Sensys Networks VDS240 Wireless Vehicle Detection System

TrafficDOT 2 Set Up and Operating Guide

P/N 152-240-001-038 Rev B
November 2011

Sensys Networks, Inc.
2560 Ninth Street, Suite 219
Berkeley, CA 94710
www.sensysnetworks.com

Contents

Document Properties

This document is reference material for the Sensys Networks VDS240 wireless vehicle detection system from Sensys Networks, Inc.

P/N 152-240-001-038 Rev B

Regulatory Statements

FCC Compliance Statement

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications to this product not authorized by Sensys Networks could void the EMC compliance and negate the authority to operate the product.

RF Exposure Statement

This device has been tested and meets the FCC RF exposure guidelines. It should be installed and operated with a minimum distance of 20 cm between the radiator of RF energy and the body of users, operators or others.

Improper use or tampering with the device is prohibited and may not ensure compliance with FCC exposure guidelines.

Warnings

No Safety Switching

Sensys Networks does not allow its equipment to be used for safety applications such as controlling a mechanical gate or switching a train to avoid a collision.

Lithium Thionyl Chloride Batteries

Sensys Networks uses Lithium Thionyl Chloride batteries in the following products:

- Sensors (VSN240-F, VSN240-T, VSN240-S)
- Repeaters (RP240-B, RP240-BH, RP240-B-LL, and RP240-BH-LL)

Lithium batteries are widely used in electronic products because they contain more energy per unit -weight than conventional batteries. However, the same properties that deliver high energy density also contribute to potential hazards if the batteries are damaged. Improper use or handling of the batteries may result in leakage or release of battery contents, explosion or fire.

Following are the recommendations of the battery manufacturer for proper use and handling of batteries in the Sensys Networks devices mentioned above:

- **DO NOT** charge or attempt to recharge the batteries (batteries are NOT rechargeable)
- **DO NOT** crush or puncture batteries
- **DO NOT** short-circuit the batteries
- **DO NOT** force over-discharge of the batteries
- **DO NOT** incinerate or expose batteries to excessive heating
- **DO NOT** expose battery contents to water
- **DO** dispose of batteries and devices containing batteries in accordance with local regulations

Note: Sensys Networks wireless sensors contain no serviceable parts and should never be disassembled. Installation and removal of sensors from pavement should only be done by trained personnel and care should be taken to insure that the sensor casing is not punctured or crushed.

Additional safety information is available from the battery's manufacturer:

- Sensor battery cell: http://www.able-battery.com/msds/ABLE_MSDS_ER14505.pdf
- Repeater battery cell: http://www.able-battery.com/msds/ABLE_MSDS_ER34615.pdf

Document Control

Sensys Networks continually reviews and revises its technical publications Please address questions, suggestions or corrections to support@sensysnetworks.com.

Contact Information

Sensys Networks, Inc.
2560 Ninth Street, Suite 219
Berkeley, CA 94710 USA
+1 (510) 548-4620
www.sensysnetworks.com

CHAPTER 1

Introduction

This guide provides information and procedures for installing and configuring TrafficDOT 2 in conjunction with the Sensys Networks VDS240 wireless vehicle detection system. This document is intended to be used by Sensys Networks customers, consultants, partners, dealers, and those who are interested in the application of wireless communication technology to the challenges of traffic detection, management and control.

What's Inside

This guide includes the following information:

- Chapter 1: *Introduction*, provides the purpose and scope of the guide, as well as an overview of each chapter. This chapter also provides the differences between the previous release of TrafficDOT.
- Chapter 2: *Understanding TrafficDOT*, describes the configuration, management, and monitoring functions of TrafficDOT.
- Chapter 3: *Installing TrafficDOT*, provides TrafficDOT hardware requirements, and an overview of the application's installation process.
- Chapter 4: *Using TrafficDOT*, provides information and instructions on using TrafficDOT to create a system network.
- Chapter 5: *Configuring and Managing Components*, provides information and instructions required to configure and manage Sensys Networks VDS240 Vehicle Detection system components using the map view.
- Chapter 6: *Monitoring Components Using the Table View,* provides information on monitoring system components using the table view.
- *Appendix*: Provides the information required to configure cellular modems on either an access point or access point controller card (APCC).

Differences From Prior Versions

This release of TrafficDOT 2 differs from prior versions. The principal changes are:

Map View

This release implements both a *map* and *table* view of the Sensys Networks components. The map view allows you to select a map from a library of common intersection schematic images or import a map image of your own, draw an intersection layout using basic drawing tools, configure and monitor key components, and access all features from individual components.

Graphical representation of drag and drop elements

This release provides graphical representations of sensors, access points, repeaters, and contact closure cards that can be dragged and dropped into place for real-world deployment.

Graphical lane creation

This release allows you to draw a representation of an intersection layout using lane creation tools. This feature provides you with the ability to assign a lane direction, adjust length and width, and add text to name streets and intersections.

Informative banner information

This release provides a banner at the top of the screen that displays the IP address and intersection name.

Color-coded sensors

This release implements color-coded sensors. The colors (red, yellow, and green) indicate sensor status, and alerts you that attention may be required, such as if the battery level drops or there is a time slot conflict. When detection is present the sensor color is black.

Unmap, Delete, and Revert

This release introduces two new concepts: *Unmap* and *Revert*. When working in the map view of the application, you must unmap a component to remove it from the map. Unmapping a component does not delete it from the Dot Table. Once a component is unmapped, it will appear in the components tray at the bottom of the screen. *Delete* is used to remove a component for the Dot Table, and Revert, which only works before you click *Apply*, restores a component to its condition prior to configuration.

Other Documents

The following product-related documentation is available from Sensys Networks.

General and Reference Information

- *Sensys Networks VDS240 Wireless Vehicle Detection System Reference Guide*

Freeway and Arterial Applications

- *Design Guidelines for Freeway & Arterial Applications*
- *Configuration Guidelines for Freeway & Arterial Applications*
- *Installation Guidelines for Freeway & Arterial Applications*

Intersection Applications

- *Design Guidelines for Intersection Applications*
- *Configuration Guidelines for Intersection Applications*
- *Installation Guidelines for Intersection Applications*

Installation and Maintenance Procedures

- *Wireless Sensor Installation Guide*
- *Access Point Installation Guide*
- *Repeater Installation Guide*
- *Contact Closure Card Installation Guide*

Sensys Networks Management Server

- *SNAPS Professional Set Up and Operating Guide*

Readers of this document are encouraged to contact Sensys Networks, Inc. (www.sensysnetworks.com) for the latest information, design guides, and best practices.

Chapter 2

Understanding TrafficDOT

This chapter describes the *configuration*, *management*, and *monitoring* functions of TrafficDOT 2.

Overview

TrafficDOT 2 is an Adobe® Flex, Windows-based application that is used in conjunction with wireless vehicle detection systems from Sensys Networks, Inc. A Sensys Networks wireless vehicle detection network uses a collection of magnetic sensors embedded in roadway pavement to detect the presence and passage of vehicles such as cars, trucks, trains, motorcycles, bikes and others. Detection events are transmitted by wireless radio to Sensys Networks access points that function as management nodes, data collection points, and packet forwarders for the network.

TrafficDOT is a configuration manager and monitoring tool for an access point and all its associated devices (sensors, repeaters, and contact closure cards). TrafficDOT 2 provides a graphical user interface (GUI) to the network's devices, settings, and operations. The GUI simplifies both configuration and management of installations.

TrafficDOT is independent of the firmware resident in sensors, access points, repeaters and contact closure cards. As a result, it can be updated to a newer version without affecting any installed devices. However it is typical for TrafficDOT versions to mirror the functionality of device firmware so it is common to update device firmware and TrafficDOT at the same time.

Configuring Equipment With TrafficDOT

TrafficDOT uses industry standard TCP/IP communications and makes a connection to an access point in one of the following ways:

- *Connection via a wired network path* – for example, bench configuration prior to installation, field access based on patching a technician's laptop to the access point via an Ethernet cable, or an available wide area network connection.
- *Connection via a wireless network path* – for example, using GSM cellular networks

(EDGE/GPRS data services) or CDMA cellular networks (1xRTT data services).

- *Proxied connection via a proxy server* (such as a Sensys Networks management server)

Configuration settings are made via TrafficDOT's GUI to the access point which, in turn, stores its settings in its local and/or memory and/or transmits them to remote sensors and repeaters via the RF channel and to controller interface cards via the required cabling.

Configuration Functions

Configuration of network equipment is accomplished with the following TrafficDOT functions:

- Configuring an access point
- Configuring sensors
- Configuring repeaters
- Configuring contact closure cards
- Configuring system properties
- Configuring settings for events, detection thresholds, reporting, etc.

Management Functions

TrafficDOT contains other functions that are not related to configuration, such as network management. The management functions are as follows:

- Forming a network by associating devices (sensors, repeaters, and contact closure cards) to an access point
- Rebooting an access point
- Updating a sensor, access point, repeater, or contact closure card's firmware

> ***Note***: TrafficDOT is independent of the firmware resident in sensors, access points, repeaters and contact closure cards. As a result, it can be updated to a newer version without affecting any installed devices. However it is typical for TrafficDOT versions to mirror the functionality of device firmware, so it is common to update device firmware and TrafficDOT at the same time.

- Backing up and restoring an access point's configuration
- Reviewing the processes executing on an access point
- Updating an access point's license file
- Discovering the network's topology
- Maintaining information about sensor location

- Produce online graphs of detection experience

See the *Configuring and Managing Components* chapter for more information.

Monitoring Detector Device Health and Performance

TrafficDOT provides a central monitoring station capable of evaluating the health and performance of up to 96 individual detector network devices. The following capabilities are available:

- *Graphical depiction of network health* – health of remote networks depicted by color-coded health-state icons
- *Radio communications status* – display of wireless signal strength (RSSI) and link quality (LQI) for all devices
- *Battery level* – effective battery output displayed for repeaters and sensors

Remotely Managing Detector Networks and Device Properties

TrafficDOT allows access to detector network devices for configuration and testing without requiring a visit to the physical location of the network. The following capabilities are available:

- *Centrally manage all Sensys Networks devices* – contact access points by unique IP address, issue configuration/management commands. A VPN service allows connections to be made over GPRS , CDMA, Ethernet or other backhaul channels.
- *Execute commands on device groups* – send the same configuration/management commands to multiple access points as members of a management group
- *Remote firmware updates* – update device firmware from remote location
- *Multiple concurrent sessions* – supports multiple simultaneous connections to a single access point
- *Remote backup/restore operations* – backup/restore access point configuration from remote location
- *Process & license management* – stop/start local access point processes and update access point license from remote location

Configuring Complex Deployments in Advance of Installation

TrafficDOT allows detector networks to be configured before devices are installed at the job site. This can improve communication between entities involved in the installation. Additionally, in cases where detection equipment is kitted in a staging or lab environment, the TrafficDOT configuration and the device settings can be synchronized using TrafficDOT import/export capability.

Troubleshooting Detection Network Behavior

TrafficDOT automatically monitors all detector network devices communicating through managed access points, and provides a range of performance parameters – including wireless radio characteristics, device restarts, battery life, and others – for which custom thresholds can be set. This allows TrafficDOT to provide value to almost any detection situation, while providing administrators a simple means to refine the device behavior profiles for their networks over time.

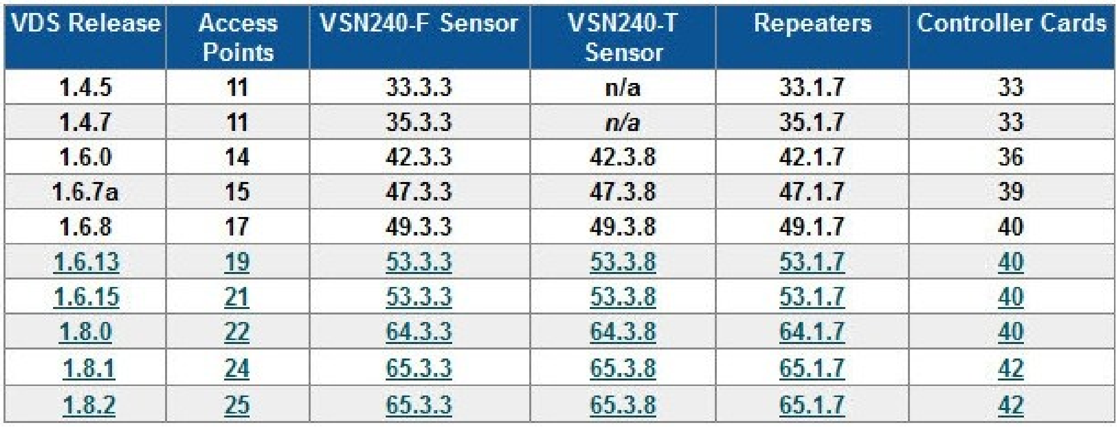
Chapter 3
Installing TrafficDOT

This chapter lists the hardware requirements for TrafficDOT 2, and provides steps for the application installation process.

What's Required for Installation

TrafficDOT is installed via a custom script provided on the distribution media. The computer hosting TrafficDOT must contain a Windows operating system. Prior to installation, ensure you are running VDS 1.6.15 or higher and your configuration is compatible with TrafficDOT 1.10.2.

The following figure provides the version numbers displayed on TrafficDOT for each component from VDS Release 1.4.5 to current.



VDS Release	Access Points	VSN240-F Sensor	VSN240-T Sensor	Repeaters	Controller Cards
1.4.5	11	33.3.3	n/a	33.1.7	33
1.4.7	11	35.3.3	n/a	35.1.7	33
1.6.0	14	42.3.3	42.3.8	42.1.7	36
1.6.7a	15	47.3.3	47.3.8	47.1.7	39
1.6.8	17	49.3.3	49.3.8	49.1.7	40
1.6.13	19	53.3.3	53.3.8	53.1.7	40
1.6.15	21	53.3.3	53.3.8	53.1.7	40
1.8.0	22	64.3.3	64.3.8	64.1.7	40
1.8.1	24	65.3.3	65.3.8	65.1.7	42
1.8.2	25	65.3.3	65.3.8	65.1.7	42

Figure 3-1: Component Version Numbers

Hardware

The computer hosting TrafficDOT should meet the minimum requirements provided in the following table:

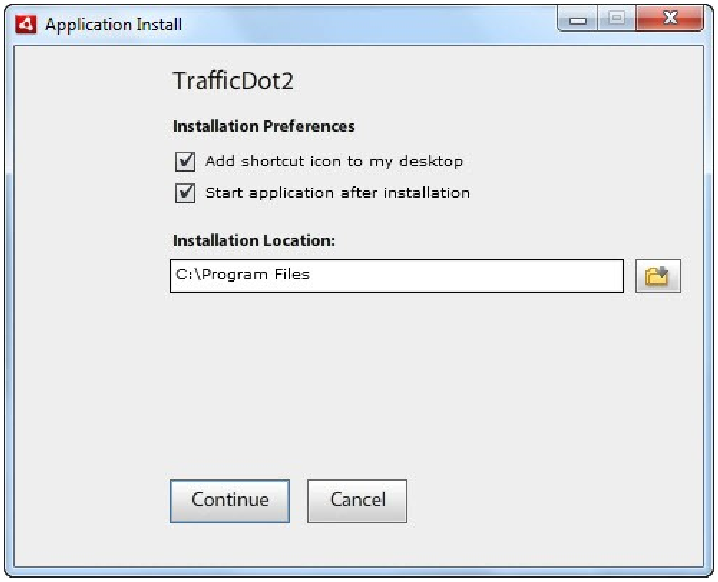
Component	Requirement
CPU	Intel® Pentium® III 1GHz or faster processor; Intel Pentium 4 2GHz or faster
RAM	1GB recommended
HDD	1 GB (minimum)
Media	CD/DVD-ROM drive
Operating system	Microsoft® Windows® XP Professional or Windows 7 (including 64-bit editions)

Table 1: TrafficDOT 2 Minimum Hardware Requirements

Installation Procedure

Use the following procedure to install TrafficDOT. The examples below are taken from an installation on a computer running Microsoft Windows 7.

1. Acquire the installation package from Sensys Networks.
2. Place the TrafficDOT 2 installation media in a CD/DVD drive.
3. Navigate to the TrafficDOT 2 installation executable and double-click. The following *Installation Preferences* window displays.



TrafficDot2

Installation Preferences

☑ Add shortcut icon to my desktop

☑ Start application after installation

Installation Location:

C:\Program Files

Figure 3-2: Selecting Installation Preferences

4. Click the check boxes to select desired preferences.

5. Click *Continue* to accept the default installation location, or click the folder icon and follow the instructions to select another location for your TrafficDOT installation. The following installation window displays.

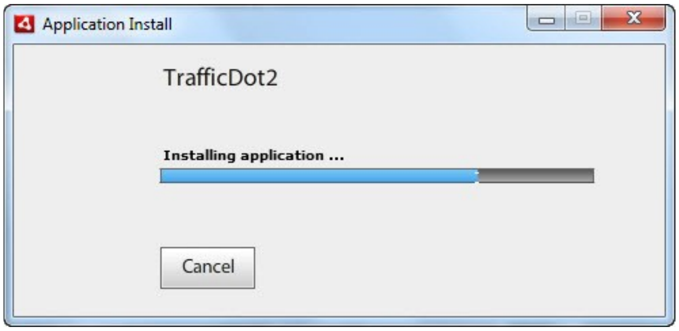
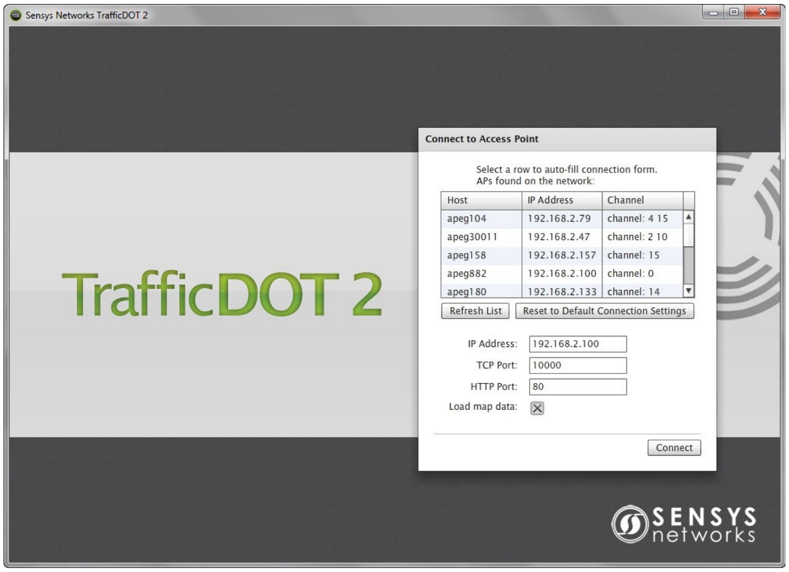


Figure 3-3: Installing Application

If you selected the preferences shown in Figure 3-1, the *TrafficDOT 2 Main Page* displays once the installation is complete.



Select a row to auto-fill connection form.
APs found on the network:

Host	IP Address	Channel
apeg104	192.168.2.79	channel: 4 15
apeg30011	192.168.2.47	channel: 2 10
apeg158	192.168.2.157	channel: 15
apeg882	192.168.2.100	channel: 0
apeg180	192.168.2.133	channel: 14

IP Address: 192.168.2.100
TCP Port: 10000
HTTP Port: 80
Load map data: ☒

Figure 3-4: TrafficDOT2 Main Window

Uninstalling the Software

For installations on computers running Microsoft Windows 7, perform the following steps to remove the software:

1. Click the *Start* menu and select *Control Panel → Programs → Programs and Features*.
2. Click the *Uninstall a program* link.
3. Navigate the the *TrafficDOT2* application.
4. Select the application and click *Uninstall*. The *Windows Installer* displays until the program is removed.
5. After the software removal process runs, click *Exit* on the *Programs and Features* window to end the task.

Note: You can also uninstall the software by rerunning the installer. A window displays with the message "*The same version of the application opened already exists on this system. Would you like to run the version installed?*" Click the *Uninstall* button at the bottom of the window to remove the application.

Chapter 4

Using TrafficDOT

This chapter provides an overview of creating a network of Sensys Networks VDS240 wireless vehicle detection components with TrafficDOT. It also provides an overview of the TrafficDOT *map view* window.

Overview

TrafficDOT 2 provides a graphical user interface that enables you to create networks of Sensys Networks VDS240 wireless vehicle detection components. The user interface provides both a *map* and *table* view of the components. The map view provides a graphical representation of Sensys Networks key elements, which include sensors, access points, repeaters, and contact closure cards.

> **Note**: The table view provides similar functionality to the previous versions of TrafficDOT. For more information regarding the table view, refer to *Monitoring Components via the Table View*.

The map view allows you to:

- Drag and drop the elements in a graphical representation that approximate real-world deployment
- Draw an intersection layout using basic drawing tools
- Assign lane directions
- Create map layers
- Adjust lane widths and lengths
- Assign intersection names that appear in banner title
- Access all features from individual components
- Configure and monitor key components

- Select maps from a library of common application images or upload a map creation of your choice
- Assign sensor's primary application (e.g., Stopbar, Speed, Advance, and Travel Time)

TrafficDOT Map View

The following is a depiction of the TrafficDOT map view. The descriptions of each callout is provided below, and an example of how to use each component is provided later in the chapter.

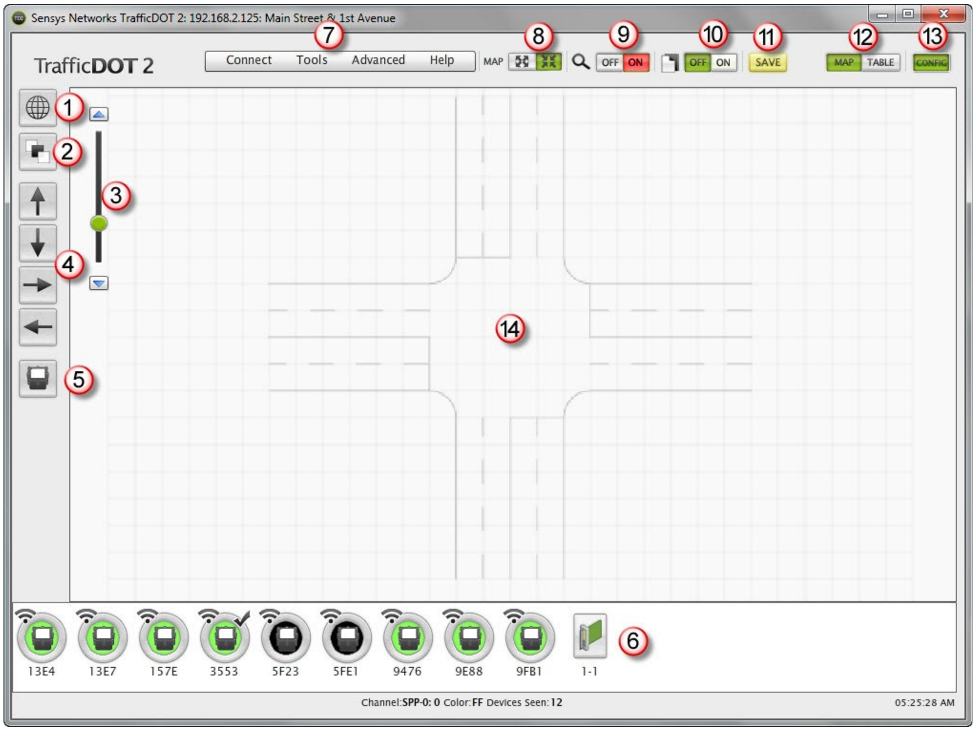


Figure 4-1: TrafficDOT Map View

1. *Map Info and Image* – Displays both the Map Info panel and the map image.
2. *Map Layers* – Provides the ability to show or hide the following map layers:
    - Tool Tips
    - Controller Card Connections
    - RF Connections
    - Sensor Pairings
    - Controller Cards
    - Sensors, AP, Repeaters
    - Lanes

- Map Image

3. *Zoom In/Zoom Out* – Allows you to increase and decrease your map view.
4. *Map Tools* – Allows you to create northbound, southbound, eastbound, and westbound lanes on your map image.
5. *Key Components* – Allows you to add sensors to your network.
6. *Components tray* – Displays all the wireless vehicle detection components. The sensors images are color-coded. The colors (red, yellow, and green) indicate sensor status. When a detection is present the sensor color is black.
7. *Menu Items* – The menus of the *map and tables* windows include:
    - *Connect* – Provides connect/disconnect operations.
    - *Tools* – Provides options for scanning for devices, auto-assigning time slots, generating real-time detection charts and graphs, turning on SNC proxy logging, clearing sensors and repeaters from the components tray, clearing the Dot Table and Dot Pair Table, setting system preferences, and checking memory usage.
    - *Advanced* – Allows you to set user mode. *Advanced Mode* allows for access to advanced device settings, and S*uper User Mode* allows authentication for diagnostic mode access
    - *Help* – Provides options to confirm the software version and access online help and support files.

   For additional information regarding the menu items, refer to the *Menus* section in the *Monitoring Components using the Table View* chapter.
8. *Map* – Allows you display a full map screen view without the *Map Tool*s icons.
9. *Discovery Mode* – Allows you to turn discovery mode on and off. Discovery mode directs all network devices communicating with the access point to include additional information in the data packets they send. Discovery mode is required for utility operations, such as firmware updates and scanning for Sensys Networks equipment on RF channels other than the channel of the access point.
10. *Command Log* – Toggles access to the command history log.
11. *Save All Changes to AP* – Allows you to save all the items on your map to an access point.
12. *Map/Table* – Allows you to toggle between the map and table views. The map and table windows provide a real-time view into the components of the network and the events they detect. All sensors in the network are shown, including sensors that communicate via repeaters.
13. *Config* – Shows or hides the *Configuration Panel* on the right side of the window. The Configuration Panel displays information about whatever item is selected on the map or in the table.

14. *Map Image* – Displays the map image. The map image is the main workspace of the TrafficDOT application.

Using TrafficDOT to Create a Network

Creating a network using TrafficDOT requires the following tasks:

- Connecting to an access point
- Entering map information
- Selecting a primary application
- Uploading a map image
- Creating lanes
- Adding sensors, access point(s), and controller cards to the map

Connecting to an Access Point

Connecting to an access point can occur as (*i*) part of starting TrafficDOT or (*ii*) via the *Connect* menu on the *Main* window.

Connect Window Contents

The *Connect* window displays the access points available on the network, and collects data that identifies the access point to which TrafficDOT will connect. The window elements are shown in the following table:

Field Name	Description
IP Address	IP address of the access point or proxy server. DNS names are supported in environments where DNS services are available.
TCP Port	The TCP port number on which the connection is made. *Note*: the default port number is 10000.
HTTP Port	The HTTP port number on which the connection is made. *Note*: the default port number is 80.

Table 2: Connect Window Fields

Identify the access point you want to connect to by providing values in the *IP Address* and *TCP Port* fields.

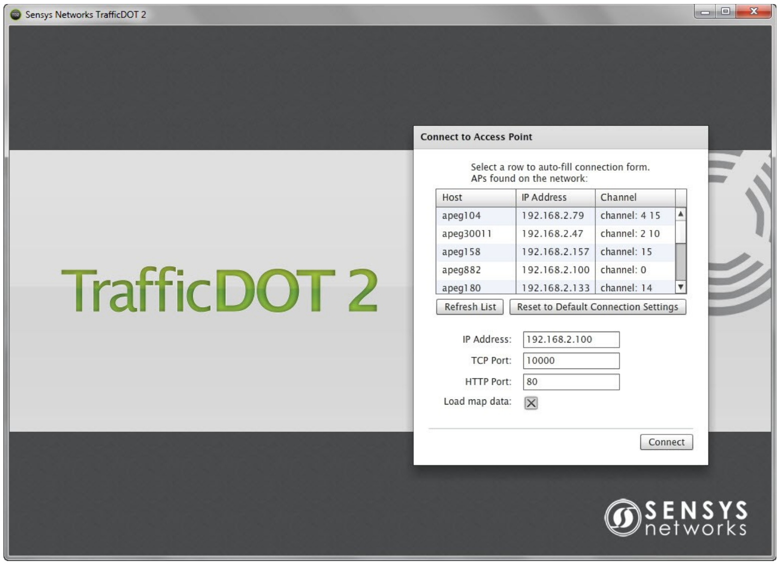
Note: The *Connect* window displays the most recent use of TrafficDOT, so values may already appear in the window.

Connecting at Start-up of TrafficDOT

Connect to the access point with TrafficDOT by performing the following steps:

1. On a Windows laptop or PC, start TrafficDOT by double-clicking its icon.

TrafficDOT's *Main* window opens with the *Connect* window open in front of it.


Sensys Networks TrafficDOT 2
TrafficDOT 2
Refresh List
Reset to Default Connection Settings
Connect
SENSYS networks

Connect to Access Point

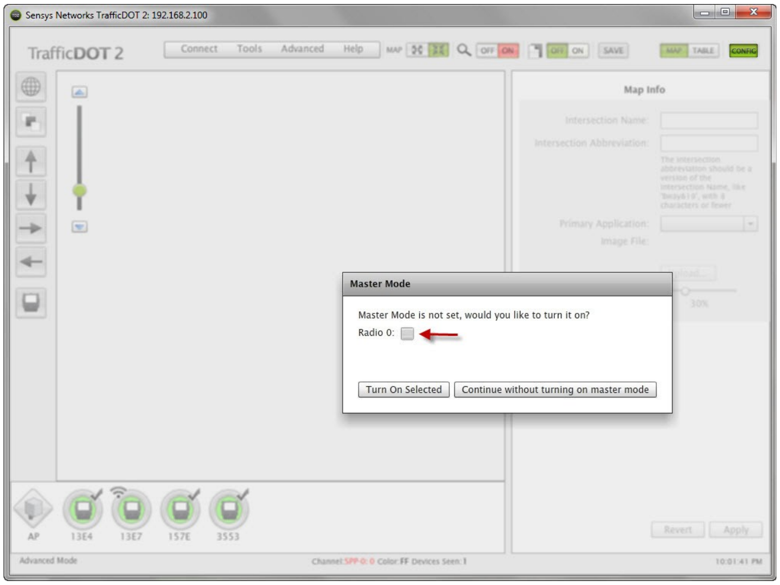
Select a row to auto-fill connection form.
APs found on the network:

Host	IP Address	Channel
apeg104	192.168.2.79	channel: 4 15
apeg30011	192.168.2.47	channel: 2 10
apeg158	192.168.2.157	channel: 15
apeg882	192.168.2.100	channel: 0
apeg180	192.168.2.133	channel: 14

IP Address: 192.168.2.100
TCP Port: 10000
HTTP Port: 80
Load map data: ☒

Figure 4-2: TrafficDOT 2 Connect Window

The *Master Mode* window then displays.



Master Mode

Master Mode is not set, would you like to turn it on?
Radio 0: ☐

Figure 4-3: Master Mode Window

2. Select the *Radio* check box, and then click *Turn On Selected* to enable *Master Mode*.

> If this feature is disabled, the access point must be commanded to begin broadcasting. You will also receive a warning when the access point is rebooted. For additional information on enabling *Master Mode*, refer to the *Enabling Master Mode* section in the *Configuring and Managing Components* chapter.

Connecting via the *Connect* menu

At anytime during a TrafficDOT session, you may connect to a different access point by disconnecting from the current access point by clicking *Disconnect* under the *Connect* menu.

Map Info Panel

TrafficDOT provides a library of common application map images. When creating a new network of Sensys Networks VDS240 wireless vehicle detection components, the first step is to provide the information in the *Map Info* panel. The Map Info panel is the area where you enter the name and abbreviation of your mapped image, select a primary application and upload either a canned map image from the library or one of your own creation.

Map Info Panel Contents

Elements for the *Map Info* panel are shown in the following table:

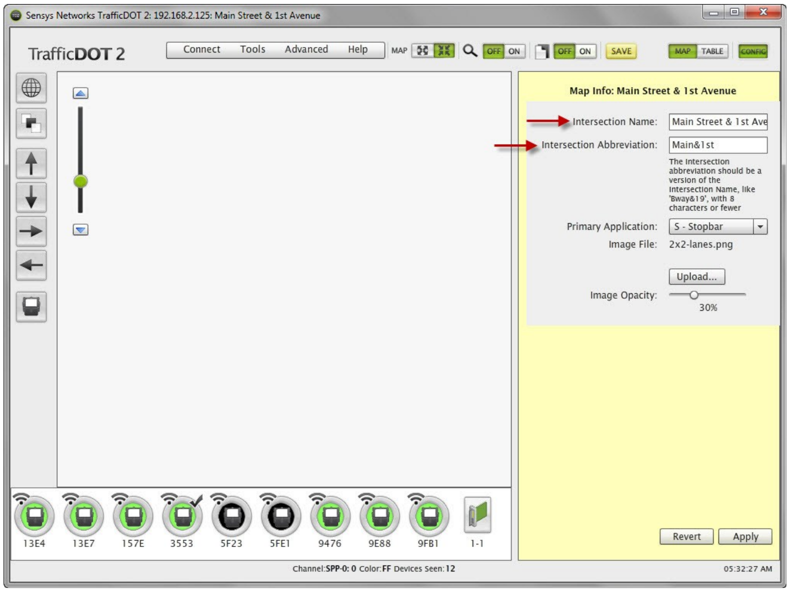
Field Name	Description
Intersection Name	The name of the intersection being monitored. This information also appears in the banner at the top of the TrafficDOT screen.
Intersection Abbreviation	The abbreviation name of the intersection being monitored. The abbreviation should be a version of the intersection name using eight characters or less.
Primary Application	The primary application of your network. The options are: Stopbar, Speed, Advance and Travel Time.
Image File	The name of the image file that currently in use.
Upload	Provides access to the library of map images and allows you to upload a canned image or one of your own creation.
Image Opacity	Determines how transparently the map image appear. The higher the opacity, the less transparent the image will be. This feature can be useful to fade a map image so your attention can focus on the sensors and other network elements.

Table 3: Map Info Panel Elements

Entering Map Information

Enter map information by performing the following steps:

1. Enter an intersection name in the *Intersection Name* field.
2. Enter an abbreviation of the intersection name in the *Intersection Abbreviation* field.



Map Info: Main Street & 1st Avenue

Intersection Name: Main Street & 1st Ave

Intersection Abbreviation: Main&1st

The intersection abbreviation should be a version of the Intersection Name, like 'Bway&19', with 8 characters or fewer

Primary Application: S - Stopbar

Image File: 2x2-lanes.png

Image Opacity: 30%

Figure 4-4: Entering Intersection and Abbreviation Name

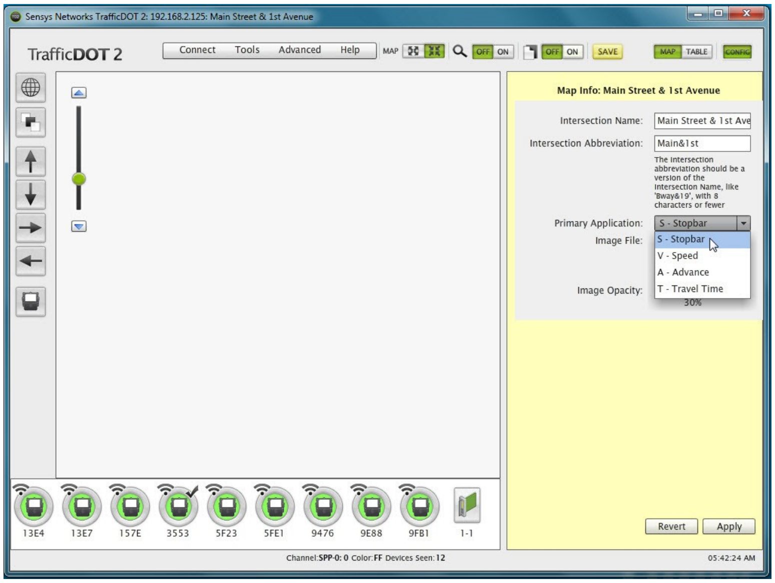
The yellow background in the Map Info panel indicates an unsaved configuration. You cannot move on to another operation until you save the information to the panel.

3. Click *Apply* to save your configuration or *Revert* to discard the changes.

> **Note**: *Apply* saves configuration to flash memory. To save all changes to the access point, you must click the *SAVE* button at the top of the window.

Selecting a Primary Application (Optional)

After entering the intersection name and abbreviation, select one of the available primary applications (*Stopbar*, *Speed*, *Advance*, or *Travel Time*) as shown in the following example.



Sensys Networks TrafficDOT 2: 192.168.2.125: Main Street & 1st Avenue

Map Info: Main Street & 1st Avenue

Intersection Name: Main Street & 1st Ave

Intersection Abbreviation: Main&1st

The intersection abbreviation should be a version of the Intersection Name, like 'Bway&19', with 8 characters or fewer

Primary Application: S - Stopbar

Image File:

Image Opacity: 30%

Channel:SPP-0: 0 Color:FF Devices Seen:12

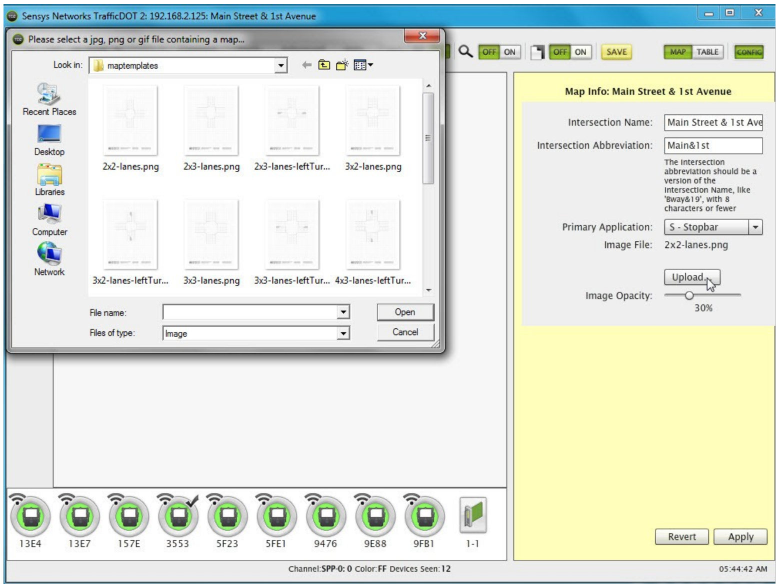
05:42:24 AM

Figure 4-5: Selecting a Primary Application

Uploading a Map Image

Upload an image map by performing the following steps:

1. Click *Upload...* to open the master template directory.



Sensys Networks TrafficDOT 2: 192.168.2.125: Main Street & 1st Avenue

Please select a jpg, png or gif file containing a map...

Look in: maptemplates

File name:

Files of type: Image

Map Info: Main Street & 1st Avenue

Intersection Name: Main Street & 1st Ave

Intersection Abbreviation: Main&1st

The intersection abbreviation should be a version of the Intersection Name, like 'Bway&19', with 8 characters or fewer

Primary Application: S - Stopbar

Image File: 2x2-lanes.png

Image Opacity: 30%

Channel:SPP-0: 0 Color:FF Devices Seen:12

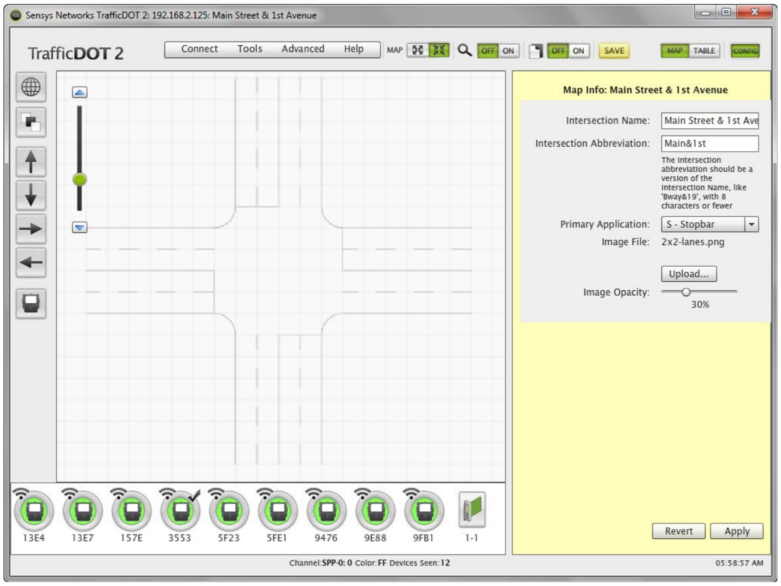
05:44:42 AM

Figure 4-6: Selecting Map Image

2. Select an image applicable to the primary application. For example, if you selected *Stopbar*, you would select the 2x2-lanes.png map image.

> **Note**: You can also upload your own custom map image. The maximum map image file size is 800000 bytes. TrafficDOT accepts .jpg, .png, and .gif image files.

3. Click *Open*. The map image displays in TrafficDOT.



Map Info: Main Street & 1st Avenue

Intersection Name: Main Street & 1st Ave

Intersection Abbreviation: Main&1st

The intersection abbreviation should be a version of the intersection Name, like 'Bway&19', with 8 characters or fewer

Primary Application: S - Stopbar

Image File: 2x2-lanes.png

Image Opacity: 30%

Figure 4-7: Unsaved Map Image

4. Click *Apply*.

Creating Lanes

TrafficDOT provides drawing tools that allow you to create northbound, southbound, eastbound, and westbound lanes on your image map. Once you select a lane direction, and drag and drop it onto your map image the *Lane* panel displays, which is the area where you configure the lane(s) to be monitored.

Lane Panel Contents

Elements for the *Lane* panel are shown in the following table:

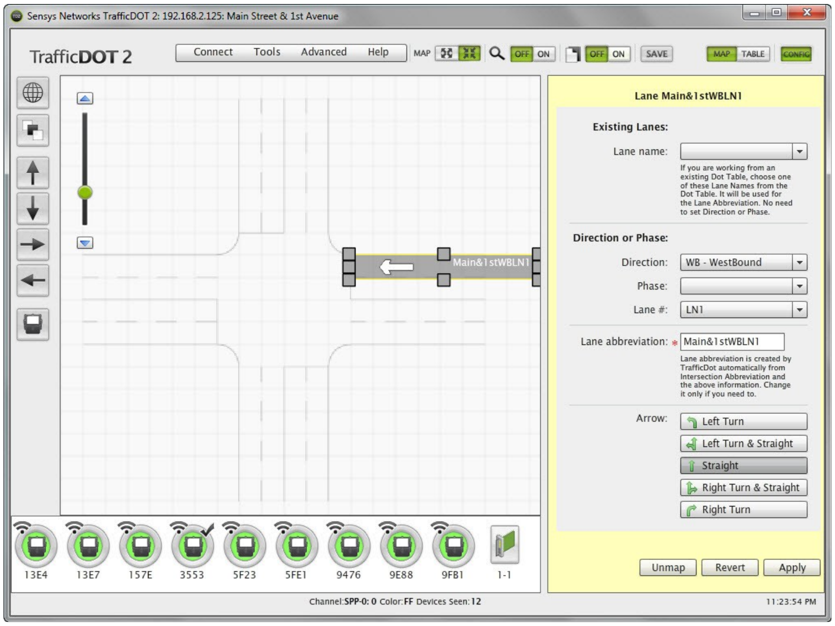
Field Name	Description
Lane Name	The name of the lane being monitored.
Direction	The direction the traffic is flowing for lane. The options are: undefined, Northbound, Southbound, Eastbound, and Westbound.
Phase	The phase of the traffic signal. When configuring a lane, you can select Direction or Phase, but not both.
Lane #	The lane number differentiates one lane from another.
Lane Abbreviation	The abbreviation name of the lane being monitored. The Lane abbreviation field populates automatically.
Arrows	Allows you to graphically depict the direction of the lane(s). The options are:4. Left Turn, Left Turn & Straight, Straight, Right Turn & Straight, and Right Turn. (Optional)

Table 4: Lane Panel Elements

Creating a Lane

To create a lane, perform the following steps:

1. Select one of the four lane icons, and drag and drop the lane in the location of your choice on the image map.



Lane Main&1stWBLN1

Existing Lanes:

Lane name:

If you are working from an existing Dot Table, choose one of these Lane Names from the Dot Table. It will be used for the Lane Abbreviation. No need to set Direction or Phase.

Direction or Phase:

Direction: WB - WestBound

Phase:

Lane #: LN1

Lane abbreviation: * Main&1stWBLN1

Lane abbreviation is created by TrafficDot automatically from Intersection Abbreviation and the above information. Change it only if you need to.

Arrow: Left Turn / Left Turn & Straight / Straight / Right Turn & Straight / Right Turn

Figure 4-8: Creating a Lane

2. Use the handles to resize the lane to your specifications.

   You can also use the rotate handle to cause the lane to rotate. This is useful when working with a map image where the lanes are at an angle.

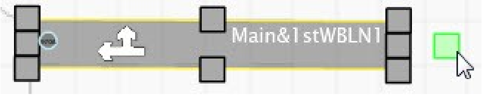


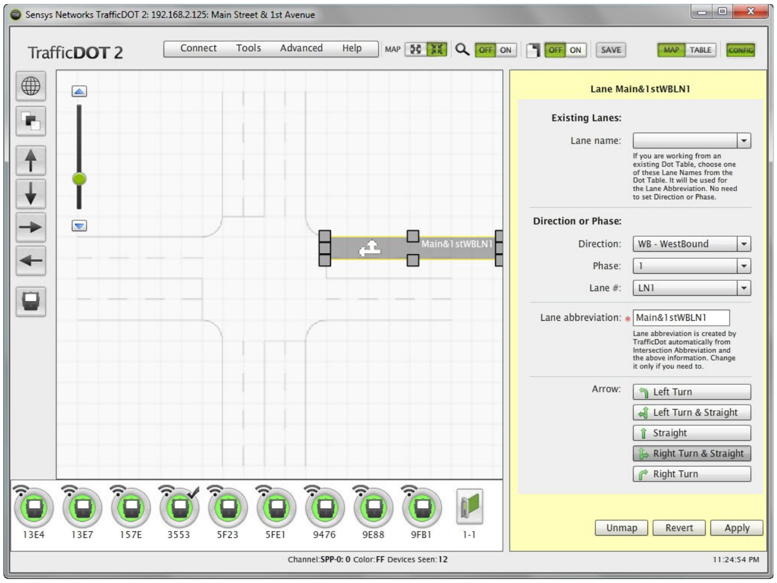
Figure 4-9: Lane Rotation Handle

3. Select the *Direction or Phase,* and the *Lane #* for the lane.

> **Note**: If you are working from an existing Dot Table, select an existing lane name for the drop-down list. The *Phase* is ignored if you select *Direction* or *Lane*. Also, selecting an existing lane overwrites the *Lane abbreviation*, but changing any of the *Direction* or *Phase* settings results in the reversion of the original *Lane abbreviation* text.

4. Select an arrow configuration to signify whether the lane is: *Left Turn*, *Left Turn & Straight*, *Straight*, *Right Turn & Straight*, or *Right Turn*. (Optional)

> **Note**: Repeat steps 1-3 to create multiple lanes.



Lane Main&1stWBLN1

Existing Lanes:

Lane name:

If you are working from an existing Dot Table, choose one of these Lane Names from the Dot Table. It will be used for the Lane Abbreviation. No need to set Direction or Phase.

Direction or Phase:

Direction: WB - WestBound

Phase: 1

Lane #: LN1

Lane abbreviation: * Main&1stWBLN1

Lane abbreviation is created by TrafficDot automatically from Intersection Abbreviation and the above information. Change it only if you need to.

Arrow:

Figure 4-10: Configuring a Lane

5. Click *Apply* to save your lane configuration(s).

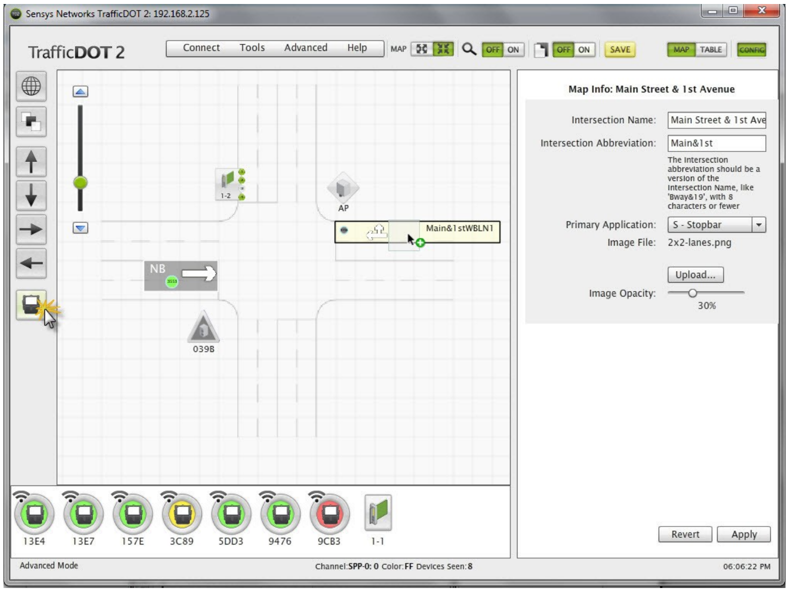
Adding Key Components

Once you have configured your lane(s), add your active Sensys Networks wireless detection components. All active components are available in the component tray. With the exception of sensors, you can drag and drop the graphical representation of the components anywhere you like on the map. Sensors are must be placed on the lanes.

Dragging a Sensor onto a Lane

To drag a sensor onto a lane, perform the following steps:

1. Left-click on the sensor icon on the left side of the screen.



Sensys Networks TrafficDOT 2: 192.168.2.125

Map Info: Main Street & 1st Avenue

Intersection Name: Main Street & 1st Ave

Intersection Abbreviation: Main&1st

The intersection abbreviation should be a version of the intersection Name, like 'Bway&19', with 8 characters or fewer

Primary Application: S - Stopbar

Image File: 2x2-lanes.png

Image Opacity: 30%

Advanced Mode

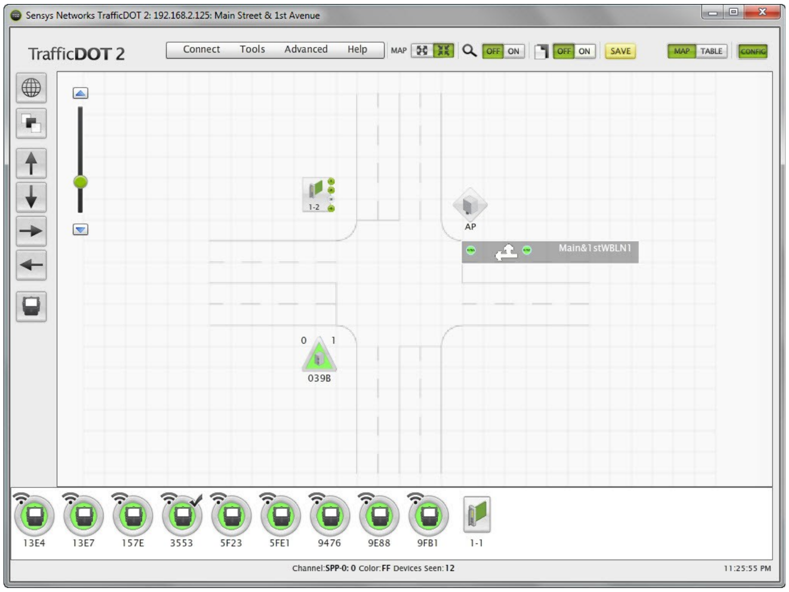
Channel:SPP-0: 0 Color:FF Devices Seen:8

06:06:22 PM

Figure 4-11: Dragging a Sensor onto a Lane

2. Hold down the mouse button and drag the sensor image over the lane.
3. Release the mouse button to place the sensor on the lane.
4. Click *Apply*.

> **Note**: You can also add sensors and other key components by dragging them from the component tray.



Sensys Networks TrafficDOT 2: 192.168.2.125: Main Street & 1st Avenue

Channel:SPP-0: 0 Color:FF Devices Seen:12

11:25:55 PM

Figure 4-12: Adding Key Components

Device Health Indicator

The colors in the map and table view, and in the component tray, visually represent the overall health of the device. The colors represented in the following tables are applicable to all of the key network components.

Color	State	Description
Green	OK	RF communications are healthy; devices are operating normally.
Yellow	Monitor	RF communications are sub-standard. Monitor the situation because in many cases this is transient; no specific end-user action is called for.
Red	Take Action	RF communications have ceased. In most cases there is a problem with the device or its configuration that requires end-user intervention. Investigate and resolve the issue.

Table 5: Device Health Indicators

Icon	Description
9FB1	Packet transmission within watchdog cycle
✓ 3553	Packet transmission and Dot Table entry
4136	State is *Present* (detecting)
3BF8	Packet transmission but other parameters beyond threshold
97EF	Packet transmission lost during current TrafficDOT session

Table 6: Active Device Legend

Chapter 5

Configuring and Managing Components

This chapter provides information about *configuring* the components of the Sensys Networks VDS240 Wireless Vehicle Detection System.

Separate sections describe the configuration procedures for sensors, access points, contact closure cards, and repeaters. In addition, this chapter contains sections describing other TrafficDOT functions useful in managing networks.

Overview

All configuration activities are performed with TrafficDOT. With TrafficDOT, a connection is made to an access point, from which all further configuration activity ensues. TrafficDOT supports configuration of access points, repeaters, sensors and contact closure cards—whether or not they are already installed in the field. Thus, components can easily be added to existing installations.

Configuration of a network involves (*i*) coordinating the radio frequency settings of all devices in the network to achieve high quality communications over a sustained period, and (*ii*) selecting the event detection and reporting parameters necessary to achieve sensing performance that is optimal for the end user application.

Configuration settings for all Sensys Networks equipment are stored in local, non-volatile flash memory. The access point has the greatest number of settings and serves as the central authority for the settings used by network devices. Sensors inherit most, but not all of their settings from the access point to which they are associated. Repeaters have few settings beyond their RF channels.

Most configuration activity occurs at the time of network design and installation. Many customers find that once the network has been installed and its performance validated, no further configuration is necessary.

Configuring Sensors

Sensors ship with a factory default configuration for count applications. Most installations require changes to the default configuration to meet site-specific needs. However, once set, a sensor's configuration typically requires no further changes.

This section describes configuring sensors with TrafficDOT and provides information about the following activities:

- Selecting sensors to configure
- Setting a sensor's operating mode
- Assigning a sensor's time slot
- Setting sensor's RF channel
- Sending a recalibration command to a sensor
- Using advanced settings
- Updating sensor firmware

Introduction

Sensor configuration involves dragging a sensor onto a lane on the map image and selecting values for the following sensor parameters:

- Operating mode
- Radio frequency channel
- Transmission time slot

Other operations related to sensor management are also performed from the sensor configuration window.

Selecting Sensors

Configuration and management commands can be applied to one, several or all of the sensors in a network. You must explicitly select the sensors to configure.

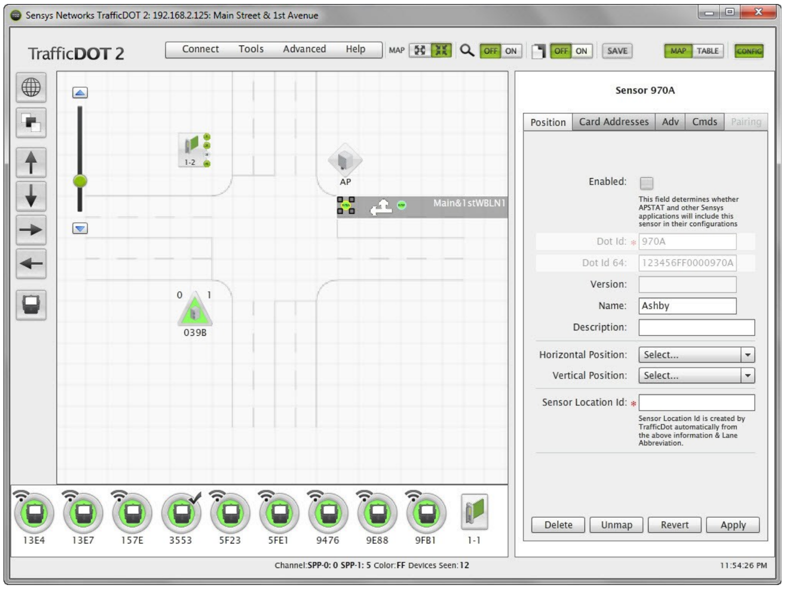
Selecting Parameters

You must explicitly select the parameters to be configured. This allows you to update all, some or a single parameter at a time.

Changes are applied “immediately” - subject to the time slot and transmit interval of your SNP network. It may take up to 30 seconds for changes to be reflected in TrafficDOT's display.

Working with the Sensor Position Window

To select a sensor for configuration, click on a sensor on your image map. The *Sensor Position* window displays.



Sensor 970A

Enabled: ☐

This field determines whether APSTAT and other Sensys applications will include this sensor in their configurations

Dot Id: * 970A

Dot Id 64: 123456FF0000970A

Version:

Name: Ashby

Description:

Horizontal Position: Select...

Vertical Position: Select...

Sensor Location Id: *

Sensor Location Id is created by TrafficDot automatically from the above information & Lane Abbreviation.

Channel:SPP-0: 0 SPP-1: 5 Color:FF Devices Seen: 12

11:54:26 PM

Figure 5-1: Sensor Configuration Window

Sensor Configuration Window Contents

The *Sensor Configuration Window* consists of five tabs: *Position*, *Card Addresses*, *Adv*, *Cmds,* and *Pairing*. Elements for the *Position* window are shown in the following table:

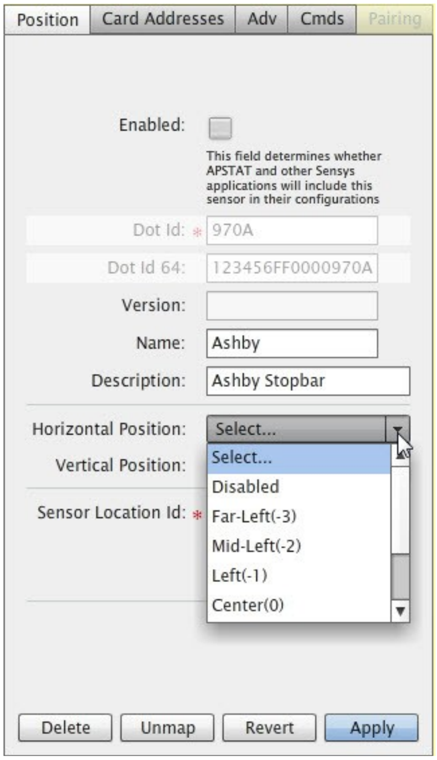
Field Name	Description
Enabled	The field determines whether APSTAT and other Sensys Networks applications will include the sensor being configured in its configuration.
Dot Id	The factory assigned hardware device identifier. This displays the least significant 16 bits as a 4-character HEX string.
Dot Id 64	The factory assigned hardware device identifier. This displays all 64 bits as a 16-character HEX string.
Version	The firmware version on the device. (Note: use the VDS Release Notes from Sensys Networks to cross references firmware version IDs to VDS releases.)
Name	The name of the sensor. You can name the sensor any 8-character name that makes sense for your application.(Optional)
Description	Description of the sensor location and use. (Optional)
Horizontal Position	Sensor's horizontal position relative to other sensors in the same lane. Values may be -3, -2, -1, 0, 1, 2 or 3 where -3 indicates the far-left sensor; -2 indicates the mid-left sensor; -1 indicates the left; 0 indicates the center sensor; 1 indicates the right sensor; 2 indicates the mid-right, and 3 indicates the far-right sensor.
Vertical Position	Sensor's vertical position relative to other sensors in the same lane. This element is used to identify sensor speed pairs. Values may be 0, 1 or 2 where 0 indicates the lead sensor, 1 indicates a trailing sensor, and 2 indicates a second trailing sensor.
Sensor Location Id	The field is populated automatically using the lane abbreviation.

Table 7: Position Window Elements

Setting a Sensor's Position

After providing a name and description of the sensor, select the position of the sensor. Enable the *Horizontal Position* by selecting a value of Far-Left (-3), Mid-Left (-2), Left (-1), Center (0), Right (1), Mid-Right (2), or Far-Right (3). Or, enable the Vertical Position by selection the value of Lead(0), Trail(1), or Trail(2).

> **Note**: If you enable the horizontal position, you must disable the vertical position and vice versa. The horizontal position is used for Travel Time, while vertical position is used for the other applications.



Enabled: ☐

This field determines whether APSTAT and other Sensys applications will include this sensor in their configurations

Dot Id: * 970A

Dot Id 64: 123456FF0000970A

Version:

Name: Ashby

Description: Ashby Stopbar

Horizontal Position: Select...

Figure 5-2: Selecting Horizontal Position

Working with the Card Addresses Window

The sensor-to-contact closure channel mappings are stored in a sensor database that resides on the access point. The four channels represent independent contact closures which, in turn, are actuated by the vehicle detection events transmitted by a defined group of wireless sensors. Each sensor may be associated with up to four *Card Address / Channel* combinations.

Up to 15 wireless sensors can be associated with the same card/channel, in which case the sensors are logically “OR-ed” together – meaning that if any sensor on the channel detects a vehicle, the corresponding contact closes.

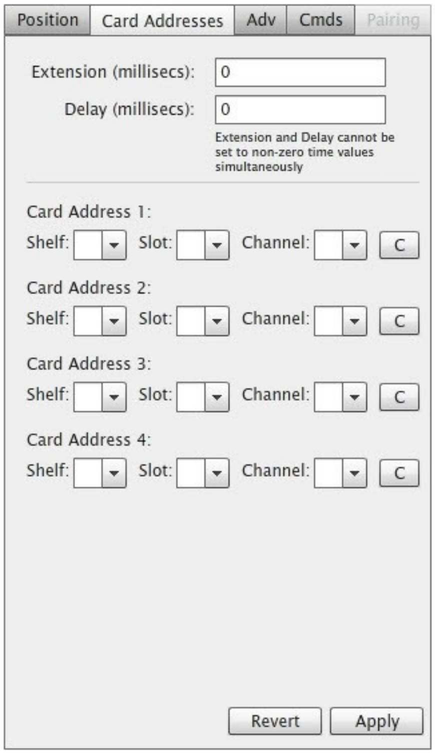
Mapping Sensors to Contact Closures

To map sensors to contact closure cards, perform the following steps:

1. Select a sensor from the image map.
2. Open the *Card Addresses* window by clicking the *Card Addresses* tab.

   The *Extension* entry extends the duration of a contact closure on a per-sensor basis. The *Delay* entry delays the duration of contact closure on a per-sensor basis; these entries are optional.

   The *shelf number-slot number* is a card address associated with a Sensys Networks contact closure master or extension card, and *channel* is between 1 and 4.



Extension (millisecs): 0

Delay (millisecs): 0

Extension and Delay cannot be set to non-zero time values simultaneously

Figure 5-3: Card Addresses Window

3. Select a *Shelf* number, a *Slot* number, and a *Channel* from the drop-down lists.

> **Note**: The **C** button clears the data in that row.

4. Click *Apply* to save configuration.

> **Note**: To assign a sensor to multiple controller channels, supply entries to the additional *Card Addresses* areas.

Working in the Advanced Settings Window

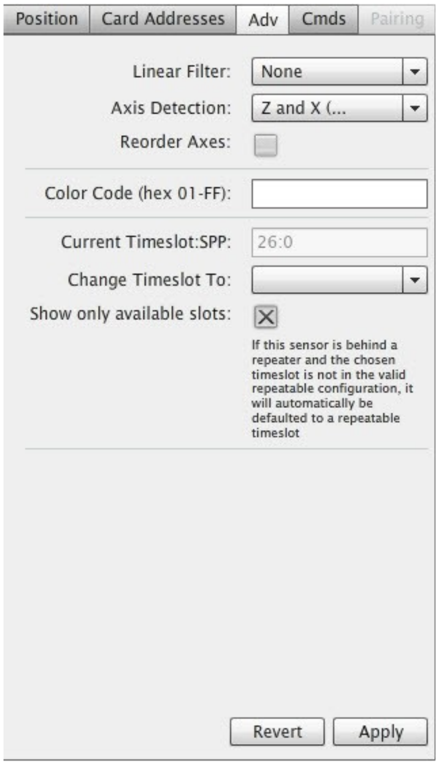
In certain situations, the performance of a sensor's magnetic detectors may be impeded by sources of electro-magnetic energy in the local environment such as power lines, trains, or other sources. Advanced sensor settings can be used to mitigate the noise introduced by such sources.

In order to change any values in the *Advanced Settings Window*, you need to be in Advanced Mode. To set Advanced Mode, click the *Advanced* menu item at the top of the screen, and select *Set Advanced Mode*.

> **Note**: This mode will be enabled for your future sessions until you choose to cancel it.

To configure advanced sensor settings, perform the following steps:

1. Open the *Advanced Setting* window by clicking the *Adv* tab.



Linear Filter: None

Axis Detection: Z and X (...

Reorder Axes: ☐

Color Code (hex 01-FF):

Current Timeslot:SPP: 26:0

Change Timeslot To:

Show only available slots: ☒

If this sensor is behind a repeater and the chosen timeslot is not in the valid repeatable configuration, it will automatically be defaulted to a repeatable timeslot

Figure 5-4: Advanced Settings Window

The *Advanced Settings* elements are as follows:

Linear Filter

- Applying a linear filter has the effect of eliminating high-frequency energy in the waveform; this filter is particularly beneficial when installations are impacted by 60Hz energy produced by power lines.

- Two filter options are available that differ by the number of samples taken. Use *Filter3* (three samples) for freeway sites and *Filter4* (four samples) for arterials. This element can be enabled independently of other advanced settings.

Axis Detection

- The axes of detection can be limited via this element. Options include the default combination (Z and X axes), or any of the X, Y, and Z axes used by themselves.
- This property is particularly useful when installations are impacted by magnetic radiation sources that are significant and effect a particular axis. This element can be enabled independently of other advanced settings.

Reorder Axes

- This element is a binary switch that directs a sensor to perform a one-time change or orientation of its axes. It is particularly useful when installations are impacted by a static energy source significant enough to saturate an detector's axis.

Color Codes (hex 01 - FF)

- The color code option allows the allocation of any of 255 possible codes to a vehicle detection system, thus making it possible for multiple signals to be carried over the same RF channel. The default is FF.

Change Time Slot To

- This option allows the user to change the sensor's time slot and is the value displayed on the *Sensor Position* window. Each sensor uses only one time slot to communicate with its access point or repeater. TrafficDOT assists in enforcing proper time slot usage by filtering the drop-down list of available time slots.

> **Note**: This entry is for manual adjustments to time slot for individual sensors. It is recommended that you use the *Auto-assign Timeslots* option in the *Tools* menu to set all sensor timeslots

2. Choose the required values from the drop-down lists.
3. Click *Apply* to save configuration.

Working in the Commands to Sensor Window

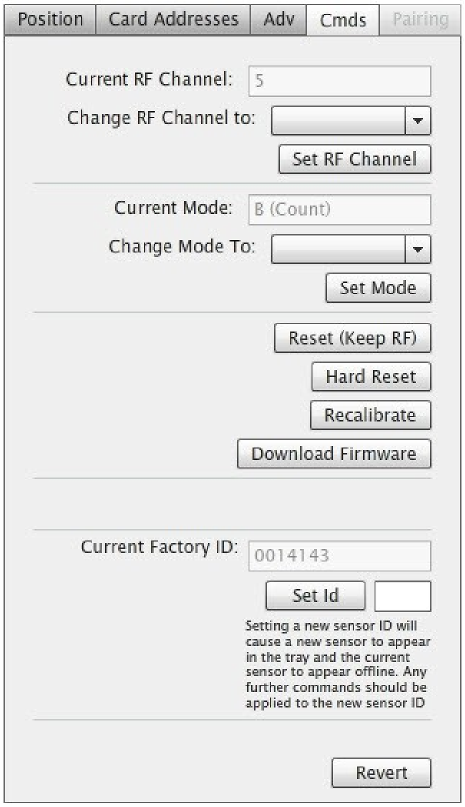
TrafficDOT's *Cmds* window includes other operations related to managing sensors including:

- setting sensor's RF channel
- changing sensor operating mode

- performing a “soft” reset
- performing a “hard” reset
- downloading sensor firmware
- recalibrating a sensor
- setting a sensor ID

> **Note**: These operations are not common. Perform them only when directed by Sensys Networks.

To configure the Command to Sensor settings, open the *Command to Sensor* window by clicking the *Cmds* tab.



Current RF Channel: 5

Current Mode: B (Count)

Current Factory ID: 0014143

Setting a new sensor ID will cause a new sensor to appear in the tray and the current sensor to appear offline. Any further commands should be applied to the new sensor ID

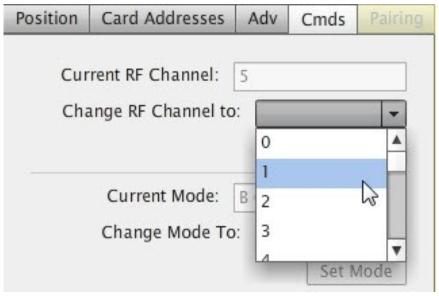
Figure 5-5: Command to Sensor Window

Setting a Sensor's RF Channel

All sensors associated with an access point must use the same RF channel as the access point; all sensors associated with a repeater must use the same frequency designated as the *downstream channel* on that repeater.

To set the RF channel, perform the following steps:

1. Select the *Change RF Channel to* drop-down list. The 16 RF channels available for use display.
2. Select an entry from the list by clicking it.


Current RF Channel: 5

Change RF Channel to:

Current Mode: B

Figure 5-6: Changing RF Channel

If you set the RF Channel to one that is not used by the access point or any repeater, the sensor is no longer be seen and communication to it is lost.

3. Click *Set RF Channel* to save configuration. The current channel displays in the *Current RF Channel* field.

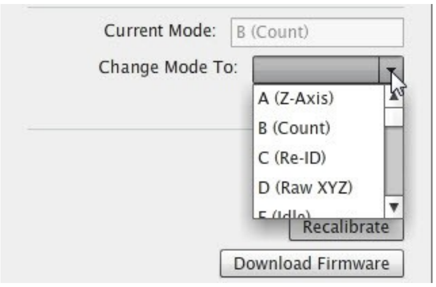
Note: The default is zero.

Setting a Sensor's Operating Mode

The sensor's operating mode defines the type of detection data it transmits.

To set the operating mode, perform the following steps:

1. Select the *Change Mode To* drop-down list. The operating modes available for sensors display.
2. Select an entry from the list by clicking it.


Current Mode: B (Count)

Change Mode To:

Figure 5-7: Setting Operation Mode

For typical detection scenarios use *Count (B)* or one of the *Stop Bar* modes; *Idle* (E) mode may also be useful for pre-installation kitting activities.

Other modes are available to support more specialized situations such as arterial travel time measurement, interfacing to specific devices, or field work by authorized Sensys

Networks technicians. Additionally, in some rare cases, measurement of the local magnetic field (using the reserved mode D) may be requested by Sensys Networks. Always check with Sensys Networks if you are unsure about which mode to specify.

> **Note**: Only model VSN240-F sensors support count mode; although TrafficDOT may appear to allow setting the mode of other sensors to count mode, the command fails.

3. Click *Set Mode* to save configuration.

Performing a Soft Reset

On occasion, a sensor may need to be reset without changing its RF communication parameters. This may occur as a result of a firmware download that was interrupted, an unexpected magnetic event in the local area or other reason. To perform a soft reset, select the sensor and click the *Reset (Keep RF)* button.

Performing a Hard Reset

A sensor may need to be reset back to its factory default configuration. This operation resets the sensor's RF channel assignment to channel zero. As such, reconfiguration may be required in order for the sensor to communicate to with the network's access point. To perform a hard reset, select the sensor and click the *Hard Reset* button.

Downloading Sensor Firmware

Updates to sensor firmware are sent from the access point via the wireless communication channel.

> **Note**: Sensor firmware updates must occur independent of repeater or access point firmware updates.

Firmware updates become operational immediately and can be reversed only by performing the firmware update procedure specifying a prior version of the appropriate firmware image. It is not necessary to reconfigure sensors after updating their firmware, although in many cases, new firmware enables additional device functionality that may require initial configuration. To download sensor firmware, select the sensor and click the *Download Firmware* button.

Recalibrating a Sensor

Sensors operate by evaluating changes in the local magnetic field. They establish a reference value known as a baseline to which detected changes are compared. Setting the baseline is called *recalibration* and occurs automatically. On occasion, you may want to recalibrate a sensor. To recalibrate a sensor, select the sensor and click the *Recalibrate* button.

Setting a Sensor IDs

Individual sensors can be renamed by assigning them a user-defined identifier. This identifier serves as an alias for the device in lieu of its factory assigned identifier.

Renaming sensors can be useful in situations where a sensor must be replaced and the original sensor's event history must be preserved. Renaming the replacement sensor with the device identifier of the original associates the event history to the new device.

Considerations for Setting Sensor IDs

Consider the following when setting sensor IDs to user-defined strings:

- User assigned sensor IDs must be four characters in length and may consist only of hexadecimal characters. Spaces and special characters are not allowed.
- The *Sensor ID* tool operates only on sensors whose VDS firmware version is release 1.8 or above. Update sensors to this release level or above before attempting to set their device identifiers.
- The *Sensor ID* tool allows multiple sensors to be aliased to the same ID, although only one of them will appear in the TrafficDOT *Main* window. A window displays a warning of this outcome when appropriate.
- In the event the firmware of a sensor that has already been aliased is downgraded to a VDS release earlier than VDS 1.8.0, the user-defined id is discarded and the device id reverts to its factory assigned value. (VDS versions prior to release 1.8.0 do not support user-defined identifiers.)

To set a sensor's ID, select the sensor. Type a new device identifier string into the *Sensor Id* field and click the *Set Id* button.

> **Note**: The string must be four characters in length and may consist only of hexadecimal characters.

Configuring Access Points

This section describes configuring and working with access points via TrafficDOT. The following activities are discussed:

- Retrieving an access point's configuration
- Configuring RF settings
- Configuring event parameters
- Configuring detection settings
- Inspecting the access point ID and firmware version
- Setting system preferences
- Working with advanced properties
- Saving the configuration

Introduction

Access point configuration involves dragging an access point onto the map image, and is the process of defining behavior and tolerances for the entire network. The configuration is implemented through a set of property collections. The collections group similar or related properties together; each collection is discussed in the sections that follow.

The property collections for access point and network configuration are as follows:

- RF communications
- Event thresholds
- Detection sensitivities

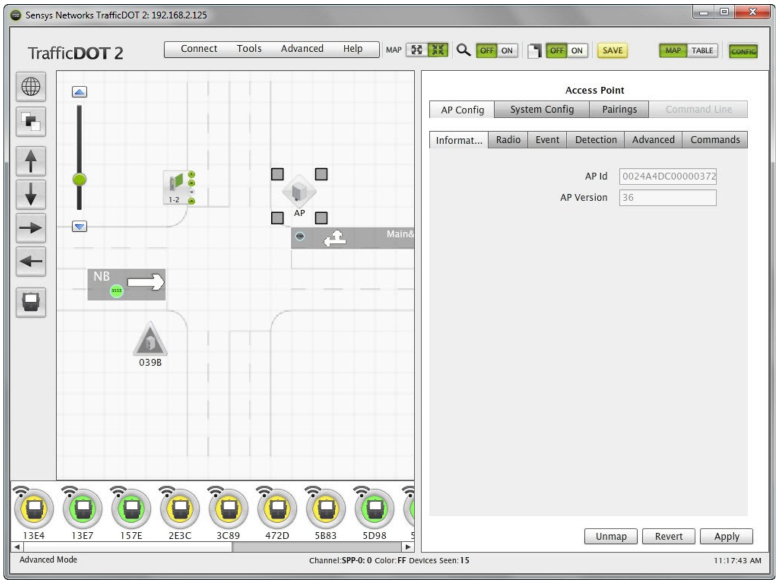
Access points ship with a default configuration suitable for a wide variety of situations. Using defaults reduces the amount of custom configuration and ensures that all critical elements have values assigned to them.

Other operations performed with TrafficDOT related to access point and network management are also discussed in this section.

Working with the Access Point Configuration Window

Before you can configure an access point, a connection to it must be established. Make a connection as described above in the section *Connecting to an Access Point*.

To select an access point for configuration, click on an access point on your image map. The *Access Point Configuration* window displays.



AP Id 0024A4DC00000372

AP Version 36

Figure 5-8: Access Point Configuration Window

Viewing the Access Point ID and Firmware Version

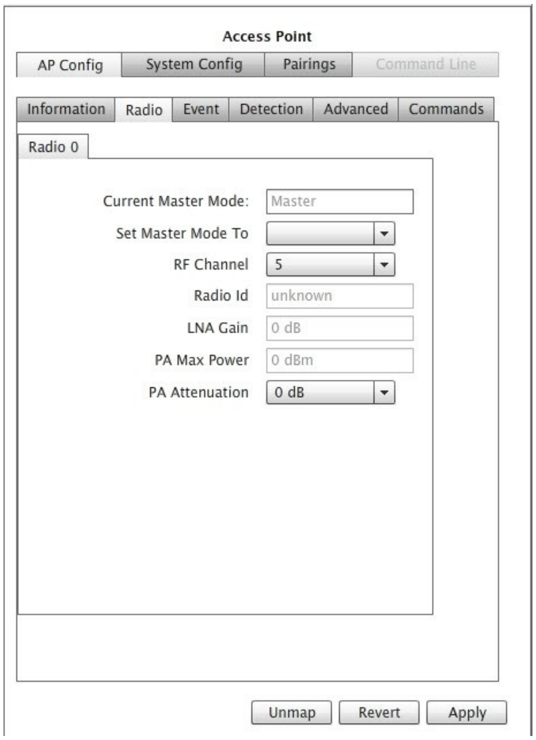
The unique, factory assigned access point ID and version of the access point's firmware can be reviewed on the *Information* tab as shown in Figure 5-8. The *Access Point ID* is expressed as a 16-character HEX string; these elements are for reference only.

Configuring RF Settings

The radio frequency of the access point defines the frequency for the entire network. Each device that communicates with the access point must be configured to use the same RF channel.

The *Radio* tab has three configurable elements:

- Set Master Mode To
- RF Channel
- PA Attenuation



Current Master Mode: Master
Set Master Mode To
RF Channel 5
Radio Id unknown
LNA Gain 0 dB
PA Max Power 0 dBm
PA Attenuation 0 dB

Figure 5-9: Radio Tab

The other elements are for reference only.

Enabling Master Mode

Master Mode directs access points to commence broadcasting as soon as they receive power. If this feature is disabled, the access point must be explicitly commanded to begin broadcasting . To enable this feature, select *Master* from the drop-down list, and click *Apply* to save configuration. To disable this feature, select *Command* from the drop-down list.

> **Note**: If you disable the feature, you will receive a warning when the access point is rebooted.

Setting the RF Channel

To configure the RF channel, perform the following steps:

1. The entries in the *RF Channel* drop-down list correspond to the 16 frequencies available for use. Select an entry from the list by clicking it.

   > **Note**: The factory default channel is zero.

2. Click *Apply* to save configuration.

Setting the PA Attenuation

To configure the power amplifier attenuation, perform the following steps:

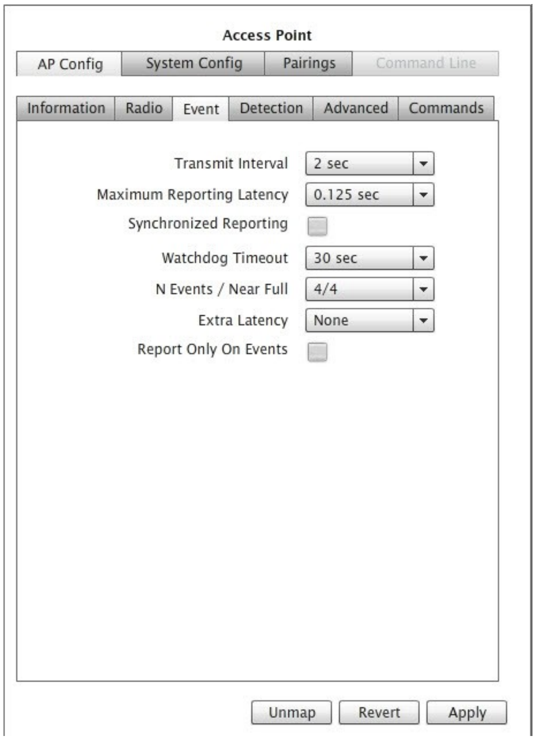
1. The entries in the *PA Attenuation* drop-down list provide a range of limiting values expressed in *db*. Select an entry from the list by clicking it.
2. Click *Apply* to save configuration.

> **Note**: Reducing the performance of the power amplifier is not a common requirement. Leave this setting at the factory default of zero unless directed otherwise by Sensys Networks.

Configuring Event Parameters

Event reporting pertains to the act of sensors transmitting detection data to the access point. Event reporting parameters are global attributes, stored in the access point's configuration, that dictate how event reporting occurs on a given network. The *Event* tab has the following configurable elements:

- Transmit Interval
- Maximum Reporting Latency
- Synchronized Reporting
- Watchdog Timeout
- N Events / Near Full
- Extra Latency
- Report Only ON Events



Transmit Interval: 2 sec
Maximum Reporting Latency: 0.125 sec
Synchronized Reporting: ☐
Watchdog Timeout: 30 sec
N Events / Near Full: 4/4
Extra Latency: None
Report Only On Events: ☐

Figure 5-10: Event Tab

Setting the Transmit Interval

The transmit interval sets the frame size for the network and, in so doing, dictates the number of time slots available for device transmissions. To set the transmit interval, perform the following steps:

1. The entries in the *Transmit Interval* drop-down list are the available frame sizes for SNP networks. Select an entry from the list by clicking it.

> **Note**: The factory default is 0.125 sec.

2. Click *Apply* to save configuration.

Setting the Maximum Reporting Latency

The maximum reporting latency is the maximum amount of time that may pass between successive transmissions from a given sensor. To set the maximum reporting latency, perform the following steps:

1. The entries in the *Maximum Reporting Latency* drop-down list are the available reporting latencies. Select an entry from the list by clicking it.

> **Note**: The factory default is 0.125 sec.

2. Click *Apply* to save configuration.

Enabling Synchronized Reporting

The synchronized reporting attribute globally enables (or disables) transmission of data by sensors on a fixed clock basis. When enabled, all sensors report their data (subject to their respective time slots) as of a fixed interval equal to *Maximum Reporting Latency* (or multiple thereof) relative to the network's system clock maintained by the access point.

1. To enable synchronized reporting, select the check box. To disable the function (the default setting), clear the check box.
2. Click *Apply* to save configuration.

Setting a Watchdog Timeout

The watchdog timeout attribute specifies a number of seconds of inactivity a sensor will wait before transmitting a packet. To set a watchdog timeout, perform the following steps:

1. The entries in the *Watchdog Timeout* drop-down list are the available timeout intervals. Select an entry from the list by clicking it.

   Note: The factory default is 30 seconds.

2. Click *Apply* to save configuration.

Configuring Event Reporting Buffer Controls (N Events / Near Full)

This parameters sets two global attributes that govern the event queue monitoring process. The attributes are as follows:

- *N Events* – the maximum number of events that may be queued; in effect, the queue size in units of “events”.
- *Near full* – the maximum number of events that may be queued before the queue is “flushed” by transmitting a packet.

To set event reporting buffer controls, perform the following steps:

1. The entries in the *N Events/Near Full* drop-down list are the available combinations of maximum event reports and reporting trigger points. Select an entry from the list by clicking it.

   Note: The factory default is 4/4.

2. Click *Apply* to save configuration.

Configuring Extra Latency

Additional latency may be required in situations where the access point interfaces with a traffic signal controller and the highest fidelity wave form generated by events is desired. To configure extra latency, perform the following steps:

1. The entries in the *Extra Latency* drop-down list are the available latency increments. Select an entry from the list by clicking it.

> **Note**: The factory default is *None*.

2. Click *Apply* to save configuration.

Limiting Reporting to “On” (Detection) Events Only

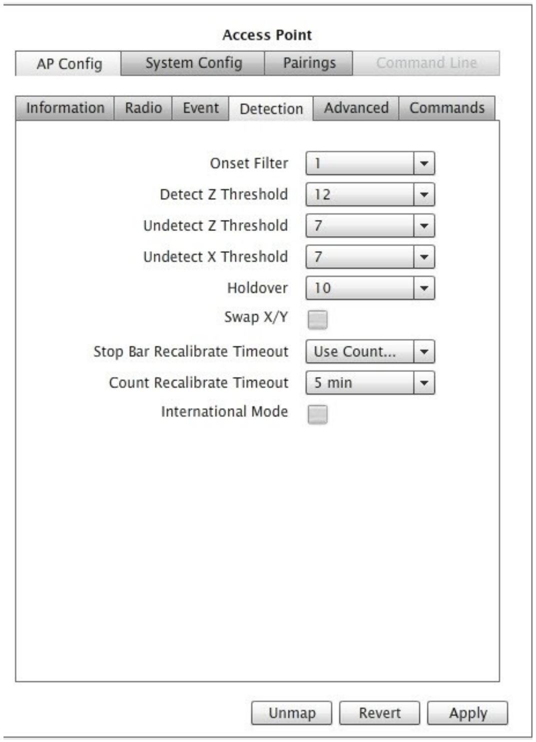
This attributes globally enables (or disables) a constraint on the nature of the data reported for a detection. Enabling this attribute results in reporting only the rising edge of a detection pulse.

1. To enable this feature, select the check box. To disable the feature (the default setting), clear the check box.
2. Click *Apply* to save configuration.

Configuring Detection Settings

Vehicles are detected by inference. Sensors continuously monitor the X, Y, and Z axes of the earth’s magnetic field. When no vehicles are present, a sensor calibrates itself by measuring the values of the background magnetic field and establishing a *reference value*. The passage and presence of vehicles are detected by measuring the magnitude of deviations from that value. The Detection tab has the following configurable elements:

- Onset Filter
- Detect Z Threshold
- Undetect Z Threshold
- Undetect X Threshold
- Holdover
- Swap X/Y
- Stop Bar Recalibrate Timeout
- Count Recalibrate Timeout
- International Mode



Onset Filter	1
Detect Z Threshold	12
Undetect Z Threshold	7
Undetect X Threshold	7
Holdover	10
Swap X/Y	☐
Stop Bar Recalibrate Timeout	Use Count...
Count Recalibrate Timeout	5 min
International Mode	☐

Figure 5-11: Detection Tab

Setting the Onset Filter

The *Onset Filter* specifies the number of consecutive samples for which the ON condition must be true before a detection event is true. To set this attribute, perform the following steps:

1. The entries in the *Onset Filter* drop-down list are the available number of consecutive samples. Select an entry from the list by clicking it.

> **Note**: The factory default is 1.

2. Click *Apply* to save configuration.

Setting Thresholds for Detection and Undetection

Thresholds specify the magnitude of change from a sensor's reference value (representing its current estimate of the local background magnetic field) necessary to declare a detect or undetect event. There are three threshold attributes.

Detect Z Threshold

Detection events are declared when the local magnetic field deviates from the baseline reference value by more than this threshold. The default value is 12.

Undetect Z Threshold, Undetect X Threshold

Undetect events are declared when the local magnetic field deviates from the baseline reference value by this threshold or less. The default value is 7. To set the threshold attributes, perform the following steps for each of the two elements:

1. The entries in the threshold drop-down lists are the available threshold values. Select an entry from the list by clicking it.
2. Click *Apply* to save configuration.

Setting the Holdover Attribute

Holdover specifies the number of consecutive samples for which the ON condition for both the X and Z magnetic axes are no longer true before an OFF event is declared. To set this attribute, perform the following steps:

1. The entries in the *Holdover* drop-down list are the available number of consecutive samples. Select an entry from the list by clicking it.

   Note: The factory default is 10.

2. Click *Apply* to save configuration.

Enabling a Swap of the X and Y Measurements

This property logically swaps the readings from the X and Y magnetic axes. (This is not common.)

1. To enable this feature, select the *Swap X/Y* check box. To disable it (the default setting), clear the *Swap X/Y* check box.
2. Click *Apply* to save configuration.

Setting the Recalibration Timeouts

A recalibration timeout is an optional parameter that specifies a duration such that, if an ON condition is true for a period greater than the timeout duration, the sensor is recalibrated. There are two recalibration timeouts – one for stop bar applications and another for count applications.

Setting the Stop Bar Recalibration Timeout

This setting applies to all sensors operating in any of the stop bar operating modes. To set the timeout, perform the following steps:

1. The entries in the drop-down list are the available recalibration timeouts. Select an entry from the list by clicking it.

> **Note**: The factory default is *Use Count Timeout* – which means that the timeout value for the element *Count Recalibrate Timeout* is used.

2. Click *Apply* to save configuration.

Setting the Count Recalibration Timeout

This setting applies to all sensors operating in the count operating mode. To set the timeout, perform the following steps:

1. The entries in the drop-down list are the available recalibration timeouts. Select an entry from the list by clicking it.

> **Note**: The factory default is *Off*.

2. Click *Apply* to save configuration.

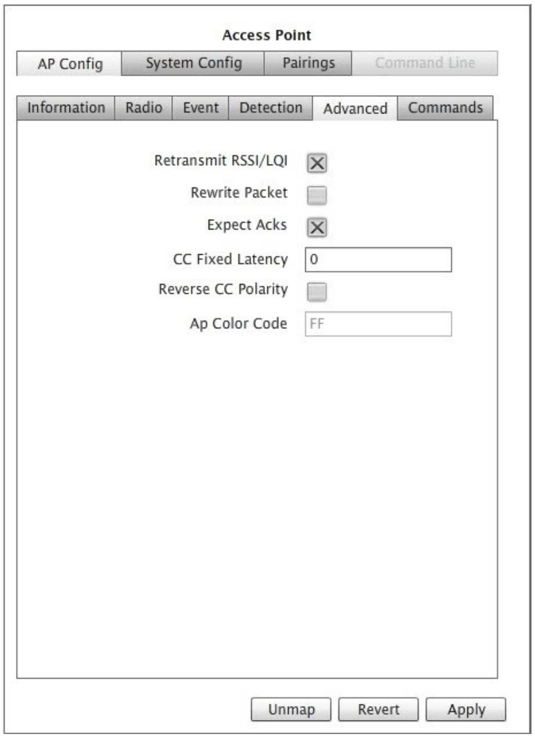
Enabling International Mode

The *International Mode* attribute is related to the recalibration timeout elements described above. This element dictates which set of timeout values are available for selection from the *Count Recalibrate Timeout* drop-down list.

Clear the check box for installations in North America. Select the check box for installations outside of North America that require the recalibration timeout feature.

Configuring Advanced Properties

The *Advanced* tab enables the configuration of advanced properties. Advanced properties dictate system behavior that is considered “default” in the sense that Sensys Networks recommends it in almost all cases. These elements allow tuning of the system behavior.



Retransmit RSSI/LQI ☒

Rewrite Packet ☐

Expect Acks ☒

CC Fixed Latency 0

Reverse CC Polarity ☐

Ap Color Code FF

Figure 5-12: Advanced Tab

Enabling Retransmission of RSSI and LQI

Retransmit RSSI/LQI tells repeaters to append the RSSI and LQI measurements of the messages received from sensors to the packets forwarded to the access point. To enable this feature, select the check box. To disable the feature, clear the check box.

Enabling Packet Rewriting

Rewrite Packet instructs the access point to replace its measures for RSSI and LQI (which relate to message from the repeater) with the RSSI and LQI values the repeater has appended to its messages (as they represent an assessment of the sensor to repeater RF communications.) To enable this feature, select the check box. To disable the feature, clear the check box.

Enabling Expectation of Acknowledgments

Expect Acks directs sensors to report detection events as they occur and to expect acknowledgment packets from the access point. To enable this feature, select the check box. To disable the feature, clear the check box.

Entering Contact Closure Card Latency and Enabling Reverse Polarity

A fixed amount of latency can be applied to all signals sent to a traffic controller via a contact closure card. Additionally, the polarity of a contact closure card can be reversed. Consult with Sensys Networks before using these features.

Assigning an Access Point Color Code

The color code option allows the assignment any of 255 possible codes to an access point, thus making it possible for multiple signals to be carried over the same RF channel. The default is FF.

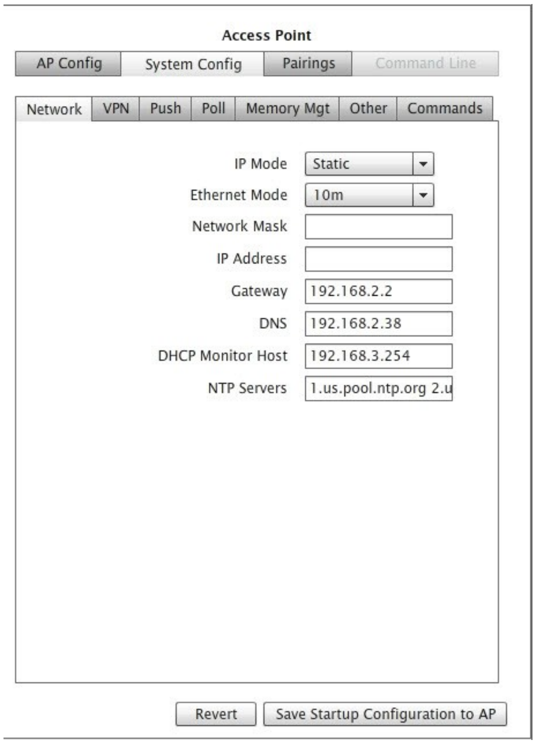
Working with the System Configuration Window

System parameters are properties of the network in an *external* sense. That is, these elements pertain to the network as an entity that communicates with other networks and systems. System parameters are grouped into the following collections:

- Network properties
- VPN (virtual private network) properties
- Modem properties
- Push settings
- Poll settings
- Memory management properties
- Other properties
- Command properties

Configuring with Network Properties

Network properties define the settings necessary to conduct IP communications with the access point including IP address, network mask, gateway and hosts providing DHCP, DNS and time services.



IP Mode: Static
Ethernet Mode: 10m
Network Mask:
IP Address:
Gateway: 192.168.2.2
DNS: 192.168.2.38
DHCP Monitor Host: 192.168.3.254
NTP Servers: 1.us.pool.ntp.org 2.u

Figure 5-13: Network Tab

Setting the IP mode

IP Mode specifies how the access point will receive its IP address such as via DHCP (the system default), a cellular ISP or other means. Click an entry from the drop down list to select it.

Note: The *Modem* tab displays only when the *IP Mode* element is set to *Modem*.

Setting the Ethernet mode

Ethernet mode designates the estimated bandwidth of the network link between the management station and the access point that operates on the access point's Ethernet interface. Click an entry from the drop down list to select it.

Specifying the Network Mask

Network Mask identifies the local portion of a local area network (LAN), and in so doing, identifies which hosts are communicated to through gateways. The system default is “`255.255.255.0`”.

Type in a network mask only if the specified IP mode (above) is “*static*” or if instructed by a service provider.

Specifying the IP Address

IP Address is a unique network address for IP communications to and from the access point over the Ethernet port. Type an IP address for the access point only if the specified IP mode (above) is "*static*" or if instructed by a service provider.

Designating the Gateway

Gateway identifies by IP address a network node to which the access point directs traffic destined for external networks. Type an IP address of a gateway server only if the specified IP mode (above) is "*static*" or if instructed by a service provider.

Designating the DNS Servers

DNS identifies by IP address a network node providing domain name services to the access point. Type an IP address of a DNS server only if the specified IP mode (above) is "*static*" or if instructed by a service provider.

Designating the DHCP Monitor Host

DHCP Monitor Host identifies by IP address a network node used by the access point to evaluate its connection to a host providing Dynamic Host Control Protocol services. Typically, the device used as the monitoring host is the DHCP server itself.

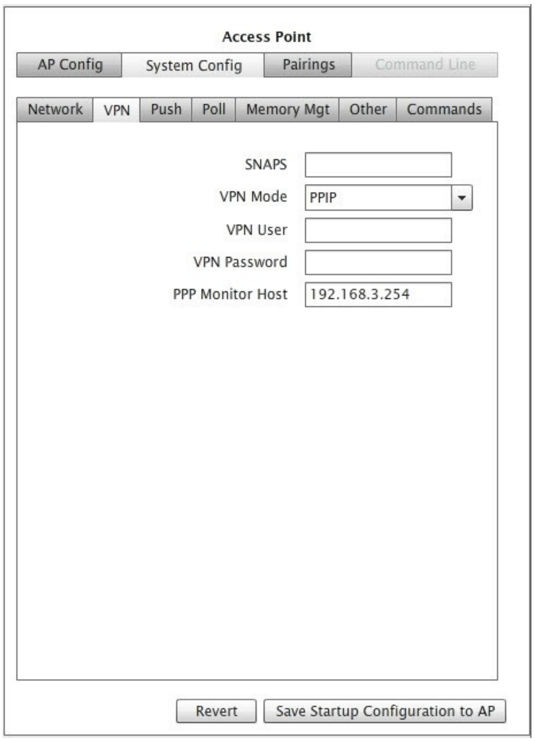
Specifying the Network Time Sources

NTP Servers specifies by hostname(s) a minimum of one server providing the current time via NTP (Network Time Protocol), a draft Internet standard for computer clock synchronization (see RFC1305). Type a minimum of one NTP hosts that provide network time services.

Configuring VPN Properties

VPN characteristics define the settings necessary to establish a virtual private network connection between the access point and and external server such as a management (SNAPS) server from Sensys Networks.

The VPN communication model is required in situations where the access point is positioned behind a firewall or router performing NAT (network address translation) services, receives its IP address via dynamic assignment, or is managed over a cellular packet data network.



SNAPS

VPN Mode: PPIP

VPN User

VPN Password

PPP Monitor Host: 192.168.3.254

Figure 5-14: VPN Tab (Optional)

Specifying the Sensys Networks Management Server

SNAPS identifies the host that acts as the VPN server. Type the host name or IP address of the management server. (*Note*: this is an optional component.)

Selecting the VPN Mode

VPN Mode specifies the protocol used for creating the VPN connection. Click an entry from the drop down list to select it.

Defining the VPN User and Password

Some VPNs require a user id and password for authentication and access to the VPN. These elements capture the values if they are required. Type a user id and password string adhering to the formatting rules of the VPN provider.

Specifying the Host to Monitor for VPN Communications

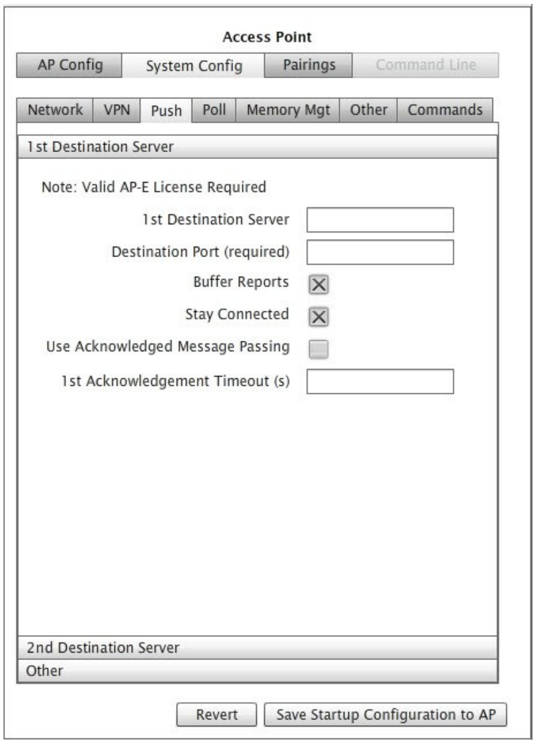
PPP Monitor Host names the host used by the access point to maintain the VPN connection. If the access point cannot contact this host for a duration of one minute or more, it drops the VPN connection and attempts to reconnect. Typically, this entry points to the VPN server itself. Type a host name or IP address.

Configuring Push Settings

A common requirement of event data statistics is the need to transfer it to other hosts or platforms. A typical technique to do this is referred to as *push*.

Push refers to movement of processed sensor data (i.e., statistical data) from one host to another initiated by the statistical server (typically an access point). This section describes the settings used by an access point's push process.

> **Note**: Use of this feature requires an appropriate license.



Note: Valid AP-E License Required

1st Destination Server
Destination Port (required)
Buffer Reports ☒
Stay Connected ☒
Use Acknowledged Message Passing ☐
1st Acknowledgement Timeout (s)

Figure 5-15: Push Tab 1st Destination Server

Destination servers

The hosts that act as the recipients of pushed data are referred to as *destination servers*. A destination server is a host that is equipped to receive processed sensor data for display, analysis or other purpose. Access points, when hosting the processes to generate statistical data from raw sensor reports, support up to *two* destination servers. At least one destination server must be designated; the second is optional.

1st Destination Server

Designates the target host by IP address or DNS name. *Note*: at least one entry is required in situations where the access point processes the raw sensor data.

Destination Port

The port number of the target server that the push process uses to communicate with it.

Buffer Reports

Designates the behavior of the access point in regard to how disconnections between the access point and the target host are handled.

Stay Connected

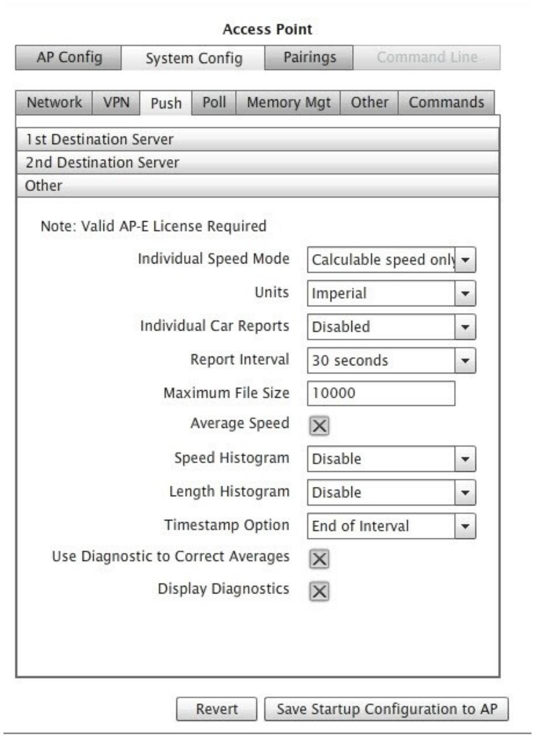
Designates the behavior of the access point in regard the status of the TCP connection during the idle time between separate “pushes” of the data from the access point to the destination servers.

Use Acknowledged Message Passing

Directs the behavior of the access point in regard to messages from the destination server that acknowledge receipt of the data transfers.

Acknowledgment Timeout

Specifies the number of seconds the push process waits for an acknowledgment packet from the destination host before declaring a transmission failure and retransmitting. An acknowledgment timeout value is available for each destination host.



Note: Valid AP-E License Required

Individual Speed Mode: Calculable speed only
Units: Imperial
Individual Car Reports: Disabled
Report Interval: 30 seconds
Maximum File Size: 10000
Average Speed: ☒
Speed Histogram: Disable
Length Histogram: Disable
Timestamp Option: End of Interval
Use Diagnostic to Correct Averages: ☒
Display Diagnostics: ☒

Figure 5-16: Push Tab (Other)

Individual Speed Mode

Determines how detection data is compiled in situations where vehicle speed and length cannot be calculated.

- *Calculable speed only* - reports only vehicles that have calculable speeds and lengths
- *All cars* - reports all vehicles regardless of the availability of speeds or lengths.

Units

Specifies the unit scale used in generating statistics. Select from the drop-down list one of the following:

- *Imperial* - denotes use of feet, miles and miles per hour (mph).
- *Metric* - denotes use of meters, kilometers and kilometers per hour (kmph).

Individual Car Reports

This element allows the designation of *real-time report* mode in which statistics are generated based on individual vehicle detections. Select from the drop-down list one of the following:

- *Disabled* – turns off the function
- *Standard* – produces output in Sensys Networks default format
- *Marksman* – produces output that complies with the Marksman specification

Report Interval

In aggregate report mode, this element specifies the time duration between writing of separate statistical report entries. In real-time report mode, this element specifies the time duration between creating separate statistical files. Select from the drop-down list one of the following:

- 10 seconds
- 15 seconds
- 30 seconds
- 1 minute
- 5 minutes
- 10 minutes
- 15 minutes

Maximum File Size

Specifies the maximum file size (in bytes) of any single statistical archive file.

Average Speed

Enables/disables the inclusion of the calculated average speed in the collection of data outputs. When average speed is enabled, this element also qualifies how the calculation of the average is performed.

Speed Histogram

Enables/disables the inclusion of speed bins suitable for building a histogram graph. Select from the drop-down list one of the following:

- *Disable* – disables the function
- *1 mph*
- *5 mph*
- *TTI* – presents data in bin widths from the Texas Traffic Institute specification

Length Histogram

Enables/disables the inclusion of length bins suitable for building a histogram graph. Select from the drop-down list one of the following:

- *Disable* – disables the function
- *1 foot*
- *TTI* – presents data in bin widths from the Texas Traffic Institute specification

Timestamp Option

Designates the point in time – relative to the entire length of reporting interval – that corresponds to the timestamp of the report entry. Select from the drop-down list one of the following:

- *End of interval*
- *Start of interval*
- *Middle of interval*

Use Diagnostic Correct to Averages

Enables/disables the use of sensor diagnostic data to generate “smart averages” when calculating averages for speeds and lengths. Smart averages disregard non-reporting sensors.

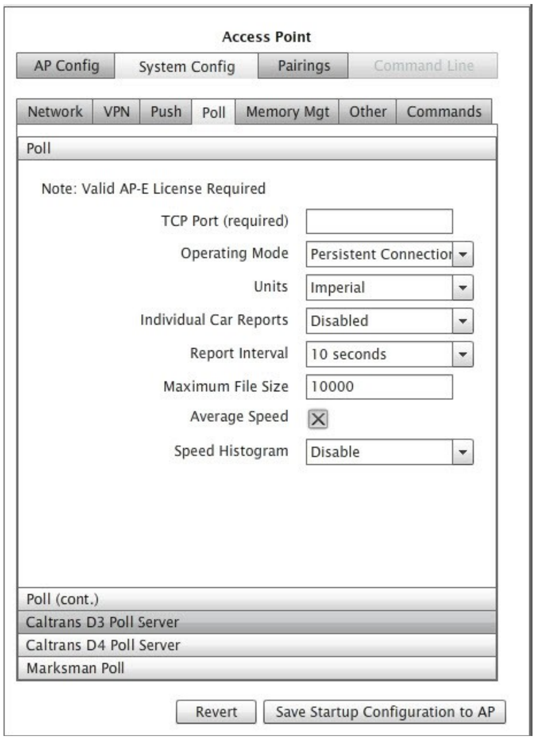
Display Diagnostics

Enables/disables inclusion of the sensor diagnostic values in the output data collection.

Configuring Poll Settings

A common requirement of event data statistics is the need to transfer it to other hosts or platforms. An accepted technique to do this is referred to as *poll*. *Poll* refers to movement of processed sensor data from the statistical server (typically, an access point) to another host based on a request by the consuming host. This section describes the settings that comprise the generic polling interface of Sensys Networks.

> **Note**: Use of this feature requires an appropriate license.



Note: Valid AP-E License Required

TCP Port (required)

Operating Mode: Persistent Connectio

Units: Imperial

Individual Car Reports: Disabled

Report Interval: 10 seconds

Maximum File Size: 10000

Average Speed ☒

Speed Histogram: Disable

Figure 5-17: Poll Tab (Other)

TCP Port Number

A required value specifying the port number on which poll requests arrive. The Sensys Networks statistical host listens for requests on this port.

Operating Mode

Specifies the nature of the connection between an access point's Poll process and the remote host. Select from the drop-down list one of the following:

- *Persistent Connection* – indicates that once a connection is established it remains in force. Reports are available at the end of the *report interval* (discussed below). For example, given a report interval of 30 seconds, if a connection is made 16 seconds into the interval, the first report would be available 14 seconds after the connection was made.

- *Connection-based Polls* – indicates that a connection is built, used and closed for each successive poll from the remote host.
- *Poll Sampling* – (*default*) indicates that a connection is treated as a request. That is, upon receiving a request, the most recent report is delivered to the client and the connection is closed. There is no built-in processing to prevent sending duplicate reports. Thus, if a subsequent connection is made before a new report is available, the same report is sent to the subsequent connection.

Units

Specifies the unit scale used in generating statistics. Select from the drop-down list one of the following:

- *Imperial* - denotes use of feet, miles and miles per hour (mph).
- *Metric* - denotes use of meters, kilometers and kilometers per hour (kmph).

Individual Car Reports

This element allows the designation of *real-time report* mode in which statistics are generated based on individual vehicle detections. Select from the drop-down list one of the following:

- *Disabled* – turns off the function
- *Standard* – produces output in Sensys Networks default format
- *Marksman* – produces output that complies with the Marksman specification

Report Interval

In aggregate report mode, this element specifies the time duration between writing of separate statistical report entries. In real-time report mode, this element specifies the time duration between creating separate statistical files. Select from the drop-down list one of the following:

- 10 seconds
- 15 seconds
- 30 seconds
- 1 minute
- 5 minutes
- 10 minutes
- 15 minutes

Maximum File Size

Specifies the maximum file size (in bytes) of any single statistical archive file.

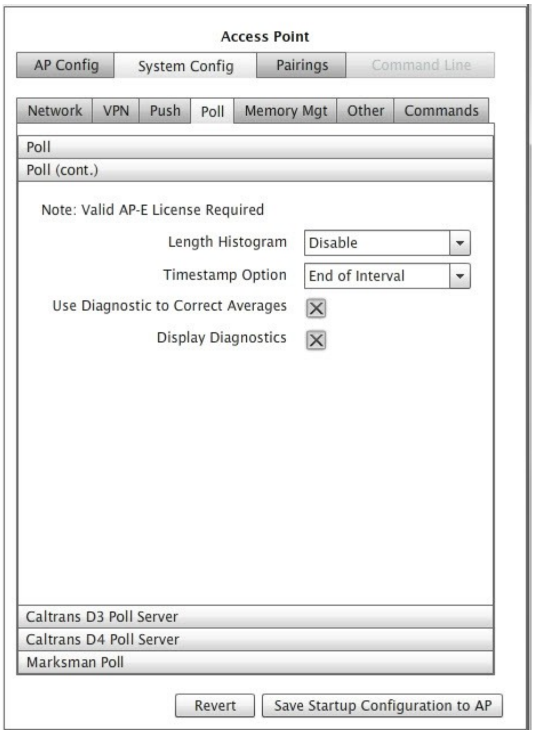
Average Speed

Enables/disables the inclusion of the average speed in the collection of data outputs.

Speed Histogram

Enables/disables the inclusion of speed bins suitable for building a histogram graph. Select from the drop-down list one of the following:

- *Disable* – disables the function
- *1 mph*
- *5 mph*
- *TTI* – presents data in bin widths from the Texas Traffic Institute specification



Note: Valid AP-E License Required

Length Histogram: Disable

Timestamp Option: End of Interval

Use Diagnostic to Correct Averages ☒

Display Diagnostics ☒

Figure 5-18: Poll Tab (cont.)

Length Histogram

Enables/disables the inclusion of length bins suitable for building a histogram graph. Select from the drop-down list one of the following:

- *Disable* – disables the function
- *1 foot*
- *TTI* – presents data in bin widths from the Texas Traffic Institute specification

Timestamp Option

Designates the point in time – relative to the entire length of reporting interval – that corresponds to the timestamp of the report entry. Select from the drop-down list one of the following:

- *End of interval*
- *Start of interval*
- *Middle of interval*

Use Diagnostic to Correct Averages

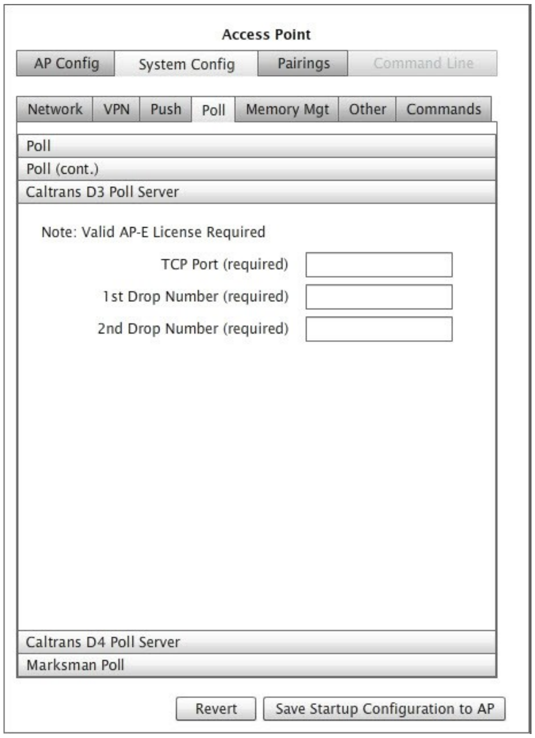
Enables/disables the use of sensor diagnostic data to generate "smart averages" when calculating averages for speeds and lengths. Smart averages disregard non-reporting sensors.

Display Diagnostics

Enables/disables inclusion of the sensor diagnostic values in the output data collection.

Configuring California DOT District 3 Poll Servers

This section describes the settings that comprise the Sensys Networks polling interface developed for CalTrans D3 Poll Servers. Use of this feature requires an appropriate license.



Note: Valid AP-E License Required

TCP Port (required)

1st Drop Number (required)

2nd Drop Number (required)

Figure 5-19: Caltrans D3 Poll Server

TCP Port Number

A required value specifying the port number on which poll requests arrive. The Sensys Networks statistical host listens for requests on this port.

1st Drop Number

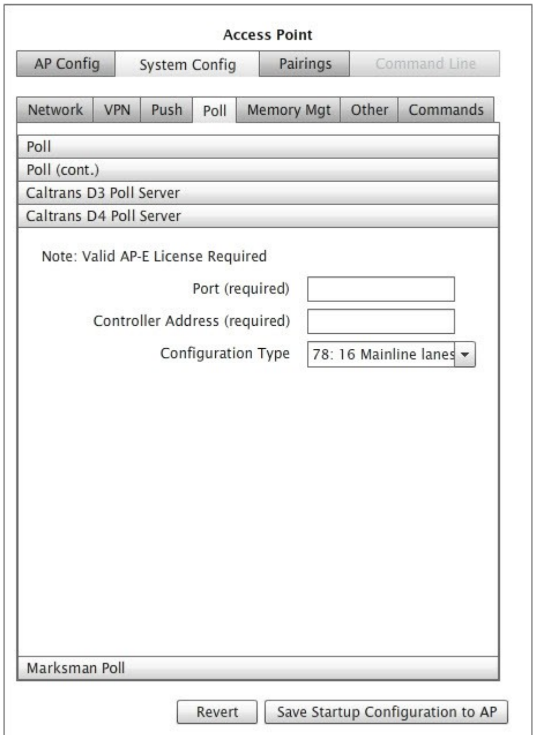
A required value originated by the polling client used by the statistical server to formulate a response message.

2nd Drop Number

A required value originated by the polling client used by the statistical server to formulate a response message.

Configuring California DOT District 4 Poll Servers

This section describes the settings that comprise the Sensys Networks polling interface developed for CalTrans D4 Poll Servers. Use of this feature requires an appropriate license.



Note: Valid AP-E License Required

Port (required)

Controller Address (required)

Configuration Type: 78: 16 Mainline lanes

Figure 5-20: Caltrans D4 Poll Server

Port Number

A required value specifying the port number on which poll requests arrive. The Sensys Networks statistical host listens for requests on this port.

Controller Address

A required value used by the statistical server to formulate a response message. Must be an integer between 1 and 255.

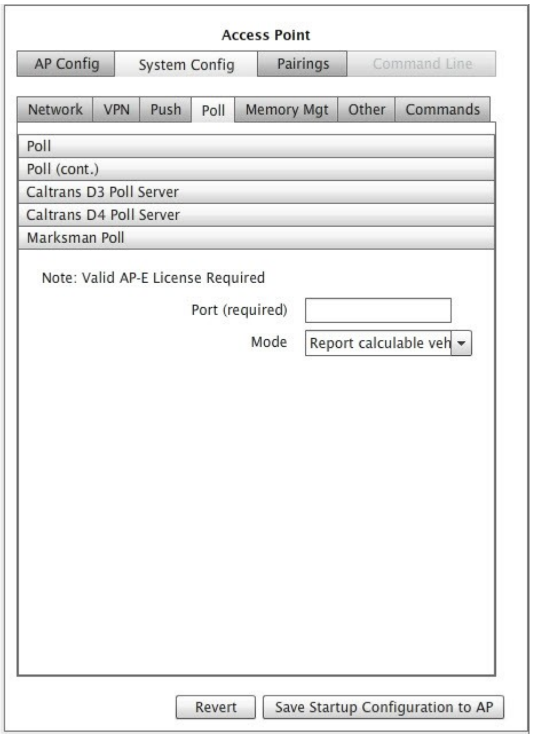
Configuration Type

Indicates the layout of the traffic site via a series of predefined configurations.

- 71: 8 Mainline lanes, 0 Ramp lanes
- 72: 8 Mainline lanes, 4 Ramp lanes
- 74: 12 Mainline lanes, 4 Ramp lanes
- 78: 16 Mainline lanes, 8 Ramp lanes

Configuring Marksman Poll Servers

Event statistics can be formatted to adhere to the Marksman protocol portion of the Australian Roads specification. Specifying these values results in a new instance of the APSTAT process being invoked the next time the access point is rebooted. Use of this feature requires an appropriate license.



Note: Valid AP-E License Required

Port (required)

Mode: Report calculable veh

Figure 5-21: Marksman Poll Server

Designating the Port Number

Port stores a required integer value that specifies the port the access point listens to for report requests.

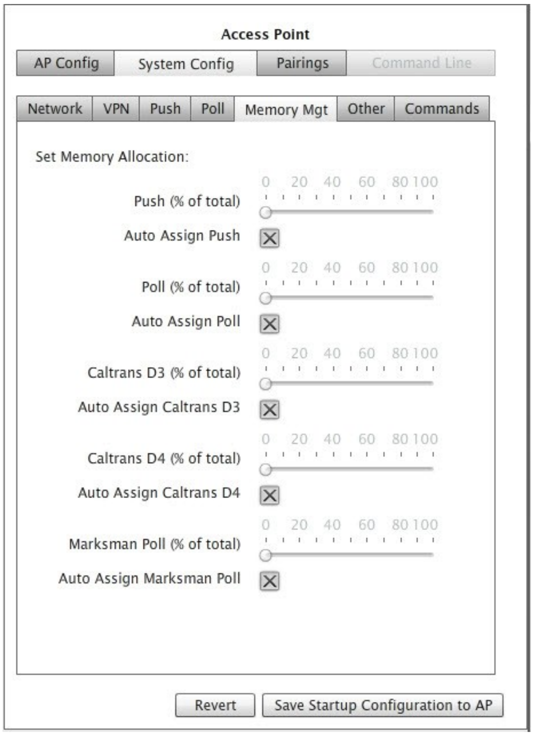
Selecting a Reporting Mode

Mode specifies the scope of the output data collection. From the *Mode* drop-down list select either of the following:

- Report calculable vehicles
- Report all

Configuring Memory Settings

Access points typically host application processes that perform data transfer and formatting; the processes are configured on the *Push*, *Poll*, *CalTrans D3 Poll*, *CalTrans D4 Poll* and the *Marksman Poll* tabs. A total of **500KB** of memory is allocated to local applications. The memory allocation is configured via the *Memory Mgt* tab.



Set Memory Allocation:

Push (% of total) 0
Auto Assign Push ☒
Poll (% of total) 0
Auto Assign Poll ☒
Caltrans D3 (% of total) 0
Auto Assign Caltrans D3 ☒
Caltrans D4 (% of total) 0
Auto Assign Caltrans D4 ☒
Marksman Poll (% of total) 0
Auto Assign Marksman Poll ☒

Figure 5-22: Memory Mgt Tab

Window Contents and Operation

The tab displays a slide bar and check box related to memory allocation to the application processes that may execute on an access point. The slide bar and check box are active only for processes that are executing on the access point. If the window elements are not accessible, the access point is not licensed for the processes or they are not running.

Automatically Allocating Memory to the Processes

By default, the system automatically allocates memory equally among each of the executing processes. Fill the *Auto Assign* check box(es) to specify this.

Manually Allocating Memory to the Processes

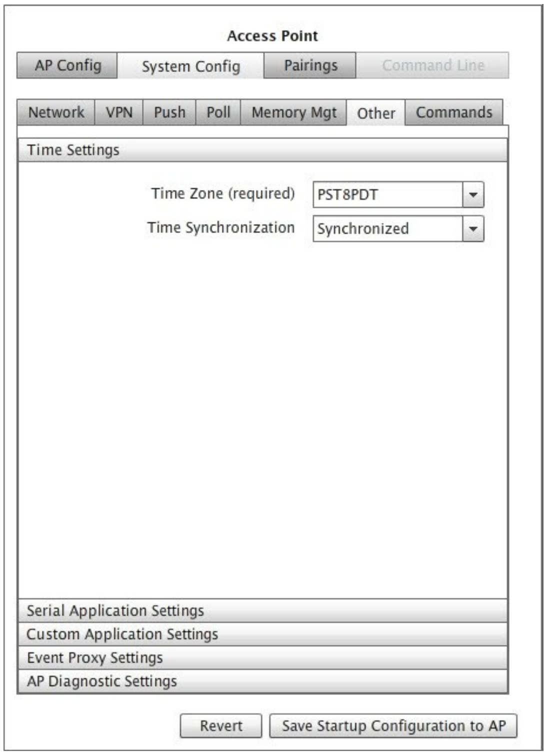
To manually set the memory allocated to one or more of the processes, do the following:

1. Locate the the slide bar related to the desired application and move it to indicate the desired percentage of application memory (500 KB) allocated to that process.
2. Click *Save Startup Configuration to AP*. This writes the change to the access point's configuration file but does not reallocate memory.
3. Reboot the access point to allocate memory according to the configuration settings.

Configuring Other Properties

The *Other* tab provides an opportunity to configure elements that are more advanced or specialized. These element include:

- Enabling the access point to interface to traffic signal controllers
- Enabling the high accuracy speed mode for the access point
- Enabling the direct interface to Siemens signal controllers
- Direct access to sensor event data via a proxy process
- Time synchronization settings
- Configuring serial mode settings
- Configuring advanced access point diagnostics settings



Time Zone (required): PST8PDT

Time Synchronization: Synchronized

Figure 5-23: Other Tab (Time Settings)

Time Settings

Time is used throughout networks for a variety of purposes. An access point can be configured to enforce on the entire network a uniform timebase sourced from a trusted timeserver.

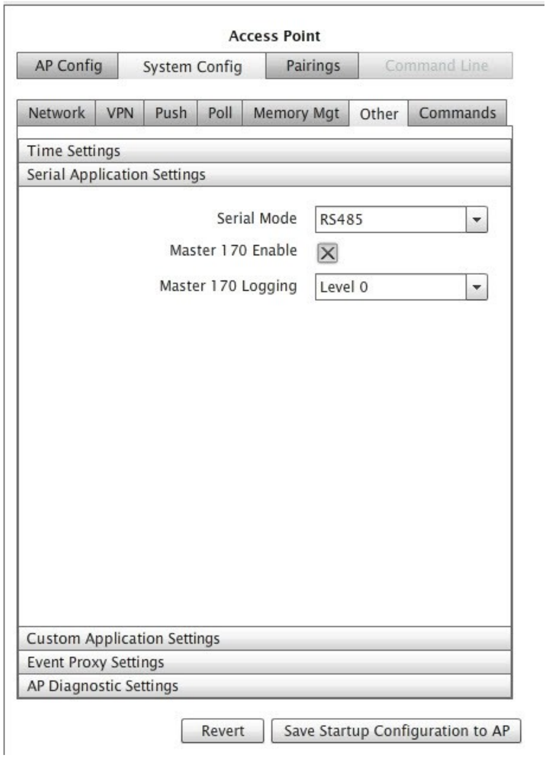
Time Zone

A required setting that designates the access point as residing in a particular time zone. A range of common North American timezones, as well as an array of *offsets from GMT* (Greenwich Mean Time) are supported.

Time Synchronization

Enables/disables synchronizing the radio clocks of all network devices to the Linux timekeeping process on the access point. Sensys Networks recommends enabling this feature and configuring the access point to acquire time from a trusted, external time server. The options supported are:

- *Synchronized* – where a base time is acquired from a timeserver and distributed throughout the network by the access point
- *Free Running* – each device uses its own internal clock.



Serial Mode RS485

Master 170 Enable ☒

Master 170 Logging Level 0

Figure 5-24: Other Tab (Serial Application Settings)

Serial Application Settings

Access points support serial communications over two on-board serial ports for communications with traffic controller equipment, cellular data networks, GPS systems or maintenance consoles.

Serial port "A" is configured by hardware settings only.

Serial Mode

Specifies how the access point configures the serial port "B" for use. Supported options include:

- *Disable* – removes the port from the active configuration of the access point
- *GPS* – sets the port for communications with a GPS system
- *RS485* – sets the port for communications with traffic signal control equipment via a contact closure card from Sensys Networks. This setting is mandatory for using the access point with signal controllers.

Enabling the Master 170 Interface for Traffic Signal Controllers

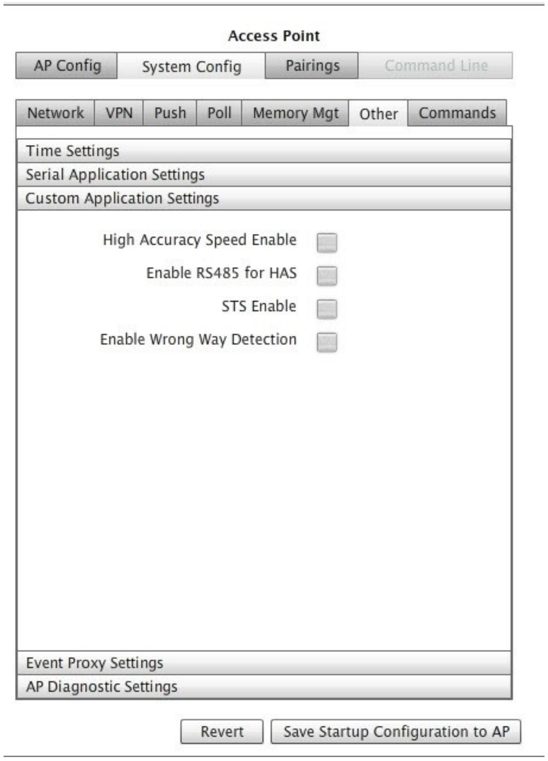
Access points can be interfaced to a variety of popular traffic signal controllers. Enable this setting on access points that will interface to such systems by filling the check-box.

Note: This setting only results in the execution of software on an access point required for traffic signal controller interfaces. Additional equipment from Sensys Networks (in the form of a CC card) is required to physically interface a Sensys Networks to a traffic signal controller.

Enabling Logging for the Master170 Interface

System logging records a range of operations between an access point and a traffic signal controller to which it is interfaced. Select via the drop-down list a logging level ranging from *no* logging (level zero) to *extensive* logging (level two).

Note: Logging requires more disk space so the typical practice is use this feature only for monitoring a new system at start-up or for troubleshooting.



High Accuracy Speed Enable ☐

Enable RS485 for HAS ☐

STS Enable ☐

Enable Wrong Way Detection ☐

Figure 5-25: Other Tab (Custom Application Settings)

Enabling High Accuracy Speed Mode

High Accuracy Speed (HAS) mode is useful for networks implemented for red-light enforcement. Fill the check-box to enable the feature.

Note: Enabling this feature requires that sensors are configured to operate using mode **H**.

Enabling RS485 for HAS

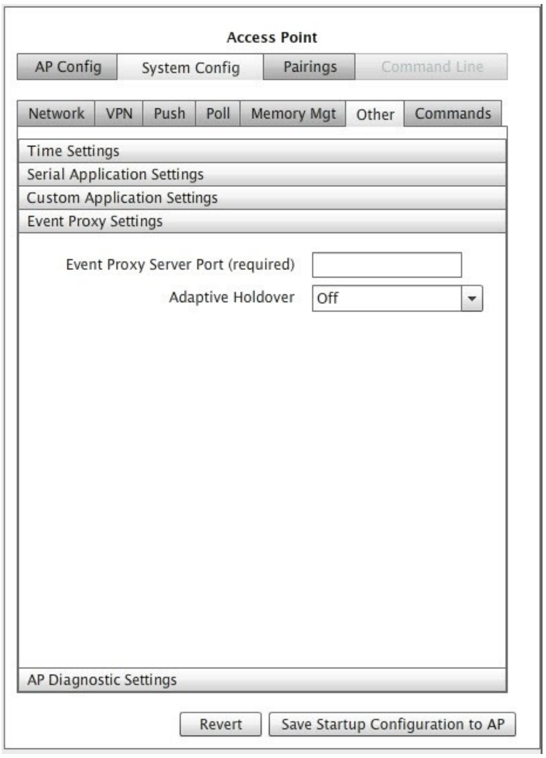
RS485 for HAS sets the port for communications with traffic signal control equipment via a contact closure card from Sensys Networks for high accuracy speed. Fill the check-box to enable the feature.

Enabling the Interface to Siemens Traffic Systems (STS)

STS Enable directs an access point to operate with a Siemens traffic controller over a proprietary interface. Fill the check-box to enable the feature. Do not enable this feature unless the access point is used with the appropriate Siemens equipment.

Enabling Wrong Way Detection

Wrong Way Detection is a Sensys Networks application that detects the direction of vehicles entering a section of road the wrong way, and allows for an emergency warning to oncoming vehicles, as well as the immediate notification of the appropriate emergency response. Fill the check-box to enable the feature.



Event Proxy Server Port (required)

Adaptive Holdover: Off

Figure 5-26: Other Tab (Event ProxySettings)

Event Proxy Settings

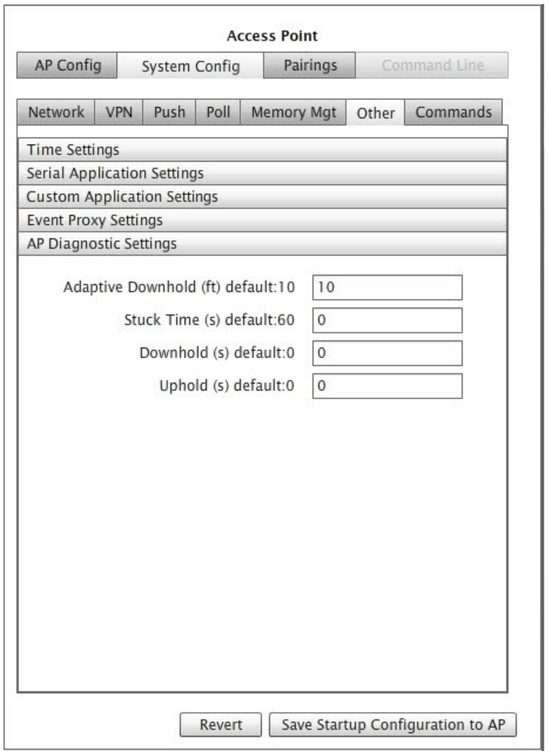
Sensor event data can be accessed by a simple line-oriented interface over TCP/IP. End users can use clients such as `telnet` to access and display event data as ASCII text.

Direct Access to Sensor Event Data

Event Proxy Server Port provides a text/line oriented interface to event data. It is intended for use by field technical staff.

Adaptive Holdover

Enables/disables the automatic adjustment of the *downhold* parameter. When enabled, the value specifies in feet the magnitude of the adjustment.



Adaptive Downhold (ft) default:10 10
Stuck Time (s) default:60 0
Downhold (s) default:0 0
Uphold (s) default:0 0

Figure 5-27: Other Tab (AP Diagnostic Settings)

Advanced AP Diagnostic Settings

These elements are used in regard to the automatic performance diagnostic reporting done by the access point by the instance of APDIAG that executes on the access point.

Adaptive Downhold (feet)

Type the length in feet used by the adaptive downhold calculation.

The algorithm calculates the amount of time the count, speed, and occupancy calculations must holdover based on an average of the five most recent speeds calculated. Time is derived from the entered length, using average speed.

The default value is 10 feet.

Stuck Time (seconds)

Type a number of seconds a sensor must report a continuous "vehicle present" state before it is considered non-reporting.

The default is 60 seconds.

Downhold (seconds)

Type a number of seconds an undetection signal must last before it is considered to represent an undetection event. The default value is zero seconds.

Uphold (seconds)

Type a number of seconds a sensor must report a continuous "vehicle present" state before

Working with the Commands Window

The *Commands* window provides the ability to backup and restore access point configuration, install and/or update an access point's license file, and download a diagnostic file.

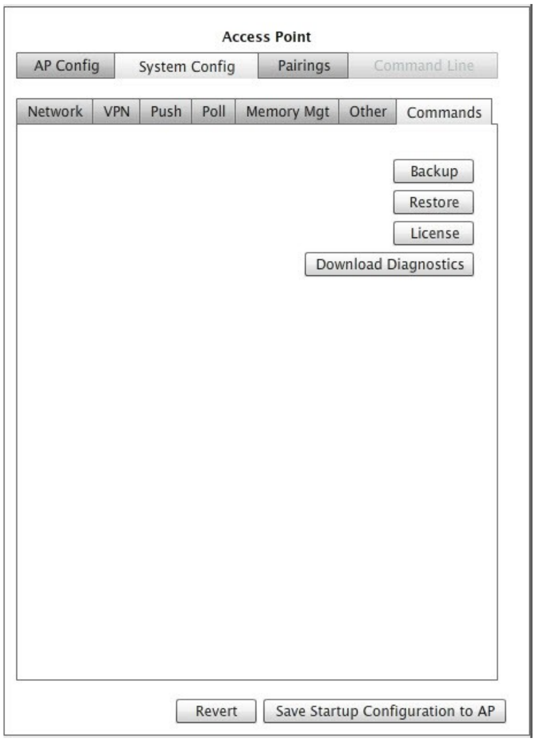


Figure 5-28: Commands Tab

Backup / Restore an Access Point's Configuration

Sensys Networks recommends backing up the configuration of an access point once it has been finalized, as well as immediately before and after any significant changes are made.

By default, backups are stored on the file system of the platform that hosts TrafficDOT.

Backup Procedure

To backup the current access point configuration, perform the following steps:

1. Click *Backup* from the *Commands* tab. The *Save Backup* window displays.
2. Name the file to store the backup. Optionally, store the file to a different folder than the default.
3. Click *Save Startup Configuration to AP* to backup the access point.

Restore Procedure

To restore an access point configuration and data, perform the following steps:

1. Click *Restore* from the *Commands* tab. The *Select files to use for restore* window displays.
2. Select the file that contains the backup that will serve as the source for the restore. Optionally, navigate to a different folder than the default.
3. Click *Open* to restore the access point from the file.

Selecting an Access Point License File

Sensys Networks stores customer permissions and product access keys in a license file stored on the access point. From time to time, there may be a need to update it.

To install/update an access point license file, perform the following steps:

1. From the *Commands* tab, click *License*. The *Select License* window displays.
2. Select the file that contains the license for the access point. Optionally, navigate to a different folder than the default.
3. Click *Open* to install or update the license file.
4. After the license file has been transferred to the access point, reboot the access point.

Note: The license will not take effect until the access point is rebooted.)

Downloading a Diagnostic File

On rare occasions, Sensys Networks Technical Support group may request a diagnostic file. This is a special type of backup that facilitates analysis of the access point and its processes.

This operation is follows a procedure very similar to that of performing a backup. Work with the Technical Support group to determine the best means to transfer the file to Sensys Networks.

Configuring Repeaters

Sensys Networks repeaters ship with a factory-installed default configuration. In most cases, the configuration is modified to fit the specific needs of an installation. However, once set, a repeater's configuration typically requires no further changes.

This section describes configuring repeaters with TrafficDOT and provides information about the following activities:

- Selecting a repeater to configure
- Specifying which time slot configuration a repeater will use
- Specifying the repeater's two RF channels
- Assigning a time slot to a repeater
- Downloading firmware to a repeater
- Adding a repeater to a network
- Removing a repeater from a network
- Performing other operations

Introduction

Repeater configuration involves dragging a repeater onto the map image and selecting values for the following parameters:

- Repeater configuration
- Radio frequency of the upstream (access point) channel
- Radio frequency of the downstream (sensor) channel
- Transmission time slot (optional)

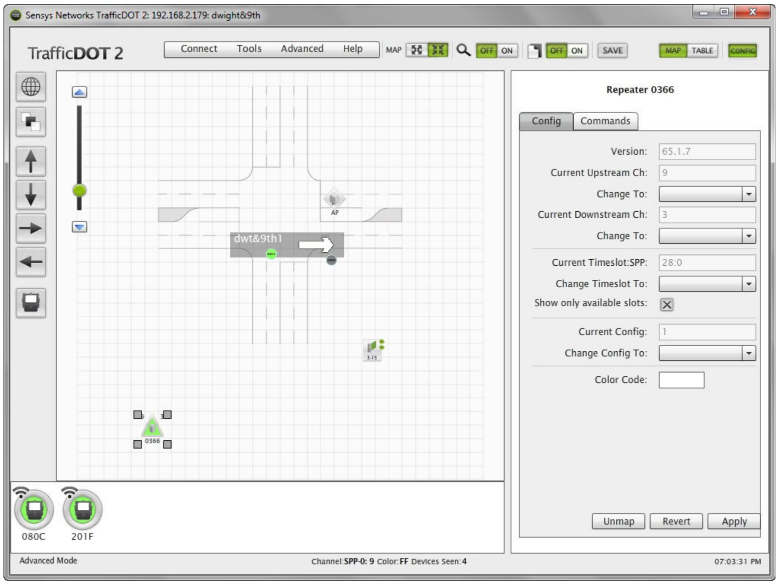
Other operations related to management of repeaters are also performed from the *Repeater Configuration* window.

Note Regarding Tandem Repeaters

Repeaters used to forward the signals of other repeaters (tandem repeaters) are configured in the same way as repeaters communicating directly with an access point. Tandem repeater topologies are implied by the RF channel assignments made to separate repeaters.

Working with the Repeater Configuration Window

To select a repeater for configuration, click on a repeater on your image map. The Repeater. *Configuration* window displays.



Repeater 0366

Version: 65.1.7
Current Upstream Ch: 9
Change To:
Current Downstream Ch: 3
Change To:
Current Timeslot:SPP: 28:0
Change Timeslot To:
Show only available slots: ☒
Current Config: 1
Change Config To:
Color Code:

Advanced Mode Channel:**SPP-0: 9** Color:**FF** Devices Seen:**4** 07:03:31 PM

Figure 5-29: Repeater Configuration Window

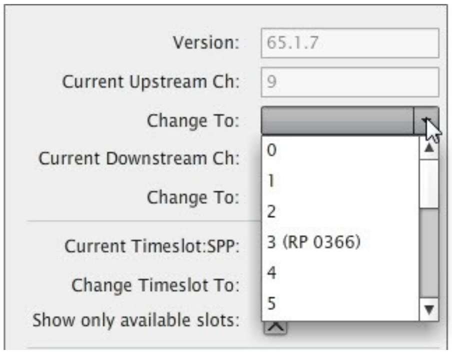
Specifying the RF Channels

Repeaters are configured with two RF channels. The first – known as the access point or upstream channel – is used to communicate with an access point. This channel is set in the access point's configuration. The second – known as the sensor or downstream channel – is used to communicate with sensors. This channel **must** not be the same channel as the access point channel.

Specifying the Access Point (Upstream) Channel

To specify the RF channel for access point transmissions, perform the following steps:

1. Click an entry from the upstream *Change To* drop-down list.



Version: 65.1.7
Current Upstream Ch: 9
Change To:
- 0
- 1
- 2
- 3 (RP 0366)
- 4
- 5

Current Downstream Ch:
Change To:
Current Timeslot:SPP:
Change Timeslot To:
Show only available slots:

Figure 5-30: Changing Current Upstream

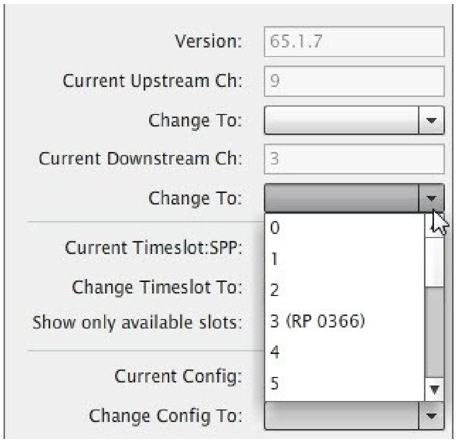
The selected channel **must be the same** RF channel that the target access point is configured to use. (See the *Configuring Access Points* section in this chapter for more information.)

2. Click *Apply*.

Specifying the Sensor (Downstream) Channel

To specify the RF channel for transmissions in the direction of sensors, do the following:

1. Click an entry from the downstream *Change To* drop-down list.



Version: 65.1.7
Current Upstream Ch: 9
Change To:
Current Downstream Ch: 3
Change To:
- 0
- 1
- 2
- 3 (RP 0366)
- 4
- 5

Current Timeslot:SPP:
Change Timeslot To:
Show only available slots:
Current Config:
Change Config To:

Figure 5-31: Changing Current Downstream

The selected channel **must not be the same** than the channel selected as the access point channel. In addition, all sensors serviced by the repeater must be configured to use the repeater's sensor channel.

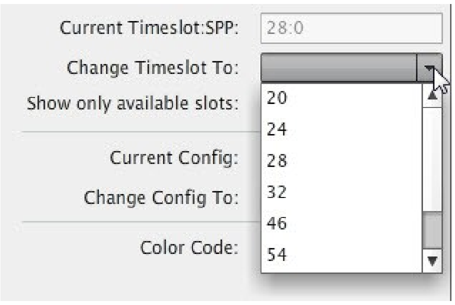
2. Click *Apply*.

Setting the Time Slot of a Repeater

In addition to forwarding event data packets to the access point and management packets to the sensors it services, repeaters originate packets of their own. Normally, repeaters transmit these “repeater packets” via a sensor time slot when the repeater detects that a sensor is not transmitting.

In some instances, however, it may be beneficial to restrict the repeater's use to a defined time slot as a means to eliminate competition to transmit. To set the time slot, do the following:

1. Click an entry from the *Change Timeslot To* drop-down list.



Current Timeslot:SPP: 28:0

Figure 5-32: Changing Timeslot

By default, TrafficDOT filters the contents of the drop-down list so that only available time slots (that is, time slots that are consistent with the network's transmit interval and not already assigned) are displayed.

To change the drop-down list to include all time slots in the network (both assigned and unassigned), remove the check in the check-box to the right of the *Show only available slots*.

The list does not include time slots that are, by definition, reserved for use by access points.

2. Click *Apply*.

Configuring Contact Closure Cards

The Sensys Networks VDS240 wireless vehicle detection system can be interfaced directly to local traffic signal controllers such as the CalTrans Type 170, Type 2070 ATC and NEMA TS-1 and TS-2 controllers via a hardware interface card installed into the controller cabinet. The interface allows detection events collected by an access point to activate contact closure relays in the controller.

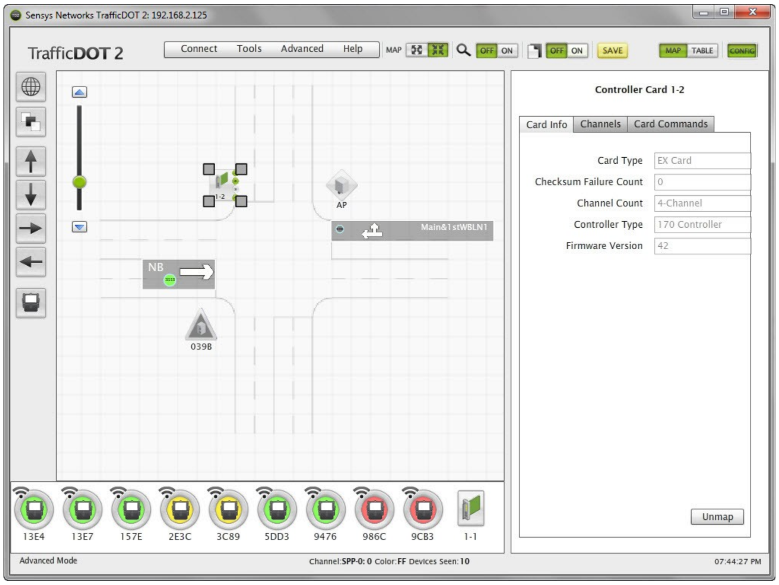
This section describes configuring and working with contact closure cards via TrafficDOT. The following activities are discussed:

- Entering controller card information
- Configuring channel state
- Configuring channel mode

- Configuring presence mode modifier
- Configuring channel holdover duration
- Setting watchdog fail mode
- Working with command properties

Working with the Controller Card Configuration Window

To select an access point for configuration, click on an access point on your image map. The *Controller Card Configuration* window displays.



Controller Card 1-2

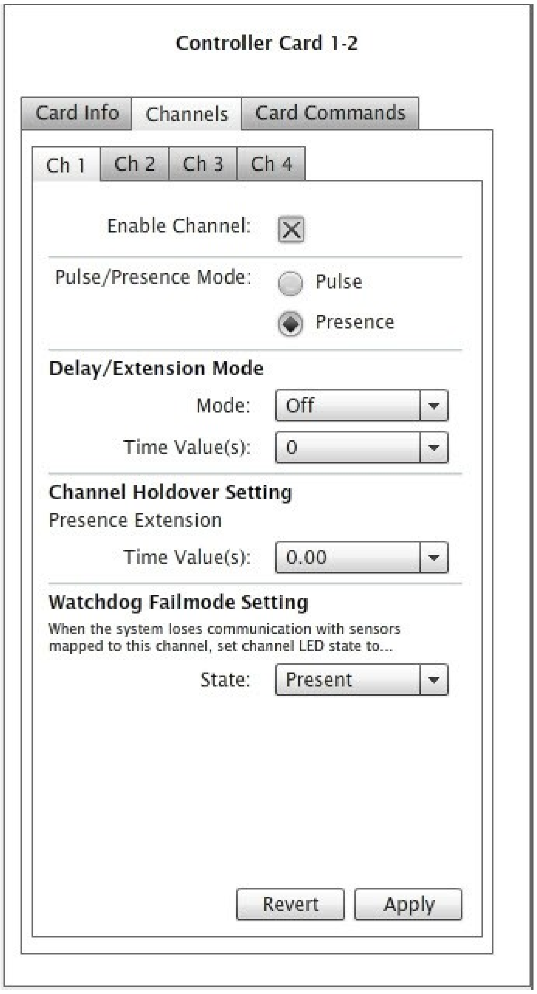
Card Type: EX Card
Checksum Failure Count: 0
Channel Count: 4-Channel
Controller Type: 170 Controller
Firmware Version: 42

Channel:SPP-0: 0 Color:FF Devices Seen:10

Figure 5-33: Controller Card Configuration Window

Entering controller card information

To enter controller card information, select the controller card image on the map and enter the information into the *Configuration Panel*, or drag and drop a sensor onto the controller card icon, and then enter the information.



Enable Channel: ☒

Pulse/Presence Mode: ○ Pulse ● Presence

Delay/Extension Mode

Mode: Off

Time Value(s): 0

Channel Holdover Setting

Presence Extension

Time Value(s): 0.00

Watchdog Failmode Setting

When the system loses communication with sensors mapped to this channel, set channel LED state to...

State: Present

Figure 5-34: Controller Card Channels Tab

Configuring Controller Card Channels

Channels refer to the vehicle detection relays of contact closure cards. Each channel consists of an optically isolated contact closure and, for cards in TS2 compatibility mode, a status contact closure to ground. Channels are independent of one another and are referred to by number (one through four).

A predetermined set of sensors (and the vehicle detection events they transmit) are grouped together by the access point and supplied to a contact closure card via one of the channels. The contact closure card, in turn, activates the channel's contact closure relay based on the vehicle detection data.

A single channel may support up to 15 sensors whose detection events are evaluated in combination (in a logical or operation). If any one of the sensors detects a vehicle, the corresponding contact closes.

Contact closure cards are available in four-channel versions. Each channel may be individually enabled/disabled and configured.

Note: The cards physically occupy one slot, but an optional extender can be used so that the card occupies two slots.

Configuring Channel State

Contact closure card channels are independent of one another and are individually configured. Each channel occupies one of the following states:

- *Enabled* – the channel is operational; Sensor event data collected by the access point is transmitted to the contact closure card.
- *Disabled* – the channel is not operational. (When a channel is disabled, its contact closure relay and status relay are continuously open.)

The factory default configuration enable channels one and two. Ensure that any unused or unavailable channels are disabled.

Configuring Channel Mode

Enabled channels operate in one of the following modes:

- *Pulse* – the contact closure relay pulses for 0.125 seconds each time the leading edge of a vehicle is detected.
- *Presence* – the contact closure relay remains closed while a vehicle is detected.

The factory default setting is *pulse* mode.

Configuring Presence Mode Modifier

The behavior of a channel operating in *presence* mode may adjusted by applying one of the following modifiers:

- *Delay* – defers the onset of the contact closure by a specified duration. If a vehicle moves off of the Sensor before the specified delay expires, the contact does not close. Delay is expressed in seconds from zero to 31.
- *Extension* – increases the duration of the contact closure by a specified increment. Extension is expressed in half-seconds from zero to 7.5.

The modifiers do not apply to channels operating in *pulse* mode.

Configuring Channel Holdover Duration

The *Channel Holderover* parameter allows an extension to the channel holdover duration when it is activated by the events from a particular sensor. Values from 0.0to 0.75 are available for selection.

Chapter 6

Monitoring Components Using the Table View

This chapter provides information on *monitoring* Sensys Networks VDS240 wireless vehicle detection components using the *table view* in TrafficDOT.

Overview

Like the map view, the t*able view* in TrafficDOT provides a real-time view into the components of the network and the events they detect. All sensors in the network are shown, including sensors that communicate via repeaters. Detection counts, detection events, RF quality metrics, version and battery information are shown in dedicated columns updated at one second intervals.

The table view consists of three display areas:

- Menus – drop-down options providing access to specific functions
- System Display – tabular, real-time display of the network including RF quality indicators, detection events and other information
- Configuration panels – the configuration panels for the key components discussed in the *Configuring and Managing Components* chapter are also accessible in the table view.

Menus

The menus in TrafficDOT are related commands and functions organized into logical groups. The menus of the table view include:

Connect

- *Connect* - Connects TrafficDOT to an access point

- *Disconnect* - Disconnects TrafficDOT from an access point

Tools

- *Scan For Devices* – Performs device scans on selected or all RF channels
- *Auto-assign Timeslots* – Automatically assigns device timeslots
- *Graphs/Charts* – Provides the ability to create diagnostic real time diagrams indicating sensor detection data
- *Browse to ...* – Activates a local HTTP browser
- *Prune Sensors and Repeaters from Tray* – Removes all sensors and repeaters from the component tray
- *Turn on SNC Proxy Logging* – Enables logging for the SNC proxy process
- *Preferences* – Enables the ability to set system preferences for connection timeout and RF quality thresholds. Also allows for setting user ID and password for FTP services hosted by the access point

Advanced

- *Set Advanced Mode* – Allows for access to advanced device settings
- *Set Super User Mode* – Allows authentication for diagnostic mode access

Help

- *About* – Provides access point version information
- *Help* – Provides access to the *TrafficDOT 2 Set Up and Operating Guide* (this document)

System Display

The system display consists of sortable columns that can be displayed in ascending or descending order by clicking on the column's heading. The columns of the display are identified in the table below and discussed further in the sections that follow:

Column Name	Description
Id	The factory assigned hardware device identifier. Sensors and repeaters are uniquely identified by a 64-bit value. This column displays the least significant 16 bits as a 4-character HEX string.
Repeater	The device id of the repeater servicing a sensor (if applicable). *AP* indicates a sensor is transmitting to the access point without using a repeater.
Channel	The RF channel on which the device is transmitting.
Sensor Location Id	The field is populated automatically using the information in the *Sensor Position Window* and the lane abbreviation.

Column Name	Description
H Position	Sensor's horizontal position relative to other sensors in the same lane. Values may be -3, -2, -1, 0, 1, 2 or 3 where -3 indicates the far-left sensor; -2 indicates the mid-left sensor; -1 indicates the left; 0 indicates the center sensor; 1 indicates the right sensor; 2 indicates the mid-right, and 3 indicates the far-right sensor.
V Position	Sensor's vertical position relative to other sensors in the same lane. This element is used to identify sensor speed pairs. Values may be 0, 1 or 2 where 0 indicates the lead sensor, 1 indicates a trailing sensor, and 2 indicates a second trailing sensor.
Volts	An estimate of the remaining battery life, expressed in volts.
Idle	The number of seconds since the latest packet was received from the device
RSSI	Received Signal Strength Indicator – a measure of the radio signal strength
LQI	Line Quality indicator – a statistical measure of the radio link quality
Present	A graphical indication of the state of detection of the sensor.
# Detections	Total number of detections since the sensor established a connection to the access point.
Mode	The operating mode of the device.
Slot#	The time slot on the access point used by the sensor or repeater.
PER	Packet Error Rate – a statistical measure of the data loss due to errors, dropped packets, noise, etc.
Adv Settings	Advanced Settings – depicts a sensor's settings regarding linear filter and axis detection.
Color Code	Displays the RF channel codes for a vehicle detection system.
Version	The firmware version on the device. (*Note*: use the *VDS Release Notes* from Sensys Networks to cross references firmware version ids to VDS releases.)
Dot Id 64	The factory assigned hardware device identifier. This displays all 64 bits as a 16-character HEX string.
Description	Additional description for sensor location and use. (*Optional*)
CC Extension	Specifies a duration of extension (in 1/1024 seconds) applied to a contact closure card channel when activated by events detected by this sensor. This element implements a per-sensor extension. (*Optional*)
CC Delay	Specifies a channel delay duration for this sensor only in 1/1024 seconds. (*Optional)*
Configured	Indicates that a sensor exists in the configured and saved Dot Table.
Pending Config	Indicates that a sensor has the minimum number of configuration change entries that have not been validated and written to the Dot Table.
Active	Devices that are transmitting during a TrafficDOT session.
Address 170	Maps a sensor table entry to a contact closure card channel. (*Required*)
Address 170 2	Maps a sensor table entry to a contact closure card channel. *(Optional)*
Address 170 3	Maps a sensor table entry to a contact closure card channel. *(Optional)*
Address 170 4	Maps a sensor table entry to a contact closure card channel. *(Optional)*

Table 8: Descriptions of Columns in the Table View

Id

Displays a 4-character HEX representation of the 16 least significant bits of the factory assigned device identifier. (Repeaters can be distinguished from sensors by observing a value of “RP” in the *Mode* column.)

The ID can be aliased or renamed subject to Sensys Networks defined naming rules. Renaming a sensor can be advantageous when devices are physically replaced but detection history must be retained.

Version

Displays firmware version information that results from a *Discover* operation or from sensors operating in *Idle* mode (mode E). Version information takes the form of *Version xx.yy.zz* where “xx” denotes the firmware version, “yy” denotes the hardware version, and “zz” denotes a configuration combination.

Volt

Displays an approximation of the current battery voltage level. This can be used to estimate the remaining battery life.

Idle

Displays the number of seconds since a packet from the device was received by the access point.

# Detections

Total number of detections since TrafficDOT connected to the access point.

RSSI

Received Signal Strength Indicator, a measurement of the strength of the radio signal between the access point and an associated sensor or repeater.

RSSI is sampled automatically as part of the SNP communications protocol. The number of seconds since the most recent sampling is displayed parenthetically next to the RSSI value.

An *RSSI Threshold* – a configurable value to which actual RSSI values are compared – is used to enable a visual indication of radio signal strength that fails to meet or exceed an acceptable level. RSSI values that fail to meet or exceed the threshold causes a device's health icon to change states.

The system default value is -88dBm. Use the *Configure* / *Preference* window to adjust this threshold.

LQI

Line Quality Indicator, a statistical measure of the quality of the radio link between the access point and an associated sensor or repeater, is automatically measured.

TrafficDOT represents LQI as a number between 40 and 99, with 99 being the best quality. In general, good LQI values are above 95; values around 90 indicate adequate LQI.

An LQI Threshold – a configurable value to which actual LQI values are compared – is used to enable a visual indication of line quality that fails to meet or exceed an acceptable level. LQI values that fall below the threshold cause a device's health icon to change states.

The system default value is 80. Use the *Configure* / *Preference* window to adjust this threshold.

PER

Packet Error Rate. This value represents the percentage of total packets expected from a sensor that were not received. It is calculated for a single sensor by dividing the number of missing packets over a fixed time period by the number of expected packets over the same fixed time period and multiplying by 100.

> **Note**: This only applies to **D** mode sensors.

Present

Current state of detection. A detection is represented by the presence of the detection color. The absence of a color indicates no detection.

Mode

The operating mode of the device. sensors are displayed as using one of the supported sensor operating modes.

A blank value in this column indicates the device is a repeater.

Slot#

The access point time slot used by the sensor or repeater.

Design rules of the SNP protocol require that no two devices transmit to the same receiver via the same time slot. Therefore, duplicate uses of a time slot are displayed in red.

Repeaters display information as `##/##` where

- the value to the left of separator represents the time slot on the access point over which the repeater most recently transmitted to the access point, and
- the value to the right of the separator is the repeater configuration identifier.

Repeater

Displays one of the following values:

- a *device ID* – indicates the sensor or repeater displayed in the row communicates to the access point through a repeater identified by the device ID shown in the column

- the *text string* “Direct” - indicates the sensor or repeater displayed in the row communicates directly to the access point

Channel

Displays the RF the device uses to transmit/receive. Sensor rows show the channel on which they communicate to the access point or repeater. Repeater rows display information as `## -> ##` where

- the value to the left of the separator is the channel over which the repeater reaches the access point that services it, and
- the value to the right of separator represents the channel the repeater uses to reach the sensors it services.

Advanced Settings

Displays the advanced magnetic detection properties that are enabled (if any). The default value –“Z&X” – indicates that the X- and Z- axes are enabled for magnetic detection. Changes to axes enabled and the application of signal filters are implemented on the *Sensor Configuration* window.

Status Line

Summary information regarding the connection session displays in the status area in the bottom of the window.

The information includes the user mode, RF channel of the access point, the number of devices in the network, and the current time acquired from the access point.

Appendix

Configuring Cellular Modems on an Access Point or an Access Point Controller Card (APCC)

This section provides the information required to configure cellular modems on either an access point or access point controller card (APCC) using TrafficDOT 2. Both the AP and APCC support two types of embedded cellular modems: GSM/GPRS and CDMA.

In order to use a cellular service, you must have the following:

1. A service contract with a service provider
2. An AP or APCC that has the correct type of modem installed

GSM/GPRS Modems

GSM/GPRS modems can be used by any GSM/GPRS service providers. Once you sign up for GSM/GPRS service, your service provider provides you with a SIMM card that needs to be inserted into the modem.

When configuring a GSM/GPRS, you need to provide the following information:

- APN
- Username
- Password

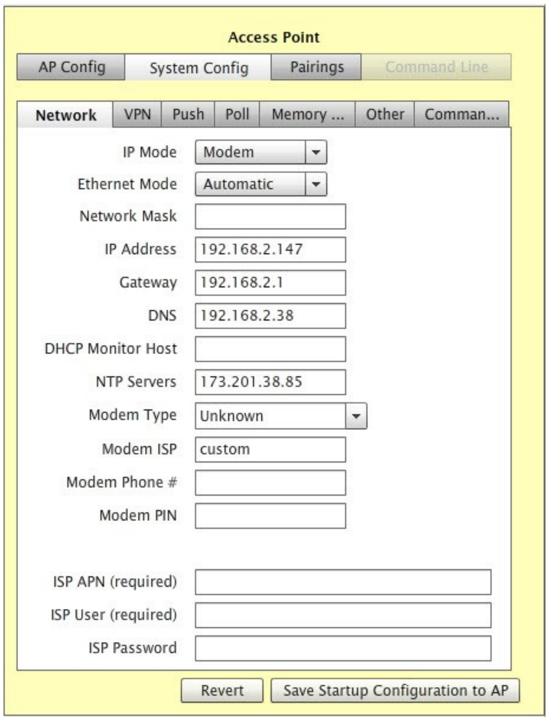
Note: The above information is provided by your service provider.

To configure a GSM/GPRS modem, perform the following steps:

1. Select an AP or APCC from the map image or components tray to open the *Access Point Configuration Window*.
2. Select the *System Config* tab.
3. Select *Modem* from the *IP Mode* drop-down list.
4. Enter “custom” in the *Modem ISP* field.

   The following fields display:

   - ISP APN
   - ISP User
   - ISP Password



IP Mode: Modem
Ethernet Mode: Automatic
Network Mask:
IP Address: 192.168.2.147
Gateway: 192.168.2.1
DNS: 192.168.2.38
DHCP Monitor Host:
NTP Servers: 173.201.38.85
Modem Type: Unknown
Modem ISP: custom
Modem Phone #:
Modem PIN:
ISP APN (required):
ISP User (required):
ISP Password:

Figure A1-1: GSM/GPRS Modem Configuration

> **Note**: The *Modem Phone #* field not required for GSM/GPRS modems, but is useful if you need to contact your service provider. The *Modem PIN* field is only required if your SIMM card is programmed with a personal identification number.

TrafficDOT recognizes the following GSM/GPRS providers:

- Cingular
- T-Mobile

For these service providers, you can simplify the modem configuration process by providing the name of the service provider in the *Modem ISP* field; TrafficDOT uses the default values for the APN, user name, and password.

Cingular

For Cingular, the default fields are:

- ISP APN: isp.cingular
- ISP User: ISP@CINGULARGPRS.COM
- Password: CINGULAR1

> **Note**: If you are using Cingular, but the parameters are different than the defaults, you must use the custom *Modem ISP* to set the parameters.

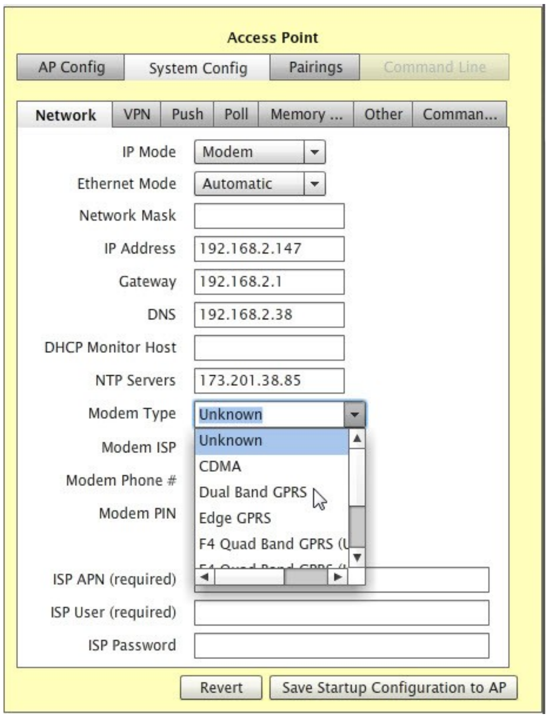
T-Mobile

For T-Mobile, the default fields are:

- ISP APN - internet3.voicestream.com
- ISP User - tmobile
- ISP Password - none

> **Note**: If you are using T-Mobile, but the parameters are different than the defaults, you must use the custom *Modem ISP* to set the parameters.

There are various types of GSM/GRPS modems for different access speed. You must select the correct modem type from the *Modem Type* drop-down list in order for the modem to work properly.



IP Mode: Modem
Ethernet Mode: Automatic
Network Mask:
IP Address: 192.168.2.147
Gateway: 192.168.2.1
DNS: 192.168.2.38
DHCP Monitor Host:
NTP Servers: 173.201.38.85
Modem Type: Unknown
Modem ISP:
Modem Phone #:
Modem PIN:
ISP APN (required):
ISP User (required):
ISP Password:

Figure A1-2: GSM/GPRS Modem Type Selection

Your package list should contain the part number of the access point. Access points with various modems installed have a different part number. For the new modems starting with G2, specific carriers are no longer supported, so you must configure the APN, user name, and password when configuring those modems.

CDMA Modems

Unlike the GSM/GPRS modems, CDMA modems are built specifically for a service provider, hence configuration of CDMA modems differ depending on the service provider. You must ensure that you order the correct modem for your service provider.

In order to use a CDMA service, you must have the following:

1. A service contract with a service provider
2. A CDMA modem that is specific for your service provider

> **Note**: Your service provider requires the ESN# or the MEID# from your modem in order for them to provision the service.

TrafficDOT recognizes the following CDMA providers:

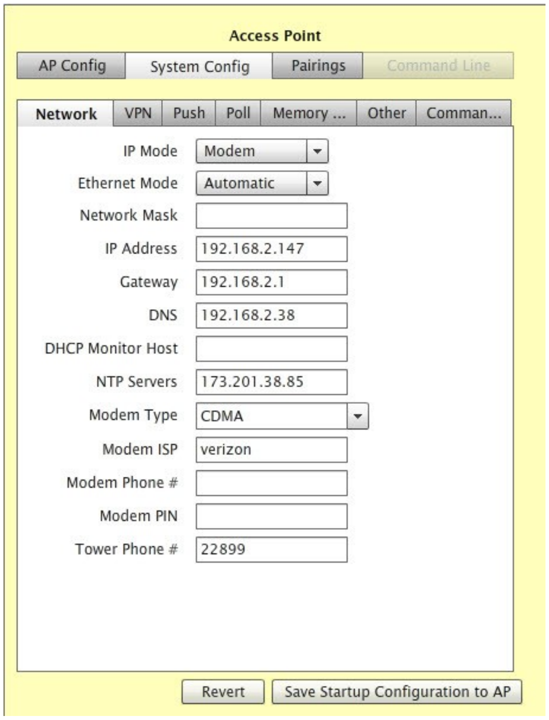
- Verizon
- Aeris

Verizon

To configure a Verizon modem, perform the following steps:

1. Select an AP or APCC from the map image or components tray to open the *Access Point Configuration Window*.
2. Select the *System Config* tab
3. Select *Modem* from the *IP Mode* drop-down list.
4. Select CDMA from the *Modem Type* drop-down list.
5. Enter “verizon” as the *Modem ISP*.
6. Enter the *Tower Phone #*.

> **Note**: You must enter “verizon” as the *Modem ISP* in order to see the *Tower Phone #* field. The *Tower Phone #* is usually is 22899.



IP Mode: Modem
Ethernet Mode: Automatic
Network Mask:
IP Address: 192.168.2.147
Gateway: 192.168.2.1
DNS: 192.168.2.38
DHCP Monitor Host:
NTP Servers: 173.201.38.85
Modem Type: CDMA
Modem ISP: verizon
Modem Phone #:
Modem PIN:
Tower Phone #: 22899

Figure A1-3: Verizon Modem Configuration

7. Click *Save Startup Configuration to AP* to save your configuration.

Aeris

To configure an Aeris modem, perform the following steps:

1. Select an AP or APCC from the map image or components tray to open the *Access Point Configuration Window*.
2. Select the *System Config* tab
3. Select *Modem* from the *IP Mode* drop-down list.
4. Select *CDMA* from the *Modem Type* drop-down list.
5. Enter “custom” in the *Modem ISP* field.
6. Enter “NNNNNNNNNN@tsp09.sprintpcs.com” as the ISP APN where *NNNNNNNNNN* is the phone number for your service.
7. Enter “guest” in the *ISP User* field.
8. Enter “guest” in the *ISP Password* field.
9. Enter the phone number provided to you by your service provider. The phone number you enter should be 10 digits and consist only numbers (e.g., 1112223333).
10. Click *Save Startup Configuration to AP* to save your configuration.