COMMSCOPE®

OneCell®

Hardware Installation and Commissioning, RP5000 series

Release 4.0

Document Number: **913035**

Document Revision: **4.0.04**

Date: **June 2019**

Contents

PART 4 APPENDICES

Appendix A
Safety

Appendix B
Installation troubleshooting

Appendix C
Specifications

Appendix D
Field Replaceable Units

Appendix E
Cable installation and power separation guidelines

List of figures

List of tables

Document revision history

The following section lists documentation changes in *OneCell® Installation and Commissioning, RP5000* (913035) for R4.0, the release for RP5000 series devices.

Revision 4.0.04 (June 6, 2019)

- Appendix D, Field Replaceable Units
  - Added topic, Replacing RF modules on page D-48

Revision 4.0.03 (May 21, 2019)

- Chapter 1, CommScope OneCell® overview
  - Revised Baseband Controller physical ports on page 1-3, including Table 1-1 on page 1-4
- Chapter 5, Configuring the OneCell system
  - Revised Timing Source, Boundary Clock Interface Port in Table 5-2 on page 5-17
  - Added GPS Information bullet to Configuring the Baseband Controller manually on page 5-25
  - Revised Whitelist Configuration in Table 5-3 on page 5-26
- Chapter 6, Verifying the OneCell installation
  - Revised Verify the OneCell system installation on page 6-2
- Added Appendix A, Safety and Appendix D, Field Replaceable Units

Revision 4.0.02 (March 27, 2019)

- Revised procedures in Chapter 4, RP5100i installation

Revision 4.0.01 (March 13, 2019)

- Initial document release

About this document

This document provides the procedures for installing and configuring the Baseband Controller and Radio Points.

Audience

This document is written for computer hardware installers and administrators, network architects and business planners who are responsible for the planning and design of the CommScope OneCell deployment environment.

Purpose

This guide provides the information necessary for installing the OneCell hardware in the operator's network.

What you need to know

The reader should have a basic understanding of:

- Data networks
- LTE technology
- General telecommunications practices

Customer documentation

The following table lists available documents in the OneCell documentation suite.

Table 1. Customer documentation

Title	Contents
Device Management System documentation	
DMS Software Installation (913150)	Provides server hardware and software requirements, software installation, and other set-up and post-installation tasks required to support the DMS platform.
DMS Installation and Management Guide for OneCell® Devices (913152)	Provides procedures for installing service packs and AFU
DMS Software Management (913153)	Describes the DMS platform software upgrade procedures from the previous patch release to the current patch release and the DMS rollback and downgrade procedures from the current patch release to the previous patch release.
DMS Network Management Portal User Guide (913156)	Describes how to manage the OneCell network using the DMS.
DMS Device Management Portal User Guide for OneCell® Devices (913158)	Describes Device Management Portal features by menu items used by technical support personnel.
DMS Administration and Utilities Reference for OneCell® Devices (913155)	Describes how to operate, administer, and maintain the DMS device server for OneCell devices.
Troubleshooting the DMS Network (913161)	Describes how to maintain the DMS and identify, verify, and resolve problems in the device environment.
DMS Disaster Recovery (913162)	Describes how system administrators can recover the DMS servers after a disaster.
OneCell Device Management System Online Help	Provides context sensitive online help integrated in the DMS.
Baseband Controller and Radio Point documentation	
OneCell® Network Planning Guide (913023)	Describes main components of the OneCell system, high-level view of HW components, how do you engineer an in-building system, how do you determine RP locations, how to design in-building systems and how to determine Radio Point locations. Contains best practices for deployment, including when to use clustering, and how to manage capacity.

Table 1. Customer documentation

Title	Contents
OneCell® Installation and Commissioning (913025)	Includes detailed installation instructions for Baseband Controller and Radio Points hardware, planning the installation, physical install, how to configure the installation, commissioning the installation to service; verification tests after the installation.
OneCell® Administration (913026)	Contains enterprise-level monitoring and alarms.
OneCell® Troubleshooting (913022)	Covers common troubleshooting scenarios in deployed devices and troubleshooting methods.
OneCell® Deployment Guide (913028)	Contains the device network overview, including CommScope provided components and required components from other vendors, DMS overview, and device overview and requirements.
OM and KPI Reference for OneCell® Devices (913159)	Describes the operational measurements and key performance indicators for OneCell devices.

Conventions

This guide uses the following text conventions, as applicable.

Table 2. Conventions

Convention	Description
Syntax symbols	
< >	Enclose a required parameter or set of parameters. For example: **`>band-class <class>`** **`<class>`** is a required parameter.
[ ]	Enclose an optional parameter or set of parameters. For example: **`>activate image <version> [reboot]`** **`[reboot]`** is an optional parameter.

Table 2. Conventions

Convention	Description
|	Separates items on a list of parameters, only one of which can be used. For example: **`>channel-included <yes|no>`** A valid command is: **`>channel-included yes`**
Font usage	
`Bold input font`	Indicates text that must be entered exactly as shown. For example: Enter **`ping 192.23.10.12`**.
`Italic input font`	Indicates a variable parameter for which you must provide an actual value. For example: **`>authentication key <aukey>`** ***`<aukey>`*** is a variable parameter. A valid command is: **`>authentication key 9782503000`**
`Plain output font`	Indicates system output in a command line or system-generated file. For example: `IP address 192.23.10.12 is alive.`
`Italic output font`	Indicates a variable in system output in a command line or system-generated file. For example: `Installation of release <release> is complete.`
Plain italic font	Indicates file names, directory paths, book titles, chapter titles, and user accounts.
Bold font	Indicates text that appears on screen exactly as shown, for example, names of screens, names of buttons, items on menus, and items on pull down lists.
blue text	Indicates a hypertext link.
Other conventions	
>	Indicates graphical user interface (GUI) menu path. For example: Select **Edit** > **Add Network** to open the Add Network screen.

Notes, cautions, and warnings

NOTE

Notes provide additional information about the subject text.

CAUTION

Cautions indicate that procedures, if performed incorrectly, can cause equipment damage or data loss.

WARNING

Warnings indicate that procedures, if performed incorrectly, can harm you.

Part I: Overview and preparation

Chapter 1

CommScope OneCell® overview

This chapter contains a high level overview of the OneCell deployment and the OneCell components installed in the OneCell system.

Overview

OneCell is a revolutionary wireless system that can deliver the ultimate in wireless performance.

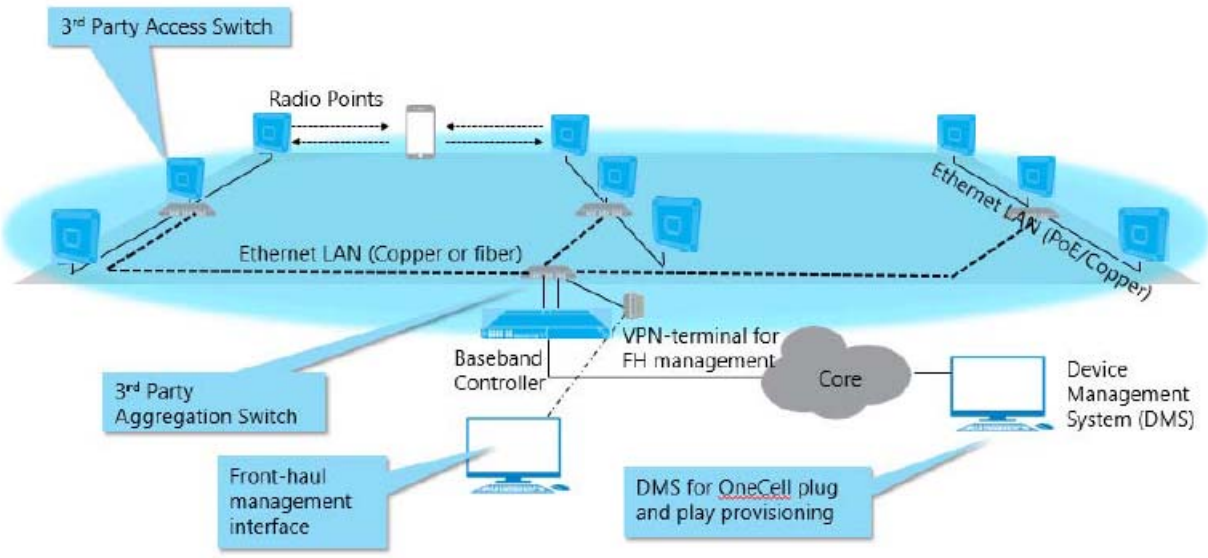
- It eliminates cell borders and handovers
- It can cover a large area with consistent user experience without any significant interference
- It can take advantage of multiple distributed radio points to deliver a stronger signal on both the downlink and the uplink
- It can deliver greater capacity through distributed (multi-user and single-user) MIMO and Coordinated Multipoint (CoMP)
- It has the flexibility to neutralize macro interference in co-channel small cell deployments
- It can be used to deliver unprecedented levels of capacity to hot spot areas by deploying radio points with overlapping coverage and enabling multi- user MIMO

In addition to these important benefits in user experience and data capacity, OneCell provides superior economics and investment protection, ease of deployment, support for multi-operator deployments.

CommScope OneCell system

OneCell is an in-building, enterprise solution for LTE that provides an in-building consistent signal. It operates as a wireless network with a single cell, called a Baseband Controller, over distributed Radio Points. Network operators benefit from the OneCell because they reduce the load on their infrastructure.

Figure 1-1. OneCell solution



OneCell hardware components

The OneCell hardware consists of the following components:

- Baseband Controller
  - — Baseband Controller Chassis
  - — Baseband Controller Module
  - — Power/Fan Unit (PFU)

Baseband Controller physical ports

The following ports are on the front panel of the Baseband Controller Module. Table 1-1 shows the port assignments. In addition, there is a connector used for the GPS antenna cable.

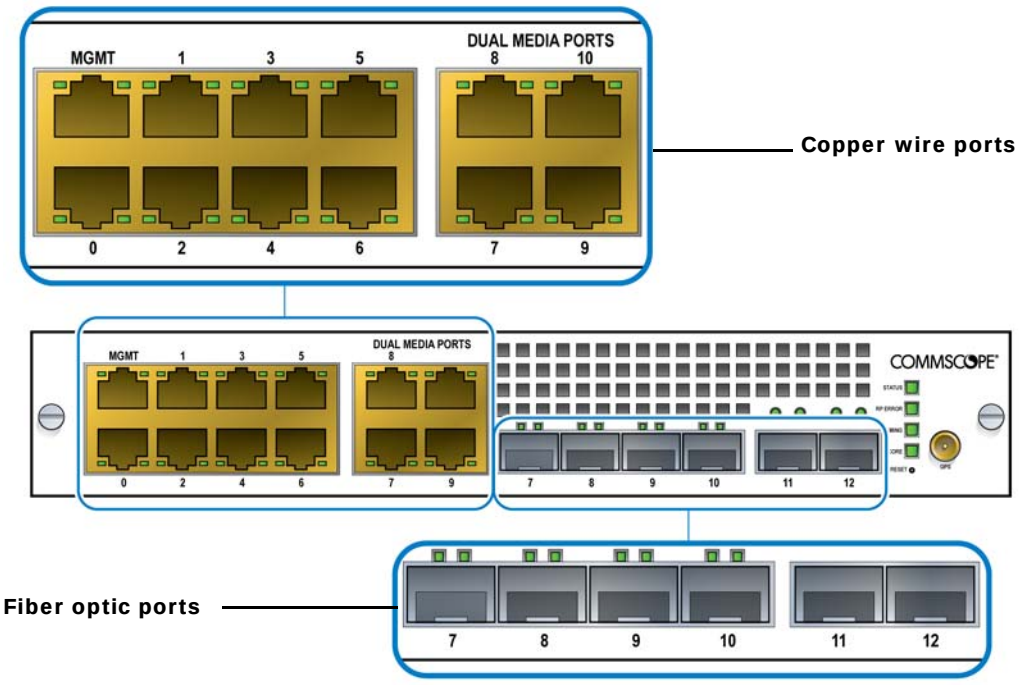
NOTE

For more detailed BC port information, see *OneCell® Network Planning Guide* (913023).

Table 1-1. Baseband Controller physical port assignments

Port Number	Description
MGMT	MGMT port to configure OneCell through the WebGUI
0	Not used
1-6	1 GB ports for IQ data connection between Baseband Controller and Radio Point (RP) through an Ethernet switch on copper cable
7	Boundary clock, IEEE1588 input dual media RJ45 or SFP port
8	Back haul dual media RJ45/SFP data port
9	Dual media RJ45/SFP port for front haul RP management, RP timing IEEE1588, Redundancy, High Availability
10	Dual media port provides 1588 timing/SOAP/XML to Radio Point (RP) units. Either this copper port or fiber port 10 (SFP not provided) is used to provide 1588 timing to RPs
11	10G/SFP+ fiber port for front-haul IQ data
12	Not used

Figure 1-2. Baseband Controller ports



Chapter 2

Preparing to install the OneCell system

This section has the steps to complete before starting the OneCell installation.

Overview

This document describes the OneCell installation and includes:

- Chapter 3, Baseband Controller installation
- Chapter 4, RP5100i installation
- Chapter 5, Ruggedized Radio Point Installation

Before installing the OneCell components

Before installing the OneCell components, the system integrator must plan the network for the topology that will be deployed. See *OneCell Network Planning Guide* (913023).

CommScope recommends that cables and switches be in place before installing the OneCell components. See Appendix E, Cable installation and power separation guidelines for more information.

Part II: OneCell component installation

Chapter 3

Baseband Controller installation

This chapter contains the Baseband Controller installation procedures, including chassis installation into a rack, Baseband Controller Module and Power/Fan Unit installation into the Baseband Controller Chassis and the cables required for a basic installation.

Preparing for Baseband Controller installation

Open the shipping box. It should have the components for one complete Baseband Controller Module:

- Baseband Controller Chassis – including four mounting screws
- Baseband Controller Module
- Power/Fan Unit (PFU)

The Baseband Controller is 1U high. Be sure there is enough room for the Baseband Controller in the rack.

Installing the Baseband Controller into a rack

The Baseband Controller can be installed in a 19-inch or 600mm rack. The Baseband Controller Chassis package contains two kits: one with 19-inch brackets and one with 600mm brackets.

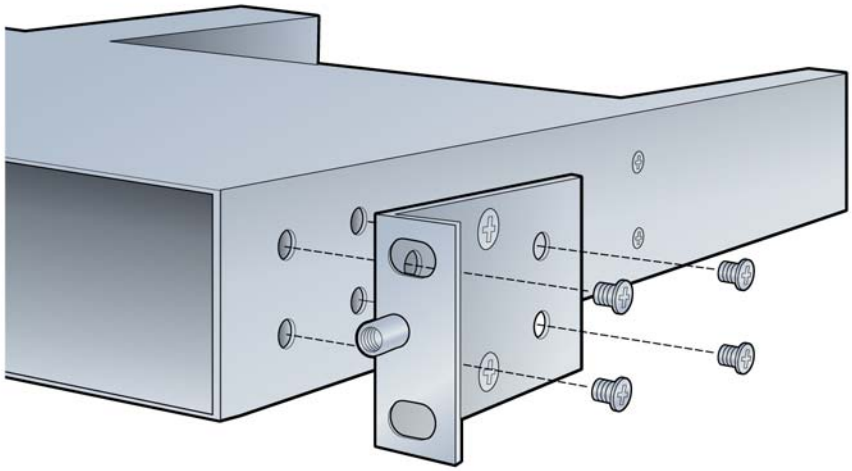
CAUTION

The Baseband Controller, when mounted, must be in the horizontal position. No other orientations are allowed.

NOTE

The chassis requires four screws to secure it into the rack.

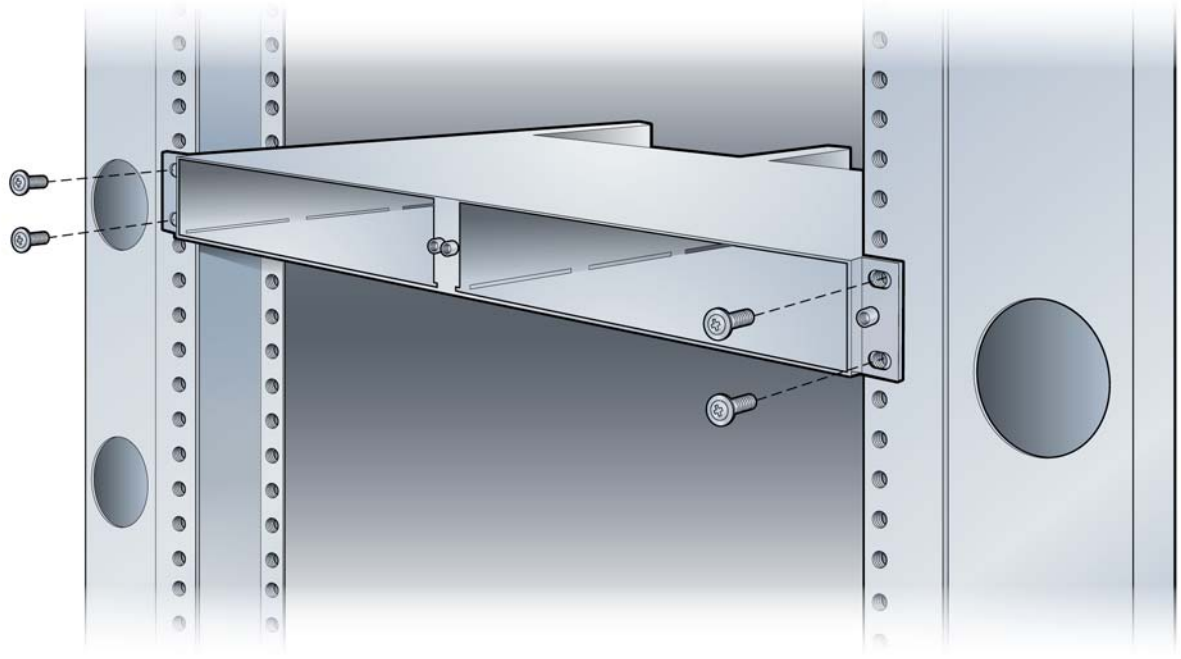
1 Select the 19-inch or 600mm bracket kit according to the size of the rack. Attach the brackets to the Baseband Controller Chassis



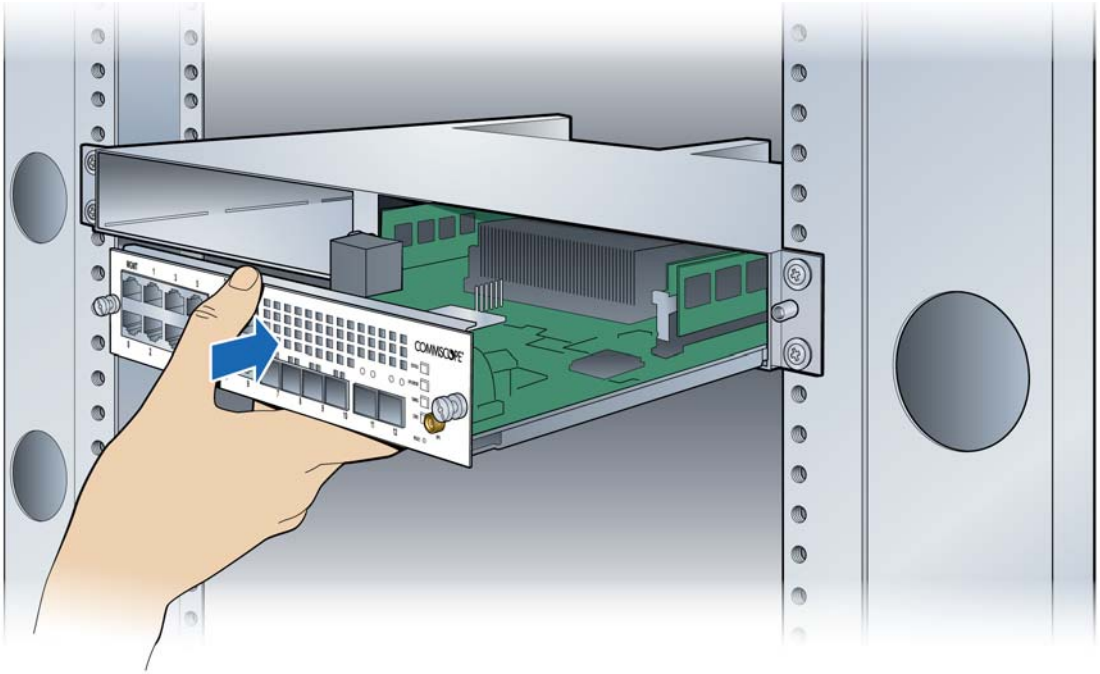
2 Slide the chassis into the rack.

3 Line up the holes in the chassis ears to the holes in the rack.

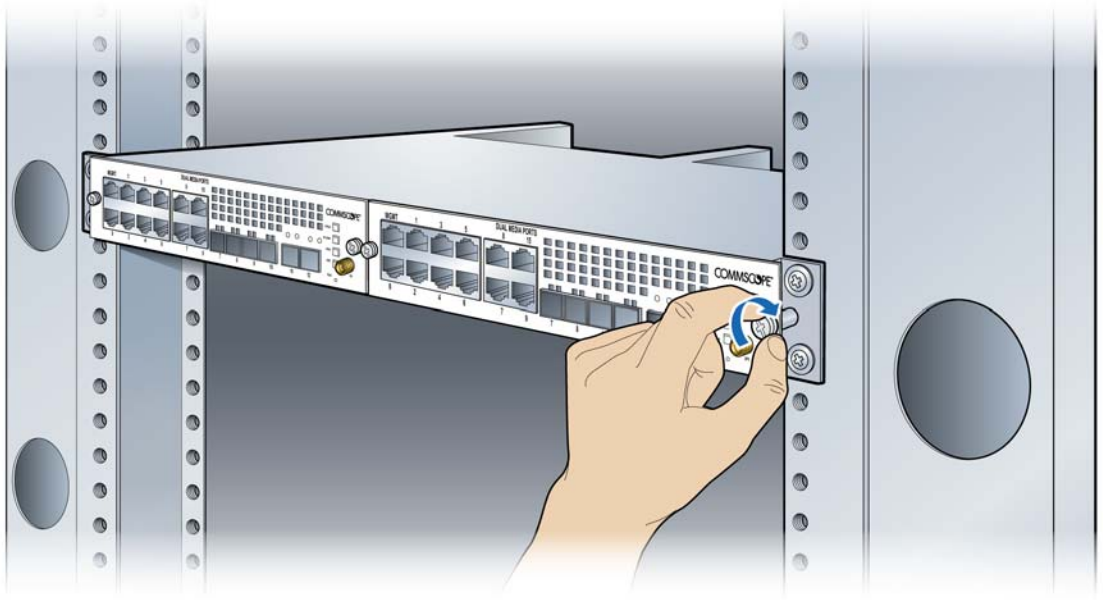
4 Secure the chassis with the screws.



5 Carefully slide the BC into the front of the chassis.



6 Secure the BC by tightening the front panel screws.

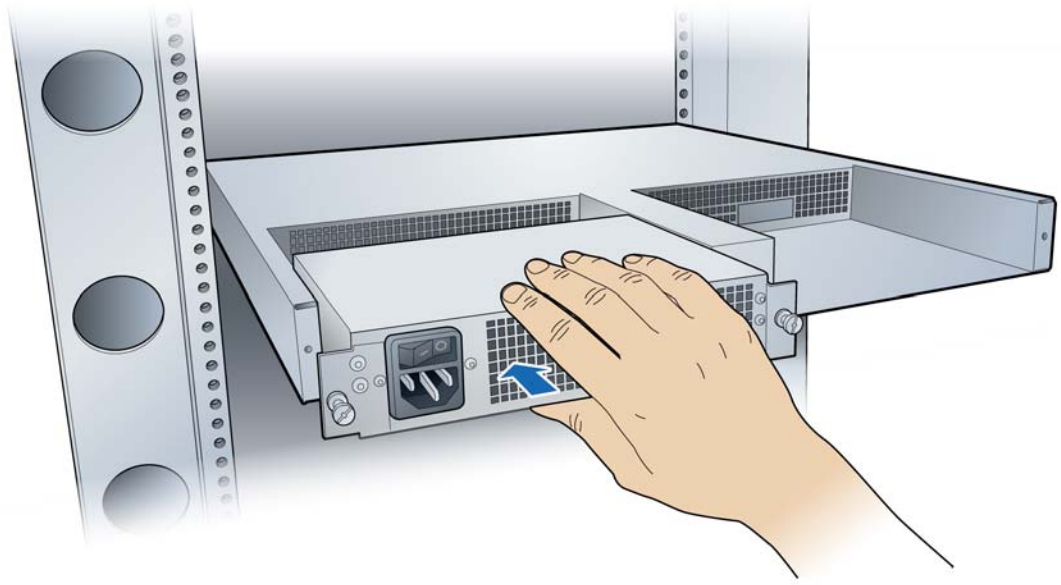


7 In the back of the rack, carefully slide the PFU into the back of the chassis.

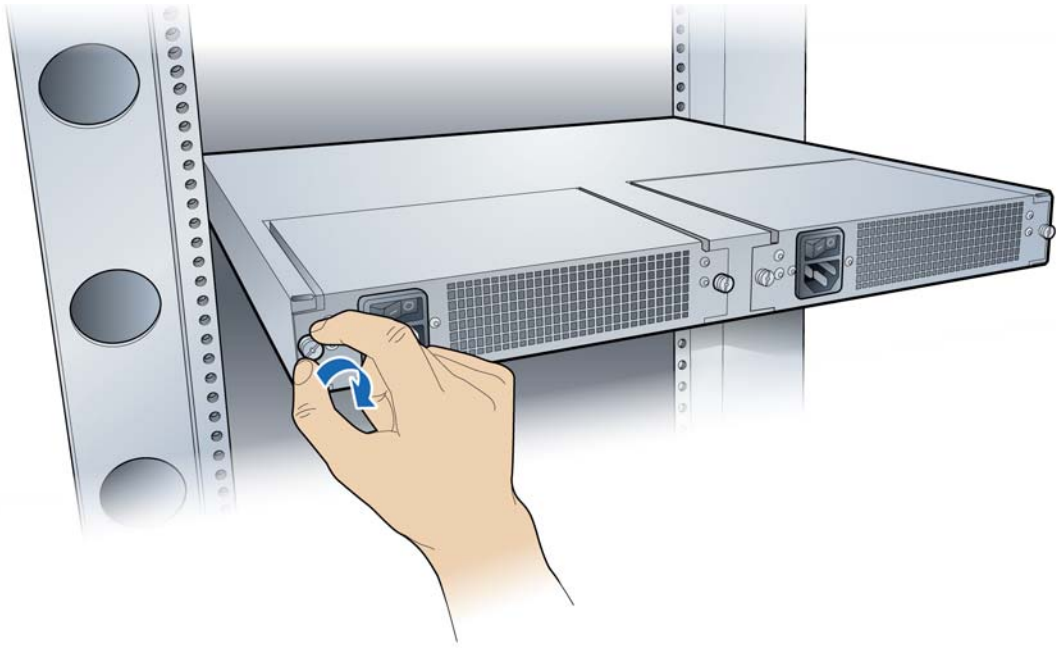
CAUTION

The PFU has a fan hazard. A label is affixed to the top of the PFU indicating the hazard.

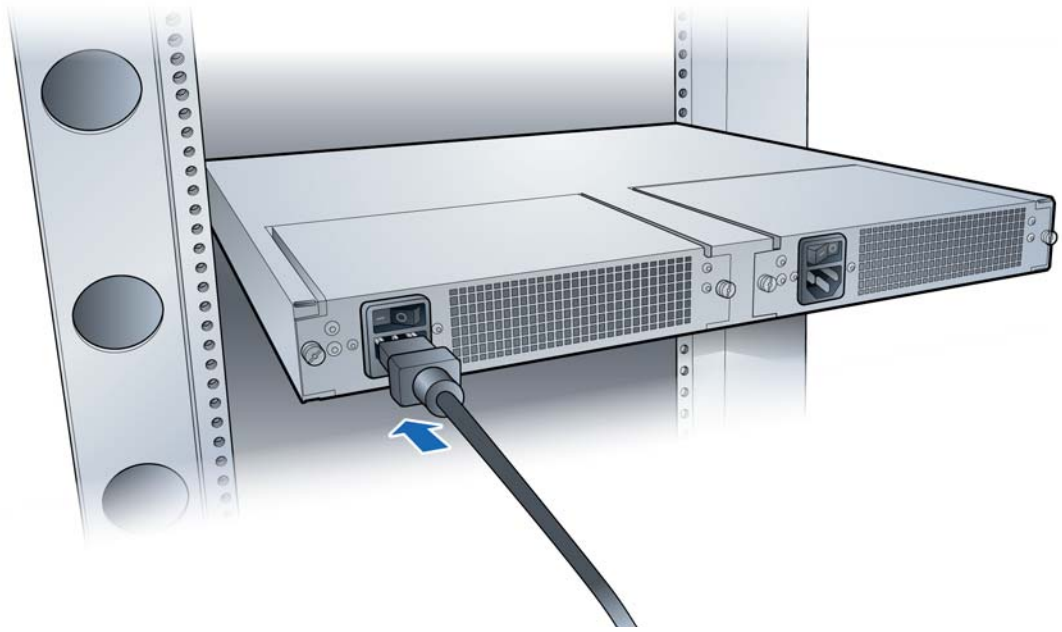
NOTE: The connectors on the PFU should fit easily into the connector on the BC. Do not force the PFU into the chassis.



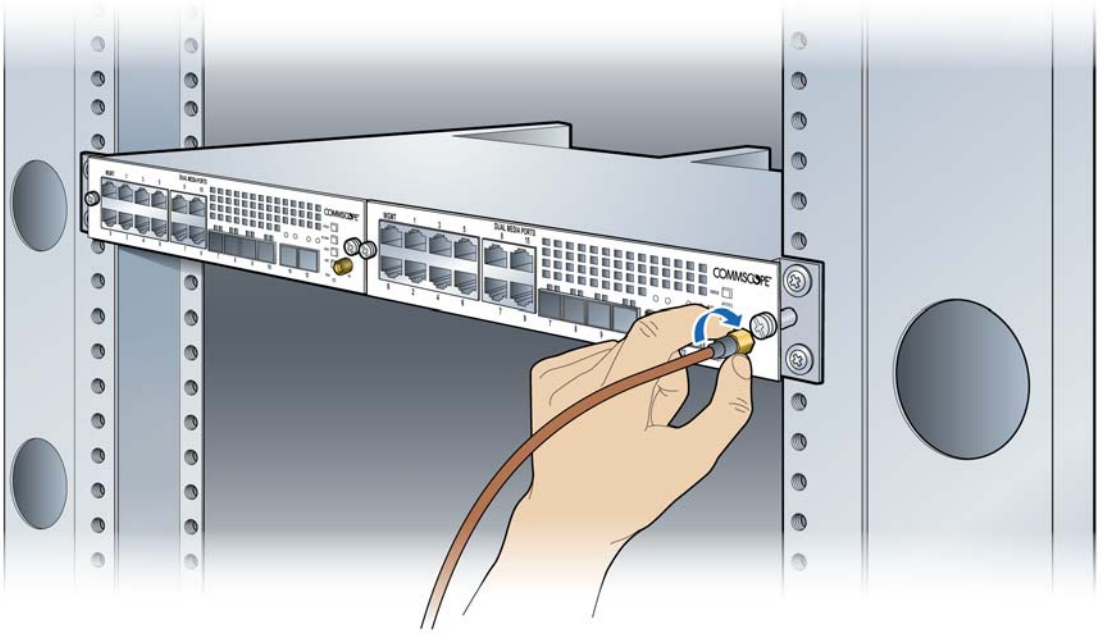
8 Secure the PFU by tightening the thumb screws.



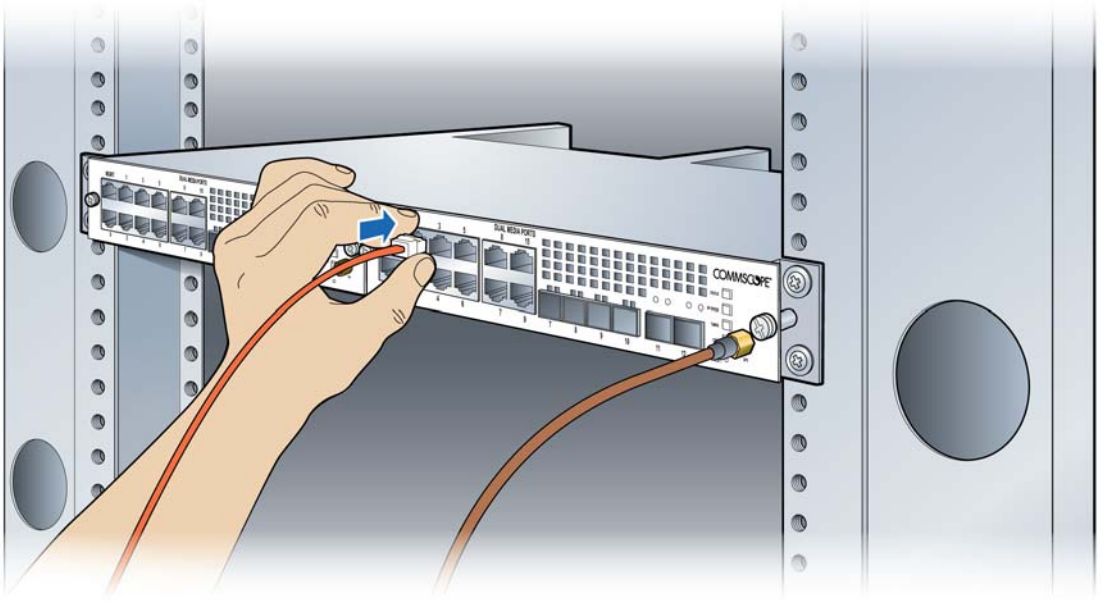
9 Connect the power cord to the PFU.



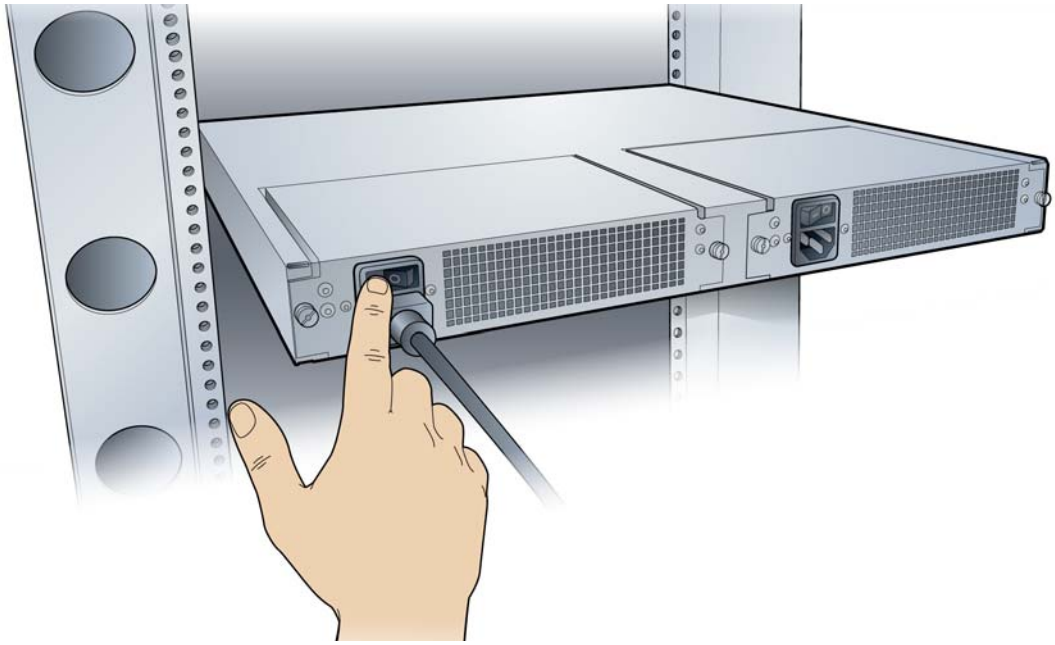
10 On the Baseband Controller Module's front panel, connect the GPS antenna cable.



11 Connect the Ethernet or fiber optic cable to the appropriate port.



12 On the back of the Baseband Controller, turn on the power.



The LEDs on the front panel will be solid green, when the power is on. If none are on, check your power connection. If the LED pattern is other than all green, see Baseband Controller LED patterns on page B-2.

Chapter 4

RP5100i installation

This chapter describes installing indoor Radio Points on ceiling tiles, above ceiling tiles, on poles and in a flown configuration.

RP5100i installation overview

The RP5100i is the Radio Point for indoor solutions.

There are four configurations for installing the RP5100i, which are dependent on the ceiling type.

- Ceiling mount, on tile
- Ceiling mount, above tile
- Flown mount
- Pole mount

NOTE

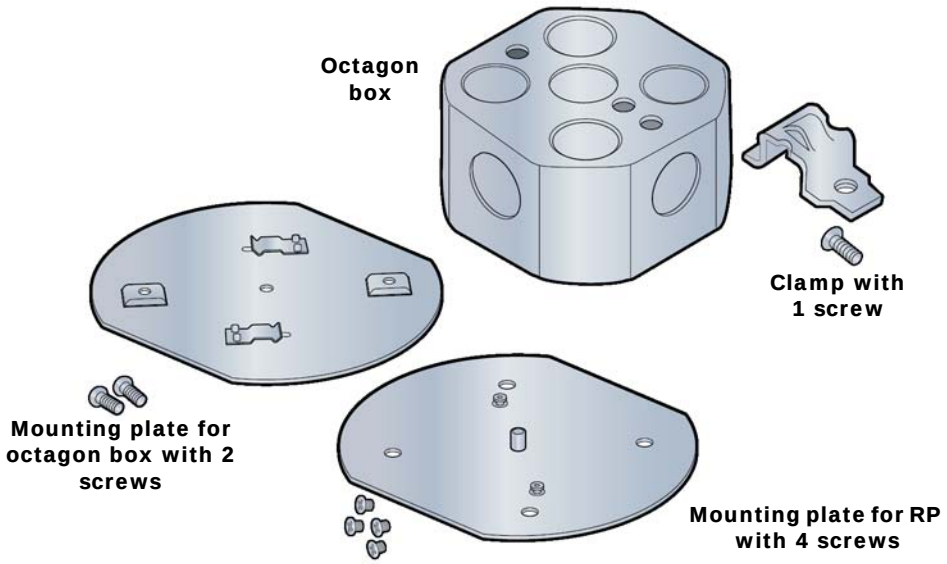
Once the Radio Point is installed and powered on, it may take up to 20 minutes for the frequency to stabilize and lock.

Ceiling mount

Mounting the Radio Point (RP) above or on the ceiling tile requires the following hardware provided by CommScope:

- Radio Point plate and screws
- 4" octagon box, 1-1/2" deep with 1/2" side cutouts
- Clamp and screw

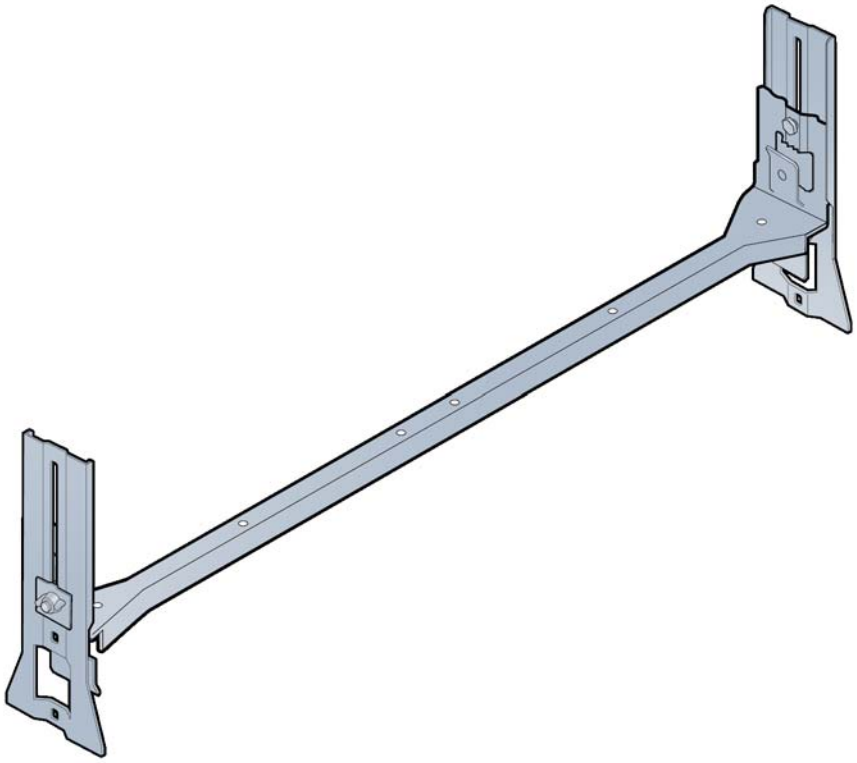
Figure 4-1. CommScope ceiling mount kit contents



Mounting the Radio Point (RP) above or on the ceiling tile requires the following hardware provided by the system integrator:

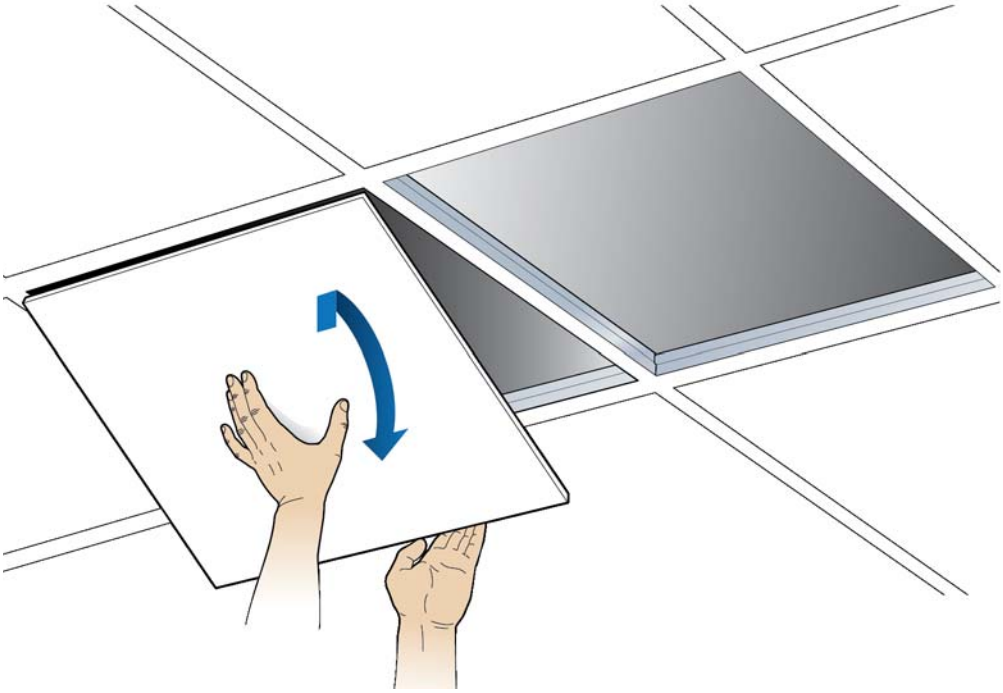
- Drop rail – Eaton B-line BA50 recommended

Figure 4-2. Drop rail, system integrator-provided



Mounting the Radio Point on the ceiling tile

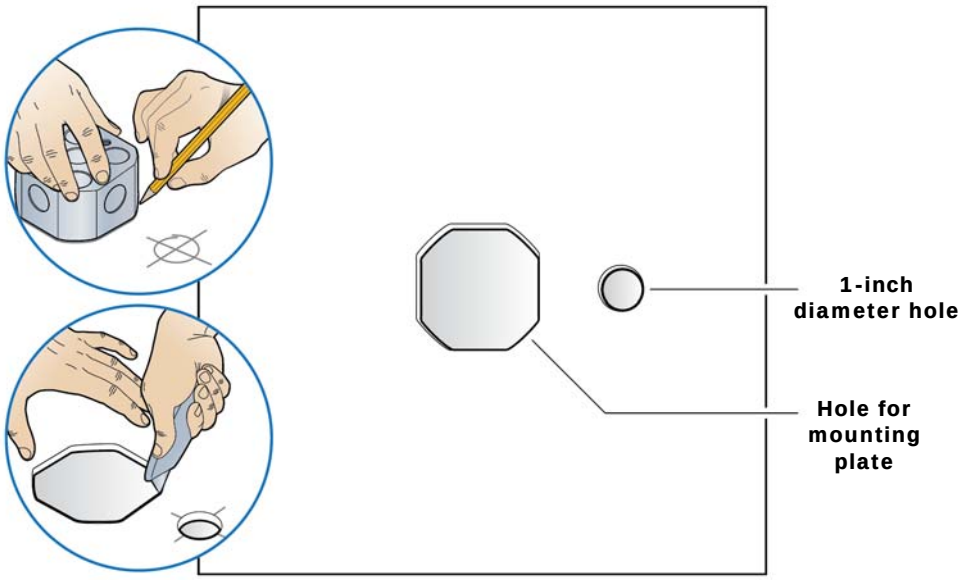
1 Remove two ceiling tiles from the overhead.



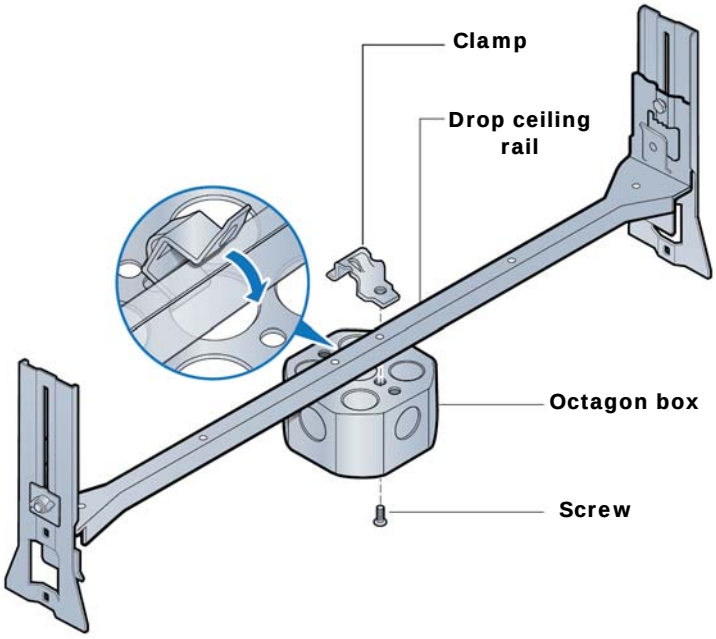
2 Place the octagon box on the tile and trace the outline. Cut the opening.

3 Drill a 1/2-inch diameter hole for the Ethernet cable pass-through.

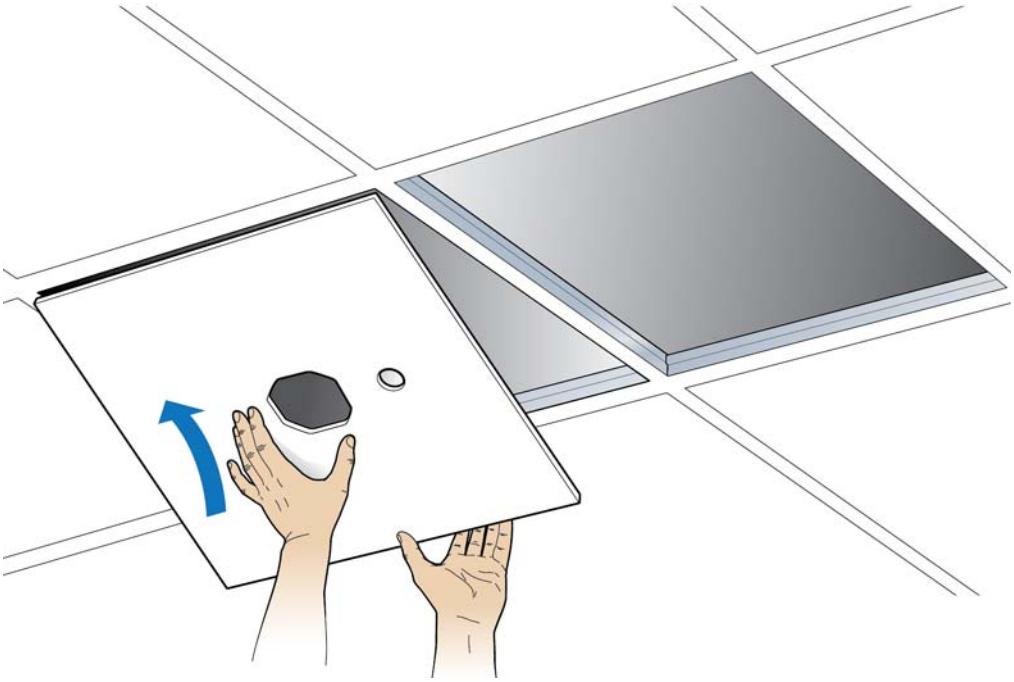
NOTE: Use a 1-1/2 deep RACO 8125 or equivalent.



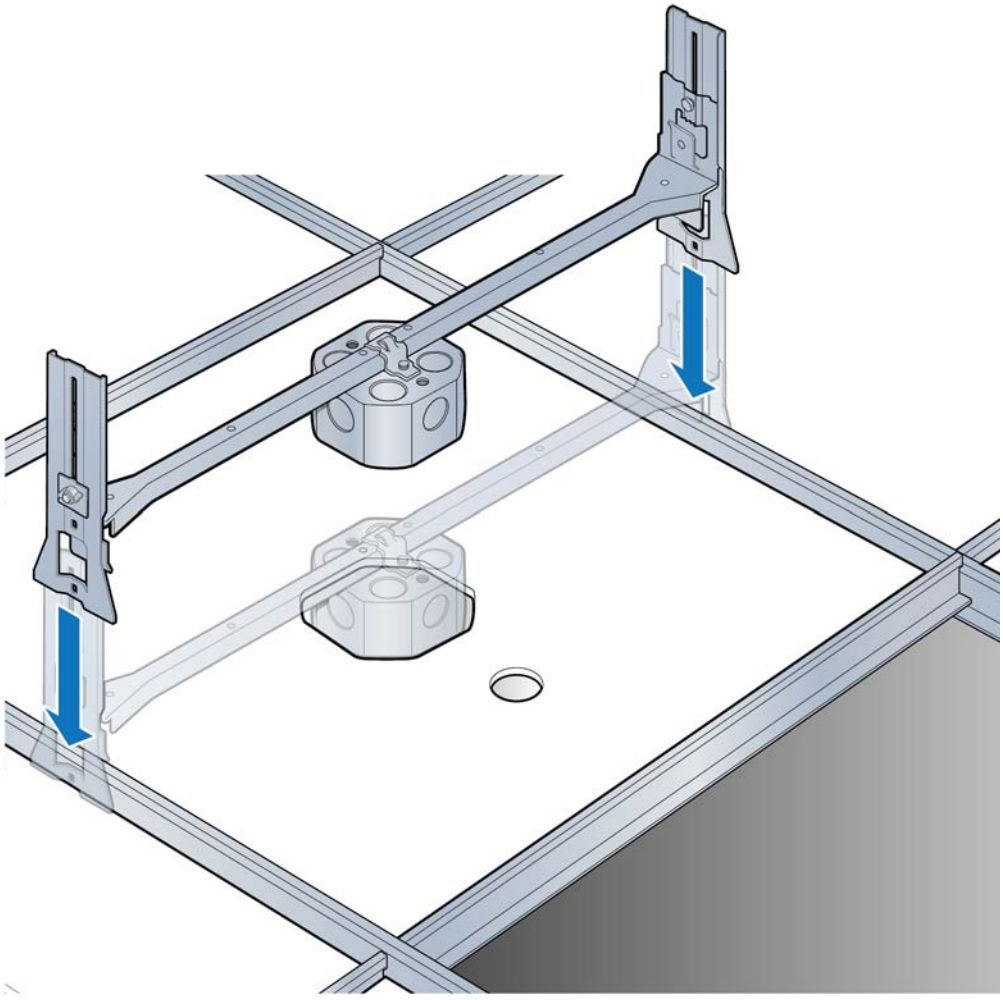
4 Attach the octagon box to the ceiling bracket using a clamp and screw.



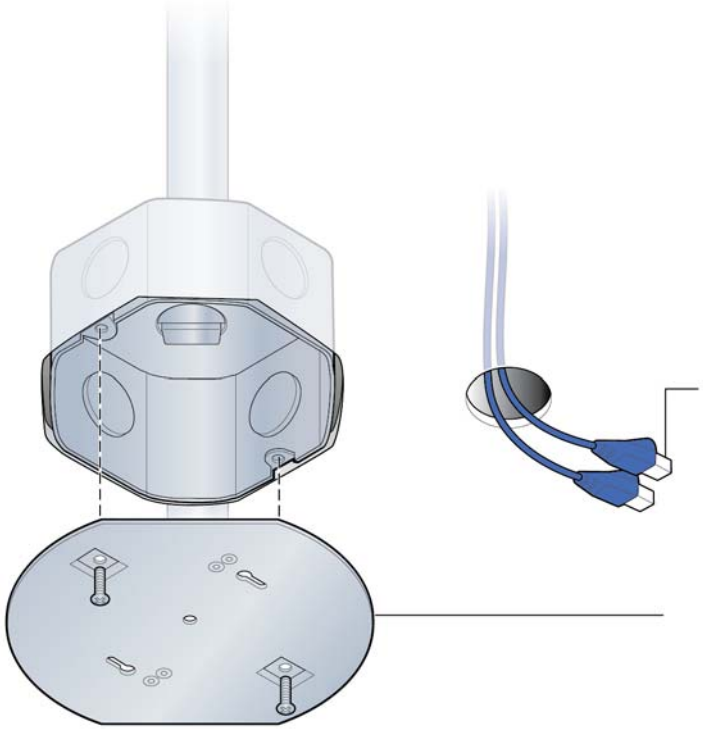
5 Replace the ceiling tile with the cutouts.



6 Install the drop rail/octagon box assembly over the modified tile.

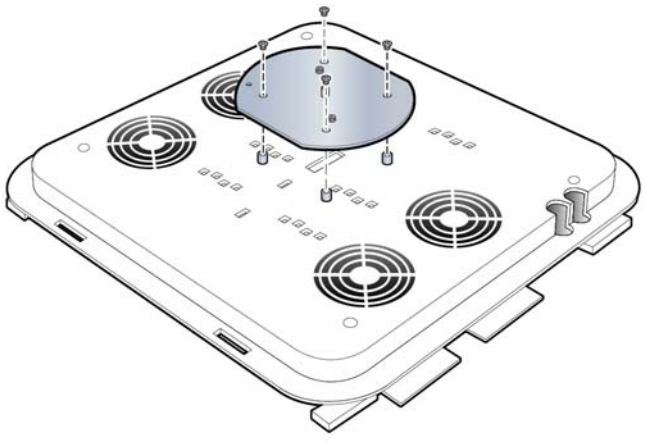


7 Attach the mounting plate onto the octagon box and feed the Ethernet cable through the small hole in the ceiling tile.



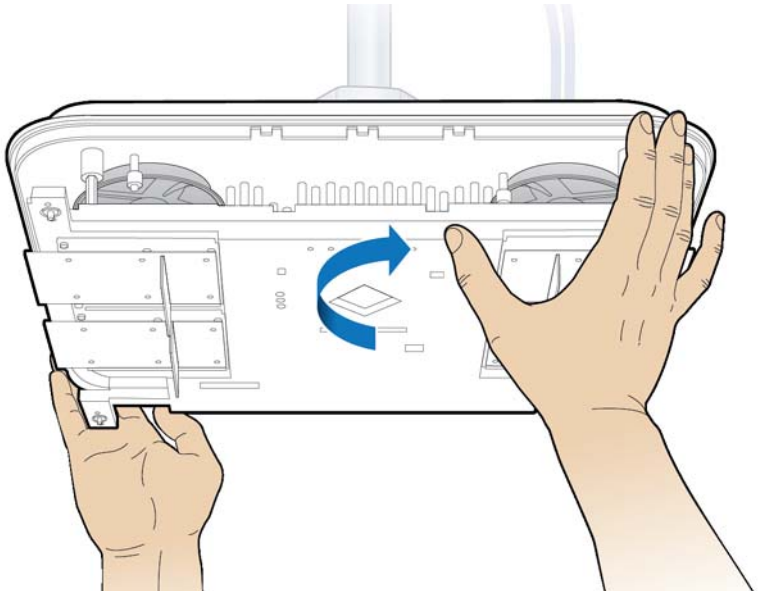
8 Attach base plate to the Radio Point.

NOTE: Apply thread locking compound to screws prior to installation.

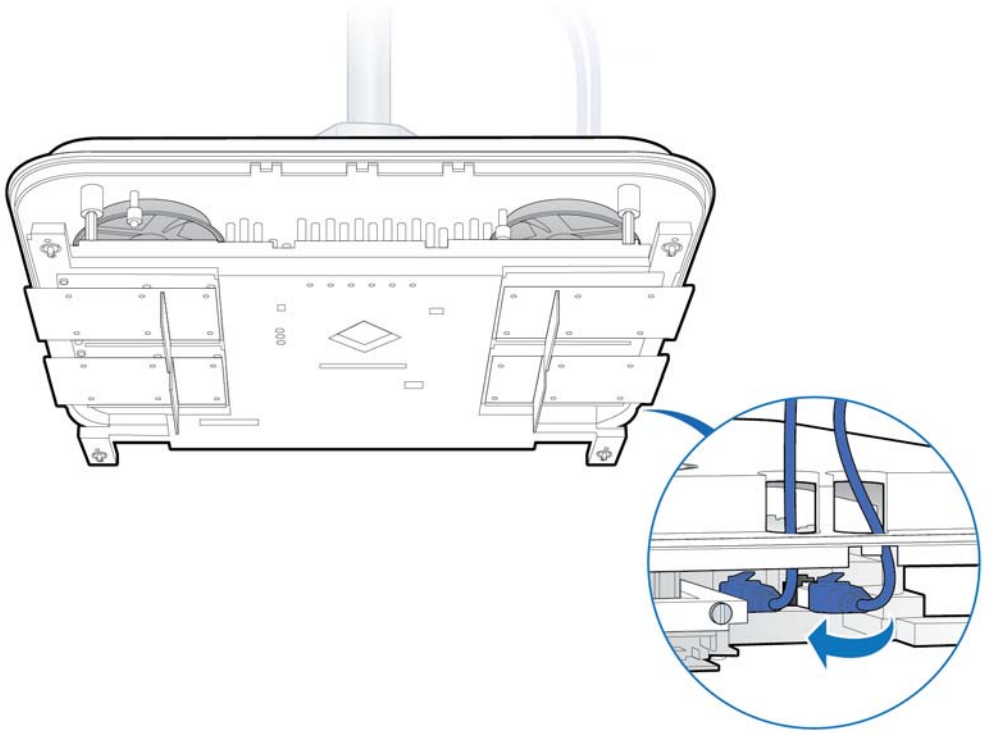


9 Mount the Radio Point on the octagon box plate.

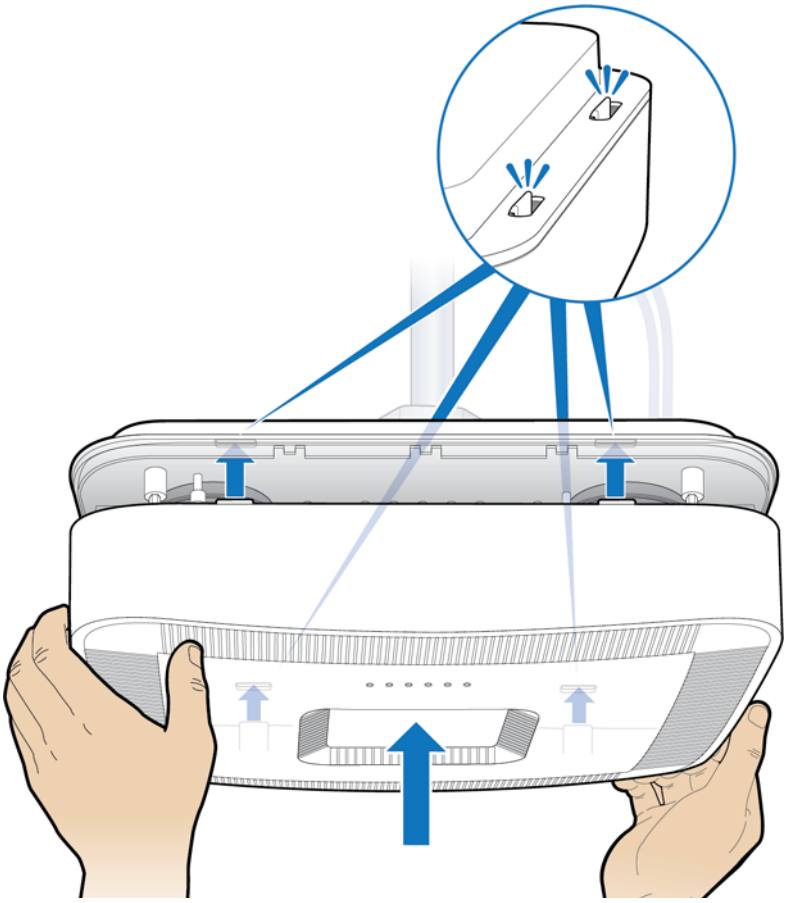
10 Secure Radio Point to plate.



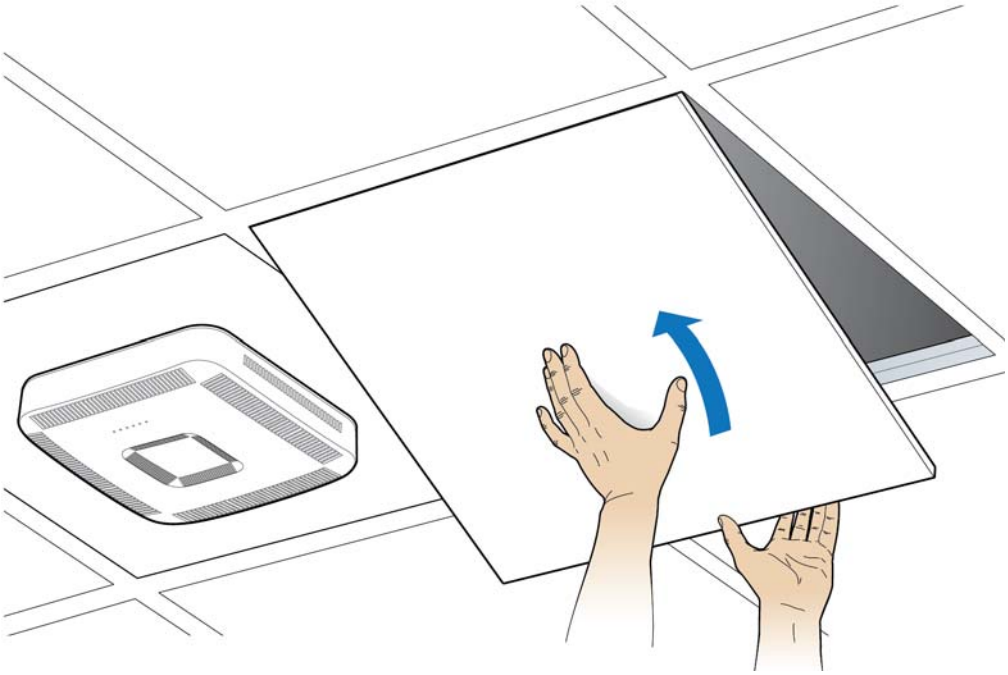
11 Connect Ethernet cables to the Radio Point.



12 Attach the plastic cover to the Radio Point.

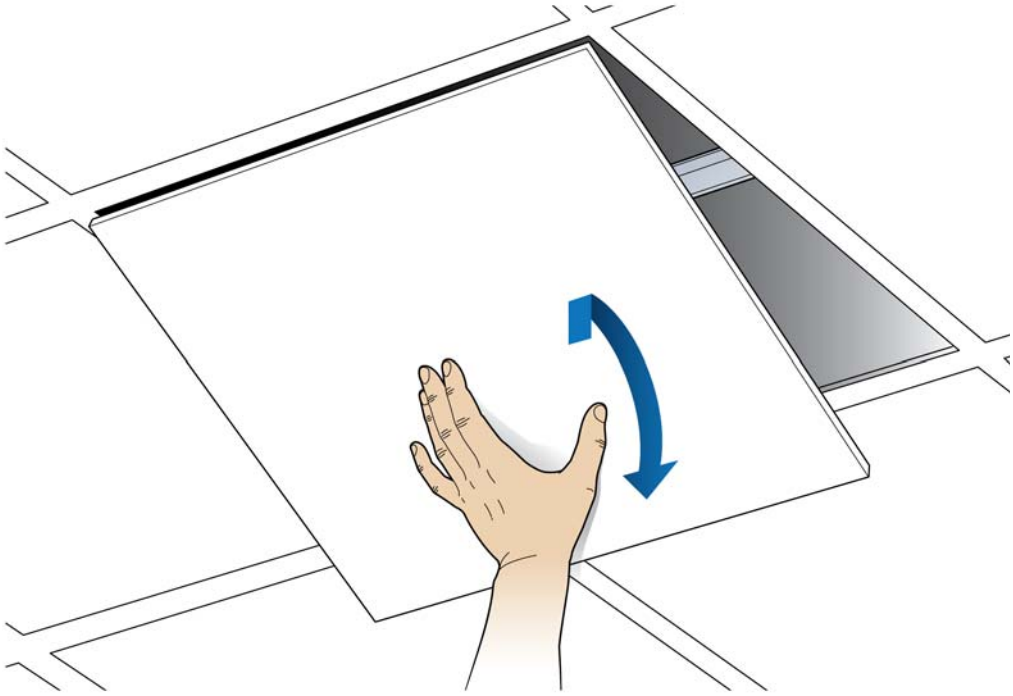


13 Replace the ceiling tile next to the Radio Point.



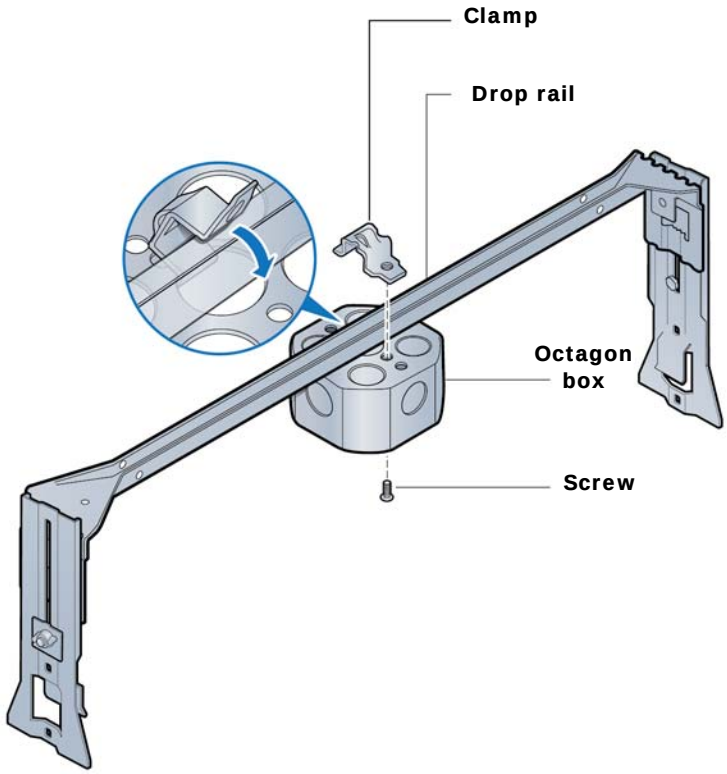
Mounting the Radio Point above the ceiling tile

1 Remove ceiling tile from the overhead.

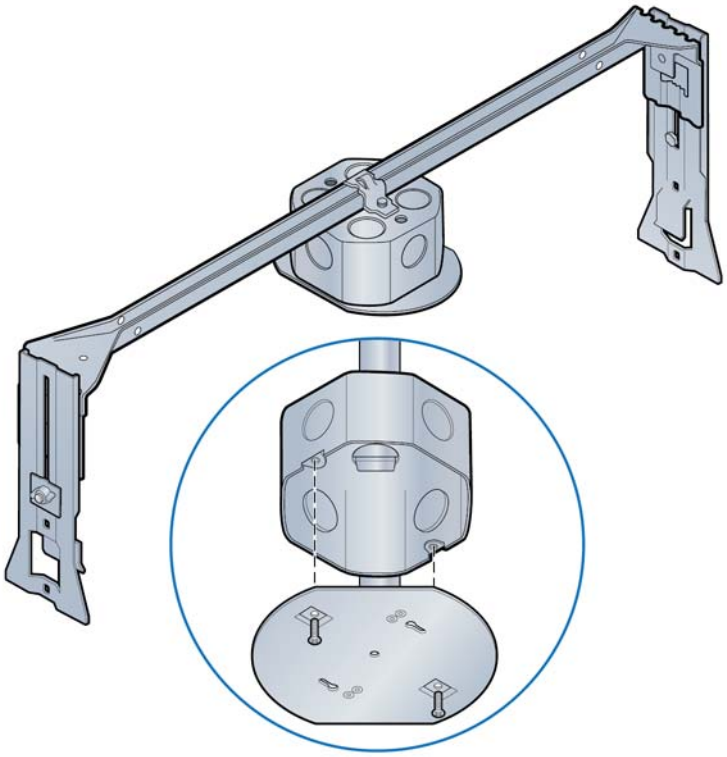


2 Attach the octagon box to the bracket.

NOTE: CommScope recommends an Eaton B-line – BA50A adjustable bracket.

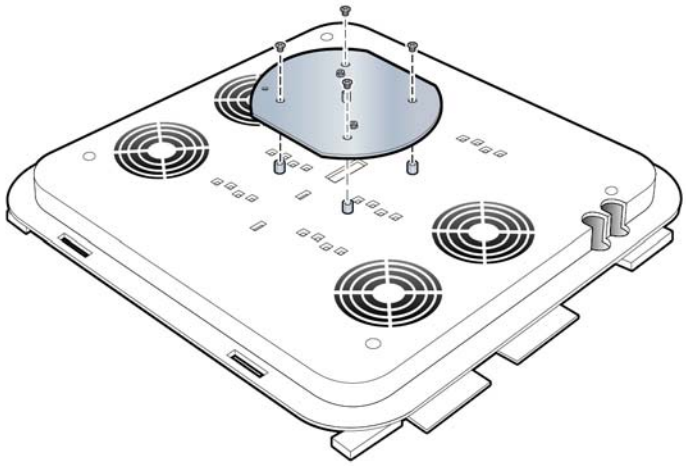


3 Attach the bracket to the mounting plate to the octagon box.

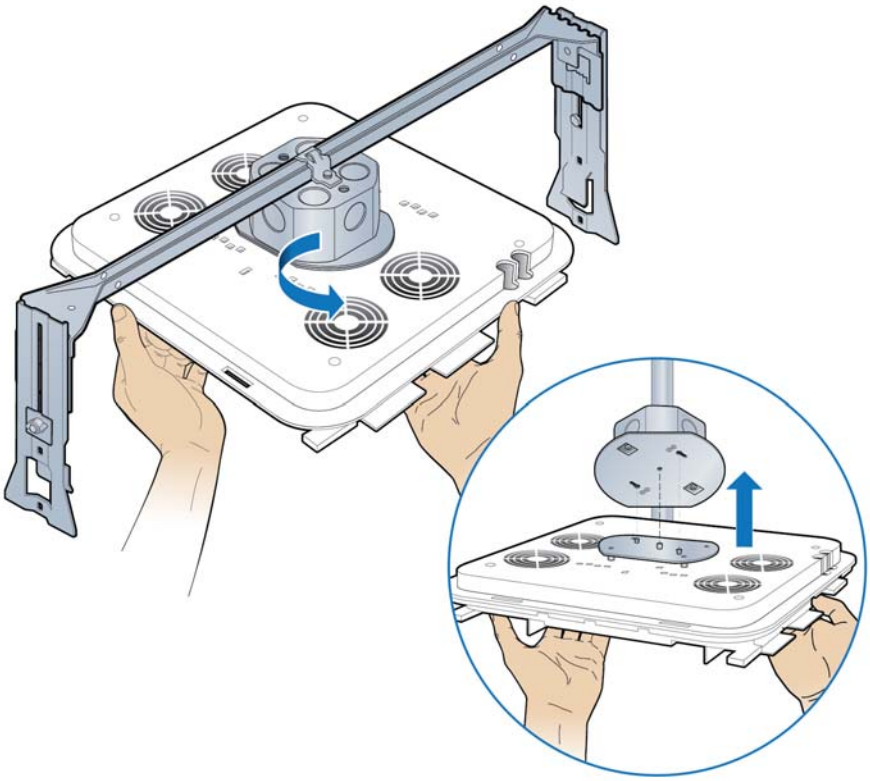


4 Attach plate to the Radio Point.

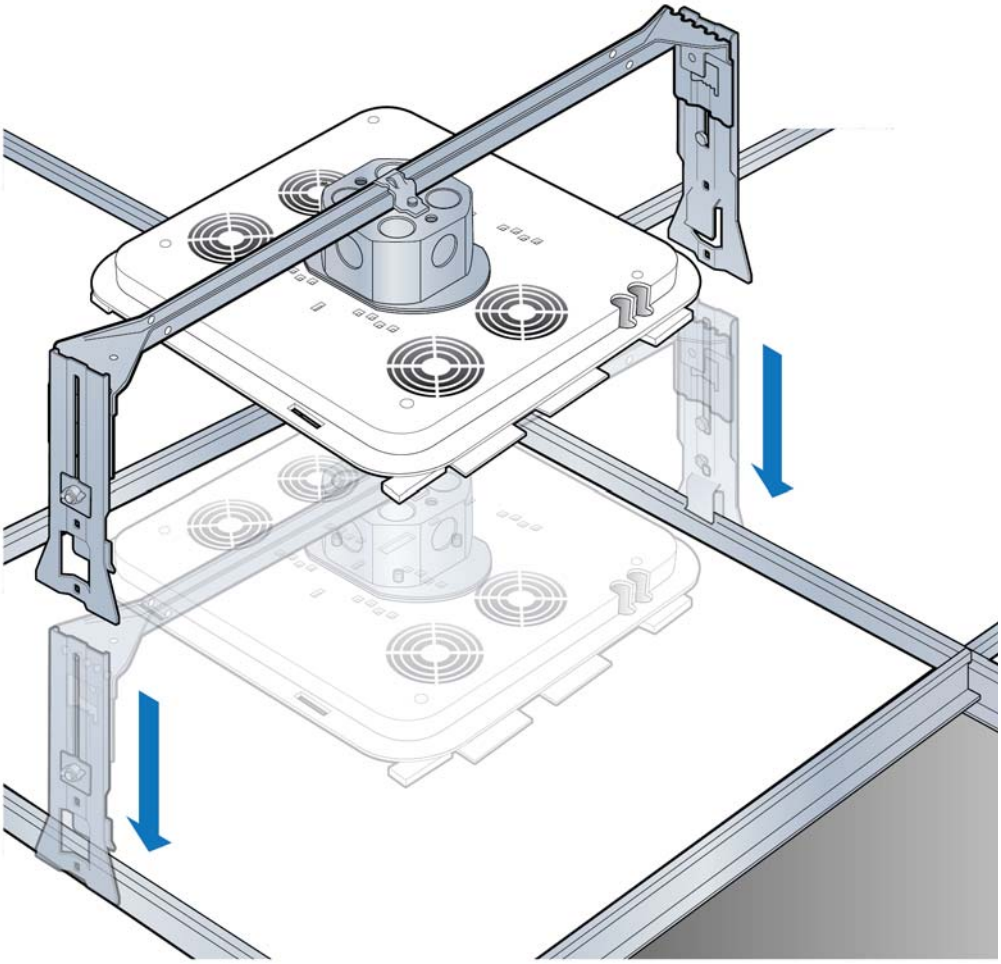
NOTE: Apply thread locking compound to screws prior to installation.



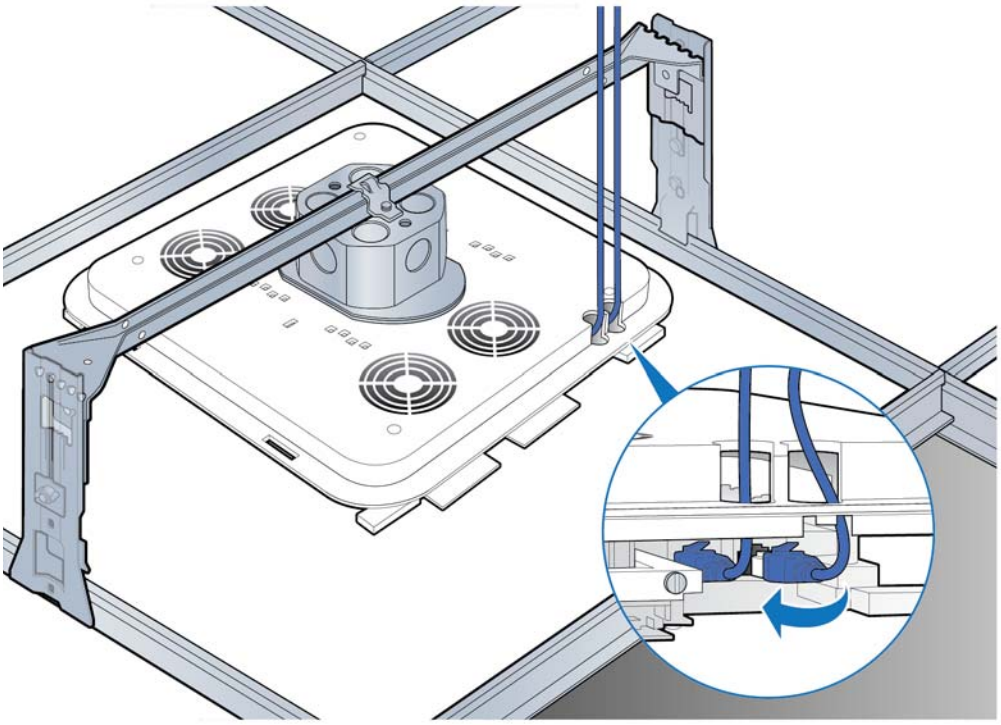
5 Attach the Radio Point to the octagon box mounting plate.



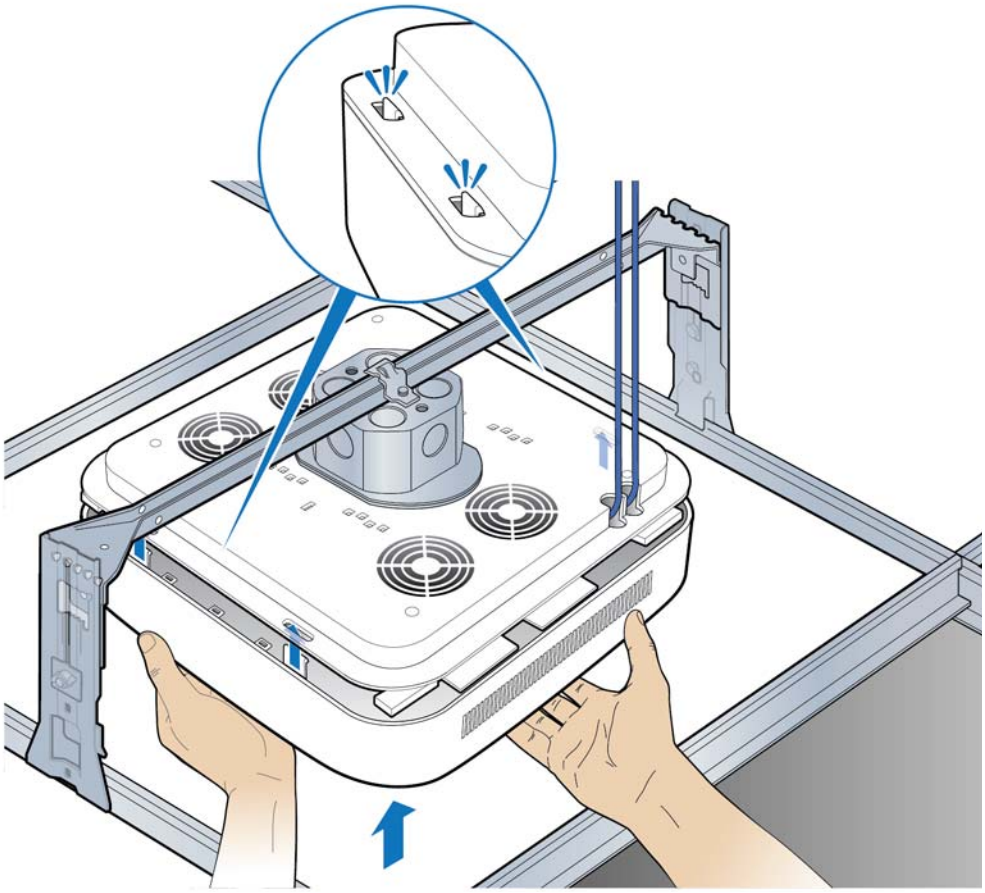
6 Install drop rail above the ceiling tile.



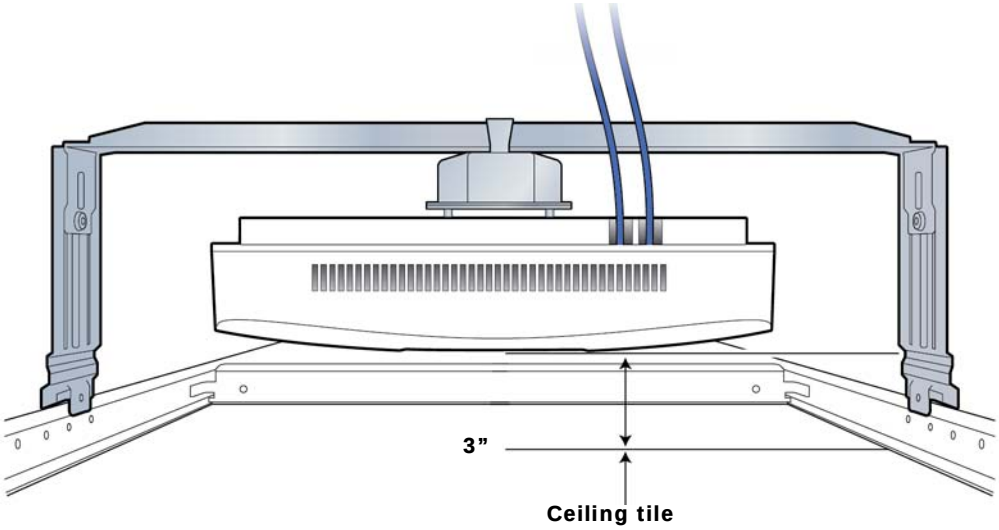
7 Connect the Ethernet cables to the Radio Point.



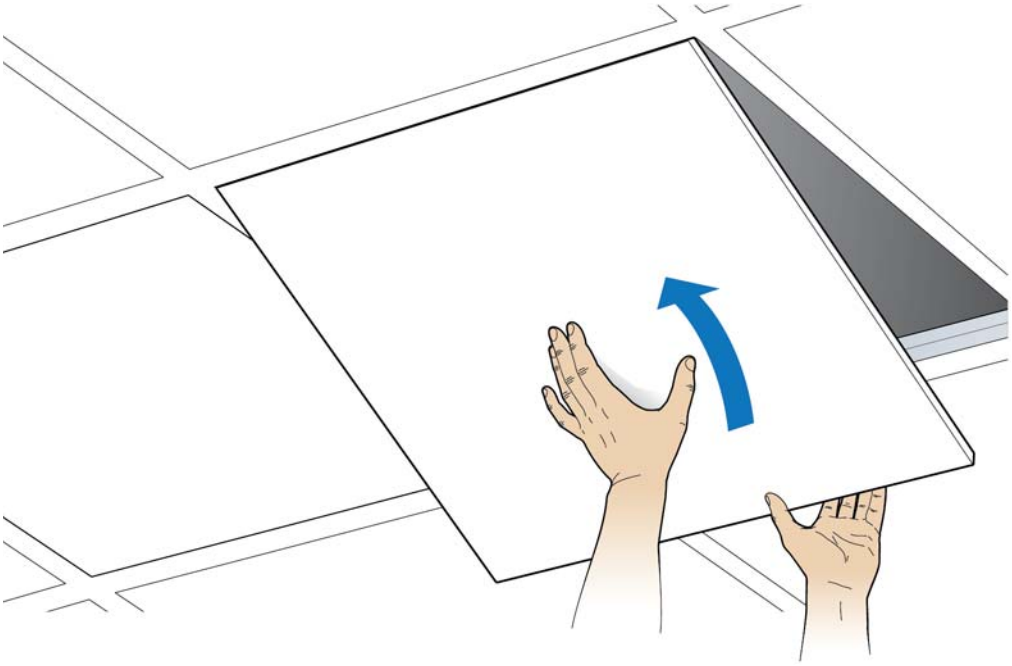
8 Attach the cover to the Radio Point.



NOTE: The minimum clearance for cooling is 3 inches.



9 Replace the ceiling tile.



Flown mount

The Radio Point can be flown mounted on the end of a rod. This configuration is used for building where there are no drop ceilings.

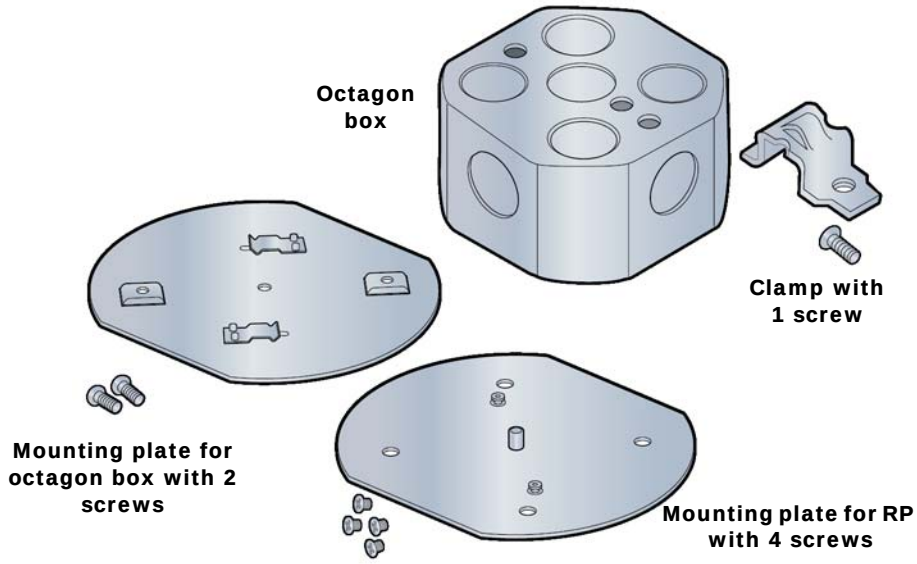
Mounting the Radio Point (RP) in the flown configuration requires the following hardware provided by CommScope in the mounting kit:

- Radio Point plate and screws
- 4" octagon box, 1-1/2" deep with 1/2" side cutouts

  NOTE: Remove the top, middle cutout.

- Clamp and screw – this hardware is not required for the flown mount option

Figure 4-3. CommScope flown mount kit contents



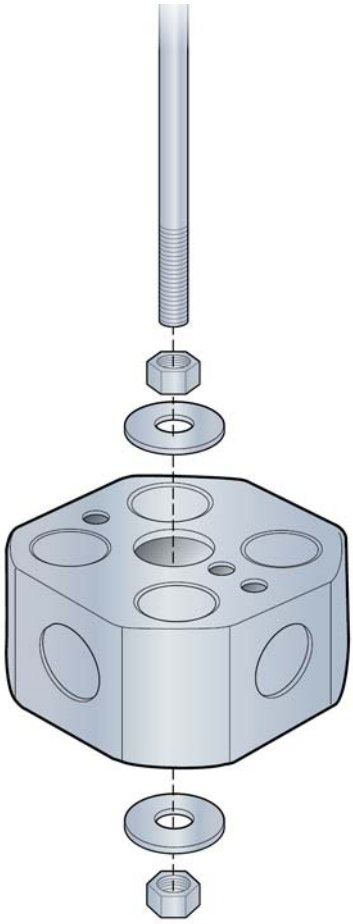
Mounting the Radio Point (RP) in the flown configuration requires the following hardware provided by the system integrator:

- Rod, 3/8-inch threaded
- Nut
- Lock nut, nylon
- Flat washers

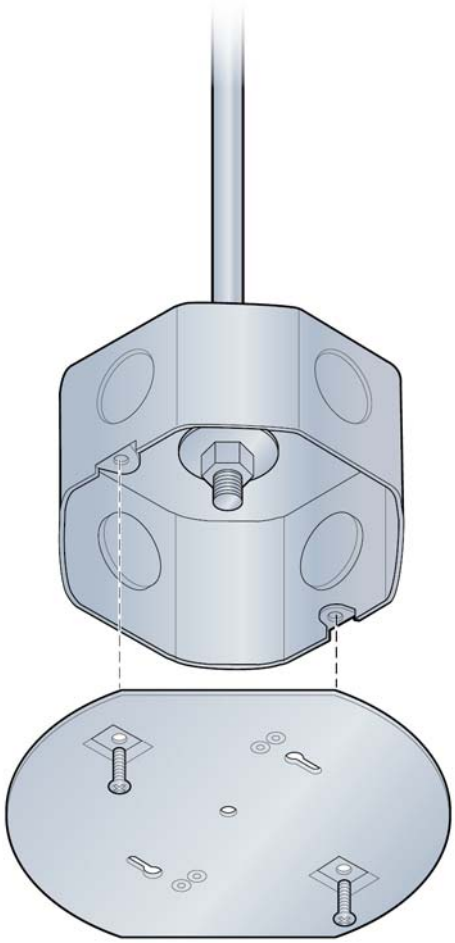
Flown mount installation

1. Attach the threaded, 3/8-inch rod, cut to the required length, to the ceiling.
2. Install the nut and a flat washer on the rod.
3. Slide the octagon box on the rod and install a flat washer and the nylon lock nut.

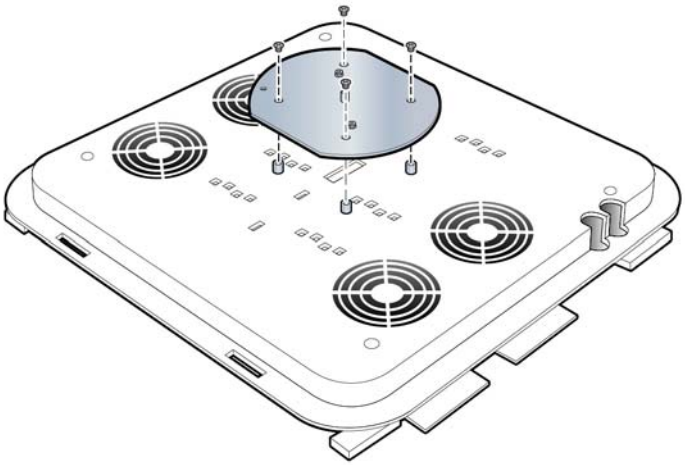
   NOTE: Be sure the bracket is tight between the nuts and there is enough clearance at the end of the rod to attach the bracket to the Radio Point.



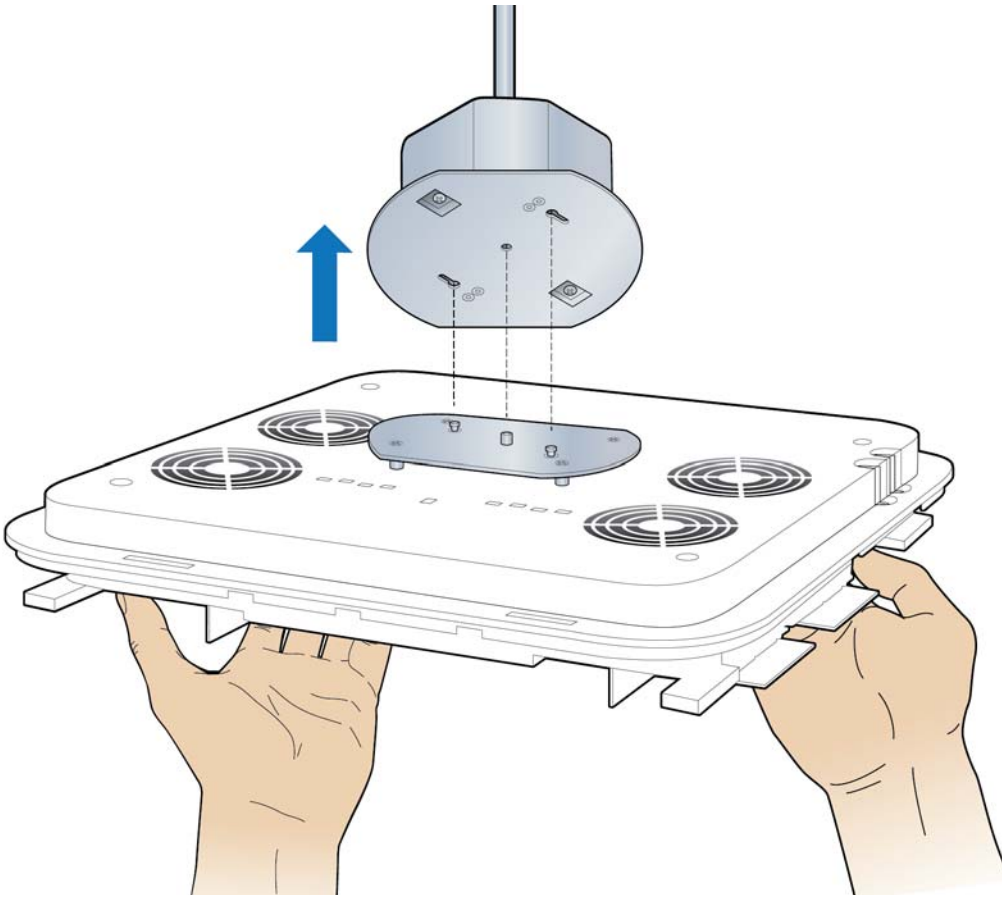
4 Attach plate to octagon box.



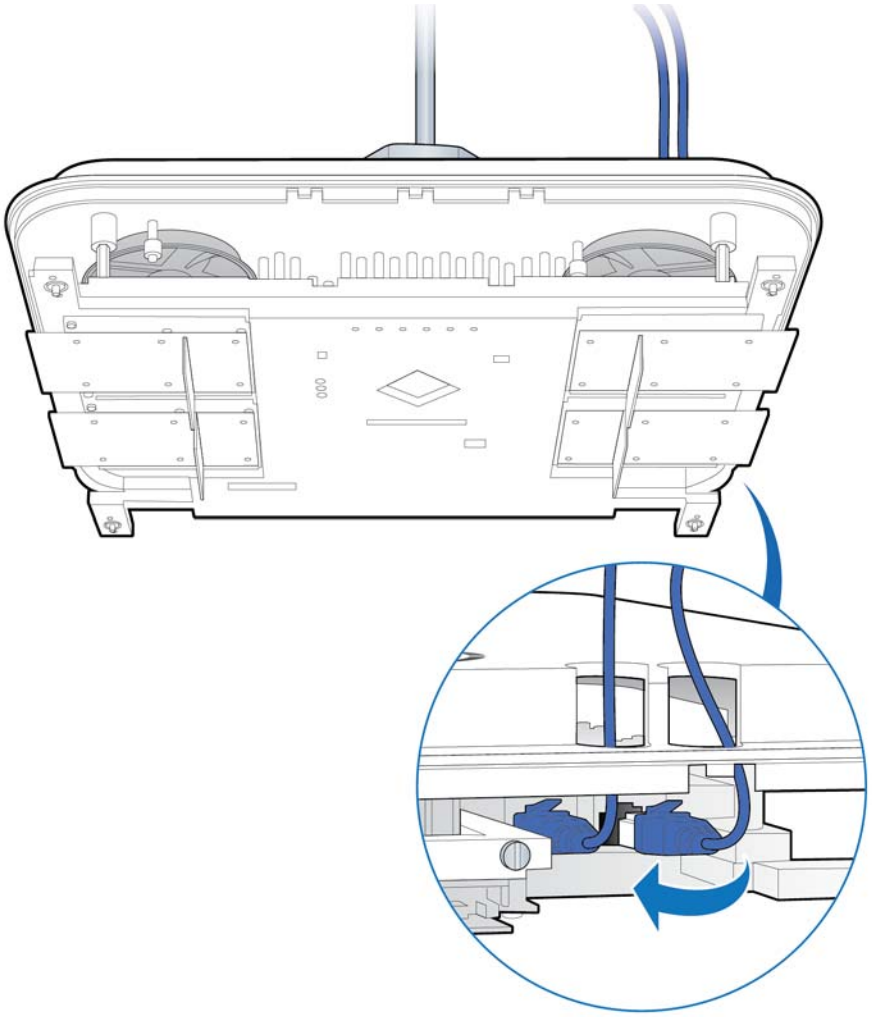
5 Attach the mounting plate to the Radio Point.



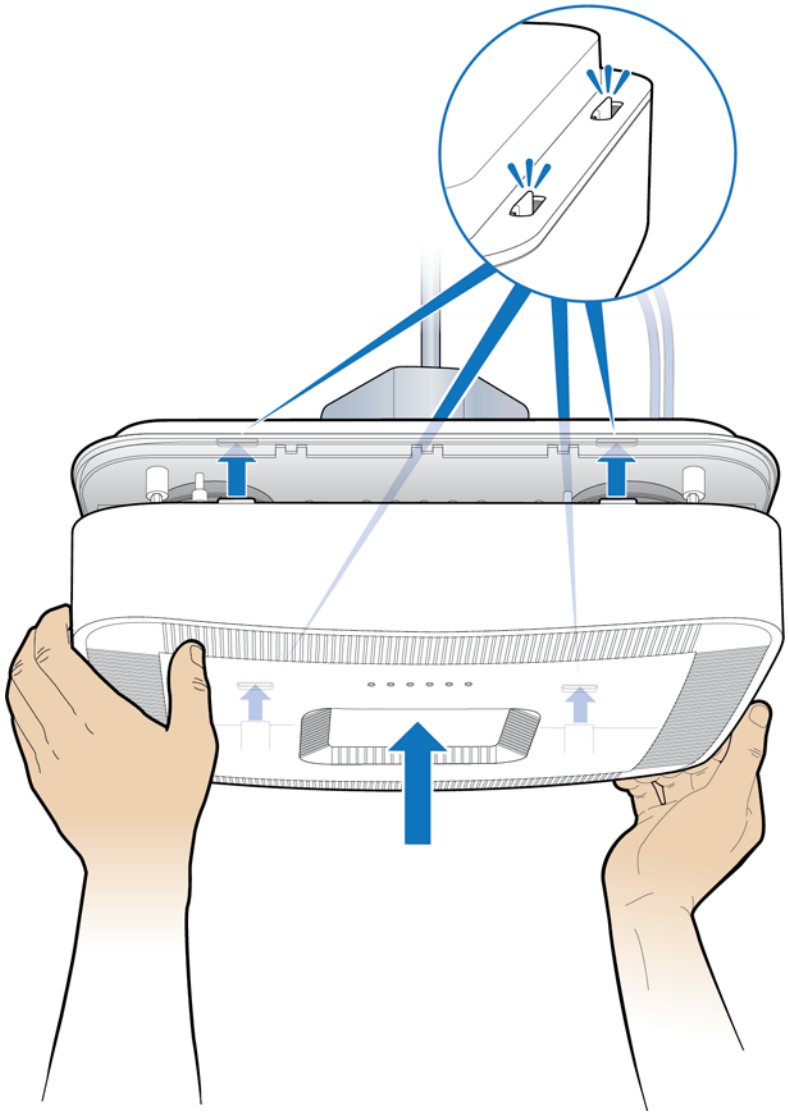
6 Attach the Radio Point to the octagon box.



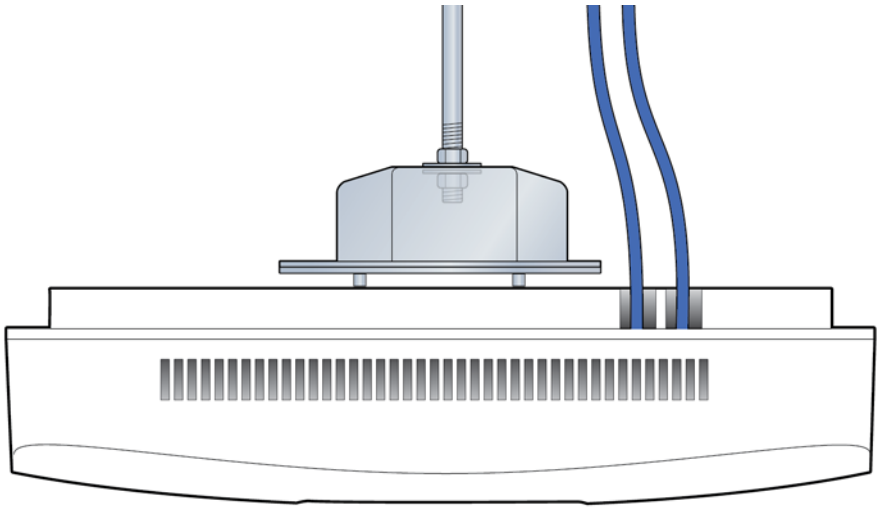
7 Connect the Ethernet cable to the Radio Point.



8 Attach the plastic cover to the Radio Point.



Installation is complete.



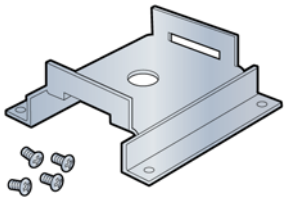
Pole mount

The Radio Point can be pole mounted. This configuration is used for building where there are no drop ceilings.

Mounting the Radio Point (RP) on a pole requires the following hardware provided by CommScope in the mounting kit:

- Mounting bracket
- Screws

Figure 4-4. Mounting bracket kit contents

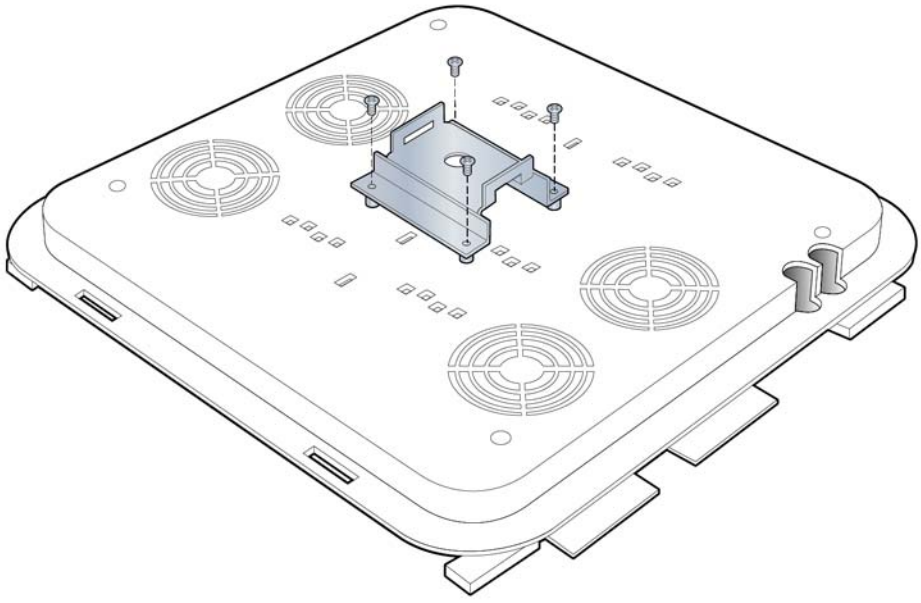


Mounting the Radio Point (RP) on a pole requires the following hardware provided by the system integrator:

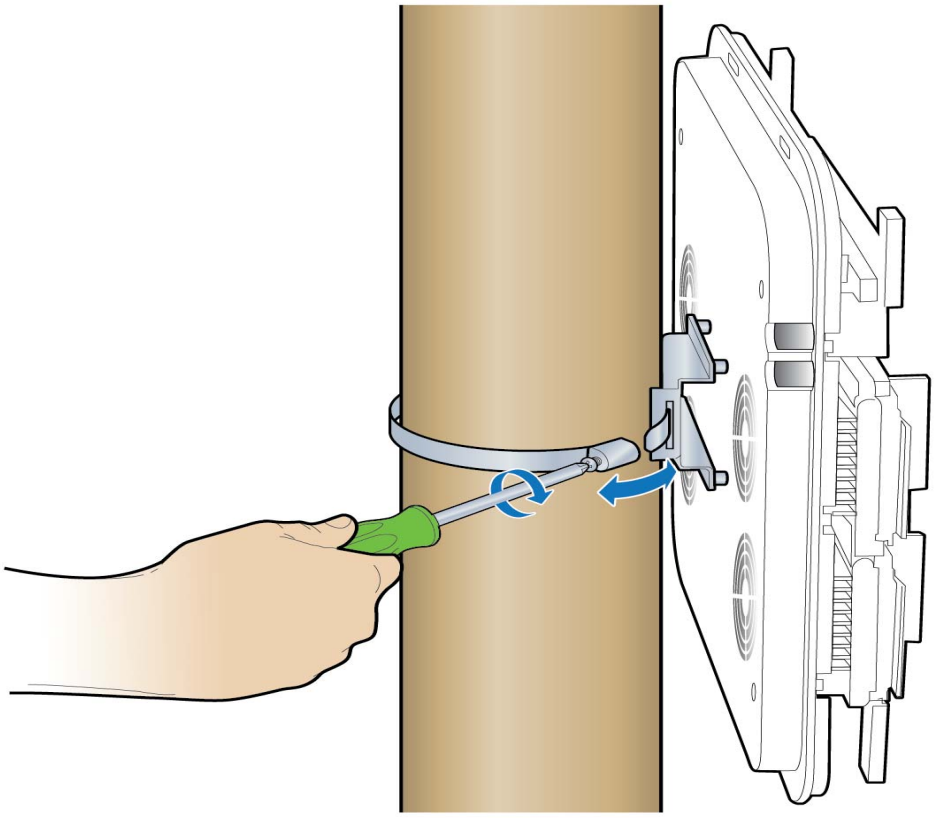
- Adjustable clamp at least 2 inches larger than the circumference of the pole

Pole mount installation

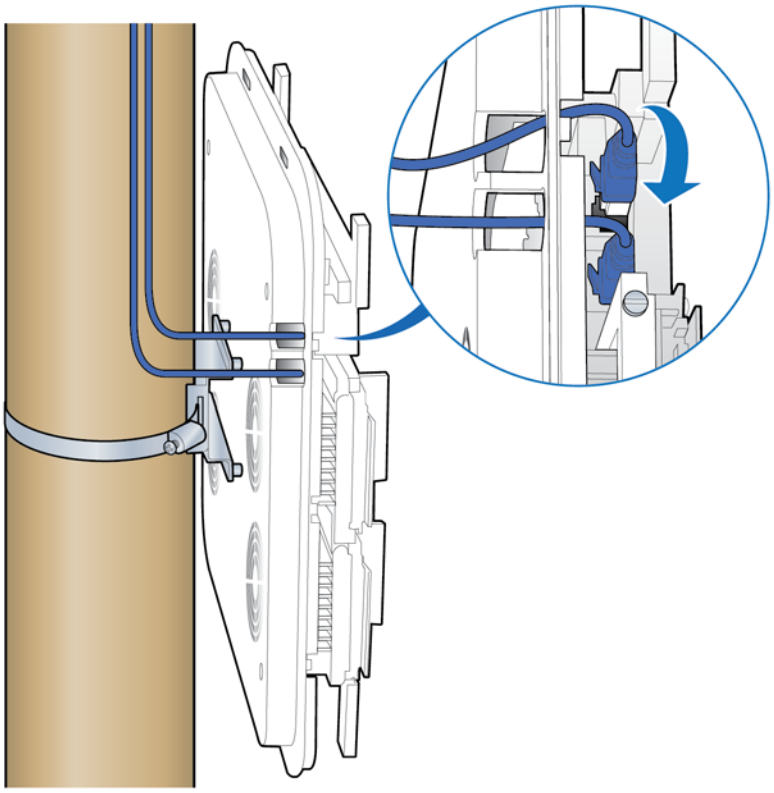
1 Attach the bracket to the Radio point.



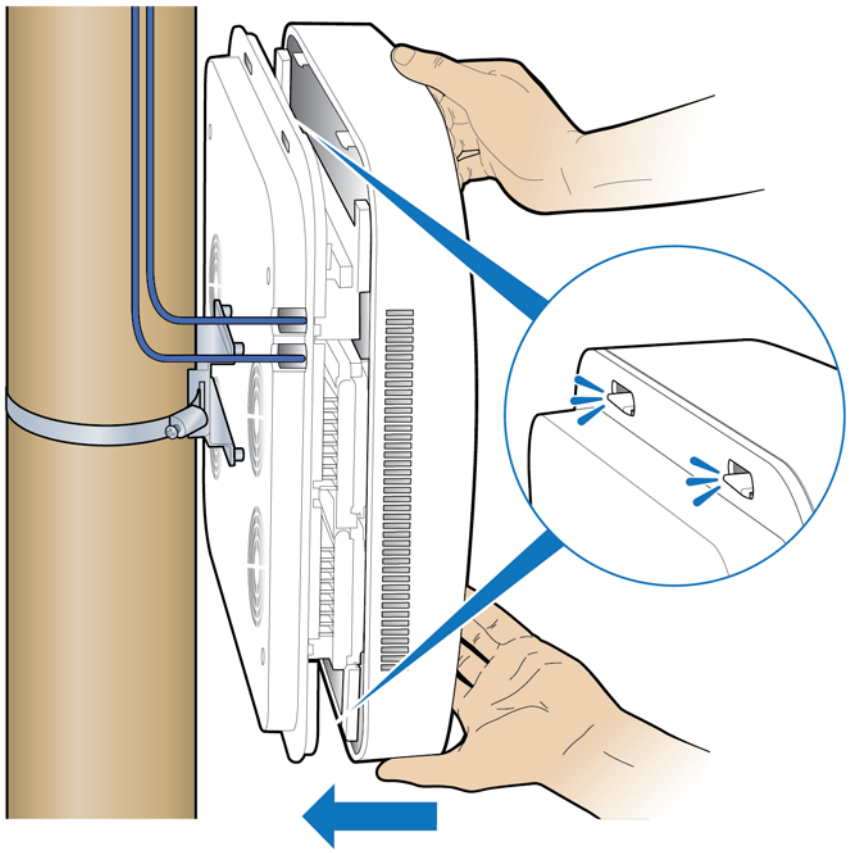
2. Slide the adjustable clamp through the slots on the Radio Point bracket.
3. Wrap the clamp around the pole and tighten the clamp screw to secure the Radio Point to the pole.



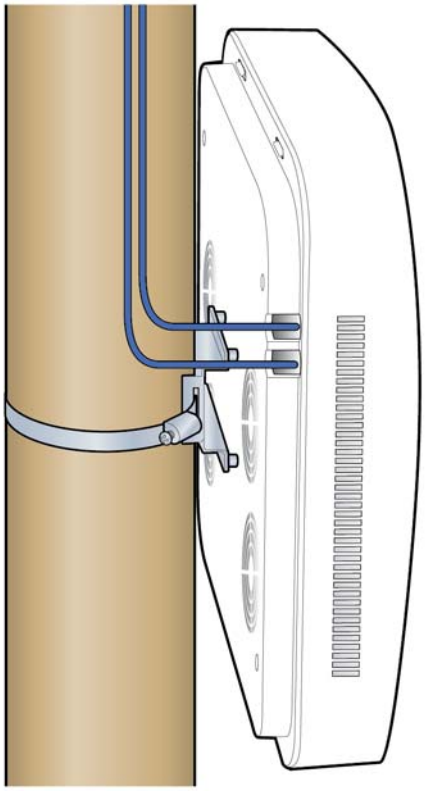
4 Connect the Ethernet cable to the Radio Point.



5 Attach the plastic cover to the Radio Point.



Installation is complete.



Part III: Commissioning

Chapter 5 Configuring the OneCell system

Chapter 5

Configuring the OneCell system

Overview

Once the Baseband Controller and Radio Point are installed and connected, you will need to configure the OneCell system. Logging onto the BC for the first time opens the Web GUI in Installation Mode. This chapter contains the procedures for initial configuration. For more information about the Installation mode, see *OneCell® Administration* (913026)

In preparation of configuring the OneCell system:

- Use the Controller GUI, called the Web GUI, to configure all components, except the Ethernet switches
- Confirm with the operator that the Baseband Controller is provisioned and configured on the DMS

Configuring the Baseband Controller using the Web GUI completes the Baseband Configuration. Once the Baseband Controller and Ethernet switches configurations are complete, go to Chapter 6, Verifying the OneCell installation to test the installation and initial configuration.

Configuring Ethernet switches

Figure 5-1 shows an example of a single OneCell Baseband Controller deployment.

Figure 5-1. OneCell Baseband single Controller deployment

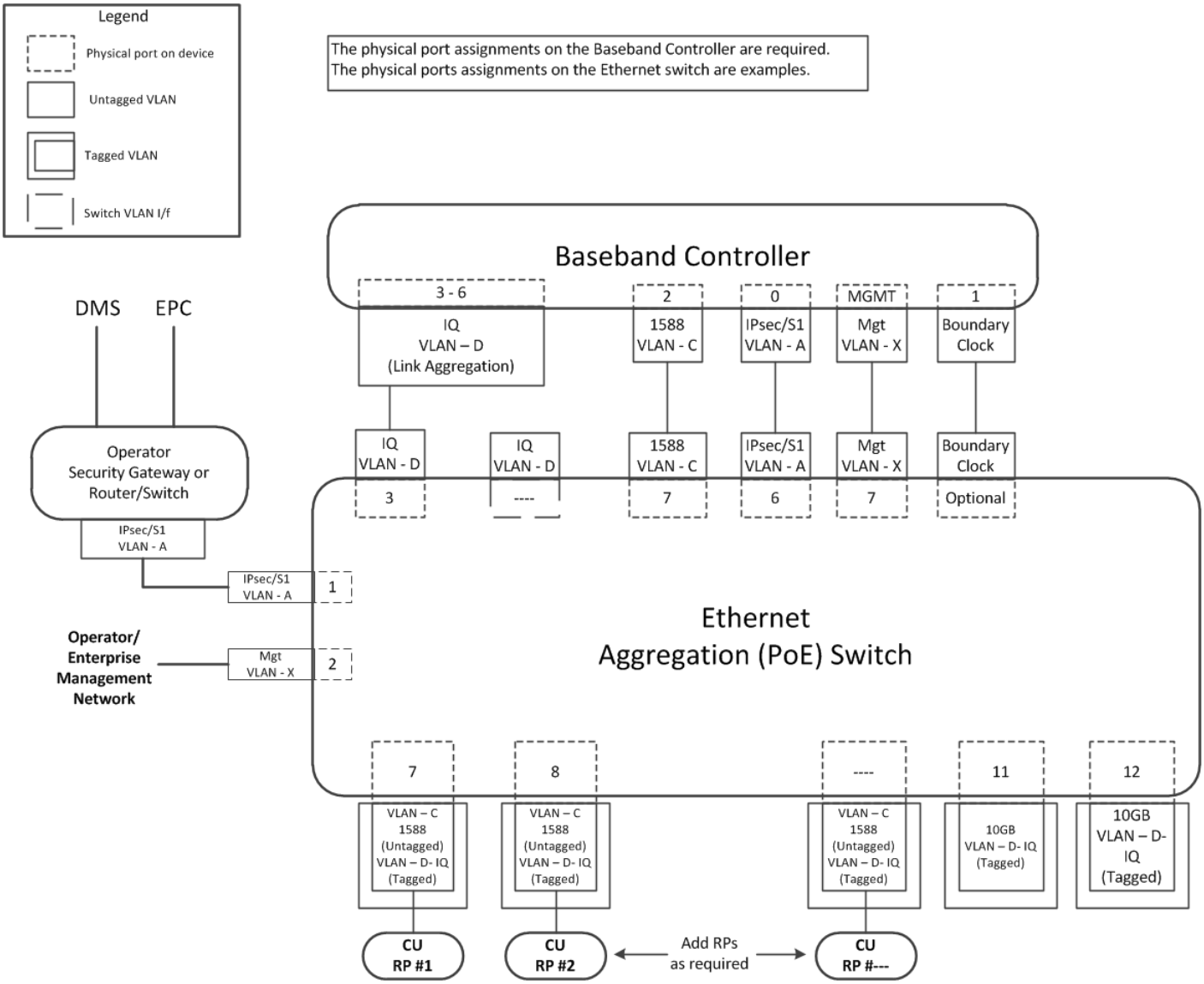


Table 5-1. Ethernet switch port assignments

Port #	Destination	VLAN Type	VLAN ID
1	Backhaul Router/Switch	Untagged	IPsec/S1
2	Management Network Enterprise	Untagged	
3	Link Aggregation	Tagged	IQ
4	BC - port 7-10	Untagged	Link Aggregation
5	BC - port 2	Untagged	1588
6	BC - port 0	Untagged	IPSec/S1
7	BC – MGT	Untagged	Management
8	CU1/RP1	Tagged Untagged	IQ 1588
9	CU1/RP2	Tagged Untagged	IQ 1588
10	Add RP as required	Tagged Untagged	IQ 1588
11	Add RP as required	Tagged Untagged	IQ 1588
12	Add RP as required	Tagged Untagged	IQ 1588
13	Add RP as required	Tagged Untagged	IQ 1588
14	Add RP as required	Tagged Untagged	IQ 1588
15	Add RP as required	Tagged Untagged	IQ 1588
16	Add RP as required	Tagged Untagged	IQ 1588
17	Add RP as required	Tagged Untagged	IQ 1588
18	Add RP as required	Tagged Untagged	IQ 1588

Table 5-1. Ethernet switch port assignments

Port #	Destination	VLAN Type	VLAN ID
19	Add RP as required	Tagged Untagged	IQ 1588
20	Add RP as required	Tagged Untagged	IQ 1588
21	Add RP as required	Tagged Untagged	IQ 1588
22	Add RP as required	Tagged Untagged	IQ 1588
23	Add RP as required	Tagged Untagged	IQ 1588
24	Add RP as required	Tagged Untagged	IQ 1588
Optional	BC - port 1	Untagged	Boundary Clock

NOTE

CommScope has certified Cisco 2960-X and HP 2530 series Ethernet switches in the OneCell network.

NOTE

The Uplink Multicast feature in OneCell requires IGMP snooping configuration changes on all Ethernet switches.

NOTE

IGMP snooping monitors IGMP traffic between multicast routers and hosts, and uses learned information to forward traffic to interfaces who's clients want to receive the traffic. In the absence of a multicast router in a network, an IGMP querier is configured to solicit requests from hosts that want to receive IP multicast traffic.

Configuring aggregate switches

Cisco switch

Configure IP Multicast on the switch. Configure IGMP snooping and IGMP querier on IQ and 1588 VLAN interfaces at the global prompt.

1. Log into the switch and configure IP Multicast routing. This will by automatically enable per port Multicast routing.

   ```
   switch# enable
   switch# configure terminal
   swtich(config)# ip multicast-routing
   ```

2. Configure IGMP snooping and querier at the global prompt.

   ```
   switch(config)# ip igmp snooping querier
   ```

3. Disable IGMP snooping on Management, IPsec/S1, and 1588-only interfaces.

   Syntax: no ip igmp snooping vlan <vlan-id>

   Example:

   ```
   switch (config)# no ip igmp snooping vlan 399
   switch (config)# no ip igmp snooping vlan 211
   ```

4. Enable jumbo frames on IQ vlan interfaces.

   ```
   switch(config)# system mtu jumbo 9198
   ```

5. Configure port channel load balancing.

   ```
   switch(config)# port-channel load-balance src-dst-ip
   ```

6. Log out of the switch.

Sample Cisco configuration

```
Cisco-SW1#show running-config
Building configuration...

Current configuration : 7109 bytes
!
! No configuration change since last restart
! NVRAM config last updated at 05:40:02 UTC Wed Aug 3 2016
!
```

```
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname SOAK-SW1
!
boot-start-marker
boot-end-marker
!
enable password 7 104F000B13161C0A
!
no aaa new-model
switch 1 provision ws-c2960x-24td-l
!
!
ip igmp snooping querier
no ip igmp snooping vlan 399
no ip igmp snooping vlan 211
no ip igmp snooping vlan 280
no ip igmp snooping vlan 230
!
mls qos
!
crypto pki trustpoint TP-self-signed-446807296
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-446807296
 revocation-check none
 rsakeypair TP-self-signed-446807296
!
!
crypto pki certificate chain TP-self-signed-446807296
 certificate self-signed 01
  30820229 30820192 A0030201 02020101 300D0609 2A864886 F70D0101
05050030
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D
43657274
  69666963 6174652D 34343638 30373239 36301E17 0D313630 38303330
35343030
  315A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403
1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3434
36383037
```

```
  32393630 819F300D 06092A86 4886F70D 01010105 0003818D 00308189
02818100
  C84BCC56 F83BD2A9 E4148CFB D3C18BC2 1F616439 69B52CC4 6AF5A351
A67F3C4F
  A42369CC 16BC6D68 0F88E41C 535550A1 85BBF515 66A93A76 B5668EE5
7638FEC9
  00B221E1 EF613285 375F98F1 63F7634B D07C38B6 E2604654 CDD8359E
952BD470
  05988CF9 B909C830 270EF6E3 CB6B4B1A 745D7B24 BFA557B4 6DC35E9C
B3994FEB
  02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F
0603551D
  23041830 168014BF 453BCF1D 307BAEB2 C298DA6F AAA57473 BEEC6F30
1D060355
  1D0E0416 0414BF45 3BCF1D30 7BAEB2C2 98DA6FAA A57473BE EC6F300D
06092A86
  4886F70D 01010505 00038181 006C74E7 7363409C 0A8C4A07 E7F56282
14691620
  26F25580 7BD60850 971C5DB6 DA1A3845 8E63C19B 2ACC9180 0142A792
E0A09061
  76D27A78 D867782F F9B4107E 91C8644C E7736783 29B69A0D 66AB1BC0
5FA34417
  35259C74 96806102 8572EEE7 95AAF18D 9B6CB5AD 5EF26936 1FA8571A
8E31E6EA
  E1DFA55E BEAC7368 40D6B8D3 F5
        quit
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
!
port-channel load-balance src-dst-ip
!
vlan internal allocation policy ascending
!
!
class-map match-all 1588
  match access-group 100
!
policy-map 1588
 class 1588
   set dscp 63
!
!
```

```
!
!
!
no macro auto monitor
!
interface Port-channel1
 switchport access vlan 10
 switchport mode access
!
interface Port-channel2
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0
 ip address x.x.x.x 255.255.255.0
!
interface GigabitEthernet1/0/1
 switchport trunk native vlan 211
 switchport trunk allowed vlan 10,211
 switchport mode trunk
 mls qos trust dscp
 service-policy input 1588
!
interface GigabitEthernet1/0/2
 switchport trunk native vlan 211
 switchport trunk allowed vlan 10,211
 switchport mode trunk
 mls qos trust dscp
 service-policy input 1588
!
interface GigabitEthernet1/0/3
 switchport trunk native vlan 211
 switchport trunk allowed vlan 10,211
 switchport mode trunk
 mls qos trust dscp
 service-policy input 1588
!
interface GigabitEthernet1/0/4
 switchport trunk native vlan 211
 switchport trunk allowed vlan 10,211
 switchport mode trunk
 mls qos trust dscp
 service-policy input 1588
!
```

```
interface GigabitEthernet1/0/5
 switchport trunk native vlan 211
 switchport trunk allowed vlan 10,211
 switchport mode trunk
 mls qos trust dscp
 service-policy input 1588
!
interface GigabitEthernet1/0/6
 switchport trunk native vlan 211
 switchport trunk allowed vlan 10,211
 switchport mode trunk
 mls qos trust dscp
 service-policy input 1588
!
interface GigabitEthernet1/0/7
 switchport trunk native vlan 211
 switchport trunk allowed vlan 10,211
 switchport mode trunk
 mls qos trust dscp
 service-policy input 1588
!
interface GigabitEthernet1/0/8
 switchport trunk native vlan 211
 switchport trunk allowed vlan 10,211
 switchport mode trunk
 mls qos trust dscp
 service-policy input 1588
!
interface GigabitEthernet1/0/9
 switchport trunk native vlan 211
 switchport trunk allowed vlan 10,211
 switchport mode trunk
 mls qos trust dscp
 service-policy input 1588
!
interface GigabitEthernet1/0/10
 switchport trunk native vlan 211
 switchport trunk allowed vlan 10,211
 switchport mode trunk
 mls qos trust dscp
 service-policy input 1588
!
interface GigabitEthernet1/0/11
 switchport access vlan 280
```

```
 switchport mode access
!
interface GigabitEthernet1/0/12
 switchport access vlan 399
 switchport mode access
!
interface GigabitEthernet1/0/13
 description "setup CU-48 mgmt interface "
 switchport access vlan 280
 switchport mode access
!
interface GigabitEthernet1/0/14
 description "setup CU-48 IP-Sec interface "
 switchport trunk allowed vlan 230
 switchport mode trunk
!
interface GigabitEthernet1/0/15
 description "setup CU-48 1588 interface "
 switchport access vlan 211
 switchport mode access
 mls qos trust dscp
 service-policy input 1588
 no ip igmp snooping tcn flood
!
interface GigabitEthernet1/0/16
 description CU-eth1 IQ
 switchport access vlan 10
 switchport mode access
 channel-protocol lacp
 channel-group 1 mode passive
!
interface GigabitEthernet1/0/17
 description CU-eth1 IQ
 switchport access vlan 10
 switchport mode access
 channel-protocol lacp
 channel-group 1 mode passive
!
interface GigabitEthernet1/0/18
 description CU-eth1 IQ
 switchport access vlan 10
 switchport mode access
 channel-protocol lacp
 channel-group 1 mode passive
```

```
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
 description IQ uplink out for 2 switch
 switchport access vlan 10
 switchport mode access
 channel-protocol lacp
 channel-group 2 mode active
!
interface GigabitEthernet1/0/21
 description IQ uplink out for 2 switch
 switchport access vlan 10
 switchport mode access
 channel-protocol lacp
 channel-group 2 mode active
!
interface GigabitEthernet1/0/22
 description IQ uplink out for 2 switch
 switchport access vlan 10
 switchport mode access
 channel-protocol lacp
 channel-group 2 mode active
!
interface GigabitEthernet1/0/23
 switchport access vlan 211
 switchport mode access
 mls qos trust dscp
 service-policy input 1588
!
interface GigabitEthernet1/0/24
 description UPlink-SIQ-core
 switchport trunk allowed vlan 211,230,280,399
 switchport mode trunk
!
interface GigabitEthernet1/0/25
!
interface GigabitEthernet1/0/26
!
interface TenGigabitEthernet1/0/1
!
interface TenGigabitEthernet1/0/2
 switchport access vlan 10
 switchport mode access
```

```
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 1.1.1.1 255.255.255.0
!
ip http server
ip http secure-server
!

access-list 100 permit udp any range 319 320 any
!
!
!
line con 0
 password 7 10480E03514244
line vty 0 4
 password 7 0820455C1F180B16
 login
line vty 5 15
 password 7 0820455C1F180B16
 login
!
!
end
```

Accessing the Web GUI

The controller GUI is accessible over secure http. The application for the GUI listens on port 6002. Use the controller GUI to configure components after initial hardware installation, view status and statistics of the controller and its associated Radio Points.

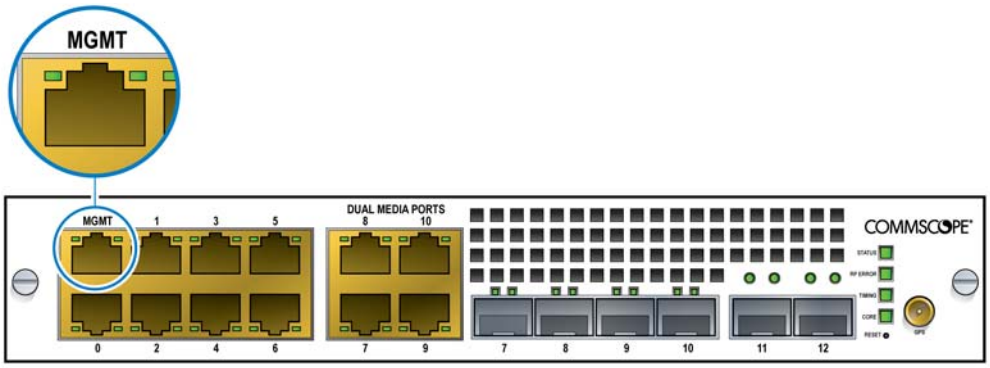
The following browsers are supported by the Web GUI:

- Mozilla Firefox
- Google Chrome
- Microsoft Internet Explorer
- Microsoft Edge
- Safari on Mac Only

NOTE

Web GUI is not supported on Safari for Windows, Linux or any other Operating System

1. Connect a laptop to the MGMT port on the Baseband Controller.



2. Assign a Static IP address to the laptop.

   Configure the following network settings:

   - IP address: 192.168.8.20
   - Subnet mask: 255.255.255.0
   - Gateway: 192.168.8.1

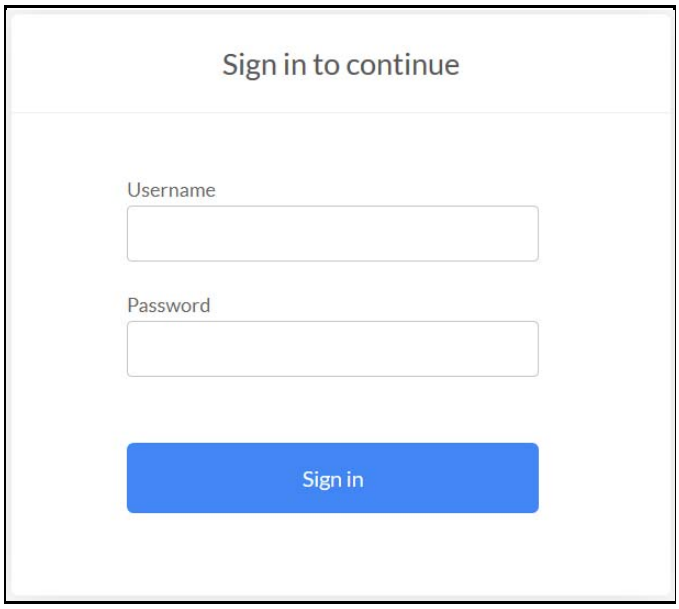
3. Open a supported browser.
4. Enter URL.

   https://192.168.8.1:6002

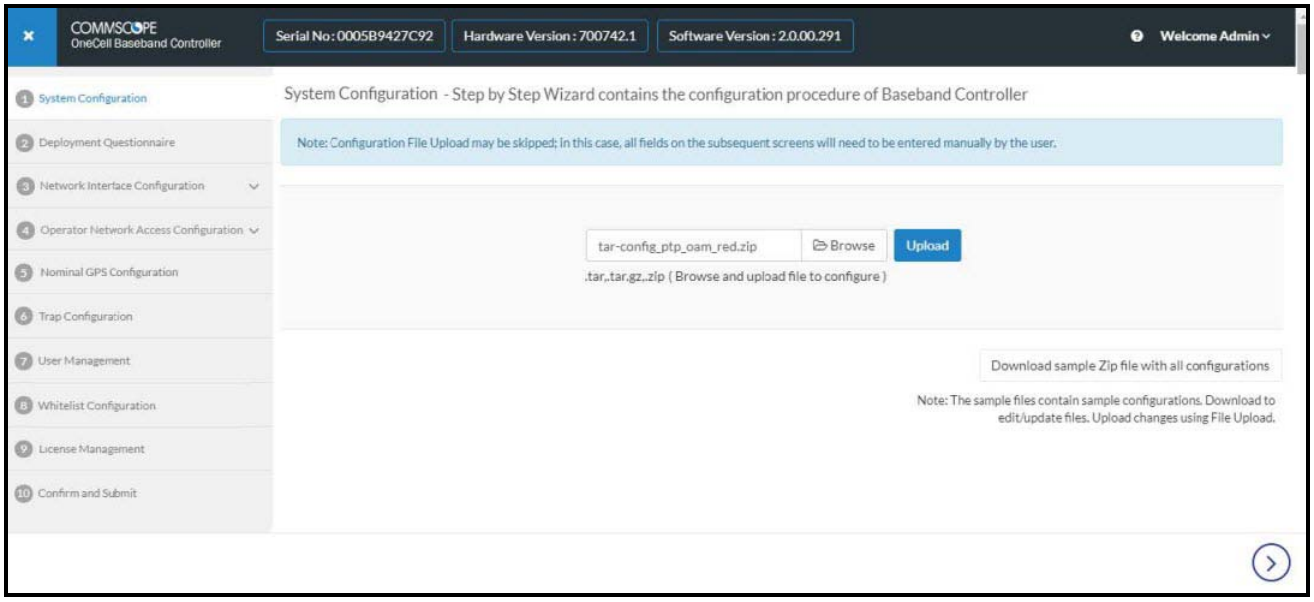
5. Sign in to the Web GUI.

   User ID: admin

   Password: admin1234



The Installation mode page displays.



Configuring the Baseband Controller

There are two methods of configuring the OneCell Baseband Controller.

- upload an XML file with Baseband Controller operator parameters – Uploading XML configuration file
- configure manually using installation wizard

  NOTE: To configure manually, skip to Configuring the Baseband Controller manually.

Uploading XML configuration file

1 Create a *.tar or *.tar.gz or *.zip file containing:

- onecell-config.xml file (Operator provided)

  Contains all the operator parameters such as HeMS and Security Gateway URL information, and the IP addresses for all of the Baseband Controller interfaces.
- Operator Root Certificate
- Licenses bin file (Optional)
- Radio Point Whitelist Configuration file (Optional)

NOTE: You may download a sample configuration file and modify it for the operator's configuration.

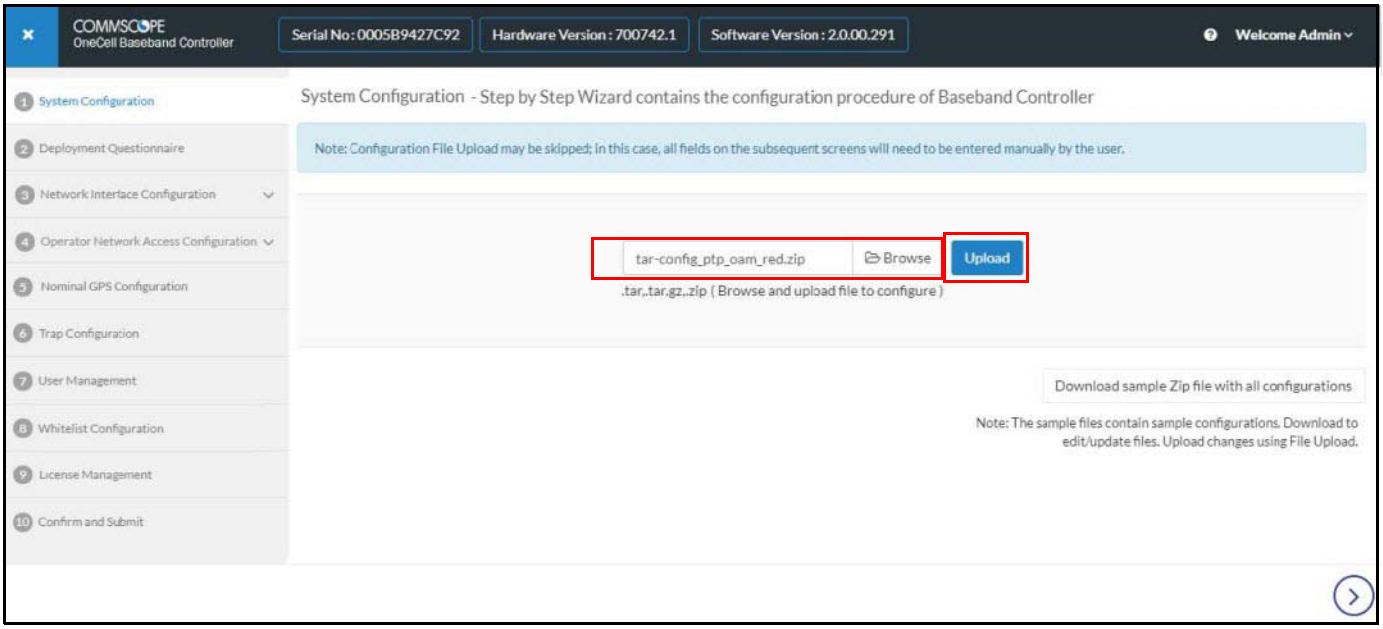


Table 5-2. Baseband Controller operator parameters, configuration file

Parameter	Description
Network Topology	
Number of IPSec Tunnels	Number of IPSec Tunnels to be used by the Baseband Controller • none – If Tunnel mode is Non IPSec • one – If Tunnel mode is Single IPSec Tunnel • two – If Tunnel mode is Dual IPSec Tunnel
EPC Traffic Mode	Tunnel Mode for EPC Communication • ipsecTunnel1 – Single IPSec Mode • nonIPSec – Non IPSec Mode
HeMS Traffic Mode	Tunnel Mode for EPC Communication • ipsecTunnel1 – Single IPSec Mode • ipsecTunnel2 – Dual IPSec Mode • nonIPSec – Non IPSec Mode
CA Traffic Mode	Tunnel Mode for EPC Communication • ipsecTunnel1 - Single IPSec Mode • ipsecTunnel2 - Dual IPSec Mode • nonIPSec - Non IPSec Mode • noCA - No CA Mode
Timing Source	
GPS	Timing Source is GPS
Boundary Clock Interface Port	• boundaryClock – Timing Source is PTP with a dedicated Boundary Clock port configured • backHaul – Timing Source is PTP with no dedicated Boundary Clock port configured
Redundancy	• True – BC Redundancy Enabled • False – BC Redundancy Disabled (Standalone)
Network Interface Port Configurations – Management Interface	
IP Address Assignment	• Static mode – IP Addresses are configured manually. • DHCP (Client) mode – The DHCP client fetches IP addresses from the DHCP server and assigns them to the interface. User configuration is not required.
IP Address	IP Address of the interface <A.B.C.D>

Table 5-2. Baseband Controller operator parameters, configuration file

Parameter	Description
Subnet Mask or CIDR (Classless Inter-Domain Routing)	Network subnet mask of the client CIDR format [1-32]
Default Gateway	The IP Address of the router on this subnet <A.B.C.D>
Primary DNS Address	IP Address of the Primary DNS Server <A.B.C.D>
Secondary DNS Address	IP Address of the Secondary DNS Server. <A.B.C.D> **Note:** This field is optional if the Primary DNS Address is configured.
Network Interface Port Configurations – EPC Interface	
IP Address Assignment	• Static mode – IP Addresses are configured manually. • DHCP (Client) mode – The DHCP client fetches IP addresses from the DHCP server and assigns them to the interface. User configuration is not required.
IP Address	IP Address of the interface <A.B.C.D>
Subnet Mask or CIDR (Classless Inter-Domain Routing)	Network subnet mask of the client CIDR format [1-32]
Default Gateway	The IP Address of the router on this subnet <A.B.C.D>
Primary DNS Address	IP Address of the Primary DNS Server <A.B.C.D>
Secondary DNS Address	IP Address of the Secondary DNS Server. <A.B.C.D> **Note:** This field is optional if the Primary DNS Address is configured.
VLAN ID	Access Mode range = 0 Trunk Mode range = 11 to 4095
MTU	Range = 64 to 1998
Network Interface Port Configurations – HeMS Interface	

Table 5-2. Baseband Controller operator parameters, configuration file

Parameter	Description
IP Address Assignment	• Static mode - IP Addresses are configured manually • DHCP (Client) mode - The DHCP client fetches IP addresses from the DHCP server and assign to the interface; user configuration is not required
IP Address	IP Address of the interface <A.B.C.D>
Subnet Mask or CIDR (Classless Inter-Domain Routing)	Network subnet mask of the client CIDR format [1-32]
Default Gateway	The IP Address of the router on this subnet <A.B.C.D>
Primary DNS Address	IP Address of the Primary DNS Server <A.B.C.D>
Secondary DNS Address	IP Address of the Secondary DNS Server. <A.B.C.D> **Note:** This field is optional if the Primary DNS Address is configured.
VLAN ID	Access Mode range = 0 Trunk Mode range = 11 to 4095
MTU	Range = 64 to 1998
Network Interface Port Configurations – Boundary Clock Configuration	
IP Address Assignment	• Static mode – IP Addresses are configured manually. • DHCP (Client) mode – The DHCP client will fetch IP addresses from the DHCP server and assign to the interface; User configuration is not required.
IP Address	IP Address of the interface <A.B.C.D>
Subnet Mask or CIDR (Classless Inter-Domain Routing)	Network subnet mask of the client CIDR format [1-32]
Default Gateway	The IP Address of the router on this subnet <A.B.C.D>
Primary DNS Address	IP Address of the Primary DNS Server <A.B.C.D>

Table 5-2. Baseband Controller operator parameters, configuration file

Parameter	Description
Secondary DNS Address	IP Address of the Secondary DNS Server <A.B.C.D>
VLAN	Access Mode range = 0 Trunk Mode range = 11 to 4095
MTU	Range = 64 to 1998
Network Interface Port Configurations – FrontHaul Configuration	
Baseband Controller ID (BC ID)	The ID of the Baseband Controller Range = 1 to 254
VLAN ID (For IQ)	The VLAN ID used for the IQ traffic Access Mode range = 0 Trunk Mode range = 11 to 4095
Timing Cluster ID (TC ID)	The Timing Cluster ID is used for generating the Multicast IP Address for 1588 packets and the Cluster Multicast IP Address used in pacemaker. Range = 1 to 254
Network Interface Port Configurations – Redundancy	
IP Address Assignment	• Static mode – IP Addresses are configured manually • DHCP (Client) mode – The DHCP client fetches IP addresses from the DHCP server and assigns them to the interface. User configuration is not required.
IP Address	IP Address of the interface <A.B.C.D>
Subnet Mask or CIDR (Classless Inter-Domain Routing)	Network subnet mask of the client CIDR format [1-32]
Default Gateway	The IP Address of the router on this subnet <A.B.C.D>
Primary DNS Address	IP Address of the Primary DNS Server <A.B.C.D>
Secondary DNS Address	IP Address of the Secondary DNS Server <A.B.C.D>

Table 5-2. Baseband Controller operator parameters, configuration file

Parameter	Description
BC State	• Active – Active member of the cluster • StandBy – StandBy member of the cluster
Virtual Cell ID	A unique ID used to tie LTE service parameters together on a Baseband Controller running in Active mode in a cluster. **Note:** This field is mandatory if Active State is selected.
Operator Configuration – Security Gateway 1 Configuration	
Security Gateway FQDN/IP Address	The Baseband Controller establishes a secure tunnel connection with this gateway for S1 or OAM traffic. IP address <A.B.C.D> or FQDN
Address Type	• Static – When set to Static, the user/operator should define a static Tunnel Inner Address for the S1 tunnel • Dynamic – When configured Dynamic - the address is dynamically assigned by the Security Gateway during IKE processing
Tunnel Inner Address	Tunnel IP Address provided by the Security Gateway after successful session establishment <A.B.C.D>
Tunnel CIDR	CIDR format [1 - 32]
Tunnel Internal DNS	IP Address <A.B.C.D>
Exclude Configuration Payload (CP)	• True – Configuration Payload is excluded during IKE processing. • False – Configuration Payload is included during IKE processing.
Operator Configuration – Security Gateway 2 Configuration	
Security Gateway FQDN/IP Address	The Baseband Controller establishes a secure tunnel connection with this gateway for S1 or OAM traffic. IP address <A.B.C.D> or FQDN
Address Type	• Static – When set to Static, the user/operator should define a static Tunnel Inner Address for the S1 tunnel • Dynamic – When configured Dynamic - the address is dynamically assigned by the Security Gateway during IKE processing
Tunnel Inner Address	Tunnel IP Address provided by the Security Gateway after successful session establishment <A.B.C.D>
Tunnel CIDR	CIDR format [1 - 32]

Table 5-2. Baseband Controller operator parameters, configuration file

Parameter	Description
Tunnel Internal DNS	IP Address <A.B.C.D>
Exclude Configuration Payload (CP)	• True – Configuration Payload is excluded during IKE processing. • False – Configuration Payload is included during IKE processing.
Operator Configuration – Root Certificate File	
Root Certificate File Name	Name of the Operator's Certificate file. **Note:** The Certificate file has to be added as part of the archive file for uploading the configuration
Operator Configuration - HeMS Configuration	
HeMS URL	The HeMS URL defines the Home eNB Management Server that resides in the Operator's network.
Operator Configuration – CA Server Configuration	
CA Server URL	The (URL) value to be used in the HTTP Post Request Header to the CA Server
CA Server Identity	Operator CA server name or ID (of the CMP Server or sub CMS CA server)
SA Certificate Identifier	Unique Identifier located in the certificate issued by the Certificate Authority (CA). It is used for Subject Alt Name of the certificate. Contains the Baseband Controller's MAC address <string> Example: 0005B94238A0.commscope1.com
PKI Message Hash	The hash algorithm used for Protection and Popo fields of CMP-IR and CMP-KUR messages sent to the CA. sha1, sha256 Default: sha256
Operator Configuration – PTP Servers	
PTP Server	A list of PTP Server IP Addresses separated by commas IP Address <A.B.C.D>
Nominal GPS Configuration	
Position Estimate	
Latitude Sign	• north • south

Table 5-2. Baseband Controller operator parameters, configuration file

Parameter	Description
Degrees of Latitude	Value (N) is derived by the formula: N <223 X / 90 < N + 1 where X is the latitude in degrees (0^o..90^o) Type: INTEGER (0..223 - 1)
Degrees of Longitude	Value (N) is derived by the formula: N <224 X / 360 < N + 1 were X is the longitude in degrees (-180^o.. +180^o) Type: INTEGER (-223 .. 223)
Altitude Info	
Degrees of Altitude	• height • depth
Altitude	The relationship between the value (N) and the altitude (a) in meters it describes as N < a < N+1, except for N=215-1, for which the range is extended to include all greater values of (a). Type: INTEGER (0..215 - 1)
Uncertainty Altitude	Uncertainty altitude “h” expressed in meters, is derived from the “Uncertainty Altitude” k, by: h=45 x (1.025k - 1) Type: INTEGER (0..127)
Position Estimate	
Uncertainty Semi-Major	Uncertainty “r” is derived from the “uncertainty code” k by: r = 10 x (1.1k - 1) Type: INTEGER (0..127)
Uncertainty Semi-Minor	Uncertainty “r” is derived from the “uncertainty code” k by: r = 10 x (1.1k - 1) Type: INTEGER (0..127)
Orientation of MajorAxis	Type: INTEGER (0..179)
Confidence	Percentage of confidence Type: INTEGER (0..100)
SNMP Configuration	
SNMP Traps	• True • False If true, SNMP traps will be generated from OneCell devices
SNMP IP address/Domain Name	The IP address or FQDN of the SNMP management server

Table 5-2. Baseband Controller operator parameters, configuration file

Parameter	Description
SNMP Port	The listening port of the SNMP management server
User-based Security Model (USM)	Values: • Yes • No If value is Yes, you will be able to configure the authentication and privacy fields. If value is No, SNMP will not be authenticated.
UserName	The default is the Baseband Controller's MAC ID
Auth Protocol	The authentication protocol Supported values: • HMAC-SHA-96 (default) • HMAC-MD5-96
Auth Key	User defined string
Private Protocol	Optional protocol Supported values: • CBC-DES • None (default)
Private Key	User defined string
SNMP Enabled Alarms	List of SNMP Trap Names that can be enabled or disabled for trap generation from the OneCell device
Whitelist Configuration	
Whitelist	Provides Radio Point MAC Addresses for Whitelist in-line in the config.xml When in-line Whitelist is provided, the Whitelist file will not be considered for upload
Whitelist File	Name of the file when Whitelist configuration is provided in an external file. **Note:** The Whitelist file has to be added as part of the archive file for uploading the configuration
License Configuration	
License File	Name of the license binary file **Note:** The license file needs to be added as part of the archive file for uploading the configuration.

2 Go to the Installation Wizard – System Configuration menu item.

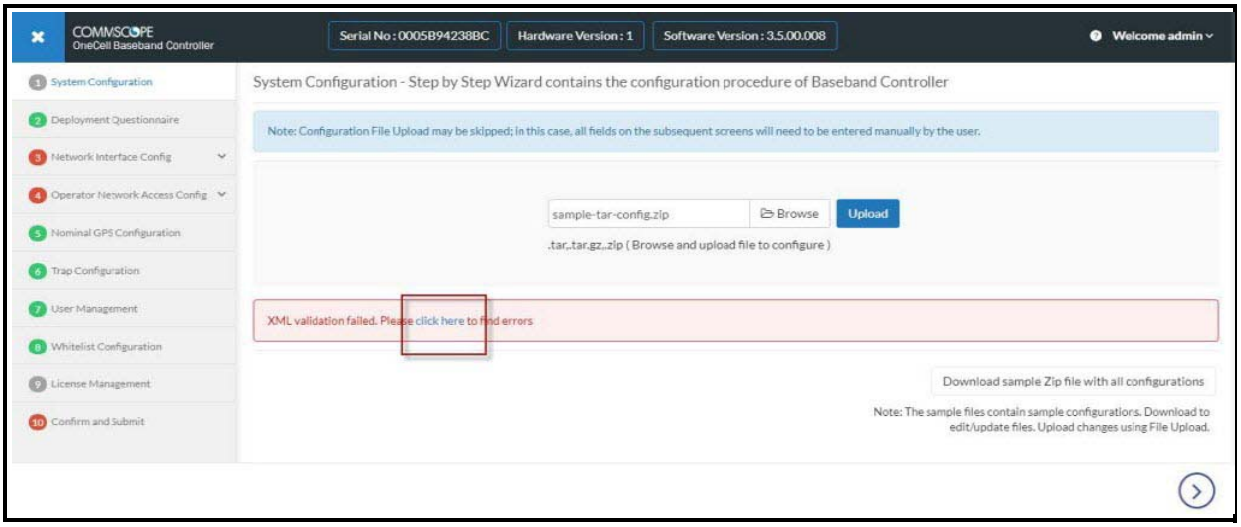
3 Upload the configuration file.

- Click Choose File and enter the name of the *.tar or *.tar.gz or *.zip file that contains operator access information.
- Click **Upload**.

Observe the colors of the menu items on the left side of the screen.

Color	Description
Gray	Configuration is either not applicable to this deployment, or has not yet been configured.
Green	Configuration has been successfully validated.
Red	Errors have been encountered that must be corrected.

If the XML file fails validation, click the hyperlink to locate the errors.



Configuring the Baseband Controller manually

If you choose to enter the configuration manually, use one of the following methods to advance to the next step.

- Select the right arrow in the bottom right corner of the screen
- Select the menu titled ‘Deployment Questionnaire’
- Select GPS Information if the BC is in GPS timing mode

Table 5-3. Deployment Wizard steps

Step	Menu Name	Description
1	System Configuration	You have the option, in the System Configuration screen, to upload a configuration file that contain all information necessary to complete the configuration cycle. If no configuration file is used, you will enter configuration manually one screen at a time.
2	Deployment Questionnaire	In the Installation Wizard, you will be asked to complete a Topology Questionnaire. This questionnaire provides information such as the IPsec tunnel configuration, timing sources and inclusion in a Redundancy cluster.
3	Network Interface configuration	Network Interface configuration contains sub-menus for configuring the following network interface items: • Management Port • Backhaul • Boundary Clock – If timing source is from a PTP server • Fronthaul • High Availability
4	Operator Network Access configuration	Operator Network Access configuration contains sub-menus for configuring the following operator access items: • HeMS • Security • PTP Server • CA Server • Root Certificate
5	Nominal GPS Configuration	This screen contains configuration for Nominal GPS parameters for Radio Points.
6	Trap Configuration	This screen contains configuration for SNMP traps and displays a list of device alarms.
7	User Management	This screen is used to create and edit users and enter authentication information for local, LDAP and RADIUS servers.
8	Whitelist Configuration	This screen is used to enter Whitelist Radio Point MAC addresses manually, separated by commas, or upload Radio Point MAC addresses from an external file.
9	License Management	This screen is used to view existing licenses, upload a file with licenses, and download a license report.

Table 5-3. Deployment Wizard steps *(continued)*

Step	Menu Name	Description
10	Confirm and submit	From this screen the user views a summary of the configuration which can be modified if needed. When configuration is correct the user applies the configuration to the Baseband Controller by authorizing a reboot.

For more information on configuring the BC manually, see *OneCell® Administration* (913026).

Configuring firewall ports

In order for the OneCell device to communicate with DMS, firewall ports need to be configured.

Table 5-4. Configurable DMS service and protocol ports

Row #	Service	TCP / UDP	Protocol port	Protocol	Configurable	Use
1	HDM Admin console	TCP	9002	HTTP	Install/Upgrade only	HDM Admin console
	HDM Managed console	TCP	7003	HTTP	Install/Upgrade only	HDM Managed console
2	Load Balancer	TCP	Configured port	HTTP	Load Balancer setup only	Load Balancer
3	DMS Admin console	TCP	7001	HTTP	Install/Upgrade only	DMS Admin console
4	DMS Network console DMS Device console DMS Service Provisioning	TCP	8001 8011	HTTP	Install/Upgrade only	DMS consoles
5	DMS to Device communication	TCP	22 80 21	SSH SFTP FTP HTTP	No	DMS to Device
6	DMS to Device communication	TCP	22 80 21	SSH SFTP FTP HTTP	No	Device to DMS

Table 5-4. Configurable DMS service and protocol ports *(continued)*

Row #	Service	TCP / UDP	Protocol port	Protocol	Configurable	Use
7	Device to DMS communication	TCP	7003	HTTP	Install/Upgrade only	Device to DMS
8	XML DB access	TCP	Configured port	FTP	Install/Upgrade only	XML DB access, To copy ODF/ Factory files into Database for import.

Chapter 6

Verifying the OneCell installation

Overview

This chapter describes how to verify component installation and configuration and make sure everything is operating properly after installation and configuration.(This process is called commissioning.)

The tools used to verify the OneCell installation are:

- Baseband Controller and Radio Point LEDs
- Baseband Controller Web GUI
- Ping tests
- User Equipment (UE) logs

Verify the OneCell system installation

To verify that the OneCell system installation is operating, check the Baseband Controller LEDs. The STATUS, TIMING and CORE LEDs should be solid green.

For more information on troubleshooting the OneCell system installation, see Baseband Controller LED patterns on page B-2.

Figure 6-1. Baseband Controller front panel

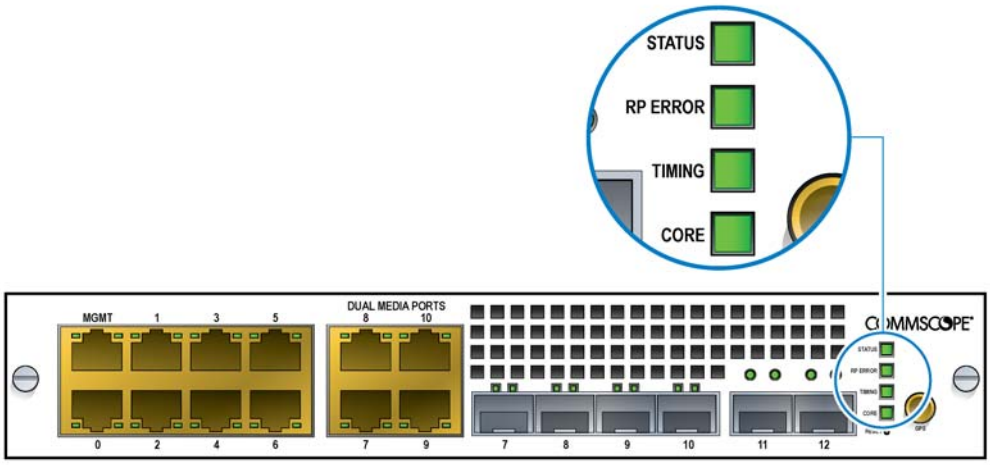


Table 6-1. OneCell Baseband Controller operational status

Case	Status LED	RP ERR LED	TIMING LED	CORE LED
Powered On	Green, solid (3 Sec)	Green, solid (3 Sec)	Green, solid (3 Sec)	Green, solid (3 Sec)
Internet - Yes	Green, solid	OFF	Green, solid	Green, solid
IPsec - Yes				
Timing - Yes				
Config from DMS - Yes				
Remotes connected - Yes				
Connection to MME - Yes				
Sectors UP - Yes				

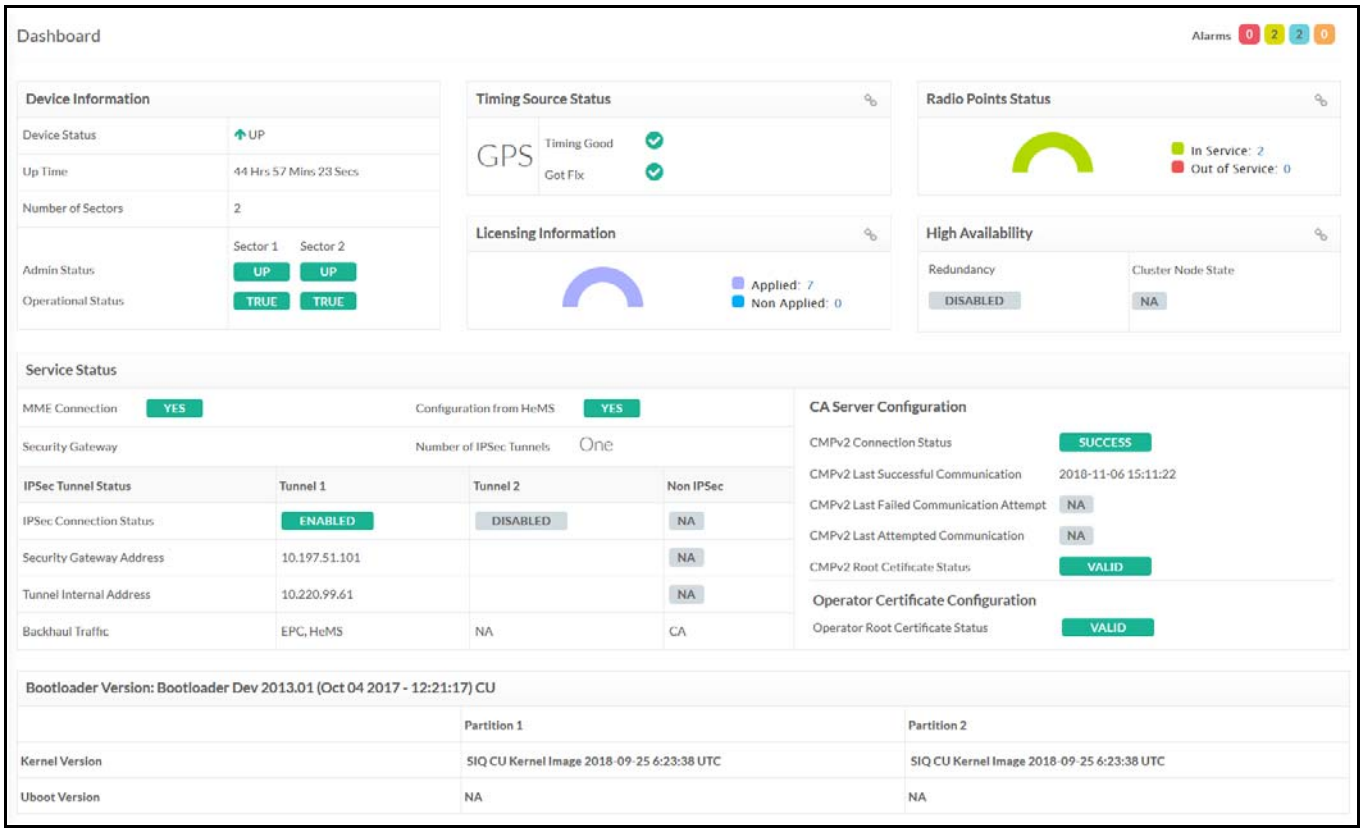
Verify the Baseband Controller installation

Once the BC reboot is complete, log into the WebGUI to display the Management Mode Dashboard.

Check the following information on the Dashboard:

- Device Information
- Timing Source Status
- Radio Points Status
- Service Status
- CA Server Configuration

Figure 6-2. Management Mode Dashboard



Device Information

The Device Information section displays the status of the overall OneCell device components at a glance. You can view the current status of the Baseband Controller.

Verify that Device Status, Admin Status and Operational Status are all green.

Table 6-2. Device Information parameters

Parameter	Description
Device Status	The current operational status of the device. Supported values: • Up • Initializing • Error • Disabled

Table 6-2. Device Information parameters *(continued)*

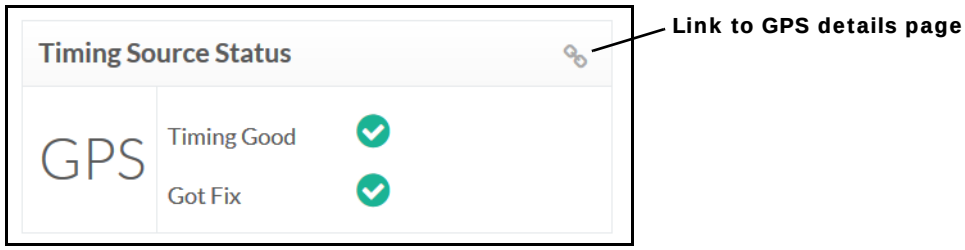
Parameter	Description
Up Time	The amount of time the OneCell has been up. HH:MM:SS
Number of Sectors	Number of sectors configured on the device Supported values: • 1 • 2
Admin Status of each Sector	• UP – The OneCell Sector is providing service. (Example: at least one Radio Point has RftxStatus of 'ON') • DOWN – The OneCell Sector is not providing service.
Operational Status of each Sector	Supported values: • TRUE • FALSE

Timing Source Status

This section displays the Timing source of the Baseband Controller, either GPS or PTP (1588).

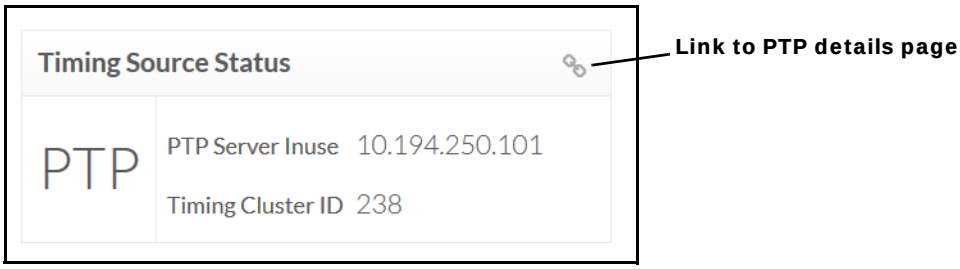
View the Timing Source Status for GPS and ensure that Timing Good and Got Fix are Green.

Figure 6-3. Timing Source Status - GPS



View the Timing Source Status for GPS and ensure that the PTP Server InUse IP address and Timing Cluster ID field have data.

Figure 6-4. Timing Source Status - PTP



Radio Point Status

The chart in this screen shows a visual glance of all the Radio Points status in the Baseband Controller. Green indicates 'In Service'. Red indicates 'Out of Service'.

Verify that the number of RPs installed matches the number of RPs In Service. If not, navigation to the Radio Point Information page. For more information on the Radio Point Information page, see *OneCell® Administration* (913026).

NOTE

Click the Link icon, in the upper right corner of this area, to navigate to the Radio Point Information page.

Service Status

Verify the status of the following:

- MME Connection
- Configuration from HeMS
- IPsec Connection Status
- IPSec Tunnel Status
- CA Server Configuration
- Operator Certificate Configuration

When you see a green status indicator for all entries, your Baseband Controller is functional and ready to operate.

Figure 6-5. Service Status

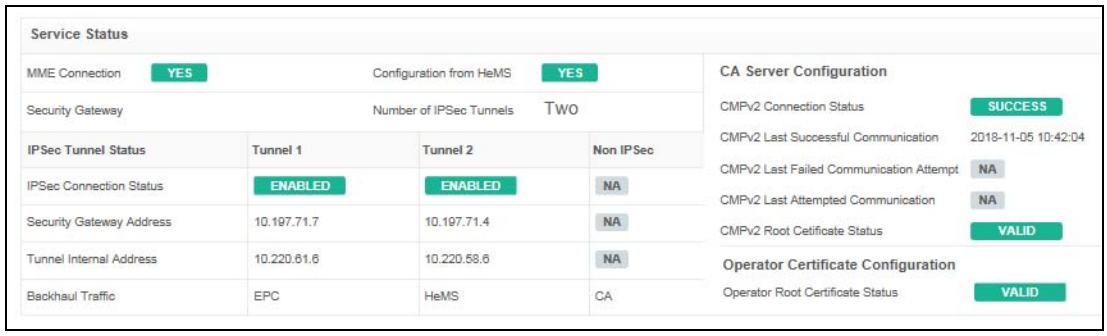


Table 6-3. Service Status

Parameter	Description
MME Connection	• YES – The Baseband Controller has S1AP connection with the MME. • NO – The Baseband Controller does not have S1AP connection with the MME.
Configuration from HeMS	• YES – The Baseband Controller has received the required configuration from HeMS • NO – The Baseband Controller has not received the configuration from HeMS.
Number of IPSec Tunnels	None - tunnel mode is Non IPSec One - tunnel mode is Single IPSec Tunnel Two - tunnel mode is Dual IPSec Tunnel
IPSec Connection Status	YES - A secure connection is established with the Security Gateway NO - No secure connection exists with the Security Gateway NON IPSec - The connection does not use IPSec. Dual Ipsec - The connection uses both OAM and S1 IPSec connections.
IPSec Tunnel (per Tunnel 1, Tunnel 2 or Non IPSec)	
IPSec Connection Status	• ENABLED – Tunnel is established and connected • DISABLED – Tunnel is not established • ERROR – Error occurred during tunnel establishment
Security Gateway Address	IP Address of the Security Gateway through which the tunnel is established
Tunnel Internal Address	Tunnel IP address provided by the Security Gateway after successful session establishment. <A.B.C.D>

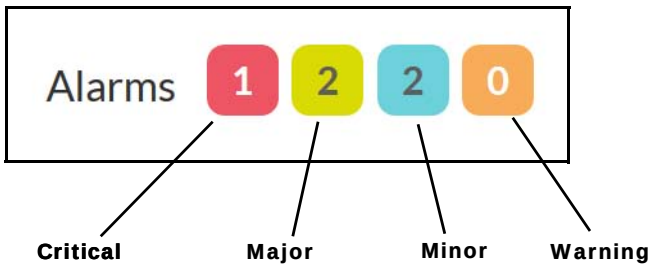
Table 6-3. Service Status

Parameter	Description
Backhaul Traffic	Shows the interfaces (EPC, HeMS and CA) are connected
CA Server Configuration	
CMPv2 Connection Status	Status of the CMPv2 connection. Valid values: •IN-PROGRESS •RE-TRYING •SUCCESS
CMPv2Root Certificate Status	Values supported: • VALID • INVALID
Operator Root Certificate Status	Values supported: • VALID • INVALID
Operator Certificate Configuration	
Operator Root Certificate Status	Values supported: • VALID • INVALID

Alarms snapshot

The alarms snapshot gives a high-level count of alarms by severity level. If any of these colored alarm icons have a non-zero value, clicking on that particular icon brings you to the alarm details screen for that severity level.

Figure 6-6. Alarms



Verify local network connectivity

The Core LED on Baseband Controller front panel helps identify if Local Network Connectivity is available for the IPSec/S1 Interface.

Use ping tests to verify connectivity for other the interfaces on the Baseband Controller.

- Controller Management interface
- Radio Point interface

Table 6-4. CORE LED – local network connectivity issues

State	Events
Red, solid	Internet – No Interface hardware issues

Verify core network connectivity

The core network includes:

- IPsec connection
- Configuration from HeMS
- MME connection

Table 6-5. CORE LED states

State	Events
Green, solid	Power ON Connection to MME – Yes
Amber, Info blink	IPsec – Yes Connection to MME – No
OFF	Firmware upgrade
Red, Info blink	Internet – Yes IPsec – No
Red, solid	Internet – No Interface hardware issues

Table 6-6. STATUS LED – core network connectivity issues

State	Events
Green, Info blink	Firmware upgrade Configuration from HeMS Sectors UP – No
Amber, Info blink	No configuration from HeMS

Verify OneCell RF coverage

To verify the OneCell RF coverage:

- Check connectivity on UEs
- Use UE Apps for checking Serving Cell PCI

  NOTE: Examples of Apps for verifying RF coverage are NEMO, ANITE

- UE Logs can be used for debugging RACH issues during UE connection