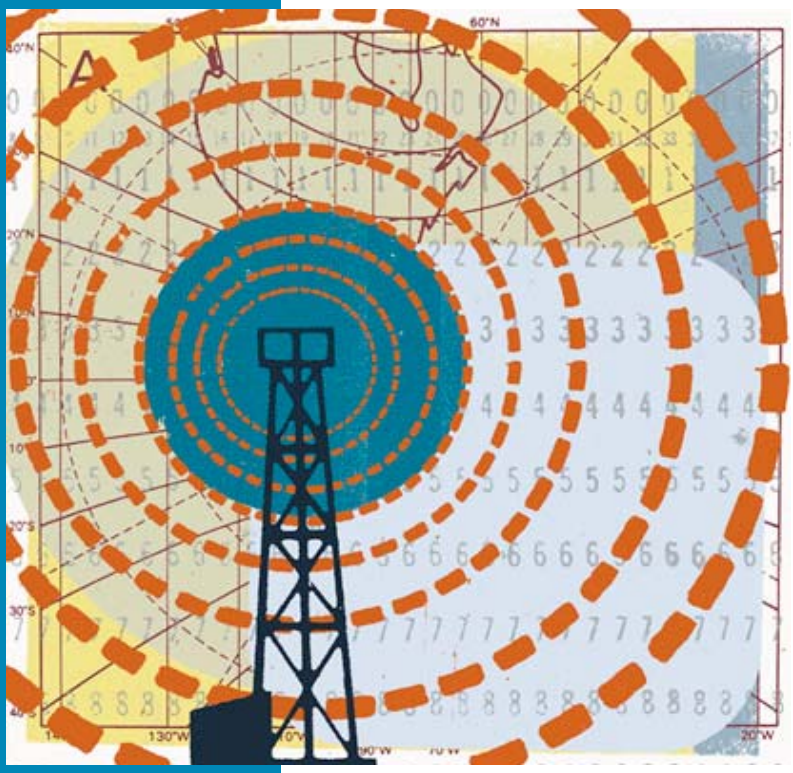
SkyControl EMS Administration Guide



SkyPilot™ NETWORKS

Trilliant

SkyPilot EMS 1.6.2.4
Document Last Revised: July 30, 2010

Contents

About This Guide

This document contains guidelines for performing operations, administration, and maintenance tasks for SkyPilot™ network deployments. Topics discussed include using SkyControl™ to monitor a SkyPilot network and to provision SkyPilot devices, and troubleshooting.

This chapter explains what's in this guide and how it's organized.

Chapter Highlights

- Audience and purpose
- How this guide is organized
- Conventions used in this guide

Audience and Purpose

This guide is intended for administrators who are responsible for managing a SkyPilot network. It explains ongoing operations, administration, and maintenance tasks, such as provisioning SkyPilot devices, customizing a SkyPilot network, and monitoring SkyPilot network status.

This guide assumes administrator-level knowledge of IP networks, basic knowledge of wireless networking, and a familiarity with the information in *Getting Started with the SkyPilot Network*. Additionally, the procedures assume that SkyPilot devices have already been successfully installed according to the procedures in their installation guides. (Complete documentation is available on the Trilliant SkyPilot website at www.skypilot.trilliantinc.com/support/.)

How This Guide Is Organized

This guide is organized as follows:

- Chapter 1, "Introduction," describes the SkyPilot Networks hardware and software components; the operations, administration, and maintenance tasks that you can perform; and how to use the SkyPilot EMS Web interface application.
- Chapter 2, "Operations," describes how to provision SkyPilot devices (either manually or automatically) and provides guidelines for configuring SkyPilot devices.
- Chapter 3, "Administration," describes routine management tasks, such as managing software and customers, configuring security, and creating reports, and directs you to the corresponding detailed procedures.
- Chapter 4, "Maintenance," describes techniques for maintaining your SkyPilot network, as well as solutions to common troubleshooting issues.
- Appendix 5, "Provisioning With SkyControl," provides detailed instructions for configuring provisioning parameters for automatically provisioned devices, and for performing administrative and maintenance functions for your SkyPilot network.

- Appendix A, "Google Earth Management System (GEMS) Reference," provides instructions for preparing network profiles for viewing in Google Earth.
- Appendix B, "Configuring a Firewall for SkyPilot Operations," tells you which ports to open for data traffic from SkyPilot devices if your server is behind a firewall.
- Appendix C, "Access Point Command-Line Interface," provides instructions for accessing an access point's Linux command shell.

Conventions Used in This Guide

This section describes the text and syntax conventions used in this guide.

Text Conventions

This guide uses the following text conventions:

- *Italic* is used to introduce new terms.
- **Bold** is used to indicate what you click in a graphical user interface (for example, commands names). In examples showing user interaction with the command-line interface, bold is used to indicate user input as opposed to command output.
- A `monospace` font is used for code elements (variable names, data values, function names, and so forth), command lines, scripts, and source code listings. It is also used to indicate text to enter in a graphical user interface.
- *`Italic-monospace`* is used for replaceable elements and placeholders within code listings.

Syntax Conventions

This guide uses the following conventions when showing syntax:

- Angle brackets, "<" and ">", enclose mandatory elements. You must enter these elements. For example:
  `ping <IP-address>`
- Square brackets, "[" and "]", enclose optional elements. You can omit these elements. For example:
  `show filter [filter-table-number]`
  Square brackets are also used to show the current value of parameters in the output of some commands.
- A vertical bar, "|", separates choices. For example:
  `show bridge [cache | port]`

1

Introduction

After becoming familiar with the SkyPilot Networks solution and deploying your SkyPilot network (as described in *Getting Started with the SkyPilot Network*), you'll need to perform operations, administration, and maintenance (OAM) tasks to increase performance, stability, and reliability. This chapter describes these tasks and the tools you use to perform them.

Chapter Highlights

- System overview
- About operations, administration, and maintenance (OAM)
- Using SkyPilot EMS

System Overview

SkyPilot Networks delivers a wireless, end-to-end broadband solution that seamlessly supports high-capacity, high-coverage networks. Designed for managed-access networks and service providers, the SkyPilot network takes broadband wireless the last mile with a cost-effective, robust infrastructure solution.

SkyPilot gives carriers an opportunity to expand rapidly into new markets and extend their offerings to include VoIP and high-bandwidth applications such as video and location-based services.

The SkyPilot solution offers a "tipping point" for converting dial-up customers to broadband and will help drive the growth of neighborhood "hotspots," offering ubiquitous wireless connectivity to local communities.

The auto-discovery and rapid provisioning features of a SkyPilot wireless mesh network can greatly reduce deployment and maintenance costs. Multiple topology options and network scalability create intriguing options for rapidly expanding a metro Wi-Fi customer base.

Hardware Components

A SkyPilot network includes the following physical components:

- **SkyGateway™ Series**—Operates as a base station for your wireless network. It provides an interface between wired infrastructure and a wireless network of subscribers who enjoy secure, high-speed access to the Internet or wide area networks.

  A SkyPilot wireless network requires at least one SkyGateway for operation. If desired, you can add additional SkyGateways to increase network capacity or provide redundancy. The SkyGateway typically resides at a location that offers easy access to wired infrastructure—usually a POP or data center. For optimal performance, the SkyGateway should be installed on an elevated site, such as a cell tower or the top of a tall building.

SkyGateways come in three flavors:

- **SkyGateway**—Provides standard base station operations.
- **SkyGateway DualBand**—Combines the features of a SkyGateway with 802.11 b/g Wi-Fi capability.
- **SkyGateway TriBand**—Combines the features of the SkyGateway DualBand with an additional radio, which is accessible through a second access point operating in parallel with the 2.4 GHz access point. The second access point leverages the 4.9 GHz Public Safety band.

NOTE There must be at least one functioning SkyGateway in your SkyPilot network before any other devices (SkyExtenders, SkyConnectors, or SkyAccess devices) can form communications links.

- **SkyExtender™ Series**—Functions as a repeater and extends the wireless range of a SkyGateway. SkyExtenders are optional equipment; by adding them to your network, you can expand your coverage area and provide redundancy through SkyPilot's mesh networking features. SkyExtenders offer a cost-effective way to add capacity and balance network loads.

  A SkyExtender's Ethernet interface can supply local subscriber service (creating a direct connection to the wireless network via the SkyExtender's Ethernet port) in addition to wirelessly forwarding data on behalf of other end users.

  For optimal performance, SkyExtenders should be installed on an elevated, fixed location, such as a roof, tower, or utility pole.

  For flexibility of installation, SkyPilot offers the following versions of the SkyConnector:

  - **SkyExtender**—Provides standard repeater functionality.
  - **SkyExtender DualBand**—Combines the features of a SkyExtender with a high-powered 802.11b/g access point that allows service providers and municipalities to offer standard Wi-Fi services over great distances, for targeted hot zones or dense, ubiquitous coverage patterns.

- **SkyExtender TriBand**—Combines the features of a SkyExtender DualBand with an additional radio, which is accessible through a second access point operating in parallel with the 2.4 GHz access point. The second access point leverages the 4.9 GHz Public Safety band, using 802.11a communication protocol. Each access point uses a single antenna, and these antennas have similar coverage patterns, providing a cost-effective solution for municipal networks.

IMPORTANT From here on in this guide, all references to "SkyExtender" refer to the SkyExtender, the SkyExtender DualBand, *and* the SkyExtender TriBand, unless otherwise noted.

- **SkyConnector™**—Links your subscribers to the SkyPilot wireless network. An Ethernet interface on the SkyConnector enables connecting to the subscribers' computers or a local area network (via a switch or router).

  For flexibility of installation, SkyPilot offers the following versions of the SkyConnector:

  - **SkyConnector SP-4700**—(Replaces SkyConnector Outdoor) Latest generation Connector, which combines features of the SkyConnector Pro and SkyConnector Mini. Its advantages include: increased frequency band support (4.9–5.25 GHz), the high power of the SkyConnector Pro, and the smaller size and weight of the SkyConnector Mini.
  - **SkyConnector Pro—**CPE (customer premise equipment) that provides robust broadband wireless connectivity to business subscribers. It uses the unlicensed 5 GHz spectrum to provide DSL- and cable-like *last-mile* broadband connectivity to permanent structures such as office buildings.
  - **SkyConnector Indoor**—A plug-and-play network device that a subscriber can easily install without technical assistance. Advise subscribers to place the SkyConnector in a location with an optimal sight line to the SkyGateway or a SkyExtender—for example, on a windowsill or in a window frame.
  - **SkyConnector Mini—**Provides economical broadband wireless in a physically smaller device (than the SkyConnector Pro) to residential or business subscriber. Instead of requiring copper or coaxial wires, the SkyConnector Mini uses the unlicensed 5 GHz spectrum to provide DSL- and cable-like broadband connectivity.
  - **SkyConnector Outdoor**—(Legacy product; replaced by SkyConnector SP-4700) Designed for installation by the service provider, the outdoor version of the SkyConnector attaches to an external structure such as eaves, a roof, or a pole. In general, the outdoor SkyConnector provides greater range than the indoor unit.

- **SkyAccess™**—Remote Wi-Fi access point that links subscribers who are in difficult coverage areas to the SkyPilot wireless network.

  For maximum flexibility, SkyPilot Offers the following versions of SkyAccess:

  - **SkyAccess DualBand SP-3800**—(Replaces SkyAccess DualBand) Dual-radio/dual-frequency device with integrated directional antenna for 4.9–6.0 GHz backhaul and omnidirectional 2.4 GHz antenna to serve Wi-Fi clients; offers improved performance over the legacy SkyAccess DualBand.
  - **SkyAccess DualBand**—(Legacy product; replaced by SkyAccess DualBand SP-3800) Dual-radio/dual-frequency device with integrated directional antenna for 4.9–5.8 GHz backhaul and omnidirectional 2.4 GHz antenna to serve Wi-Fi clients.

Software Components

The software components of a SkyPilot system are:

- SkyControl™—A Web server-based application that automates device provisioning by enabling devices to get their configuration information from the SkyPilot EMS server. SkyControl is also used for updating network node firmware and for setting device and system configuration options.

  SkyControl provisioning functions are accessed using the EMS Web application. For installation information, refer to *SkyPilot EMS Installation*.

  SkyControl includes an integrated SNMP management system for real-time SkyPilot device monitoring and management. This software provides a graphical view of your network topology with at-a-glance updates on topology, routing, and performance.

  SkyControl functions are accessed using the SkyPilot EMS Web application. For installation information, refer to *SkyPilot EMS Installation*.

- **Third-party applications**—Provided as part of the SkyPilot EMS server installation. The server package includes open-source versions of FTP, HTTP, and DHCP servers plus an open-source database for storing device configuration information. For more information about these third-party applications, refer to *SkyPilot EMS Installation*.

- **Google Earth™ mapping service**—Seamlessly integrated into SkyControl. and using the GPS positioning capabilities of SkyPilot's mesh infrastructure products, the Google Earth mapping service provides automatic and dynamic mesh network visualization within the Google Earth Pro application (the commercial version of the free Google Earth application). Combining these

two powerful tools provides great flexibility in designing, building, and operating wireless mesh networks. Additionally, SkyControl includes the Google Earth Management Service (GEMS) Launchpad.

- **SkyPilot command-line interface**—A text-based interactive application built into all SkyPilot devices. This interface enables you to manually provision a device, retrieve information about the device's status, and perform real-time logging.

  NOTE This interface is typically referred to as the "command-line interface" (without the preceding "SkyPilot").

- **SkyPilot Device Web interface**—A Web-based application built into all SkyPilot devices. This tool provides much the same functionality as the SkyPilot command-line interface in an easy to use graphical interface.

  NOTE This interface is typically referred to as the device's "Web interface" (without the preceding "SkyPilot").

- **Access point command-line interface**—The Linux command shell interface of DualBand and TriBand access points. This interface enables you to execute standard Linux commands to configure and retrieve access point settings directly (versus through the SkyPilot Web interface). This interface is intended for SkyPilot use only.

For more information about how to use the software components, see "OAM Tools and Resources" on page 8.

About Operations, Administration, and Maintenance

After deploying your SkyPilot network, you will need to perform *operations, administration, and maintenance (OAM)* tasks to optimize performance and uptime. *Operations* refer to ongoing provisioning and customizing activities. *Administration* involves routine management tasks, such as managing software and customers, configuring security, and creating reports. *Maintenance* encompasses system monitoring, address management, and troubleshooting strategies.

OAM Tasks

A SkyPilot network administrator is usually responsible for the tasks described in Table 1-1.

Table 1-1. OAM Tasks

Task	Refer to
Provisioning SkyPilot devices	"Provisioning Overview" on page 22
Managing devices' firmware	"About Software Images" on page 72
Creating reports	"About Reports" on page 81
Monitoring system status	"Monitoring a Network's Topology with SkyControl" on page 84 "Monitoring Events and Alarms" on page 85 "Monitoring Link States" on page 93
Troubleshooting	"Troubleshooting" on page 100

OAM Tools and Resources

Table 1-2 describes the tools and resources related to performing OAM tasks.

Table 1-2. OAM Tools and Resources

Tool or resource	Description
SkyControl	SkyControl provisioning functions are part of the SkyPilot EMS (Element Management System) and automate device provisioning by enabling devices to get their configuration information from the EMS server. Using SkyControl, you create configuration profiles that are distributed to devices across the wireless mesh network. For more information, see "Automatic Provisioning" on page 61. Additionally, SkyControl includes an integrated SNMP management system for real-time SkyPilot device monitoring and management. This software provides a graphical view of your network topology with at-a-glance updates on topology, routing, and performance. For more information, see "Monitoring a Network's Topology with SkyControl" on page 84.
Command-line interface	A comprehensive command-line interface is built into all SkyPilot devices to enable you to manually provision a device, retrieve information about the device's status, and perform real-time logging. For more information, see "Command-Line Interface Provisioning" on page 69.
Web interface	A comprehensive Web-based application is built into all SkyPilot devices to provide much the same functionality of the command-line interface in an easy to use graphical interface. For more information, see "Device Web Interface Provisioning" on page 69.

Using SkyPilot EMS

The SkyPilot EMS Web client is a Web-based application that is built into the EMS server and can be accessed through a Web browser.

Logging in to the EMS Web Client

To use the EMS Web client to manage your SkyControl network and to provision devices, you must be able to access the EMS server via a Web browser. You'll need a user name and password in addition to the EMS server's IP address.

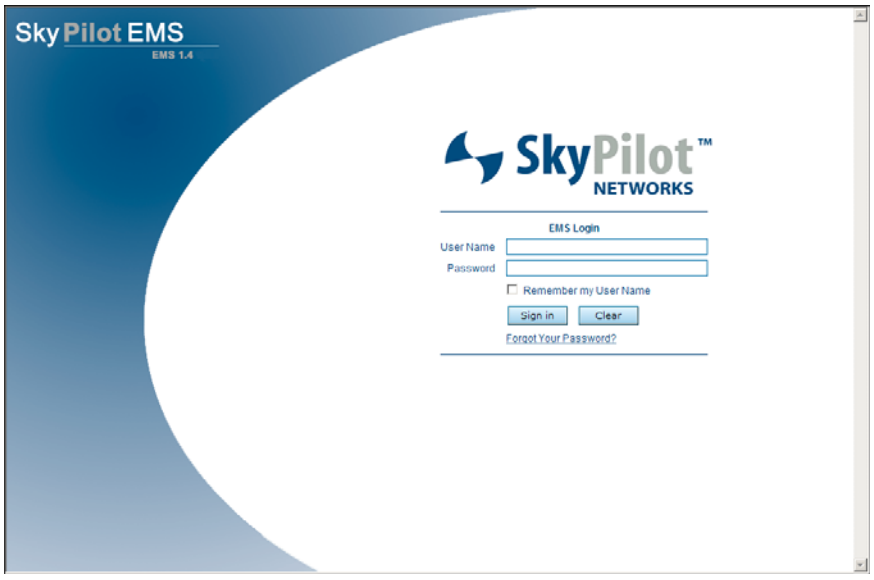
NOTE The SkyPilot EMS Web Client supports Microsoft® Internet Explorer® 7 and Firefox™ 3.6. Other browsers may work but have not been tested.

To log in to the EMS Web client:

1. Open a Web browser and enter the URL for the SkyPilot EMS server's client login page: the server's IP address or host name, preceded by `http://` (for example, `http://192.168.1.228`).

   The Web client displays a login screen (Figure 1-1).

   Figure 1-1. EMS Web client login screen



2. Enter the user name and password. The default user name is `admin`, and the default password is also `admin`. Optionally, click **Remember my User Name** to enable this option.

3 Click **Sign in**.

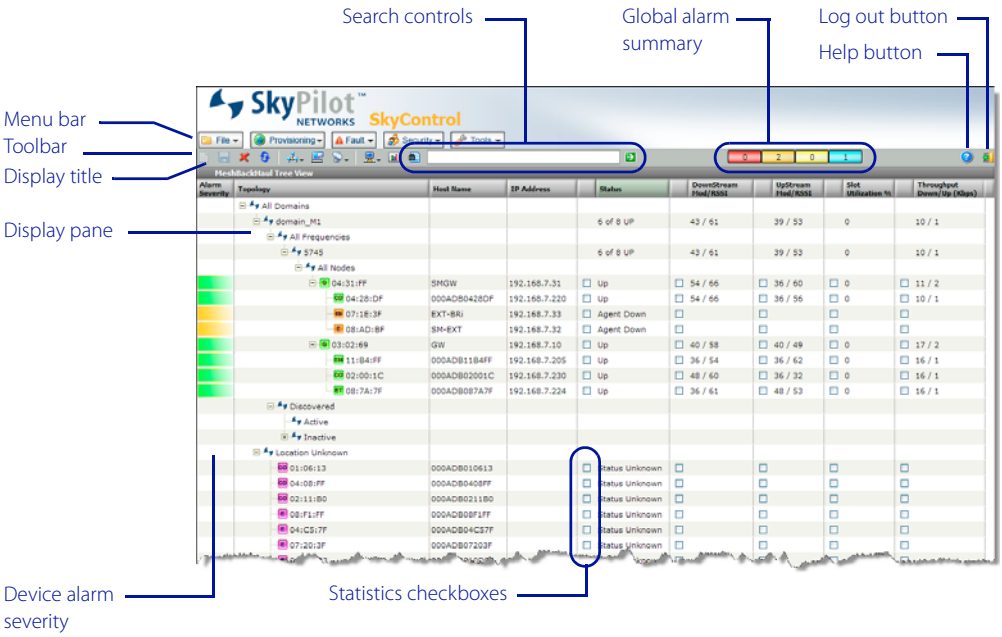
The Web client displays your SkyPilot network topology, in the Mesh Backhaul Tree View (Figure 1-2).

NOTE After 30 minutes of inactivity, the EMS Web client session expires, at which point you'll need to repeat the login procedure to continue using SkyPilot EMS.

The SkyPilot EMS Interface

Figure 1-2 illustrates the parts the SkyPilot EMS interface.

Figure 1-2. SkyPilot EMS Web interface



The various parts of the interface are as follows:

- **Menu bar**—Contains menus of commands that allow you to set global network configuration items, as well as manage the windows in the display pane. For details, see "Using the Menus" on page 15.
- **Toolbar**—Contains context-sensitive buttons used to view and manage your SkyPilot network; for details, see "Using the Toolbar Buttons" on page 18. The toolbar buttons are enabled only when they're applicable to the display pane's active window. Although they appear at the far right of the display, the **Log Out** and **Help** buttons are considered part of the toolbar.

- **Display title**—Indicates the display pane's current display.
- **Display pane**—Shows the selected view of your SkyPilot network.
- **Device alarm severity**—Color-coded indication of the alarm severity. To see alarm details, double-click in the alarm's color indicator.
- **Search Controls**—Search for a device; see "Searching" on page 19.
- **Global alarm summary**—Shows the number of active alarms for each alarm type: critical, major, minor, and warning.

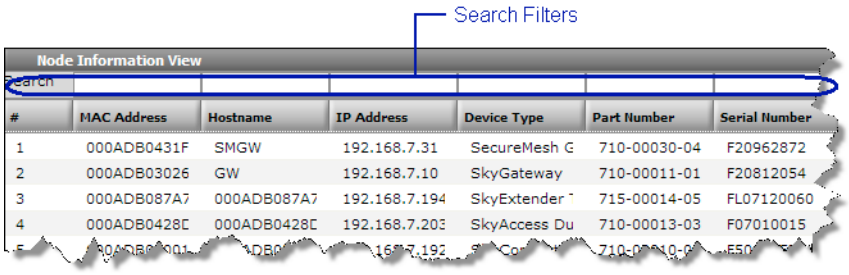
Using the Display Pane

The display pane is the viewing area for your network components, configuration screens, alarms, events, reports, and integrated applications such as Google Earth.

The display pane user interface provides typical functionality:

- Display context-sensitive menus by right-clicking a row; for example, right-click any node to display the device menu (see "Node Device Views" on page 13).
- Select multiple rows by using ctrl-click; select a contiguous range of rows by using shift-click.
- (Available only in some displays) Filter a long page of many rows by using the Search filters at the top of the columns. Type a value into any filter box and click the **Funnel** icon to the right of the filter boxes (or press **Enter)**, and only those rows matching your entry will be shown. To redisplay all the rows, delete the text from the filter box and click the **Funnel** icon (or press **Enter**).

Figure 1-3. Search Filters



Tree Views

When the mesh backhaul tree view or the access point treeview are displayed, you can easily determine a node's device type and state from the node icon (Table 1-3) and its color (Table 1-4 on page 13).

Table 1-3. Node Icons

	SkyConnector Indoor
	SkyConnector Outdoor
	SkyConnector Mini
	SkyConnector Pro
	SkyConnector SP-4700
	Ubiquiti NanoStation 5
	Ubiquiti PowerStation 5
	Ubiquiti NanoStation Loco 5
	Ubiquiti Bullet 5
	SkyAccess DualBand
	SkyAccess DualBand SP-3800
	SkyExtender
	SkyExtender DualBand
	SkyExtender TriBand
	SkyGateway
	SkyGateway DualBand
	SkyGateway TriBand

Table 1-4. Node Icon Colors

Color	Status	Description
green	Up	Node is managed, reachable, and responding.
orange	Agent Down	Node is managed and reachable, but not responding (the SNMP agent is down).
red	Down	Node is managed but unreachable.
blue	Discovered	Node is discovered (via the Gateway), but not managed. The device may be active (provisioned and communicating with the Gateway, but not managed by the EMS) or inactive (device is up but not provisioned).
purple	• Status Awaited • Status Unknown	For managed, reachable, and responding nodes, "Status Awaited" is a transitory state, such as when polling is enabled after being disabled. For non-managed, non-reachable, or non-responding nodes, the state is "Status Unknown".
gray	Polling Disabled	Device polling has been disabled through SkyControl.

Node Device Views

You can view node devices in both tree and flat views. In either case, to access a device's context-sensitive menu (Figure 1-4 and Table 1-5), right-click anywhere in the device's row. Depending on the device and its status, some choices may not be shown or may be disabled (grayed out).

Figure 1-4. SkyControl device menu

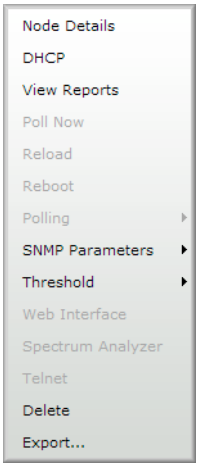


Table 1-5. Device Menu Options (Page 1 of 2)

Option	Description/Reference
Node Details	Displays the device's configuration settings, polling details, Ethernet statistics, and link information.
DHCP	Configure DHCP for the device.
View Reports	Displays a window in which you can select a report to view or to chart.
Poll Now	Enables an immediate single SkyControl poll of the device to update the default task statistics.
Reload	Reloads the node's configuration. See "Automatically Provisioning a Device" on page 63.
Reboot	Reboots the node.
Polling	Enable or disable polling or display a window in which you can add, modify, start, and stop data collection tasks.
SNMP Parameters	Configure SNMP traps for the device.
Threshold	Enable, disable, or configure alarm and trap thresholds for the device.
Web Interface	Opens the device's Web interface in a new browser tab.

Table 1-5. Device Menu Options (Page 2 of 2)

Option	Description/Reference
Spectrum Analyzer	(Devices that have built-in access points: SkyAccess, DualBand, and TriBand devices only) Displays, in a separate browser tab, spectrum analyzer information for the node.
Provision Node	(Unprovisioned nodes only) Displays a window in which you can provision the node.
Telnet	Opens a Telnet session to the device's command-line interface; helpful for debugging.
Delete	Deletes the selected node. (This is a shortcut for the Node Maintenance delete function.)
Refresh	Refreshes the node's information in the current display.
Export	Export the current display information to a CSV-delimited file.

Using the Menus

The EMS Web client menu bar contains menus of commands that allow you to set global network configuration items, as well as manage the windows in the display pane:

File Menu

The **File** menu offers the following choices:

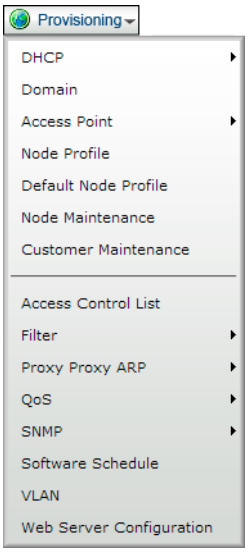
- **New**—Context-sensitive command to create an entity of the type currently shown in the display pane.
- **Edit**—Context-sensitive command to edit the currently selected entity.
- **Attributes**—Context-sensitive command to show attributes of the currently selected entity.
- **Save**—Context-sensitive command to save the entity currently being created or edited.
- **Delete**—Context-sensitive command to delete the currently selected entity.

- **DHCP**—(Enabled only when viewing the Node Maintenance display) Opens a combined DHCP Host and DHCP Subnet configuration screen.
- **Export**—Save the current display pane information in a CSV file.
- **Batch Provisioning**—Load a CSV file to use for automatically creating Node Maintenance profiles.
- **Logout**—End you SkyPilot EMS session.

Provisioning Menu

The Provisioning menu (Figure 1-5) provides detailed instructions for configuring provisioning parameters for automatically provisioned devices, and for performing administrative functions for your SkyPilot network. For detailed provisioning information, see Appendix 5, "Provisioning With SkyControl."

Figure 1-5. EMS Provisioning menu



Fault Menu

The **Fault** menu provides access to alarm maintenance, event log, and trap functions. For procedural information, see "Monitoring Events and Alarms" on page 85.:

Security Menu

The **Security** menu (Figure 1-6) enables you to manage network security (by choosing **Security ➤ Security Manager**). See "Managing Network Security" on page 79.

Figure 1-6. EMS Security Menu

Tools Menu

The **Tools** menu offers the following choices:

- **Telnet**—To open a Telnet connection from your computer to any SkyPilot device through a serial connection.
- **GEMS Launchpad**—To launch Google Earth. For details, see Appendix A, "Google Earth Management System (GEMS) Reference."
- **Open Links in New Window**—To enable or disable opening hyperlinks in new browser windows.
- **Mail Server Configuration**—To configure a mail server to use for northbound trap events.
- **Server Status**—To show the status of all known EMS servers.

Using the Toolbar Buttons

Table 1-6 describes the SkyPilot EMS toolbar buttons and their functions.

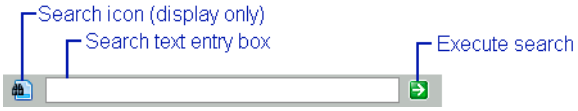
Table 1-6. SkyPilot EMS Toolbar Buttons

Button	Function	Description
	New	Context-sensitive "new" function creates the same type of item as is shown in the display area.
	Save	Saves any new or revised items on the current display area.
	Delete	Context-sensitive "delete" function deletes the currently selected item.
	Refresh	Refreshes the current display area.
	Mesh Backhaul View	Provides choices to display the Tree View or Flat View of your SkyPIlot network.
	Node Information View	Provides choices to display the Tree View or Flat View of your SkyPIlot network.
	AP Client View	Provides choices to display the Tree View or Flat View of your access points.
	DHCP View	Provides choices to display the Tree View or Flat View of your DHCP server, as well as manage the server and logs.
	Reports	Displays charts showing the status for up to four selected devices.
 	Search	Case-insensitive search for any text value; the text represent anything in the system, such as a node, profile, or address. For more information, see "Searching" on page 19.
	Help	Provides version and copyright information about the SkyPilot EMS client.
	Logout	Ends your current SkyPilot EMS session.

Searching

In addition to the display pane's search filters (see "Using the Display Pane" on page 11), you can use the search controls (Figure 1-7) to perform global searches.

Figure 1-7. Search Controls



To perform a search, type the desired information into the **Search Text Entry Box** and click the **Execute Search** button.

Keep in mind the following points about searching:

- Searches are case-insensitive.
- The search function looks for a match in node maintenance, node profile, customer maintenance, and access point station records.
- Table 1-7 lists the information you can search for in each searchable record set.

Table 1-7.

Record set	Possible search criteria
node maintenance	MAC address, host name, IP address, and node type
node profile	Node profile name, node type
customer maintenance	All fields shown in the Customer Maintenance view
access point station	MAC address, IP address

2

Operations

SkyPilot operations tasks include ongoing provisioning and customizing activities. This chapter describes how to provision SkyPilot devices (either manually or automatically) and provides guidelines for configuring SkyPilot devices.

Chapter Highlights

- Provisioning overview
- Provisioning parameters overview
- Required provisioning parameters
- Optional provisioning parameters
- General provisioning guidelines
- Automatic provisioning
- Manual provisioning

Provisioning Overview

Provisioning is the process of customer authorization and service configuration. When a SkyPilot device is provisioned, it authenticates itself on the network and downloads a configuration file containing customer-specific settings, such as firmware images and Quality of Service rate limits. This device provisioning is independent of end-user provisioning, but it can be used to assist with end-user provisioning by serving IP addresses via DHCP to user equipment such as personal computers and home routers.

Table 2-1 summarizes the steps required to provision a SkyPilot device.

Table 2-1. Device Provisioning Steps

	Step	Refer to
1	Decide whether to configure the device for manual or automatic provisioning.	"Choosing a Device Provisioning Mode" on page 22
2	Provision the device.	Either of the following: • "Manual Provisioning" on page 66 • "Automatic Provisioning" on page 61

Choosing a Device Provisioning Mode

SkyPilot offers a choice of two device provisioning modes:

- **Automatic**—Allows unattended configuration of SkyPilot devices from a central SkyPilot EMS server at your network operations center (NOC). Automatic provisioning requires more initial setup time than manual provisioning, but it greatly simplifies network administration as your network grows.
- **Manual**—Allows device configuration with the minimum settings required for a wireless link. Configuration settings are entered through the command-line interface or Web interface and are stored in flash memory; manually provisioned devices do not depend on a SkyPilot EMS server for configuration. Manual provisioning is a logical choice if you're installing a test network or rolling out a small-scale installation that's not expected to expand.

Provisioning Mode and Device Operations

The provisioning mode you choose for devices (automatic or manual) affects the procedure that the devices use to come online.

Figures 2-1 and 2-2 illustrate the steps taken by devices—both manually and automatically provisioned—from power-on through the formation of network links.

- Figure 2-1 shows the steps taken by a SkyGateway up to the point at which the device begins sending hello beacons, which other SkyPilot devices can use to form links on the wireless network.
- Figure 2-2 shows the steps taken by SkyExtenders and SkyConnectors up to the point at which the device starts forming links with other devices on the wireless network.

Figure 2-1. SkyGateway power-on and link formation

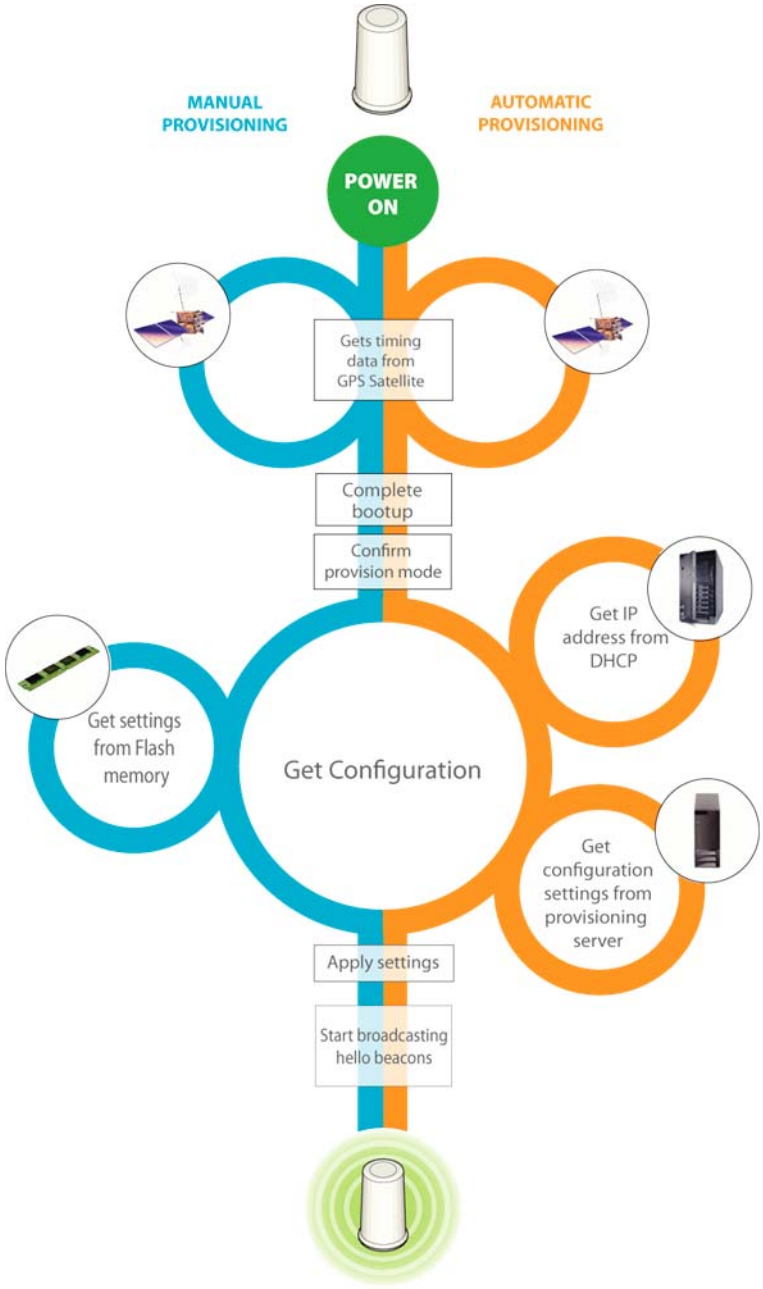


Figure 2-2. SkyConnector/SkyExtender/SkyAccess power-on, link formation (Page 1 of 2)

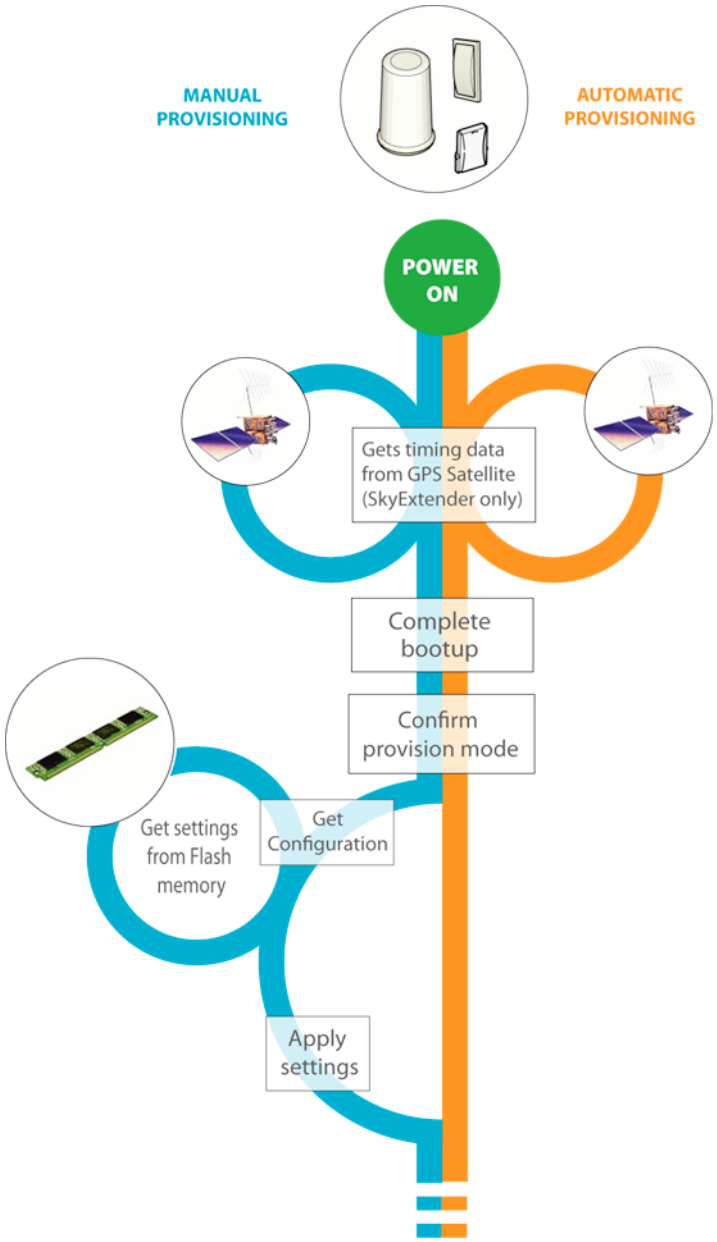
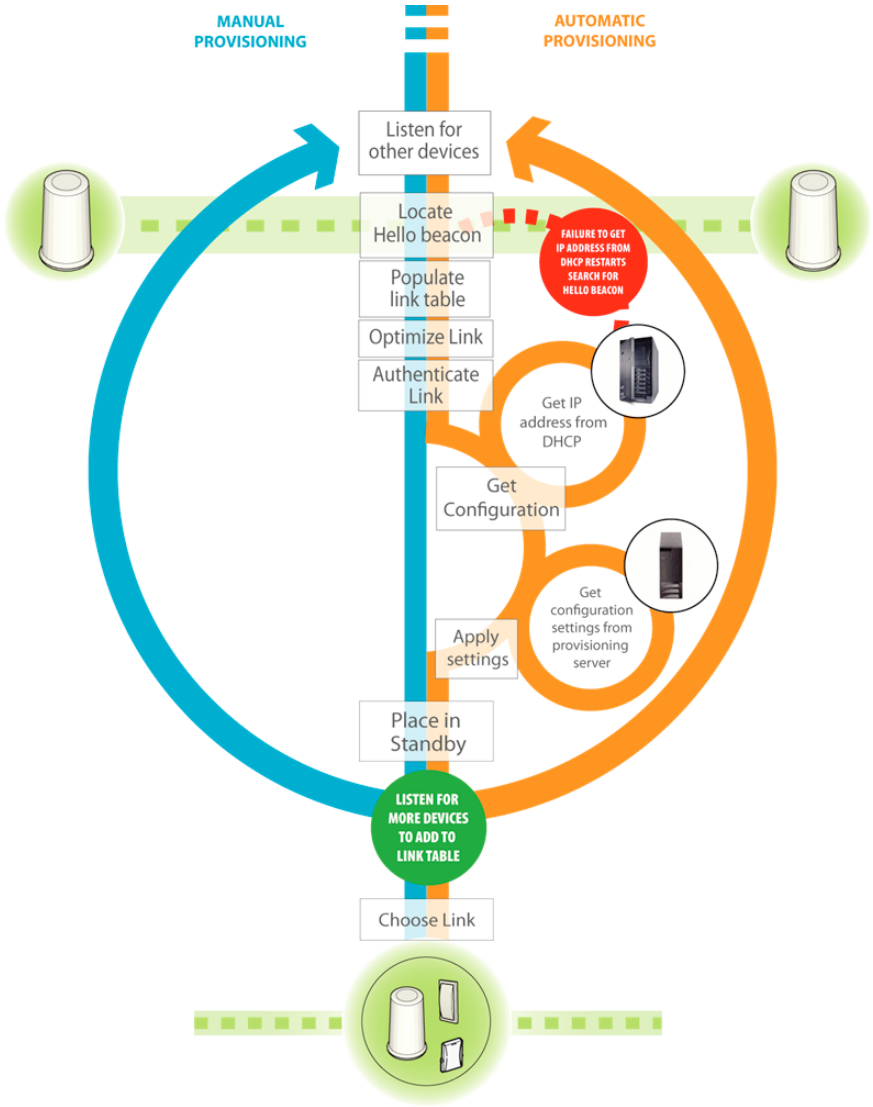


Figure 2-2. SkyConnector/SkyExtender/SkyAccess power-on, link formation (Page 2 of 2)



Hybrid Network Provisioning

If necessary, you can set up a *hybrid network*—a SkyPilot network in which different devices use different device provisioning modes. Although a hybrid network will operate normally, individual devices will behave differently depending on their provisioning mode:

- Automatically provisioned devices will establish network links only when SkyControl provisioning is available to provide configuration information from an EMS server.
- Manually provisioned devices will form network links according to configuration settings stored in flash memory.

There is no requirement that all devices be configured the same way (automatic provisioning or any method of manual provisioning). For example, you could use the command-line interface to manually provision and test individual nodes before adding them to your network.

Provisioning Parameters Overview

Table 2-2 lists the provisioning parameters (as they would be specified from the command line for manually provisioned devices) and shows whether they're required or optional, as well as how they can be set: on manually provisioned devices, from the command-line interface or Web interface, and/or on automatically provisioned devices via SkyControl.

Table 2-2. Provisioning Parameters (Page 1 of 2)

Parameter	Req.	Opt.	CLI	Web Interface	Sky-Control ‡
access point #		✔		✔	✔
acl		✔	✔	✔	✔
auto		✔	✔		
buzzer		✔	✔		✔
classifier		✔	✔	✔	✔
domain	✔		✔		✔
eth	✔ †		✔	✔	✔
filter		✔	✔	✔	✔
freq	✔		✔	✔	✔
ip	✔ †		✔	✔	✔
manual		✔	✔		
netkey	✔ †		✔		

Access point settings are not itemized in this table; they are configured through the Web interface or EMS client.

† Depends on system configuration.

‡ All parameters that can be set with SkyControl are set indirectly via node profile settings that are then assigned to specific devices.

Table 2-2. Provisioning Parameters (Page 2 of 2)

Parameter	Req.	Opt.	CLI	Web Interface	Sky-Control ‡
parent		✔	✔		✔
password		✔	✔		✔
power		✔	✔		✔
proxy2arp		✔	✔	✔	✔
radar		✔	✔		✔
snmp		✔	✔	✔	✔
timezone		✔	✔		✔
trafficrate		✔	✔	✔	✔
vlan	✔ †		✔	✔	✔
web		✔	✔		✔

Access point settings are not itemized in this table; they are configured through the Web interface or EMS client.

† Depends on system configuration.

‡ All parameters that can be set with SkyControl are set indirectly via node profile settings that are then assigned to specific devices.

Required Provisioning Parameters

Regardless of which provisioning mode you configure for a SkyGateway, the device must have the frequency and domain parameters set before it can be operational, as described in the next two sections.

In addition, if you're planning to operate a SkyPilot device as a manually provisioned device, you must change its provisioning mode from the default (automatic) to manual.

Depending on your deployment, you may need to configure additional provisioning parameters:

- If virtual local area networks (VLANs) are being used in the wired network to which the SkyGateway will connect, you may need to configure the management VLAN parameters for the SkyGateway. See "Virtual Local Area Networks (VLANs)" on page 32.
- If the SkyPilot device's Ethernet interface is configured to autonegotiate but the device fails to negotiate Ethernet connectivity (possibly because the device doesn't support autonegotiation), you may need to configure the Ethernet interface for a fixed speed and duplexity. See "Ethernet Interface" on page 34.
- If the network is using a nonstandard netkey (that is, anything other than the default netkey, `SkyPilot Network, Inc.`), you need to set the device's netkey to match the other devices. Refer to the `set netkey` command, described in the *SkyPilot Command-Line Interface Reference*. (The netkey can't be changed using SkyControl or the Web interface.)
- Although not required by SkyPilot devices in order to forward end-user data, you should configure the IP address information so that you can access and manage the device itself. See "Managing IP Addresses" on page 94.

Frequency

In order for devices within a SkyPilot network to form links, they must operate on the same frequency. You can configure a variety of frequency settings, including the primary (preferred) frequency, multiple allowed frequencies, and the dwell time a device waits on its primary frequency before attempting to use a frequency from its Allow list to achieve successful communications with network nodes. Which frequencies you can set depends on the device:

- For a SkyGateway, you can set the frequency over which it will be broadcasting. (This is the primary frequency; the Allow list is ignored.)
- For SkyExtenders, SkyConnectors, and SkyAccess devices, you can set the primary frequency, as well as the range of frequencies that the device is allowed to use in its hunting. SkyExtenders and SkyConnectors dwell on the primary frequency longer than frequencies in their Allow list.

For automatically provisioned devices, you modify the frequency settings in the node profile that's assigned to the device (see "Configuring Node Profiles" on page 126).

For manually provisioned devices, you set the frequency by using the `set prov freq` command, described in the *SkyPilot Command-Line Interface Reference*.

Domains

A single domain can be defined to encompass your entire SkyPilot network, including all its nodes. Or domains can be used to segregate a network into two or more smaller networks, where each smaller network has the same characteristics as the larger network: one or more SkyGateways, any number of SkyConnectors (including none), any number of SkyExtenders (including none), and any number of SkyAccess devices (including none).

A SkyConnector, SkyExtender, or SkyAccess device can be configured to belong to a single domain or all domains (the default). If configured for only a single domain, it can use any of the SkyGateways within its domain, and it will choose the one with the lowest *cost route*, taking into account the current link quality in both

directions (upstream and downstream), as well as the link quality further along the route to the ultimate destination. The SkyConnector/SkyExtender/SkyAccess cannot, however, form links with SkyGateways outside its domain even if those SkyGateways are operating at a frequency in the device's Allow list. Conversely, if the SkyConnector/SkyExtender/SkyAccess belongs to all domains, it can join any device operating on an allowed frequency, regardless of that device's domain.

Typical domain configuration activities include:

- Creating a domain for each SkyGateway and then load-balancing the SkyConnectors across multiple SkyGateways (domains). In addition to performance considerations, load balancing enables you to offer differentiated services. For example, a smaller number of business users could be assigned to one SkyGateway, while a larger number of residential users could be allocated to a second SkyGateway.
- Establishing domains with multiple SkyGateways that provide redundancy. In this case, the SkyConnectors will select a SkyGateway based on cost route. If a SkyGateway goes offline, the SkyConnectors using that SkyGateway automatically select another SkyGateway within the same domain.

For automatically provisioned devices, you use the Domain Maintenance function within SkyControl to add, modify, and delete domains (see "Configuring Domains" on page 122), and then you apply the domains to node profiles (see "Configuring Node Profiles" on page 126).

For manually provisioned devices, you set the domain by using the `set prov domain` command, described in the *SkyPilot Command-Line Interface Reference*.

Virtual Local Area Networks (VLANs)

Virtual local area networks (VLANs) are portions of a network that are configured as logical topologies defined by software, connected to the same physical network infrastructure. Devices on separate VLANs of a network behave as if they're on physically separated networks. VLANs function by logically segmenting the network into different broadcast domains so that packets are switched only between ports that are designated for the same VLAN.

By enabling the following capabilities, VLANs offer significant benefits, such as efficient bandwidth use, flexibility, performance, and security:

- Restricting the dissemination of broadcast and node-to-node traffic, thereby reducing the burden of extraneous network traffic.
- Using standard router-based security measures (since all packets traveling between VLANs must also pass through a router).
- Segregating and switching ISP traffic. Wholesale operators can offer end users a choice of any provider instead of only the provider operating a particular network. In such cases, each SkyConnector would be assigned to a single ISP. Additionally, end-user data can be separated by assigning VLANs to each SkyExtender or SkyConnector's Ethernet interface.
- Isolating management traffic from user traffic. You can configure a management VLAN, independent of a VLAN for end users. Management traffic is thereby segmented and secure.

There are two types of VLAN:

- **Management VLAN**—Used to tag and strip data with a configured VLAN ID as the data enters or exits the management interface of a device. In a SkyPilot network, you configure the management VLAN only on the SkyGateway, which then automatically propagates the VLAN configuration throughout the network.

  You must manually configure the SkyGateway VLAN because the VLAN tag can affect whether the SkyGateway's management traffic can reach a provisioning server (the EMS server).

- **Data VLAN**—Used to tag and strip data with a configured VLAN ID as the data enters or exits the Ethernet interface of SkyExtenders and SkyConnectors. The VLAN tag is added on a per-SkyExtender and per-SkyConnector basis.

The Ethernet interface of a SkyConnector, (non-DualBand) SkyExtender, or SkyAccess device can be configured to either a single VLAN or no VLAN. If it's configured to a VLAN, all user Ethernet traffic transmitted upstream by the SkyConnector, SkyExtender, or SkyAccess device is tagged with the configured VLAN ID. However, this VLAN tag is stripped from all Ethernet packets sent from a local SkyConnector, SkyExtender, or SkyAccess device 10/100bT Ethernet interface. (Packets forwarded by the SkyGateway and SkyExtenders retain the VLAN tag.)

Data VLANs should not be configured on the SkyExtender portion of a DualBand or TriBand. Instead, VLANs can be configured on the access point's WLAN. (See "Access Point SSID Profiles" on page 55.)

TIP To avoid time-consuming troubleshooting, remember that once a SkyConnector, SkyExtender, or SkyAccess device is configured to a VLAN, any packets received through their 10/100bT ports that contain a different VLAN tag are dropped. (In contrast, if a SkyConnector or SkyExtender is not configured to a VLAN, any tagged packets are forwarded unchanged.)

For automatically provisioned devices, you use SkyControl to add, modify, and delete VLANs (see "Configuring VLANs" on page 140).

For a manually provisioned device, you configure its VLAN by using the command-line interface command (refer to the `set prov vlan` command, described in the *SkyPilot Command-Line Interface Reference*) or its Web interface counterpart (refer to the *SkyPilot Web Interface Reference*).

Ethernet Interface

A node's 10/100bT Ethernet interface can be enabled or disabled; in addition its physical settings can be configured for autonegotiation or set to full or half duplex, and its speed can be set to 100 or 10.

NOTE This section does not apply to SkyExtender DualBands, which don't have an Ethernet interface. (Other DualBand devices have Ethernet interfaces.)

For SkyExtender-only applications (that is, where there is no subscriber interface), if you do not plan to connect any devices to a SkyExtender's Ethernet interface, you may want to disable the Ethernet interface for security reasons.

For SkyConnector-only or combined applications (where a SkyExtender forms wireless links to SkyConnectors and serves a local customer via the SkyExtender's Ethernet interface), you can selectively enable or disable the Ethernet interface to control subscriber access.

For automatically provisioned devices, you use the Node Profile function within SkyControl to create profiles with the desired Ethernet interface status (see

"Configuring Node Profiles" on page 126), and then you apply the node profiles to specific nodes (see "Configuring Nodes" on page 136).

For manually provisioned devices, you set the Ethernet interface status by using the command-line interface command (refer to the `set eth` command, described in the *SkyPilot Command-Line Interface Reference*) or its Web interface counterpart (refer to the *SkyPilot Web Interface Reference*).

Optional Provisioning Parameters

As shown in Table 2-2 on page 28, most of the provisioning parameters are optional—that is, you don't have to set them in order for your SkyPilot network devices to be operational. However, to fully use and customize SkyPilot functions such as reporting, you'll typically set many of the provisioning parameters discussed in these sections:

- "Proxy Proxy ARP" on page 36
- "Radar Detection" on page 36
- "SNMP" on page 38
- "Time Zones" on page 39
- "Quality of Service (QoS)" on page 40
- "Filtering" on page 44
- If SkyExtender/SkyAccess DualBand/TriBand devices are being used, you may need to configure their access points, including (possibly) the access points' default WPA-shared key, `publicpublic`. See "Access Points" on page 50.

You can find information about the remaining optional parameters listed in Table 2-2 in the applicable reference appendices and guides:

- Appendix 5, "Provisioning With SkyControl"
- *SkyPilot Command-Line Interface Reference*
- *SkyPilot Web Interface Reference*

Proxy Proxy ARP

Similar to standard proxy ARP performed on a router, proxy proxy ARP functionality is the process of the SkyGateway forwarding the ARP (Address Resolution Protocol) to a router. The router forwards an ARP response (using proxy ARP) back to the SkyGateway, which then sends the response to the intended client device.

When two SkyPilot devices attempt to communicate over layer 3 (TCP/IP), ARP is used to find the proper MAC of the specified IP address. This scenario commonly occurs when SkyPilot devices are prevented from communicating over layer 2 for security reasons.

Available configuration settings are **Enabled** and **Disable**.

For automatically provisioned devices, you use the Node Profile function within SkyControl to create profiles with the desired proxy proxy ARP settings (see "Configuring Node Profiles" on page 126), and then you apply the node profiles to specific nodes (see "Configuring Nodes" on page 136).

For manually provisioned devices, you configure proxy proxy ARP by using the command-line interface the `set proxy2arp` command.

Radar Detection

SkyPilot devices can be configured to detect radar transmission within their reception range and take appropriate action if radar is detected. You configure SkyGateways explicitly, which then propagate the setting to SkyExtenders, SkyConnectors, and SkyAccess devices as links are formed.

Available configuration settings are:

- **Default**—Depends on the region (identified by a communications governing body) for which this device is manufactured:
  - FCC (US): default = Disable
  - ETSI (EU): default = Enable-shutdown
  - AUS-ACA (Australia): default = Disable
  - Public Safety (US/Latin America Public Safety): default = Disable

- **Disable**—Disables radar transmission detection.
- **Enable-shutdown**—Enables radar transmission detection, and takes appropriate action, depending on device type, when radar is detected:
  - SkyGateways sever all links and then begin operating on the lowest frequency in the Allow list on which there's been no radar detected, enabling links to reform on the network. The SkyGateway stays on the new channel indefinitely or until radar is detected.
  - SkyExtenders and SkyConnectors sever all links on the current operating frequency and begin searching on all other allowed frequencies for 30 minutes. If links are found on other frequencies, the device remains on that frequency until the links are severed or the device is restarted (even after the 30 minutes are up).
- **Enable-ignore**—Enables radar transmission detection, and logs a message whenever radar is detected.

For automatically provisioned SkyGateways, you use the Node Profile function within SkyControl to create profiles with the desired radar detection settings (see "Configuring Node Profiles" on page 126), and then you apply the node profiles to specific nodes (see "Configuring Nodes" on page 136).

For manually provisioned SkyGateways, you configure radar detection by using the command-line interface command (refer to the `set radar` command, described in the *SkyPilot Command-Line Interface Reference*) or its Web interface counterpart (refer to the *SkyPilot Web Interface Reference*).

SNMP

SNMP (Simple Network Management Protocol) is a standard for gathering statistical data about network traffic and the behavior of network components. SNMP uses management information bases (MIBs), which define what information is available from any manageable network device.

SNMP is an application-layer protocol designed to facilitate the exchange of management information between network devices. By using SNMP-transported data (such as packets per second and network error rates), administrators can manage network performance, find and solve network problems, and plan for network growth.

IMPORTANT Although you can disable SNMP for a device, it's highly recommended that you do not. If you disable SNMP for any device, your monitoring capabilities with SkyControl will be limited, providing an incomplete picture of your SkyPilot network.

SNMP Community Strings

A *community string* functions as an identifier (similar to a user ID) that enables access through an SNMP agent to network information or *objects* defined within a device's MIB. The community string is transmitted with all SNMP requests to a device. If the community string is correct (that is, if it matches the configured value), the device responds with the requested information; otherwise, the device simply discards the request and does not respond. There are three types of community strings for SNMP-capable devices (and all are configurable):

- **Read-only**—Enables a remote device to retrieve information from an SNMP-capable device. The read-only community string's default value is `public`. The read-only string is also referred to as an SNMP *get*.
- **Read-write**—Allows a remote device to retrieve information from or modify settings on an SNMP-capable device. The read-write community string's default value is `private`. The read-write string is also referred to as an SNMP *set*.
- **Trap**—Enables an SNMP-capable device to asynchronously send information to a remote device.

SNMP Trap Receivers

SNMP trap receivers instruct a node (device) where to send SNMP traps. To avoid a negative impact on performance, SkyPilot recommends a maximum of 10 trap receivers.

Applying SNMP Settings

You can create custom SNMP community strings and trap receivers; for details, see "Configuring SNMP Parameters" on page 143.

For automatically provisioned devices, you use the Node Profile function within SkyControl provisioning to create profiles with the desired default or custom SNMP settings (see "Configuring Node Profiles" on page 126), and then you apply the node profiles to specific nodes (see "Configuring Nodes" on page 136).

For manually provisioned devices, you configure SNMP by using the command-line interface command (refer to the `set snmp` command, described in the *SkyPilot Command-Line Interface Reference*) or its device Web interface counterpart (refer to the *SkyPilot Web Interface Reference*).

Time Zones

You can specify an NTP (Network Time Protocol) server IP address and set the GMT offset for accurate time. The NTP server provides the time to NTP clients (SkyPilot nodes). When a SkyPilot node starts up, it has a default date and time of January 1, 1970, 00:00:00 GMT. Using an NTP server, the node adjusts its time to be synchronized with the NTP server, which is usually UTC (Coordinated Universal Time) or GMT.

SkyPilot equipment does not display the correct time until an NTP server is specified. You must specify an NTP server in your DHCP configuration and set the time zone during provisioning (by setting the time zone in an automatically provisioned node's node profile, or by using command-line interface or Web interface manual provisioning).

Quality of Service (QoS)

To maintain high QoS, the SkyPilot network implements a variety of controls:

- **Ingress rate control**—The SkyPilot system offers support for operator-configured maximum data rates in both directions: downstream (traffic going to a subscriber) and upstream (traffic coming from a subscriber). The SkyGateway controls the maximum downstream rate on a per-subscriber basis, while the individual subscriber nodes control the maximum upstream rate. This policing and shaping of traffic at the ingress points of the network controls access to critical bandwidth resources and minimizes the QoS mechanisms needed for traffic routed through the mesh network.
- **Scheduling fairness**—To manage any shared-access system (including broadband wireless) economically, a network operator must be able to oversubscribe user data rates relative to the overall bandwidth of the system. Therefore, there will likely be times when the overall demand is higher than the available bandwidth. SkyGateway supports per-subscriber queuing in the downstream direction, with queue control based on the configured maximum downstream rate for each subscriber. These mechanisms ensure that each user receives a proportionate share of available bandwidth during oversubscribed periods.
- **Prioritization**—SkyPilot software architecture allows for prioritization of data based on protocol type, IP address, or other differentiators. This provides a means of prioritizing the transmission of VoIP packets and any other type of data.
- **Traffic rate controls**—You can set traffic levels based on subscription rates. For example, you could create a gold level for fastest service and a silver level for slower service. The traffic levels are achieved by rate limiting. In oversubscription conditions the data rates from subscribers may be reduced proportionately. That is, a user with a 1 Mbps configured rate could be reduced to 500 Kbps while a configured rate of 500 Kbps is reduced to 250 Kbps.
- **QoS classifiers**—These are used to classify traffic according to the types of packets that will be directed to a subscriber's high-priority queue, for both upstream and downstream traffic. All other traffic will be directed to the subscriber's standard (low-priority) queue.

  For any given subscriber, this classification mechanism ensures that all queued high-priority packets are transferred before any queued low-priority packets.

However, the system as a whole transfers packets based on traffic rate control and fairness criteria, thus ensuring that the low-priority packets of one subscriber will continue to flow even when high-priority packets are queued for another subscriber.

NOTE You're not required to configure traffic rate controls or QoS classifiers. By default (that is, with no QoS classifiers applied), there is no restriction on the maximum throughput, and no traffic priorities or classifications are observed.

Configuring QoS

For automatically provisioned devices, you use the QoS functions within SkyControl (see "Configuring QoS" on page 145).

For manually provisioned devices, you configure QoS by using command-line interface commands (refer to the `set trafficrate` and `set classifier` commands, described in the *SkyPilot Command-Line Interface Reference*) or their Web interface counterparts (refer to the *SkyPilot Web Interface Reference*).

Traffic Rate Controls

Table 2-3 lists the elements that describe traffic rate controls.

Table 2-3. Traffic Rate Controls (Page 1 of 2)

Element	Description
Name	Name of the traffic rate control profile (unique among all such names), as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
Upstream Rate	(No effect on SkyGateways) Number from 64 to 10000, specifying upstream traffic rate (relative to the device using the profile) in kilobits per second; 0 to specify no traffic rate limit.
Downstream Rate	(No effect on SkyGateways) Number from 64 to 10000, specifying downstream traffic rate (relative to the device using the profile) in kilobits per second; 0 to specify no traffic rate limit.

Table 2-3. Traffic Rate Controls (Page 2 of 2)

Element	Description
Broadcast Rate	(SkyGateways only) Number from 64 to 10000, specifying the maximum downstream broadcast and multicast data rate in kilobits per second; 0 to specify no broadcast rate limit.
Comment	(Optional) Free-form text of up to 255 characters. This is not used by SkyControl; it is for administrator reference only.
Date Created	(Read-only) Date and time this traffic rate control record was created.
Date Modified	(Read-only) Date and time this traffic rate control record was last modified.

QoS Classifiers

Table 2-4 lists the elements that describe QoS classifiers.

Table 2-4. QoS Classifiers (Page 1 of 3)

Element	Description
Name	Name of the QoS classifier (unique among all such names), as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
IP TOS Low	Along with **IP TOS High** and **IP TOS Mask**, matching parameters for the IP TOS (Type of Service) byte range and mask. An IP packet with IP TOS byte value `ip-tos` is considered a match if: `tos-low <= (ip-tos AND tos-mask) <= tos-high` If any of these fields is omitted, comparison of the IP packet TOS byte for this entry is irrelevant.
IP TOS High	See **IP TOS Low** above.
IP TOS Mask	See **IP TOS Low** above.
IP Protocol	Protocol name, selected from the provided list.
IP Protocol Number	(Read-only unless Other is selected as the **IP Protocol**) Protocol number. For the list of protocol type numbers, refer to the following IEEE Web page: http://standards.ieee.org/regauth/ethertype/eth.txt.

Table 2-4. QoS Classifiers (Page 2 of 3)

Element	Description
IP Source Address	Maximum of 12 digits in dotted notation.
IP Source Mask	Maximum of 15 digits in dotted notation.
IP Destination Address	Maximum of 12 digits in dotted notation.
IP Destination Mask	Maximum of 15 digits in dotted notation.
TCP/UDP Source Port Start	Starting value for the source port as a number from 1 to 65535. The combination of IP address and port must be unique within all configured QoS classifiers.
TCP/UDP Source Port End	Ending value for the source port as a number from 1 to 65535. The combination of IP address and port must be unique within all configured QoS classifiers.
TCP/UDP Destination Port Start	Starting value for the destination port as a number from 1 to 65535. The combination of IP address and port must be unique within all configured QoS classifiers.
TCP/UDP Destination Port End	Ending value for the destination port as a number from 1 to 65535. The combination of IP address and port must be unique within all configured QoS classifiers.
Source MAC Address	Maximum of 12 digits in dotted notation.
Source MAC Address Mask	Maximum of 15 digits in dotted notation.
Destination MAC Address	Maximum of 12 digits in dotted notation.
Destination MAC Address Mask	Maximum of 15 digits in dotted notation.
Ether Type	Protocol of the traffic to filter, selected from the provided list.

Table 2-4. QoS Classifiers (Page 3 of 3)

Element	Description
Ether Type Number	(Read-only unless Other is selected as the **Ether Type**) Protocol number. For the list of protocol type numbers, refer to the following EEEE Web page: http://standards.ieee.org/regauth/ethertype/eth.txt
IEEE 802.1P User Priority Low	Lower limit of the range of the 801.1p flag in the TCP/IP header for which packets are forwarded instead of dropped, selected from provided list.
IEEE 802.1P User Priority High	Upper limit of the range of the 801.1p flag in the TCP/IP header for which packets are forwarded instead of dropped, selected from provided list.
IEEE 802.1Q VLANID	Virtual LAN ID to which to apply the QoS service policy. All traffic that passes through the VLAN will be subject to the QoS policy.
Mesh Queue Priority	(Read-only) Priority level from 1 (High) to 3 (Low) for packets that match the priority queue setting.
Date Created	(Read-only) Date and time this QoS classifier record was created.
Date Modified	(Read-only) Date and time this QoS classifier record was last modified.
Comment	(Optional) Free-form text of up to 255 characters. This is not used by SkyControl; it is for administrator reference only.

Filtering

Filters are used to control the transfer of user data packets through a SkyPilot network. The filtering actions are performed on data packets received over the SkyPilot device's 10/100bT Ethernet interface. Four protocol fields can be configured. Filtering to allow or deny packets is applied separately to these protocol fields. If multiple filters are defined for a given protocol field, the filters are performed in the order in which they're listed in the SkyControl display (for devices in automatic provisioning mode) or in command-line interface output (for devices in manual provisioning mode). The default filter is always applied last.

Unlike access control lists, which examine data *destined* for a given SkyPilot node, filters are used to filter *all data passing through* a given node.

You can configure filters for the following protocol fields:

- **Ethernet Type**—Limits the traffic through a node to data of a specific protocol type. EtherType values include the following (refer to the IEEE Web page, http://standards.ieee.org/regauth/ethertype/eth.txt, for the current complete list):

`0x0800`	IPv4
`0x0806`	RP
`0x809b`	AppleTalk over Ethernet
`0x8137`	IPX
`0x8191`	NetBIOS/NetBEUI
`0x86dd`	IPv6

- **IP Address**—Limits the traffic through a node to data with specified source and/or destination IP addresses.

- **IP Protocol**—Limits the traffic through a node to IP data of a specific subprotocol type. Subprotocol types include:

`0x01`	ICMP
`0x02`	IGMP
`0x06`	TCP
`0x11`	UDP
`0x73`	L2TP

- **Port**—Limits the traffic through a node to data with a specified port number, which generally identifies a subprotocol type. Valid port numbers include:

`137-139`	NetBIOS
`161-162`	SNMP
`67`	DHCP Client
`68`	DHCP Server

Configuring Filters

For automatically provisioned devices, you configure filters by using SkyControl and selecting **Enable** in the **Filter** field of the node's node profile. You must also set the permission to **Allow** in the corresponding **Filter** field of the node's node profile. (For more information, see "Configuring Node Profiles" on page 126.)

For manually provisioned devices, you configure filters by using the command-line interface command (refer to the `set filter` command, described in the *SkyPilot Command-Line Interface Reference*) or its Web interface counterpart (refer to the *SkyPilot Web Interface Reference*).

EtherType Filters

Table 2-5 lists the elements that describe EtherType filter records.

Table 2-5. EtherType Filters

Element	Description
Name	Name of the EtherType filter (unique among all such names), as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
Protocol	EtherType protocol name allowed by this filter, selected from the provided list.
EtherType	(Read-only unless Other is selected as the **Protocol**) EtherType value in hexadecimal. For the list of protocol type numbers, refer to the following IEEE Web page: http://standards.ieee.org/regauth/ethertype/eth.txt.
Permission	(Default = **Allow**) Setting to allow or deny filtering of data that matches this filter's criteria.
Comment	(Optional) Free-form text of up to 255 characters. This is not used by SkyControl; it is for administrator reference only.
Date Created	(Read-only) Date and time this filter record was created.
Date Modified	(Read-only) Date and time this filter record was last modified.

IP Address Filters

Table 2-6 lists the elements that describe IP address filter records.

Table 2-6. IP Address Filters

Element	Description
Name	Name of the IP address filter (unique among all such names), as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
IP Address	IP address to compare to a packet's source or destination address to determine how this filter is applied; up to 12 digits in dotted notation.
Subnet Mask	Subnet mask used of the IP address group to compare to a packet's source or destination address to determine how this filter is applied; up to 12 digits in dotted notation.
Type	Packet data to which the **IP Address** and **Subnet Mask** fields are compared, specified as one of the following: • **Destination**—Packet destination address • **Source**—Packet destination address • **ARP**—Source IP address of an ARP request or response
Permission	(Default = **Allow**) Setting to allow or deny filtering of data that matches this filter's criteria.
Comment	(Optional) Free-form text of up to 255 characters. This is not used by SkyControl; it is for administrator reference only.
Date Created	(Read-only) Date and time this filter record was created.
Date Modified	(Read-only) Date and time this filter record was last modified.

IP Protocol Filters

Table 2-7 lists the elements that describe IP protocol filter records.

Table 2-7. IP Protocol Filters

Element	Description
Name	Name of the IP protocol filter (unique among all such names), as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
Protocol	IP subprotocol allowed by this filter, selected from the provided list.
IP Protocol	(Read-only unless Other is selected as the **Protocol**) Number of this filter's protocol. For the list of protocol numbers, refer to the following IEEE Web page: http://www.iana.org/assignments/protocol-numbers.
Permission	(Default = **Allow**) Setting to allow or deny filtering of data that matches this filter's criteria.
Comment	(Optional) Free-form text of up to 255 characters. This is not used by SkyControl; it is for administrator reference only.
Date Created	(Read-only) Date and time this filter record was created.
Date Modified	(Read-only) Date and time this filter record was last modified.

Port Filters

Table 2-8 lists the elements that describe port filter records.

Table 2-8. Port Filters

Element	Description
Name	Name of the port filter (unique among all such names), as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
Port	Port number to compare to a packet's source or destination port to determine how this filter is applied; a number from 1 to 65535.
Protocol	(Default = **TCP**) Protocol allowed by this filter, selected from the provided list.
Type	What the filter's **Port** value is compared to, specified as follows: • **Destination**—Data packet's destination port • **Source**—Data packet's protocol source port
Permission	(Default = **Allow**) Setting to allow or deny filtering of data that matches this filter's criteria.
Comment	(Optional) Free-form text of up to 255 characters. This is not used by SkyControl; it is for administrator reference only.
Date Created	(Read-only) Date and time this filter record was created.
Date Modified	(Read-only) Date and time this filter record was last modified.

Access Points

SkyExtender DualBand/TriBand devices incorporate access points, which enable 802.11 network device communication. Automatically provisioned DualBands and TriBands are assigned access point profiles, which in turn are assigned an assortment of profiles as attributes, as described in the following sections.

Wireless Local Area Networks

For every access point, you can define 16 distinct WLANs, which offers significant benefits such as efficient bandwidth use, flexibility, performance, and security. WLANs offer these benefits by enabling the following capabilities:

- Restricting the dissemination of broadcast and node-to-node traffic, thereby reducing the burden of extraneous network traffic.
- Using standard router-based security measures.
- Segregating and switching ISP traffic. Wholesale operators can offer end users a choice of any provider instead of only the provider operating a particular network. In such cases, each WLAN would be assigned to a single ISP.
- Isolating management traffic from user traffic. You can configure a management WLAN, independent of a WLAN for end users. Management traffic is thereby segmented and secure.

Most WLAN deployments use one of two common types of WLAN configuration:

- **Open**—Allows anyone with Wi-Fi capability to connect to the wireless network via the SkyExtender DualBand/TriBand access point. An open WLAN does not authenticate users at the network layer, nor does it depend on authentication by a backend system.

  An open configuration raises obvious security concerns. The lack of encryption makes the network vulnerable to unauthorized access and malicious actions (including denial-of-service attacks).

  You can provide backend authentication at the application layer through a *captive portal* mechanism operating outside your wireless mesh network. A captive portal forces all HTTP traffic from an unauthenticated user to a login Web page and blocks the traffic until the user successfully logs in. (For more information about captive portal mechanisms, refer to the following Web page: http://en.wikipedia.org/wiki/Captive_portal.)

An additional disadvantage of open configurations is that users must begin each session from a Web browser before they can use other Internet applications, such as `email`, `ssh`, `ftp`, and chat clients.

- **Protected**—A Wi-Fi Protected Access (WPA) network, which uses standards-based client authentication and encryption. Users may be authenticated via a Radius server (which you'll need to implement using a third-party solution).

  WPA uses the IEEE 802.11b/g and IETF EAP protocols to give users a secure connection with both the access point and the Radius server, allowing the exchange of credentials (`username@domain` and `password`) and keys for encrypting all traffic between the client and the access point—even after authentication.

  WPA encryption is by WEP, with the addition of keys that are unique to each session and client. This additional keying mechanism eliminates the security problems of the original WEP. You can use AES encryption with the DualBand/TriBand for even stronger encryption capabilities.

  (The access point's default WPA-shared key is `publicpublic`)

  WPA-shared key, `publicpublic`. For more information about WPA, refer to the following Web page:

  http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access.

  If you plan to configure a DualBand/TriBand access point for WPA operating without a pre-shared key, you must configure a Radius server (see "Access Point Radius Server Profiles" on page 53).

Configuring Access Points

For automatically provisioned devices, you modify the settings in the access point profiles that are assigned to the device (see "Configuring Access Point Profiles" on page 122).

For manually provisioned devices, you configure access points by using the Web interface (refer to the *SkyPilot Web Interface Reference*).

Access Point Security Profiles

Table 2-9 lists the elements that describe access point security profiles.

Table 2-9. Access Point Security Profile Elements (Page 1 of 2)

Element	Description
Name	Name of the access point security profile (unique among all such names), as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
Max Remote Login Sessions	(Optional) Maximum number of simultaneous remote Telnet or `ssh` sessions allowed, or 0 to specify unlimited sessions.
Max Remote Login Timeout	(Optional) Number of minutes a Telnet or `ssh` session stays connected without activity, or 0 to never time out.
Telnet Server	Enables or disables the Telnet server for remote access to the access point's command line.
Admin Telnet Password	(Optional) Password and user name for logging in to the Telnet server.
Peer to Peer	Enables or disables peer-to-peer (blocks Layer 2 broadcast and ARP traffic between wireless clients). Typically you'll disable peer-to-peer in a public network if you want to prevent users from "sniffing" traffic or creating accidental "network neighborhoods" at the Ethernet or VLAN level. A private enterprise network may want to enable peer-to-peer to allow shared LAN services such as file sharing.
Management From Wireless Clients	Enables or disables wireless client access to the access point's Web interface; if the check box is not selected, access is disabled (and the Web interface will be accessible only through the SkyPilot wireless mesh network).
Syslog	Enables or disables system logging to a remote syslog server.
Syslog Server	(Available only if **Syslog** is enabled) Syslog server's IP address; maximum of 12 digits in dotted notation.
Syslog Port	(Available only if **Syslog** is enabled; default = 514) Port for syslog server access.

Table 2-9. Access Point Security Profile Elements (Page 2 of 2)

Element	Description
Comment	(Optional) Free-form text of up to 255 characters. This is not used by SkyControl; it is for administrator reference only.
Date Created	(Read-only) Date and time this access point security profile record was created.
Date Modified	(Read-only) Date and time this access point security profile record was last modified.

Access Point Radius Server Profiles

If you plan to configure a DualBand/TriBand access point for WPA with password authentication (instead of using pre-shared keys) you must configure a Radius server with the following:

- The IP address and shared secret of the access point.
- EAP-PEAP/MSCHAPv2 and EAP-TTLS/PAP, or MSCHAPv2 (not EAP-TLS) suitable for WPA. (Your Radius supplier can provide instructions.)
- A Users database with user names and passwords. (You may also need to identify a proxy Radius if you're delegating some domains to other service providers.)

Table 2-10 lists the elements that describe access point Radius server profiles.

Table 2-10. Access Point Radius Server Profile Elements (Page 1 of 2)

Element	Description
Name	Name of the access point Radius server profile (unique among all such names), as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
Primary Host	Primary Radius server's IP address; maximum of 12 digits in dotted notation.
Primary Shared Secret	Shared secret string as specified in the primary Radius server's client configuration.

Table 2-10. Access Point Radius Server Profile Elements (Page 2 of 2)

Element	Description
Primary Authentication Port	(Default = 1812) TCP/UDP port for primary Radius server authentication services; must match the port number configured for authentication on the primary Radius server.
Primary Accounting Port	(Default = 1813) TCP/UDP port for primary Radius server accounting services; must match the port number configured for accounting services on the primary Radius server.
Secondary Host	(Optional) Same as **Primary Host** above, but for the secondary Radius server.
Secondary Shared Secret	(Available only if **Secondary Host** is configured) Same as **Primary Shared Secret** above, but for the secondary Radius server.
Secondary Authentication Port	(Available only if **Secondary Host** is configured) Same as **Primary Authentication Port** above, but for the secondary Radius server.
Secondary Accounting Port	(Available only if **Secondary Host** is configured) Same as **Primary Accounting Port** above, but for the secondary Radius server.
Comment	(Optional) Free-form text of up to 255 characters. This is not used by SkyControl; it is for administrator reference only.
Date Created	(Read-only) Date and time this access point Radius server profile record was created.
Date Modified	(Read-only) Date and time this access point Radius server profile record was last modified.

Access Point SSID Profiles

To accommodate the access point WLANs (see "Wireless Local Area Networks" on page 50), each DualBand has 32 MAC addresses assigned to it, and each TriBand has 64 MAC addresses. The MAC address of the SkyExtender's 5 GHz radio (as seen from the SkyGateway) is printed on the label affixed to the bottom of the DualBand. MAC addresses are allocated as follows:

- DualBand 2.4 GHz/TriBand 4.9 GHz access point is 1 less than the MAC address of the 5 GHz radio.
- TriBand 2.4 GHz access point is 33 less than the MAC address of the 5 GHz radio minus 31.
- DualBand 2.4 GHz WLAN BSSIDs begin with the MAC address of the 5 GHz radio minus 31.

  For example, if the MAC address of a DualBand is 000ADB01319F (hexadecimal), the reserved addresses start at 000ADB013180.
- TriBand 2.4 GHz WLAN BSSIDs begin with the MAC address of the 5 GHz radio minus 63:
- TriBand 4.9 GHz WLAN BSSIDs begin with the MAC address of the 5 GHz radio minus 31.

  For example, if the MAC address of a TriBand is 000ADB017A3F (hexadecimal), the 2.4 GHz access point's MAC address is 000ADB017A1E, and the reserved addresses for the 2.4 GHz WLAN BSSIDs start at 000adb017a00. The 4.9 GHz access point's MAC address is 000ADB017A20, and the 4.9 GHz WLAN BSSIDs start at 000ADB017A20.

Table 2-11 lists the elements that describe access point SSID profiles.

Table 2-11. Access Point SSID Profile Elements (Page 1 of 4)

Element	Description
SSID	Name of the access point SSID profile (unique among all such names), as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
VLAN Name	(Optional) Virtual LAN for which ESSID traffic will be mapped. This name is used to populate the provisioning VLAN selection list.

Table 2-11. Access Point SSID Profile Elements (Page 2 of 4)

Element	Description
Broadcast SSID	Enables or disables access point broadcasting of the SSID to 802.11 clients (making the SSID visible to users). If Broadcast SSID is disabled, users can still associate with this SSID if they know the SSID and can configure their client software to connect to the SSID. Typically, you'll want to enable SSID broadcasting.
802.1p	(Optional) Class of service priority.
SSID Status	Enables or disables this SSID. If SSID Status disabled, the SSID can still be fully configured, but the access point will not announce or respond to connection requests or other traffic directed to the SSID.
Multicast Filter	(Optional) Enable or disable filtering multicast traffic from the ESSID. When enabled, multicast traffic is dropped, freeing resources for other network tasks.
Heartbeat Shutdown	(Optional) Enable or disable preventing clients from accessing the network when the WAN link is down (indicated by the lack of the heartbeat signal).
Dual Power	(Optional) Enable or disable segmenting devices that are capable of transmitting up to 400 mw into a separate BSSID from low-power radio devices. When dual power is enabled, access points can use the high power radio with client nodes that are capable of receiving and transmitting at high power.

Table 2-11. Access Point SSID Profile Elements (Page 3 of 4)

Element	Description
Security Policy	Encryption and/or authentication scheme used by this SSID: • **None**—Open network (no authentication or encryption). • **WEP**—Static WEP; no authentication, shared WEP key, no key rotation, and WEP encryption. Static WEP is easily cracked, and should not be used in production environments. • **802.1x**—802.1x/EAP authentication via dynamic WEP. The WEP key is unique per session and is automatically changed at a periodic rate via Radius reauthentication. This is the preferred choice for older clients that do not support WPA. • **WPA-TKIP**—802.1x/EAP authentication via TKIP (Temporal Key Integrity Protocol), a hardened version of the older WEP standard. The key is updated automatically and transparently with DES or AES encryption. This option provides higher security than WEP or 802.1x but requires users to have a WPA client (which is built into recent versions of Windows XP, Mac OS X, and Linux). WPA-TKIP can be configured to use Radius authentication or a pre-shared key. • **WPA-AES:CCMP**—Complete 802.11i (WPA2) standard, replacing WEP/DES and TKIP with a specific mode of the Advanced Encryption Standard (AES): the Counter Mode with Cipher Block Chaining-Message Authentication Code (CBC–MAC) Protocol (CCMP). CCMP provides both data confidentiality (encryption) and data integrity. This is the highest security option you can choose, but some legacy 802.11 clients may not support it.
WEP Key Size	(Available only if WEP is selected as the **Security Policy**) Key size to use for this network's encryption: 40 bits or 104 bits (also known as 64-bit or 128-bit, respectively). 104 bits is preferred unless the SSID clients are unable to accept that setting.
WEP Allow Shared Key	(Available only if WEP is selected as the **Security Policy**) Enables or disables use of a pre-shared key.
WEP Key Format	(Available only if WEP is selected as the **Security Policy**) Format for the WEP key (ASCII or hexadecimal).

Table 2-11. Access Point SSID Profile Elements (Page 4 of 4)

Element	Description
WEP Encryption Key	(Available only if WEP is selected as the **Security Policy**) Text string that functions as a password; up to 255 printable characters.
802.1x Key Size	(Available only if 802.1x is selected as the **Security Policy**) Key size to use for this network's encryption: 40 bits or 104 bits (also known as 64-bit or 128-bit, respectively). 104 bits is preferred unless the SSID clients are unable to accept that setting.
802.1x Rekeying Period	(Available only if 802.1x is selected as the **Security Policy**) Number of seconds between dynamic key updates. For maximum protection, enter 300 seconds (5 minutes) or less. Don't use too small a value; rekeying requires about a second to complete, so too frequent rekeying can increase downtime.
WPA Pre-Shared Key	(Available only if WPA-TKIP or WPA-AES:CCMP is selected as the **Security Policy**) Enables or disables use of a pre-shared key.
WPA Passphrase	(Available only if WPA-TKIP or WPA-AES:CCMP is selected as the **Security Policy**) Text string that functions as a password; up to 255 printable characters.
Comments	(Optional) Free-form text of up to 255 characters. This is not used by SkyControl; it is for administrator reference only.
Date Created	(Read-only) Date and time this access point SSID profile record was created.
Date Modified	(Read-only) Date and time this access point SSID profile record was last modified.

Access Point High Power MAC Profiles

If the devices in your network are high power as defined by the US FCC rules (FCC 90.1215) for output power, you must define high power MAC profiles for your access points.

Nodes defined as *high power* use the **High Power Level** as defined in the access point profile (see Table 5-2 on page 123). This enables client nodes that have the

capability to transmit using high power (up to 400mw) to communicate over longer distances. Those nodes that are lower power (such as laptops and handheld devices) will communicate with the access point by using the **Low Power Level** as defined in the access point profile (see Table 5-2 on page 123).

The FCC rules allow for this high power usage, but the key use is that many client nodes are low power and cannot receive data from a high power access point, and do not have the radio power to transmit back to the access point. Therefore, to enable such nodes to properly communicate, the nodes must be placed into the low power group.

Table 2-12 lists the elements that describe access point high power MAC profiles.

Table 2-12. Access Point High Power MAC Profile Elements

Element	Description
Enable	Enable or disable high power operations for the client device; select or clear the checkbox.
MAC	Unique 12-character hexadecimal hardware address for this node.
Comments	(Optional) Free-form text of up to 255 characters. This is not used by SkyControl; it is for administrator reference only.
Date Created	(Read-only) Date and time this access point SSID profile record was created.
Date Modified	(Read-only) Date and time this access point SSID profile record was last modified.

Access Point SkyAccess Profiles

Access point SkyAccess profiles define global settings for access points to use regardless of their communications band (2.4 GHz or 4.0 GHz).

Table 2-13 lists the elements that describe access point SkyAccess profiles.

Table 2-13. Access Point SkyAccess Profile Elements

Element	Description
Name	Name of the access point SkyAccess profile (unique among all such names), as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
Transmit Power	Power level for access point transmission.
Beacon Interval	Number of milliseconds between 802.11 beacons. Beacons provide information about the available ESSID/BSSIDs and connection parameters (such as available data rates).
Peer To Peer	Enable or disable wireless client communications within the ESSID. Disabling peer to peer allows clients to communicate only with devices outside the local hotspot.
Management From Wireless Clients	Enable or disable management of the SkyAccess device from the local ESSID.
Radius Profile	RADIUS profile that defines how client users on the access point will authenticate before being allowed access.
Comments	(Optional) Free-form text of up to 255 characters. This is not used by SkyControl; it is for administrator reference only.
Date Created	(Read-only) Date and time this access point SSID profile record was created.
Date Modified	(Read-only) Date and time this access point SSID profile record was last modified.

General Provisioning Guidelines

Some requirements are independent of the provisioning mode you choose. To ensure that network devices form effective links, always follow these guidelines:

- Set the domain of SkyExtenders and SkyConnectors to match the domain assigned to the SkyGateway, or to all domains.
- To allow devices to establish network links more quickly, make sure that the primary frequency of SkyExtenders and SkyConnectors is the same as the primary frequency assigned to the SkyGateway.
- Avoid adding unused frequencies to a device's Allow list.
- Make sure that the *netkeys* (shared network keys) match on all devices attempting for form links. All SkyPilot devices ship with a same default public netkey: `SkyPilot Network, Inc.`

Automatic Provisioning

Automatically provisioned SkyPilot nodes use the parameters configured through the SkyPilot EMS SkyControl provisioning functions. The parameter settings are stored in a SkyPilot server's database and are retrieved by devices upon completion of the devices' startup (for SkyGateway) or formation of links (for SkyExtenders and SkyConnectors). Once the device receives its configuration information from the server, the device is available to participate in the SkyPilot network.

Automatically Provisioning All Network Devices

Table 2-14 summarizes the steps required to automatically provision all devices on a network. Although SkyPilot devices can be provisioned in any order, by following this sequence you can ensure that devices are able to form links as soon as they come online.

Table 2-14. Automatically Provisioning All Network Devices (Page 1 of 2)

	Step	Refer to
1	For new SkyPilot network deployments, custom-install the operating system software on the SkyPilot EMS server.	The appropriate SkyPilot OS installation manual, available on the Trilliant SkyPilot website at www.skypilot.trilliantinc.com/support/
2	For new SkyPilot network deployments, install the server component of SkyPilot EMS, and then install the client component of SkyPilot EMS on any appropriate computer.	*SkyPilot EMS Installation*
3	For new SkyGateways, set up the DHCP server and, if the provisioning server is behind a firewall, open ports for data traffic between the server and SkyPilot devices.	"Adding Devices to the DHCP Configuration" on page 95 "Configuring a Firewall for SkyPilot Operations" on page 161
4	Provision the SkyGateway(s).	"Automatically Provisioning a Device" on page 63
5	For new SkyGateways, complete the installation and power it on.	*SkyGateway/SkyExtender Installation and Setup*
6	(Optional) Log in to the SkyGateway and configure the management VLAN.	"Configuring VLANs" on page 140
7	Provision the SkyExtender(s).	"Automatically Provisioning a Device" on page 63
8	For DualBands and TriBands, provision the access point(s).	For information about access point settings, refer to *SkyPilot Network Administration*. For configuration procedures, refer to the *SkyPilot Web Interface Reference*

Table 2-14. Automatically Provisioning All Network Devices (Page 2 of 2)

	Step	Refer to
9	For new SkyExtenders, install the device and power it on.	*SkyGateway/SkyExtender Installation and Setup*
10	Provision the SkyConnector(s).	"Automatically Provisioning a Device" on page 63
11	For new SkyConnectors, install the device and power it on.	The appropriate installation manual: ● *SkyConnector Indoor Installation* ● *SkyConnector Outdoor Installation*
12	Provision the SkyAccess device(s).	"Automatically Provisioning a Device" on page 63
13	For new SkyAccess device, install the device and power it on.	*SkyAccess DualBand Installation*

Automatically Provisioning a Device

SkyPilot automatic device provisioning is a modular process whereby you use SkyControl to add specific configuration parameter building blocks to the provisioning server's database. Then you create a *profile*—a collection of configuration parameters that can be assigned to multiple devices that require the same parameter settings. This enables you to easily change a parameter setting for every device that uses a common profile, just by changing the parameter setting once in that profile. After a profile is changed, every device inherits the change the next time the device requests its configuration.

Automatically provisioned devices receive their configuration from the provisioning server (the SkyPilot EMS server) in the following situations:

- Every time the device attempts to form a link
- Every time the device reroutes
- At an interval previously configured within the device's configuration file
- When the **Reload** command is selected from SkyControl

- When the `reload` command is entered from the command line
- When an SNMP write occurs on the device's MIB `reload` variable

Table 2-15 describes the necessary steps to using SkyControl to configure a SkyPilot device for automatic provisioning.

Table 2-15. Automatically Provisioning a SkyPilot Device (Page 1 of 2)

Step	Description	Refer to
1	Make sure the most current software images are available in the EMS provisioning server's `/var/ftp/pub/images` directory.	
2	Start SkyPilot EMS.	"Using SkyPilot EMS" on page 9
3	Choose the software image the provisioning server will use to configure the new device.	"About Software Images" on page 72
4	For SkyGateways, assign a domain. If no domain exists, create one. For other devices, specify a domain for the device that's consistent with the domain assigned to the SkyGateway operating as a hub for the wireless mesh network.	"Configuring Domains" on page 122
5	(Optional) Configure a data VLAN to which the device can be assigned. (Management VLANs are configured through a SkyGateway's command-line interface.)	"Configuring VLANs" on page 140

Table 2-15. Automatically Provisioning a SkyPilot Device (Page 2 of 2)

Step	Description	Refer to
6	For DualBands/TriBands, confirm that appropriate access point profiles exist (including component security profiles). If profiles don't exist, create them in the following order: • Access point security profile • (For protected access networks, not open access networks) Access point Radius profile • Access point SSID profile • Access point profile(s)	"Configuring Access Point Profiles" on page 122
7	Confirm that an appropriate node profile exists for the device. If no appropriate profile exists, create one.	"Configuring Node Profiles" on page 126
8	Add a node to the network for the device, assigning to it the appropriate node profile and attributes.	"Configuring Nodes" on page 136
9	Verify that the newly configured device has been successfully added as a node on the mesh network.	"Node Device Views" on page 13
10	(Optional) Set device polling intervals and other provisioning parameters.	Appendix 5, "Provisioning With SkyControl"

This table describes only those SkyControl provisioning functions that are necessary for enabling a device for automatic provisioning; you can perform many additional functions using SkyControl provisioning (see "Optional Provisioning Parameters" on page 35).

Manual Provisioning

Manually provisioned SkyPilot nodes use parameters configured through the command-line interface or Web interface. The nodes store the parameter settings in flash memory, where they remain available for recall when the device starts up. Once the device starts up, it is operationally ready.

Assuming no security changes have been made that would affect the ability of SkyPilot devices to proceed (such as netkey values or domain IDs), all SkyPilot devices will discover and establish links with the wireless network without any required commands, even in manual provisioning mode. However, the following are exceptions that may require manual intervention on the part of the operator:

- The SkyGateway must be configured with a primary transmit frequency, which it will use to transmit data and establish links.
- If your deployment uses a management VLAN, the VLAN must be manually configured on the SkyGateway. This is necessary because a VLAN ID could affect whether SkyPilot management traffic passes through the wired network to which the SkyGateway is connected through its Ethernet interface.
- If VLANs have been configured for end-user data in the wired network to which the SkyGateway is connected through its Ethernet interface, VLANs must be configured on all SkyExtender and SkyConnector devices in order for end-user data to be appropriately tagged, sent, and received.
- If netkeys have been changed on connected devices, the new netkey must be manually configured on any device trying to join that network. This is necessary because the netkey is the basis for determining whether a link is trusted, which would make it impossible to rely on automated provisioning to supply this parameter. If default netkeys are used, no change is necessary.

The remaining configuration settings are optional; they're not required to be set in order for a device to join the network and pass end-user data. Changes made during manual provisioning are stored in flash memory, and therefore do not take effect until the device is restarted.

Manual Provisioning Procedure

Table 2-16 summarizes the steps required to manually provision a device.

Table 2-16. Manually Provisioning a Device (Page 1 of 2)

	Step	Refer to
1	Decide whether to provision the device by using the command-line interface or the Web interface. (For DualBand/TriBand access points, you must use the Web interface.)	"Choosing a Manual Provisioning Method" on page 68
2	If the device is not already installed in a SkyPilot network, prepare the device for installation by installing the necessary cabling and readying the device for service.	The appropriate installation manual: • *SkyGateway/SkyExtender Installation and Setup* • *SkyConnector Indoor Installation* • *SkyConnector Outdoor Installation*
3	Power on the device.	
4	Connect a computer to the device and access the command-line interface or the Web interface. (For DualBands/TriBands, this step refers to the SkyExtender portion of the device.)	*SkyPilot Command-Line Interface Reference* *SkyPilot Web Interface Reference*
5	Provision the device, making sure to set at least the minimum provisioning parameters. (For DualBands/TriBands, this step refers to the SkyExtender portion of the device.)	"Required Provisioning Parameters" on page 30 and either of the following: • *SkyPilot Command-Line Interface Reference* • *SkyPilot Web Interface Reference*

Table 2-16. Manually Provisioning a Device (Page 2 of 2)

	Step	Refer to
6	For DualBands/TriBands, reboot the device, connect a computer to the device's 2.4 GHz access point, and provision the access point.	*SkyPilot Web Interface Reference*
7	For TriBands, connect a computer to the 4.9 GHz access point and provision it.	*SkyPilot Web Interface Reference*
8	Power off the device.	
9	If the device is not already installed in a SkyPilot network, complete the installation.	The appropriate installation manual: • *SkyGateway/SkyExtender Installation and Setup* • *SkyConnector Indoor Installation* • *SkyConnector Outdoor Installation*
10	Power on the device.	

Choosing a Manual Provisioning Method

As described in more detail in the sections that follow, there are two methods of performing manual provisioning:

- **Command-line interface**—A set of command-line commands for SkyPilot devices' configuration options (except DualBand/TriBand access points).
- **Device Web interface**—A Web-based interface that provides configuration options for all SkyPilot devices.

NOTE The device Web interface is an interface to a single device. This interface is distinct from the SkyPilot EMS Web interface that is the primary focus of this guide.

Command-Line Interface Provisioning

For manual provisioning, all SkyPilot devices (except the access point portion of DualBands/TriBands) provide a command-line interface that allows you to interact with the equipment through typed commands.

You can access the command-line interface by connecting a PC or laptop to the device's Ethernet interface (except for DualBands, which don't have an Ethernet interface) and using Telnet to start a communications session. The SkyGateway and SkyExtender also include a serial port for connecting to a console via a serial cable.

TIP The `set prov` command provides a convenient method for setting all the basic provisioning parameters for a device. This command queries you for all the provisioning parameters so that you don't need to set each parameter individually. For more information, refer to the description of the `set prov` command in the *SkyPilot Command-Line Interface Reference*.

For details about accessing and using the command-line interface and a full description of the command-line interface commands, refer to the *SkyPilot Command-Line Interface Reference*.

Device Web Interface Provisioning

The Device Web interface provides two levels of access:

- **View-only level**—Provides access to a single Web page displaying the current operating status of a SkyPilot device.
- **Administrator level**—Provides password-protected access to multiple pages of content and a mechanism for modifying the configuration of the monitored SkyPilot device.

The Web interface provides access to a manually provisioned DualBand/TriBand access point as well as an easy alternative to the command-line interface for an administrator to use to monitor and manage SkyPilot devices.

For details about accessing and using the Web interface and a full description of its functions, refer to the *SkyPilot Web Interface Reference*.

3

Administration

SkyPilot network administration involves routine management tasks, such as managing software and customers, configuring security, and creating reports. This chapter describes these management tasks and directs you to the corresponding detailed procedures.

Chapter Highlights

- About software images
- Managing software change schedules
- Managing customers
- Managing access control lists
- Managing network security
- About reports

About Software Images

Every SkyPilot device has two partitions (A and B) for storing software in flash memory. At any given time, one partition (either A or B) is designated the active partition, and the other partition is designated the backup partition.

Correspondingly, every SkyPilot device has two software images embedded in flash memory:

- **Active image**—The software image stored in the partition currently designated the active partition. This image is used by a device when it starts up.
- **Backup image**—The software image stored in the partition currently designated the backup partition. This image is used by a device if the active image becomes unbootable (as explained below).

When a new software image is downloaded to a given partition, the image previously in that partition is overwritten.

If you use SkyControl to manage the software images, you simply specify the name of the desired software image, and SkyControl takes care of downloading it to the proper partition and managing which partition is designated the active partition.

If you're manually managing the software images, you'll specify which partition a software image is downloaded into and then designate which partition to make the active one (which implicitly designates the corresponding image as the active image).

The device assigns every image a state:

- **Accepted**—Either the image is known to be good (the device has successfully formed links) or its state has been manually set to `accepted` (via the `set activeimage` command, described in the *SkyPilot Command-Line Interface Reference*).

- **Trial**—The image has been successfully downloaded but has not yet been used to form links.
- **Unbootable**—The image either was partially downloaded or was determined during startup to be corrupt. (You can't manually accept an unbootable image.)

Nodes on a SkyPilot network are able to interoperate using different software versions within the same major version release. For example:

- Software versions 1.0.0 to 1.0.2p2 are all compatible with each other.
- Software versions 1.1 through 1.1p2 are all compatible with each other.
- Software versions 1.2 through 1.2p3 are all compatible with each other.

SkyPilot nodes use anonymous FTP to download new software images. The FTP server therefore becomes the central repository of software images.

Managing Software Change Schedules

For manually provisioned devices, you configure a device's software by using the command-line interface commands (refer to the `ftpimage` and `set activeimage` commands, described in the *SkyPilot Command-Line Interface Reference*) or their Web interface counterparts (refer to the *SkyPilot Web Interface Reference*).

For automatically provisioned devices, you can schedule a future software version change by using the Software Schedule screen in SkyControl.

To configure a software change schedule:

1. On the **Provisioning** menu, click **Software Schedule**.

   The display pane changes to show the Software Schedule screen.

2. Perform the desired operation:
   - To add a schedule—On the toolbar, click **New**; enter the information for the new schedule (see Table 3-1 on page 74); on the toolbar, click **Save**.

- To modify a schedule—Right-click the desired schedule's row and click **Edit**; edit the desired elements (see Table 3-1); on the toolbar, click **Save**.
- To delete a schedule—Right-click the desired schedule's row and click **Delete**; then click **Yes**.

Table 3-1. Software Schedule Elements

Element	Description
Name	Name of the software schedule record (unique among all such names), as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
Schedule Date	Date on which the specified software will be downloaded, selected by clicking **Calendar**.
Status	(Optional) Activates or inactivates the scheduled software download.
Selected Node Profile	Node profile(s) to which this software schedule is assigned; moved between the **Select Node Profile** and **Selected Node Profile** lists by using the desired direction's move button (**>>** or **<<**).
Comments	(Optional) Free-form text of up to 255 characters. This is not used by SkyControl; it is for administrator reference only.
Date Created	(Read-only) Date and time this software schedule record was created.
Date Modified	(Read-only) Date and time this software schedule record was last modified.

Managing Customers

Customers are individual subscribers, as well as companies with users of their own. Multiple automatically provisioned SkyPilot nodes can be assigned to any given customer (although each node can be assigned to *only a single* customer). You can perform searches for existing customers based on any combination of customer information, including customer name, company name, or customer address or phone number. In addition to adding, modifying, and deleting customers, by modifying a customer profile you can assign nodes to customers and remove such assignments.

To manage customer records:

1 On the **Provisioning** menu, click **Customer Maintenance**.

The display pane changes to show the Customer Maintenance screen.

2 Perform the desired operation:

- To add a customer—On the toolbar, click **New**; enter the information for the new customer (see Table 3-2); on the toolbar, click **Save**.
- To modify a customer—Right-click the desired customer's row and click **Edit**; edit the desired elements (see Table 3-2); on the toolbar, click **Save**.
- To delete a schedule—Right-click the desired customer's row and click **Delete**; then click **Yes**.

Table 3-2. Customer Profile Elements (Page 1 of 2)

Element	Description
First Name	Free-form text of up to 64 alphanumeric characters.
Last Name	Free-form text of up to 64 alphanumeric characters.
Company Name	Free-form text of up to 64 alphanumeric characters.
Address 1	Free-form text of up to 255 alphanumeric characters.
Address 2	(Optional) Free-form text of up to 255 alphanumeric characters.

Table 3-2. Customer Profile Elements (Page 2 of 2)

Element	Description
City	Free-form text of up to 255 alphanumeric characters.
State	Free-form text of up to 255 alphanumeric characters.
Country	Selected from a provided list.
Postal Code	Free-form text of up to 255 alphanumeric characters.
Day Phone	(Optional) Free-form text of up to 255 alphanumeric characters.
Evening Phone	(Optional) Free-form text of up to 255 alphanumeric characters.
E-mail	(Optional) Free-form text of up to 255 alphanumeric characters.
Comment	(Optional) Free-form text of up to 255 characters. This is not used by SkyControl; it is for administrator reference only.
Date Created	(Read-only) Date and time this customer profile record was created.
Date Modified	(Read-only) Date and time this customer profile record was last modified.

Managing Access Control Lists

Access control lists (ACLs) enhance system security by controlling access to the local management interface on a SkyPilot node port—for example, restricting access to a given node to a specified set of management stations.

ACLs also can limit the number of management stations permitted to gain Telnet access to a given node port. Management stations that are denied Telnet access can still use SNMP to monitor a node's status.

Unlike filters, which filter *all data passing through* a given SkyPilot node, ACLs examine data *destined* for a given node.

By default (that is, if you do not configure ACLs), there are no restrictions to accessing SkyPilot devices. To avoid a negative impact on performance, SkyPilot recommends limiting the number of ACLs you configure to eight.

For a manually provisioned device, you configure its ACL by using the command-line interface command (refer to the `set acl` command, described in the *SkyPilot Command-Line Interface Reference*) or its Web interface counterpart (refer to the *SkyPilot Web Interface Reference*).

For automatically provisioned devices, you use the Access Control List screen in SkyControl.

To configure access control lists:

1. On the **Provisioning** menu, click **Access Control LIst**.

   The display pane changes to show the Access Control List screen.

2. Perform the desired operation:

   - To add an access control list—On the toolbar, click **New**; enter the information for the new access control list (see Table 3-3); on the toolbar, click **Save**.

- To modify an access control list—Right-click the desired access control list's row and click **Edit**; edit the desired elements (see Table 3-3); on the toolbar, click **Save**.
- To delete an access control list—Right-click the desired access control list's row and click **Delete**; then click **Yes**.

Table 3-3. Access Control List Elements

Element	Description
Name	Name of the ACL list (unique among all such names), as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
IP Address	IP address from which this ACL allows access; up to 12 digits in dotted notation.
Subnet Mask	Subnet mask used to allow a group of IP addresses to access a node; up to 12 digits in dotted notation.
Port	Destination port through which access is granted; a number from 1 to 65535.
Protocol	(Default = **TCP**) Protocol allowed by this ACL, selected from a provided list.
Comment	(Optional) Free-form text of up to 255 characters. This is not used by SkyControl; it is for administrator reference only.
Date Created	(Read-only) Date and time this ACL record was created.
Date Modified	(Read-only) Date and time this ACL record was last modified.

Managing Network Security

The SkyPilot Security Manager provides a complete set of network security functions, including the capability to set up user profiles, to assign users to security groups, and to configure which EMS functions users or groups can access.

Managing Users

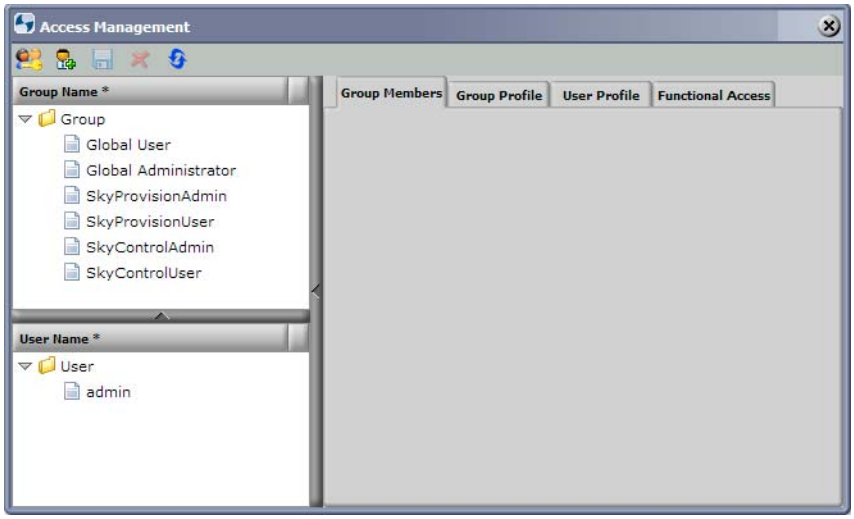
Using customized roles is the key to limiting access and capability for system users.

To manage users:

1 From the menu bar, choose **Security ➤ Access Management**.

SkyPilot EMS displays the Access Management screen (Figure 3-1).

Figure 3-1. Access Management screen



2 Add, modify, or delete users or groups as desired.

3 Click the **Save** button.

You can also change the logged in user's SkyPilot EMS password (except for the admin user).

Changing Passwords

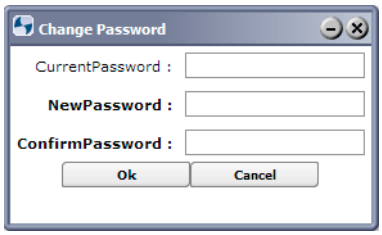
Except if you are logged in as the admin user, you can change your password directly—that is, without using the more complex access management functions.

To change the logged in user's SkyPilot EMS password:

1 From the menu bar, choose **Security ➤ Change Password**.

SkyPilot EMS displays the Change Password screen (Figure 3-2).

Figure 3-2. Change Password screen



2 Enter the **Current Password** and **New Password**, **Confirm** the password (retype it), and click **OK**.

NOTE Although there are no restrictions passwords, it is recommended that you follow standard secure password guidelines, such as using a minimum of eight characters, including both letters and numbers, and so on.

The password is changed.

About Reports

You can view a chart of data for up to four devices at a time and choose a different reporting interval (latest, daily, weekly, and so on) for each device.

About the SkyPilot MIB

The SkyPilot MIB contains objects that have been configured to enable data collection through collection tasks (both default and user-configured), as described in this section. The collected information is used by SkyControl's reporting and system statistics functions.

The SkyPilot MIB is also the source of information for SkyPilot alarms (through SNMP trap and performance threshold mechanisms).

For the current MIB object definitions, refer to the `spMib.txt` file, located in the `/usr/local/skypilot/EMS/client/mibs` directory.

WARNING Do not change the `spMib.txt` file. If you change this file and load it into a MIB browser, the SkyPilot nodes' SNMP operations will not work properly, and SkyControl will not be able to perform its monitoring functions.

Data Collection Tasks

Data collection tasks collect data from the SkyPilot MIB for a specific device, at defined intervals, for defined periods of time. The collected information is stored on the EMS server, in its database.

When you add a device to your network, SkyPilot EMS automatically creates the following data collection tasks for the device:

- `Status_Poll`—Collects the device's status. The default polling interval is 60 seconds, and you can change this interval from 1 second to hundreds of days. You'll gain network accuracy the smaller you make the interval, but values less than 60 seconds can have an adverse effect on EMS performance.

- `Statistics`—Collects an array of statistics for the device. The default polling interval is 120 seconds, and you can change this interval from 1 second to hundreds of days. You'll gain accuracy the smaller you make the interval, but values less than 120 seconds can have an adverse effect on EMS performance.

You can configure the data collection to poll more or less frequently.

TIP If you know you're not going to need a data collection task's statistics for a while, you can stop it from running, which decreases the EMS server's load and may improve performance. You can stop and start either of the device's default data collection tasks as well as any custom tasks you've configured.

4

Maintenance

SkyPilot maintenance tasks include developing monitoring and troubleshooting strategies. This chapter describes techniques for maintaining your SkyPilot network, as well as solutions to common troubleshooting issues.

Chapter Highlights

- Monitoring a network's topology with SkyControl
- Monitoring events and alarms
- Monitoring link states
- Managing IP addresses
- Configuring DHCP
- Using utilities
- Troubleshooting

Monitoring a Network's Topology with SkyControl

SkyControl is SkyPilot's customized SNMP management system for real-time monitoring and management of automatically provisioned devices. One of SkyControl's unique features is that it provides tree and flat views of your network topology as well as a graphical view (via the integrated Google Earth Management System) with at-a-glance updates on topology, routing, and performance.

SkyControl's SNMP implementation includes:

- Default community strings—`public` (read-only) `private` (read-write), and `public` (trap)
- Support for the following standard MIBs:
  - MIB II
  - Ether-Like
  - Bridge
- The private/enterprise SkyPilot MIB, which offers information about the following SkyPilot hardware components and software elements:
  - Nodes—status, uptime, software/hardware version, and more
  - Links—state, RSSI, modulation, antenna, and more
  - Routing tables—forwarding, routing, MAC, and more
  - ACLs (access control lists)
  - Filters

Monitoring Events and Alarms

SkyPilot EMS includes comprehensive event and monitoring functions. SNMP traps cause events, which in turn cause alarms based on default conditions and custom-defined performance thresholds.

There are three types of SkyPilot alarm:

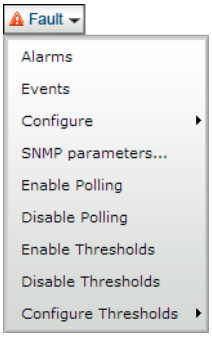
- **Polling alarm**—The EMS server automatically polls every SkyPilot network device, and can therefore report the following:
  - Agent down
  - Agent unreachable
  - IP conflict
- **SNMP trap alarm**—An event reported by a device when it detects a value change of a MIB object that's been configured to generate traps. The SkyPilot EMS includes a large set of preconfigured traps, and you can customize and create additional traps corresponding to any MIB OID (organization ID).

  In order for SNMP trap alarms to be generated, you need to configure the following:
  - The corresponding EMS trap receivers (see "Configuring SNMP Parameters" on page 143)
  - The community string for notification, which must match the device's hardcoded default community string, `public` (see "Configuring SNMP Parameters" on page 143)
  - The device's SNMP community string and trap receiver attributes (select the device's node profile and associate the desired attributes as described in "Configuring Node Profiles" on page 126)
- **Threshold alarm**—An event triggered by SkyPilot EMS when it detects that a MIB object's value crosses a preconfigured threshold.

Configuring Alarms

You can manage alarms, create alarm filters, and configure alarm forwarding and notification email from the SkyPilot EMS **Fault** menu.

Figure 4-1. EMS Fault menu



Of particular interest are the following operations:

- Viewing alarms—From the alarms display (which is shown by choosing **Fault ➤ Alarms** from the EMS menu bar), you can display details for any single alarm by double-clicking anywhere in the alarm line's text.
- Viewing events—From the events display (which is shown by choosing **Fault ➤ Events** from the EMS menu bar), you can display details for any single event by double-clicking anywhere in the event line's text.
- Alarm trap forwarding—You can add, modify, and delete SNMP listeners for alarm traps; choose **Fault ➤ Configure ➤ Northbound Trap Receivers** from the EMS menu bar. For details, see "Configuring Trap Parsers" on page 88 and "Configuring Northbound Trap Receivers" on page 90.
- Setting up email notifications—You can configure email notification to automatically send email for selected alarms to selected recipients; choose choose **Fault ➤ Configure ➤ Alarm Mail Notification** from the EMS menu bar.

You can configure alarm levels, set up email notifications, generate reports, and more. By monitoring alarms, you can take appropriate corrective action, as well as prevent major network disruptions.

Performance Threshold Operations

Performance thresholds are severity level profiles that can be associated with MIB objects for which data collection tasks are configured and alarms are generated. So, for example, you can specify that when a MIB object's value crosses a threshold level, a threshold event will be generated and a corresponding alarm is created.

1 From the SkyPilot EMS menu bar, choose **Fault ➤ Configure Thresholds ➤** [**Link** | **Modulation** | **RSSI**].

SkyPilot EMS displays the applicable configure threshold screen.

2 Perform the desired operation:

- To add a threshold—On the toolbar, click **New**; enter all the information for the new trap parser (see Table 4-1); on the threshold screen toolbar, click **Save**.
- To modify a threshold—Right-click the desired threshold in the Threshold list and click **Edit**; edit the desired elements (see Table 4-1); on the toolbar, click **Save**.
- To delete a threshold—Select the desired trap in the threshold list; on the threshold screen toolbar, click **Delete**; then click **Yes**.

Table 4-1. Link Threshold Elements (Page 1 of 2)

Element	Description
Field Type	(Default = **All**) Type of entity for which this threshold is applicable; select from the provided list.
Field Value	(Dependent on **Field Type** selection) Identification of the specific entity for which this threshold is applicable; selected from the provided list.
Operator	(Default is **<=**) Alarm trigger point. To trigger the alarm when the value falls to less than or equal to the corresponding threshold (RSSI Value or Modulation Value), choose **<=**; to trigger the alarm only when the value falls below the corresponding threshold, choose **<**.
RSSI Value	(Modulation Threshold and RSSI Threshold only) Received signal strength indicator threshold at which to trigger the alarm.

Table 4-1. Link Threshold Elements (Page 2 of 2)

Element	Description
Operator	(Default is **<=**) Alarm trigger point. To trigger the alarm when the value falls to less than or equal to the corresponding threshold (RSSI Value or Modulation Value), choose **<=**; to trigger the alarm only when the value falls below the corresponding threshold, choose **<**.
Modulation Value	Threshold at which the corresponding alarm is triggered; selected from provided list.
Alarm Severity	Type of alarm to associate with this threshold.

3 Edit the threshold elements and click **Save**.

Focus returns to the Configure Threshold screen.

4 Click **Close**.

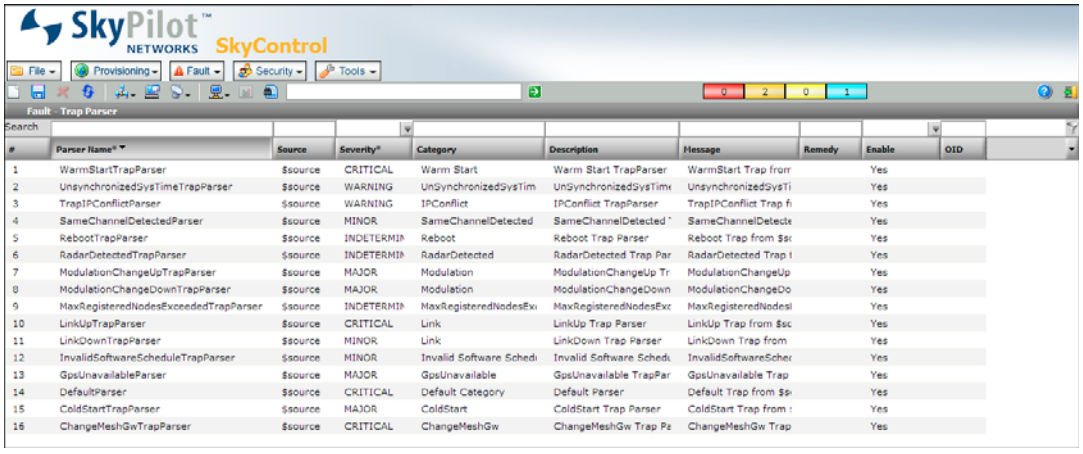
Configuring Trap Parsers

To configure trap parsers:

1 From the SkyPilot EMS menu bar, choose **Fault ➤ Configure ➤ Trap Parsers**.

The SkyPilot EMS display pane shows all the trap parsers (Figure 4-2).

Figure 4-2. Trap Parsers display



2 Perform the desired operation:

- To add a trap—On the toolbar, click **New**; enter all the information for the new trap parser (see Table 4-2); on the toolbar, click **Save**.
- To modify a trap—Right-click the desired trap in the Trap Parsers list and click **Edit**; edit the desired elements (see Table 4-2); on the toolbar, click **Save**.
- To delete a trap—Select the desired trap in the Trap Parsers list; on the toolbar, click **Delete**; then click **Yes**.

Table 4-2. Trap Parser Elements (Page 1 of 2)

Element	Description
Parser Name	Name of the SNMP trap (unique among all such names), as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
Source	(Optional) Devices(s) from which the trap was received.
Severity	Trap alarm severity (such as Critical or Major).
Category	(Optional) Group to which an SNMP trap should be associated. Applicable when configuring a specific group of traps that should be forwarded as part of the northbound trap receivers configuration.
Description	(Optional) User-configurable description of the SNMP trap. This name is not used by SkyControl; it is for administrator reference only.
Message	(Optional) Text message to forward as part of the SNMP trap to describe the alert. This field can be used to customize which traps are forwarded: define this text to match the northbound trap receiver **Message Detai**l field (see Table 4-3 on page 91).

Table 4-2. Trap Parser Elements (Page 2 of 2)

Element	Description
Remedy	(Optional) User-entered text explaining what was done to address the issue.
Enable	(Optional) Enable or disable processing of the trap. If a trap parser is not enabled, SkyControl will not trigger the corresponding alarm, even if the trap is received.
OID	(Optional) SNMP Object Identifier for the trap. The trap receiver uses this information to associate trap information in the SkyPilot MIB.

Configuring Northbound Trap Receivers

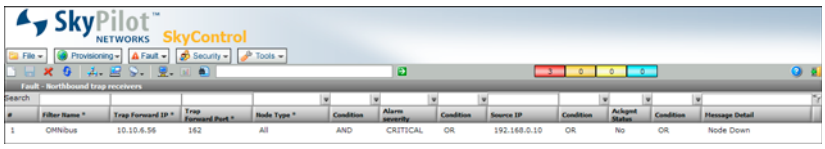
Generally you use a Network Management System (such as IBM Tivoli) to aggregate traps from multiple sources and provide event correlation. To receive SkyPilot EMS traps and events, you use SkyControl to configure northbound trap receivers, which enables the SkyPilot EMS to forward all traps and events in the system to your upstream trap aggregator.

To northbound trap receivers:

1. From the SkyPilot EMS menu bar, choose **Fault ➤ Configure ➤ Northbound Trap Parsers**.

   The SkyPilot EMS display pane shows all the northbound trap receivers (Figure 4-3).

   Figure 4-3. Northbound Trap Receivers display



2. Perform the desired operation:

   - To add a northbound trap receiver—On the toolbar, click **New**; enter all the information for the new northbound trap receiver (see Table 4-3); on the toolbar, click **Save**.

- To modify a northbound trap receiver—Right-click the desired northbound trap receiver in the Northbound Trap Receivers list and click **Edit**; edit the desired elements (see Table 4-3); on the toolbar, click **Save**.
- To delete a northbound trap receiver—Select the desired northbound trap receiver in the Northbound Trap Receivers list; on the toolbar, click **Delete**; then click **Yes**.

Table 4-3. Northbound Trap Receiver Elements (Page 1 of 2)

Element	Description
Filter Name	Name of the trap receiver profile (unique among all such names), as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
Trap Forward IP	IP address of SNMP trap receiver; maximum of 12 digits in dotted notation.
Trap Forward Port	(Default = **162**) Port in which the trap receiver listens for the trap; number from 1 to 65535. The combination of Trap Forward IP address and port must be unique (to northbound trap receivers).
Node Type	(Default = **All**) Type of SkyPilot device from which SkyPilot EMS forwards SNMP traps; selected from a provided list
Condition	(Optional) Filtering condition statement that defines which traps are forwarded (AND or OR). For example, to forward SNMP traps from SkyExtenders whose links are down, select the AND condition. Using the condition filtering enables forwarding predetermined types of SNMP traps instead of all traps.
Alarm Severity	(Optional) Trap alarm severity (such as Critical or Major).
Condition	(Optional) Filtering condition statement that defines which traps are forwarded (AND or OR). For example, to forward SNMP traps from SkyExtenders whose links are down, select the AND condition. Using the condition filtering enables forwarding predetermined types of SNMP traps instead of all traps.
Source IP	(Optional) IP address of the single device from which to forward SNMP traps. If this is not specified, SNMP traps will be forwarded from all devices whose traps match this trap receiver configuration.

Table 4-3. Northbound Trap Receiver Elements (Page 2 of 2)

Element	Description
Condition	(Optional) Filtering condition statement that defines which traps are forwarded (AND or OR). For example, to forward SNMP traps from SkyExtenders whose links are down, select the AND condition. Using the condition filtering enables forwarding predetermined types of SNMP traps instead of all traps.
Ackgmt Status	(Optional) Filter based on whether the alarm has been acknowledged (**Yes**) or not (**No**).
Condition	(Optional) Filtering condition statement that defines which traps are forwarded (AND or OR). For example, to forward SNMP traps from SkyExtenders whose links are down, select the AND condition. Using the condition filtering enables forwarding predetermined types of SNMP traps instead of all traps.
Message Detail	(Optional) Filter to send only alarms that have a matching message detail, which is customized by configuring the trap parsers' **Message** field (see Table 4-2 on page 89).

Monitoring Link States

By monitoring link states in your SkyPilot network, you can troubleshoot a variety of provisioning and operational problems.

Table 4-4 describes the possible link states as shown in GEMS; Table 4-5 describes the possible link states as shown through a device's command-line interface.

Table 4-4. Link States: GEMS Monitoring

State	Description	Firmware version
active	The link is active	All
standby	The link is in standby state and is available for failover.	All
transition	The link's state is changing from active to standby, or vice versa.	All

Table 4-5. Link States: Command-Line Interface Monitoring (Page 1 of 2)

State	Description	Firmware version
act mgmt	The link is to a child node and is active.	All
act path	The link is the next hop to the gateway and is active.	All
standby	The link is in standby state and is available for failover.	1.0.0 to 1.0.2p2
standby-o	The link is in standby state and has been optimized.	1.1 and later
standby-h	The link is in standby state but has not yet been optimized.	1.1 and later
inactive	The link is currently inactive; there is no longer a connection.	All

Table 4-5. Link States: Command-Line Interface Monitoring (Page 2 of 2)

State	Description	Firmware version
non-opt	The link is currently being optimized.	All
pre-auth	The link is being authorized and provisioned.	All
auth fail	Authentication has failed (usually caused by incorrect netkeys).	All
prov fail	Provisioning has failed due to DHCP failure or provisioning server failure.	All
parent	A hello beacon has been received from a child node, and the connection is initiating.	All
child	A hello beacon has been received from a parent node, and the connection is initiating.	All

Managing IP Addresses

All SkyPilot devices ship with the default IP address 192.168.0.2, accessible only from the Ethernet interface. A SkyGateway replaces this default when it receives a new address through DHCP or if it's explicitly configured with a static IP address. However, SkyExtenders and SkyConnectors keep this default IP address available in addition to any IP address received through DHCP or static configuration.

Adding Devices to the DHCP Configuration

To enable automatic assignment of a fixed IP address to a SkyPilot device, you must add the device to your DHCP server's configuration.

NOTE If you have disabled SkyControl's integrated DHCP management, you must manually edit your `dhcp.conf` file (typically located in the `/etc` directory) instead of using the SkyPilot EMS DHCP functions.

For further details about DHCP, see "Configuring DHCP" on page 95.

Monitoring DHCP Activity

You can monitor the DHCP activity on your SkyPilot network by entering the following command at a SkyPilot EMS terminal window:

```
tail -f /var/log/messages
```

To end DHCP monitoring, press CTRL+C.

The DHCP leases file, `dhcpd.leases`, is located in the `/var/lib/dhcp/` directory, and can be viewed using `more/vi/less`.

You can also use the toolbar's **DHCP** button and choose **View Log**.

Configuring DHCP

The DHCP integration within SkyControl provides a front end for manipulating the SkyPilot `dhcpd.conf` file (which contains header information and a pointer to the `dhcpd_skypilot.conf` file) and the subnet and host declarations that are stored in the `dhcpd_skypilot.conf` file. Both files are regenerated every time you change the confutation though the SkyPilot EMS.

NOTE If you already have a dhcpd configuration file, SkyPilot can parse it and place its items into the EMS database, so you do not need to use the DHCP functions described here to re-create your configuration.

The DHCP subnet and host functions are configurable at several levels (scope of applicability):

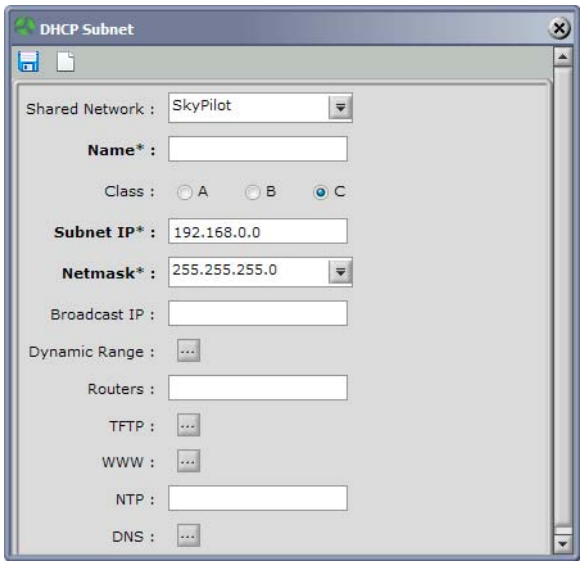
- Globally, through the **DHCP Operations Menu** toolbar button
- Provisioning server, through the **Provisioning** menu
- For devices, by right-clicking a device record and selecting **DHCP**

DHCP Subnet

1 Access the DHCP subnet function; for example, from the SkyPilot EMS menu bar, choose **Provisioning ➤ DHCP ➤ DHCP Subnet**.

SkyPilot EMS displays the Configure DHCP Subnet screen (Figure 4-4).

Figure 4-4. Configure DHCP Subnet screen



2 Edit the DHCP Subnet elements (Table 4-6) as necessary, click the form's **Save** icon, and click **X** (in the top-right corner) to close the form.

Table 4-6. DHCP Subnet Elements

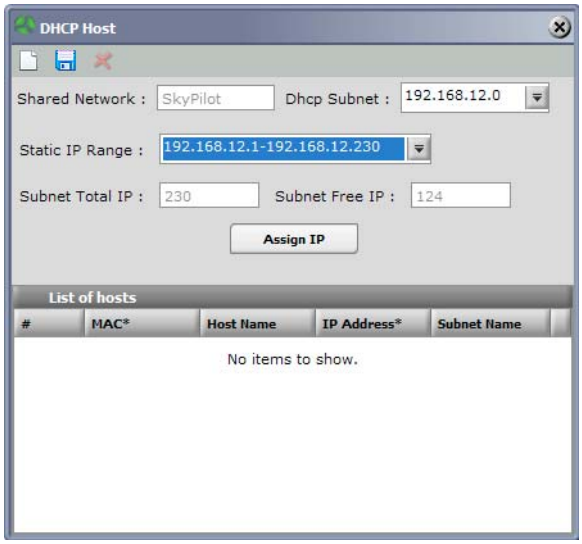
Element	Description
Shared Network	Group of DHCP options that will be provided to devices located in the configured subnet; select from provided list.
Name	Name of the subnet (unique among all such names), as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
Class	Subnet mask class that will be provided to the subnet IP range; select from A, B, or C.
Subnet IP	IP network to use for the subnet; maximum of 12 digits in dotted notation.
Broadcast IP	(Optional) IP address for broadcasting by all the subnet's devices; maximum of 12 digits in dotted notation. This is used by applications that use broadcast IP messages instead of unicast communication.
Dynamic Range	(Optional) Range of IP address for this subnet; selected from provided values.
Routers	(Optional) Default gateway for the subnet to use.
TFTP	(Optional) Firmware provisioning server IP address.
WWW	(Optional) Configuration provisioning server IP address.
NTP	(Optional) Network Time Protocol server IP address.
DNS	(Optional) Domain Name System server for translating names to IP addresses.

DHCP Host

1 Access the DHCP subnet function; for example, from the SkyPilot EMS menu bar, choose **Provisioning ➤ DHCP ➤ DHCP Host**.

SkyPilot EMS displays the Configure DHCP Host screen (Figure 4-4).

Figure 4-5. Configure DHCP Host screen



2 Edit the DHCP Host elements (Table 4-7) as necessary.

Table 4-7. DHCP Host Elements (Page 1 of 2)

Element	Description
Shared Network	Group of DHCP options provided to devices located in the configured subnet; select from provided list.
DHCP Subnet	Subnet (see "DHCP Subnet" on page 96) for this DHCP host to use; select from provided list.
Static IP Range	Subnet in which the host address resides.; select from provided list. As an example, if the subnet is 192.168.0.0, the host address must be 192.168.0.1–192.168.0.254.
Subnet Total IP	Number of IP addresses in the subnet.
Subnet Free IP	Number of unused IP addresses in the subnet. If the value is 0 (zero), there are no addresses available for use as a host.

Table 4-7. DHCP Host Elements (Page 2 of 2)

Element	Description
MAC	MAC address of the host that will use the IP address.
Hostname	Name of the host (unique among all such names) that will use the static IP address, as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
IP Address	Host address; maximum of 12 digits in dotted notation.
Subnet name	Name of the subnet (unique among all such names) in which the **IP Address** resides, as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.

3. (Optional) To assign an available IP address from the subnet to the host, click **Assign IP**. This is particularly useful to help find an unused address, such as when the range has a pool of IP addresses that are dynamically assigned.

4. Click the forms's **Save** icon, and click **X** (in the top-right corner) to close the form.

Using Utilities

SkyPilot devices include a number of built-in utilities to help with your troubleshooting and maintenance tasks, as described in the following list:

- **Ping**—Layer 3 ping utility
- **Node test**—Two-way link layer ping test
- **Reboot**—Device reboot
- **Traceroute**—Path trace from the local node through the mesh network to the SkyGateway

These utilities are available through the similarly named command-line command (as described in the *SkyPilot Command-Line Interface Reference*) or through the Web interface (refer to the *SkyPilot Web Interface Reference*).

Troubleshooting

This section presents procedures for troubleshooting problems of various kinds, including startup and connectivity, with a SkyPilot device. Each procedure is presented in a table set up like this (with varying numbers of steps and substeps).

1	You'll be told to check for something as described in what follows:	
a	Here there will be a description of an action to take to accomplish the check.	Here you'll see paragraphs describing what to do next, depending on the outcome of the action you took. The following open-lock symbol is shown when you've solved the problem:  If advised to contact SkyPilot customer support, you can do so by email (support@skypilot.com) or by telephone at (408) 764-8000.

For additional troubleshooting information, refer to the appropriate device documentation or to the SkyPilot website at www.skypilot.com/support/.

This section makes numerous references to commands that are available through the command-line interface; for details, refer to the *SkyPilot Command-Line Interface Reference*.

The specific troubleshooting procedures are described in the following sections:

- "Power-On Problems" (the next section)
- "Ethernet Connectivity Problems" on page 102
- "IP Connectivity Problems" on page 103
- "SkyGateway Transmission Problems" on page 107
- "Link Failure Problems" on page 109

Power-On Problems

Use the following procedure to troubleshoot the failure of a SkyPilot device to power on. This procedure applies to any SkyPilot device and to either provisioning mode (manual or automatic).

Table 4-8. Power-On Troubleshooting (Page 1 of 2)

1	Check whether the device is getting power:	
a	Verify that the device is plugged into an AC power supply.	If plugged in, go to substep **b**. If not plugged in, plug in and restart.
b	Test your power source with a voltage meter.	If power is available, go to step **2**. If power is not available, try an alternate power source and restart.
2	Check whether the power injector is OK:	
	Check whether the red light on the power injector is lit.	If the red light is lit, go to step **3**. If the red light is not lit, replace the power injector and restart.
3	Check whether the device is properly cabled:	
	Verify that the device is connected to the power injector with a straight-through cable.	If the correct cable is being used, go to step **4**. If the wrong cable is connecting the device, replace it with the correct cable and restart.
4	Check whether the cable is defective:	
	Use a cable tester to check the cable.	If the cable is not defective, go to step **5**. If the cable is defective, replace it and restart.

Table 4-8. Power-On Troubleshooting (Page 2 of 2)

5	Check whether the cable is plugged into the correct port:	
	On a SkyGateway or SkyExtender, confirm that the cable is plugged into the horizontal powered Ethernet interface and not the vertical serial port.	If the cable is plugged into the serial port, attach it to the powered Ethernet interface and restart. If the cable is connected to the correct port on a SkyGateway or SkyExtender, or if the device is a SkyConnector, contact SkyPilot customer support.

Ethernet Connectivity Problems

Use the following procedure to address problems that a SkyPilot device can have in making Ethernet connections. This procedure applies to any SkyPilot device and to either provisioning mode (manual or automatic).

Table 4-9. Ethernet Connectivity (Page 1 of 2)

1	Check whether the SkyPilot device is connected with the proper cables:	
	Verify the use of the following CAT5 twisted-pair cables: • Straight-through cable between power injector and the device • For SkyExtenders and SkyGateways: straight-through cable between power injector and an Ethernet switch or hub • For SkyExtenders and SkyGateways: crossover cable between power injector and computer	If the correct cables are being used, go to step **2**. If an incorrect cable is being used, replace it and restart.
2	Check whether any of the cables are defective:	
	Use a cable tester to check each cable connected to the device.	If none of the cables are defective, go to step **3**. If a cable is defective, replace it and restart.

Table 4-9. Ethernet Connectivity (Page 2 of 2)

3	Check whether Ethernet is enabled on all network devices connected to the SkyPilot device:	
	Confirm that Ethernet is enabled on all equipment connected to the SkyPilot device you're troubleshooting.	If the Ethernet is enabled on all devices, go to step **4**.
4	Check whether all of the connected devices are able to autonegotiate an Ethernet connection:	
a	Confirm that each network device is able to autonegotiate an Ethernet connection.	If all network device settings are correct go to substep **b**. If the settings for any device are incorrect, modify its configuration and restart the device.
b	To check the SkyPilot device, use the `show eth` command to view its current settings.	If the settings for the SkyPilot device are incorrect, use the `set eth` command to modify the Ethernet configuration, and then restart the device. If the device settings are correct and the problem persists, contact SkyPilot customer support.

IP Connectivity Problems

The primary causes of IP connectivity problems with SkyPilot devices are a failure to acquire a GPS signal (in the case of a SkyGateway or SkyExtender), the location of a device on the wrong subnet, and conflicts with VLAN management solutions.

This section addresses device problems related to IP connectivity. It includes the following subsections:

- "Manually Provisioned SkyGateway IP Connectivity Problems" (the next section)
- "Automatically Provisioned SkyGateway IP Connectivity Problems" on page 105
- "SkyExtender and SkyConnector IP Connectivity Problems" on page 106 (applies to both manual and automatic provisioning)

Manually Provisioned SkyGateway IP Connectivity Problems

Use the following procedure to troubleshoot IP connectivity problems with a manually provisioned SkyGateway.

Table 4-10. Manually Provisioned SkyGateway Connectivity

1	Check whether the SkyGateway is able to acquire a GPS signal:	
	Log in to the SkyGateway via the serial port and observe the output at startup to verify the acquisition of a GPS signal. Refer to "Accessing the Command-Line Interface" in the *SkyPilot Command-Line Interface Reference* for instructions on accessing the command-line interface of a SkyPilot device.	If the output confirms that the SkyGateway is receiving a GPS signal, go to step **2**. If the SkyGateway is failing to acquire a signal, move it to an alternate location and restart.
2	Check whether the SkyGateway is on the correct subnet:	
	Use the `show prov` command to verify that the SkyGateway is configured with the desired IP address.	If the command output shows the correct IP address, go to step **3**. If the output shows an incorrect IP address, use the `set ip` command to assign the correct IP address, and then restart the SkyGateway.
3	Check whether VLAN settings are preventing access to the SkyGateway:	
	Use the `show vlan` command to check whether a management VLAN is configured on the SkyGateway.	If the SkyGateway has been incorrectly configured with a management VLAN, modify (or remove) the VLAN with the `set vlan` command and restart.

Automatically Provisioned SkyGateway IP Connectivity Problems

Use this procedure to troubleshoot IP connectivity problems with a SkyGateway that's provisioned automatically from the EMS server.

Table 4-11. Automatically Provisioned SkyGateway Connectivity

1	Check whether the SkyGateway is able to acquire a GPS signal:	
	Log in to the SkyGateway via the serial port and observe the output at startup to verify the acquisition of a GPS signal. Refer to "Accessing the Command-Line Interface" in the *SkyPilot Command-Line Interface Reference* for instructions on accessing the command-line interface of a SkyPilot device.	If the output confirms that the SkyGateway is receiving a GPS signal, go to step **2**. If the SkyGateway is failing to acquire a signal, move it to an alternate location and restart.
2	Check whether VLAN settings are preventing access to the SkyGateway:	
	If a management VLAN is present, it might be preventing local access to the SkyGateway from the network. Use the `show vlan` command to check whether a management VLAN is configured on the SkyGateway.	If the SkyGateway has been incorrectly configured with a management VLAN, modify (or remove) the VLAN with the `set vlan` command and retest. If the VLAN settings are correct and the problem persists, contact SkyPilot customer support.
3	Check whether the SkyGateway is on the correct subnet:	
	Use the `show dhcp` command to verify that the SkyGateway received an IP address from DHCP. (A SkyGateway does not have a default IP address.)	If the command output shows that the SkyGateway did not get an IP address from DHCP or that it received an incorrect IP address, modify the configuration on the DHCP server and retest. If the output shows that the SkyGateway has received an IP address from DHCP, contact SkyPilot customer support.

SkyExtender and SkyConnector IP Connectivity Problems

Use this procedure to troubleshoot IP connectivity problems with a SkyExtender or SkyConnector (applies to both automatically and manually provisioned devices).

Table 4-12. SkyExtender and SkyConnector Connectivity (Page 1 of 2)

1	(SkyExtender only) Check whether the device is able to acquire a GPS signal:	
	Log in to the SkyExtender via the serial port and observe the output at startup to verify the acquisition of a GPS signal. Refer to "Accessing the Command-Line Interface" in the *SkyPilot Command-Line Interface Reference* for instructions on accessing the command-line interface of a SkyPilot device.	If the output confirms that the SkyExtender is receiving a GPS signal, go to step **2**. If the SkyExtender is failing to acquire a signal, move it to an alternate location and retest.
2	Check whether the computer is on the correct subnet:	
	To communicate over the LAN, the computer must be on the same subnet as the SkyPilot device. Both SkyExtenders and SkyConnectors use the IP address 192.168.0.2. Open the network settings panel of the computer to confirm that it's using these settings: • IP address: 192.168.0.2 • Subnet mask: 255.255.255.0	If the computer's network settings are correct, go to step **3**. If the computer's network settings are incorrect, apply the correct settings and retest.

Table 4-12. SkyExtender and SkyConnector Connectivity (Page 2 of 2)

3	Check whether VLAN settings are preventing access to the device:	
a	If a management VLAN is present on the SkyGateway, it will prevent local network access to a SkyExtender or SkyConnector after the device forms a link with the SkyGateway. On the SkyGateway, use the `show vlan` command to check whether a management VLAN is configured for that device.	If the SkyGateway has not been configured with a management VLAN, go to substep **b**. If the SkyGateway has been configured with a management VLAN, modify (or remove) the VLAN with the `set vlan` command and retest.
b	If a data VLAN is present on the SkyExtender or SkyConnector, it will prevent local network access to the device. For a SkyExtender, log in to the device via the serial port; for a SkyConnector, log in via Telnet across the wireless network. Then use the `show vlan` command to check whether a data VLAN has been enabled on the device.	If the command output indicates that a data VLAN is present on the device, use the `set vlan` command to remove the VLAN, and then retest. If the output does not indicate that a data VLAN is present and the problem persists, contact SkyPilot customer support.

SkyGateway Transmission Problems

Use the procedures in this section to troubleshoot SkyGateway devices with wireless transmission problems. There are two subsections, one for each type of provisioning:

- "Manually Provisioned SkyGateway Transmission Problems" (the next section)
- "Automatically Provisioned SkyGateway Transmission Problems" on page 108

Manually Provisioned SkyGateway Transmission Problems

Use this procedure to troubleshoot wireless transmission problems with a manually provisioned SkyGateway (which immediately begins transmitting network signals upon completing startup).

Table 4-13. Manually Provisioned SkyGateway Transmission

•	Check whether the SkyGateway is in manual provisioning mode:	
	Log in to the SkyGateway via the serial port and use the `show prov` command to confirm that the SkyGateway was placed in manual provisioning mode.	If the command output indicates that the device is not in manual provisioning mode, use the `set prov manual` command to set that mode, and then restart the SkyGateway. (After a SkyGateway is placed in manual provisioning mode, restarting it is necessary to activate the mode.) If the SkyGateway is in manual provisioning mode but is unable to transmit signals, contact SkyPilot customer support.

Automatically Provisioned SkyGateway Transmission Problems

Use this procedure to troubleshoot wireless transmission problems with a SkyGateway that's set up for automatic provisioning.

Table 4-14. Automatically Provisioned SkyGateway Transmission (Page 1 of 2)

1	Check whether the SkyGateway is getting its IP settings from DHCP:	
	Log in to the SkyGateway via the serial port and use the `show dhcp` command to confirm that the SkyGateway received the correct IP settings, including IP address, subnet mask, default gateway, HTTP server (SkyControl), and FTP server (SkyControl).	If the command shows that the device received the correct IP settings, go to step **2**. If the device did not receive IP settings from DHCP or has incorrect settings, modify the configuration on the DHCP server and retest.

Table 4-14. Automatically Provisioned SkyGateway Transmission (Page 2 of 2)

2	Check whether the SkyGateway received a configuration file with correct settings:	
	A SkyGateway set up for automatic provisioning receives its configuration from the SkyControl server. Use the `show config` command to confirm that the device received correct configuration information, including the desired frequency and domain. If no settings are present, the SkyGateway did not receive a configuration file. You can also review the contents of the `/var/log/messages` file on the SkyControl server to verify that the SkyGateway is requesting a configuration and, if so, that SkyControl is responding to the request.	If the command output indicates that the SkyGateway is not getting its configuration from SkyControl or that it received incorrect settings, first confirm that the SkyControl server is running. If it is, modify the configuration settings for the SkyGateway and retest. If the output indicates that the SkyGateway is getting the correct configuration settings from the SkyControl server, contact SkyPilot customer support.

Link Failure Problems

This section describes steps for troubleshooting all SkyPilot devices having problems forming links that allow network communications. By branching off to different subsections where applicable, this troubleshooting procedure applies to both manually provisioned devices and devices set up for automatic provisioning through SkyControl.

Failing to Form Links (General)

To troubleshoot problems that any SkyPilot device (whether provisioned manually or automatically) may have in forming links that allow it to connect with other devices on the wireless network, begin with the following steps.

Table 4-15. Link Formation Troubleshooting (General) (Page 1 of 5)

1	Check whether the device is listening on the desired frequency:	
a	Initially, a SkyPilot device scans for frequencies that are on its list of primary frequency or allowed frequencies. Use the `show prov freq` command on the device to verify that the desired frequency is on the list. (You can also use this command on the SkyGateway to check the frequency.)	If the command output indicates that the desired frequency is on the list of primary or allowed frequencies, go to substep **b**. If the desired frequency is not on the list, use the `set freq` command to specify the desired frequency as the device's primary frequency, and then restart.
b	Use the `set log hello 3` and (Telnet only) `debug on` commands to observe frequency hunting in real time. The log will tell you whether the device is switching to the desired frequency. Note that after attempting each allowed frequency twice, the device opens up to all frequencies.	If the log confirms that the device is switching to the desired frequency, go to step **2**. If the log does not show the device switching to the desired frequency, use the `set freq` command to specify the desired frequency as the primary frequency, and then restart.
2	Check whether the device is detecting signals from other devices:	
a	Use the `show link` command to find out whether the device is also receiving hello packets from a SkyGateway or SkyExtenders.	If the command output indicates that the device is not hearing a SkyGateway or any SkyExtenders, go to substep **b**. If the output confirms that the device is hearing a SkyGateway or one or more SkyExtenders, go to step **3**.

Table 4-15. Link Formation Troubleshooting (General) (Page 2 of 5)

b	Use the `set log hello 3` and (Telnet only) `debug on` commands to observe frequency hunting in real time. The log will tell you whether the device is receiving hello packets from other devices when it switches to the desired frequency.	If the log indicates that the device is switching to the desired frequency but failing to receive hello packets, go to substep **c**. If the log confirms that the device is switching to the desired frequency and also receiving hello packets from other devices, go to step **3**.
c	Adjust the device mount for improved signal reception and display the log again as in substep **b**.	If the log indicates that the device is still not receiving hello packets, try additional mounting points. If the device still fails to receive hello packets, go to substep **d**. If the log confirms that the device is now receiving hello packets, secure the mount and restart the device.
d	Move the device to an alternate site with proven coverage (for example, next to a connected device) and display the log again as in substep **b**.	If the log confirms that the device is now receiving hello packets, add an intermediary SkyExtender to improve signal coverage at the device's original location. If the log indicates that output is significantly less than shown by other devices operating at this location, contact SkyPilot customer support.
3	Check whether the device is failing to start optimization:	
a	Use the `show link` command to see if the MAC addresses heard by the device are remaining inactive. Look for evidence of link states that have changed from `inactive` to `non-opt` (non-optimized).	If the command output fails to show inactive links that have changed to the `non-opt` state, go to substep **b**. If the output shows `non-opt` states, the device is starting link optimization. Go to step **4**.
b	Use the `set log link 3` and (Telnet only) `debug on` commands to observe link state changes in real time. Look for link states that change from `inactive` to `non-opt`.	If the log fails to show `inactive` links changing to `non-opt` links, go to substep **c**. If the log shows `inactive` links changing to `non-opt` links, the device is starting link optimization. Go to step **4**.

Table 4-15. Link Formation Troubleshooting (General) (Page 3 of 5)

c	Use the `show link opt` command to view a table displaying average RSSI and the number of hello packets the device is hearing. (The device will not attempt to optimize a link until it hears 5 packets.) An RSSI value of less than 10 on the optimal antenna pair indicates a weak signal. An RSSI value of 20 or greater is preferred.	If the table shows a low RSSI value (less than 10), the signal is probably too weak for the device to attempt optimization. Go to substep **d**. If the table indicates a threshold RSSI value (10 or greater), the signal should be strong enough for the device to attempt optimization. The problem is likely related to local radio interference, which can reduce the number of packets the device can hear. Monitor the area for sources of interference and retest.
d	Adjust the device mount for improved signal reception and display the table again as in substep **c**.	If the table shows RSSI values less than 10, try additional mount adjustments. If the device continues to display RSSI values less than 10, go to substep **e**. If the table shows that RSSI is now 10 or greater, secure the mount and restart the device.
e	Move the device to an alternate site with demonstrated signal coverage (for example, next to a connected device) and display the table again as in substep **c**.	If the table shows RSSI values of 10 or greater, add an intermediary SkyExtender to improve signal coverage at the device's original location. If the table indicates that output is significantly lower than shown by other SkyPilot devices operating at this location, contact SkyPilot customer support.
4	Check whether the device is failing to complete link optimization:	
a	Use the `show link` command to see if the MAC addresses heard by the device have ever reached the `pre-auth` (pre-authorized) state, which indicates optimized links.	If the command output does not show `pre-auth` states, go to substep **b**. If the output shows `pre-auth` states, the device is able to optimize links. Go to step **5**.
b	Use the `set log link 3` and (Telnet only) `debug on` command to observe link state changes in real time. Look for link states that change from `non-opt` to `pre-auth`.	If the log fails to show `non-opt` links changing to `pre-auth` links, go to substep **c**. If the log shows `non-opt` links changing to `pre-auth` links, the device is successfully optimizing links. Go to step **5**.

Table 4-15. Link Formation Troubleshooting (General) (Page 4 of 5)

c	Use the `show link opt` command to view a table displaying average RSSI and the number of hello packets the device is hearing. (The device will not complete optimization of a link until it hears 5 packets.) An RSSI value of less than 10 on the optimal antenna pair indicates a weak signal. An RSSI value of 20 or greater is preferred.	If the table shows a low RSSI value (less than 10), the signal is probably too weak for the device to attempt optimization. Go to substep **d**. If the table indicates a threshold RSSI value (10 or greater), the signal should be strong enough for the device to complete optimization. The problem is likely related to local radio noise that's interfering with SkyPilot signals. (Local radio interference on either side of a link can reduce the number of packets a device can hear, and prevent it from completing optimization.) Monitor the area for sources of interference and retest.
d	Adjust the device mount for improved signal reception and display the table again as in substep **c**.	If the table shows RSSI values remaining below 10, try additional mount adjustments. If the device continues to display RSSI values less than 10, go to substep **e**. If the table shows that RSSI is now 10 or greater, secure the mount and restart the device.
e	Move the device to an alternate site with demonstrated signal coverage (for example, next to a connected device) and display the table again as in substep **c**.	If the table shows RSSI values of 10 or greater, add an intermediary SkyExtender to improve signal coverage at the device's original location. If the table indicates that output is significantly lower than shown by other SkyPilot devices operating at this location, contact SkyPilot customer support.
5	Check whether the device is authenticating links:	
a	Use the `show link` command to see if the MAC addresses heard by the device have ever reached the `standby` state, which indicates authorized links. If authentication failures prevent link states from reaching `standby`, the states will return to `auth-fail` and `inactive`.	If the command output does not show `standby` states, go to substep **b**. If the output shows `standby` states, the device is successfully forming links and is probably looking for alternates. Once the device exhausts attempts to form more links, it will choose an optimal `standby` link as the active path and come online.

Table 4-15. Link Formation Troubleshooting (General) (Page 5 of 5)

b	Use the `set log link 3` and (Telnet only) `debug on` commands to observe link state changes in real time. Look for link states that change from `pre-auth` to `standby`.	If the log fails to show `pre-auth` links changing to `standby` links, go to substep **c**. If the log shows `pre-auth` links changing to `standby` links, the device is successfully forming links and is probably looking for alternates. Once the device exhausts attempts to form more links, it will choose an optimal `standby` link as the active path and come online.
c	Use the `set log auth 3` and (Telnet only) `debug on` commands to observe authentication events in real time. Look for reports of authentication failure due to timeouts or mismatched netkeys.	If the log reports any failure to authenticate due to timeouts or mismatched netkeys, go to substep **d**. If the log reports successful authentication, the problem may be with provisioning. Go to step **6**.
d	Use the `verifykey` command to confirm the presence of a SkyPilot public/private key pair for the device.	If a public/private key pair exists, go to substep **e**. If no keys exists, contact SkyPilot to obtain a public/private key pair.
e	Use the `show netkey` command to confirm that the hashed equivalent of the netkey is identical to the value on all other connected devices. Mismatched keys will cause authentication to fail.	If the netkeys do not match, use the `set netkey` command to modify the public key so that it matches the key used by other devices on the network. Restart the device. If the netkeys match and the device continues to report authentication failures, contact SkyPilot customer support.
6	Continue this procedure with the steps in the next section for manually provisioned devices, or with the steps in "Failing to Form Links (Automatic Provisioning)" on page 116 for automatically provisioned devices.	

Failing to Form Links (Manual Provisioning)

The following steps continue the general procedure in the preceding subsection to address problems that manually provisioned SkyPilot devices may have in forming links that allow it to connect with other devices on the wireless network. Be sure to first perform the steps in that subsection ("Failing to Form Links (General)" on page 110).

Table 4-16. Link Formation Troubleshooting (Manual Prov.) (Page 1 of 2)

7	Check whether the problem is related to a conflict due to configuration:	
a	Use the `show link` command to see if the MAC addresses heard by the device have ever reached the `standby` state. If authentication is successful but link states fail to change from `pre-auth` to `standby`, they will return to `prov-fail` and eventually go back to `inactive`.	If the command output does not show `standby` states, go to substep **b**. If the output shows `standby` states, the device is successfully forming links and is probably looking for alternates. Once the device exhausts attempts to form more links, it will choose an optimal `standby` link as the active path and come online.
b	Use the `set log link 3` and (Telnet only) `debug on` commands to observe link state changes in real time. Look for link states that change from `pre-auth` to `standby`.	If the log fails to show `pre-auth` links changing to `standby` links, go to substep **c**. If the log shows `pre-auth` links changing to `standby` links, the device is successfully forming links and is probably looking for alternates. Once the device exhausts attempts to form more links, it will choose an optimal `standby` link as the active path and come online.

Table 4-16. Link Formation Troubleshooting (Manual Prov.) (Page 2 of 2)

c	If the SkyGateway's configuration parameters do not match the frequency or domain settings of the SkyGateway or SkyExtender it's using to form links, devices will sever the links before connections can be made. Use the `show prov` command to confirm that the SkyGateway's configuration settings for frequency and/or domain match the frequency and/or domain it's trying to use.	If the command output shows mismatched configuration information, modify the configuration to allow the SkyGateway's frequency and/or domain and retest. If the provisioning information matches the SkyGateway's frequency and/or domain and the device is still reporting provisioning failures, contact SkyPilot customer support.

Failing to Form Links (Automatic Provisioning)

The following steps continue the general procedure in the subsection "Failing to Form Links (General)," on page 110, to address problems that an automatically provisioned SkyPilot device may have in forming links that allow it to connect with other devices on the wireless network. Be sure to first perform the steps in the earlier subsection.

Table 4-17. Link Formation Troubleshooting (Automatic Prov.) (Page 1 of 4)

8	Check whether the device is failing to receive a configuration due to problems related to DHCP:	
a	Use the `show link` command to see if the MAC addresses heard by the device have ever reached the `standby` state, which indicates successful provisioning. If authentication is successful but link states fail to change from `pre-auth` to `standby`, they will return to `prov-fail` and eventually go back to `inactive`.	If the command output does not show `standby` states, go to substep **b**. If the output shows `standby` states, the device is successfully forming links and is probably looking for alternates. Once the device exhausts attempts to form more links, it will choose an optimal `standby` link as the active path and come online.

Table 4-17. Link Formation Troubleshooting (Automatic Prov.) (Page 2 of 4)

b	Use the `set log link 3` and (Telnet only) `debug on` commands to observe link state changes in real time. Look for link states that change from `pre-auth` to `standby`.	If the log fails to show `pre-auth` links changing to `standby` links, go to substep **c**. If the log shows `pre-auth` links changing to `standby` links, the device is successfully forming links and is probably looking for alternates. Once the device exhausts attempts to form more links, it will choose an optimal `standby` link as the active path and come online.
c	An incorrect DHCP configuration will prevent the device from obtaining its configuration from the provisioning server. Use the `show dhcp` command to verify that the device is getting an IP address and other configuration information from the DHCP server.	If the command output indicates that the device received an IP address from the DHCP server, go to step **9**. If the command output indicates that the device is not getting an IP address from the DHCP server, or that it's receiving incorrect information from the DHCP server, edit the DHCP content to include the correct information, and restart. If the provisioning information matches the SkyGateway's frequency and/or domain and the device is still reporting provisioning failures, contact SkyPilot customer support.
d	Use the `set log prov 3` and (Telnet only) `debug on` commands to observe provisioning events in real time. Monitor the DHCP server log to confirm that the device successfully made its request, and check the server's response. Note that if you're using the ISC DHCP server, you can monitor server output in real time by monitoring the `/var/log/messages` file.	If the log indicates that the device received an IP address from the DHCP server, go to step **9**. If the log indicates that the device is not getting an IP address and other configuration information from the DHCP server, or that it's receiving incorrect information from the DHCP server, edit the DHCP content to include the correct information, and restart.

Table 4-17. Link Formation Troubleshooting (Automatic Prov.) (Page 3 of 4)

9	Check whether the problem is related to unsuccessful provisioning:	
a	Use the `show link` command to see if the MAC addresses heard by the device have ever reached the `standby` state, which indicates successful provisioning. If authentication is successful but link states fail to change from `pre-auth` to `standby`, they will return to `prov-fail` and eventually go back to `inactive`.	If the command output does not show `standby` states, go to substep **b**. If the output shows `standby` states, the device is successfully forming links and is probably looking for alternates. Once the device exhausts attempts to form more links, it will choose an optimal `standby` link as the active path and come online.
b	Use the `set log link 3` and (Telnet only) `debug on` commands to observe link state changes in real time. Look for link states that change from `pre-auth` to `standby`.	If the log fails to show `pre-auth` links changing to `standby` links, go to substep **c**. If the log shows `pre-auth` links changing to `standby` links, the device is successfully forming links and is probably looking for alternates. Once the device exhausts attempts to form more links, it will choose an optimal `standby` link as the active path and come online.

Table 4-17. Link Formation Troubleshooting (Automatic Prov.) (Page 4 of 4)

c	If the device's configuration parameters do not match the frequency and/or domain settings of the SkyGateway or SkyExtender it's using to form links, devices will sever the links before connections can be made. Use the `show config` command to confirm that the device has completed provisioning, and to view configuration parameters.	If the command output does not show configuration parameters, SkyControl may have no record of the SkyGateway. Go to substep **d**. If the output shows mismatched configuration information, modify the configuration to allow the SkyGateway's frequency or domain, and restart.
d	Use the `set log prov 3` and (Telnet only) `debug on` commands to observe provisioning events in real time. Look for reports of failure to download the device's configuration file, or rejection of a link's domain or frequency based on the contents of the device configuration. Note that you can verify that SkyControl is offering a configuration file by monitoring the `/var/log/messages` file, which contains a log of SkyControl configuration transactions.	If the log reports failures related to the domain and frequency values stored in the device's configuration file, edit the settings to include the correct values, and restart the device. If the log does not report any offering of a configuration file, verify that the device's information has been correctly added into SkyControl, and restart. If you confirm that the provisioning server is sending the correct configuration file to the device but the device continues to report that the file was not offered or that the device continues to sever links, contact SkyPilot customer support.

5

Provisioning With SkyControl

SkyControl provisioning functions enable you to configure provisioning parameters for automatically provisioned devices and to perform administrative functions for your SkyPilot network. This chapter provides detailed instructions for using those provisioning and administrative functions through the SkyPilot EMS Java client.

Appendix Highlights

- Configuring domains
- Configuring access point profiles
- Configuring node profiles
- Configuring nodes
- Configuring VLANs
- Configuring SNMP parameters
- Configuring QoS
- Configuring Web servers

Configuring Domains

A single domain can be defined to encompass your entire SkyPilot network, including all its nodes. Or domains can be used to segregate a network into two or more smaller networks, each of which has the same characteristics as a larger SkyPilot network. For more information about domains, see "Domains" on page 31.

To configure a new domain, choose **Provisioning ➤ Domain**.

Table 5-1 lists the elements that describe domains.

Table 5-1. Domain Elements

Element	Description
Domain Name	Name of the domain (unique among all such names), as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
Domain #	Identification number from 1 to 10000 used by all nodes within a given domain.
Comments	(Optional) Free-form text of up to 255 characters. This is not used by SkyControl; it is for administrator reference only.
Date Created	(Read-only) Date and time this domain record was created.
Date Modified	(Read-only) Date and time this domain record was last modified.

Configuring Access Point Profiles

Access point profiles are used to save settings that define a SkyExtender DualBand/TriBand access point and that can be applied to multiple generic, DualBand, and TriBand node profiles. Access point profiles are composed of the following profiles: access point security, access point Radius (for protected networks), and access point SSID.

For general access point information, see "Access Points" on page 50. For element information, see "Access Point Security Profiles" on page 52.

Access Point Radius Profile Operations

To configure an access point RADIUS profile, choose **Provisioning ➤ Access Point**. ➤ **Radius Profile**.

For element information, see See "Access Point Radius Server Profiles" on page 53.

Access Point SSID Profile Operations

To configure an access point SSID profile, choose **Provisioning ➤ Access Point**. ➤ **SSID Profile**.

For element information, see See "Access Point SSID Profiles" on page 55.

Access Point AP Profile Operations

To configure an access point radius profile, choose **Provisioning ➤ Access Point**. ➤ **AP Profile**.

Table 5-2 lists the elements that describe access point profiles.

Table 5-2. Access Point Profile Elements (Page 1 of 2)

Element	Description
Name	Name of the access point profile (unique among all such names), as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
Software	Name of the software image to store in the node's memory and to use as its active running software; selected from a provided list. If the selected image is different from what is currently stored in the node's backup partition, the node will automatically download the selected image, overwriting what is currently in the backup flash partition.
Access Point Security Profile	Access point security profile to be used by nodes that are assigned this access point profile.
Access Point Radius Profile	(Optional) Access point Radius profile to be used by nodes that are assigned this access point profile.

Table 5-2. Access Point Profile Elements (Page 2 of 2)

Element	Description
Frequency Band	Frequency of antenna attached to this access point; selected from provided list. This setting limits the available **Channel** options.
Dual Antenna Diversity	(Available only if 2.4 is selected for **Frequency Band**) Enables or disables antenna diversity (which allows the access point's radio driver to select the antenna with the best signal reception).
Transmit Power	Access point's transmit power, selected from a provided list.
Low Power Level	Power level for client devices that are not configured as high power devices (see "Access Point High Power MAC Profiles" on page 58); select from provided list.
High Power Level	Power level for client devices that *are* configured as high power devices (see "Access Point High Power MAC Profiles" on page 58); select from provided list.
Comment	(Optional) Free-form text of up to 255 characters. This is not used by SkyControl; it is for administrator reference only.
Date Created	(Read-only) Date and time this access point profile record was created.
Date Modified	(Read-only) Date and time this access point profile record was last modified.

Access Point SkyAccess Profile Operations

To configure an access point SkyAccess profile, choose **Provisioning ➤ Access Point**. ➤ **SkyAccess Profile**.

Table 5-3 lists the elements that describe access point SkyAccess profiles.

Table 5-3. Access Point SkyAccess Profile Elements

Element	Description
Name	Name of the access point SkyAccess profile (unique among all such names), as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
Transmit Power	Access point's transmit power, selected from a provided list.
Beacon interval	Interval (ins seconds) at which the SkyAccess DualBand access point announces itself to the network.
Peer-to-peer	Enable or disable peer-to-peer communications through the access point.
Management from Wireless Clients	Enable or disable management of SkyAccess DualBand access point from a wireless client.
Radius Profile	(Optional) Radius profile to be used by nodes that are assigned this access point profile.
Comment	(Optional) Free-form text of up to 255 characters. This is not used by SkyControl; it is for administrator reference only.
Date Created	(Read-only) Date and time this access point profile record was created.
Date Modified	(Read-only) Date and time this access point profile record was last modified.

Configuring Node Profiles

Node profiles are used to save settings that define a SkyPilot network node and that can be applied to multiple nodes. Using node profiles simplifies the process of configuring nodes and making subsequent changes. For example, you could create a node profile named Orangevale that contains settings common to all SkyConnectors in the Orangevale neighborhood. Then whenever you have a new SkyConnector to configure for someone living in Orangevale, you can simply assign the Orangevale profile to the new SkyConnector network node. And to make the same change to all those SkyConnector nodes, you'd need to make the change only once, to the Orangevale node profile.

When you configure a node profile, you specify the device type to which the profile can be applied: generic or a specific SkyPilot device. A generic node profile enables you to configure all possible node profile elements. Specific node types enable you to configure just those elements that apply to that device.

To configure a node profile, choose **Provisioning ➤ Node Profile**.

Node Profile Elements

Table 5-4 lists the elements that describe node profiles. (The elements apply to all nodes using the given node profile).

Table 5-4. Node Profile Elements (Page 1 of 4)

Element	Description
Name	Name of the node profile (unique among all such names), as a string of up to 128 alphanumeric characters. This name is not used by SkyControl; it is for administrator reference only.
Node Type	(Default = **Generic**) Type of SkyPilot device to which this node profile can be applied; selected from a provided list.
Domain	(Default = **All**) Name of the domain to which the node will belong; selected from a provided list. See "Domains" on page 31.

Table 5-4. Node Profile Elements (Page 2 of 4)

Element	Description
Frequency Region	(Default = **All High Band**) Identification of a range of frequencies, largely based on the geographic region in which the device will operate; selected from a provided list.
Frequency	(Default = **5735**) Primary frequency at which the node will communicate over the network; selected from a provided list.
Frequency Dwell Time	(Default = **1**) Length of time, from 1 to 30 minutes, that the device will search for a signal on the primary frequency; selected from a provided list.
Primary Software	(Default = **images.zip**) Name of the software image to store in the node's memory and to use as its active running software; selected from a provided list. If the selected image is different from what is currently stored in the node's backup partition, the node will automatically download the selected image, overwriting what is currently in the backup flash partition.
Backup Software	(Default = **images.zip**) Name of the software image to store in the node's backup partition; selected from a provided list. For information about when and how nodes update the software in their active partition, see "About Software Images" on page 72.
Traffic Rate Control	(Default = **None**) Traffic rate control profile, if any, to apply to the node. In the absence of a traffic rate control, there will be no restriction on the maximum throughput. For more information about traffic rate controls, see "Quality of Service (QoS)" on page 40.
Primary Backhaul Ping Address	Primary IP address for pinging ICMP to verify backhaul connectivity; maximum of 12 digits in dotted notation.
Secondary Backhaul Ping Address	Secondary IP address for pinging ICMP to verify backhaul connectivity; maximum of 12 digits in dotted notation.
Backhaul Ping Retry Count	(Default = **12**) Number of times to retry the primary ping address before trying the secondary ping address, and number of times to retry the secondary ping address before triggering an alarm.

Table 5-4. Node Profile Elements (Page 3 of 4)

Element	Description
SNMP Alarm Severity	(Default = **Major**) SNMP timeout alarm severity (such as Critical or Major) for network devices.
ICMP Alarm Severity	(Default = **Critical**) ICMP timeout alarm severity (such as Critical or Major) for network devices.
Timezone	(Default = **American Samoa, Midway Islands**) Time zone setting for the node. See "Time Zones" on page 39.
SNMP	(Default = **Read-Write**) Type of community string for the node. See "Configuring SNMP Parameters" on page 143.
Password	(Optional) Password for Telnet session access to the node. Free-form text of up to 32 alphanumeric characters. In the absence of a password, the default password, `public`, will apply.
Telnet Timeout	Number of minutes a Telnet or `ssh` session stays connected without activity, or 0 to never time out
Filter	(Default = **Disable**) Enables or disables the node's filtering. When **Disable** is selected, the corresponding filter-related node profile fields are set to **Allow**. See "Filtering" on page 44.
EtherType Filter	Setting to allow or deny the node's EtherType filtering. When **Allow** is selected, any EtherType filters currently defined will be applied. See "Filtering" on page 44.
IP Protocol Filter	Default setting (applied when there are no explicit filters matched) to allow or deny the node's IP protocol filtering. See "Filtering" on page 44.
IP Address Destination	Default setting (applied when there are no explicit filters matched) to allow or deny the node's IP destination address filtering. See "Filtering" on page 44.
IP Address Source	Default setting (applied when there are no explicit filters matched) to allow or deny the node's IP source address filtering. See "Filtering" on page 44.
Port Destination	Default setting (applied when there are no explicit filters matched) to allow or deny the node's port destination filtering. See "Filtering" on page 44.

Table 5-4. Node Profile Elements (Page 4 of 4)

Element	Description
Port Source	Default setting (applied when there are no explicit filters matched) to allow or deny the node's port source filtering. See "Filtering" on page 44.
ARP Source	Setting to allow or deny the node's ARP (Address Resolution Protocol).
Proxy Proxy ARP	(Default = **Disable**) Enable or disable proxy proxy ARP for this node.
Power Mode	Transmit power level. Available modes are based on where the device will operate.
Radar Detection	Setting for the node's radar transmission detection and subsequent operation. See "Radar Detection" on page 36.
Buzzer Time	(Recent SkyConnectors only; optional) Number of seconds from 0 to 3600 that the buzzer sounds after the device starts up.
Web Server Configuration	Web server profile to apply to this node profile; selected from a provided list. See "Configuring Web Servers" on page 145.
Lease Time	(Optional) Number of minutes from 30 to 259200 that the device's waits before checking for configuration updates. If not set, the device will never check for configuration updates while the link is active.
DHCP IP Assignment	Specify that nodes using this profile receive their IP addresses dynamically or statically. (SkyGateways must use statically assigned IP addresses.)
IP Address Range	(Available only if **Static** is selected for **DHCP IP Assignment**) One or more address ranges to use for nodes assigned to this node profile.
Comments	(Optional) Free-form text of up to 255 characters. This is not used by SkyControl; it is for administrator reference only.
Date Created	(Read-only) Date and time this node profile record was created.
Date Modified	(Read-only) Date and time this node profile record was last modified.

Default Node Profile Elements

Table 5-5 lists the elements that describe default node profiles. (The elements apply to all nodes using the given node profile).

Table 5-5. Default Node Profile Elements (Page 1 of 6)

Element	Description
Name	Name of the node profile (unique among all such names), as a string of up to 128 alphanumeric characters. This name is not used by SkyControl; it is for administrator reference only.
Node Type	(Default = **Generic**) Type of SkyPilot device to which this node profile can be applied; selected from a provided list.
Domain	Name of the domain to which the node will belong; selected from a provided list. See "Domains" on page 31.
Frequency Region	Identification of a range of frequencies, largely based on the geographic region in which the device will operate; selected from a provided list.
Frequency	Primary frequency at which the node will communicate over the network; selected from a provided list.
Frequency Dwell Time	Length of time, from 1 to 30 minutes, that the device will search for a signal on the primary frequency; selected from a provided list.
Primary Software	Name of the software image to store in the node's memory and to use as its active running software; selected from a provided list. If the selected image is different from what is currently stored in the node's backup partition, the node will automatically download the selected image, overwriting what is currently in the backup flash partition.
Backup Software	Name of the software image to store in the node's backup partition; selected from a provided list. For information about when and how nodes update the software in their active partition, see "About Software Images" on page 72.

Table 5-5. Default Node Profile Elements (Page 2 of 6)

Element	Description
Access Point 2.4 GHz	(Available only for DualBand devices) Access point profile containing settings to apply to this node's 2.4 GHz access point; selected from a provided list. For detailed information about using access point profiles, see "Configuring Access Point Profiles" on page 122.
Access Point 4.9 GHz	(Available only for TriBand devices) Access point profile containing settings to apply to this node's 4.9 GHz access point; selected from a provided list. For detailed information about using access point profiles, see "Configuring Access Point Profiles" on page 122.
Access Point SkyAccess profile	(Available only if a device with a built-in access point is selected as the **Node Type**: any SkyAccess, DualBand, or TriBand device) Access point configuration profile.
Status	Enable or disable the built-in access point on SkyAccess, DualBand, or TriBand devices.
Traffic Rate Control	Traffic rate control profile, if any, to apply to the node. In the absence of a traffic rate control, there will be no restriction on the maximum throughput. For more information about traffic rate controls, see "Quality of Service (QoS)" on page 40.
SNMP Alarm Severity	(Default = **Major**) SNMP timeout alarm severity (such as Critical or Major) for network devices.
ICMP Alarm Severity	(Default = **Critical**) ICMP timeout alarm severity (such as Critical or Major) for network devices.
SNMP	(Default = **Read-Write**) Type of community string for the node. See "Configuring SNMP Parameters" on page 143.
Password	(Optional) Password for Telnet session access to the node. Free-form text of up to 32 alphanumeric characters. In the absence of a password, the default password, `public`, will apply.
Telnet Timeout	Number of minutes a Telnet or `ssh` session stays connected without activity, or 0 to never time out

Table 5-5. Default Node Profile Elements (Page 3 of 6)

Element	Description
Primary Backhaul Ping Address	Primary IP address for pinging ICMP to verify backhaul connectivity; maximum of 12 digits in dotted notation.
Secondary Backhaul Ping Address	Secondary IP address for pinging ICMP to verify backhaul connectivity; maximum of 12 digits in dotted notation.
Backhaul Ping Retry Count	(Default = **12**) Number of times to retry the primary ping address before trying the secondary ping address, and number of times to retry the secondary ping address before triggering an alarm.
SNMP Alarm Severity	(Default = **Major**) SNMP timeout alarm severity (such as Critical or Major) for network devices.
Power Mode	Transmit power level. Available modes are based on where the device will operate.
Radar Detection	Setting for the node's radar transmission detection and subsequent operation. See "Radar Detection" on page 36.
Preferred Parent MAC Address	The upstream node that a device using this profile will use to connect to the mesh network. If this is not specified, a node scans for available parents and chooses the best parent based on a wireless statistics such as signal strength. To configure a child node to always connect to a specific parent node (a Gateway or Extender), set the Preferred Parent MAC address accordingly.
Customer	Customer maintenance profile to associate with the node. Customer maintenance profiles provide information about the customer (such as name and address) who is responsible for the node.
Channel Width 2.4 GHz	(Default = **All**) Channel width to use on the 2.4 GHz spectrum.
Channel 2.4 GHz	Channel on which to communicate on the 2.4 GHz spectrum.
Radio Policy 2.4 GHz	Type of 802.11 specification to use when communicating with client devices on the 2.4 GHz spectrum.

Table 5-5. Default Node Profile Elements (Page 4 of 6)

Element	Description
Channel Width 4.9 GHz	(Default = **All**) Channel width to use on the 4.9 GHz spectrum.
Channel 4.9 GHz	Channel on which to communicate on the 4.9 GHz spectrum.
Radio Policy 4.9 GHz	Type of 802.11 specification to use when communicating with client devices on the 4.9 GHz spectrum.
Timezone	(Default = **American Samoa, Midway Islands**) Time zone setting for the node access point client. See "Time Zones" on page 39.
Filter	(Default = **Disable**) Enables or disables the node's filtering. When **Disable** is selected, the corresponding filter-related node profile fields are set to **Allow**. See "Filtering" on page 44.
EtherType Filter	Setting to allow or deny the node's EtherType filtering. When **Allow** is selected, any EtherType filters currently defined will be applied. See "Filtering" on page 44.
IP Protocol Filter	Default setting (applied when there are no explicit filters matched) to allow or deny the node's IP protocol filtering. See "Filtering" on page 44.
IP Address Destination	Default setting (applied when there are no explicit filters matched) to allow or deny the node's IP destination address filtering. See "Filtering" on page 44.
IP Address Source	Default setting (applied when there are no explicit filters matched) to allow or deny the node's IP source address filtering. See "Filtering" on page 44.
Port Destination	Default setting (applied when there are no explicit filters matched) to allow or deny the node's port destination filtering. See "Filtering" on page 44.
Port Source	Default setting (applied when there are no explicit filters matched) to allow or deny the node's port source filtering. See "Filtering" on page 44.
ARP Source	Setting to allow or deny the node's ARP (Address Resolution Protocol).

Table 5-5. Default Node Profile Elements (Page 5 of 6)

Element	Description
Buzzer Time	(Recent SkyConnectors only; optional) Number of seconds from 0 to 3600 that the buzzer sounds after the device starts up.
Web Server Configuration	Web server profile to apply to this node profile; selected from a provided list. See "Configuring Web Servers" on page 145.
Lease Time	(Optional) Number of minutes from 30 to 259200 that the device's waits before checking for configuration updates. If not set, the device will never check for configuration updates while the link is active.
Address 1	(Optional) Address information (such as street address) specifying where the node is physically located (for example, a user's home address where a SkyConnector outdoor device is mounted); free-form text of up to 255 alphanumeric characters.
Address 2	(Optional) Additional address information indicating where the device is physically located; free-form text of up to 255 alphanumeric characters.
City	(Optional) City where the device is physically located; free-form text of up to 128 alphanumeric characters.
State/Province	(Optional) State or province where the device is physically located; free-form text of up to 64 alphanumeric characters.
Postal Code	(Optional) Postal code of where the device is physically located; up to 10 digits.
Country	(Optional) Country where the device is physically located; selected from provided list.
Ethernet State	Enable or disable the node's Ethernet port.
Ethernet Auto Negotiation	Enable or disable autonegotiation, whereby the Ethernet port's speed and duplex is automatically defined.
Ethernet Speed (bT)	Speed of the Ethernet connection.
Ethernet Duplexity	Ethernet connection's duplex setting: full or half.

Table 5-5. Default Node Profile Elements (Page 6 of 6)

Element	Description
Comments	(Optional) Free-form text of up to 255 characters. This is not used by SkyControl; it is for administrator reference only.
Date Created	(Read-only) Date and time this node profile record was created.
Date Modified	(Read-only) Date and time this node profile record was last modified.

Node Profile Attribute Elements

Table 5-6 lists the elements that describe node profile attributes. These elements enable you to associate a variety of preconfigured options, such as QoS classifiers, with existing node profiles.

Table 5-6. Node Profile Attribute Elements

Element	Refer to
ACL	"Configuring QoS" on page 145
Classifier	"Quality of Service (QoS)" on page 40
Filters	"Filtering" on page 44
Frequency	"Frequency" on page 31
SNMP	"Configuring SNMP Parameters" on page 143
VLAN	"Configuring VLANs" on page 140

Configuring Nodes

A SkyPilot network *node* is any SkyPilot device on the mesh network—SkyGateways, SkyExtenders, and SkyConnectors (both indoor and outdoor).

To configure a new node, choose **Provisioning ➤ Node Maintenance**, and click the **New** toolbar button.

To modify an existing node's attributes, choose **Provisioning ➤ Node Maintenance**, right-click the desired node's row, and click **Attributes**. (Attributes apply only to nodes, not other SkyControl entities.)

Table 5-7 lists the elements that describe node records.

Table 5-7. Node Elements (Page 1 of 4)

Element	Description
MAC Address	Unique 12-character hexadecimal hardware address for this node.
Node Type	(Default = **SkyConnector Indoor**) Type of SkyPilot device that constitutes this node; selected from a provided list.
Node Profile	Node profile containing settings to apply to this node; selected from a provided list. (From the EMS Java client, you can click **Detail** to view the configuration settings for the selected node profile). For detailed information about using node profiles, see "Configuring Node Profiles" on page 126.
DHCP IP Assignment	Specify that nodes using this profile receive their IP addresses dynamically or statically.
IP Address	(Optional except for SkyGateways) IP address (including mask settings) that enables SkyControl to poll the node; up to 12 digits in dotted notation. In the absence of a setting for this element, SkyControl will poll the SkyGateways, which maintain records of every connected device's IP address. For more information about SkyControl polling, see "Node Device Views" on page 13.
Host Name	(Optional) Unique free-form text of up to 32 alphanumeric characters. This is not used by SkyControl; it is for administrator reference only.

Table 5-7. Node Elements (Page 2 of 4)

Element	Description
Frequency Region	(Default = **All High Band**) Identification of a range of frequencies, largely based on the geographic region in which the device will operate; selected from a provided list.
Frequency	(Default = **5735**) Primary frequency at which the node will communicate over the network; selected from a provided list.
Frequency Dwell Time	Length of time, from 1 to 30 minutes, that the device will search for a signal on the primary frequency; selected from a provided list.
Preferred Parent MAC Address	(Non-SkyGateway only) MAC address of a SkyGateway, SkyExtender, DualBand, or TriBand to use as the parent, even if it doesn't provide the best path.
Access Point 2.4 GHz	(Available only for DualBand devices) Access point profile containing settings to apply to this node's 2.4 GHz access point; selected from a provided list. For detailed information about using access point profiles, see "Configuring Access Point Profiles" on page 122.
Access Point 4.9 GHz	(Available only for TriBand devices) Access point profile containing settings to apply to this node's 4.9 GHz access point; selected from a provided list. For detailed information about using access point profiles, see "Configuring Access Point Profiles" on page 122.
Access Point SkyAccess profile	(Available only if a device with a built-in access point is selected as the **Node Type**: any SkyAccess, DualBand, or TriBand device) Access point configuration profile.
Antenna Sectors	Enable or disable any of the Gateway or Extender antennas.
Customer	(Optional) Customer associated with the device; selected from a provided list. (From the EMS Java client, you can click **Detail** to view the complete customer record for the selected customer.) For detailed information about using customer profiles, see "Configuring SNMP Parameters" on page 143.
Country	(Optional) Country where the device is physically located; selected from a provided list.

Table 5-7. Node Elements (Page 3 of 4)

Element	Description
Channel Width 2.4 GHz	(Default = **All**) Channel width to use on the 2.4 GHz spectrum.
Channel 2.4 GHz	Channel on which to communicate on the 2.4 GHz spectrum.
Radio Policy 2.4 GHz	Type of 802.11 specification to use when communicating with client devices on the 2.4 GHz spectrum.
Channel Width 4.9 GHz	(Default = **All**) Channel width to use on the 4.9 GHz spectrum.
Channel 4.9 GHz	Channel on which to communicate on the 4.9 GHz spectrum.
Radio Policy 4.9 GHz	Type of 802.11 specification to use when communicating with client devices on the 4.9 GHz spectrum.
GPS Timing	Enable or disable use of GPS timing of data transmission among the device's antennas; select from provided list. If a SkyGateway receives a GPS signal, downstream nodes derive their timing from the SkyGateway; otherwise downstream nodes use derived time.
GPS Coordinates	Enable or disable manual entry of the device's location. Enable only if there is no GPS available.
Latitude	(Available only if Enable is selected for **GPS Coordinates**) Node's latitude.
Longitude	(Available only if Enable is selected for **GPS Coordinates**) Node's longitude.
Altitude	(Available only if Enable is selected for **GPS Coordinates**) Node's altitude.
Ethernet State	Enable or disable the node's Ethernet port.
Ethernet Auto Negotiation	Enable or disable autonegotiation, whereby the Ethernet port's speed and duplex is automatically defined.
Ethernet Speed (bT)	Speed of the Ethernet connection.

Table 5-7. Node Elements (Page 4 of 4)

Element	Description
Ethernet Duplexity	Ethernet connection's duplex setting: full or half.
Address 1	(Optional) Address information (such as street address) specifying where the node is physically located (for example, a user's home address where a SkyConnector outdoor device is mounted); free-form text of up to 255 alphanumeric characters.
Address 2	(Optional) Additional address information indicating where the device is physically located; free-form text of up to 255 alphanumeric characters.
City	(Optional) City where the device is physically located; free-form text of up to 128 alphanumeric characters.
State/Province	(Optional) State or province where the device is physically located; free-form text of up to 64 alphanumeric characters.
Postal Code	(Optional) Postal code of where the device is physically located; up to 10 digits.
Comment	(Optional) Free-form text of up to 255 characters. This is not used by SkyControl; it is for administrator reference only.
Date Created	(EMS Java client only; read-only) Date and time this node record was created.
Date Modified	(EMS Java client only; read-only) Date and time this node record was last modified.

Configuring VLANs

Virtual local area networks (VLANs) are portions of a network that are configured as logical topologies defined by software, connected to the same physical network infrastructure. Devices on separate VLANs of a network behave as if they are on physically separated networks. VLANs function by logically segmenting the network into different broadcast domains so that packets are switched only between ports that are designated for the same VLAN. For more information, see "Virtual Local Area Networks (VLANs)" on page 32.

To configure a new VLAN, choose **Provisioning ➤ VLAN**, and click the **New** toolbar button.

Table 5-8 lists the elements that describe VLANs.

Table 5-8. VLAN Elements

Element	Description
Name	Name of the VLAN (unique among all such names), as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
VLAN Tag	Number from 1 to 4096 used as the VLAN tag for all nodes within the given VLAN.
Comment	(Optional) Free-form text of up to 255 characters. This is not used by SkyControl; it is for administrator reference only.
Date Created	(Read-only) Date and time this VLAN record was created.
Date Modified	(Read-only) Date and time this VLAN record was last modified.

Configuring Proxy Proxy ARPs

Proxy Proxy ARP is a routing technique that uses the ARP (Address Resolution Protocol) as an ad hoc mechanism. A multi-port networking device (such as a router) that implements this protocol can respond to ARP requests on an interface, allowing the device to receive and forward packets addressed to the other devices.

To configure a new proxy proxy ARP, choose **Provisioning ➤ [Proxy Proxy ARP Setting | Proxy Proxy ARP Exclusion]**, and click the **New** toolbar button.

Proxy Proxy ARP Setting Elements

Table 5-9 lists the elements that describe Proxy Proxy ARP Settings.

Table 5-9. Proxy Proxy ARP Elements

Element	Description
Name	Name of the Proxy Proxy ARP (unique among all such names), as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
VLAN Name	Name of the VLAN (unique among all such names), as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
Router IP Address	IP address of the router that will forward addresses.
Subnet Mask	Used in conjunction with the network address to determine which part of the address is the network address and which part is the host address.
Comment	(Optional) Free-form text of up to 255 characters. This is not used by SkyControl; it is for administrator reference only.

Proxy Proxy ARP Exclusion Elements

Table 5-10 lists the elements that describe Proxy Proxy ARP Exclusion settings.

Table 5-10. Proxy Proxy ARP Exclusion Elements

Element	Description
#	Sequence number for Proxy Proxy ARP profile; auto-generated by EMS.
Name	Name of the Proxy Proxy ARP Exclusion (unique among all such names), as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
Proxy Proxy ARP Setting	Name of the Proxy Proxy ARP (unique among all such names), as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
IP Address	IP address of the router that will forward addresses.
Subnet Mask	Used in conjunction with the network address to determine which part of the address is the network address and which part is the host address.
Comment	(Optional) Free-form text of up to 255 characters. This is not used by SkyControl; it is for administrator reference only.
Date Created	(Read-only) Date and time this ARP exclusion record was created.
Date Modified	(Read-only) Date and time this ARP exclusion record was last modified.

Configuring SNMP Parameters

To enable SNMP trap alarms and SkyControl monitoring of devices, you must first configure corresponding SNMP parameters—SNMP community strings and SNMP trap receivers.

Related topics include:

- For general information about SNMP, "SNMP" on page 38
- For general information about SkyControl, "Monitoring a Network's Topology with SkyControl" on page 84
- For information about customizing SNMP trap descriptions, messages, and associated alarm severity, "Monitoring Events and Alarms" on page 85.

SNMP Community String Elements

Table 5-11 lists the elements that describe SNMP community strings.

Table 5-11. SNMP Community String Elements (Page 1 of 2)

Element	Description
Name	Name of the SNMP community string (unique among all such names), as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
Community String	Identifier that allows access through an SNMP agent to a device's MIB objects. Free-form text of up to 128 alphanumeric characters.
Type	(Default = **Read-Only**) Specifies type of access allowed by this community string: • **Read-Only**—MIB object can be read but not modified. • **Read-Write**—MIB object can be read and modified. • **Trap**—Community string used to authenticate and process received traps.

Table 5-11. SNMP Community String Elements (Page 2 of 2)

Element	Description
Comment	(Optional) Free-form text of up to 255 characters. This is not used by SkyControl; it is for administrator reference only.
Date Created	(Read-only) Date and time this community string record was created.
Date Modified	(Read-only) Date and time this community string record was last modified.

SNMP Trap Receiver Elements

Table 5-12 lists the elements that describe SNMP trap receivers.

Table 5-12. SNMP Trap Receiver Elements

Element	Description
Name	Name of the SNMP trap receiver (unique among all such names), as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
IP Address	IP address to which any node using this trap receiver will send SNMP traps; up to 12 digits in dotted notation. The combination of IP address and port (below) must be unique (to SNMP trap receivers).
Port	(Default = **162**) Port to which any node using this trap receiver will send SNMP traps; number from 1 to 65535. The combination of IP address and port must be unique (to SNMP trap receivers).
Comment	(Optional) Free-form text of up to 255 characters. This is not used by SkyControl; it is for administrator reference only.
Date Created	(Read-only) Date and time this trap receiver record was created.
Date Modified	(Read-only) Date and time this trap receiver record was last modified.

Configuring QoS

QoS classifiers (which classify traffic according to the types of packets that will be directed to a subscriber's high-priority queue) and traffic filters (which control user data packet transfer through a SkyPilot network) contribute to maintaining high QoS. (For more information, see "Quality of Service (QoS)" on page 40.)

To configure a new QoS classifier, choose **Provisioning ➤ [Classifier | Traffic Rate Control]**, and click the **New** toolbar button.

Configuring Web Servers

SkyControl allows you to configure the Web server settings on your SkyPilot devices.

To configure a new ACL, choose **Provisioning ➤ Web Server Configuration**, and click the **New** toolbar button.

Table 5-13 lists the elements that describe Web servers.

Table 5-13. Web Server Elements (Page 1 of 2)

Element	Description
Name	Name of the Web server (unique among all such names), as a string of up to 64 alphanumeric characters. This name is used only within SkyControl.
Status	Enables or disables access to the Web server on the SkyPilot device.
Customer Access	Enables or disables view-only (non-administrator) access to the device's Web interface.
Administrator Password	Password for logging in to the Web server.

Table 5-13. Web Server Elements (Page 2 of 2)

Element	Description
Comments	(Optional) Free-form text of up to 255 characters. This is not used by SkyControl; it is for administrator reference only.
Date Created	(Read-only) Date and time this Web server record was created.
Date Modified	(Read-only) Date and time this Web server record was last modified.

A

Google Earth Management System (GEMS) Reference

SkyPilot EMS is fully integrated with Google Earth Management System (GEMS), enabling you to view your SkyPilot Network in Google Earth. With Google Earth, you can visualize that physical layout of your networks and plan future expansion on the basis of real world representations. This appendix provides instructions for using GEMS to define profiles for viewing your network in Google Earth.

Appendix Highlights

- Starting Google Earth Management System
- Downloading icons
- Changing views and creating profiles
- Submitting profiles to Google Earth

Starting Google Earth Management System

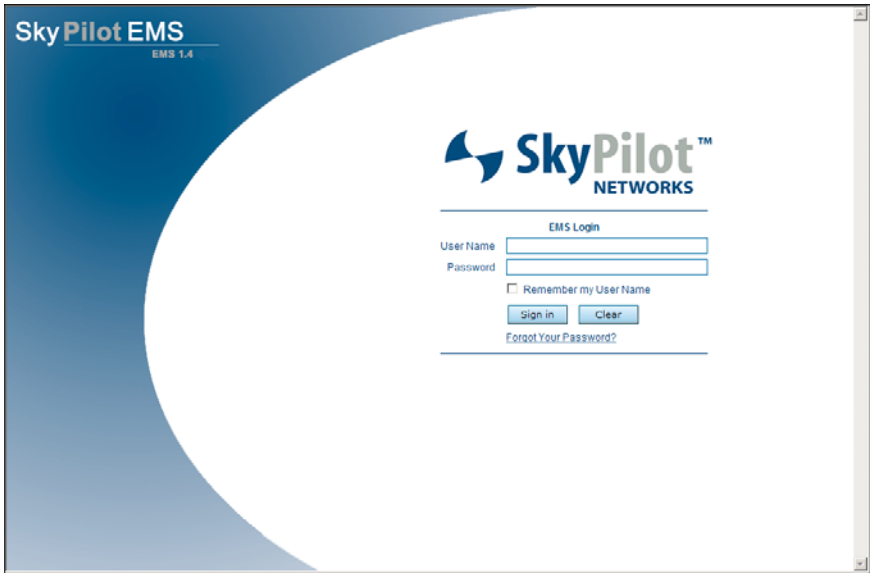
The Google Earth Management System (GEMS) component is automatically included as part of your SkyPilot EMS server software installation.

To start GEMS:

1. Open a Web browser and enter the URL for the SkyPilot EMS server login page: the server's IP address or host name, preceded by `http://` (for example, `http://192.168.1.228`).

   The Web client displays a login screen.

   Figure A-1. EMS Web client login screen



2. Enter the user name and password. Both the default user name and the default password are `admin`.

3. Click **Sign in**.

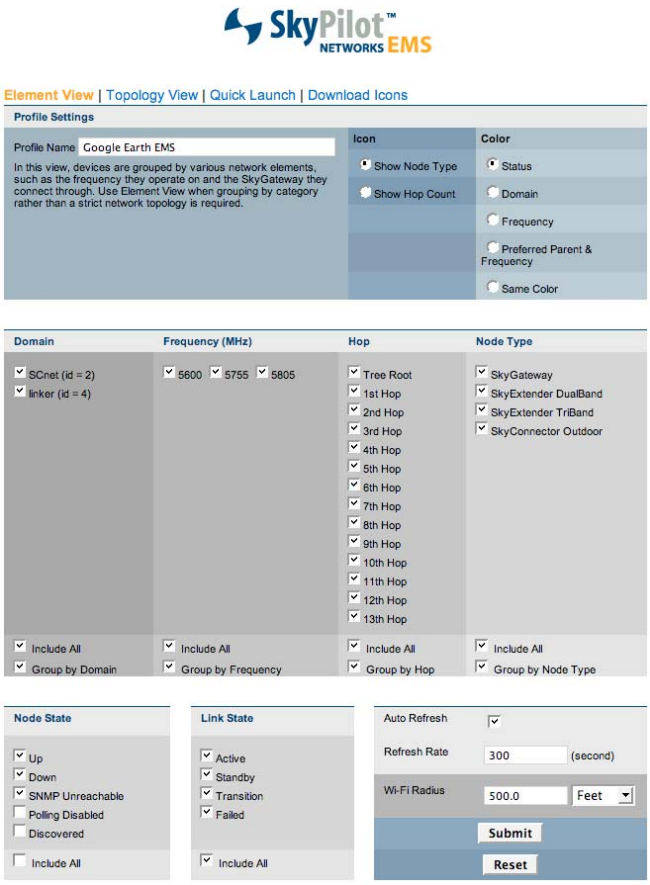
   The Web client displays your SkyPilot network topology, in the Mesh Backhaul Tree View.

4. On the **Tools** menu, click **GEMS Launchpad.**

   A new browser tab opens displaying **the GEMS Element View** (Figure A-2), where you specify how nodes and node information is displayed in Google Earth.

Just below the logo (and above the Profile Settings section), the command banner provides links to build profiles (**Element View** and **Topology View**), perform a **Quick Launch**, and **Download Icons** for network nodes displayed in Google Earth.

Figure A-2. GEMS: Element View



Downloading and Installing Icons

SkyPilot provides GEMS custom node icons for use with Google Earth. If you want to use the icons tor represent network nodes, you must download the icons.

To download the GEMS icons:

- Click **Download Icons** in the banner menu.

  The Web client displays a login screen.

If the icons are not currently installed on your computer, SkyPIlot EMS will display a reminder in the message area of GEMS asking you to install the icon package:

- If you are using a Windows computer as the EMS client, you will download an installer the walks you through the installation process.
- If the SkyPilot EMS client is running on a computer OS other than Windows, click **Non-Windows** to download a package of icons with a Readme file containing instructions for installing the icons on your computer.

To install the GEMS icon package on a Windows-based client:

1. In the Operating System column, click **Microsoft Windows**.

   A prompt appears, providing options for downloading the installer, `gems_icons.exe`.

2. Choose a destination and click **Save**.

3. Run **gems_icons.exe** (double-click it).

   The Installer starts and asks you to select which components to install.

4. Select S**kyPilot EMS 1.5 Google Earth Icons** and click **Install**.

   The installer copies the SkyPilot icons to a location where they will be available to Google Earth.

5. Click **Close**.

Creating and Viewing Network Profiles

You view SkyPilot networks in Google Earth by defining a profile and opening it in Google Earth as a "place: that you can browse and save for later viewing".

When you submit a profile, GEMS creates a KML (keyhole markup language) file which Google Earth uses to map network node information to the physical world.

Google Earth adds the network profile to your `Temporary Places` folder as the subfolder with the same name as the profile.

When you click the entry, Google Earth *flies* to the physical location of the network and zooms in to show the nodes you specified in the profile.

IMPORTANT Newly created profiles appear as items in the Temporary Places folder. If you do not move these items to the My Places folder to save them, they will be lost when you quit Google Earth.

You can create profiles for both ways that you can view your network:

- **Element view**—Devices are shown based on their device type (hardware, frequency, and so on). In this view, all links related to the nodes are shown, regardless of their state: active, standby, or transition.
- **Topology view**—Only devices with active links are shown, enabling an at-a-glance understanding of the network hierarchy; that is, what path does a device take in order to connect to the gateway?

Element View Profile

This section describes how to create an Element View profile and how to view the Element View display.

Creating a Profile

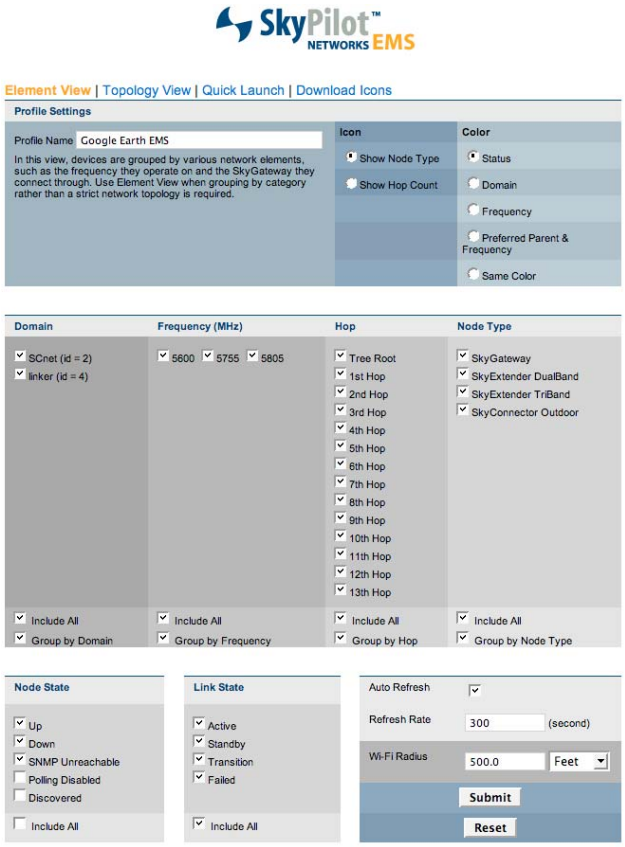
Element view prepares a Google Earth view of your network based on your SkyPilot network elements, including type of node, node state, link state, device frequency, and number of hops.

To create a Google Earth Element View profile:

1 On the command banner, click **Element View**.

SkyPIlot EMS displays the Profile Settings Element View screen (Figure A-3). The domain, frequency, hops, node type, node state, and link state settings' choices are populated based on what is available in SkyControl. For example, if the network has only two hops, the available selections are Tree Root, 1st Hop, and 2nd Hop.

Figure A-3. Profile Settings Element View screen



2 Select the information to display (Table A-1 lists the elements that describe Google Earth profile settings) and click **Submit**.

Google Earth creates the KML files., and Microsoft® Windows® asks how you want to open the file.

Table A-1. Google Earth Element View Profile Settings (Page 1 of 2)

Element	Description
Profile Name	Name of the element view profile (unique among all such names), as a string of alphanumeric characters.
Icons Show	Type of icons to display in Google Earth (such as **Node Type Info** or **Hop Count**).
Icon Colors Indicate	Information conveyed by the icon colors; for example, connection status colors use green for connected, red for down, and so on.
Domain	Enables or disables display of nodes in specific active SkyPilot network domains. The domains are placed in alphabetical order. Select the **Include All** checkbox to select all domains. Select the **Group by Domain** checkbox to group the nodes according to the domain in which they are located.
Frequency (MHz)	Enables or disables display of nodes operating at specific frequencies in current use in your SkyPIlot network. The frequencies are placed in alphanumeric order. Select the **Include All** checkbox to select all frequencies. Select the **Group by Domain** checkbox to group the nodes according to their frequencies.
Hop	Enables or disables display of nodes that are specific numbers of hop values away from the network gateway. Select the **Include All** checkbox to select all frequencies. Select the **Group by Hop** checkbox to group the nodes according to their hop values.

Table A-1. Google Earth Element View Profile Settings (Page 2 of 2)

Element	Description
Node Type	Enables or disables display of specific node types. The nodes are ordered in the standard hierarchy (Gateway, Extender, Connector, and so on) from the root (Gateway) to the end (Connector). Select the **Include All** checkbox to select all node types. Select the **Group by Node Type** checkbox to group the nodes according to their frequencies.
Node State	Enables or disables display of nodes in specific node states. Select the **Include All** checkbox to select all node states.
Link State	Enables or disables display of nodes in specific link states. Select the **Include All** checkbox to select all link states.
Auto Refresh	Enables or disables automatic refresh of the Google Earth display. (You can control the refresh interval by setting the **Refresh Rate** value, described below.)
Refresh Rate	(Default = **300** (5 minutes)) Number of seconds between refreshes of the Google Earth display.
Wi-Fi Radius	(SkyExtender DualBand and SkyExtender TriBand nodes only) Value used by Google Earth to draw a circle to represent the estimated Wi-Fi coverage. Enter a number, and select **Feet** or **Meters** from the provided list.

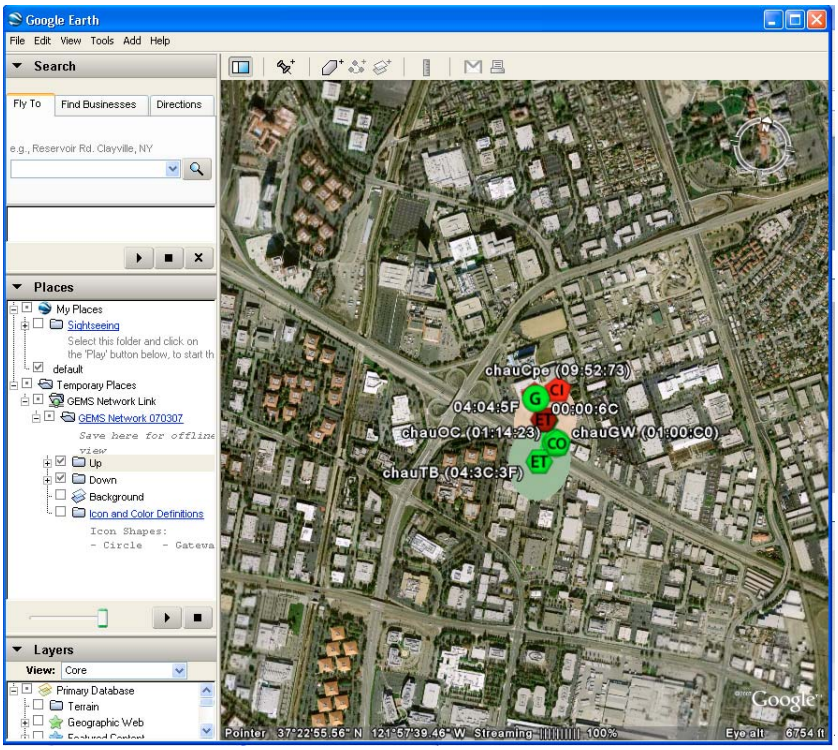
3 (Optional) To enable automatically opening Google Earth the next time you click Submit, click **Do This Automatically for Files Like This From Now On**.

Viewing the Google Earth Element View

After setting your parameters for an Element profile, click **Submit** to open the profile in Google Earth.

Isolate the view of your network place by clicking the GEMS Network folder. Filter elements and nodes by clicking items in the subfolders.

Figure A-4. Sample SkyPilot network place (Element view)



Topology View Profile

This section describes how to create a Topology View profile and how to view the Topology View display.

Creating a Profile

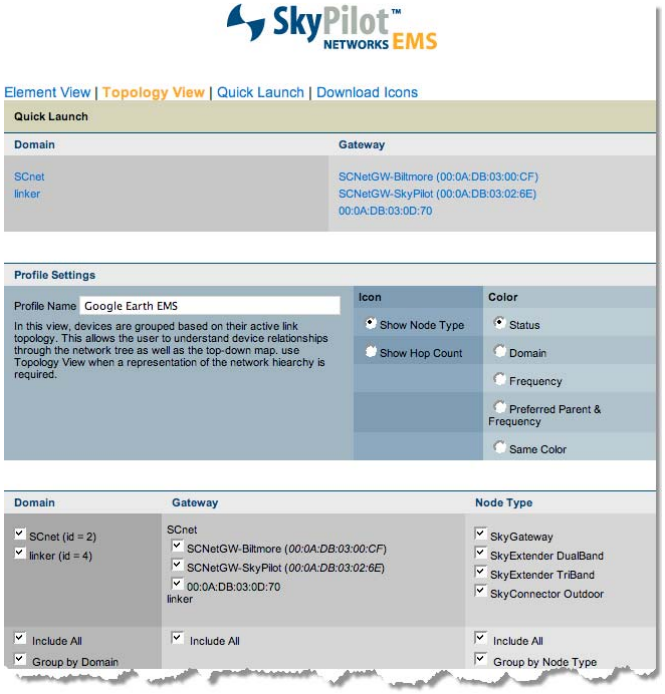
Use the Topology view to prepare a Google Earth view of your network that groups devices on the basis of their active link topology. A topology view helps you understand the relationships between the devices and is useful for viewing the network hierarchy.

To create a Google Earth Topology View profile:

1 On the command banner, click **Topology View**.

SkyPIlot EMS displays the Profile Settings Topology View screen (Figure A-5). The domain, frequency, hops, node type, node state, and link state settings' choices are populated based on what is available in SkyControl. For example, if the network has only two hops, the available selections are Tree Root, 1st Hop, and 2nd Hop.

Figure A-5. Profile Settings Topology View screen



2 Select the information to display (Table A-2 lists the elements that describe Google Earth profile settings) and click **Submit**.

Google Earth creates the KML files., and Microsoft® Windows® asks how you want to open the file.

Table A-2. Google Earth Topology View Profile Settings

Element	Description
Profile Name	Name of the element view profile (unique among all such names), as a string of alphanumeric characters.
Icons Show	Type of icons to display in Google Earth: **Node Type** or **Hop Count**.
Icon Colors Indicate	Information conveyed by the icon colors; for example, connection status colors use green for connected, red for down, and so on.
Domain	Enables or disables display of nodes in specific active SkyPilot network domains. The domains are placed in alphabetical order. Select the **Include All** checkbox to select all domains. Select the **Group by Domain** checkbox to group the nodes according to the domain in which they are located.
Gateway	Enables or disables display of specific SkyGateway devices. Select the **Include All** checkbox to select all SkyGateway devices.
Node Type	Enables or disables display of specific node types. The nodes are ordered in the standard hierarchy (Gateway, Extender, Connector, and so on) from the root (Gateway) to the end (Connector). Select the **Include All** checkbox to select all node types. Select the **Group by Node Type** checkbox to group the nodes according to their frequencies.
Node State	Enables or disables display of nodes in specific node states. Select the **Include All** checkbox to select all node states.

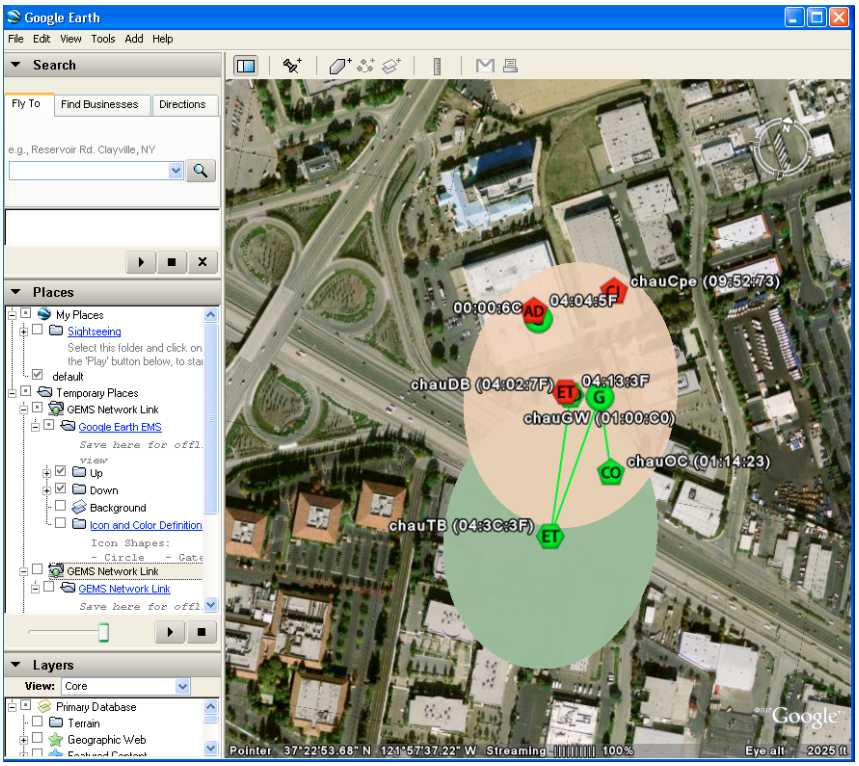
3 (Optional) To enable automatically opening Google Earth the next time you click Submit, click **Do This Automatically for Files Like This From Now On**.

Viewing the Google Earth Topology View

After setting the parameters for a topology view, click **Submit** to send the profile to Google Earth.

Isolate the view of your network place by clicking the GEMS Network folder. Filter elements and nodes by selecting and clearing items in the GEMS Network subfolders.

Figure A-6. Sample SkyPilot network place (Topology view)



Quick Launch

This section describes how to perform a Quick Launch and how to create a quick launch profile.

Performing a Quick Launch

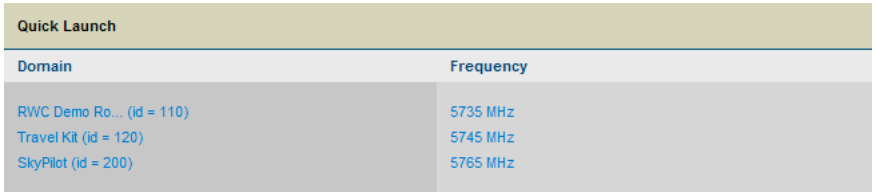
Use the Quick Launch view to quickly prepare and submit a Google Earth view of your network based on specific network elements such as the domain or SkyGateway that serves as the network hub.

To create a Google Earth Quick Launch profile:

1 On the command banner, click **Quick Launch**.

SkyPIlot EMS displays the Profile Settings Quick Launch screen (Figure A-7).

Figure A-7. Profile Settings Quick Launch screen



2 To view a domain or frequency with their default selections, click the desired domain or frequency link at the top of the page.

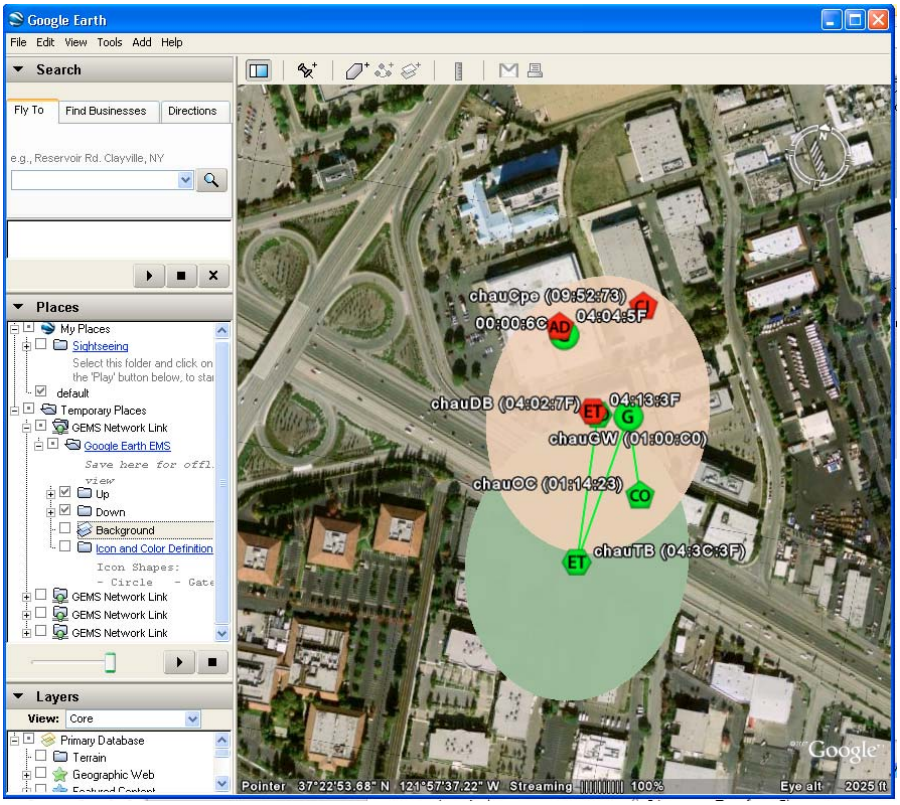
A Google Earth view of the SkyPilot network based on the selected domain or SkyGateway is instantly launched.

Viewing the Google Earth Quick Launch Display

After setting the parameters for a quick launch view, click **Submit** to send the profile to Google Earth.

Isolate the view of your network place by clicking the GEMS Network folder. Filter elements and nodes by clicking items in the folder.

Figure A-8. Sample SkyPilot network place (Quick Launch view)



B

Configuring a Firewall for SkyPilot Operations

For optimal SkyPilot operations, you should install your operating system without a firewall. However, if security concerns or other issues force you to use a firewall, you must configure the firewall to allow incoming data traffic on ports that SkyPilot clients and devices use for server communications (see Table B-1).

NOTE Each port you open reduces the overall security provided by the firewall.

Table B-1. Ports to Open

To do this	Open these ports
Allow EMS Web clients to connect to the EMS server	80 (HTTP server)
Allow SkyControl to configure SkyPilot devices outside the firewall	8000 TCP (HTTP server) 20 TCP (FTP server) 21 TCP (FTP server) 67 TCP/UDP (DHCP server)
Allow SkyControl to monitor SkyPilot devices outside the firewall	161 TCP/UDP (SNMP Read) 162 UDP (SNMP Traps)

C

Access Point Command-Line Interface

The access point command-line interface enables SkyPilot support to debug the access point configuration through the Linux command shell. This appendix provides instructions for accessing the interface.

Checking VLAN Status

Before you can access a DualBand's or TriBand's access point command-line interface, you must first check the VLAN status.

If your SkyPilot network is configured to use a management VLAN, the access point automatically uses that VLAN for management traffic. Therefore, you'll need to access the access point from a PC that's a member of that management VLAN. Typically this means you'll need to access the Web interface from the SkyPilot EMS server or other management workstation across the SkyPilot mesh network. If you've previously configured a management SSID as a member of the management VLAN, you can use this SSID to connect directly to the access point.

Accessing the Interface

You use a Wi-Fi connection to access a DualBand or TriBand access point's command-line interface. To complete the connection, you'll need a computer that's capable of Wi-Fi communication and that's within operating range of the access point.

To gain direct Wi-Fi network access:

1. Set up your host computer's 802.11b/g interface to connect to the access point's default SSID (which is a case-sensitive string representation of the DualBand or TriBand MAC address, without the colon characters).

   The default SSID uses a Wi-Fi Protected Access–Pre-Shared Key (WPA-PSK) protection scheme that uses a public key (password) of `publicpublic` to control access. You're prompted for this key when you connect to the SSID from your computer.

2. Set an IP address for your computer's 802.11b/g interface:

   Enter the IP address 192.168.0.5 and the netmask 255.255.255.0, and apply the setting.

3. Confirm that your computer can communicate with the access point by pinging it using its default IP address: for 2.4 GHz access points, 192.168.0.3, and for 4.9 GHz access points, 192.168.0.3. (This is same IP address you use to log in directly to the access point's Web interface.)

   If the ping is successful, you're ready to debug the access point using Linux shell commands.