Copyright 2005 by Tropos Networks

All rights reserved. Rights reserved under the copyright laws of the United States.

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 MetroMesh routers comply with Part 15 of the FCC rules. Operation of the Tropos MetroMesh 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

Preface ........................................................................................................ vi

1 Overview .............................................................................................. 1
   Product Overview .................................................................................. 1
   Product Features .................................................................................. 1
   Tropos Networks Architecture ............................................................ 2
   Tropos Mobile MetroMesh Networks .................................................... 4
   Tropos Network Management and Administration ................................ 7

2 Getting Started ...................................................................................... 8
   Setting Up a New Wireless Network ...................................................... 8
   Setting the Gateway Configuration ...................................................... 9
   Using the Configuration Utility ............................................................ 13
      Top Information Bar ........................................................................ 14
      Committing Changes .................................................................... 14
   Adding Fixed Nodes to the Network .................................................... 15
   Adding Mobile Nodes to the Network ............................................... 17
   Adding Clients to the Network ........................................................... 20
   Reassigning Gateways and Nodes ..................................................... 24
      Confirming Router Identity ............................................................. 25
   Checking the Current Configuration ................................................ 26
      Accessing the Configuration Utility Through a Wireless Connection 27
   Setting the Time ................................................................................. 28

3 Configuring Wireless Settings .............................................................. 30
   Service Sets ......................................................................................... 30
   Transmission Rates and Channels ....................................................... 31
      Automatic Channel Selection .......................................................... 31
   Security ................................................................................................. 32
   Client Security ..................................................................................... 32
This guide contains the information and instructions required to install, configure and maintain Tropos MetroMesh routers using the Tropos Configuration Utility. It is intended for use by network engineers and administrators who are responsible for setting up and administering Tropos wireless networks. Some familiarity with local area networking and wireless networking concepts is assumed.

This guide contains the following chapters:

Chapter 1, “Overview,” introduces the features of the Tropos MetroMesh router and provides an overview of the Tropos Networks wireless network architecture.

Chapter 2, “Getting Started,” provides information and instructions for setting up Tropos MetroMesh routers to create a wireless network.

Chapter 3, “Configuring Wireless Settings,” describes the parameters available to control RF communications in the Tropos MetroMesh router network.

Chapter 4, “Configuring Network Settings,” describes the configuration options available to implement a variety of wireless network topologies.

Chapter 5, “Managing Clients,” describes the configuration options available to provide services to network clients.

Chapter 6, “Maintaining the Network,” contains information on how to keep the Tropos MetroMesh routers working effectively.

“Glossary,” contains definitions of terms relating to Tropos wireless networking.
Tropos Technical Support

For technical assistance, contact the Tropos Technical Assistance Center.

<table>
<thead>
<tr>
<th>Whom to contact</th>
<th>How to contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Support Toll-free Number</td>
<td>1-877-987-6767</td>
</tr>
<tr>
<td>Website</td>
<td><a href="http://www.Tropos.com">www.Tropos.com</a></td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:Support@Tropos.com">Support@Tropos.com</a></td>
</tr>
</tbody>
</table>

Supporting Documentation

The following documents are available on the installation CD or shipped with Tropos Networks equipment.

- Release Notes — Contains information specific to the current product release.
- Quick Start Guide — Contains instructions on installing and configuring a Tropos wireless network quickly and easily.
- Tropos Networks Configuration Reference Guide — Contains detailed information on the fields in the Configuration Utility and provides descriptions of the command line interface (CLI) commands.
- Tropos Control Element Management System User Guide — Contains instructions on installing and configuring Tropos Control EMS.
- Professional Hardware Installation Guide, Model 3210 — Explains how to install the Tropos 3210 MetroMesh router hardware.
- Tropos Networks MetroMesh Router Installation Guide, Model 4210— Explains how to install the Tropos 4210 mobile MetroMesh router hardware.
Document Conventions

The following conventions are used in this document.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Notice Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Note" /></td>
<td>Note</td>
<td>Information in notes, while useful, is not as urgent as information following a Caution or Warning sign.</td>
</tr>
<tr>
<td><img src="image" alt="Caution" /></td>
<td>Caution</td>
<td>The Caution icon indicates careful attention is required to prevent loss of data or damage to equipment.</td>
</tr>
<tr>
<td><img src="image" alt="Warning" /></td>
<td>Warning</td>
<td>The Warning icon indicates that careful attention is required to avoid bodily injury. Any activities, such as those involving electrical connections require extreme caution, constant attention, and strict adherence to standard safety practices to prevent injury.</td>
</tr>
</tbody>
</table>

Nested menu items are separated by a angle bracket (>). For example, Start > Programs > Tropos > Tropos Control EMS means first choose the Start button, then choose Programs, then choose Tropos on the submenu, and finally choose 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 to the reader.

Keyboard buttons are enclosed in brackets. For example `<Alt>` indicates the Alt key on the keyboard.

Keys that are to be pressed simultaneously are separated by the addition sign (+). The following example indicates that the Ctrl key and the letter y should be pressed simultaneously `<Ctrl> + y`. 
This chapter introduces the features of the Tropos MetroMesh router and provides an overview of the Tropos Networks wireless network architecture. It contains information on the following topics:

- **Product Overview**
- **Product Features**
- **Tropos Networks Architecture**
- **Tropos Mobile MetroMesh Networks**
- **Tropos Network Management and Administration**

**Product Overview**

Tropos MetroMesh routers make possible wireless computer networking by providing the infrastructure for wireless hot spots and metropolitan scale wireless meshes. The Tropos MetroMesh router models support both indoor and outdoor installations:

- Tropos 3110 MetroMesh router and Tropos 3210 MetroMesh router for indoor coverage
- Tropos 5110 MetroMesh router and Tropos 5210 MetroMesh router for outdoor coverage
- Tropos 4210 MetroMesh router for mobile vehicle installation

All Tropos MetroMesh routers are under the control of the Tropos Network Operating System. Configuration and management are supported through the Tropos Configuration Utility, which is described in this guide, and the Tropos Control Element Management System, which is described in the *Tropos Control Element Management System Installation and User Guide*.

**Product Features**

All Tropos MetroMesh routers provide the following features:

- High-performance Wi-Fi communications
- Integrated 1W radio, optimized for outdoor use
- Scalable 802.11b coverage, up to 11Mbps
- Session-persistent roaming
- Secure local and remote configuration via HTTPS
- WEP and Open security
- AES security for router-router control and management messages
- IP address-based Virtual Local Area Network (VLAN) support
- Quality of Service (QoS) support based on user groups and application
- SNMP-based element management system
- Tropos Network Operating System Layer 3 intelligent path selection
- Auto-discovery and auto-configuration on power-up
- Continuous, real-time adjustment of optimum data paths
- Redundant, self-healing network architecture
- User-defined traffic filters, including filters that allow access only to authorized VPN servers
- MAC address access control lists
- Full VPN compatibility
- Global Positioning System (GPS) integration
- UL/cUL listed for outdoor use and able to be mounted on external structures (Tropos 5210 and 5110 MetroMesh routers)

In addition, the Tropos 5210, 4210, and 3210 routers provide the following advanced features:
- WPA-1X and WPA-PSK security with EAP-TTLS
- Scalable 802.11g coverage, up to 54Mbps
- Multi-use network management using ESSID and IP based VLANs
- Multi-ESSID support/Multi-authentication support

**Tropos Networks Architecture**

You can configure each fixed Tropos router (5210/5110/3210/3110) to operate as a **gateway** or a **node**. Configured as a gateway, the router establishes communications between the wired Ethernet network and other Tropos routers that operate as nodes. Tropos nodes, in turn, form radio communications links with the clients (users) on the network. Gateways can also service clients directly. Tropos 4210 MetroMesh routers always operate as nodes.

A Tropos wireless network consists of Tropos gateways connecting directly to the wired network and Tropos nodes delivering wireless communications support for clients and providing wireless backhaul to other upstream Tropos nodes and gateways. The Tropos routers form a **meshed cluster** to dynamically route wireless signals from clients through the gateway and on to the wired network. Figure 1 illustrates a basic Tropos wireless network.
Each Tropos node communicates with standard 802.11 clients and passes data back through a wireless link to a Tropos gateway attached to the wired network. All routers continually monitor the quality of the wireless links and jointly 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 with 802.11b/g.

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. As shown in Figure 2, 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 Tropos nodes back the Tropos gateway and the wired network.

**Figure 2  Typical Tropos Wireless Network**

Due to dynamic re-clustering, it is not necessary to engineer individual paths 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. Changing interference conditions and new backhaul options are among the conditions that cause automatic regeneration of optimal paths. Overall network performance improves due to the maximization of throughput; and reliability increases because there is no system-wide single point of failure.

Tropos wireless networks permit easy addition of new Tropos routers to support growth in the number of client subscribers. You can add new nodes to extend coverage at any location with power. As the number of subscribers continue to grow, you can add new gateways to further increase coverage, performance, and reliability.

**Tropos Mobile MetroMesh Networks**

Tropos 4210 mobile MetroMesh routers extend the Tropos wireless network to mobile node operation. By installing Tropos 4210 routers in fire, police, or other public service vehicles, you can provide immediate high-bandwidth access to network services. As with other Tropos routers, the Tropos 4210 router dynamically associates to upstream nodes or gateways.
**Note**
You can install Tropos 4210 routers in networks with mixed Tropos gateways and nodes (models 5210, 5110, 3210, and 3110). To support the Tropos 4210 routers, it is necessary for all routers to be running Tropos Release 5.0 or later software.

Clients connect to the Tropos 4210 router through a wireless or wired connection. In the typical vehicle installation, the client computer is connected directly to the Tropos 4210 router through a wired downstream sub-interface connection.

Since the Tropos 4210 routers may be in motion, special rules apply to the association of wireless clients to Tropos 4210 routers and from Tropos 4210 routers to other upstream nodes or gateways. The following guidelines and properties apply:

- It is recommended that you configure a separate ESSID for the mobile nodes. Wireless clients accessing this ESSID will always try to associate to mobile nodes, and clients accessing other ESSIDs will always attempt to associate to fixed nodes. This arrangement prevents typical fixed 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 to the mobile nodes.

- The Tropos 4210 router always attempts to establish backhaul connection to an upstream fixed Tropos node or gateway. If that is not possible, a router will attempt to connect to another 4210 router.

- A fixed Tropos node will not attempt to establish uplink to a Tropos 4210 router.

If any Tropos router loses backhaul connectivity, it shifts to standalone mode so that it does not 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 node is more likely to lose wireless connectivity than a fixed node, clients associated to a mobile node may encounter more frequent service disruptions than those associated to fixed nodes. To prevent unsuccessful data transmission attempts from the client when upstream connectivity is lost, the downstream wired interface for the Tropos 4210 is immediately switched off.
Figure 3 shows a typical Tropos network with mobile nodes added, and Figure 4 illustrates automatic rerouting actions if connectivity to the fixed Tropos network is interrupted.

**Figure 3  Typical Tropos Mobile MetroMesh Network**
Tropos Network Management and Administration

The Tropos Configuration Utility includes a secure HTTPS interface to control and manage each Tropos router. Connection is through the wired Management port on the Tropos router or association of a laptop client. This guide describes the configuration selections available through the Tropos Configuration Utility.

Tropos Networks also offers the Tropos Control Element Management System (EMS) to administer multiple Tropos routers across the network. Tropos Control EMS includes network-wide fault monitoring to assess the overall state of the network and enables provisioning of multiple routers.

Together, the Tropos Configuration Utility and Tropos Control EMS provide a comprehensive administrative structure for managing the network.
2 Getting Started

This chapter provides instructions on setting up Tropos MetroMesh routers to create a wireless network. Before you begin, make sure that you have followed the mounting and connection instructions detailed in the appropriate Tropos MetroMesh Router Installation Guide. See “Supporting Documentation” on page vii for a list of installation documentation.

This chapter contains information on the following topics:
- Setting Up a New Wireless Network
- Setting the Gateway Configuration
- Using the Configuration Utility
- Adding Fixed Nodes to the Network
- Adding Clients to the Network
- Reassigning Gateways and Nodes
- Checking the Current Configuration
- Setting the Time

Setting Up a New Wireless Network

To form a Tropos wireless network, you first install and connect a Tropos router as a gateway and then expand network coverage by adding additional Tropos routers as nodes, ensuring that they are within radio range of each other.

The default settings in each Tropos router are intended for easy initial set-up. Each fixed router (Tropos 3110, 3210, 5110, or 5210) is shipped from the factory is pre-configured as a gateway. In this default configuration, the router configuration mode is “DHCP,’’ and the router receives an IP address from an external DHCP server. You can readily connect the new wireless network to an existing Ethernet network with working DHCP address services.

Each Tropos 4210 mobile MetroMesh router is shipped from the factory with the Mobile Node setting.
Set up a new network

1. Follow the instructions in the appropriate Tropos MetroMesh Router Installation Guide (see list in “Supporting Documentation” on page vii) to unpack and connect power for the Tropos router you intend to use as your network gateway (Tropos gateway).

2. Connect an Ethernet cable from your working network to the LAN port on the Tropos gateway.

   **Note**
The RJ45 connectors of the Tropos 5210 Outdoor router may source DC power on pins 4, 5 and 7, 8. The IEEE 802.3 standards allow for pins 4, 5 and 7, 8 to be used for Power Over Ethernet. Some products may be incompatible with the Tropos Power Over Ethernet capability. If such problems occur, make sure that the unit is configured with the Power Over Ethernet capability set to Off (default setting). If problems persist, use Ethernet cables that have no connections to the unused pins 4, 5 and 7, 8.

3. Power-up the Tropos gateway.

4. Wait for the status indicator light on the Tropos node to turn green (Tropos 5210, 4210, or 3210 router) or start blinking (Tropos 3210 or 3110 router). For more information on the operational lights, see “Viewing Equipment Status” on page 109.

A new wireless network is now established. Before adding nodes and clients to the network, it is strongly recommended that you access the Tropos Configuration Utility to confirm or modify configuration settings.

**Note**
If the status indicator light is red, check the cable connections. Make sure that DHCP services are working for other clients on the wired network. For further information on the power-up sequences for the Tropos routers, see “Viewing Equipment Status” on page 109.

Setting the Gateway Configuration

Use Table 1 to record basic configuration parameters for the Tropos gateway. Additional information regarding these parameters is contained in Chapter 3, “Configuring Wireless Settings.”

**Note**
The items identified in bold in Table 1 must be the same for all gateways, nodes, and clients on the network.
Table 1 Gateway Configuration Worksheet

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Default</th>
<th>Your Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESSID</td>
<td>Unique, easy-to-remember alphanumeric name for the network, with no spaces</td>
<td>TroposNetworks</td>
<td></td>
</tr>
<tr>
<td>ESSID Suppression</td>
<td>Indication of whether the Tropos router excludes the ESSID from the radio beacons it broadcasts. Can be assigned on a per-ESSID basis in multiple ESSID configurations</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Client authentication method for the network</td>
<td>Open</td>
<td></td>
</tr>
<tr>
<td>WEP Type</td>
<td>Encryption type, if WEP is selected as an authentication type</td>
<td>Hex64-bit</td>
<td></td>
</tr>
<tr>
<td>WEP Key</td>
<td>Choice of encoding key, if WEP is enabled</td>
<td>aabbccddeee</td>
<td></td>
</tr>
<tr>
<td>PSK Passphrase</td>
<td>Password used, if WPA-PSK is selected as an authentication type</td>
<td>whatever</td>
<td></td>
</tr>
<tr>
<td>RADIUS Server</td>
<td>IP address of a RADIUS authentication server, if WPA-1x is selected as an authentication type</td>
<td>10.88.22.50</td>
<td></td>
</tr>
<tr>
<td>RADIUS Authentication Port</td>
<td>RADIUS server port used for authentication messages, if WPA-1x is selected as an authentication type</td>
<td>1812</td>
<td></td>
</tr>
<tr>
<td>RADIUS Secret</td>
<td>Password used for routers to connect to the RADIUS server, if WPA-1x is selected as an authentication type</td>
<td>mysecret</td>
<td></td>
</tr>
<tr>
<td>Wireless Routing Domain ID</td>
<td>Sixteen character string that uniquely identifies your network</td>
<td>1234123412341234</td>
<td></td>
</tr>
<tr>
<td>Router-Router Tx Rate</td>
<td>Desired rate for communications between Tropos routers in the network</td>
<td>11 Mbps</td>
<td></td>
</tr>
<tr>
<td>Channel</td>
<td>Radio channel on which the gateway will communicate with downstream nodes and clients</td>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>
To configure the gateway settings, you must first configure your computer to start the Tropos Configuration Utility. Access to this utility is through the management port on the Tropos gateway.

### Configure your computer to access the Tropos Configuration Utility

1. From the Start button, open the Network Connections control panel.

   Start → Settings → Network and Dial-Up Connections

   or

   Start → Control Panel → Network Connections

2. Right-click the Ethernet (for example, 10BaseT) or Local Area Connections icon for your PC, and select Properties.

3. Select Internet Protocol (TCP/IP), and click Properties.

4. Click Use the following IP address.

5. In the IP address box, enter the following IP address: **192.168.167.160**. For wireless connection, use the address **192.168.166.160**. These are the addresses that are pre-
configured on each Tropos router. “Accessing the Configuration Utility Through a Wireless Connection” on page 27.

6. In the Subnet mask box, enter **255.255.255.0**.

7. Click **OK**.

8. Click **Close** or **OK** to close the Local Area Connection Properties window.

9. If prompted, restart your computer.

You can now prepare to access the Tropos Configuration Utility.

**Access the Tropos Configuration Utility**

1. Connect your computer to the port marked MGT on the Tropos router using an IEEE 802.3 RJ-45 DC blocking crossover cable.

2. Open the Web browser (Explorer or Netscape) on your PC.

3. In the URL window of the browser, enter the management IP address of the Tropos router: **https://192.168.167.166**. This is the address that is pre-configured on each Tropos router.
   
   Note that you must use the secure https protocol, and not http.

4. If you receive security alerts about viewing pages over a secure connection, click **Yes** to proceed.

   You may receive an additional security alert. The name of the security certificate issued by Tropos Networks may not match the name of the site.

   **Note**
   
   To avoid future security warnings, generate a security certificate according to the instructions in “Generating SSL Certificates” on page 124.

5. Click **Yes** to proceed.

6. When the Enter Network Password dialog box opens, enter the username **admin** and password **tropos**.

7. Click **OK**.

   The Tropos Configuration Utility opens.

To complete the initial gateway configuration, you must open the Wireless Configuration screen and verify the wireless settings for your network. Refer to Chapter 3, “Configuring Wireless Settings,” for instructions, using the values that you recorded in Table 1 on page 10.
Using the Configuration Utility

The left side menu of the Configuration Utility, shown in Figure 5, provides access to all the configuration screens. This guide explains how to use each screen; for a complete list of parameters on each screen, refer the Tropos Networks Configuration Reference Guide.

Figure 5 Configuration Utility Interface
Top Information Bar

The top information bar displays the following information:

- Name assigned to the router
- Global Positioning System (GPS) coordinates, if they are available from an external GPS receiver installed with the router. Only Tropos qualified GPS receivers are supported. For further information, see the *Tropos 4210 Mobile MetroMesh Router Installation Guide*.
- Length of time since the router was last powered up.

Committing Changes

For flexible control over configuration changes, the Configuration Utility provides the ability to build configuration changes and then choose when to make them operational. To make a configuration change, you first store the changes in a temporary location. You can then choose when to commit the changes and whether there should be a time delay. During the window of time between committing changes and having the changes take place, you can cancel the process.

After you commit changes, the committed values are displayed in a read-only column at on the right side of the screen, as shown in Figure 5.

**Store configuration changes**
- Click *Store Changes* at the bottom of the configuration screen.

**Commit configuration changes that you have previously stored**
1. Click *Commit Changes* on the left menu bar to open the Commit Changes screen.
2. Enter a time delay in seconds, if desired.
3. Click the *Commit Changes* button.

To confirm the new settings, return to the screen or screens on which you made the changes and view the values in the Committed column.

**Cancel changes that have been requested**
1. Open the Commit Changes screen.
2. Click *Cancel Changes*.

**Note**
Changes that are stored but not committed are deleted if power is lost to the gateway or node.
Adding Fixed Nodes to the Network

With the Tropos gateway set up and configured, you can now add fixed Tropos nodes to the network. First use the configuration worksheet in Table 2 to enter wireless configuration settings for the nodes. The items in bold must be the same for all gateways, nodes, and clients on the network.

**Add nodes to the network**

1. Supply power to the Tropos router you plan to use as a node (Tropos node). Do not connect an Ethernet cable to the LAN port. Instead, connect your computer to the port labeled MGT on the Tropos router using an IEEE 802.3 RJ-45 DC blocking crossover cable.

2. Open the Configuration Utility according to the instructions in “Access the Tropos Configuration Utility” on page 12.

3. Select Device & IP.

4. On the Device & IP Configuration screen, change the router setting to Node.¹

5. Click Store Changes.

6. Select Wireless on the side menu.

7. On the Wireless Configuration screen, enter or confirm the values in Table 2.

8. Click Store Settings.

9. To commit the changes made on the Device & IP Configuration screen and the Wireless Configuration screen, select Commit Changes from the side menu. Enter a time delay, if desired, and click Commit Changes.

Monitor the status indicator on the Tropos node. When the status indicator light turns green (Tropos 5210/4210/3210 routers) or starts blinking (Tropos 5110/3210 router), the node is fully connected and communicating with the Tropos gateway. You can now add additional nodes or client stations. For more information on the operational lights, see “Viewing Equipment Status” on page 109.

---

**Note**

If the status indicator light is red, check the cable connections. Make sure that DHCP services are working for other clients on the wired network. For further information on the power-up sequences for the Tropos routers, see “Viewing Equipment Status” on page 109.

---

¹ This step is optional. If no Ethernet is detected, the router automatically shifts to node operation.
### Table 2: Node Configuration Worksheet

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Default</th>
<th>Your Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESSID</td>
<td>Unique, easy-to-remember alphanumeric name for the network, with no spaces</td>
<td>TroposNetworks</td>
<td></td>
</tr>
<tr>
<td>ESSID Suppression</td>
<td>Indication of whether the Tropos router excludes the ESSID from the radio beacons it broadcasts. Can be assigned on a per-ESSID basis in multiple ESSID configurations</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Client authentication method for the network</td>
<td>Open</td>
<td></td>
</tr>
<tr>
<td>WEP Type</td>
<td>Encryption type, if WEP is selected as an authentication type</td>
<td>Hex64-bit</td>
<td></td>
</tr>
<tr>
<td>WEP Key</td>
<td>Choice of encoding key, if WEP is enabled</td>
<td>aabbccdddee</td>
<td></td>
</tr>
<tr>
<td>PSK Passphrase</td>
<td>Password used, if WPA-PSK is selected as an authentication type</td>
<td>whatever</td>
<td></td>
</tr>
<tr>
<td>RADIUS Server</td>
<td>IP address of a RADIUS authentication server, if WPA-1x is selected as an authentication type</td>
<td>10.88.22.50</td>
<td></td>
</tr>
<tr>
<td>RADIUS Authentication Port</td>
<td>RADIUS server port used for authentication messages, if WPA-1x is selected as an authentication type</td>
<td>1812</td>
<td></td>
</tr>
<tr>
<td>RADIUS Secret</td>
<td>Password used for routers to connect to the RADIUS server, if WPA-1x is selected as an authentication type</td>
<td>mysecret</td>
<td></td>
</tr>
<tr>
<td>Wireless Routing Domain ID</td>
<td>Sixteen character string that uniquely identifies your network</td>
<td>1234123412341234</td>
<td></td>
</tr>
<tr>
<td>Router-Router Tx Rate</td>
<td>Desired rate for communications between Tropos routers in the network</td>
<td>11 Mbps</td>
<td></td>
</tr>
<tr>
<td>Channel</td>
<td>Radio channel on which the gateway will communicate</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Router Name</td>
<td>Alphanumeric name for the gateway</td>
<td>TroposRouter</td>
<td></td>
</tr>
<tr>
<td>Router Location</td>
<td>Physical location of the gateway</td>
<td>Sunnyvale</td>
<td></td>
</tr>
</tbody>
</table>
Adding Mobile Nodes to the Network

To add Tropos 4210 mobile MetroMesh routers to the network, first use the configuration worksheet in Table 3 to enter wireless configuration settings for the nodes. The items in bold must be the same for all gateways, nodes, and clients on the network.

**Add nodes to the network**

1. Install the Tropos 4210 node according to the instructions in the *Tropos 4210 Mobile MetroMesh Router Installation Guide*. Connect your computer to the port labeled MGT on the Tropos router using an IEEE 802.3 RJ-45 DC blocking crossover cable.
2. Open the Configuration Utility according to the instructions in “Access the Tropos Configuration Utility” on page 12.
3. Select Device & IP.
4. On the Device & IP Configuration screen, confirm that the settings is Mobile Node.
5. Click Store Changes.
6. Select Wireless on the side menu.
7. On the Wireless Configuration screen, enter or confirm the values in Table 3.
8. To use the automatic channel selection option for the node, follow these steps:
   a. Choose auto from the Channel pull-down list, and click Store Changes. The screen reopens to display an entry area for the channels you would like make available for automatic selection.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Default</th>
<th>Your Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Person</td>
<td>Name or email address of the person responsible for the gateway</td>
<td><a href="http://www.troposnetworks.com">www.troposnetworks.com</a></td>
<td></td>
</tr>
<tr>
<td>Router Longitude</td>
<td>Longitude to identify router location (format is xx.xxxxxxxx, with up to 8 digits permitted to the right of the decimal point)</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Router Latitude</td>
<td>Latitude to identify router location (format is xx.xxxxxxxx, with up to 8 digits permitted to the right of the decimal point)</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Client Rate</td>
<td>Transmission rate between clients and the Tropos router.</td>
<td>auto</td>
<td></td>
</tr>
</tbody>
</table>
b. Enter up to six channels. The default channels are 1, 6, and 11.

9. Click Store Changes.

10. To commit the changes made on the Device & IP Configuration screen and the Wireless Configuration screen, select Commit Changes from the side menu. Enter a time delay, if desired, and click Commit Changes.

Monitor the status indicator on the Tropos node to determine when it is fully connected and communicating with the Tropos gateway. For more information on the operational lights, see “Viewing Equipment Status” on page 109.

When the node is fully connected and communicating with the gateway or other nodes, you can add additional nodes or client stations. If the router does not start communicating with the gateway or other nodes, check to see whether the settings for ESSID, WEP, and Wireless Routing Domain ID exactly match those in the router.
### Table 3  Tropos 4210 Configuration Worksheet

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Default</th>
<th>Your Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESSID</td>
<td>Unique, easy-to-remember alphanumeric name for the network, with no spaces</td>
<td>TroposNetworks</td>
<td></td>
</tr>
<tr>
<td>ESSID Suppression</td>
<td>Indication of whether the Tropos MetroMesh router excludes the ESSID from the radio beacons it broadcasts. Can be assigned on a per-ESSID basis in multiple ESSID configurations</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Client authentication method for the network</td>
<td>Open</td>
<td></td>
</tr>
<tr>
<td>WEP Type</td>
<td>Encryption type, if WEP is selected as an authentication type</td>
<td>Hex64-bit</td>
<td></td>
</tr>
<tr>
<td>WEP Key</td>
<td>Choice of encoding key, if WEP is enabled</td>
<td>aabbccddee</td>
<td></td>
</tr>
<tr>
<td>PSK Passphrase</td>
<td>Password used, if WPA-PSK is selected as an authentication type</td>
<td>whatever</td>
<td></td>
</tr>
<tr>
<td>RADIUS Server</td>
<td>IP address of a RADIUS authentication server, if WPA-1x is selected as an authentication type</td>
<td>10.88.22.50</td>
<td></td>
</tr>
<tr>
<td>RADIUS Authentication Port</td>
<td>RADIUS server port used for authentication messages, if WPA-1x is selected as an authentication type</td>
<td>1812</td>
<td></td>
</tr>
<tr>
<td>RADIUS Secret</td>
<td>Password used for routers to connect to the RADIUS server, if WPA-1x is selected as an authentication type</td>
<td>mysecret</td>
<td></td>
</tr>
<tr>
<td>Wireless Routing Domain ID</td>
<td>Sixteen character string that uniquely identifies your network</td>
<td>1234123412341234</td>
<td></td>
</tr>
<tr>
<td>Router-Router Tx Rate</td>
<td>Desired rate for communications between Tropos routers in the network</td>
<td>11 Mbps</td>
<td></td>
</tr>
<tr>
<td>Channel</td>
<td>Radio channel on which the gateway will communicate. To activate the auto-select channel option for mobile nodes, choose auto.</td>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>
Adding Clients to the Network

The process of configuring client PC settings to use the Tropos wireless network varies somewhat according to the operating system of the PC. This section provides the standard Windows instructions for Windows XP and Windows NT or 2000.

**Note**
If you are configuring the network for WPA security, you can configure this option in Windows XP by using the Wireless Zero Config (WZC) feature, as explained in this section. To configure WPA security on Windows 2000, it is necessary to use a third party tool such as Funk Odyssey for configuration. You can also use Funk Odyssey with Windows XP.

Setting the Client Configuration

The instructions in this section apply if you are using the Windows configuration utility, not one that was supplied with the wireless network card.

**Note**
Make sure the client network adapter (wireless adapter) is set for DHCP so that an IP address is automatically assigned to the client device.
Configure a Windows XP PC client

1. From the Start button, select Control Panel → Network Connections.
2. Right-click the Wireless Connections icon and select Properties.
3. Click the Wireless Networks tab.
4. Select the desired network from the list. If the desired network is not available and you would like to add it, click Add, and enter requested information (including the ESSID in the SSID field).

5. Click Properties.
6. The next steps depend upon the selections that you make on this screen. For further information on security options, see Chapter 3, “Configuring Wireless Settings.”

**WEP Security:**

a. Select Open under Network Authentication, and select WEP for data encryption.

b. Enter and confirm the WEP key or select the WEP Enabled checkbox, or indicate if the key is provided automatically in your network.

c. Click OK as needed to close the Properties windows.

**WPA-PSK Security:**

a. Select WPA-PSK under Network Authentication.

b. Select AES or TKIP for data encryption.

c. Enter the WPA pre-shared key.
d. Click OK as needed to close the Properties windows.

WPA-1x Security:
a. Select WPA under Network Authentication.
b. Select AES or TKIP for data encryption.
c. Select the Authentication tab.

d. Confirm that the EAP type is “Smart Card or other Certificate.”
e. Confirm that the checkbox entitled “Authenticate as computer when computer information is available” is selected.
f. Click **Properties** to open the Certificate Properties box.

![Certificate Properties dialog box]

- **g.** Confirm that “Use a certificate on this computer” is selected along with “Use simple certificate selection.”
- **h.** Select the checkbox entitled “Validate server certificate.”
- **i.** Select the checkbox “Connect to these servers” and enter the IP address of your RADIUS authentication server.
- **j.** Select the certificate authority or authorities approved for your network. The list should include the certificate authority used for your RADIUS server.
- **k.** Select the checkbox entitled “User a different user name for the connection.”
- **l.** Click **OK** as needed to close the Properties windows.

**Configure a Windows NT or 2000 PC client**

1. From the **Start** button select **Settings → Network and Dial-Up Connections**.
2. Right-click the **Local Area Connections** icon and select **Properties**.
3. Select **Client for Microsoft Networks** and click **Configure**.
4. Click the **Advanced** tab.
5. Select **SSID** from the list on the left, and enter the **ESSID** for your network in the space provided.
6. Click **OK**.
7. Click the **Wireless LAN Configuration Utility** icon in the system tray at the bottom of your screen.

8. Click the **Configuration** tab.

9. Select **Infrastructure** from the Mode list.

10. Select the **SSID** pull-down menu.

11. Click the **Encryption** tab.

12. Select the **WEP** option that matches your network (enabled or disabled). If you select one of the WEP options, enter the key for your network.

13. Click **OK**.

Once you have configured the settings on a client device, the device requests an IP address from the wireless network. The client then receives IP address, default route assignment and DNS settings from a DHCP server which may be on the wired network or on an Tropos gateway within your wireless network.

### Reassigning Gateways and Nodes

Gateway is the factory default setting for the Tropos router; however, you can change a gateway to a node or a node to a gateway.

**Change the gateway or node setting**

1. Open the Configuration Utility.

2. Click **Device & IP** on the side menu.

3. Select **Gateway** or **Node** from the Router Setting pull-down menu.

4. Click **Store Changes**, and then select **Commit Changes** on the side menu to implement the change. Enter a time delay, if desired, and click **Commit Changes**. After you commit the changes, they are displayed in the Committed columns on the screens.

The new setting is indicated at the top of the Configuration Utility screen (see Figure 5 on page 13).

**Note**

The Tropos gateway reverts to node operation automatically if it loses connection to the Ethernet network. The label at the top of the Configuration Utility screen does not change, however, and the router reverts back to gateway operation as soon as network connectivity is re-established.
Confirming Router Identity

Use the Router Identity screen, shown in Figure 6, to record information about the name and location of the Tropos router.

**Figure 6 Router Identity Screen**

<table>
<thead>
<tr>
<th>Cell Identity</th>
<th>Stored</th>
<th>Committed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cell Name</td>
<td>TroposCell</td>
<td>TroposCell</td>
</tr>
<tr>
<td>Cell Location</td>
<td>Sunnyvale</td>
<td>SanMateo</td>
</tr>
<tr>
<td>Cell Contact</td>
<td><a href="http://www.troposnetworks.com">www.troposnetworks.com</a></td>
<td><a href="http://www.troposnetworks.com">www.troposnetworks.com</a></td>
</tr>
<tr>
<td>Cell Latitude</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Cell Longitude</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Set the router identity**

1. Open the Configuration Utility.
2. Select Identity from the side menu.
3. Enter an alphanumeric name and location for the router.
4. Enter the name or email address of the contact person for issues relating to router operation.
5. Enter the longitude and latitude that represent the global position of the Tropos router. The fields are in the format xx.xxxxxxxx, with up to 8 digits permitted to the right of the decimal point.
6. Click Store Changes.
7. Select Commit Changes on the side menu to implement the changes.
Checking the Current Configuration

Check current configuration settings at any time by selecting **Current Config** from the side menu of the Configuration Utility (Figure 7). For detailed information about the information on this screen, refer to the *Tropos Networks Configuration Reference Guide*.

**Figure 7  Current Configuration Screen (Excerpt)**

```
<table>
<thead>
<tr>
<th>Interface</th>
<th>Setting</th>
<th>Status</th>
<th>PoE Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN (eth0)</td>
<td>10baseT-HD</td>
<td>no link</td>
<td>Disabled</td>
</tr>
<tr>
<td>Management (eth1)</td>
<td>10baseT-HD</td>
<td>no link</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
```
Accessing the Configuration Utility Through a Wireless Connection

It is not always convenient or possible to access the Tropos Configuration Utility using a direct cable connection to the Management port. To address this concern, Tropos routers support the ability to connect to the Configuration Utility using a wireless connection.

Access the Configuration Utility through a wireless connection

1. Configure a laptop computer to access the Tropos Configuration Utility according to the instructions in “Setting the Gateway Configuration” on page 9.

2. Associate the laptop to the Tropos router. To do so, turn off other routers within range or move the laptop close enough to associate to the router.

3. Open a Web browser.

4. In the URL window of the browser, enter the wireless management IP address of the Tropos router: https://192.168.166.166. This is the wireless address that is pre-configured on each Tropos router. Note that you must use https, not http.

5. You may receive a security alert about viewing pages over a secure connection. Click Yes to proceed.

6. You may receive an additional security alert. Note that the name of the security certificate, which is issued by Tropos Networks, may not match the name of the site. Click Yes to proceed.

Note
To avoid future security warnings, generate a security certificate according to the instructions in “Generating SSL Certificates” on page 124.

7. When the Enter Network Password dialog box appears, enter the username admin and password tropos.

8. Click OK to open the Configuration Utility.
Setting the Time

The Tropos router supports accurate time setting through connection to a Network Time Protocol (NTP) server. Use the Time screen (Figure 8) to configure connection to an NTP server, identify the time zone in which the router is operating, or set the time manually. If you use NTP, it is not necessary to set the time manually.

Figure 8 Time Screen

<table>
<thead>
<tr>
<th>Timezone</th>
<th>Stored</th>
<th>Committed</th>
</tr>
</thead>
<tbody>
<tr>
<td>US/Pacific</td>
<td></td>
<td>US/Pacific</td>
</tr>
<tr>
<td>Time Servers</td>
<td>66.243.43.21</td>
<td>66.243.43.21</td>
</tr>
</tbody>
</table>

1. Select **Time** from the side menu.
2. To use an NTP server for time synchronization:
   - Select the time zone from the Timezone pull-down list. The UTC option refers to Universal Time Coordinated, which is the same as Greenwich Mean Time.
   - Enter the IP address of an NTP server or servers in the Time Servers field. You must specify a server if NTP is used. You can enter multiple servers using comma-separated IP addresses.
   - Click **Store Changes**. When you have finished, click **Commit Changes** on the side menu.
3. To set the time manually, select from the pull-down lists at the bottom of the screen, and click **Set Time**.

**Note**
It is not necessary to commit your changes when setting the time manually; the time is applied immediately without commit. It is necessary to commit the changes when configuring time using an NTP server.
Note

Enabling NTP on a router after a DHCP lease has already been obtained may change the duration of the DHCP lease.
3 Configuring Wireless Settings

This chapter describes how to set the parameters that control radio frequency (RF) communications in the Tropos wireless network. It contains information on the following topics:

- Service Sets
- Transmission Rates and Channels
- Security
- Roaming
- Multiple ESSIDs
- Power Levels and Transmit Antenna Diversity
- Setting the Wireless Configuration
- Configuring Multiple ESSIDs

Service Sets

Each Tropos MetroMesh router, together with associated clients, forms a Basic Service Set (BSS), or 802.11 wireless communications unit. Multiple routers, such as those in a Tropos cluster, form an Extended Service Set (ESS), also known as an 802.11 wireless network. The alphanumeric Extended Service Set Identifier (ESSID) functions as a group identifier. By entering the same ESSID into every Tropos gateway, node, and client, you add all of the wireless devices into the same wireless network.

Each Tropos gateway is shipped with a default ESSID, which you should change to uniquely identify your own wireless network. Select an alphanumeric string (no spaces) that is unique to your organization and easy to remember.

By default, the ESSID is sent in the RF beacon of each wireless device in the network. It is possible to suppress the ESSID broadcast for the Tropos router, thereby excluding the ESSID from the packets the router transmits and making it more difficult for unauthorized devices to obtain the ESSID and detect the presence of the wireless network. In multiple ESSID configurations, you can suppress or permit broadcast of the identifier on a per-ESSID basis.
Transmission Rates and Channels

Tropos routers conform to the IEEE 802.11b and 802.11g specifications for wireless communications, which apply to the 2.4 GHz RF band. The data transmission rates that apply between client machines and the Tropos router and between Tropos routers are user-configurable. The supported data rates range up to 54Mbps.

The Router-Router Tx Rate parameter determines the data rate for communications between Tropos routers. The default setting is 5.5 Mbps. If path quality is excellent, it may be possible to increase the data rate to 11Mbps (for the Tropos 3110 and 5110 routers) or 54Mbps for the (Tropos 5210, 4210, and 3210 routers) without suffering loss of path quality. If router-to-router connections are subject to interference or router density is low, it may be necessary to lower the data rate setting to 1 or 2Mbps.

The wireless channels that clients use when associating to Tropos router are user-configurable. The most commonly used channels for 802.11b/g communications are 1, 6, and 11 because they operate in non-overlapping frequency bands.

If you have multiple wireless networks in the same vicinity, determine what channels the other networks are using, and configure your Tropos routers on a different channel. Make sure all of the wireless router on the same network are set to the same channel.

Automatic Channel Selection

Automatic channel selection is supported. If you choose auto, you can enter a set of channels from which the router chooses an operating channel. The following automatic channel rules apply for gateways, fixed nodes, and mobile nodes:

**Gateway:** When the gateway is booted, it cycles through the channel list to find the best channel for operation based upon noise measurements and radio signal interference. That channel is used for communications within the cluster. During operation, the gateway measures channel noise in 10 minute windows. The gateway continues to use the selected channel until one of the following occurs:

- The measurements indicate that noise exceeds a pre-set threshold. The gateway performs a channel cycle, measuring the noise on all the channels in the channel list in a 10 minute window. If a channel with lower average noise during that period is identified, then the gateway shifts to that channel.
- During the configured maintenance window, the gateway identifies a channel with better noise characteristics than the current channel. If so, the gateway shifts the cluster to that channel. The maintenance window last 1.5 hours, beginning at the configured time and day (default interval is 1 day).

**Fixed node:** Fixed nodes collect signal data every 10 minutes. The node changes channels if any of the following occur:

- If a channel with lower average noise is identified, then the gateway shifts to that channel.
- If the packet success probability (PSP) drops below a pre-set threshold, then the node performs a channel cycle to determine if another channel with better PSP characteristics is available. If a better channel is found, the node switches. This includes the case in which the current channel is no longer available because the gateway has switched to a different channel.

- If the gateway has selected a new operating channel during a maintenance window, then all nodes in the cluster are reconfigured to use that channel.

**Mobile node:** Upon boot-up, Tropos 4210 mobile nodes scan for the best available channel. During normal operations, a mobile node will scan for another channel if the following applies:

- If the packet success probability (PSP) drops below a pre-set threshold, then the node performs a channel cycle to determine if another channel with better PSP characteristics is available. If a better channel is found, the mobile node switches.

### Security

Tropos provides several options for securing client access and traffic in the wireless network and for securing control and management traffic between Tropos routers.

#### Client Security

The client authentication options available today reflect evolving technology and the need for continuing responses to attempts to compromise existing security solutions. The current generation solutions are part of the Wi-Fi Protected Access (WPA) standard, some of which is codified in the IEEE 802.1x standard for user authentication with a central authentication server. Adopted by the Wi-Fi Alliance in response to needs for improved security, the WPA solutions encompass the central authentication methods now included in 802.1x plus a method for decentralized authentication using pre-shared keys.

Previous generation security is based on the Wired Equivalence Privacy (WEP) standard. Although not as effective as the WPA solutions, WEP is still widely used.

#### 802.1x

The 802.1x approach relies on an external authentication server that verifies client identity by means of digital certificates. The most widely used authentication servers are based on the Remote Authentication Dial-In User Service (RADIUS) protocol, which allows the Tropos gateway to communicate with the authentication server to exchange certificate information. Authentication messages sent between the RADIUS server and Tropos routers are protected by means of Extensible Authentication Protocol with Transport Layer Security (EAP-TLS) and EAP with Tunneled Transport Layer Security (EAP-TTLS).
If a RADIUS authentication server is accessible to the Tropos network, you can implement 802.1x authentication and RADIUS accounting by configuring the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS Authentication Server</td>
<td>IP address of the RADIUS server</td>
</tr>
<tr>
<td>RADIUS Authentication Port</td>
<td>Server port number for authentication requests</td>
</tr>
<tr>
<td>RADIUS Authentication Secret</td>
<td>Pass code for authorization of authentication requested by the Tropos router</td>
</tr>
<tr>
<td>RADIUS Accounting Server</td>
<td>IP address of the RADIUS accounting server used to log client activity</td>
</tr>
<tr>
<td>RADIUS Accounting Port</td>
<td>Server port number for RADIUS accounting requests</td>
</tr>
<tr>
<td>RADIUS Accounting Secret</td>
<td>Passcode to verify the connection between the accounting server and the Tropos router</td>
</tr>
<tr>
<td>RADIUS Accounting Interval</td>
<td>Interval in seconds between RADIUS accounting updates</td>
</tr>
</tbody>
</table>

RADIUS accounting enables you to do the following:
- Limit the number of concurrent sessions for a user account.
- Examine client roaming patterns to better respond to client support requests.
- Track unauthorized usage by linking a MAC address to a client at a specific time with evidence of traffic usage.
- Enable for-fee client service based upon usage plans.
- Correlate client activities with network events to detect whether a client has poor compatibility or is sending destabilizing traffic.
- Detect client-to-client traffic that might indicate hacking attempts.
- Determine the nodes that experience the most traffic flow or the times of day that are the busiest.

**WPA with Pre-Shared Keys**

Organizations that do not have a centralized authentication server can still take advantage of strong WPA authentication security by using the WPA pre-shared key (PSK) option. In the WPA-PSK approach, each network device for which authentication is required is configured with the same password, or key. Clients access the network by presenting the password. As with RADIUS authentication, WPA-PSK uses EAP to send authentication messages.

WPA/802.1x and WPA-PSK are compatible with a variety of data encryption options. Tropos currently supports the Advanced Encryption Standard (AES) and Temporal Key Integrity Protocol (TKIP). The encryption method is determined by settings on the client station.
Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) is an earlier generation wireless authentication and encryption solution that is still widely used, especially in devices that are not equipped to support WPA/802.1x. WEP relies on security keys, which must be the same on all Tropos routers and all client devices. From a user perspective, the process of configuring WEP keys is similar to configuring WPA keys; however, the authentication algorithms are not as secure as the EAP algorithms.

The Tropos router supports two types of WEP keys

- 64-bit Key. This key length consists of 40 bits of data encryption plus a 24-bit initialization number generated randomly by the WEP encryption algorithm. Total key length is 64-bit.
- 128-bit Key. This key length consists of 104 bits of data encryption plus a 24-bit initialization number generated randomly by the WEP encryption algorithm. Total key length is 128-bit.

Example keys:

- 64-bit ASCII: AZY23
- 128-bit ASCII: 9843DTGKLH334
- 64-bit hexadecimal: 0A3C4D5F4B
- 128-bit hexadecimal: 987ADE78F4458DDB03489CA00F

After creating a key, you can use it to program all client devices and Tropos routers in the wireless network.

Client Security Options

In addition to the authentication options listed in this section, the Tropos router supports the option of forgoing authentication and encryption entirely and permitting clients to access the network with no protection for data traffic. This option provides no protection for clients and should not be selected if network security is of concern.

The Tropos 5210, 4210, and 3210 routers support Open, WEP, WPA-PSK, and WPA-1x security. For WPA-PSK and WPA-1x, the encryption method is determined by settings on the client machine. In networks with multiple ESSIDs, each ESSID can be configured to support a different authentication type.

The Tropos 3110 and 5110 routers support only WEP and Open security.

Router-to-Router Security

All control and management communication between Tropos routers is encrypted at Layer 3 using Advanced Encryption Standard (AES). In Tropos networks comprised of Tropos 3210 and 5210 routers, you can elect to add additional protection for router-to-router data and control traffic by enabling the AES Encrypt Forwarded Packets feature on the Wireless screen. The following guidelines apply to the AES Encrypt Forward Packet feature:
- The feature should be enabled in networks with 5210, 4210, and 3210 model routers that use WPA-1x or WPA-PSK security.
- If AES Encrypt Forwarded Packets is enabled, then all gateways and nodes in the cluster must have at least one SSID configured for WPA-PSK or WPA-1x.
- AES Encrypt Forwarded Packets should be disabled for Tropos 4210 mobile nodes and to assure communications in networks with a mix of 5210/4210/3210 and 5110/3110 router models. For the highest level of router-router security, assign the 5210/4210/3210 routers to a different wireless routing domain (WRD) than the 5110/3110 routers.
- If AES Encrypt Forwarded Packets is disabled, router-to-router communications use the security settings for the primary ESSID (as set on the Wireless screen).

### Beacon Rates

It is possible to change the rate at which 802.11 beacons are transmitted from the router and to change the interval between beacons. The default settings for beacon rate and beacon interval (11 Mbps and 250 ms) should work well in almost all situations; however, it may be desirable to change the rates to support some non-compliant client devices or network configurations. In large, highly connected networks in which each router has numerous neighbors, the overhead from 802.11 beacons could become significant. Increasing both the beacon interval and beacon rate may reduce the overhead without a significant impact on network performance.

### Roaming

Since clients operate at lower power than nodes, nodes may be able to detect a client even if the client cannot detect the node. Network initiated roaming detects clients that lose uplink to a node, and forces them to associate to another neighboring node. This feature is disabled by default, and should be used with care. Client systems function in different ways, and tuning may be required for network initiated roaming to operate effectively with multiple client platforms.

Client initiated roaming is automatically supported throughout the network wireless routing domain, which is identified by the Wireless Routing Domain ID.

### Multiple ESSIDs

The Tropos 5210, 4210, and 3210 routers can support multiple ESSIDs. When multiple ESSIDs are configured, the router accepts packets destined for any of configured ESSIDs and forwards them to the appropriate networks. Multiple ESSIDs are used in conjunction with virtual LANs (VLANs) to support multiple use networks. For further information, see “Configuring VLANs” on page 89.

Configured on the Wireless screen, the primary ESSID is the identifier that is advertised in the router’s beacon (“Setting the Wireless Configuration” on page 37). In addition to the primary
ESSID, it is possible to define up to 15 additional secondary ESSIDs. The Tropos router will accept and forward packets intended for those networks.

Configuring a secondary ESSID creates a virtual interface for the wlan0 radio interface. The interface is designated as wlan0sN, where N is the number of secondary interfaces that have been created. For example, wlan0s1 refers to the first secondary ESSID.

You can configure the authentication type on a per ESSID basis. The authentication type for the primary ESSID is set on the Wireless screen (“Setting the Wireless Configuration” on page 37), and the authentication types for secondary ESSIDs are set on the Multi-ESSID screen. See “Configuring Multiple ESSIDs” on page 39 for configuration instructions.

If an ESSID has authentication type as Open, then you cannot create another ESSID using WEP. The combination is not supported. Multiple ESSIDs using the same authentication type will also use the same encryption configuration. In order to choose WPA authentication, you must first enable AES packet forwarding on the Wireless screen (“Setting the Wireless Configuration” on page 37).

You can enable or disable ESSID suppression on a per-ESSID basis. If ESSID suppression is disabled, then the ESSID is included in the router’s beacon. If you enable suppression, then the ESSID is not sent in the beacon.

Note
In order for clients to see all non-suppressed ESSID from the Windows Wireless Zero Config (WZC) window, it is necessary to refresh the display once for each ESSID. Each time the screen is refreshed, another ESSID is added to the list. In addition, make sure that none of the ESSIDs is configured as a preferred network in WZC.

**Power Levels and Transmit Antenna Diversity**

To adjust the power output of the Tropos router radio, set the attenuation level for transmit power. Increasing the attenuation reduces the output power of the router; reducing the attenuation increases the output power. Available settings range from 0dB to 10dB in 1bB increments. When 0dB is selected, the router operates at full power; when 20dB is selected, the router operates at the lowest positive power setting.

You can also assign following antenna diversity settings:
- 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
Setting the Wireless Configuration

Use the Wireless Configuration screen (Figure 9) to change wireless parameters. For further information, refer to the Tropos Networks Configuration Reference Guide.

Figure 9 Wireless Configuration screen

<table>
<thead>
<tr>
<th>Wireless Configuration</th>
<th>Stored</th>
<th>Committed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary ESSID</td>
<td>rootTop</td>
<td>rootTop</td>
</tr>
<tr>
<td>ESSID Suppression</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Client Transmit Rate</td>
<td>auto</td>
<td>auto</td>
</tr>
<tr>
<td>Unit-Unit Tx Rate</td>
<td>24M</td>
<td>24M</td>
</tr>
<tr>
<td>Channel</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Transmit Power</td>
<td>0 dB</td>
<td>0 dB</td>
</tr>
<tr>
<td>Transmit Antenna</td>
<td>auto</td>
<td>auto</td>
</tr>
<tr>
<td>Allow 802.11b Clients</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Short Preamble</td>
<td>Short Preamble</td>
<td></td>
</tr>
<tr>
<td>Authentication Type</td>
<td>WEP</td>
<td>WEP</td>
</tr>
<tr>
<td>WEP Type</td>
<td>Hex64bit</td>
<td>Hex64bit</td>
</tr>
<tr>
<td>WEP Key</td>
<td>aabbccddee</td>
<td>aabbccddee</td>
</tr>
<tr>
<td>AES Encrypt Forwarded</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Beacon Interval</td>
<td>250ms</td>
<td>250ms</td>
</tr>
<tr>
<td>Beacon Rate</td>
<td>11Mbps</td>
<td>11Mbps</td>
</tr>
<tr>
<td>PSK Passphrase</td>
<td>8b6677bd</td>
<td>8b6677bd</td>
</tr>
<tr>
<td>RADIUS Authentication</td>
<td>172.20.125.2</td>
<td>172.20.125.2</td>
</tr>
<tr>
<td>Port</td>
<td>1812</td>
<td>1812</td>
</tr>
<tr>
<td>Secret</td>
<td>whatever</td>
<td>whatever</td>
</tr>
<tr>
<td>Accounting Server</td>
<td>172.20.125.2</td>
<td>172.20.125.2</td>
</tr>
<tr>
<td>Authentication Port</td>
<td>1813</td>
<td>1813</td>
</tr>
<tr>
<td>Secret</td>
<td>whatever</td>
<td>whatever</td>
</tr>
<tr>
<td>Accounting Interval</td>
<td>900</td>
<td>900</td>
</tr>
<tr>
<td>Network Initiated</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Wireless Routing Domain</td>
<td>8b667781d0c1b6677</td>
<td>8b667781d0c1b6677</td>
</tr>
</tbody>
</table>
### Change wireless configuration settings

1. Choose **Wireless** from the side menu to open the Wireless Configuration screen.

2. Enter or confirm the primary ESSID and indicate whether the ESSID will be suppressed in the router’s 802.11 beacon.

3. Select the transmission rates for client communications in the Client Transmit Rate field. The Automatic setting is acceptable for most networks.

4. Select the transmission rate for communications between Tropos routers in the Router-Router Tx Rate field.

5. Choose an operating channel, or choose **auto** and click **Store Changes** to use automatic channel selection.
   - If you choose **auto** and click **Store Changes**, the screen reopens to display the channel list fields. Enter up to six channels.
   - If the router is a gateway and you choose **auto**, the screen reopens to display the channel list fields and channel maintenance fields. Enter the hour, date, month, and year for the maintenance window, and also enter the interval at which the maintenance window repeats. For example, the default settings of 02:01:Oct:2005 for Channel Maintenance Time and 1 day for Channel Maintenance Repeat Every means that the maintenance window will occur every day at 2AM, beginning on October 1, 2005.

6. Select a non-zero value for transmit power attenuation if you need to control the power level for radio transmission. Increasing the attenuation reduces the power output of the router.

7. Select **Allow 802.11b Clients** if you need to support clients that conform to the 802.11b standard. If the network contains some older 802.11b devices, it may also be necessary to select the long preamble in the Ancient 802.11b Compatibility field. The short preamble is more efficient, but is not compatible with all older 802.11 devices. These settings must be consistent across all routers in the network.

8. Select an option for client authentication. The authentication fields you must configure depend upon the option that is chosen. You can select a single option or a mix of options that is compatible with multiple client configurations:

<table>
<thead>
<tr>
<th>Option</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
<td>No additional authentication settings are required.</td>
</tr>
<tr>
<td>WEP</td>
<td>Select <strong>WEP Type</strong> and enter <strong>WEP Key</strong>.</td>
</tr>
<tr>
<td>WPA-PSK</td>
<td>Enter <strong>PSK Passphrase</strong>, which must be 8-64 characters in length.</td>
</tr>
<tr>
<td>WPA-1X (EAP-TLS, EAP-TTLS, PEAP)</td>
<td>Enter <strong>RADIUS Address</strong>, <strong>RADIUS Authentication Port</strong>, and <strong>RADIUS Secret</strong>. See “802.1x” on page 32 for a description of these fields.</td>
</tr>
</tbody>
</table>

---

1. Security settings are not retained if the Tropos router software is rebooted to an older software release.
9. If WPA-1x is chosen and you want to use RADIUS accounting to log client activity, enter the IP address of the RADIUS accounting server, server port, secret (passcode), and the interval between accounting updates.

10. If needed, change the beacon rate and beacon interval.

11. Select whether to enable network initiated roaming.

12. Confirm the appropriate wireless routing domain ID for the network, which must be the same for all Tropos routers in the network.

13. Click **Store Changes**. To commit changes that you have stored, select **Commit Changes** from the side menu.

### Configuring Multiple ESSIDs

Use the Multi-ESSID screen (Figure 10) to configure secondary ESSIDs.

**Figure 10  Multi-ESSID Screen**

#### Multi-ESSID Configuration

<table>
<thead>
<tr>
<th>Secondary ESSID</th>
<th>Authentication</th>
<th>ESSID Suppression</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department1</td>
<td>Open</td>
<td>Disabled</td>
</tr>
<tr>
<td>Department2</td>
<td>WPA-1x</td>
<td>Disabled</td>
</tr>
<tr>
<td>Department3</td>
<td>Open</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**Committed List of Secondary ESSID for Multi-ESSID**

<table>
<thead>
<tr>
<th>ESSID</th>
<th>Interface</th>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department1</td>
<td>wlan0s1</td>
<td>Open</td>
</tr>
<tr>
<td>Department2</td>
<td>wlan0s2</td>
<td>WPA-1x</td>
</tr>
</tbody>
</table>

#### Add a secondary ESSID

1. Choose **Multi-ESSID** from the side menu to open the Multi-ESSID Configuration screen.
2. Enter a name for the secondary ESSID.
3. Choose an authentication type for the ESSID. Note the following restrictions:

   - Open and WEP authentication are not compatible. If you choose either type for an ESSID, you cannot choose the other type for any other ESSID.
In order to choose WPA-1X or WPA-PSK authentication, you must first enable AES packet forwarding on the Wireless screen. See “Security” on page 32.

4. Choose whether to enable ESSID suppression. If you choose Enabled, then that ESSID is not broadcast in the router beacon.

5. Click Add.

6. Continue adding interfaces as needed. If you attempt to add more than 15 interfaces, you receive an error message.

7. To commit changes, select Commit Changes from the side menu. Committed changes are listed in a table on the screen.
This chapter describes the configuration options available to implement a variety of wireless network topologies. It contains information on the following topics:

- Overview
- Configuring DHCP Settings
- Configuring Network Address Translation
- Configuring Dual Subnet Support
- Configuring Wired Ports
- Supporting Layer 2 Emulation
- Configuring Uplink Check
- Configuring Power Sourcing for Power Over Ethernet
- Configuring a Service Gateway

**Overview**

If you have followed the instructions in Chapter 2, “Getting Started,” a basic wireless network cluster is now configured, similar to the one illustrated in Figure 11.

Tropos supports numerous variations on this basic network topology. You can choose alternative approaches for providing IP address services and determine the area controlled by each Tropos gateway.

To choose the best network configuration, consider the following:

- **DHCP service** - You can provide DHCP service through an external DHCP server or through the on-board DHCP server available on the Tropos gateway. If the network has multiple Tropos gateways and you select the on-board DHCP server option, it is possible to configure back-up DHCP support. Use of the on-board DHCP server is recommended only for smaller networks. See “Configuring DHCP Settings” on page 43.

- **NAT service** - If the network is served by a single Tropos gateway, you can configure network address translation to provide a range of IP addresses for the internal network. See “Configuring Network Address Translation” on page 53.
• Dual subnet coverage - If the network contains two distinct subnets, you can serve both of them with a single Tropos gateway. Use an external DHCP server to provide address service, unless the network is small.¹ See “Configuring Dual Subnet Support” on page 55.

• Wired port configuration for downstream sub-interface - You can extend wired coverage in the area served by the Tropos wireless network by configuring the management port of the Tropos router to serve as the wired interface for an additional subnet or subnets. See “Configuring Dual Subnet Support” on page 55.

• Mobile nodes and wired clients - You can mount the Tropos 4210 mobile MetroMesh router in a moving vehicle to provide network access for a wired client located in the vehicle. The wired client is connected directly to the Tropos 4210 mobile node. See “Configuring Networks with Mobile Nodes” on page 52.

• Layer 2 emulation - Layer 2 emulation permits the router to presenting client and node MAC addresses (for example, for subscriber gateways) in order to interoperate with devices that require Layer 2 operation from the Tropos network. See “Supporting Layer 2 Emulation” on page 62.

• Uplink check - You can improve the robustness of the network by implementing a strategy for network re-clustering in the event that a gateway loses backhaul to the wired network. See “Configuring Uplink Check” on page 64.

• Multi-subnet roaming - You can permit client stations to retain links to the wireless network when they move from one Tropos router subnet to another. See “Supporting Multi-Subnet Roaming” on page 70.

• VLANs - VLANs enable organizations to selectively forward different types of network traffic that travel over the same physical network. See “Configuring VLANs” on page 89.

• Packet filtering - You can use packet filter forwarding rules to determine which IP packets are forwarded by the Tropos router and which are rejected. See “Defining Packet Filter Forwarding Rules” on page 83.

Note
The IP address 1.1.1.1 is reserved and should never be assigned for use on the Tropos router or SNMP trap assignment.

¹ The term dual subnet refers to two subnets that are served by a single Tropos gateway. The term multi-subnet or cross-subnet refers to a movement between subnets that are served by different Tropos gateways.
Configuring DHCP Settings

The Dynamic Host Configuration Protocol (DHCP) is a widely used method for assigning dynamic IP addresses within a network. Instead of entering IP addresses manually on each network device, network administrators can use a DHCP server to automatically assign IP addresses on a dynamic basis. If a device is moved or its configuration changes, the DHCP server automatically reassigns an address that does not conflict with existing or previously assigned addresses. DHCP leases determine the amount of time each address is valid before it is automatically reassigned.

Each Tropos router includes an optional on-board DHCP server that can be used to provide IP address service for clients if an external DHCP server is not available. In the basic wireless network configuration shown in Figure 11, the DHCP server feature of the Tropos gateway is disabled. The Tropos gateway obtains IP addresses for its own wired and wireless interfaces through an external DHCP server. The gateway also acts as a DHCP relay, forwarding DHCP requests and responses between client devices and the DHCP server.
If the on-board DHCP server is enabled, then the Tropos router must have static (non-DHCP) IP addresses assigned to its own wired and wireless interfaces.

You can use the on-board DHCP server to provide client address service in a single or multiple Tropos gateway configuration. In a multiple gateway network, you can configure DHCP servers to operate on one Tropos gateway or on all the Tropos gateways on the network. If you configure the DHCP server on more than one gateway, you must configure the server on all of them.

**Note**
The on-board DHCP server does not support DHCP service for wired clients attached to Tropos 4210 mobile routers. You must use an external DHCP server to provide service for those wired clients.
Configuring a Single DHCP server

In this configuration, a single Tropos gateway provides DHCP services for the entire network. All other Tropos gateways in the network relay DHCP address requests to that gateway. Figure 12 shows this configuration. In the figure, the server with wired IP address 192.168.101.151 is used as the DHCP server.

Figure 12 Example network with multiple Tropos gateways, one DHCP server

Note: Example DHCP addresses xx are in the range 100-200.
Configure a single on-board DHCP server

1. Open the Tropos Configuration Utility.
2. Click Device & IP on the side menu to open the Device and IP Configuration screen (Figure 13).

Figure 13 Device and IP Configuration Screen - Gateway

3. Select Static in the IP Configuration Method field. The DHCP selection for IP Configuration Method applies only when an external DHCP server is used.

4. Enable NAT if you want to freely assign addresses within the network. You can only use NAT if there is a single Tropos gateway in the network. See “Configuring Network Address Translation” on page 53.
5. Enter a static IP address and subnet mask for the wired interface. Each Tropos router configured with the on-board DHCP server must have a static IP address assigned to the wired interface.

6. Assign a default gateway, wireless interface, and wireless netmask.

7. Enter a static IP address and subnet mask for the wireless interface. Each Tropos router configured with the on-board DHCP server must have a static IP address assigned for the wireless interface.

8. Click **Store Changes**.

9. Open the DHCP Server screen. The contents of this screen differ according to whether NAT is disabled (Figure 14) or enabled (Figure 15) on the Device and IP Settings screen. To configure the DHCP server, the configuration method field must be set to Static or NAT must be enabled, or both.

**Figure 14  DHCP Server Screen, NAT Disabled**

### DHCP Server Configuration

<table>
<thead>
<tr>
<th></th>
<th>Stored</th>
<th>Committed</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Server On Board</td>
<td>Enable</td>
<td>Enabled</td>
</tr>
<tr>
<td>DHCP Relay</td>
<td>Enable</td>
<td>Disabled</td>
</tr>
<tr>
<td>DHCP Relay To</td>
<td>192 168 101 1</td>
<td>192.168.101.1</td>
</tr>
</tbody>
</table>

Please specify an IP address range large enough to accommodate both the Tropos units and users on the wireless network:

<table>
<thead>
<tr>
<th></th>
<th>Stored</th>
<th>Committed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting Address</td>
<td>192 168 101 100</td>
<td>192.160.101.100</td>
</tr>
<tr>
<td>Ending Address</td>
<td>192 168 101 200</td>
<td>192.160.101.200</td>
</tr>
<tr>
<td>Netmask</td>
<td>255 255 255 0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Domain Name Server 1</td>
<td>0 0 0 0</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Domain Name Server 2</td>
<td>0 0 0 0</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Domain Name Server 3</td>
<td>0 0 0 0</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Lease Duration (Seconds)</td>
<td>86400</td>
<td>86400</td>
</tr>
<tr>
<td>WINS Servers</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Store Changes**
Figure 15 DHCP Server Screen, NAT Enabled

DHCP Server Configuration

NAT is enabled

DHCP Server is automatically enabled.

Please specify an IP address range large enough to accommodate both the Tropos units and users on the wireless network.

<table>
<thead>
<tr>
<th></th>
<th>Stored</th>
<th>Committed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting Address</td>
<td>192.168.101.100</td>
<td>192.168.101.100</td>
</tr>
<tr>
<td>Ending Address</td>
<td>192.168.101.200</td>
<td>192.168.101.200</td>
</tr>
<tr>
<td>Netmask</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Domain Name Server 1</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Domain Name Server 2</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Domain Name Server 3</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Lease Duration (Seconds)</td>
<td>86400</td>
<td>86400</td>
</tr>
<tr>
<td>WINS Servers</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
10. For DHCP Server on Board, select **Enable**.

11. Enter information for the following fields:
   - Starting Address—The first IP address in the address range for the Tropos gateway DHCP server.
   - Ending Address—The last IP address in the address range for the Tropos gateway DHCP server.
   - Netmask—The subnet mask for this Tropos gateway DHCP server.
   - Broadcast Address—The broadcast address for your network.
   - Domain Name Servers—The IP addresses of up to three DNS servers on your network.
   - Lease Duration—The time in seconds you want before the IP address expires and it needs to be renewed. Lease times of at least 12 hours (43200 seconds) are recommended.
   - WINS Server—The IP information for the Windows Name Server used for Windows clients.

12. Click **Store Changes**. When you have finished, click **Commit Changes** on the side menu.
**Configuring Multiple Redundant DHCP servers**

Since valid IP addressing is essential to network operations, it can be helpful to set up redundant DHCP servers, thereby enabling network service to continue uninterrupted in the event of service loss to an individual Tropos gateway. To provide redundant DHCP service, configure all the Tropos gateways in the network as DHCP servers, making sure that the DHCP server address pools for the multiple gateways are non-overlapping and that each is large enough to service any areas that might be affected by DHCP server outages. Figure 16 shows an example configuration with address ranges that are sufficient to provide redundant DHCP coverage.

**Figure 16 Example network, multiple Tropos gateways, redundant DHCP servers**

---

Example DHCP addresses xx are in the range 1-50.
Example DHCP addresses yy are in the range 101-150.
**Configure multiple, redundant DHCP servers**

Perform the following steps for each Tropos gateway.

1. Open the Tropos Configuration Utility.

2. Click **Device & IP** on the side menu to open the Device and IP Configuration screen (Figure 13).

3. Select **Static** as the configuration method. The DHCP method applies only when an external DHCP server is used.

4. Enable NAT if you want to freely assign addresses within the network and the network has a single Tropos gateway that represents all internal clients to the external network. When you enable NAT, the internal DHCP server of the Tropos gateway is automatically enabled. For more information on NAT requirements, see “Configuring Network Address Translation” on page 53.

5. Enter a static IP address and subnet mask for the wired interface. Each Tropos router configured with the on-board DHCP server must have a static IP address assigned for the wired interface.

6. Assign a default gateway, wireless interface, and wireless netmask.

7. Enter a static IP address and subnet mask for the wireless interface. Each Tropos router configured with the on-board DHCP server must have a static IP address assigned for the wireless interface.

8. Click **Store Changes**.

9. Click **DHCP** on the side menu to open the DHCP Server screen (Figure 14). The contents of this screen differ according to whether NAT has been enabled or disabled on the Device and IP Settings screen.

10. Under DHCP Server on Board, select the checkbox entitled **Enable**.

11. Enter address information. Make sure that the address ranges do not overlap with those for the other gateways, and that the address range determined by the starting and ending addresses is large enough to cover the addresses that would be lost in the event of service interruption from another gateway:

   - **Starting Address**—The first IP address in the address range for the Tropos gateway DHCP server
   - **Ending Address**—The last IP address in the address range for the Tropos gateway DHCP server
   - **Netmask**—The subnet mask for this Tropos gateway DHCP server
   - **Broadcast Address**—The broadcast address for your network.
   - **Domain Name Servers**—The IP addresses of up to three DNS servers on your network
   - **Lease Duration**—The time in seconds you want before the IP address expires and it needs to be renewed. Lease times of at least 12 hours (43200 seconds) are recommended.
   - **WINS Server**—The IP information for the Windows Name Server used for Windows clients.

12. Click **Store Changes**. When you have finished, click **Commit Changes** on the side menu.
Relaying DHCP Requests to an External Server

If an external DHCP server is available on the network, you can disable the DHCP server on the Tropos gateway and relay all client DHCP requests to the external server.

**Bypass the Tropos gateway DHCP server**

1. Open the Tropos Configuration Utility.
2. Open the Device & IP screen (Figure 13) and confirm that the configuration method is set to Static. If not, change the value to Static and store and commit the changes.
3. Open the DHCP Server screen (Figure 14).
4. Under DHCP Relay, select Enable, if the DHCP server is not already listed as enabled.
5. To the right of the DHCP Relay to box, enter the IP address of the DHCP server to receive DHCP relay requests. For the relay process to work, the entered IP address must be for a functioning DHCP server that properly supports DHCP relay requests.
6. Click Store Changes. When you have finished, click Commit Changes on the side menu.

Configuring Networks with Mobile Nodes

The Tropos 4210 mobile MetroMesh router supports attachment of a wired client to the eth1 port of the router. As shown in Figure 17, the client connects directly to the mobile node for network access. The mobile node establishes backhaul connection through a fixed node and upstream to the gateway.

The following rules apply when configuring a wired client for the Tropos 4210:

- The eth0 port is reserved for the management configuration interface.
- The mobile node can have an IP address assigned statically or using DHCP
- The eth1 interface is reserved for a wired client. You can assign an IP address statically or using DHCP. If DHCP is used, the address service must be through an external DHCP server, not the DHCP server on the mobile node. For instructions on configuring these interfaces, see “Configuring DHCP Settings” on page 43.

<<Do we need more instructions here?>>
Configuring Network Address Translation

Network Address Translation (NAT) permits network administrators to create a set of internal IP addresses for intra-organization use, while still maintaining public addresses for Internet communications. The NAT protocol alters outgoing network packets to insert a valid Internet return address. Upon return, NAT modifies the incoming packets, directing them to the correct internal address. NAT greatly extends the pool of available addresses and can preserve the privacy of internal addresses.

Tropos supports Network Address Translation (NAT) in the case where the wireless network has a Tropos gateway, as shown in Figure 18. Using NAT, a single gateway can support numerous Tropos nodes; the practical maximum is limited by throughput considerations. Enabling NAT creates an available address range throughout the wireless cluster.

**Note**
NAT is not supported with multiple Tropos gateways or with the Layer 2 emulation feature.
Figure 18  Example NAT configuration with a single Tropos gateway

When you enable NAT, the DHCP server on the single Tropos gateway is automatically enabled, and DHCP is used to assign the NAT addresses. There are two options available for assigning IP addresses to the wired and wireless interfaces of the Tropos gateway itself:

- **Static configuration method:** You assign static (non-DHCP) IP addresses to the wired and wireless interfaces of the Tropos gateway.
- **DHCP configuration method:** The IP address for the wired Tropos gateway interface is obtained from an external DHCP server (not the on-board DHCP server used to assign NAT addresses). The IP address for the wireless Tropos gateway interface is the first address of the internal NAT pool. Do not reserve the first address in the DHCP pool for any other devices.

**Enable NAT with static configuration method**

1. Open the Tropos Configuration Utility.
2. Open the **Device & IP** screen (Figure 13).
3. Select **Static** as the configuration method. The DHCP method applies only when an external DHCP server is used.
4. Select **NAT enabled**.
5. Click **Store Changes**. Make sure to commit the changes when you have finished.
Enable NAT with dynamic configuration method
1. Open the Device and IP Configuration screen.
2. Select **DHCP** as the configuration method. The DHCP method applies only when an external DHCP server is used.
3. Select **NAT enabled**.
4. Click **Store Changes**. When you have finished, click **Commit Changes** on the side menu.

### Configuring Dual Subnet Support

The dual subnet feature permits a gateway’s wired segment to be on one subnet while the wireless cluster is on another subnet. This approach offers network administrators the flexibility to manage the wireless network as distinct from the wired network. You can configure multiple gateways in this way provided that the upstream router is able to route traffic to the wireless subnet using next hop routes or supernetting principles. See Figure 19 for an illustration of a dual subnet configuration.

You must assign static IP addresses to the gateway’s wired and wireless interfaces, with each interface in a separate subnet. You can use the on-board DHCP server or DHCP relay. NAT must be disabled.

**Figure 19 Example network in dual subnet mode with a Tropos gateway running a DHCP server**

Note: Example DHCP addresses xx are in the range 1-150.
**Dual Subnets and DHCP Relay**

The DHCP relay feature allows DHCP requests to be sent to a DHCP server anywhere on the network, including those located in different subnets. Together with the dual subnet feature, DHCP relay enables the network to obtain DHCP addresses from an external DHCP server that has multiple address pools for different subnets. As shown in **Figure 20**, the client in the 192.168.3.0 subnet can obtain DHCP addresses for that subnet from the server in the 192.168.101.0 subnet.

**Figure 20**  Example network in dual subnet mode with DHCP relay

**Provide dual subnet support**

1. Open the Tropos Configuration Utility.
2. Open the **Device & IP** screen (Figure 13)
3. Select **Static** as the configuration method.
4. For the wired interface, enter a static IP address and subnet mask in the existing wired subnet.
5. For the wireless interface, enter a static IP address and subnet mask in the subnet intended for wireless coverage.
6. Enter other settings on the screen as needed.
7. Click **Store Changes**.
8. Open the DHCP Server screen. Select whether to enable the on-board DHCP server or to relay DHCP requests to an external server.
9. Click **Store Changes**. When you have finished, click **Commit Changes** on the side menu.
Configuring Wired Ports

Each Tropos router has two wired Ethernet ports:

- On the fixed Tropos routers (5210, 5110, 3210, and 3110), the LAN port is used for backhaul to the wired network, and the Management port is used as the wired interface to the Tropos Configuration Utility. You can also use the Management port to extend network coverage by creating a downstream sub-interface.
- On the Tropos 4210 mobile router, the CPE port is used to connect a wired client to the router. This is the recommended option for a client located in the same vehicle as the router. The Management port is used as the wired interface to the Tropos Configuration Utility.

Ethernet Speed and Duplex

The transmission and duplex rates for the Ethernet ports are user-configurable on the Device & IP Configuration screen.

- For fixed routers, eth0 refers to the wired LAN port, and eth1 refers to the Management port.
- For the 4210 mobile router, eth0 refers to the Management port, and eth1 refers to the Customer Premise Equipment (CPE) port reserved for the wired client.

Table 4 shows the available values for each.

<<I need to see the Configurator for a 4210 to check how this is listed.>>

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Current Configuration screen shows the assigned and operating values for eth0 and eth1. If you select Auto for either of these and the operating rate shown on the Current Configuration screen does not include a duplex value, that indicates that the Tropos Gateway and Node is connected to a repeater.</td>
</tr>
</tbody>
</table>

Table 4  Available values for eth0 and eth1

<table>
<thead>
<tr>
<th>Value</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto</td>
<td>Rate automatically negotiated with neighboring units</td>
</tr>
<tr>
<td>100base Tx-FD</td>
<td>100 Mbit transmission, full-duplex setting</td>
</tr>
<tr>
<td>100base Tx-HD</td>
<td>100 Mbit transmission, half-duplex setting</td>
</tr>
<tr>
<td>10base T-FD</td>
<td>10 Mbit transmission, full-duplex setting</td>
</tr>
<tr>
<td>10base T-HD</td>
<td>10 Mbit transmission, half-duplex setting</td>
</tr>
</tbody>
</table>
Wired Interface (MTU)

Maximum Transmission Unit (MTU) refers to the largest packet size in bytes transmitted over the network. It is recommended that you retain the default value of 1500 specified on the Device and IP Settings screen.

Modify the Ethernet Speed and Duplex or MTU settings

1. Open the Tropos Configuration Utility.
2. Open the Device and IP Settings screen (Figure 13).
3. Select the desired speed and duplex setting from the pull-down list for LAN (eth0). Refer to Table 4 for the available options.
4. Confirm the desired MTU.
5. Click Store Changes. When you have finished, click Commit Changes on the side menu.

Downstream Sub-Interface

To extend wired network coverage from the Tropos wireless network infrastructure, you can configure the management port of the Tropos router to serve as the wired interface for an additional subnet or subnets. Each management port on a Tropos gateway or node can support downstream sub-interfaces, or virtual interfaces, that extend the network downstream from the gateway or node.

Figure 21 shows an example network with downstream sub-interfaces. One of the Tropos gateways is configured with a single downstream sub-interface supporting a single wired subnet, and one of the Tropos nodes is configured with two downstream sub-interfaces supporting two wired subnets.
The following restrictions apply to downstream sub-interfaces:

- The on-board DHCP server is not supported. DHCP requests must be relayed to an external DHCP server.
- Multiple subnets are allowed, but only one subnet per router is addressable through DHCP; the others must be statically assigned.
- NAT is not supported.
- Layer 2 emulation is not supported.

**Add a downstream interface**

1. Set up a physical Ethernet network extending from the eth1 interface port on the Tropos node.
2. Open the Tropos Configuration Utility.
3. Click **Sub-interface** on the side menu to open the Management Port Sub-Interface Configuration screen.
4. Enter the IP address and the netmask for the sub-interface.

5. To reserve the entered route for DHCP addressing, select the checkbox entitled DHCP Available. If you are configuring multiple subnets from a single Tropos node, only one subnet can use DHCP service; all others must be assigned static IP addresses.

6. Click Add.

   The new route appears in the list of routes at the bottom of the screen. If this subnet is served by DHCP, then it appears in bold.

7. Add additional routes as desired. If you add a new route for DHCP, the new assignment replaces the previous assignment.

8. When you have finished, click Commit Changes on the side menu.

9. Configure clients on the subnet to use the static IP address you entered in the Downstream Sub-Interface screen as their default gateway.

   The sub-interface is now ready to route data from clients on the downstream subnets through the wireless network to the Tropos gateway.

**Delete a downstream interface**

1. Open the Tropos Configuration Utility.

2. Click Sub-Interface on the side menu.

3. Click the Delete button to the right of the route.

4. When you have finished, click Commit Changes on the side menu.
Re-Clustering Issues

In subnets with multiple Tropos gateways, routing issues can arise when a Tropos node with a working downstream sub-interface attempts to associate to a different cluster in response to changing signal conditions. In some circumstances, addresses for the downstream clients may not be available for routing in the new cluster.

You can ensure proper rerouting in the event of re-clustering by assigning client addresses from the first six available IP addresses for each downstream subnet. For example, if you create a downstream sub-interface with address 192.168.2.0 (subnetmask 255.255.255.0), assign clients on the subnet the IP addresses 192.168.2.1 through 192.168.2.6. If you create a downstream sub-interface with address 192.168.2.64 (subnetmask 255.255.255.192), assign clients on the subnet the IP addresses 192.168.2.65 through 192.168.2.70. These address ranges are dynamically routed when adaptive re-clustering occurs.
Figure 23 illustrates a downstream sub-interface configuration with the downstream IP addresses assigned to enable re-clustering.

**Figure 23  Example downstream sub-interface with re-clustering**

---

**Supporting Layer 2 Emulation**

Layer 2 emulation permits the network to inter-operate with devices that expect Layer 2 operation from the Tropos network, by presenting client and node MAC addresses. In Layer 2 emulation mode, the Tropos wireless network appears as a wireless bridge or access point to Layer 2 devices on the wired side. Network routing functionality still comes from the Tropos routers; however, they appear as Layer 2 devices to the rest of the network. The default setting for Layer 2 emulation is Disabled.

The following notes apply to Layer 2 emulation:

- Configure Layer 2 emulation when first deploying the network. If Layer 2 emulation is turned on or off in a working network, it may be necessary to reboot the entire network.
- You can use Layer 2 emulation in conjunction with a captive portal that supports MAC address authentication.
Layer 2 emulation is not supported if the configuration method is static for all the Tropos nodes on the network, or if NAT is enabled.

- Statically addressed routers are not reachable when Layer2 is enabled. ARP resolutions for their IP addresses are not answered, and the routers become unreachable from the upstream direction. Wireless clients are not affected by this and may be assigned static addresses.

**Note**
The Tropos 4210 Mobile MetroMesh router does not support Layer 2 emulation for wired clients.

Figure 24 shows an example network with a Layer 2 device upstream (wired side) from the Tropos gateway.

**Figure 24  Example network with Layer 2 Emulation**

---

**Enable Layer 2 emulation**

1. Open the Device and IP screen (Figure 13).
2. Select **Enable** from the Layer 2 emulation pull-down list.
3. Click **Store Changes**. When you have finished, click **Commit Changes** on the side menu.
Chapter 4 • Configuring Network Settings

Configuring Uplink Check

To minimize loss of connectivity, the Tropos gateway automatically switches to node operation if it loses physical connectivity to the wired network. When the wired connection is restored, the router automatically reverts back to gateway operation.

To enhance this default automatic capability, Tropos provides an Uplink Check feature. When this feature is enabled on the Tropos gateway, the gateway checks every 5 seconds to determine whether it can connect to a designated uplink check server or servers. It also checks for IP connectivity to other key network equipment such as the upstream network router or external DHCP server. If unsuccessful after a user-specified number of attempts, the gateway shifts to node operation. Traffic is routed to another Tropos gateway, if available, or association is denied to clients if another gateway is not available. When the user-configured bring-up conditions are met and the Tropos gateway is able to reestablish the link to the wired network, it automatically reverts back to gateway operation and permits clients to re-associate.

The uplink check feature causes the Tropos gateway to respond in the following ways:

- Switch to node operation, under the following conditions:
  - Physical connectivity is lost.
  - The Tropos gateway cannot communicate with the uplink server.

- Disassociate clients and prevent new clients from associating, under the following conditions:
  - The Tropos gateway has shifted to node operation, but is unable to communicate with another upstream node or gateway.
  - The router has lost its IP address and is unable to obtain another.

Note

Uplink check is intended for situations in which one or a few of the network gateways lose IP uplink connectivity. If all gateways lose uplink, then when uplink is restored, you must renew all DHCP leases by either rebooting all the Tropos routers using the System Reboot option in the Configuration Utility or by recycling the power on all the routers. See “Restarting the Tropos Router” on page 113.

Use the Device and IP Settings screen to configure uplink check parameters for the Tropos gateway. Uplink check does not apply if the Tropos router is configured for node operation.

Set the Uplink Check server configuration

1. Open the Tropos Configuration Utility.
2. Open the Device and IP Settings screen (Figure 13).
3. In the Uplink Check field, select Enabled.
4. In the Uplink Check Take Down Threshold field, enter the number of attempts to send packets to the designated server or servers, with one packet sent at each 5-second interval. If the number of consecutive unsuccessful attempts reaches the take down threshold for all of the Uplink Check servers, the gateway automatically switches to node operation and seeks another gateway for access to the wired network.
5. In the Uplink Check Bring Up Threshold field, enter the number of attempts to send packets to the designated server or servers, with one packet sent at each 5-second interval. If the number of consecutive successful attempts reaches the bring up threshold for any of the Uplink Check servers, the router automatically switches back to gateway mode.

6. In the Uplink Check Servers field, enter the IP addresses of the servers to check for connectivity (or up to three addresses, comma-separated).

7. Click **Store Changes**. When you have finished, click **Commit Changes** on the side menu.

---

**Note**
You can tell by visual inspection whether each Tropos router is functioning. For the Tropos 3210 and 3110 routers, the link is functioning if the red LED is blinking. For the Tropos 5210 and 5110 routers, the link is functioning if the light is green.

---

**Configuring Power Sourcing for Power Over Ethernet**

You can configure the Tropos 3210 and 5210 routers to source DC power on the Ethernet connector pins 4, 5, and 7, 8. This capability allows the router to power remote peripherals such as backhaul point-to-point radios, video cameras, or fiber optic transceivers.

---

**Note**
PoE power sourcing supported only on the Tropos 5210 and 3210 routers.

---

**Note**
The Tropos PoE power sourcing capability is not compliant with the IEEE 802.3af standard; however, many IEEE 802.3af-compliant power devices (PDs) will operate using the power sourcing equipment capabilities of the Tropos 3210 and 5210 routers.

---

The router can supply up to a total of 14W of DC power distributed to the LAN port, Management port, or both. You must configure each port for the same voltage: 12Vdc, 24Vdc, or Off state (0Vdc). **Table 5** lists the maximum power output as a function of voltage.

**Table 5 PoE Power Sourcing Power Output**

<table>
<thead>
<tr>
<th>Voltage</th>
<th>Max Power Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>12Vdc</td>
<td>14W</td>
</tr>
<tr>
<td>24Vdc</td>
<td>12W</td>
</tr>
<tr>
<td>48Vdc</td>
<td>10W</td>
</tr>
</tbody>
</table>
Configure PoE power output settings
1. Open the Tropos Configuration Utility.
2. Open the Device and IP Settings screen (Figure 13 on page 46).
3. Select whether to enable or disabled the PoE capability on the LAN port (eth0) and the Management port (eth1).
4. In the Load for PoE field, select the voltage for the ports based on the maximum desired power output, as shown in Table 5.
5. Click Store Changes. When you have finished, click Commit Changes on the side menu.

Configuring a Service Gateway

You can configure connection to a service gateway that provides authentication, authorization and accounting (AAA) and other network services such as DHCP, NTP, and Tropos Control EMS.

A service gateway may be one or more Layer 3 hops away from the Tropos gateway. To ensure adequate security for communications between the Tropos gateway and the service gateway, it is necessary to set up a secure tunnel through which DHCP, RADIUS, and management messages can travel. The Generic Routing Encapsulation GRE protocol is used to create the point-to-point link between the Tropos gateway and aggregating router, which is responsible for forwarding the traffic on to the service gateway. The Border Gateway Protocol (BGP) provides the routing mechanism for same-subnet roaming.

A service gateway is local if it is in the same subnet as the Tropos gateway and remote if it is at least one Layer 3 hop away from the Tropos gateway.

Figure 25 shows a Tropos Network with aggregating router and service gateway. The aggregating router operates as a BGP peer for the Tropos router through the GRE tunnel.
Figure 25  Service Gateway Configuration
Configure connection to a service gateway

1. Open the Tropos Configuration Utility.
2. Open the Service Gateway screen (Figure 26).
3. Select Enable to activate the service gateway feature.
4. Enter the IP address of the physical interface of the aggregating router in the Aggregating Router Address field.

5. Select Enable in the BGP Protocol Status fields to activate BGP. BGP is needed to support same-subnet client roaming.

6. Enter the IP address of the loopback interface of the aggregating router in the BGP Peer Address field.

7. Enter the Autonomous System (AS) number of the Tropos gateway in the Remote AS Number field.

8. Enter the AS number of the aggregating router in the Remote AS Number field.

9. Indicate whether traffic forwarding is local or remote by default.

10. Select the Remote or Local checkbox for the server, if you want to change the traffic forwarding rule for a specific server.

11. Enter IP addresses (comma-separated) in the space provided, if you want to change the traffic forwarding rule for traffic destined for other IP addresses.

12. Click Store Changes. When you have finished, click Commit Changes on the side menu.
This chapter describes the configuration options available to provide services to network clients and preserve network security. It contains information on the following topics:

- Supporting Multi-Subnet Roaming
- Configuring DHCP MAC Address Filters and Address Reservations
- Client Access
- Supporting Static IP Clients
- Defining Packet Filter Forwarding Rules
- Configuring VLANs
- Configuring Quality of Service
- Configuring Rate Limits

**Supporting 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 Tropos router subnet to another. Clients associated to a Tropos gateway can automatically roam to neighboring clusters, provided that the following conditions are met:

- For each gateway, the Multi-Subnet Roaming Configuration screen lists all the other gateways in the roaming domain, except those in the same subnetwork as the gateway to which the configuration is being applied.
- The Wireless Routing Domain ID is the same for all networks in the roaming domain.
- If VLANs are configured with the wired client DHCP relay option selected, then subnet and subnet mask information is configured for all the VLANs defined on the gateway. For further information, see “Multi-Subnet Roaming with VLANs” on page 93.
- The IP address of the wired client for each Tropos 4210 router is added to the Multi-Subnet Roaming screen. A wired client attached to mobile nodes could have an address that is in a different subnet from the wireless interface on the mobile node. If the mobile node moves to a different cluster, the address information for the wired client is lost unless the IP address is added to the Multi-Subnet Roaming screen.

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.

Use the Multi-Subnet Roaming Configuration screen (Figure 27) to identify the list of gateways available for client roaming and to identify redundant gateways. For instructions on setting the Wireless Routing Domain ID, see Chapter 3, “Configuring Wireless Settings.”

**Figure 27 Multi-Subnet Roaming Configuration screen**

![Multi-Subnet Roaming Configuration screen](image)

### Add gateways for multi-subnet roaming

1. Open the Tropos Configuration Utility.
2. Click **Gateway List** on the side menu to open the Multi-Subnet Roaming screen.
3. Enter the IP address and subnet mask of the wireless interface for a Tropos gateway that you want to make available for roaming.
4. Click **Add**.
   
   The gateway is displayed in the list below the address entry area. Repeat for all other gateways in the wireless routing domain.
If VLANs are configured on the wired interfaces for any of the gateways added to this screen, follow these additional steps in the Add Vlan Roaming Routes to Gateway List area:

a. For each gateway in the gateway IP address list at the top of the screen, enter the subnet and subnet mask for each VLAN interface defined on the gateway.

b. Click Add after entering each gateway IP, subnet, and subnet mask.

If wired clients are configured on any mobile nodes, follow these additional steps in the Add Wired Client area:

a. For each gateway in the gateway IP address list at the top of the screen, enter the subnet and subnet mask for each wired client defined on the gateway.

b. Click Add after entering each gateway IP, subnet, and subnet mask.

5. When you have finished, click Commit Changes on the side menu.

**Note**
The gateway list for the home gateway must include all other remote gateways in the wireless routing domain, and each remote gateway must include the home gateway in its gateway list.

**Delete a gateway from the list**

1. Select the gateway, and click Delete. Repeat for remote gateways.

2. When you have finished, click Commit Changes on the side menu.
Multi-Subnet Roaming Example:

Consider an example network with two subnets (Figure 28). The first, 192.168.1.0/24, has two gateways with wireless IP addresses 192.168.1.1 and 192.168.1.2. The second subnet, 192.168.2.0/24, has one gateway with wireless IP address 192.168.2.1. To configure multi-subnet roaming between the two subnets, each of the three gateways must be able to reach each other over the wired network. In addition, the gateway list for each must include the wireless IP address of the gateway or gateways in the other subnet.

On gateway 192.168.1.1, add the following entry to the gateway list:
- IP address: 192.168.2.1, subnet mask: 255.255.255.0

On gateway 192.168.1.2, add the following entry to the gateway list:
- IP address: 192.168.2.1, subnet mask: 255.255.255.0

On gateway 192.168.2.1, add the following entries to the gateway list:
- IP address: 192.168.1.1, subnet mask: 255.255.255.0
- IP address: 192.168.1.2, subnet mask: 255.255.255.0
Note
The on-board DHCP server cannot be used with multi-subnet roaming.

Figure 28  Multi-Subnet Roaming Example

Configuring DHCP MAC Address Filters and Address Reservations

DHCP MAC address filters enable the internal DHCP server of the Tropos gateway to limit assignment of IP addresses to wireless clients. DHCP address reservations provide a means to associate individual IP addresses with specific MAC addresses, thus ensuring that designated
devices always retain the same IP address. Perform these tasks to configure DHCP MAC address filters:

1. Enable the internal DHCP server, as explained in “Configuring DHCP Settings” on page 43.
2. Configure the DHCP MAC feature, described in this section, on all Tropos gateways that run an internal DHCP server.
3. Use the DHCP MAC Filter/Reservation screen, shown in Figure 29, to configure the address filters and reservations. If you enable MAC address filters on the Tropos gateway, then you must add the MAC addresses for each Tropos gateway, Tropos node, and client, to the DHCP MAC Address Filter Address Reservation screen.
Note
It is recommended that you create DHCP MAC reservations before bringing any clients onto the network. If you create reservations after clients have already been assigned IP addresses, pick different IP addresses for the reservations.

Figure 29  DHCP MAC Address Filter and Address Reservation screen

DHCP MAC Filter/Reservation Configuration

<table>
<thead>
<tr>
<th>Stored</th>
<th>Committed</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP MAC Address Filter</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Note: DHCP MAC Address Filter may or may not be enabled for IP Address Reservation

Add or delete DHCP MAC addresses to the List

Note: IP Address has to be in the DHCP address pool

<table>
<thead>
<tr>
<th>DHCP MAC Address</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Add DHCP MAC  Delete DHCP MAC

DHCP MAC Address Filter

DHCP MAC Address

00:60:17:CC:00:22  Delete

DHCP MAC Address Reservation

<table>
<thead>
<tr>
<th>IP Address</th>
<th>DHCP MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.101.115</td>
<td>00:60:B3:72:B7D2</td>
</tr>
</tbody>
</table>

Committed DHCP MAC addresses

<table>
<thead>
<tr>
<th>IP Address</th>
<th>DHCP MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:60:17:CC:00:22</td>
<td></td>
</tr>
<tr>
<td>192.168.101.115</td>
<td>00:60:B3:72:B7D2</td>
</tr>
</tbody>
</table>
Configure MAC address filters
1. Open the Tropos Configuration Utility.
2. Click DHCP Clients on the side menu to open the DHCP MAC Filter/Reservation screen.
3. Select Enabled for the field entitled DHCP MAC Address Filter.
4. Enter a MAC address, but do not enter a corresponding IP address.
5. Click Add DHCP MAC.
6. Continue adding MAC addresses as desired.
7. When you have finished, click Commit Changes on the side menu.
8. When you have finished adding MAC addresses and committed the changes, reboot the Tropos gateway and all Tropos nodes, and renew the DHCP leases for all clients.

Remove a MAC Address
1. Click the Delete button to the right of the address.
2. Click Commit Changes on the side menu.
3. Reboot the Tropos gateway and all Tropos nodes.

Caution
When you enable MAC address filters, only clients explicitly listed are able to access the network. Before you enable the MAC address filters, confirm that you are not interrupting active sessions for existing clients.

Set up DHCP reservations
1. Open the Tropos Configuration Utility.
2. Click DHCP Clients on the side menu to open the DHCP MAC Filter/Reservation screen.
3. Enter a MAC address and its associated IP address.
4. Click Add DHCP MAC.
   The MAC address appears in the list of DHCP reservations. Continue adding addresses as desired.
5. Click Store Changes. When you have finished, click Commit Changes on the side menu.

Note
The reserved IP addresses must be in the range of the DHCP server. Do not create reservations for IP addresses already assigned in the network, unless you are reserving that IP address for its current lease holder.
Client Access

Use the Client Access Configuration screen, shown in Figure 30, to create a list of clients, specified by MAC addresses, that are explicitly permitted or not permitted to associate to the Tropos router. This capability enhances your ability to control the network by prohibiting unwanted clients from gaining access or by allowing only known clients to be granted access.

By default, the Deny list is enabled. All clients are allowed to associate (if they have the correct WEP settings and ESSID), unless specifically denied in the list. To prohibit a client from accessing the entire wireless network, you must enter the deny client information in each Tropos router.

Figure 30  Client Access Configuration screen

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:60:FC:AA:00:55</td>
<td>Delete</td>
</tr>
<tr>
<td>00:60:FC:AA:04:22</td>
<td>Delete</td>
</tr>
</tbody>
</table>

Committed Deny Client List

<table>
<thead>
<tr>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:60:FC:AA:00:55</td>
</tr>
<tr>
<td>00:60:FC:AA:04:22</td>
</tr>
</tbody>
</table>
If you add more than 10 clients to the client list, the screen presents a link instead of the full list. Click the link to display the list of client MAC addresses.

**Figure 31 Client Access Configuration Screen, More than Ten Clients**

<table>
<thead>
<tr>
<th>Client Access Rule</th>
<th>Stored</th>
<th>Committed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny</td>
<td></td>
<td>Deny</td>
</tr>
</tbody>
</table>

Wireless access is denied to the following clients

### MAC Address

<table>
<thead>
<tr>
<th>Deny</th>
<th>Delete</th>
</tr>
</thead>
</table>

**Committed Deny Client List**

<table>
<thead>
<tr>
<th>MAC Address</th>
</tr>
</thead>
</table>

**Deny association to designated clients**

1. Open the Tropos Configuration Utility.
2. Click **Client Access** on the side menu.
3. Verify that the current Client Access Rule is Deny. If not, click **Change Client Access Rule to Deny**.
4. Enter the MAC address of the client.
5. Click **Deny**. The designated client is listed in the table at the bottom of the screen.
6. When you have finished, click **Commit Changes** on the side menu.

The client is now prohibited from associating to the Tropos router. If the client was associated at the time you committed the Deny Client record, the association is dropped.

**Permit a denied client to reassociate**

Follow these steps if ten or fewer clients are in the Deny list:

1. Select the MAC address from the table.
2. Click **Delete**.
3. When you have finished, click **Commit Changes** on the side menu.
Follow these steps if more than ten clients are in the Deny list:

1. Enter the MAC address of the client.
2. Click Delete.
3. When you have finished, click Commit Changes on the side menu.

**Allow association only to designated clients**

1. Open the Tropos Configuration Utility.
2. Click Client Access on the side menu.
3. Verify that the current Client Access Rule is Allow. If not, click Change Client Access Rule to Allow.
4. Enter the MAC address of the client.
5. Click Allow. The designated client is listed in the table at the bottom of the screen.
6. When you have finished, click Commit Changes on the side menu.

The client is now permitted to associate to the Tropos router.

**Deny access to a currently allowed client**

Follow these steps if ten or fewer clients are in the Allow list:

1. Select the MAC address from the table.
2. Click Delete.
3. When you have finished, click Commit Changes on the side menu.

Follow these steps if more than ten clients are in the Allow list:

1. Enter the MAC address of the client.
2. Click Delete.

When you have finished, click Commit Changes on the side menu.
Supporting Static IP Clients

Use the Static IP Client Configuration screen to configure clients that require static IP addresses rather than DHCP-supplied addresses. The screen includes an auto-detection capability. If you select auto-detection, then the Tropos router can automatically detect the presence of static IP clients and route them, even though their addresses are not explicitly entered. Figure 32 shows the Static IP Clients screen for fixed Tropos router. For information on configuring a static IP client for a mobile node, see “Static Client for Mobile Node” on page 83.

The static IP client feature is disabled by default. If security is an issue and you want to route only clients that are explicitly recognized, do not enable this feature.

The Static IP Client Configuration screen also includes the ability to route customer premise equipment (CPE), such as wireless-to-Ethernet bridges. You can route CPE devices by entering the MAC address of the CPE in addition to the addresses of the clients that are connected to the CPE device.

Note
If you use auto-detection for static clients, it must be enabled on all the gateways and nodes in the wireless routing domain (WRD).

Enable auto-detection of clients with static IP addresses:
1. Open the Tropos Configuration Utility.
2. Choose Static IP Clients from the side menu.
3. Select Enabled for the field entitled Auto-Detect Client with Static IP. If you select this feature, it is not necessary to enter individual IP addresses.
4. Click Store Changes. Make sure to commit the changes when you have finished.

Enable manually-configured clients with static IP addresses
1. If necessary, disable auto-detection on the Static IP Client screen.
2. Enter the client’s MAC address and static IP address. To route a CPE device, enter the MAC address of the CPE in addition to the addresses of all clients connected to the CPE device. Figure 32 shows the configuration of two static IP clients connected to the same CPE device, along with an additional static IP client.
3. Click Add Static IP Client. Add additional clients as needed.
4. When you have finished, click **Commit Changes** on the side menu.

**Figure 32  Static IP Client Configuration Screen (Gateway)**

### Static IP Client Configuration

<table>
<thead>
<tr>
<th>Stored</th>
<th>Committed</th>
</tr>
</thead>
<tbody>
<tr>
<td>enabled</td>
<td>enabled</td>
</tr>
</tbody>
</table>

#### List of Clients with Static IP

<table>
<thead>
<tr>
<th>Client MAC Address</th>
<th>Static IP Address</th>
<th>CPE MAC Address</th>
<th>Add</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:60:B3:73:C4:34</td>
<td>192.168.128.27</td>
<td>00:30:1A:01:E2:F4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:60:B3:73:C4:25</td>
<td>192.168.128.15</td>
<td>00:30:1A:01:E2:F4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:60:B3:73:C0:71</td>
<td>192.168.128.45</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Committed List of Clients with Static IP Address

<table>
<thead>
<tr>
<th>Client MAC Address</th>
<th>IP Address</th>
<th>CPE MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:60:B3:73:C4:34</td>
<td>192.168.128.27</td>
<td>00:30:1A:01:E2:F4</td>
</tr>
<tr>
<td>00:60:B3:73:C4:25</td>
<td>192.168.128.15</td>
<td>00:30:1A:01:E2:F4</td>
</tr>
<tr>
<td>00:60:B3:73:C0:71</td>
<td>192.168.128.45</td>
<td></td>
</tr>
</tbody>
</table>
**Static Client for Mobile Node**

Use the Static IP Client Configuration screen ([Figure 33](#)) to assign an IP address for a wired client connected to a Tropos 4210 node over the router’s MGT interface.

**Figure 33  Static IP Client Configuration Screen (Mobile Node)**

---

**Static IP Client Configuration**

<table>
<thead>
<tr>
<th>Stored</th>
<th>Committed</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTO DETECT CLIENTS WITH STATIC IP</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

---

List of Wired Clients (clients connected to eth1 interface) with static IP addresses. Available only when the unit is in the "MobileNode" setting.

<table>
<thead>
<tr>
<th>Client MAC Address</th>
<th>Static IP Address</th>
<th>CPE MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:00:02</td>
<td>5.0.0.0</td>
<td></td>
</tr>
</tbody>
</table>

Committed list of Clients with Static IP Address

<table>
<thead>
<tr>
<th>Client MAC Address</th>
<th>IP Address</th>
<th>CPE MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:00:02</td>
<td>5.0.0.0</td>
<td></td>
</tr>
</tbody>
</table>

---

**Configure a wired client IP address for a mobile node**

1. If necessary, disable auto-detection on the Static IP Client screen.
2. Enter the client’s MAC address and static IP address.
3. Click Add Static IP Client.
4. When you have finished, click Commit Changes on the side menu.

---

**Defining Packet Filter Forwarding Rules**

Packet filter forwarding rules determine which IP packets are forwarded by the Tropos router and which are rejected. Select the packet filtering rules in the Packet Filter Forwarding screen.

- If the packet filter policy is **Permit Forwarding**, then the Tropos router accepts all packets, except those explicitly denied in the Packet Forwarding Deny rules ([Figure 35](#)).
- If the packet filter policy is **Deny Forwarding**, then the Tropos router rejects all IP packets, except those explicitly enabled in the Packet Forwarding Permit rules ([Figure 34](#)).
**Note**
Packet filter forwarding rules apply only to packets that travel through the Tropos gateway, not packets that originate or terminate at the router.
Figure 34  Packet Filtering Forwarding Screen (Filtering Permitted)

Packet Filter Forwarding Configuration

<table>
<thead>
<tr>
<th>Stored</th>
<th>Committed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Filter Policy</td>
<td>Permit Forwarding</td>
</tr>
</tbody>
</table>

Change Packet Filter Policy to Deny Forwarding

Packets of the following rules will be discarded and all other packets will be forwarded.

**Stored Packet Forwarding Deny Rules**

<table>
<thead>
<tr>
<th>Name</th>
<th>Protocol</th>
<th>Source IP</th>
<th>Source Mask (bits)</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Mask (bits)</th>
<th>Destination Port</th>
</tr>
</thead>
</table>

**Committed Packet Forwarding Deny Rules**

<table>
<thead>
<tr>
<th>Name</th>
<th>Protocol</th>
<th>Source IP</th>
<th>Source Mask (bits)</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Mask (bits)</th>
<th>Destination Port</th>
</tr>
</thead>
</table>
Figure 35 Packet Filtering Forwarding Screen (Filtering Denied)

Packet Filter Forwarding Configuration

<table>
<thead>
<tr>
<th>Stored</th>
<th>Committed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Filter Policy</td>
<td>Deny Forwarding</td>
</tr>
</tbody>
</table>

Change Packet Filter Policy to Permit Forwarding

Packets of the following rules will be permitted and all other packets will be discarded.

### Stored Pre-defined Packet Forwarding Permit Rules

<table>
<thead>
<tr>
<th>Rule</th>
<th>Protocol</th>
<th>Permit to/from these addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit</td>
<td>DNS</td>
<td>any</td>
</tr>
<tr>
<td>Permit</td>
<td>Cisco VPN</td>
<td>any</td>
</tr>
<tr>
<td>Permit</td>
<td>ICMP</td>
<td>any</td>
</tr>
<tr>
<td>Permit</td>
<td>HTTPS</td>
<td>any</td>
</tr>
<tr>
<td>Permit</td>
<td>SSH</td>
<td>any</td>
</tr>
<tr>
<td>Permit</td>
<td>IPSec</td>
<td>any</td>
</tr>
<tr>
<td>Permit</td>
<td>POP3</td>
<td>any</td>
</tr>
<tr>
<td>Permit</td>
<td>HTTP</td>
<td>any</td>
</tr>
<tr>
<td>Permit</td>
<td>SMTP</td>
<td>any</td>
</tr>
<tr>
<td>Permit</td>
<td>Telnet</td>
<td>any</td>
</tr>
<tr>
<td>Permit</td>
<td>SNMP</td>
<td>any</td>
</tr>
</tbody>
</table>

### Committed Pre-defined Packet Forwarding Permit Rules

<table>
<thead>
<tr>
<th>Rule</th>
<th>Protocol</th>
<th>Input Hits</th>
<th>Forward Hits</th>
<th>Restrict to/from these addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit</td>
<td>DNS</td>
<td>0</td>
<td>0</td>
<td>any</td>
</tr>
<tr>
<td>Permit</td>
<td>Cisco</td>
<td>0</td>
<td>0</td>
<td>any</td>
</tr>
<tr>
<td>Permit</td>
<td>ICMP</td>
<td>7</td>
<td>0</td>
<td>any</td>
</tr>
<tr>
<td>Permit</td>
<td>HTTPS</td>
<td>1723</td>
<td>0</td>
<td>any</td>
</tr>
<tr>
<td>Permit</td>
<td>SSH</td>
<td>14</td>
<td>0</td>
<td>any</td>
</tr>
<tr>
<td>Deny</td>
<td>IPSec</td>
<td>0</td>
<td>0</td>
<td>any</td>
</tr>
<tr>
<td>Deny</td>
<td>POP3</td>
<td>0</td>
<td>0</td>
<td>any</td>
</tr>
<tr>
<td>Deny</td>
<td>HTTP</td>
<td>0</td>
<td>0</td>
<td>any</td>
</tr>
<tr>
<td>Deny</td>
<td>SMTP</td>
<td>0</td>
<td>0</td>
<td>any</td>
</tr>
<tr>
<td>Deny</td>
<td>Telnet</td>
<td>0</td>
<td>0</td>
<td>any</td>
</tr>
<tr>
<td>Permit</td>
<td>SNMP</td>
<td>0</td>
<td>0</td>
<td>any</td>
</tr>
</tbody>
</table>
Set the default packet filter forwarding policy

1. Open the Tropos Configuration Utility.
2. Click **Packet Filtering**.
3. Select **Permit Packet Filter Forward** or **Deny Packet Filter Forwarding**.
4. Scroll down and click **Store Changes**. Make sure to commit the changes when you have finished.

Deny selected packets when the default policy is Permit Packet Filter Forwarding

1. Open the Tropos Configuration Utility.
2. Click **Packet Filtering** and confirm that the default policy is Permitted.
3. Enter an alphanumeric name for the deny rule.
4. Select a protocol, if appropriate.
5. Specify the deny conditions for source packets, if desired, by entering a source IP address, number of subnet mask bits, and a source port number associated with a protocol or function.
6. Specify the deny conditions for destination packets, if desired, by entering a destination IP address, number of subnet mask bits, and a destination port number associated with a protocol or function. For an example of how this works, see “NTP Session Example” on page 88.
7. Click **Add**. Continue adding deny rules as needed.
8. When you have finished, click **Commit Changes** on the side menu.

Permit selected packets when the default policy is Deny Packet Filter Forwarding

1. Open the Tropos Configuration Utility.
2. Click **Packet Filtering** and confirm that the default policy is Denied.
3. To permit packets from specific protocols:
   a. Enable the protocols in Packet Forwarding Permit Rules list. Refer to Table 6 for a list of the standard protocols and ports.
   b. To restrict the rules to specific IP addresses, enter a comma-separated lists of addresses.
4. To permit packets based on custom rules:
   a. Scroll down to the area entitled Stored Custom Packet Forwarding Permit Rules.
   b. Enter an alphanumeric name for the deny rule.
   c. Select a protocol, if appropriate.
   d. Specify the permit conditions for source packets, if desired, by entering a source IP address, number of subnet mask bits, and a source port number associated with a protocol or function.
Chapter 5 • Managing Clients

e. Specify the permit conditions for destination packets, if desired, by entering a destination IP address, number of subnet mask bits, and a destination port number associated with a protocol or function. For an example of how this works, see “NTP Session Example” on page 88.

f. Click Add. Continue adding permit rules as needed.

5. When you have finished, click Commit Changes on the side menu.

Table 6 Standard Protocols and Ports

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Ports Allowed</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP (Dynamic Host Configuration Protocol)</td>
<td>UDP ports 67/68</td>
</tr>
<tr>
<td>DNS (Domain and Host Name Service)</td>
<td>UDP ports 42/53</td>
</tr>
<tr>
<td>Cisco (Cisco VPN 3000 Concentrator Series)</td>
<td>UDP ports 500/10000</td>
</tr>
<tr>
<td>ICMP (Ping and Traceroute)</td>
<td>N/A</td>
</tr>
<tr>
<td>HTTPS (Secure HTTP)</td>
<td>TCP port 443</td>
</tr>
<tr>
<td>SSH (Secure Shell)</td>
<td>TCP port 22</td>
</tr>
<tr>
<td>IPSec (Internet Protocol Security)</td>
<td>protocol 50 UDP port 500</td>
</tr>
<tr>
<td>POP3 (Post Office Protocol 3)</td>
<td>TCP port 110</td>
</tr>
<tr>
<td>HTTP (hypertext transfer protocol)</td>
<td>TCP port 80</td>
</tr>
<tr>
<td>SMTP (simple mail transfer protocol)</td>
<td>TCP port 25</td>
</tr>
<tr>
<td>Telnet</td>
<td>TCP port 23</td>
</tr>
<tr>
<td>SNMP (Simple Network Management Protocol)</td>
<td>TCP port 161 and 162</td>
</tr>
</tbody>
</table>

Note
If you disable DHCP, client devices and Tropos nodes are not able to obtain the DHCP lease required for operation. If you disable HTTPS, all HTTPS traffic is dropped.

NTP Session Example

This section explains how to enable incoming and outgoing NTP sessions using custom rules. The process of enabling or disabling other protocols is similar.

Enable all NTP sessions
1. Confirm that the default packet forwarding policy is Denied.
2. Enter Incoming NTP in the Name box.
3. Enter udp in the Protocol box.
Permitted values for the Protocol field include TCP, UDP or the protocol number.

4. Enter any in the Source IP box.
5. Enter any in the Source Mask box.
6. Enter 123 in the Source Port box. This is the port number for NTP.
7. Enter any in the Destination IP, Destination Mask and Destination Port boxes.
8. Click Store Changes.
9. Add a second rule to enable outgoing NTP sessions by entering Outgoing NTP in the Name box.
10. Enter udp in the Protocol box.
11. Enter any in the Source IP, Source Mask, Source Port, Destination IP and Destination Mask boxes.
12. Enter 123 in the Destination Port box.
13. Click Store Changes. Make sure to commit the changes when you have finished.

You have now created two rules to enable incoming and outgoing NTP sessions. Make sure to repeat this process for all the Tropos routers in the network.

Packet Hit Counts

When the default packet forwarding policy is Denied, the Committed Pre-defined Packet Forwarding Permit Rules table on the Packet Filter screen shows the count of packets directed towards the Tropos gateway, and those forwarded by the gateway. This information is displayed for each pre-defined filtering rule, but not for any custom rules.

Reset all hit counts on the screen
- Click Reset Hit Counts at the bottom of the screen.

Configuring VLANs

A virtual local area network (VLAN) is a logical grouping of client stations that enables them to function as if they are on the same subnetwork, regardless of their physical location. Using VLANs, organizations can selectively forward different types of network traffic that travel over the same physical network. For example, a municipality may want to install a Tropos wireless network to serve both its local police and fire departments, while, at the same time, restrict client traffic intended for each department to that department’s internal network. Assigning each department to a different VLAN allows the municipality to manage the two networks as if they were physically segregated, although they are part of the same physical infrastructure.

VLAN traffic is managed through the assignment of VLAN tags. A VLAN tag includes a unique VLAN ID and is transmitted as part of each Ethernet packet. Tropos gateways tag each packet with a VLAN tag. When packets arrive at a VLAN-capable Ethernet switch, the traffic is directed to the appropriate destination based on VLAN access ports.
VLANs can serve as an effective management tool when clients roam within the same subnet or across subnets. Since VLAN assignment is not tied to physical location, clients remain in the same VLAN regardless of where they roam in the overall Tropos network.

All VLAN features are compatible with Tropos 4210 mobile MetroMesh routers.

**Management VLAN**

In addition to assigning VLANs for client traffic, it is important to reserve a separate VLAN ID per subnet for management and control traffic between Tropos gateways and nodes. This ensures that communications among gateways and nodes will take place regardless of client VLAN assignments. The same management VLAN ID should be assigned to all the Tropos gateways and nodes in the subnet and should not be used as an ESSID- or IP-based VLAN ID.

Tropos supports two types of VLANs: ESSID-based and IP-based.

**ESSID-Based VLANs**

ESSID-based VLANs associate a VLAN ID with a specific ESSID. When a client associates to a Tropos router using that ESSID, the client is automatically assigned to the corresponding VLAN. ESSID-based VLANs are supported only on the Tropos 5210, 4210, and 3210 routers.

---

**Note**

Before setting up ESSID-based VLANs, it is necessary to configure all the ESSIDs that the router will support. Use the Multi-ESSID screen to configure additional ESSIDs, as explained in “Configuring Multiple ESSIDs” on page 39.

---

*Figure 36* shows an example network that uses ESSID-based VLANs. ESSID 1 and VLAN 10 are assigned to the police department, while ESSID 2 and VLAN 20 are assigned to the fire department. Each police department client associates to a node using ESSID 1, which automatically places that user in VLAN 10. Traffic from the user is tagged with VLAN 10 as it leaves the wireless network and enters the Ethernet network. When the traffic reaches a VLAN-enabled Ethernet switch, it is forwarded to the appropriate access network for that VLAN.
Similarly, fire department clients associate using ESSID 2, which places them in VLAN 20 and assures that their traffic will be correctly forwarded to fire department clients.

**Figure 36 ESSID-Based VLANs**

IP-based VLANs associate a VLAN ID with an individual subnetwork. When the client associates to a Tropos router, it is assigned to the VLAN that has been mapped to the client’s subnetwork. This method of VLAN assignment is compatible with both static and DHCP IP addresses.

**Figure 37** shows a network that uses IP-based VLANs. VLAN 10 is assigned to the police department, which is also assigned to the subnetwork 10.88.100.x/24. VLAN 20 is assigned to the fire department, which is also assigned to the subnetwork 10.88.200.x/24. Fire department clients are configured to be part of subnetwork 10.88.200.x/24, which automatically places them in the fire department VLAN; police department clients are configured to be part of subnetwork 10.88.100.x/24, which automatically places them in the police department VLAN. Traffic
continues to be forwarded to the correct departments, even if clients roam to another Tropos node.

**Figure 37** IP-Based VLANs

As these examples show, both ESSID- and IP-based VLANs can be used to achieve the same or similar objectives. The following guidelines may be useful in choosing which type of VLAN to configure:

- ESSID-based VLANs are easier than IP-based VLANs to deploy and administer; however, they are supported only on the Tropos 5210, 4210, and 3210 routers.
- IP-based VLANs are supported on all Tropos routers. This is the only type of VLAN support available for networks that contain a mix of different router types (5210/4210/3210 and 3110/5110).
- IP-based VLANs can be used for downstream sub-interface clients to separate the traffic that flows to those clients.
- If ESSID- and IP-based VLAN rules conflict in their treatment of client traffic, the ESSID-based rules take precedence.
- Wired clients attached to mobile nodes can be placed in IP-based VLANS but not in ESSID-based VLANs.
Configure ESSID-based VLANs on all the Tropos gateways and nodes. Configure IP-based VLANs only on the Tropos gateways.

**Client DHCP Relay Policy**

If the VLAN feature is not used, then client DHCP requests are serviced by the on-board DHCP server on the Tropos gateway or relayed to an external DHCP server. If VLANs are configured, then additional options become available for assigning relay agents for client DHCP requests:

- **Wireless relay.** Each Tropos gateway has one wireless IP address. If the wireless relay option is selected, then this wireless IP address is used as the relay agent IP address for client DHCP requests.
- **Wired relay.** Each VLAN interface is assigned its own IP address. If wired relay is selected, then IP address of the VLAN interface is used as the relay agent IP address for DHCP requests.

The wireless and wired relay settings on the VLAN screen supersede the settings on the DHCP server screen for client requests. If relay is configured on the VLAN screen, then the relay setting on the DHCP server screen applies only to the management VLAN. For static clients ("Supporting Static IP Clients" on page 81), the relay settings on the DHCP server screen and VLAN screen are ignored.

Table 7 lists the available client DHCP relay options as a function of VLAN type. Wireless relay is supported with ESSID- and IP-based VLANs; however, wired relay is supported only with ESSID-based VLANs.

**Table 7 VLAN Relay Options**

<table>
<thead>
<tr>
<th>ESSID-Based VLANs</th>
<th>IP-Based VLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Relay</td>
<td>Supported</td>
</tr>
<tr>
<td>Wired Relay</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Non-Supported</td>
</tr>
</tbody>
</table>

**Multi-Subnet Roaming with VLANs**

Multi-subnet roaming is supported in networks with VLANs. To configure multi-subnet roaming with VLANs, perform these tasks:

1. Set up the VLAN configuration (see “VLAN Configuration Steps” on page 95).
2. If you choose the wired client DHCP relay option on the VLAN screen, add all gateways to the multi-subnet roaming list, and enter subnet and subnet mask information for each VLAN defined on each gateway in the VLAN roaming list (see “Supporting Multi-Subnet Roaming” on page 70).
Figure 38 shows a multi-subnet roaming example with VLANs. Two Tropos clusters are configured: for subnet 10.10.10.x/24 and subnet 9.9.9.x/24, and the wired relay option is chosen. The following VLAN assignments are made, and the gateway IP addresses and VLAN subnet information are entered in the Multi-Subnet Roaming screen:

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Description</th>
<th>IP Address</th>
<th>Address Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Police Department VLAN</td>
<td>11.11.11.1/24</td>
<td>VLAN interface IP address</td>
</tr>
<tr>
<td>20</td>
<td>Fire Department VLAN</td>
<td>12.12.12.1/24</td>
<td>VLAN interface IP address</td>
</tr>
<tr>
<td>30</td>
<td>Management VLAN for subnet 10.10.10.x/24</td>
<td>10.10.10.1/24</td>
<td>IP address of wireless interface</td>
</tr>
<tr>
<td>40</td>
<td>Management VLAN for subnet 9.9.9.x/24</td>
<td>9.9.9.1/24</td>
<td>IP address of wireless interface</td>
</tr>
</tbody>
</table>

When a client roams from the home subnet to another subnet, the client’s traffic is still routed to the correct VLAN. As shown in Figure 38, a police or fire department client can still reach its own VLAN even when associated to the other department’s subnet.

**Figure 38  Multi-Subnet Roaming with VLANs**
**Downstream Sub-Interfaces with VLANs**

Downstream sub-interfaces are supported only with IP-based VLANs. The relay agent for the DHCP transactions is the IP address of the downstream sub-interface (see “Downstream Sub-Interface” on page 58).

The wired or wireless relay option does not apply to the downstream sub-interface. The DHCP server used to supply client DHCP addresses for the downstream clients is the server specified for the VLAN interface. The management VLAN is used for all DHCP transactions for downstream interfaces. When configuring the downstream sub-interfaces, be sure the DHCP server is reachable over the management VLAN.

**VLAN Configuration Steps**

Configure VLAN settings for a Tropos cluster by using the VLAN screen for the Tropos gateway (Figure 39). Perform the following tasks from this screen:

1. Enable the VLAN feature.
2. Assign a VLAN ID to the Tropos cluster.
3. Configure the VLAN interface.
4. Determine client DHCP relay policy.
5. Configure IP-based VLANs.
6. Configure ESSID-based VLANs.

**Note**

Mobile nodes support only IP-based VLANs.
### VLAN Configuration

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Stored</th>
<th>Committed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Enable**: Enabled

**Store Changes**

### Subnet/Tropos Node VLAN ID

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Stored</th>
<th>Committed</th>
</tr>
</thead>
<tbody>
<tr>
<td>40</td>
<td></td>
<td>40</td>
</tr>
</tbody>
</table>

**Store Changes**

### Client DHCP Relay Policy

<table>
<thead>
<tr>
<th>Relay Policy</th>
<th>Stored</th>
<th>Committed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless-Relay</td>
<td>Wired-Relay</td>
<td>Wired-Relay</td>
</tr>
</tbody>
</table>

**Store Changes**

### VLAN Interface Static IP Address Configuration

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Default Gateway Address</th>
<th>DHCP server address</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>150</td>
<td>6.6.150.2</td>
<td>255.255.255.0</td>
<td>6.6.150.1</td>
<td>15.15.15.2</td>
<td>Add</td>
</tr>
<tr>
<td>200</td>
<td>6.6.200.4</td>
<td>255.255.255.0</td>
<td>6.6.200.1</td>
<td>6.6.200.2</td>
<td>Delete</td>
</tr>
<tr>
<td>500</td>
<td>6.6.9.4</td>
<td>255.255.255.0</td>
<td>6.6.9.7</td>
<td>6.6.9.9</td>
<td>Delete</td>
</tr>
<tr>
<td>910</td>
<td>10.10.12.1</td>
<td>255.255.255.0</td>
<td>10.10.12.2</td>
<td>15.15.15.2</td>
<td>Delete</td>
</tr>
<tr>
<td>920</td>
<td>10.10.13.1</td>
<td>255.255.255.0</td>
<td>10.10.13.2</td>
<td>15.15.15.2</td>
<td>Delete</td>
</tr>
</tbody>
</table>

### Committed List

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Default Gateway Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>150</td>
<td>6.6.150.2</td>
<td>255.255.255.0</td>
<td>6.6.150.1</td>
</tr>
<tr>
<td>200</td>
<td>6.6.200.4</td>
<td>255.255.255.0</td>
<td>6.6.200.1</td>
</tr>
<tr>
<td>500</td>
<td>6.6.9.4</td>
<td>255.255.255.0</td>
<td>6.6.9.7</td>
</tr>
<tr>
<td>910</td>
<td>10.10.12.1</td>
<td>255.255.255.0</td>
<td>10.10.12.2</td>
</tr>
<tr>
<td>920</td>
<td>10.10.13.1</td>
<td>255.255.255.0</td>
<td>10.10.13.2</td>
</tr>
</tbody>
</table>
Figure 40 VLAN Screen Lower Section

<table>
<thead>
<tr>
<th>ESSID TO VLAN MAPPING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan Id</td>
</tr>
<tr>
<td>---------</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>25</td>
</tr>
</tbody>
</table>

**Committed List of ESSID to VLAN Mappings**

<table>
<thead>
<tr>
<th>Vlan Id</th>
<th>ESSID</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>DelRay</td>
</tr>
<tr>
<td>25</td>
<td>ManAve</td>
</tr>
</tbody>
</table>

**IP to VLAN MAPPING**

<table>
<thead>
<tr>
<th>Vlan Id</th>
<th>IP/Subnet Address</th>
<th>IP/Subnet Mask</th>
<th>Add</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>910</td>
<td>10.10.12.0</td>
<td>255.255.255.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>920</td>
<td>10.10.13.0</td>
<td>255.255.255.0</td>
<td></td>
<td>Delete</td>
</tr>
</tbody>
</table>

**Committed List of IP to VLAN Mappings**

<table>
<thead>
<tr>
<th>Vlan Id</th>
<th>IP Address</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>910</td>
<td>10.10.12.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>920</td>
<td>10.10.13.0</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>
Enable the VLAN feature
1. Open the Tropos Configuration Utility.
2. Click VLAN on the side menu to open the VLAN screen.
3. Select Enable.
4. Click Store Changes. Remember to commit changes when you have finished your configuration tasks.

Assign a management VLAN ID for the Tropos cluster
1. Enter the VLAN ID in the Subnet/Tropos Node VLAN ID field. This ID should be used only for the management VLAN.
2. Click Store Changes. Remember to commit changes when you have finished your configuration tasks.

Select a client DHCP relay policy
1. Select Wireless Relay or Wired Relay from the Client DHCP Relay Policy pull-down list. See “Client DHCP Relay Policy” on page 93.
2. Click Store Changes. Remember to commit changes when you have finished your configuration tasks.

Configure the VLAN interfaces
You can configure VLAN interfaces statically or by using DHCP address assignments.

For static assignments:
1. Enter a VLAN ID for the VLAN interface in the Vlan Interface IP Address Configuration area.
2. Enter an IP address and subnet mask for the VLAN interface. This should be an address that is not used anywhere else in the network.
3. Enter the IP address of the default network gateway (router).
4. Enter the IP address of the server that supplies DHCP service for relayed client DHCP requests (as set in the Client DHCP Relay Policy field).
5. Click Add.
6. Define additional mappings as needed.

For DHCP assignment:
1. Make sure that the IP Configuration Method setting for the gateway on the Device and IP screen is DHCP. See Figure 13 on page 46.
2. Assign a static IP address for each VLAN interface, as if you were using the static address assignment option. The static address will serve as a placeholder until the DHCP server is able to supply the IP address. Include the IP address of the DHCP server that will supply addresses for the VLAN.
3. The gateway will now try to obtain IP addresses for its interfaces from the specified DHCP servers. Once the gateway has obtained addresses, then the placeholder entries will be automatically overwritten.

**Create an ESSID-based VLAN**

ESSID-based VLANs are configured on all the Tropos gateways and nodes.

1. Enter the VLAN ID in the ESSID to VLAN IP mapping area.
2. Enter the ESSID for the VLAN.
3. Click Add.
4. Define additional mappings as needed.

**Create an IP-based VLAN**

IP-based VLANs are configured only on the Tropos gateways.

1. Enter the VLAN ID in the IP to VLAN mapping area.
2. Enter the IP subnet address for the VLAN and the associated subnet mask.
3. Click Add.
4. Define additional mappings as needed.
Configuring Quality of Service

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.

For example, a municipality may have a wireless network that is used jointly by the police department, fire department, and other non-emergency services. Although the police and fire departments might have relatively low bandwidth requirements, it is essential that their messages be able to be transmitted at all times without loss or delay. An effective QoS solution would guarantee a certain bandwidth to each department, leaving the remaining network bandwidth for all the other non-critical government entities.

To illustrate another type of QoS solution, consider an organization that supports a variety of client applications. If some applications depend upon uninterrupted data flow or demand large packet sizes, the best QoS solution may be to provide preferential treatment for the protocols that support the high-demand applications, rather than for the clients who run the applications. Examples of such applications include streaming media and voice over IP.

Tropos supports these needs by way of QoS policies that reserve network bandwidth or assign priorities for packet forwarding for downstream traffic. The Tropos QoS policies do not apply to upstream traffic.

Bandwidth Reservations

With bandwidth reservations, the affected clients addresses or protocols are guaranteed a fixed slice of the total available network bandwidth. You can specify the average bandwidth to be reserved and a maximum rate to be accommodated for traffic bursts. To use bandwidth reservations effectively, it is important to estimate the effective bandwidth available in the network and then determine the fraction of that bandwidth that can meet the needs of the organization while still leaving room for non-reserved applications. An estimate is required because effective bandwidth may differ from the configured client bandwidth due to distances between routers, the average number of hops from the client to the gateway, and overall link and signal quality. In addition, .1Mbps is automatically reserved for Tropos router-to-router control traffic.

For example, a typical multiple-hop 802.11b network will have available bandwidth of 3Mbps. Reserving .8 Mbps for the police department and .8 Mbps for the fire department plus .1Mbps leaves 1.3 Mbps available for other clients. If the maximum rate for each department is set to 10% above the configured rate, or .88Mbps for each, that permits some burst traffic to be accommodated without further reducing the average bandwidth available to other clients.

Keep the following points in mind when planning a QoS solution based on bandwidth reservations:

- Bandwidth reservations are strictly observed. The reserved bandwidth is never available to other than configured uses.
If you overbook bandwidth reservations, then the actual reserved bandwidth may be less than the configured amount. In the police and fire department example, if 1.7Mbps is reserved for each department, then neither department may be guaranteed the full bandwidth. Moreover, regardless of the reservation policy, 100Kbps is still guaranteed for non-reserved traffic.

Only the reserved bandwidth is made available for the designated use. For the municipality in the example, the police and fire departments have .8 Mbps reserved for each, but no more than is allocated. If bandwidth requirements increase beyond that point, there will be delays introduced or packets dropped.

**Note**
The bandwidth rules apply only to downstream traffic. Upstream traffic is not subject to reservations.

These factors suggest that good planning is important for effective bandwidth reservations. For guidelines on network planning to accommodate bandwidth requirements, please see the *Tropos Networks System Design Guidelines*.

**Priority Based Forwarding**

In priority based forwarding, the total available network bandwidth is shared among all clients and applications; however, certain clients or applications are given priority treatment. A set of traffic prioritization rules is defined and each rule is assigned a class of service from 1 to 7, with 1 representing the highest priority and 7 the lowest. You can map each rule to one or more sets of clients, as determined by IP address, or to a protocol. Once the rules are in place, bandwidth contention is resolved by giving preference to the higher priority traffic.
## Classification Rules

Classification rules determine how bandwidth reservations or priority based forwarding is assigned to clients or applications, or both. You can define rules for any combination of the following assignments of bandwidth or priority:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Specify the protocol to which the rule applies. Default value of <code>any</code> indicates all protocols.</td>
</tr>
<tr>
<td>Source IP address</td>
<td>Specify the originating IP address or subnet (determined by subnet mask). Default value of <code>any</code> for the IP address means all addresses; default of <code>any</code> for the subnet mask means a 32-bit mask.</td>
</tr>
<tr>
<td>Destination IP address</td>
<td>Specify the terminating IP address or subnet (determined by subnet mask).</td>
</tr>
<tr>
<td>Source port</td>
<td>Indicate the device port that originates the traffic.</td>
</tr>
<tr>
<td>Destination port</td>
<td>Indicate the device port that terminates the traffic.</td>
</tr>
<tr>
<td>Preference</td>
<td>Determine relative precedence, if priority rules are conflicting. Positive numbers refer to user-assigned preferences, with lower numbers indicating higher preference. The default is 0.</td>
</tr>
</tbody>
</table>

Filter that operates on offsets measured from the beginning of the packet:

- **32-bit Word Offset**: Specify the number of bytes measured from the beginning of the packet.
  
  Example: Offset of 20 means that the filter will operate on the word that is 20 bytes (160 bits) from the beginning of the packet.

- **32-bit Word Value**: Enter the 32-bit hex value that is searched for in the word, subject to the filter
  
  Example: Search for hex string 1fccd123

- **32-bit Word Mask**: Enter the hex string that defines the filter
  
  Example: 00ff0000 means that the filter will mask all data except the third and fourth digits of the hex word, therefore, it will search for the hex string 1e in the third and fourth locations.
Use the QoS screen to configure QoS settings. Figure 41 shows the screen with bandwidth reservations selected, and Figure 42 shows the screen with priority based forwarding selected.

**Figure 41  QoS Screen with Bandwidth Reservations**

### QoS Configuration

<table>
<thead>
<tr>
<th>QoS Status</th>
<th>Stored</th>
<th>Committed</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS Policy</td>
<td>Enable</td>
<td>Enabled</td>
</tr>
<tr>
<td>Bandwidth-Reservation</td>
<td></td>
<td>Bandwidth-Reservation</td>
</tr>
<tr>
<td>Effective Wireless Rate (kbps)</td>
<td>1500</td>
<td>5500</td>
</tr>
</tbody>
</table>

**Note:** Effective Wireless Rate must take into account the average distance of clients (no. of hops) and the link quality/signal strength.

#### Traffic Reservation Classes

<table>
<thead>
<tr>
<th>Name</th>
<th>Rate (kbps)</th>
<th>Max Rate (kbps)</th>
<th>Priority</th>
<th>Add</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>1000</td>
<td>1100</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Elit</td>
<td>750</td>
<td>800</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Committed List of Traffic Reservation Classes**

<table>
<thead>
<tr>
<th>Name</th>
<th>Rate (kbps)</th>
<th>Max Rate (kbps)</th>
<th>Priority</th>
<th>Add</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>1000</td>
<td>1100</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Elit</td>
<td>750</td>
<td>800</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Classification Rules for Reservation

**Stored Packet Reservation Rules**

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Protocol</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Preference</th>
<th>32-bit Word Offset</th>
<th>32-bit Word Value</th>
<th>32-bit Word Mask (HexString)</th>
<th>Reservation Class Name</th>
<th>Add</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>0</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>AList</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DeptX</td>
<td>any</td>
<td>172.20.88.33</td>
<td>any</td>
<td>any</td>
<td>12.15.88.1</td>
<td>3</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>Elit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DeptY</td>
<td>any</td>
<td>10.22.73.44</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>3</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>AList</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Committed Packet Reservation Rules**

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Protocol</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Preference</th>
<th>32-bit Word Offset</th>
<th>32-bit Word Value</th>
<th>32-bit Word Mask (HexString)</th>
<th>Reservation Class Name</th>
<th>Add</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeptX</td>
<td>any</td>
<td>172.20.88.33</td>
<td>any</td>
<td>12.15.88.1</td>
<td>any</td>
<td>1</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>BList</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DeptY</td>
<td>any</td>
<td>10.22.73.44</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>3</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>AList</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configure QoS

1. Open the Tropos Configuration Utility.

2. Click QoS on the side menu to open the QoS screen.

   If QoS is currently disabled, only the QoS Status field is visible.

3. Select Enable in the QoS Status field, and click Store Changes.

   The QoS screen reopens with all fields displayed.

4. Select whether to use bandwidth reservations or priority based forwarding.
5. Enter the effective wireless rate estimated for your network.
6. Click **Store Changes**.
7. The entries you complete on the rest of the screen depend on whether you select bandwidth reservations or priority based forwarding.

   For bandwidth reservations:
   a. Enter a name for the reservation rule in the Traffic Reservation area.
   b. Enter the rate to be reserved in the Rate field and the maximum rate to be permitted in the Max Rate field. The unit are Kb/s.
   c. Enter a priority from 1 to 7 (1 is the highest priority; 7 is the lowest). This setting determines priority if any bandwidth reservation rules conflict.
   d. Click **Add**.
   e. In the Classification Rules for Reservation area, enter parameters as needed. See “Classification Rules” on page 102 for a description of the parameters.
   f. Click **Add**.

   For priority-based forwarding:
   a. Enter a name for the reservation rule in the Traffic Prioritization field, and select a priority from 1 to 7 (1 is the highest; 7 is the lowest).
   b. Click **Add**.
   c. In the Classification Rules for Reservation area, enter parameters as needed. See “Classification Rules” on page 102 for a description of the parameters.
   d. Click **Add**.
8. To implement the rules you have configured, click **Commit Changes** on the side menu.

### Configuring Rate Limits

Use the Rate Limiting screen, shown in Figure 43, to limit the bandwidth available to individual clients, thereby preventing some clients from taking up too much bandwidth. If the client transmits or receives too much data over a specified period of time, then client rate limits are triggered. The rate limits last a specified period of time, after which they are removed. The router triggers the rate limits again any time that the trigger settings are exceeded.
Figure 43  Rate Limiting Screen

<table>
<thead>
<tr>
<th>Rate Limiting Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Limiting Egregious Users</strong></td>
</tr>
<tr>
<td>This enforces a selective cap on anyone who exchanges too much data for too long. The caps are per association, so multiple IP behind the same bridge share a cap. This count 802.11 frame length, not just IP datagrams.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stored</th>
<th>Committed</th>
</tr>
</thead>
<tbody>
<tr>
<td>To client trigger (kbits)</td>
<td>40000</td>
</tr>
<tr>
<td>From client trigger (kbits)</td>
<td>40000</td>
</tr>
<tr>
<td>Trigger Time (seconds)*</td>
<td>20</td>
</tr>
<tr>
<td>To client cap (kbits/sec)</td>
<td>1000</td>
</tr>
<tr>
<td>From client cap (kbits/sec)</td>
<td>1000</td>
</tr>
<tr>
<td>Minimum cap duration (seconds)*</td>
<td>590</td>
</tr>
</tbody>
</table>

* rounded up to the nearest 10 seconds

| Store Changes |

**Differentiated Service Classes**

Only the first multiplier matched is used. This multiplier is for egregious users and fairness capping. Durations are unmodified.

**Stored**

<table>
<thead>
<tr>
<th>Subnet of client</th>
<th>Netmask</th>
<th>Multiplier</th>
</tr>
</thead>
<tbody>
<tr>
<td>255.255.0.0</td>
<td>1.0</td>
<td>Add</td>
</tr>
</tbody>
</table>

**Connected**

<table>
<thead>
<tr>
<th>Subnet of client</th>
<th>Netmask</th>
<th>Multiplier</th>
</tr>
</thead>
<tbody>
<tr>
<td>cornerstone</td>
<td>1.0</td>
<td></td>
</tr>
</tbody>
</table>

| Store Changes |

**Configure rate limits**

1. Open the Tropos Configuration Utility.
2. Click **Rate Limiting** on the side menu to open the Rate Limiting screen.
3. In the To client trigger field, enter the total quantity of data (kbits) that triggers the rate limit if the client receives that quantity of data in the time specified in the Trigger Time field.
4. In the From client trigger field, enter the total quantity of data (kbits) that will trigger the rate limit if the client transmits that quantity of data in the time specified in the Trigger Time field.

5. In the Trigger Time field, enter the length of time (seconds) used to determine whether to trigger rate limits.

6. In the To client cap field, enter the rate limit (kbits/sec) for data sent upstream by the client.

7. In the From client cap field, enter the rate limit (kbits/sec) for data sent downstream to the client.

8. In the minimum cap duration field, enter the number of seconds that the rate limit applies.

<<Need to add differentiated service classes.>>
This chapter contains information on how to keep Tropos routers working effectively. It contains information on the following topics:

- Viewing Equipment Status
- Viewing Current Configuration Settings
- Restarting the Tropos Router
- Managing Router Access
- Updating Software
- Managing Configuration Profiles
- Configuring SNMP and Trap Settings
- Generating SSL Certificates
- Viewing Event Logs

**Note**
A command line interface (CLI) is also available for maintenance and diagnostics. For further information, see the *Tropos Networks Configuration Reference Guide*. 
**Viewing Equipment Status**

The operational lights on the Tropos router provide information on whether the unit is powered and communicating over the network.¹

**Tropos 5210, 4210, and 5110 Routers**

Each Tropos 5210, 4210, and 5110 router has a light or LED status indicator that turns green when the router is operational. Figure 44, Figure 45, and Figure 46 show the locations of the status indicator.

- When the router is plugged in and has power, the status indicator is red.
- When the router has a working IP address and network connectivity, the status indicator is green.

**Figure 44  Location of Tropos 5210 Status Indicator**

---

¹ It may be necessary for some older clients to renew their DHCP leases in order to reassociate to a Tropos router after the router has been rebooted.
Figure 45 Location of Tropos 4210 MetroMesh Router Status Indicator

Figure 46 Location of Tropos 5110 Status Indicator
Operational Lights on Indoor Tropos Routers

Figure 48 shows the location of the operational lights on the Tropos 3210 router, and Figure 48 shows the lights on the Tropos 3110 router.

Figure 47 Location of operational lights on the Tropos 3210 router

The green Power LED on the Tropos 3210 router is located towards the left and remains on while the unit is powered. The red signal strength LED shows the strength of the network connection. The Net LED flashes to indicate network traffic, and the Disk LED flashes when the flash boot memory is accessed.

Figure 48 Location of operational lights on the Tropos 3110 router

The green power light on the Tropos 3110 router is located towards the left of the unit. It remains lit while the unit is powered. The red LED to the right of the power light shows the strength of the network connection. The LEDs for the Management port and the LAN port show whether connectivity has been established over those ports, and they blink when traffic is moving through the ports.

When you boot the Tropos gateway, the following sequence takes place.

1. The green power LED turns on, the signal strength LED remains off.
2. When the unit begins to obtain network settings, the signal strength LED turns solid red.
3. Once the unit has obtained network settings and is fully operational, the red signal strength LED begins flashing, and continues to do so during normal operation.
When you boot the Tropos node, the following sequence takes place.

1. The green power LED turns on, the signal strength LED remains off.
2. When the unit begins to obtain network settings, the signal strength LED turns solid red.
3. Once the unit is fully operational, the red signal strength LED flashes to indicate the strength of the optimal path connection back to the wired network.
   - If there is no connection, the LED is solid red.
   - If there is a connection, the speed of the blinking red light indicates its strength, with faster blinking indicating a stronger connection.

**Note**

If the unit is a Tropos Gateway, the unit converts to Tropos node operation if the LAN cable is not connected.

### Viewing Current Configuration Settings

You can view current Tropos router configuration settings at any time from the Tropos configuration utility. For detailed information on each field contained on the screen, refer to the *Tropos Networks Configuration Reference Guide*.

The Current Configuration screen contains an auto-refresh setting. If auto-refresh is enabled, the information on the Current Configuration screen is updated every 10 seconds. Auto-refresh is off by default.

**View the current configuration**

1. Open the Tropos Configuration Utility.
2. Select **Current Config** from the side menu to open the Current Router Configuration screen (Figure 49).
3. Scroll down to find the desired settings.
4. To use the auto-refresh option, click **Turn It On** at the top of the screen. To disable auto-refresh, click **Turn It Off** at the top of the screen.
Figure 49 Current Router Configuration screen (Excerpt)

Current Cell Configuration

Auto-refresh: OFF  Turn it on

<table>
<thead>
<tr>
<th>Cell Setting</th>
<th>Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Software Version</td>
<td>6.1.0.2</td>
</tr>
<tr>
<td>Board Type</td>
<td>2210</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Setting</th>
<th>Status</th>
<th>PoE Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN (eth0)</td>
<td>10baseT-HD</td>
<td>no link</td>
<td>Disabled</td>
</tr>
<tr>
<td>Management (eth1)</td>
<td>10baseT-HD</td>
<td>no link</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Restarting the Tropos Router

Use the Restart screen, shown in Figure 50, to reboot the Tropos router or restart the software. When you reboot the router, the hardware and software are restarted. When you restart the software only, the hardware remains powered on.

Figure 50 Restart screen

Restart the Tropos software or hardware

1. Open the Tropos Configuration Utility.
2. Click Restart on the side menu.
3. To restart the router software, click Software Restart, and click OK when prompted to confirm.
4. To restart the software and hardware, click System Reboot, and click OK when prompted to confirm.
Caution
Ensure that the router does not lose power during the restart operations and for five minutes thereafter. The router requires sufficient time to fully restart all software processes. Loss of power during this interval may result in corruption of the software.

Managing Router Access

Use the Security Management screen, shown in Figure 51, to set the administrative password and control access to the router command line interface.

The Upload Public Key option allows you to upload SSH public keys for access to the router CLI.

Figure 51 Security Management screen

<table>
<thead>
<tr>
<th>Security Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stored</td>
</tr>
<tr>
<td>Administration Password</td>
</tr>
<tr>
<td>Re-enter Administration Password</td>
</tr>
</tbody>
</table>

Admin Public Key Upload

Stored public key:

Committed admin public key:

You have to upload a public key to use the admin cli interface.

Public Key Filename [Browse...]

Upload Public Key
Assign the administrative password

1. Open the Tropos Configuration Utility.
2. Click Security on the side menu.
3. Enter and confirm the administrator password in the Admin Password boxes.
4. Click Store Changes. Make sure to commit the change when you have finished.
Upload a public key for CLI access

1. Open the Tropos Configuration Utility.
2. Click Security on the side menu.
3. Click the Browse button, and select the file that contains the public key.
4. Click Upload Public Key.

Restoring the Default Password

You can restore the factory default password on the Tropos router by contacting Tropos Customer Support at 1-877-987-6767. Record the serial number of the Tropos router before calling.

Updating Software

Use the Software Update screen (Figure 52) to install a new software image in the Tropos router. The screen also displays the current software version.

To provide for easy software upgrade and restoration, the Tropos router stores two copies of the software image. The primary image is the image that is normally used when you reboot the router. When you upgrade the software image, the uploaded software file is loaded as the secondary image. After the image is installed, the system automatically boots the newly installed image. To roll back to the older image, set the field entitled “Boot other image at next boot” to Yes before restarting the router.
When upgrading, begin with end nodes and work back towards the gateways to minimize disruption to the network during the upgrade process. Keep at least one gateway running while upgrading the other gateways and nodes.

**Install a new software image**

1. Open the Tropos Configuration Utility.
2. Click **Software Updates** on the side menu.
3. Click **Browse**, and navigate to the location of the software image.
4. Click **Upload Software Image**.
5. When you see a message stating that the software image was successfully uploaded (see Figure 53), click **Install Software**.

**Figure 53  Software Update Screen After Successful Upload**
The software is automatically installed and the screen automatically refreshes every few sections to display the progress of the installation (Figure 54).

**Figure 54 Software Install Progress Messages**

```
Software Install
Software image was successfully uploaded!!!
Uploaded Software Version 4.0.0.0
Install

10:54:24 install begin
10:54:24 calling set-config-version 1 4.0.0.0
Success
10:54:24 making a new file system...
10:54:25 mounting the new file system...
10:54:25 uncompressing the uploaded image...
10:56:12 syncing the partition...
10:56:21 verifying the checksum...
```

When the process is complete, you can log in to the Configuration Utility again.

**Note**

While installing software, make sure that the router does not lose power during the operation and for five minutes following. The router requires sufficient time to fully restart all software processes. If you refresh your browser during installation, you may see a "Page cannot be found" screen. This is normal, since the web session must be interrupted for the router to reboot with the new software image.

**Roll back to the older stored image**

1. Set Boot other image at next boot to **Yes**.
2. Click **Store Changes**. When you have finished, click **Commit Changes** on the side menu.
3. Click **Restart** from the side menu.
4. Click **System Reboot**, and click **OK** when prompted to confirm.

**Managing Configuration Profiles**

Use the Profile Management screen, shown in Figure 55, to perform the following tasks:

- Upload a previously saved configuration file to the Tropos router.
- Bundle the configuration files resident on the Tropos router and download them to your computer.
Caution
Configuration profiles saved in previous releases of Tropos software are not compatible with newer versions. The router may not function properly if an unsupported profile is uploaded. To avoid this problem, always define new profiles after upgrading the system software.

- Restore the factory default profile.

Figure 55 Profile Management screen

Upload a configuration to the Tropos router
1. Open the Tropos Configuration Utility,
2. Click Profiles on the side menu.
3. Click Browse and select the configuration file to be uploaded to the router.
4. Click Export Committed Profile.
Download a configuration file from the Tropos router

1. Click Save Configuration.
2. Browse to select a location for the saved file.
3. Click Save.

Restore the factory default profile

1. Click Restore Factory Default Profile.
2. Click OK when prompted to confirm.

Configuring SNMP and Trap Settings

Use the SNMP screen, shown in Figure 56, to configure the SNMP MIB and trap settings for the Tropos gateway.

To use Tropos Control to manage the Tropos router, you must register Tropos Control to allow SNMP access to the router and to receive SNMP traps. This allows you to access the SNMP MIBs and use Tropos Control. In addition, registering the IP address causes SNMP traps 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 traps.

As a security precaution, when you specify the IP address for Tropos Control, the system prompts you to change the SNMP read/write community strings.

Table 8 lists the SNMP traps.

Note
The IP address 1.1.1.1 is reserved and should never be assigned for use on the Tropos router or SNMP trap assignment.
Figure 56  SNMP Configuration screen

<table>
<thead>
<tr>
<th>SNMP Configuration</th>
<th>Stored</th>
<th>Committed</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Read Community</td>
<td>public</td>
<td>public</td>
</tr>
<tr>
<td>SNMP Read/Write Community</td>
<td>private</td>
<td>private</td>
</tr>
</tbody>
</table>

Store Changes

EMS Registration

<table>
<thead>
<tr>
<th>IP</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Add</td>
</tr>
</tbody>
</table>

Committed EMS Registration

<table>
<thead>
<tr>
<th>IP</th>
</tr>
</thead>
</table>
Configure SNMP and register Tropos Control

1. Open the Tropos Configuration Utility
2. Click SNMP.
3. Enter the SNMP Read/Write community.
4. Enter the IP addresses of all machines with MIB browsers that need to access the MIB for this gateway. This must include the IP address of the Tropos Control EMS server, if Tropos Control is used in the network.
5. Click Add after each addition.
6. Continue adding machine addresses as needed.
7. When you have finished, commit the changes you have made.

Note
By default, SNMP MIB access is blocked. It must be explicitly allowed in the Configuration Utility.

Delete IP addresses for SNMP

1. Click the Delete button to the right of the address.
2. When you have finished, commit the changes you have made.

Note
Remember to commit changes that you have stored by selecting Commit Changes on the side menu. Include a time delay, if desired.

Table 8 SNMP Traps and Tropos Control

<table>
<thead>
<tr>
<th>Event Name Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abort Changes</td>
<td>This event is generated when a change made by an operator is aborted.</td>
</tr>
<tr>
<td>About to Commit Changes</td>
<td>This event is generated when a change made by an operator is about to be committed.</td>
</tr>
<tr>
<td>Battery Failed</td>
<td>This event is generated when a battery fails to emit a signal</td>
</tr>
<tr>
<td>Switch to Battery</td>
<td>This event is generated when a node is switched to battery power</td>
</tr>
<tr>
<td>Commit Changes</td>
<td>This event is generated when a change made by an operator on the configurator is committed.</td>
</tr>
<tr>
<td>Configurator Login Failed</td>
<td>This event is generated when a login attempt to the configurator on a particular node is unsuccessful.</td>
</tr>
<tr>
<td>Configurator Login Success</td>
<td>This event is generated when a login attempt to the configurator on a particular node is successful.</td>
</tr>
</tbody>
</table>
### Table 8  SNMP Traps and Tropos Control (continued)

<table>
<thead>
<tr>
<th>Event Name Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node Install New Software</td>
<td>This event is generated when new software is installed.</td>
</tr>
<tr>
<td>Node Reset Factory Default</td>
<td>This event is generated when the settings on a node are reset to their factory defaults.</td>
</tr>
<tr>
<td>Node Soft Start</td>
<td>This event is generated when the software on a node is restarted.</td>
</tr>
<tr>
<td>Node Becomes Gateway</td>
<td>This event is generated when a node starts functioning as a gateway within the network</td>
</tr>
<tr>
<td>Node Belongs to Foreign Gateway</td>
<td>This event signifies the node has roamed to a gateway that has not been discovered by EMS</td>
</tr>
<tr>
<td>Node Reachability</td>
<td>This event indicates the state of IP connectivity to the node</td>
</tr>
<tr>
<td>Duplicate Trap</td>
<td>This event is generated if the Tropos Control software detects a duplicate SNMP trap has been generated by a gateway.</td>
</tr>
<tr>
<td>Out of Sequence Trap</td>
<td>This event is generated if the Tropos Control software detects a SNMP trap generated by a gateway which has a trap sequence number less than the last sequence number received from that gateway.</td>
</tr>
<tr>
<td>Lost Traps</td>
<td>This event is generated if the Tropos Control software receives an SNMP trap with a sequence number that indicates traps have been generated by that gateway which were not received by the management station.</td>
</tr>
<tr>
<td>Device Changed IP Address</td>
<td>This event is generated when the Tropos Control software detects that a node has changed its IP address.</td>
</tr>
<tr>
<td>Node Lost Redundant Paths</td>
<td>This event is generated when the Tropos Control software detects that a node no longer has any redundant paths.</td>
</tr>
<tr>
<td>Discovery Error</td>
<td>This event is generated when configuration problems prevent the discovery processes from completing successfully.</td>
</tr>
<tr>
<td>Device Discovery Failure</td>
<td>This event is generated when errors were encountered during the discovery of a particular device. Causes of this error are things like SNMP timeouts.</td>
</tr>
<tr>
<td>Display Name Not Unique</td>
<td>This event is generated when the display name configured for a particular device is not globally unique within the network.</td>
</tr>
<tr>
<td>Display Name Not Set</td>
<td>This event is generated when the display name for a node is not set in its running MIB configuration. The alarm associated with this event is cleared by the Tropos Control software when the display name is set.</td>
</tr>
<tr>
<td>EMS link Generation</td>
<td>This event is generated when the node is orphaned, and EMS attempts to generate the link based on the information on the node.</td>
</tr>
</tbody>
</table>
Generating SSL Certificates

Secure Sockets Layer (SSL) is a standard security protocol for Internet networks. With SSL, a network server responds to a client request for secure communications by opening an encrypted port. Public-key encryption-based methods are then used to establish an authenticated handshake connection between server and client. This process requires an SSL encryption certificate, which is the means of assuring that the public-encryption key used for authentication actually belongs to the targeted owner.

Use the Certificate screen, shown in Figure 57, to generate an encryption certificate for secure SSL communications. In the name field, enter the IP address or fully resolved name you plan to use to access the Configuration Utility on the Tropos router. This assures that any external servers are presented with the correct certificate when accessing your wireless network.

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Latitude Longitude Not Set</td>
<td>This event is generated when the latitude and longitude values are not set for a device in its running MIB configuration. This alarm associated with this event is cleared by the Tropos Control software when the latitude and longitude values are set.</td>
</tr>
<tr>
<td>SNMP failure</td>
<td>EMS detected that SNMP agent on the node is not responding, possibly due to network overloaded or wireless path quality is poor.</td>
</tr>
</tbody>
</table>
**Generate an encryption certificate**

1. Open the Tropos Configuration Utility.
2. Click **Certificate** on the side menu.
3. In the Certificate Name field, enter the IP address or fully resolved name to access the router’s Tropos Configuration Utility.
4. Enter your company name, organization, location, state, and 2-character country code.
5. Enter a contact name or email address.
6. Click **Store Changes**. Make sure to commit the changes when you have finished.

**Viewing Event Logs**

The Logging screen, shown in **Figure 58**, contains links to the current statistics and event logs for each client directly associated to the Tropos router.
Open the log files

1. Click **Logging** on the side menu.
2. Click the link for the desired log file.

The following choices are available. For a full description of the logging files, refer to the *Tropos Networks Configuration Reference Guide*.

- **Click Current This Node Stats** to display statistics for this Tropos router. One row of node statistics is generated each minute. Example:

```
Wed Dec  8 16:01:26 2004;172.20.125.53;00:0D:97:00:10:6F;172.20.125.60;172.20.125.60;1;0.825000;0.825000;0.825000;0.574000;35;-66;-101;35;2147483647;1150303275
Wed Dec  8 16:02:26 2004;172.20.125.53;00:0D:97:00:10:6F;172.20.125.60;172.20.125.60;1;0.843750;0.843750;0.843750;0.731000;36;-66;-102;36;2147483647;1150464484
```

- **Click Current Clients Stats** to display statistics for all clients associated to this Tropos router. Each minute a row is generated for each wireless clients associated to this Tropos router. Example:

```
Fri May 28 13:43:42 2004;;172.20.125.41;00:02:2D:57:8F:D9;3;1;;Fri May 28 09:07:15 2004;Fri May 28 13:43:35 2004;371643;680396;67;-66;-88;22
Fri May 28 13:44:42 2004;;172.20.125.41;00:02:2D:57:8F:D9;3;1;;Fri May 28 09:07:14 2004;Fri May 28 13:43:55 2004;373335;682682;66;-66;-81;15
```

- **Click Current Event Log** to display the list of notable occurrences with date and time stamp. Events are maintained in this file until the maximum size (200KB) is reached, and then older event information is deleted as needed. Example:

```
May 13 11:36:35 flagship lookupd: 1084473395;1:00:02:6f:03:87:35
May 13 11:36:36 flagship lookupd: 1084473396;1:00:02:6f:03:87:35
May 13 11:38:35 flagship lookupd: 1084473515;1:00:02:6f:03:87:35
```
3. Click **Current Neighbor Stats** to display information on Tropos routers downstream and within radio range of this router. Example:

```
Wed Dec 8 16:01:20
2004;;172.20.125.53;00:0d:97:00:10:6f;0;955012907;168549301;26;-75;-101;26
```

```
Wed Dec 8 16:01:20
2004;;172.20.125.74;00:0d:97:00:10:6c;0;1063831630;238466800;47;-54;-101;47
```
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.

Autonomous System (AS)
Collection of networks under a single administrative structure.

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.

Basic Service Set (BSS)
The set of all wireless client stations controlled by a single Tropos MetroMesh router. The BSS is identified by the BSS identifier (BSSID), often the MAC address of the router.

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.

Domain Name Service (DNS)
Standard used to convert alphanumeric Internet domain names to IP addresses.
**Downstream sub-interface**
Connection of a wired interface to the management port on the Tropos MetroMesh router, in order to provide wired network service in the area covered by the wireless network.

**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.

**Extended Service Set (ESS)**
A wireless network which consist of multiple Tropos routers, each of which provide 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.

**Gateway**
Tropos router that connects directly to the wired network and provides backhaul for downstream Tropos nodes and clients.

**Hypertext Transfer Protocol (HTTP)**
Protocol that manages data transfers between web browsers and servers.

**Hypertext Transfer Protocol over SSL (HTTPS)**
Secure version of HTTP that 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, and which 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 Time Protocol (NTP)
Method of synchronizing clocks on network devices.

Node
Tropos router that provides delivers 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 (PWPR)
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.

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. Network initiated roaming detects clients that lose uplink to a node and forces them to associate to another neighboring node. Tropos supports client initiated roaming throughout the wireless routing domain. It can also be configured to support network initiated roaming.

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 fea-
ture 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 trap**
Process to save or drop specific types of SNMP messages.

**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 shared many commons attributes with TCP but without the reli-
ability capabilities of TCP. UDP is often used for applications that can toler-
ate 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.

**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 Network, or Wireless Local Area Network (WLAN)**
Local area network based on 802.11 wireless communications.
Index

Numerics
128-bit WEP key 34
2.4 GHz band 31
64-bit WEP key 34
802.11 3, 128
802.11b 31
802.11b/g 3
802.11g 31
802.1x 32

A
AAA server
  definition 128
access
  allowing and denying 78
  accessing
    Configuration Utility 11
    Configuration Utility through wireless connection 27
Advanced Encryption Standard. See AES
AES 33
AES encrypt forwarded packets 35
antenna diversity 36
AS 128
ascii key 34
attenuation 36
authentication
  open 34
  auto-detection of static clients 81

B
backhaul 128
Basic Service Set. See BSS
beacon interval 35
beacon rate 35
bring up threshold 64
BSS 30, 128

C
certificates, SSL 124
channels 31
client access
  description 78
  more than 10 clients 79
  client DHCP relay policy 93
  client initiated roaming 35
  client security 32
  client stats 126
  clients
    adding to the network 20
    allowing access 78
    configuring 20
    denying association 79
    static IP 81
    Windows NT or 2000 23
    Windows XP 21
  cluster 2
  configuration
    basic network 43
    download 120
    downloading 118
    managing profiles 118
    upload 119
    uploading 118
    viewing current 112
  configuring
    clients 20
    DHCP settings 43
    gateway 9
  NAT 53
  network settings 41
  new network 8
  SNMP traps 122
  uplink check 64
  wired ports 57
  wireless settings 30, 37
  connectivity loss 64
  current configuration 26, 112
  viewing 112
  current event log 126
  custom protocols 88
  customer premise equipment (CPE) 81

D
data rates 31
  default
    configuration 8
    ESSID 30
    profile 120
  deny
    client association 79
  packet filter forwarding 83
  DHCP
    and NAT 47
    bypass 52
    configuring 43

E
EAP 32
ESS 30, 129
ESSID 30
  definition 129
  multiple 35
  suppression 30
  ESSID-based VLANs
    and client DHCP relay policy 93
    description 90
    guidelines 92
  eth0, eth1 57
  Ethernet speed and duplex settings 57
  event log 126
  event logs 125
  Extended Service Set. See ESS

F
factory default profile 120

G
gateway
  definition 129
  list 71
  reassigning 24
gateways 2
getting started 8

H
hardware restart 113
hexadecimal key 34
HTTP
definition 129
packet filtering 88
HTTPS
definition 129
packet filtering 88
Hypertext Transfer Protocol over SSL. See HTTPS
Hypertext Transfer Protocol. See HTTP

I
ICMP
definition 129
packet filtering 88
Internet Control Message Protocol over SSL. See ICMP
Internet Protocol Security. See IPSec
IP
client device address 24
reserved 1.1.1.1 address 42
IP-based VLANs
and client DHCP relay policy 93
description 91
guidelines 92
IPSec
definition 129
packet filtering 88

L
LAN port 57
layer 2 emulation 42, 62
restrictions 63
lease duration 49
LEDs 111
logs
client stats 126
current event 126
description 125
neighbor stats 127
this node stats 126
loss of connectivity 64

M
MAC address
configuring filters 77
definition 130
DHCP filters and reservations 74
removing filters 77
management port 57
management VLAN 90
Maximum Transmission Unit. See MTU
Media Access Control. See MAC
meshed cluster 2, 130
mobile node 130
MTU 58, 130
multiple DHCP servers 50
multiple ESSIDs 35
multi-subnet roaming 70
and VLANs 70, 72
example 73
gateway list 71

N
NAT
and DHCP 47
configuring 53
definition 130
options 41
restrictions 53
with DHCP configuration 54
with static configuration 54
neighbor stats 127
netmask 130
Network Address Translation. See NAT
network initiated roaming 35
network management and administration 7
network settings, configuring 41
Network Time Protocol. See NTP
node 130
node stats 126
nodes 2
adding to the network 15
reassigning 24
NTP
definition 130
packet filter example 88
using with time setting 28

O
open authentication 34

P
packet filter
deny forwarding 83
example 88
forwarding rules 83
hit counts 89
permit forwarding 83
protocols and ports 88
Packet Success Probability. See PSP
password
changing 115
restoring default 116
permit, packet filter forwarding 83
ping 130
PoE 65
POP3 88
ports
management and LAN 57
packet filtering 88
Post Office Protocol 3. See POP3
power levels 36
Power Over Ethernet. See PoE
Predictive Wireless Routing Protocol. See PWRP
pre-shared key 33
primary ESSID 35
primary software image 116
product
features 1
product overview 1
profiles 118
protocols and ports 88

R
RADIUS
accounting interval 33
accounting port 33
accounting secret 33
and 802.1x 32
authentication port 33
authentication secret 33
server 33
reassigning gateways and nodes 24
re-clustering 61
relay policy 93
relaying DHCP requests 52
Remote Authentication Dial-in User Service. See RADIUS
restarting
software or hardware 113
Tropos router 113
RJ45 connectors 9
roaming 35
definition 131
multi-subnet 70
router identity 25
router-router security 34
router-router transmission rate 31
Tropos Networks User Guide

routing, in a Tropos network 3

S
secondary ESSID 36
secondary software image 116
Secure Shell See SSH
secure sockets layer (SSL) 131
security
  client 32
  overview 32
service set identifier 131
service sets 30
Simple Mail Transfer Protocol. See SMTP
Simple Network Management Protocol. See SNMP
SMTP
  definition 132
  packet filtering 88
SNMP 120
  definition 132
  MIB 120
  packet filtering 88
  traps (table) 122
  traps, definition 132
software
  restart 113
  updating 116
  uploading image 117
SSH
  definition 131
  packet filtering 88
SSL certificates 124
static IP
  client auto-detection 81
  clients 81
  manually configured clients 81
static IP address 132
status indicator light 9, 15
sub-interface
  definition 129
subnet 132
subnet mask 130, 132
subnets, dual support 55
suppressing ESSID 30

T
take down threshold 64
telnet
  example 88
  packet filtering 88
Temporal Key Integrity Protocol. See TKIP
time
  manual setting 28
  setting 28
  TKIP 33
  TLS 32
Transmission Control Protocol/Internet Protocol (TCP/IP) 132
transmission rates 31
transmit antenna diversity 36
Transport Layer Security. See TLS 132
traps 120
Tropos Configuration Utility 1
  accessing 12
  preparing to access 11
Tropos Control Element Management System (EMS) 1, 7
Tropos network
  adding clients 20
  adding nodes 15
  operation 3
  routing 3
Tropos Operating System 1
Tropos router 1, 131
  operational lights 109, 111
  power-on sequence 111
  TTLS 32
Tunneled Transport Layer Security. See TTLS 132

U
Universal Time Coordinated. See UTC
uplink check 42, 64
  bring up threshold 64
  take down threshold 64
User Datagram Protocol (UDP) 132

V
virtual local area network. See VLAN
Virtual Private Network (VPN) 133
VLAN
  client DHCP relay policy 93
  configuring interfaces 98
  ESSID-based 90
  guidelines 92
  ID 89
  interfaces 98
  IP-based 91
  management 90
  overview 89
  tags 89
  with multi-subnet roaming 70, 72