Cisco Ultra-Reliable Wireless Backhaul command-line interface (CLI)

Command-line interface user manual

(Formerly Fluidmesh)
Firmware versions 7.8.0, 8.5.0 & 9.3.0 (Edition 1.0)

1. DOCUMENT CONFIDENTIALITY

This user manual contains information that is sensitive and proprietary to Cisco and/or its subsidiaries. By continuing to read this document, you give consent to be bound by the confidentiality restrictions imposed on it by Cisco Systems Inc and agree that you will not disclose its contents to any unauthorized third parties.

Unauthorized disclosure and/or distribution of any information contained in this document may violate non-disclosure agreements (NDAs) to which you may be subject and may also constitute a criminal offence under state and/or federal law.

If it comes to your attention that any part of this document has been subject to accidental or unauthorized distribution, or has otherwise been compromised, please notify the management of Cisco Networks without delay.

Reproduction, distribution, utilization and/or communication of this document, or any part thereof without express authorization is strictly prohibited. Offenders will be held liable for payment of damages.

Table of Contents

2. HAZARDOUS CONDITION WARNINGS

Only suitably qualified personnel may use the command-line interface (CLI). All Cisco hardware and software installations must conform to all relevant legislation in the country of use. In some countries, legislation may require that hardware devices be installed only by a certified electrician.

All Cisco products are designed with safety in mind. However, improper use of electronic devices and/or their control software has potential to cause serious injury and/or property damage. To avoid such injury and damage, install, configure and operate Cisco products only if you are properly qualified to do so.

If any Cisco hardware unit breaks down or malfunctions, emits smoke or an unusual smell, if water or other foreign matter enters the unit enclosure, or if the unit is dropped onto a hard surface or damaged in any way, power off the unit immediately and contact an authorized Cisco dealer for assistance.

If you are adjusting and/or controlling a Cisco device using control software such as the command-line interface or the device's offline Configurator, do not make configuration changes unless you know with certainty that your changes will not negatively impact people or animals in the vicinity of the device and its antennas.

2.1. Radio-frequency transmission hazard

RADIO-FREQUENCY RADIATION

Non-ionizing radio frequency (RF) transmissions can be hazardous to human and animal health.

In sufficient quantity, RF radiation is capable of causing radiation burns, tissue damage and other injuries. Keep a safe distance from all RF-radiating devices such as antennas, when such devices are powered ON. Never stand in line with a powered RF-radiating device.

Before activating any device capable of transmitting RF signals, make sure that all persons and animals are protected from possible RF exposure.

Make sure that all RF feeds are securely connected to an appropriate antenna. Never activate any RF-capable device that is not connected to an antenna.

2.2. Optical radiation hazard

LASER RADIATION

If any Cisco hardware device is equipped with one or more SFP fiber-optic modules, it is classified as a Class 1 laser product. It may use laser-emitting components and/or very high-intensity light sources.

Do not look directly at the input/output end of the unit's SFP connector, or at the input/output end of any fiber-optic cable. Fiber-optic systems frequently use high-intensity light from laser or LED sources that may cause temporary or permanent blindness.

For additional guidance regarding the safe use of laser-based and LED-based fiber-optic technology, refer to ANSI Z136.2 *(Safe Use of Optical Fiber Communication Systems Utilizing Laser Diode and LED Sources).*

2.3. Hot surfaces hazard

HOT SURFACES

The outer surfaces of some radio transceiver and gateway unit enclosures may become hot during normal operation. The outer enclosures of such devices are marked with the symbol seen above. During normal operation, do not touch or handle the unit enclosure without personal protective equipment.

3. REPORTING MISTAKES

You can help improve this document.

If you find any mistakes, or if you know of a way to improve the procedures that are given, please let us know by E-mailing your suggestions to the following addresses:

- documentation@fluidmesh.com
- support@fluidmesh.com

4. INTRODUCTION

This manual explains how to use the Cisco Command-line interface (CLI) as a means to configure and control Cisco hardware devices that are part of a network.

The CLI is intended for use by wireless networking professionals who have been tasked with configuring Cisco gateway units and/or radio transceivers, and/or configuring and maintaining the system using Cisco software.

Throughout this manual, configuration and adjustment settings are given for Cisco device parameters. You must have a thorough understanding of each parameter before attempting to configure or adjust it. Many configuration parameters are interdependent. Misconfiguration or poor adjustment of parameters could degrade the performance of a Cisco device, or make it inoperable.

IMPORTANT

The functions of all device configuration parameters are explained in detail in the *Cisco RACER Configuration Manual*, and in the user manual for your Cisco gateway device or radio transceiver device.

Be sure to read and understand the documents above before attempting to configure your device using the command-line interface.

This manual is applicable only to the following Cisco device firmware versions and their relevant hardware devices:

- 7.8.0 (FM1200 Volo radio transceiver)
- 8.5.0 (FM3200-series and FM4200-series radio transceivers)
- 9.3.0 (FM3500 Endo and FM4500-series radio transceivers)

This manual may contain commands and/or command parameters that are being newly introduced as part of a firmware version described in this manual, or that must be expressed in a way that is different to a previous version of the same command. All sub-sections containing new and/or modified commands are marked with:

NEW

This manual is not applicable to device firmware versions that are more recent than the firmware versions above. For these firmware versions, refer to the appropriate version of the Cisco Command-line interface user manual.

4.1. CLI account types

Users can log onto the CLI using Administrator or View Mode credentials.

The differences between credential types are shown in the table below.

Account passwords can be changed by an Administrator, using RACER or the offline Configurator interface.

Account	Default user name	Default password	Permissions
Administrator	admin	admin	Full access, with read and write permissions.
View Mode	user	viewmode	Read permissions only. The user cannot change configuration parameters.

If you are logging onto the device as an administrative user, log on using the following command:

```
ssh <admin_user>@<device IP address>
```

If you are logging onto the device in View Mode, log on using the following command:

```
ssh <view_mode>@<device IP address>
```

5. UNDERSTANDING THE CLI

The Cisco Networks command-line interface (CLI) is used to issue configuration commands to a Cisco device over a Secure Shell (SSH) service. SSH is a cryptographic network protocol that allows secure operation of network services over an unsecured network.

The CLI can be regarded as a ‘backup’ user interface, giving an alternative method of configuring Cisco radio transceiver and gateway devices.

Like the RACER™ and on-board Configurator interfaces, the CLI allows you to inspect and modify the configuration parameters of the relevant unit.

TIP

The on-board Configurator interface features a limited set of configuration options for most Cisco devices.

To gain access to the full set of configuration options for the relevant Cisco device, use the RACER interface or command-line interface to configure the device.

6. USING THE CLI TO CONFIGURE CISCO DEVICES

IMPORTANT

Device configuration parameters can only be changed if you are accessing a device as an Administrator.

If you are accessing a device in View Mode, you can view the device's configuration settings, but cannot change them.

To use the CLI to configure a Cisco device, do the steps below:

1. Install an SSH client on the computer that you will use to configure the Cisco device. Recommended SSH clients include Secure CRT (Windows computers) and the built-in SSH terminal (Linux and Mac systems).
2. Use the SSH client to log in to the Cisco device as an administrative user, substituting **<device IP address>** with the IP address of the Cisco unit. Do this by entering the following command using the terminal:

```
ssh <admin_user>@<device IP address>
```

3. Use the SSH client to configure the Cisco device using the appropriate commands as given in this manual. Be sure to use the correct command-line syntax.
4. Confirm the configuration changes by entering the following command:

```
write
```

5. Reboot the unit by entering the following command:

```
reboot
```

7. UNDERSTANDING COMMAND-LINE SYNTAX

The logical structure of the configuration commands given using the CLI is referred to as syntax.

The configuration command syntax used by Cisco devices is simple. The command-line syntax can be used to issue one command, or to issue multiple commands within a single command entry, before pressing the **Enter** key.

If multiple commands are made within a single command entry, all commands must be separated by spaces.

For demonstration, here are typical examples that show ways in which a radio transceiver's Ethernet parameters can be configured.

To show the current configuration for a specific Ethernet port, you would enter the following command:

```
ethernet port eth 1
```

To configure the data transfer speed and duplex mode for a specific Ethernet port, you would make the needed choices based on:

- The specifications given in the network design document, and
- The characteristics of the Cisco device.

As a typical example, an FM3500 Endo radio transceiver has the following features:

- Two RJ-45 Ethernet ports, numbered 1 and 2.
- A choice of two duplex modes (half and full).

Based on this information, if you wanted to set Ethernet port 2 of the FM3500 Endo to transmit and receive data in full duplex mode, you would enter the following command:

```
ethernet port eth 2 duplex full
```

8. CLI COMMANDS

8.1. Help content

Configuration objective	CLI command	Parameter options
Show context-sensitive help content for the current command. To be typed after the command name and command parameters.	`?`	

8.2. Manage the device status logs

Configuration objective	CLI command	Parameter options
View or clear the device status logs.	`status A`	Possible parameters for A are: • *show-logs* (show the device status logs that have been created since the last clear command was executed.) • *clear-logs* (delete all existing device status logs.) • *delete-logs* (deep-clean the repository containing all device status logs.)

8.3. View the current network uptime duration

Configuration objective	CLI command	Parameter options
Show the amount of time for which the connected network has been operational.	`uptime`	

8.4. View the device configuration that is currently running

Configuration objective	CLI command	Parameter options
Show a detailed view of the currently running device configuration.	`show-running-config`	

8.5. Viewing and setting the device name

Configuration objective	CLI command	Parameter options
Show the device name that has been assigned to the device.	`devicename`	
Edit the device name that has previously been assigned to the device.	`devicename A`	Parameter A is the new device name.

8.6. Running an installed iperf server or client

Configuration objective	CLI command	Parameter options
Run the installed iperf server or client.	`iperf`	
Specify iperf configuration options.	`iperf B`	Parameter B is the specified iperf configuration option. For a detailed list of iperf commands, refer to

		https://www.mankier.com/1/iperf.

8.7. Connecting to a remote host using SSH

Configuration objective	CLI command	Parameter options
Connect the device to a remote host using Secure Shell.	`ssh C`	Parameter C is the hostname or IP address of the remote host.

8.8. Pinging the configured device

Configuration objective	CLI command	Parameter options
Send a ping from the hardware device to another, specified hardware device.	`ping A`	Parameter A is the IP address of the hardware device that is not the local device.
Set the ping count (in other words, to stop pinging after a specified number of packets).	`ping -c B`	Parameter B is the specified number of echo request packets (optional).

8.9. Tracing the route from the device to its connected host

Configuration objective	CLI command	Parameter options
Return a description of the connected route from the local device, to its specified host (A).	`traceroute A`	Parameter A is the hostname of the specified host.
Specify the maximum number of hops included in the traceroute result.	`traceroute -m B`	Parameter B is the specified maximum number of hops. Note that the maximum number of hops cannot exceed 255.

8.10. Wireless interface

IMPORTANT

If commands and values from this section are entered, they are validated in accordance with the installed software plug-ins and the regulatory mode to which the device has been set.

Configuration objective	CLI command	Parameter options
Show the active parameters of the wireless interface.	`wireless`	
Set the frequency, channel width and status parameters to be changed at runtime, without having to reboot the device.	`wireless live`	
Set the device's operating frequency.	`wireless frequency A`	Parameter A is the specified frequency in MHz.
Set the device's operating channel width.	`wireless cwidth B`	Parameter B is the specified channel width in MHz. Depending on radio transceiver type, possible channel width values are *5, 10, 20, 40* or *80*.
Enable and disable advanced encryption standard (AES) traffic encryption.	`wireless crypto aes C`	Possible parameters for C are *enable* and *disable*.
Set the device's mesh network passphrase.	`wireless passphrase D`	Parameter D is the network passphrase.

Set the device's maximum transmission power output.	`wireless txpower E`	Parameter E is the maximum transmission power level in dBm. This parameter must be expressed as an unsigned integer between 0 and 36. Alternatively, enable automatic transmission-power selection by entering `wireless txpower AUTO` (note that AUTO must be entered in capitals).
FM1200 Volo, FM3200-series and FM4200-series radio transceivers only: Enable and disable Promiscuous Mode (backwards compatibility with legacy Fluidmesh units).	`wireless promisc F`	Possible parameters for F are *enable* (enable full backwards compatibility) and *disable* (maintain compatibility with newer devices only).
Enable and disable the device's wireless interface.	`wireless interface G`	Possible parameters for G are *enable* and *disable*.
Set the device's transmission chain parameters.	`wireless txchain H`	Possible parameters for H are *first* (transmission chain 1 only), *second* (transmission chain 2 only) or *both*.
Set the device's maximum modulation and coding scheme (the schema by which the unit automatically chooses its maximum data transmission rate using parameters such as channel width, number of spatial streams, coding method, modulation technique and guard interval).	`wireless maxmcs I`	Parameter I is expressed in Mbps. Alternatively, allow the device to choose the MCS automatically by entering *auto*.
FM1200 Volo, FM3200-series and FM4200-series radio transceivers only: Enable and disable noise floor calibration.	`wireless nfcal J`	Possible parameters for J are *enable* and *disable*.
Enable and disable reduction of false positive results during dynamic frequency selection (DFS) if the device is being operated in the UNII2 frequency band.	`wireless dfs reduce-false-positives K`	Possible parameters for K are *enable* and *disable*.
FM3500 Endo and FM4500-series radio transceivers only: Enable and disable the device's IEEE 802.11 request-to-send (RTS) setting.	`wireless rts L`	Possible parameters for L are *enable* and *disable*.
FM3500 Endo and FM4500-series radio transceivers only: Set the packet size threshold	`wireless rts M`	Possible parameters for M are *retry-limit A* (where A is the maximum allowable number of RTS retry attempts), and

for IEEE 802.11 request-to-send (RTS) send requests.		*disable* (disables packet size threshold setting).
FM3500 Endo and FM4500-series radio transceivers only: Set the maximum number of spatial streams (NSS).	`wireless maxnss A`	A is the maximum number of spatial streams. For FM3500 Endo and 4500-series devices, the minimum NSS value is *1* and the maximum value is *2.*
FM3500 Endo and FM4500-series radio transceivers only: Set the wireless multimedia (WMM) queue configuration string.	`wireless wmm N`	Parameter N is the WMM configuration string. This string takes the following form: *[bk|be|vi|vo] aifs A cwmin B cwmax C txop D ampdu E* In the string above, [bk|be|vi|vo] represents the class-of-service (CoS) parameters: • *bk* is the CoS background queue parameter. • *be* is the CoS best-effort queue parameter. • *vi* is the CoS video queue parameter. • *vo* is the CoS voice queue parameter. Also in the string above: • *A* is the arbitration inter-frame spacing value. • *B* is the minimum transmission channel width value. • *C* is the maximum transmission channel width value. • *D* is the transmit opportunity value. • *E* is the aggregated MAC protocol data unit value.
FM3500 Endo and FM4500-series radio transceivers only: These settings are used to configure automatic recovery if data packets are sent, but not acknowledged. The following values can be expressed in combinations, as shown in the right-hand cell: • Value A is the maximum number of transmission retries per chain. • Value B is the level to which the data stream is allowed to 'fall back' (i.e. at which a re-transmission is attempted using a more conservative	`wireless retries O`	These values can be entered in any of the following combinations, as needed: • *A B* • *C B* • *A D* • *C D* • *A B D* • *C B D* Possible parameters for *D* are enable and disable.

combination of parameters for rate transmission). • Value C is the maximum delay period in which attempted re-transmissions are allowed before the attempt is halted. • Value D activates and de-activates the single-stream fall-back function. If activated, attempted re-transmissions will include single-stream modulation and coding schemes.		
FM3500 Endo and FM4500-series radio transceivers only: Set the mesh beacon period and modulation and coding scheme.	`wireless beacon D E`	Value D is the mesh beacon period in milliseconds, and value E is the modulation and coding scheme that will be used for mesh beacons.
FM3500 Endo and FM4500-series radio transceivers only: Set the aggregated MAC protocol data unit (AMPDU) timeout value.	`wireless ampdu timeout Q`	Value Q is the AMPDU re-order buffer timeout value in milliseconds.
FM3500 Endo and FM4500-series radio transceivers only: Override the network allocation vector timer, or disable the timer override.	`wireless nav_time R`	Possible parameters for R are *enable* and *disable*.
FM3500 Endo and FM4500-series radio transceivers only: Set the radio unit’s transmission frequency according to the factory default settings, or to custom settings.	`wireless caldata S`	Possible parameters for S are *factory* (use the factory default settings for all frequencies), *default* (use custom settings for 4 980 MHz only) or *alternate* (use custom settings for all frequencies).
Set the operational mode for dynamic frequency selection (DFS) when the device is operated in the UNII2 frequency band.	`wireless radar-role U`	Possible parameters for U are *auto* (The unit will automatically participate in a Principal/Subordinate role-election process, and the elected Principal unit will determine the operating frequency), *master* (All Subordinate units connected to the unit will match the unit’s DFS frequency selection) or *slave* (The unit will match the DFS frequency selection of the closest Principal unit). Note that if value U is set to *auto*, all radio units that are part of the network must also be set to auto.

IMPORTANT

If a Cisco radio device is operated in the UNII2 frequency band, and the *wireless radar-role* is set as *master*, the device will continuously monitor the chosen operating frequency for known radar patterns.

If the network detects a known radar pattern, the elected Principal (i.e. master) radio device coordinates a distributed frequency-switching procedure with all Subordinate (i.e. slave) radio units, allowing the network to continue operating on an alternate frequency without interruption.

Scan a preset list of alternate frequencies. If the device is being operated in the UNII2 frequency band and detects a TDWR transmission on the current operational frequency, it will scan the preset frequency list for an unoccupied frequency.	**`wireless backup-frequencies V`**	Parameter V is the preset list of alternate frequencies in MHz. Note that each frequency value added to the list must include a specified channel width in MHz. Depending on radio transceiver type, possible channel width values are 5, 10, 20, 40 or 80. A typical command entry might be **`wireless backup-frequencies 5255 20 5300 40 5310 40`**.
Set the signal gain of the antenna connected to the wireless device.	**`wireless antenna-gain W`**	Parameter W is the maximum antenna gain in dBm. This parameter must be expressed as an unsigned integer between 0 and 36. Alternatively, reset antenna gain to the factory default level by entering **`wireless antenna-gain UNSELECTED`**. Note that UNSELECTED must be entered in capitals.
Scan a preset list of alternate frequencies. If the device is being operated in the UNII2 frequency band and detects a TDWR transmission on the current operational frequency, it will scan the preset frequency list for an unoccupied frequency.	**`wireless backup-frequencies V`**	Parameter V is the preset list of alternate frequencies in MHz. Note that each frequency value added to the list must include a specified channel width in MHz. Depending on radio transceiver type, possible channel width values are 5, 10, 20, 40 or 80. A typical command entry might be **`wireless backup-frequencies 5255 20 5300 40 5310 40`**.
NEW Specify the country in which the radio transceiver will be operated.	**`wireless country W`**	Parameter W is the identification string for the country in which the radio transceiver will be operated.

		Typical examples are *UNITED STATES* and *ITALY*. Note that the country name must be entered in capitals.
FM3500 Endo and FM4500-series radio transceivers only: Change the reference transmission power value that was set during factory calibration of the unit.	`wireless target-power X`	Possible parameters for X are *default* (use the default reference transmission power value) or *alternate* (use an alternate transmission power value).

8.11. FluidMax settings

Configuration objective	CLI command	Parameter options
Show the device's current FluidMax parameters.	`fluidmax`	
Set the device's FluidMax mode.	`fluidmax mode A`	Possible parameters for A are *auto*, *master*, *slave*, or *off*.
Set the device's FluidMax cluster ID value.	`fluidmax cluster-id B`	Parameter B is the device's FluidMax cluster ID value.
Set the device's FluidMax token status tracker to decide whether or not to temporarily block a low-performing Subordinate radio that is affecting the performance of other radios (this setting applies to devices in FluidMax master mode only).	`fluidmax tktrk D`	Possible parameters for D are *enable* and *disable*.
Set the device's FluidMax autoscan settings.	`fluidmax autoscan E`	Possible parameters for E are *enable* (enable autoscan without including 5 and 10 MHz channel widths) or *disable* (disable autoscan; devices in FluidMax slave mode only). Additional parameters for FM1200 Volo, 3200-series and 4200-series radios only are: • *enable-all-cwidth* (enable autoscan including 5 and 10 MHz channel widths). • *enable autoscan including 5-10MHz cwidth.*
Set or disable the device's tower ID value. This value is used to identify all Principal radio units installed on the same tower. This feature can be used in conjunction with TITAN to correctly identify primary and secondary Principal units.	`fluidmax tower-id F`	Possible parameters for F are the device tower ID value, or *disable*.
Set or disable the device's RSSI threshold at which a scan for new Principal units will be triggered.	`fluidmax rssi-th G`	Possible parameters for G are the device's FluidMax RSSI threshold value (devices in FluidMax slave mode only), or *disable*.
FM1200 Volo, FM3200-series and FM4200-series radio	`fluidmax token-passing H`	Possible parameters for H are *enable* and *disable*.

transceivers only: Set or disable the device's Fluidmax token-passing setting.		

8.12. IP address parameters

Configuration objective	CLI command	Parameter options
Show the device's IP address parameters.	`ip`	
Set the device's IP address.	`ip addr A`	Parameter A is the specified IP address.
Set the device's netmask parameter.	`ip netmask B`	Parameter B is the netmask.
Set the device's IP gateway parameter.	`ip gateway C`	Parameter C is the IP gateway.
Set the device's DNS1 address parameter.	`ip dns1 D`	Parameter D is the DNS1 address.
Set the device's DNS2 address parameter.	`ip dns2 E`	Parameter E is the DNS2 address.

8.13. Administrative user password

IMPORTANT

Before changing the administrative user password, make sure that the password is known to all personnel who will use it.

If an administrative user password has been set, the system cannot recall it or display it for reference.

Configuration objective	CLI command	Parameter options
NEW Set the Administrative user password for access to the device's offline Configurator interface and CLI.	`admin-user username Y passwd Z`	Parameter Y is the new administrator user name. Parameter Z is the new password.

8.14. View Mode user password

IMPORTANT

Before changing the View Mode user password, make sure that the password is known to all personnel who will use it.

When a password has been entered, the system cannot recall it or display it for reference.

Configuration objective	CLI command	Parameter options
NEW Set the View Mode user password for access to the device's offline Configurator interface and CLI.	`viewmode-user username F passwd G`	Parameter F is the new view-mode user name. Parameter G is the new password.

8.15. Ethernet port parameters

Configuration objective	CLI command	Parameter options
NEW Show the current configuration for a specific Ethernet port on the local device.	`ethernet port A`	Parameter A is the number of the Ethernet port (or SFP interface) being queried. If the radio has two Ethernet ports, possible values for A are *eth 1* (LAN 1 port) or *eth 2* (LAN 2 port). For FM4200 Fiber and FM4500 Fiber radios, possible values for A are *eth* (LAN port) or *sfp* (fiber-optic port).
NEW Set the maximum port speed for the device's Ethernet ports.	`ethernet port A speed B`	Parameter A is the number of the Ethernet port (or SFP interface) whose speed is being modified. Possible values for A are *eth 1* or *eth 2.* Parameter B is the data transfer speed for the relevant port. Ethernet port speeds are expressed in Mbps. Possible values for B are *10*, *100*, or *auto*.
NEW FM1200 Volo, FM3200-series and FM4200-series radio transceivers only: Set the duplex mode for the device's Ethernet ports.	`ethernet port A duplex C`	Parameter A is the number of the Ethernet port (or SFP interface) for which the duplex mode is being set. Parameter C is the port duplex mode. Possible values for C are *half* or *full*.
NEW Change the size of the Ethernet maximum transmission unit (MTU) for the device ports.	`ethernet mtu D`	Parameter D is the port MTU size setting in bytes. The value can be set between a minimum of 1530 and a maximum of 1650 for FM1200V, FM3200, FM4200 and 2000 for FM3500 and FM4500.

8.16. Mesh routing table parameters

Configuration objective	CLI command	Parameter options
Show the device's mesh routing table in the form of hop-by-hop mesh ID numbers.	`meshroute`	
Show the device's Pass list and Block list routing list.	`meshroute show`	
Set the device's Pass list or Block list link sequence.	`meshroute set A`	Parameter A is the list selection setting. Possible values for A are *pass list* or *block list*.
Clear the device's Pass list or Block list.	`meshroute set A clear`	Parameter A is the list selection setting. Possible values for A are *pass list* or

		block list. When the command is executed, the specified list will be deleted.
Add new Block listed or Pass listed devices to the device's Pass list/Block list link sequence.	`meshroute set A add B`	Parameter A is the list selection setting. Possible values for A are *pass list* or *block list*. Parameter B consists of block listed or pass listed devices being added to the devices on the existing block list and/or pass list.

8.17. MPLS parameters

Configuration objective	CLI command	Parameter options
If Prodigy 2.0 is enabled, show all multi-protocol label switching (MPLS) label-switched paths that are currently installed on the device.	`mpls`	
Display the MPLS Virtual Bridge table.	`mpls vbr show`	
Clear the MPLS Virtual Bridge table.	`mpls vbr clear`	
Configure the controlled unicast-flooding feature.	`mpls unicast-flood A`	Possible values for A are *enabled*, *disabled* or *unrestricted*. *unrestricted* allows forwarding of packets carrying non-private IP addresses.
Specify whether the device will perform unicast flooding on ARP request.	`mpls arp-unicast B`	Possible values for B are *enabled* or *disabled*.
Configure the fast failover feature.	`mpls fastfail status C`	Possible values for C are *enabled* or *disabled*.
Set the fast failover timeout for device failure detection.	`mpls timeout D`	Value D is the set timeout for device failure detection, in milliseconds.
Set the delay in letting the core switches update ARP cache WAN IP address data, as used by the L2TP tunnels.	`mpls wan-delay E`	Value E is the update delay in milliseconds.
Set the virtual IP address of the redundant device group in Layer-3 scenarios (applicable to global gateways and on-board radio transceivers only).	`mpls primary F`	Value F is the virtual IP address.
Set the time delay before a primary Principal unit takes over from its secondary unit after a primary-Principal failure has been resolved.	`mpls preempt-delay G`	Value G is the fast failover pre-emptive delay in seconds.
Specify the peers the device will establish pseudo-wires (label-switched paths, or LSPs) with. If value H is set as mesh-end, the device will only establish LSPs with other	`mpls pw-set H`	Possible values for H are *all* or *mesh-end*.

Mesh-end devices.		
Set the device-cluster ID of the device (Layer-2 scenarios only).	`mpls cluster-id I`	Possible values for I are *set CI* (sets the cluster ID of the device) or *clear* (erases the device's cluster ID and configures it as a stand-alone unit).
Show, clear or add a new entry in the static local virtual bridge table.	`mpls mac-list J K L`	Possible values for J are: • *show* (Show all current entries in the MPLS virtual bridge table). • *clear* (Delete all current entries from the MPLS virtual bridge table). • *add* (Add a new entry to the MPLS virtual bridge table). Value K is the MAC address of the client device. Value L is the VLAN ID of the client device.
Enable or disable reduction of the allowed number of broadcast packets. This feature can be used to minimize unnecessary network load.	`mpls reduce-broadcast M`	Possible values for M are *enable* or *disable*.
NEW Set the maximum allowed traffic rate for ARP traffic.	`mpls arp-limit rate N`	Parameter N is the maximum allowed rate for ARP traffic (expressed in packets per second). ARP packets received in excess of this threshold within a one-second interval will be dropped. Set the value to *0* to disable the feature.
NEW Set the ARP traffic-blocking grace period.	`mpls arp-limit grace O`	Parameter O is the ARP traffic-blocking grace period in milliseconds. If the configured maximum allowed rate for ARP traffic (parameter N above) is exceeded for the length of the ARP traffic-blocking grace period, all ARP traffic will be blocked for the configured ARP bocking time (parameter P below).
NEW Set the ARP traffic-blocking period.	`mpls arp-limit block P`	Parameter P is the ARP traffic blocking time in milliseconds. Set the value to *0* to disable the feature.

8.18. Address Resolution Protocol settings

Configuration objective	CLI command	Parameter options
Enable or disable transmission of gratuitous ARP packets	`gratuitous-arp B`	Possible values for B are *enable* or *disable*.

following network topology changes.		
Set a delay before transmission of gratuitous ARP packets.	`gratuitous-arp delay C`	Value C is the delay period before transmission of gratuitous ARP packets, expressed in milliseconds.

8.19. Prodigy and Operating Mode settings

Configuration objective	CLI command	Parameter options
Show the device's current Prodigy engine and operating mode.	`modeconfig`	
Set the device's current operating mode.	`modeconfig mode A`	Possible values for A are *bridge*, *meshpoint* or *meshend*. Note that Fluidity devices are always set in either mesh end or mesh point mode according to their specified device role.
Set the device's selected Prodigy engine and MPLS OSI layer.	`modeconfig prodigy B layer C`	Possible values for B are *1* (Prodigy 1.0) or *2* (Prodigy 2.0). Possible values for C are *2* (OSI Layer-2) or *3* (OSI Layer-3).

8.20. Hardware Reset button

Configuration objective	CLI command	Parameter options
Set the device's hardware Reset button to trigger: • A unit reboot if the button is pressed for one second and released. • A factory reset if the button is pressed for 7 seconds and released.	`reset-button enable`	
Set the device's hardware Reset button to trigger a factory reset if the button is pressed for 7 seconds and released (the unit reboot option will be unavailable).	`reset-button factory`	
Disable the hardware Reset button functionality.	`reset-button disable`	

8.21. Telnet functionality

Configuration objective	CLI command	Parameter options
Enable or disable the device's Telnet capability.	`telnet A`	Possible values for A are *on* or *off*.

8.22. Committing configuration settings to memory

IMPORTANT

After the **write** command is entered, you must re-boot the device for the current configuration to take effect.

Configuration objective	CLI command	Parameter options
Commit the current configuration settings to memory.	`write`	

8.1. Rebooting the device

Configuration objective	CLI command	Parameter options
Reboot the device immediately.	`reboot`	
Reboot the device after a configured amount of time.	`reboot A`	Value A is the delay period before the device reboots.

8.2. Discarding configuration changes made during the current session

Configuration objective	CLI command	Parameter options
Discard all configuration changes made during the current session.	`discard`	

8.3. Resetting the unit to factory default condition

Configuration objective	CLI command	Parameter options
Reset the unit to factory default condition.	`factory YES` Note that YES must be typed in capitals.	

8.4. Showing command-line history for the current session

Configuration objective	CLI command	Parameter options
Show a complete list of all CLI commands that have been entered during the current session.	`history`	
Show a chosen number of CLI commands that have been entered during the current session, in reverse chronology from the most recent command.	`history A`	Value A is the maximum number of recent commands.

8.5. Adding, removing and showing installed plug-in licenses

Configuration objective	CLI command	Parameter options
Show a complete list of the software plug-in licenses that are currently installed on the device.	`plugins`	
NEW Add a new software plug-in license to the radio transceiver.	`plugins add B`	Value B is the activation code for the relevant plug-in license.

NEW Delete a new software plug-in license from the radio transceiver.	`plugins remove C`	Value C is the name of the relevant plug-in license.

8.6. Showing the device model and firmware revision number

Configuration objective	CLI command	Parameter options
Show the device model and firmware revision number.	`version`	

8.7. Showing the device mesh ID number

Configuration objective	CLI command	Parameter options
Show the device's Cisco mesh ID number.	`meshid`	

8.8. Fluidity settings

Configuration objective	CLI command	Parameter options
Enable or disable Fluidity.	`fluidity status A`	Possible values for A are *enabled* or *disabled*.
Set the device's Fluidity mode.	`fluidity id B`	Possible values for B are: • *infrastructure* (infrastructure mode). • *wireless-relay* (wireless infrastructure with no Ethernet connection to the backhaul). • *vehicle-auto* (vehicle mode, with automatic vehicle ID selection).
Set the device's rate adaptation algorithm for packet transmission.	`fluidity rate-control D`	Possible values for D are *standard* or *advanced*.
Set the device's Fluidity backhaul check setting.	`fluidity backhaul-check E`	Possible values for E are: • *handoff-inhibition* (if the unit is set as an infrastructure unit, it will not be eligible for handoff if its Ethernet ports are not connected to the backhaul). • *relay-switch* (the unit will temporarily switch to wireless relay mode until a broken Ethernet connection is restored). • *disabled* (Ethernet status will be ignored).
Set the device's Fluidity Mesh-end connection check setting.	`fluidity backhaul-check E me-check F`	Possible values for E are as above. Possible values for F are: • *handoff-inhibition* (if the unit is set as an infrastructure unit, it will not be eligible for handoff if the local mesh-end unit is unreachable). • *relay-switch* (the unit will

		temporarily switch to wireless relay mode if the local mesh-end unit is unreachable). - *disabled* (the connection status of the local mesh-end unit will be ignored).

TIP

Fluidity backhaul check settings and Mesh-end connection check settings can be used in combination.

Typical combinations include:

```
fluidity backhaul-check me-
    check relay-switch
```

The command above enables mesh-end backhaul check mode, and switches the unit to *Infrastructure wireless relay* mode if the mesh end is unreachable.

```
fluidity backhaul-check me-
  check handoff-inhibition
```

The command above enables mesh-end backhaul check mode, and inhibits traffic handoff if the local mesh-end is unreachable.

```
fluidity backhaul-check me-
     check disabled
```

The command above disables mesh-end backhaul check mode.

Monitor the device’s Fluidity statistics through a relevant UDP port.	`fluidity monitor G1 G2`	Parameter G1 is the IP address of the monitoring device. Parameter G2 is the UDP port number (optional).
If the device is set as a mobile unit, set the device’s hand-off algorithm.	`fluidity handoff H`	Possible values for H are: - *standard* (system default). - *load-balancing* (balances signal strength against signal-traffic load). - *v2v* (enables vehicle-to-vehicle handoff).
Set the device’s Fluidity traffic routing setting.	`fluidity routes I`	Possible values for I are: - *backhaul* (advertise routes to infrastructure radio units only). - *all* (advertise routes to mobile and infrastructure radio units).
If the device is set as a mobile unit, set the mesh ID of the infrastructure unit the unit can connect to.	`fluidity connect J`	Value J is the Cisco mesh ID number of the infrastructure unit the unit must be set to connect to.
Set the device’s Fluidity autoscan setting.	`fluidity scan K`	Possible values for K are: - *disabled* (disable frequency autoscan). - *isolation M* (the unit will do

		an autoscan if it is disconnected from infrastructure for the amount of time (in ms) specified by parameter M. • *list* (set a list of channels and bandwidths (in MHz) to scan for other Fluidity units). A typical example might be `fluidity scan list 5180 40 5220 20`. • *rssi-threshold L* (set the critical RSSI threshold at which an autoscan will be triggered, where L is the threshold in dB). • *live* (force a scan for live frequencies. If a frequency with better signal strength is available, the device will automatically switch to that frequency). • *periodic* (set the time interval (in ms) at which periodic autoscanning happens when the unit is idle). • *vehicle-frequency B* (Choose whether or not vehicle-mounted radio units can use different operating frequencies. Possible values for B are *locked, open* or *reset "freq cwidth" live*.)
Set the upper limit for the device's degree of preference (DoP).	`fluidity dop limit L`	The device will not attempt or accept hand-off requests if the current DoP value exceeds value L. Set value L to *0* for unlimited DoP.
Set the fixed bias value that is applied to the computed DoP value to give greater (positive) or less (negative) importance to a Fluidity access point for load-balancing purposes.	`fluidity dop bias M`	Value M is the set DoP bias value, expressed as an unsigned integer. Note that the bias value can be positive or negative.
Set the overhead value that is applied to each DoP advertised by connected clients.	`fluidity dop client N`	Value N is the set DoP overhead value, expressed as an unsigned integer.
Set the maximum number of clients (mobile transceiver units) that can connect to an infrastructure access point.	`fluidity max-clients B`	Value B is the maximum number of clients that will be allowed to connect to the access point.
Set the warm-up time if the unit is in Infrastructure mode or Vehicle mode. During the warm-up period, the unit will not accept handoff	`fluidity warmup O`	Value O is the device warm-up time in milliseconds.

requests if it is in Infrastructure mode, and will not attempt to connect to the network if it is in Vehicle mode. The unit enters a warm-up period under the following conditions: • Whenever the unit is activated. • If the LAN link to the unit is activated or de-activated. • When the unit does its first RADIUS authentication. • When a backhaul check is triggered.		
Set the time period for which the unit's infrastructure records are saved, if the unit is in Vehicle mode. If the unit does not receive a signaling packet from the closest Infrastructure unit within this period of time, it will discard all information associated with that Infrastructure unit. The default time-out value is 800 milliseconds.	`fluidity timeout P`	Value P is the infrastructure time-out period in seconds.
Set the device's large-network optimization setting.	`fluidity lno R`	Possible values for R are: • *enabled* (Enabling LNO also enables Mesh-end only pseudo-wire creation, and disables STP forwarding). • *disabled* (Disabling LNO also disables Mesh-end only pseudo-wire creation, and sets STP forwarding to auto).
Enable load-balancing in a way that allows or blocks a specific mobile radio unit.	`fluidity access S`	Value S must be expressed in the form of [A] [B] [C], where: • Value A is the access-control list (ACL) operation command. Possible values for A are *allow* or *block*. • Value B is the mesh ID number of the Cisco unit whose access to the local unit is being allowed or blocked. • Value C is the time period for which a blocked unit will be blocked, expressed in seconds. A typical example of this command might be:

		`fluidity access block 5.1.2.3 3600`

Set the device's hand-off hysteresis and RSSI low/high zones threshold settings.	`fluidity delta-high T`
	`fluidity delta-low U`
	`fluidity delta-threshold V`
		- Value *delta-high T* is the optimal upper handoff hysteresis threshold. Value T is always expressed as a number greater than 0.
		- Value *delta-low U* is the optimal lower handoff hysteresis threshold. Value U is always expressed as a number greater than 0.
		- Value *delta-threshold V* is the optimal RSSI low/high zone threshold value. Value V is always expressed as a number greater than 0.

Set the maximum number of vehicles allowed to connect to the device simultaneously if the device is set to Infrastructure mode.	`fluidity max-clients W`	Value W must be expressed as a number greater than 0. Alternatively, allow an unlimited number of vehicles by setting value W as *0*.
Show a summary of the Fluidity network's settings and statistics.	`fluidity show`	
Configure the device's VLAN settings if the Fluidity device is part of a VLAN on board a vehicle.	`fluidity vlan X`	Possible values for X are: - *show* (shows the current on-board VLAN configuration.) - *clear* (deletes all configured Fluidity VLAN entries.) - *add A B C* (adds the device to the on-board VLAN, where value A is the device ID tag in context of the on-board VLAN, value B is the device's IP address, and value C is the device's netmask). A typical example of the add A B C command might be: `fluidity vlan add 10 192.168.10.1 255.255.255.0`.
Enable or disable FMQuadro-based telemetry.	`fluidity fmquadro Y`	Possible values for Y are *enabled* and *disabled*.
Set the maximum number of data packets that are consecutively lost before fast wireless disconnection is triggered.	`fluidity fastdrop count Z`	Value Z is the maximum number of consecutively lost data packets.
FM3500 Endo and FM4500-series radio transceivers only: Ban incoming transmissions from the connected	`fluidity rssi-ban-delta AA`	Value AA is the maximum allowed RSSI difference (expressed in dB) between two consecutive signal samples. AA must be expressed as a

infrastructure unit for 10 seconds if there is more than the specified difference between the RSSI values of two consecutive signal samples.		positive value. Set AA to *0* to disable this feature.
NEW FM1200 Volo, FM3200-series, FM3500 Endo and FM4500-series radio transceivers only: Advanced rate controller flags.	`fluidity advanced-rc-opts flags AB`	Value AB is provided by Tech Support or R&D during the commissioning phase.
NEW FM3500 Endo and FM4500-series radio transceivers only Configure the MCS ranges for VHT channels.	`fluidity advanced-rc-opts vht-mcs-sets AC`	Value AC is composed of six different MCS ranges relating to VHT channels. These ranges define which MCSs can be chosen by the radio unit for transmitting at a specific RSSI level, as defined by the relative group set. This is valid for VHT channels with a channel width of 80 MHz.
NEW FM3500 Endo and FM4500-series radio transceivers only: Configure the MCS group indices for VHT channels.	`fluidity advanced-rc-opts vht-group-sets AD`	Value AD is composed of six different ranges of group index values used to populate the advanced rate controller table. Each group index represents a combination of channel width, stream number, and SGI/LGI. This is valid for VHT channels with a channel width of 80 MHz.
FM1200 Volo, FM3200-series, FM3500 Endo and FM4500-series radio transceivers only: Configure the MCS ranges for 20 MHz HT channels.	`fluidity advanced-rc-opts ht-mcs-sets AE`	Value AE is composed of six different MCS ranges relating to VHT channels. These ranges define which MCSs can be chosen by the radio unit for transmitting at a specific RSSI level, as defined by the relative group set. FM3500 Endo and FM4500-series radio transceivers only: this command is valid for HT channels with a channel width of 20 MHz. FM1200 Volo, FM3200-series and FM4200-series radio transceivers only: this command is valid for all HT channels.
NEW FM3500 Endo and FM4500-series radio transceivers only: Configure the MCS group	`fluidity advanced-rc-opts ht-20-group-sets AF`	Value AF is composed of six different ranges of group index values used to populate the advanced rate controller table. Each group index represents a

indices for HT channels.		combination of channel width, stream number, and SGI/LGI. This is valid for HT channels with a channel width of 20 MHz.
NEW FM3500 Endo and FM4500-series radio transceivers only: Configure the MCS ranges for 40 MHz HT channels.	`fluidity advanced-rc-opts ht-40-group-sets AG`	Value AG is composed of six different ranges of group index values. These ranges are used to populate the advanced rate controller (RC) table. Each group index represents a combination of channel width, stream number and SGI/LGI. This is valid for HT channels with a channel width of 20 MHz.
NEW FM1200 Volo, FM3200-series and FM4200-series radio transceivers only: Configure the group ranges for HT channels.	`fluidity advanced-rc-opts ht-group-sets AH`	Value AH is composed of six different ranges of group index values. These ranges are used to populate the advanced rate controller (RC) table. Each group index represents a combination of channel width, stream number and SGI/LGI. This is valid for all HT channels.
NEW FM1200 Volo, FM3200-series and FM4200-series radio transceivers only: Change the state of the advanced rate controller.	`fluidity state P`	Possible values for P are: • *load* (load an advanced rate controller state.) • *save* (save the current advanced rate controller state.) • *delete* (delete the previously saved rate controller state.) • *show* (show the current learning status of the advanced rate controller.)
Set the device's Fluidity pole-proximity settings.	`fluidity pole-prox Q`	Possible values for Q are: • *mode A* (referring to the device's pole-ban operational mode.) Possible values for A are: ○ *disable* (Disables pole-ban mode.) ○ *pole-ban* (Enables the classic pole-ban feature. This mode assumes that a single frequency is used for the ground base stations.) ○ *mf-mono* (If mono-directional antennas are installed, this enables multi-frequency pole-banning. This mode assumes that the ground base-station frequencies are staggered in ABABAB fashion.)

		○ *mf-bidi* (If bi-directional antennas are installed, this enables multi-frequency pole-ban. This mode assumes that the ground base-station frequencies are staggered in ABABAB fashion.) ○ *head-det* (Enables the automatic head-radio detection algorithm. If necessary, this is used in conjunction with *mf-bidi* and *mf-mono*.) • *threshold B* (The critical threshold at which the pole-ban function is triggered. Value B is entered in dB.) • *duration C* (The pole-ban proximity duration value. Value C is entered in milliseconds.) • *pb-pause D* (The pole-ban inhibition interval. Value D is entered in milliseconds.) • *pb-second-best-min-rssi E* (The minimum available RSSI needed from the second-best infrastructure unit to allow the pole-ban function to be triggered. Value E is entered in dB.) • *pb-second-best-max-ler* (The maximum LER percentage needed to revert the pole-ban). • *pb-second-best-max-per* (The maximum PER percentage needed to revert the pole-ban). • *delta F* (Used to enable selection of an automatic pole-ban threshold. The highest RSSI value is calculated based on the RSSI readings at each vehicle passage. If entered, value F will be used by the algorithm to subtract to the previously-calculated highest RSSI, to compute the ban threshold. To disable automatic threshold selection, set value F as -1.) • *pb-fixed-mcs G* (If pole-banning is prevented by the pb-second-best-min-rssi

		check, this setting specifies the fixed-rate modulation and coding schema that will be used for transmission between the currently connected devices.) Value G is expressed in ranges. Possible values for G are: ○ *0* to *9* (80 MHz channel width). ○ *0* to *7* (20 to 40 MHz channel width). ○ Alternatively, disable the feature by entering *-1*. • *mf-list H* (Value H is the list of frequencies to be used by the multi-frequency algorithm. A maximum of two frequency values can be entered.) • *mf-reset live* (reset the multi-frequecy algorithm.) • *clear-learning live* (clear all RSSI threshold learning data.)
Set the device’s on-board client connection setting. Note that this function requires TITAN to be installed and enabled.	`fluidity enforce-pws-master C`	Possible values for C are: • *enabled* (Forces edge devices behind multiple mobile units to be mapped to the pseudowires of the Principal unit. Used to manage the bootstrapping of mobile units at different times. • *disabled* (Mapping of edge devices to mobile Principal unit pseudowires is not enforced).
FM3500 Endo and FM4500-series radio transceivers only: Display a readout of the current state of the device’s Fluidity advanced rate controller.	`fluidity state D`	Possible values for D are: • *load* (load the current advanced rate controller state for viewing.) • *save* (save the current advanced rate controller state.) • *delete* (delete the rate controller state that was previously saved.) • *show* (show the current learning progress status of the advanced rate controller.)
NEW Enable or disable assignment of specific colors to improve the Fluidity handoff algorithm.	`fluidity color mode E`	Possible values for E are *disabled* or *enabled*.
NEW Assign specific colors	`fluidity color`	Parameter E represents the

within the Fluidity handoff algorithm.	`value E`	assigned color value. Possible values for E are: • *clear* • *1* • *2* • *3* • *4* • *5* • *6* • *7* • *p* (if this value is used, only one additional value can be present. This value is used to configure the infrastructure node as the 'painter'.)

8.9. Spanning tree settings

Configuration objective	CLI command	Parameter options
Enable or disable BPDU snooping.	`spanning-tree snoop Y`	Possible values for Y are *enable* or *disable*.
Set the device's BPDU forwarding setting.	`spanning-tree filter Z`	Possible values for Y are: • *0* (Pass. Use this setting if the unit must pass all data traffic, regardless of BPDU content.) • *1* (Auto. Use this setting if the unit must pass or prohibit data traffic based on relevant BPDU content.) • *2* (Stop. Use this setting if the unit must prohibit data traffic regardless of BPDU content.)
Set the device's BPDU link guard setting.	`spanning-tree link-guard A`	Value A is the link guard time, expressed in seconds. This is extra time, added to the standard Principal election interval when the device's Ethernet port status changes.

8.10. Intra-car settings

Configuration objective	CLI command	Parameter options
Enable the Intra-car function.	`intra-car id W`	Value W must be a natural number of at least 1. This activates the Intra-car function and assigns the local transceiver unit its Car ID number (a unique identity number that distinguishes the unit from all other units in the same Intra-car network).
Set the minimum RSSI required to pair with another Intra-car unit.	`intra-car rssi-min X`	Value X is the minimum RSSI required for pairing.
Set the RSSI threshold at which the unit will break connection	`intra-car rssi-delta Y`	Value Y is the minimum RSSI required to break connection

with the currently-connected Intra-car unit to pair with an Intra-car unit with a higher RSSI.		with the currently-connected unit and establish connection with a unit transmitting at a higher RSSI.
Disable the Intra-car function.	`intra-car disabled`	

8.11. Enabling transmission of oversized MPLS packets

Configuration objective	CLI command	Parameter options
Enable or disable transmission of MPLS packets of up to 9 000 bytes through the device Ethernet ports (standard packets are up to 1 518 bytes).	`jumbo-frames D`	Possible values for D are *enable* or *disable*. This setting should only be enabled if you experience problems with sending large packets across the backhaul network. Wirelessly-transmitted packets are not affected by this setting.

8.12. Show an engineering statistics summary

NOTE

The commands in this section can be used to produce statistics for a wireless transceiver if the transceiver is in *Mesh Point* mode or *Mesh End* mode. Statistics will not be produced if the transceiver is in *Bridge* mode.

Configuration objective	CLI command	Parameter options
Show an instantaneous summary of current engineering statistics for the device.	`eng-stats`	
Show a summary of engineering statistics for the device that is updated once per second.	`eng-stats refresh`	

8.13. Quality of Service settings

IMPORTANT

If you are not familiar with Quality of Service (QoS), Class of Service (CoS) and their management principles, refer to the *Cisco QoS Specification* document for detailed information.

Configuration objective	CLI command	Parameter options
Activate QoS processing.	`qos status E`	Possible values for E are *enable* or *disable*.
Specify the CoS re-mapping vector.	`qos cos-map F`	Value F is the CoS re-mapping vector. This is specified as an 8-value string (for example, *0 1 2 3 4 5 6 7* for transparent 1:1 mapping).
Activate per-CoS shaping.	`qos shaping G`	Possible values for G are *enable* or *disable*.
Specify the CoS shaping bitrate	`qos shaper-rates H`	Value H is the CoS shaping

for each CoS.		rate. This is specified as an 8-value string (for example, 1 2 3 4 5 6 7 8) for each CoS. Note that the sum of the rates cannot exceed the bandwidth limit of the bandwidth license installed on the device.
Specify the Type of Service (ToS) reading from VLAN tags.	`qos 8021p I`	Possible values for I are *enable* (forces ToS reading from VLAN tags) or *disable* (ToS data is read from the TOS/DSCP field in Layer-3 packets).

8.14. Remote authentication dial-in user service (RADIUS) settings

Configuration objective	CLI command	Parameter options
Activate RADIUS device authentication. If the device is a trackside-mounted Fluidity device, this parameter can be used to simultaneously activate RADIUS device authentication and enable RADIUS passthrough (communication between RADIUS-authenticated vehicle-mounted devices, and non-authenticated trackside-mounted devices).	`radius J`	Possible values for J are: • *enable* • *passthrough* (enables RADIUS communication for non-authenticated trackside Fluidity devices.) • *disable*
Specify the RADIUS server address.	`radius server K`	Value K is the IP address of the RADIUS server.
Specify the port number of the RADIUS server.	`radius port L`	Value L is the port number of the RADIUS server. The default value is *1812*.
Specify the RADIUS access password.	`radius secret M`	Value M is the RADIUS access password.
Specify the RADIUS authentication method.	`radius auth-method N O P`	If using a RADIUS authentication method that does **not** include an inner authentication method, value N is the chosen authentication method. Possible values for N are *mschapv2, md5, gtc, tls, ttls* or *peap*. If *ttls* or *peap* are specified, an inner authentication method **must** be specified. See the *Specify the RADIUS authentication method and inner authentication method (protocol-dependent)* row below for details.

		If TLS authentication must be used, see the *Specify RADIUS authentication using TLS* row below for details. Value O is the chosen RADIUS user name. Value P is the chosen RADIUS user password.

NEW Specify RADIUS authentication using TLS.	Command 1:
	`radius auth-method tls credentials O P`
	Command 2:
	`certificates A upload B C`
		In Command 1:
		• Value O is the chosen RADIUS user name.
		• Value P is the chosen RADIUS user password.
		If TLS authentication has been selected, upload a TLS security certificate using TFTP by entering Command 2 (left).
		• Possible values for A are:
		○ *client-key*
		○ *ca-cert*
		○ *client-cert*
		• Value B is the file name of the security certificate file.
		• Value C is the IP address of the TFTP server.

Specify the RADIUS authentication method and inner authentication method (protocol-dependent).	`radius auth-method Q R S inner-auth-method T`	If using TTLS or PEAP as the RADIUS authentication method, value Q is the chosen authentication method, and value T is the chosen inner authentication method. Possible values for Q are *ttls* or *peap*. Possible values for T are *mschapv2*, *md5* or *gtc*. Value R is the chosen RADIUS user name. Value S is the chosen RADIUS user password.
Specify the host name or IP address of a secondary RADIUS server.	`radius secondary-server U`	Value U is the IP address of a secondary RADIUS server.
Specify the port of a secondary RADIUS server to which the device must connect.	`radius secondary-port V`	Value V is the specified secondary RADIUS server port.
Specify the RADIUS server authentication time-out value.	`radius timeout W`	Value W is the specified RADIUS server authentication time-out in seconds.
Specify the number of attempts the device can make to switch from the primary RADIUS server to a backup RADIUS	`radius switch-attempts X`	Value X is the specified maximum number of authentication attempts the device can make to switch from

server, if the primary RADIUS server cannot be reached.		the primary RADIUS server to the backup RADIUS server.
Trigger an immediate authentication request from the device to the RADIUS server.	`radius send-request`	
Stop authentication requests to the designated RADIUS server if server authentication is not completed within a specified number of attempts.	`radius backoff-time Y`	Value Y is the specified maximum number of RADIUS server authentication attempts.
Set the RADIUS authentication validation or expiration time, in seconds.	`radius expiration Z`	Value Z is the specified expiration time in seconds. If RADIUS authentication cannot be completed within this time period, the authentication attempt will be abandoned.

8.15. Network Time Protocol settings

Configuration objective	CLI command	Parameter options
Synchronize the device's time settings with a chosen internet time server by activating network time protocol (NTP).	`ntp Q`	Possible values for Q are *enable* or *disable*.
Synchronize the device with a chosen primary NTP server.	`ntp server R`	Value R is the URL of the chosen primary NTP server.
Synchronize the device with a chosen backup NTP server.	`ntp server2 S`	Value S is the URL of the chosen secondary NTP server.
Set the designated time zone in which the device is located.	`ntp timezone T`	Value T is the local time zone. Composite names must be bracketed with double quotation marks. A typical example might read `"America/New York"`.
Set the time and date immediately, instead of waiting for the standard NTP setting period.	`ntp set`	

8.16. Virtual LAN settings

IMPORTANT

If you are unfamiliar with virtual LAN (VLAN) networks and their management principles, refer to the *Cisco VLAN specification* document for detailed information.

Configuration objective	CLI command	Parameter options
Activate VLAN capability.	`vlan status U`	Possible values for U are *enable* or *disable*.
Specify the management identification number of the VLAN (used to communicate with the device's operating system).	`vlan mgm-vid V`	Value V is the management VLAN identification number (integer != 0).
Specify the native identification number (the VLAN ID that is implicitly assigned to untagged	`vlan native-vid W`	Value W is the native VLAN identification number (integer).

packets received on trunk ports).		

8.17. Global Positioning System settings

> **IMPORTANT**
>
> These settings are only valid for FM3200 Mobi+GPS and FM4200 Mobi+GPS radio transceivers.

Configuration objective	CLI command	Parameter options
Activate GPS capability.	`gps X`	Possible values for X are *enable* or *disable*.
Show the status of the device's on-board GPS module.	`gps status`	

8.18. Layer 2 Transfer Protocol settings

Configuration objective	CLI command	Parameter options
Activate L2TP tunnel and WAN interface capability.	`l2tp status Y`	Possible values for Y are *enable* or *disable*.
Specify the device port that will be used as the physical L2TP WAN interface.	`l2tp interface Z`	Possible values for Z are *1* and 2. If the radio unit is equipped with two Ethernet ports: • Value *1* assigns the L2TP role to the power-over-Ethernet (PoE) port. • Value *2* assigns the L2TP role to the non-PoE port. If the radio unit is equipped with an Ethernet port and a fiber-optic (SFP) port: • Value *1* assigns the L2TP role to the SFP port. • Value *2* assigns the L2TP role to the LAN (Ethernet) port.
Specify the IP address, netmask and default gateway to use for the L2TP WAN.	`l2tp wan A B C`	Value A is the WAN interface IP address. Value B is the WAN interface netmask. Value C is the WAN interface default gateway.
Specify the Layer-3 maximum transmission unit (MTU) size used by the L2TP WAN.	`l2tp mtu D`	Value D is the maximum Layer-3 MTU size in bytes. The default MTU size is 1 480 bytes.
Specify the UDP transmission port to be used for L2TP encapsulation.	`l2tp port E`	Value E is the number of the specified UDP port for L2TP encapsulation. If IP encapsulation must be used instead, set value E to *0*.
Specify the maximum number of L2TP tunnels that can be created.	`l2tp max-tunnels-num F`	Value F is the configured number of L2TP tunnels. The maximum allowable number of

		tunnels is 99.
Specify the local L2TP tunnel ID number, the remote L2TP tunnel ID number, the WAN IP address of the remote peer, and the UDP port of the remote peer for L2TP encapsulation.	`l2tp add G H I J`	Note that values G, H, I and J cannot be entered separately. Value G is the local L2TP tunnel ID number. Value H is the remote L2TP tunnel ID number. Value I is the WAN IP address of the remote peer. Value J is the UDP port of the remote peer for L2TP encapsulation. If IP encapsulation must be used instead, set value J as *0*.
Delete a local L2TP tunnel.	`l2tp del K`	Value K is the identity number of the local L2TP tunnel to be deleted.

8.19. Simple Network Management Protocol settings

Configuration objective	CLI command	Parameter options
Enable or disable SNMP functionality.	`snmp A`	Possible values for A are *enable* or *disable*.
Specify the SNMP protocol version.	`snmp version B`	Possible values for A are *v2c* or *v3*.
Specify the SNMP v2c community ID number (SNMP v2c only).	`snmp community-id C`	Value C is the SNMP v2c community ID number.
Specify the SNMP v3 user name (SNMP v3 only).	`snmp username D`	Value D is the SNMP v3 user name.
Specify the SNMP v3 user password (SNMP v3 only).	`snmp password E`	Value E is the SNMP v3 user password.
Specify the SNMP v3 authentication protocol (SNMP v3 only).	`snmp auth-method F`	Possible values for F are *md5* or *sha*.
Specify the SNMP v3 encryption protocol (SNMP v3 only).	`snmp encryption G`	Possible values for G are *des* or *aes*. Alternatively, enter *none* if a v3 encryption protocol is not needed.
Specify the SNMP v3 encryption passphrase (SNMP v3 only).	`snmp secret H`	Value H is the SNMP v3 encryption passphrase.
Specify the SNMP periodic trap settings.	`snmp periodic-trap I`	Possible values for Y are *enable* or *disable*.
Specify the notification trap period for periodic SNMP traps.	`snmp trap-period J`	Value J is the notification trap period in minutes.
Enable or disable SNMP event traps.	`snmp event-trap K`	Possible values for Y are *enable* or *disable*.
Specify the SNMP NMS hostname or IP address.	`snmp nms-hostname L`	Value L is the hostname or IP address of the SNMP NMS.

8.20. Transport Layer Security settings

NOTE

Cisco hardware devices feature support for all versions of transport-layer security (TLS).

Configuration objective	CLI command	Parameter options
Show the versions of TLS that are supported by the device.	`tls`	
Restrict the device's TLS support capability to TLS 1.2 only.	`tls 1.2-only A`	Possible values for A are *enabled* or *disabled*. If the disabled command is executed, the device will support TLS 1.0, 1.1 and 1.2.

8.21. Device cloud-management settings

NOTE

For instructions on how to configure your Cisco device using the cloud-based RACER portal, refer to the *Cisco RACER configuration manual.*

Configuration objective	CLI command	Parameter options
Activate or deactivate Cisco RAdio Configuration EnviRonment (RACER) configuration capability.	`racer B`	Possible values for B are: • *online-cloud-managed* (the device will take its configuration settings from the cloud-based RACER profile that is assigned to it.) • *offline* (the device is disconnected from RACER and must be manually configured using the CLI, or its offline Configurator interface.)

8.22. MONITOR settings

NOTE

For instructions on how to do operational monitoring and gather statistics from your Cisco device using the MONITOR application, refer to the *Cisco Radio Monitoring Dashboard Configuration Manual.*

Configuration objective	CLI command	Parameter options
View the device's current Cisco Radio Monitoring Dashboard (MONITOR) connection status.	`monitor`	Possible values for L are *enable* or *disable*.
Disconnect the device from MONITOR.	`monitor detach`	Possible values for L are *enable* or *disable*.

Note that the device can be re-connected to MONITOR at any time, using the MONITOR application.		

8.23. PROFINET settings

Configuration objective	CLI command	Parameter options
Activate PROFINET packet transmission capability.	`profinet status L`	Possible values for L are *enable* or *disable*.

8.24. QNET settings

Configuration objective	CLI command	Parameter options
Activate QNET packet transmission capability.	`qnet status M`	Possible values for M are *enable* or *disable*.

8.25. CANBUS settings

Configuration objective	CLI command	Parameter options
Activate CANBUS packet transmission capability.	`canbus status A`	Possible values for A are *enable* or *disable*.

8.26. Link Layer Discovery Protocol settings

Configuration objective	CLI command	Parameter options
Activate LLDP capability.	`lldp B`	Possible values for B are *enable* or *disable*.
Enable or disable the link layer discovery protocol-data SNMP management information database.	`lldp snmp-mib C`	Possible values for C are *enable* or *disable*.
Show neighboring devices that are also LLDP-enabled.	`lldp neighbors`	

8.27. Multicast settings

Note the following points in respect of multicast capability:

- If the radio transceiver is in Mesh end mode, multicast routes can be added and deleted.
- If the radio transceiver is in Bridge mode, multicast capability can only be enabled or disabled.
- If the radio transceiver is in Mesh point mode, multicast capability is not available.

Configuration objective	CLI command	Parameter options
NEW Enable or disable multicast forwarding capability.	`multicast status D`	Possible values for D are *enable* or *disable*.
NEW Add a specified multicast destination group to the radio transceiver's forwarding table.	`multicast add multicast-group E destination-address F`	Value E is the multicast group address, with a possible range from *224.0.0.0* to *239.255.255.255*. You can also specify multicast network masks (such as *224.1.1.0/24*). Note that if the Prodigy 1.0 protocol is being used, network masks are ignored.

		Value F is the destination address, consisting of a device Mesh ID number in the format *5.a.b.c.* If needed: • The wildcard address *5.255.255.255* can be used to include all units within the mesh network. • The address *5.0.0.0* can be used to force each unit to send multicast traffic to the primary mesh end unit.
NEW Delete a specified multicast destination group from the radio transceiver's forwarding table.	`multicast del multicast-group E destination-address F`	Value E is the multicast group address, with a possible range from *224.0.0.0* to *239.255.255.255*. You can also specify multicast network masks (such as *224.1.1.0/24*). Note that if the Prodigy 1.0 protocol is being used, network masks are ignored. Value F is the destination address, consisting of a device Mesh ID number in the format 5.a.b.c. If needed: • The wildcard address *5.255.255.255* can be used to include all units within the mesh network. • The address *5.0.0.0* can be used to force each unit to send multicast traffic to the primary mesh end unit.

8.28. Applet settings

Configuration objective	CLI command	Parameter options
NEW Edit applets within the radio transceiver's firmware.	`edit V`	Value V is the applet name. This command will shift the radio transceiver's firmware to applet editing mode. Additional commands available when in edit mode are: • *save* (saves the content of the current applet.) • *discard* (discards the content of the current applet.) • *clear* (clears the content of the current applet.)
NEW List all applets contained in the radio transceiver's firmware.	`applet list`	
NEW Show an activity log for all applets contained in the radio	`applet log`	

transceiver's firmware.		
NEW Show the specified applet.	`applet show W`	Value W is the applet name.
NEW Delete the specified applet.	`applet delete X`	Value X is the applet name.
NEW Execute the specified applet.	`applet exec Y`	Value Y is the applet name.
NEW Trigger the specified applet under certain circumstances.	`applet trigger Z`	Possible values for Z are: • *color A B*: trigger the applet in the event of the specified color event. Value A is an unsigned integer. Value B is the applet name. • *clear color C*: remove the specified color binding from the applet. Value C is an unsigned integer. • *show*: show a list of all triggers that are currently configured to trigger the applet.

8.29. Device firmware upgrade settings

These settings allow you to upgrade the firmware of the connected Cisco device using trivial file transfer protocol (TFTP).

Configuration objective	CLI command	Parameter options
Specify the IP address of the TFTP server containing the needed firmware image.	`tftp-fw-upgrade tftp-server D`	Value D is the IP address of the TFTP server.
Specify the file name of the needed firmware image.	`tftp-fw-upgrade upgrade-fw-image E`	Value E is the file name of the needed firmware image.
Enable or disable automated firmware upgrades.	`tftp-fw-upgrade automatic-upgrade F`	Possible values for F are *enable* or *disable*.
Specify the periodic interval at which the device checks for the presence of a newer firmware upgrade package.	`tftp-fw-upgrade check-period G`	Value G is the automatic upgrade check period in hours.
Force an immediate check for a newer firmware upgrade package.	`tftp-fw-upgrade check-now`	

8.30. Remote tech-support setting

⚠ **CAUTION**

Improper use of this setting may cause a security weakness.

It is strongly recommended that this setting is only enabled if requested by Cisco Technical Support, and disabled immediately after use.

Configuration objective	CLI command	Parameter options
Activate elevated-access capability for Cisco remote technical support.	`support-privileges N`	Possible values for N are *enable* or *disable*.

8.31. Enabling a CLI session time-out

Configuration objective	CLI command	Parameter options
NEW Specify an 'inactive' time period after which, if user activity is still not detected within the CLI console, the current user will automatically be logged out.	`session-timeout O`	Value O is the specified 'inactive' time period in minutes after which the current user will automatically be logged out. Possible values for O are: • *1* to *35791* (i.e. a maximum inactive period of 596 hours.) • *0* (time-out option disabled.)

8.32. Exit the command-line interface console

Configuration objective	CLI command	Parameter options
Exit the command-line interface console.	`exit`	

9. APPENDIX 1: CLI COMMAND RESULTS

This section describes how to understand and interpret the feedback given by the Cisco command-line interface (CLI) under specific circumstances.

9.1. Interpreting # eng-stats output

The table below shows the CLI output for # eng-stats.

Kbps:	Total	Rx	Tx
LAN:	0	0	0
WLAN:	100	72	28

Fluidity role: master vehicle id 142186476

static 5.0.147.3 [00:F1:CA:80:93:03]	mobile 5.0.41.57 [00:F1:CA:80:29:39]	snr 47	rssi -49	handoff 1486754405.001680979	time 1	acq 0	
static 5.0.147.3 [00-F1-CA-80-93-03]	mobile 5.0.41.57 [00-F1-CA-80-29-39]		rssi 47				updated 11
static 5.0.88.123 [00-F1-CA-80-58-7B]	mobile 5.0.41.57 [00-F1-CA-80-29-39]		rssi 46				updated 11

WLAN Rx:

00:F1:CA:80:93:03	rate 162	mcs 12	mcs-flags 1	snr 45	rssi -51	received 433	evm 21 26
00:F1:CA:80:58:7B	rate 54	mcs 0	mcs-flags 0	snr 46	rssi -50	received 115	evm 0 0

WLAN Tx:

00:F1:CA:80:93:03	rate 108	mcs 5	mcs-flags 1	sent 1134	failed 0	retries 16	LER 1%	PER 0%

The results shown in the table above are interpreted as follows:

Kbps:	Total	Rx	Tx
LAN:	0	0	0
WLAN:	100	72	28

The section above shows the real-time transmission and receiving rates of the wireless and LAN interfaces.

Fluidity role: master vehicle id 142186476

The section above shows the role of the Cisco device being interrogated. This example is a Principal vehicle unit, with unit ID number 142186476.

static 5.0.147.3 [00:F1:CA:80:93:03]	mobile 5.0.41.57 [00:F1:CA:80:29:39]	snr 47	rssi -49	handoff 1486754405.001680979	time 1	acq 0	
static 5.0.147.3 [00-F1-CA-80-93-03]	mobile 5.0.41.57 [00-F1-CA-80-29-39]		rssi 47				updated 11
static 5.0.88.123 [00-F1-CA-80-58-7B]	mobile 5.0.41.57 [00-F1-CA-80-29-39]		rssi 46				updated 11

In the section above:

- Radio unit 5.0.147.3 (first row) currently has access to radio coverage from two APs (which are also Cisco radio units).
- The first line shows the access point (AP) to which the device being interrogated is currently connected AP.

- The second and third lines show other available APs and the status of those APs.
- The information in the time 1 cell shows that a time of 1ms was taken to create the new MPLS tunnel.
- The information in the acq 0 cell shows a connection acquisition time of 0ms. In other words, the vehicle radio took 0ms to connect to the wireless infrastructure radio from outside the coverage zone.
- The information in the handoff cell shows a timestamp at which the handoff occurred of 1486754405.001680979.
- The information in the updated cell shows the timestamp at which the last control packet was received from the connected AP.

WLAN Rx:

00:F1:CA:80:93:03	rate 162	mcs 12	mcs-flags 1	snr 45	rssi -51	received 433	evm 21 26
00:F1:CA:80:58:7B	rate 54	mcs 0	mcs-flags 0	snr 46	rssi -50	received 115	evm 0 0

WLAN Tx:

00:F1:CA:80:93:03	rate 108	mcs 5	mcs-flags 1	sent 1134	failed 0	retries 16	LER 1%	PER 0%

The tables above show the physical status of the wireless TX (transmission) connection and RX (reception) connection:

- rate shows the data transfer rate in Mbps.
- SNR shows the signal-to-noise ratio.
- RSSI shows the received signal strength in decibel-milliwatts.
- LER shows the link error rate.
- PER shows the packet error rate.

Ethernet 1 role:	ingress/egress
Ethernet 2 role:	Down

The table above shows the role of the radio unit's Ethernet ports:

- If a Down result is shown, the port is not connected.
- If a mesh result is shown, the port allows only MPLS packets.
- If an ingress/egress mesh result is shown, the port allows all types of data packets.

9.2. Interpreting # mpls output

NOTE

The table heading will be *layer 2* if the radio unit is operating in MPLS layer 2 (single subnet).

The table heading will be *layer 3* if the radio unit is operating in MPLS layer 3 (routed subnets).

layer 2		
local_gw 5.0.88.123	global_gw 0.0.0.0	pwlist { }

mobility true	vehicle_id 142186476	v2v_handoff 0		v2v_pws false		static_pws { 0.0.0.0 }
lsps 2						
<5.0.41.57 5.0.88.123 2125987507> ESTABLISHED		ftn 3	ilm 102002	pim 53.380379788	ka 0	{ 5.0.41.57 5.0.88.123 }
<5.0.41.57 5.0.147.3 1661637949> ESTABLISHED		ftn 1	ilm 102000	pim 53.380420781	ka 0	{5.0.41.57 5.0.88.123 5.0.147.3 }

The table above shows the CLI output for # mpls with the radio unit in layer 2 operating mode:

- The local_gw cell contains the Cisco Mesh ID number of the primary Mesh End unit with the lowest Mesh ID of all Mesh-end units connected to the network.
- The global_gw cell contains the DNS address of the global gateway. Note that this cell is only applicable if the unit is configured for MPLS layer 3.
- The mobility cell will read true if the unit is set as a mobile unit, and false if it set as a wayside unit.
- The vehicle_id cell contains the current vehicle ID hash number.
- The v2v_handoff cell will read 0 if vehicle-to-vehicle handoff is not enabled, and 1 if it is enabled.
- The v2v_pws cell will read true if vehicle-to-vehicle pseudo-wires are enabled (through the wireless backbone), and will read false if pseudo-wires are not enabled.
- The static_pws cell contains information regarding manually-configured pseudo-wires.
- The lsps2 cell contains information regarding pseudo-wires that have been established between the local unit and other radio units that are part of the network:
  - The example above shows that pseudo-wires have been established between the local unit (mesh ID 5.0.41.57) and units 5.0.88.123 and 5.0.147.3.
  - The ftn cell contains the forwarding table entry index.
  - The ilm cell contains the incoming label mapping entry index.
  - The pim cell contains the flag indicating the status of the pseudowire. m stands for mobile, and – stands for infrastructure.
  - The cells containing Mesh ID numbers bounded by { } indicate the relevant pseudo-wire path.

9.3. Interpreting # mpls vbr show output

The table below shows the CLI output for # mpls vbr show.

40-36-5A-00-58-7B	192.168.0.10	5.0.88.123
40-36-5A-00-93-03	192.168.0.15	5.0.147.3

The virtual bridge shows the REMOTE devices behind each remote radio, as seen through ARP requests.

10. NOTICES AND COPYRIGHT

⚠ **WARNING**

Installation of Cisco hardware devices and their supporting infrastructure must be done by suitably qualified personnel only. In some countries, installation by a certified electrician may be required.

Cisco hardware installations must comply with all applicable local legislation.

⚠ **WARNING**

To avoid danger from non-ionizing radiation and/or electric shock and/or high-intensity laser or LED light sources, be sure to install the unit only in a location with restricted access.

⚠ **WARNING**

To avoid danger from electric shock, do not expose the unit to water or high humidity if the unit is powered ON, or if any access covers have been removed from the unit enclosure. Do not place liquid-filled objects on or above the unit.

12. NOTICES AND COPYRIGHT

NOTICE TO THE USER

Cisco Systems Inc provides no warranty with regard to this manual, software or other information contained herein, and hereby expressly disclaims any implied warranties of merchantability or fitness for any particular purpose with regard to this manual, the software or such other information. In no event shall Cisco Systems Inc be held liable for any incidental, consequential or special damages, whether based on tort, contract or otherwise, arising out of or in connection with this manual, the software or other information contained herein, or use thereof.

Cisco Systems Inc reserves the right to make any modification to this manual or the information contained herein at any time, without notice. The software described herein may also be governed by the terms of a separate end-user license agreement.

Cisco is a registered trademark of Cisco Systems Inc.
MeshWizard, EasyMesh, FMQuadro, FluidThrottle, VOLO, Fluidity, Virtual Gig, ENDO and MOBI are trademarks of Cisco Systems Inc. Microsoft, Windows, Internet Explorer and Microsoft Edge are registered trademarks of the Microsoft Corporation in the United States and/or other countries.

Ethernet is a registered trademark of the Xerox Corporation.

Adobe and Flash Player are registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

All other brands and product names that appear in this document are trademarks or registered trademarks of their respective owners.

11. CISCO END-USER LICENSE AGREEMENT

11.1. Preamble

This License Agreement strictly prohibits you from using the Cisco Firmware on any device other than a Cisco Device. You are also prohibited from removing or modifying any Cisco copyright notice, trademark or user interface of the Cisco Firmware or any Cisco Device.

The Cisco Firmware is copyright-protected material under United States and international copyright and other applicable laws. Unauthorized copying, use or modification of any part of this firmware, or violation of the terms of this Agreement, will be prosecuted to the maximum extent allowable under law.

11.2. Notice

This is an agreement between you and Cisco Systems Inc (hereafter known as 'Cisco').

You must read and agree to the terms of this firmware license agreement (hereafter known as the 'agreement') before any Cisco firmware can be downloaded, installed or used. By clicking the 'Accept' button on any Cisco firmware download webpage, or by downloading, installing or using Cisco firmware and/or by using any Cisco device running Cisco firmware, you are agreeing to be bound by the terms and conditions of this agreement. If you do not agree with the terms and conditions of this agreement, then you should not download, install or use any Cisco firmware, and you agree to forego any implied or stated rights to download, install or use Cisco firmware.

11.3. Definitions

For the purpose of this Agreement, the following terms shall have the following meanings:

'Open Source Software' means any software or software component, module or package that contains, or is derived in any manner (in whole or in part) from, any software that is distributed as free software, open source software or similar licensing or distribution models, including, without limitation, software licensed or distributed under any of the following licenses or distribution models, or licenses or distribution models similar to any of the following: (a) GNU's General Public License (GPL) or Lesser/Library GPL (LGPL); (b) the Artistic License (e.g., PERL); (c) the Mozilla Public License; (d) the BSD License; and (e) the Apache License;

'Cisco Device' means a Cisco networking device that you purchase or otherwise rightfully acquire; 'Cisco Firmware' means the firmware in object code form made available by Cisco for Cisco Devices; and

'You' and 'Your' mean the company, entity or individual who owns or otherwise rightfully acquires the Cisco Device into which the

Cisco Firmware will be incorporated.

11.4. License grant

Cisco grants you a non-exclusive, non-transferable license to use a copy of the Cisco Firmware and accompanying documentation and any updates or upgrades thereto provided by Cisco according to the terms set forth below. You are authorized by this license to use the Cisco Firmware in object code form only and solely in conjunction with applicable and permitted Cisco-branded products and/or services and in accordance with the applicable documentation. You are granted a limited and non-exclusive license (without the right to sublicense)
to use the software solely for the Cisco Devices that you own and control, and solely for use in conjunction with the Cisco Firmware.

11.5. Uses and restrictions on use

You may:
(a) download and use Cisco Firmware for use in Cisco Devices, and make copies of the Cisco Firmware as reasonably necessary for such use, provided that you reproduce, unaltered, all proprietary notices that exist on or in the copies.
You may not, and shall not permit others to:
(a) use the Cisco Firmware on any devices or products that are not owned by you or your business organization;
(b) use the Cisco Firmware on any non-Cisco Devices;
(c) copy the Cisco Firmware (except as expressly permitted above), or copy the accompanying documentation;
(d) modify, translate, reverse engineer, decompile, disassemble or otherwise attempt (i) to defeat, avoid, bypass, remove, deactivate, or otherwise circumvent any software protection mechanisms in the Cisco Firmware, including without limitation any such mechanism used to restrict or control the functionality of the Cisco Firmware, or (ii) to derive the source code or the underlying ideas, algorithms, structure or organization from the Cisco Firmware (except that the foregoing limitation does not apply to the extent that such activities may not be prohibited under applicable law); or
(e) distribute, rent, transfer or grant any rights in the Cisco Firmware or modifications thereof or accompanying documentation in any form to any person without the prior written consent of Cisco. (f) remove any Cisco copyright notice or Cisco branding from the Cisco Firmware or modify any user interface of the Cisco Firmware or Cisco Device.
Cisco Devices must be properly installed and they are sold for installation by a professional installer only. Cisco Devices must be installed by a professional installer of wireless networking products certified by Cisco and they are not designed for installation by the general public. It is your responsibility to follow local country regulation including operation within legal frequency channels, output power, and

Dynamic Frequency Selection (DFS) requirements. You are responsible for keeping the devices working according to these rules.
(g) The Cisco Firmware contain technological protection or other security features designed to prevent unauthorized use of the Cisco Firmware, including features to protect against use of the Cisco Fimrware beyond the scope of the license granted herein or in a manner prohibited herein. You agree that you shall not, and shall not attempt to, remove, disable, circumvent or otherwise create or implement any workaround to, any such copy protection or security features.
This license is not a sale. Title and copyrights to the Cisco Firmware, and any copy made by you, remain with Cisco and its suppliers. Unauthorized copying of the Cisco Firmware or the accompanying documentation, or failure to comply with the above restrictions, will result in automatic termination of this license and will make other legal remedies available to Cisco.

11.6. Open-source software

You hereby acknowledge that the Cisco Firmware may contain Open Source Software. You agree to review any documentation that accompanies the Cisco Firmware or is identified in the documentation for the Cisco Firmware in order to determine which portions of the Cisco Firmware are Open Source Software and are licensed under an Open Source Software license. To the extent that any such license requires that Cisco provide you with rights to copy, modify, distribute or otherwise use any Open Source Software that are inconsistent with the limited rights granted to you in this Agreement, then such rights in the applicable Open Source Software license shall take precedence over the rights and restrictions granted in this Agreement, but solely with respect to such Open Source Software. You acknowledge that the Open Source Software license is solely between you and the applicable licensor of the Open Source Software. You shall comply with the terms of all applicable Open Source Software licenses, if any.
Copyrights to the Open Source Software are held by the copyright holders indicated in the copyright notices in the corresponding source files or as disclosed at www.cisco.com.

11.7. Termination

This license will continue until terminated. Unauthorized copying of the Cisco Firmware or failure to comply with the above restrictions will result in automatic termination of this Agreement and will make other legal remedies available to Cisco. This license will also automatically terminate if you go into liquidation, suffer or make any winding-up petition, make an arrangement with your creditors, or suffer or file any similar action in any jurisdiction in consequence of debt.
Furthermore, Cisco may immediately terminate this Agreement if (i) you fail to cure a breach of this Agreement (other than a breach pursuant

to Cisco intellectual property rights) within thirty (30) calendar days after its receipt of written notice regarding such breach, or (ii) you breach any Cisco intellectual property right. Upon termination of this license for any reason, you agree to destroy all copies of the Cisco Firmware. Any use of the Cisco Firmware after termination is unlawful.

11.8. Feedback

You may provide suggestions, comments or other feedback ('Feedback') with respect to Cisco Firmware, and Cisco Devices. Feedback, even if designated as confidential by you, shall not impose any confidentiality obligations on Cisco. You agree that Cisco is free to use, disclose, reproduce, license or otherwise distribute and exploit any Feedback provided by you as Cisco sees fit, entirely without obligation or restriction of any kind on account of intellectual property rights, or otherwise.

11.9. Consent to use of data

You acknowledge and agree that Cisco may, directly or indirectly through the services of third parties, collect and store information regarding the use and performance of the Cisco Firmware and Cisco Devices, and about equipment through which it otherwise is accessed and used.

You further agree that Cisco may use such information for any purpose related to any use of the Cisco Firmware and Cisco Devices by you, including, without limitation, improving the performance of the Cisco Firmware or developing updates and verifying your compliance with the terms of this Agreement and enforcing Cisco's rights, including all intellectual property rights in and to the Cisco Firmware.

Cisco shall have the right to collect and analyze data and other information relating to the provision, use and performance of various aspects of the Cisco Firmware and Cisco Devices and related systems and technologies ('Data'), and you give Cisco the right to use and disclose such Data (during and after the term of this Agreement) in accordance with Cisco's Privacy Policy. If you choose to allow diagnostic and usage collection, you agree that Cisco and its subsidiaries and agents may collect, maintain, process and use diagnostic, technical, usage and related information, including but not limited to unique system or hardware identifiers, information about your device, system and software, that is gathered periodically to provide and improve Cisco's products and services, facilitate the provision of software updates, product support and other services to you (if any) related to Cisco products, and to verify compliance with the terms of this license. Cisco may use this information, as long as it is collected in a form that does not personally identify you, for the purposes described above.

To enable Cisco’s partners and third-party developers to improve their software, hardware and services designed for use with Cisco products, Cisco may also provide any such partner or third-party developer with a subset of diagnostic information that is relevant to that partner’s or developer’s software, hardware and/or services, as long as the diagnostic information is in a form that does not personally identify you.

11.10. Warranty disclaimer

Cisco Firmware, including without limitation any open source software, any Cisco Device, and any accompanying documentation are provided 'As is', and Cisco and its suppliers make, and you receive, no warranties or conditions, whether express, implied, statutory or otherwise, or in any communication with you, and Cisco and its suppliers specifically disclaim any implied warranty of merchantability, satisfactory quality, fitness for a particular purpose, or non-infringement and their equivalents.

Cisco does not warrant that the operation of the Cisco Firmware will be uninterrupted or error-free or that the Cisco Firmware will meet your specific requirements. You acknowledge that Cisco has no support or maintenance obligations for the Cisco Firmware.

11.11. Limitation of liability

Except to the extent that liability may not by law be limited or excluded, in no event will Cisco or its suppliers be liable for loss of, or corruption to data, lost profits or loss of contracts, cost of procurement of substitute products or other special, incidental, punitive, consequential or indirect damages arising from the supply or use of the Cisco Firmware, howsoever caused and on any theory of liability (including without limitation negligence).

This limitation will apply even if Cisco or an authorized distributor or authorized reseller has been advised of the possibility of such damages, and notwithstanding the failure of essential purpose of any limited remedy. In no event shall Cisco's or its suppliers' or its resellers’ liability exceed five hundred United States dollars (US$500). You acknowledge that this provision reflects a reasonable allocation of risk.

11.12. Exclusion of liability for emergency services

Cisco does not support, nor are the services intended to support or carry, emergency calls to any emergency services, including but not limited to 911 dialing.

Cisco will not be held responsible for any liability or any losses, and you, on behalf of yourself and all persons using the services through the licensed products, hereby waive any and all such claims or causes of action for losses arising from, or relating to, any party’s attempts to contact emergency service providers using the licensed products, including but not limited to calls to public safety answering points.

Cisco will not be held liable for any losses, whether in contract, warranty, tort (including negligence), or any other form of liability, for any claim, damage, or loss, (and you hereby waive any and all such claims or causes of action), arising from or relating to your (i) inability to use the services to contact emergency services, or (ii) failure to make additional arrangements to access emergency services.

The parties expressly acknowledge and agree that Cisco has set its prices and entered into this agreement in reliance upon the limitations of liability and disclaimers of warranties specified herein, which allocate the risk between Cisco and the end user and form a basis of the bargain between the parties.

11.13. Export control

You acknowledge that the Cisco Devices, Cisco Firmware, documents, technical data, and any other materials delivered under this Agreement are subject to U.S. export control laws, and may also be subject to export or import regulations in other countries. You agree to comply strictly with these laws and regulations and acknowledge that you have the responsibility to obtain any licenses to export, re-export, or import as may be required after delivery to you. You shall not, directly or indirectly, export, re-export or release the Cisco Devices and Cisco Firmware, to, or make the Cisco Devices and Cisco Firmware accessible from any jurisdiction or country to which export, reexport or release is prohibited by law, rule or regulation. In particular, but without limitation, the Cisco Devices and Cisco Firmware may not be exported or re-exported (a) into any U.S. embargoed countries or (b) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Department of Commerce Denied Person's List or Entity List.

By using the Cisco Devices and Cisco Firmware, you represent and warrant that you are not located in any such country or on any such list. You acknowledge and agree that you shall strictly comply with all applicable laws, regulations and rules, and complete all required undertakings (including obtaining any necessary export license or other governmental approval), prior to operating the Cisco Devices and Cisco Firmware, or exporting, re-exporting, releasing or otherwise making the Cisco Devices and Cisco Firmware available outside the U.S. You acknowledge and agree that Cisco has no further responsibility after the initial delivery to you, and you hereby agree to indemnify and hold Cisco harmless from and against all claim, loss, liability or damage suffered or incurred by Cisco resulting from, or related to your failure to comply with all export or import regulations.

11.14. General

This Agreement shall not be governed by the 1980 U.N. Convention on Contracts for the International Sale of Goods. Rather, this Agreement shall be governed by the laws of the State of Illinois, including its Uniform Commercial Code, without reference to conflicts of laws principles. You agree to the exclusive jurisdiction and venue of the State and Federal courts in Illinois, United States.

This Agreement is the entire agreement between you and Cisco, and supersedes any other communications or advertising with respect to the Cisco Firmware and accompanying documentation. If any provision of this Agreement is held invalid or unenforceable, such provision shall be revised to the extent necessary to cure the invalidity or unenforceability, and the remainder of the Agreement shall continue in full force and effect.

This Agreement and all documents, notices, evidence, reports, opinions and other documents given or to be given under this Agreement (collectively with this Agreement, 'Documents') are and will be written in the English language only. In the event of any inconsistency between any Document in the English language and any translation of it into another language, the English-language Document shall prevail. If you are acquiring the Cisco Firmware on behalf of any part of the U.S. Government, the following provisions apply: The Cisco Firmware and accompanying documentation are deemed to be 'commercial computer software' and 'commercial computer software documentation', respectively, pursuant to DFAR Section 227.7202 and FAR 12.212(b), as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Cisco Firmware and/or the accompanying documentation by the U.S. Government or any of its agencies shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement. Any technical data provided that is not covered by the above provisions is deemed to be 'technical data-commercial items' pursuant to DFAR Section 227.7015(a). Any use, modification, reproduction, release, performance, display or disclosure of such technical data shall be governed by the terms of DFAR Section 227.7015(b).

Cisco is a trademark of Cisco, LLC in the United States and worldwide.

12. CONTACT US

Worldwide Headquarters:

81 Prospect Street
Brooklyn, New York 11201
United States of America
Tel. +1 (617) 209 -6080
Fax. +1 (866) 458-1522
info@fluidmesh.com
Technical Support desk: support@fluidmesh.com
www.cisco.com

Regional headquarters for Europe, the Middle East and Africa:

Tel. +39 02 0061 6189

Regional headquarters for the United Kingdom:

Tel. +44 2078 553 132

Regional headquarters for France:

Tel. +33 1 82 88 33 6

Regional headquarters for Australia and New Zealand:

Tel: +61 401 747 403