

Tropos[®] Control Element Management System User Guide

Release 7.5



Tropos Networks, Inc.
555 Del Rey Ave.
Sunnyvale, CA 94085 USA
www.troposnetworks.com
408-331-6800

Part No. 200033-75 Rev C0
2011_05_13_00

Copyright Notice

©2003-2011 Tropos Networks, Inc. All rights reserved. Tropos and PWRP are registered trademarks of Tropos Networks, Inc. Tropos Networks, AMCE, TMCX, SABRE, CMDP, MESM and Metro-Scale Mesh Networking Defined are trademarks of Tropos Networks, Inc. All other brand or product names are trademarks or registered trademarks of their respective holder(s).

Information contained herein is subject to change without notice. The only warranties for Tropos products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Tropos shall not be liable for technical or editorial errors or omissions contained herein.

This product includes technology protected by U.S. Patents 6,704,301; 6,965,575; 7,016,328; 7,031,293; 7,058,021; 7,362,737; 7,376,087; 7,382,778; 7,397,789; 7,450,552; 7,460,489; 7,489,932; 7,499,409; 7,505,426; 7,542,421; 7,551,562; 7,564,781; 7,564,862; 7,580,393, 7,580,705; 7,586,879

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(II) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR52.227-19.

Important Note to Users

This software is provided by Tropos Networks, Inc. as is and any express or implied warranties, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall Tropos Networks, or its affiliates, subsidiaries or suppliers be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

Tropos reserves the right to make changes without further notice to any products herein.

FCC Notice to Users and Operators

Tropos routers comply with Part 15 of the FCC rules. Operation of the Tropos router is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits of a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in an office environment. This equipment generates, uses and radiates radio frequency energy, and if not installed and used in accordance with the instructions, the device may cause harmful interference. However, there is no guarantee that interference will not occur. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to correct the interference by using one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician.

This Part 15 radio device operates on a non-interference basis with other devices operating at this frequency. Any changes or modification to said product not expressly approved by Tropos Networks could void the user's authority to operate this device.

Contents

- Prefacevii
- 1 Overview1
 - Product Overview..... 2
 - Product Features 3
 - Mid-Tier Mesh Architecture 4
 - Mobile Router Networks 6
 - Network Management and Administration 8
- 2 Installation9
 - Pre-Installation Requirements 10
 - Installing Tropos Control 12
 - Updating ARP Cache Settings 14
 - Uninstalling the System 14
 - Backing Up and Restoring the Tropos Control Server 15
 - Upgrading the Server 16
 - Resetting the Administrative Password 16
- 3 Getting Started17
 - Getting Ready to Manage the Network 18
 - Starting and Stopping the Server 18
 - Using the Web Interface 19
 - Accessing and Exiting the Web Interface 19
 - Navigating the Web Interface 20
 - Discovery 23
- 4 Viewing Network Health Information24
 - Preparing to Access the Network Health Panels 25
 - Using the Dashboard 25
 - Viewing Geographic Maps 27
 - Using the Network Optimization Panels 30
 - Using the Client Optimization Panels 34

Understanding the Client Query Reports	36
Using the Voice Optimization Panels	39
Using the Device Ping Utility	40
Modifying Network Health Thresholds and Report Options	42
Modifying Network Health Thresholds	42
Modifying Report Options	44
5 Viewing Fault Information	49
Viewing Network Events	50
Viewing Alarms	51
Viewing Event Counts	52
Configuring Alarms	53
SNMP Trap Forwarding	57
6 Viewing Network Configuration Information	58
Network Configuration Panels	59
Configuration View Actions	60
Updating the Device Database	62
Creating Custom Views	64
Configuring Gateways for Multi-Subnet Roaming	65
7 Provisioning	68
About Provisioning Operations	69
Provisioning Routers Using Web Forms	74
Provisioning from Forms - Tasks	74
Provisioning Routers From a File	76
Provisioning from Files - Tasks	77
Provisioning Forms	78
Router Identity Page	79
IP and VLAN Page	81
Wireless Page	86
Client Access	92
DHCP Server	97
SNMP	98
Time	100
DHCP Clients	102
Static IP Client	103
Packet Filtering	105
P2P Blocking	109
Multi-Subnet Roaming	110
Backhaul Routing	111
Rate Limiting	112
QoS	115

Voice	118
Software	120
Security	120
Other Provisioning Operations	123
Provisioning Tasks - Administration	125
Auditing Provisioning Jobs	126
8 Performing Administrative Tasks	129
Generating Diagnostic Information	130
Upgrading Router Software	131
Tracking Router Inventory	134
Backing Up Router Configurations	136
Restoring Router Configurations	140
Supporting RADIUS Authentication	143
Managing Administrative Users	144
Using Router Auto Discovery	145
Viewing the User Audit Log	149
Configuring Banner Text	149
Configuring FIPS Mode	150
A Redundant Tropos Control Servers for Failover	152
Primary and Secondary Servers	152
Set Up the Primary and Secondary Servers	152
Set Up the Secondary Server as Backup	153
Perform Failover from the Primary to Secondary Server	153
Returning to the Primary Server when it Recovers	154
Glossary	155
Index	162

Preface

This guide contains the information and instructions needed to install, configure and use the Tropos[®] Control Element Management System to manage your wireless network.

About this Guide

Tropos Control is a comprehensive, real-time management system for Tropos wireless networks. The system allows you to view the status of all Tropos gateways and nodes, modify configurations, and assess network performance, all from a central management station.

This guide contains information and instructions on installing, configuring, and optimizing Tropos Control, and is divided into the following chapters:

[Chapter 1, “Overview,”](#) provides an overview of the Tropos network architecture and introduces the system features.

[Chapter 2, “Installation,”](#) contains information needed to install the Tropos Control server, including system requirements and step-by-step installation instructions.

[Chapter 3, “Getting Started,”](#) contains basic information on using Tropos Control, including how to start and stop the server, establish a new wireless network, and perform discovery.

[Chapter 4, “Viewing Network Health Information,”](#) describes how to display detailed information on network connectivity and performance using the Network Health panels in the web interface.

[Chapter 5, “Viewing Fault Information,”](#) describes how to display alarm and network event information using the Fault Management panels in the web interface.

[Chapter 6, “Viewing Network Configuration Information,”](#) describes how to display device information using the Network Configuration panels in the web interface.

[Chapter 7, “Provisioning,”](#) describes how to use the web interface to provision Tropos routers for operation in the wireless network.

[Chapter 8, “Performing Administrative Tasks,”](#) describes how to manage router inventory, upgrade router software, and generate diagnostic information using the web interface.

[“Glossary”](#) contains definitions of terms relating to Tropos wireless networking.

Tropos Technical Support

If you need technical assistance, you can contact the Tropos Technical Assistance Center by telephone, web, or email.

Whom to contact	How to contact
Technical Support Toll-free Number	1-877-987-6767
Website	www.Tropos.com
Email	Support@Tropos.com




Supporting Documentation

Refer to the Tropos Control online help system for further assistance. For more information about managing and configuring a Tropos wireless network, refer to the following documents which are available on the installation CD or by download:

- Release Notes -- Current product release information.
- Tropos Mesh Router Quick Start Card -- Instructions on installing Tropos routers.
- Tropos Mesh Router User Guide -- Information on configuring and maintaining Tropos routers by way of the Tropos Configuration Utility.
- Tropos Networks Mesh Router Installation Guide, Model 7320— Explains how to install the Tropos 7320 router hardware.
- Tropos Networks Mesh Router Installation Guide, Model 6320 and 6310-- Explains how to install the Tropos 6320 and 6310 Mesh router hardware.
- Tropos Networks Mesh Router Installation Guide, Model 5320 and 9532 -- Instructions on installing the Tropos 5320 and 9532 router hardware.
- Tropos Networks Mesh Router Installation Guide, Models 4310 and 9432— Explains how to install the Tropos 4310 and 9432 mobile Mesh router hardware.
- Tropos Networks Mesh Router Installation Guide, Models 4210 and 9422— Explains how to install the Tropos 4210 and 9422 mobile Mesh router hardware.

Document Conventions

The document uses the conventions described here.

Icon	Notice Type	Description
	Note	Useful information (less urgent than Caution or Warning).
	Caution	Careful attention required to prevent loss of data or damage to equipment.
	Warning	Careful attention required to avoid bodily injury (NOTE: activities involving electrical connections require extreme caution, constant attention, and strict adherence to standard safety practices).

Nested menu items are separated by an angle bracket (>) (example: **Start > Programs > Tropos > Tropos Control EMS**).

In parameter tables, default values are listed in bold italics. If there are only two choices, the choices are separated by a vertical line (example: Enabled | ***Disabled***).

Items shown in **bold** text most often represent a user selection. However, important names or menus are occasionally bolded for emphasis.

Graphical user interface variables are presented in italic font. (example: *host.domain.com*)

Text entered in a command line is presented in **bold courier** font. Command output and system file names are presented in *courier* font.

Command line variables and keyboard buttons are enclosed in brackets. (examples: <Alt>, <filename>).

Keys to be pressed simultaneously are separated by the addition sign (+) (example: <Ctrl> + y).

1 Overview

This chapter provides an overview of the Tropos Networks wireless network architecture and introduces the features of the Tropos Control Element Management System.

Chapter contents:

- [Product Overview](#)
- [Product Features](#)
- [Mid-Tier Mesh Architecture](#)
- [Network Management and Administration](#)

Product Overview

Tropos routers make possible wireless computer networking by providing the infrastructure for wireless hot spots and metropolitan scale wireless meshes. [Table 1](#) lists the routers and associated characteristics.

TABLE 1 Router Models

Router Model	Characteristics
9532	<ul style="list-style-type: none"> • Outdoor use, FCC public safety applications • 802.11a/b/g • 2.4 GHz and 4.9 GHz • AC power
9432 9422 ^a	<ul style="list-style-type: none"> • Mobile router for use in vehicles, FCC public safety applications • 802.11a/b/g • 2.4 GHz and 4.9 GHz • DC power
7320	<ul style="list-style-type: none"> • Outdoor use • 802.11a/b/g/n • 2.4 GHz and 5.8 GHz (FCC), 2.4 GHz and 5.4 GHz (ETSI) • AC power
7320 DC	<ul style="list-style-type: none"> • Outdoor use • 802.11a/b/g/n • 2.4 GHz and 5.8 GHz (FCC), 2.4 GHz and 5.4 GHz (ETSI) • DC power
6320	<ul style="list-style-type: none"> • Outdoor use • 802.11a/b/g/n • 2.4 GHz and 5.8 GHz (FCC), 2.4 GHz and 5.4 GHz (ETSI) • DC power
6310	<ul style="list-style-type: none"> • Outdoor use • 802.11b/g/n • 2.4 GHz • DC power
5320	<ul style="list-style-type: none"> • Outdoor use • 802.11a/b/g • 2.4 GHz and 5.8 GHz (FCC), 2.4 GHz and 5.4 GHz (ETSI) • AC power
5320 DC	<ul style="list-style-type: none"> • Outdoor use • 802.11a/b/g • 2.4 GHz and 5.8 GHz (FCC), 2.4 GHz and 5.4 GHz (ETSI) • DC power

TABLE 1 Router Models (*continued*)

Router Model	Characteristics
5210 ^a	<ul style="list-style-type: none"> • Outdoor use • 802.11b/g • 2.4 GHz • AC power
5210 DC ^a	<ul style="list-style-type: none"> • Outdoor use • 802.11b/g • 2.4 GHz • DC power
4310 4210 ^a	<ul style="list-style-type: none"> • Mobile router for use in vehicles • 802.11b/g • 2.4 GHz • DC power

a. For the 5210, 4210, and 9422 routers, software support is limited to the correction of service affecting bugs. The 3110, 3210, and 5110 routers are no longer supported.

The term *mobile router* refers to the Tropos 4310, 4210, 9432, and 9422 models, which are designed for installation and use in moving vehicles. The term *stationary routers* (or *fixed routers*) refers to all the other router models, which are designed to be installed in a fixed location.

All Tropos routers are controlled by the Tropos Sphere Network Operating System. The Tropos Control Element Management System (Tropos Control) described in this guide enables network-wide control, management, and router configuration. The Tropos Configuration Utility, described in the *Tropos Networks Configuration Guide*, provides an interface for direct configuration of individual routers.

Note

The Tropos routers and the Tropos Control EMS server in your network must run compatible versions of software. For compatibility information, refer to the Tropos Control EMS Release Notes for your release.

Product Features

Tropos Control includes the following features:

- Network control from a single management station with convenient web interface (as well as legacy client interface)
- Quick, uniform bulk provisioning of router configuration and security settings
- Automatic discovery and graphical placement of routers
- Google map views of router location, status, and channels
- Reporting of global positioning system (GPS) location data in network maps for mobile nodes
- Network health check with point-and-click graphs

- Overview of network performance and optimization priorities
- Multiple views of network capacity and wireless link quality
- Central configuration and software updates
- Point-and-click access to configuration and security information
- Support for Federal Information Processing Standards, version 140-2 (FIPS 140-2)
- Link state and client connectivity information and monitoring
- Quick access to the fault, performance, and statistical information
- MAC address filtering
- Rogue client blacklisting
- Continuous alarm and event monitoring
- Automatic collection and monitoring of performance data
- Long term trend data
- Performance reporting
- Remote configuration and software updates
- Comprehensive logging

Mid-Tier Mesh Architecture

Each stationary router can be configured to operate as a *gateway* or *node*. As a gateway, the router establishes communications between the wired Ethernet network and other routers that operate as nodes; nodes, in turn, form radio communications links with the clients (users) on the network. Gateways can also service clients directly.

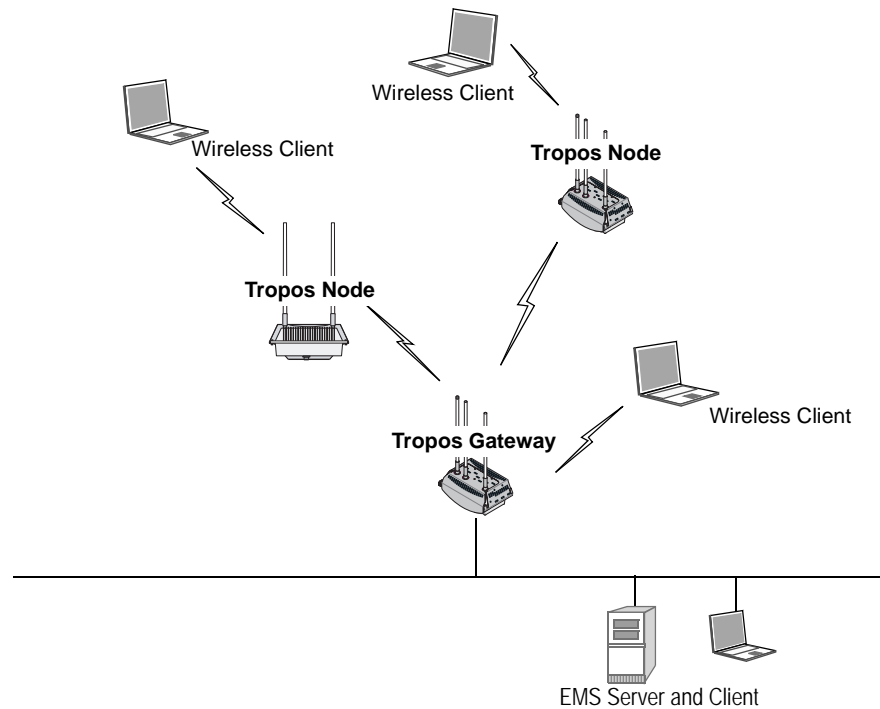
i Note

Each Tropos mobile router is shipped from the factory with the mobile node setting, but can also operate as a gateway. If a mobile router is operating as a gateway and the wired connection is disabled, the router automatically reverts to mobile node operation.

A Tropos wireless network consists of gateways that are directly connected to the wired network and nodes that deliver wireless communications support for clients and provide wireless backhaul to other upstream Tropos nodes and gateways. The nodes and gateways form a *meshed cluster* to route wireless signals dynamically from clients through the gateway and on to the wired network.

Figure 1 shows basic Tropos wireless network.

FIGURE 1 Typical Tropos Wireless Network

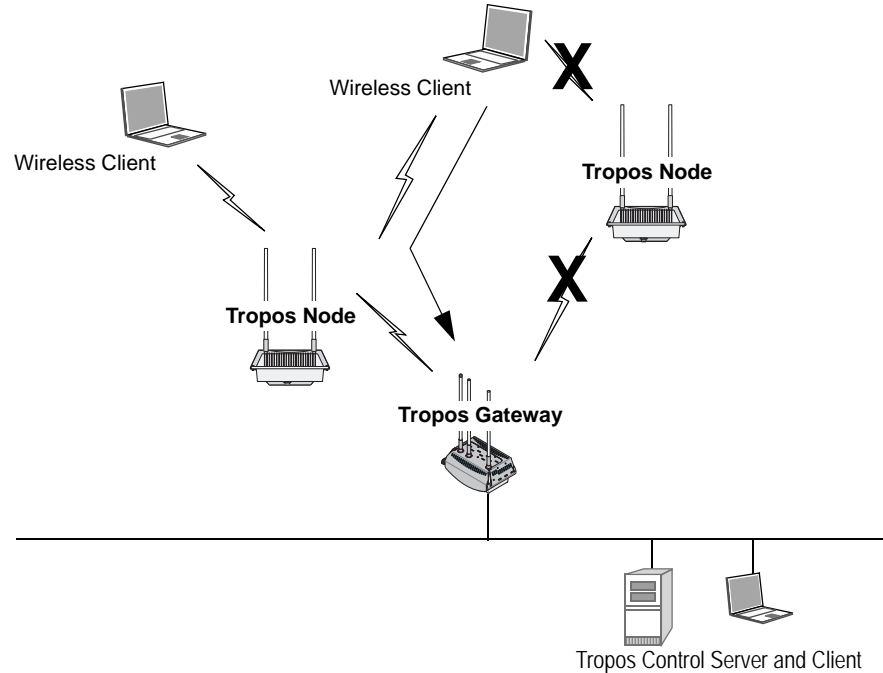


Tropos networks can be deployed on a small or large scale. The largest deployments are able to support thousands of routers over a wide geographic area.

Each node communicates with standard 802.11 clients and passes data back through a wireless link to a gateway that is attached to the wired network. All routers continually monitor the quality of the wireless links and select the optimal path for routing traffic to the wired gateway. By overcoming the effects of interference and multi-path fading across the mesh, the Tropos network is able to deliver consistent throughput up to the maximum available.

Routing decisions are made by way of the Tropos Predictive Wireless Routing Protocol (PWRP[®]), which manages network routing based on self-organizing principles. The PWRP implements dynamic re-clustering to maximize available throughput and ensure reliability. Dynamic re-clustering refers to the ability of the network to respond to changes in radio signal availability and quality by modifying the paths that data packets take. When a node becomes unavailable or the signal quality degrades due to distance or other ambient conditions, the network automatically reorganizes to create another path from the client through the mesh of nodes back the gateway and the wired network (Figure 2).

FIGURE 2 Rerouting in a Typical Tropos Wireless Network



Due to dynamic re-clustering, individual paths need not be engineered on a link-by-link basis. The PWRP automatically sets up and maintains routes by dynamically identifying the path that achieves the highest throughput between the wireless client and the wired backhaul connection. Throughput maximization improves overall network performance, and lack of a system-wide point of failure increases reliability.

Tropos wireless networks permit easy addition of new routers to support growth in the number of client subscribers. New nodes may be added to extend coverage at any location that has available power. As the number of subscribers continues to grow, gateways may also be added to further increase coverage, performance, and reliability.

Mobile Router Networks

Tropos mobile routers extend the wireless network to mobile node operation. Installing mobile routers in fire, police, or other public service vehicles allows for immediate high-bandwidth access to network services. As with other Tropos routers, the mobile router dynamically associates to upstream nodes or gateways.

Clients connect to the mobile router through a wireless or wired connection. In a typical vehicle installation, the client computer is connected directly to the mobile router through a wired interface connection.

Since mobile routers may be in motion, special rules apply to the association of wireless clients to and from mobile routers. The following guidelines and properties apply:

- A mobile node will always attempt to establish backhaul connection to an upstream stationary Tropos node or gateway. If this is not possible, it will attempt to connect to another mobile router.
- A stationary Tropos node will not attempt to establish uplink to a mobile router.
- Configuring a separate ESSID for mobile routers is recommended. Wireless clients accessing this ESSID will always attempt to associate with mobile nodes, while clients accessing other ESSIDs will always attempt to associate with stationary nodes. This arrangement prevents typical stationary clients from associating to mobile nodes that may move in and out of coverage, while also permitting special sets of wireless clients (such as passengers on a bus with a mobile node installed) to associate with mobile nodes.

If any router loses backhaul connectivity, it shifts to standalone mode so as not to advertise wireless service to associated clients. When connectivity is recovered, service is automatically restored. (This process takes approximately ten seconds after connectivity is re-established.)

Because a mobile router is more likely to lose wireless connectivity than a stationary node, clients associated with a mobile node may encounter more frequent service disruptions than those associated to stationary nodes. To prevent unsuccessful data transmission attempts from the client when upstream connectivity is lost, the downstream wired interface for the mobile is immediately switched off when connectivity is lost.

Figure 3 shows a typical Tropos network with mobile nodes added, and Figure 4 illustrates automatic rerouting actions if connectivity to the stationary Tropos network is interrupted.

FIGURE 3 Typical Tropos Mobile Network

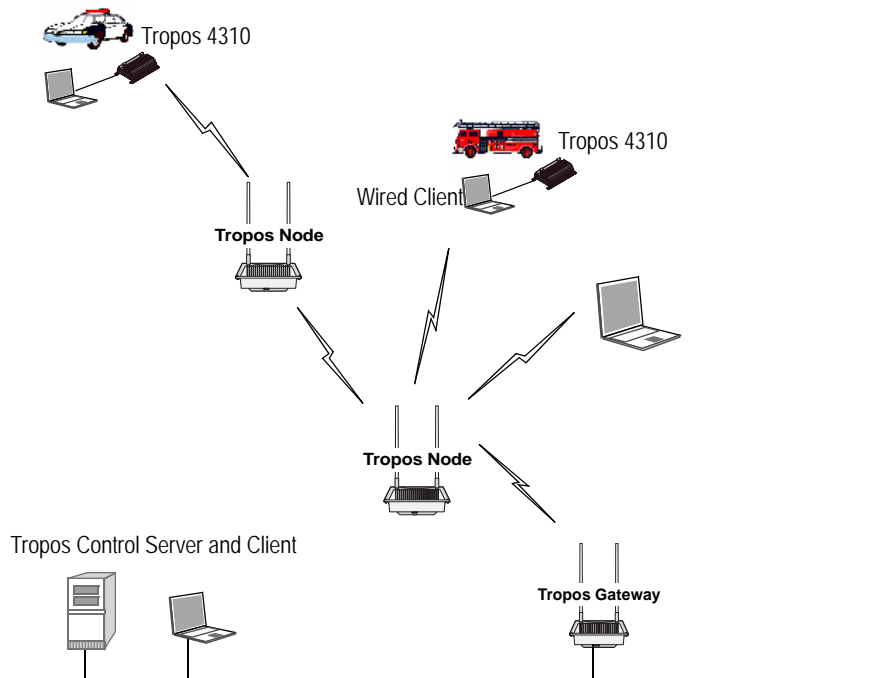
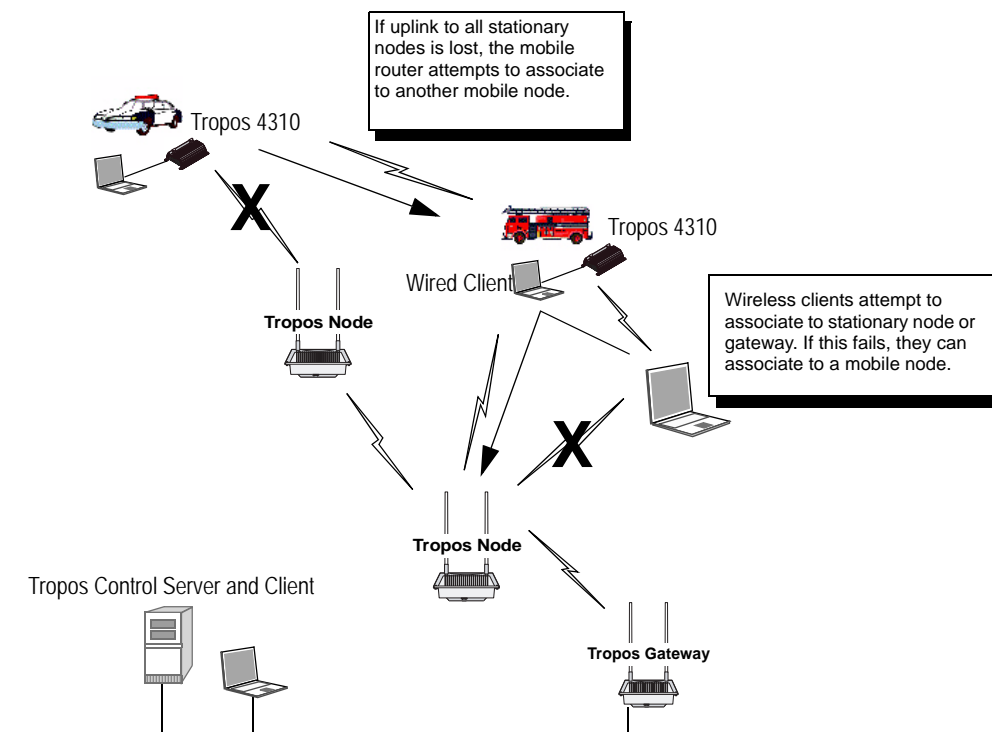


FIGURE 4 Rerouting in a Tropos Mobile Network



Network Management and Administration

The Tropos Control Element Management System (Tropos Control) enables network operators to administer an entire Tropos network consisting of numerous gateways and nodes distributed over a wide geographical area. Tropos Control presents geographic views of all the routers in a network along with detailed configuration information. Operators can view network health statistics, monitor performance, events, and alarms, and provision individual routers or groups of routers. Support is also provided for batch updates of configurations and software.

Note
Multiple Tropos Control servers may be used to manage a network.

Individual routers may also be provisioned using Tropos Control or the Tropos Configuration Utility. The Tropos Configuration Utility provides a secure HTTPS interface to access and control individual routers, connecting through the wired Management port on the router or association of a laptop client.

2 Installation

This chapter provides Tropos Control installation instructions.

Chapter contents:

- [Pre-Installation Requirements](#)
- [Installing Tropos Control](#)
- [Updating ARP Cache Settings](#)
- [Uninstalling the System](#)
- [Backing Up and Restoring the Tropos Control Server](#)
- [Upgrading the Server](#)
- [Resetting the Administrative Password](#)

Pre-Installation Requirements

- [Sizing Requirements](#)
- [Server and Client System Requirements](#)
- [Supported Routers](#)
- [Firewall Requirements](#)

Sizing Requirements

[Table 2](#) lists the minimum requirements for a Tropos Control server that uses an external Oracle database and [Table 3](#) lists the Oracle database requirements.

Table 2 Tropos Control Server Requirements (Using an External Oracle Database)

Size of Network (# of devices)	Minimum Number of CPU cores	Minimum Memory (RAM) Requirements	Minimum Disk Requirements
< 500	2	2 GB	2 GB
500-2000	2	4 GB	4 GB
2000-5000	4	8 GB	8 GB
5000-6500	4	8 GB	8 GB

Table 3 Oracle Database Server Requirements

Size of Network (# of devices)	Minimum Number of CPU cores	Minimum Memory (RAM) Requirements	Minimum Disk Requirements
< 500	2	2 GB	100 GB
500-2000	2	4 GB	300 GB
2000-5000	4	8 GB	500 GB
5000-6500	4	8 GB	600 GB

Server and Client System Requirements

- CentOS 5 must be installed on the Tropos Control Server. Visit support@tropos.com for instructions and to download a Tropos-customized CentOS installation image.
- There should be only one user account created on the Tropos Control server.
- [Table 4](#) lists the client browser requirements for access to the Tropos Control web client.

TABLE 4 Client Browser Requirements for Web Client Access

Web Browser	Windows	Linux
Internet Explorer 6	Yes	N/A
Firefox 3.5	Yes	Yes

Supported Routers

We recommend that current customers upgrade existing TropoControl installations to Release 7.5 only if all the routers in the network will be running Release 7.1 or later software.

Firewall Requirements

If the Tropo Control EMS server or routers are behind a firewall, then the ports listed in [Table 5](#) must be opened on the firewall.

TABLE 5 Firewall Ports

Port Number and Type	Protocol	Direction	Description
8443 - TCP	HTTPS	Both	EMS Apache Server port
1099 - TCP	RMI	Both	RMI Registry
Random/4567 - TCP	TCP	Both	EMS FE Secondary Port
Random/5008 - TCP	TCP	Inbound only	EMS Transport Provider
Random/16010 - TCP	RMI	Both	This port is used by the EMS Server for RMI communication
161 - UDP	SNMP	Both	SNMP Request/Response
162 - UDP	SNMP	Both	SNMP Informs (Traps)
5000 - TCP	NUTTCP	Both	Performance Benchmarking
5001 - TCP	NUTTCP	Both	Performance Benchmarking
22 - TCP	SSH	Both	
80 - TCP	HTTP	Both	Web Service
443 - TCP	HTTPS	Both	Secured Web Service
7 - UDP	ICMP/PING	Both	Ping utility
0,8 - UDP	ECHO	Both	Echo request/reply
123 - UDP	NTP	Both	NTP client
8900 - TCP	TCP	Both	Used by EMS for router configuration

TABLE 5 Firewall Ports (*continued*)

Port Number and Type	Protocol	Direction	Description
1521 (default)	TCP	Both	(connection port - only for Oracle database) Consult your Oracle database administrator to verify the right port before installing Tropos Control

Installing Tropos Control

Complete the installation procedures in the following order:

1. [Install CentOS.](#)
2. [Configure CentOS to operate in single user mode.](#)
3. [Install Tropos Control.](#)

Install CentOS

i Note

The partitioning portion of the CentOS installation process formats all partitions. Before starting the installation, verify that you have backed up any data that you want to keep.

1. Download and install the pre-configured version of CentOS from support.tropos.com.
2. Boot the server from the CentOS CD.
3. Type **install** and press **Enter**. (If you need to abort the installation, just remove the CD and reboot the machine.)
4. Click **Next**.
5. Click **Yes** when prompted to remove all partitions.
6. On the page that appears, click **Edit** in the Network Devices area. Select the check box to enable IPv4 support, choose **Manual Configuration**, and enter the IP address and netmask for the Tropos Control server. Clear the **Enable IPv6 Support** check box, and then click **OK**.
7. In the Hostname area of the page, choose **manually** and enter a host name in the form *host.domain.com*.
8. Enter IP addresses for the network gateway and primary and secondary DNS servers.
9. Click **Next**.
10. Click a dot on the map to choose the nearest city in your time zone. Verify the selection in the menu below the map, and then click **Next**.
11. Enter and confirm a root password (minimum eight characters) and click **Next**.

The installation begins. This process may take up to 20 minutes. When the process is complete, the system reboots automatically.

12. Remove the CD.

Log in as **root** using the password that you configured in [step 11](#). If the graphical user interface does not start automatically, enter the command **startx**.

Configure CentOS to operate in single user mode

1. Log in as the root user.
2. Edit the `/etc/passwd` and `/etc/shadow` files and remove all the users except **root** and the pseudo-users. Make sure that the password fields in `/etc/shadow` for the pseudo-users are either a star (*) or double exclamation mark (!!). This prevents users from logging in as the pseudo-users.
3. Edit the `/etc/nsswitch.conf` system file and make `files` the only option for `passwd`, `shadow`, and `group`. This disables Network Information Service (NIS) and other name services for users and groups.
4. In the `/etc/xinetd.d` directory, edit the files `eklogin`, `gssftp`, `klogin`, `krb5-telnet`, `kshell`, `rexec`, `rlogin`, `rsh`, `rsync`, `telnet`, and `tftp`, and set the value of `disable` to `yes`.
5. Reboot the system for the changes to take effect.

Install Tropos Control

1. Obtain a static IP address in your network for the Tropos Control server (management station).
2. Obtain the Tropos Control software image (`<imagefile>.bin`) and copy it to a temporary folder.
3. Set the permission on the image file to execute:


```
chmod +x <imagefile>.bin
```
4. If you are upgrading Tropos Control, stop the server.


```
service watchdog stop
```
5. Run the executable file.


```
./<imagefile>.bin
```

The installation wizard opens and asks whether you want to install a new release or upgrade from a previous release. Select an option and choose **OK**.

If you choose **Install Fresh 7.5**, the wizard presents the following prompts:

- a. License - Choose **OK** to accept the terms of the license agreement.
- b. Administrative password - Enter the administrative password (minimum eight characters) for the **ems** user, and choose **Next**. Reenter the password and choose **Next**.
- c. Router password - Enter the router admin password (minimum eight characters) and choose **Next**. Reenter the password and choose **Next**. For instructions on changing the

router admin password at a later time, see [“Resetting the Administrative Password”](#) on page 16.

- d. Select database - Enter **Y** if you want to use bundled MySQL database or **N** if you want to use your own Oracle database.
- e. (Oracle only) Enter host address - Enter the host IP address where the Oracle database is running.
- f. (Oracle only) Enter port number - Enter the port number used by the Oracle database.
- g. (Oracle only) Enter global database name - Enter the Oracle global database name.
- h. (Oracle only) Enter user name - Enter the user name to connect to Oracle database.

i **Note**

The oracle user must have RESOURCE and Create Session privileges and must be a dedicated user for Tropos Control (not shared with any other applications). If possible, there should be a dedicated tablespace associated with the user.

- i. (Oracle only) Enter password - Enter the password for the user.

If you choose **Upgrade to 7.5**, the installation begins automatically. If the existing Tropos Control installation uses an Oracle database, then the upgrade process prompts for database details as in [step e](#) - [step i](#) above. If the installation uses a MySQL database, the upgrade continues without the need for any user intervention.

6. When the installation is complete, choose **OK**.

The server automatically starts, and you can access the web interface. See [“Using the Web Interface”](#) on page 19.

Updating ARP Cache Settings

In environments where the devices under management are on the same subnet as the Tropos Control Server, default Address Resolution Protocol (ARP) cache settings on the Linux server should be changed. Execute the following commands to modify the ARP cache settings, and also add the same command lines to the `/etc/rc.local` file.

```
echo "1024" > /proc/sys/net/ipv4/neigh/default/gc_thresh1
echo "4096" > /proc/sys/net/ipv4/neigh/default/gc_thresh2
echo "8192" > /proc/sys/net/ipv4/neigh/default/gc_thresh3
```

Uninstalling the System

Follow the steps in this section to remove the Tropos Control server from your system.

i **Note**

For installations with an Oracle database: The uninstall script does not remove data from the Oracle database. It removes only files and folders. After uninstalling Tropos Control, you must manually delete the data stored in the database.

Uninstall Tropos Control

1. Go to the bin directory in the Tropos Control installation directory:

```
cd /<installdirectory>/bin
```

2. Shut down the Tropos Control server:

```
service watchdog stop
```

3. Run the uninstall command:

```
./uninstall.sh
```

The Tropos Control system is uninstalled and removed from the system.

Backing Up and Restoring the Tropos Control Server

Follow the procedures in this section to back up and restore the Tropos Control server.

ⓘ Note

For installations with an Oracle database: The backup/restore script does not back up or restore any data from the Oracle database. Follow the Oracle procedures to back up and restore your data.

Back up the TroposControl server

1. Go to the bin directory in the Tropos Control installation directory:

```
cd /<installdirectory>/bin
```

2. Execute the backup script:

```
./backup.sh /<installdirectory>
```

3. Enter the database password for the root account. This is the password for the **ems** user account, not the root password for the machine.

The backup is created and stored in the current directory. The following files are created:

— backup file - Tropos_EMS_Backup_<date>.tar.gz

— checksum file - Tropos_EMS_Backup_<date>.md5

4. Move the backup and checksum files to /tmp or another temporary location that is not part of the TC installation tree.

Restore the server

1. Copy the backup and checksum files to the bin directory in the Tropos Control installation directory, and go to that directory:

```
cd /<installdirectory>/bin
```

2. Stop the server:

```
service watchdog stop
```


3. Execute the restore script, using the name of the previously-backed up tar.gz and .md5 files:

```
./restore_ems.sh /<installdirectory>  
Tropos_EMS_Backup_<date>.tar.gz Tropos_EMS_Backup_<date>.md5
```
4. Enter **Y** to continue.
5. Enter the password for the root account, as prompted.
The database is restored and the server is restarted.

Upgrading the Server

Tropos Control upgrades are supported only from Release 7.3. If you have an earlier version of Tropos Control, you must upgrade to Release 7.3 before upgrading to Release 7.5.

Upgrade the Tropos Control server from 7.3

Follow the procedure to install Tropos Control (“[Install Tropos Control](#)” on page 13). Choose the Upgrade to Release 7.5 option.

Resetting the Administrative Password

Follow these steps to reset the Tropos Control administrative password.

i Note

The administrative password must have a minimum of eight characters. The password change doesn't affect the password stored in the router; it only changes the password that is stored in the Tropos Control server and used for communication between Tropos Control and the routers.

Reset the administrative password

1. Go to /<installdirectory>/ems/bin and execute the following command:

```
./setRouterPasswd
```
2. Respond to the prompts to enter and confirm the password.

3 Getting Started

This chapter describes how to start using Tropos Control to manage the network.

Chapter contents:

- [Getting Ready to Manage the Network](#)
- [Starting and Stopping the Server](#)
- [Using the Web Interface](#)
- [Discovery](#)

Getting Ready to Manage the Network

To use Tropos Control to manage the Tropos network, you must first configure each router to recognize the Tropos Control server and verify that all routers are in the same wireless routing domain. Use the Tropos Configuration Utility to perform these tasks, as outlined in this section. For detailed information on using the Tropos Configuration Utility, see the *Tropos Networks User Guide*.

i Note

Use the following procedure for initial device configuration after installing Tropos Control. See [“About Provisioning Operations”](#) on page 69 for information on configuring devices on an existing network.

Configure routers

1. Perform these tasks as described in the *Tropos Mesh Router User Guide*.
2. Open the Tropos Configuration Utility for the router.
3. Open the Passwords and Security page and enter the Router-EMS Authentication Key. Confirm that each router in the network has the same wireless routing domain ID. If you make a change, click **Store Changes**.
4. Commit any changes.
5. Repeat for all the routers to be managed by Tropos Control.

You can now use Tropos Control to discover and manage the routers.

Starting and Stopping the Server

Start the server

- Issue the following command on the server:
`service watchdog start`

Stop the server

- Issue the following command on the server:
`service watchdog stop`

Using the Web Interface

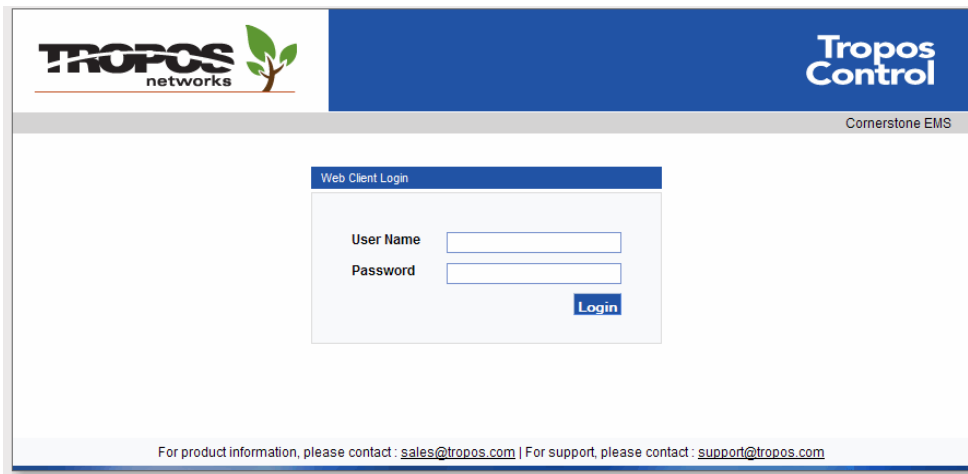
The web interface may be reached from the Tropos Control server or from any other web-enabled computer on the network.

Accessing and Exiting the Web Interface

Follow the instructions in this section to access and exit the web interface, display details about the current login session, and access the online help system.

Access the web interface

1. Open the following URL on a web browser that has a network connection to the Tropos Control server:
`https://<Tropos Control Server IP address>:8443`
2. If security alerts appear about viewing pages over a secure connection, click **Yes** to proceed.
3. The login panel opens.



The screenshot shows the Tropos Control web interface. At the top left is the Tropos networks logo, and at the top right is the Tropos Control logo. Below the logos is a grey bar with the text "Cornerstone EMS". The main content area is white and contains a "Web Client Login" form. The form has two input fields: "User Name" and "Password", and a "Login" button. At the bottom of the page, there is a footer with contact information: "For product information, please contact : sales@tropos.com | For support, please contact : support@tropos.com".

4. Log in with the user name and password used for Tropos Control client access. The default user name is `root`, and the default password is `public`.

5. The system prompts you to change the password.

The screenshot shows the Tropos Control web interface. At the top left is the Tropos networks logo, and at the top right is the Tropos Control logo. Below the logos, the text "Welcome root" is displayed, followed by the message "You are using default password. Please Change your password." A "Change Password" form is centered on the page. The form includes two input fields for "New Password" and "Confirm Password", a checkbox for "Password expires in" followed by a text input for "days", and a "Submit" button. At the bottom of the page, contact information is provided: "For product information, please contact : sales@tropos.com | For support, please contact : support@tropos.com".

6. Enter and confirm a new password.

7. Click **Submit**.

The Tropos Control Web Interface opens to display the Network Health Dashboard.

Display session details

- Click **Clients** in the upper right corner of the web interface.

Access online help

- Click **Help** in the upper right corner of the web interface. The online help system (based on this guide) opens in a new window.

Exit the web interface

- Click **Logout** in the upper right corner of the web interface. The current user name is presented along with the Logout link.

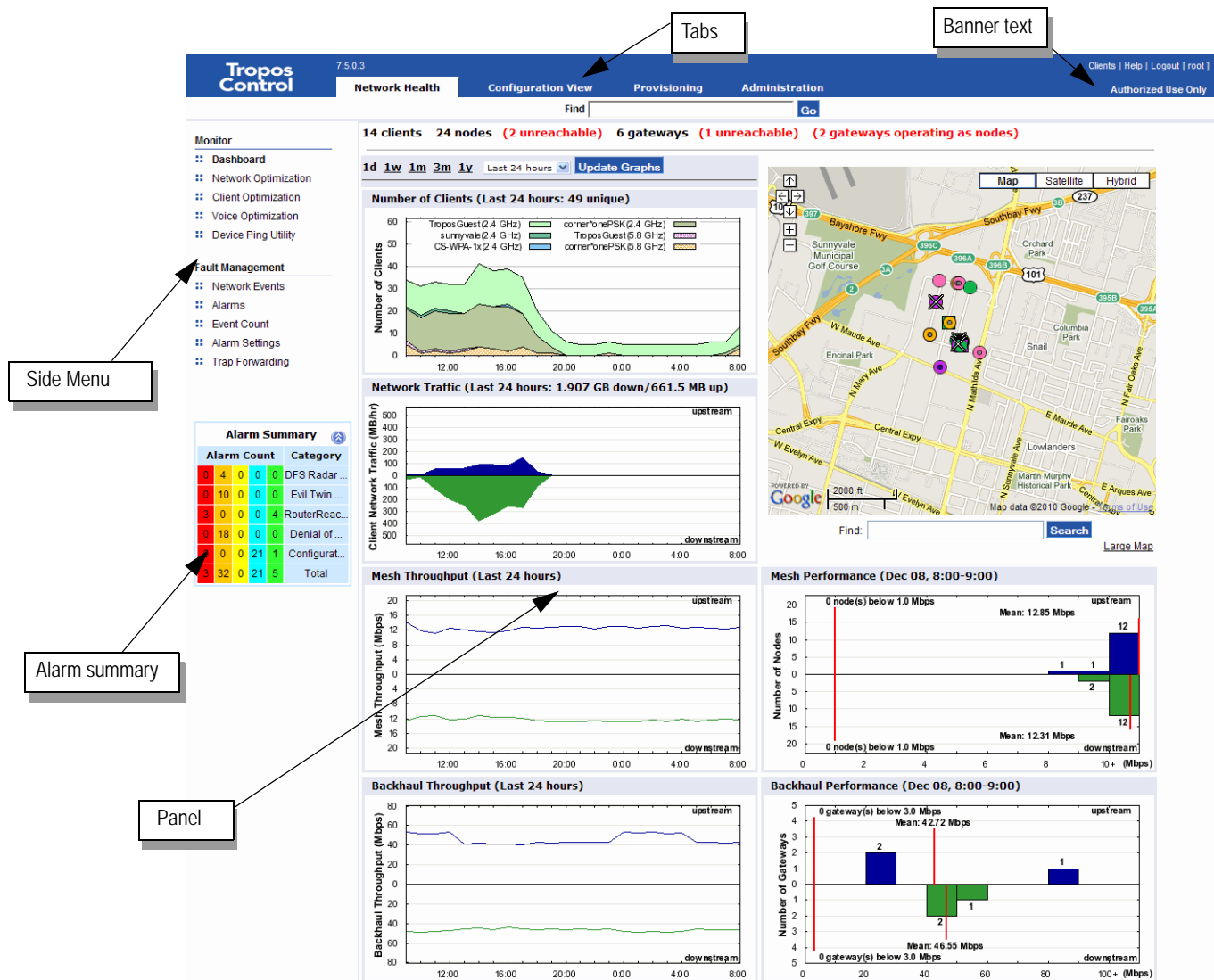
Navigating the Web Interface

The Tropos Control web interface (Figure 5) contains the following elements:

- Tabs---Major categories of information:
 - Network Health--- See “[Viewing Network Health Information](#)” on page 24.
 - Provisioning---See “[Provisioning](#)” on page 68.
 - Configuration View---See “[Viewing Network Configuration Information](#)” on page 58.
 - Administration---See “[Performing Administrative Tasks](#)” on page 129.
- Panels---Detailed information, which varies according to tab and side menu selection.

- Side menu---Access to panels. Contents are specific to each tab, and expandable items are marked with an arrow.
- Alarm summary---Summary of the numbers of alarms of each level of severity.
- Banner text--Optional configurable banner text.

FIGURE 5 Web Interface



Using Tables

Much of the information in the web interface is presented in tables.

- Use checkboxes to choose one or more rows, or use the checkbox at the top of the column to select all rows.
- Click a column header to sort the column. Click once for an ascending sort (up arrow) and twice for a descending sort (down arrow).

<input type="checkbox"/>	Name	IP Address ▲	Longitude	Latitude	Location	Contact	Display Na
<input type="checkbox"/>	9302907	10.88.2.111	0	0	Sunnyvale,CA	www.troposnetworks.com	SM_N_10
<input checked="" type="checkbox"/>	930088e	10.88.2.2	0	0	Sunnyvale,CA	www.troposnetworks.com	SM_GW_1
<input checked="" type="checkbox"/>	12630	10.88.4.100	0	0	Sunnyvale,CA	www.troposnetworks.com	SM_N_1
<input type="checkbox"/>	9300fca	10.88.4.101	0	0	Sunnyvale,CA	www.troposnetworks.com	SM_N_6
<input type="checkbox"/>	93008b6	10.88.4.104	0	0	Sunnyvale,CA	www.troposnetworks.com	SM_N_4

- Some tables support multiple contiguous selection. Select the checkbox for the first chosen entry and then hold down the Shift key while selecting the checkbox for the last chosen entry.

Using Router Details Windows

Some of the panels list individual routers using an ID link.

Do one of the following to open a router details window:

- Click an underlined router ID in any of web interface panels.
- Enter the router IP address in the Find Device field at the top of the screen, and click **GO**.

This window contains the following tabs:

- Gateway/Node Information---View summary information about the router.

Device Information		Configurator	Map	Performance History
System				
Name	Router A5			
Serial Number	109055			
SSID	sunnyvale			
Type	Gateway			
Location	Pastoria Pole			
Lat / Long	37.394509 / -122.032968			
Model	7320			
Software Version	7.5.0.3			
Network				
Interface	IP	MAC	Channel	
2.4 GHz	172.20.125.236	00:0d:97:00:c0:24	11	
5.8 GHz	172.20.125.235	00:0d:97:00:c0:65	161	
LAN/Backhaul	172.20.125.234	00:0d:97:16:00:f8		

- Configurator---Open the Configuration Utility for the router.
- Map---Open a Google Maps window showing the router location.

- Performance History---View recent performance statistics for the router.
The following screen shows an example for a fixed gateway or node.

Performance Information for Gateway 172.20.125.99 [Export Data](#)

Time	Upstream (Mbps)	Downstream (Mbps)	Latency (ms)	Packet Loss	Noise	Tx Rate (Kbps)	Rx Rate (Kbps)	# Associated Clients	# Routed Clients	# Neighbors	# Cluster Routed Clients	Cluster Node Count	# Interfering gateways	Channel
Feb 14 07:00-08:00	N/A	N/A	N/A	100.0%	-101.9	20.1	129.2	N/A	N/A	10	0	2	2	11
Feb 14 06:00-07:00	N/A	N/A	N/A	100.0%	-101.86	18.2	130.4	N/A	N/A	10	0	2	2	11

Discovery

Discovery is the formal process by which Tropos Control recognizes and establishes router connections. To take advantage of Tropos Control management capabilities, the Tropos gateways in the network must be discovered.

You can configure the system to perform discovery in the following ways:

- Auto discovery---See [“Using Router Auto Discovery”](#) on page 145.
- Manual discovery---See [“Updating the Router Database”](#) on page 61.
- Discover from file---See [“Discovering Gateways from a File”](#) in the next section.

Discovering Gateways from a File

Data on the gateways in the network is stored on the Tropos Control server in the following location and in the indicated format:

```
/<installdirectory>/ems/conf/server/discover_devices.txt
```

Format:

```
<device ip>=<snmp port>;<read only community>;<readwrite community>;<management station ip>;<trap community>;<trap port>;<mesh id>;<router auth key>
```

Example:

```
172.20.125.60=161;public;private;192.168.128.96;public;162;123412341212341234;123412341212341234
```

Each hour, the Tropos Control server automatically checks the discover_devices.txt file, discovering all the gateways listed in the file that have not already been discovered and that have registered the Tropos Control server. In large networks with numerous gateways, saving discovery parameters to a file can streamline the process of performing discovery, and provides for easy rediscovery if new software is installed.

4 Viewing Network Health Information

This chapter describes the Network Health panels in the web interface and how network health thresholds are defined.

Chapter contents:

- [Preparing to Access the Network Health Panels](#)
- [Using the Dashboard](#)
- [Using the Network Optimization Panels](#)
- [Using the Client Optimization Panels](#)
- [Using the Voice Optimization Panels](#)
- [Using the Device Ping Utility](#)
- [Modifying Network Health Thresholds](#)

Preparing to Access the Network Health Panels

If client side certificates are enabled on the routers, you must configure the `/<installdirectory>/ems/networkhealth/certificateconf` file to support Network Health. Configure the following parameters in the file (the file contains an example for each):

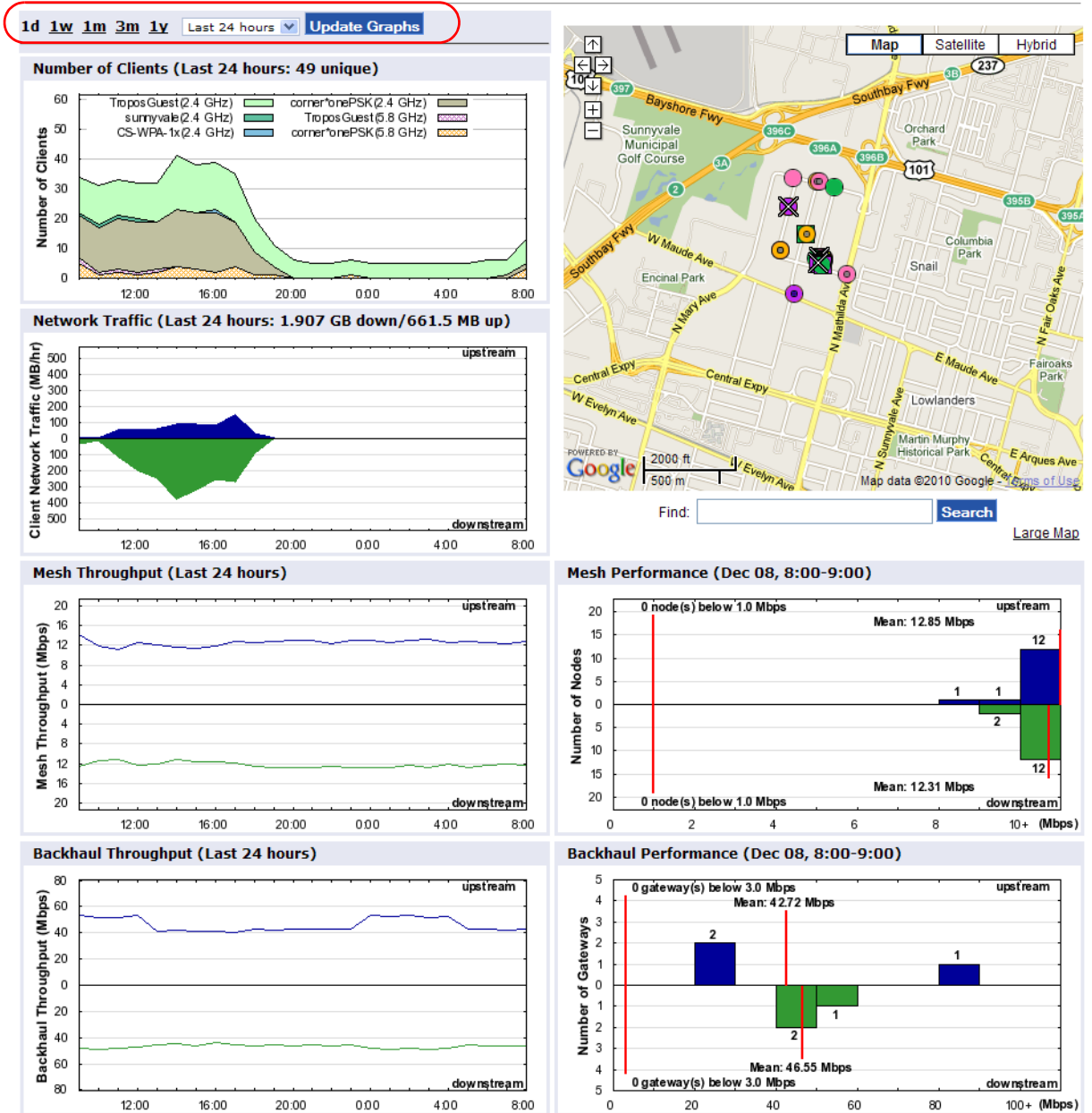
- CIPHER - Signature algorithm (for example, SHA1)
- CLIENTCERT - location of certificate file
- CLIENTCERTPASS - password for the key store file
- CACERTKEY - location of the key file

Using the Dashboard

When you access the web interface, the Dashboard opens. The Dashboard presents summary network status and performance information. The top line shows the total number of clients, nodes, and gateways in the network. It also shows the number of gateways that are currently operating as nodes, and vice versa. You can return to the Dashboard at any time by choosing **Dashboard** from the side menu on the Network Health tab.

FIGURE 6 Dashboard

14 clients 24 nodes (2 unreachable) 6 gateways (1 unreachable) (2 gateways operating as nodes)



You can display information for the past day (1d), week (1w), month (1m), three months (3m), or year (1yr) by clicking the appropriate link near the top of the page (see circled area in [Figure 6](#)). If you choose the days option, you can view historical information for a specific time period within the past week by selecting the time period (last 24 hours - 6 days ago) from the drop-down list.

Graphs display the following information:

- Number of Clients---Total number of distinct clients, color-coded and labeled by SSID.
- Client Network Traffic---Total upstream (blue) and downstream (green) traffic for all clients (MB).
- Mesh Throughput---Average Upstream (blue) and downstream (green) wireless throughput between nodes and the gateway (Mbps).
- Backhaul Throughput---Average upstream (blue) and downstream (green) throughput between the gateway and the Tropos Control server (Mbps).
- Mesh Performance---Performance of the mesh for the past hour (Mbps).
- Backhaul Performance---Backhaul performance for the past hour (Mbps).

Viewing Geographic Maps

You can view network routers in geographic context by using the Google Maps area on the right side of the dashboard.



Note

If a map is not visible when you open the dashboard, you must first obtain a map key from Google. This needs to be done only once. Make sure you have Internet connectivity from your browser.

Obtain the Google maps key

1. Open the web interface.
2. Click the **Google Map API Key Signup** link in the Google maps area of the dashboard.

The Google Maps API key for this website was not found. Please generate a key for the website at [Google Map API Key Signup](#) and **upload** the key to your website, then **refresh** the page.

3. Enter the IP address and port of the Tropos Control server:
4. `https://<ipaddress>:8443`

I have read and agree with the terms and conditions ([printable version](#))

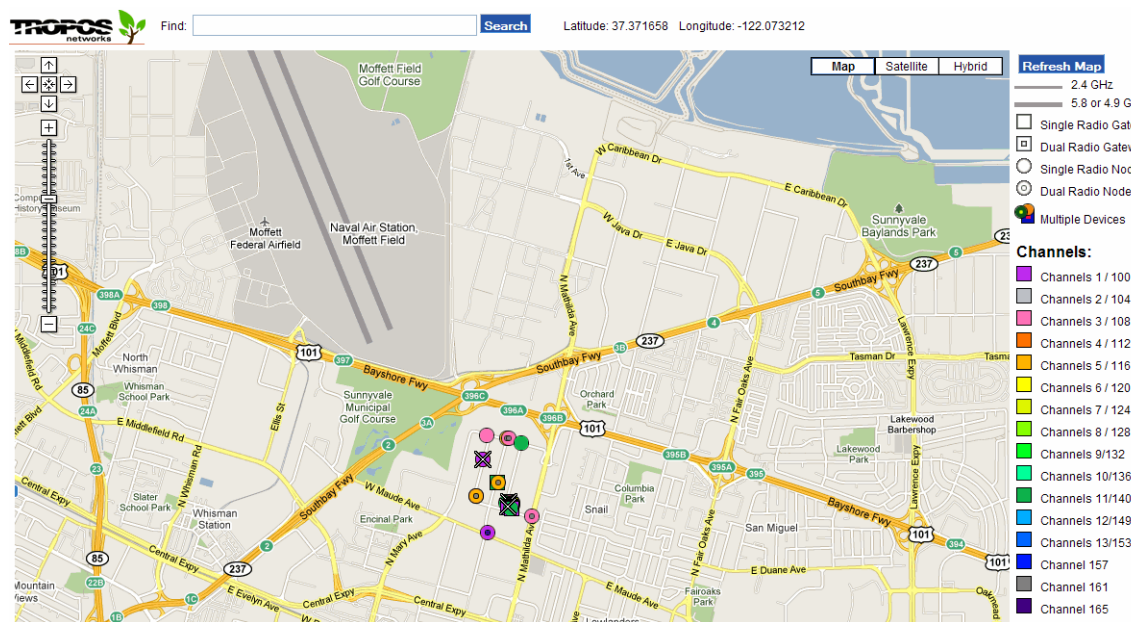
My web site URL:

5. Select the checkbox to accept the terms and conditions for use of the key, and click **Generate API Key**.

6. The key is generated and displayed.
7. Copy the key.
8. Click **Upload** in the Google Map area of the Tropos Control web interface.
9. Past the key into the space provided, and click **Upload**.

Please upload the Google Map API Key to server:

10. Click **Close** to close the upload window.
11. Click **refresh** to reopen the page and display the map.



Using the Geographic Maps

Each router is represented as an icon on the map. The following conventions apply to the maps:

- Square icons represent gateways.
- Round icons represent nodes, include mobile nodes.
- Dual radio routers have a smaller square or circle inside.
- Routers that are currently unreachable are shown with an X.
- Routers and links sharing the same channel are shown in the same color.
- Thin lines represent 2.4 GHz connections; thick lines represent 4.9, 5.4, or 5.8 GHz connections.
- If routers are clustered on the map, you may need to zoom in to display the individual icons.
- If there are no Tropos routers shown on the map, the following message appears:


“We are sorry, but we don’t have maps at this zoom level for this region.”

If you see this message, zoom out and pan as necessary to bring your network into view.

You can perform the following operations:

- View summary information about a router by clicking the router icon. Click the icon once to change the zoom level and then click the router icon again to display the summary information.
- Find a specific router by entering the IP address and clicking **Search**.
- Zoom in or out or pan by using the Google Maps controls.
- Observe updates to the map when a mobile router moves.
- View a standard map, satellite image, or hybrid map and satellite image by using the Google Maps controls.
- View a larger version of the map by clicking the **Large Map** link below the map area.
- View detailed information about a router by clicking the underlined IP address in the bubble. The Gateway/Node information window (Figure 7) opens to show additional information.

FIGURE 7 Gateway/Node Information Window

Device Information			
Configurator		Map	Performance History
System			
Name	SV-PastoriaPole		
Serial Number	49009		
SSID	sunnyvale		
Type	Node		
Location	Pastoria		
Lat / Long	37.394501 / -122.032877		
Model	5320		
Software Version	7.5.0.4		
Network			
Interface	IP	MAC	Channel
2.4 GHz	172.20.125.65	00:0d:97:00:50:b8	5
5.8 GHz	172.20.125.153	00:0d:97:00:50:b9	161

You can perform these actions from the Gateway/Node information window:

- Click **Configurator** to open the Configuration Utility. For more information on using the utility, see the *Tropos Networks Configuration Guide*.
- Click **Map** to open a standard Google Maps window that shows the location of the router.

- Click **Performance History** to open a window containing recent performance history for the router.

Performance Information for Node 172.20.125.97 Export Data

Time	Upstream (Mbps)	Downstream (Mbps)	Latency (ms)	Packet Loss	Noise	PSP	RPSP	Tx Rate (Kbps)	Rx Rate (Kbps)	# Associated Clients	# Routed Clients	# Neighbors	Hop Count
06/27 13:00-14:00	3.3	2.3	13.3	0.0%	-101.33	93%	57%	10.5	19.2	3	2	10	1.0
06/27 12:00-13:00	3.6	2.7	5.3	3.0%	-101.56	92%	58%	11.0	19.6	6	4	9	1.0
06/27 11:00-12:00	3.7	2.4	8.4	0.0%	-101.7	88%	59%	84.0	89.1	5	5	9	1.0
06/27 10:00-11:00	3.8	2.2	14.9	0.0%	-101.68	89%	60%	41.6	50.2	6	6	9	1.0
06/27 09:00-10:00	4.5	4.1	3.3	0.0%	-101.69	95%	77%	11.9	24.8	4	3	10	1.0
06/27 08:00-09:00	6.9	5.0	1.8	0.0%	-101.61	96%	77%	13.2	28.5	2	2	10	1.0
06/27 07:00-08:00	6.8	5.1	3.4	0.0%	-101.64	96%	79%	12.4	30.1	1	1	10	1.0
06/27 06:00-07:00	6.6	5.8	2.9	0.0%	-101.69	96%	79%	12.9	30.7	0	N/A	10	1.0

- Click **Export** in the Performance History window to save the performance history in csv format.

Using the Network Optimization Panels

The Network Optimization panels present statistics to help assess current and recent router behavior and performance.

Thresholds are applied to a variety of performance metrics to determine whether problems exist in the network. If the problem thresholds are not met, the cell is listed as problem free. You can adjust the thresholds based on the network and user preferences for each network health report by selecting from the drop-down lists below the optimization table (see figure). To save the thresholds as defaults, select **Save above thresholds as default thresholds** and click **Submit**.

Failure time threshold: hours Check history for

Status Key:
Excellent: failure percentage=0%
Good: 0% < failure percentage <= 5%
Marginal: % < failure percentage <= 10%
Poor: % < failure percentage <= 25%
Bad: % < failure percentage

Save above thresholds as default thresholds

Access the panels

- Open the Network Health tab and choose **Network Optimization** on the side menu. The summary Optimization panel opens (Figure 8).

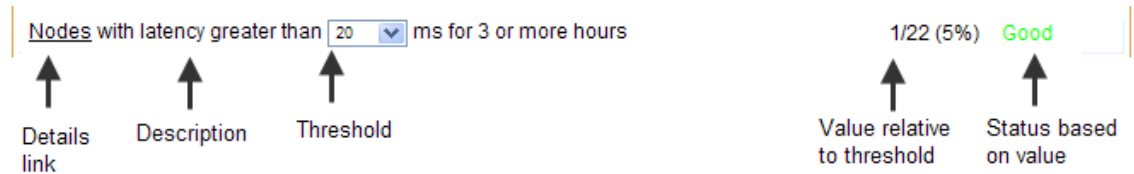
FIGURE 8 Network Optimization Panel

Submit		
Missing Data (Dec 07 09:00 - Dec 08 09:00)		
Routers with missing data for <input type="text" value="4"/> or more hours	3/28 (11%)	Poor
Gateways with missing backhaul throughput data for <input type="text" value="3"/> or more hours	2/6 (33%)	Bad
Nodes with missing mesh throughput data for <input type="text" value="3"/> or more hours	6/22 (27%)	Bad
Backhaul Performance (Dec 07 09:00 - Dec 08 09:00)		
Gateways with downstream throughput less than <input type="text" value="3.0"/> Mbps for 3 or more hours	0/6 (0%)	Excellent
Gateways with upstream throughput less than <input type="text" value="3.0"/> Mbps for 3 or more hours	0/6 (0%)	Excellent
Gateways with backhaul utilization exceeding <input type="text" value="300"/> MB/hour for 3 or more hours	0/6 (0%)	Excellent
Devices with backhaul latency greater than <input type="text" value="10"/> ms for 3 or more hours	0/6 (0%)	Excellent
Devices with backhaul packet loss greater than <input type="text" value="5%"/> for 3 or more hours	4/6 (67%)	Bad
Mesh Performance (Dec 07 09:00 - Dec 08 09:00)		
Nodes with downstream throughput less than <input type="text" value="1.0"/> Mbps for 3 or more hours	0/22 (0%)	Excellent
Nodes with upstream throughput less than <input type="text" value="1.0"/> Mbps for 3 or more hours	0/22 (0%)	Excellent
Nodes with packet loss rate greater than <input type="text" value="10%"/> for 3 or more hours	1/22 (5%)	Good
Nodes with latency greater than <input type="text" value="20"/> ms for 3 or more hours	1/22 (5%)	Good
Nodes with traffic exceeding <input type="text" value="100"/> MB/hour for 3 or more hours	2/22 (9%)	Marginal
Routers with <input type="text" value="1"/> or more 2.4 GHz channel changes per hour for 3 or more hours	0/28 (0%)	Excellent
Routers with <input type="text" value="1"/> or more 5.8 GHz channel changes per hour for 3 or more hours	1/28 (4%)	Good
Routers with 2.4 GHz noise level greater than <input type="text" value="-85"/> dBm for 3 or more hours	1/28 (4%)	Good
Routers with 5.8 GHz noise level greater than <input type="text" value="-85"/> dBm for 3 or more hours	0/28 (0%)	Excellent
Routers with 2.4 GHz airtime greater than <input type="text" value="80%"/> for 3 or more hours	0/28 (0%)	Excellent
Routers with 5.8 GHz airtime greater than <input type="text" value="80%"/> for 3 or more hours	0/28 (0%)	Excellent
Nodes with default PSP less than <input type="text" value="30.0%"/> for 3 or more hours	0/22 (0%)	Excellent
Nodes with default RPSP less than <input type="text" value="30.0%"/> for 3 or more hours	0/22 (0%)	Excellent
Nodes that are flapping with PSP less than <input type="text" value="30.0%"/> for 3 or more hours	0/22 (0%)	Excellent
Nodes that are flapping with RPSP less than <input type="text" value="30.0%"/> for 3 or more hours	0/22 (0%)	Excellent
Nodes with hop count of <input type="text" value="3"/> or more for 3 or more hours	0/22 (0%)	Excellent
Routers with <input type="text" value="20"/> or more neighbors (in 2.4 GHz channel) for 3 or more hours	0/28 (0%)	Excellent
Routers with <input type="text" value="40"/> or more 2.4 GHz associated clients for 3 or more hours	0/28 (0%)	Excellent
Routers with <input type="text" value="40"/> or more 5.8 GHz associated clients for 3 or more hours	0/28 (0%)	Excellent
Routers with <input type="text" value="40"/> or more 2.4 GHz routed clients for 3 or more hours	0/28 (0%)	Excellent
Routers with <input type="text" value="40"/> or more 5.8 GHz routed clients for 3 or more hours	0/28 (0%)	Excellent
Gateways with <input type="text" value="20"/> or more nodes for 3 or more hours	0/6 (0%)	Excellent
Gateways with <input type="text" value="10"/> or more interfering gateways (in 2.4 GHz channel) for 3 or more hours	0/6 (0%)	Excellent
Clusters with <input type="text" value="150"/> or more clients for 3 or more hours	0/6 (0%)	Excellent

The Network Optimization panel presents summary statistics for the following categories:

- Missing Data---Nodes, gateways, and all routers with errors in transmitting or receiving data.
- Backhaul performance---Gateways with throughput, latency, packet loss, and utilization relative to specified thresholds.
- Mesh performance---Mesh links, nodes, gateways, and all routers with performance statistics relative to specified thresholds.

Each row in the network optimization panel describes the statistic, the current value (ratio and percentage), and a description of the status, as in the following example.



This example indicates that 1 of 22 routers have had latency greater than 20ms for 3 or more hours (the other routers have had lower latency), which is considered good performance for this metric.

Change status key or thresholds

1. Choose values from any of the pull-down lists on the optimization panel. To use the thresholds as the new defaults, select **Save above thresholds as default thresholds**.
2. Click **Submit**.

View network optimization details

- Click the underlined link for the parameter to open the associated details panel.

Each panel includes pull-down lists for setting thresholds, and a table containing statistics for each hour in the selected time period. For 24-hour details, green numbers indicate that the data is within threshold for that hour, red indicates that the data violates the threshold, and black indicates that no data is available.

Threshold settings

Nodes with traffic exceeding MB/hour for or more hours : 2 (Dec 07 09:00 - Dec 08 09:00)

Check history for [Show Failed Records](#) [Show All Records](#) [Show Map](#)

IP	Last Hour Average	24 Hour Average	# Failed Hours	24 Hour Details																							
172.20.125.189	22.47	77.02	6	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8
172.20.125.65	36.86	52.75	3	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8

Past hour to past 24 hours measured from current local time

↑ Details link

↑ Average value for last hour

↑ Average value for last 24 hours

↑ # hours of threshold violation

↑ No data available for this hour

↑ Data this hour violates threshold (red)

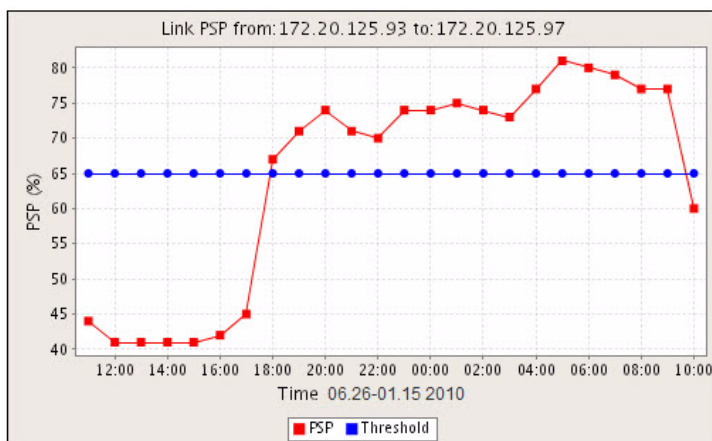
↑ Data this hour within threshold (green)

↑ Link to graph

You can do the following on this panel:

- Choose thresholds from the pull-down lists.
- Click **Show Fail Records** to display all records for routers that violated the threshold during the specified period.
- Click **Show All Records** to display all records for the specified period.
- Click **Show Maps** to open a Google Maps window showing the router location.
- Click an underlined router link to open an information window for the router. For more information, see the description of the Gateway/Node Information window in “Using the Geographic Maps” on page 28.

- Click the graph icon on the right to display a graph of the data. For example, the next graph shows link PSP data for a gateway.



Using the Client Optimization Panels

The Client Optimization panels present detailed statistics on client performance.

Access the panels

- Open the Network Health tab and choose **Client Optimization** on the side menu.

The Client Optimization panel (Figure 9) opens.

FIGURE 9 Client Optimization Panel

Optimization	Value	Status
Clients with SNR less than 10 dB for 3 or more hours	0/49 (0%)	Excellent
Clients with signal less than -75 dBm for 3 or more hours	5/49 (10%)	Poor
Clients with noise over -85 dBm for 3 or more hours	0/49 (0%)	Excellent
Clients with traffic over 100 MB/hour for 3 or more hours	1/49 (2%)	Good
Clients rate limited for more than 5 mins for 3 or more hours	0/49 (0%)	Excellent

Failure time threshold: 3 hours Check history for: Last 24 hours

Status Key:
Excellent: failure percentage=0%
Good: 0% < failure percentage <= 5%
Marginal: 5% < failure percentage <= 10%
Poor: 10% < failure percentage <= 25%
Bad: 25% < failure percentage

Save above thresholds as default thresholds

Submit

Each row in the client optimization panel describes the statistic, the current value (ratio and percentage) and a description of the status, as in the following example:

Client Performance (May 16 13:00 - May 17 13:00)

Optimization	Value	Status
Clients with SNR less than <input type="text" value="10"/> dB for 3 or more hours	1/78 (1%)	Good
Clients with signal less than <input type="text" value="-75"/> dBm for 3 or more hours	2/78 (3%)	Good
Clients with noise over <input type="text" value="-85"/> dBm for 3 or more hours	0/78 (0%)	Excellent

↑ Details link ↑ Threshold ↑ Value relative to threshold ↑ Status based on value

Change status key or thresholds

1. Choose values from any of the pull-down lists on the optimization panel. If you want to use the thresholds as the new defaults, select **Save above thresholds as default thresholds**.
2. Click **Submit**.

View client optimization details

- Click the underlined link for the parameter to open the associated details panel.

Each panel includes pull-down lists for setting thresholds, and a table containing statistics for each hour in the selected time period. For the 24-hour details, green numbers indicate that the data is within threshold for that hour, red indicates that the data violates the threshold, and black indicates that no data is available.

Threshold settings

Clients with signal less than dBm for or more hours : 2 (Jan 27 08:00 - Jan 28 08:00)

Check history for [Show Failed Records](#) [Show All Records](#)

Client MAC Address	Interface	Last Hour Average	24 Hour Average	# Failed Hours	24 Hour Details
IntelCorpo:C8:AE:85	2.4 GHz	-85.0	-79.33	13	8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 0 1 2 3 4 5 6 7
ArcadvanTe:85:87:B0	2.4 GHz	-78.3	-81.43	6	8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 0 1 2 3 4 5 6 7

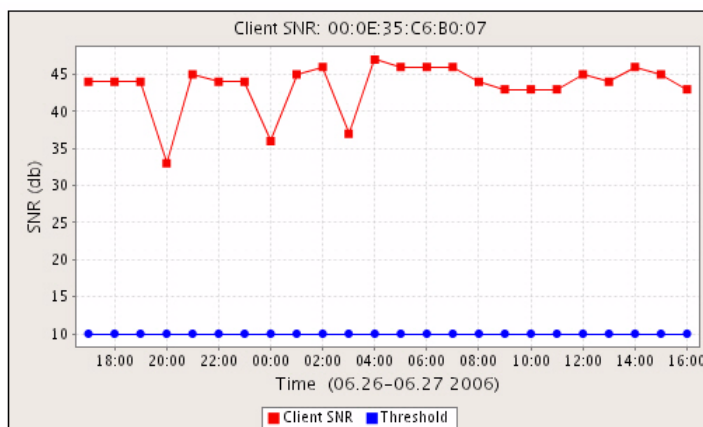
↑ Client details link ↑ Averages ↑ Total # hours of threshold violation ↑ Data for this hour violates threshold ↑ No data for this hour ↑ Data for this hour within threshold ↑ Graph icon

Past hour to past 24 hours measured from current local time

You can do the following on this panel:

- Choose thresholds from the pull-down lists.
- Click **Show Fail Records** to display all records for routers that violated the threshold during the specified period.
- Click **Show All Records** to display all records for the specified period.

- Click the graph icon on the right to display a graph of the data.



- Click an underlined Client MAC address link to open the Client Query window for the selected client (see next section). The MAC addresses include prefixes.

Understanding the Client Query Reports

You can access the detailed client information by clicking any of the MAC address links on the Client Optimization page. The Client Query report presents information about the client's network activity over the past 24 hours.

Client Query		Troubleshooting							
Client/CPE Average History Information									
MAC Address	00:19:d2:7b:61:b3	Clients behind CPE							
IP Address	172.20.125.187	index	IP Address MAC Address						
Rx Kbps	6	1	172.20.125.187 00:19:D2:7B:61:B3						
Tx Kbps	1								
Signal	-47								
Noise	-97								
SNR	50								
Visited Node/Gateway History Average Information									
Type	Node IP	Node ID	Duration (min)	Signal	Noise	SNR	Rx Kbps	Tx Kbps	Location
Node	172.20.125.96	19040	95	-47	-99	52	6	1	Ozone Conference Room
Gateway	172.20.125.128	49014	16	-49	-91	42	7	2	Systemt
Detailed Data (2008.10.14-2008.10.15)									

Table 6 describes information summarized in the Client/CPE Average History Information area at the top of the panel.

TABLE 6 Client/CPE Average History Information

Item	Description
MAC Address	MAC address of the client machine about which to be reported
IP Address	IP address of the client machine about which to be reported
Rx Kbps	Average Kbps received over the past 24 hours
Tx Kbps	Average Kbps transmitted over the past 24 hours
Signal	Average signal strength over the past 24 hours (dB)
Noise	Average noise level over the past 24 hours (dB)
SNR	Average signal-to-noise ratio over the past 24 hours

The Visited Node/Gateway History Average Information area lists statistics for node and gateway associations. Each row presents information for a node or gateway to which the client associated over the past 24 hours. [Table 7](#) lists the information reported for each associated node and gateway.

TABLE 7 Visited Node/Gateway History Average Information

Item	Description
Type	Node or gateway.
Node IP	IP address of the node or gateway. To view this information, click the underlined line to open the Configuration Utility for the particular node or gateway.
Node ID	Tropos identifier for the node or gateway.
Duration (min)	Total number of minutes that the client was associated with the node or gateway in the past 24 hours.
Signal	Average signal strength for the period of association (dB). Click the underlined line to open a signal and noise graph.
Noise	Average signal strength for the period of association (dB).
SNR	Average signal strength for the period of association.
Rx Kbps	Average Kbps received for the period of association. Click the underlined link to open a graph of the data.
Tx Kbps	Average Kbps transmitted over the past 24 hours.
Location	GPS coordinates of the node or gateway, if available.

The Detail Data area, which opens when you click the double arrows on the Detail Data bar, shows the pattern of associations over the past 24 hours.

Detailed Data (2008.10.14-2008.10.15)											
Node IP	Signal	Noise	SNR	Rx Kbps	Tx Kbps	CPE MAC	ESSID	VLAN ID	Channel	Duration (min)	TimePeriodWithDate
172.20.125.128	-49	-91	42	1	2	00:19:D2:7B:61:B3	TroposGuest		1	13	10/14 16:00-17:00
172.20.125.96	-46	-99	53	5	1	00:19:D2:7B:61:B3	cornerstonePSK		3	42	10/14 16:00-17:00
172.20.125.96	-48	-99	51	8	2	00:19:D2:7B:61:B3	cornerstonePSK		3	53	10/14 15:00-16:00
172.20.125.128	-49	-94	45	35	3	00:19:D2:7B:61:B3	TroposGuest		1	3	10/14 14:00-15:00

Each row represents a period of association with one of the nodes or gateways listed in the Visited Node/Gateway area.

Note

If a client associates with more than one node in a given hour, then there will be multiple entries for that time period in the listing.

Table 7 lists the information reported for association.

TABLE 8 Detail Data

Item	Description
Node IP	IP address of the node or gateway. Click the underlined line to open the Configuration Utility for the particular node or gateway.
Signal	Average signal strength for the period of association (dB). Click the underlined line to open a signal and noise graph.
Noise	Average signal strength for the period of association (dB)
SNR	Average signal strength for the period of association
Rx Kbps	Average Kbps received for the period of association. Click the underlined link to open a graph of the data
Tx Kbps	Average Kbps transmitted over the past 24 hours
CPE MAC	MAC address of any customer premise equipment (CPE) between the client and the node or gateway
ESSID	ESSID of the node or gateway
VLAN ID	ID of the VLAN to which the node or gateway belongs, if applicable
Channel	Channel used for communication with the client
Duration (min)	Total number of minutes that the client was associated with the node or gateway in the past 24 hours.
Time Period With Date	Interval of association, with the date (mm/dd) followed by start and end times.

To display detailed client statistics and events, click **Troubleshooting**. Use the time filters at the top of the page to restrict the display to a specified time period.

Client MAC or IP Address:

Time Filter: From: ... To: ...

Troubleshooting (Jan 25 2010 17:01 - Jan 26 2010 17:01)

MAC Address: 00:11:6E:80:E5:84 IP Address: 172.20.126.26

Statistics (Top 100 entries)

Time	Interface	Gateway	Next Hop	Client IP	SNR (dB)	Latency (ms)	ARP PSP (%)	Tx Num Ucast ARP	RSSI (dBm)	Rx Rt Limit	Tx Rt Limit	Rx Airtime (%)	Tx Airtime (%)	Rx Frames	Tx Frames	Rx Bytes	Tx Bytes	Rx Noise (dBm)
01/26/2010 16:00:00	wlan0	172.20.125.128	172.20.125.128	172.20.126.26	59	1.58	100	2	-35	0	0	0.001	0.002	2	2	128	136	-94
01/26/2010 15:59:00	wlan0	172.20.125.128	172.20.125.128	172.20.126.26	58	3.30	100	2	-36	0	0	0.001	0.002	2	2	128	136	-94
01/26/2010 15:58:00	wlan0	172.20.125.128	172.20.125.128	172.20.126.26	58	1.22	100	2	-35	0	0	0.004	0.0076	8	8	866	1001	-94
01/26/2010 15:57:00	wlan0	172.20.125.128	172.20.125.128	172.20.126.26	59	1.86	100	2	-35	0	0	0.001	0.0039	2	2	128	136	-94
01/26/2010 15:56:00	wlan0	172.20.125.128	172.20.125.128	172.20.126.26	59	4.46	0	0	-34	0	0	0.0102	0.0117	18	18	4774	7657	-94
01/26/2010 15:55:00	wlan0	172.20.125.128	172.20.125.128	172.20.126.26	58	4.46	100	2	-35	0	0	0.0034	0.0046	7	7	618	916	-94
01/26/2010 15:54:00	wlan0	172.20.125.128	172.20.125.128	172.20.126.26	59	5.82	100	1	-35	0	0	0.0005	0.0029	1	1	64	68	-94
01/26/2010 15:53:00	wlan0	172.20.125.128	172.20.125.128	172.20.126.26	59	10.64	50	2	-35	0	0	0.001	0.002	2	2	128	136	-94
01/26/2010 15:52:00	wlan0	172.20.125.128	172.20.125.128	172.20.126.26	59	1.56	100	2	-35	0	0	0.001	0.002	2	2	128	136	-94
01/26/2010 15:51:00	wlan0	172.20.125.128	172.20.125.128	172.20.126.26	59	3.25	100	1	-34	0	0	0.0025	0.0031	5	5	488	508	-94
01/26/2010 15:50:00	wlan0	172.20.125.128	172.20.125.128	172.20.126.26	59	5.50	100	2	-35	0	0	0.001	0.002	2	2	128	136	-94

Using the Voice Optimization Panels

The Voice Optimization panels present detailed statistics on voice calls within the network. To access the panel, open the Network Health tab and choose **Voice Optimization** on the side menu.

Each row in the voice optimization panel describes the statistic, the current value (ratio and percentage) and a description of the status.

Change status key or thresholds

1. Choose values from any of the pull-down lists on the optimization panel. If you want to use the thresholds as the new defaults, select **Save above thresholds as default thresholds**.
2. Click **Submit**.

View voice optimization details

- Click the underlined link for the parameter to open the associated details panel.

Each panel includes pull-down lists for setting thresholds, and a table containing statistics for each hour in the selected time period. For the 24-hour details, green numbers indicate that the data is within threshold for that hour, red indicates that the data violates the threshold, and black indicates that no data is available.

You can do the following on this panel:

- Choose thresholds from the pull-down lists.
- Click **Show Fail Records** to display all records for routers that violated the threshold during the specified period.
- Click **Show All Records** to display all records for the specified period.
- Click the graph icon on the right to display a graph of the data.
- Click an underlined Client MAC address link to open the Client Query window for the selected client (see next section).

Using the Device Ping Utility

The Device Ping Utility panel reports on ping operations for specified devices or for all discovered routers. The Ping utility is off by default, but it can be turned on from the web interface.

By default, the devices included in the ping list are listed in the `device_pinglist.txt` file, which is found in the following location:

`<installdirectory>/ems/conf/tropos/device_pinglist.txt`. The default file contents are as follows:

```
# number of threads to do ping
number_threads=20
# interval between every ping cycle, in seconds
ping_interval=20
# number of retries
retries=1
# timeout for each ping request in seconds
timeout=1
# list of IPAddress need to be pinged here
# for gateway use: IPAddress=G,<backhaul IPAddress>
# example: 192.168.128.3=G,192.168.128.4
# for node use: IPAddress=N
# example: 192.168.128.5=N
```

Add specific devices to the ping list

1. Open the `device_pinglist.txt` file.
2. Enter the IP addresses of the devices, according to the format given in the comment text. N refers to node, G to gateway, and B to any non-Tropos device.
3. Save the file.

The entered devices will now appear in the device ping list.

View device ping results

1. Open the Network Health tab and choose **Device Ping Utility** from the side menu. The Device Ping Utility panel (Figure 10) opens.

FIGURE 10 Device Ping Utility Panel

Device Ping Utility

Total: 3 Gateways, 9 Nodes, 0 Backhauls. Total down devices: 0
(Timeout:1s, Retries:1, Interval:20s. Count started at:06/27/2006 12:15.

Device IP	Type	Status	Success Rate	Last Ping Time	Backhaul IP	Failed Ping Count	Total Ping Count
172.20.125.84	node	Up	100%	06/27/2006 12:37		0	63
172.20.125.95	gateway	Up	100%	06/27/2006 12:37		0	63
172.20.125.86	node	Up	100%	06/27/2006 12:37		0	63
172.20.125.97	node	Up	100%	06/27/2006 12:37		0	63
172.20.125.80	node	Up	100%	06/27/2006 12:37		0	63
172.20.125.83	node	Up	100%	06/27/2006 12:37		0	63
172.20.125.81	node	Up	100%	06/27/2006 12:37		0	63
172.20.125.165	node	Up	100%	06/27/2006 12:37		0	63
172.20.125.98	node	Up	100%	06/27/2006 12:37		0	63
172.20.125.135	gateway	Up	100%	06/27/2006 12:37		0	63

2. Perform any of the following operations:
 - Click **Start Ping** to start performing ping operations. (The button is visible only if ping operations are currently off.)
 - Click **Stop Ping** to stop performing ping operations. (The button is visible only if ping operations are currently on.)
 - Click **Clear Counter** to clear current ping counts.
 - Click **Turn Off Refresh** to prevent information from being automatically refreshed as new ping results come in. (This button is visible only if refresh is currently turned on.)
 - Click **Turn On Refresh** to allow information to be automatically refreshed as new ping results come in. (This button is visible only if refresh is currently turned off.)
 - Click **Add IPs in topo DB** to add all the discovered gateways and nodes to the list of devices to which ping messages are sent. Devices specified in the device_pinglist.txt file will continue to be included.
 - Click **Remove topo IPs** to remove all the discovered gateways and nodes the list of devices to which ping messages are sent. Devices specified in the device_pinglist.txt file will continue to be included.

The Device Ping Utility table includes the following columns of information:

TABLE 9 Device Ping Utility Table

Column	Description
Device IP	IP address of device
Type	Gateway, node, or backhaul
Status	Up (responding to ping commands) or down (not responding)

TABLE 9 Device Ping Utility Table (*continued*)

Column	Description
Success Rate	Percentage of successful ping responses
Last Ping Time	Time last ping request was sent
Backhaul IP	IP address of device used to check backhaul connectivity
Failed Ping Count	Number of failed ping attempts
Total Ping Count	Total number of ping attempts

Modifying Network Health Thresholds and Report Options

The default Network Health thresholds and report selection options are appropriate for most deployments; however, you can modify them, if necessary, by editing the appropriate configuration files.

Modifying Network Health Thresholds

Thresholds are applied to a variety of performance metrics to determine whether problems exist in the network. If the problem thresholds are not met, the cell is listed as problem free.

The thresholds are set in the file `threshold.txt`, which is in the following location:

```
<installdirectory>/ems/networkhealth
```

If you choose to edit the file, be sure to maintain a backup copy with the default values.

Default file contents

```
# used for worst used link
# if linkpsp is below MINUSEDLINKPSP or MINUSEDLINKRPSP and the link
activity is above the MINUSEDLINKACTIVITY
# this link will be included into the Lowest used link
# link activity defined as the link was seen by node for a given hour.
# example: linkA was in the node 20 minutes, it means that this link's
activity is 20/60 = 0.33
#
# MINUSEDLINKPSP values = 0..1
# MINUSEDLRPSP values = 0..1
# MIN
MINUSEDLINKPSP0.65
MINUSEDLINKRPSP0.65
MINUSEDLINKACTIVITY0
```

```
#
## used for deciding the redundant path
# if the linkpsp is > MINLINKACTIVITY and > MINLINKPSP, this link will
be counted as redundant path
#
MINLINKPSP0.65
MINLINKRPSP0.65
MINLINKACTIVITY0
#
# max hops is used to test if node should be put into highest hop count
# if hops is above this MAXHOPS, the node will be put into highest hop
count
MAXHOPS4
#
#
# is used for lowest psp
# if PSP is below this MINPSP, the node will be included into lowest
psp
# value between 0..1
MINPSP.65
#
#
# for lowest rpsp
# if rPSP is below this MINRPSP, the node will be included into lowest
rpsp
MINRPSP.65
#
#
# for high noise
# if noise is above this MAXNOISE, the node will be included into the
highest noise
MAXNOISE-80
#
# for reachability
# if the reachability is below this MINREACHABILITY, the node will be
included in the reachability category
#
MINREACHABILITY 97
#
# if client has snr below this LOWESTSNR, the client will be included
into the lowest SNR client
LOWESTSNR15
```

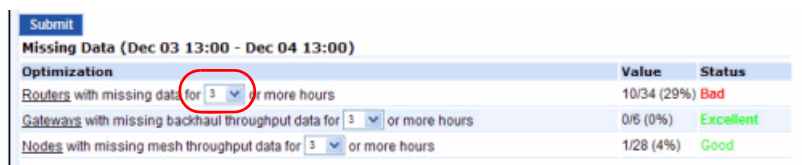
```

#
# if node has redundancy below this LOWESTREDUNDANCY, the node will be
# included into the Insufficient Redundancy
LOWESTREDUNDANCY2
#
#
# if node throughput (up/down) is lower than MINTHROUGHPUT(UP/DOWN),
# the node will be included into
# the Lowest estimated throughput
MINTHROUGHPUTUP 256
MINTHROUGHPUTDOWN 512

```

Modifying Report Options

Drop-down lists on the Network Optimization page determine the thresholds that apply to network optimization reports.



Optimization	Value	Status
Routers with missing data for 3 or more hours	10/34 (29%)	Bad
Gateways with missing backhaul throughput data for 3 or more hours	0/5 (0%)	Excellent
Nodes with missing mesh throughput data for 3 or more hours	1/28 (4%)	Good

These thresholds are controlled by the following files, which are located in `<installdirectory>/conf/server/`:

- `fhp_ems_networkhealth_report_threshold.properties.txt` -- determines the possible choices of values for the drop-drop list.
- `server_networkhealth_threshold.txt` -- determines the default value that is preselected in the drop-down list.

Note the following:

- If you choose to edit these file, be sure to maintain a backup copy with the default values.
- You can modify only the parameters that are in a given file. You cannot create new entries.
- If you change a default values in the `server_networkhealth_threshold.txt` file, make sure that the value is included in the possible selections for that parameter in the `fhp_ems_networkhealth_report_threshold.properties`.

The parameters in the files map to values and report names as follows.

- `messageCountOptions=10000,5000,2000,1000,500,300,200,150,100,50,10` - it is used by
 - message count report
- `BackhaulThroughputOptions=1.0,2.0,3.0,4.0,5.0,8.0,10.0,20.0,30.0,50.0,80.0` - it is used by
 - Gateways with downstream throughput report
 - Gateways with upstream throughput report

- ThroughputOptions=0.25,0.5,0.75,1.0,1.5,2.0,2.5,3.0,3.5,4.0,5.0 - it is used by
 - Nodes with downstream report
 - Nodes with upstream report
- LatencyOptions=2000,500,200,100,50,30,20,15,10,5,1 it is used by
 - Devices with backhaul latency report
 - Nodes with latency report
- LinkOptions=30,40,50,60,65,70,80,90,100 it is used by
 - Nodes with default PSP report
 - Nodes with default RPSP report
 - Nodes that are flapping with PSP report
 - Nodes that are flapping with RPSP report
- NoiseOptions=-150,-100,-90,-85,-80,-70,-60,-50 - it is used by
 - Clients with noise report
 - Routers with 2.4 GHz noise level report
 - Routers with 5.8 GHz noise level report
 - Routers with 24.9 GHz noise level report
- ChChangeOptions=1,2,3,4,5,6,7,8,9,10 - it is used by
 - Routers with 2.4 GHz channel change report
 - Routers with 5.8 GHz channel change report
 - Routers with 4.9 GHz channel change report
- AirtimeOptions=40,50,60,70,80,90 - it is used by
 - Routers with 2.4 GHz airtime report
 - Routers with 5.8 GHz airtime report
 - Routers with 4.9 GHz airtime report
- MissingDataOptions=1,2,3,4,6,8,12,24 -it is used by the:
 - Routers with missing data report
 - Gateways with missing backhaul report
 - Nodes with missing mesh throughput report
- voiceMissingDataOptions=1 - not currently used
- MissingDataOptionsWithZero=0,1,2,3,4,6,8,12,24 - not currently used
- nodeNumberOptions=1,2,3,4,5,6,7,8,9,10,15,20,30,40,50,60,70,80 - it is used by
 - Routers with 2.4 GHz associated client report
 - Routers with 5.8 GHz associated client report
 - Routers with 4.9 GHz associated client report
 - Routers with 2.4 GHz routed client report
 - Routers with 5.8 GHz routed client report
 - Routers with 4.9 GHz routed client report
 - Gateways with nodes report

- gatewayNumberOptions=1,2,3,4,5,10,15,20,25,30,35,40 - it is used by
 - Routers with neighbors report
 - Gateway with interfering gateways (in 2.4 GHz channel) report
- clientNumberOptions=1,5,10,30,50,70,80,90,100,120,150,200 - not currently used
- clusterclientNumberOptions=1,10,20,30,50,80,100,120,150,200,300,500 - it is used by
 - Clusters with clients report
- trafficOptions=50,80,100,120,150,200,300,500,1000,2000,3000,4000,5000,10000 - it is used by
 - Gateways with backhaul utilization report.
 - Nodes with traffic report
 - Clients with traffic report
- packetLossOptions=1,5,10,15,20,25,30,40 - it is used by
 - Devices with backhaul packet loss report
 - Nodes with packet loss report
- hopCountOptions=1,2,3,4,5,6,7,8,9,10 - it is used by
 - Nodes with hop count report
- signalOptions=-100,-90,-85,-80,-75,-70,-60,-50 - it is used by
 - Clients with signal report
- SNROptions=1,5,10,15,20,25,30,50,80 - it is used by
 - Clients with SNR report
- ClientRateLimitOptions=1,5,10,20,30,40,50 - it is used by
 - Clients rate limited report
- marginalOptions=3,5,8,10,15,20,25,30,40 - it is used as marginal options
- poorOptions=10,15,20,25,30,40,50,60,70 - it is used as poor options
- badOptions=15,20,25,30,40,50,60,70,80,90 - it is used as bad options
- voiceCallsOptions=0,1,2,3,4,5,6,7,8,9,10,25,50,100 - it is used by
 - Routers with number of voice calls
- voiceCallsDowngradedOptions=0,1,2,3,4,5,6,7,8,9,10,25,50,100 - it is used by
 - Routers with number of downgraded voice calls
- voiceCallsTimeOptions=0,10,30,60,120,240,360 - it is used by
 - Routers with total minutes voice calls

Default fhp_ems_networkhealth_report_threshold.properties file:

```
messageCountOptions=10000,5000,2000,1000,500,300,200,150,100,50,10
BackhaulThroughputOptions=1.0,2.0,3.0,4.0,5.0,8.0,10.0,20.0,30.0,50.0,
80.0
ThroughputOptions=0.25,0.5,0.75,1.0,1.5,2.0,2.5,3.0,3.5,4.0,5.0
LatencyOptions=2000,500,200,100,50,30,20,15,10,5,1
LinkOptions=30,40,50,60,65,70,80,90,100
```

```

NoiseOptions=-150,-100,-90,-85,-80,-70,-60,-50
ChChangeOptions=1,2,3,4,5,6,7,8,9,10
AirtimeOptions=40,50,60,70,80,90
MissingDataOptions=1,2,3,4,6,8,12,24
voiceMissingDataOptions=1
MissingDataOptionsWithZero=0,1,2,3,4,6,8,12,24
nodeNumberOptions=1,2,3,4,5,6,7,8,9,10,15,20,30,40,50,60,70,80
gatewayNumberOptions=1,2,3,4,5,10,15,20,25,30,35,40
clientNumberOptions=1,5,10,30,50,70,80,90,100,120,150,200
clusterclientNumberOptions=1,10,20,30,50,80,100,120,150,200,300,500
trafficOptions=50,80,100,120,150,200,300,500,1000,2000,3000,4000,5000,
10000
packetLossOptions=1,5,10,15,20,25,30,40
hopCountOptions=1,2,3,4,5,6,7,8,9,10
signalOptions=-100,-90,-85,-80,-75,-70,-60,-50
SNROptions=1,5,10,15,20,25,30,50,80
ClientRateLimitOptions=1,5,10,20,30,40,50
marginalOptions=3,5,8,10,15,20,25,30,40
poorOptions=10,15,20,25,30,40,50,60,70
badOptions=15,20,25,30,40,50,60,70,80,90
voiceCallsOptions=0,1,2,3,4,5,6,7,8,9,10,25,50,100
voiceCallsDowngradedOptions=0,1,2,3,4,5,6,7,8,9,10,25,50,100
voiceCallsTimeOptions=0,10,30,60,120,240,360

```

Default server_networkhealth_thresholds.txt file

```

nodeMissingThroughputDataThreshold=3
nodeNoiseThreshold=-85
clientNoiseThreshold=-85
nodeRoutedClientThreshold=40
nodeAssociateClientThreshold=40
clientSignalThreshold=-75
clientRateLimitThreshold=5
voiceCallsDowngradedThreshold=10
gatewayMissingThroughputDataThreshold=3
missingStatsThreshold=3
nodeAssociateClient1Threshold=40
gatewayTrafficThreshold=300
nodeTrafficThreshold=100
poorThreshold=10
voiceCallsThreshold=10
gatewayInterferingCountThreshold=10
clientSNRThreshold=10
nodeMissingDataThreshold=3
failureTimeThreshold=3

```



```
clientTrafficThreshold=100
nodeNoise1Threshold=-85
nodeNoise4_9Threshold=-85;
nodeAssociateClient4_9Threshold=40
nodeRoutedClient4_9Threshold=40
nodeChChangeThreshold=1
nodeChChange1Threshold=1
nodeChChange4_9Threshold=1
nodeAirtimeThreshold=60
nodeAirtime1Threshold=60
nodeAirtime4_9Threshold=60
```

5 Viewing Fault Information

This chapter describes the Fault Management panels in the web interface.

Chapter contents:

- [Viewing Network Events](#)
- [Viewing Alarms](#)
- [Viewing Event Counts](#)
- [Configuring Alarms](#)

Viewing Network Events

Network events convey general information or current status of devices within the network.

View network events

- Open the Network Health tab and choose **Network Events** on the side menu.

The Network Events panel (Figure 11) opens to display a list of current events for devices configured in the network.

FIGURE 11 Network Events Panel

Network Events

Search | Print | Customize Columns

Page Length|entries per page 50 1351 to 1372 of 1372

View Alarms

Status	IP Address	displayName	Event Details Message	Date / Time	Source	Category	Information
<input type="checkbox"/>	172.20.125.190	FredCell	Evil Twin Detected	Dec 08,2010 09:57:00 AM	19983	Evil Twin Detected	evil_twin_00:0d:97:10:50:36_with_ssid_corne
<input type="checkbox"/>	172.20.125.190	FredCell	Evil Twin Detected	Dec 08,2010 09:57:00 AM	19983	Evil Twin Detected	evil_twin_00:0d:97:00:50:36_with_ssid_Tropo
<input type="checkbox"/>	172.20.125.132	NewLabGW	DFS Radar Detected	Dec 08,2010 09:50:02 AM	49014	DFS Radar Detected	DFS_Channel:5700
<input type="checkbox"/>	172.20.125.132	NewLabGW	Loss trap detected	Dec 08,2010 09:50:02 AM	49014	LostTrap	DFS_Channel:5700

Table 10 lists the columns of information presented in the Network Events table.

TABLE 10 Network Events List

Item	Description
• Status	Color code for the severity of the event: <ul style="list-style-type: none"> • Red---Critical • Orange---Major • Yellow---Minor • Blue---Warning • Green---Clear • White---Informational
• IP address	IP address of the router that generated the event.
• Display name	The alphanumeric name assigned to the router.
• Event Details/Message	Brief summary of the event message. Click the underlined link to open the Event Properties window for the event.
• Date/Time	Date and time that event occurred.
• Source	Serial number of the router.
• Category	Type of event.
• Information	Full text of event message.

Viewing Alarms

Alarms call attention to serious events concerning devices in the network.

View alarms

- Open the Network Health tab and choose **Alarms** on the side menu.

The Alarms panel (Figure 11) opens to display a list of current alarms for devices configured in the network.

FIGURE 12 Alarms Panel

Status	IP Address	Actions	DisplayName	Alarm Details/Alarm Message	Date / Time	Failure Object	Alarm Group
	172.20.125.50		sunpower	<u>Auto Recovery had occurred</u>	Jan 23, 2010 09:02:03 AM	118780_AutoRecoveryChanged	AutoRecoveryChanged
	172.20.125.231		solarpower	<u>Router unreachable</u>	Jan 22, 2010 05:33:28 PM	00027_RouterReachability	RouterReachability
	172.20.125.239		NewLabGw2	<u>Router unreachable</u>	Jan 22, 2010 01:37:34 PM	054057_RouterReachability	RouterReachability
	172.20.125.217		Guppy_42	<u>Evil Twin Detected</u>	Jan 21, 2010 10:36:28 AM	00034_Evil Twin Detected	Evil Twin Detected

Table 11 lists the columns of information presented in the table.

TABLE 11 Alarms List

Item	Description
Status	Color code for the severity of an event: <ul style="list-style-type: none"> • Red---Critical • Orange---Major • Yellow---Minor • Blue---Warning • Green---Clear • White---Informational
IP address	IP address of the router that generated the event.
Actions	Icons for alarm pickup and annotation: For alarm pickup, click the icon to assign the alarm to your user ID. For annotation, click the icon to open the pop-up Annotation window. Enter a comment and click Annotate . Click Close to close the Annotation window.
Display Name	The alphanumeric name assigned to the router.
Alarm Details/Message	Brief summary of the alarm message. Click the underlined link to open the Alarm Properties window for the event.
Date/Time	Date and time that the event occurred.
Failure Object	Code for the type of failure.

TABLE 11 Alarms List (*continued*)

Item	Description
Alarm Group	Type of failure.
Information	Full text of the event message.

Viewing Event Counts

The Event Counts panel provides a consolidated summary of event for each router.

View alarms

1. Open the Network Health tab and choose **Event Count** on the side menu.
2. The Event Count panel ([Figure 13](#)) opens to display a summary of events by router IP address.

FIGURE 13 Event Count Panel

Event/Alarm Count Reporting Period

Last Refreshed at : 12/08/2010 09:59 Reporting Period : ALL

IP ▲	Host Name	Node ID	Node Type	Total	Device Reachability	SNMP Timeout	Gateway Becomes Node	Configurator Login	Failed Install New Image	SSH Login
172.20.125.116	Groom2	00053	node	76	0	0	0	9	0	0
172.20.125.118	Atheros	18060	node	20	4	0	0	13	0	0
172.20.125.128	NewLabGW	49014	gateway	68	0	0	0	10	0	0
172.20.125.130	ppc3	35434	node	177	154	0	0	23	0	0
172.20.125.155	McDonalds	19918	node	13	2	0	0	7	0	0

You can choose the following options from the Event Counts panel:

- To restrict the reporting time interval, select from the pull-down list at the top of the panel, and click **Submit**.
- To display all the events for a given router, click an underlined link in the Total column.
- To display details about a router, click the underlined IP address.
- To access the Configuration Utility for the router, click the underlined IP address link.
- To open an SSH window to access the router CLI, click an underlined link in the SSH column.

[Table 12](#) lists the columns of information presented in the Event Count table.

TABLE 12 Event Count Information

Item	Description
Node IP	IP address of the router that generated the event
Host name	Unique numeric ID assigned to the node
Node type	Gateway, node, or mobile
Total	Total event count
Router Reachability	Count of events concerning the ability to reach other routers
SNMP Timeout	Counts of SNMP timeout events
Gateway Becomes Node	Number of times a gateway has lost uplink to the wired network and automatically taken on node status
Configurator Login	Number of times someone has logged into the Tropos Configuration Utility to access the router
Failed Install New Image	Number of times an attempt to install a new software image on the router has failed
SSH Login	Number of times someone has accessed the router CLI through an SSH connection
Hardware Fault	Number of times a hardware problem has been detected
Software Start	Number of times the router software has been restarted
Others	Count of other events that do not fit into the specific categories list in this table

Configuring Alarms

The Alarm Settings panel allows you to create alarm notifications based on filtering criteria. You can set up an alarm actions to send email notification or an SNMP trap under specified conditions, or create an exception whereby a notification is not sent in response to a condition.

To manage alarm settings

1. Open the Network Health tab and choose **Alarm Settings** on the side menu to open the panel and view the list of currently defined alarm actions.

FIGURE 14 Adding Alarm Actions

Alarm Settings

Alarm Actions : [Add Actions](#) | [Save Actions](#) | [Load Actions](#)

Name	Delete	Enable/Disable
Router Unreach 1	X	Disable
Battery action	X	Disable

2. Perform any of the following actions on this panel.
 - To add a new action, click **Add Actions** and follow the instructions in “[To add new alarm actions](#)” on page 54.
 - To edit an action, link the action name and modify settings as described in [Table 13](#).
 - To Delete the action, click the **Delete** icon.
 - To activate an action, click the **Enable** link.
 - To inactivate an action, click the **Disable** link.
 - To export action settings, click **Save Actions**, specify a file name, and click **Save**. Actions are saved in the /<installdirectory>/ems/conf directory.
 - To load previously saved actions, click **Load Actions**. Specify the file name from the /<installdirectory>/ems/conf directory, and click **Load**.

To add new alarm actions

1. Click **Add Actions**.

FIGURE 15 Adding Alarm Actions

Alarm Settings

Name

Source [Select/View Routers](#)

Severity

Category

Actions

Available Actions		Associated Actions
Bin-Email	<input type="button" value=">>"/> <input type="button" value="<<"/>	Router_unreach_suppre:
<input type="button" value="New Email Action"/>	<input type="button" value="New Suppress Action"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

2. Configure the settings in [Table 13](#).
3. You can associate actions that have already been defined, or create new actions and then associate them.
 - To create a new email action, click **New Email Action**, configure the settings described under New Email action in the table, and click **Submit**.
 - To create a new email action, click **New Suppression Action**, specify a name for the action, and click **Submit**.
 - To associate actions, highlight them in the Available Actions column and use the arrows to move it them to the Associated Actions column.
 - To edit an existing action, select it and click **Edit**.
4. Click **Submit** to save the actions and return to the Alarm Settings page.

TABLE 13 Alarm Settings

Item	Description
Name	Enter a unique name to identify the action.
Source	Click the link to select the devices to include in the action. Select the devices that you want to include in the Available Routers list, and click the right-facing arrow to move them to the Selected Routers area. You can use the links near the bottom of the screen to select or sort the groups of devices in the list, or use the double arrows to move the entire list.
Severity	Select an alarm severity, or select All to include alarms of all severities.
Category	<p>Select one of the following alarm categories or select Any Category to include alarms in all categories:</p> <ul style="list-style-type: none"> • Router Reachability: There has been a change in the ability to reach the device. • Gateway Becomes Node: Gateway has lost its wired connection and switched to node operation. • Switched to Battery: Router has lost power and switched to battery operation. • Configurator Login: User has logged into the router's Configuration Utility. <p>Note: <i>The alarm categories take precedence over the severity settings. For example, all router reachability alarms are of critical severity. If you choose Router Reachability as the category with a non-critical severity, the alarm action is still treated as critical.</i></p>
New Email Action	<p>Specify the following settings:</p> <ul style="list-style-type: none"> • Notification Name: Name to identify the email action. • SMTP Server: IP address or host name of the Simple Mail Transfer Protocol (SMTP) server. • SMTP Account Name: User name for access to the SMTP server. • Password: User password for access to the SMTP server. • To Address: Email address that will appear in the To line of the email notification. • From Address: Email address that will appear in the To line of the email notification. • Aggregate after (secs): Number of seconds to enter if you want to collect all matching alarms during that interval and then send them in one email notification. • Message: Body of the email notification. • Select drop down list: Preset entries that you can add to the message: category, severity, and source.

TABLE 13 Alarm Settings (*continued*)

Item	Description
New Suppression Action	Enter a name to identify the action.

SNMP Trap Forwarding

Use the SNMP trap forwarding page to forward SNMPv3 traps to an external trap manager.

Forward SNMP traps

1. Open the Network Health tab and choose **Trap Forwarding** on the side menu.

Add Trap Destination

Trap Destination IP:	<input type="text"/>
SNMP User Name:	<input type="text"/>
Auth Type:	<input type="text" value="No Auth"/> ▼
Auth Key:	<input type="text"/>
SNMP Port:	<input type="text" value="162"/>
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

2. Configure the settings in the following table.
3. Click **Submit**.

TABLE 14 Alert Filter Settings

Item	Description
Trap Destination IP	Enter the IP address of the external server designated to receive the SNMP traps.
SNMP User Name	User name for SNMP access.
Auth Type	Choose the cryptographic algorithm (MD5, SHA, or No Auth) to use in authenticating communications between Tropos Control and the external server.
Auth Key	Enter an authentication key to secure the communications between Tropos Control and the external server designated to receive the SNMP traps.
SNMP Port	Enter the Tropos Control server port to use for SNMP communications.

6 Viewing Network Configuration Information

This chapter describes how to display device information using the Network Configuration panels in the web interface.

Chapter contents:

- [Network Configuration Panels](#)
- [Configuration View Actions](#)
- [Updating the Device Database](#)
- [Configuring Gateways for Multi-Subnet Roaming](#)

Network Configuration Panels

The Configuration View tab presents device information from the Tropos Control database. The information shown in each panel is described in “[Provisioning Forms](#)” on page 78.

(i) Note

The Configuration View displays only the menu items that are included in your product.

The Configuration View tab includes the following panels:

- Complete View---General status information
- Router Synchronization---Make router configurations consistent with each other
- Inventory---List of routers in the database.
- Router Identity---Identity and location information
- Device and IP---Interface and network address information
- Wireless---Information on wireless signal characteristics
- DHCP Server---Status of the on-board DHCP server
- Time---Time configuration and Network Time Protocol (NTP) server information
- Packet Filtering Predefined Rules---Rules currently defined, listed by router and protocol type
 - Customized Rules---Special filtering rules
 - Deny Rules---Rules to deny access
- VLAN---VLAN configuration information
- VLAN Information---Provides status information and lists the type of VLAN
- Rate Limiting---Information status, caps, and triggers for rate limiting
- QoS---Information on Quality of service (QoS) settings
- QoS ESSID Parameters---Information on QoS settings defined for specific ESSIDs
- Static IP Client---Information on clients that are configured with static IP addresses
- P2P Blocking---Information on blocking of communications between clients in specified subnets
- Backhaul Routing---Information on neighboring Border Gateway Protocol (BGP) routers that are one Layer 3 hop away
- Multi-ESSID---Information on secondary ESSIDs and multiple BSSIDs
- Router Access Control---Information on access restrictions for packet filtering
- Multi-Subnet---Source and destination information for multi-subnet roaming
 - Gateway List---Gateway information for multi-subnet roaming
 - Additional Subnets---Subnets available for roaming
- Voice---Information on voice parameters
- Security---Information on security settings
- SNMP users--List of current SNMP users
- SNMP--List of configured SNMP trap destinations

Configuration View Actions

You can perform all of the following actions from the Configuration View panels:

- [View configuration information](#)
- [Search in a configuration view panel](#)
- [Print the configuration view list](#)
- [Export the configuration view list](#)
- [View alarms or events for selected routers](#)
- [Customize the configuration view columns](#)
- [Add a device](#)
- [Delete routers](#)
- [Synchronize routers](#)
- [Customize the configuration view columns](#)

View configuration information

1. Open the web interface and choose **Configuration View**.
2. Choose the desired panel from the side menu.

Search in a configuration view panel

1. Click **Search** to open the Search window.
2. Choose an item to match from the pull-down list.
3. Choose the matching criterion from the pull-down list.
4. Enter the text to match. To match additional items:
 - a. Click **More** and choose additional criteria. You can continue to request more items by clicking **More** repeatedly.
 - b. Select a radio button to match any one of the criteria (OR match) or all of the criteria (AND match).
5. Click **Search**.

The window opens to display the matching items.

Print the configuration view list

1. Click **Print** to open a window containing a print-formatted version of the list.
2. Click **Print**.

Export the configuration view list

1. Click **Export**.

A pop-up window prompts you to open or save the view information in csv (comma-separated) format.
2. Click **Save**, browse for a file location, enter the file name, and click **Save**.

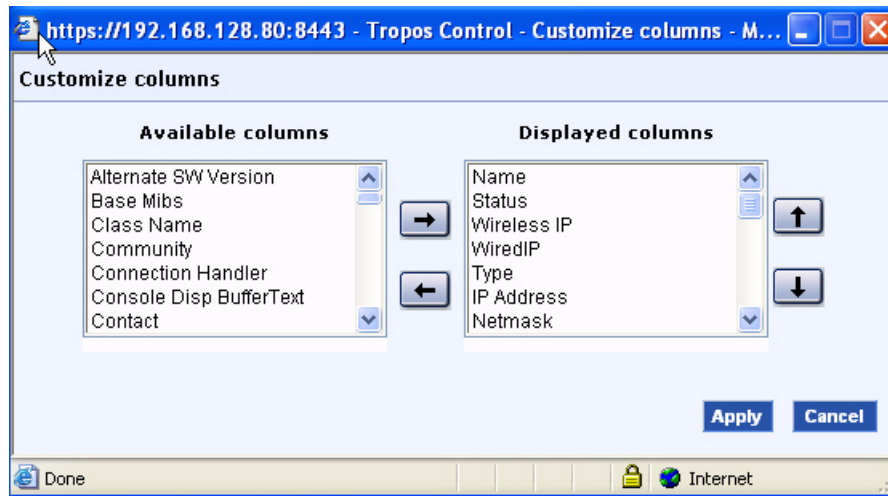
View alarms or events for selected routers

- Select the routers, and click View Alarms or View Events.

The Events or Alarms panel opens to show the list for the selected routers.

Customize the configuration view columns

1. Click **Customize Columns** to open the Customize Columns window.



2. Select columns from the Available Columns list and use the right-facing arrows to move the selected columns to the Displayed Columns area.
3. To order the columns, use the upward and downward facing arrows.
4. Click **Apply**.

Updating the Device Database

You can add devices and synchronize the device database from any of the Configuration View panels. Use the buttons at the top of the panel.

Router Synchronization

[Add View](#) | [Edit View](#) | [Remove View](#) | [Search](#) | [Print](#) | [Export](#) | [Customize Columns](#)

[Add Gateway](#) | [Delete Router](#) | [Synchronize Router](#) | [View Events](#) | [View Alarms](#) | [Provision](#) | [Show Map](#)

Page Length|entries per page | 25 | 1 to 25 of 30 | < > >>

ID	Display Name	Last Boot Time	Router Synchronized on	Model	Wireless IP (WLAN0)	Wireless IP (WLAN1)	Type
<input type="checkbox"/> 00034	Guppy_42	Nov 6, 2010 11:41:14 PM	Nov 6, 2010 11:57:04 PM	6320 DC	172.20.125.217	172.20.125.213	node
<input type="checkbox"/> 00041	LuckyLake	Nov 6, 2010 11:47:37 PM	Nov 6, 2010 11:53:25 PM	6320 DC	172.20.125.225	172.20.125.229	node

Add a device

1. Open the Configuration View panel and choose **Add Gateway**.
2. Click **Add Gateway** to open the Discover New Gateway window.

Discover New Gateway

IP Address	<input type="text" value="root"/>	
Mesh ID	<input type="text" value="●●●●●●●●"/>	* For routers with 7.1 and earlier versions
Router Authentication Key	<input type="text"/>	* For routers with 7.3 and later versions
Confirm Router Authentication Key	<input type="text"/>	
Management Station IP Address	<input type="text" value="192.168.128.96"/> ▼	
<input type="checkbox"/> Save to File		

[Add Gateway](#)

3. Enter values as described in [Table 15](#).

TABLE 15 Gateway Settings for Adding to the Device Database

Item	Description
IP Address	Enter the IP address of the gateway.
Mesh ID	Enter and confirm the 16-character code that identifies the area of the managed routers. Each managed router must be configured with the same wireless routing domain ID. <i>Note: This is the same as the Mesh ID that is configured on the router.</i>
Router Authentication Key Confirm Router Authentication Key	Enter and confirm 16-character ASCII authentication key for communication between the router and Tropos Control.
Management Station IP Address	Enter the IP address of the Tropos Control server in the Management Station IP Address field, or select from the drop down menu.
Save to File	Select to save the discovery parameters in the <code><installdirectory>/ems/conf/server/discover_devices.txt</code> file.

4. Click **Add Gateway**.

Tropos Control searches and discovers the indicated gateway, along with all the nodes in its cluster. When the discovery process is complete, the gateways are added to the Configuration View panels.

Delete routers

1. Select one or more routers, and click **Delete Routers**.
2. Click **OK** to confirm.

The selected routers are removed from the Tropos Control database.

Synchronize routers

The Synchronize Routers option writes the configuration information in the selected routers to the Tropos Control database. Synchronization occurs automatically every 5 minutes. Use the Synchronize Routers button to perform an immediate update or if a previous update was unsuccessful. You can synchronize up to 10 routers at one time.

1. Select the routers in the table.
2. Click **Synchronize Routers**.
3. A pop-up message explains that the routers will be synchronized. Click **OK** to acknowledge the message.

The information in the Tropos Control database is updated to match the information in the selected routers. When the update is completed, any new information is reflected in the Configuration View panels.

View Events or Alarms

1. Select the routers in the table.
2. Click **View Events** or **View Alarms** to open the Events or Alarms page for the selected routers. See [“Viewing Fault Information”](#) on page 49 for more information.

Provision

1. Select the routers in the table.
2. Click **Provision** to open the Provisioning pages for the selected routers. See [“Provisioning”](#) on page 68 for more information.

Show Map

1. Select the routers in the table.
2. Click **Show Map** to open a Google Maps window that shows the selected routers. See [“Viewing Geographic Maps”](#) on page 27 for more information.

Creating Custom Views

You can save lists that match search criteria by creating custom views.

Create view

1. Open the Configuration View tab.
2. Open the view for which you want to create the child view.
3. Click the **Add Child View link**.

Add Topology Child View * Mandatory fields

Custom view name : *

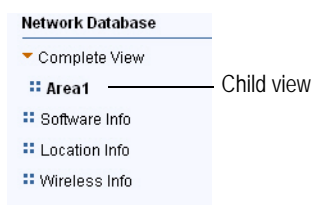
Criteria Properties :

More **Fewer**

Preview Results **Add Child View**

4. Enter the view name.
5. Choose an item to match from the pull-down list.
6. Choose the matching criterion from the pull-down list.
7. Enter the text to match.

8. To match additional items:
 - a. Click **More** and choose additional criteria. You can continue to request more items by clicking **More** repeatedly.
 - b. Select a radio button to match any one of the criteria (OR match) or all of the criteria (AND match).
9. To preview the results, click Preview Results.
The matching list is presented at the bottom of the window.
10. To save the view, click **Add Child View**.
The new view is listed as a sub-item on the side menu.



Modify view

1. Click **Edit View Criteria**.
2. Make changes as desired.
3. Click **Apply/Edit View Criteria**.

Delete view

1. Click **Remove View**.
2. Click **OK** to confirm.

Configuring Gateways for Multi-Subnet Roaming

Multi-subnet roaming refers to the ability of client stations to retain links to the wireless network when they move from one router subnet to another. To support multi-subnet roaming, each gateway must store the IP address of all the gateways in the roaming domain.

During multi-subnet roaming, the client's traffic is routed through its home gateway (the gateway to which it was originally associated). If the home gateway loses its uplink while an associated client is roaming, the client will lose connectivity, unless a redundant gateway is operational in the same home subnet and included in the multi-subnet roaming list. To restore connectivity, the old gateway must become available again or the client must obtain an IP address from the new gateway.

To support multi-subnet roaming, you can configure Tropos Control to automatically distribute the gateway list to all the gateways in the managed network. The distributed gateway list includes all the gateways in the Tropos Control database. See [“Multi-Subnet Roaming”](#) on page 110.

Use the web interface to view the current multi-subnet roaming information and status and to update all gateways with the latest gateway information. The information is presented in the following panels.

Multi-Subnet

This panel lists all the interconnections between gateways and subnets. To access this panel, open the Configuration View tab and choose **Multi-Subnet**.

Configuration:

This configuration is used by gateways to support cross subnet roaming.

Update Gateway List	Update all gateways with the current complete gateway list.
Clear Gateway List	Remove gateway list on all gateways. This action will disable cross subnet roaming.
Show Current Tunnels	Get the current cross subnet roaming tunnels from the gateways.

Warning: The action of "Update Gateway List" and "Clear Gateway List" will commit all the outstanding (stored) configurations on gateways.

Note: In a multi-subnet network with VLANs, each management VLAN prefix must be on the list of allowed IP subnets.

Status:

Show Current Status	Show current configuration status.
Show Configuration Summary	Summarize the current configuration result here.

Tunnel View (total: 0)

Perform the following actions from this panel. To abort an operation before completion, click **Abort**. When the operation is complete, the window opens and prompts you to export the file.

Action	Description
Update Gateway List	Send the current, complete Gateway List to all gateways.
Clear Gateway List	Remove the gateway list from all gateways. This action disables multi-subnet roaming.
Show Current Tunnels	Obtain the current multi-subnet roaming tunnels from the gateways. When you click this button the window reopens to show progress.
Show Current Status	Show the status any current configuration jobs, such as Update Gateway List or Clear Gateway List.
Show Configuration Summary	Show a summary of the current multi-subnet roaming configuration in a new window.

Gateway List

This panel displays the current gateway list. To access this panel, open the Configuration View tab, choose **Multi-Subnet**, and then choose **Gateway List**.

Gateway List

Export Result to File Provision

Page Length|entries per page 25 1 to 6 of 6

<input type="checkbox"/>	ID	Wireless IP(2.4)	IP	Mask
<input type="checkbox"/>	19207	172.20.125.99	172.20.125.128	255.255.255.0
<input type="checkbox"/>	19207	172.20.125.99	172.20.125.96	255.255.255.0
<input type="checkbox"/>	19207	172.20.125.99	172.20.125.99	255.255.255.0
<input type="checkbox"/>	19040	172.20.125.96	172.20.125.128	255.255.255.0
<input type="checkbox"/>	19040	172.20.125.96	172.20.125.96	255.255.255.0
<input type="checkbox"/>	19040	172.20.125.96	172.20.125.99	255.255.255.0

Perform the following actions from this panel:

- Export Result to File--Send the information for the items with selected check boxes to a CSV file.
- Provision--Open the Multi-Subnet Roaming provisioning form to provision the routers in the list, as described in [“Multi-Subnet Roaming”](#) on page 110.

7 Provisioning

Provisioning refers to the process of configuring Tropos routers to operate in the wireless network. Tropos Control supports XML-based provisioning through the web interface to assure that configurations are consistent across the network. This chapter explains how to provision devices.

Chapter contents:

- [About Provisioning Operations](#)
- [Provisioning Routers Using Web Forms](#)
- [Provisioning Routers From a File](#)
- [Provisioning Forms](#)
- [Other Provisioning Operations](#)
- [Auditing Provisioning Jobs](#)

About Provisioning Operations

The web interface supports the following types of provisioning:

- Provisioning from Forms---Use the web interface forms to specify the configuration parameters to provision (“[Provisioning Routers Using Web Forms](#)” on page 74).
- Provisioning from Files---Provision router identity or client black list/white list using information stored in files (“[Provisioning Routers From a File](#)” on page 76).
- Administrative Operations---Perform a variety of router administration tasks (“[Other Provisioning Operations](#)” on page 123).



Caution

It is possible for conflicts to arise in applying provisioning changes if multiple administrators are logged in and performing provisioning operations at the same time.

Each provisioning operation involves the tasks listed in [Table 16](#).

TABLE 16 Provisioning Tasks

Step	Task	Description
1	Router selection	Choose the routers that will receive the new configuration values (“ Select routers to provision ” on page 70).
2	Configuration	Specify any of the following changes to be made: Configure values and store them on the Tropos Control server. See “ Configure router parameters ” on page 75. Specify the type of file provisioning and the source file. See “ Specify the type of provisioning and the source file. ” on page 77. Choose an administrative task. See “ Other Provisioning Operations ” on page 123.
3	Schedule the provisioning job	Send the stored configuration values or file to the designated routers (“ Schedule the provisioning job ” on page 72).
4	Commit	Activate the new configuration values on the designated routers (“ Commit the provisioning job ” on page 73).

Select routers to provision

1. Open the Provisioning tab (Figure 16) and choose the panel for the type of provisioning that you plan to implement.

FIGURE 16 Provisioning Tab

The screenshot shows the Tropos Control Provisioning Tab. The left sidebar has a 'Provision' section with 'Provision from Form' selected. The main content area is titled 'Provision from Form' and includes a 'Provision Job Name' field with the value 'provision2011_03_22_14_46_02'. Below this are 'Retry' and 'Schedule' sections. The 'Retry' section has a checked box for 'Retry failed routers' and a 'Retry' field set to 3 times with a 30-second interval. The 'Schedule' section has radio buttons for 'Provision Now' (selected) and 'Provision at'. A 'Provision Summary' section on the right lists tasks to finish a provision job, including filling in configuration data. At the bottom, there are two tables: 'Selected Devices' and 'Golden Devices'.

Selected Devices:	
Gateways	0
Nodes	2
Mobile Nodes	0
Total	2

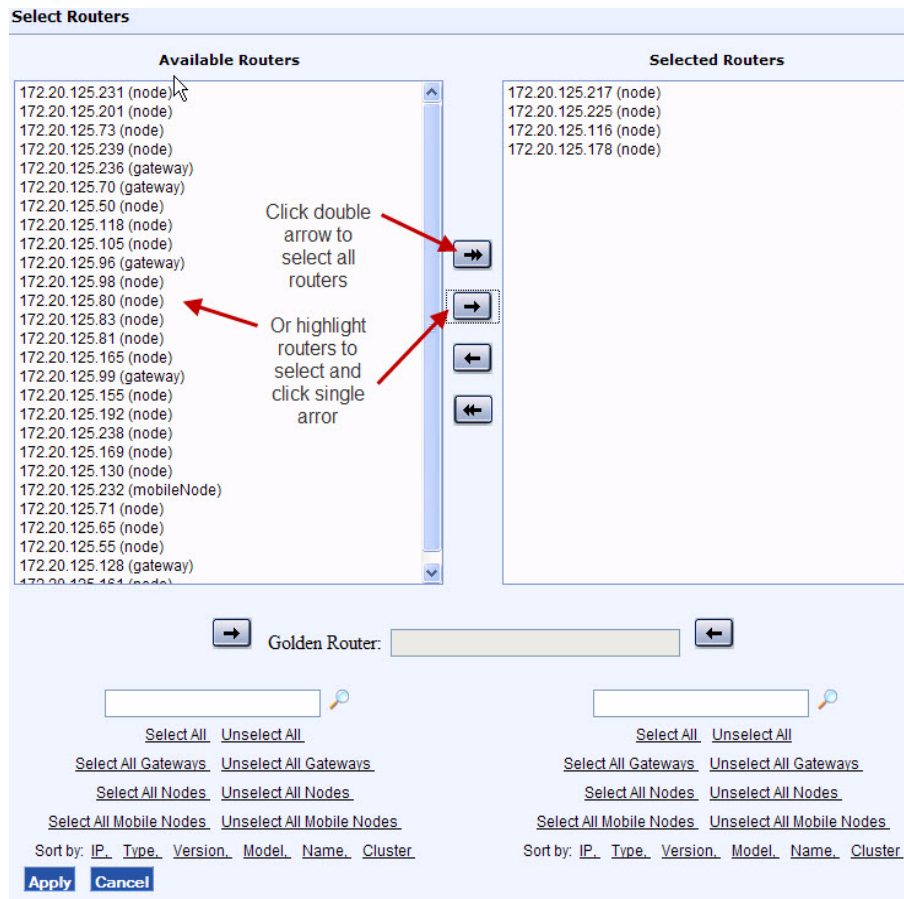
Golden Devices:	
Name	CS-NE-entrance-cell
Type	node
ID	19134
IP	172.20.125.84

2. Click **Select Devices**.

This screenshot shows the 'Selected Devices' table after clicking the 'Select Devices' button. The table is empty, showing 0 for all categories.

Selected Devices:	
Gateways	0
Nodes	0
Mobile Nodes	0
Total	0

A selection window opens.



3. Select the routers that you want to provision in the Available Routers list, and click the right-facing arrow to move them to the Selected Routers area. You can use the links near the bottom of the screen to select or sort the groups of routers in the list, or use the double arrows to move the entire list.



Note

Choose only the routers that you want to provision with the same new parameter settings. Only the settings that you specify as part of the provisioning process must be the same; all other settings can be different.

4. You can also select a *golden* router by highlighting the router and then clicking one of the arrows adjacent to the Golden Router field. The golden router parameter values are the values that are displayed when you open the individual provisioning forms. If you do not explicitly choose a golden router, the first router in the list is automatically designated as golden.



Note

The golden router is provisioned only if it is selected. If it is not selected, its values are displayed but it is not including in the provisioning operation.

5. Click **Apply**.

The Provision from Form or Provision from Files panel reopens to show the number of selected routers and information about the golden router.

[Select Devices \(v6.7+\)](#) [Clear Devices](#)

Selected Devices:

Gateways	0
Nodes	2
Mobile Nodes	0
Total	2

Golden Devices:

Name	CS-NE-entrance-cell
Type	node
ID	19134
IP	172.20.125.84

You can now configure parameters on provisioning forms, specify provisioning files, or perform other administrative operations. See [“Provisioning Routers Using Web Forms”](#) on page 74, [“Provisioning Routers From a File”](#) on page 76, or [“Other Provisioning Operations”](#) on page 123.

i **Note**

*To clear the list of selected routers, click **Clear Routers**.*

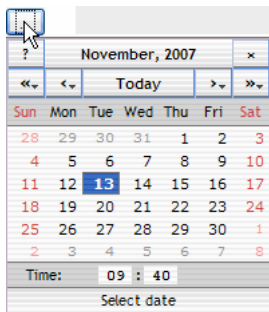
Schedule the provisioning job

1. Open the Provisioning tab and choose the panel for the type of provisioning that you plan to implement.
2. Enter a name for the provisioning job, or keep the default name assigned by the system. The default name incorporates the date and time.

Provision Job Name:

3. Specify the number of retries before the provisioning action is deemed to have failed and the time interval between retries. Provisioning actions may fail if the router cannot be reached or is not in a state to accept the configuration changes.

- Choose **Provision Now** to begin the provisioning activity immediately, or choose **Provision At**, click to open the calendar, and select a date and time.



At the specified time, the new parameter values are sent to the designated routers. You can now view the provisioning job list and commit the new values.

Commit the provisioning job

- Open the Provisioning tab.
- Choose **Provision Job List** from the side menu to open the Provision Job list.

Provision Job List

View Provision Detail View Provision Result Stop Commit Redo

Page Length|entries per page 50 1 to 50 of 114

Name: Filter

ID	Name	Type	Scheduled Time	Executed Time	Finished Time	Status	User Name
<input type="checkbox"/> 1602	provision2011_03_16_14_22_10	Form Provision	Mar 16 2011 14:23:00	Mar 16 2011 14:23:00	Mar 16 2011 14:23:02	Success	root
<input type="checkbox"/> 1467	Disable FIPS	Form Provision	Jan 18 2011 17:36:16	Jan 18 2011 17:36:16	Jan 18 2011 17:36:23	Failed	root
<input type="checkbox"/> 1440	Qun's_additional_-2	Form Provision	Jan 05 2011 18:00:59	Jan 05 2011 18:00:59	Jan 05 2011 18:01:05	Partial Success	root

- Select checkboxes for the jobs that you want to commit.
- Confirm that provisioning was successful for the selected jobs (Status column).
- Click **Commit**.

The Provision from Form panel reopens to show that the requested commit command is to commit the stored data to the routers.

Provision

Choose command to be sent to routers below:

Commit the stored data in routers

- Click **Provisioning** to commit the values that have been successfully provisioned on the selected routers.

The provisioning process is now complete.

Provisioning Routers Using Web Forms

This section describes how to provision routers using the Provision from Form panel in the web interface (Figure 17).

FIGURE 17 Provisioning from Form Panel

The screenshot displays the Tropos Control web interface. The top navigation bar includes 'Network Health', 'Configuration View', 'Provisioning', and 'Administration'. The 'Provisioning' tab is active. On the left sidebar, 'Provision from Form' is highlighted. The main content area is titled 'Provision from Form' and contains the following elements:

- Provision Job Name:** A text input field containing 'provision2011_03_22_14_46_02'.
- Retry:** A section with a checked checkbox for 'Retry failed routers'. Below it, a 'Retry' field is set to '3' times, with an interval of '30' seconds.
- Schedule:** A section with radio buttons for 'Provision Now' (selected) and 'Provision at'. The server time is shown as 'Mar 22 2011 15:50:19'.
- Buttons:** 'Provision' and 'Cancel' buttons are located below the schedule options.
- Selected Devices:** A table showing the count of selected devices:

Gateways	0
Nodes	2
Mobile Nodes	0
Total	2
- Golden Devices:** A table showing details for a selected device:

Name	CS-NE-entrance-cell
Type	node
ID	19134
IP	172.20.125.84
- To perform a Form based Provisioning Job:** A callout box with instructions:
 - Select devices to be configured by clicking "Select Devices"
 - Click "Fill data" to link to the Provision Form
 - Submit the provision job
- Provision Summary:** A section stating 'To finish a provision job, you need to finish the following tasks:' followed by a bullet point: 'Fill in the configuration data within Configuration Forms: [Fill data](#)'.

Provisioning from Forms - Tasks

Perform these tasks in the specified order to provision routers using web forms:

1. [Select routers to provision](#) (on page 70)
2. [Configure router parameters](#) (on page 75)
3. [Schedule the provisioning job](#) (on page 72)
4. [Commit the provisioning job](#) (on page 73)

Configure router parameters

1. Open the Provisioning tab and select the routers to provision (“[Select routers to provision](#)” on page 70).
2. Choose one of the provisioning forms listed under Device Settings or Service Settings in the side menu.
3. The selected form opens, as in this Time form example. Configuration parameters from the golden router are displayed.

Time

0 Gateways 2 Nodes 0 MobileNodes are selected [Adjust Selection](#)

Golden Device: (default value comes from this device)
 Name: CS-NE-entrance-cell Type: node ID: 19134 IP: 172.20.125.84

<input type="checkbox"/>	Module Name	Value	Notes
<input type="checkbox"/>	NTP Server:	192.43.244.18	*1 *2
<input type="checkbox"/>	Time Zone:	US/Pacific	
<input type="checkbox"/>	Set Router Time:	<input type="text"/> ...	

* 1: Up to 3 time (ntp) server addresses (separated by comma) can be configured.
 * 2: For pre 7.5 release routers, it can be "," separated string of 3 ip addresses. Otherwise it can be ";" separated string of 3 ip addresses or host names

4. Select checkboxes for each field that you want to provision, and modify the field value as desired. See “[Provisioning Forms](#)” on page 78 for descriptions of the parameters on each form.



Note

The fields with checkboxes selected are the ones that will be provisioned on the selected routers. All other values will be ignored. If you modify a field value, the checkbox for that field is automatically selected.

5. Click **Submit** to save the values on the Tropos Control EMS server.

You can now schedule the provisioning job (“[Schedule the provisioning job](#)” on page 72).

Provisioning Routers From a File

This section describes how to provision routers using the Provision from Files panel in the web interface (Figure 18).

FIGURE 18 Provisioning from Files Panel

The screenshot shows the Tropos Control web interface. The top navigation bar includes 'Network Health', 'Configuration View', 'Provisioning', and 'Administration'. The 'Provisioning' tab is active. On the left sidebar, under 'Provision', the 'Provision from Files' option is circled in red. The main content area is titled 'Provision from Files' and contains the following elements:

- Provision Job Name:** A text input field containing 'provision2010_12_08_08_54_11'.
- Retry:** A section with a checked checkbox 'Retry failed routers' and a 'Retry' field set to '3' times with an interval of '30' seconds.
- Schedule:** A section with radio buttons for 'Provision Now' (selected) and 'Provision at', along with a 'Server Time' indicator showing 'Dec 08 2010 10:16:43'.
- Provision:** A blue button.
- Choose provisioning file type below:** A dropdown menu currently set to 'Using Router Static IP file'.
- Select file from local file system:** A dropdown menu with a 'Browse...' button next to it.

On the right side of the interface, there is a grey box titled 'To use a configuration CSV file to perform a provisioning job:' with the following instructions:

- Use excel to create a CSV file that contains configuration information for the routers to be provisioned
- Load the CSV file
- Submit the job

You can provision the following types of information from a file:

- **Router identity**---Identify the router for the managed network, applying basic identity and location information.

The file must begin with the following line and conform to this format:

```
#uniqueid,display name,latitude,longitude,location,contact
```

Example:

```
#uniqueid,display name,latitude,longitude,location,contact
35036,Gateway,37.3935,-122.033,Sunnyvale CA 94085,www.company.com
```

- **Black list or white list**---Identify clients that are permitted or denied access to the Tropos network.

- **ACL Block**---Refuse association to the devices with specified MAC addresses.
- **ACL Allow**---Permit the devices with specifies MAC addresses to associate.

The following black list/white list provisioning operations are supported:

- **Apply**---Upload a file with MAC addresses to the selected router or routers.
- **Retrieve**---Copy a file with MAC addresses from the selected router or routers to the Tropos Control server, storing the file in the cell configuration directory in the Tropos Control installation directory.

The black list or white list file must consist of a list of MAC addresses, one per line.

Example:

```
00:11:22:33:44:55
aa:bb:cc:dd:ee:ff
```

- **Static IP addresses**--Add routers with static IP address assignments.

The file must begin with the following line and conform to this format:

```
#uniqueid,wiredip,wiredmask,wlan0ip,wlan0mask,wlan1ip,wlan1mask,
defaultgw
```

Example:

```
#uniqueid,wiredip,wiredmask,wlan0ip,wlan0mask,wlan1ip,wlan1mask,
defaultgw
19040,172.20.125.95,255.255.255.0,172.20.125.96,255.255.255.0,,,172
.20.125.254
18505,,,172.20.125.105,255.255.255.0,,,
```

Provisioning from Files - Tasks

Perform these tasks in order to provision routers from files:

1. [Select routers to provision](#) (on page 70)
2. [Specify the type of provisioning and the source file.](#) (on page 77)
3. [Schedule the provisioning job](#) (on page 72)
4. [Commit the provisioning job](#) (on page 73)

Specify the type of provisioning and the source file.

1. Open the Provisioning tab and select the routers to provision (“[Select routers to provision](#)” on page 70).
2. Select the type of provisioning:

For router identity:

— Choose **Using Router Identity CSV** file from the provisioning type pull-down list.

For black list/ white list:

— Choose **Using Black List or White List file** from the provisioning type pull-down list.

— Choose whether to provision the list to the routers or retrieve the list from the routers.

— Choose whether the clients in the list will be allowed to access the network or blocked from accessing the network.

For static provisioning:



— Choose **Using Router Static IP** file from the provisioning type pull-down list.

3. Choose whether to select the file from your local file server or the Tropos Control server, and browse to locate and open the file.

4. Click **Provision**.

Provisioning Forms

The following notes apply to use of the provisioning forms in the web interface:

- Fields marked as unique  can be provisioned only to one router at a time.
- Fields marked with a version  apply only to routers with the indicated software release.
- Fields that do not apply to the selected routers are grayed out (such as gateway-only fields if only nodes are selected for provisioning).
- Only the fields that have a check box selected are included in the provisioning job. When you enter or modify a value, the associated check box is automatically selected.

This section lists the available provisioning forms and fields:

Device Settings

- [Router Identity Page](#)
- [IP and VLAN Page](#)
- [Wireless Page](#)
- [Client Access](#)
- [DHCP Server](#)
- [SNMP](#)
- [Time](#)

Service Settings

- [DHCP Clients](#)
- [Static IP Client](#)
- [Packet Filtering](#)
- [P2P Blocking](#)
- [Multi-Subnet Roaming](#)
- [Backhaul Routing](#)
- [Rate Limiting](#)
- [QoS](#)
- [Voice](#)

Administration

- [Software](#)
- [Security](#)

Router Identity Page

The Router Identity page (Figure 19) contains information on the physical identity and location of the router. Table 17 describes the parameters on the page.

FIGURE 19 Router Identity

Router Identity

0 Gateways 1 Nodes 0 MobileNodes are selected [Adjust Selection](#)

Golden Device: (default value comes from this device)
Name: LuckyLake **Type:** node **ID:** 00041 **IP:** 172.20.125.225

Router Identity

<input type="checkbox"/>	Module Name	Value	Notes
<input type="checkbox"/>	Router Mode:	Node	
	Model number:	6320 DC	
<input type="checkbox"/>	Name:	LuckyLake	Unique
<input type="checkbox"/>	Location:	roof	
<input type="checkbox"/>	Contact:	www.troposnetworks.com	
<input type="checkbox"/>	Latitude(+/-dd.ddddddd):	37.396142	Unique
<input type="checkbox"/>	Longitude(+/-ddd.ddddddd):	-122.034223	Unique
<input type="checkbox"/>	Location Services:	Disabled	
<input type="checkbox"/>	Banner:		

The field can only be provisioned to one router at time

TABLE 17 Router Identity Settings

Field	Range, Default	Description
Router Mode	Gateway Node Mobile Node	Identifies the setting for the type of router.
Model number	TroposRouter	Identifies the router (text string). Note: <i>The router name is not displayed in the wireless client utility on the client's PC. The router is identified only by MAC address.</i>
Name	TroposRouter	Identifies the router (text string). The router name is not displayed in the wireless client utility on the client's PC. The router is identified only by MAC address.
Location	Sunnyvale	Identifies the location where the router is installed.
Contact	---	Identifies the person responsible for the router.

TABLE 17 Router Identity Settings (*continued*)

Field	Range, <i>Default</i>	Description
Longitude	-180.00000 - 180.000000; 0	Represents the global longitudinal position of the router (fields are in the format +/- <i>ddd.ddddddd</i> , with up to 8 digits permitted to the right of the decimal point).
Latitude	-90.00000 - 90.000000; 0	Represents the global latitudinal position of the router (fields are in the format +/- <i>ddd.ddddddd</i> , with up to 8 digits permitted to the right of the decimal point).
Location Services	Enabled <i>Disabled</i>	If enabled, allows router location information to be sent to a client using a special XML call.
Banner	Enabled <i>Disabled</i>	Optional text that is displayed above the information bar. See Figure 5 on page 21. Allows you to specify the use characteristics for the router, as required by NERC-CIP. The maximum length is 128 characters and special characters such as @, &, <, > are not supported.

IP and VLAN Page

The IP and VLAN Configuration page (Figure 20) lists network parameters for the router. Table 18 describes all parameters on the page.

FIGURE 20 IP and VLAN (Excerpt)

IP and VLAN

0 Gateways 0 Nodes 0 MobileNodes are selected [Adjust Selection](#)
Please select devices to provision

IP Configuration

<input type="checkbox"/>	Module Name	Value	Notes
<input type="checkbox"/>	Mode:	Static	
<input type="checkbox"/>	LAN/Backhaul IP:	<input type="text"/>	Unique
<input type="checkbox"/>	LAN/Backhaul Mask:	<input type="text"/>	
<input type="checkbox"/>	WLAN0 Wireless IP:	<input type="text"/>	Unique
<input type="checkbox"/>	WLAN0 Wireless Mask:	<input type="text"/>	
<input type="checkbox"/>	WLAN1 Wireless IP:	<input type="text"/>	Unique
<input type="checkbox"/>	WLAN1 Wireless Mask:	<input type="text"/>	
<input type="checkbox"/>	Default Gateway:	<input type="text"/>	
<input type="checkbox"/>	Domain Name Servers:	<input type="text"/>	Ver. 7.5 - 2
<input type="checkbox"/>	Backhaul Check:	Enabled	
<input type="checkbox"/>	Backhaul Check IP:	<input type="text"/>	

* 1: For pre-7.1 Mobile Node, use Configurator to change the settings.
* 2: Up to 3 dns server addresses (separated by comma) can be configured.

VLAN Configuration

<input type="checkbox"/>	Module Name	Value	Notes
<input type="checkbox"/>	VLANs:	Enabled	
<input type="checkbox"/>	Management VLAN:	<input type="text"/>	

VLAN IP Mapping

VLAN ID	VLAN Name	IP	Mask	Default Gateway	DHCP Server	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

TABLE 18 IP and VLAN Page Parameters

Field	Range, Default	Description
Mode	<i>DHCP</i> Static	Method used to obtain the device IP address (static or DHCP).
LAN/Backhaul IP Address	--	IP address of the LAN/backhaul interface (x.x.x.x/n format). This field is grayed out if Mode is set to DHCP.
LAN/Backhaul Mask	--	Subnet mask of the LAN/backhaul interface (x.x.x.x/n format). This field is active only if Mode is Static.
WLAN0 Wireless IP	--	IP address of the wlan0 interface (x.x.x.x/n format). This field is grayed out if Mode is set to DHCP.
WLAN0 Wireless Mask	--	Subnet mask of the wlan0 interface (x.x.x.x/n format). This field is active only if Mode is Static.
WLAN1 Wireless IP	--	IP address of the wlan1 interface (x.x.x.x/n format). This field is grayed out if Mode is set to DHCP.
WLAN1 Wireless Mask	--	Subnet mask of the wlan1 interface (x.x.x.x/n format). This field is active only if Mode is Static.
Default Gateway	--	IP address of the default network device (not the device). This field is active only if Mode is Static.
Domain Name Servers	--	Specifies the name of a DNS server on the network (up to three servers are supported).
Backhaul Check	<i>Disabled</i> Enabled	IP address of a device to be used to verify backhaul connectivity.
Backhaul Check IP		IP address of a device to be used to verify backhaul connectivity.
<i>VLAN Configuration</i>		
VLANs	Disabled <i>Enabled</i>	Indication of whether VLANs are enabled.
Management VLAN	--	VLAN ID of the management VLAN.
<i>VLAN IP Mapping</i>		
VLAN IP Mapping	--	VLAN ID of the management VLAN.
VLAN ID		Numeric identifier for the VLAN. Note: Do not assign four-digit VLAN IDs in mixed environments (networks that have some routers running Release 7.1 software and some routers running Release 6.7 software).
VLAN Name		Text name to identify the VLAN.

TABLE 18 IP and VLAN Page Parameters (*continued*)

Field	Range, Default	Description
IP/Mask		IP address and subnet mask of the VLAN interface (x.x.x.x/n format). Note: The IP/Mask, Default Gateway, and DHCP Server fields are active only if Mode is static.
Default Gateway		IP address of the default network routing gateway.
DHCP Server		IP address of the server that supplies DHCP service for the VLAN.
Wired Client Interface Configuration		
Wired Clients	<i>Disabled</i> Enabled	Indication of whether wired clients are supported on the Management/Wired Interface.
Wired Clients Interface Mode	<i>DHCP</i> Static	Method used to obtain the IP address of the wired clients (static or DHCP). This field is active only if Wired Clients is enabled.
Wired Clients IP/Mask	--	Subnet for wired clients, specified by IP address and subnet mask (x.x.x.x/n format). This field is active only if Wired Clients is enabled and Wired Clients Interface Mode is Static.
VLAN Mode	<i>Access</i> Trunk	Type of VLAN support for wired clients. Trunk mode: Permits separate VLAN assignment for each wired interface. Access mode: Permits assignment of one VLAN for all wired interfaces.
Access VLAN		For access mode only, select the VLAN for all wired clients.
Wired Client Interface VLAN Mapping List		
VLAN Name	--	For trunk mode only: Select the VLAN name.
VLAN Name IP/Mask	--	For trunk mode only: Enter the IP address/mask, and click Add . Repeat to assign additional VLANs. Click Remove to delete an entry.
Device Settings		
PoE	<i>Off</i> , 12V, 24V, 48V	Setting for PoE power output. Off indicates that PoE power output is not available.

TABLE 18 IP and VLAN Page Parameters (*continued*)

Field	Range, <i>Default</i>	Description
PoE Port	<i>None</i> , LAN, Mgmt, LAN & Mgmt	Port for PoE power output.
LAN/Backhaul Interface Speed/Duplex	<i>Auto</i>	Characteristics of this interface. Auto: Rate automatically negotiated with other devices 100base Tx-FD: 100 Mbit transmission, full-duplex setting 100base Tx-HD: 100 Mbit transmission, half-duplex setting 10base T-FD: 10 Mbit transmission, full-duplex setting 10base T-H: 10 Mbit transmission, half-duplex setting
Management/Wired Interface Speed/Duplex	<i>Auto</i>	Characteristics of this interface. Auto: Rate automatically negotiated with other devices 100base Tx-FD: 100 Mbit transmission, full-duplex setting 100base Tx-HD: 100 Mbit transmission, half-duplex setting 10base T-FD: 10 Mbit transmission, full-duplex setting 10base T-H: 10 Mbit transmission, half-duplex setting
LAN/Backhaul Interface MTU	--	Largest packet size (Maximum Transmission Unit) transmitted over this interface. (bytes)
Management/Wired Interface MTU	--	Largest packet size (Maximum Transmission Unit) transmitted over this interface. (bytes)
<i>Advanced Settings</i>		
Backhaul Capacity	0-30 <i>25</i> for one-radio gateways and <i>30</i> for two-radio gateways	Maximum capacity that the gateway can support. Typically depends on the capacity of the link from the gateway to the capacity injection layer. Nodes usually prefer a gateway with higher backhaul capacity.
Layer 2 Emulation	Enabled <i>Disabled</i>	Indication of whether the network works with wireless devices that operate at Layer 2 of the OSI hierarchy. If enabled, the network appears as a wireless bridge or access point to upstream wired Layer 2 devices.
DRSet Priority	1-10, <i>2</i>	Priority, or relative willingness, of the gateway to be a designated device (DR).
Subnet DRSet Size	1-40, <i>10</i>	Total number of gateways included in the set of DRs for intra-subnet roaming. Make sure that all gateways in the subnet have the same Subnet DRSet size configured.

TABLE 18 IP and VLAN Page Parameters (*continued*)

Field	Range, <i>Default</i>	Description
DHCP Release Packets	Allow Drop	Indication of whether DHCP release packets are allowed to reach the DHCP server. Choosing Drop reduces the number of client IP address changes. The resulting RADIUS accounting data is cleaner and easier to process. This field is active only if Mode is DHCP.
Backhaul Check Failure Threshold (Consecutive Pings)	3 – 999999, 18	Number of failed ICMP ping messages that constitutes failure of the backhaul link.
Backhaul Check Restore Threshold (Consecutive Pings)	1 – 999999, 3	Number of successful ICMP ping messages that causes restoration of the backhaul link.

FIGURE 22 Wireless Configuration (Bottom)

Rate and Power Configuration			
<input type="checkbox"/>	Module Name	Value	Notes
<input type="checkbox"/>	2.4 GHz Mesh Control Transmit Rate:	Auto	
<input type="checkbox"/>	5.8 GHz Mesh Control Transmit Rate:	Auto	
<input type="checkbox"/>	4.9 GHz Mesh Control Transmit Rate:	Auto	
<input type="checkbox"/>	2.4 GHz Power Curve:	off	
<input type="checkbox"/>	5.8 GHz Power Curve:	off	
<input type="checkbox"/>	4.9 GHz Power Curve:	off	
<input type="checkbox"/>	2.4 GHz Mesh Unicast Transmit Rate:	Fixed (Mesh Control Tx Rate)	
<input type="checkbox"/>	5.8 GHz Mesh Unicast Transmit Rate:	Fixed (Mesh Control Tx Rate)	
<input type="checkbox"/>	4.9 GHz Mesh Unicast Transmit Rate:	Fixed (Mesh Control Tx Rate)	
<input type="checkbox"/>	2.4 GHz Transmit Power Attenuation (0-15dB):		
<input type="checkbox"/>	5.8 GHz Transmit Power Attenuation (0-15dB):		
<input type="checkbox"/>	4.9 GHz Transmit Power Attenuation (0-15dB):		
<input type="checkbox"/>	Additional Attenuation for 2.4 GHz 802.11 Beacons and Management Frames:	0 dB	Ver. 7.1
<input type="checkbox"/>	Additional Attenuation for 5.8 GHz 802.11 Beacons and Management Frames:	0 dB	Ver. 7.1
<input type="checkbox"/>	Additional Attenuation for 4.9 GHz 802.11 Beacons and Management Frames:	0 dB	Ver. 7.1
<input type="checkbox"/>	2.4 GHz Additional Client Transmit Power Attenuation (0-15dB):		

Advanced Settings			
<input type="checkbox"/>	Module Name	Value	Notes
<input type="checkbox"/>	Support Mesh Links to Downstream Routers on 2.4 GHz Interface:		
<input type="checkbox"/>	Support Mesh Links to Downstream Routers on 5.8 GHz Interface:		
<input type="checkbox"/>	Support Mesh Links to Downstream Routers on 4.9 GHz Interface:		
<input type="checkbox"/>	Support Mesh Links to Upstream Routers on 2.4 GHz Interface:		Ver. pre 7.1 ⁺ ₁
<input type="checkbox"/>	Support Mesh Links to Upstream Routers on 5.8 GHz Interface:		Ver. pre 7.1 ⁺ ₁
<input type="checkbox"/>	Support Mesh Links to Upstream Routers on 4.9 GHz Interface:		Ver. pre 7.1 ⁺ ₁
<input type="checkbox"/>	2.4 GHz RTS Threshold:		
<input type="checkbox"/>	5.8 GHz RTS Threshold:		
<input type="checkbox"/>	4.9 GHz RTS Threshold:		
<input type="checkbox"/>	2.4 GHz Maximum Link Distance:	4.2 km (max delay: 48us)	
<input type="checkbox"/>	5.8 Maximum Link Distance:	4.2 km (max delay: 48us)	
<input type="checkbox"/>	4.9 Maximum Link Distance:	4.2 km (max delay: 48us)	
<input type="checkbox"/>	Transmit Diversity (2.4 GHz):	auto	
<input type="checkbox"/>	Evil Twin Detection:		
<input type="checkbox"/>	DoS Detect Threshold:		
<input type="checkbox"/>	Mobile Node Forced Standalone:		
<input type="checkbox"/>	Low Path Quality Watermark:		
<input type="checkbox"/>	High Path Quality Watermark:		

TABLE 19 Wireless Page Parameters

Field	Range, <i>Default</i>	Description
Mesh ID Confirm Mesh ID	---	16-character code that must be the same for all routers in your network. To support multi-subnet roaming, the Mesh ID must be the same for all networks in the roaming domain, so when you first access the Configuration Utility, you are prompted to change the value.
<i>Channel Configuration</i>		
Auto Channel (entry for each wireless interface)	Enabled <i>Disabled</i>	Indication of whether auto channel functionality is enabled or disabled.
Channel List (entry for each wireless interface)	2.4 GHz: 1, 6, 11 5.8 GHz: 149, 153, 157, 161, 165 5.4 GHz: 100, 104, 108, 112, 116	Available channels for auto channel. Active only if Auto Channel is enabled.
Channel (entry for each wireless interface)	2.4 GHz: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, <i>auto</i> 5.8 GHz: <i>149</i> , 153, 157, 161, and 165 5.4 GHz: <i>100</i> , 104, 108, 112, 116 4.9 GHz: <i>9220</i> , 9620	Operating channel. Active only if Auto Channel is disabled. The default channel for the 5.4 GHz band is determined automatically based on the calibration (country) code.
Maintenance Window	---	Date and time at which the gateway begins a channel scan. Active only if channel is auto.
Maintenance Interval	0-30, <i>0</i>	Frequency (days) at which the gateway performs the channel scan. Active only if channel is auto.
<i>Rate and Power Configuration</i>		
Mesh Control Transmit Rate (entry for each wireless interface)	<i>Auto</i> Fixed (Mesh Control Tx Rate)	Bit rate for data traffic between routers. See PowerCurve description for additional information. This field is active only if PowerCurve is disabled.

TABLE 19 Wireless Page Parameters

Field	Range, <i>Default</i>	Description
PowerCurve	On Off	Implementation of adjustments for efficient network resource utilization. Choosing on activates the following parameter changes and restrictions: <ul style="list-style-type: none"> • Mesh unicast transmit rate is automatically set to auto. • Power attenuation settings apply only to router-router control traffic. You can continue to assign data rates for mesh control transmission. Turning power curve adjustments off results in the following change: <ul style="list-style-type: none"> • Power attenuation settings apply to all data and control traffic.
Mesh Unicast Transmit Rate	Auto Fixed (Mesh Control Tx Rate)	Bit rate for data traffic between routers. See PowerCurve description for additional information. This field is active only if PowerCurve is disabled.
Transmit Power Attenuation	0-15 dB 0 dB	This is a global power attenuation that applies to all traffic.
Additional Attenuation for 802.11 Beacons and Management Frames (entry for each wireless interface)	0-15 dB 0 dB	Additional attenuation added on top of the Maximum Power Attenuation and applied to 802.11 beacons and management traffic.
Additional Client Transmit Power Attenuation	0 -15 dB	Determines the reduction in power transmitted by the router radio. Applies only to client links. The total client attenuation is Transmit Power Attenuation + Additional Client Transmit Power Attenuation
<i>Advanced Settings</i>		
Support Mesh Links to Downstream Routers (entry for each wireless interface)	Enabled Disabled	Indication of whether downstream meshing is enabled for each radio. We recommend that you enable this field to support downstream meshing for all applications.

TABLE 19 Wireless Page Parameters

Field	Range, <i>Default</i>	Description
Support Mesh Links to Upstream Routers (entry for each wireless interface, node only)	<i>Enabled</i> Disabled	<p>Indication of whether downstream meshing is enabled for each radio.</p> <p>We recommend that you enable this field for all except 4.9 GHz public safety applications. For 4.9 GHz public safety applications, choose the following settings:</p> <ul style="list-style-type: none"> • Enabled---for 802.11b/g interface, static and mobile nodes • Disabled---for 802.11a interface (4.9 GHz), static and mobile nodes.
RTS Threshold (entry for each wireless interface)	<i>2346</i> bytes	<p>Indicates the packet size for collision protection. When the request to send (RTS) packet size is larger than the threshold, collision protection is provided.</p> <p>Each protected packet is preceded by an RTS (Request To Send) frame. Default 2346 is recommended except in congested environments, in which a setting between 500 and 1500 may improve reliability. Due to overhead and possible loss in throughput, settings below 500 are not recommended.</p>
Maximum Link Distance (entry for each wireless interface)	5 - 20, <i>4.2</i>	Maximum distance permitted for a single wireless link (km). Increase this value to avoid excessive timeouts in areas where links between routers are long.
Transmit Diversity (2.4 GHz) (802.11b/g interface only; not supported on 6310 and 6320 routers)	<i>auto</i> , main, aux	<p>Antenna selection for transmission:</p> <ul style="list-style-type: none"> • Auto – automatically pick the Tx (transmit) antenna (automatic transmit diversity) • Main – use the main antenna only for transmit • Aux – use the auxiliary antenna only for transmit <p>Note: <i>The router receives wireless signals on both antennas.</i></p>
Evil Twin Detection	Enabled <i>Disabled</i>	<p>Indication of whether unauthorized devices that advertise an ESSID used by the Tropos mesh are detected.</p> <p>If an evil twin is detected, an SNMP inform is sent to Tropos Control EMS, which reports the event.</p>

TABLE 19 Wireless Page Parameters

Field	Range, <i>Default</i>	Description
DoS Detect Threshold	0 - 10,000	<p>Number of management frames that are acceptable to be sent within 5 seconds.</p> <p>If this number is exceeded, a DoS attack is assumed and an SNMP inform is sent to Tropos Control EMS, which reports on the activity. The default value of 0 disables the feature.</p> <p>The following will trigger the DoS feature and send an SNMP inform to Tropos Control EMS:</p> <ul style="list-style-type: none"> • The number of management frames set in the DOS threshold is exceeded. • A broadcast deauthentication packet is detected. • A spoofing MAC address of a router is detected. <hr/> <p>Note: <i>The appropriate DoS threshold depends upon network conditions. If the threshold is too high, you might miss notification of a DoS attack; if the threshold is too low, unnecessary SNMP informs might be generated. For example, in a busy network with crowded channels, a threshold in the range of 500 or more may be appropriate.</i></p>
Mobile Node Forced Standalone (mobile node only)	Enabled Disabled	<p>When enabled, the mobile node is forced to stay in standalone mode when the path quality falls out of the range indicated in the watermark settings.</p> <p>For example, if the watermark levels are 40 and 60 and path quality of the mobile node falls to 30, then the mobile node is forced to stay in standalone mode until path quality reaches 60 level.</p>
Low Path Quality Watermark (mobile node only)	--	Path quality level (1-80) that forces the mobile node to standalone mode.
High Path Quality Watermark (mobile node only)	--	Path quality level (1-100) that, if reached, causes the mobile node to leave standalone mode.

Client Access

The settings on the Client Access Configuration page (Figure 23) allow you to configure SSIDs, authentication, and other settings that control client access to the wireless network.

Table 20 describes the settings on the page.

FIGURE 23 Client Access Page (Excerpt)

Client Access

0 Gateways 0 Nodes 0 MobileNodes are selected [Adjust Selection](#)
Please select routers to provision

Multi-SSID

SSID	Hidden	Authentication	PSK Passphrase	Confirm PSK Passphrase	BSSID index (0-15)	Primary ESSID Preferred	VLAN
	Disabled	Open			0	No	No

Standalone SSID Configuration

Module Name	Value	Notes
SSID:	Standalone	Ver: 7.1
Authentication Type:	open	Ver: 7.1
PSK Passphrase:		Ver: 7.1
Confirm PSK Passphrase:		Ver: 7.1

WEP Configuration

Module Name	Value	Notes
2.4 GHz WEP Type:	64bit	*1
2.4 GHz WEP Key:		*1 *2
5.8 GHz WEP Type:	64bit	*1
5.8 GHz WEP Key:		*1 *2
4.9 GHz WEP Type:	64bit	*1
4.9 GHz WEP Key:		*1 *2

* 1: WEP Type and WEP Key have to be provisioned at the same time.

* 2: Ensure that the WEP key corresponds to the WEP type:
 - For 64bit, enter 5 ascii characters or 10 hexadecimal number.
 - For 128bit, enter 13 ascii characters or 26 hexadecimal number.

TABLE 20 Client Access Page Parameters

Field	Range, <i>Default</i>	Description
<i>Multi-ESSID</i>		

TABLE 20 Client Access Page Parameters (*continued*)

Field	Range, Default	Description
SSID	---	Enter a name that uniquely identifies the network on which the router is operating. Note: <i>To fully support SSID-based VLANs, configure the same VLAN ID and SSID-VLAN mappings on each router in the network.</i>
Hidden	No Yes	Choose whether the router will include (No) or exclude (Yes) the SSID from the packets it transmits. Hiding the SSID makes it more difficult for unauthorized devices to obtain the SSID.
Authentication	Open WEP WPA1-PSK WPA1-1x WPA2-PSK AES only WPA1&2-PSK AES only WPA2-PSK WPA1&2-PSK WPA1-1X AES only WPA1&2-1X AES only WPA2-1X WPA1&2-1X	Select the authentication method.
PSK Passphrase Confirm PSK Passphrase	---	Enter a passphrase, if you choose one of the WPA-PSK options.
BSSID Index (MAC Address)	0-15, 0	Indicates the BSSID index used for this secondary ESSID.
Primary ESSID Preferred	No Yes	Indicates whether this ESSID is the primary ESSID for this BSSID.
VLAN	---	Choose the VLAN for this SSID. Note: <i>To fully support SSID-based VLANs, configure the same VLAN ID and SSID-VLAN mappings on each router in the network.</i>
2.4 GHz 5.8 GHz 4.9 GHz	---	Wireless interfaces for this SSID.

TABLE 20 Client Access Page Parameters (*continued*)

Field	Range, Default	Description
Standalone SSID		
SSID	---	Use this entry to configure a single SSID. Enter a name that uniquely identifies the network on which the router is operating. Choose an authentication type and enter a PSK passphrase, as described above in this table.
Authentication	Open WEP WPA1-PSK WPA1-1x WPA2-PSK AES only WPA1&2-PSK AES only WPA2-PSK WPA1&2-PSK WPA1-1X AES only WPA1&2-1X AES only WPA2-1X WPA1&2-1X	Select the authentication method.
PSK Passphrase Confirm PSK Passphrase	---	Enter a passphrase, if you choose one of the WPA-PSK options.
WEP Configuration		
WEP Type (entry for each wireless interface)	Hex64bit Hex128bit ASCII64bit ASCII128bit	Choose the type of WEP key: <ul style="list-style-type: none"> • Hex64bit---Hexadecimal string with 64-bit encryption key (40-bit encryption plus 24-bit initialization number) • Hex128bit---Hexadecimal string with 104-bit encryption key (40-bit encryption plus 24-bit initialization number) • ASCII64bit---ASCII string with 64-bit encryption key (40-bit encryption plus 24-bit initialization number) • ASCII128bit---ASCII string with 104-bit encryption key (40-bit encryption plus 24-bit initialization number)

TABLE 20 Client Access Page Parameters (*continued*)

Field	Range, Default	Description
WEP Key (entry for each wireless interface)	---	Enter the encryption key, which is required for each WEP type. The format depends on the WEP type: <ul style="list-style-type: none"> • Hex64bit---Enter 5 hexadecimal characters • Hex128bit---Enter 5 hexadecimal characters • ASCII64bit---Enter 10 ASCII characters • ASCII128bit---Enter 26 ASCII characters <hr/> Note: <i>After you create a key, use it to program all client devices and routers on the wireless network.</i>
RADIUS		
RADIUS Server	---	Enter the IP address of the RADIUS server that authenticates user requests for network access, if WPA1-1X or WPA2-1X (or both) are selected as an authentication type.
RADIUS Authentication Port	1812	Enter the port on the RADIUS server to be used for client authentication requests, if WPA1-1X or WPA2-1X (or both) are selected as an authentication type.
RADIUS Secret Confirm RADIUS Secret	mysecret	Enter a shared secret code to verify the connection between the RADIUS server and the router, if WPA1-1X or WPA2-1X (or both) are selected as an authentication type.
RADIUS Accounting Server	0.0.0.0	Enter the IP address of the RADIUS accounting server, if RADIUS accounting services are used to log client activity. An IP address of 0.0.0.0 disables this feature.
RADIUS Accounting Port	1813	Enter the port on the accounting server to be used for RADIUS accounting requests, if RADIUS accounting services are used to log client activity.
RADIUS Accounting Secret Confirm RADIUS Accounting Secret	---	Enter the shared secret code to verify the connection between the accounting server and the router, if RADIUS accounting services are used to log client activity.
RADIUS Accounting Interval	900	Enter an interval (seconds) between RADIUS accounting updates, if RADIUS accounting services are used to log client activity. an interval of 0 disables interim updates.

TABLE 20 Client Access Page Parameters (*continued*)

Field	Range, Default	Description
Delay RADIUS Accounting Start for Authentication and IP	Yes No	Choose whether the RADIUS accounting session will begin when the client associates to the router (No) or when the client has associated, been authenticated and obtained an IP address (Yes). Because debugging information is gathered as part of the debugging session, choosing No may help in troubleshooting authentication or IP addressing issues.
IPSec for RADIUS	Disabled Enabled	Choose whether to enable IPSec security for communication with the RADIUS server.
IPSec Tunnel Endpoint	--	Specify the IP address of the system that terminates the RADIUS tunnel endpoint that starts at the router.
IPSec Preshared Key Confirm IPSec Preshared Key		Specify the preshared key for authentication of the IPSec tunnel.
Advanced Settings		
Client Access Rule	Deny Allow	Choose the type of rule: <ul style="list-style-type: none"> Deny---Clients in the list are denied access; all others are permitted to associate. Allow---Only the clients in the list are permitted to associate.
802.11b Support	Disabled Short Preamble Long Preamble Mixed	Choose a value according to whether the router must operate with older 802.11b devices that require a long preamble in the 802.11 frame format. <ul style="list-style-type: none"> Short Preamble is more efficient, but incompatible with some older 802.11 devices. Long Preamble ensures compatibility with most early models of wireless clients. Mixed allows 802.11b clients using short or long preamble to associate. Disabled prevents all 802.11b clients from associating with the router. <p>Note: <i>This setting does not apply to mobile routers.</i></p>
Beacon Interval (entry for each wireless interface)	250 (802.11b/g) 100 (801.11a/n)	Choose the time interval between the transmission of 802.11 beacons by the router (ms).
Beacon Rate (entry for each wireless interface)	11 (802.11b/g) 6 (801.11a/n)	Enter the rate at which the router transmits 802.11 beacons (Mbps).

TABLE 20 Client Access Page Parameters (*continued*)

Field	Range, Default	Description
IP to VLAN Mapping		To create or edit IP to VLAN mappings, enter the VLAN ID and the subnet (x.x.x.x/n format). Click Add after each addition. Note: Before you create IP to VLAN mappings, enable and define VLANs on the IP and VLAN page. See "IP and VLAN Page" on page 81.

DHCP Server

The DHCP Server page (Figure 24) lists DHCP parameter settings for routers. Table 21 lists all parameters on the page along with an explanation of the purpose of each and how it should be interpreted and used.

FIGURE 24 DHCP Server

DHCP Server

0 Gateways 0 Nodes 0 MobileNodes are selected [Adjust Selection](#)
Please select routers to provision

<input type="checkbox"/>	Module Name	Value	Notes
<input type="checkbox"/>	Network Address Translation:	Enabled	
<input type="checkbox"/>	DHCP server on board:	Enabled	
<input type="checkbox"/>	DHCP Relay To:		
<input type="checkbox"/>	Starting Address:		
<input type="checkbox"/>	Ending Address:		
<input type="checkbox"/>	Netmask:		
<input type="checkbox"/>	Domain Name Server 1:		
<input type="checkbox"/>	Domain Name Server 2:		
<input type="checkbox"/>	Domain Name Server 3:		
<input type="checkbox"/>	Lease Duration(sec):		
<input type="checkbox"/>	WINS Server:		
<input type="checkbox"/>	DHCP MAC Address Filter:	Enabled	

TABLE 21 DHCP Server Page Parameters

Field	Range, <i>Default</i>	Description
Network address translation	Enabled <i>Disabled</i>	Choose whether to enable Network Address Translation (NAT) for IP address assignment. Enable NAT if either of these conditions apply: <ul style="list-style-type: none"> You want to use internal addressing within your wireless network. The network has a single gateway that represents all internal clients to the external network. <hr/> <p>Note: <i>When you enable NAT, the internal DHCP server on the gateway is automatically enabled.</i></p>
DHCP Server On Board	Enable <i>Disable</i>	Indicates whether the DHCP server is enabled on the router.
DHCP Relay To	--	Specifies the IP address of the DHCP server that receives the relayed DHCP requests.
Starting Address	--	Specifies the first IP address in the address range for the Tropos gateway.
Ending Address	--	Specifies the last IP address in the address range for the Tropos gateway DHCP server; the address range should be large enough to accommodate all routers and users on the network.
Netmask	--	Specifies the subnet mask for the IP addresses provided by the DHCP server.
Domain Name Server	--	Specifies the IP address of the DNS server that supplies name resolution for the DHCP server.
DHCP Server Lease Time	--	Specifies the time in seconds before the IP address expires and must be renewed (it is recommended that you assign lease times of at least 12 hours, or 43200 seconds).
WINS Servers	--	Specifies the IP address of a Windows name server to be passed on to DHCP clients.
MAC Address Filter	Enabled <i>Disabled</i>	Indicates whether MAC address filtering is enabled.

SNMP

The SNMP page (Figure 25) lists the SNMP community for the router and specifies where to send SNMP informs. To use Tropos Control to manage the router, you must register Tropos Control to allow SNMP access to the router and to receive SNMP informs. This allows access to the SNMP MIBs and use of Tropos Control. In addition, registering the IP address allows SNMP

informs to be sent to that address. You can configure multiple IP addresses if you want other addresses to have SNMP access and the ability to receive informs.

Table 22 lists the settings on the page along with an explanation of the purpose of each and how they should be interpreted.



Note

Tropos Control does not support encrypted traps.

FIGURE 25 SNMP

SNMP

0 Gateways 1 Nodes 0 MobileNodes are selected [Adjust Selection](#)

Golden Device: (default value comes from this device)
Name: LuckyLake **Type:** node **ID:** 00041 **IP:** 172.20.125.225

Trap Destinations

IP Address	Community
root	●●●●●●●●

* 1: This configuration is applicable to Routers prior to version 7.5

SNMP Usm User Table

Security Username	Auth Type	Auth Key	Priv Type	Priv Key
openUser	No Authentication		No Privacy	

[Remove](#)

No Authentic: No Privacy

* 1: This configuration is applicable to Routers from version 7.5

SNMPv3 Trap Destinations

Target Address Name	Target Address	User Name
openuser1	172.20.125.149	openUser

[Remove](#)

* 1: This configuration is applicable to Cell Relays and Routers from version 7.5

SNMPv3 Enable Management Server

	Module Name	Value	Notes
<input type="checkbox"/>	SNMP:	Enabled	

* 1: This configuration is applicable to Routers from version 7.5.0.3

Allowed Management Servers

EMS IP
<input type="text"/>

TABLE 22 SNMP Page Parameters

Field	Range, Default	Description
Trap Destinations	--	IP address and SNMP community of the server that receives SNMP traps. These settings are for SNMPv2 traps, which apply only to routers running pre-Release 7.5 software.
SNMP User Table	--	SNMP user information: <ul style="list-style-type: none"> • Security User Name - SNMP user • Auth Type - MD5, SHA1, or No Authentication • Auth Key - for the authentication protocol • Priv Type - AES, DES, or none • Priv Key - Privacy key for the privacy type These settings are for SNMPv3 and apply only to routers running Release 7.5 and later software.
SNMPv3 Trap Destinations	--	Name, target IP address, and user name for each SNMP trap destination. These settings are for SNMPv3 and apply only to routers running Release 7.5 and later software.
SNMP Enable Management Servers	Enabled <i>Disabled</i>	Indication of whether SNMP is enabled or disabled for management.
Allowed Management Servers	--	IP address of each Tropos Control server that is allowed to manage this device.

Time

The time page ([Figure 26](#)) contains settings for Network Time Protocol (NTP) servers used to synchronize time on the router, and may also be used to set the time manually. [Table 23](#) lists parameters and tasks on the page.

FIGURE 26 Time Page

Time

0 Gateways 2 Nodes 0 MobileNodes are selected [Adjust Selection](#)

Golden Device: (default value comes from this device)
Name: CS-NE-entrance-cell **Type:** node **ID:** 19134 **IP:** 172.20.125.84

<input type="checkbox"/>	Module Name	Value	Notes
<input type="checkbox"/>	NTP Server:	<input type="text" value="192.43.244.18"/>	*1 *2
<input type="checkbox"/>	Time Zone:	<input type="text" value="US/Pacific"/>	
<input type="checkbox"/>	Set Router Time:	<input type="text" value=""/>	

* 1: Up to 3 time (ntp) server addresses (separated by comma) can be configured.
* 2: For pre 7.5 release routers, it can be "," separated string of 3 ip addresses. Otherwise it can be "." separated string of 3 ip addresses or host names

TABLE 23 Time Page Parameters and Tasks

Field	Default	Description
NTP Server	---	Indicates the IP address or domain name of an NTP server. If NTP is used, at least one server must be specified; specify up to three servers by entering comma-separated IP addresses or host names.
Time Zone	UTC	Presents a list of time zones. Note: <i>Universal Time (UTC) is the same as Greenwich Mean Time.</i>
Set Router Time	---	Permits manual setting of the date and time using the pull-down lists. Manual time changes take effect immediately. Click <input type="button" value="..."/> to open a calendar and select a date and time.

DHCP Clients

The DHCP MAC Filter/Reservation page (Figure 27) contains parameters to configure the internal DHCP server of the Tropos gateway in order to limit assignment of IP addresses to wireless clients. Table 24 lists the settings on the page, which can be opened by clicking **DHCP Clients** on the side menu.

FIGURE 27 DHCP Clients

DHCP Clients

0 Gateways 0 Nodes 0 MobileNodes are selected [Adjust Selection](#)
Please select routers to provision

DHCP ACL

MAC

DHCP Reservation

IP | MAC

TABLE 24 DHCP Clients Page Settings

Field	Range, Default	Description
MAC	---	Specifies the MAC address of the client to be accepted. Click Add to include this entry in the list.

TABLE 24 DHCP Clients Page Settings (*continued*)

Field	Range, Default	Description
IP	---	Specifies the IP address to be reserved for the client with the specified MAC address. The reserved IP addresses must be in the range of the DHCP server. Reservations simply reserve an IP address for a particular MAC address; they do not control access. Therefore, do not enable ACL when adding reservations unless you would like to control access as well. Click Add to include this entry in the list.
MAC	---	Specifies the MAC address to be reserved for the client with the specified IP address. Click Add to include this entry in the list.

Static IP Client

The Static IP Client Configuration page ([Figure 28](#)) contains settings for clients that require static IP addresses rather than DHCP-supplied addresses. The Static IP Client Configuration page also provides the ability to configure static IP addresses for clients behind customer premise equipment (CPE), such as Wireless-to-Ethernet bridges. [Table 25](#) lists the parameters on the page.

-
- Note**
If you use auto-detection, you must enable it on all the gateways and nodes in the wireless routing domain (WRD). If the WRD is changed in Tropos Control, all gateways and nodes must be deleted from the Tropos Control using the Configuration View
-
- Note**
For static IP clients, you must add the client entries on all gateways in the wireless routing domain in order for the clients to be able to roam across the full domain.
-

FIGURE 28 Static IP Clients Page

Static IP Client

0 Gateways 0 Nodes 0 MobileNodes are selected [Adjust Selection](#)
Please select routers to provision

<input type="checkbox"/>	Module Name	Value	Notes
<input type="checkbox"/>	Auto Detect Wireless Clients with Static IP:	<input type="text"/>	

Wireless Clients with Static IP Addresses

Client MAC Address	Static IP Address	CPE MAC Address
<input type="text"/>	<input type="text"/>	<input type="text"/>

Wired Clients with Static IP Addresses

Permanent Static Routes will be added for these wired clients
Wired Clients should be configured unique for each router
For pre 7.1.2 routers, Client MAC Address and CPE MAC Address are required.

Static IP Address	Client MAC Address	CPE MAC Address	Vlan Name
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

TABLE 25 Static IP Client Page Parameters

Field	Range, <i>Default</i>	Description
Auto Detect Static Clients	Enabled <i>Dis-abled</i>	If enabled, allows the router to automatically detect the presence of static IP clients and permit them to be routed, even though their addresses are not explicitly entered. If security is an issue and you do not want to route clients that are not explicitly recognized, you can disable this feature.
Client MAC Address	---	Specifies the MAC address of the client to be added to the Static IP list.
Static IP Address	---	Specifies the IP address of the client to be added to the Static IP list.
CPE MAC Address	---	Specifies the MAC address of any customer premise equipment (CPE), in addition to the MAC and IP addresses of the client connected to the CPE.
Client MAC Address	---	Specifies the MAC address of the client to be added to the Static IP list.
Static IP Address	---	Specifies the IP address of the client to be added to the Static IP list.

TABLE 25 Static IP Client Page Parameters (*continued*)

Field	Range, Default	Description
CPE MAC Address	---	Specifies the MAC address of any customer premise equipment (CPE), in addition to the MAC and IP addresses of the client connected to the CPE.
VLAN Name	---	Specifies the VLAN for the wired client.

Packet Filtering

Packet Filtering ([Figure 29](#)) determines the types of packets forwarded or rejected by the router. Forwarding applies to packets that pass through the router, not those that begin or terminate at the router. Usage for the Packet Filter Forwarding page differs according to whether the default packet filter forwarding policy is Permitted or Denied (see [Table 26](#)).

FIGURE 29 Packet Filtering

Packet Filtering

0 Gateways 1 Nodes 0 MobileNodes are selected [Adjust Selection](#)**Golden Device:** (default value comes from this device)

Name: LuckyLake Type: node ID: 00041 IP: 172.20.125.225

<input type="checkbox"/>	Module Name	Value	Notes
<input type="checkbox"/>	Packet Forwarding:	Allowed	

 Predefined Forwarding Rules

This table takes effect only when packet forwarding is denied.

Enabled	Protocol Type	Permit to/from the address
---------	---------------	----------------------------

 Customized Forwarding Rules

This table takes effect only when packet forwarding is denied.

Name	Protocol	Source IP	Source Mask	Source Port	Destination IP	Destination Mask	Destination Port	
<input type="text"/>	any	any	any	any	any	any	any	Add

* 1: Protocol should be a number or tcp/udp.

 Packet Forwarding Deny Rules

This table takes effect only when packet forwarding is allowed.

Name	Protocol	Source IP	Source Mask	Source Port	Destination IP	Destination Mask	Destination Port	
<input type="text"/>	any	any	any	any	any	any	any	Add

* 1: Protocol should be a number or tcp/udp.

Submit **Reset**

TABLE 26 Packet Filtering Page Parameters

Field	Range, <i>Default</i>	Description
Packet Forwarding	<i>Allowed</i> Denied	If enabled, allows all packets except those explicitly blocked. If disabled, blocks all packets except those explicitly permitted.
Predefined Forwarding Rules	--	Indicates whether this protocol has a forwarding rule applied. The following information applies to each rule: <ul style="list-style-type: none"> • Enabled--Indicates whether the rule is active. • Protocol Type---Indicates the protocol to which the filtering applies. See Table 27. • Permit to/from the address---Specifies the IP address or subnet to which the filtering applies. (Format a.b.c.d).
Customized Forwarding Rules	--	Indicates whether a custom forwarding rule is applied. The following information applies to each rule: <ul style="list-style-type: none"> • Name---Custom name for the filtering rule. • Protocol---Protocol to be filtered. • Source IP---IP address of the packet source. • Source Mask (bits)---Subnet mask for the packet source. • Source Port---Port for the packet source. • Destination IP---IP address of the packet termination point. • Destination Mask (bits)---Number of maskbits for the IP address where the packet will terminate. • Destination Port---Port where the packet will be received.

TABLE 26 Packet Filtering Page Parameters (*continued*)

Field	Range, <i>Default</i>	Description
Packet Forwarding Deny Rules	--	<p>Indicates whether a deny rule is applied. The following information applies to each rule:</p> <ul style="list-style-type: none"> • Name---Custom name for the filtering rule. • Protocol---Protocol to be filtered. • Source IP---IP address of the packet source. • Source Mask (bits)---Subnet mask for the packet source. • Source Port---Port for the packet source. • Destination IP---IP address of the packet termination point. • Destination Mask (bits)---Number of maskbits for the IP address where the packet will terminate. • Destination Port---Port where the packet will be received.

TABLE 27 Packet Forwarding - Standard Permit Rules

Field	Description
DHCP (Dynamic Host Configuration Protocol)	UDP ports 67/68
DNS (Domain and Host Name Service)	UDP ports 42/53
Cisco (Cisco VPN 3000 Concentrator Series)	UDP ports 500/10000
ICMP (Ping and Traceroute)	Not applicable
HTTPS (Secure HTTP)	TCP port 443
SSH (Secure Shell)	TCP port 22
IPSec (Internet Protocol Security)	protocol 50 UDP port 500
POP3 (Post Office Protocol 3)	TCP port 110
HTTP (hypertext transfer protocol)	TCP port 80
SMTP (simple mail transfer protocol)	TCP port 25
Telnet	TCP port 23
SNMP	TCP port 161 and 162

**Caution**

If DHCP is disabled, client devices and Tropos nodes cannot obtain the DHCP lease required for operation. If HTTPS is disabled, all HTTPS traffic will be dropped.

P2P Blocking

Use the Peer-to-Peer Blocking page (Figure 30) to block clients in the same subnet or in different subnet (VLANs) from communicating with each other. Table 28 lists parameters on the page.

FIGURE 30 Peer-to-Peer Blocking Configuration Page

P2P Blocking

0 Gateways 0 Nodes 0 MobileNodes are selected [Adjust Selection](#)

Please select routers to provision

Peer to Peer Blocking

name	Peer 1 IP	Peer 1 Mask	Peer 2 IP	Peer 2 Mask
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

* 1: Mask should be 1-32 or any.

TABLE 28 Peer-to-Peer Blocking Parameters

Field	Range, <i>Default</i>	Description
Name	---	Text name for the peer-to-peer block rule
Peer1 IP	any	IP address of one of the peers
Peer1 Mask	any	Subnet mask that applies to the first peer IP address (bits)
Peer2 IP	any	IP address of the second peer
Peer2 Mask	any	Subnet mask that applies to the second peer IP address (bits)

Multi-Subnet Roaming

The Multi-Subnet Roaming page (Figure 20) identifies the list of gateways available for roaming across multiple subnets. Table 29 lists parameters on the page.

Note

During multi-subnet roaming, the client's traffic is routed through its home gateway (to which it was originally associated). If the home gateway loses its uplink while an associated client is roaming, the client will lose connectivity. To restore connectivity, the old gateway must become available again or the client must obtain an IP address from the new gateway.

FIGURE 31 Multi-Subnet Roaming Page

Multi-subnet Roaming

1 Gateways 0 Nodes 0 MobileNodes are selected [Adjust Selection](#)

Golden Router: (default value comes from this Router)
 Name: 532019967 Type: gateway ID: 19967 Wlan0 IP: 10.11.11.179

Gateway List

Gateway IP	Mask
<input type="text"/>	<input type="text"/>

Additional Roaming Subnets
 Use this for wired clients, sub-interface subnets

Subnet	Mask
<input type="text"/>	<input type="text"/>

TABLE 29 Multi-Subnet Roaming Page Parameters

Field	Range, Default	Description
Gateway IP	---	Specifies the IP address of a gateway to make available for roaming.
Mask	---	Specifies the subnet mask for the gateway.
Subnet Route	---	Specifies the subnet of a mobile node or downstream interface associated with the subnet of this gateway.
Subnet Mask	---	Specifies the subnet mask of a mobile node or downstream interface associated with the subnet of this gateway.
Add/Delete	---	Adds an entry to the list or deletes one from the list.

Backhaul Routing

The Backhaul Routing page (Figure 20) permits selection of advanced routing protocols such as Border Gateway Protocol (BGP) to support backhaul traffic. The Tropos gateway establishes BGP sessions with configured neighbors and exchanges routes for all multi-subnet roaming clients. The clients' upstream traffic is sent directly to the neighbor without requiring tunneling between the home and foreign subnets.

Table 29 lists parameters on the page.

FIGURE 32 Backhaul Routing Page

Backhaul Routing

0 Gateways 0 Nodes 0 MobileNodes are selected [Adjust Selection](#)
Please select routers to provision

<input type="checkbox"/>	Module Name	Value	Notes
<input type="checkbox"/>	Backhaul Routing Type:	Disabled	

BGP Neighbors

Neighbor Name	Neighbor IP	Local ASN	Remote ASN	Service/VLAN ID ^{* 1}	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

* 1: When VLANs are enabled, Service/VLAN ID should be a valid VLAN ID.

TABLE 30 Backhaul Routing Page Parameters

Field	Range, Default	Description
Backhaul Routing Type	<i>Disabled</i> Enabled	Specifies whether gateway-to-gateway tunnels are automatically set up for multi-subnet roaming.
Neighbor Name	---	Specifies the name of an Internet or IP router that will serve as a BGP neighbor.
Neighbor IP	---	Specifies the IP address of the neighbor.
Local AS Number	---	Identifies the assigned local autonomous system (AS) number for the BGP neighbor.
Remote AS Number	---	Identifies the assigned remote autonomous system (AS) number for the BGP neighbor.

TABLE 30 Backhaul Routing Page Parameters (*continued*)

Field	Range, Default	Description
Remote AS Number	---	Identifies the assigned remote autonomous system (AS) number for the BGP neighbor.
Service/VLAN ID	---	Specifies the VLAN that is served by the BGP neighbor. If VLANs are disabled, leave the Service/VLAN ID field blank, or enter 0.

Rate Limiting

Rate Limiting page ([Figure 33](#)) contains settings to limit the bandwidth available to individual clients. Rate limiting provides the joint benefits of limiting the impact of denial of service (DoS) attacks and users who consume too much bandwidth. Users can exceed bandwidth in brief bursts, but if they send more than the permitted amount of data (trigger) in a specified period of time, they are temporarily subjected to rate limits.

FIGURE 33 Rate Limiting Page

Rate Limiting

0 Gateways 0 Nodes 0 MobileNodes are selected [Adjust Selection](#)
 Please select routers to provision

<input type="checkbox"/>	Module Name	Value	Notes
<input type="checkbox"/>	Airtime Congestion Control:	Enabled	

This enforces a selective cap on anyone who exchanges too much data for too long. The caps are per association, so multiple IP addresses behind the same bridge share a cap. Bits count 802.11 frame length, not just IP datagrams.

<input type="checkbox"/>	Module Name	Value	Notes
<input type="checkbox"/>	Throughput Rate Limiting:	Enabled	
<input type="checkbox"/>	Downstream Trigger (kbits):		
<input type="checkbox"/>	Upstream Trigger (kbits):		
<input type="checkbox"/>	Trigger Time (sec):		*1
<input type="checkbox"/>	Downstream Cap (kbps):		
<input type="checkbox"/>	Upstream Cap (kbps):		
<input type="checkbox"/>	Minimum Cap Duration (sec):		*1

*1: Rounded up to the nearest 10 seconds

 Throughput Rate Limiting Multipliers

Only the first multiplier matched is used. This multiplier is for egregious usage (both trigger and selective cap). Durations are unmodified.

SSID	2.4GHz	5.8GHz	4.9GHz	Multiplier

 Qos Subnet Differentiated Service Classes

Only the first multiplier matched is used. This multiplier is for egregious usage (both trigger and selective cap). Durations are unmodified.

IP	Mask	Multiplier
<input type="text"/>	<input type="text"/>	<input type="text"/>

TABLE 31 Rate Limiting Parameters

Field	Range, <i>Default</i>	Description
Airtime Congestion Control	Enabled <i>Dis-abled</i>	Indication of whether congestion events are detected and averted. If enabled, allows networks to operate closer to their maximum capacity.
Downstream Trigger (kbits)	---	Total quantity of data (kbits) that triggers the rate limit if the client receives that amount of data in the time interval specified in the Trigger Time field.
Upstream Trigger (kbits)	---	Total quantity of data (kbits) that triggers the rate limit if the client transmits that amount of data in the time specified in the Trigger Time field.
Trigger Time (seconds)	---	Length of time used to determine whether to trigger rate limits (seconds).
Downstream Cap (kbits/sec)	---	Rate limit for data sent downstream to the client (kbits/sec).
Upstream Cap (kbits/sec)	---	Rate limit for data sent upstream from the client (kbits/sec).
Minimum Cap Duration (seconds)	---	Number of seconds that the rate limit applies, if triggered.
ESSID	---	ESSID to which a rate limiting multiplier applies.
Wireless Interface	---	Wireless interfaces for this SSID.
Multiplier	.2 - 10, <i>1</i>	Rate limiting multiplier that applies to the To client cap and From client cap fields; traffic to and from the subnet is restricted to the client caps times the multiplier. Examples: <ul style="list-style-type: none"> • Multiplier 0: No traffic permitted to or from the subnet • Multiplier 2: Rate limit for the subnet is equal to two times the To client cap and From client cap settings
IP	---	IP address of the subnet to which a rate limiting multiplier applies.
Mask	---	Subnet mask for the subnet to which a rate limiting multiplier applies.

TABLE 31 Rate Limiting Parameters (*continued*)

Field	Range, <i>Default</i>	Description
Multiplier	.2 - 10, <i>1</i>	Rate limiting multiplier that applies to the To client cap and From client cap fields; traffic to and from the subnet is restricted to the client caps times the multiplier. Examples: <ul style="list-style-type: none"> • Multiplier 0: No traffic permitted to or from the subnet • Multiplier 2: Rate limit for the subnet is equal to two times the To client cap and From client cap settings

QoS

Quality of Service (QoS) refers to a set of methods for assigning preferential access to network bandwidth based on pre-defined rules. QoS rules can assure that traffic for certain functional organizations is always accommodated or that certain applications and users are given higher priority. Tropos implements QoS by way of policies that reserve network bandwidth or assign priorities for packet forwarding. [Figure 34](#) shows the page, and [Table 32](#) describes the page settings.

FIGURE 34 QoS Page

QoS

0 Gateways 0 Nodes 0 MobileNodes are selected [Adjust Selection](#)
Please select routers to provision

SSID Parameters

SSID	2.4GHz	5.8GHz	4.9GHz	QoS Class	Max Clients
------	--------	--------	--------	-----------	-------------

QoS Specifics

<input type="checkbox"/>	Module Name	Value	Notes
<input type="checkbox"/>	Downstream Quality Selection:	802.1p ▼	
<input type="checkbox"/>	DSCP for Bronze:	<input type="text"/>	
<input type="checkbox"/>	DSCP for Silver:	<input type="text"/>	
<input type="checkbox"/>	DSCP for Gold:	<input type="text"/>	
<input checked="" type="checkbox"/>	802.1p Priority 0 to:	Voice ▼	
<input checked="" type="checkbox"/>	802.1p Priority 1 to:	Gold ▼	
<input checked="" type="checkbox"/>	802.1p Priority 2 to:	Silver ▼	
<input type="checkbox"/>	802.1p Priority 3 to:	Bronze ▼	
<input type="checkbox"/>	802.1p Priority 4 to:	Bronze ▼	
<input type="checkbox"/>	802.1p Priority 5 to:	Bronze ▼	
<input type="checkbox"/>	802.1p Priority 6 to:	Bronze ▼	
<input type="checkbox"/>	802.1p Priority 7 to:	Bronze ▼	
<input checked="" type="checkbox"/>	Bronze to:	802.1p Priority 3 ▼	
<input checked="" type="checkbox"/>	Silver to:	802.1p Priority 2 ▼	
<input checked="" type="checkbox"/>	Gold to:	802.1p Priority 1 ▼	
<input type="checkbox"/>	Voice to:	802.1p Priority 0 ▼	
<input type="checkbox"/>	Wired Sub-interface Priority:	Bronze ▼	

TABLE 32 QoS Page

Field	Range, <i>Default</i>	Description
SSID	---	Displays the currently configured ESSIDs.
2.4 GHz 5.8 GHz 4.9 GHz	---	Displays the wireless interfaces on the router.

TABLE 32 QoS Page (*continued*)

Field	Range, Default	Description
QoS Class	---	<p>Class of service for the specified ESSID.</p> <hr/> <p>Note: <i>This setting applies only to upstream traffic. To apply a class of service to downstream traffic, you must use an off-mesh device to pre-mark traffic in the downstream direction (using 802.1p or DSCP).</i></p>
Max Clients	---	<p>Indicates the maximum number of wireless clients that can connect to this ESSID simultaneously. This constraint is in addition to the constraint that limits each radio to 50 clients total, regardless of the ESSID.</p>
Downstream Quality Selection	DSCP	<p>Quality of traffic flows from the gateway's wired interface to wireless clients. If 802.1p is chosen but traffic does not have 802.1p tags because VLAN (trunking) is not enabled, then all traffic is treated as Silver traffic.</p> <hr/> <p>Note: <i>802.1p is a layer 2 header, while DSCP is part of the layer 3 IP datagram.</i></p>
DSCP for Bronze DSCP for Silver DSCP for Gold	24 (Bronze) 0 (Silver) 32 (Gold)	<p>DSCP assigned to upstream traffic when remarking is enabled. The value is chosen by the ESSID of the client for upstream traffic.</p> <p>If Downstream Quality Selection is set to DSCP, these values classify traffic headed from a gateway's wired interface to the wireless client.</p>
802.1p Priority <i>M</i> to	Bronze Silver Gold Voice	<p>Control of the QoS class of traffic flowing from a gateway's wired interface to wireless clients and from a node's sub-interface through the mesh. To use these values, VLAN (trunking) and Downstream Quality Selection of 802.1p on the respective interfaces must be enabled.</p>
Bronze to... Silver to... Gold to... Voice to...	802.1p priority 0-7, 802.1p priority 0	<p>Determination of 802.1p traffic marking from the gateway's wired interface. The marking requires VLAN (trunking) to be enabled.</p>
Wired Sub-Interface Priority	Bronze Silver Gold Voice	<p>QoS class of all traffic received by a node on the router's wired sub-interface, if VLAN (trunking) is not enabled on the sub-interface.</p>

Voice

Use the Voice page (Figure 35) to improve QoS for voice over IP (VoIP) traffic. Table 33 lists the parameters on the page.

FIGURE 35 Voice Page

Voice

0 Gateways 0 Nodes 0 MobileNodes are selected [Adjust Selection](#)
Please select routers to provision

<input type="checkbox"/>	Module Name	Value	Notes
<input type="checkbox"/>	Voice Service:	Enabled	
<input type="checkbox"/>	Voice Percentage of Available Airtime:		
<input type="checkbox"/>	WMM classification:	Enabled	
<input type="checkbox"/>	Heuristic classification:	Enabled	
<input type="checkbox"/>	DSCP values to recognize as voice (Decimal):		
<input type="checkbox"/>	Maximum per-call packet rate (pps):		
<input type="checkbox"/>	Maximum per-call bandwidth (kbps):		
<input type="checkbox"/>	Remarking:	Enabled	
<input type="checkbox"/>	DSCP value to remark to (Decimal):		
<input type="checkbox"/>	Fast Handoff Optimization:	None	

Voice Correspondent Prefixes
Voice Correspondent Prefixes don't take effect when Voice Service is disabled.
 IP Prefix

TABLE 33 Voice Parameters

Field	Range, Default	Description
Voice Service	Enabled Disabled	Enables the voice QoS features. You must enable this field and store changes to display all the rest of the fields on the Voice page.

TABLE 33 Voice Parameters (*continued*)

Field	Range, Default	Description
Voice Percentage of Available Airtime	1-100; 50	Limits the amount of bandwidth available for prioritized voice traffic (0-100).
WMM Classification	Enabled Disabled	Specifies whether the WMM extensions are enabled.
Heuristic classification	Disabled Enabled	Specifies whether heuristic priority rules are used in cases where WMM and DSCP priorities are not available.
DSCP values to recognize as voice (Decimal)	46	Specifies the incoming DSCP values that are recognized as voice traffic. Use comma-separated entries for multiple DSCP values.
Maximum per-call packet rate (pps)	100	Limits the packet rate (packets per second) that can be used for an individual voice call.
Maximum per-call bandwidth (kbps)	150	Limits the bandwidth (kbps) that can be used for an individual call.
Remarking	Enabled / Disabled	Specifies whether the DSCP field can be reassigned for forwarded packets.
DSCP value to remark to (Decimal)	46	Specifies the reassigned DSCP value, if remarking is enabled.
Fast Handoff Optimization	Pre-Fetch Only Packet Snoop Only Pre-Fetch and Packet Snoop None	Indicates the optimization method to reduce the time required for handoff when clients move from one router to another in the same ESS: <ul style="list-style-type: none"> • Pre-Fetch Only---Perform ARP resolution upon receipt of a qualified probe request. • Packet Snoop Only---Determine client IP address by inspecting the packets coming from the client. • Pre-Fetch and Packet Snoop---Perform pre-fetch and packet snoop. • None---Do not use either handoff optimization method.
IP Prefix	---	Identifies the IP addresses and netmasks (format a.b.c.d/n) of any voice gateways that are used exclusively for voice traffic.

Software

Use the Software page (Figure 36) to enable auto-recovery for the router and select backward compatibility options. Table 34 lists the parameters on the page.

FIGURE 36 Software Page

Software

0 Gateways 0 Nodes 0 MobileNodes are selected [Adjust Selection](#)
 Please select routers to provision

<input type="checkbox"/>	Module Name	Value	Notes
<input type="checkbox"/>	Auto Recovery:	Enabled	
<input type="checkbox"/>	Backward Compatibility:	All releases	*1

* 1: Value '7.1 and later' is applicable to routers from 7.1 release only

TABLE 34 Software Parameters

Field	Range, Default	Description
Auto Recovery	<i>Enabled</i> Disabled	Enables the auto-recovery feature. Auto recovery helps the router recover from failure during bootup.
Backward Compatibility	<i>All Releases</i> / 6.7 and later 7.1 and later	Indicates the mix of router software releases in the network. If Release 7.1 is used throughout the network, select the 7.1 and later option. If you have 6.7 software on some routers, you must select the 6.7 and later option. The All Releases option is most compatible in a mixed release network, however, it is not as secure as the other choices.

Security

Use the Security page (Figure 36) to enable auto-recovery for the router and select backward compatibility options. Table 34 lists the parameters on the page.

FIGURE 37 Security Page

Security

0 Gateways 0 Nodes 0 MobileNodes are selected [Adjust Selection](#)
Please select routers to provision

<input type="checkbox"/>	Module Name	Value	Notes
<input type="checkbox"/>	Router-EMS Authentication Key:	<input type="text"/>	Ver. 7.3
<input type="checkbox"/>	Confirm Router-EMS Authentication Key:	<input type="text"/>	Ver. 7.3
<input type="checkbox"/>	Infrared Port Status:	Enabled	
<input type="checkbox"/>	Infrared Access Code:	<input type="text"/>	
<input type="checkbox"/>	Confirm Infrared Access Code:	<input type="text"/>	

Configurator Access

<input type="checkbox"/>	Module Name	Value	Notes
<input type="checkbox"/>	Configurator Access Control:	Enabled	

Allowed IP Subnets for Configurator Access
In a multi-subnet network with VLANs, each management VLAN prefix must be on the list of allowed IP subnets.

IP	Netmask
<input type="text"/>	<input type="text"/>

FIPS

<input type="checkbox"/>	Module Name	Value	Notes
<input type="checkbox"/>	FIPS Mode:	Enabled	Ver. 7.3 *1

* 1: FIPS Mode should not be provisioned on 3210 and 5210 routers.

Ver. The field can only be provisioned to the routers with the specified version and above or specified pre release versions

TABLE 35 Software Parameters

Field	Range, Default	Description
Router-EMS Authentication Key Confirm Router-EMS Authentication Key	16 ASCII characters	Specifies the key that is used to authenticate communications between devices and Tropos Control. Enter and confirm the key.
Infrared Port Status	<i>Enabled</i> Disabled	Enables or disabled access to the router by way of an infrared remote device.

TABLE 35 Software Parameters (*continued*)

Field	Range, <i>Default</i>	Description
Infrared Access Code Confirm Infrared Access Code	---	Specifies the security code for using the infrared remote device.
Configurator Access Control	Enabled <i>Disabled</i>	Enables or disables access to the router Configuration utility.
Allowed IP Subnets for Configurator Access	---	Restricts access to the Configuration utility to the specified subnet. Click Add to add multiple subnets.
FIPS Mode	Enabled <i>Disabled</i>	Enables FIPS mode (FIPS 140-2) on the router (Release 7.3 and later routers only). See "Configuring FIPS Mode" on page 150.

Other Provisioning Operations

This section describes how to use the Administer Routers panel (Figure 38) to perform the provisioning functions described in Table 36.

FIGURE 38 Administer Routers Panel

7.3.1.1

Tropos Control

Network Health Configuration View Provisioning Administration

Find Go

Provision

- Provision from Form
- Provision from Files
- Administer Routers**

Provision Audit

- Provision Job List
- Provision Result

Form - Device Settings

- Router Identity
- IP and VLAN
- Wireless
- Client Access
- DHCP Server
- SNMP
- Time

Form - Service Settings

- DHCP Clients
- Static IP Client
- Packet Filtering
- P2P Blocking
- Multi-Subnet Roaming
- Backhaul Routing
- Rate Limiting
- QoS
- Voice

Administer Routers

Provision Job Name:

Retry:

Retry failed routers

Retry times, with interval second(s)

Schedule: Server Time: Jan 23 2010 17:43:23

Provision Now Provision at

Provision

Choose command to be sent to routers below:

[Select Routers \(v6.7+\)](#) [Clear Routers](#)

Selected Routers:

Gateways	0
Nodes	0
Mobile Nodes	0
Total	0

Golden Routers:

Name	
Type	
ID	
Wlan IP	

To send administrative commands to routers:

- Select the routers to be affected
- Select the router command
- Fill in necessary data fields
- Submit the job

After commit, all the stored data becomes committed data and takes effect

Time delay before committing: minute(s)

Abort the action and rollback all selected routers if any router in the list fails to commit configuration

TABLE 36 Other Provisioning Operations

Operation	Description	Commit Required
Commit the stored data in routers	Activates the changes that have been provisioned on the selected routers.	
Rollback the stored data in routers	Cancels the application of provisioned data that has not yet been committed. Provisioned data is saved in stored profiles on each router. During commit, the data is written to committed profiles. If a rollback operation is sent before commit, the provisioned data are lost.	
Reboot routers	Restart the hardware and software on the selected routers.	
Restart routers	Restart the software on the selected routers.	
Install an uploaded software image on routers	Install the uploaded software image on the selected routers.	
Change the administrative password on the routers	Change the password used to administer the selected routers.	Yes
Save configuration as known good profile	Store the configuration on the selected routers, identifying it as the last known good profile.	
Restore the configuration to the last saved known good profile	Change the configuration on the selected routers to the last good profile that was saved.	Yes
Save the minimum profile	Store the minimum profile on the selected routers.	
Restore the configuration to the last save minimum profile	Change the configuration on the selected routers to the last minimum profile that was saved.	Yes
Restore the configuration to factory defaults	Change the configuration on the selected routers to the factory defaults.	Yes
Upload admin public key	Upload a public key to restrict access to the router command line interface (CLI).	
Upload Profile	Upload a configuration profile to the specified routers. You can select a profile from the Tropos Control server or from your local computer.	
Enable/Disable Client Statistics	Enable or disable the collection of client statistics on the specified routers.	

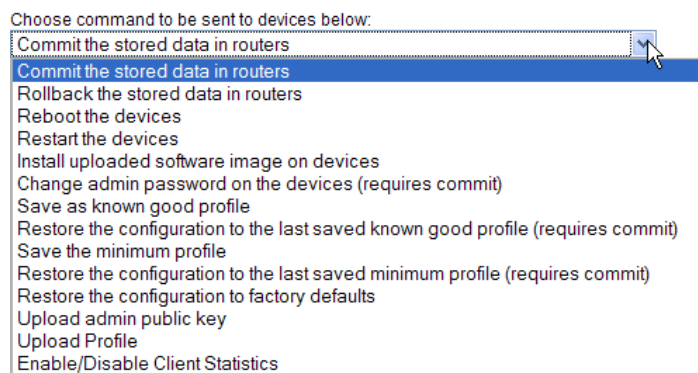
Provisioning Tasks - Administration

Perform these tasks in the specified order to complete the operations listed in [Table 36](#):

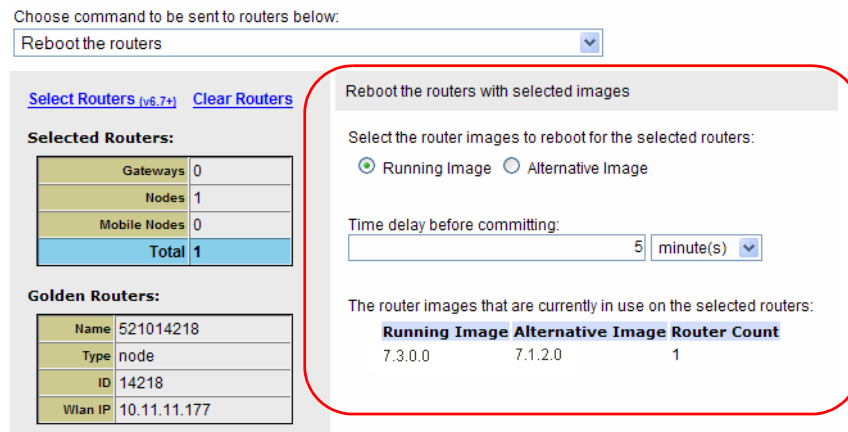
1. [Select routers to provision](#) (on page 70)
2. [Schedule the provisioning job](#) (on page 72)
3. [Set up and commit the provisioning job](#) (on page 75)

Set up and commit the provisioning job

1. Open the Administer Routers panel under the Provisioning tab and select the routers to provision (“[Select routers to provision](#)” on page 70).
2. Choose the command from the pull-down list.



3. For some commands, additional settings are presented in the lower right area of the panel, as in this example of the rebooting command.



4. Complete any additional settings, as described in [Table 36](#).
5. Click **Provision**.

The job instructions are sent to the selected routers.

Some operations must be committed after provisioning. The operations that require commit are indicated in the menu and also listed in [Table 36](#).

- To commit any required changes, select **Commit the stored data in routers** from the pull-down list and click **Provision**.

The changes are activated on the selected routers.

Auditing Provisioning Jobs

This section describes how to track and audit provisioning jobs:

- [Use the Provision Job List](#)---Check on the status of jobs and link to other status information.
- [Use the Provisioning Result panel](#)---Check on the results of provisioning jobs and link to other result information.

Use the Provision Job List

- Choose **Provisioning > Provision Job List** to open the list ([Figure 39](#)).

FIGURE 39 Provision Job List

Provision Job List

[View Provision Detail](#)
[View Provision Result](#)
[Stop](#)
[Commit](#)
[Redo](#)

Page Length|entries per page 1 to 50 of 110

Name: [Filter](#)

<input type="checkbox"/>	ID	Name	Type	Scheduled Time	Executed Time	Finished Time	Status	User Name
<input type="checkbox"/>	1123	provision2010_08_27_18_10_46	Commit	Aug 27 2010 18:11:01	Aug 27 2010 18:11:01	Aug 27 2010 18:12:56	Partial Success	root
<input type="checkbox"/>	1122	provision2010_08_27_18_06_57	Commit	Aug 27 2010 18:07:14	Aug 27 2010 18:07:14	Aug 27 2010 18:09:09	Partial Success	user-1
<input type="checkbox"/>	1121	provision2010_08_27_18_03_25	Form Provision	Aug 27 2010 18:04:21	Aug 27 2010 18:04:21	Aug 27 2010 18:06:16	Partial Success	root
<input type="checkbox"/>	1004	provision2010_06_30_18_58_38	Commit	Jun 30 2010 18:58:43	Jun 30 2010 18:58:43	Jun 30 2010 18:58:44	Success	user-1
<input type="checkbox"/>	1003	provision2010_06_30_17_15_39	Form Provision	Jun 30 2010 18:57:57	Jun 30 2010 18:57:57	Jun 30 2010 18:58:08	Success	user-1

- Choose from the options list in [Table 37](#).

TABLE 37 Provision Job List Operations

Operation	Description
Check job status	View the Status column, and click the underlined link to open a window that contains additional details about the job.
View job results	Click the underlined ID link or select the checkbox for a job and click View Provision Result .
Open the provision panel for the selected job	Click the underlined job name or select the checkbox for a job and click View Provision Detail .

TABLE 37 Provision Job List Operations (*continued*)

Operation	Description						
Create a new job based on the current	<p>Select the job to modify, and click Redo. A new panel opens to allow you to modify or remove settings. For example:</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Provision Summary</p> <hr/> <p>Interface 1 Change Remove</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #4a7ebb; color: white;">Module Name</th> <th style="background-color: #4a7ebb; color: white;">Value</th> </tr> </thead> <tbody> <tr> <td>Primary ESSID</td> <td>11234567</td> </tr> <tr> <td>ESSID Suppression</td> <td>Disabled</td> </tr> </tbody> </table> </div> <p>After you modify the settings, click Provision to restart the provisioning process.</p> <p><i>Note: This option is useful if an existing job failed and you want to make changes before resubmitting it or if you want to apply the same settings to provision other routers.</i></p>	Module Name	Value	Primary ESSID	11234567	ESSID Suppression	Disabled
Module Name	Value						
Primary ESSID	11234567						
ESSID Suppression	Disabled						
Cancel a scheduled job	Select checkboxes for the jobs you want to cancel, and click Stop . Click OK to confirm.						
Commit a job	Select a checkbox for the job that you want to commit, and click Commit . Click Provision on the panel that opens.						
Control which jobs are listed.	<p>Use either or both of the following controls:</p> <ul style="list-style-type: none"> Choose from the pull-down list at the top of the panel to select the number of jobs to display on each page. Enter the job name and click Filter. 						

Use the Provisioning Result panel

1. Choose **Provisioning > Provision Result** to open the list ([Figure 40](#)).

FIGURE 40 Provision Results

The screenshot shows the 'Provision Result' panel. At the top, there are 'Commit' and 'Show All' buttons. Below them is a 'Page Length' dropdown set to '50' and a pagination indicator '1 to 50 of 826'. The main part of the panel is a table with the following data:

	Job Name	Device	Executed Time	Finished Time	Retries	Status	Reason	User Name
<input type="checkbox"/>	provision2010_08_27_18_10_46_172.20.125.73	172.20.125.73	Aug 27 2010 18:12:49	Aug 27 2010 18:12:56	3	Failed	Router is not reachable	root
<input type="checkbox"/>	provision2010_08_27_18_10_46_172.20.125.236	172.20.125.236	Aug 27 2010 18:11:01	Aug 27 2010 18:11:02	0	Success	Success	user-1
<input type="checkbox"/>	provision2010_08_27_18_10_46_172.20.125.99	172.20.125.99	Aug 27 2010 18:11:01	Aug 27 2010 18:11:02	0	Success	Success	user-1
<input type="checkbox"/>	provision2010_08_27_18_10_46_172.20.125.128	172.20.125.128	Aug 27 2010 18:11:01	Aug 27 2010 18:11:02	0	Success	Success	root

2. Choose from the options list in [Table 38](#).

TABLE 38 Provision Result Operations

Operation	Description
View result information	Examine the Time, Status, and Reason columns for information about the specific job.
Open the provision panel for the selected job	Click the underlined job name.
View details for the selected router	Click the underlined device name to open a window with details about the selected router.
Control which jobs are listed.	Use any of the following controls: <ul style="list-style-type: none"> • Choose from the pull-down list at the top of the panel to select the number of jobs to display on each page. • Click Show All to show all the provision results that are in the database.
Commit a job	Select a checkbox for the job that you want to commit, and click Commit. Click Provision on the panel that opens.

8 Performing Administrative Tasks

This chapter describes how to use the web interface to manage router inventory, upgrade router software, and generate diagnostic information to assist Tropos Customer Support in troubleshooting Tropos Control problems.

Chapter contents:

- [Generating Diagnostic Information.](#)
- [Upgrading Router Software.](#)
- [Tracking Router Inventory](#)
- [Backing Up Router Configurations](#)
- [Restoring Router Configurations](#)
- [Supporting RADIUS Authentication](#)
- [Managing Administrative Users](#)
- [Using Router Auto Discovery](#)
- [Viewing the User Audit Log](#)
- [Configuring Banner Text](#)

Generating Diagnostic Information

If the Tropos Control server has operational problems, you can use the Tech Support tab to generate a diagnostic file that you can send to Tropos Customer Support for analysis.

Generate diagnostic files

1. Open the Administration tab and click **Tech Support**.
2. Click **Collect Techdump**.

The file is generated and listed in the panel.

Collect Techdump		Delete	
<input type="checkbox"/>	Filename	Created At	Size
<input type="checkbox"/>	<u>techsupport_201001231746.tar.gz</u>	Sat Jan 23 17:47:48 PST 2010	14.1M

3. Click the underlined file name. Browse to select a location, and click **Save**.
4. When requested, email the file to support@tropos.com.

If the web interface is not available, you can generate the techdump file from the command line. Go to the support directory in the Tropos Control installation directory, and execute the techdump.sh script. The script automatically generates the diagnostic tar file, which you can then send to Tropos Customer Support:

```
cd /<installdirectory>/ems/support
./techdump.sh
Average disk space required : 58M
Available disk space       : 107583M
+
|
| This command collects information from your server to send to
| customer support. When this process is complete, there will be a file
| in /<installdirectory>/ems/support called:
| techsupport_200708201045.tar.gz
|
| Please send all files to your support staff.
+
/<installdirectory>/ems/support
Cleaning old files (if any) :
Done.
```

Upgrading Router Software

Use the following router software upgrade panels under the Administration tab to install new router software and manage the upgrade process:

- Add Schedule---Schedule router upgrades. For instructions, see “[Schedule router software upgrades](#)” on page 131.
- Status---Check the status of a specific upgrade job. For instructions, see “[Check upgrade job status](#)” on page 133.
- History---Check the status of all upgrade jobs. For instructions, see “[View upgrade job history](#)” on page 133.
- Add Image---Upload router software images to the Tropos Control server. For instructions, see “[Upload a software image](#)” on page 134.

Schedule router software upgrades

1. Open the Administration tab and click **Router Software Update**.

The Add Schedule panel ([Figure 41](#)) opens.

FIGURE 41 Add Schedule Panel

Add Schedule

Job Name:

Schedule: (Current Server Time: Mar 17 2011 09:17)

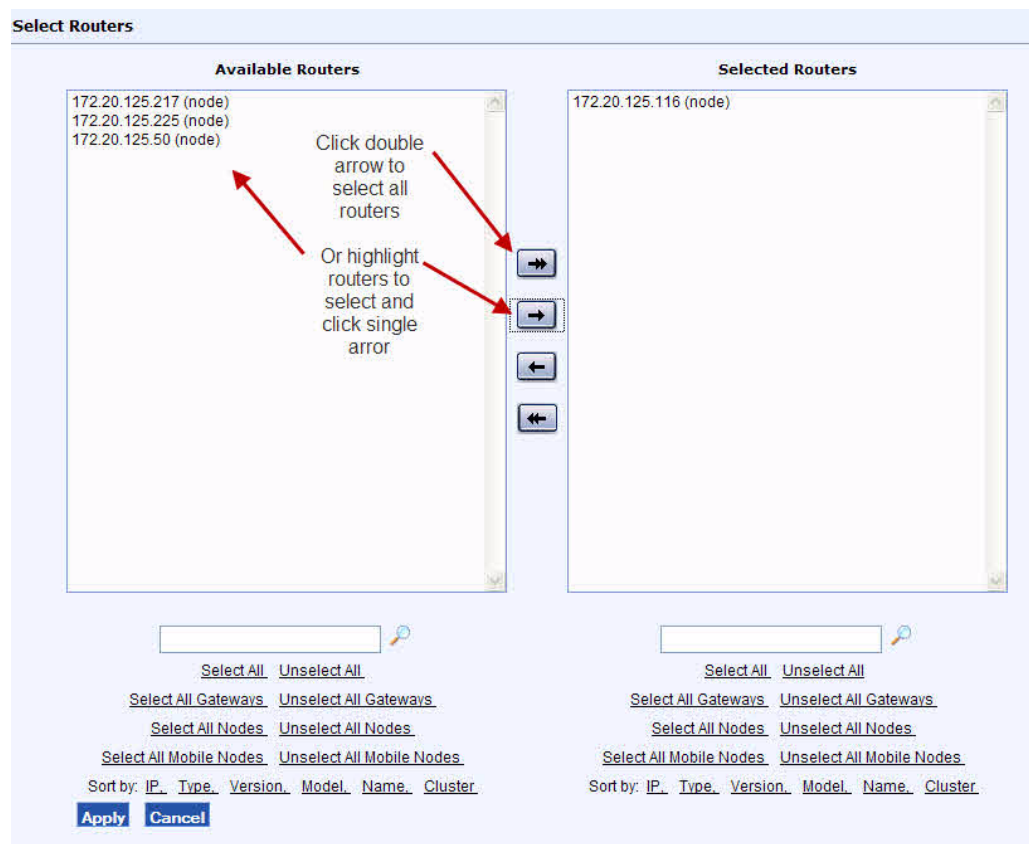
Upload now Upload at

Select Image: Retry time(s)

Select Routers:

version 7.5.0.4	model 6320 DC	3 device(s)	0 selected device(s)	Select Device
version 7.5.0.4	model 5320	10 device(s)	0 selected device(s)	Select Device
version 7.5.0.4	model 7320	1 device(s)	0 selected device(s)	Select Device
version 7.5.0.0	model 5320	1 device(s)	0 selected device(s)	Select Device
version 7.1.2.6	model 6320 DC	1 device(s)	0 selected device(s)	Select Device
version 7.5.0.4	model 5210	2 device(s)	0 selected device(s)	Select Device
version 7.5.0.4	model 3210	8 device(s)	0 selected device(s)	Select Device
version 7.1.2.5	model 5320 DC	1 device(s)	0 selected device(s)	Select Device
version 7.5.0.4	model 5320 DC	1 device(s)	0 selected device(s)	Select Device
version 7.5.0.4	model 4210	1 device(s)	0 selected device(s)	Select Device
version 7.5.0.3	model 4310	1 device(s)	0 selected device(s)	Select Device

2. Enter a name to identify the upgrade job.
3. Choose **Upload Now** or click the Calendar icon and select a date and time to schedule the upload.
4. Select the number of times to retry the upgrade process if the initial attempt fails.
5. Enter the user name and password for administrative access to the router or routers targeted for upgrade.
6. Select a software image from the pull-down list. If the software image you want to use is not in the list, click **Add Image**, and follow the instructions in “[Upload a software image](#)” on page 134.
7. To choose the routers to be upgraded, click the **Select Device** link.
8. Use the arrows and links to highlight the desired routers and move them to the Selected Routers area. Links are also available to sort the list for easier viewing. The single-headed arrows move only the selected routers, while the double headed arrows move all routers in the list.



9. Click **Apply** to save the list and return to the Add Schedule panel.
10. Click **Submit** to schedule the process of loading the new software on the selected routers.

- The Status page opens to display the status of the scheduled job. The display is refreshed every few seconds. You can click the underlined wireless IP link to display detailed information about a router in the list.

Status

Job ID: 2 [Cancel This Job](#)

Job Name: job1

Status Summary: 1 Scheduled

Page Length|entries per page 50 1 to 1 of 1

Device	Device Id	SW Version	wirelessIP	Retries	Executed Time	Finished Time	Status	Reason
building5	19937	6.5.1.1	172.20.125.192	--	--	--	Scheduled	--

- When the scheduled job is complete and the software is loaded on the router, an Install button is displayed on the Status panel. Click **Install** to install the new image on the router or routers.

Check upgrade job status

- Open the Administration tab and click **Router Software Update > Status**.

The Status panel opens. The panel refreshes every few seconds to show the current job status.

i Note

The Status panel opens automatically when you submit an upgrade job.

- Use the controls at the top of the panel to choose the number entries to display and to navigate from page to page. Click a column header to sort according to that column. Clicking the column header again changes the sort order.

View upgrade job history

- Open the Administration tab and click **Router Software Update > History**.

The History panel opens. The panel refreshes every few seconds to show the current job status.

History

Page Length|entries per page 50 1 to 50 of 78

Job ID	Job Name	Job Type	Scheduled Time	Executed Time	Finished Time	Status
579	Ace-7.3.0.1-5274	Upload Image	Dec 01 2009 22:57:40	Dec 01 2009 22:57:40	Dec 01 2009 23:01:00	Success
578	7124 upgrade490_install	Install Image	Nov 20 2009 14:08:08	Nov 20 2009 14:08:08	Nov 20 2009 14:08:16	Success
577	pAce 7124491_install	Install Image	Nov 20 2009 14:07:55	Nov 20 2009 14:07:55	Nov 20 2009 14:08:02	Success

- Use the controls at the top of the panel to choose the number entries to display and to navigate from page to page. Click a column header to sort according to that column. Clicking the column header again changes the sort order.
- To open the status panel for a specific job, click the underlined job link.

Upload a software image

1. Open the Administration tab and click **Router Software Update > Add Image**.

The panel opens to show a list of uploaded images.

Add Image

Images on EMS Server:

- Ace20-6.6.0.0-2834-efs.bin

Add a new image to EMS Server:

2. Click **Browse** to locate the new image, and then click **Open** in the Browse window to select the image.
3. Click **Upload**.

The image is copied to the Tropos Control server and becomes available in the Select Image pull-down list on the Add Schedule panel. For instructions on scheduling an upgrade using the image, see [“Schedule router software upgrades”](#) on page 131.

Tracking Router Inventory

To manage the inventory of routers in your network, open the Tropos Control web interface Administration tab, and click **Inventory Tracking to open the Inventory Tracking panel** (Figure 42).

FIGURE 42 Inventory Tracking Panel

Inventory Check		Upload Inventory (Serial Number) File			
Summary of Result:					
Total number of routers in inventory	:	15			
Total number of routers found	:	14			
Total number of routers never found	:	1			
Total number of mystery routers found	:	0			
Delete <input type="button" value="Export"/> Showing all routers from the inventory Page Length entries per page 5 1 to 5 of 15					
<input type="checkbox"/>	Serial Number ▲	IP Address	Status	Location	Reason
<input type="checkbox"/>	19040	172.20.125.96	Discovered	Sunnyvale Tropos	
<input type="checkbox"/>	19125	172.20.125.98	Discovered	Sunnyvale CA	
<input type="checkbox"/>	19134	172.20.125.84	Discovered	Sunnyvale CA	
<input type="checkbox"/>	19153	172.20.125.80	Discovered	Sunnyvale	
<input type="checkbox"/>	19173	172.20.125.83	Discovered	Sunnyvale CA	

The upper part of the Inventory Tracking panel lists the information in [Table 39](#). All the routers in inventory are listed below the summary area, along with the information listed in [Table 40](#).

TABLE 39 Router Information

Item	Description
Total number of routers in inventory	Total number of router included in the inventory.
Total number of routers found	Number of discovered routers.
Total number of routers never found	Number of routers in inventory that have not been discovered.
Total number of mystery routers found	Number of routers that have been discovered but are not in the inventory.

TABLE 40 Router Inventory Summary Information

Item	Description
Serial number	Router serial number.
IP Address	Router IP address.
Status	Discovered or Unknown.
Location	Location as configured on the router's Router Information page.
Reason	If discovery fails, reason that the router was not discovered.

The following inventory-related functions are supported on this panel:

- [Verify inventory](#)
- [Upload an inventory file](#)
- [Export the inventory list](#)
- [Delete routers from inventory](#)

Verify inventory

1. Open the Administration tab and click **Inventory Tracking**.
2. Click **Inventory Check**.

Tropos Control compares the inventory contents with the list of most recently discovered routers and presents the results in the table on the panel.

Upload an inventory file

1. Create a text file in which each row contains the serial number of a router, as in this example:

19967

35435

14563

50310

2. Open the Administration tab and click **Inventory Tracking**.
3. Click **Upload Inventory (Serial Number) File**.
4. Browse to find locate the inventory file, and click **Open**.

The file is uploaded and the inventory is added to the list. Discovery and other monitoring and management functions are automatically activated.

Export the inventory list

1. Open the Administration tab and click **Inventory Tracking**.
2. Select checkboxes for the routers you want to include in the export, and click **Export**.
3. Browse to find choose a save location, and click **Save**.

The file is saved in csv format.

Delete routers from inventory

You can remove routers from the inventory list. This action does not remove the routers from the Tropos Control database. Use the map menu options as described under [“Delete node, mobile node, or fixed node”](#) on page 47.

1. Open the Administration tab and click **Inventory Tracking**.
2. Select checkboxes for the routers you want to remove, and click **Delete**.

Backing Up Router Configurations

Follow the steps in the section to back up router configuration profiles on the Tropos Control server. You can schedule daily backups, perform a manual backup, or export backed up configuration profile. Daily backups include all routers.

- [Set up automatic daily backups](#)---Set up the system to back up the configuration profiles of all managed routers once per day.
- [Perform a manual backup](#)---Backup the configuration profiles of selected routers on demand.
- [Export a backed up configuration profile](#)---Export a backed up configuration file to a location of your choice.
- [View the Backup Events list](#)---Monitor the status of backup operations.

Set up automatic daily backups

1. Open the Administration tab and click **Router Backup**.

The Router Backup panel (Figure 41) opens.

FIGURE 43 Router Backup Panel

Router Backup

Automatic Backup

Enable daily backup at: (HH:MM) Save file for: days **Submit**

Manual Backup

File name prefix:

Select routers to be backed up: [0 routers are selected](#) **Backup Now**

Export Backup

Backup file name: **Browse...** **Download**

Backup Events

[Refresh Events List](#) Page Length|entries per page 1 to 25 of 254

ID	Start Time	End Time	Status
254	Jan 22 2010 00:02:11	Jan 22 2010 00:04:13	Success: 29 Failure: 4
253	Jan 21 2010 00:02:11	Jan 21 2010 00:04:17	Success: 29 Failure: 4
252	Jan 20 2010 00:02:11	Jan 20 2010 00:04:13	Success: 29 Failure: 4
251	Jan 19 2010 00:02:10	Jan 19 2010 00:02:19	Success: 29 Failure: 4
250	Jan 18 2010 00:02:10	Jan 18 2010 00:02:19	Success: 29 Failure: 4

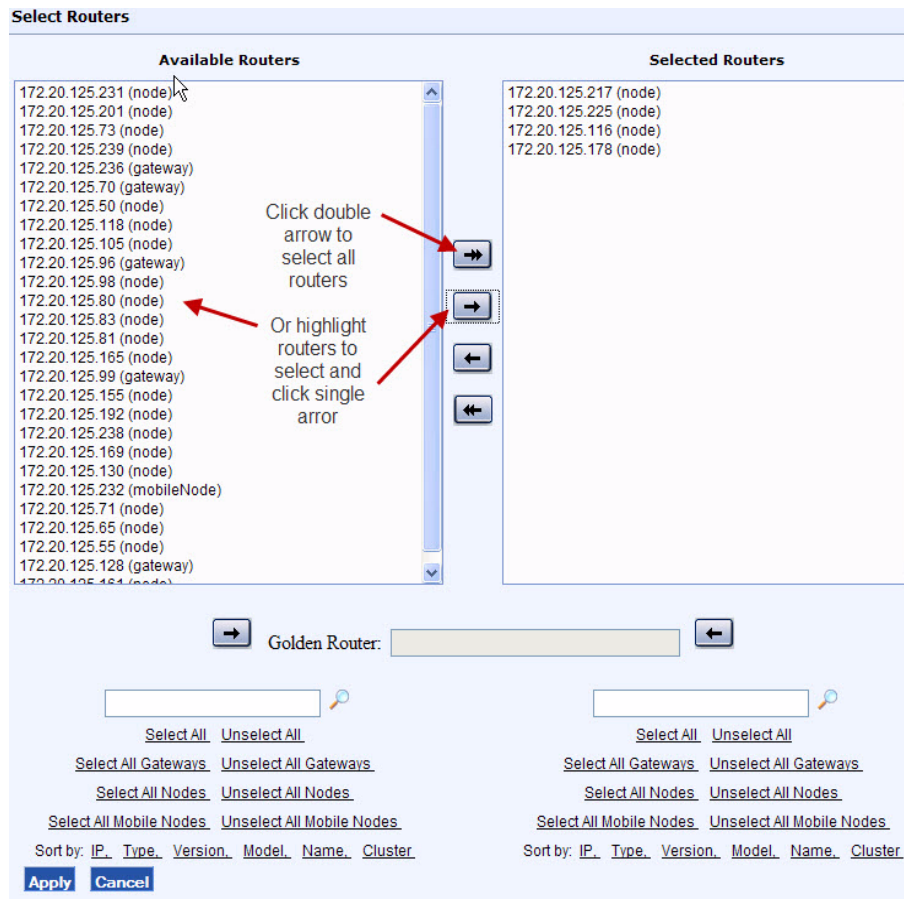
2. Select **Enable daily backup at** and enter the time in HH:MM format.
3. Enter the number of days to keep the backup.
4. Click **Submit**.

The daily backup job is scheduled. Every day, the configuration profiles for all routers are backed up at the specified time.

Perform a manual backup

1. Open the Administration tab and click **Router Backup**.
2. Click the underlined **routers are selected** link to choose the routers to include in the backup.

A selection window opens.



3. Select the routers that you want to back up Available Routers list, and click the right-facing arrow to move them to the Selected Routers area. You can use the links near the bottom of the screen to select or sort the groups of routers in the list, or use the double arrows to move the entire list.
4. Click **Apply**.

The panel reopens to show the number of selected routers.

Manual Backup
 File name prefix:
 Select routers to be backed up: **4 routers are selected** [Clear Selection](#) [Backup Now](#)

5. Enter a prefix to identify the backup job. Date and time information is automatically appended to the prefix.
6. Click **Backup Now**.

The selected router configurations are backed up, and the Backup Events list at the bottom of the panel is updated with status information.

Export a backed up configuration profile

1. Open the Administration tab and click **Router Backup**.
2. In the Export Backup area, click **Browse** to select the file to export.
3. Click an underlined link to open the Manual or Scheduled backups directory.

/opt/TroposControl/ems/routerBackup/ **Submit** **Close**

Name	Size	Type	Date
[scheduled backup]		DIR	Jan 23, 2010 12:02:19 AM

4. Click the link for the job that you want to export.

/opt/TroposControl/ems/routerBackup/scheduled_backup/ **Submit** **Close**

Name	Size	Type	Date
[..]			
[2010 01 09 000210]		DIR	Jan 9, 2010 12:02:10 AM
[2010 01 10 000210]		DIR	Jan 10, 2010 12:02:10 AM
[2010 01 11 000210]		DIR	Jan 11, 2010 12:02:10 AM
[2010 01 12 000210]		DIR	Jan 12, 2010 12:02:10 AM

5. Select the item to export and click **Submit**.

/opt/TroposControl/ems/routerBackup/scheduled_backup/2010_01_10_000210/ **Submit** **Close**

Name	Size	Type	Date
[..]			
<input type="radio"/> 00027.cfg	7.69 KB	.cfg	Jan 10, 2010 12:02:10 AM
<input checked="" type="radio"/> 00034.cfg	8.36 KB	.cfg	Jan 10, 2010 12:02:10 AM
<input type="radio"/> 00041.cfg	8.37 KB	.cfg	Jan 10, 2010 12:02:10 AM

6. The main panel reopens to show the file name in the Export area.

Export Backup
 Backup file name: **Browse...** **Download**

7. Click **Download** to save the file in a location of your choice.

View the Backup Events list

1. Open the Administration tab and click **Router Backup**.

The Backup Events list is displayed at the bottom of the panel.

Backup Events

Refresh Events List Page Length|entries per page 25 1 to 25 of 254

ID	Start Time	End Time	Status
254	Jan 22 2010 00:02:11	Jan 22 2010 00:04:13	Success: 29 Failure: 4
253	Jan 21 2010 00:02:11	Jan 21 2010 00:04:17	Success: 29 Failure: 4
252	Jan 20 2010 00:02:11	Jan 20 2010 00:04:13	Success: 29 Failure: 4
251	Jan 19 2010 00:02:10	Jan 19 2010 00:02:19	Success: 29 Failure: 4

2. Click an underlined link in the Status column to display details about the job.

Backup Task (Job 253)

Start Time: Jan 21 2010 00:02:11 End Time: Jan 21 2010 00:04:17

Summary:

Success: 29 Failure: 4

Details:

Page Length|entries per page 25 1 to 25 of 33

Device	Start Time	End Time	Status	Detail	File Name
172.20.125.238	Jan 21 2010 00:03:15	Jan 21 2010 00:04:15	Failed	Unknown Error: java.net.SocketTimeoutException: connect timed out	/opt/TroposControl /ems/routerBackup /scheduled_backup /2010_01_21_000210/19965.cfg
172.20.125.128	Jan 21 2010 00:02:19	Jan 21 2010 00:02:21	Success	Downloaded	/opt/TroposControl /ems/routerBackup /scheduled_backup /2010_01_21_000210/49014.cfg
172.20.125.55	Jan 21 2010 00:02:19	Jan 21 2010 00:02:20	Success	Downloaded	/opt/TroposControl /ems/routerBackup /scheduled_backup /2010_01_21_000210/49011.cfg
172.20.125.65	Jan 21 2010 00:02:19	Jan 21 2010 00:02:20	Success	Downloaded	/opt/TroposControl /ems/routerBackup /scheduled_backup /2010_01_21_000210/49009.cfg

Restoring Router Configurations

Follow the steps in the section to restore router configurations that were previously backed up:

- [Restore router configuration to the same router](#)---Restore a previously-backed up configuration to the same router.
- [Restore router configuration to a different router](#)---Restore a previously-backed up configuration to a different router. This procedure is useful for restoring configurations after a router has been replaced in the field.
- [View the Restore Events list](#)---Monitor the status of restoration operations.

Restore router configuration to the same router

1. Open the Administration tab and click **Router Restore**.

The Router Restore panel (Figure 44) opens.

FIGURE 44 Router Restore Panel

The screenshot shows the 'Router Restore' panel with the following elements:

- Restore Router** section:
 - Text: 'Restore Router'
 - Form: 'Select Backup File:' followed by a text input field and a 'Browse...' button.
 - Button: A blue 'Restore' button.
- Restore file to selected router** section:
 - Text: 'Restore file to selected router'
 - Form: 'Backup file name:' followed by a text input field and a 'Browse...' button.
 - Form: 'Select router to restore:' followed by a dropdown menu showing '321035050 (10.11.11.184)'.
 - Button: A blue 'Restore' button.
- Restore Events** section:
 - Text: 'Restore Events'
 - Button: A blue 'Refresh Events List' button.
 - Table:

ID	Start Time	End Time	Status
----	------------	----------	--------

2. Click **Browse** in the Restore Router area. Navigate to the directory containing the file, select the file, and then click **Submit**.
3. Click **Restore**.

Restore router configuration to a different router

1. Open the Administration tab and click **Router Restore**.

The Router Restore panel opens.

Router Restore

Restore Router

Select Backup File:

Restore file to selected router

Backup file name:

Select router to restore: 321035050 (10.11.11.184)

Restore Events

ID	Start Time	End Time	Status
----	------------	----------	--------

2. Click **Browse** in the Restore file to selected router area. Navigate to the directory containing the file, select the file, and then click **Submit**.
3. Select the router to receive the restored file from the pull-down list.



Note

The router selected for restoration should be the same type of router (gateway, node, mobile node) that was used to generate the backup file.

4. Click **Restore**.

View the Restore Events list

1. Open the Administration tab and click **Router Restore**.

The Restore Events list is displayed at the bottom of the panel.

Restore Events

Page Length|entries per page 25 1 to 1 of 1

ID	Start Time	End Time	Status
2	Dec 06 2008 14:44:58	Dec 06 2008 14:45:02	Success

- Click an underlined link in the Status column to display details about the job.

Backup Task (Job 2)

Start Time: Dec 06 2007 14:44:58 End Time: Dec 06 2007 14:45:02

Summary:
Success

Details:

Page Length|entries per page 25 1 to 1 of 1

Device	Start Time	End Time	Status	Detail	File Name
10.11.11.175	Dec 06 2008 14:45:00	Dec 06 2008 14:45:02	Success	Restore successfully	/opt/TroposControl/ems/routerBackup/scheduled_backup/2007_12_06_000159/35435.cfg

Supporting RADIUS Authentication

You can configure the Tropos Control server to forward any authentication requests for access to the Tropos Control server to an external RADIUS server.

i Note

Password Authentication Protocol (PAP) is used as the authentication protocol.

Set up RADIUS authentication for access to the Tropos Control server

- Open the Administration tab and click **AAA Server**.

A list of currently configured RADIUS servers is displayed.

Add **Modify** **Delete**

<input type="checkbox"/>	Server Name	Host/IP	Port	Timeout
<input type="checkbox"/>	NewsServer	101.1.1	1812	60

- Perform the following operations from this panel:

Add a new server:

- Click **Add**.
- Enter values as described in [Table 41](#).
- Click **Submit**.

The panel reopens to show the new server.

Modify a server entry:

- Select the server and click **Modify**.
- Change values as described in [Table 41](#).
- Click **Submit**.

The panel reopens to show the modified values.

Delete a server entry:

- a. Select the server and click **Delete**.
- b. Click **OK** to confirm.

TABLE 41 RADIUS Server Settings

Item	Description
RADIUS Server Name	Enter a name to identify the RADIUS server.
Server Host Name/IP	Enter the IP address or host name of the server.
Server Port Number	Enter the RADIUS server port number for authentication requests. Default: 1812
Shared Secret Key Confirm Shared Secret Key	Enter and confirm the code used to verify the connection between the RADIUS server and the router.
Timeout	Enter the number of seconds after which an authentication request times out. Range: 1-30 seconds; default: 5 seconds

Managing Administrative Users

You can use the web interface to set up administrative user accounts.

- Note**
Only the user with root privileges can set up other user accounts.

Manage administrative user accounts

1. Open the Administration tab and click **AAA Server**.

A list of currently configured users is displayed.

Add Modify Delete					
<input type="checkbox"/>	Username	Full Name	Role	Authentication Server	Status
<input type="checkbox"/>	root	Default Root User	root		Enabled
<input type="checkbox"/>	guest	Default Guest User	readonly	Local	Disabled
<input type="checkbox"/>	test		root	Local	Enabled

2. Perform the following operations from this panel:

Add a new user:

- a. Click **Add**.
- b. Enter values as described in [Table 42](#).

- c. Click **Submit**. The panel reopens to the list the new user.

Modify a user entry:

- a. Select the user and click **Modify**.
 b. Change values as described in [Table 42](#).
 c. Click **Submit**. The panel reopens to the list the modified values.

Delete a user:

- a. Select the server and click **Delete**.
 b. Click **OK** to confirm.

TABLE 42 Administrative User Settings

Item	Description
Username	Enter a name that identifies the user.
Full Name	Enter the full name of the user.
Role	Select a role from the pull-down list. <ul style="list-style-type: none"> • Root—Permitted to view all information and perform all tasks that relate to the system and to the server platform. • Read/Write—Permitted to view information and perform most tasks. • Read Only—Permitted to view information but not make any changes to the system.
Status	Choose whether the user account is active (Enabled) or inactive (Disabled).
Authenticate with	Choose whether authentication is performed from the server using username and password, or by using a RADIUS server. If you choose Local , the password fields are activated; if you choose Remote , the Preferred Server field is activated.
Preferred Server	If RADIUS is chosen for the Authenticate with field, select the RADIUS server.
Password Confirm Password	If Local is chosen for the Authenticate with field, enter and confirm the password used for access.

Using Router Auto Discovery

You can set up the system to automatically discover all routers in a network from a single gateway (seed gateway). When auto discovery is configured, the Tropos Control server requests that the seed gateway obtain the list of available gateways in the network. When the list is obtained, the server contacts each gateway to obtain its local list of nodes. Auto discovery operations are run once per day.

Note

If the network is composed of multiple subnets, a gateway from each subnet must be added.

For resilience, a second gateway can be configured for each subnet. If the first (primary) gateway is not reachable, the server contacts the secondary gateway to obtain the list of routers.

Note

For additional information on adding routers to the Tropos Control database, see *"Tracking Router Inventory"* on page 134.

Configure SNMP parameters for auto discovery

1. Open the Administration tab and choose **Auto Discovery > Configuration**.

A list of currently configured seed gateways is displayed.

Auto Discovery Configuration

Enable :

SNMP Port Number :

SNMP Read Community String :

SNMP Write Community String :

SNMP Trap Port Number :

SNMP Trap Community String :

2. Configure parameters as listed in [Table 43](#).

3. Click **Submit**.

TABLE 43 Auto Discovery Configuration

Item	Description
Enable	Select to enable auto discovery.
SNMP Port Number	Enter the port number for SNMP messages (default 161).
SNMP Read Community String	Enter the write community string.
SNMP Write Community String	Enter the read community string.
SNMP Trap Port Number	Enter the port number for SNMP traps.
SNMP Trap Community String	Enter the trap community string.

Set up auto discovery

1. Make sure that auto discovery is enabled, as described in the previous procedure.
2. Open the Administration tab and click **Auto Discovery > Seed List**.

A list of currently configured seed gateways is displayed.

Add Modify Delete Rediscover			
<input type="checkbox"/>	Seed Gateway	Secondary Gateway	Description
<input type="checkbox"/>	10.1.1.1	10.1.1.2	Gateway information for subnet 1

Last Discovered at Wed Dec 31 16:00:00 PST 1969.

3. Perform the following operations from this panel:

Add a new gateway:

- a. Click **Add**.
- b. Enter values as described in [Table 44](#).
- c. Click **Submit**.
The panel reopens to the list the new user.
- d. To rediscover the new gateway immediately, without waiting for the next daily auto discovery, click **Rediscover**.

Modify a gateway entry:

- a. Select the user and click **Modify**.
- b. Change values as described in [Table 44](#).
- c. Click **Submit**.
The panel reopens to the list the modified values.
- d. To rediscover the new gateway immediately, without waiting for the next daily auto discovery, click **Rediscover**.

Delete a gateway entry:

- a. Select the server and click **Delete**.
- b. Click **OK** to confirm.

TABLE 44 Auto Discovery Settings

Item	Description
Seed Gateway IP	Enter the IP address of a gateway with nodes that you want to include in the auto discovery.
Secondary Gateway IP	Enter the IP address of a gateway to contact if the seed gateway is not reachable.
Wireless Routing Domain ID Confirm Wireless Routing Domain ID	Enter and confirm the 16-character code that identifies the area of the managed routers. All managed routers must be configured with the same wireless routing domain ID.

TABLE 44 Auto Discovery Settings (*continued*)

Item	Description
Admin User Password Confirm Admin User Password	Enter and confirm the password required for access to the gateway.
Description	Enter text to describe the gateway.

Viewing the User Audit Log

The User Audit Log page shows the history of user sessions on the Tropos Control server.

View the user audit log

1. Open the Administration tab and click **Use Audit Log**.

The user login history is displayed.

Refresh Audit Log		Page Length entries per page 25 1 to 8 of 8		
User Name	Log Time	Client IP	Operation	Description
root	Jun 05 2008 11:03:02	192.168.1.151	LOGIN	root logged in
root	Jun 05 2008 11:00:59	192.168.128.102	LOGIN	root logged in
root	Jun 04 2008 16:57:00	192.168.128.102	LOGIN	root logged in
root	Jun 04 2008 15:40:39	192.168.128.102	LOGIN	root logged in
root	Jun 04 2008 14:18:56	192.168.128.63	LOGIN	root logged in
root	Jun 04 2008 14:16:59	192.168.128.102	LOGIN	root logged in
root	Jun 03 2008 12:56:50	192.168.128.63	LOGIN	root logged in
root	Jun 02 2008 17:19:14	127.0.0.1	LOGIN	root logged in

2. Click **Refresh Audit Log** to update the list.

Configuring Banner Text

Use the Server Configuration page to configure optional banner text that is displayed in the upper right portion of the each page, as shown in [Figure 5](#) on page 21.

Configure banner text

1. Open the Administration tab and click **Server Configuration**.

Tropos Control Configuration

Banner:

FIPS Mode:

* Tropos Control Server will be restarted upon FIPS Mode modification.

* Tropos Control users password length should be of minimum 8 characters for it to be running in FIPS Mode .

2. Enter the banner text. The maximum length is 128 characters and special characters such as @, &, <, > are not supported.
3. Click **Submit**.

Configuring FIPS Mode

Tropos supports the Federal Information Processing Standards, version 140-2 (FIPS 140-2), which are general security standards for protection of sensitive information, required by government agencies in the U.S. and Canada.

-
- Note**
Refer to the complete security policy for detailed FIPS instructions. The security policy is distributed to Tropos FIPS customers along with router software and tamper-evident seals.
-

Note the following properties and restrictions:

- For FIPS 140-2 support, FIPS mode must be enabled on the Tropos Control server and the managed routers must be running Release 7.3 or later with FIPS mode enabled.
- FIPS mode is disabled by default.
- Changing to FIPS mode automatically causes the Tropos Control EMS server to restart.
- After changing to FIPS mode, you must close and then reopen your web browser.
- In FIPS mode, the Router-EMS Authentication key (not the mesh ID) is used to establish communication between the routers and the Tropos Control EMS server.
- FIPS 140-2 support includes a “zeroize” capability that automatically removes any clear text critical security parameters (CSPs) and shuts down the system.

-
- Caution**
The zeroize function should be used only in extreme cases when it is necessary to remove sensitive information. After zeroizing, the server software must be reinstalled.
-

-
- Note**
Tropos Control can manage both FIPS and non-FIPS enabled routers when running in FIPS disabled mode; however, in this case the management is not FIPS 140-2 compliant.
-

Enable FIPS mode

1. Make sure that SSH access to the router is disabled.
2. Configure the Router-EMS Authentication Key for local authentication, as described in [“Security”](#) on page 120. The password must have a minimum of eight characters. Do not configure RADIUS authentication for Tropos Control users.
3. Open the Administration tab and click **Server Configuration**.
4. Select **Enabled** from the FIPS Mode drop-down list, and click **Submit**.

5. FIPS is enabled, and the Tropos Control EMS server restarts. After a few minutes, close and reopen your browser and then log in. When you reopen the Server Configuration page, a **Zeroize** button is displayed.

Tropos Control Configuration

Banner:

FIPS Mode:

Network Health History: days

* Tropos Control Server will be restarted upon FIPS Mode modification.

* Tropos Control users password length should be of minimum 8 characters for it to be running in FIPS Mode .

The Zeroize button allows you to immediately secure the system in the event of a potential security problem. If you click the button, all critical security parameters stored in clear text are automatically removed from the system. This action also shuts down the Tropos Control server. Following shutdown, you must reinstall the server software.

B Redundant Tropos Control Servers for Failover

This appendix describes how to configure primary and secondary Tropos Control servers so that the secondary server takes over if the primary server is not available.

- [Primary and Secondary Servers](#)
- [Set Up the Primary and Secondary Servers](#)
- [Set Up the Secondary Server as Backup](#)
- [Perform Failover from the Primary to Secondary Server](#)
- [Returning to the Primary Server when it Recovers](#)

Primary and Secondary Servers

The primary Tropos Control Server is responsible for managing the Tropos network. As part of its normal management function, the primary server maintains a current database of devices. When a secondary server is configured, the primary server automatically copies the database to the secondary server. If the primary server fails for any reason, the secondary server is able to immediately take over the management functions and discover any routers that it has not already discovered.

During failover, the secondary server can provide most management functions. An exception is that the secondary server cannot execute network performance measurements. Implementation is limited in that network performance data can run only on a single server. During normal operations, performance measurements are disabled on the secondary server. Following failover, they are enabled on the secondary server.

Set Up the Primary and Secondary Servers

Follow this process to download, install, and configure the primary and secondary servers:

1. Install Tropos Control on the primary and secondary servers, as described in [Chapter 2, “Installation.”](#) Make sure that you install the same version of Tropos Control on both servers. Also, if you are using an Oracle database, make sure to stop the primary server (by

running the command **service watchdog stop**) before installing the secondary server. After the secondary server is installed, power off the secondary server to keep it in standby mode.

2. If you are using MySQL, start both the primary and secondary servers. If you are using Oracle, start only the primary server.
3. If you are using MySQL configure each server to discover the entire network, as described in “Discovery” on page 19.

Set Up the Secondary Server as Backup

1. Log in to the primary server as root.
2. Install the “expect” software package on CentOS if it is not installed:
3. Install the redundancy file by issuing the following commands in a terminal window:

```
[root@localhost]# yum install expect
[root@localhost]# cd /<installdirectory>/ems/bin/redundancy
[root@localhost]# chmod a+x *
[root@localhost]# ./setupRedundantServer <Secondary IP Address> <Secondary
root password>
```

Example:

```
[root@localhost]# ./setupRedundantServer.sh 192.168.128.194 passwd
1 Checking for secure password-less logins to 192.168.128.194, please
wait... done
2 Querying the system for all the devices, please wait... done
3 Finding Control Server Installations on 192.168.128.194... done
4 Copying discover_devices.txt to 192.168.128.194:/opt/ControlServer/ems/
conf/server... done
5 Setting up crontab on 192.168.128.194... done
6 Setting up crontab on this server... done
[root@localhost]#
```

Perform Failover from the Primary to Secondary Server

Follow these steps to move operations to the secondary server upon service interruption or failure of the primary server:

1. Disconnect the primary server from the network. Unexpected results may arise if the primary server is still active and managing the network.
2. Issue the following commands on the secondary server to take over primary server operations:

For Oracle database:

```
% service watchdog restart
```

For MySQL database:

```
[root@localhost]# cd /<installdirectory>/ems/bin/redundancy
[root@localhost]# chmod a+x *
[root@localhost]# ./disableRedundancy.sh
```

Example:

```
[root@localhost redundancy]# ./disableRedundancy.sh
Disabling secure password-less logins to this server, please wait... done
Restoring crontab... done
[root@localhost redundancy]#
```

Make sure to provision all the gateways with the secondary server's IP address in the SNMP page for Trap-Receiver-Registration and EMS-Registration so that the secondary server receives traps from the routers and generates alarms/notifications correctly.

Returning to the Primary Server when it Recovers

For the Oracle database, when the primary server becomes available again, first power off the secondary server to keep it in standby mode and then start the EMS watchdog service on the primary server.

For the MySQL database, when the primary server becomes available again, start the EMS watchdog service on the primary server and make sure to run the `setupRedundantServer.sh` script on it to enable redundancy and to keep the secondary server in standby mode.

Glossary

This glossary defines terms pertaining to wireless and networking technology.

802.11

IEEE wireless networking standards developed by IEEE. There are multiple versions of the 802.11 specification; Tropos Networks products conform to the 802.11b specification.

802.1x

IEEE standard for port-based client authentication using a central authentication server to verify client identity.

AAA Server

Server that provides authentication, authorization and accounting services over a network.

Adaptive Noise Immunity (ANI)

adaptive noise immunity (ANI).

Address Resolution Protocol (ARP)

Standard protocol for mapping an IP address to a hardware (MAC) address.

Airtime Congestion Control

Tropos Networks method of allowing networks to be operated close to their maximum capacity by detecting and averting congestion events.

Autonomous System (AS)

Collection of networks under a single administrative structure and with a single, well-defined routing policy.

Advanced Encryption Standard (AES)

Effective single-key encryption standard originally adopted by the National Institute of Standards and Technology for use by U.S. government organizations and later adopted as an industry standard.

Backhaul

Process of transmitting data so it can be sent over a backbone network, typically to the Internet. Tropos wireless networks provide wireless backhaul from client stations through the wireless Tropos mesh to the wired network.

Basic Service Set (BSS)

The set of all wireless client stations controlled by a single Tropos router. The BSS is identified by the BSS identifier (BSSID), often the MAC address of the router.

Border Gateway Protocol (BGP)

Internet protocol that allows routers to share information and provides the routing mechanism for same-subnet roaming in the Tropos network.

Certificate Authority (CA)

Trusted network entity that issues digital security credentials.

Call Admission Control (CAC)

Mechanism for improving QoS for VoIP communications by causing calls to be rejected in the presence of contention.

Domain Name Service (DNS)

Standard used to convert alphanumeric Internet domain names to IP addresses.

Dynamic Host Configuration Protocol (DHCP)

Protocol used for central, dynamic management of IP addresses. A DHCP server leases DHCP addresses to individual network entities for a specified period of time. Leases can be renewed automatically when the lease period ends. DHCP assures flexibility in IP address assignment and precludes the necessity of generating and entering static IP addresses for each network entity.

Differentiated Services Code Point (DHCP)

Integer value that is included in the DS field of an IP header and which designates a specific QoS value.

Extended Service Set (ESS)

A wireless network that consists of multiple Tropos routers, each of which provides wireless service to network clients.

Extensible Authentication Protocol (EAP)

Effective authentication protocol that supports multiple authentication methods, including passwords, tokens, certificates and public-key authentication.

ESSID

Alphanumeric name that uniquely identifies the wireless network.

Federal Information Processing Standards (FIPS)

General security standards for protection of sensitive information, required by government agencies in the U.S. and Canada.

- Gateway**
Tropos router that connects directly to the wired network and provides backhaul for downstream Tropos nodes and clients.
- Generic Route Encapsulation (GRE)**
Protocol used in creating virtual private networks between clients or between clients and servers.
- Global Positioning System (GPS)**
Satellite navigation system used for accuracy positioning.
- Hypertext Transfer Protocol (HTTP)**
Protocol that manages data transfers between web browsers and servers.
- Hypertext Transfer Protocol over SSL (HTTPS)**
Secure version of HTTP based on Secure Sockets Layer (SSL).
- Internet Control Message Protocol (ICMP)**
Error and control message protocol for the Internet. ping uses ICMP echo requests and replies.
- Internet Protocol (IP)**
Packet routing protocol operating at the network level which associates individual addresses with network nodes.
- IP address**
Method of identifying a network entity as a 32-bit number, usually presented as four, period-separated 8-bit (3-digit) numbers according to the Internet Protocol specification.
- Internet Protocol Security (IPSec)**
Internet security protocol used in virtual private networks (VPNs).
- Management Information Base (MIB)**
A set of objects that can be managed by SNMP or another network management system.
- Maximum Transmission Unit (MTU)**
The largest packet size in bytes transmitted over the network.
- Media Access Control (MAC) Address**
Device-specific identifier, assigned during device manufacture, that uniquely identifies a network node. MAC address filters can be used to limit assignment of IP addresses to wireless clients.
- Meshed cluster**
Collection of Tropos gateways and nodes providing wireless communications services to network clients and establishing backhaul to the wired network. Clients communicate with Tropos nodes, which communicate in turn

with other nodes, and finally to Tropos gateways, which connect to the wired network.

Mobile node

Tropos router that is designed to be mounted in a moving vehicle.

Netmask (subnet mask)

The broadcast domain for a subnetwork, consisting of the subnet prefix for an IP address (example: 255.255.255.0).

Network Address Translation (NAT)

Method whereby nodes within a local area network can access the Internet without having a public Internet address assigned. Administrators can assign local IP addresses from their own address pool and use NAT to translate these into publicly-accessible addresses. NAT can also be used to map multiple local nodes to a single globally-accessible IP address.

Network Mode

Optimization level for 802.11 beacons and probe responses.

Network Time Protocol (NTP)

Method of synchronizing clocks on network devices.

Node

Tropos router that provides wireless communications support for clients and provides wireless backhaul to other upstream Tropos nodes and gateways.

Packet Success Probability (PSP)

The probability that a transmitted packet will be received successfully.

Ping Packet Internet Groper (ping)

Method of troubleshooting network connections by determining whether a specific IP address is reachable and the amount of time required for the addressed device to respond.

Post Office Protocol 3 (POP3)

Industry standard protocol that permits users to receive email from an email server.

Power Over Ethernet (PoE)

Method of supplying electrical power to a device through an Ethernet network data cable. This permits devices to be powered without a separate electrical power connection.

Predictive Wireless Routing Protocol (PWRP)

Tropos technique for managing network routing based on self-organizing principles.

Quality of Service (QoS)

Any of a variety approaches to guaranteeing network performance for specified uses. Tropos supports QoS through bandwidth reservations and priority-based forwarding.

Remote Authentication Dial-In User Service (RADIUS)

Client/server protocol that allows organizations to store client account information in a centrally located database and call up the information as needed to verify client identity.

Request to send (RTS)

Signal sent from a transmitting device to a receiving device that requests approval to send packets. To approve, the receiving device responds with a clear to send (CTS) message.

Reverse Packet Success Probability (PSP)

The probability that a transmitted backhaul packet will be received successfully.

Roaming

The ability to move from one wireless coverage area to another without loss of service. Client initiated roaming occurs when the client detects loss of association and associates with another router. Tropos supports client initiated roaming throughout the wireless routing domain.

Router (Tropos)

Tropos Networks devices that provide the communications infrastructure for wireless mesh networks.

Secure SHell (SSH)

Secure method of accessing a remote computer.

Service Set Identifier (SSID)

Alphanumeric identifier for a network, used interchangeably with ESSID.

Secure Sockets Layer (SSL)

A common protocol for message transmission security on the Internet. Existing as a program layer between Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers, SSL is a standard feature in Internet Explorer, Netscape, and most web server products.

Simple Mail Transfer Protocol (SMTP)

Protocol that governs transfer of email messages between email servers.

Simple Network Management Protocol (SNMP)

Protocol used for device and network management.

SNMP inform

SNMP message sent to a notification server, indicating noteworthy activity or events.

Static IP Address

Permanent IP address assigned to a node in a TCP/IP network.

Subnet

Portion of a larger network, distinguished by a subnet mask or broadcast domain.

Subnet Mask

Method of addressing subnets. For example, the subnet mask 255.255.255.0 refers to the subnet in which the first three triplets of the IP address are fixed, and the available subnet addresses use the last triplet of the IP address.

Telnet

Terminal emulation protocol for connecting to a remote computer.

Temporal Key Integrity Protocol (TKIP)

Encryption standard included in the 802.11i specification, which improves on WEP encryption by adding effective key mixing and message integrity checks.

Transmission Control Protocol/Internet Protocol (TCP/IP)

The suite of protocols on which Internet communications are based.

Transport Layer Security (TLS)

Protocol that provides security for local and Internet applications. TLS is a newer generation version of Secure Sockets Layer (SSL).

Tunneled Transport Layer Security (TTLS)

Security protocol that combines network-based certificates with token or password authentication. Often used in conjunction with EAP.

Universal Time Coordinated (UTC)

Official world time, equivalent to Greenwich Mean Time.

User Datagram Protocol (UDP)

Protocol that shares many common attributes with TCP but without the reliability capabilities of TCP. UDP is often used for applications that can tolerate some level of error.

Virtual LAN (VLAN)

Logical grouping of client stations that enables them to function as if they are on the same subnetwork, regardless of their actual physical location.

Virtual Private Network (VPN)

Network in which remote users are securely connected over the Internet and operate as if connected locally.

Voice over IP (VoIP)

Network in which remote users are securely connected over the Internet and operate as

Wi-Fi Protected Access (WPA)

Effective wireless authentication security solution introduced by the Wi-Fi Alliance, an industry consortium. WPA is compatible with and now contained in the IEEE 802.11i specification.

Windows Name Service (WINS)

Microsoft Windows standard for converting alphanumeric Internet domain names to IP addresses.

Wired Equivalent Privacy (WEP)

Default security system for 802.11 networks.

Wireless Multimedia Extensions (WMM)

Wi-Fi Alliance standard that specifies QoS capabilities for wireless networks with wireless traffic.

Wireless Network, or Wireless Local Area Network (WLAN)

Local area network based on 802.11 wireless communications.

Wi-Fi Multimedia (WMM)

IEEE 802.11e standard used voice QoS in 802.11 networks. Also known as Wireless Multimedia Extensions (WME).

Index

Numerics

802.11 5
802.1p 117

A

additional client transmit power attenuation 89
administration tab
 inventory tracking 134
 router software update 131
 tech support 130
administration tag
 diagnostic information 130
alarms
 actions 51
 color codes 51
 configuration view button 64
 filters 53
 settings 53
 viewing on web 51
ARP cache 14
AS number
 local 111
 remote 111, 112
auto-detect
 static IP clients 104
automatic discovery 23

B

backhaul
 mobile routers 7
 standalone mode 7
backhaul routing 111
 service/VLAN ID 112
BGP
 and backhaul routing 111

C

Cisco 108
Client Access page 92
client optimization
 statistics 34
client reports

 detailed data 38
 reported information 36
 visited nodes and gateways 37
cluster 4
configuration information
 viewing on web 59
Configuration Utility 3, 18, 68, 77
configuration view
 actions 60
 exporting list 60
 panels 59
 printing 60
 searching 60
 selecting alarms and events 61
contact person 79
CPE
 and static IP clients 104
 MAC address 104, 105
custom views 64

D

dashboard
 information 25
database
 Oracle 10
 updating router 62
detailed data for client reports 38
DHCP
 lease duration 98
 netmask 98
 packet filtering 108
 server on board 98
DHCP Server page 97
diagnostic information 130
Differentiated Services Code Point.
 See DSCP
discovery
 automatic 23
 manual 23
DNS 108
downstream quality selection 117
DSCP 117, 119
dynamic re-clustering 5

E

ESSID
 with mobile routers 7
events
 configuration view button 64
 counts 52
 list 50

F

fault information
 alarms 51
 network events 50
 viewing on web 49
Federal Information Processing Standards (FIPS) 3
filters
 alarm 53
 configuring 53
FIPS
 and EMS authentication 121
 enabling 150
 properties and restrictions 150
 support 150
 zeroize capability 150

G

gateway
 about 4
 adding cluster 62
 and multi-subnet roaming 65
 discovering 23
 IP address, subnet mask 110
 list 110
gateway list 66

H

HTTP 108
HTTPS 108

I

ICMP 108
installing
 overview 12
 Tropos Control 13
inventory
 tracking router 134
inventory tracking 134
IP address
 of Tropos Control server 13
IPSec 108

L

lease duration 98
local ASN 111

M

map
 configuration view button 64
mesh ID

- description 88
- meshed cluster 4
- mobile router
 - ESSID 7
 - losing backhaul 7
 - network 6
 - network example 7
 - rules 6
- multi-ESSID
 - primary ESSID 93
 - secondary ESSID 93
- multiplier for rate limiting 114, 115
- multi-subnet roaming
 - BGP 111
 - configuring gateways 65
 - gateway list 66
- Multi-Subnet Roaming page 110

N

- network
 - events list 50
 - mobile router 6
 - routing 5
- network events
 - viewing on web 50
- network health
 - overview 20
 - thresholds file 30, 42
- network optimization
 - actions 33
 - backhaul performance 32
 - change key or threshold 32, 35
 - mesh performance 32
 - missing data 32
 - statistics 32
 - view actions 40
 - view details 32, 35, 39
- node
 - about 4

O

- Oracle database 10

P

- packet forwarding
 - permit rules 108
- permit rules 108
- ping
 - operations 40
 - options 41
 - view results 41
- POP3 108
- Predictive Wireless Routing Protocol.

- See PWRP
- product
 - features 3
- product overview 2
- provisioning
 - configuration view button 64

Q

- QoS 115

R

- rate limiting
 - multiplier 114, 115
- Rate Limiting page 113, 116
- remote ASN 111, 112
- router
 - checking upgrade status 133
 - deleting 63
 - fixed 3
 - inventory tracking 134
 - mobile 3
 - models 2
 - scheduling upgrades 131
 - software update panel 131
 - stationary 3
 - synchronizing 63
 - tracking inventory 134
 - updating database 62
 - upgrade 131
- Router Identity page 79
- router-EMS authentication key 121, 150
- routing 5
- RTS 90

S

- server
 - exiting 18
- show map button 64
- SMTP 108
- SNMP 108
 - parameters 100
- software
 - uploading image 134
- SSH 108
- standalone mode 7
- Static IP Client page 104
- static IP clients
 - auto-detect 104
- sub-interface
 - wired priority 117
- subnet route 110
- synchronizing

- router databases 63
- system requirements
 - Tropos Control server 10

T

- tables
 - in web interface 22
- tech support panel 130
- telnet 108
- threshold
 - network optimization 32, 35
 - voice optimization 39
- thresholds file 30, 42
- Time page 101
- time zone 101
- Tropos Control Element Management System (EMS) 3, 8
- Tropos Control server
 - IP address 13
 - system requirements 10
- Tropos Sphere Network Operating System 3
- tunnels, showing current roaming 66

U

- uninstalling
 - server 15
- upgrading
 - checking status 133
 - router software 131
- UTC 101

V

- VLAN ID
 - and backhaul routing 112
- voice optimization
 - change key or threshold 39
 - statistics 39
 - view actions 35
- voice over IP (VoIP)
 - Voice page 118
- Voice page 118

W

- web interface
 - accessing 19
 - adding gateway cluster 62
 - configuration information 59
 - custom views 64
 - tables 22
- WINS 98
- wired sub-Interface priority 117

Wireless page 86, 87
WMM 119