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

Command-line interface user manual

(Formerly Fluidmesh)
Firmware versions 1.5.0 and 2.2.0 (Edition 1.9)

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 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 here. 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:

- 1.5.0 (FM1000 and first-generation FM10000 Gateway devices)
- 2.2.0 (Second-generation FM10000 Gateway devices)

This manual may contain commands and/or command parameters that are being newly introduced as part of a hardware and/or 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 SecureCRT (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.) • NEW *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).
Set the time interval between sent ping packets.	`ping "-i C"`	Parameter C is the specified time interval between sent ping packets. Note that: • The time interval command and the specified time interval must be bounded by double quotation marks (see left for correct format). • The default ping packet time interval is one second. • If unicast flooding is enabled, there is no specified time interval between ping packets. • Only superusers may set ping packet intervals to 0.2 seconds or less.

8.9. 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.

8.1. 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.

8.2. 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.

8.3. 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.

8.4. 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 Mesh-end devices.	`mpls pw-set H`	Possible values for H are *all* or *mesh-end.*
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 Adjust the maximum allowed rate for ARP traffic. If ARP packets are received at a rate that exceeds the specified threshold value over a one-second interval, the packets will be dropped.	`mpls arp-limit rate N`	Value N is expressed in packets per second. Set N to *0* to disable this function.
NEW *Gen. 2 FM10000 Gateway only:* Adjust the ARP blocking grace period. If the maximum allowed ARP traffic rate (Value N, above) is exceeded for the amount of time specified by value O, all ARP traffic will be blocked for the amount of time specified by the ARP block-limit time (Value P, below).	`mpls arp-limit grace O`	Value O is expressed in milliseconds.
NEW *Gen. 2 FM10000 Gateway only:* Adjust the ARP block-limit time. This value specifies the amount of time for which ARP traffic arriving at more than the specified ARP traffic rate will be blocked.	`mpls arp-limit block P`	Value P is expressed in milliseconds. Set P to *0* to disable this function.

8.5. Address Resolution Protocol settings

Configuration objective	CLI command	Parameter options
Enable or disable transmission of gratuitous ARP packets following network topology changes.	`gratuitous-arp B`	Possible values for B are *enable* or *disable*.
Set a delay before transmission of gratuitous ARP	`gratuitous-arp delay C`	Value C is the delay period before transmission of

packets.		gratuitous ARP packets, expressed in milliseconds.

8.6. Operating Mode settings

Configuration objective	CLI command	Parameter options
Show the device's current operating mode.	`modeconfig`	
Set the device's current operating mode.	`modeconfig mode A`	Possible values for A are *gateway* or *meshend.*
Set the device's selected MPLS OSI layer.	`modeconfig layer B`	Possible values for B are *2* (OSI Layer-2) or *3* (OSI Layer-3).
Set the device's network passphrase.	`passphrase C`	Value C is the device's network passphrase.

8.7. 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.

8.1. 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 device.	`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 device.	`plugins remove C`	Value C is the name of the relevant plug-in license.

8.2. Showing the device model and firmware revision number

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

8.3. Showing the device mesh ID number

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

8.4. Fluidity settings

Configuration objective	CLI command	Parameter options
Enable or disable Fluidity functionality.	`fluidity status A`	Possible values for A are *enabled* or *disabled.*
Set the device's large-network optimization setting.	`fluidity lno B`	Possible values for B 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*).
Show a summary of the Fluidity network's settings and statistics.	`fluidity show`	
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).
NEW Enable or disable FM Quadro telemetry capability.	`fluidity fmquadro D`	Possible values for Y are *enable* or *disable*.

8.5. 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 Z 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.

8.6. 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 B`	Possible values for B 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.

8.7. Ethernet port settings

Configuration objective	CLI command	Parameter options
NEW View the link state of the physical Ethernet and SFP+ ports.	`ethernet`	
NEW *Gen. 2 FM10000 Gateway only:* Set the link state of the physical Ethernet and SFP+ ports.	`ethernet link-aggregation C`	Possible values for D are: • *backup* (The first physical port to be connected is assigned the role of Primary port. If the Primary port is disconnected or fails, the next port will be used. This progression takes place along all

		physical ports on the device.) • *broadcast* (Use all connected physical ports.)
NEW *All FM10000 Gateways:* Enable or disable the device's physical Ethernet and SFP+ ports.	`ethernet D E`	Possible values for D are *enable* or *disable*. Parameter E is a list of the device's physical interface ports, separated by spaces. • For SFP ports, the syntax must be *sfp1…n* • For Ethernet ports, the syntax must be *eth1…n* All interfaces of a certain bridge can be specified using the syntax *sfpX/** or *ethX/**. Ranges of interfaces can be specified using the syntax *sfpX/A-B* or *ethX/A-B.*
NEW *Gen. 2 FM10000 Gateway only:* Show a list of the device's physical Ethernet and SFP+ ports.	`ethernet status E`	Parameter E is a list of the device's physical interface ports, separated by spaces. • For SFP ports, the syntax must be *sfp1…n* • For Ethernet ports, the syntax must be *eth1…n* All interfaces of a certain bridge can be specified using the syntax *sfpX/** or *ethX/**. Ranges of interfaces can be specified using the syntax *sfpX/A-B* or *ethX/A-B.*
NEW Change the size of the Ethernet maximum transmission unit (MTU) for the device ports.	`ethernet mtu F`	Parameter F is the port MTU size setting in bytes. The value can be set between a minimum of 1530 and a maximum of 2000.

8.8. 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`	

8.9. 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 for each CoS.	`qos shaper-rates H`	Value H is the CoS shaping 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).

8.10. 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 server, if the primary RADIUS server cannot be reached.	`radius switch-attempts X`	Value X is the specified maximum number of authentication attempts the device can make to switch from 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.

8.11. Network Time Protocol (NTP) 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`	

8.12. 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 packets received on trunk ports).	`vlan native-vid W`	Value W is the native VLAN identification number (integer).

8.13. Layer 2 Transfer Protocol (L2TP) 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: • *1* assigns the L2TP role to the power-over-Ethernet (PoE) port. • *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: • 1 assigns the L2TP role to the SFP port. • 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.

8.14. Simple Network Management Protocol (SNMP) 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.

8.15. 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.

8.16. 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.)

8.17. 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. Note that the device can be re-connected to MONITOR at any	`monitor detach`	Possible values for L are *enable* or *disable*.

time, using the MONITOR application.		

8.18. PROFINET settings

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

8.19. QNET settings

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

8.20. CANBUS settings

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

8.21. 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`	

8.22. Multicast settings

Note the following points in respect of multicast capability:

- If the device is in Mesh-end mode, multicast routes can be added and deleted.
- If the device 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 device'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 device'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.

8.23. Managing the device's disk partitions

Configuration objective	CLI command	Parameter options
NEW *Gen. 2 FM10000 Gateway only:* Show the current status of the device's hard disk partitions.	`boot-image`	When this command is entered, the CLI will return a disk partition status update. A typical example might read: *Available partitions:* *Partition 1: ACTIVE, firmware 2.2.0* *Partition 2: INACTIVE, firmware 2.1.0*
NEW *Gen. 2 FM10000 Gateway only:* Specify the disk partition to be used at the next boot-up event.	`boot-image G`	Value G is the argument specifying the disk partition that will be used during the next boot-up event. As a typical example, booting from the disk image located on partition #2 would require the command *boot-image 2* followed by *reboot.*

8.24. 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`	
NEW *Gen. 2 FM10000 Gateway only:* Load a firmware upgrade package from a USB mass storage device.	`usb-fw-upgrade upgrade-fw-image H`	Value H is the file name of the image firmware to be uploaded and installed. Note that the relevant storage device must be formatted to FAT32, with at least 2 GB of free space. The unit will search the connected storage device for the specified firmware image and start the upgrade. The upgrade image file can take a few minutes to transfer, depending on the speed of the storage device. Do not disconnect the storage device or reboot the gateway unit until the file transfer is complete.

8.25. 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*.

8.26. 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.)

8.27. 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, re-export 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