARM

Adaptive Radio Management. ARM dynamically monitors and adjusts the network to ensure that all users are allowed ready access. It enables full utilization of the available spectrum to support maximum number of users by intelligently choosing the best RF channel and transmit power for APs in their current RF environment.

ARP

Address Resolution Protocol. ARP is used for mapping IP network address to the hardware MAC address of a device.

Aruba Activate

Aruba Activate is a cloud-based service that helps provision your Aruba devices and maintain your inventory. Activate automates the provisioning process, allowing a single IT technician to easily and rapidly deploy devices throughout a distributed enterprise network.

ASCII

American Standard Code for Information Interchange. An ASCII code is a numerical representation of a character or an action.

B-RAS

Broadband Remote Access Server. A B-RAS is a server that facilitates and converges traffic from multiple Internet traffic resources such as cable, DSL, Ethernet, or Broadband wireless.

band

Band refers to a specified range of frequencies of electromagnetic radiation.

BGP

Border Gateway Protocol. BGP is a routing protocol for exchanging data and information between different host gateways or autonomous systems on the Internet.

BLE

Bluetooth Low Energy. The BLE functionality is offered by Bluetooth® to enable devices to run for long durations with low power consumption.

BMC

Beacon Management Console. BMC manages and monitors beacons from the BLE devices. The BLE devices are used for location tracking and proximity detection.

BPDU

Bridge Protocol Data Unit. A BPDU is a data message transmitted across a local area network to detect loops in network topologies.

BRE

Basic Regular Expression. The BRE syntax standards designed by the IEEE provides extension to the traditional Simple Regular Expressions syntax and allows consistency between utility programs such as grep, sed, and awk.

BSS

Basic Service Set. A BSS is a set of interconnected stations that can communicate with each other. BSS can be an independent BSS or infrastructure BSS. An independent BSS is an ad hoc network that does not include APs, whereas the infrastructure BSS consists of an AP and all its associated clients.

BSSID

Basic Service Set Identifier. The BSSID identifies a particular BSS within an area. In infrastructure BSS networks, the BSSID is the MAC address of the AP. In independent BSS or ad hoc networks, the BSSID

is generated randomly.

BYOD

Bring Your Own Device. BYOD refers to the use of personal mobile devices within an enterprise network infrastructure.

CA

Certificate Authority or Certification Authority. Entity in a public key infrastructure system that issues certificates to clients. A certificate signing request received by the CA is converted into a certificate when the CA adds a signature generated with a private key. See digital certificate.

CAC

Call Admission Control. CAC regulates traffic volume in voice communications. CAC can also be used to ensure or maintain a certain level of audio quality in voice communications networks.

CALEA

Communications Assistance for Law Enforcement Act. To comply with the CALEA specifications and to allow lawful interception of Internet traffic by the law enforcement and intelligence agencies, the telecommunications carriers and manufacturers of telecommunications equipment are required to modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities.

Campus AP

Campus APs are used in private networks where APs connect over private links (LAN, WLAN, WAN or MPLS) and terminate directly on controllers. Campus APs are deployed as part of the indoor campus solution in enterprise office buildings, warehouses, hospitals, universities, and so on.

captive portal

A captive portal is a web page that allows the users to authenticate and sign in before connecting to a public-access network. Captive portals are typically used by business centers, airports, hotel lobbies, coffee shops, and other venues that offer free Wi-Fi hotspots for the guest users.

CCA

Clear Channel Assessment. In wireless networks, the CCA method detects if a channel is occupied or clear, and determines if the channel is available for data transmission.

CDP

Cisco Discovery Protocol. CDP is a proprietary Data Link Layer protocol developed by Cisco Systems. CDP runs on Cisco devices and enables networking applications to learn about the neighboring devices directly connected to the network.

CDR

Call Detail Record. A CDR contains the details of a telephone or VoIP call, such as the origin and destination addresses of the call, the start time and end time of the call, any toll charges that were added through the network or charges for operator services, and so on.

CEF

Common Event Format. The CEF is a standard for the interoperability of event or log-generating devices and applications. The standard syntax for CEF includes a prefix and a variable extension

formatted as key-value pairs.

CGI

Common Gateway Interface. CGI is a standard protocol for exchanging data between the web servers and executable programs running on a server to dynamically process web pages.

CHAP

Challenge Handshake Authentication Protocol. CHAP is an authentication scheme used by PPP servers to validate the identity of remote clients.

CIDR

Classless Inter-Domain Routing. CIDR is an IP standard for creating and allocating unique identifiers for networks and devices. The CIDR IP addressing scheme is used as a replacement for the older IP addressing scheme based on classes A, B, and C. With CIDR, a single IP address can be used to designate many unique IP addresses. A CIDR IP address ends with a slash followed by the IP network prefix, for example, 192.0.2.0/24.

ClearPass

ClearPass is an access management system for creating and enforcing policies across a network to all devices and applications. The ClearPass integrated platform includes applications such as Policy Manager, Guest, Onboard, OnGuard, Insight, Profile, QuickConnect, and so on.

ClearPass Guest

ClearPass Guest is a configurable ClearPass application for secure visitor network access management.

ClearPass Policy Manager

ClearPass Policy Manager is a baseline platform for policy management, AAA, profiling, network access control, and reporting. With ClearPass Policy Manager, the network administrators can configure and manage secure network access that accommodates requirements across multiple locations and multivendor networks, regardless of device ownership and connection method.

CLI

Command-Line Interface. A console interface with a command line shell that allows users to execute text input as commands and convert these commands to appropriate functions.

CN

Common Name. CN is the primary name used to identify a certificate.

CNA

Captive Network Assistant. CNA is a popup page shown when joining a network that has a captive portal.

CoA

Change of Authorization. The RADIUS CoA is used in the AAA service framework to allow dynamic modification of the authenticated, authorized, and active subscriber sessions.

CoS

Class of Service. CoS is used in data and voice protocols for classifying packets into different types of traffic (voice, video, or data) and setting a service priority. For example, voice traffic can be assigned a higher priority over email or HTTP traffic.

CPE

Customer Premises Equipment. It refers to any terminal or equipment located at the customer premises.

CPsec

Control Plane Security. CPsec is a secure form of communication between a controller and APs to protect the control plane communications. This is performed by means of using public-key self-signed certificates created by each master controller.

CPU

Central Processing Unit. A CPU is an electronic circuitry in a computer for processing instructions.

CRC

Cyclic Redundancy Check. CRC is a data verification method for detecting errors in digital data during transmission, storage, or retrieval.

CRL

Certificate Revocation List. CRL is a list of revoked certificates maintained by a certification authority.

cryptobinding

Short for cryptographic binding. A procedure in a tunneled EAP method that binds together the tunnel protocol and the tunneled authentication methods, ensuring the relationship between a collection of data assets. Cryptographic binding focuses on protecting the server; mutual cryptographic binding protects both peer and server.

CSA

Channel Switch Announcement. The CSA element enables an AP to advertise that it is switching to a new channel before it begins transmitting on that channel. This allows the clients, which support CSA, to transition to the new channel with minimal downtime.

CSMA/CA

Carrier Sense Multiple Access / Collision Avoidance. CSMA/CA is a protocol for carrier transmission in networks using the 802.11 standard. CSMA/CA aims to prevent collisions by listening to the broadcasting nodes, and informing devices not to transmit any data until the broadcasting channel is free.

CSR

Certificate Signing Request. In PKI systems, a CSR is a message sent from an applicant to a CA to apply for a digital identity certificate.

CSV

Comma-Separated Values. A file format that stores tabular data in the plain text format separated by commas.

CTS

Clear to Send. The CTS refers to the data transmission and protection mechanism used by the 802.11 wireless networking protocol to prevent frame collision occurrences. See RTS.

CW

Contention Window. In QoS, CW refers to a window set for access categories based on the type of traffic. Based on the type and volume of the traffic, the minimum and maximum values can be calculated to provide a wider window when necessary.

DAI

Dynamic ARP inspection. A security feature that validates ARP packets in a network.

DAS

Distributed Antenna System. DAS is a network of antenna nodes strategically placed around a geographical area or structure for additional cellular coverage.

dB

Decibel. Unit of measure for sound or noise and is the difference or ratio between two signal levels.

dBm

Decibel-Milliwatts. dBm is a logarithmic measurement (integer) that is typically used in place of mW to represent receive-power level. AMP normalizes all signals to dBm, so that it is easy to evaluate performance between various vendors.

DCB

Data Center Bridging. DCB is a collection of standards developed by IEEE for creating a converged data center network using Ethernet.

DCE

Data Communication Equipment. DCE refers to the devices that establish, maintain, and terminate communication network sessions between a data source and its destination.

DCF

Distributed Coordination Function. DCF is a protocol that uses carrier sensing along with a four-way handshake to maximize the throughput while preventing packet collisions.

DDMO

Distributed Dynamic Multicast Optimization. DDMO is similar to Dynamic Multicast Optimization (DMO) where the multicast streams are converted into unicast streams on the AP instead of the controller, to enhance the quality and reliability of streaming videos, while preserving the bandwidth available to non-video clients.

DES

Data Encryption Standard. DES is a common standard for data encryption and a form of secret key cryptography, which uses only one key for encryption and decryption.

designated router

Designated router refers to a router interface that is elected to originate network link advertisements for networks using the OSPF protocol.

destination NAT

Destination Network Address Translation. Destination NAT is a process of translating the destination IP address of an end route packet in a network. Destination NAT is used for redirecting the traffic destined to a virtual host to the real host, where the virtual host is identified by the destination IP address and the real host is identified by the translated IP address.

DFS

Dynamic Frequency Selection. DFS is a mandate for radio systems operating in the 5 GHz band to be equipped with means to identify and avoid interference with Radar systems.

DFT

Discrete Fourier Transform. DFT converts discrete-time data sets into a discrete-frequency representation. See FFT.

DHCP

Dynamic Host Configuration Protocol. A network protocol that enables a server to automatically assign an IP address to an IP-enabled device from a defined range of numbers configured for a given network.

DHCP snooping

DHCP snooping enables the switch to monitor and control DHCP messages received from untrusted devices that are connected to the switch.

digital certificate

A digital certificate is an electronic document that uses a digital signature to bind a public key with an identity—information such as the name of a person or an organization, address, and so forth.

Digital wireless pulse

A wireless technology for transmitting large amounts of digital data over a wide spectrum of frequency bands with very low power for a short distance. Ultra Wideband radio can carry a huge amount of data over a distance up to 230 ft at very low power (less than 0.5 mW), and has the ability to carry signals through doors and other obstacles that tend to reflect signals at more limited bandwidths and a higher power.

Disconnect-Ack

Disconnect-Ack is a NAS response packet to a Disconnect-Request, which indicates that the session was disconnected.

Disconnect-Nak

Disconnect-Nak is NAS response packet to a Disconnect-Request, which indicates that the session was not disconnected.

Disconnect-Request

Disconnect-Request is a RADIUS packet type sent to a NAS requesting that a user or session be disconnected.

distribution certificate

Distribution certificate is used for digitally signing iOS mobile apps to enable enterprise app distribution. It verifies the identity of the app publisher.

DLNA

Digital Living Network Alliance. DLNA is a set of interoperability guidelines for sharing digital media among multimedia devices.

DMO

Dynamic Multicast Optimization. DMO is a process of converting multicast streams into unicast streams over a wireless link to enhance the quality and reliability of streaming videos, while preserving the bandwidth available to non-video clients.

DN

Distinguished Name. A series of fields in a digital certificate that, taken together, constitute the unique identity of the person or device that owns the digital certificate. Common fields in a DN include country, state, locality, organization, organizational unit, and the “common name”, which is the primary name used to identify the certificate.

DNS

Domain Name System. A DNS server functions as a phone book for the intranet and Internet users. It converts human-readable computer host names into IP addresses and IP addresses into host names. It stores several records for a domain name such as an address 'A' record, name server (NS), and mail exchanger (MX) records. The Address 'A' record is the most important record that is stored in a DNS server, because it provides the required IP address for a network peripheral or element.

DOCSIS

Data over Cable Service Interface Specification. A telecommunication standard for Internet access through cable modem.

DoS

Denial of Service. DoS is any type of attack where the attackers send excessive messages to flood traffic and thereby preventing the legitimate users from accessing the service.

DPD

Dead Peer Detection. A method used by the network devices to detect the availability of the peer devices.

DPI

Deep Packet Inspection. DPI is an advanced method of network packet filtering that is used for inspecting data packets exchanged between the devices and systems over a network. DPI functions at the Application layer of the Open Systems Interconnection (OSI) reference model and enables users to identify, categorize, track, reroute, or stop packets passing through a network.

DRT

Downloadable Regulatory Table. The DRT feature allows new regulatory approvals to be distributed for APs without a software upgrade or patch.

DS

Differentiated Services. The DS specification aims to provide uninterrupted quality of service by managing and controlling the network traffic, so that certain types of traffic get precedence.

DSCP

Differentiated Services Code Point. DSCP is a 6-bit packet header value used for traffic classification and priority assignment.

DSL

Digital Subscriber Line. The DSL technology allows the transmission of digital data over telephone lines. A DSL modem is a device used for connecting a computer or router to a telephone line that offers connectivity to the Internet.

DSSS

Direct-Sequence Spread Spectrum. DSSS is a modulation technique used for reducing overall signal interference. This technique multiplies the original data signal with a pseudo random noise spreading code. Spreading of this signal makes the resulting wideband channel more noisy, thereby increasing the resistance to interference. See FHSS.

DST

Daylight Saving Time. DST is also known as summer time that refers to the practice of advancing clocks, so that evenings have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.

DTE

Data Terminal Equipment. DTE refers to a device that converts user information into signals or re-converts the received signals.

DTIM

Delivery Traffic Indication Message. DTIM is a kind of traffic indication map. A DTIM interval determines when the APs must deliver broadcast and multicast frames to their associated clients in power save mode.

DTLS

Datagram Transport Layer Security. DTLS communications protocol provides communications security for datagram protocols.

dynamic authorization

Dynamic authorization refers to the ability to make changes to a visitor account's session while it is in progress. This might include disconnecting a session or updating some aspect of the authorization for the session.

dynamic NAT

Dynamic Network Address Translation. Dynamic NAT maps multiple public IP addresses and uses these addresses with an internal or private IP address. Dynamic NAT helps to secure a network by masking the internal configuration of a private network.

EAP

Extensible Authentication Protocol. An authentication protocol for wireless networks that extends the methods used by the PPP, a protocol often used when connecting a computer to the Internet. EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and public key encryption authentication.

EAP-FAST

EAP – Flexible Authentication Secure Tunnel (tunneled).

EAP-GTC

EAP – Generic Token Card. (non-tunneled).

EAP-MD5

EAP – Method Digest 5. (non-tunneled).

EAP-MSCHAP

EAP Microsoft Challenge Handshake Authentication Protocol.

EAP-MSCHAPv2

EAP Microsoft Challenge Handshake Authentication Protocol Version 2.

EAP-PEAP

EAP–Protected EAP. A widely used protocol for securely transporting authentication data across a network (tunneled).

EAP-PWD

EAP-Password. EAP-PWD is an EAP method that uses a shared password for authentication.

EAP-TLS

EAP–Transport Layer Security. EAP-TLS is a certificate-based authentication method supporting mutual authentication, integrity-protected ciphersuite negotiation and key exchange between two endpoints. See RFC 5216.

EAP-TTLS

EAP–Tunneled Transport Layer Security. EAP-TTLS is an EAP method that encapsulates a TLS session, consisting of a handshake phase and a data phase. See RFC 5281.

EAPoL

Extensible Authentication Protocol over LAN. A network port authentication protocol used in IEEE 802.1X standards to provide a generic network sign-on to access network resources.

ECC

Elliptical Curve Cryptography or Error correcting Code memory. Elliptical Curve Cryptography is a public-key encryption technique that is based on elliptic curve theory used for creating faster, smaller, and more efficient cryptographic keys. Error Correcting Code memory is a type of computer data storage that can detect and correct the most common kinds of internal data corruption. ECC memory is used in most computers where data corruption cannot be tolerated under any circumstances, such as for scientific or financial computing.

ECDSA

Elliptic Curve Digital Signature Algorithm. ECDSA is a cryptographic algorithm that supports the use of public or private key pairs for encrypting and decrypting information.

EDCA

Enhanced Distributed Channel Access. The EDCA function in the IEEE 802.11e Quality of Service standard supports differentiated and distributed access to wireless medium based on traffic priority and Access Category types. See WMM and WME.

EIGRP

Enhanced Interior Gateway Routing Protocol. EIGRP is a routing protocol used for automating routing decisions and configuration in a network.

EIRP

Effective Isotropic Radiated Power or Equivalent Isotropic Radiated Power. EIRP refers to the output power generated when a signal is concentrated into a smaller area by the Antenna.

ESI

External Services Interface. ESI provides an open interface for integrating security solutions that solve interior network problems such as viruses, worms, spyware, and corporate compliance.

ESS

Extended Service Set. An ESS is a set of one or more interconnected BSSs that form a single sub network.

ESSID

Extended Service Set Identifier. ESSID refers to the ID used for identifying an extended service set.

Ethernet

Ethernet is a network protocol for data transmission over LAN.

EULA

End User License Agreement. EULA is a legal contract between a software application publisher or author and the users of the application.

FCC

Federal Communications Commission. FCC is a regulatory body that defines standards for the interstate and international communications by radio, television, wire, satellite, and cable.

FFT

Fast Fourier Transform. FFT is a frequency analysis mechanism that aims at faster conversion of a discrete signal in time domain into a discrete frequency domain representation. See also DFT.

FHSS

Frequency Hopping Spread Spectrum. FHSS is transmission technique that allows modulation and transmission of a data signal by rapidly switching a carrier among many frequency channels in a random but predictable sequence. See also DSSS.

FIB

Forwarding Information Base. FIB is a forwarding table that maps MAC addresses to ports. FIB is used in network bridging, routing, and similar functions to identify the appropriate interface for forwarding packets.

FIPS

Federal Information Processing Standards. FIPS refers to a set of standards that describe document processing, encryption algorithms, and other information technology standards for use within non-military government agencies, and by government contractors and vendors who work with these agencies.

firewall

Firewall is a network security system used for preventing unauthorized access to or from a private network.

FQDN

Fully Qualified Domain Name. FQDN is a complete domain name that identifies a computer or host on the Internet.

FQLN

Fully Qualified Location Name. FQLN is a device location identifier in the format: APname.Floor.Building.Campus.

frequency allocation

Use of radio frequency spectrum as regulated by governments.

FSPL

Free Space Path Loss. FSPL refers to the loss in signal strength of an electromagnetic wave that would result from a line-of-sight path through free space (usually air), with no obstacles nearby to cause reflection or diffraction.

FTP

File Transfer Protocol. A standard network protocol used for transferring files between a client and server on a computer network.

GARP

Generic Attribute Registration Protocol. GVRP is a LAN protocol that allows the network nodes to register and de-register attributes, such as network addresses, with each other.

GAS

Generic Advertisement Service. GAS is a request-response protocol, which provides Layer 2 transport mechanism between a wireless client and a server in the network prior to authentication. It helps in determining a wireless network infrastructure before associating clients, and allows clients to send queries to multiple 802.11 networks in parallel.

gateway

Gateway is a network node that allows traffic to flow in and out of the network.

Gbps

Gigabits per second.

GBps

Gigabytes per second.

GET

GET refers HTTP request method or an SNMP operation method. The GET HTTP request method submits data to be processed to a specified resource. The GET SNMP operation method obtains information from the Management Information Base (MIB).

GHz

Gigahertz.

GMT

Greenwich Mean Time. GMT refers to the mean solar time at the Royal Observatory in Greenwich, London. GMT is the same as Coordinated Universal Time (UTC) standard, written as an offset of UTC +/- 00:00.

goodput

Goodput is the application level throughput that refers to the ratio of the total bytes transmitted or received in the network to the total air time required for transmitting or receiving the bytes.

GPS

Global Positioning System. A satellite-based global navigation system.

GRE

Generic Routing Encapsulation. GRE is an IP encapsulation protocol that is used to transport packets over a network.

GTC

Generic Token Card. GTC is a protocol that can be used as an alternative to MSCHAPv2 protocol. GTC allows authentication to various authentication databases even in cases where MSCHAPv2 is not supported by the database.

GVRP

GARP VLAN Registration Protocol or Generic VLAN Registration Protocol. GARP is an IEEE 802.1Q-compliant protocol that facilitates VLAN registration and controls VLANs within a larger network.

H2QP

Hotspot 2.0 Query Protocol.

hot zone

Wireless access area created by multiple hotspots that are located in close proximity to one another. Hot zones usually combine public safety APs with public hotspots.

hotspot

Hotspot refers to a WLAN node that provides Internet connection and virtual private network (VPN) access from a given location. A business traveler, for example, with a laptop equipped for Wi-Fi can look up a local hotspot, contact it, and get connected through its network to reach the Internet.

HSPA

High-Speed Packet Access.

HT

High Throughput. IEEE 802.11n is an HT WLAN standard that aims to achieve physical data rates of close to 600 Mbps on the 2.4 GHz and 5 GHz bands.

HTTP

Hypertext Transfer Protocol. The HTTP is an application protocol to transfer data over the web. The HTTP protocol defines how messages are formatted and transmitted, and the actions that the w servers and browsers should take in response to various commands.

HTTPS

Hypertext Transfer Protocol Secure. HTTPS is a variant of the HTTP that adds a layer of security on the data in transit through a secure socket layer or transport layer security protocol connection.

IAS

Internet Authentication Service. IAS is a component of Windows Server operating systems that provides centralized user authentication, authorization, and accounting.

ICMP

Internet Control Message Protocol. ICMP is an error reporting protocol. It is used by network devices such as routers, to send error messages and operational information to the source IP address when network problems prevent delivery of IP packets.

IDS

Intrusion Detection System. IDS monitors a network or systems for malicious activity or policy violations and reports its findings to the management system deployed in the network.

IEEE

Institute of Electrical and Electronics Engineers.

IGMP

Internet Group Management Protocol. Communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships.

IGMP snooping

IGMP snooping prevents multicast flooding on Layer 2 network by treating multicast traffic as broadcast traffic. Without IGMP snooping, all streams could be flooded to all ports on that VLAN. When multicast flooding occurs, end-hosts that happen to be in the same VLAN would receive all the streams only to be discarded without snooping.

IGP

Interior Gateway Protocol. IGP is used for exchanging routing information between gateways within an autonomous system (for example, a system of corporate local area networks).

IGRP

Interior Gateway Routing Protocol. IGRP is a distance vector interior routing protocol used by routers to exchange routing data within an autonomous system.

IKE

Internet Key Exchange. IKE is a key management protocol used with IPsec protocol to establish a secure communication channel. IKE provides additional feature, flexibility, and ease of configuration for IPsec standard.

IKEv1

Internet Key Exchange version 1. IKEv1 establishes a secure authenticated communication channel by using either the pre-shared key (shared secret), digital signatures, or public key encryption. IKEv1 operates in Main and Aggressive modes. See RFC 2409.

IKEv2

Internet Key Exchange version 2. IKEv2 uses the secure channel established in Phase 1 to negotiate Security Associations on behalf of services such as IPsec. IKEv2 uses pre-shared key and Digital Signature for authentication. See RFC 4306.

IoT

Internet of Things. IoT refers to the internetworking of devices that are embedded with electronics, software, sensors, and network connectivity features allowing data exchange over the Internet.

IPM

Intelligent Power Monitoring. IPM is a feature supported on certain APs that actively measures the power utilization of an AP and dynamically adapts to the power resources.

IPS

Intrusion Prevention System. The IPS monitors a network for malicious activities such as security threats or policy violations. The main function of an IPS is to identify suspicious activity, log the information, attempt to block the activity, and report it.

IPsec

Internet Protocol security. IPsec is a protocol suite for secure IP communications that authenticates and encrypts each IP packet in a communication session.

IPSG

Internet Protocol Source Guard. IPSG restricts IP address from untrusted interface by filtering traffic based on list of addresses in the DHCP binding database or manually configured IP source bindings. It prevents IP spoofing attacks.

IrDA

An industry-sponsored organization set up in 1993 to create international standards for the hardware and software used in infrared communication links. In this special form of radio transmission, a focused ray of light in the infrared frequency spectrum, measured in terahertz (THz), or trillions of hertz (cycles per second), is modulated with information and sent from a transmitter to a receiver over a relatively short distance.

ISAKMP

Internet Security Association and Key Management Protocol. ISAKMP is used for establishing Security Associations and cryptographic keys in an Internet environment.

ISP

Internet Service Provider. An ISP is an organization that provides services for accessing and using the Internet.

JSON

JavaScript Object Notation. JSON is an open-standard, language-independent, lightweight data-interchange format used to transmit data objects consisting of attribute–value pairs. JSON uses a "self-describing" text format that is easy for humans to read and write, and that can be used as a data format by any programming language.

Kbps

Kilobits per second.

KBps

Kilobytes per second.

keepalive

Signal sent at periodic intervals from one device to another to verify that the link between the two devices is working. If no reply is received, data will be sent by a different path until the link is restored. A keepalive can also be used to indicate that the connection should be preserved so that the receiving device does not consider it timed out and drop it.

L2TP

Layer-2 Tunneling Protocol. L2TP is a networking protocol used by the ISPs to enable VPN operations.

LACP

Link Aggregation Control Protocol. LACP is used for the collective handling of multiple physical ports that can be seen as a single channel for network traffic purposes.

LAG

Link Aggregation Group . A LAG combines a number of physical ports together to make a single high-bandwidth data path. LAGs can connect two switches to provide a higher-bandwidth connection to a public network.

LAN

Local Area Network. A LAN is a network of connected devices within a distinct geographic area such as an office or a commercial establishment and share a common communications line or wireless link to a server.

LCD

Liquid Crystal Display. LCD is the technology used for displays in notebook and other smaller computers. Like LED and gas-plasma technologies, LCDs allow displays to be much thinner than the cathode ray tube technology.

LDAP

Lightweight Directory Access Protocol. LDAP is a communication protocol that provides the ability to access and maintain distributed directory information services over a network.

LDPC

Low-Density Parity-Check. LDPC is a method of transmitting a message over a noisy transmission channel using a linear error correcting code. An LDPC is constructed using a sparse bipartite graph.

LEAP

Lightweight Extensible Authentication Protocol. LEAP is a Cisco proprietary version of EAP used in wireless networks and Point-to-Point connections.

LED

Light Emitting Diode. LED is a semiconductor light source that emits light when an electric current passes through it.

LEEF

Log Event Extended Format. LEEF is a type of customizable syslog event format. An extended log file contains a sequence of lines containing ASCII characters terminated by either the sequence LF or CRLF.

LI

Lawful Interception. LI refers to the procedure of obtaining communications network data by the Law Enforcement Agencies for the purpose of analysis or evidence.

LLDP

Link Layer Discovery Protocol. LLDP is a vendor-neutral link layer protocol in the Internet Protocol suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, which is principally a wired Ethernet.

LLDP-MED

LLDP–Media Endpoint Discovery. LLDP-MED facilitates information sharing between endpoints and network infrastructure devices.

LMS

Local Management Switch. In multi-controller networks, each controller acts as an LMS and terminates user traffic from the APs, processes, and forwards the traffic to the wired network.

LNS

L2TP Network Server. LNS is an equipment that connects to a carrier and handles the sessions from broadband lines. It is also used for dial-up and mobile links. LNS handles authentication and routing of the IP addresses. It also handles the negotiation of the link with the equipment and establishes a session.

LTE

Long Term Evolution. LTE is a 4G wireless communication standard that provides high-speed wireless communication for mobile phones and data terminals. See 4G.

MAB

MAC Authentication Bypass. Endpoints such as network printers, Ethernet-based sensors, cameras, and wireless phones do not support 802.1X authentication. For such endpoints, MAC Authentication Bypass mechanism is used. In this method, the MAC address of the endpoint is used to authenticate the endpoint.

MAC

Media Access Control. A MAC address is a unique identifier assigned to network interfaces for communications on a network.

MAM

Mobile Application Management. MAM refers to software and services used to secure, manage, and distribute mobile applications used in enterprise settings on mobile devices like smartphones and tablet computers. Mobile Application Management can apply to company-owned mobile devices as well as BYOD.

Mbps

Megabits per second

MBps

Megabytes per second

MCS

Modulation and Coding Scheme. MCS is used as a parameter to determine the data rate of a wireless connection for high throughput.

MD4

Message Digest 4. MD4 is an earlier version of MD5 and is an algorithm used to verify data integrity through the creation of a 128-bit message digest from data input.

MD5

Message Digest 5. The MD5 algorithm is a widely used hash function producing a 128-bit hash value from the data input.

MDAC

Microsoft Data Access Components. MDAC is a framework of interrelated Microsoft technologies that provides a standard database for Windows OS.

MDM

Mobile Device Management. MDM is an administrative software to manage, monitor, and secure mobile devices of the employees in a network.

mDNS

Multicast Domain Name System. mDNS provides the ability to perform DNS-like operations on the local link in the absence of any conventional unicast DNS server. The mDNS protocol uses IP multicast User Datagram Protocol (UDP) packets, and is implemented by the Apple Bonjour and Linux NSS-mDNS services. mDNS works in conjunction with DNS Service Discovery (DNS-SD), a companion zero-configuration technique specified. See RFC 6763.

MFA

Multi-factor Authentication. MFA lets you require multiple factors, or proofs of identity, when authenticating a user. Policy configurations define how often multi-factor authentication will be required, or conditions that will trigger it.

MHz

Megahertz

MIB

Management Information Base. A hierarchical database used by SNMP to manage the devices being monitored.

microwave

Electromagnetic energy with a frequency higher than 1 GHz, corresponding to wavelength shorter than 30 centimeters.

MIMO

Multiple Input Multiple Output. An antenna technology for wireless communications in which multiple antennas are used at both source (transmitter) and destination (receiver). The antennas at each end of the communications circuit are combined to minimize errors and optimize data speed.

MISO

Multiple Input Single Output. An antenna technology for wireless communications in which multiple antennas are used at the source (transmitter). The antennas are combined to minimize errors and optimize data speed. The destination (receiver) has only one antenna.

MLD

Multicast Listener Discovery. A component of the IPv6 suite. It is used by IPv6 routers for discovering multicast listeners on a directly attached link.

MPDU

MAC Protocol Data Unit. MPDU is a message exchanged between MAC entities in a communication system based on the layered OSI model.

MPLS

Multiprotocol Label Switching. The MPLS protocol speeds up and shapes network traffic flows.

MPPE

Microsoft Point-to-Point Encryption. A method of encrypting data transferred across PPP-based dial-up connections or PPTP-based VPN connections.

MS-CHAP

Microsoft Challenge Handshake Authentication Protocol. MS-CHAP is Password-based, challenge-response, mutual authentication protocol that uses MD4 and DES encryption.

MS-CHAPv1

Microsoft Challenge Handshake Authentication Protocol version 1. MS-CHAPv1 extends the user authentication functionality provided on Windows networks to remote workstations. MS-CHAPv1 supports only one-way authentication.

MS-CHAPv2

Microsoft Challenge Handshake Authentication Protocol version 2. MS-CHAPv2 is an enhanced version of the MS-CHAP protocol that supports mutual authentication.

MSS

Maximum Segment Size. MSS is a parameter of the options field in the TCP header that specifies the largest amount of data, specified in bytes, that a computer or communications device can receive in a single TCP segment.

MSSID

Mesh Service Set Identifier. MSSID is the SSID used by the client to access a wireless mesh network.

MSTP

Multiple Spanning Tree Protocol. MSTP configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each spanning tree.

MTU

Maximum Transmission Unit. MTU is the largest size packet or frame specified in octets (eight-bit bytes) that can be sent in networks such as the Internet.

MU-MIMO

Multi-User Multiple-Input Multiple-Output. MU-MIMO is a set of multiple-input and multiple-output technologies for wireless communication, in which users or wireless terminals with one or more antennas communicate with each other.

MVRP

Multiple VLAN Registration Protocol. MVRP is a Layer 2 network protocol used for automatic configuration of VLAN information on switches.

mW

milliWatts. mW is 1/1000 of a Watt. It is a linear measurement (always positive) that is generally used to represent transmission.

NAC

Network Access Control. NAC is a computer networking solution that uses a set of protocols to define and implement a policy that describes how devices can secure access to network nodes when they initially attempt to connect to a network.

NAD

Network Access Device. NAD is a device that automatically connects the user to the preferred network, for example, an AP or an Ethernet switch.

NAK

Negative Acknowledgement. NAK is a response indicating that a transmitted message was received with errors or it was corrupted, or that the receiving end is not ready to accept transmissions.

NAP

Network Access Protection. The NAP feature in the Windows Server allows network administrators to define specific levels of network access based on identity, groups, and policy compliance. The NAP Agent is a service that collects and manages health information for NAP client computers. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of network access.

NAS

Network Access Server. NAS provides network access to users, such as a wireless AP, network switch, or dial-in terminal server.

NAT

Network Address Translation. NAT is a method of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.

NetBIOS

Network Basic Input/Output System. A program that lets applications on different computers communicate within a LAN.

netmask

Netmask is a 32-bit mask used for segregating IP address into subnets. Netmask defines the class and range of IP addresses.

NFC

Near-Field Communication. NFC is a short-range wireless connectivity standard (ECMA-340, ISO/IEC 18092) that uses magnetic field induction to enable communication between devices when they touch or are brought closer (within a few centimeters of distance). The standard specifies a way for the devices to establish a peer-to-peer (P2P) network to exchange data.

NIC

Network Interface Card. NIC is a hardware component that allows a device to connect to the network.

Nmap

Network Mapper. Nmap is an open-source utility for network discovery and security auditing. Nmap uses IP packets to determine such things as the hosts available on a network and their services, operating systems and versions, types of packet filters/firewalls, and so on.

NMI

Non-Maskable Interrupt. NMI is a hardware interrupt that standard interrupt-masking techniques in the system cannot ignore. It typically occurs to signal attention for non-recoverable hardware errors.

NMS

Network Management System. NMS is a set of hardware and/or software tools that allow an IT professional to supervise the individual components of a network within a larger network management framework.

NOE

New Office Environment. NOE is a proprietary VoIP protocol designed by Alcatel-Lucent Enterprise.

NTP

Network Time Protocol. NTP is a protocol for synchronizing the clocks of computers over a network.

OAuth

Open Standard for Authorization. OAuth is a token-based authorization standard that allows websites or third-party applications to access user information, without exposing the user credentials.

OCSP

Online Certificate Status Protocol. OCSP is used for determining the current status of a digital certificate without requiring a CRL.

OFDM

Orthogonal Frequency Division Multiplexing. OFDM is a scheme for encoding digital data on multiple carrier frequencies.

OID

Object Identifier. An OID is an identifier used to name an object. The OIDs represent nodes or managed objects in a MIB hierarchy. The OIDs are designated by text strings and integer sequences and are formally defined as per the ASN.1 standard.

OKC

Opportunistic Key Caching. OKC is a technique available for authentication between multiple APs in a network where those APs are under common administrative control. Using OKC, a station roaming to any AP in the network will not have to complete a full authentication exchange, but will instead just perform the 4-way handshake to establish transient encryption keys.

onboarding

The process of preparing a device for use on an enterprise network, by creating the appropriate access credentials and setting up the network connection parameters.

OpenFlow

OpenFlow is an open communications interface between control plane and the forwarding layers of a network.

OpenFlow agent

OpenFlow agent. OpenFlow is a software module in Software-Defined Networking (SDN) that allows the abstraction of any legacy network element, so that it can be integrated and managed by the SDN controller. OpenFlow runs on network devices such as switches, routers, wireless controllers, and APs.

Optical wireless

Optical wireless is combined use of conventional radio frequency wireless and optical fiber for telecommunication. Long-range links are provided by using optical fibers; the links from the long-range endpoints to end users are accomplished by RF wireless or laser systems. RF wireless at Ultra High Frequencies and microwave frequencies can carry broadband signals to individual computers at substantial data speeds.

OSI

Open Systems Interconnection. OSI is a reference model that defines a framework for communication between the applications in a network.

OSPF

Open Shortest Path First. OSPF is a link-state routing protocol for IP networks. It uses a link-state routing algorithm and falls into the group of interior routing protocols that operates within a single Autonomous System (AS).

OSPFv2

Open Shortest Path First version 2. OSPFv2 is the version 2 of the link-state routing protocol, OSPF. See RFC 2328.

OUI

Organizationally Unique Identifier. Synonymous with company ID or vendor ID, an OUI is a 24-bit, globally unique assigned number, referenced by various standards. The first half of a MAC address is OUI.

OVA

Open Virtualization Archive. OVA contains a compressed installable version of a virtual machine.

OVF

Open Virtualization Format. OVF is a specification that describes an open-standard, secure, efficient, portable and extensible format for packaging and distributing software for virtual machines.

PAC

Protected Access Credential. PAC is distributed to clients for optimized network authentication. These credentials are used for establishing an authentication tunnel between the client and the authentication server.

PAP

Password Authentication Protocol. PAP validates users by password. PAP does not encrypt passwords for transmission and is thus considered insecure.

PAPI

Process Application Programming Interface. PAPI controls channels for ARM and Wireless Intrusion Detection System (WIDS) communication to the master controller. A separate PAPI control channel connects to the local controller where the SSID tunnels terminate.

PBR

Policy-based Routing. PBR provides a flexible mechanism for forwarding data packets based on polices configured by a network administrator.

PDU

Power Distribution Unit or Protocol Data Unit. Power Distribution Unit is a device that distributes electric power to the networking equipment located within a data center. Protocol Data Unit contains protocol control Information that is delivered as a unit among peer entities of a network.

PEAP

Protected Extensible Authentication Protocol. PEAP is a type of EAP communication that addresses security issues associated with clear text EAP transmissions by creating a secure channel encrypted and protected by TLS.

PEF

Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PEFNG

Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PEFV

Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PFS

Perfect Forward Secrecy. PFS refers to the condition in which a current session key or long-term private key does not compromise the past or subsequent keys.

PHB

Per-hop behavior. PHB is a term used in DS or MPLS. It defines the policy and priority applied to a packet when traversing a hop (such as a router) in a DiffServ network.

PIM

Protocol-Independent Multicast. PIM refers to a family of multicast routing protocols for IP networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN, or the Internet.

PIN

Personal Identification Number. PIN is a numeric password used to authenticate a user to a system.

PKCS#n

Public-key cryptography standard n. PKCS#n refers to a numbered standard related to topics in cryptography, including private keys (PKCS#1), digital certificates (PKCS#7), certificate signing requests (PKCS#10), and secure storage of keys and certificates (PKCS#12).

PKI

Public Key Infrastructure. PKI is a security technology based on digital certificates and the assurances provided by strong cryptography. See also certificate authority, digital certificate, public key, private key.

PLMN

Public Land Mobile Network. PLMS is a network established and operated by an administration or by a Recognized Operating Agency for the specific purpose of providing land mobile telecommunications services to the public.

PMK

Pairwise Master Key. PMK is a shared secret key that is generated after PSK or 802.1X authentication.

PoE

Power over Ethernet. PoE is a technology for wired Ethernet LANs to carry electric power required for the device in the data cables. The IEEE 802.3af PoE standard provides up to 15.4 W of power on each port.

PoE+

Power over Ethernet+. PoE+ is an IEEE 802.3at standard that provides 25.5W power on each port.

POST

Power On Self Test. An HTTP request method that requests data from a specified resource.

PPP

Point-to-Point Protocol. PPP is a data link (layer 2) protocol used to establish a direct connection between two nodes. It can provide connection authentication, transmission encryption, and compression.

PPPoE

Point-to-Point Protocol over Ethernet. PPPoE is a method of connecting to the Internet, typically used with DSL services, where the client connects to the DSL modem.

PPTP

Point-to-Point Tunneling Protocol. PPTP is a method for implementing virtual private networks. It uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets.

private key

The part of a public-private key pair that is always kept private. The private key encrypts the signature of a message to authenticate the sender. The private key also decrypts a message that was encrypted with the public key of the sender.

PRNG

Pseudo-Random Number Generator. PRNG is an algorithm for generating a sequence of numbers whose properties approximate the properties of sequences of random numbers.

PSK

Pre-shared key. A unique shared secret that was previously shared between two parties by using a secure channel. This is used with WPA security, which requires the owner of a network to provide a passphrase to users for network access.

PSU

Power Supply Unit. PSU is a unit that supplies power to an equipment by converting mains AC to low-voltage regulated DC power.

public key

The part of a public-private key pair that is made public. The public key encrypts a message and the message is decrypted with the private key of the recipient.

PVST

Per-VLAN Spanning Tree. PVST provides load balancing of VLANs across multiple ports resulting in optimal usage of network resources.

PVST+

Per-VLAN Spanning Tree+. PVST+ is an extension of the PVST standard that uses the 802.1Q trunking technology.

QoS

Quality of Service. It refers to the capability of a network to provide better service and performance to a specific network traffic over various technologies.

RA

Router Advertisement. The RA messages are sent by the routers in the network when the hosts send multicast router solicitation to the multicast address of all routers.

Radar

Radio Detection and Ranging. Radar is an object-detection system that uses radio waves to determine the range, angle, or velocity of objects.

RADIUS

Remote Authentication Dial-In User Service. An Industry-standard network access protocol for remote authentication. It allows authentication, authorization, and accounting of remote users who want to access network resources.

RAM

Random Access Memory.

RAPIDS

Rogue Access Point identification and Detection System. An AMP module that is designed to identify and locate wireless threats by making use of all of the information available from your existing infrastructure.

RARP

Reverse Address Resolution Protocol. RARP is a protocol used by a physical machine in a local area network for determining the IP address from the ARP table or cache of the gateway server.

Regex

Regular Expression. Regex refers to a sequence of symbols and characters defining a search pattern.

Registration Authority

Type of Certificate Authority that processes certificate requests. The Registration Authority verifies that requests are valid and comply with certificate policy, and authenticates the user's identity. The Registration Authority then forwards the request to the Certificate Authority to sign and issue the certificate.

Remote AP

Remote APs extend corporate network to the users working from home or at temporary work sites. Remote APs are deplyed at branch office sites and are connected to the central network on a WAN

link.

REST

Representational State Transfer. REST is a simple and stateless architecture that the web services use for providing interoperability between computer systems on the Internet. In a RESTful web service, requests made to the URI of a resource will elicit a response that may be in XML, HTML, JSON or some other defined format.

RF

Radio Frequency. RF refers to the electromagnetic wave frequencies within a range of 3 kHz to 300 GHz, including the frequencies used for communications or Radar signals.

RFC

Request For Comments. RFC is a commonly used format for the Internet standards documentss.

RFID

Radio Frequency Identification. RFID uses radio waves to automatically identify and track the information stored on a tag attached to an object.

RIP

Routing Information Protocol. RIP prevents the routing loops by limiting the number of hops allowed in a path from source to destination.

RJ45

Registered Jack 45. RJ45 is a physical connector for network cables.

RMA

Return Merchandise Authorization. RMA is a part of the product returning process that authorizes users to return a product to the manufacturer or distributor for a refund, replacement, or repair. The customers who want to return a product within its Warranty period contact the manufacturer to initiate the product returning process. The manufacturer or the seller generates an authorization number for the RMA, which is used by the customers, when returning a product to the warehouse.

RMON

Remote Monitoring. RMON provides standard information that a network administrator can use to monitor, analyze, and troubleshoot a group of distributed LANs.

RoW

Rest of World. RoW or RW is an operating country code of a device.

RSA

Rivest, Shamir, Adleman. RSA is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet.

RSSI

Received Signal Strength Indicator. RSSI is a mechanism by which RF energy is measured by the circuitry on a wireless NIC (0-255). The RSSI is not standard across vendors. Each vendor determines its own RSSI scale/values.

RSTP

Rapid Spanning Tree Protocol. RSTP provides significantly faster spanning tree convergence after a topology change, introducing new convergence behaviors and bridge port roles to do this.

RTCP

RTP Control Protocol. RTCP provides out-of-band statistics and control information for an Real-Time Transport Protocol session.

RTLS

Real-Time Location Systems. RTLS automatically identifies and tracks the location of objects or people in real time, usually within a building or other contained area.

RTP

Real-Time Transport Protocol. RTP is a network protocol used for delivering audio and video over IP networks.

RTS

Request to Send. RTS refers to the data transmission and protection mechanism used by the 802.11 wireless networking protocol to prevent frame collision occurrences. See CTS.

RTSP

Real Time Streaming Protocol. RTSP is a network control protocol designed for use in entertainment and communications systems to control streaming media servers.

RVI

Routed VLAN Interface. RVI is a switch interface that forwards packets between VLANs.

RW

Rest of World. RoW or RW is an operating country code of a device.

SA

Security Association. SA is the establishment of shared security attributes between two network entities to support secure communication.

SAML

Security Assertion Markup Language. SAML is an XML-based framework for communicating user authentication, entitlement, and attribute information. SAML enables single sign-on by allowing users to authenticate at an identity provider and then access service providers without additional authentication.

SCEP

Simple Certificate Enrollment Protocol. SCEP is a protocol for requesting and managing digital certificates.

SCP

Secure Copy Protocol. SCP is a network protocol that supports file transfers between hosts on a network.

SCSI

Small Computer System Interface. SCSI refers to a set of interface standards for physical connection and data transfer between a computer and the peripheral devices such as printers, disk drives, CD-ROM, and so on.

SD-WAN

Software-Defined Wide Area Network. SD-WAN is an application for applying SDN technology to WAN connections that connect enterprise networks across disparate geographical locations.

SDN

Software-Defined Networking. SDN is an umbrella term encompassing several kinds of network technology aimed at making the network as agile and flexible as the virtualized server and storage infrastructure of the modern data center.

SDR

Server Derivation Rule. An SDR refers to a role assignment model used by the controllers running ArubaOS to assign roles and VLANs to the WLAN users based on the rules defined under a server group. The SDRs override the default authentication roles and VLANs defined in the AAA and Virtual AP profiles.

SDU

Service Data Unit. SDU is a unit of data that has been passed down from an OSI layer to a lower layer and that has not yet been encapsulated into a PDU by the lower layer.

SFP

The Small Form-factor Pluggable. SFP is a compact, hot-pluggable transceiver that is used for both telecommunication and data communications applications.

SFP+

Small Form-factor Pluggable+. SFP+ supports up to data rates up to 16 Gbps.

SFTP

Secure File Transfer Protocol. SFTP is a network protocol that allows file access, file transfer, and file management functions over a secure connection.

SHA

Secure Hash Algorithm. SHA is a family of cryptographic hash functions. The SHA algorithm includes the SHA, SHA-1, SHA-2 and SHA-3 variants.

SIM

Subscriber Identity Module. SIM is an integrated circuit that is intended to securely store the International Mobile Subscriber Identity (IMSI) number and its related key, which are used for identifying and authenticating subscribers on mobile telephony devices.

SIP

Session Initiation Protocol. SIP is used for signaling and controlling multimedia communication session such as voice and video calls.

SIRT

Security Incident Response Team. SIRT is responsible for reviewing as well as responding to computer security incident reports and activity.

SKU

Stock Keeping Unit. SKU refers to the product and service identification code for the products in the inventory.

SLAAC

Stateless Address Autoconfiguration. SLAAC provides the ability to address a host based on a network prefix that is advertised from a local network router through router advertisements.

SMB

Server Message Block or Small and Medium Business. Server Message Block operates as an application-layer network protocol mainly used for providing shared access to files, printers, serial ports, and for miscellaneous communications between the nodes on a network.

SMS

Short Message Service. SMS refers to short text messages (up to 140 characters) sent and received through mobile phones.

SMTP

Simple Mail Transfer Protocol. SMTP is an Internet standard protocol for electronic mail transmission.

SNIR

Signal-to-Noise-Plus-Interference Ratio. SNIR refers to the power of a central signal of interest divided by the sum of the interference power and the power of the background noise. SINR is defined as the power of a certain signal of interest divided by the sum of the interference power (from all the other interfering signals) and the power of some background noise.

SNMP

Simple Network Management Protocol. SNMP is a TCP/IP standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

SNMPv1

Simple Network Management Protocol version 1. SNMPv1 is a widely used network management protocol.

SNMPv2

Simple Network Management Protocol version 2. SNMPv2 is an enhanced version of SNMPv1, which includes improvements in the areas of performance, security, confidentiality, and manager-to-manager communications.

SNMPv2c

Community-Based Simple Network Management Protocol version 2. SNMPv2C uses the community-based security scheme of SNMPv1 and does not include the SNMPv2 security model.

SNMPv3

Simple Network Management Protocol version 3. SNMPv3 is an enhanced version of SNMP that includes security and remote configuration features.

SNR

Signal-to-Noise Ratio. SNR is used for comparing the level of a desired signal with the level of background noise.

SNTP

Simple Network Time Protocol. SNTP is a less complex implementation of NTP. It uses the same , but does not require the storage of state over extended periods of time.

SOAP

Simple Object Access Protocol. SOAP enables communication between the applications running on different operating systems, with different technologies and programming languages. SOAP is an XML-based messaging protocol for exchanging structured information between the systems that support web services.

SoC

System on a Chip. SoC is an Integrated Circuit that integrates all components of a computer or other electronic system into a single chip.

source NAT

Source NAT changes the source address of the packets passing through the router. Source NAT is typically used when an internal (private) host initiates a session to an external (public) host.

SSH

Secure Shell. SSH is a network protocol that provides secure access to a remote device.

SSID

Service Set Identifier. SSID is a name given to a WLAN and is used by the client to access a WLAN network.

SSL

Secure Sockets Layer. SSL is a computer networking protocol for securing connections between network application clients and servers over the Internet.

SSO

Single Sign-On. SSO is an access-control property that allows the users to log in once to access multiple related, but independent applications or systems to which they have privileges. The process authenticates the user across all allowed resources during their session, eliminating additional login prompts.

STBC

Space-Time Block Coding. STBC is a technique used in wireless communications to transmit multiple copies of a data stream across a number of antennas and to exploit the various received versions of the data to improve the reliability of data transfer.

STM

Station Management. STM is a process that handles AP management and user association.

STP

Spanning Tree Protocol. STP is a network protocol that builds a logical loop-free topology for Ethernet networks.

SU-MIMO

Single-User Multiple-Input Multiple-Output. SU-MIMO allocates the full bandwidth of the AP to a single high-speed device during the allotted time slice.

subnet

Subnet is the logical division of an IP network.

subscription

A business model where a customer pays a certain amount as subscription price to obtain access to a product or service.

SVP

SpectraLink Voice Priority. SVP is an open, straightforward QoS approach that has been adopted by most leading vendors of WLAN APs. SVP favors isochronous voice packets over asynchronous data packets when contending for the wireless medium and when transmitting packets onto the wired LAN.

SWAN

Structured Wireless-Aware Network. A technology that incorporates a Wireless Local Area Network (WLAN) into a wired Wide Area Network (WAN). SWAN technology can enable an existing wired network to serve hundreds of users, organizations, corporations, or agencies over a large geographic area. SWAN is said to be scalable, secure, and reliable.

TAC

Technical Assistance Center.

TACACS

Terminal Access Controller Access Control System. TACACS is a family of protocols that handles remote authentication and related services for network access control through a centralized server.

TACACS+

Terminal Access Controller Access Control System+. TACACS+ provides separate authentication, authorization, and accounting services. It is derived from, but not backward compatible with, TACACS.

TCP

Transmission Control Protocol. TCP is a communication protocol that defines the standards for establishing and maintaining network connection for applications to exchange data.

TCP/IP

Transmission Control Protocol/ Internet Protocol. TCP/IP is the basic communication language or protocol of the Internet.

TFTP

Trivial File Transfer Protocol. The TFTP is a software utility for transferring files from or to a remote host.

TIM

Traffic Indication Map. TIM is an information element that advertises if any associated stations have buffered unicast frames. APs periodically send the TIM within a beacon to identify the stations that are using power saving mode and the stations that have undelivered data buffered on the AP.

TKIP

Temporal Key Integrity Protocol. A part of the WPA encryption standard for wireless networks. TKIP is the next-generation Wired Equivalent Privacy (WEP) that provides per-packet key mixing to address the flaws encountered in the WEP standard.

TLS

Transport Layer Security. TLS is a cryptographic protocol that provides communication security over the Internet. TLS encrypts the segments of network connections above the Transport Layer by using asymmetric cryptography for key exchange, symmetric encryption for privacy, and message authentication codes for message integrity.

TLV

Type-length-value or Tag-Length-Value. TLV is an encoding format. It refers to the type of data being processed, the length of the value, and the value for the type of data being processed.

ToS

Type of Service. The ToS field is part of the IPv4 header, which specifies datagrams priority and requests a route for low-delay, high-throughput, or a highly reliable service.

TPC

Transmit Power Control. TPC is a part of the 802.11h amendment. It is used to regulate the power levels used by 802.11a radio cards.

TPM

Trusted Platform Module. TPM is an international standard for a secure cryptoprocessor, which is a dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices.

TSF

Timing Synchronization Function. TSF is a WLAN function that is used for synchronizing the timers for all the stations in a BSS.

TSPEC

Traffic Specification. TSPEC allows an 802.11e client or a QoS-capable wireless client to signal its traffic requirements to the AP.

TSV

Tab-Separated Values. TSV is a file format that allows the exchange of tabular data between applications that use different internal data formats.

TTL

Time to Live. TTL or hop limit is a mechanism that sets limits for data expiry in a computer or network.

TTY

TeleTypeWriter. TTY-enabled devices allow telephones to transmit text communications for people who are deaf or hard of hearing as well as transmit voice communication.

TXOP

Transmission Opportunity. TXOP is used in wireless networks supporting the IEEE 802.11e Quality of Service (QoS) standard. Used in both EDCA and HCF Controlled Channel Access modes of operation, TXOP is a bounded time interval in which stations supporting QoS are permitted to transfer a series of frames. TXOP is defined by a start time and a maximum duration.

U-APSD

Unscheduled Automatic Power Save Delivery. U-APSD is a part of 802.11e and helps considerably in increasing the battery life of VoWLAN terminals.

UAM

Universal Access Method. UAM allows subscribers to access a wireless network after they successfully log in from a web browser.

UCC

Unified Communications and Collaboration. UCC is a term used to describe the integration of various communications methods with collaboration tools such as virtual whiteboards, real-time audio and video conferencing, and enhanced call control capabilities.

UDID

Unique Device Identifier. UDID is used to identify an iOS device.

UDP

User Datagram Protocol. UDP is a part of the TCP/IP family of protocols used for data transfer. UDP is typically used for streaming media. UDP is a stateless protocol, which means it does not acknowledge that the packets being sent have been received.

UDR

User Derivation Rule. UDR is a role assignment model used by the controllers running ArubaOS to assign roles and VLANs to the WLAN users based on MAC address, BSSID, DHCP-Option, encryption type, SSID, and the location of a user. For example, for an SSID with captive portal in the initial role, a UDR can be configured for scanners to provide a role based on their MAC OUI.

UHF

Ultra high frequency. UHF refers to radio frequencies between the range of 300 MHz and 3 GHz. UHF is also known as the decimeter band as the wavelengths range from one meter to one decimeter.

UI

User Interface.

UMTS

Universal Mobile Telecommunication System. UMTS is a third generation mobile cellular system for networks. See 3G.

UPnP

Universal Plug and Play. UPnp is a set of networking protocols that permits networked devices, such as personal computers, printers, Internet gateways, Wi-Fi APs, and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment.

URI

Uniform Resource Identifier. URI identifies the name and the location of a resource in a uniform format.

URL

Uniform Resource Locator. URL is a global address used for locating web resources on the Internet.

USB

Universal Serial Bus. USB is a connection standard that offers a common interface for communication between the external devices and a computer. USB is the most common port used in the client devices.

UTC

Coordinated Universal Time. UTC is the primary time standard by which the world regulates clocks and time.

UWB

Ultra-Wideband. UWB is a wireless technology for transmitting large amounts of digital data over a wide spectrum of frequency bands with very low power for a short distance.

VA

Virtual Appliance. VA is a pre-configured virtual machine image, ready to run on a hypervisor.

VBR

Virtual Beacon Report. VBR displays a report with the MAC address details and RSSI information of an AP.

VHT

Very High Throughput. IEEE 802.11ac is an emerging VHT WLAN standard that could achieve physical data rates of close to 7 Gbps for the 5 GHz band.

VIA

Virtual Intranet Access. VIA provides secure remote network connectivity for Android, Apple iOS, Mac OS X, and Windows mobile devices and laptops. It automatically scans and selects the best secure connection to the corporate network.

VLAN

Virtual Local Area Network. In computer networking, a single Layer 2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only

pass between them through one or more routers; such a domain is referred to as a Virtual Local Area Network, Virtual LAN, or VLAN.

VM

Virtual Machine. A VM is an emulation of a computer system. VMs are based on computer architectures and provide functionality of a physical computer.

VoIP

Voice over IP. VoIP allows transmission of voice and multimedia content over an IP network.

VoWLAN

Voice over WLAN. VoWLAN is a method of routing telephone calls for mobile users over the Internet using the technology specified in IEEE 802.11b. Routing mobile calls over the Internet makes them free, or at least much less expensive than they would be otherwise.

VPN

Virtual Private Network. VPN enables secure access to a corporate network when located remotely. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.

VRD

Validated Reference Design. VRDs are guides that capture the best practices for a particular technology in field.

VRF

VisualRF. VRF is an AirWave Management Platform (AMP) module that provides a real-time, network-wide views of your entire Radio Frequency environment along with floor plan editing capabilities. VRF also includes overlays on client health to help diagnose issues related to clients, floor plan, or a specific location.

VRF Plan

VisualRF Plan. A stand-alone Windows client used for basic planning procedures such as adding a floor plan, provisioning APs, and generating a Bill of Materials report.

VRRP

Virtual Router Redundancy Protocol. VRRP is an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN.

VSA

Vendor-Specific Attribute. VSA is a method for communicating vendor-specific information between NASs and RADIUS servers.

VTP

VLAN Trunking Protocol. VTP is a Cisco proprietary protocol for propagating VLANs on a LAN.

W-CDMA

Wideband Code-Division Multiple Access. W-CDMA is a third-generation (3G) mobile wireless technology that promises much higher data speeds to mobile and portable wireless devices.

walled garden

Walled garden is a feature that allows blocking of unauthorized users from accessing network resources.

WAN

Wide Area Network. WAN is a telecommunications network or computer network that extends over a large geographical distance.

WASP

Wireless Application Service Provider. WASP provides a web-based access to applications and services that would otherwise have to be stored locally and makes it possible for customers to access the service from a variety of wireless devices, such as a smartphone or Personal Digital Assistant (PDA).

WAX

Wireless abstract XML. WAX is an abstract markup language and a set of tools that is designed to help wireless application development as well as portability. Its tags perform at a higher level of abstraction than that of other wireless markup languages such as HTML, HDML, WML, XSL, and more.

web service

Web services allow businesses to share and process data programmatically. Developers who want to provide integrated applications can use the API to programmatically perform actions that would otherwise require manual operation of the user interface.

WEP

Wired Equivalent Privacy. WEP is a security protocol that is specified in 802.11b and is designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN.

WFA

Wi-Fi Alliance. WFA is a non-profit organization that promotes Wi-Fi technology and certifies Wi-Fi products if they conform to certain standards of interoperability.

Wi-Fi

Wi-Fi is a technology that allows electronic devices to connect to a WLAN network, mainly using the 2.4 GHz and 5 GHz radio bands. Wi-Fi can apply to products that use any 802.11 standard.

WIDS

Wireless Intrusion Detection System. WIDS is an application that detects the attacks on a wireless network or wireless system.

WiMAX

Worldwide Interoperability for Microwave Access. WiMAX refers to the implementation of IEEE 802.16 family of wireless networks standards set by the WiMAX forum.

WIP

Wireless Intrusion Protection. The WIP module provides wired and wireless AP detection, classification, and containment. It detects Denial of Service (DoS) and impersonation attacks, and prevents client and network intrusions.

WIPS

Wireless Intrusion Prevention System. WIPS is a dedicated security device or integrated software application that monitors the radio spectrum of WLAN network for rogue APs and other wireless threats.

WISP

Wireless Internet Service Provider. WISP allows subscribers to connect to a server at designated hotspots using a wireless connection such as Wi-Fi. This type of ISP offers broadband service and allows subscriber computers called stations, to access the Internet and the web from anywhere within the zone of coverage provided by the server antenna, usually a region with a radius of several kilometers.

WISPr

Wireless Internet Service Provider Roaming. The WISPr framework enables the client devices to roam between the wireless hotspots using different ISPs.

WLAN

Wireless Local Area Network. WLAN is a 802.11 standards-based LAN that the users access through a wireless connection.

WME

Wireless Multimedia Extension. WME is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic QoS features to IEEE 802.11 networks. WMM prioritizes traffic according to four ACs: voice (AC_VO), video (AC_VI), best effort (AC_BE) and background (AC_BK). See WMM.

WMI

Windows Management Instrumentation. WMI consists of a set of extensions to the Windows Driver Model that provides an operating system interface through which instrumented components provide information and notification.

WMM

Wi-Fi Multimedia. WMM is also known as WME. It refers to a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic QoS features to IEEE 802.11 networks. WMM prioritizes traffic according to four ACs: voice (AC_VO), video (AC_VI), best effort (AC_BE), and background (AC_BK).

WPA

Wi-Fi Protected Access. WPA is an interoperable wireless security specification subset of the IEEE 802.11 standard. This standard provides authentication capabilities and uses TKIP for data encryption.

WPA2

Wi-Fi Protected Access 2. WPA2 is a certification program maintained by IEEE that oversees standards for security over wireless networks. WPA2 supports IEEE 802.1X/EAP authentication or PSK technology, but includes advanced encryption mechanism using CCMP that is referred to as AES.

WSDL

Web Service Description Language. WSDL is an XML-based interface definition language used to describe the functionality provided by a web service.

WSP

Wireless Service Provider. The service provider company that offers transmission services to users of wireless devices through Radio Frequency (RF) signals rather than through end-to-end wire communication.

WWW

World Wide Web.

X.509

X.509 is a standard for a public key infrastructure for managing digital certificates and public-key encryption. It is an essential part of the Transport Layer Security protocol used to secure web and email communication.

XAuth

Extended Authentication. XAuth provides a mechanism for requesting individual authentication information from the user, and a local user database or an external authentication server. It provides a method for storing the authentication information centrally in the local network.

XML

Extensible Markup Language. XML is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

XML-RPC

XML Remote Procedure Call. XML-RPC is a protocol that uses XML to encode its calls and HTTP as a transport mechanism. Developers who want to provide integrated applications can use the API to programmatically perform actions that would otherwise require manual operation of the user interface.

ZTP

Zero Touch Provisioning. ZTP is a device provisioning mechanism that allows automatic and quick provisioning of devices with a minimal or at times no manual intervention.