SENSYS
Networks

Sensys™ Wireless Vehicle Detection System

Reference Guide

P/N 152-240-001-001 Rev D
July 2010

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

Contents

Document Properties

This document is reference material for the Sensys™ Wireless Vehicle Detection System from Sensys Networks, Inc.

P/N 152-240-001-001 Rev D

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, Inc., 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, Inc. 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)
- Repeaters (RP240-B, and RP240-B-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 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

Sensys Networks 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

1 Introduction

This reference guide provides information and procedures for use with the Sensys™ Wireless Vehicle Detection System.

It is intended to be used by Sensys customers, consultants, partners, dealers and others with an interest in the application of wireless communication technology to the challenges of traffic detection, management and control.

1.1 What's Inside

This guide includes the following information:

- Chapter One, *Introduction*, defines the purpose and scope of the guide
- Chapter Two, *System Description*, is a detailed reference to the hardware and software components that comprise a Sensys network
- Chapter Three, *Network Management* explains how to configure Sensys Networks equipment and manage network as a whole
- a *Glossary* defines terms used throughout this guide
- a set of *Appendixes* provides supplementary information

1.2 Other Documents

General and Reference Information

- *The Sensys Wireless Vehicle Detection System – System Overview*
- *Sensys 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

- *Sensys Wireless Sensor Installation Guide*
- *Sensys Wireless Sensor Removal Guide*
- *Sensys Access Point Installation Guide*
- *Sensys Repeater Installation Guide*
- *Sensys Contact Closure Card Installation Guide*
- *Tools Required for Installing Sensys Equipment*
- *Replacing Batteries in the RP240B Repeater*

Application Notes

- *Using Sensys Networks With Motorcycles*
- *Executing Commands on a Access Point with HTTP*

Sensys Management Server

- *SNAPS Professional 2.0 Set Up and Operating Guide*
- *Sensys System Manager 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.

2 System Description

This chapter provides an overview of the Sensys™ Wireless Vehicle Detection System, describes its components, and identifies traffic management applications to which it is suited.

2.1 Overview

The Sensys™ Wireless Vehicle Detection System detects the presence and movement of vehicles with magneto-resistive *Sensors* mounted in the pavement. The Sensors continuously transmit detection data via low power radio technology to *Access Points* that collect and forward data upstream to local traffic controllers, remote traffic management systems, or other applications.

The wireless technology used for communications between a Sensor network and an Access Point is subject to certain physical limitations – notably distance. Thus, it is not uncommon to include one or more *Repeaters* in an installation. Repeaters receive data transmissions from Sensors and relay them to a designated Access Point, thereby “extending” the reach of an Access Point.

Vehicle detection data can be forwarded directly to traffic signal control equipment local to the installation, transmitted to remote systems via a wired or wireless connection to an available IP data network, or both.

Remote systems include traffic management centers, advanced transportation management systems, public traveler information systems, or custom applications performing data analysis, reporting, or control operations.

A typical system is shown in the figure below.

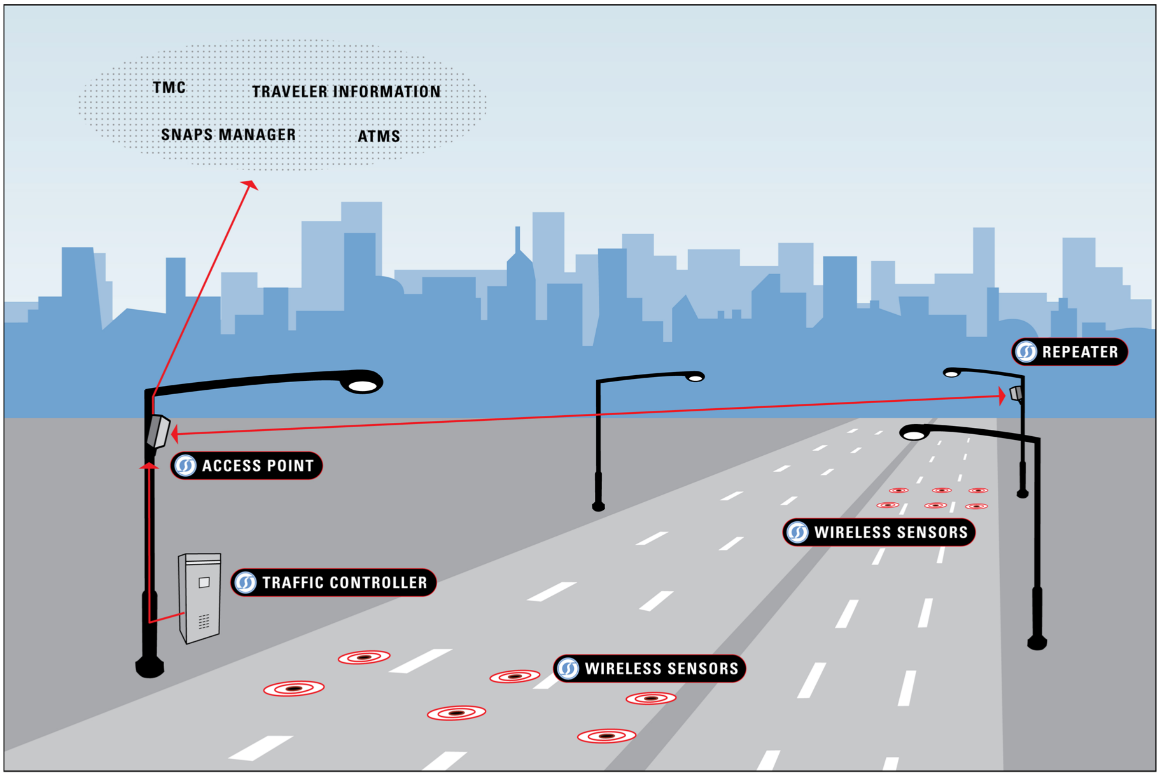


Figure 2.1: Sensys Wireless Vehicle Detection System

2.1.1 Key Features of the Wireless Vehicle Detection System

The wireless vehicle detection system operates as an integrated, self-managing system requiring little in the way of field maintenance or adjustments.

2.1.1.1 Wireless Sensors

- Self-contained, self-calibrating, maintenance free units with an operating lifespan of up to 10 years
- Simple in-pavement installation process
- Managed remotely from a central console
- Firmware updated via wireless download
- Configurable detection zone, event thresholds, transmit intervals and communication frequencies
- Suitable for any inductive loop application

2.1.1.2 Communications

- Ultra-low power, wireless communications protocol with built-in buffering, signal quality monitoring and re-transmission processing
- Configurable channel (frequency) selection in the unlicensed RF range
- Range limits extended with signal Repeaters
- Upstream connections made with standard IP protocol over available wired or wireless (GSM, CDMA) networks

2.1.1.3 Event Data Processing

- Detection data is time-synchronized throughout the system
- Direct interface to local traffic control equipment
- Optional interface to upstream traffic management applications
- Central process to generate and store statistics such as speed and volume

2.1.1.4 Network Management

- Central point of authority and management access
- Remote management via standards-based, PC software application
- Local (on-site) management supported
- Monitor RF performance, change device configuration, download firmware updates

2.1.2 Application Solutions

The system provides accurate vehicle detection applicable to a wide variety of traffic applications.

2.1.2.1 Freeway and Arterial Count Applications

Count applications include circumstances where traffic census data (vehicle counts, occupancy and speed) are the primary objects of interest. Typical deployments are shown in the figure below.

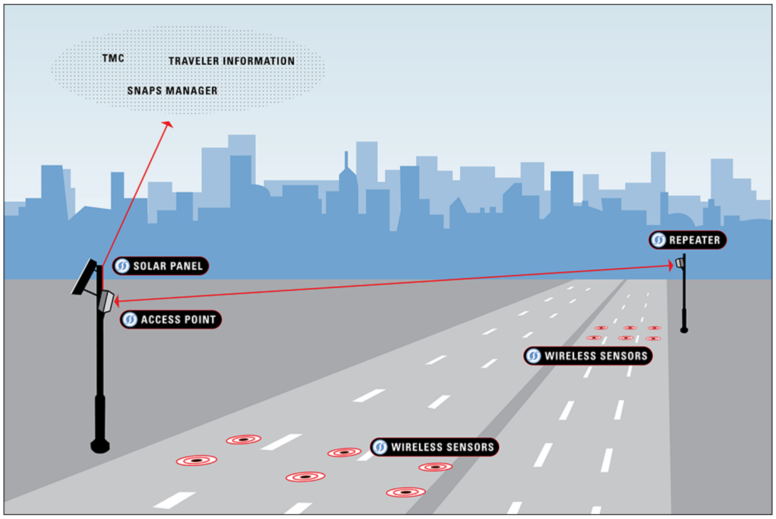


Figure 2.2: Count Station (typical) powered by solar panel

2.1.2.2 Intersection Applications

Intersection applications include circumstances where detection is required at the stop bar, at approaches or departures, or for queue management.

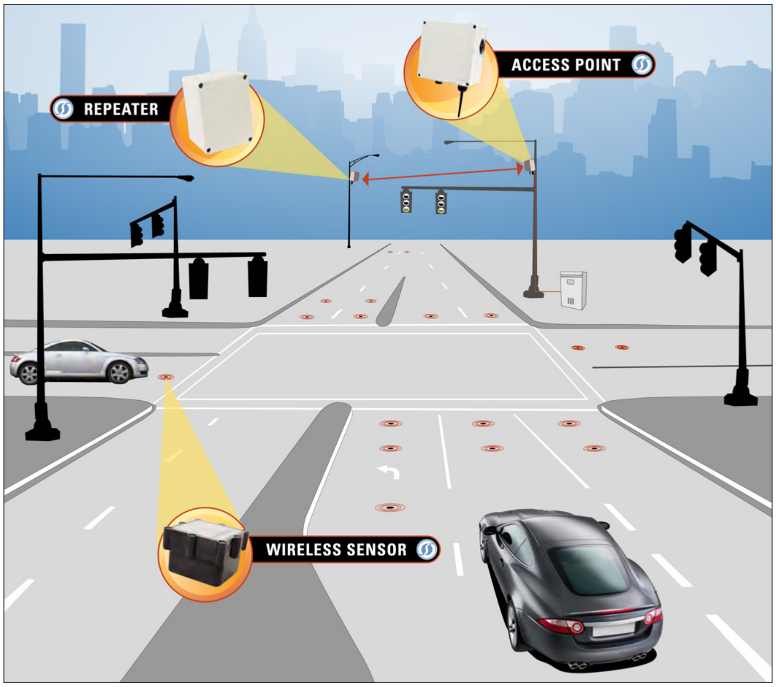


Figure 2.3: Intersection installation (typical)

Other solutions – such as red-light enforcements, high importance vehicle preemption, pedestrian phasing, and the like – can be implemented using the Sensys Wireless Vehicle Detection System. The components of the Sensys Wireless Vehicle Detection System are described in the next section.

2.2 System Components

This section describes each component of the Sensys Wireless Vehicle Detection System. Information regarding configuration of the components can be found in the *Network Management* chapter. Additional information on the appropriate use of the components can be found in the design, installation and configuration documents developed by Sensys Networks.

An implementation of a Sensys network includes *required* components –components that are essential to the basic functioning of the system– and *optional* components –products and services that augment the basic operation of the system but are not strictly required.

2.2.1 Required Components

The required components are:

- *Sensys Wireless Sensors* – pavement mounted magnetometers equipped with wireless radio transmitters
- *Sensys Access Point* – a pole-mounted device that provides access to and control of a collection of Sensors and/or Repeaters
- *TrafficDOT* -- network configuration utility from Sensys Networks

2.2.2 Optional Components

The optional components include the following:

- *Sensys Repeater* – a pole mounted device that relays wireless signals between Sensors and an Access Point (or other Repeater)
- *Sensys Contact Closure Card* – a hardware card that interfaces a Sensys Wireless Vehicle Detection Network to a traffic signal controller
- *APDIAG* – a software application used to monitor and assess the behavior of Sensors in a network
- *APPOLLSTAT* – a software application that allows a Sensys Wireless Vehicle Detection network to emulate a Type 170 signal controller when communicating with a front-end processor expecting CalTrans SDRMS formatted packets
- *APPOLLSTAT_CALTRANSD4* – a software application that allows a Sensys Wireless Vehicle Detection network to transfer data to traffic controller in California DOT District 4 complying with the TOX 2.1 specification.

- *APPOLLSTAT_TCP* – a software application that facilitates transferring event reports from an Access Point to a generalized external poll server using Sensys Networks formatted packets
- *APPUSHSTAT* – a software application used to intelligently move Sensor data to designated hosts
- *APSTAT*– a software application that processes raw detection data to compile measures such as volume, occupancy, and speed
- *APSTATRECV* – a software application that receives data packets sent by APPUSHSTAT enabling a distributed network of statistics servers
- *EVENTPROXY* – a software application that provides a text/line-oriented interface into raw event data
- *Sensys Management Servers* – Sensys Networks provides two computing platforms (*SNAPS Professional* and *Sensys System Manager*) that enable management and statistical data services to one or more Sensys network installations
- *SNCPROXY* – a software application that provides proxy services for an Access Point, thereby offloading from the Access Point event reporting and processing of management commands

Each component is described in more details in the sections that follow.

2.3 Sensys Wireless Sensor

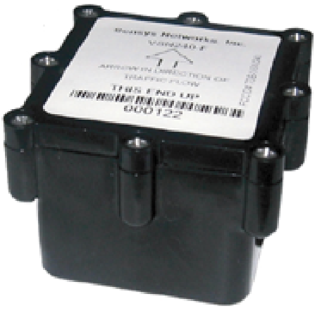


Figure 2.4: VSN240-F Wireless Sensor

A Sensys wireless Sensor is a magnetometer capable of low-power radio communications packaged in a small, hardened plastic case suitable for in-pavement installation. (*Note*: flush mount Sensor shown at right.)

2.3.1 In This Section

This section discusses the following topics:

- Typical Use
- Operation
- Vehicle Detection
- Detection Zones and Sensitivity
- Data Communications
- Data Characteristics and Transmission
- Event Data Processing
- Expected Maintenance

2.3.2 Typical Use

In typical traffic management applications, a Sensor is placed in the middle of a traffic lane to detect the presence and passage of vehicles.

Two Sensors – installed in the same lane – can be used to measure vehicle length and speed. The recommended distance between Sensors depends on the range of expected speeds.

In addition, Sensors placed on approaches to key targets provide advance detection, while Sensors configured at intersections are used in stop bar applications.

2.3.3 Operation

An advanced magneto-resistive sensing device embedded in each Sensor measures the X-, Y-, and Z-axis components of the Earth's magnetic field at a 128 Hz sampling rate. Sophisticated signal processing algorithms are used to provide accurate vehicle detection.

In the most common use, approaching vehicles cause changes in the X, Y, or Z axes of the magnetic field that are detected by the Sensor. The changes are translated into detection events via configurable detection thresholds. Detection events are communicated to an Access Point for additional processing and transmission to other systems.

2.3.3.1 Identification

Each Sensor is uniquely identified by its *SensorId* (also known as *dotId*) – a factory assigned 64-bit value that cannot be changed. In practice, the *dotId* is represented as a four-character HEX string (i.e., the 16 least significant bits of the full 64-bit value). SensorIds must be unique within a Sensys network; the id (in text and a barcode) appears on the Sensor's label.

2.3.3.2 User Operating Modes

Each Sensor operates in one of the modes shown in Table 1. The most common modes are:

- *Count* – a single mode used for all count applications
- *Stop Bar* – a series of modes suited to a range of stop bar applications

The following table presents the Sensor modes supported for application use,

Mode	GUI Label[1]	Application	Relative Sensitivity	Holdover
Count	B	Vehicle count stations	n/a	(*see Notes*)
Re-id	C	Vehicle re-identification mode for arterial travel time applications	ren/a	n/a
Idle	E	Suspend detection; conserve power	n/a	(*see Notes*)
ATS	H	High accuracy speed mode	n/a	n/a
Stop Bar 0	Stop Bar 0	Bicycle/scooter	0.12	None
Stop Bar 1	Stop Bar 1	Motorcycle	0.16	None
Stop Bar 2	Stop Bar 2	Motorcycle (Recommended)	0.22	None
Stop Bar 3	Stop Bar 3	Auto	0.29	None
Stop Bar 4	Stop Bar 4	Auto	0.39	None
Stop Bar 5	Stop Bar 5	Auto (Recommended for normal recalibration)	0.50	None
Stop Bar 6	Stop Bar 6	Auto	0.75	None
Stop Bar 7	Stop Bar 7	Auto (Recommended for fast recalibration)	1.00	None
Stop Bar 8	Stop Bar 8	Auto	1.25	None
Stop Bar 9	Stop Bar 9	Auto	1.75	None
Stop Bar 10	Stop Bar 10	Truck	2.38	None
Stop Bar 11	Stop Bar 11	Truck	3.25	None
Stop Bar 12	Stop Bar 12	Light Rail	5.50	0.5 seconds
Stop Bar 13	Stop Bar 13	Light Rail	9.00	0.5 seconds
Stop Bar 14	Stop Bar 14	Light Rail (Recommended)	15.25	0.5 seconds
Stop Bar 15	Stop Bar 15	Light Rail	25.60	0.5 seconds

Table 1: User-selectable Sensor Operating Modes

---

[1] This column shows how the operating mode is displayed on TrafficDOT's main window, the *Access Point Main window*.

Notes

- Sensors operating in *Count* mode acquire sensitivity and holdover settings from the Access Point to which they report. All count-mode Sensors in a network use the same settings.
- Sensors operating in a *Stop Bar* mode acquire sensitivity and holdover settings from the mode algorithm. This allows stop-bar Sensors to be finely tuned to the requirements of their use.
- Holdover times are generally not useful in stop bar applications.
- Sensors may be placed into an *Idle* mode. Idle mode suspends detection and preserves battery life.[2]

All of the modes in the table above are user-selectable via TrafficDOT. See the section *Configuring Sensors* in the *Network Management* chapter for more information.

2.3.3.3 Reserved Operating Modes

Certain operating are intended for use only by Sensys Networks Technical Support and should not be used without prior consultation with Sensys Networks. These restricted modes are shown in the table below.

Mode	Abbreviation	Function
Raw Z	A	Sends raw Z axis magnetic Sensor data
Raw XYZ	D	Sends raw X, Y, and Z axes magnetic Sensor data
Gated Raw XYZ	F	Combination of Mode B and Mode D - sends raw X, Y, and Z axes magnetic Sensor data while a vehicle is near the Sensor
Signature	G	Sends magnetic signature data

Table 2: Reserved Operating Modes (for use by Sensys Networks only)

Note: in certain rare situations overhead or buried power lines may interfere with vehicle detection. Testing of the environment using a reserved detection mode may be required if conditions such as this exist at or near the site of the detection system.

2.3.4 Vehicle Detection

Sensors detect vehicles by inference. The presence and absence of vehicles is determined by comparing a detected change in the local magnetic field to a self-maintaining baseline value. If the magnitude and duration of the difference meets or exceeds certain thresholds, a *detection event* (representing either vehicle presence or absence) is declared by the Sensor.

The attributes that compose the detection model are discussed in this section. Configuration of the

---

[2] Sensors in this mode continue to transmit software version and battery information. However, the preferred method of acquiring this information is via TrafficDOT's *Discover* operation.

attributes is covered in the section *Configuring Access Points* in the *Network Management* chapter.

2.3.4.1 Overview

During normal operation, 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 background magnetic field and establishing a *baseline reference value*. This accounts for any long-term variations in the local magnetic field. Vehicles are detected by measuring deviations from the reference value.

Detection events (sometimes referred to as ON events) are declared when changes in the local magnetic field exceed defined thresholds for a defined period of time; the same is true for "undetection" events (sometimes referred to as OFF events).

2.3.4.2 Detection Components

Vehicle detection is summarized in the figure below.

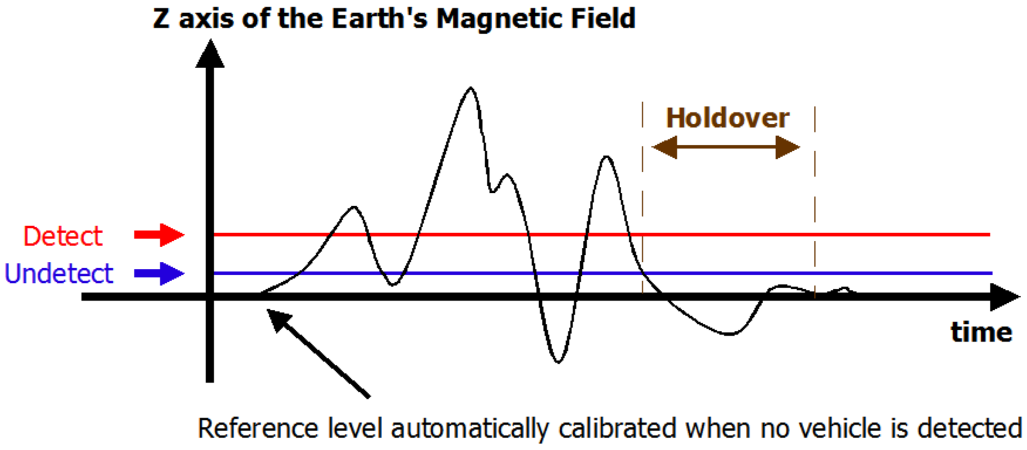

Z axis of the Earth's Magnetic Field
Holdover
Detect
Undetect
time
Reference level automatically calibrated when no vehicle is detected

Figure 2.5: Components of the vehicle detection model

In the figure above, detection thresholds and the baseline reference value appear as straight, horizontal lines. The curvilinear line is a plot of a given Sensor's measurement of the local magnetic field versus time. Detection events are declared by the Sensor when the plot exceeds the detect threshold and meets other conditions.

2.3.4.3 Adjusting Detection Behavior

Sensors ship with a default configuration for "typical" vehicle count stations. However, certain situations may require modifying a Sensor's detection behavior – for example, to avoid the possibility of double-counting certain vehicle types such as long tractor trailers.

Detection behavior is changed via the following elements:

- Detection thresholds
- Onset filter
- Holdover duration

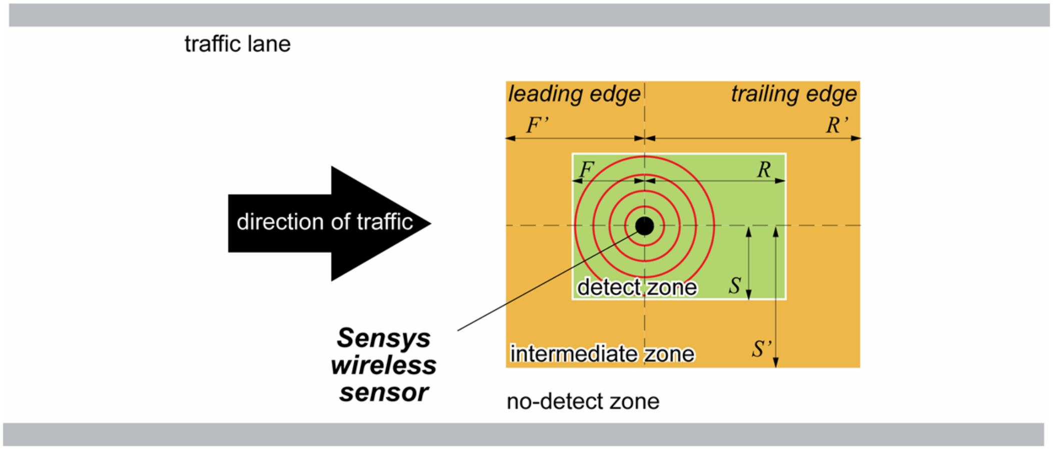
Note: for Sensors operating in Count mode the parameters above are configured with TrafficDOT. For Sensors operating in one of the Stop Bar modes the detection settings are part of the mode algorithm.

2.3.4.4 Detection Zones and Sensitivity

Detection zones are theoretical areas projecting outward from the Sensor that help conceptualize what a Sensor can detect. The zones represent physical areas where the presence or passage of a vehicle is (or is not) detected with varying likelihoods. The zones are as follows:

- *Detect zone* – a vehicle is likely to be detected with high probability
- *Intermediate zone* – a vehicle may or may not be detected depending on its size and type
- *No Detect zone* – a vehicle is not likely to be detected with high probability

The figure below depicts approximate detection zones using default settings.



	F	F'	R	R'	S	S'
freeway & arterial applications (typical configuration)	~2 feet / ~0.6 meters	~4 feet / ~1.2 meters	~4 feet / ~1.2 meters	~6 feet / ~1.8 meters	~2 feet / ~0.6 meters	~4 feet / ~1.2 meters
intersection applications (typical configuration for automobiles)	~3 feet / ~0.9 meters	~5 feet / ~1.5 meters	~3 feet / ~0.9 meters	~5 feet / ~1.5 meters	~3 feet / ~0.9 meters	~5 feet / ~1.5 meters

Figure 2.6: Detection zones (approximate dimensions)

For a given application, the detection zone dimensions are determined by (*i*) whether all the detection axes of a Sensor are enabled and (*ii*) the respective threshold settings.

For example, to detect through traffic for freeway or arterial applications, Sensors are configured with relatively low sensitivity to minimize false detections from vehicles in neighboring lanes.

In contrast, to detect the presence of a vehicle at an intersection for traffic control applications, Sensors are configured with relatively high sensitivity and an expanded detection zone to ensure that a vehicle is detected when present, even if false detections may be occasionally generated. A roadside traffic controller will typically require a sustained "vehicle present" signal, thus minimizing the impact of any false detection signals that may be generated by the relatively high sensitivity setting.

2.3.4.5 Detection Thresholds

Thresholds specify the magnitude of change from a Sensor's reference value (representing its current estimate of the long-term local magnetic field) necessary to declare a detect or undetect event. The higher the threshold value, the larger a disturbance in the magnetic field must be to result in a detection or undetection.

Note: there is an inverse relationship between threshold values and sensitivity. Higher threshold values mean that a Sensor will be relatively insensitive to small or medium sized changes in the local magnetic field. Lower threshold values mean a Sensor will be sensitive to even the smallest change.

Three threshold elements – *Detect Z Threshold*, *Undetect Z Threshold* and *Undetect X Threshold* – are used to configure relative sensitivities for Sensors operating in *count* mode (mode B). Use TrafficDOT and the *Access Point Configuration* window to work with these elements when circumstances warrant. (See the section *Configuring Detection Settings* later in this manual for more information.)

As the Sensys VDS technology has evolved, additional modes of Sensor operation have been introduced that implement detection sensitivity in other ways – an example being the range of *stopbar* operating modes. Thus, the applicability of the elements described in this section may be subject to the nature and purpose of a particular installation.

2.3.4.6 Onset Filter

This element specifies the number of consecutive samples for which a detection condition must be true before a detection event is declared.

2.3.4.7 Holdover

This element specifies the amount of time that – once a detection event is declared – any deviation from the baseline can be less than the undetect threshold before the detection event is declared terminated.

2.3.4.8 Swap X/Y

This element logically swaps the readings from the X and Y magnetic Sensors. (*Note*: this is not common, but is useful in situations where the Sensor is installed with a non-standard orientation.)

2.3.4.9 Recalibration and Recalibration Timeouts

Recalibration refers to a Sensor's measurement of the local magnetic field for the purposes of establishing a baseline reference value. This behavior is automatic – occurring when vehicles are not present – and is essential for the long-term effectiveness of Sensors as the local magnetic field may change over time.

In certain circumstances, a Sensor may become “stuck” in the ON state. This occurs if the magnetic environment around the Sensor changes (for example, when a vehicle is parked on top of, or very near to, the Sensor). In this case, the Sensor's continuous recalibration algorithm is disabled and the Sensor does not return to the OFF state. To manage this situation, Sensors can be configured to use a recalibration timeout.

A recalibration timeout is an optional parameter that specifies a duration in seconds such that, if an ON condition is true for a period greater than the timeout duration, the Sensor recalibrates. (In addition, a Sensor can be directed to recalibrate via a management command sent with Traffic DOT.)

2.3.4.9.1 Fast Recalibration and Stop Bar Recalibration Timeout

On occasion, the level of magnetic noise at an intersection can be very high – higher, in fact, than the detection threshold. In such cases, vehicle presence might be held indefinitely because the Sensor cannot distinguish between the noise and the vehicle.

Detection in these circumstances requires setting the detection threshold higher and recalibrating the Sensor very quickly – in one or two seconds (versus the default of 30 seconds) – after detection.

When a vehicle passes the Sensor, it generates either one or two pulses depending on the speed at which it passes. A traffic controller can then be configured to hold detection until the next green phase.

This operation is referred as *fast recalibration* and is applicable to all stop bar modes. Fast recalibration is set via the element *Stop Bar Recalibrate Timeout*. (See the section *Configuring Access Points* in the *Network Management* chapter for more information.)

2.3.4.9.2 Count Recalibrate Timeout

Count mode Sensors use a discrete setting for the recalibration timeout. This setting is implemented via the element *Count Recalibrate Timeout*.

Separate timeout settings are available for installations outside of North America.

2.3.4.10 Factory Default Settings

Sensors ship with default settings for detection zones and sensitivities suitable for typical count applications. When changes are required, TrafficDOT is used to make them. (See the section *Configuring Access Points* in the *Network Management* chapter for more information.)

The default detection settings for Sensors operating in Count mode are shown below:

Parameter	Value	Notes
Z Axis Detect Threshold	12	A relative value
Z Axis Undetect Threshold	7	A relative value
X Axis Undetect Threshold	7	A relative value
Onset Filter	1	Approximately 7.8 milliseconds
Holdover	10	Approximately 78 milliseconds
Swap X/Y	0	0 = do not swap X and Y magnetic axes
Stop bar Recalibrate Timeout	(30)	Specified as taking the value of the *Count Recalibrate Timeout*
International Mode	Off	International count recalibration timeout values are off.
Count Recalibrate Timeout	30	Number of elapsed seconds before recalibration.

Table 3: Factory Default Detection Parameters – Count Mode Sensors

> *Note*: Sensors operating in one of the Stop Bar modes take their detection settings from the mode itself. To adjust their behavior, select a different Stop Bar mode.

2.3.5 Wireless Radio Communications

Wireless communications between Sensys Sensors and Access Points/Repeaters is based on the Sensys NanoPower Protocol (SNP), a patented technology that provides reliable packet data communication with very low latency and ultra-low power consumption.

2.3.5.1 Band and Channel

Sensys equipment operates in the 2.4GHz unlicensed ISM frequency band and requires no operating license to be deployed. Sensys networks operate on any of 16 channels in that band.

When shipped, Sensors, Access Points, and Repeaters are set to channel *zero*. Alternative channels can be used to avoid potential interference from other equipment in the vicinity transmitting in the ISM band.

2.3.5.2 Antenna

Sensors use an embedded directional antenna known as a *microstrip patch antenna*. The antenna's directional beam pattern provides a main lobe directed perpendicular to the Sensor's top surface, with its maximum power radiated along this boresight and decreasing symmetrically as the elevation (vertical) or azimuth (horizontal) angle from the boresight increases.

At either an azimuth or elevation angle of ±60°, approximately half the maximum signal strength is transmitted, diminishing rapidly as the azimuth or elevation angle increases. The transmit beam pattern also describes the antenna's response to received radiation.

A Sensor's transmitted and received signal is likely to be affected by its installation in or on the roadway as well as by nearby stationary and moving objects. (See also the Sensys documents *Design Guidelines for Freeway Applications* and *Design Guidelines for Intersection Applicationss* for more information.)

2.3.5.3 Radio Performance

Two measures characterize the quality of the wireless channel – *Received Signal Strength Indicator* and *Line Quality Indicator*. Each measure can be monitored with TrafficDOT. (See the section regarding the *Access Point Main* window in the *Network Management* chapter for more information.)

2.3.5.3.1 Received Signal Strength Indicator (RSSI)

RSSI is measured in dBm, dB relative to 1 mW into a 50 Ohm impedance. Typical RSSI numbers will range from -50dBm (for Sensors very close to a receiver) to -95dBm (the far edge of RF coverage).

It is possible to operate with an RSSI as low as -90dBm, but doing so leaves no margin for signal degradation. Signal degradation can occur either in short bursts – for example, when a vehicle is driving over the Sensor – or in long intervals (up to days), as may occur when a vehicle is parked very near the Sensor or during a heavy snow storm.

Recommended performance ranges are given in the table below:

Application	RSSI range of all RF Links
Count	Greater than -79dBm
Stop bar detection	Greater than -69dBm

Table 4: Recommended RSSI Performance for Applications

Note: RSSI expresses the amount of signal loss, thus it is a negative number. Better RSSI is represented by values closer to zero.

2.3.5.3.2 Line Quality Indicator (LQI)

LQI is an indicator of link error rate or signal-to-noise ratio (SNR). LQI is affected by both RF signal strength and local RF interference. TrafficDOT displays LQI as a number between 40 and 99, with 99 representing optimal quality. LQI values above 95 are considered "good"; LQI values around 90 are considered "adequate".

Poor LQI in the presence of strong RSSI is indicative of local ISM band interference (for example a nearby Wi-Fi modem). Use an alternative RF channel to improve performance.

2.3.5.4 Radio Settings

A Sensor's RF channel, time slot and operating mode are stored in flash memory. These elements are configured with TrafficDOT. (See *Configuring Sensors* in the *Network Management* chapter for more information.)

Note: RF communications is not an exact science. Sensys Networks recommends staying within the standard transmission ranges described herein and monitoring RSSI and LQI for all Sensors prior to installation to insure satisfactory performance.

2.3.6 Network Protocol

The Sensys NanoPower Protocol (SNP) ensures reliable wireless communications between Sensors and an Access Point or Repeater. The protocol is discussed in this section.

2.3.6.1 Time-Synchronization

The SNP protocol provides packet data communications with very low latency and ultra-low power consumption. The internal clocks of all Sensors in an installation can be synchronized to the network Access Point. This conserves power as Sensors "wake up" at a specific time, communicate their data, and then shut themselves down until the next transmission cycle.

2.3.6.2 Full Duplex

Communications between an Access Point and its Sensors are two-way: *uplink* packets from the Sensor to the Access Point contain detection data, while *downlink* packets from the Access Point to the Sensors are used for synchronizing and sending commands to the Sensors.

2.3.6.3 Packet Acknowledgment and Retransmission

By default, Access Points explicitly acknowledge every data transmission received from a Sensor. In the field, it is not uncommon to experience a degree of packet loss due to local, transient interference. To accommodate this, Sensors automatically retransmit their data if they do not receive an acknowledgment within an expected time interval.

2.3.6.4 SYNC Packets

Access Points transmit synchronization (SYNC) packets to the Sensors in the network to elicit data transmissions.

Each Sensor automatically listens for its own SYNC packet. After detecting two consecutive SYNC packets, a Sensor begins transmitting events.

2.3.6.4.1 Sleep Mode

To reduce power consumption, a Sensor detecting only one or no SYNC packets enters “sleep mode”. After approximately 60 seconds it again listens for Access Point packets. If such a packet is received, the Sensor attempts to synchronize to the Access Point and, if successful, activates its magnetic Sensor and resumes operations according to its mode.

If the RF connection is lost, either because the Access Point is off line or the Access Point's RF signal cannot be received, the Sensor returns to “sleep”. The RF outage must be a complete loss of signal for between 15 and 34 seconds. If such an outage occurs, the Sensor “sleeps” for approximately 60 seconds, missing all traffic during that interval.

2.3.6.4.2 Fast Recovery

In cases where traffic is moving, such as on freeways or arterials, long RF outages are not common and the operation above is acceptable. However, in stop bar applications and certain count applications, RF outages may be more common because (*i*) there is a very high density of vehicles near the Sensors and (*ii*) those vehicles are not moving.

To accommodate these situations, the reacquisition of Access Point synchronization after an RF outage is shortened for stop-bar applications to two seconds. This is referred to as *fast recovery*. Fast recovery is enabled for ten minutes following an RF outage at which point ordinary, “sleep” mode operations resume.

2.3.6.5 Time Slots

Wireless communications in a Sensys networks observe a Time Division Multiple Access (TDMA) scheme. In a given network, each device shares a common RF channel and avoids interference by transmitting and receiving according to a predetermined plan that dictates the following:

- the order in which devices will transmit/receive
- the duration any particular device uses to transmit/receive
- the duration between successive opportunities any particular device has to transmit/receive

The order of device communications in a Sensys network is implemented via a network element known as a *time slot*. Each device transmits on a unique time slot.

The duration any particular device uses to transmit/receive is fixed by the manufacturer and is not configurable by the end-user. The duration between successive opportunities to transmit/receive is implemented in the *transmit interval* element.

See the discussion of time slots in the Access Point section below for more information.

2.3.6.5.1 Sensor Time Slots

Each Sensor is assigned a unique time slot with TrafficDOT. To simplify the process, TrafficDOT automatically analyzes the transmit interval and the current time slot assignments to restrict the list of time slots presented to the end user to only those that are available (i.e., unassigned). (See the section *Configuring Sensors* in the *Network Management* chapter for more information.)

2.3.7 Data Characteristics and Transmission

Each Sensor is individually addressable . Data collected from any Sensor is therefore uniquely identifiable and each Sensor can be independently controlled and monitored.

2.3.7.1 Event Data Payload and Acknowledgment

Sensors transmit each detection event with a time-stamp (with 1 ms resolution) and its *SensorID*. Because RF communications are not perfect, especially in the presence of large vehicles, packets may occasionally fail to be received by the target Access Point or Repeater. To avoid data loss, Sensys networks use a packet acknowledgment scheme wherein events are retransmitted by Sensors until they are acknowledged by the Access Point.

2.3.7.2 Time Synchronization

When Sensors synchronize to an Access Point, their internal clocks are set by the Access Point, so that all Sensors in a given installation have an identical absolute time reference. This enables the system-wide recording of detection events with time-stamps accurate to within one millisecond and facilitates comparisons of event data from different Sensors.

2.3.7.3 Other SNP Protocol Characteristics

Under the SNP protocol a Sensor listens to its associated Access Point (or Repeater) once during each 30 second interval. Within the 30 second interval, each Sensor listens for a particular SYNC packet derived from its Sensor Id.

The result is a limitation on the speed at which commands are received by a Sensor. Depending on when a command is issued, it may take up to 30 seconds for a Sensor to receive it. In addition, commands are not explicitly acknowledged. It is presumed that, once configured, Sensors will not require subsequent commands for normal operation.

2.3.8 Event Data Processing

Fundamentally, event data reflect the presence or absence of a vehicle as a function of time. Sensor data generates a time-based record of vehicle detections which enable derivation of more significant measures such as:

- *Vehicle volume* – number of vehicles observed per time unit
- *Lane occupancy* – fraction of time vehicles are present over a specific averaging time
- *Headway* – time between the front edge of successive vehicles
- *Gap* – time between the rear and front edges of successive vehicles

Note: Sensors are not involved in calculating measures like those noted above. Sensors only transmit time-stamped detection event data to be processed further at an Access Point, a SNAPS Professional server, a Sensys System Manager server, or other remote processing facility.

2.3.9 Expected Maintenance

Sensors are engineered to operate in a pavement mounted environment, within an ambient temperature range from -40°F to 176°F (-40°C to +85°C).

2.3.9.1 Battery Life

Considerable investment has been made to minimize the power requirements of a Sensor's wireless communications. Engineered battery life is approximately 10 years. However, the Sensor's use and its configuration settings both influence battery life.

Sensor batteries cannot be replaced. However, TrafficDOT displays the current operating voltage of Sensor batteries when operated in *Discover* mode. This value is approximate due to the battery chemistry, but is still meaningful.

Under typical use, a Sensor battery maintains a constant voltage for most of its operational life, with reported voltage falling rapidly near end of life. A battery voltage read-out of 3.2V or higher is considered “healthy” in most environments.

2.3.9.2 Firmware Upgrades

From time Sensys Networks may make available upgrades to the firmware on which Sensors operate. These upgrades are optional and typically add new functionality while, to the extent possible, maintain backward compatibility.

Firmware upgrades are applied over the wireless link from the Access Point to the Sensors with TrafficDOT. Customers are not required to unearth Sensors to upgrade firmware.

2.4 Sensys Access Point

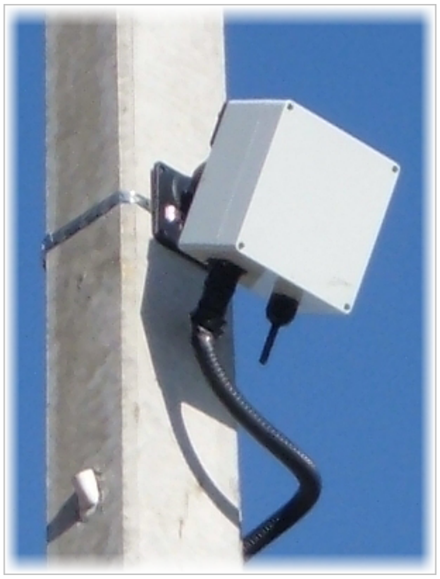


Figure 2.7: AP240-EG Access Point

The Sensys Access Point collects event data from wireless Sensors and Repeaters, optionally aggregates it, and forwards it to local signal control equipment, traffic management systems or a 3rd party application server.

2.4.1 In This Section

This section discusses the following topics:

- Typical Use
- Operation
- Wireless Radio Communications
- Network Protocol
- Event Reporting Parameters
- Event Detection Parameters
- Network Management
- Network System Definition
- Communication Interfaces
- Power
- Expected Maintenance

2.4.2 Typical Use

Access Points provide a central point of authority, device management, identification, and service definition for networks consisting of equipment from Sensys Networks including wireless Sensors, Repeaters and Contact Closure cards.

Access Points are installed at the roadside to collect via a wireless link vehicle detection data from Sensors installed as freeway/arterial count stations and at intersections.

Event data is collected, optionally processed and stored by the Access Point, and optionally forwarded to central traffic management systems, remote traffic information systems, or local traffic signal controllers.

2.4.3 Operation

An Access Point is a 6¼” x 6¼” x 3½”(15.9 cm x 15.9 cm x 8.9 cm), line-powered enclosure with an on-board 66MHz 5272 Coldfire processor hosting a version of the Linux operating system.

Access Points are identified by a unique factory assigned hardware id, as well as by an optional IP address assigned by customers to facilitate remote management.

Detection event data is acquired directly from Sensors (as well as from Sensors transmitting through Repeaters) by continuous, full-duplex radio communications. The RF channel also enables device and network management. Access Points automatically monitor the performance of the RF channel and provide quality statistics that can be inspected in real-time via TrafficDOT and/or stored and reported as data outputs.

Up to 54 Sensors can be associated with an Access Point with nominal latency. In applications where additional latency is acceptable, the maximum number of Sensors can exceed 2,000.

2.4.3.1 Event Data Handling

Vehicle detection events can be transparently sent to a designated server, aggregated locally on the Access Point and bulk transferred to another server, forwarded to a traffic signal controller (via a Sensys Contact Closure card) or any combination of the above.

Event data is transferred to other hosts via an IP network connection. IP backhaul connectivity is provided by a wired Ethernet network connection or an optional integrated radio modem supporting either GPRS or CDMA services.

Target hosts may be any platform supporting standard port-based IP connections including VPNs, 3rd party application servers, or the management servers from Sensys Networks, SNAPS Professional or Sensys System Manager.

2.4.3.2 Central Point of Authority

An Access Point dictates and stores the operating parameters of devices on a Sensys network[3]. These parameters are associated with:

- wireless radio communications
- event reporting
- event detection behavior
- time synchronization

These parameters are discussed later in this section.

---

[3] A limited number of parameters are stored in individual wireless Sensors, Repeaters and Contact Closure cards.

2.4.3.3 Central Point of Management

Management of network equipment is performed via the Access Point with TrafficDOT, a software tool that establishes a connection to the network through the Access Point. All configuration, device manipulation and firmware updates occur in this manner. (See the *Network Management* chapter.)

2.4.3.4 Central Point of System Definition

Access Points define global network characteristics such as IP address, DHCP and DNS hosts, VPN targets, event data transfer details (push settings, poll settings, etc.), graphing parameters and other attributes. These elements are discussed later in this section.

2.4.4 Wireless Radio Communications

Radio communications occur in the 2.4 GHz unlicensed ISM frequency band with radios based on the IEEE 802.15.4 PHY industry standard with a raw over-the-air data rate of 250 kbps. A Sensys Wireless Vehicle Detection System operates on one of 16 defined channels in the 2.4 GHz ISM band. Each channel has a nominal bandwidth of 2 MHz and is centered at the following frequencies:

Channel 0	2.405 GHz	Channel 1	2.410
Channel 2	2.415	Channel 3	2.420
Channel 4	2.425	Channel 5	2.430
Channel 6	2.435	Channel 7	2.440
Channel 8	2.445	Channel 9	2.450
Channel 10	2.455	Channel 11	2.460
Channel 12	2.465	Channel 13	2.470
Channel 14	2.475	Channel 15	2.480

An Access Point operates on a single channel, fixed channel configured by the customer at installation. All Sensors and Repeaters[4] that directly communicate with the Access Point use the same channel.

Equipment from Sensys Networks ships configured to channel zero. A total of sixteen channels provides a range of alternatives for installations that experience interference as a result of other local RF transmissions.

2.4.4.1 Antenna

Access Points use an embedded directional antenna known as a *microstrip patch antenna*. The antenna's directional beam pattern provides a main lobe directed perpendicular to the top surface, with its maximum signal radiated along this boresight and decreasing symmetrically as the elevation (vertical) or azimuth (horizontal) angle from the boresight increases.

---

[4] The Repeater channel referred to here is the *Repeater-to-Access Point* channel. By definition, the *Sensor-to-Repeater* channel will differ.

At either an azimuth or elevation angle of ±60°, approximately half the maximum signal strength is transmitted, diminishing rapidly as the azimuth or elevation angle increases. The transmit beam pattern also describes the antenna's response to received radiation.

The transmitted and received signal is likely to be affected by its orientation to other devices as well as by nearby stationary and moving objects. (See also the Sensys documents *Design Guidelines for Freeway Applications* and *Design Guidelines for Intersection Applications* for more information.)

2.4.4.2 Orientation and Beam Pattern

In general, the ideal orientation of an Access Point is such that its Sensors and Repeaters are within an approximate 120° field of view (±60° in both elevation and azimuth from the boresight).

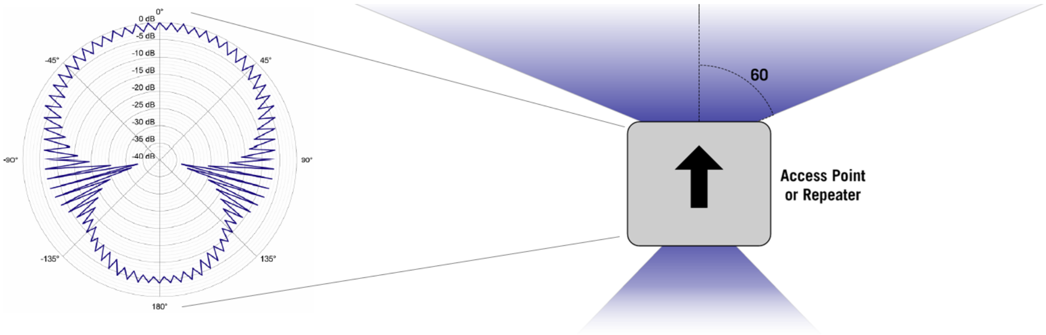


Figure 2.8: Antenna beam pattern (approximate)

Note, however, the antenna transmits one-quarter its maximum power level in the opposite direction from the boresight, radiating from the back of the Access Point. In certain cases, the beam pattern toward the back of an Access Point can be used, although its range is much less than the range in the forward direction.

For example, if two Sensys Repeaters are needed to support Sensors located at opposite approaches to an intersection or freeway ramp entrance, it may be possible to use the front and rear beams from a single Access Point to establish radio links of acceptable quality to the Repeaters rather than implementing multiple Access Points.

2.4.4.3 Proximity to Sensors

The maximum range between an Access Point and any Sensor is determined by such site-specific variables as the local terrain, the mounting height of the Access Point and the orientation of the Access Point to the Sensor (for example, pointing directly at the Sensor).

In general, a maximum range of 125 feet (38 meters) can be obtained. Range expectations as a function of mounting height are summarized in the following table:

Height of Access Point Relative to Road Surface	Maximum Recommended Range to Sensor
16 feet (5 meters)	125 feet (38 meters)
20 feet (6 meters)	150 feet (46 meters)
30 feet (9 meters)	175 feet (53 meters)

Table 5: Recommended Maximum Access Point to Sensor Ranges by Access Point Mounting Height

In practice, the quality of radio communications in the field may differ significantly from the above. Sensys Networks provides measures of RF signal strength and quality (see *RSSI* and *LQI* below) that should be used to assess a particular network design prior to final installation.

Note: the values shown above are guidelines. Actual field values for RSSI and LSI must be monitored to ensure signal strength and link quality are adequate to the range and the needs of the application.

2.4.4.4 Proximity to Repeaters

The maximum range between an Access Point and a Repeater – while influenced by local terrain and the mounting heights of each device – depends more critically on the orientation of the devices to each other.

The gain of each unit's built-in directional antenna is maximized when they are within 60° of facing each other. Given a clear line-of-sight between the face of the Access Point and the face of a Repeater, reliable communications can be expected across distances up to 1,000 feet (305 meters). Given a clear line-of-sight between the face of an Access Point or Repeater and the *back* of the other unit, use 400 feet (122 meters) as a maximum separation. Back-to-back topologies are not recommended.

In some installations, to ensure adequate coverage of Sensors, it may be necessary to point the Repeater in a direction other than within 60° of the Access Point. Doing so limits the range between the Repeater and Access Point.

2.4.4.5 Radio Performance

Two measures characterize the quality of the wireless channel – *Received Signal Strength Indicator* and *Line Quality Indicator*. Each measure can be monitored with TrafficDOT. (See the section regarding the *Access Point Main* window in the *Network Management* chapter for more information.)

2.4.4.5.1 Received Signal Strength Indicator (RSSI)

RSSI is measured in dBm, dB relative to 1 mW into a 50 Ohm impedance. Typical RSSI numbers will range from -50dBm (for Sensors very close to a receiver) to -95dBm (the far edge of RF coverage).

It is possible to operate with an RSSI as low as -90dBm, but doing so leaves no margin for signal degradation. Signal degradation can occur either in short bursts – for example, when a vehicle is driving over the Sensor – or in long intervals (up to days), as may occur when a vehicle is parked very near the Sensor or during a heavy snow storm.

Recommended performance ranges are given in the table below:

Application	RSSI range of all RF Links
Count	Greater than -79dBm
Stop bar detection	Greater than -69dBm

Table 6: RSSI Performance for Applications

Note: RSSI expresses the amount of signal loss, thus it is a negative number. Better RSSI is represented by values closer to zero.

2.4.4.5.2 Line Quality Indicator (LQI)

LQI is an indicator of link error rate or signal-to-noise ratio (SNR). LQI is affected by both RF signal strength and local RF interference. TrafficDOT displays LQI as a number between 40 and 99, with 99 representing optimal quality. LQI values above 95 are considered “good”; LQI values around 90 are considered “adequate”.

It is not uncommon to find LQI values “bouncing” between low, marginal and acceptable values. This usually results from occasional interference such as burst transmissions from nearby Wi-Fi equipment or other sources of RF energy. While it is optimal to avoid such interference, occasional degradation will typically not impair the network's performance.

2.4.4.5.3 Trend Monitoring

When evaluating either RSSI or LQI the long-term trend is much more significant than any particular point-in-time measurement. The diagnostic application APDIAG is provided to aid in assessing performance trends of Sensys Networks.

2.4.4.6 Radio Settings

An Access Point's RF parameters are stored in flash memory. The parameters described in this section are:

- RF channel
- Radio identifier
- LNA Gain
- Power Amplifier (PA) Maximum Power
- Power Amplifier (PA) Attenuation

See the section *Configuring Access Points* in the *Network Management* chapter for more information.

2.4.4.7 Radio Frequency (RF) Channel

There are 16 available frequencies in the unlicensed channel band in which an Access Point and its Sensors and Repeaters communicate. The frequencies are not interleaved nor do they overlap.

2.4.4.8 Radio Id, LNA Gain, PA Max. Power

These elements represent hardware attributes acquired by the Access Point from various components. They are for information only and are not customer configurable.

2.4.4.9 PA Attenuation

Power Amplifier Attenuation specifies an amount (in dB) by which the signal strength of the radio broadcast is reduced. This is intended for situations outside the USA where foreign government regulations or local transmitters prohibit RF transmissions in excess of a specified dB.

2.4.5 Network Protocol

Reliable wireless communications between Sensys devices is based on the SNP protocol. The attributes of the protocol are discussed in this section.

2.4.5.1 Network Time

Access Points use two clocks: the *radio transmitter clock* and the *timekeeping process* that is a part of the Linux operating system executing on the Access Point.

The radio transmitters of Sensors and Repeaters are always synchronized to the radio clock of the Access Point. The Linux clock may operate on its own or be synchronized to an trusted, external time source, such as a time server maintained by NIST or other authority. Additionally, a system parameter allows for binding the radio clock to the Linux clock.

For optimal reporting results, Sensys Networks recommends that (*i*) the Linux clocks of all Access Points be configured to acquire time from a trusted source, and (*ii*) all Access Points are configured to synchronize the radio clocks of the devices it services with that Access Point's Linux clock. Configuring network time in any other way – while having no impact on the detection capabilities of the network – creates the possibility of event data lacking portability or meaningful context.

See the section *Configure and Manage System Parameters* in the *Network Management* chapter for specific information on configuring network time and Access Points.

2.4.5.2 Security

SNP radio transmissions never carry commands; only data is transmitted. Therefore, while RF communications may be subject to local interference, there is no opportunity to embed malicious instructions to a network device or upstream traffic system.

IP communications with Access Point – be they over wired or cell-based connections – adhere to industry standards, thereby allowing the integration of any IP-based security or authentication product. Access Points natively support VPN connections, role-based access, *superuser* password protection, and other techniques.

2.4.5.3 Full Duplex

Communications between an Access Point and its Sensors and Repeaters are two-way: *uplink* packets from the Sensor to the Access Point contain detection data, while *downlink* packets from the Access Point to the Sensors are used for synchronizing and sending commands to the Sensors.

2.4.5.4 Packet Acknowledgment and Retransmission

By default, Access Points explicitly acknowledge every data transmission received from a Sensor. In the field, it is not uncommon to experience a degree of packet loss due to local, transient interference. To accommodate this, Sensors automatically retransmit their data if they do not receive an acknowledgment within an expected time interval.

2.4.5.5 SYNC Packets

Access Points transmit synchronization (SYNC) packets to the Sensors in the network to elicit data transmissions. SYNC packets are derived from individual Sensor IDs so that each Sensor can identify its SYNC packet. After detecting two consecutive SYNC packets a Sensor begins transmitting events.

2.4.5.6 Time Slots

Sensys networks operate via a Time Division Multiple Access (TDMA) scheme. A general model is shown below.

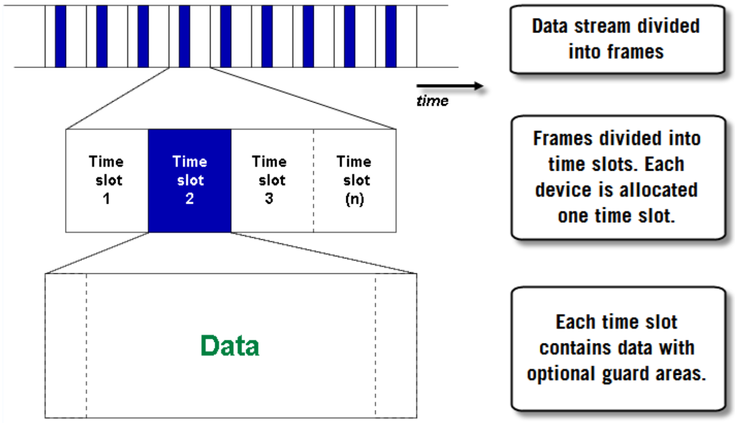

time
Time slot 1
Time slot 2
Time slot 3
Time slot (n)
Data
Data stream divided into frames
Frames divided into time slots. Each device is allocated one time slot.
Each time slot contains data with optional guard areas.

Figure 2.9: Generalized TDMA communications model

In a given network, each device shares a common RF channel and avoids interference by transmitting and receiving according to a predetermined plan that dictates the following:

- the order in which devices will transmit/receive
- the duration any particular device uses to transmit/receive
- the duration between successive opportunities any particular device has to transmit/receive

The order of device communications in a Sensys network is implemented via a network element known as a *time slot*. Each device transmits on a unique time slot.

The duration any particular device uses to transmit/receive is fixed (at approximately 2 milliseconds) and is not configurable by the end-user.

The duration between successive opportunities to transmit/receive is implemented in the *transmit interval* element (discussed below).

Sensys networks operate with a nominal actual frame size of 125 milliseconds, divided into 64 time slots.

2.4.5.7 Time Slot Use

Time slots transmit the following types of information between devices:

- time synchronization codes sent by Access Points
- event data sent by Sensors
- acknowledgment of receipt of event data by Access Points
- status and identity data sent by Sensors and Repeaters
- management and device configuration commands sent by system administrators through Access Points

The relationship between *types of packets* and the *time slots* used to transmit them in a Sensys network is shown below:

Time Slot	Packet Content and Use	Packet Origin
0	System (synchronization packet)	Access Point
1	System (sync. packet continued)	Access Point
2	Download (management commands, firmware download)	Access Point
3	Download (continued)	Access Point
4	Acknowledgment (of Sensor data transmission)	Access Point
5	Acknowledgment (of Sensor data transmission)	Access Point
6 through 32	Detection event data transmission	Sensors or Repeaters
33	Reserved for Sensys Networks	n/a
34	Acknowledgment (of Sensor data transmission)	Access Point
35	Reserved for Sensys Networks	n/a
36 through 62	Detection event data transmission	Sensors or Repeaters
63	Reserved for Sensys Networks	n/a

Table 7: Time Slot Allocation for Standard 125ms Sensys Frame

Note: Sensors prior to VDS release 1.6 represented time slots slightly differently. After upgrading a Sensor's firmware to VDS release 1.6, its time slot must be reassigned.

2.4.5.8 Transmit Interval

For a given Sensys network, the end-user configurable element *transmit interval* specifies the duration between successive opportunities to transmit/receive on the part of any particular device on the network. In so doing, it also determines:

- the number of devices in the network
- the optimal latency for transmission by any device

2.4.5.8.1 Transmit Interval and Network Size

The transmit interval sets the *effective communications frame size*[5] for a given Sensys network. That is, it sets the number of time slots that comprise the entire set of time slots processed in a single communication cycle. Longer transmit intervals result in more time slots – which in turn leads to more devices and larger networks.

For example, *Table 7* above presents the time slots reserved for system management packets (that is, those that are not available for vehicle event packets) for a network operating at the nominal transmit interval of 125 milliseconds. Ten time slots are reserved, leaving 54 time slots for vehicle event data. Given that each device requires its own unique time slot, the network can support up to 54 transmitting devices (Sensors and Repeaters).

---

[5] Not to be confused with the *actual frame size* which is fixed by Sensys Networks at 125 ms.

If more Sensors or Repeaters are needed, the transmit interval – and therefore the network latency – must be increased.

2.4.5.8.2 Transmit Interval and Latency

The transmit interval also defines the minimum amount of delay experienced between two communicating devices under *optimal* conditions. (Because wireless communications are neither guaranteed nor impervious to interference, *actual* latency may be greater than the optimal as a result of the need to retransmit data.) Latency is typically a key concern in applications.

2.4.5.8.3 Latency and Sensor Event Reporting

Sensors can be set to handle event data transmission in either of the following ways:

- events are transmitted as they occur
- events are buffered (up to a maximum of 16) and transmitted at (*i*) a fixed reporting interval or (*ii*) as needed to maintain a preset amount of free space in the event buffer.

Transmitting events as they occur minimizes data latency but consumes more of the Sensor's battery. Buffering events, by communicating more event data per transmission, limits power consumption and typically reduces total bandwidth utilization. However, it also introduces reporting latency of as much as 10 seconds. The choice between these options is normally determined by the needs of the application.

2.4.5.8.4 A General Rule for Transmit Interval/Latency

For a given network and application, Sensys Networks recommends configuring the network to operate with the lowest possible latency for the number of Sensors required.

The nominal transmit interval (latency) of a Sensys network is 125 milliseconds. Transmit interval is one of the *Event Reporting* parameters maintained with TrafficDOT.

(Refer to *Table 8* below for more information regarding latencies supported by Sensys Networks and total network size.)

2.4.5.9 Low Latency Modes

In certain intersection applications, overall latency is critical. To address such applications, Sensys supports two low-latency modes — ¼-frame mode and ½-frame mode — that reduce the TDMA latency to 31.25 ms and 62.5 ms, respectively. These modes result in maximum responsiveness to vehicle detections but impose constraints on network capacity and topology.

2.4.5.10 Access Point Capacity

The number of devices (Sensors and Repeaters) an Access Point can support follows directly from the network's transmit interval as shown in the table below.

Transmit Interval / Latency	Total Time Slots	Maximum Number of Devices
32.25 ms	16	11
62.5 ms	32	27
125 ms	64	54
250 ms	128	108
500 ms	256	216
1 sec	512	432
2 sec	1,024	864
3 sec	1,536	1,296
5 sec	2,560	2,160
6 sec	3,072	2,592

Table 8: Access Point Device Capacity (nominal transmit interval highlighted)

Larger installations may include Repeaters that impose additional rules regarding capacity. See the section *Sensys Repeater* below for more information.

2.4.6 Event Reporting Parameters

Sensors detect vehicles by inference. The presence and absence of vehicles is determined by comparing the difference between the detected local magnetic field and a self-maintaining baseline value. If the magnitude and duration of the difference meets or exceeds certain thresholds, a *detection event* is declared and communicated to the Access Point.

The attributes that define how the events are communicated to the Access Point are discussed in this section. All of the parameters are configured with TrafficDOT. (See the section *Configuring Access Points* in the *Network Management* chapter for more information.)

2.4.6.1 Reporting Overview

Event reporting pertains to Sensors transmitting detection data to an Access Point. Event reporting parameters are end-user configurable global attributes, stored in the Access Point's configuration, that dictate how event reporting occurs on a given network.

The parameter *transmit interval* – described in the preceding section – defines how often devices may transmit, and thus, the shortest interval for reporting. However, there are circumstances that may dictate event reporting that occurs on a less frequent basis. These situations involve queuing events prior to reporting them. There are several considerations:

- *Battery life* – packet transmission consumes power. Thus, packets that contain multiple events use power more efficiently than packets that contain only one event. Buffering events allows more events to be sent per packet.
- *Packet volume* – packet receipt and acknowledgment consume processor resources on the Access Point. Again, increasing the number of events per packet minimizes processor resources per a given level of events.
- *Application requirements* – the nature of the application with respect to its tolerance for latency must be considered. If minimal latency is required, Sensors should be configured to report as frequently as possible.

The attributes *Maximum reporting latency*, *N Events / Near full*, and *Synchronized reporting* work together to define when Sensors report their event data.

In addition, two other parameters are described in this section. *Report only ON events* adjusts what type of detection event is reported, and *Watchdog timeout* dictates Sensor behavior in the prolonged absence of events.

2.4.6.2 Event Parameters

The event reporting parameters are as follows:

- Transmit Interval (discussed above)
- Maximum Reporting Latency
- N Events / Near Full
- Synchronized Reporting
- Report Only ON Events
- Watchdog Timeout

2.4.6.3 Maximum Reporting Latency

The maximum reporting latency is the maximum amount of time that may pass between successive transmissions from a given Sensor. Or, alternatively, it can be described as the maximum period during which events will be queued prior to reporting. Events are queued until this time value is reached, at which point all events are transmitted in one packet.

Because event frequency cannot be known in advance, and retransmission of events may be required, the event queue may fill before the time value is reached. Therefore, a queue control mechanism is implemented via the *N Events / Near full* setting (see next element). *Maximum Reporting Latency* is a global parameter.

Note: To configure Sensors to report at the first opportunity after the event occurs, set this parameter equal to Transmit Interval. Additionally, this parameter should never be less than the value of Transmit Interval.

2.4.6.4 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.

When the “near full” state is reached, the Sensor transmits data at its next opportunity (its next time slot) without regard to how much time is left in the *Max. Reporting Latency* counter.

TrafficDOT presents these parameters as pairs representing typical combinations. Although a range of paired values is presented, Sensys Networks recommends using the “`16 / 12`” setting in every case where a more reporting latency can be tolerated.

Setting a relatively high value for this parameter in conjunction with a longer *Max. Reporting Latency* results in a “data driven” event reporting model. A “time driven” reporting model can be achieved via the following parameter.

2.4.6.5 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) at successive fixed time intervals. The interval is set via the *Max. Reporting Latency* which is used with the Access Point's Linux timekeeping process.

For example, given a network time of 12:00:00 AM and a *Max. Reporting Latency* of 5 seconds, Sensor reporting would be as of these intervals:

12:00:05 AM
12:00:10 AM
12:00:15 AM ... and so on.

Setting this attribute “on” results in a “time driven” event reporting model that is useful in situations where data is required to produce statistics at fixed intervals. Setting this attribute “off” results in a “data driven” event reporting model.

Note: Sensys Networks recommends the use of synchronized reporting as a best practice.

2.4.6.6 Common Event Reporting Configurations

Many applications have the same requirements with respect to event reporting. The table below presents the most common applications and the configuration settings Sensys Networks recommends for each.

Application	Max. Reporting Latency (secs)	N Events / Near full	Synchronized Reporting
Freeway count station	10.000	16 / 12	On
Arterial count station	10.000	16 / 12	On
Advance detection	00.125	4 / 4	n/a
Stop bar	00.125	4 /4	n/a

Table 9: Event Reporting Configurations for Common Applications

2.4.6.7 Report Only ON Events

This attribute globally enables (or disables) a constraint on the nature of the data reported for a detection. Enabling this attribute restricts event reporting to the ON event (defined as the rising edge of a detection pulse). Disabling this attribute results in the reporting of both the ON event and the OFF event (defined as the falling edge of a detection pulse).

2.4.6.8 Watchdog Timeout

The watchdog timeout attribute specifies a number of seconds of inactivity a Sensor will wait before transmitting a packet. That is, in the absence of events a Sensor will wait no longer than this value before transmitting a packet to its Access Point.

This guarantees that an Access Point has contact with the Sensor even during periods of prolonged inactivity with regard to event detections. This can be compared to a "heartbeat packet" in other network environments. Timeout values may range from zero to five minutes. Higher values conserve battery power.

2.4.7 Event Detection Parameters

Event detection parameters are a collection of elements that define the network's detection zones and sensitivity. For Sensors operating in Count mode, the parameters are inherited from the Access Point's configuration which can be adjusted with TrafficDOT. For Sensors operating in one of the Stop Bar modes, the settings are embedded in the mode's algorithm. (Vehicle detection is discussed in the section *Sensys Wireless Sensor* above.)

2.4.8 Network Management

Sensys networks are managed via TrafficDOT, Sensys Network's network management application, after a connection is made to an Access Point.

2.4.8.1 Network Management Activities

TrafficDOT enables a range of activities useful in operating and managing wireless Sensor networks. With TrafficDOT, you can:

- View current detection activity via the real-time detection window
- Configure equipment including Sensors, Access Points, Repeaters and Contact Closure cards
- Maintain databases of Sensor locations and pairs
- Update device firmware
- Define global, identifying characteristics of the network
- Perform backup and restore operations
- Review and update the software license file
- Issue commands from the Access Point's command line interface
- Generate charts/graphs of selected Sensors
- Perform other miscellaneous functions

See the section *Configuring Access Points* in the *Network Management* chapter for more information.

2.4.9 Network System Definition

Access Points serve as the central repository for global, identifying information that defines a network. Network characteristics (including IP address, service hosts providing DHCP and DNS services, VPN targets), event data transfer details (push settings, poll settings, etc.), graphing parameters and other attributes are set through the Access Point via TrafficDOT.

The system configuration elements are discussed below.

2.4.9.1 Network Characteristics

Network characteristics define the settings necessary to conduct IP communications with the Access Point.

2.4.9.1.1 IP Mode

Designates how the Access Point will acquire its IP address.

By default, Access Points function as DHCP (Dynamic Host Control Protocol) clients that dynamically “lease” IP addresses from a pre-authorized range. If DHCP is not used, an IP address must be specified. (The system default value for this element is “`DHCP`”.)

Use the value “`modem`” for Access Points that connect to the Internet via a wireless packet data service. It is assumed that the data provider will supply the IP configuration for the Access Point (on the data modem interface), so other IP settings are not required.

Use the value “`static`” for Access Points that will operate using a predetermined IP address assigned to the device via this element. When a static address is supplied, other elements of the IP configuration are required.

Use the value “`Off`” in situations where IP communications with the Access Point are not required. This conserves battery power. (This is not common.)

2.4.9.1.2 Modem Type

Specifies the type of cellular data modem used on an Access Point for back haul communications. Modems are an optional feature.

2.4.9.1.3 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.

This element defaults to “`10m`”, a setting that is useful in situations where the length of the physical cable used to make the connection exceeds the limits for higher speed communications.

Use the value “`automatic`” to direct the system to sense the link speed without user input.

Set the value to “`off`” in situations where communications on the Access Point's Ethernet port are not required; this conserves power.

2.4.9.1.4 Network Mask

A 32-bit mask that identifies the local portion of a local area network (LAN), and in so doing, identifies which hosts are communicated to through gateways.

This setting is required when the *IP mode* is “`static`”.

The system default is “`255.255.255.0`”.

2.4.9.1.5 IP Address

Unique network address for IP communications to and from the Access Point over the Ethernet port.

This value is assigned automatically when the IP mode is set to "`DHCP`"; otherwise an entry conforming to standard IP notational format is required.

The system default is "`192.168.2.100`".

2.4.9.1.6 Gateway

The IP address of a network node to which the Access Point directs traffic destined for external networks.

This value is assigned automatically when the IP mode is set to "`DHCP`"; otherwise an entry conforming to standard IP notational format is required.

2.4.9.1.7 DNS

The IP address of a network node providing domain name services to the Access Point.

This value is assigned automatically when the IP mode is set to "`DHCP`"; otherwise an entry conforming to standard IP notational format is required.

2.4.9.1.8 DHCP Monitoring Host

The IP address of a network node providing DHCP services to the Access Point.

2.4.9.1.9 NTP Servers

The hostname(s) of servers providing the current time via NTP (Network Time Protocol), a draft Internet standard for computer clock synchronization (see RFC1305).

The time supplied by the time servers can be used by the Access Point to synchronize the time base of the network.

The system default host names reference US based timeservers that are made available via a collaborative project coordinated by ntp.org and are:

```
1.us.pool.ntp.org
2.us.pool.ntp.org
```

Multiple hostnames for timeservers are recommended for contingency purposes.

2.4.9.2 VPN (Virtual Private Network) Characteristics

VPN characteristics define the settings necessary to establish a virtual private network connection between the Access Point and and an external server such as a SNAPS server from Sensys Networks.

Virtual private networks (VPNs) use a public network and specialized security protocols to establish a network link between two nodes that operates as a "point to point" connection without requiring dedicated, physical infrastructure between the nodes. 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, or receives its IP address via dynamic assignment.

For example, it is common for providers of cellular data services to allow end-point IP nodes to originate communications but not to terminate them. This is understandable when the end-point node is a mobile phone, PDA or other device. However, when the end-point node is an Access Point, this policy is problematic: an Access Point would be able to transmit, but management commands and other instructions could not be received by the Access Point.

Thus, a VPN connection originated by the Access Point, is used to enact full, two-way communications between an Access Point and a management/application server; communications can be originated by either side of the VPN connection.

2.4.9.2.1 SNAPS

Designates a Sensys Management Server acting as the VPN server. Hosts can be specified by their IP address or DNS name.

The default value for this element is "`snaps.sensysnetworks.net`".

2.4.9.2.2 VPN Mode

Specifies the protocol used for creating the VPN connection.

The value "`PPTP`" indicates use of *Point-To-Point Tunneling Protocol*, an approach to establishing and authenticating VPN connections popularized by Microsoft Corporation.

The value "`PPIP`" indicates use of a Sensys Networks private implementation of a network tunneling protocol used in situations where PPTP cannot be used. PPIP implements PPP over TCP. Do not select this value without prior consultation with Sensys Networks.

2.4.9.2.3 VPN User

The user account string used to establish and authenticate the VPN connection. Use of this element is dependent on the configuration of the VPN host.

2.4.9.2.4 VPN Password

The user account permissions string used to establish and authenticate the VPN connection. Use of this element is dependent on the configuration of the VPN host.

2.4.9.2.5 Monitor Host

Specifies 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.

Hosts may be specified by either their IP address or DNS name.

2.4.9.2.6 Modem ISP

Designates the provider of the packet data service by name. The Access Point is designed to detect the provider, however, in some cases automatic detection does not occur. See the sections *Working With Modem Properties* and *Working With VPN Properties* in the *Network Management* chapter for more information. Contact Sensys Networks if the provider is new or uncommon.

2.4.9.2.7 Modem PIN

Designates the PIN (personal identification number) associated with the SIM card used in the cellular data modem. This is an optional element dependent on the requirements of the provider of the cellular data service.

2.4.9.3 Statistical Data Transfer

Statistical analysis of Sensor data includes value-added activities such as summarization, aggregation, derivation of other values, etc.

Access Points may optionally be used as hosts for processing Sensor data and transferring it to other platforms, but these activities exact a cost in terms of CPU and disk resources. Alternatively, Access Points may be configured to forward raw detection events to upstream systems.

2.4.9.3.1 Storage Limits

An Access Point reserves 130 kilobytes (KB) for caching raw detection data prior to upstream transmission.

Additionally, a total of 500 KB is reserved for local instances of Sensys Networks' statistical application, APSTAT. Multiple instances of APSTAT may be invoked on the Access Point according to the needs of the application, but all instances share the 500 KB memory pool. The allocation of the pool to APSTAT instances can be tuned with TrafficDOT.

Estimating storage capacity is dependent on how the Access Point is configured in regard to (*i*) the type of reporting (*per-lane* versus *per-vehicle*), and (*ii*) the reporting frequency.

For example, per-lane records consume approximately 100 bytes per instance. Assuming a reporting frequency of 5 minutes, up to 17 days of statistics could be stored on the Access Point.

Two archiving and data transfer plans are built into the system to enable managing data collected over time. There are the *push* and the *poll* methods.

Push refers to moving Sensor data from one host to another triggered by actions of the the Access Point. (See also the sections in this chapter regarding the software applications APSTAT and APPUSHSTAT for more information.)

Poll refers to moving Sensor data from the Access Point to another host based on a request by the consuming host (i.e., the host that uses the statistics).

2.4.9.4 Data Transfer via the Push Method

Settings for push type interfaces are configured in TrafficDOT's *System Configuration* window via the *Push* tab. Completing the *Push* tab fields and saving the data results in a new instance of APSTAT launching on the Access Point the next time the Access Point is restarted.

2.4.9.4.1 Push Targets

The hosts that act as the recipients of pushed data are referred to as *destination servers*. A destination server is a host able to receive Sensor data for display or analysis.

Access Points support up to two destination servers. Both servers are described in terms of the same elements listed below. (See the reference content for the application APPUSHSTAT for more information.)

2.4.9.4.2 Destination Server

Designates the target host by IP address or DNS name. (*Note*: at least one entry is required to push data.)

2.4.9.4.3 Destination Port

The port number on the target server used by the Access Point's push process to communicate with it.

2.4.9.4.4 Buffer Reports

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

Enabling this feature directs the Access Point, on encountering a disconnection, to send all data since the time of the disconnection once the connection is restored. If the duration of the disconnection is such that more data is queued than can be stored, then all of the data in the queue is sent, and some data may be lost. (The queue size is given by the element *Maximum Space* described below.)

Disabling this feature directs the Access Point, on encountering a disconnection, to drop data since the time of the disconnection and transmit only the last line in the buffer once the connection is restored.

2.4.9.4.5 Stay Connected

Designates the behavior of the Access Point in regard to the status of the TCP connection during the idle time between separate “pushes” of the data from the Access Point to the destination server.

Enabling this feature directs the Access Point to retain the connection across idle times between data transmissions. Disabling it directs the Access Point to drop the connection between separate data transmissions.

2.4.9.4.6 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.

Enabling this function results in the Access Point waiting a period of five seconds after a transmission to receive an acknowledgment from the destination server. If an acknowledgment is not received within that time, the transmission is deemed by the Access Point as unsuccessful. Disabling it suspends acknowledgment messages for all data pushed by the Access Point.

2.4.9.4.7 Acknowledgment Timeout

Specifies the amount of time (in seconds) the push process waits to receive an acknowledgment packet from the destination server before declaring a transmission failure and retransmitting.

2.4.9.4.8 Units

Specifies the unit scale used in generating statistics. *Imperial* denotes use of feet, miles and miles per hour (mph). *Metric* denotes use of meters, kilometers and kilometers per hour (kmph).

2.4.9.4.9 Individual Car Reports

The Sensys Networks statistical analysis application – APSTAT – compiles statistics in one of two operating modes. The default operating mode is *aggregate report* mode. This element allows the designation of *real-time report* mode in which statistics are generated based on individual vehicle detections. Real-time report mode also supports outputting of data compatible with the Marksman format.

2.4.9.4.10 Report Interval

In aggregate report mode, this element specifies the time duration between writing of separate report *entries*. In real-time report mode, this element specifies the time duration between creating statistical *files*. Supported intervals range from 10 seconds to 15 minutes.

2.4.9.4.11 Maximum File Size

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

2.4.9.4.12 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.

2.4.9.4.13 Speed Histogram

Enables/disables the inclusion of speed bins suitable for building a histogram graph. When enabled, bin ranges may be 1 mph, 5 mph, or the ranges defined in the TTI specification.

2.4.9.4.14 Length Histogram

Enables/disables the inclusion of length bins suitable for building a histogram graph. When enabled, bin ranges may be 1 foot or the ranges defined in the TTI specification.

2.4.9.4.15 Timestamp Assignment

Designates the point in time – relative to the entire length of reporting interval – that corresponds to the timestamp of the report entry. Supported values include:

- time at the *start* of the reporting interval
- time at the *middle* of the reporting interval
- time at the *end* of the reporting interval

2.4.9.4.16 Diagnostic Correction of Averages

Enables/disables the use of Sensor diagnostic data to generate "smart averages" when calculating averages for speeds and lengths. "Smart" averages remove non-responding Sensors from calculations.

2.4.9.4.17 Diagnostic Disclosure

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

2.4.9.5 Data Transfer via the Poll Method

An alternative method to move Sensor data to a destination server is the *poll* method. The poll method is used when data movements are initiated by a request from the destination server.

Completing the data elements on any of the *Poll* tabs results in a new instance of the polling application (such as APPOLLSTAT, APPOLLSTAT_TCP, etc.) to be launched on the Access Point the next time the Access Point is restarted.

Note: Moving data between hosts requires a license file valid for the Sensys Networks Access Point with an Ethernet interface.

2.4.9.5.1 California Department of Transportation (CalTrans) Poll Servers

Sensys networks interface with many different types of traffic management systems. Detector output for California DOT districts 3 and 4 are specifically catered to via custom interfaces.

Settings for these interface sare configured in TrafficDOT's *System Configuration* window via the *CalTrans D3 Poll* and *CalTrans D4 Poll* tabs. Additionally, information about the applications that support those interfaces can be found in the sections APPOLLSTAT and APPOLLSTAT_CALTRANSD4 respectively.

2.4.9.5.2 Sensys Networks Poll Server

Sensys Networks provides a generalized poll server that operates in conjunction with the Sensys statistics generation application operating in aggregate report mode. The server listens for poll requests on a predetermined port and returns the most recent report entry to the client in standard CSV format. Following the response to the client, the TCP connection is closed.

Settings for this type of interface are configured in TrafficDOT's *System Configuration* window via the *Poll* tab.

2.4.9.5.3 TCP Port Number

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

2.4.9.5.4 Units

Specifies the unit scale used in generating statistics. *Imperial* denotes use of feet, miles and miles per hour (mph). *Metric* denotes use of meters, kilometers and kilometers per hour (kmph).

2.4.9.5.5 Individual Car Reports

The APSTAT application compiles statistics in one of two operating modes. The default operating mode is *aggregate report* mode. This element allows the designation of *real-time report* mode in which statistics are generated based on individual vehicle detections. Real-time report mode also supports outputting of data compatible with the Marksman format.

2.4.9.5.6 Report Interval

In aggregate report mode, this element specifies the time duration between writing of separate report *entries*. In real-time report mode, this element specifies the time duration between creating separate *files*. TrafficDOT supports intervals ranging from 10 seconds to 15 minutes; advanced users may specify other values.

2.4.9.5.7 Maximum File Size

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

2.4.9.5.8 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.

2.4.9.5.9 Speed Histogram

Enables/disables the inclusion of speed bins suitable for building a histogram graph. When enabled, bin ranges may be 1 mph, 5 mph, or the ranges defined in the TTI specification.

2.4.9.5.10 Length Histogram

Enables/disables the inclusion of length bins suitable for building a histogram graph. When enabled, bin ranges may be 1 foot or the ranges defined in the TTI specification.

2.4.9.5.11 Timestamp Assignment

Designates the point in time – relative to the entire length of reporting interval – that corresponds to the timestamp of the report entry. Supported values include:

- time at the *start* of the reporting interval
- time at the *middle* of the reporting interval
- time at the *end* of the reporting interval

2.4.9.5.12 Diagnostic Correction of Averages

Enables/disables the use of Sensor diagnostic data to generate “smart averages” when calculating averages for speeds and lengths. “Smart” averages remove non-responding Sensors from calculations.

2.4.9.5.13 Diagnostic Disclosure

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

2.4.9.6 Marksman Output Format

Event statistics can be formatted to adhere with the Marksman protocol portion of the Australian Roads specification. These settings are configured with TrafficDOT, from the *System Configuration* window and *Marksman* tab. Specifying these values results in a new instance of APSTAT being invoked the next time the Access Point is rebooted.

2.4.9.6.1 Port Number

A required integer value that specifies the port the Access Point listens to for report requests.

2.4.9.6.2 Mode

Specifies the scope of the output data collection. Supported options are:

- Report only vehicles for which calculations can be made
- Report all vehicles

2.4.9.7 Memory Allocation for Statistics Processes

Access Points may host application processes that perform data transfer and formatting; the processes are configured on the *Push*, *Poll*, *CalTans D3 Poll*, *CalTrans D4 Poll* and the *Marksman* tabs of TrafficDOT. Access Points reserve a total of 500KB of memory for local applications. Memory allocation can be manually set via the *Advanced* tab of the *System Configuration* window, or automatically set by the system. (See the *Network Management* chapter for more detail.)

2.4.10 Communication Interfaces

Access Points have three communication interfaces. They are:

- Ethernet
- Serial port A
- Serial port B

In addition to transmitting system data, in selected circumstances, customer requirements require that power is routed over certain of these interfaces as described in the *Power* section below.

2.4.10.1 Ethernet

The Access Point Ethernet interface supports 10BaseT communications in conjunction with IP environment settings that are dynamically assigned via DHCP or preset via end-user configuration settings.

The factory default IP address is `192.168.2.100`. See the section *Network System Definition* above for more information on IP network settings.

Ethernet cabling is supported via an on-board IP67 rated RJ45 connector. The Ethernet interface supports both standard Power Over Ethernet (PoE) and a Sensys Networks implementation of PoE.

2.4.10.1.1 Siemens Ethernet Interface

Additionally, effective with VDS release 1.8.0, a custom Ethernet interface for use with selected traffic controllers from Siemens Traffic Solutions. (See the section *Configuring System Properties* in the Network Management chapter for more information.)

2.4.10.2 Serial Port A

The first serial port – designated port “A” – supports the following forms of serialized communications and is selectable only by hardware switches. See *VPN Characteristics* above for more information.

- GSM GPRS connectivity - dual-band 850/1900 MHz GSM (North American version), dual-band 900/1800 MHz GSM (International version); up to 85.6 kbps
- CDMA2000 1xRTT connectivity - dual-band 800/1900 MHz CDMA (per specific cellular service provider); up to 153.6 kbps

2.4.10.3 Serial Port B

The second serial port – designated port “B” – supports the following forms of serialized communications; this port is selectable by software via TrafficDOT's *System Configuration* window.

- Optional connection to Global Positioning Satellite (GPS) system
- RS485 communications at a nominal rate of 115kbs required for interfacing to Type 170, NEMA TS1, NEMA TS2 or Type 0270 ATC traffic controllers

Serial Port B must be configured via TrafficDOT for the port's intended use. Additionally, port B supports a Sensys Networks implementation of power delivery via a serialized port.

2.4.11 Power

2.4.11.1 Input Voltages

Access Points use either of the following:

- 36VDC – 60VDC (48VDC nominal) - typically supplied from a power pole near the Access Point
- 10VDC – 20 VDC (12VDC nominal) - typically supplied from a solar panel

2.4.11.2 Draw

Approximate Access Point power consumption is as follows:

- **3.5** watts – AP models with cellular modem back haul support (AP240-EC, AP240-EG, AP240-ESC, AP-240-ESG)
- **2.0** watts – AP models without cellular modem back haul support (AP240-E, AP240-ES, AP240-S

2.4.11.3 Cabling

Access Points receive power via an implementation of Power over Ethernet (PoE). PoE or "Active Ethernet" eliminates the need to run 110/220 VAC power to Access Points. Using PoE, system installers need to run only a single CAT5 Ethernet cable that carries both power and data to each Access Point.

Voltages and cable pin-outs may vary by the requirements of the installation. The combinations are depicted in the following table:

Power Model	Discussion
I. Standard voltage / Standard Pin-out	Typical of a count station where power is supplied by an available power pole and there is no interface to a traffic control system.
II. Non-standard voltage / Standard Pin-out	Typical of a count station where power is supplied by a solar panel and there is no interface to a traffic control system. Non-standard voltage is defined as 9VDC – 20VDC commonly produced by small solar panels.
III. Standard voltage / Non-standard Pin-out	Typical of sites with an interface to a traffic control system that supplies power to the Access Point. The cable pin-out supports both power to the Access Point and control signal to the traffic signal control equipment.

Table 10: Access Point Power Models and Typical Applications

In cases numbered *I* and *II* above, a PoE injector (supplied by Sensys Networks) is used to “inject” the DC voltage onto the CAT5 cable.

In the case numbered *III* above – where in the Access Point is interfaced to a traffic signal controller – an adaptation to the industry standard pin-out has been made by Sensys Networks to accommodate the requirement for the cable to carry both power for the Access Point and signal data for the controller equipment.

The RJ45 cable pin-outs for each of the power models in the table above are shown below:

RJ45 Pin	Power Model I	Power Model II	Power Model III	Notes
Pin 1	ETXD+	ETXD+	ERXD+	
Pin 2	ETXD-	ETXD-	ERXD-	
Pin 3	ERXD+	ERXD+	ETXD+	
Pin 4	PWR+	PWR+	RS485+	RS485 is half-duplex isolated
Pin 5	PWR+	PWR+	RS485-	RS485 is half duplex isolated
Pin 6	ERXD-	ERXD-	ETXD-	
Pin 7	PWR RTN	PWR RTN	PWR+	PWR is polarity insensitive
Pin 8	PWR RTN	PWR RTN	PWR RTN	PWR is polarity insensitive

Table 11: RJ45 Connector Pin-outs for the Power Models described in the preceding table

2.4.12 Expected Maintenance

The enclosure of an Access Point conforms to the NEMA Type 4X standard and the IEC IP67 degree of ingress protection. Access Points are specified for operation from -40°F to +176°F (-40°C to +85°C). No physical maintenance is expected.

2.4.12.1 Firmware Upgrades

Access Points receive software updates over an IP network connection from TrafficDOT, the Sensys Networks network management application.

2.4.13 Additional Capabilities

As a Linux-based device, an Access Point can be readily extended to offer enhanced capabilities. For example, in some custom applications Sensys has enabled an Access Point to function as an IP router, taking advantage of the Access Point's IP connectivity to enhance the system's overall traffic management and monitoring capabilities with those of other peripheral devices. Contact Sensys Networks to discuss a customization requirement.

2.4.14 Reset and Restore Buttons

There are two command buttons inside of the Access Point: *Reset* and *Restore*. These buttons are for the use of Sensys Networks field engineers or certified dealer technicians only. Customers are advised not to use these buttons.

2.4.14.1 Reset

Press the *Reset* button to stop all internal operations of the Access Point, reboot the device, and restart operations. This is equivalent to cycling power to the unit.

2.4.14.2 Restore

To boot an Access Point to its factory default state, use the *Restore* button in combination with the *Reset* button as follows:

- Press the *Restore* button and keep it down while pressing the *Reset* button.

Do not release the *Restore* button until the Access Point has initiated operations – as indicated by the red LED turning off.

Note: while the Access Point will function, it's state may not match its configuration files. RESET and RESTORE are restricted to Sensys Networks technical staff or certified dealer engineers only.

2.5 Sensys Repeater

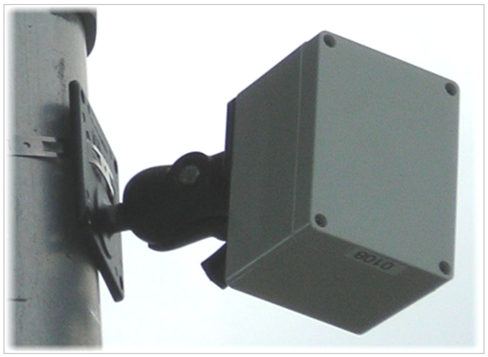


Figure 2.10: RP240-B Repeater

The Sensys Repeater is an *optional* system component that extends the range of an Access Point by receiving and forwarding RF communications between the Access Point and Sensors that would otherwise be out of signal range.

Under optimal conditions, a Repeater relays packets at a rate of 80 packets per second over a distance of up to 1,000 feet (305 meters).

2.5.1 In This Section

This section discusses the following topics:

- Typical Use
- Operations
- Expected Maintenance
- Replacing a Repeater Battery

2.5.2 Typical Use

Repeaters are used wherever the locations of Sensors and Access Points are far enough apart so as to fail to consistently deliver acceptable RF performance. Typically, these conditions occur at large intersections, in ramp management applications, or advance detection situations. Additionally, in some situations, the orientation of an Access Point relative to its Sensors may dictate the use of a Repeater.

2.5.3 Operations

Repeaters are battery-powered and, like Access Points, require a clear line-of-sight to Sensors and an Access Point. A “long life” Repeater is available that contains additional batteries.

Repeaters are identified by a unique hardware id assigned at the factory. Multiple Repeaters may be used with a single Access Point subject to time slot limitations. Additionally, a Repeater may repeat the signals from a second Repeater in a topology referred to as *Tandem Repeaters*.

Repeaters can be introduced to an existing installation at any time without changing hardware or software. However, because Repeaters use two discrete RF channels, some minor reconfiguration of the network may be required.

2.5.3.1 Antenna

Repeaters use a directional antenna known as a *microstrip patch antenna* located parallel to and behind the front face of the device. The antenna's directional beam pattern provides a main lobe directed perpendicular to the top surface, with its maximum power radiated along this boresight and decreasing symmetrically as the elevation (vertical) or azimuth (horizontal) angle from boresight increases.

At either an azimuth or elevation angle of ±60°, approximately half the maximum power level is transmitted, with the power level then diminishing rapidly as the azimuth or elevation angle further increases. This transmit beam pattern also describes the antenna's response to received radiation. The actual beam pattern of a Repeater when installed will be affected by how the device is mounted, its orientation to the Sensors, and other site factors.

2.5.3.2 Orientation and Beam Pattern

In general, the ideal orientation of a Repeater is such that the devices its serves are within an approximate 120° field of view (±60° in both elevation and azimuth from the boresight). Beyond this angular extent, power levels drop off significantly.

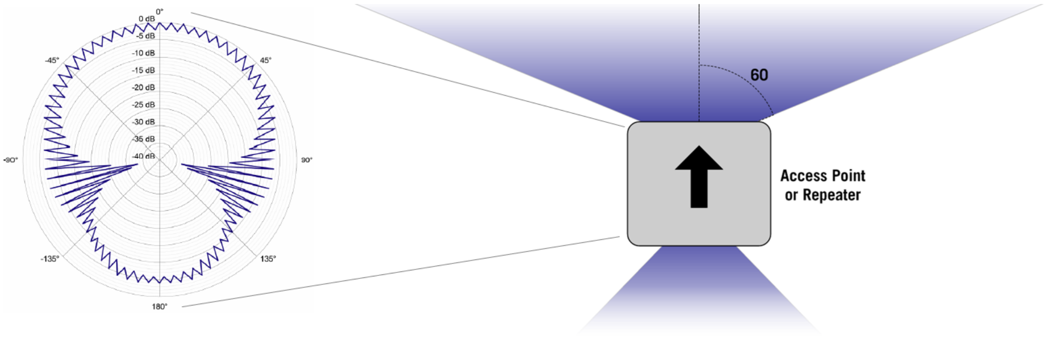


Figure 2.11: Antenna beam pattern (approximate)

Note, however, the antenna transmits one-quarter its maximum power level in the opposite direction from the boresight, radiating from the back of the device. In certain cases, the beam pattern toward the back can be used, although its range is less than the range in the forward direction.

For example, if two Sensys Repeaters are needed to support Sensors located at opposite approaches to an intersection or freeway ramp entrance, it may be possible to use the front and rear beams from a single Access Point to establish radio links of acceptable quality to the Repeaters.

2.5.3.3 Proximity to Other Devices

2.5.3.3.1 Proximity to an Access Point

The acceptable range between a Repeater and its Access Point depends on local terrain, the mounting height of each device, and the orientation of the devices. The gain of each unit's built-in directional antenna is maximized when they are within 60° of facing each other.

Given a clear line-of-sight between the face of the Access Point and the face of a Repeater, reliable communications can be expected across distances up to 1,000 feet (305 meters). Given a clear line-of-sight between the face of an Access Point or Repeater and the *back* of the other unit, use 400 feet (122 meters) as a maximum separation. Back-to-back topologies are not recommended.

In some instances, to ensure adequate coverage of Sensors it may be necessary to point the Repeater in a direction other than within 60° of the Access Point. Doing so limits the range between the Repeater and Access Point.

2.5.3.3.2 Proximity to Sensors

The guidelines for Repeater to Sensor proximity are the same as for Access Point to Sensor proximity. See the table in the Access Point section above for more information.

2.5.3.3.3 Proximity to Other Repeaters

In certain situations – such as to design around a physical object hat impedes a clear line-of-sight between devices or to extend the signal range vector from the rear of an Access Point – more than one Repeater can be arranged in series.

Sites with this arrangement are said to employ *Tandem Repeaters* or *Tier-2 Repeaters*. In such cases, the Repeater closest to the Access Point serves as a packet forwarder in regard to communications between the Access Point and the Repeater farthest away from the Access Point. Using this topology does not constrain the Access Point nor the Repeaters from servicing Sensors.

Distances between Repeaters should conform to the Access Point-to-Repeater rules outlined in the section *Proximity to an Access Point* above.

2.5.3.4 Repeater Channels[6]

Repeaters use a wireless radio that transmits on alternate RF channels. The first channel – known as the Sensor channel – services *downlink* devices (devices toward the edge of the network). The second channel – known as the Access Point channel – services *uplink* devices (devices toward the center of the network).

---

[6] This section uses the terms *uplink* and *downlink* with respect to the destination of network transmissions. Think in terms of satellite communications using an Access Point as the “satellite” and Sensors as the “ground stations”.

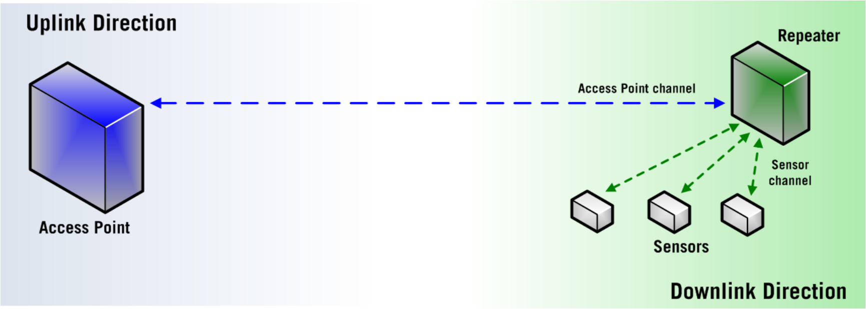


Figure 2.12: Repeater channels

RF communications on the channels are not simultaneous; a latency of approximately four milliseconds is introduced with each Repeater as the radio switches from one channel to another.

2.5.3.5 Using Repeaters

2.5.3.5.1 Repeater Configurations

Repeaters are pre-programmed with two alternate configurations. The configurations differ with regard to which time slots are used to repeat Sensor packets as shown below:

Time Slots Used in Configuration 0	Time Slots Used in Configuration 1
14	16
18	20
22	24
26	28
30	32
44	46
48	50
52	54
56	58
58	62

Table 12: Time Slots Reserved for Use by Repeaters

Only one configuration is active at a time; the default is Configuration zero. (See *Configuring Repeaters* in the *Network Management* chapter for more.)

2.5.3.5.2 Number of Repeaters Per Network

Repeaters are optional. Using nominal settings, a maximum of 10 Repeaters are allowed per network. However, the actual maximum number of Repeaters supported for a given network depends on how the Sensors (and other Repeaters in the case of tandem Repeaters) are allocated to the Repeaters, and the physical disbursement of the Repeaters throughout the installation.

2.5.3.5.3 Number of Sensors Per Repeater

The number of Sensors serviced by Repeaters is a function of the following:

- the transmit interval of the network
- the network topology (specifically, whether tandem Repeaters are used)

A Repeater may service a single device up to the maximum given in the table below. In all cases, the constraint is the total number of Sensors whose packets are repeated.

Transmit Interval	Max. Sensors Per Single Repeater	Max. Sensors From All Repeaters (*see Note 2*)	Max. Sensors Per Tandem Repeater
32.25 ms	1 or 2 (*see Note 1*)	3	Not allowed
62.5 ms	5	10	Not allowed
125 ms	10	20	6
250 ms	20	40	12
500 ms	40	80	24
1 sec	80	160	48
2 sec	160	320	96
3 sec	240	480	144
5 sec	400	800	240
6 sec	480	960	288

Table 13: Repeater Capacities at Alternate Transmit Intervals (nominal transmit interval highlighted)

2.5.3.5.4 Notes

1. The difference results from how time slots are mapped to the two configurations of Repeaters. At the lowest transmit interval, *configuration zero* supports two Sensors while *configuration one* supports one.
2. The figures indicate maximums based on a network that does not employ tandem Repeaters. (That is, all Repeaters communicate directly to an Access Point.)

2.5.3.5.5 Repeater Time Slots

Repeaters typically perform uplink transmissions using the time slot assigned to one of the the Sensor it services. However, in some cases it is advantageous to assign a time slot to the Repeater itself. (See the section *Configuring Repeaters* in the *Network Management* chapter for more information.)

2.5.3.6 Tandem Repeaters

A network topology where a Repeater forwards the packets of a second Repeater is referred to as *Tandem Repeaters*. This topology can be advantageous in situations where the location of Sensors and/or the orientation of Repeaters to an Access Point do not allow acceptable RF performance.

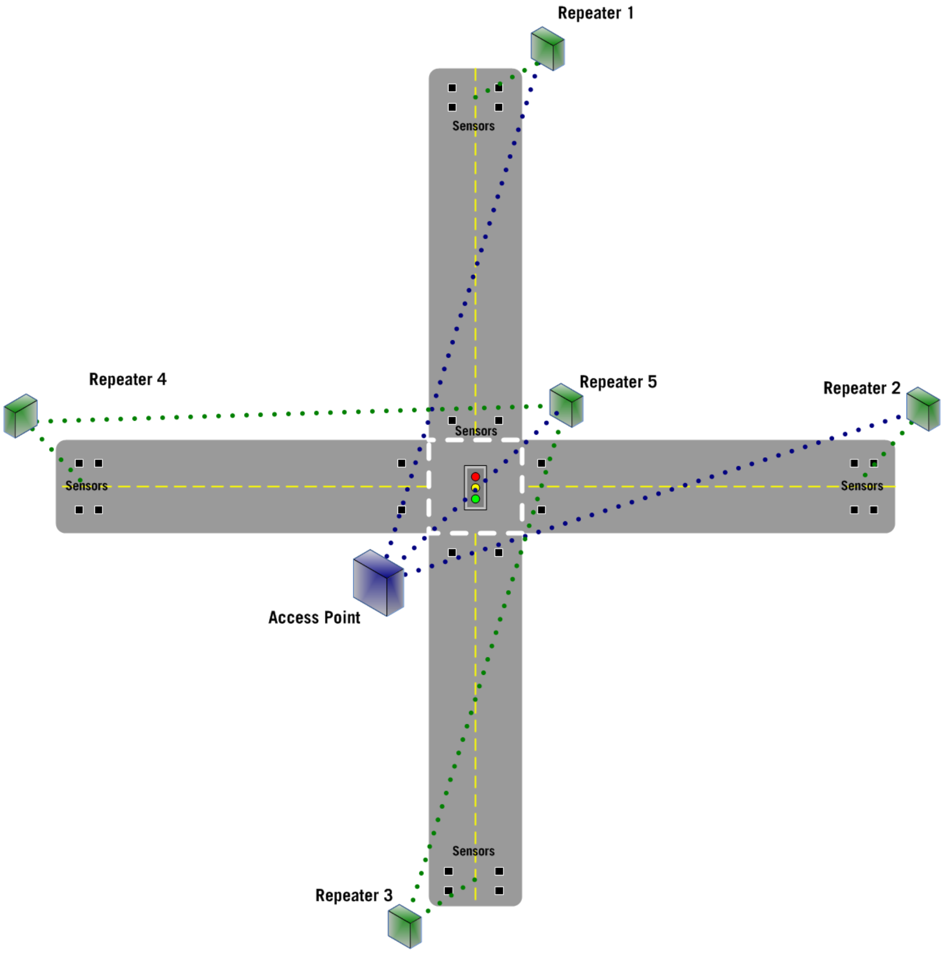


Figure 2.13: Sample Network Topology Using Tandem Repeaters

An example is shown below depicting an intersection with advance detection on all four approaches provided by Sensors that are serviced by Repeaters.

2.5.3.6.1 Notes

1. Sensors providing advance detection use Repeaters 1, 2, 3 and 4.
2. Repeaters 1 and 2 communicate directly to the Access Point.
3. Repeaters 3 and 4 use Repeater 5 (the tandem) to communicate with the Access Point.
4. Repeater 5 communicates directly with the Access Point.

The Tandem Repeater topology introduces the following limitations:

- Tandem Repeaters support fewer devices than “regular” Repeaters. (See the Repeater capacity table above.)
- Additional Repeater latency is experienced.

- Between an Access Point and a given Sensor, the number of Repeaters forwarding packets from the Sensor may not exceed two.
- Tandem Repeaters are not allowed on networks using transmit intervals of less than 125 milliseconds.
- Tandem Repeaters normally do not allow doubling the nominal distance between Access Points and Repeaters due to antenna orientation requirements.

In addition, use of tandem Repeaters alters slightly the paradigm of RF channel labeling used in TrafficDOT. (See the section *Configuring Repeaters* in the *Network Management* chapter for more information.)

2.5.4 Expected Maintenance

The enclosure of a Repeater conforms to the NEMA Type 4X standard and the IEC IP67 degree of ingress protection. Like Access Points, Repeaters are specified for operation from -40°F to 176°F (-40°C to +85°C).

2.5.4.1 Battery Life

Repeaters consumes more power than Sensors. Unlike a Sensor, a Repeater:

- continuously listens for Sensor transmissions
- receives data from multiple Sensors as well as transmits data to its Access Point
- sends a SYNC packet on a continuous basis (every 125 milliseconds)

Consequently, the Repeater has an estimated battery life of two years. Replacement of the Repeater battery can be easily performed in the field, typically without requiring lane closure.

2.5.4.2 Firmware Upgrades

Sensys Repeaters receive optional firmware upgrades over the wireless channel via the Access Point and the TrafficDOT management application.

2.5.5 Replacing a Repeater Battery

The nominal battery life of an RP240-B (standard) Repeater is two years; the nominal battery life of an RP240-B-LL (long life) Repeater is seven years.

Refer to the Sensys document *Replacing Batteries in the RP240-B Repeater* (P/N 152-240-020-004) for procedures regarding battery replacement.

2.6 Sensys Contact Closure Card

The Sensys™ 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 in exactly the same manner as inductive loops.

2.6.1 Sensys Contact Closure Master Card

The Contact Closure Master Card (CC card) is a rack-mountable, hardware interface card that provides up to four configurable control channels to a signal controller and 48VDC isolated power to a Sensys Access Point. Master cards can be configured to occupy one or two slots in a standard controller shelf. (*Note*: one-slot Master card shown at right.)

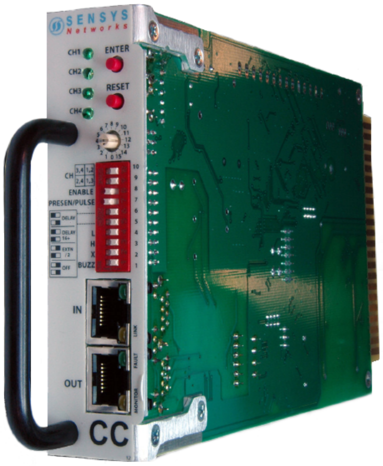


Figure 2.14: CC-170 Master Card

2.6.2 Sensys Contact Closure Expansion Card

Additional capacity (to handle more Sensors or controller channels) is provided by a Sensys Contact Closure Expansion card (EX card). Expansion cards use the same form factor as Master cards and are daisy-chained to a Master card by front-panel RJ45 jacks. Up to 63 Expansion cards can be used per Contact Closure Master card.

2.6.3 Sensys AccessBox

A Sensys AccessBox is a small, three-port junction device that provides the following services:

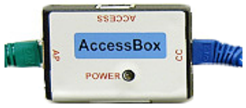


Figure 2.15: CC-ACC AccessBox

- connects an Access Point to a Contact Closure Master card
- isolates and routes power from the controller backplane to the Access Point
- provides a wired port for IP network access (suitable for network configuration, management and data acquisition)

2.6.4 In This Section

This section discusses the following topics:

- Typical Use
- Operations
- Components
- Front Panel Interface
- Circuit-board Controls
- Conformance to TS1 and TS2 Specifications
- Interfaces

2.6.5 Typical Use

Sensys Contact Closure Master and Expansion cards interface the Sensys Wireless Vehicle Detection System to traffic signal controllers so that vehicle detection events, generated by Sensys Wireless Sensors, activate contact closure relays used at intersections.

2.6.6 Operations

The key features of the Contact Closure card are outlined in this section. Throughout the section, references to Contact Closure and Master cards also apply to Expansion cards except as noted.

2.6.6.1 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).[7]

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 fifteen 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 two-channel and four-channel versions. Each channel may be individually enabled/disabled and configured. (*Note*: the cards physically occupy one slot but an optional extender may be used such that the card occupies two slots.)

---

[7] Channels three and four are not available on the 2-channel version of the Contact Closure card.

2.6.6.2 Channel States

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.

2.6.6.3 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.

2.6.6.4 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.
- *None* – channel behavior is not modified.

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

2.6.6.5 Per-Channel and Per-Sensor Holdover

Sensys Contact Closure cards can be configured to use either *per-channel* or *per-Sensor* holdover durations.

2.6.6.5.1 Per-Sensor Holdover

Individual Sensor channel holdover allows an extension to the channel holdover duration when it is activated by the events from a particular Sensor. This features is specified on TrafficDOT's *Dot Configuration* window.

2.6.6.5.2 Per-Channel Holdover

The channel holdover feature is obsolete and should not be used.

2.6.6.6 Channel Summary

The channel states and modes are summarized in the diagram below:

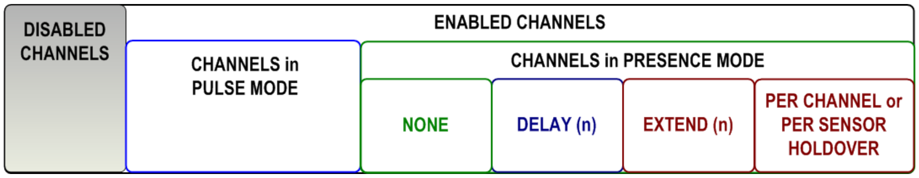


Figure 2.16: Contact Closure Card Channel States, Modes and Modifiers

2.6.6.7 Extra Latency

The design of Sensors results in a trade off between responsiveness to detected events and accuracy of the waveform generated by detections. In applications where waveform fidelity is preferred over responsiveness, a fixed amount of latency can be added by the system by the Access Point. This will generally result in the most accurate count, occupancy and speed calculations. (See the section *Configuring Access Points* in the *Network Management* chapter for more information.)

2.6.6.8 Sensor Allocation

Up to fifteen Sensors can be allocated to a channel. Individual Sensors are assigned to channels via configuring the Access Point. The Sensor-to-channel mappings are stored in a database on the Access Point and are maintained with TrafficDOT's *Dot Configuration* window. Individual Sensors may be allocated to up to four discrete channels. (See the section *Managing Sensor Tables* in the *Network Management* chapter for more information.)

2.6.6.9 Channel Fault Indication

Channels that experience a fault condition are detected and result in an alert indicated by the front panel FAULT LED. Fault conditions may include:

- All Sensors on the channel are inactive
- Some Sensors on the channel are inactive
- Card failure (e.g., a power failure)

Fault indication is dependent on the operating mode of the card (TS1 or TS2). See *Conformance to TS1 and TS2 Specifications* below for more information.

2.6.6.10 Channel Status Monitoring

The status of a single channel may be monitored with the real-time channel status displayed via the LEDs on the card front panel.

2.6.6.10.1 Monitoring Enhancement Via Audible Tone

Channel status monitoring can be enhanced through the optional use of an audible tone generated each time the channel relay is closed. This is particularly useful in field conditions where ambient lighting makes the LEDs difficult to see.

2.6.6.11 Power Source for Access Point

The Contact Closure card provides isolated power to the Access Point from the 12 or 24V input voltage on the traffic controller backplane, eliminating the need for an external power supply. The card draws up to 6 Watts in the case of powering an Ethernet enabled Access Point that is connected to a wide area network.

2.6.7 Components

The Wireless Vehicle Detection System interfaces to standard traffic signal control equipment via the following components:

- *Contact Closure Master card* – one required per Access Point
- *Sensys AccessBox* – one required per Contact Closure Master card
- *Contact Closure Expansion card(s)* – up to 63 cards as needed to accommodate additional channels or Sensors

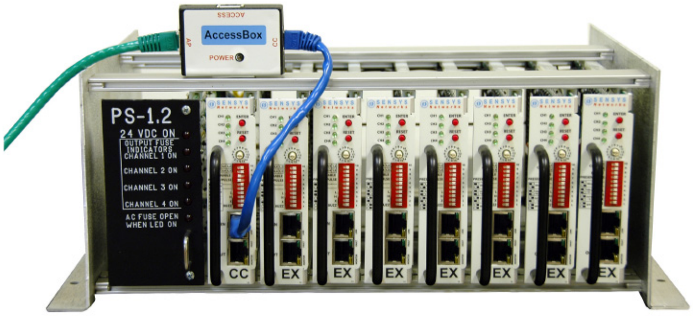


Figure 2.17: Master (CC) card with Extension (EX) cards

The components are assembled as shown in the figure above. (Note: the figure does not show the cables required to daisy chain the Expansion (EX) cards to the Master (CC) card (CC). See also the section *Cabling Summary* for more information).

2.6.7.1 AccessBox

An AccessBox – typically installed inside the controller cabinet - bridges a Sensys Access Point to a Contact Closure Master card and supplies power to the Access Point.. Each Contact Closure Master card is connected to one AccessBox.

2.6.7.2 Contact Closure Master Card

A Contact Closure Master card – installed into a controller shelf slot – forms the head end of a series of hardware interfaces (cards) that conduct vehicle detection information to discrete signal controller channels. A Contact Closure Master card connects to an AccessBox. Additional cards are optionally daisy chained from the Contact Closure Master card if circumstances warrant.

2.6.7.3 Contact Closure Expansion Card

Expansion cards are optional, used only if additional capacity is required. Expansion cards are the same as Master cards except they do not connect to a Sensys AccessBox. They connect only to a Master card or another Expansion card.

2.6.8 Configuration

Contact Closure Master and Expansion cards are configured from either their front-panel interface or with TrafficDOT. (Refer to the document *Sensys Contact Closure Installation Guide* for detailed information regarding configuring the cards.) AccessBoxes are not configurable.

2.6.9 Card Addressing

All CC and EX cards in the same controller cabinet must have a unique address called the *Card ID*. This address is essential to (*i*) associating Sensors to one of the card's channels, and (*ii*) polling the card to report its status in circumstances where the network Access Point is connected to a wide-area network for remote monitoring and management.

2.6.9.1 Address Format

Card ID values are expressed as: `[ shelf number ] – [ slot number ]` with the following conditions:

- *Shelf number* and *slot number* are decimal numbers.
- *Shelf number* and *slot number* are combined using a hyphen to separate the figures[8].

---

[8] Note: use of the hyphen does not indicate subtraction of the numbers.

- *Shelf number* is an integer between zero and three.
- *Slot number* is an integer between zero and 15.

Both *shelf-number* and *slot-number* must be determined to create a *Card ID*. Installers set the Card ID via hardware switches on the side of the card. (See *Circuit-board Switches – SW1 and SW2* below.)

2.6.10 Front Panel Interface

The CC/EX card front panel contains command buttons, LEDs (light emitting diodes) that display channel status information, and other controls used to configure the card. This section describes each element of the front panel interface.

2.6.10.1 Command Buttons

The command buttons ENTER and RESET operate on the card's configuration settings.

ENTER is used to send the configuration (as set via the other front panel controls) to device flash memory.

RESET performs a "soft" reset of the card, clearing any pending events in the card's internal buffers (regardless of channel). In addition, events are ignored while this button is held down.

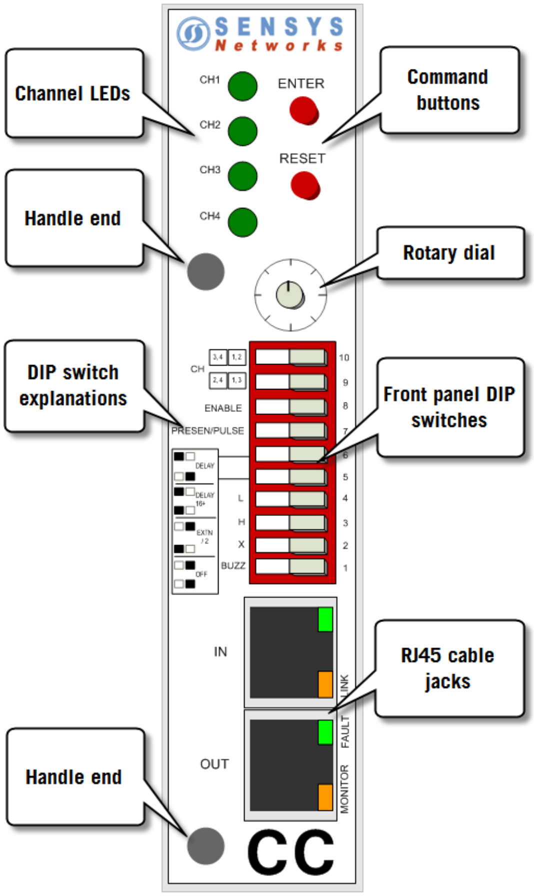


Figure 2.18: Faceplate of CC-170 Master Card (annotated)

2.6.10.2 Channel LEDs

Four green LEDs, labeled CH1 through CH4, correspond to the channels of the card and display in real-time the state of the channel relay.

A lighted LED indicates a closed channel relay (i.e., a call). An unlighted LED indicates an open channel relay. The table below shows the common states for channel LEDs.

Channel LED State	Channel Disposition
Blinking	Vehicle detected
Off (unlit)	No vehicle present or channel disabled
On (lit)	Vehicle present or no Sensors detected for channel

Table 14: Channel LED Display States

2.6.10.3 Rotary Dial

A 16-step rotary dial switch allows for selection of numeric values required by some configuration settings. The dial is used in conjunction with the following:

- Specifying the duration of delay before activating a contact closure
- Specifying the extension to the amount of time a contact closure is held

2.6.10.4 Front Panel DIP Switches

An array of ten DIP switches is used to set channel states, channel modes and mode modifier settings. Each switch is assigned a specific function as indicated in the table below.

DIP switch	Label	Function
10	CH [3,4] [1,2]	Sets channel address bit 1
9	CH [2,4] [1,3]	Set channel address bit 0
8	ENABLE	Enables (disables) the channel
7	PRESEN/PULSE	Sets the channel mode
6	DELAY, DELAY+16, EXTN, OFF	Sets presence mode modifier, bit 1
5	DELAY, DELAY+16, EXTN, OFF	Sets presence mode modifier, bit 0
4	L	Reserved for Sensys Networks
3	H	Reserved for Sensys Networks
2	X	Specifies card address display mode
1	BUZZ	Enables (disables) the audible monitor

Table 15: Functions of the Front Panel DIP Switches

The individual switch settings are described below. (*Note*: In the diagrams, a gray-shaded raised block represents a switch moved to the left or right position.)

2.6.10.5 Switches 9 & 10: Channel Number

Switches 9 and 10 together set the channel number. Channels are numbered one through 4.

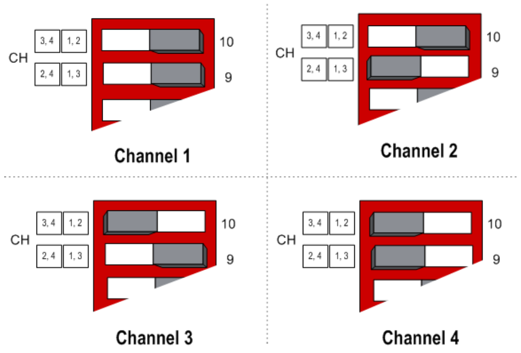


Figure 2.19: Switches 9 & 10 Specify Channel

2.6.10.6 Switch 8 : Channel State

Switch 8 sets the channel status – enabling or disabling the selected channel.

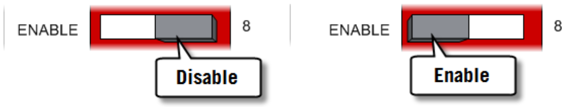


Figure 2.20: Switch 8 Enables / Disables Channel

Enable Channel

Set the switch to the *left* position to enable the channel.

Disable Channel

Set the switch to the *right* position to enable the channel.

2.6.10.7 Switch 7: Channel Mode

Switch 7 sets the channel mode – specifying pulse or presence mode the selected channel.

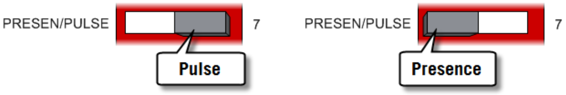


Figure 2.21: Switch 7 Sets Channel Mode

Presence Mode

Set the switch to the *left* position to specify presence mode.

Pulse Mode

Set the switch to the *right* position to specify pulse mode.

2.6.10.8 Switches 5 & 6: Presence Mode Modifier

Switches 5 and 6 together specify an optional modifier to a channel operating in presence mode. These switches also require the use of the rotary dial switch to set the number of seconds associated with each setting. (See also the *Presence Mode Modifier* section above.)

The figure below shows the possible combinations for switches 5 and 6 and how the combinations are interpreted.

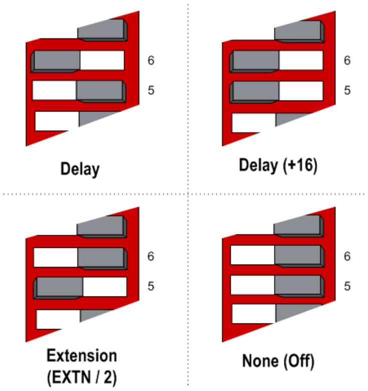


Figure 2.22: Switches 5 & 6 Specify Presence Mode Modifiers

Using the Rotary Switch With Delay, Delay + 16 and Extension

When *Delay*, *Delay+16* or *Extension* are specified, the rotary dial is used to express the amount of time to delay the onset of the contact closure or extend its duration.

Delay is expressed in seconds. Use *Delay* for delay amounts of 0 to 15 seconds. Use *Delay+16* for delay amounts of 16 to 31 seconds. (When *Delay+16* is specified, the value set on the rotary dial is incremented by 16.)

Extension is expressed in half-seconds. When *Extension* is specified, the value set on the rotary dial is divided by 2.

2.6.10.9 Switches 3 & 4

These switches are reserved for Sensys Networks, Inc.

2.6.10.10 Switch 2: Card Address Display Mode

Switch two directs the card to operate in a special mode related to the Card ID set via the circuit-board switches.

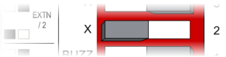
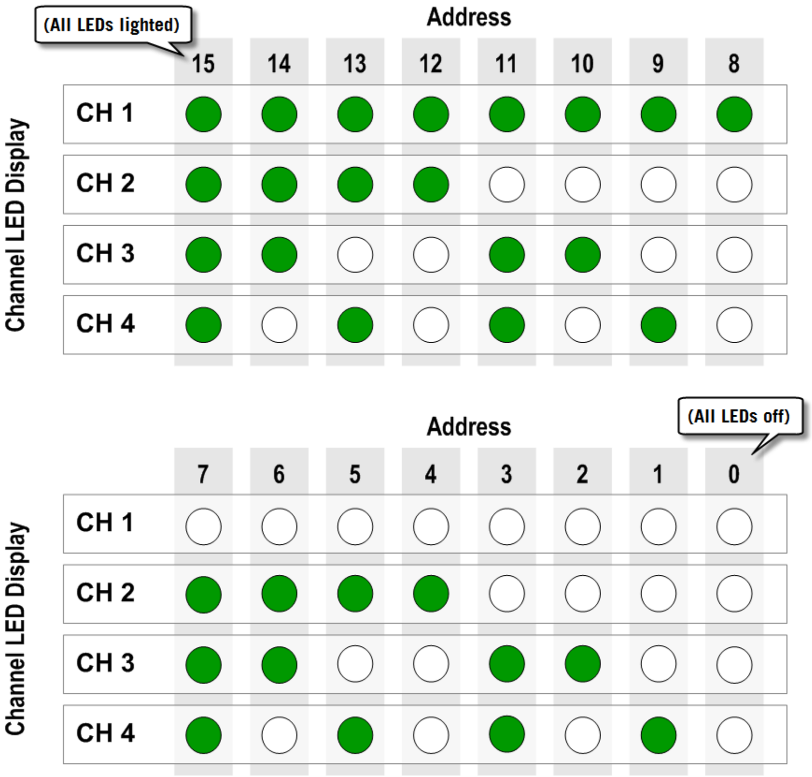


Figure 2.23: Switch 2 Enables X-mode

When enabled, this mode directs the CC/EX card to display the *slot number* component of its Card ID via the four channel LEDs. The possible LED combinations are depicted in the figure below.

This mode is enabled by moving the dip to the *left* position and rebooting the card (via the internal reset button or physically removing the card from the shelf and re-installing it). Vehicle detection events are ignored in card address display mode.



Address	15	14	13	12	11	10	9	8
CH 1	●	●	●	●	●	●	●	●
CH 2	●	●	●	●	○	○	○	○
CH 3	●	●	○	○	●	●	○	○
CH 4	●	○	●	○	●	○	●	○

Address	7	6	5	4	3	2	1	0
CH 1	○	○	○	○	○	○	○	○
CH 2	●	●	●	●	○	○	○	○
CH 3	●	●	○	○	●	●	○	○
CH 4	●	○	●	○	●	○	●	○

Figure 2.24: Channel LED displays of the slot number component of Card ID

2.6.10.10.1 Examples

1. All fours channel LEDs lighted indicates *slot number 15*.
2. Single lighted LED on channel 2 indicates *slot number 4*.

2.6.10.11 Switch 1: Audible Monitor

Switch one enables/disables the audible monitor (buzzer) for the selected channel.

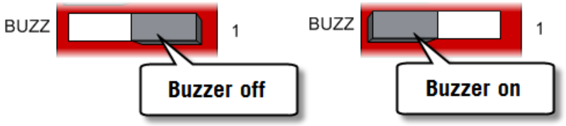


Figure 2.25: Switch 1 Activates Audible Channel Status Monitor

Enabling the audible monitor results in an audible tone each time a contact closure occurs. This helps ensure that the channel is associated with the appropriate Sensors.

In addition, when enabled, the audible tone is emitted when a card reconfiguration is process and ends when the settings have been accepted. This helps field staff determine how long the ENTER button must be held down to send the configuration to device flash memory.

2.6.10.12 RJ 45 Cable Jacks

Two RJ45 jacks – labeled IN and OUT respectively – accommodate cable connections to the card.

2.6.10.13 IN Jack

On a Contact Closure Master card, the IN jack accepts a cable from an AccessBox, which in turn, is connected to the Access Point. On an Expansion card, the IN jack accepts a cable from a Contact Closure Master card or another Expansion card.

The LED labeled LINK indicates the status of the communication link between a Contact Closure card and the Access Point and/or PC host connected via the AccessBox. Status values are shown in the table below.

IN jack LED State	Status of communication link
Blinking (long blinks)	Normal operation. Link is up and Access Point polling is in process
Blinking (short blinks)	Error. Polls are being sent to the card, but not time-codes. This can occur if the Access Point radio is not operational.
Solid on (lit)	Error. Contact Sensys Networks.
Off (unlit)	Error. Access Point to Card communication link is down.

Table 16: Front panel IN jack LED states

2.6.10.14 OUT Jack

The OUT jack is used to connect to an Expansion card. Two LEDS are associated with it.

2.6.10.14.1 FAULT LED

The LED labeled FAULT lights for ½ second when the card is first installed, thereafter, the FAULT LED lights if any enabled channel has a fault condition.

2.6.10.14.2 MONITOR LED

The LED labeled MONITOR reflects the real-time state of the currently selected channel. The LED lights when a contact closure occurs. (Note: visual monitoring of the channel can be augmented by enabling the audible tone. See *Switch 1: Audible Monitor* above.)

2.6.11 Circuit-board Controls

CC/EX cards have important controls mounted on the circuit board that are used in configuration and setup. They are described in this section.

2.6.11.1 Master Reset

A master reset button reinitializes the host processor. Pressing this button is equivalent to removing the card from the controller shelf and re-installing it.

2.6.11.2 Circuit-board Switches – SW1 and SW2

Two DIP switch banks – labeled SW1 and SW2, respectively – are mounted onto the circuit-board of the card. They resemble the switch shown in the figure below.

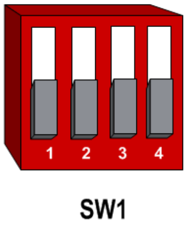


Figure 2.26: Switch bank SW1

SW1

Circuit-board switch SW1 is used for for two purposes: (*i*) setting the *shelf number* component of the card's address and (*ii*) specifying the type of traffic control equipment.

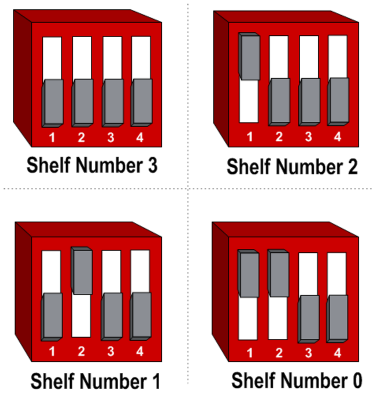
The functions assigned to the switches are shown in the following table.

Switch #	Function	Up represents...	Down represents...
1	CardID, address bit 4	0	1
2	CardID, address bit 5	0	1
3	Selection of TS1 or TS2	TS2	TS1
4	Reserved for Sensys Networks	n/a	n/a

Table 17: SW1 Functions

2.6.11.2.1 Shelf Number

The figure below depicts how switches one and two of SW1 are set for the *shelf number* component of the Card ID. These switches are set by the installer. (Refer to the document *Sensys Contact Closure Installation Guide* for more information.)

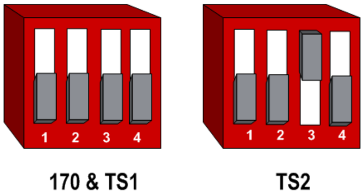


Shelf Number 3
Shelf Number 2
Shelf Number 1
Shelf Number 0

Figure 2.27: SW1 Settings for Shelf-Number

2.6.11.2.2 TS1 / TS2 Selection

The figure below depicts how switch three of SW1 is set for selecting the type of traffic controller. This switch is set by the installer. (Refer to the document *Sensys Contact Closure Installation Guide* for more information.)



170 & TS1
TS2

Figure 2.28: SW1 Settings for Controller Type

SW2

Circuit-board switch SW2 is used exclusively for setting the *slot number* component of the Card ID. All four switches are used as indicated in the following table:

DIP #	Function	Up represents...	Down represents...
1	CardID, address bit 0	0	1
2	CardID, address bit 1	0	1
3	CardID, address bit 2	0	1
4	CardID, address bit 3	0	1

Table 18: SW2 Functions

The figure below depicts how the SW2 switches are set for slot numbers. These switches are set by the installer. (Refer to the document *Sensys Contact Closure Installation Guide* for more information.)

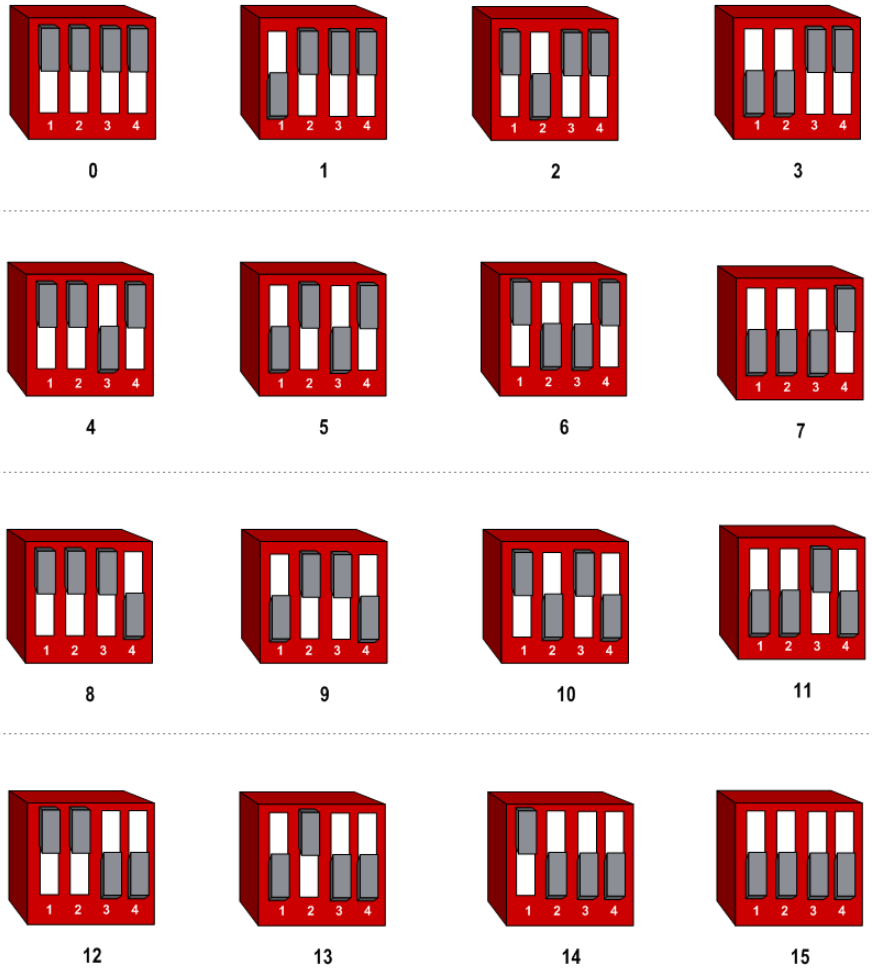


Figure 2.29: SW2 Switch Settings for Slot Number (Slot number values appear below each switch)

2.6.12 Conformance to TS1 and TS2 Specifications

As noted above, CC/EX cards are configured via circuit-board switch SW1 (switch 3) to conform to either the TS1 or TS2 Specification. This section provides additional information.

2.6.12.1 Status Relay

In TS2 mode, each channel uses a separate relay to indicate channel status as shown in the following table.

Condition	Status Relay	TS2 State
All Sensors on the channel are active	Closed	1-Normal
All Sensors on the channel are inactive	Open	2-Failure
Some Sensors on the channel are active	150 millisecond pulse	5-Excess Inductance Charge

Table 19: TS2 Status Reporting

Sensor activity is determined by the existence of packets received from the Sensors assigned to a channel. If no packets are received for 60 seconds, a Sensor is considered inactive. (For proper operation Sensys Networks recommends a *watchdog timeout* value of 30 seconds.) When operated in TS1 mode, channel status relays are reported as “open”.

2.6.12.2 Channel Fault

Contact Closure cards indicate a channel fault by permanently closing their contacts. To be TS2 compliant, faults generated by a complete card failure (for example, no power to the card) are indicated in the same way.

2.6.13 Interfaces

Contact Closure cards support external connections made via the IN RJ45 connector and the OUT RJ 45 connector. (See *Appendix 3* for more information.)

2.6.14 Sensys AccessBox

An AccessBox – a small, three-port junction device - is mounted inside the controller enclosure to provide the following services:

- connect an Access Point to a Contact Closure Master card
- routes 48VDC power from the controller to the Access Point
- provide a field service/management port

An AccessBox is required for each Contact Closure Master card.

2.6.14.1 Ports

Each Sensys AccessBox port accepts an male RJ45 connector and is dedicated to a specific use.

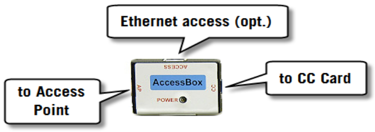


Figure 2.30: AccessBox Ports

2.6.14.1.1 Sensys Access Point Port (AP)

The *Sensys Access Point Port* (labeled “AP”) accepts a cable connecting an AccessBox to a Access Point. Use a regular CAT5 or better 4-pair cable, terminated with a male RJ45 connector using the EIA 568-B standard for *straight-through* Ethernet cables. Observe the industry standard Ethernet cable length limitations for 10BaseT transmissions.

The CAT5 cable carries three signals:

- *Power* – 48VDC nominal carried on one pair
- *Control* – half-duplex control bus (RS-485) carried on one pair
- *Access* – Ethernet connectivity through the ACCESS port carried on two pairs

2.6.14.1.2 Sensys Contact Closure Port (CC)

The *Sensys Contact Closure Port* (labeled "CC") accepts a cable connecting an AccessBox to a Contact Closure Master card. Use a regular CAT5 or better 4-pair cable, terminated with a male RJ45 connector using the EIA 568-B standard for *straight-through* Ethernet cables. Observe industry standard Ethernet cable length limitations for 10BaseT transmissions.

2.6.14.1.3 Wired Network Access Port (ACCESS)

The *Wired Network Access Port* (labeled "ACCESS") provides wired Ethernet connectivity to an Access Point. Such connectivity is used to configure the devices and/or connect the installation to a larger network for management, monitoring and reporting.

2.6.14.2 Connecting a PC or Laptop to the ACCESS Port

Use a *straight-through* Ethernet cable to connect an AccessBox directly to a PC or laptop.

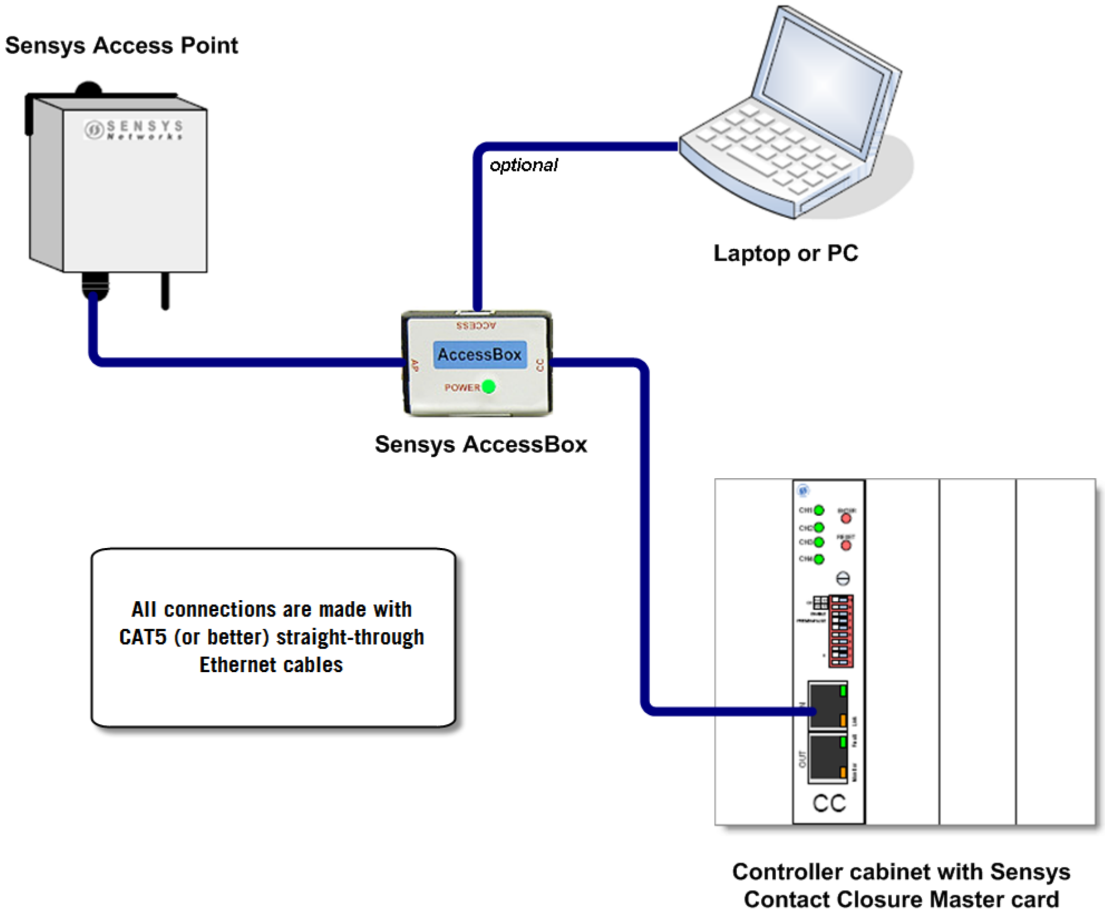
2.6.14.3 Connecting a Hub, Switch, Router or Other Device to the ACCESS Port

Use a *crossover* Ethernet cable to connect an AccessBox to a network hub, switch, router , modem or other non-PC device.

2.6.15 Cabling Summary

The cabling to connect a Sensys AccessBox, Sensys Access Point and Sensys Contact Closure Master card is shown in the figures below.

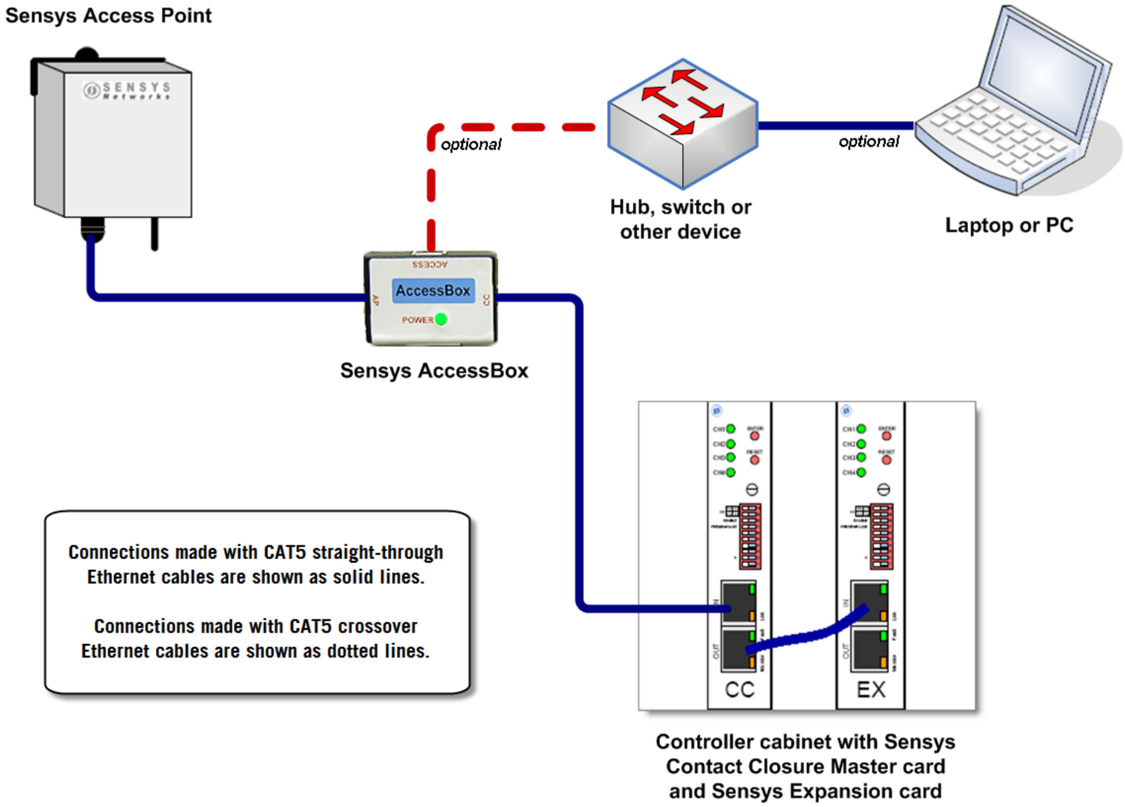
2.6.15.1 Cabling for Access Point, Contact Closure Master card and Optional Management Link to PC



All connections are made with CAT5 (or better) straight-through Ethernet cables

Figure 2.31: Cabling Diagram for Access Point, Contact Closure Master card and Optional Management Link to PC

2.6.15.2 Cabling Diagram for Access Point, CC Master and Expansion cards, and Optional Management Link via Hub, Router, or Other Device


Sensys Access Point
SENSYS Networks
optional
Hub, switch or other device
optional
Laptop or PC
ACCESS
AccessBox
AP
CC
POWER
Sensys AccessBox
CC
EX
Controller cabinet with Sensys Contact Closure Master card and Sensys Expansion card

Connections made with CAT5 straight-through Ethernet cables are shown as solid lines.

Connections made with CAT5 crossover Ethernet cables are shown as dotted lines.

Figure 2.32: Cabling Diagram for Access Point, CC Master and Expansion cards, and Optional Management Link via Hub, Router, etc.

2.7 TrafficDOT

TrafficDOT, a Java software application developed by Sensys Networks, is a configuration manager and monitoring tool for an Access Point and all of its associated devices (Sensors, Repeaters and Contact Closure cards).

2.7.1 Typical Use

TrafficDOT provides a graphical user interface (GUI) to the network's devices, settings and operations. The GUI simplifies configuration and management of Sensys installations.

2.7.2 Operations

TrafficDOT is Java-based. It runs on any computing platform that supports the Java run-time environment. With TrafficDOT, you can:

- Connect to an Access Point
- Form a Sensys network by associating devices (Sensors, Repeaters, Contact Closure cards) to an Access Point
- Configure settings for events, detection thresholds, reporting, etc.
- Maintain information about Sensor location
- Download firmware updates to all devices
- Backup/restore the configuration of an Access Point
- Produce online graphs of detection experience
- Perform special support commands[9]

See the *Network Management* chapter for more information.

Note: TrafficDOT can be used to manage Sensys networks over any link that supports IP communications. To manage a Sensys installation over a public network such as the Internet, the host PC must be able to access that network.

TrafficDOT is independent of the firmware resident in Sensys 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.

---

[9] As directed by Sensys Networks Technical Support staff.

2.8 Software Applications

Sensys Networks has developed a suite of software applications that provide a range of services related to event processing, data transfer and reporting. The applications are as follows:

2.8.1 APDIAG

APDIAG measures the health of a Sensys Networks installation. It computes uptime, average radio signal strength (RSSI), total counts by Sensor, as well as the average speed and deviation from the average speed (if three Sensors are present in lane) for each lane. Sensys Networks recommends running APDIAG on an automatic basis once per day.

2.8.2 APPOLLSTAT

APPOLLSTAT allows a Sensys Wireless Vehicle Detection network to emulate a Type 170 signal controller when communicating with a front-end traffic processor expecting California DOT (CalTrans) SDRMS formatted packets.

2.8.3 APPOLLSTAT_CALTRANSD4

APPOLLSTAT_CALTRANSD4 allows a Sensys Wireless Vehicle Detection network to operate with traffic controllers operated in California DOT District 4.

2.8.4 APPOLLSTAT_TCP

APPOLLSTAT_TCP allows a Sensys Wireless Vehicle Detection network to supply data to any external TCP client based on poll requests made on a predetermined IP port. The output takes the form of the default Sensys Networks aggregated data format.

2.8.5 APPUSHSTAT

APPUSHSTAT provides a means to intelligently transfer processed Sensor data from the statistics host (normally an Access Point) to another host. Built in buffering and data-aware recovery make it a better choice for file transfer than simple IP tools.

2.8.6 APSTAT

APSTAT processes events into *per-lane* or *per-vehicle* statistics. Statistics include per-lane counts, occupancy, average and median speeds, as well as binned speeds and vehicle lengths over a range of time intervals. In addition, an output of one line per vehicle containing vehicle start time, gap, speed and length can be produced. APSTAT runs on real-time or archived data. Output can be transferred to another host (the *push* model) or stored locally for later retrieval (the *poll* model).

2.8.7 APSTATRECV

APSTATRECV implements a TCP server to accept data transfers from one or more instances of APPUSHSTAT. Normally this process runs on an external host that is a consumer of event data from a given Sensys network.

2.8.8 EVENTPROXY

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

2.8.9 Sensys Management Servers

Sensys Networks provides two management servers – *SNAPS Professional* and *Sensys Systems Manager*. Both products provide comprehensive remote management capabilities, event data archiving, and statistical reporting functions. Offloading these functions to a remote host redices the performance overhead on Access Points and is often essential to meeting security and administrative requirements found in large, multiple network installations.

SNAPS Professional is a software-only solution; *Sensys System Manager* is a hardware/software bundle that require less customer involvement to deploy.

2.8.10 SNCPROXY

SNCPROXY provides proxy services for an Access Point and is used to control administrative access and archiving of detection data.

2.9 APDIAG

APDIAG measures the health a Sensys Networks installation. It reports diagnostic statistics describing SNP protocol connection integrity, Sensor detection differences, global reboots and unknown Sensors.

The APDIAG process executes on a Sensys Management Server and, beginning with VDS release 1.8.0, on the Access Point itself. Operations of the instance located on the Access Point are limited to ensure adequate resources for detection event processing by the Access Point. Results are output to a summary file formatted with tab-delimited fields.

2.9.1 Typical Use

APDIAG is a diagnostic tool used to (*i*) evaluate overall network effectiveness and (*ii*) identify unknown Sensors. It is typically run against a full day's worth of log data produced by SNCPROXY.

Beginning with VDS release 1.8.0, the instance of APDIAG executing on the Access Point maintains a rolling seven-days of diagnostic data. History is automatically maintained by the process to ensure that the memory allocated to the data cannot exceed a fixed amount.

2.9.2 Operations

APDIAG reads operational log data from a specified Access Point and produces a tab-delimited output file storing diagnostic statistics.

2.9.2.1 Output Data

The output data consists of the elements described below. Elements that are *counts* are expressed as integers; elements that are *statistics* include the values in the table below unless *condensed output* is specified. (See the *Parameters* section below for more detail.)

Measures Computed for All Statistical Elements
Average
Median
Standard Deviation
95th percentile
90th percentile
80th percentile

Table 20: Measures computed for all statistical output elements

2.9.2.2 Output Data Elements

Count

The number of detection events received from a Sensor for the duration of the input data.

If the input argument *snpFile* (generated by SNCPROXY) is used, the period will be 24 hours. Otherwise, if archive data is used as input, the period is the time from *archiveStart* to *archiveEnd*.

Reboots

The number of times a Sensor has not been heard from for a period exceeding the timeout period by approximately 1.5 times.

For example, because Sensors send a heartbeat message every *watchdog interval* (typically 30 seconds), it is possible to infer when a Sensor is not communicating with an Access Point. In this example, this value shows the number of disjoint instances in which the time between consecutive messages from a Sensor exceeds 45 seconds.

If a global reboot is detected, that instance is not added to the tally. A global reboot is defined to be a period of downtime that overlaps with *all* Sensors' downtime on the Access Point. (A global reboot is an indication of an Access Point reboot or some other Access Point outage).

Downtime

The total time (in seconds) a Sensor has not been heard from.

For example, because Sensors send a heartbeat message every *watchdog interval* (the default value is 30 seconds), it is possible to infer when a Sensor is not communicating with an Access Point. In this example, this value shows the accumulation of all time in which a Sensor is not heard from for more than 45 seconds.

For example, assume a Sensor sends a message at time 0 (zero) seconds, 78 seconds, and 133 seconds. The value of downtime would be 211.

stuckHi

The total number of disjoint instances where a Sensor is held in the present state for more than 60 seconds. This is an indication that the magnetic environment has changed and the Sensor requires a recalibration. By default, recalibration is done automatically.

blips

The total number of zero width pulses reported by the Sensor. This is usually an indication of a noisy magnetic environment.

RSSI (statistic)

Received Signal Strength Indicator; signal strength between two communicating devices. See the section on *Received Signal Strength Indicator (RSSI)* for more information.

LQI (statistic)

Line Quality Indicator; transmission quality between two communicating devices. See the section on *Line Quality Indicator (LQI)* for more information.

Latency (statistic)

The number of seconds between the event detection time and the time the message was received by the Access Point.

Speed (statistic)

The calculated speed from a Sensor pair. (*Note*: this measure is only reported for Sensors that are configured as "trailing" Sensors in a Sensor pair. Otherwise, it is not reported.)

Speed difference (statistic)

The difference between the speed calculated for a given Sensor and the average speed calculated from all Sensor pairs in this lane for the same vehicle. (*Note*: this measure is only reported for Sensors that are configured as "trailing" Sensors in a Sensor pair.)

2.9.2.3 Condensed Output Data

When the input argument *condensed* is used, the output data elements are limited to the following:

Count
Reboots
Downtime
RSSI (average)
RSSI (standard deviation)
Latency (average)
Latency (Median)
Speed (average)
Speed (median)
Speed difference (average)
Speed difference (95 percentile)

2.9.3 Hosts

APDIAG can be run on a centralized event server (such as a Sensys management server), however, beginning with VDS release 1.8.0, an instance of APDIAG also executes on the Access Point.

2.9.4 Command-line Syntax

The arguments recognized by the application are shown below. Required arguments are shown in bold.

See also the discussion under the section *Configuring and Managing System Parameters* in the *Network Management* chapter that pertains to the configuration parameters available for the instance of APDIAG that executes on the Access Point.

```
apdiag snpFile = <filename>
       dotFn = <dotFN database file>
       dptpairFn = <dotpairFn database file>
       [host = hostname or IP address]
       [udp = <0|1>]
       [port = <SNCProxy port #>]
       [tablehost = <SNCProxy table IP Address>]
       [tableport = <SNCProxy table port>]
       [report_int = <time in secs>]
       [GMTOffset = <hour difference from GMT> (pos or neg)]
       [delayproc = <1-30 secs>]
       [watchdog = <timeout in seconds>]
       [showRebootdetail = <0|1>]
       [uphold = <time in 1/1024 secs>]
       [downhold = <time in 1/1024 secs>]
       [adaptive_downhold = <distance in feet>]
       [stuckTime = <time in 1/1024 secs>]
       [encdb = <encrypt key database filename>]
       [condensed = <0|1>]
       [summary = <filename>]
```

2.9.5 Parameters

2.9.5.1 Input Source Specification

APDIAG requires an input data source argument. Either the filename of an *snpFile* or a host IP address for a direct connection to an Access Point.

2.9.5.1.1 snpFile

Specifies by name a log file generated by SNCPROXY typically storing 24 hours worth of data.

2.9.5.2 dotFn

Specifies by name a “dot table” file in APTABLE format that identifies the Sensors used in a given network.[10]

---

[10] APTABLE format is a proprietary data representation of Sensys Networks, Inc. Consult Sensys Networks before using this parameter.

2.9.5.3 dotpairFn

Specifies by name a “dot pair table” in APTABLE format that identifies the Sensor pairings used in a given network.

2.9.5.4 host

Hostname or IP address of an Access Point. Use this element to replace the elements *snpFile*, *dotFn*, *dotpairFn* when connecting directly to an Access Point.

2.9.5.5 udp

Set to 1 (one) when when using a SNC server UDP connection.

2.9.5.6 port

The port specified for a SNC server process.

2.9.5.7 tableHost

IP address of the host storing the dot table; when connecting to a SNC server, this parameter is necessary.

2.9.5.8 tablePort

Port number on the host storing the dot table; when connecting to a SNC server, this parameter is necessary.

2.9.5.9 report_int

The number of seconds in a reporting interval; TrafficDOT supports values of 10, 15, 30, 60, 300, 600, 900. *Default* = zero, where zero indicates no reporting interval. Thus, the report is produced only when at the end of an input file. (*Note*: intended for advanced users only.)

2.9.5.10 GMTOffset

This parameter allows for timezone modification of the output timestamps. If this value is not entered, timestamps in the reports will be GMT. *Default* = zero

2.9.5.11 delayproc

The number of seconds APDIAG waits before processing event data to generate speeds/lengths. Must be between 1 and 30.

2.9.5.12 watchdog

Specifies the watchdog timeout value in seconds.

2.9.5.13 showRebootdetail

Specifies whether or not detailed statistics regarding Sensor reboots are included.

2.9.5.14 uphold

Specifies the minimum amount of time a detection signal must last before it is considered a detection event. Given in 1/1024 seconds.

2.9.5.15 downhold

Specifies the minimum amount of time an undetect signal must last before it is considered an undetect event. Given in 1/1024 seconds.

2.9.5.16 adaptive_downhold

Specifies the minimum amount of distance an undetect signal must last before it is considered an undetect event. Given in feet.

2.9.5.17 stuckTime

Specifies an amount of time during which a Sensor does not report before the Sensor is considered “stuck high”.

2.9.5.18 encdb

Specifies the name of an encryption key database file.

2.9.5.19 condensed

Enables output reporting using a limited set of elements.

0 = disable condensed output reporting (*default*)
1 = enable condensed output reporting

2.9.5.20 summary

Name of the file storing the output data.

2.10 APPOLLSTAT

APPOLLSTAT is used with a Sensys Wireless Vehicle Detection Network to emulate the behavior of a Type 170 signal controller. This allows a Sensys network to directly interface with front-end traffic processors that expect SDRMS formatted communications.

2.10.1 Typical Use

In circumstances where a Sensys network is used in conjunction with a traffic signal controller operated by CalTrans District 3, APPOLLSTAT responds to requests (polls) from a centralized traffic management system and replies with recent event data formatted according to the SDRMS communications specification.

2.10.2 Operations

APPOLLSTAT executes in conjunction with an instance of APSTAT configured for aggregate reporting. It listens on a predetermined port for requests and replies by forming an SDRMS normal packet from the most recent event report written to the archive by APSTAT. A single line is read from the *workingFile* and parsed to form the response.

If the most recent event report has already been transferred by APPOLLSTAT (in a prior transfer), the process waits for the next event to be written before responding. In other words, poll requests may be queued as opposed to replied-to immediately.

2.10.2.1 Notes

1. APSTAT must be configured with *speedAvg* = 1, *diagOpt* = 1 and *no histograms* to enable APPOLLSTAT to correctly parse the detection event reports.
2. Only lanes numbered from one through 12 will be recognized by APPOLLSTAT.

2.10.3 Hosts

APPOLLSTAT must run on the same host as the APSTAT instance that generates the event reports to be transferred.

2.10.4 Command-line Syntax

The arguments recognized by the application are shown below. Required arguments are shown in bold.

```
appollstat listen = <port>
           position = <filename>
           [logDir = <file system location>]
           [dropNumber = <dropNumber>]
```

2.10.5 Parameters

2.10.5.1 listen

(*Required*) The port number on which server requests (polls) are made.

2.10.5.2 position

(*Required*) Names the file that stores the current position of APPOLLSTAT as it transmits an archive file. This is used during recovery of an interrupted transmission. The process retransmits from the position stored in the file once the connection is restored.

2.10.5.3 logDir

Names the parent directory storing the data to be transferred to the polling client. *Default* = `/var/apstat`

2.10.5.4 dropNumber

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

2.10.6 Related Applications

APPOLLSTAT_CALTRANSD4
APPOLLSTAT_TCP
APSTAT
SNCPROXY

2.11 APPOLLSTAT_CALTRANSD4

APPOLLSTAT_CALTRANSD4 is used with a Sensys Wireless Vehicle Detection Network to communicate with CalTrans District 4 traffic controllers.

2.11.1 Typical Use

APPOLLSTAT_CALTRANSD4 responds to requests (polls) from District 4 controllers and replies with recent event data formatted according to TOS v2.1 specifications.

2.11.2 Operations

APPOLLSTAT_CALTRANSD4 operates in conjunction with an instance of APSTAT configured customized output. It may not be used with any other application, and APSTAT must be configured specially for D4 use.

Adhering to the TOS v2.1 communications specification, it listens on a predetermined port for requests made by PCDC controllers. The response is formed from the most recent report written to archive by APSTAT.

District controllers post a Detector Data Request that is identified by an *address* value. The address must match the value specified in the configuration element *Address* (see below.) Detector Data Reply transmissions are created by APPOLLSTAT_CALTRANSD4 by reading a single line from the file `<logDir>/working/workingFile`. The replies are filtered so as to include only data for Sensors that reside in predefined configurations. The element *Configuration* (see below) specifies the mainline lanes and ramp lanes for which data will be reported. Replies are always sent to the client that makes the request.

2.11.2.1 Notes

1. APSTAT must be configured with *custom-output* = 1, *report_int* = 30 to enable APPOLLSTAT_CALTRANSD4 to correctly parse the detection event reports.
2. Only the lanes/ramps defined through the configuration property will be reported.

2.11.3 Command-line Syntax

The arguments recognized by the application are shown below. Required arguments are shown in bold.

```
appollstat_caltransD4
            listen = <port>
            position = <filename>
            [logDir = <file system location>]
            [configuration = < 71 | 72 | 74 | 78 >]
            [address = <controller address> (1-255)]
```

2.11.4 Parameters

2.11.4.1 listen

(*Required*) The port number on which server requests (polls) are made.

2.11.4.2 position

(*Required*) Names the file that stores the current position of APPOLLSTAT_CALTRANSD4 as it transmits an archive file. This is used during recovery of an interrupted transmission. The process retransmits from the position stored in the file once the connection is restored.

2.11.4.3 logDir

Names the parent directory storing the data to be transferred to the polling client. *Default* = `/var/apstat`

2.11.4.4 configuration

(*Default = 78*) Defines the size and contents of the Detector Data Reply communications as specified in TOS v2.1. For example, configuration 71 supports 8 mainline detectors with no ramp detectors.

2.11.4.5 address

(Default = 1) Specifies an identifying tag used to validate each Detector Data Request received by a given Access Point. Only requests with an address value that match the value stored in this property result in a response. Address values may range from 1 to 255.

2.11.5 Related Applications

APPOLLSTAT
APPOLLSTAT_TCP
APSTAT
SNCPROXY

2.12 APPOLLSTAT_TCP

APPOLLSTAT_TCP allows a Sensys Wireless Vehicle Detection System to interface with any polling client supporting TCP communications that is a consumer of event data reports.

2.12.1 Typical Use

APPOLLSTAT_TCP is a generalized form of a poll/response server for transferring event data based on external request. The data transferred to the requester is formatted as *aggregated output*, the default format of the APSTAT utility.

2.12.2 Operations

APPOLLSTAT_TCP executes in conjunction with an instance of APSTAT configured for aggregate reporting. It listens on a predetermined port for requests and replies by accepting a TCP connection, sending a response and optionally closing the connection. A parameter designates whether the connection is kept open or closed after each response.

The response is formed by reading the most recent event report written to an APSTAT archive and transferring it to the polling client unchanged.

If the most recent event report has already been sent (as part of a prior response), the process waits until a new event report is written to the monitored archive file. Thus, polls may be queued and not replied to immediately.

2.12.3 Hosts

APPOLLSTAT_TCP must run on the same host as the APSTAT instance that generates the events reports to be transferred.

2.12.4 Command-line Syntax

The arguments recognized by the application are shown below. Required arguments are shown in bold.

```
appollstat_tcp listen = <port>
               position = <filename>
               [logDir = <file system location>]
               [connect_opt = < 0 | 1 | 2 >]
```

2.12.5 Parameters

2.12.5.1 listen

(*Required*) The port number on which server requests (polls) are made.

2.12.5.2 position

(*Required*) Names the file that stores the current position of APPOLLSTAT_TCP as it transmits an archive file. This is used during recovery of an interrupted transmission. The process retransmits from the stored position in the file once the connection is restored.

2.12.5.3 logDir

Names the parent directory storing the data to be transferred to the target server. *Default* = `/var/apstat`

2.12.5.4 connect_opt

Designates the handling of the TCP connection following a response.

0 = Keep connection open after accepting a new connection. New reports are sent to the client upon generation.

1 = Treat connection as a poll. Upon receiving a connection,the latest report is delivered to the client and the connection is closed. However, if a subsequent poll arrives sooner than the reporting interval, the connection is kept open until the next report is ready, the report is sent and then the connection is closed. Duplicate reports are never sent.

2 = (*Default*) Treat connection as a sample. Upon receiving a connection, the latest report is delivered to the client and the connection is closed. If a subsequent poll arrives sooner than the reporting interval, the connection is kept open and the latest report is delivered to the client. Because there is *no* checking for duplicate reporting, the requesting client many receive the same report as was previously delivered.

2.12.6 Related Applications

APPOLLSTAT
APSTAT
SNCPROXY

2.13 APPUSHSTAT

APPUSHSTAT moves Sensor data to an external server via TCP.

2.13.1 Typical Use

APPUSHSTAT transfers data produced by other Sensys Networks applications to 3rd party servers for further display and analysis. It is used in conjunction with APSTAT and must execute on the same host.

For installations with multiple instances of APSTAT / APPUSHSTAT, communications on the target host (the host receiving the pushed data) can optionally be managed by executing APSTATRECV.

2.13.2 Operations

APPUSHSTAT reads archive files produced by APSTAT and transfers them to a defined target server when changes are detected in the files. This results is a buffered transmission of the archived data to the target applications.

APPUSHSTAT reads a single line from its input file and sends the line unchanged to the target. The TCP connection can be configured to be dropped or preserved between each data transmission.

Messages are sent from the host receiving data from APPUSHSTAT that acknowledge successful transmissions; these can be suppressed via a configuration option.

Additionally, APPUSHSTAT can be configured to use a data buffering model that specifies the amount of data retransmitted when a connection is lost and restored. If so configured, APPUSHSTAT remembers the position of its most recent transmission and transmits the stored line of data when the connection is recovered.

APPUSHSTAT monitors the contents of the file structure storing the archive files and initiates transmission when (*i*) a change in the current archive file is detected, or (*ii*) the current archive file is moved to a different location.

2.13.3 Hosts

APPUSHSTAT must execute on the host that runs the APSTAT instance that compiles the statistics data it pushes.

Note: this application must execute on the host that executes one or more instances of APSTAT, the process that generates the output moved by this application.

2.13.4 Command-line Syntax

The arguments used by the application are shown below. Required arguments are shown in bold.

```
appushstat host = <host>
           port = <port>
           position = <filename>
           [logDir = <file system location>]
           [connect_opt = <0 | 1>]
           [ackMode = <0 | 1>]
           [noBuf = <0 | 1>]
```

2.13.5 Parameters

2.13.5.1 host

(*Required*) The host name of the target server.

2.13.5.2 port

(*Required*) The port number on the target server.

2.13.5.3 position

(*Required*) Names the file that stores the current position of APPUSHSTAT as it transmits an archive file. This is used during recovery of an interrupted transmission. The process retransmits from the stored position in the file once the connection is restored.

2.13.5.4 logDir

Names the parent directory storing the data to be transferred to the target server. *Default* = `/var/apstat`

2.13.5.5 connect_opt

Directs the application to preserve (or drop) the TCP socket connection in the idle time between discrete data transmissions.

- `0 (zero) –` (*Default*) keep the socket open between messages.
- `1 (one) –` disconnect the socket during idling and reconnect it as necessary.

2.13.5.6 ackMode

Directs the application to expect messages from the target host that acknowledge receipt of data transmissions.

- A value of "`0`" (zero) disables the function.
- A value of "`1`" (one) enables the function such that, prior to transmission, each line from the archive file is prefixed with a sequence number that ranges from 0 (zero) to 999 as shown below:

  ```
  [sequence number],[data line from archive file]
  ```

  Upon receipt, the target host responds with an acknowledgment of the following form:

  ```
  ACK,[sequence number],[new line11]
  ```

If APPUSHSTAT does not receive the acknowledgment within five seconds, the transmission is assumed failed and the line is resent.

2.13.5.7 noBuf

Designates the behavior of the application regarding handling disconnections between the Access Point and the target host.

- A value of "`0`" (zero) directs the application, on encountering a disconnection, to send all data since the time of the disconnection once the connection is restored. If the duration of the disconnection is such that more data is queued than can be stored, then all of the data in the queue is sent, and some data may be lost. (The queue size is a parameter of the application APSTAT.)
- A value of "`1`" (one) directs the application, on encountering a disconnection, to drop data since the time of the disconnection and transmit only the last line in the buffer once the connection is restored.

2.13.6 Data Transmission Model

As each report is generated, APPUSHSTAT seeks a connection on a designated TCP socket on the target server. If the connection succeeds (or if it is already open), the report is sent along with any prior reports that have been buffered. If so configured, the target server acknowledges receipt of each report.

On receiving an acknowledgment, APPUSHSTAT sends the next report. If five seconds pass between sending a report and receiving its acknowledgment, the transmission is considered failed and APPUSHSTAT resends the data with its original sequence number. Therefore, it is possible that the server will receive duplicate transmissions; it is assumed that server-side processing will accommodate this.

---

[11] This is interpreted as an LF (line feed) character.

By default, the TCP connection between APPUSHSTAT and the target server is maintained. Connection drops are detected and an attempt to reconnect is made when the next report is generated.

A partial log of the dialog between an APPUSHSTAT instance and a target server is shown below with annotations. (*Note*: connection set-up details are not shown.)

Origin	Data
APPUSHSTAT	`1,2006-06-01 13:26:00,1234567890123456,1,1.46,3,71.0,0,2,2.80,5,72.0,0`
Target Server	`ACK, 1`
APPUSHSTAT	`2,2006-06-01 13:26:30,1234567890123456,1,5.03,4,71.0,0,2,2.60,4,67.0,0`
Target Server	`ACK, 2`
APPUSHSTAT	`3,2006-06-01 13:26:30,1234567890123456,1,5.03,4,71.0,0,2,2.60,4,67.0,0`
Target Server	`ACK, 3`
APPUSHSTAT	`4,2006-06-01 13:27:00,1234567890123456,1,1.41,4,76.0,0,2,3.23,5,72.0,0`
Target Server	`ACK, 4`
….	`....`

Table 21: Sample Dialog between APPUSHSTAT and Target Server

2.13.7 Related Applications

APPOLLSTAT
APPOLLSTAT_TCP
APSTAT
SNCPROXY

2.14 APSTAT

APSTAT generates statistics from raw detection event data. Data is stored in comma delimited flat files suitable for further processing by other applications. APSTAT can execute on an Access Point or other platform that supports the Linux operating environment.

2.14.1 Typical Use

APSTAT typically executes on an Access Point to generate per-lane or per-vehicle data aggregates subsequently used for detailed analysis of traffic patterns or graphical displays of traffic volume, occupancy and speed.

A separate application from Sensys Networks – APPUSHSTAT – facilitates transferring the aggregated data to other platforms; it executes in conjunction with APSTAT.

Note: Certain constraints apply to installations where APSTAT is used to prepare output in Marksman format. See the sections on APPUSHSTAT and APSTATRECV for more information.

2.14.2 Operations

APSTAT operates in one of two modes, *aggregate report mode* or *real-time report mode*. In addition, output from APSTAT can be configured via settings for statistics interval, automatic archive interval, as well as speed and vehicle length histograms.

2.14.2.1 Aggregate Report mode

Aggregate report mode – also known as *per-lane* mode – is the default reporting mode of APSTAT. In this mode statistics for vehicle counts, occupancy and speed data for each lane in an installation are calculated. The default output format is a PeMS compatible format.

2.14.2.2 Real-time Report mode

In this mode – also known as *per-vehicle* mode – statistics are not calculated at specified intervals. Instead, each detected vehicle generates a report with a timestamp that contains the following:

- when the vehicle was detected
- lane identifier
- the vehicle's speed
- the vehicle's prior gap
- the length of the vehicle

Note: gap is defined as the time in seconds between the rear of the preceding vehicle and the front of the current vehicle.

Real-time reporting – also referred to as *individual speed mode* or *individual car reports* – is enabled with TrafficDOT. See *Working with Push Settings* in the *Network Management* chapter for more information. More information about APSTAT is given in the following sections.

2.14.2.3 Counts and Occupancy Measurements

Statistics for counts and occupancy are calculated over a configurable time interval. Supported intervals are 10 seconds, 15 seconds, 30 seconds, 1 minute, 5 minutes, 10 minutes, 15 minutes or one half-hour.

2.14.2.4 Speed and Length Measurements

Vehicle speeds ranging from 1 mph to 100 mph are derived from the events of a Sensor pair installed at a known distance from one another. (A typical distance is 22 feet.) Average and median speeds are calculated over a configurable time interval. Supported intervals are 10 seconds, 15 seconds, 30 seconds, 1 minute, 5 minutes, 10 minutes, and 15 minutes.

In addition, speed data is presented in tabular form or as a histogram with resolution of 1 mph, 5 mph or as defined in the TTI specification. (See the section on optional data outputs below.)

Vehicle length is presented in tabular form or as a histogram with bin widths of 1 foot, or as defined in the TTI or *AustRoads* specification. (See the section on optional data outputs below.)

2.14.2.5 Data Sources

APSTAT opens a TCP connection to a designated Access Point or archive to acquire raw detection event data.

2.14.2.6 Data Processing and Storage

APSTAT writes its output files to a file system on the host on which it executes. The file system location varies slightly according to the host platform type and operating mode (aggregate or real-time) of APSTAT.

2.14.2.6.1 Non Access Point Platforms / Aggregate Report Mode

When APSTAT executes in aggregate report mode on a platform other than an Access Point (such as a PC or Linux workstation), output files are stored in a location as follows:

```
/var/apstat/apeg124567890123456
```

where “`/var/apstat/`” is a constant and the lowest level folder name is created by concatenating the string “`apeg`” with the unique, 16-character HEX id of the Access Point.

Because an instance of APSTAT binds with one and only one Access Point, this convention allows multiple instances of APSTAT to execute on a given platform.

2.14.2.6.2 File Handling

During compilation of the files, APSTAT writes to a file named `/var/apstat/apeg<#>/working/workingFile` until the size of that file exceeds the value of the *bpf* (bytes per archive file) setting. Once that occurs, `workingFile` is copied to its parent directory and renamed using the timestamp of the last data entry in it, a new `workingFile` is created, and APSTAT continues.

If a maximum amount of disk space allocated to archives is set (see parameter *maxSpace* below) and that amount of space is reached – calculated as *maxSpace* / *bpf* (see *bpf* below) – the oldest data file in the archive file system is deleted and APSTAT continues.

2.14.2.6.3 Non Access Point Platform / Real-time Report Mode

When APSTAT executes in real-time report mode on a platform other than an Access Point (such as a PC or Linux workstation), output files are stored in a file system named as follows:

```
/var/apstat/apeg124567890123456/speedLogs
```

where “`/var/apstat/`” and “`speedLogs`” are constants and a variable folder name is created by concatenating the string “`apeg`” with the unique, 16-character HEX id of the Access Point.

Because an instance of APSTAT binds with one and only one Access Point, this convention allows multiple instances of APSTAT to execute on a given platform.

In this mode, detection events result in data points being recorded, while the reporting interval determines when individual speed log files are created in the file system. The same file handling procedures described above are used.

2.14.2.6.4 Access Point as Platform / Aggregate Report Mode

When APSTAT executes in aggregate report mode on the Access Point itself, output files are stored in a file system named as follows:

```
/var/apstat/
```

The same file handling procedures described above are used.

2.14.2.6.5 Access Point as Platform / Real-time Report Mode

When APSTAT executes in real-time report mode on the Access Point itself, output files are stored in a file system named as follows:

```
/var/apstat/speedLogs
```

The same file handling procedures described above is used.

2.14.2.7 Data Outputs

Output consists of one or more comma delimited files storing data aggregated according to the application's parameters. Data aggregations include *default* outputs and *optional* outputs as defined below. (See also the section *Output Data Specification* later in this section.)

2.14.2.7.1 Default outputs

The default output data consists of the following elements:

- *Volume* – a count of the number of vehicles detected during the reporting interval
- *Occupancy* – the average of the individual occupancies calculated for each Sensor in the lane over the reporting interval
- *Speed median* – the median speed as measured for the lane
- *Sensors not responding* – the number of Sensors in the lane that have not transmitted over the reporting interval; also known as *diagnostic*

If watchdog packets are enabled (see the WatchDog Timeout parameter in the section Configuring Access Points), the reporting interval must be greater than the timeout value.

2.14.2.7.2 Optional outputs

The optional output data consists of the following elements:

Speed Histogram

Speed histogram slot widths can be set to 1 mph, 5 mph, or TTI spec widths (or 2 kmph and 10 kmph in metric units). (See also the section on *Speed median* below.)

Note: Bin counts may be rounded to an integer value due to count differences between the two Sensor pairs (in cases where there are three Sensors per lane.) Rounding is applied with an alternating rounding bias (that is, bin 1 is rounded up, bin 2 is rounded down, and so on.)

Length Histogram

Length is calculated as *speed* * (*time of detection* – *time of "undetection"*). Each senor pair produces two lengths, which are averaged and entered into the lane lengths histogram.

(See also the section on *Speed median* below.)

Length histogram slots widths are one of the following:

- 1 foot
- bins specified by the TTI or *AustRoad* classification specifications

2.14.2.8 Data Transfer

Output files can be manipulated with common TCP/IP based file utilities such as *ftp*.

In addition, Sensys Networks provides special purpose helper applications, APPUSHSTAT and APSTATRECV, that enable automatic, intelligent transfer of output data files to other hosts.

2.14.3 Hosts

APSTAT runs on a Sensys Access Point or other platform supporting Unix/Linux executables.

2.14.4 Command-line Syntax

The arguments recognized by the application are shown below. Required arguments are shown in bold. This application uses the Sensys Networks common connection interface arguments.

```
apstat tty = /dev/ttyXX  |
       snpFile = <filename>  |
       {host = hostname port = port} |
       {archiveapeg = <#>
        archiveStart = <start time>
        archiveEnd = <end time>
        archiveDir = <base dir of archives>}
       [listen = <port>]
       [dotFn = <filename>]
       [dotpairFn = <filename>]
       [apeg = <apeg_id>]
       [clockOffset = <time in secs> (positive or negative)]
       [GMTOffset = <hour difference from GMT> (positive or negative)]
       [logDir = <directory>]
       [report_int = <time in secs>]
       [delayproc = <1-30 secs>]
       [uphold = <time in 1/1024 secs>]
       [downhold = <time in 1/1024 secs>]
       [adaptive_downhold = <distance in feet>]
       [bpf = <bytes per archive file>]
       [maxSpace = <bytes allocated for archives | -1>]
       [speedavg=<0|1|2|3>]
       [speedstd=<0|1>]
       [units = <0|1>]
       [speedhist = <0|1|2|3>]
```

```
[lengthhist = <0|1|2>]
[time_opt =< 0|1|2>
[diagopt = <0|1|2|3>]
[lengthThres = <length percentage deviation allowed>]
[indivspeed_log = <0|1|2|3>
[indivspeed_mode = <0|1>
[custom_output = <0|1>]
```

2.14.5 Parameters

Common Connection Interface Argument

There are four options for designating the source of event data. The options are mutually exclusive.

2.14.5.1.1 tty

Specifies the serial device for connecting to an Access Point via its management console serial port.

2.14.5.1.2 snpFile

Specifies by name a log file generated by the SNCPROXY utility.

2.14.5.1.3 host, port

Specifies the IP address and port number of an Ethernet Access Point or SNCPROXY server as the event data source.

2.14.5.1.4 archiveapeg, archiveStart, archiveEnd, archiveDir

Collectively, these parameters define a specific archive as the source of event data. The parameters are used as follows:

- *archiveapeg* – designates by ID a unique Access Point that stores the event data
- *archiveStart* – designates in Unix time format the start of the event data set
- *archiveEnd* – designates in Unix time format the end of the event data set
- *archiveDir* – designates the path of the root folder storing the archive files

listen

Specifies the commands interface port APSTAT listens to for real-time modification of reporting intervals and other settings.

The specified port must not be used by other APSTAT instances or other applications executing on the host. If not specified, APSTAT attempts to use port 10005.

Note: if the parameters dotFn, dotpairFn and apeg are not supplied, and APSTAT is connected directly to an Ethernet Access Point, Sensor location data is acquired directly from the dot table database of the Access Point.

dotFn

Specifies by name a file storing a sensor configuration array. The format of the data must conform to the *Sensys Networks Dot Table* format.

dotpairFn

Specifies by name a file storing a dot pair configuration array. The format of the data must conform to the *Sensys Networks Dot Pair Table* format.

apeg

Specifies the Access Point monitored by APSTAT. The unique 64-bit value is rendered as a 16 character HEX value. This value is used as a text string in the output data files.

clockOffset

Time in seconds used to adjust APSTAT's internal time-stamp mechanism. It is used in cases where output from an Access Point must be synchronized with the output of another system. This parameter provides a way for APSTAT's “midnight” to be set to match the “midnight” of a 3rd party system. *Default* = zero

GMTOffset

This parameter allows for timezone modification of the output timestamps. If this value is not entered, timestamps in the reports will be GMT. *Default* = zero

logDir

The parent directory of the file system in which the processed Sensor data is stored as statistical archive files. The file system naming conventions differ by the platform hosting APSTAT.

For APSTAT instances hosted on a PC, archives are stored in a directory named "*apeg<HEX ID#>*" under the specified *logDir* where the string “`apeg`” is appended with the 16-character HEX ID of the Access Point. For example, `/var/apstat/apeg124567890123456`.

For APSTAT instances hosted on an Access Point, the subfolder named for the Access Point is omitted. *Default* = `/var/apstat`

report_int

The number of seconds in a reporting interval; the TrafficDOT GUI supports values of 10, 15, 30, 60, 300, 600, 900. (*Note*: advanced users may use other values; contact Sensys Networks for more information.) *Default* = 30

delayproc

The number of seconds APSTAT waits before processing event data to generate speeds/lengths. Must be between 1 and 30; *Default* = 5

uphold

Specifies the minimum amount of time a *detect signal* must last before it is considered a detection event. Specified in 1/1024 seconds; *Default* = zero

downhold

Specifies the minimum amount of time a *undetect signal* must last before it is considered an un-detection event. Setting this to a non-zero value will disable the *adaptive_downhold* feature (see below). Specified in 1/1024 seconds; *Default* = zero

adaptive_downhold

Sets the distance the system uses to adaptively change the *downhold* parameter. Specified in feet; *Default* = 10

bpf (bytes per archive file)

Sets the maximum size of *workingFile* before it is copied to the archive. Specified in bytes; *Default*=10,000

maxSpace

The approximate maximum amount of space allocated to archives. If the “next” archive file results in more than this amount of space being occupied by archives, the oldest archive file is deleted.

Set to -1 to disable this feature and allow an unlimited amount of space to be allocated to archive files. Specified in bytes; *Default*=-1

speedavg

Enables the speed average output feature.

0 = disable speed average output (*Default*)
1 = enable speed average output; averages are computed as the sum of all speeds divided by the number of cars
2 = enable speed average output; averages are computed as the sum of speeds (weighted over time) divided by the total time
3 = enable speed average output; averages are computed using the occupancy for that lane and an average vehicle length. If less than five vehicles are counted for the interval, the calculation reverts to the process defined for option value 1 above.

speedstd

Enables the standard deviation of speeds as an output.

0 = disable speed standard deviation as an output (*Default*)
1 = enable speed standard deviation as an output.

units

Specifies the unit of measure for distance calculations.

0 = Imperial scale (*Default*)
1 = Metric scale

speedhist

Enables the speed histogram feature and configures the bin widths.

0 = disable speed histogram reporting (*Default*)
1 = speed histogram reporting with 1 mph slots
2 = speed histogram reporting with 5 mph slots
3 = TTI spec speed histogram

lengthhist

Enables the length histogram feature and configures the bin widths.

0 = disable length histogram reporting (*Default*)
1 = length histogram reporting with 1 ft slots
3 = TTI spec length histogram / AustRoads specification

time_opt

Specifies the relationship between the reported timestamps and the reporting interval.

0 = reported timestamps match end time of reporting interval (*Default*)
1 = reported timestamps match start time of reporting interval
2 = reported timestamps match middle time of reporting interval

diagopt

Specifies whether diagnostic data is used to generate averages and whether the values are included on reports.

0 = use diagnostics data to generate "smart averages" for statistics and print this value in the report (*Default*)

1 = use diagnostics data to generate "smart averages" for statistics;. This value is NOT printed in the report.
2 = disable the use of diagnostics (good for instances where a *watchdog timeout* is not set) and print this value in the report
3 = disable the use of diagnostics (good for instances where a *watchdog timeout* is not set). This value is NOT printed in the report.

lengthThres

Used for filtering bad speed calculations that result from vehicle lane changes. It specifies the allowable deviation between the length calculations of two Sensors in a "speed pair." If the lengths calculated deviate more than this percentage, the speed is dropped.

indivspeed_log

Enables the individual speed output feature and specifies the output option.

0 = disable individual speed output (*Default*)
1 = enable individual speed output with new log files created at *report_int* seconds.
2 = enable individual speed output to a single log file. (Single log files are used by a web based GUI of APSTAT's output.)
3 = enable Marksman spec output with new log files created at *report_int* seconds.

Note: Enabling this option directs APSTAT to operate in real-time reporting mode and disables the default reporting mode that performs output aggregation. Therefore, counts, occupancy, etc. will not be reported.

indivspeed_mode

Specifies how APSTAT – when operating in real-time reporting mode - handles situations where vehicle speed and length cannot be calculated.

0 = report only vehicles that have calculable speeds and lengths (*Default*)
1 = report all vehicles regardless of the availability of speeds or lengths. (This option fills speed and length fields with "-" if they are unavailable.)

custom_output

Directs the use of optional output formats.

0 = disabled, use standard output (*Default*)
1 = enable output options for CalTrans D4 – TOSv21 compatibility mode. Mainline lane names must be numeric values corresponding to the lane numbers supported in the configuration options of the application APPOLLSTAT_CalTransD4. Ramp names must be numeric values preceded by an upper case R character (ASCII 82).[12]

2.14.6 Output Data Specifications

APSTAT outputs statistical data in CSV (comma separated values) format typically stored as flat files. The organization/content of the data depends on which reporting mode has been selected.

---

[12] Note: use of this option requires the use of the application *APPOLLSTAT_CalTransD4* for data delivery. Failure to use this application will result in indeterminate outcomes.

2.14.7 Aggregate Report Mode

The data organization for APSTAT's output when operating in the default, aggregate report mode is described in this section.

2.14.7.1 Report Scope

With regard to statistical data acquired from a Sensys network, the term *report* means an individual entry in an output file that contains measures and calculated values that pertain to a particular *Access Point* for a particular *reporting interval*. Thus, one file will contain numerous reports from an Access Point. Additionally, one report may contain values that relate to multiple lanes as described below.

2.14.7.2 Report Identification

Each report in an output file conforms to a standard format given in the following table:

Field Name	**Description**
Sequence Number	(*Optional*) Integer between 0 and 999, assigned to successive reports.
Timestamp	Specifies the date and time associated with the report data
Access point id	Unique, 16-character HEX id of the Access Point

Table 22: Report Identification Data

These elements begin each row of the output file. The s*equence number* is required only when APSTAT output is transferred to other hosts using receipt acknowledgment. (See the section on APPUSHSTAT in this chapter for more information.)

2.14.7.3 Report Data

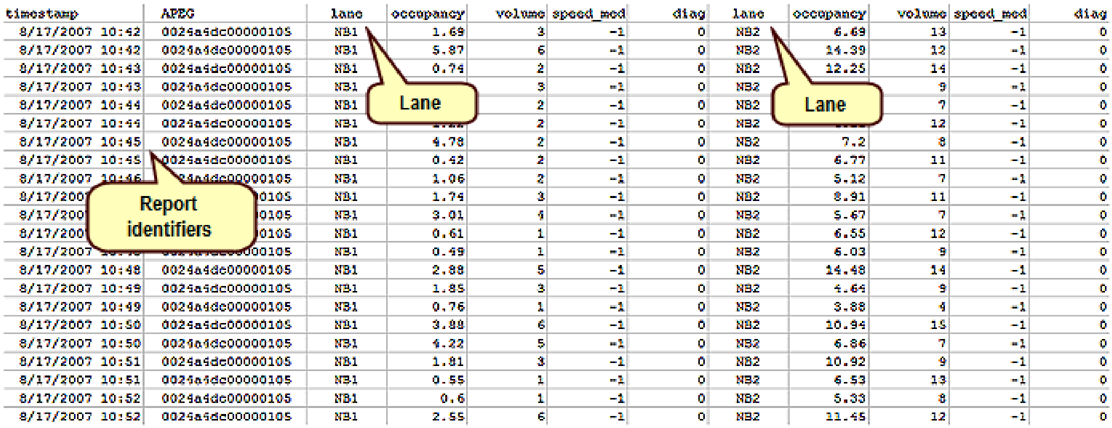
Report data consists (at a minimum) of the five elements given in the following table:

Field Name	**Description**
Lane id	Enumerates the lane to which the other fields pertain
Occupancy	Percentage specifying the measured lane occupancy
Volume	Number of vehicles measured for the lane
Speed median	Median speed calculated for the lane
Diagnostic count	Total number of non-reporting Sensors for the lane

Table 23: Minimum Data Elements Reported by APSTAT for Aggregated Reporting

Data for multiple lanes is represented as repeating groups of the five fields described above, with the lane id indicating the different lanes for which data is reported.

A file sample (including column names) for a two lane installation (without acknowledgments) is shown in the figure below:



timestamp	APEG	lane	occupancy	volume	speed_med	diag	lane	occupancy	volume	speed_med	diag
8/17/2007 10:42	0024a4dc00000105	NB1	1.69	3	-1	0	NB2	6.69	13	-1	0
8/17/2007 10:42	0024a4dc00000105	NB1	5.87	6	-1	0	NB2	14.39	12	-1	0
8/17/2007 10:43	0024a4dc00000105	NB1	0.74	2	-1	0	NB2	12.25	14	-1	0
8/17/2007 10:43	0024a4dc00000105	NB1	[illegible]	3	-1	0	NB2	[illegible]	9	-1	0
8/17/2007 10:44	0024a4dc00000105	NB1	[illegible]	2	-1	0	NB2	[illegible]	7	-1	0
8/17/2007 10:44	0024a4dc00000105	NB1	[illegible]	2	-1	0	NB2	[illegible]	12	-1	0
8/17/2007 10:45	0024a4dc00000105	NB1	4.78	2	-1	0	NB2	7.2	8	-1	0
8/17/2007 10:45	0024a4dc00000105	NB1	0.42	2	-1	0	NB2	6.77	11	-1	0
8/17/2007 10:46	[illegible]	NB1	1.06	2	-1	0	NB2	5.12	7	-1	0
[illegible]	[illegible]	NB1	1.74	3	-1	0	NB2	8.91	11	-1	0
[illegible]	[illegible]	NB1	3.01	4	-1	0	NB2	5.67	7	-1	0
[illegible]	[illegible]	NB1	0.61	1	-1	0	NB2	6.55	12	-1	0
[illegible]	[illegible]	NB1	0.49	1	-1	0	NB2	6.03	9	-1	0
8/17/2007 10:48	0024a4dc00000105	NB1	2.88	5	-1	0	NB2	14.48	14	-1	0
8/17/2007 10:49	0024a4dc00000105	NB1	1.85	3	-1	0	NB2	4.64	9	-1	0
8/17/2007 10:49	0024a4dc00000105	NB1	0.76	1	-1	0	NB2	3.88	4	-1	0
8/17/2007 10:50	0024a4dc00000105	NB1	3.88	6	-1	0	NB2	10.94	15	-1	0
8/17/2007 10:50	0024a4dc00000105	NB1	4.22	5	-1	0	NB2	6.86	7	-1	0
8/17/2007 10:51	0024a4dc00000105	NB1	1.81	3	-1	0	NB2	10.92	9	-1	0
8/17/2007 10:51	0024a4dc00000105	NB1	0.55	1	-1	0	NB2	6.53	13	-1	0
8/17/2007 10:52	0024a4dc00000105	NB1	0.6	1	-1	0	NB2	5.33	8	-1	0
8/17/2007 10:52	0024a4dc00000105	NB1	2.55	6	-1	0	NB2	11.45	12	-1	0

Figure 2.33: Sample Two-lane Output From Default Per-lane Report Mode

2.14.7.3.1 Optional Output Fields

Additional data elements are available for output depending on the configuration of the Access Point. The following table depicts the position of these fields in the report data when the Access Point is configured to include them. (For more information, see *Data Outputs* above and *Working With Push Settings* in the *Network Management* chapter.)

Field Name	Description
Lane id	Enumerates the lane to which the other fields pertain
Occupancy	Percentage specifying the measured lane occupancy
Volume	Number of vehicles measured for the lane
Speed median	Median speed calculated for the lane
Speed average	Average speed calculated for the lane
Speed standard deviation	Standard deviation of calculated speeds
Speed histogram bins	Speed values for the lane/interval placed into preset histogram bins
Length histogram bins	Length values for the lane interval place into preset histogram bins
Diagnostic count	Total number of non-reporting Sensors for the lane

Table 24: Full Set of Data Elements Reported by APSTAT for Aggregated Reporting

The histogram fields are represented by a series of “bins” that represent discrete regions along a continuum of possible values. The histograms are enabled via the *Speed Histogram* and *Length Histogram* attributes set via TrafficDOT. For example, a one lane report with a length histogram configured to the TTI specification would have the data organization shown in the following table:

Field Name	Description
Sequence Number	(*Optional*) Integer between 0 and 999, assigned to successive reports
Timestamp	Specifies the time associated with the report data
Access point id	Unique, 16-character HEX id of the Access Point
Lane id	Enumerates the lane to which the other fields pertain
Occupancy	Percentage specifying the measured lane occupancy
Volume	Number of vehicles measured for the lane
Speed median	Median speed calculated for the lane
Length (0 – 11 ft)	Values that fall within bin range
Length (11 – 22 ft)	Values that fall within bin range
Length (22 – 30 ft)	Values that fall within bin range
Length (30 – 38 ft)	Values that fall within bin range
Length (38+ ft)	Values that fall within bin range
Diagnostic count	Total number of non-reporting Sensors for the lane

Table 25: Data output elements for Single Lane report with TTI Length Histogram

2.14.7.4 Data Element Descriptions

The default outputs for aggregate report mode include:

2.14.7.4.1 Sequence Number

An integer between 0 (zero) and 999 that is incremented by one for each report that is generated. This value is used when the data transfer utility APPUSHSTAT is operated with message acknowledgment enabled.

The target server is expected to acknowledge each data transfer by replying on the same TCP port with the message in CSV format that contains the string “`ACK`” followed by the sequence number value of the report received.

2.14.7.4.2 Timestamp

The time of the report in `YYYY-MM-DD HH:MM:SS` format. By default, this is “local” time (the timezone of the Access Point) and represents the time at the end of a reporting interval. Configuration options allow adjustment of the timezone and use of the time at the beginning or mid-point of the reporting interval.

2.14.7.4.3 Access Point ID

The unique, 16-character HEX id string of the Access Point taken from the raw detection data.

2.14.7.4.4 Lane ID

ASCII string that identifiers the lane for which measurements are taken. To create a globally unique identifier, combine this field with *Access Point ID*.

2.14.7.4.5 Occupancy

The measured lane occupancy over the reporting interval represented as a percentage with two decimal places. Occupancy is calculated by taking the average of the individual occupancies calculated on each Sensor in the lane.

Individual occupancies are calculated as (*# of ticks a Sensor reported a vehicle above it*) / (*total # of ticks in the reporting interval*).

2.14.7.4.6 Volume

Integer count of the number of vehicles that passed the monitored area. There are no leading zeros nor limits on the number of digits.

2.14.7.4.7 Speed Median

Median speed of measurements in the lane over the interval. This figure is represented as mile-per-hour (mph) with one decimal point and is set to negative one(-1.0) if no vehicles were detected during the reporting interval.

The median speed is the speed at which 50% of the total number of vehicles were traveling at or below.

In implementations using three Sensors per lane, speed is calculated from both Sensor pairs. If both Sensor pairs report a speed (for the same car), each speed is separately entered into the lane's speed histogram. If only one of the Sensor pairs reports a speed for a single car, the speed is entered into the histogram twice.

2.14.7.4.8 Diagnostic Count

The number of Sensors in the lane that have not been heard from over the entire reporting interval or have experienced extended latency during the interval. It is used to prevent averaging from bad values as well as to indicate possible disabled Sensors.

This figure is also useful as a first-order diagnostic tool for determining the number of failed Sensors in the lane. The value will vary depending on the number of Sensors in the lane.

In the event that this count equals the total number of Sensors in the lane, the values of *occupancy*, *volume* and *speed median* are set to negative one.

2.14.8 Real-time Report Mode

The data organization for APSTAT's output when operating in real-time report mode is described in this section. Real-time reporting is enabled via TrafficDOT by specifying *Individual Car Reports*. (See the section *Working With Push Settings* in the *Network Management* chapter for more information.)

2.14.8.1 Report Scope

As with aggregate report mode, the term *report* means an individual entry in an output file that contains measures and calculated values that pertain to a particular *Access Point*. However, real-time reporting is driven by vehicle detection; each detection generates a report entry.

The configured reporting interval stipulates when separate output files are created, but depending on the volume of vehicles detected, separate output files may contain multiple report entries.

2.14.8.2 Report Identification

Each report in an output file conforms to the standard format described above in the section discussing aggregate report mode. Data elements include *sequence number*, *timestamp* and *Access Point ID*.

2.14.8.3 Report Data

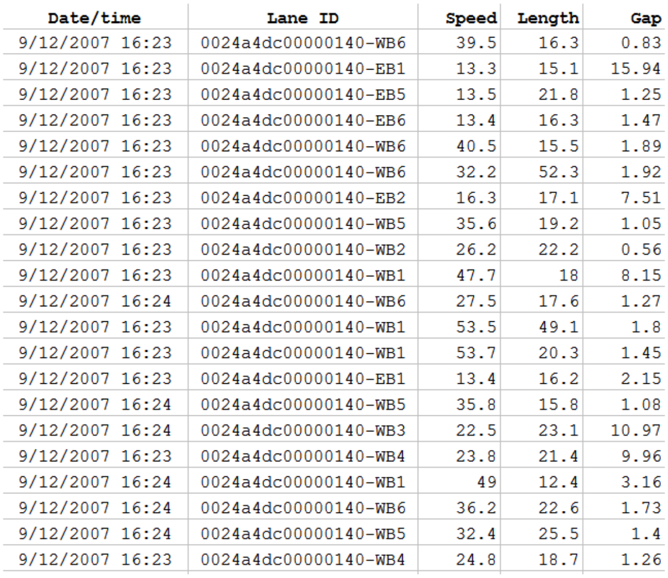
Report data consists of the four elements given in the following table:

Field Name	Description
Lane id	Globally unique lane identifier
Speed	Measured speed of the vehicle
Length	Calculated length of the vehicle
Gap	Calculated gap between successive vehicles

Table 26: Data Elements Reported by APSTAT for Individual Vehicle Reporting

Data for all lanes are commingled in the output file differentiated by the value of *lane id* and *timestamp* (from the report identification data).

A file sample (including column names) for a two lane installation (without acknowledgments) is show in the figure below:



Date/time	Lane ID	Speed	Length	Gap
9/12/2007 16:23	0024a4dc00000140-WB6	39.5	16.3	0.83
9/12/2007 16:23	0024a4dc00000140-EB1	13.3	15.1	15.94
9/12/2007 16:23	0024a4dc00000140-EB5	13.5	21.8	1.25
9/12/2007 16:23	0024a4dc00000140-EB6	13.4	16.3	1.47
9/12/2007 16:23	0024a4dc00000140-WB6	40.5	15.5	1.89
9/12/2007 16:23	0024a4dc00000140-WB6	32.2	52.3	1.92
9/12/2007 16:23	0024a4dc00000140-EB2	16.3	17.1	7.51
9/12/2007 16:23	0024a4dc00000140-WB5	35.6	19.2	1.05
9/12/2007 16:23	0024a4dc00000140-WB2	26.2	22.2	0.56
9/12/2007 16:23	0024a4dc00000140-WB1	47.7	18	8.15
9/12/2007 16:24	0024a4dc00000140-WB6	27.5	17.6	1.27
9/12/2007 16:23	0024a4dc00000140-WB1	53.5	49.1	1.8
9/12/2007 16:23	0024a4dc00000140-WB1	53.7	20.3	1.45
9/12/2007 16:23	0024a4dc00000140-EB1	13.4	16.2	2.15
9/12/2007 16:24	0024a4dc00000140-WB5	35.8	15.8	1.08
9/12/2007 16:24	0024a4dc00000140-WB3	22.5	23.1	10.97
9/12/2007 16:23	0024a4dc00000140-WB4	23.8	21.4	9.96
9/12/2007 16:24	0024a4dc00000140-WB1	49	12.4	3.16
9/12/2007 16:24	0024a4dc00000140-WB6	36.2	22.6	1.73
9/12/2007 16:24	0024a4dc00000140-WB5	32.4	25.5	1.4
9/12/2007 16:23	0024a4dc00000140-WB4	24.8	18.7	1.26

Figure 2.34: Sample Output From Individual Car Reporting

2.14.8.4 Data Element Descriptions

The default outputs for real-time report mode include:

2.14.8.4.1 Sequence Number

An integer between 0 (zero) and 999 that is incremented by one for each report that is generated. This value is used when the data transfer utility APPUSHSTAT is operated with message acknowledgment enabled.

The target server is expected to acknowledge each data transfer by replying on the same TCP port with the message in CSV format that contains the string "`ACK`" followed by the sequence number value of the report received.

2.14.8.4.2 Timestamp

The time of the report in `YYYY-MM-DD HH:MM:SS` format. By default, this is "local" time (the timezone of the Access Point) and represents the time at the end of a reporting interval. Configuration options allow adjustment of the timezone and use of the time at the beginning or mid-point of the reporting interval.

2.14.8.4.3 Lane ID

Globally unique lane identifier formed by concatenating the 16-character HEX id of the Access Point and the user defined lane id.

2.14.8.4.4 Speed

The calculated speed of the vehicle. Speed is expressed as mile-per-hour (mph) or kilometers-per-hour (kmph) with one decimal point. It is set to negative one if no vehicles were detected during the reporting interval.

2.14.8.4.5 Length

The calculated length of the vehicle. Length is calculated as {*speed* * (*time of detection – time of "undetection"*)}.

2.14.8.4.6 Gap

The calculated separation between two successive vehicles. Gap is defined as the time in seconds between the rear of the preceding vehicle and the front of the current vehicle.

2.14.9 Related Applications

APPOLLSTAT
APPOLLSTAT_TCP
APPUSHSTAT
SNCPROXY

2.15 APSTATRECV

APSTATRECV implements a TCP server to accept data transfers from one or more instances of APPUSHSTAT.

2.15.1 Typical Use

In a typical installation, event data is collected and aggregated locally on an Access Point by APSTAT. The aggregated data can then be optionally delivered to an external server via a local instance of APPUSHSTAT. APSTATRECV executes on the external host and receives data transfers initiated by APPUSHSTAT.

Note: APSTATRECV does not support APPUSHSTAT transfers when the statistical data has been created in Marksman output format.

2.15.2 Operations

APSTATRECV implements a TCP server that can receive messages from multiple instances of APPUSHSTAT executing on multiple Access Points. Incoming messages are parsed for the unique, 64-bit device id of the originating Access Point and written to a file stored under a subdirectory whose name matches the Access Point ID. A file name is created based on the file's contents.

APSTATRECV acknowledges individual messages by returning to APPUSHSTAT a standard Sensys Networks acknowledgment that includes the sequence number of the message being acknowledged.

Note: For APSTATRECV to function properly, APPUSHSTAT must be configured to execute with message acknowledgments (ackMode = 1); this is the system default.

2.15.3 Hosts

APSTATRECV executes on hosts the receive statistics data transferred by APPUSHSTAT.

2.15.4 Command-line Syntax

The arguments recognized by the application are shown below. Required arguments are shown in bold.

```
apstatrecv listen = <port>
           logDir = <file system location>
```

2.15.5 Parameters

2.15.5.1 listen

(*Required*) The port number on which incoming messages are communicated. (*Note*: this port should match the port argument of the APPUSHSTAT instance that originates the data transfer.)

2.15.5.2 logDir

(*Required*) Names the parent directory (on the host executing APSTATRECV) storing the subdirectories named with the unique Access Point ID of the devices that originally collected the event data. *Default* = `/var/apstatrecv`

2.15.6 Related Applications

APPUSHSTAT
APSTAT

2.16 EVENTPROXY

EVENTPROXY provides a text/line oriented interface to event data.

2.16.1 Typical Use

EVENTPROXY provides low-level (raw) access to event data in the form of individual event packets. Thus, it is typically used for spot monitoring or debugging purposes.

2.16.2 Operations

EVENTPROXY implements a simple text and line-oriented TCP/IP interface to event data packets transmitted to an Access Point from Sensors. The application connects to an Access Point or archive file and converts event packets into standard ASCII text, one event per line.

EVENTPROXY implements a TCP server through which connected clients are served an ASCII stream of event data formatted as described below. Upon connecting to EVENTPROXY, a client receives the current states of all Sensors known to the Access Point. (Sensors that have not SYNCed to the Access Point, or that have lost SYNC, are not reported.) Event data is formatted as follows:

2.16.2.1 SensorID

The 4-character HEX string displayed on the *Access Point Main* window in the column *Sensor ID*.

2.16.2.2 event time

Double precision floating number in EPOCH time format[13].

2.16.2.3 event

A decimal value where:

- a value of zero (0) indicates *Off*
- a value of one (1) indicates *On*
- a value of two (2) indicates a *Sync* packet
- a value of three (3) indicates a *Watchdog* (high) packet
- a value of five (5) indicates a *Watchdog* (low) packet

---

[13] A system for describing points in time widely used in Unix, Linux and other environments; it is the number of seconds elapsed since midnight UTC of January 1, 1970, not counting leap seconds.

Sync packets are periodically sent to Sensors to allow them to measure the offset between the time of the Access Point and the local time.

Watchdog packets indicate the current state of the detector (low/high) and confirm that the Sensor can reach the Access Point in the absence of detection events. The interval at which watchdog packets are generated is user configurable with TrafficDOT. (Refer to the *Event Reporting Parameters* discussion in Chapter 2.)

2.16.3 Hosts

EVENTPROXY executes on any platform that supports Linux executables.

2.16.4 Command-line Syntax

The arguments recognized by the application are shown below. Required arguments are shown in bold. This application uses the four Sensys Networks common connection interface arguments.

```
eventproxy tty = /dev/ttyXX  |
           snpFile = <filename>  |
           {host = hostname  port = port}  |
           {archiveapeg = <#>
            archiveStart = <start time>
            archiveEnd = <end time>
            archiveDir = <base dir of archives> }
           [serverPort = <port>]
           [dotFn = <filename>  dotpairFn = <filename>]
           [adaptiveHold = <distance in feet | 10>]
```

2.16.5 Parameters

2.16.5.1 Common Connection Interface Argument

There are four options for designating the source of event data. The options are mutually exclusive.

2.16.5.1.1 tty

Specifies the serial device for connecting to an Access Point via its management console serial port.

2.16.5.1.2 snpFile

Specifies by name a log file generated by SNCPROXY.

2.16.5.1.3 host, port

Specifies the IP address and port number of a Ethernet Access Point or SNCProxy server as the event data source.

2.16.5.1.4 archiveapeg, archiveStart, archiveEnd, archiveDir

Collectively, these parameters define a specific archive as the source of event data. The parameters are used as follows:

- *archiveapeg* – designates by ID a unique Access Point that stores the event data
- *archiveStart* – designates in Unix time format the start of the event data set
- *archiveEnd* – designates in Unix time format the end of the event data set
- *archiveDir* – designates the path of the root folder storing the archive files

2.16.5.2 serverPort

The port EVENTPROXY listens to for requests.

2.16.5.3 dotFn

Specifies by name a “dot table” file in APTABLE format. This file identifies the Sensors used in a given network.

2.16.5.4 dotpairFn

Specifies by name a “dot pair table” in APTABLE format. This file identifies the Sensor pairs used in a given network.

Note: APTABLE format is a proprietary data representation of Sensys Networks, Inc. Do not use parameters in this format without consulting Sensys Networks.

2.16.5.5 adaptiveHold

Specifies in feet the distance used by the system to dynamically adapt the *holdover* parameter. If both *dotFn* and *dotpairFn* are specified, the contents of those files are used for Sensor geographical (location and separation) information. Otherwise, the geographical information is acquired from the Access Point's on-board Sensor tables. *Default* = 10.

2.17 Sensys Management Servers

Sensys Networks provides two network management platforms (*SNAPS Professional* and *Sensys System Manager*) that enable management and statistical data services to one or more Sensys network installations.

2.17.1 Typical Use

Large installations often require centralization of control and management access, systematic and automatic processing of event data, real-time access to event data, and support for network architectures that position Access Points behind firewalls, NAT servers, and similar devices. Sensys Management servers simplify the use of Sensys Networks equipment in such implementations.

Note: Sensys Management servers are optional. All Sensys Network equipment and software support standard TCP/IP based communications and can be integrated with custom or 3rd party applications.

2.17.2 Operations

Sensys Management servers provide the following services to a Sensys network:

- Remote management and maintenance of detection networks
- Diagnostic and health monitoring of detection equipment
- Traffic data acquisition and analysis

Each service is discussed below.

2.17.2.1 Remote Management and Maintenance of Detection Networks

All Sensys devices can be managed through a management server. Access Points are contacted via an unique IP address, and via the AP's built-in command set, configuration and management commands are issued to the Sensors, Repeaters, and CC cards serviced by the Access Point.

Access Points can be grouped to enable issuance of management commands to all APs in a given jurisdiction or system. This simplifies configuration changes and device firmware updates. Access Points managed by a Sensys Management server automatically enable multiple concurrent sessions without special provisioning.

Other administrative tasks – including backup and restore operations, and license upgrades – can be performed remotely by authorized users.

2.17.2.2 Diagnostic and Health Monitoring of Detection Equipment

Sensys Management servers use a graphical user interface to communicate system state conditions. Overall network health is depicted by color-coded icons; the status of the management server process is refreshed automatically; radio communication status metrics (wireless signal strength [RSSI] and link quality [LQI]) are updated in real-time; battery device levels are polled and displayed according to the network communications properties of each managed network.

Automatic alarm notifications are set based on user configured thresholds associated with key system properties. Alarms are triggered when network behavior exceeds the thresholds. Alarms are delivered by email to defined recipients or groups of recipients.

Daily diagnostics reports provide detailed performance data for all devices in a network can be automatically generated and distributed to administrators via email.

An optional feature provides geographical depiction of network location. Rendering a network against a background based on satellite imagery or political map is used to aid understanding and improve documentation.

2.17.2.3 Traffic Data Acquisition and Analysis

Raw event detection data is collected from managed networks on a predefined schedule. Event data is automatically processed and archived on the Sensys management server. (In the case of *Sensys System Manager*, an aging policy is applied by the system to event data to provide unattended maintenance of the platform.)

Detection data analysis provides an array of per-vehicle or per-lane statistics presented in browser-based formats (HTML tables, PNG images) or down loadable as CVS or text files.

2.17.2.4 Role-based Access

Sensys management servers use a role-based security system. User accounts may be established with full, read-only, or permissions based on a custom definition.

2.17.3 Types of Management Servers from Sensys Networks

Sensys management servers require a supported Linux distribution[14] and the TCP/IP network protocol. The servers also use additional software components that are shipped with the product; these include Sensys proprietary objects and certain open source distributions.

Management servers from Sensys are available in the following forms:

---

[14] Approved distributions include Fedora Core 10 and Redhat Enterprise 5.0

- *SNAPS Professional* - a software-only solution that resides and runs on customer supplied hardware. This solution is targeted at enterprises with existing Linux infrastructure, IT staff, and complex networking requirements.
- *Sensys System Manager* i- a hardware/software bundle for customers without IT resources to implement the management server with a minimum of effort.

2.18 SNCPROXY

SNCPROXY is a proxy server for Sensys Networks Access Points.

2.18.1 Typical Use

In larger installations, SNCPROXY is used to reduce (*i*) the work load of the processors on Access Points and (*ii*) the overall bandwidth necessary to manage the system. In addition, SNCPROXY acquires and archives Sensor data from Access Points.

Hosts executing SNCPROXY can optionally be authenticated via a RADIUS server. Authentication is used to allow/disallow user access, permit *administrative* (full rights) access or permit *monitoring-only* (limited rights) access. A user with monitoring-only rights is not allowed to issue configuration commands.

2.18.2 Operations

SNCPROXY connects via TCP to a designated Access Point and retrieves its Sensor data to an archive file – typically once per day. As such, SNCPROXY works as an archive server.

In addition, SNCPROXY brokers management access to the Access Point. TrafficDOT connects to an instance of SNCPROXY to make changes or review the network's configuration or perform other activities. (See the *Network Management* chapter for more information.)

SNCPROXY is commonly executed via a start-up script that reads the configuration file `/etc/sncproxy.conf`. The configuration file contains one for each Access Point to which SNCPROXY will connects. Each line contains the following elements:

2.18.2.1 Access Point ID

The name of the Access Point. For example, “apeg100”.

2.18.2.2 Access Point host

The IP address of the Access Point.

2.18.2.3 Access Point port

The port number on the Access Point to which SNCPROXY will connect.

2.18.2.4 local listening port

The port number SNCPROXY listens to for client requests.

2.18.2.5 radius server user

The RADIUS server user name used by SNCPROXY to do authentication.

2.18.2.6 radius server password

The RADIUS server password used by SNCPROXY to do authentication.

2.18.2.7 radius server secret

The RADIUS server shared secret used by SNCPROXY to do authentication.

2.18.3 Hosts

SNCPROXY is executed on a Sensys management server as part of the management server application.

2.18.4 Command-line Syntax

The arguments recognized by the application are shown below. Required arguments are shown in bold.

```
sncproxy host = <apip>
         [port = port]
         [listen = <port>]
         [logdir = <dir>]
         [logSubDir = <subdir>]
         [monitor = <0 | 1>]
         [radius-server = <radiushost>]
         [radius-port = <port>]
         [radius-user = <user>]
         [radius-pass] = <password>]
         [radius-secret = <secret>]
```

2.18.5 Parameters

2.18.5.1 host

The IP address or host name of the Access Point to which SNCPROXY connects.

2.18.5.2 port

The remote port (the port on the Access Point) SNCPROXY uses to connect to the Access Point.
Default = 10000

2.18.5.3 listen

The local port (the port on the host executing SNCPROXY) on which client requests are made.

2.18.5.4 logdir

The file system on the host executing SNCPROXY that stores the Sensor data as archive files.
Default = `/var/sncproxy/`

2.18.5.5 logSubDir

The sub directory in which the archive files are stored. The default name is formed from the Access Point. ID.

2.18.5.6 monitor

Specifies the processing mode of SNCPROXY.

0 = forward configuration requests to the Access Point and archive its data
1 = do not forward configuration requests to the Access Point; do not archive its data

2.18.5.7 radius-server

The host name or IP address of a *radius server* used for authentication and authorization. The radius server must include the Sensys Dictionary which defines the Sensys-Role.

2.18.5.8 radius-port

The port number SNCPROXY uses to contact the radius server.

2.18.5.9 radius-user

A text string used as user id for authentication with the radius server.

2.18.5.10 radius-pass

A text string used as password for authentication with the radius server.

2.18.5.11 radius-secret

A text string used as a shared secret between the radius server and the clients it serves. This element is defined in the radius server configuration.

3 Network Management

This chapter provides information about configuring and managing the components of the Sensys™ Wireless Vehicle Detection System. An overview of the configuration process is given, followed by an introduction to *TrafficDOT*, the configuration and network management application from Sensys Networks.

Separate sections describe the configuration procedures for Sensys Access Points, Repeaters and Sensors.

> *Note*: configuration of Sensys Contact Closure cards is covered in the document *Sensys Contact Closure Card – Installation Guide*.

In addition, this chapter contains sections describing other TrafficDOT functions useful in managing Sensys networks.

3.1 Overview

Configuration of a Sensys network involves (*i*) co-ordinating 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 Sensys 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.

All configuration activities are performed with TrafficDOT, a software tool from Sensys Networks for network administration and management. 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.

3.2 TrafficDOT

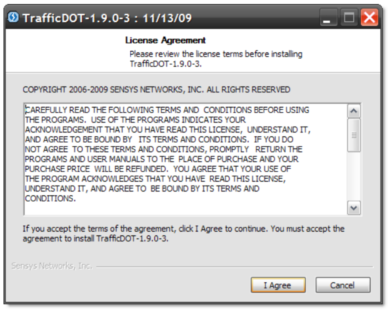
TrafficDOT is a small, self-installing program that provides a graphical user interface (GUI) to the components of a Sensys network. It runs on the Java™ Platform, Standard Edition Runtime Environment (JRE) – an industry standard application framework that ensures portability of TrafficDOT's functions across different platforms and operating systems. You can run TrafficDOT on any computer that supports the JRE (including Windows, Mac, Unix and Linux platforms).

Note: if the Java Runtime Environment is not found on the computer that TrafficDOT is installed on, the installation process automatically acquires it and optionally installs it for you. This requires a connection to the Internet.

3.2.1 Installation Procedure

Use the following procedure to install TrafficDOT. The examples below are taken from an installation on a computer running Microsoft Windows XP. (TrafficDOT is also available for computers running the Linux or MAC OS operating systems.)

1. Acquire the installation package from Sensys Networks.
2. *License Agreement* - run the executable to open the *License Agreement* window.



TrafficDOT-1.9.0-3 : 11/13/09

License Agreement

Please review the license terms before installing TrafficDOT-1.9.0-3.

COPYRIGHT 2006-2009 SENSYS NETWORKS, INC. ALL RIGHTS RESERVED

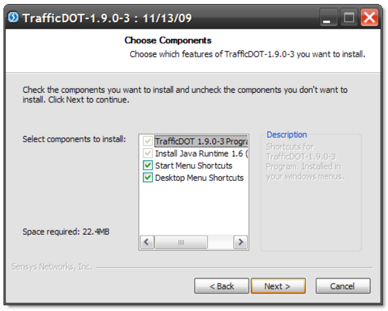
CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE USING THE PROGRAMS. USE OF THE PROGRAMS INDICATES YOUR ACKNOWLEDGEMENT THAT YOU HAVE READ THIS LICENSE, UNDERSTAND IT, AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, PROMPTLY RETURN THE PROGRAMS AND USER MANUALS TO THE PLACE OF PURCHASE AND YOUR PURCHASE PRICE WILL BE REFUNDED. YOU AGREE THAT YOUR USE OF THE PROGRAM ACKNOWLEDGES THAT YOU HAVE READ THIS LICENSE, UNDERSTAND IT, AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install TrafficDOT-1.9.0-3.

Figure 3.1: License Agreement

Carefully review the license terms and conditions. Click *I Agree* to continue or *Cancel* to abort the installation.

3. *Component Selection* – Select the objects that you want to install from the *Choose Components* window by filling the check box to the left of the object's description.


TrafficDOT-1.9.0-3 : 11/13/09

Choose Components

Choose which features of TrafficDOT-1.9.0-3 you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

☑ TrafficDOT 1.9.0-3 Progra
☑ Install Java Runtime 1.6 (
☑ Start Menu Shortcuts
☑ Desktop Menu Shortcuts

Description

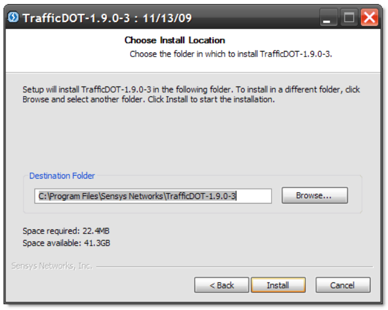
Shortcuts for TrafficDOT-1.9.0-3 Program. Installed in your windows menus.

Space required: 22.4MB

Figure 3.2: Choose Components to Install

Note: TrafficDOT is always installed, so it's check box is not accessible.

4. *Install Location* – Designate the location on your computer to which TrafficDOT will install on the *Choose Install Location* window.


TrafficDOT-1.9.0-3 : 11/13/09

Choose Install Location

Choose the folder in which to install TrafficDOT-1.9.0-3.

Setup will install TrafficDOT-1.9.0-3 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

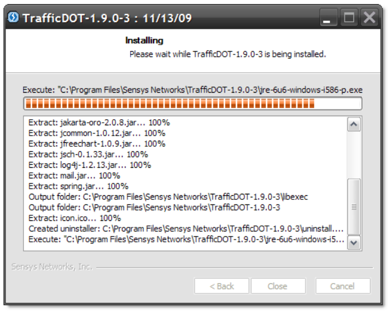
Destination Folder: C:\Program Files\Sensys Networks\TrafficDOT-1.9.0-3

Space required: 22.4MB
Space available: 41.3GB

Figure 3.3: Choose Install Location

The installer reports the amount of space required by TrafficDOT and the total amount of free space on the target computer.

5. *Installation* – The progress of the installation is reported on the *Installation* window. Optionally click *Show Details* for more information about the current process step.


TrafficDOT-1.9.0-3 : 11/13/09

Installing

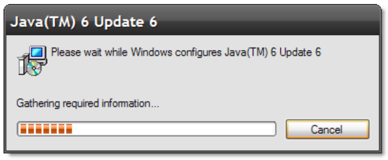
Please wait while TrafficDOT-1.9.0-3 is being installed.

```
Execute: "C:\Program Files\Sensys Networks\TrafficDOT-1.9.0-3\jre-6u6-windows-i586-p.exe
```

```
Extract: jakarta-oro-2.0.8.jar... 100%
Extract: jcommon-1.0.12.jar... 100%
Extract: jfreechart-1.0.9.jar... 100%
Extract: jsch-0.1.33.jar... 100%
Extract: log4j-1.2.13.jar... 100%
Extract: mail.jar... 100%
Extract: spring.jar... 100%
Output folder: C:\Program Files\Sensys Networks\TrafficDOT-1.9.0-3\libexec
Output folder: C:\Program Files\Sensys Networks\TrafficDOT-1.9.0-3
Extract: icon.ico... 100%
Created uninstaller: C:\Program Files\Sensys Networks\TrafficDOT-1.9.0-3\uninstall....
Execute: "C:\Program Files\Sensys Networks\TrafficDOT-1.9.0-3\jre-6u6-windows-i5...
```

Figure 3.4: Installation Status

6. *JRE Installation* – The Java Runtime Environment (JRE) is a required component; it's installation via a separate process that occurs at this point.

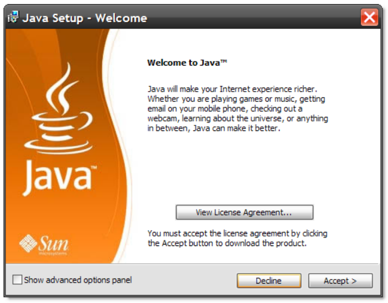


Please wait while Windows configures Java(TM) 6 Update 6

Gathering required information...

Figure 3.5: Java Install Wizard

7. *Java Setup* – Click *Accept* to begin the JRE installation. Click *Finish* on the completion screen to end the task.

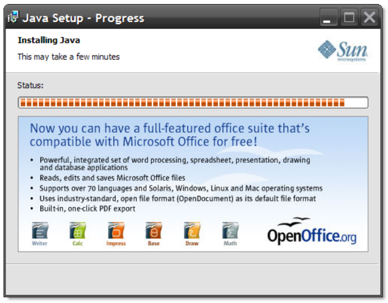


Welcome to Java™

Java will make your Internet experience richer. Whether you are playing games or music, getting email on your mobile phone, checking out a webcam, learning about the universe, or anything in between, Java can make it better.

You must accept the license agreement by clicking the Accept button to download the product.

Figure 3.6: Java Setup – Welcome



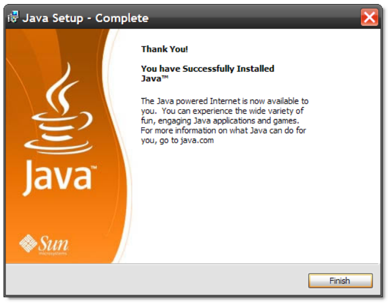
Installing Java

This may take a few minutes

Now you can have a full-featured office suite that's compatible with Microsoft Office for free!

- Powerful, integrated set of word processing, spreadsheet, presentation, drawing and database applications
- Reads, edits and saves Microsoft Office files
- Supports over 70 languages and Solaris, Windows, Linux and Mac operating systems
- Uses industry-standard, open file format (OpenDocument) as its default file format
- Built-in, one-click PDF export

Figure 3.7: Java Setup – Progress



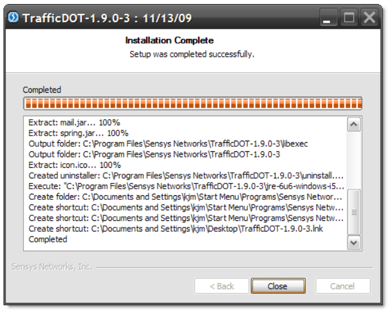
Thank You!

You have Successfully Installed Java™

The Java powered Internet is now available to you. You can experience the wide variety of fun, engaging Java applications and games. For more information on what Java can do for you, go to java.com

Figure 3.8: Java Setup – Completion

8. *TrafficDOT Installation Completion* – The results of the installation appear on the *Installation* window. Click *Close* to complete the TrafficDOT installation.



```
Extract: mail.jar... 100%
Extract: spring.jar... 100%
Output folder: C:\Program Files\Sensys Networks\TrafficDOT-1.9.0-3\libexec
Output folder: C:\Program Files\Sensys Networks\TrafficDOT-1.9.0-3
Extract: icon.ico... 100%
Created uninstaller: C:\Program Files\Sensys Networks\TrafficDOT-1.9.0-3\uninstall....
Execute: "C:\Program Files\Sensys Networks\TrafficDOT-1.9.0-3\jre-6u6-windows-i5...
Create folder: C:\Documents and Settings\kjm\Start Menu\Programs\Sensys Networ...
Create shortcut: C:\Documents and Settings\kjm\Start Menu\Programs\Sensys Netw...
Create shortcut: C:\Documents and Settings\kjm\Start Menu\Programs\Sensys Netw...
Create shortcut: C:\Documents and Settings\kjm\Desktop\TrafficDOT-1.9.0-3.lnk
Completed
```

Figure 3.9: TrafficDOT Installation Results

9. *Finding the TrafficDOT Application* – The default installation process places an application shortcut on the desktop.

Figure 3.10: TrafficDOT Icon

Additionally, TrafficDOT can be found in the *Sensys Networks* folder under the Windows Start menu.

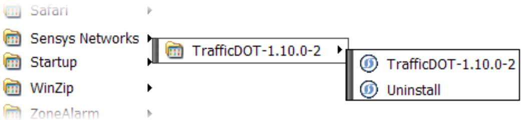


Figure 3.11: Sensys Networks Program Folder

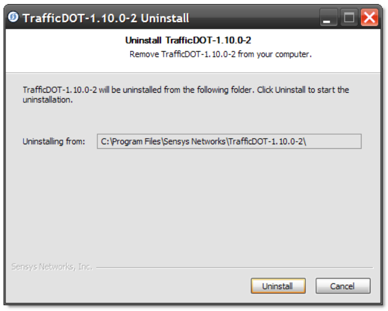
3.2.2 Uninstalling the Software

For installations onto computers running Microsoft Windows, access the *Sensys Networks* program folder from the *Start* menu. Navigate to the TrafficDOT folder and click *Uninstall*. (See figure 3.11 above.)

(*Note*: on hosts with other operating systems, use the operating system's standard method for removing applications from the computing environment.)

Perform the following steps to remove the software:

1. *Confirming the removal of TrafficDOT* – Click *Uninstall* on the *Uninstall TrafficDOT* window to verify that the application should be removed.


TrafficDOT-1.10.0-2 Uninstall
Uninstall TrafficDOT-1.10.0-2
Remove TrafficDOT-1.10.0-2 from your computer.

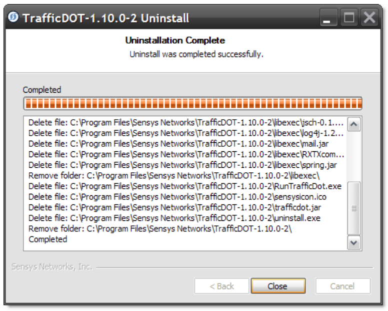
TrafficDOT-1.10.0-2 will be uninstalled from the following folder. Click Uninstall to start the uninstallation.

Uninstalling from: C:\Program Files\Sensys Networks\TrafficDOT-1.10.0-2\

Sensys Networks, Inc.
Uninstall
Cancel

Figure 3.12: Uninstall TrafficDOT Window

2. *Close the uninstall window* – After the software removal process runs, click *Close* on the *Uninstall TrafficDOT* window to end the task.


TrafficDOT-1.10.0-2 Uninstall
Uninstallation Complete
Uninstall was completed successfully.
Completed

```
Delete file: C:\Program Files\Sensys Networks\TrafficDOT-1.10.0-2\libexec\jsch-0.1....
Delete file: C:\Program Files\Sensys Networks\TrafficDOT-1.10.0-2\libexec\log4j-1.2...
Delete file: C:\Program Files\Sensys Networks\TrafficDOT-1.10.0-2\libexec\mail.jar
Delete file: C:\Program Files\Sensys Networks\TrafficDOT-1.10.0-2\libexec\RXTXcom...
Delete file: C:\Program Files\Sensys Networks\TrafficDOT-1.10.0-2\libexec\spring.jar
Remove folder: C:\Program Files\Sensys Networks\TrafficDOT-1.10.0-2\libexec\
Delete file: C:\Program Files\Sensys Networks\TrafficDOT-1.10.0-2\RunTrafficDot.exe
Delete file: C:\Program Files\Sensys Networks\TrafficDOT-1.10.0-2\sensysicon.ico
Delete file: C:\Program Files\Sensys Networks\TrafficDOT-1.10.0-2\trafficdot.jar
Delete file: C:\Program Files\Sensys Networks\TrafficDOT-1.10.0-2\uninstall.exe
Remove folder: C:\Program Files\Sensys Networks\TrafficDOT-1.10.0-2\
Completed
```

Figure 3.13: Closing Uninstall Window

3.3 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 Sensys 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 management server)

Configuration settings are made via TrafficDOT's GUI from the Access Point which, in turn, stores the settings in its local flash memory and/or transmits them to remote Sensors and Repeaters via the RF channel and to controller interface cards via the required cabling.

3.3.1 Configuration Functions

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

- Connecting to and disconnecting from an Access Point
- Discovering the network's topology
- Configuring an Access Point
- Configuring Sensors
- Configuring Repeaters
- Configuring Contact Closure cards[15]
- Configuring System properties

Each function is described in the sections that follow.

3.3.2 Management Functions

TrafficDOT contains other functions that are not related to configuration; some of these will be covered in this chapter. The management functions discussed in this guide are as follows:

- Rebooting an Access Point
- Updating an Access Point's firmware
- Backing up and restoring an Access Point's configuration
- Reviewing the processes executing on an Access Point
- Updating an Access Point's license file

3.4 Connecting to an Access Point

To configure and manage equipment in a Sensys network, a TCP/IP connection must be made between the TrafficDOT software application and the network's Access Point. TrafficDOT may be connected to only one Access Point at any given time.

3.4.1 Procedure

Connecting to an Access Point can occur (*i*) as a part of starting TrafficDOT or (*ii*) via the *Connect* command and *Connect* window.

---

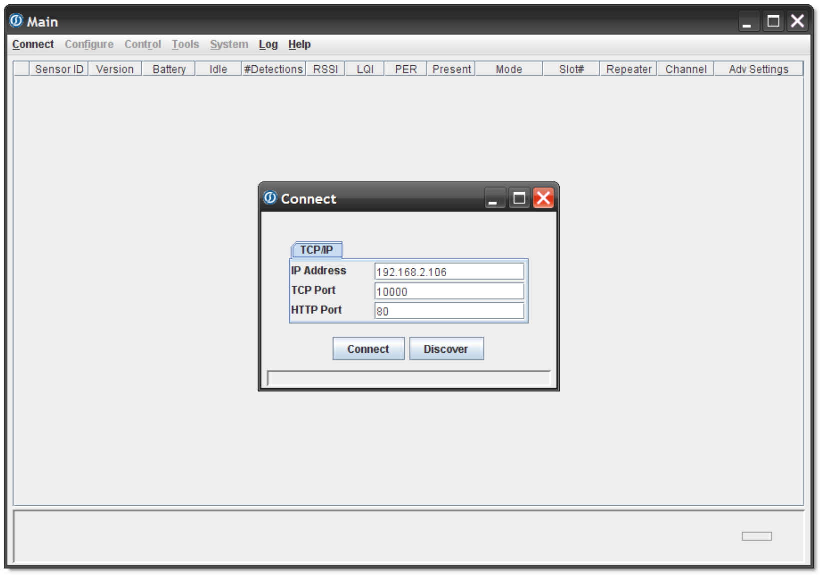
[15] Configuring Sensys Contact Closure cards is described in the document *Sensys Networks Contact Closure Card Installation Guide*.

3.4.1.1 Connecting at Start-up of TrafficDOT

Connect to the Access Point with TrafficDOT by following these steps:

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

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



IP Address 192.168.2.106
TCP Port 10000
HTTP Port 80

Figure 3.14: Connect Window

The *Connect* window designates the Access Point to which you will connect. Identify the Access Point by supplying values to both of the fields and click *Connect*.

3.4.1.1.1 Connect Window Contents

The *Connect* window collects data that identifies the Access Point to which TrafficDOT will connect. The window elements are shown below:

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.

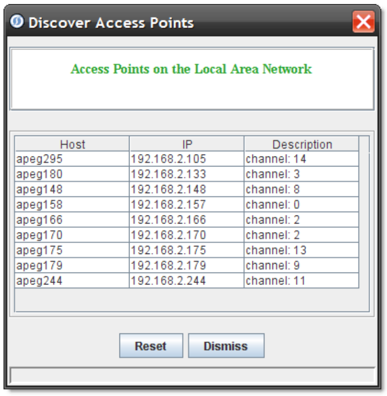
Table 27: Connect window fields

The *Connect* window “remembers” the most recent use of TrafficDOT. Therefore, values may already appear in the window.

If you do not know the IP address of the Access Point, click the *Discover* button.

3.4.1.1.2 Discovering Access Points

The *Discover* button queries the local network and opens a window that lists all Access Points on the network.



Host	IP	Description
apeg295	192.168.2.105	channel: 14
apeg180	192.168.2.133	channel: 3
apeg148	192.168.2.148	channel: 8
apeg158	192.168.2.157	channel: 0
apeg166	192.168.2.166	channel: 2
apeg170	192.168.2.170	channel: 2
apeg175	192.168.2.175	channel: 13
apeg179	192.168.2.179	channel: 9
apeg244	192.168.2.244	channel: 11

Figure 3.15: Discover APs Window

Make a note of the IP address of the Access Point you wish to connect to. Click *Dismiss* to close the window and return to the *Connect* window.

3.4.1.1.3 Discover Access Points Window Contents

The *Discover Access Points* window displays the Access Point ID (in the *Host* column), the IP address, and RF channel of each Access Point on the local network. It allows the following operations:

- *Reset* – sends a reset command to a selected Access Point.

  This directs the Access Point to reconfigure itself to the factory default IP address of `192.168.2.100` and network mask of `255.255.255.0`.

  (*Note*: you must first select an Access Point by clicking anywhere in its row.)

- *Dismiss* – closes the window.

Note: The Discover Access Points window doesn't allow you to connect to Access Points. Record the IP address of the Access Point you want to connect to, close the window and then type the IP address into the Connect window.

3.4.1.2 Connecting via the *Connect* menu

At anytime during a TrafficDOT session, you may connect to a different Access Point by doing the following:

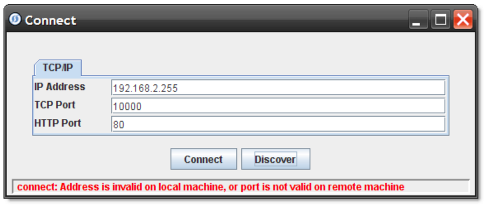
1. Disconnect from the current Access Point by clicking *Disconnect* from the *Connect* menu.

2. Click *Connect* from the *Connect* menu.

   The *Connect* window appears. Follow the instructions in the prior section to *Discover* Access Points and/or connect to an Access Point.

3.4.1.3 Connection Failure Display

If a connection cannot be made, the result is indicated along the bottom of the *Connect* window as shown below:



IP Address: 192.168.2.255
TCP Port: 10000
HTTP Port: 80

connect: Address is invalid on local machine, or port is not valid on remote machine

Figure 3.16: Connect Window Error Message

Correct the IP address and port number and click *Connect* again.

3.5 Exiting TrafficDOT

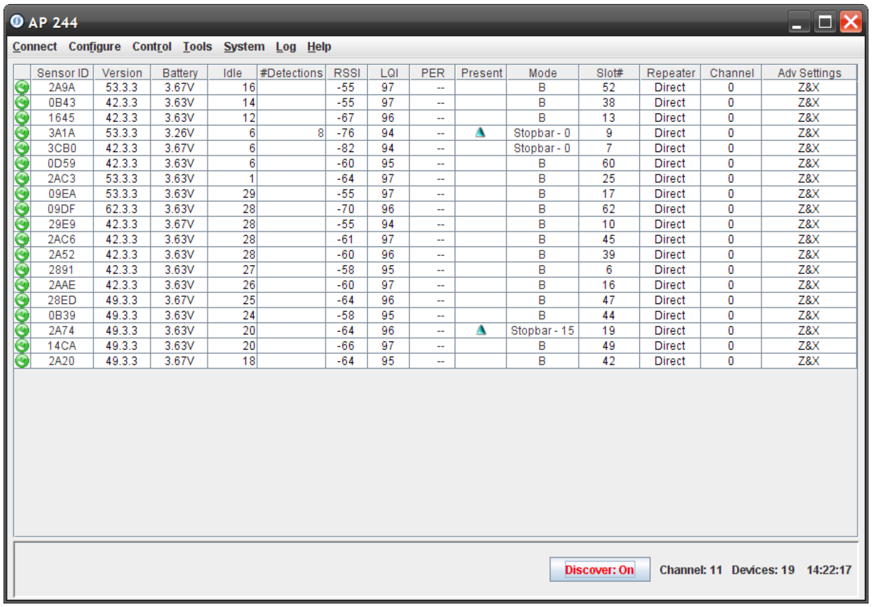
To end a TrafficDOT session, do the following:

1. From the *Connect* menu, click *Disconnect*.
2. Click *Exit* from the *Connect* menu.

Alternatively, you can terminate TrafficDOT by clicking the close window control in the upper right-hand corner of the *Access Point Main* window.

3.6 Using the Access Point Main Window

The *Main* window is the main workspace of the TrafficDOT application. The window 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.



	Sensor ID	Version	Battery	Idle	#Detections	RSSI	LQI	PER	Present	Mode	Slot#	Repeater	Channel	Adv Settings
●	2A9A	53.3.3	3.67V	16		-55	97	--		B	52	Direct	0	Z&X
●	0B43	42.3.3	3.63V	14		-55	97	--		B	38	Direct	0	Z&X
●	1645	42.3.3	3.63V	12		-67	96	--		B	13	Direct	0	Z&X
●	3A1A	53.3.3	3.26V	6	8	-76	94	--	▲	Stopbar - 0	9	Direct	0	Z&X
●	3CB0	42.3.3	3.67V	6		-82	94	--		Stopbar - 0	7	Direct	0	Z&X
●	0D59	42.3.3	3.63V	6		-60	95	--		B	60	Direct	0	Z&X
●	2AC3	53.3.3	3.63V	1		-64	97	--		B	25	Direct	0	Z&X
●	09EA	53.3.3	3.63V	29		-55	97	--		B	17	Direct	0	Z&X
●	09DF	62.3.3	3.63V	28		-70	96	--		B	62	Direct	0	Z&X
●	29E9	42.3.3	3.67V	28		-55	94	--		B	10	Direct	0	Z&X
●	2AC6	42.3.3	3.63V	28		-61	97	--		B	45	Direct	0	Z&X
●	2A52	42.3.3	3.63V	28		-60	96	--		B	39	Direct	0	Z&X
●	2891	42.3.3	3.63V	27		-58	95	--		B	6	Direct	0	Z&X
●	2AAE	42.3.3	3.63V	26		-60	97	--		B	16	Direct	0	Z&X
●	28ED	49.3.3	3.67V	25		-64	96	--		B	47	Direct	0	Z&X
●	0B39	49.3.3	3.63V	24		-58	95	--		B	44	Direct	0	Z&X
●	2A74	49.3.3	3.63V	20		-64	96	--	▲	Stopbar - 15	19	Direct	0	Z&X
●	14CA	49.3.3	3.63V	20		-66	97	--		B	49	Direct	0	Z&X
●	2A20	49.3.3	3.67V	18		-64	95	--		B	42	Direct	0	Z&X

Figure 3.17: TrafficDOT Main Window

The window serves as a central console for managing a Sensys network. From here you can:

- Connect to / Disconnect from Access Points
- Discover the topology of a Sensys network
- Configure network devices including Sensys Sensors, Access Points, Repeaters and Contact Closure cards
- Manage Sensor location and Sensor-Pair reference tables
- Apply firmware updates to any devices
- Configure and manage system parameters
- Generate real-time detection graphs and charts
- Reboot an Access Point
- Backup / Restore an Access Point's configuration
- Send management commands to an Access Point, review its command log, and access its command-line interface
- Generate a list of processes executing on an Access Point

- Rename Sensors
- Use an RF channel scan tool to discover Sensys equipment communicating on a channel other than the channel used by the Access Point
- Inspect the license file
- Access help and support information

3.6.1 Contents of the Access Point Main Window

The window 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
- *Status Line* – summary information regarding the current connection, toggle control for *Discovery* mode

Each area is discussed in more detail in the sections that follow.

3.6.1.1 Menus

Menus organize related commands and functions into logical groups. All TrafficDOT operations are invoked via menu selections.

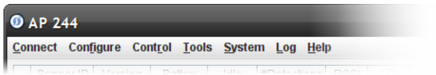


Figure 3.18: TrafficDOT Menu Bar

The menus of the *Access Point Main* window include:

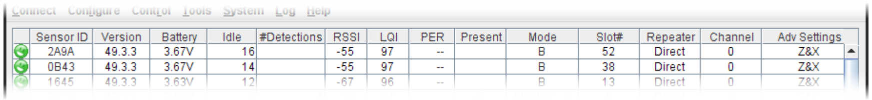
- *Connect* – provides connect/disconnect operations, options for display control, virtual private network (VPN) commands and exiting the program.
- *Configure* – consists of individual configuration options, dot table maintenance options, user preferences and a command to write configuration settings to flash memory.
- *Control* – provides a means to run a specific management command and reboot an Access Point.
- *Tools* – provides options for downloading firmware to Sensors, Repeaters and Contact Closure cards, renaming Sensors, performing an RF channel scan, generating real-time detection charts and useful functions.
- *System* – provides options for global system configuration, management of Access Point configuration files (including backup, restore and

formatting for transmittal to Sensys Networks technical support), updates to Access Point firmware, license file query, and special Access Point functions.

- *Log* – provides access to the command history log.
- *Help* – provides options to confirm the software version and access online help and support files.

3.6.1.2 System Display

The window displays real-time device and detection information for the entire network in a tabular format. Each row represents a discrete device – either a Sensor (including Sensors that communicate to the Access Point through a Repeater) or a Repeater.



	Sensor ID	Version	Battery	Idle	#Detections	RSSI	LQI	PER	Present	Mode	Slot#	Repeater	Channel	Adv Settings
●	2A9A	49.3.3	3.67V	16		-55	97	--		B	52	Direct	0	Z&X
●	0B43	49.3.3	3.67V	14		-55	97	--		B	38	Direct	0	Z&X
●	1645	49.3.3	3.63V	12		-67	96	--		B	13	Direct	0	Z&X

Figure 3.19: Columns of TrafficDOT's Main window

Detection counts, detection events, RF quality metrics, version and battery information are shown in dedicated columns updated at one second intervals. The columns of the display are identified in the table below and discussed further in the sections that follow:

Column Name	**Description**
<none>	Visual indication of the device's health.
Sensor 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.
Version	The firmware version on the device. (*Note*: use the *VDS Release Notes* [P/N 152-240-001-006] from Sensys Networks to cross references firmware version ids to VDS releases.)
Battery	An estimate of the remaining battery life, expressed in volts.
Idle	The number of seconds since the latest packet was received from the device
# Detections	Total number of detections since the Sensor established a connection to the Access Point. (See the notes below for information about other uses of this column.)
RSSI	Received Signal Strength Indicator – a measure of the radio signal strength
LQI	Line Quality indicator – a statistical measure of the radio link quality
PER	Packet Error Rate – a statistical measure of the data loss due to errors, dropped packets, noise, etc.
Present	A graphical indication of the state of detection of the Sensor.
Mode	The operating mode of the device.
Slot#	The time slot on the Access Point used by the Sensor or Repeater.
Repeater	The device id of the Repeater servicing a Sensor (if applicable). *Direct* indicates a Sensor is transmitting to the Access Point without using a Repeater.
Channel	The RF channel on which the device is transmitting
Adv Settings	Advanced Settings – depicts a Sensor's settings regarding linear filter and axis detection.

Table 28: Descriptions of Columns on TrafficDOT's Main Window

3.6.1.2.1 Sorting the Display

Click a column heading to sort the display in ascending order on the data in the coumn whose heading is clicked.

3.6.1.3 Understanding the Contents of the System Display

3.6.1.3.1 Device Health Indicator

A colored icon visually represents the overall health of the device.

Icon	State	Description
🟢	OK	RF communications are healthy; devices are operating normally.
🟡	Monitor	RF communications are sub-standard. Monitor the situation because in many cases this is transient; no specific end-user action is called for.
🔴	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 29: TrafficDOT Device Health Indicators

3.6.1.3.2 SensorID

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 Sensor ID can be aliased or renamed subject to Sensys defined naming rules. Renaming a Sensor can be advantageous when devices are physically replaced but detection history must be retained. (See the section *Setting Sensor Ids* in the *Network Management* chapter for more information.)

3.6.1.3.3 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.

3.6.1.3.4 Battery

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

Note: system firmware and TrafficDOT versions released after Q2 2008 will change the background color of this element to solid red for Repeaters whose battery or battery packs require replacement.

3.6.1.3.5 Idle

Displays the number of seconds since a packet from the device was received by the Access Point.

3.6.1.3.6 # Detections

Total number of detections since TrafficDOT connected to the Access Point.

3.6.1.3.7 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. (See *Setting System Preferences* below for more information.)

3.6.1.3.8 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. (See *Setting System Preferences* below for more information.)

3.6.1.3.9 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.

3.6.1.3.10 Present

Current state of detection. A detection is represented by the presence of the detection icon (a blue triangle). The absence of an icon indicates no detection.

3.6.1.3.11 Mode

The operating mode of the device. Sensors are displayed as using one of the supported Sensor operating modes (See the section *Wireless Sensors* in the *System Description* chapter for more information.)

A value of "RP" in this column indicates the device is a Repeater.

3.6.1.3.12 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.

3.6.1.3.13 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

3.6.1.3.14 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[16], and
- the value to the right of separator represents the channel the Repeater uses to reach the Sensors it services[17].

---

[16] Or upstream Repeater in the case of tandem Repeaters.

[17] Or downstream Repeater in the case of tandem Repeaters.

3.6.1.3.15 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. (*Note*: this column relates only to Sensors.)

3.6.1.4 Status Line

Summary information regarding the connection session appears in the status area in the botom-right corner of the window.

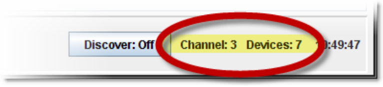


Figure 3.20: TrafficDOT status area

The information includes the RF channel of the Access Point, the number of devices in the network, and the current time acquired from the Access Point. In addition, a command button to the left of the status information serves as a control for enabling or disabling *Discovery* mode on the Access Point.

3.6.1.5 Understanding Discovery Mode

Discovery mode directs all network devices communicating with the Access Point to include additional information in the data packets they send. The additional data populates the following columns in the *Access Point Main* window:

- Version
- Battery
- Repeater
- Channel

The command button operates as a “toggle” switch. Click the button to enable or disable *Discovery* mode. The button's label changes to indicate the current state of *Discovery* mode.

3.6.1.5.1 Uses for Discovery Mode

Use *Discovery* mode to understand the topology of an installed network. However, because *Discovery* requires all devices to transmit additional data to the Access Point, operating a network continuously in this mode is not recommended.

Note, however, that *Discovery* mode is required for utility operations such as firmware updates and scanning for Sensys equipment on RF channels other than the channel of the Access Point.

3.6.2 Clearing the Window

The contents of the window can be refreshed with a command from the *Tools* menu.

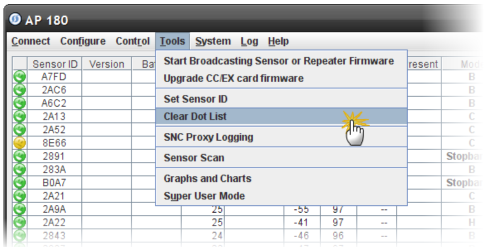


Figure 3.21: TrafficDOT Tools Menu

Click the command *Clear Dot List* to clear and repopulate the display.

3.6.3 Closing Open Windows

TrafficDOT allows multiple windows to be open concurrently, provided that each window corresponds to a different menu command. Only one window per command may be open.

Use *Connect* / *Hide All* to close all open windows except for the *Access Point Main* window.

3.7 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
- Settings Sensor's RF channel
- Sending a recalibration command to a Sensor
- Using advanced settings
- Updating Sensor firmware
- Reaching Sensors that are not transmitting
- Performing other operations

3.7.1 Introduction

Sensor configuration involves 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.

3.7.1.1 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. See *Selecting Sensors to Configure* below.

3.7.1.2 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.

3.7.2 Starting Work

To work with Sensors, access the *Configure* menu and click *Sensors*.

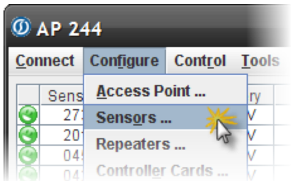
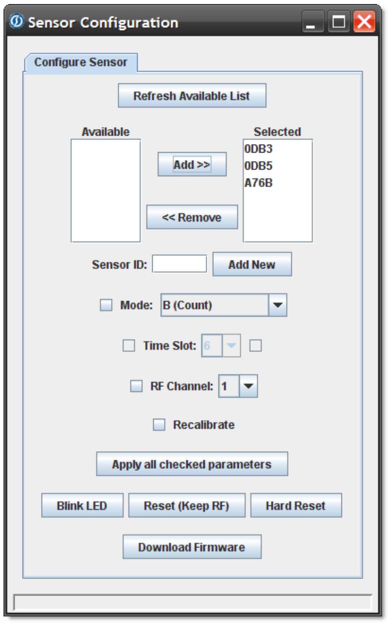


Figure 3.22: Configure / Sensors

The *Sensor Configuration* window appears.



Selected: 0DB3, 0DB5, A76B

☐ Mode: B (Count)

☐ Time Slot: 6 ☐

☐ RF Channel: 1

☐ Recalibrate

Figure 3.23: Sensor Configuration Window

3.7.3 Selecting Sensors to Configure

Configuration operations are performed on one or more Sensors in a network. Before proceeding, the Sensor(s) that are the target of the configuration commands must be designated. This is accomplished by populating the scrolling list area labeled *Selected* with the Sensor IDs of the target Sensor(s).

3.7.3.1 Available Sensors

The Sensors in a network that listen/transmit on the RF channel of the Access Point, or are associated with a Repeater that communicates to the Access Point on that RF channel, appear in a scrolling list area labeled *Available*.

The list of Sensors is refreshed when the *Sensor Configuration* window is opened. Additionally, you can refresh the list at any time by clicking *Refresh Available list*.

3.7.3.2 Selecting and De-selecting Sensors

Sensors are selected by moving their IDs from the *Available* list to the *Selected* list as follows:

1. From the *Available* list, click one or more Sensor IDs. (Note: on MS Windows platforms hold down the SHIFT key while clicking to select multiple entries.)
2. Click the button labeled *Add* >>. The Sensor ID(s) appear in the *Selected* list.

To remove IDs from the *Selected* list, do the following:

1. From the *Selected* list, click one or more Sensor IDs.
2. Click << Remove. The Sensor ID(s) are removed from the Selected list and appear in the Available list.

3.7.3.3 Manually Adding a Sensor to the Selected List

On rare occasions, a Sensor may revert to a passive state. While still listening to its associated Access Point or Repeater, it does not transmit. In these cases, the Sensor does not appear on the available list and thus cannot be moved to the *Selected* list. See *Reaching Sensors That Are Not Transmitting* below for more information.

3.7.4 Applying Configuration Changes and Sending Commands

3.7.4.1 Applying Configuration Changes

The configuration attributes to be changed are designated by filling the selection check box to the left of each attribute, supplying a value for the attribute, and clicking *Apply all checked parameters*. Configuration changes are applied to each of the Sensors on the *Selected* list.

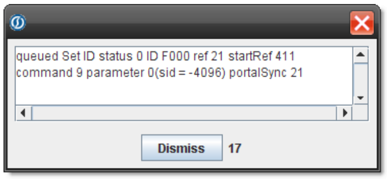
3.7.4.2 Sending Management Commands

Management commands are sent to each of the Sensors on the *Selected* list by clicking the appropriate command button.

Note: an exception to the above is made for the command that directs a Sensor to recalibrate. The Recalibration command includes a parameter (number of seconds) and is presented on the window like a configurable attribute. See Sending a Recalibration Command to a Sensor for more information.

3.7.4.3 Tracking Results

In the case of applying a configuration change and sending a management command to one or more Sensors, a command transmission window such as the one below appears.



```
queued Set ID status 0 ID F000 ref 21 startRef 411
command 9 parameter 0(sid = -4096) portalSync 21
```

Figure 3.24: Command transmission window

Note that this window confirms only that the command is queued for communication to the target devices; it does *not* report the results of the command as it is processed by the devices.

The integer to the right of the *Dismiss* button counts down the seconds until the command is transmitted over the Access Point's radio. This is for informational purposes only as the command is queued and transmitted automatically. Click *Dismiss* at any time to close the window.

3.7.5 Setting a Sensor's Operating Mode

The Sensor's operating mode defines the type of detection data it transmits. (See the section on *Sensor operations* of the *System Description* chapter for more information.)

To set the operating mode, do the following:

1. Fill the check box to the left of the label *Mode* by clicking it.
2. The entries on the *Mode* drop-down list are the operating modes available for Sensors. Select an entry from the list by clicking it.

   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 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.

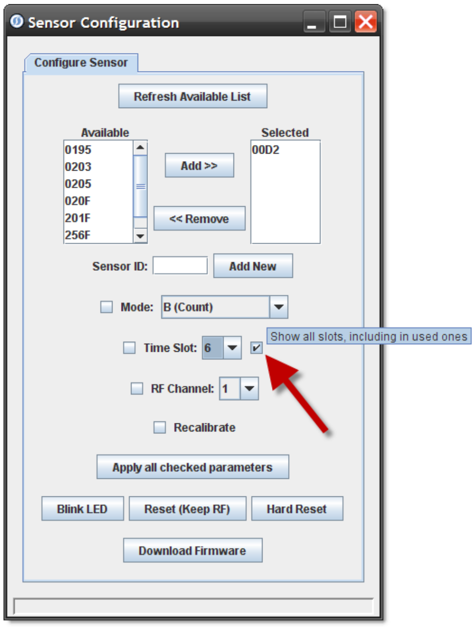
3. Click *Apply all checked parameters*.

3.7.6 Assigning a Sensor's Time Slot

Each Sensor uses one and 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.

To set the time slot, do the following:

1. Fill the check-box to the left of the label *Time Slot* by clicking it.
2. Choose a value from the *Time Slot* drop-down list.



Available: 0195, 0203, 0205, 020F, 201F, 256F

Selected: 00D2

Sensor ID:

☐ Mode: B (Count)

☐ Time Slot: 6 ☑ Show all slots, including in used ones

☐ RF Channel: 1

☐ Recalibrate

Figure 3.25: Enabling Display of All Time Slots

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), fill the check-box to the right of the *Time Slot* drop-down list as shown below

The list does not include time slots that are, by definition, reserved for use by Access Points. (See the *Time Slots* discussion in *System Description* chapter for more.)

3. Click *Apply all checked parameters*.

> *Note: Because time slots assigned to Sensors must be unique, ensure that only one Sensor has been selected for this operation. If a time slot is assigned to more than one device, the conflict will be displayed in red on TrafficDot's **Main** window.*

3.7.7 Setting a Sensor's RF Channel

All Sensors associated with an Access Point must use the same frequency as the Access Point; all Sensors associated with a Repeater must use the same frequency designated as the *Sensor channel* on that Repeater.

To set the RF channel, do the following:

1. Fill the check-box to the left of the label *RF Channel* by clicking it.
2. 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.

3. Click *Apply all checked parameters*.

3.7.8 Sending a Recalibration Command to 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 wish to request a Sensor to recalibrate. To accomplish this, do the following:

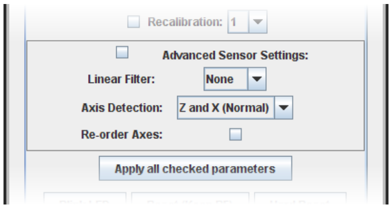
1. Fill the check-box to the left of the label *Recalibration* by clicking it.
2. The entries in the *Recalibration* drop-down list are the number of seconds before the command is executed by the Sensor. Select an entry from the list by clicking it.

   Note: values range from 1 to 30 seconds.

3. Click *Apply all checked parameters*.

3.7.9 Using Advanced Sensor Settings

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.



☐ Recalibration: 1

☐ Advanced Sensor Settings:

Linear Filter: None

Axis Detection: Z and X (Normal)

Re-order Axes: ☐

Figure 3.26: Advanced Sensor Settings

To configure advanced Sensor settings, do the following:

1. Put the TrafficDOT session into *Advanced Mode*. This is done via the *Preference* window found on the *Configure* menu. (See the section *Setting System Preferences* for information on how to set and use preferences.)
2. Open the *Sensor Configuration* window.
3. Fill the check-box *Advanced Sensor Settings*.
4. Set the properties that are appropriate to your environment. (See *Notes* below.)
5. Click *Apply All Checked Parameters* and close the window.

Advanced Settings override global settings found on the *Detection* tab of the *Access Point Configuration* window.

Note: the Advanced Sensor settings change fundamental properties of the Sensor; use them only after consultation with Sensys Networks.

3.7.9.1 Notes

The *Advanced Settings* elements are as follows:

3.7.9.1.1 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.

3.7.9.1.2 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.

3.7.9.1.3 Re-order 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.

This element can be enabled independently of other advanced settings.

3.7.10 Updating Sensor Firmware

Updates to Sensor firmware are sent from the Access Point via the wireless communication channel. The procedure is a two-part process consisting of the following activities:

- Setting up the Access Point to download firmware
- Setting up Sensors to receive a firmware image

> *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.

3.7.10.1 Pre-Update Considerations

Consider these ramifications of firmware update operations before proceeding:

1. *Effect on vehicle detection* – during a Sensor firmware update operation detection is suspended on the Sensors receiving the firmware image. Additionally, updating the firmware of a Repeater effectively suspends the detection capability of Sensors downstream of the Repeater[18] or Sensors serviced by a tandem repeater downstream of the Repeater being updated.
2. *Effect on signal control channels* – CC and EX cards receiving detections from Sensors directly involved in a firmware update, or Sensors downstream of a Repeater involved in a firmware update will receive a constant call for the duration of the update operation.
3. *Effect on Access Point* – the Access Point maintains all standard processes and capabilities during an update operation.
4. *Scope of firmware updates* – in regard to Repeaters and Sensors only, an Access Point broadcasts the new firmware image via its wireless radio; only one image can be broadcast at a time. Thus, Repeaters must be updated in a separate operation from Sensors. Additionally, the two types of Sensors (F-type and T-type) must be updated in separate operations.

> *Note*: Sensys Networks recommends applying firmware updates first to Sensors, then to Repeaters, and then to the Access Point.

3.7.10.2 Procedure

To update Sensor firmware, do the following:

---

[18] Note: we say *effectively* because the downstream Sensors are not directly involved in a Repeater update operation, but by definition, those Sensors lose their communication path to the Access Point.

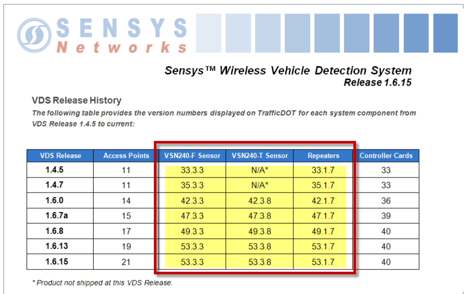
1. Determine the sensor type for the devices whose firmware will be updated. Use the table below as a guide.

Sensor Type	Use	Image File Name
VSN240-F	Flush-mount wireless sensor; freeways, arterials, traffic signal control	dot.ldrec
VSN240-T	Flush-mount wireless sensor; traffic signal control only	dotstopbar.ldrec

Table 30: VDS240 Sensor Types

> *Note*: always use the correct firmware image associated with each sensor type. If the type of the target device(s) cannot be determined, do not proceed and contact Sensys Networks Technical Support for assistance. Additionally, only one type of Sensor can be updated at a time.

2. Determine the *version id* of the firmware image you intend to download to the Sensors. This information is available in the *Release Notes* document that accompany each release of the Sensys VDS 240 software. This information will be used to confirm the update procedure at the end of this procedure.



Sensys™ Wireless Vehicle Detection System
Release 1.6.15

VDS Release History

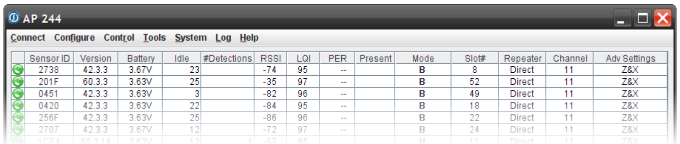
The following table provides the version numbers displayed on TrafficDOT for each system component from VDS Release 1.4.5 to current:

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

** Product not shipped at this VDS Release.*

Figure 3.27: VDS240 Release Notes

3. Start TrafficDOT and connect to the Access Point servicing the Sensors whose firmware will be updated. Allow the window to fully populate and make a note of the data displayed in the *Version* and *Mode* column of each Sensor whose firmware will be updated.

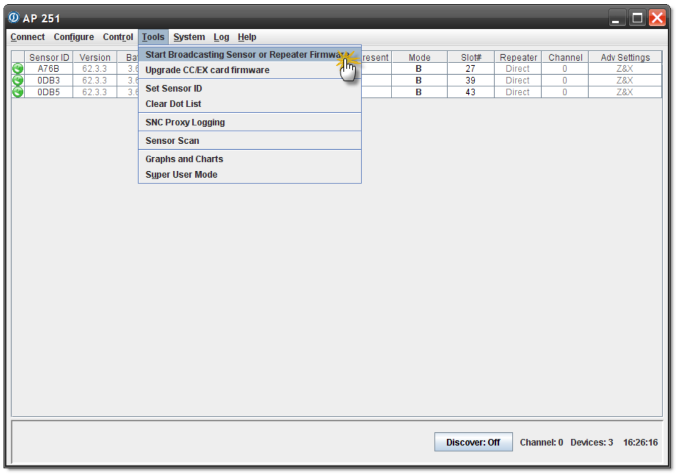


Sensor ID	Version	Battery	Idle	#Detections	RSSI	LQI	PER	Present	Mode	Slot#	Repeater	Channel	Adv Settings
2738	42.3.3	3.67V	23		-74	95	--		B	8	Direct	11	Z&X
201F	60.3.3	3.63V	25		-35	97	--		B	52	Direct	11	Z&X
0451	42.3.3	3.63V	3		-82	96	--		B	49	Direct	11	Z&X
0420	42.3.3	3.63V	22		-84	95	--		B	18	Direct	11	Z&X
256F	42.3.3	3.63V	25		-86	96	--		B	22	Direct	11	Z&X
2707	42.3.3	3.67V	12		-72	97	--		B	24	Direct	11	Z&X
1CE4	60.3.14	3.63V	12	1	-57	95	--		H	11	Direct	11	Z&X

Figure 3.28: Record version and mode settings beforehand

4. From the *Tools* menu of the *Access Point Main* window, click *Broadcast Sensor or Repeater Firmware*. This places the Access Point into a special mode used to broadcast firmware images over the wireless radio channel.

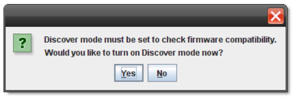
> *Note*: vehicle detections are not processed by the Access Point when it is operating in firmware broadcast mode.



Sensor ID	Version	Ba	resent	Mode	Slot#	Repeater	Channel	Adv Settings
A76B	62.3.3	3.6		B	27	Direct	0	Z&X
0DB3	62.3.3	3.6		B	39	Direct	0	Z&X
0DB5	62.3.3	3.6		B	43	Direct	0	Z&X

Figure 3.29: Put Access Point into firmware broadcast mode

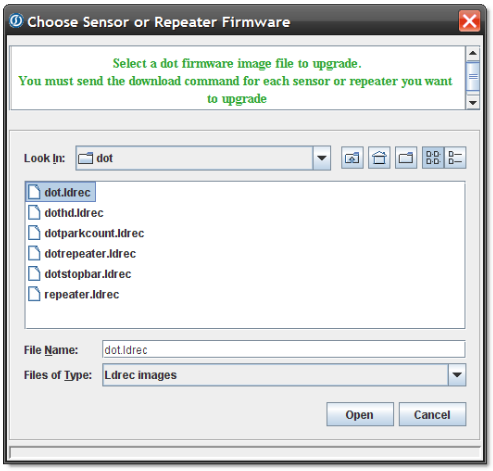
5. TrafficDOT confirms that the *Discover* mode is enabled before proceeding. If it is not, a window appears to enable it. Click *Yes* to continue; the *Choose Sensor or Repeater Firmware* window opens.



Discover mode must be set to check firmware compatibility.
Would you like to turn on Discover mode now?

Figure 3.30: Enable Discovery

6. Designate the firmware image file to broadcast and click *Open*.



Select a dot firmware image file to upgrade.
You must send the download command for each sensor or repeater you want to upgrade

Look In: dot

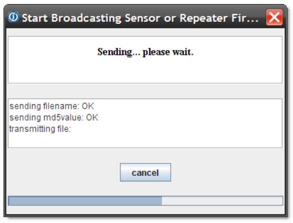
dot.ldrec
dothd.ldrec
dotparkcount.ldrec
dotrepeater.ldrec
dotstopbar.ldrec
repeater.ldrec

File Name: dot.ldrec
Files of Type: Ldrec images

Figure 3.31: Select the image file to broadcast

Be certain to select the firmware image file appropriate for the Sensors to be updated. Refer to *Table 30* above for more information.

The *Start Broadcasting Sensor or Repeater Firmware* window appears. This window displays a progress bar that tracks the transfer of the image file from the computer running TrafficDOT to the Access Point.

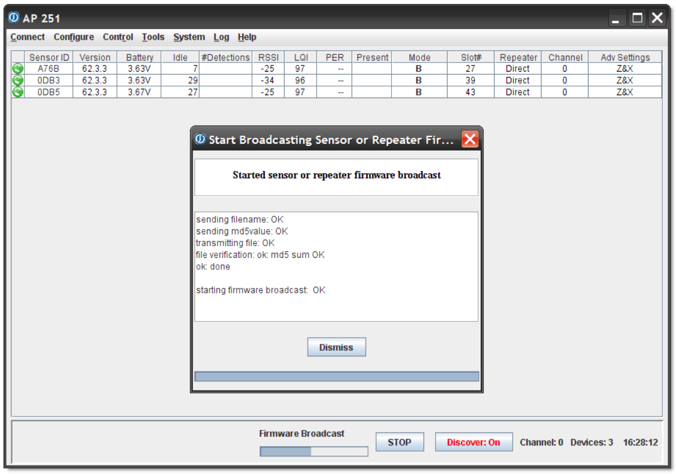


Sending... please wait.

```
sending filename: OK
sending md5value: OK
transmitting file:
```

Figure 3.32: Transfer progress bar

7. When the file transfer is complete (the progress bar is fully colored-in), confirm that the TrafficDOT's *Main* window displays the *Firmware Broadcast* indicator at the bottom of the window.


AP 251
Connect Configure Control Tools System Log Help
Start Broadcasting Sensor or Repeater Fir...
Dismiss
Firmware Broadcast
STOP
Discover: On
Channel: 0 Devices: 3 16:28:12

	Sensor ID	Version	Battery	Idle	#Detections	RSSI	LQI	PER	Present	Mode	Slot#	Repeater	Channel	Adv Settings
	A76B	62.3.3	3.63V	7		-25	97	--		B	27	Direct	0	Z&X
	0DB3	62.3.3	3.63V	29		-34	96	--		B	39	Direct	0	Z&X
	0DB5	62.3.3	3.67V	27		-25	97	--		B	43	Direct	0	Z&X

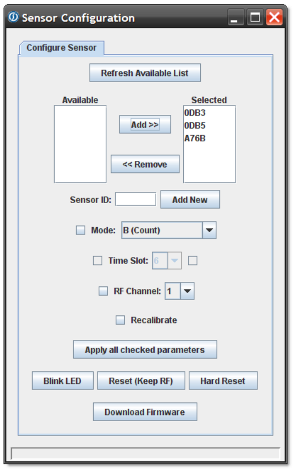
Started sensor or repeater firmware broadcast

```
sending filename: OK
sending md5value: OK
transmitting file: OK
file verification: ok: md5 sum OK
ok: done

starting firmware broadcast:  OK
```

Figure 3.33: Animation confirms AP is broadcasting firmware

The animated *Firmware Broadcast* indicator confirms the Access Point as acquired an image file from the TrafficDOT computer and is transmitting it over its wireless radio. Click *Dismiss* to close the *Start Broadcasting Sensor or Repeater Firmware* window.

8. From TrafficDOT's *Configure* menu, open the *Sensor Configuration* window.



Selected: 0DB3, 0DB5, A76B

Sensor ID:

☐ Mode: B (Count)

☐ Time Slot: ☐

☐ RF Channel: 1

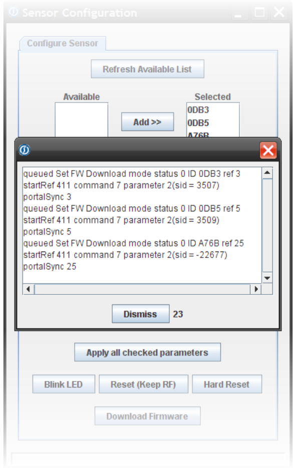
☐ Recalibrate

Figure 3.34: Select Sensors

9. Select one or more Sensors by moving the device ids from the *Available* list to the *Selected* list. (See *Selecting Sensors to Configure* above for more information.)

> *Note*: ensure that the type of Sensors selected matches the sensor type inferred by the firmware image selected earlier in the procedure.

10. Click *Download Firmware*. A TrafficDOT command status window appears and the designated Sensors are put into an operating mode to receive the firmware image being broadcast by the Access Point.

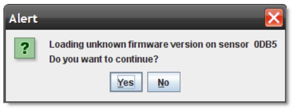


```
queued Set FW Download mode status 0 ID 0DB3 ref 3
startRef 411 command 7 parameter 2(sid = 3507)
portalSync 3
queued Set FW Download mode status 0 ID 0DB5 ref 5
startRef 411 command 7 parameter 2(sid = 3509)
portalSync 5
queued Set FW Download mode status 0 ID A76B ref 25
startRef 411 command 7 parameter 2(sid = -22677)
portalSync 25
```

Figure 3.35: Status window

Click *Dismiss* to close the command status window.

11. Depending on the version of the VDS firmware currently installed on the Sensor(s) selected for the firmware update, a verification window like the following may appear.

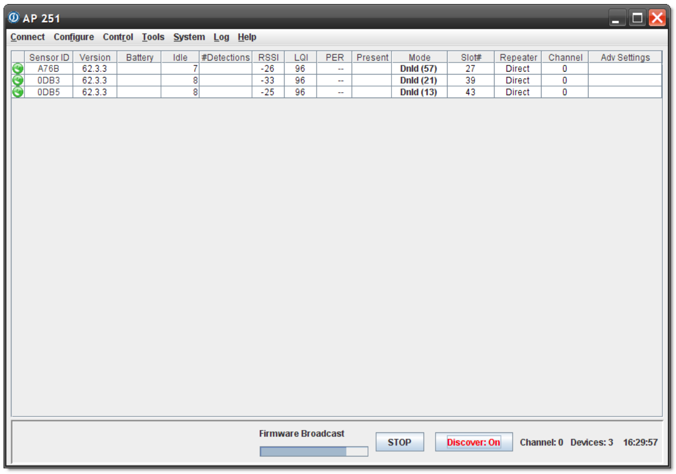


Loading unknown firmware version on sensor 0DB5
Do you want to continue?

Figure 3.36: Verification window

Click *Yes* to continue the operation. (*Note*: the window may appear multiple times depending on the firmware version of the target Sensors.)

12. Review the target Sensor(s) on TrafficDOT's *Main* window. Confirm that each Sensor designated for the firmware update is shown with the value "**DnId(####)**" in the *Mode* column, where **####** is an integer.



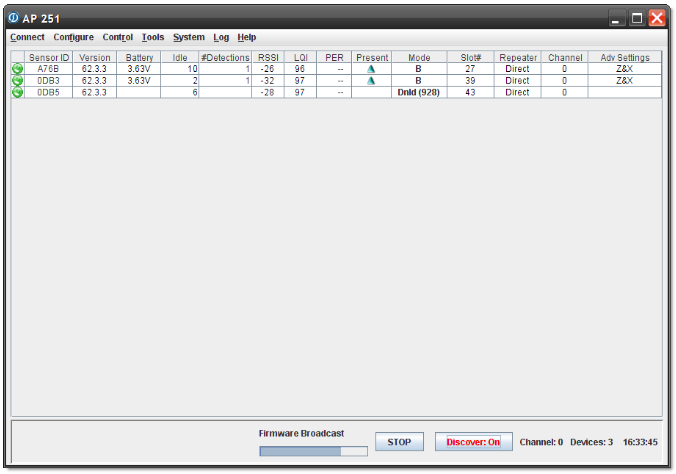
Sensor ID	Version	Battery	Idle	#Detections	RSSI	LQI	PER	Present	Mode	Slot#	Repeater	Channel	Adv Settings
A76B	62.3.3		7		-26	96	--		**Dnld (57)**	27	Direct	0	
0DB3	62.3.3		8		-33	96	--		**Dnld (21)**	39	Direct	0	
0DB5	62.3.3		8		-25	96	--		**Dnld (13)**	43	Direct	0	

Channel: 0 Devices: 3 16:29:57

Figure 3.37: Mode column indicates device receiving a firmware image

> *Note*: it is expected that the health indicator for each device will briefly turn red before the device begins receiving the firmware image.

13. Observe TrafficDOT's *Main* window to monitor the progress of the download operation. Sensors automatically resume normal operations after receiving and installing a new firmware image.


AP 251
Connect Configure Control Tools System Log Help
Firmware Broadcast
STOP
Discover: On
Channel: 0 Devices: 3 16:33:45

	Sensor ID	Version	Battery	Idle	#Detections	RSSI	LQI	PER	Present	Mode	Slot#	Repeater	Channel	Adv Settings
●	A76B	62.3.3	3.63V	10	1	-26	96	--	▲	B	27	Direct	0	Z&X
●	0DB3	62.3.3	3.63V	2	1	-32	97	--	▲	B	39	Direct	0	Z&X
●	0DB5	62.3.3		6		-28	97	--		Dnld (928)	43	Direct	0	

Figure 3.38: Devices resume operations automatically

After all Sensors have resumed normal operations, confirm the following for each Sensor:

- the data displayed in the *Version* column matches the expected value acquired from the *Release Notes* in step two above,
- the data displayed in the *Mode* column matches the mode as documented in step three above,
- The *RSSI* and *LQI* metrics are within acceptable ranges,
- the device health indicator indicates acceptable operating status (green)

When the Version, Mode, RSSI, LQI and Health Indicator display acceptable and expected value for all devices targeted for the firmware update, a successful operation is confirmed.

> *Note*: the amount of time required to perform a firmware update depends on multiple factors including the quality of the RF communication between the Access Point and the devices, the number of devices upgraded, the presence/use of Repeaters or tandem Repeaters, the size of the image, and other properties. The duration you experience may differ significantly from site to site. Sensys Networks recommends testing the process to establish a baseline.

14. After the operation has been confirmed, click *STOP* at the bottom of TrafficDOT's Main window. The Access Point is taken out of firmware image broadcast mode and resumes normal operations.

15. Disconnect from the Access Point and exit TrafficDOT.

3.7.10.3 Canceling a Firmware Update Operation

To cancel a firmware update operation before it completes, click *STOP* at the bottom of TrafficDOT's *Main* window.

3.7.10.4 Re-Running a Firmware Update Operation

Re-running a firmware update operation may be required if some devices fail to receive complete firmware images. (This may result of wireless communication errors.)

Running a firmware operation again is accomplished by repeating the procedure outline above in the section *Updating Sensor Firmware.*

3.7.11 Reaching Sensors That Are Not Transmitting

On occasion, a Sensor may not appear on the *Available* list in the *Sensor Configuration* window, yet still be “listening” on the network's RF channel. To reach a Sensor suspected to be in this state, manually insert its ID to the *Selected* list by doing the following:

1. Type the ID of the Sensor into the *Sensor ID* field.
2. Click the *Add New* button. (*Note*: This is not the same as the button *Add* >>.)

The Sensor ID appears in the *Selected* area. Then, perform a configuration or management operation in the normal manner described in this section.

Note: while the Sensor ID you supply is edited for appropriate form (that is, it must be a valid 4-character HEX string), TrafficDOT cannot not determine if a Sensor with such an identifier actually exists in your network. Be sure to use actual Sensor IDs.

3.7.12 Performing Other Operations

TrafficDOT's *Sensor Configuration* window includes other operations related to managing Sensors including:

- directing the Sensor to activate its light-emitting diode (LED)
- performing a “soft” reset
- performing a “hard” reset

These operations are not common. Perform them only when directed by Sensys Networks.

3.7.12.1 Activating the LED

(This feature is used for lab testing of Sensors only.)

3.7.12.2 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 accomplish a soft reset, select the Sensor and click the *Reset (Keep RF)* button.

3.7.12.3 Performing a Hard Reset

On occasion, 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.

See the section *Scanning RF Channels for Sensys Devices* for information about locating Sensys equipment communicating over any of the 16 supported RF channels.

To perform a hard rest, select the Sensor and click the *Hard Reset* button.

3.8 Configuring Access Points

An Access Point provides a central point of authority, device management, identification, and service definition for all Sensys network equipment.

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

3.8.1 Introduction

Access Point configuration 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.

3.8.2 Starting Work

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 configure an Access Point, access the *Configure* menu and click *Access Point*.

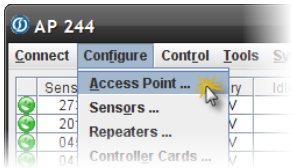
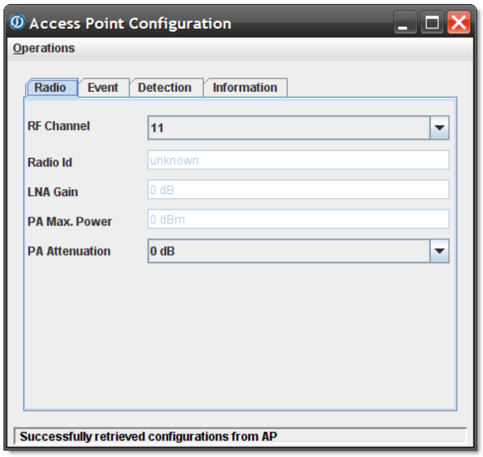


Figure 3.39: Configure menu

The *Access Point Configuration* window appears with the current configuration data loaded into its tabular display.



RF Channel: 11
Radio Id: unknown
LNA Gain: 0 dB
PA Max. Power: 0 dBm
PA Attenuation: 0 dB

Successfully retrieved configurations from AP

Figure 3.40: Access Point Configuration

3.8.2.1 Window Workflow and Operations

The *Access Point Configuration* window presents configurable elements via tabs. Each tab corresponds to a collection of Access Point properties. Typically, settings are reviewed or changed on all of the tabs and then the changes are applied to the Access Point. This is accomplished via the *Operations* menu.

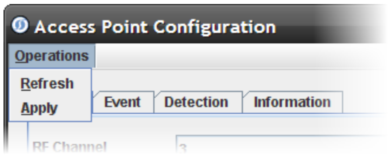


Figure 3.41: Access Point Operations menu

The *Operations* menu contains the following commands:

- *Refresh* – reacquires the current, active configuration from the Access Point

- *Apply* – applies the configuration element on the *Access Point Configuration* window to the Access Point, replacing its run-time configuration

3.8.2.1.1 Refresh command

Use the *Refresh* command to reload the current active configuration at any time.

3.8.2.1.2 Apply command

Note that *Apply* does not effect the Access Point's configuration saved in the device's flash memory. The Access Points reads its configuration from flash memory when it is powered on or rebooted.

3.8.2.1.3 Save command

To overwrite the configuration stored in flash memory, use the *Save* menu command from the *Access Point Main* window's *Configure* menu.

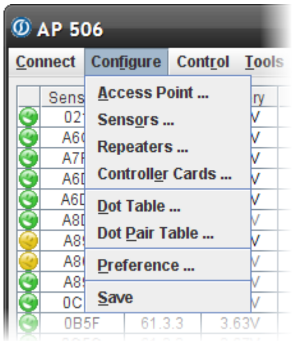


Figure 3.42: Configure menu

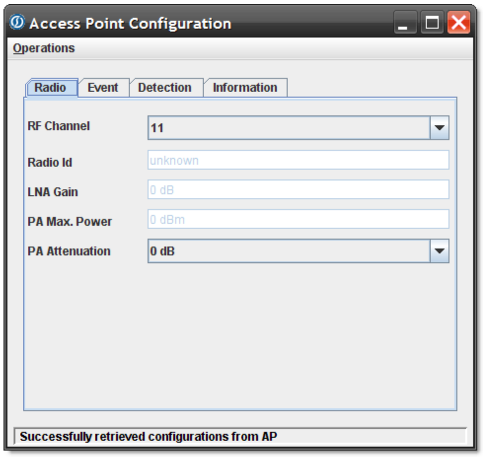
See the section *Saving the Configuration* below for more information.

3.8.3 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 two configurable elements:

- RF Channel
- PA Attenuation

The other elements are for reference only.



RF Channel: 11

Radio Id: unknown

LNA Gain: 0 dB

PA Max. Power: 0 dBm

PA Attenuation: 0 dB

Successfully retrieved configurations from AP

Figure 3.43: Access Point P Radio tab

3.8.3.1 Setting the RF Channel

To configure the RF channel, do the following:

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* from the *Operations* menu to apply the change or continue configuring the Access Point.

3.8.3.2 Setting the PA Attenuation

To configure the power amplifier attenuation, do the following:

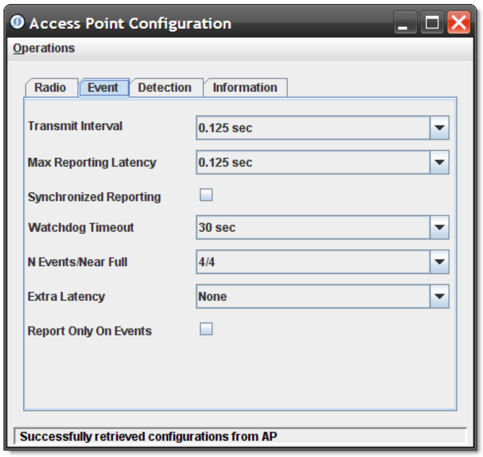
1. The entries in the *PA Attenuation* drop-down list provide a range of limiting values expressed in db. Select an entry from the list by clicking it.
2. Click *Apply* from the *Operations* menu to apply the change or continue configuring the Access Point.

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.

3.8.4 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	0.125 sec
Max Reporting Latency	0.125 sec
Synchronized Reporting	☐
Watchdog Timeout	30 sec
N Events/Near Full	4/4
Extra Latency	None
Report Only On Events	☐

Successfully retrieved configurations from AP

Figure 3.44: Access Point Event tab

3.8.4.1 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, do the following:

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 125 milliseconds.

2. Click *Apply* from the *Operations* menu to apply the change or continue configuring the Access Point.

3.8.4.2 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, do the following:

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

   Note: the factory default is 125 milliseconds.

2. Click *Apply* from the *Operations* menu to apply the change or continue configuring the Access Point.

3.8.4.3 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 *Max. Reporting Latency* (or multiple thereof) relative to the network's system clock maintained by the Access Point.

1. To enable synchronized reporting, fill the check box. To disable the function (the default setting), clear the check box.
2. Click *Apply* from the *Operations* menu to apply the change or continue configuring the Access Point.

3.8.4.4 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, do the following:

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* from the *Operations* menu to apply the change or continue configuring the Access Point.

3.8.4.5 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, do the following:

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* from the *Operations* menu to apply the change or continue configuring the Access Point.

3.8.4.6 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, do the following:

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* from the *Operations* menu to apply the change or continue configuring the Access Point.

3.8.4.7 Limiting Reporting to “On” (Detection) Events Only

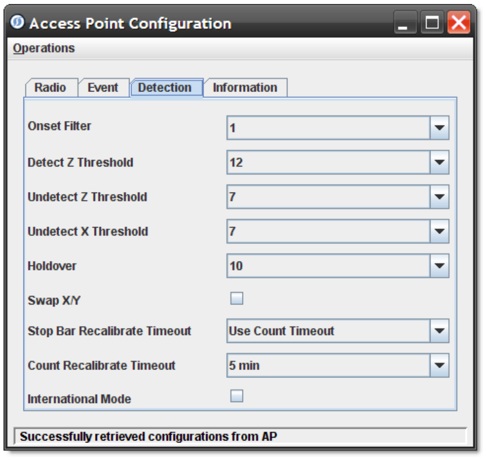
This attributes globally enables (or disables) a constraint on the nature of the data reported for a detection. Enabling this attribute results in reporting only the rising edge of a detection pulse.

1. To enable this feature, fill the check box. To disable the feature (the default setting), clear the check box.
2. Click *Apply* from the *Operations* menu to apply the change or continue configuring the Access Point.

3.8.5 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 Timeout
Count Recalibrate Timeout: 5 min
International Mode: ☐

Successfully retrieved configurations from AP

Figure 3.45: Access Point Detection tab

3.8.5.1 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, do the following:

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* from the *Operations* menu to apply the change or continue configuring the Access Point.

3.8.5.2 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.

3.8.5.2.1 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.

3.8.5.2.2 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, do the following for each of the three 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* from the *Operations* menu to apply the change or continue configuring the Access Point.

3.8.5.3 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, do the following:

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* from the *Operations* menu to apply the change or continue configuring the Access Point.

3.8.5.4 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.)[19]

1. To enable this feature, fill the check box. To disable it (the default setting), clear the check box.
2. Click *Apply* from the *Operations* menu to apply the change or continue configuring the Access Point.

3.8.5.5 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.

Note: see also the discussion of *International Mode* below which optionally adjusts the range of timeout values that can be applied.

3.8.5.5.1 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, do the following:

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* from the *Operations* menu to apply the change or continue configuring the Access Point.

---

[19] See also Sensor advanced settings in the Network Management chapter.

3.8.5.5.2 Setting the Count Recalibration Timeout

This setting applies to all Sensors operating in the count operating mode. To set the timeout, do the following:

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* from the *Operations* menu to apply the change or continue configuring the Access Point.

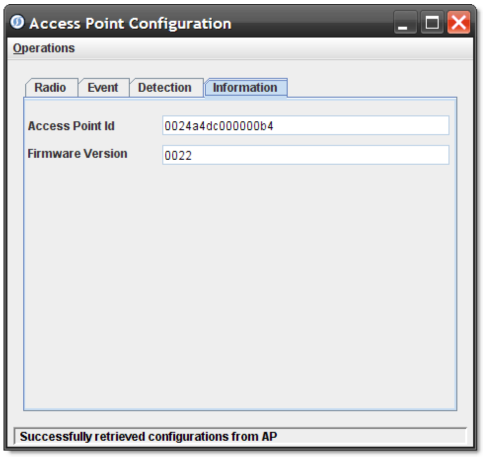
3.8.5.6 Enabling International Mode

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. Fill the check box for installations outside of North America that require the recalibration timeout feature.

3.8.6 Inspecting 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.



Access Point Id: 0024a4dc000000b4

Firmware Version: 0022

Successfully retrieved configurations from AP

Figure 3.46: Access Point Information tab

The Access Point Id is expressed as a 16-character HEX string. (*Note*: these elements are for reference only.)

3.8.7 Setting System Preferences

System preferences are user configurable elements that specify miscellaneous properties used by the network. The properties include:

- Connection timeout
- RF quality thresholds
- Advanced configuration mode
- User id and password for ftp services hosted by the Access Point

From the *Configure* menu, click *Preference* to access these elements.

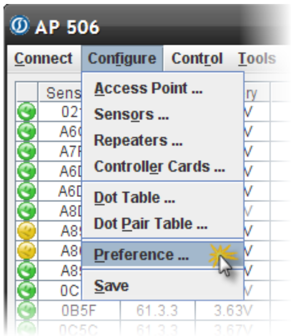
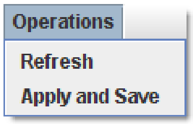


Figure 3.47: Configure menu

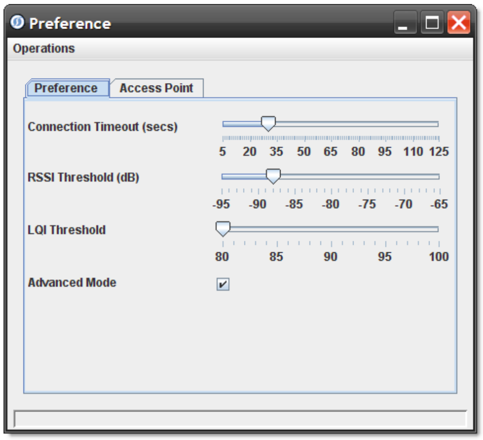
3.8.7.1 Preference Window Tabs

The *Preference* window is organized into two tabs – *Preference* and *Access Point*. Normally, elements are reviewed and/or changed on both tabs and then applied to the system.



Note that the *Operations* menu combines the apply and save function into a single command. This means that applying changes made on the *Preference* window also saves them to flash memory. (This differs slightly from how other Access Point configuration changes are saved.)

3.8.7.2 Preference Tab



Advanced Mode ☑

Figure 3.48: Preference window

3.8.7.2.1 Specifying a Connection Timeout

The connection timeout defines how long (in seconds) TrafficDOT will wait after attempting to connect to an Access Point before declaring the attempt a failure.

To set the timeout, move the slider along the slidebar to rest above the desired value. (The default value is 10 seconds.)

3.8.7.2.2 Specifying RF Quality Thresholds

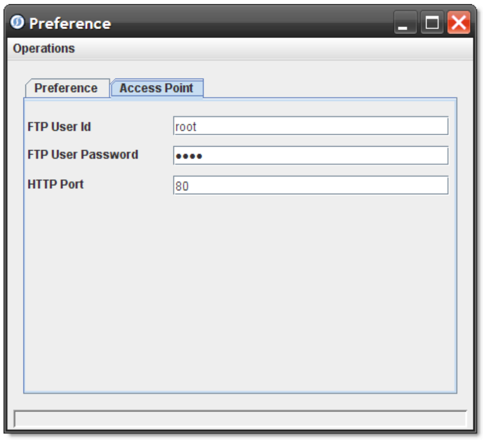
The RSSI and LQI threshold values are minimum levels of radio signal strength and line quality used by TrafficDOT to visually render RF performance on the *Access Point Main window*. (See the discussion of RSSI and LQI in the *System Description* chapter for more information.)

To set the thresholds, move the the slider along the slidebar to rest above the desired values. (The default values are -88dB for RSSI and 80 for LQI.)

3.8.7.2.3 Enabling Advanced Configuration Mode

Enabling advanced configuration mode results in the display of an additional window elements on the *Sensor Configuration* and *Access Point Configuration* windows. Fill the check box to enable the additional tab. (See *Working with Advanced Properties* below.)

3.8.7.3 Access Point Tab



FTP User Id: root
FTP User Password: ••••
HTTP Port: 80

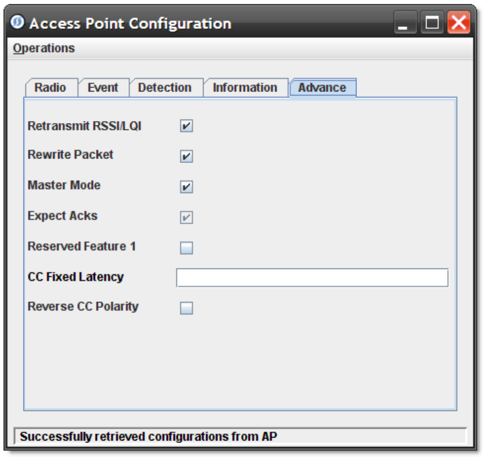
Figure 3.49: Preference window, Access Point tab

Access Points execute a local `ftp` server to provide a means of file transfer and disk access to authorized users. The *Access Point* tab collects the user identifier and password string for the ftp user.

3.8.8 Working with Advanced Properties

An additional tab, *Advance*, enables configuring a set of more advanced properties. By default, the tab is not shown. To enable it, fill the check box *Advanced Mode* on the *Preference* window.

Advanced properties dictate system behavior that is considered "default" in the sense that Sensys Networks recommends it in almost all cases. However, because unusual conditions can and do occur, these elements allow tuning of the system behavior.



Retransmit RSSI/LQI ☑
Rewrite Packet ☑
Master Mode ☑
Expect Acks ☑
Reserved Feature 1 ☐
CC Fixed Latency
Reverse CC Polarity ☐

Successfully retrieved configurations from AP

Figure 3.50: Access Point Configuration Advance Tab

3.8.8.1 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, fill the check box. To disable the feature, clear the check box.

3.8.8.2 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, fill the check box. To disable the feature, clear the check box.

3.8.8.3 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 – typically down from the command line interface by a field technician. To enable this feature, fill the check box. To disable the feature, clear the check box.

3.8.8.4 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, fill the check box. To disable the feature, clear the check box.

3.8.8.5 Reserved Feature 1

This function is reserved for Sensys Networks, Inc.

3.8.8.6 Sensys Contact Closure Card Settings

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

3.8.9 Saving the Configuration

Changes made to the configuration of an Access Point can be made permanent by saving them to flash memory via the *Configure* menu.

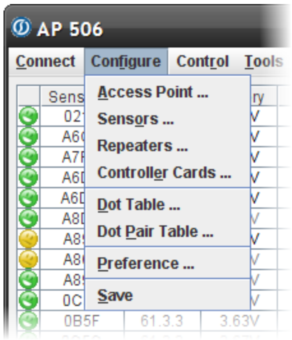


Figure 3.51: Configure menu

To save the configuration, access the *Configure* menu and click *Save*.

3.9 Configuring Repeaters

Sensys 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

3.9.1 Introduction

Repeater configuration involves selecting values for the following parameters:

- Repeater configuration
- Radio frequency of the uplink (Access Point) channel
- Radio frequency of the downlink (Sensor) channel
- Transmission time slot (optional)

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

3.9.1.1 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.

3.9.1.2 Selecting Repeaters

Configuration and management commands are applied to designated Repeaters in a network. You must explicitly specify a Repeater to configure. See *Selecting a Repeater to Configure* below.

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.

> *Note: The window element Repeater is Sensor is obsolete in this version of TrafficDOT. It is preserved for reasons of backward compatibility. Leave this check box unfilled unless directed otherwise by Sensys Networks.*

3.9.2 Starting Work

To work with Repeaters, access the *Configure* menu and click *Repeaters*.

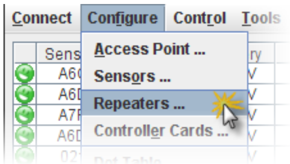
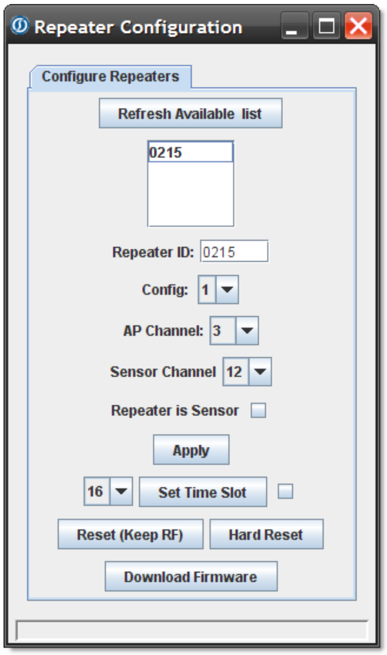


Figure 3.52: Configure Repeaters

The *Repeater Configuration* window appears.



0215

Repeater ID: 0215

Config: 1

AP Channel: 3

Sensor Channel 12

Repeater is Sensor ☐

16 ☐

Figure 3.53: Repeater Configuration window

The Repeaters transmitting on the Access Point's RF channel appear in the display area beneath the button *Refresh Available list*. Repeaters are identified by their unique, 4-character HEX id.

The list of Repeaters is refreshed when the *Repeater Configuration* window is opened. Additionally, you can refresh the list at any time by clicking *Refresh Available list*.

3.9.3 Selecting a Repeater to Configure

Designate a Repeater to configure by clicking on it's id in the display area or by typing its 4-character device id into the field *Repeater ID*.

3.9.4 Specifying a Repeater Configuration

Repeaters use one of two predetermined configurations that define the time slots used for the repeated packets. To select a configuration, do the following:

1. Click an entry from the *Config* drop-down list.
2. Click *Apply*.

3.9.5 Specifying the RF Channels

Repeaters are configured with two RF channels. The first – known as the Access Point or uplink 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 downlink channel – is used to communicate with Sensors. This channel may not be the same channel as the Access Point channel.

3.9.5.1 Note Regarding Tandem Repeaters

Tandem Repeater topologies require a bit more understanding in regard to RF channel designation and assignment - primarily due to nomenclature. Review the *Tandem Repeater* section of the *System Description* chapter for more information.

3.9.5.2 Specifying the Access Point (Uplink) Channel

To specify the RF channel for Access Point transmissions, do the following:

1. Click an entry from the *AP Channel* drop-down list.

   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*.

3.9.5.3 Specifying the Sensor (Downlink) Channel

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

1. Click an entry from the *Sensor Channel* drop-down list.

   The selected channel must be different 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. (See the *Configuring Sensors* section in this chapter for more information.)

2. Click *Apply*.

3.9.5.4 Specifying Channels On Tandem Repeaters

When working with tandem Repeaters, the field labels AP Channel and Sensor Channel on the *Repeater Configuration* window may be hard to understand. Follow the procedures described in the preceding section while observing the following rules:

- For a tandem Repeater that communicates directly with an Access Point (Repeater 1 above) , the RF channel specified as the *Sensor Channel* must be the same as the channel specified as the *AP Channel* in the downstream tandem Repeater (Repeater 2 above).
- For a tandem Repeater that communicates with Sensors (Repeater 2 above) , the RF channel specified as the *AP Channel* must be the same as the channel specified as the *Sensor Channel* in the upstream tandem Repeater (Repeater 1 above).

3.9.6 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 a value from the drop-down list to the left of the *Set Time Slot* button.

   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), fill the check-box to the right of the *Set Time Slot* button. (An arrow points to this check box in the figure above.)

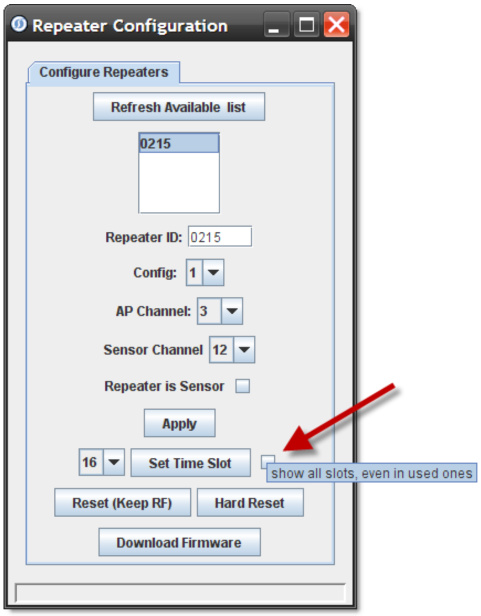


Figure 3.54: Show all time slots option

The list does not include time slots that are, by definition, reserved for use by Access Points. (See the *Time Slots* discussion in System Description chapter.)

2. Click *Set Time Slot*.

3.9.7 Updating Repeater Firmware

Updates to Repeater firmware are sent from the Access Point via the wireless communication channel. The procedure is a two-part process consisting of the following activities:

- Setting up the Access Point to download firmware
- Setting up Repeaters to receive a firmware image

> *Note*: Repeater firmware updates must occur independent of Sensor 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 Repeaters after updating their firmware, although in many cases, new firmware enables additional device functionality that may require initial configuration.

3.9.7.1 Pre-Update Considerations

Consider these ramifications of firmware update operations before proceeding:

1. *Effect on vehicle detection* – during a Repeater firmware communication between the Repeater and Access Point is interrupted. Thus, the detection events transmitted by

Sensors downstream of the Repeater or Sensors serviced by a tandem repeater downstream of the Repeater being updated may not reach the Access Point.

2. *Effect on signal control channels* – CC and EX cards receiving detections from Sensors downstream of a Repeater involved in a firmware update will receive a constant call for the duration of the update operation.
3. *Effect on Access Point* – the Access Point maintains all standard processes and capabilities during an update operation.
4. *Scope of firmware updates* – in regard to Repeaters and Sensors only, an Access Point broadcasts the new firmware image via its wireless radio; only one image can be broadcast at a time. Thus, Repeaters must be updated in a separate operation from Sensors.

> *Note*: Sensys Networks recommends applying firmware updates first to Sensors, then to Repeaters, and then to the Access Point.

3.9.7.2 Procedure

To update Repeater firmware, do the following:

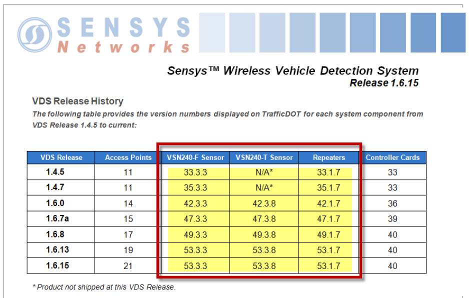
1. A single firmware image is applied to the RP240-B and RP240-B-LL Repeaters.

Repeater Type	Use	Image File Name
RP240-B, RP240-B-LL	Standard repeater, Long-life repeater	repeater.ldrec

Table 31: VDS240 Repeater Types

> *Note*: do not use other repeater image files unless directed to by Sensys Networks.

2. Determine the *version id* of the firmware image you intend to download to the Repeaters. This information is available in the *Release Notes* document that accompany each release of the Sensys VDS 240 software. This information will be used to confirm the update procedure at the end of this procedure.



SENSYS Networks

Sensys™ Wireless Vehicle Detection System
Release 1.6.15

VDS Release History

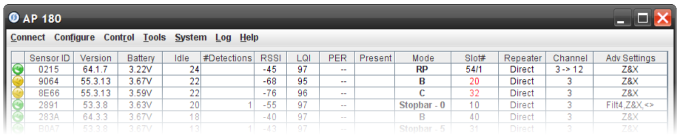
The following table provides the version numbers displayed on TrafficDOT for each system component from VDS Release 1.4.5 to current:

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

** Product not shipped at this VDS Release.*

Figure 3.55: VDS Release Notes

3. Start TrafficDOT and connect to the Access Point servicing the Repeaters whose firmware will be updated. Allow the window to fully populate and make a note of the data displayed in the *Version* column of each Repeater whose firmware will be updated.

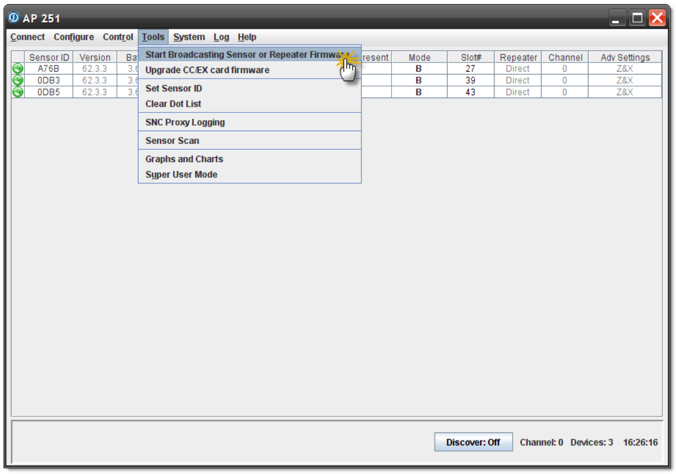


Sensor ID	Version	Battery	Idle	#Detections	RSSI	LQI	PER	Present	Mode	Slot#	Repeater	Channel	Adv Settings
0215	64.1.7	3.22V	24		-45	97	--		RP	54/1	Direct	3 -> 12	Z&X
9064	55.3.13	3.67V	22		-68	95	--		B	20	Direct	3	Z&X
8E66	55.3.13	3.59V	22		-76	96	--		C	32	Direct	3	Z&X
2891	53.3.8	3.63V	20	1	-55	97	--		Stopbar - 0	10	Direct	3	Filt4,Z&X,<>
283A	64.3.3	3.67V	18		-40	97	--		B	40	Direct	3	Z&X
B0A7	53.3.8	3.67V	13	1	-43	97	--		Stopbar - 5	31	Direct	3	Z&X

Figure 3.56: Record version and mode prior to beginning the task

4. From the *Tools* menu of the *Access Point Main* window, click *Broadcast Sensor or Repeater Firmware*. This places the Access Point into a special mode used to broadcast firmware images over the wireless radio channel.

> *Note*: vehicle detections are not processed by the Access Point when it is operating in firmware broadcast mode.



Sensor ID	Version	Ba	resent	Mode	Slot#	Repeater	Channel	Adv Settings
A76B	62.3.3	3.6		B	27	Direct	0	Z&X
0DB3	62.3.3	3.6		B	39	Direct	0	Z&X
0DB5	62.3.3	3.6		B	43	Direct	0	Z&X

Figure 3.57: Set Access Point to broadcasting mode

5. TrafficDOT confirms that the *Discover* mode is enabled before proceeding. If it is not, a window appears to enable it. Click *Yes* to continue; the *Choose Sensor or Repeater Firmware* window opens.

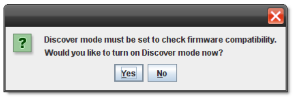
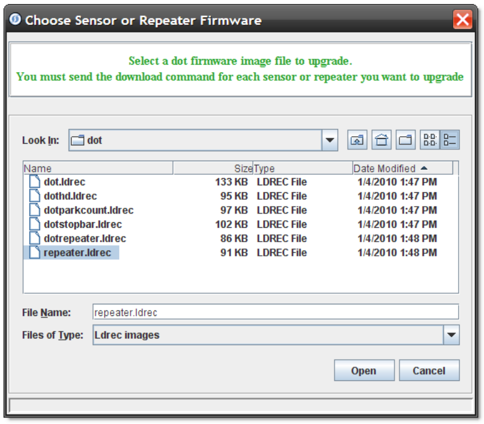

Discover mode must be set to check firmware compatibility.
Would you like to turn on Discover mode now?

Figure 3.58: Set Discover on

6. Designate the firmware image file to broadcast and click *Open*.



Select a dot firmware image file to upgrade.
You must send the download command for each sensor or repeater you want to upgrade

Look In: dot

Name	Size	Type	Date Modified
dot.ldrec	133 KB	LDREC File	1/4/2010 1:47 PM
dothd.ldrec	95 KB	LDREC File	1/4/2010 1:47 PM
dotparkcount.ldrec	97 KB	LDREC File	1/4/2010 1:47 PM
dotstopbar.ldrec	102 KB	LDREC File	1/4/2010 1:47 PM
dotrepeater.ldrec	86 KB	LDREC File	1/4/2010 1:48 PM
repeater.ldrec	91 KB	LDREC File	1/4/2010 1:48 PM

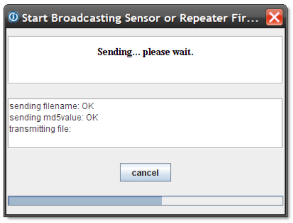
File Name: repeater.ldrec
Files of Type: Ldrec images

Figure 3.59: Select firmware image file

Be certain to select the appropriate firmware image file.

> *Note*: do not select any image file other than *repeater.ldrec* unless directed to by Sensys Networks.

The *Start Broadcasting Sensor or Repeater Firmware* window appears. This window displays a progress bar that tracks the transfer of the image file from the computer running TrafficDOT to the Access Point.

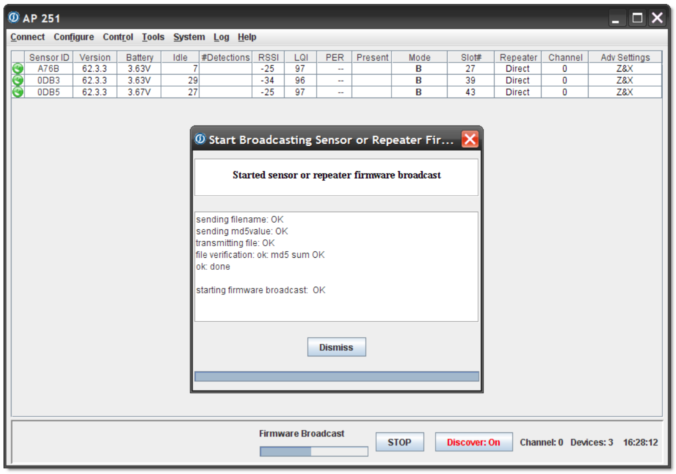


Sending... please wait.

```
sending filename: OK
sending md5value: OK
transmitting file:
```

Figure 3.60: File transfer progress

7. When the file transfer is complete (the progress bar is fully colored-in), confirm that the TrafficDOT's *Main* window displays the *Firmware Broadcast* indicator at the bottom of the window.


AP 251
Connect Configure Control Tools System Log Help
Start Broadcasting Sensor or Repeater Fir...
Dismiss
Firmware Broadcast
STOP
Discover: On

	Sensor ID	Version	Battery	Idle	#Detections	RSSI	LQI	PER	Present	Mode	Slot#	Repeater	Channel	Adv Settings
●	A76B	62.3.3	3.63V	7		-25	97	--		B	27	Direct	0	Z&X
●	0DB3	62.3.3	3.63V	29		-34	96	--		B	39	Direct	0	Z&X
●	0DB5	62.3.3	3.67V	27		-25	97	--		B	43	Direct	0	Z&X

Started sensor or repeater firmware broadcast

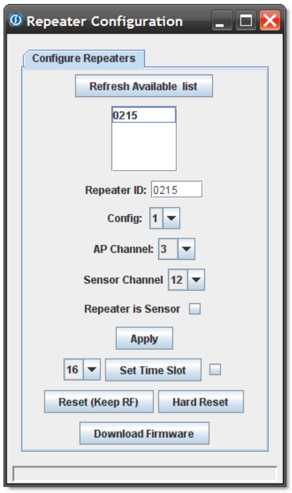
```
sending filename: OK
sending md5value: OK
transmitting file: OK
file verification: ok: md5 sum OK
ok: done

starting firmware broadcast:  OK
```

Channel: 0 Devices: 3 16:28:12

Figure 3.61: Animated Firmware Broadcast indicator

The animated *Firmware Broadcast* indicator confirms the Access Point as acquired an image file from the TrafficDOT computer and is transmitting it over its wireless radio. Click *Dismiss* to close the *Start Broadcasting Sensor or Repeater Firmware* window.

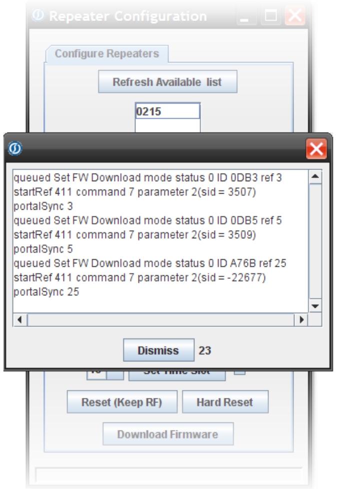
8. From TrafficDOT's *Configure* menu, open the *Repeater Configuration* window.



Repeater ID: 0215
Config: 1
AP Channel: 3
Sensor Channel 12
Repeater is Sensor ☐
16 Set Time Slot ☐

Figure 3.62: Select Repeaters

9. Select one or more Repeaters by moving the device ids from the *Available* list to the *Selected* list. (See *Selecting a Repeater to Configure* above for more information.)
10. Click *Download Firmware*. A TrafficDOT command status window appears and the designated Repeaters are put into an operating mode to receive the firmware image being broadcast by the Access Point.

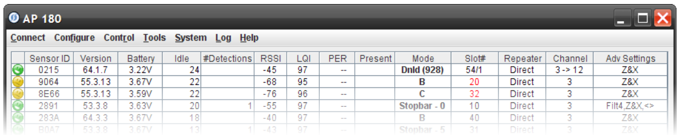


```
queued Set FW Download mode status 0 ID 0DB3 ref 3
startRef 411 command 7 parameter 2(sid = 3507)
portalSync 3
queued Set FW Download mode status 0 ID 0DB5 ref 5
startRef 411 command 7 parameter 2(sid = 3509)
portalSync 5
queued Set FW Download mode status 0 ID A76B ref 25
startRef 411 command 7 parameter 2(sid = -22677)
portalSync 25
```

Figure 3.63: Command status

Click *Dismiss* to close the command status window.

11. Review the target Repeaters(s) on TrafficDOT's *Main* window. Confirm that each Repeater designated for the firmware update is shown with the value “**DnId(####)**” in the *Mode* column, where **####** is an integer.

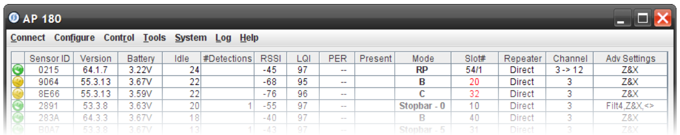


	Sensor ID	Version	Battery	Idle	#Detections	RSSI	LQI	PER	Present	Mode	Slot#	Repeater	Channel	Adv Settings
●	0215	64.1.7	3.22V	24		-45	97	--		**DnId (928)**	54/1	Direct	3 -> 12	Z&X
●	9064	55.3.13	3.67V	22		-68	95	--		**B**	20	Direct	3	Z&X
●	8E66	55.3.13	3.59V	22		-76	96	--		**C**	32	Direct	3	Z&X
●	2891	53.3.8	3.63V	20	1	-55	97	--		**Stopbar - 0**	10	Direct	3	Filt4,Z&X,<>
●	283A	64.3.3	3.67V	18		-40	97	--		**B**	40	Direct	3	Z&X
●	B0A7	53.3.8	3.67V	13	1	-43	97	--		**Stopbar - 5**	31	Direct	3	Z&X

Figure 3.64: Mode column indicates devices receiving a firmware image

> *Note*: it is expected that the health indicator for each device will briefly turn red before the device begins receiving the firmware image.

12. Observe TrafficDOT's *Main* window to monitor the progress of the download operation. Repeaters automatically resume normal operations after receiving and installing a new firmware image.



	Sensor ID	Version	Battery	Idle	#Detections	RSSI	LQI	PER	Present	Mode	Slot#	Repeater	Channel	Adv Settings
●	0215	64.1.7	3.22V	24		-45	97	--		**RP**	54/1	Direct	3 -> 12	Z&X
●	9064	55.3.13	3.67V	22		-68	95	--		**B**	20	Direct	3	Z&X
●	8E66	55.3.13	3.59V	22		-76	96	--		**C**	32	Direct	3	Z&X
●	2891	53.3.8	3.63V	20	1	-55	97	--		**Stopbar - 0**	10	Direct	3	Filt4,Z&X,<>
●	283A	64.3.3	3.67V	18		-40	97	--		**B**	40	Direct	3	Z&X
●	B0A7	53.3.8	3.67V	13	1	-43	97	--		**Stopbar - 5**	31	Direct	3	Z&X

Figure 3.65: Devices automatically resume operations

After all Repeaters have resumed normal operations, confirm the following for each Repeater and all Sensors positioned downstream of the Repeaters:

- the data displayed in the *Version* column matches the expected value acquired from the *Release Notes* in step two above,
- The *RSSI* and *LQI* metrics are within acceptable ranges,

- the device health indicator indicates acceptable operating status (green)

When the Version, Mode, RSSI, LQI and Health Indicator display acceptable and expected value for all devices targeted for the firmware update, a successful operation is confirmed.

Note: the amount of time required to perform a firmware update depends on multiple factors including the quality of the RF communication between the Access Point and the devices, the number of devices upgraded, the presence/use of Repeaters or tandem Repeaters, the size of the image, and other properties. The duration you experience may differ significantly from site to site. Sensys Networks recommends testing the process to establish a baseline.

13. After the operation has been confirmed, click *STOP* at the bottom of TrafficDOT's Main window. The Access Point is taken out of firmware image broadcast mode and resumes normal operations.

14. Disconnect from the Access Point and exit TrafficDOT.

3.9.7.3 Canceling a Firmware Update Operation

To cancel a firmware update operation before it completes, click *STOP* at the bottom of TrafficDOT's *Main* window.

3.9.7.4 Re-Running a Firmware Update Operation

Re-running a firmware update operation may be required if some devices fail to receive complete firmware images. (This may result of wireless communication errors.)

Running a firmware operation again is accomplished by repeating the procedure outline above in the section *Updating Repeater Firmware*.

3.9.8 Adding a Repeater to a Network

Repeaters starting operating as soon as they receive power and require only minimal configuration. To add a Repeater to an existing network, do the following:

- Confirm the installation location and the Repeater coverage area (the Sensors that the Repeater will serve)
- Configure the Repeater's time slot configuration, Access Point channel and Sensor channel
- Install the Repeater

Verify the Repeater is operating by running TrafficDOT, accessing the *Access Point Main window* and reviewing the table of devices to locate the Repeater and its Sensors.

3.9.9 Removing a Repeater from a Network

Typically, installed Repeaters are not removed from a network. However, if the need arises to so, consider the following alternatives – all of which accomplish “removing” a Repeater.

- Physically deinstall the device
- Detach or remove the Repeater's battery
- Configure the Repeater's Access Point channel to a channel other than the one the Access Point uses

Note that any of the above steps will also render the Sensors serviced by the Repeater inoperative from the perspective of the Access Point as it will have no communication link by which to reach them.

In the event that the Sensors must be “moved” to a different Repeater or additional Access Point, configure them appropriately according to the procedures in the *Configuring Sensors* section above.

3.9.10 Performing Other Operations

TrafficDOT's *Repeater Configuration* window includes other operations related to managing Repeaters including:

- performing a “soft” reset
- performing a “hard” reset

These operations are not common. Perform them only when directed by Sensys Networks.

3.9.10.1 Performing a Soft Reset

On occasion, a Repeater 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 RF event in the local area or other reason. To accomplish a soft reset, select the Repeater and click the *Reset (Keep RF)* button.

3.9.10.2 Performing a Hard Reset

On occasion, a Repeater may need to reset back to its factory default configuration. Performing a hard reset clears any configured RF channel assignments and replaces the channel assignments as follows:

- AP channel: 0 (zero)

- Sensor channel: 1 (one)

Additionally, the Repeater Configuration assignment is set to configuration 0 (zero). Document these settings before performing this operation so that the device can be reconfigured to participate in your Sensys network.

To accomplish a hard reset, select the Repeater and click the *Hard Reset* button.

3.10 Managing Sensor Tables

Access Points store information describing Sensor locations and relative positions in two databases. The databases are:

- *Sensor table* – also referred to as the “dots” configuration table, this database stores an entry for each Sensor in the network including its lane position and traffic signal controller address (if used)
- *Sensor-pair table* – also referred to as the “dot pairs” configuration table, this database includes one entry for each Sensor-to-Sensor relationship forming a *speed pair*

The tables are manually maintained. Maintaining accurate records of Sensor location relative to lanes, signal controller and other other Sensors is essential to effectively operating the system, troubleshooting problems and generating meaningful statistics and reports. For example, elements such as speed and length cannot be produced without Sensor pair data.

3.10.1 Starting Work

Sensor tables are accessed via TrafficDOT's configure menu.

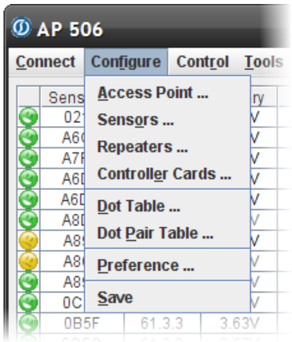
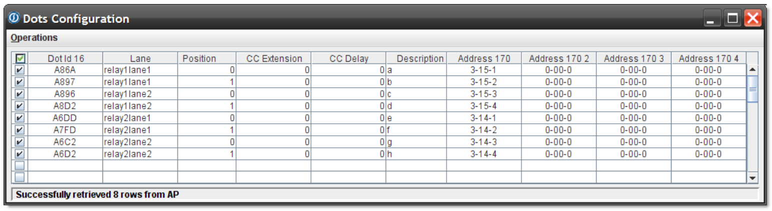


Figure 3.66: Configure menu

Click either *Dot Table* or *Dot Pair Table* to display a Sensor table.

3.10.2 Working with the Dots Table

The *Dots Configuration* window provides display and maintenance of the Sensor table entries for a network. (*Note*: use the *Access Point Main window* to monitor all Sensors in a network in real time.)



☑	Dot Id 16	Lane	Position	CC Extension	CC Delay	Description	Address 170	Address 170 2	Address 170 3	Address 170 4
☑	A86A	relay1lane1	0	0	0	a	3-15-1	0-00-0	0-00-0	0-00-0
☑	A897	relay1lane1	1	0	0	b	3-15-2	0-00-0	0-00-0	0-00-0
☑	A896	relay1lane2	0	0	0	c	3-15-3	0-00-0	0-00-0	0-00-0
☑	A8D2	relay1lane2	1	0	0	d	3-15-4	0-00-0	0-00-0	0-00-0
☑	A6DD	relay2lane1	0	0	0	e	3-14-1	0-00-0	0-00-0	0-00-0
☑	A7FD	relay2lane1	1	0	0	f	3-14-2	0-00-0	0-00-0	0-00-0
☑	A6C2	relay2lane2	0	0	0	g	3-14-3	0-00-0	0-00-0	0-00-0
☑	A6D2	relay2lane2	1	0	0	h	3-14-4	0-00-0	0-00-0	0-00-0
☐										
☐										

Successfully retrieved 8 rows from AP

Figure 3.67: Dots Configuration window

3.10.2.1 Understanding the Window Contents

The window displays one Sensor per row using the following columns:

Column Name	Description
<check-box>	Logical 'toggle' switch representing whether the Sensor is enabled for statistical reporting. (*Required*)
DotId 16	The factory assigned hardware device identifier. This column displays the least significant 16 bits as a 4-character HEX string. (*Required*)
Lane	Short text description of the lane in which the Sensor has been installed. (*Required*)
Position	Sensor's 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** only where **0** indicates the lead Sensor, **1** indicates a trailing Sensor,and **2** indicates a second trailing Sensor. (*Required*)
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*)
Description	Additional description for Sensor location and use. (*Optional*)
Address 170	Maps a sensor table entry to a Contact Closure card channel. (*Required, see Notes below*)
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 32: Columns of the Dot Configuration Window

Notes

- Fill the checkbox to indicate that the entry is active for the configuration. (*Note*: this element has no effect on the actual detection behavior of a Sensor.)
- Rows may be manually entered into the table as needed.
- At least one *Address 170* entry is required and must adhere to the following form: [`shelf number  – slot number – channel`] where *shelf number – slot number* is a Card ID[20] associated with a Sensys Contact Closure Master or Extension card and *channel* is between 1 and 4. Always use the first *Address 170* column for the first entry.

---

[20] Refer to the Sensys document *Sensys Contact Closure Card Installation Guide* for more information regarding Card IDs.

- To assign a Sensor to multiple controller channels, supply entries to the additional *Address 170* (*Address 170 2* through *Address 170 4*) columns, moving left to right.
- *CC Extension* entries extend the duration of a contact closure on a per-Sensor basis. These entries are optional.
- *CC Delay* entries delay the duration of contact closure on a per-Sensor basis; these entries are optional.
- *Lane* , *Position,* and *Description* are not required to map sensors to channels.

Entries are added, revised or deleted directly in the table. The *Operations* menu provides a set of commands that act on the table data.

3.10.2.2 Operations Menu Commands

The Operations menu provides a means to acquire the current Sensor table information from an Access Point, save changes to the table, and perform other tasks.

- *Refresh* – reads the current Sensor table data from an Access Point. (*Note*: this operation reads stored table data only – it does not query the network for actual Sensors.)
- *Apply* – saves the table data displayed on the window to the Access Point.
- *Import* – reads a CSV formatted file and adds the contents to the window.
- *Export* – reads the window contents and saves the entries to a CSV formatted file.
- *Clear* – empties the window of all entries. (*Note*: this command does not change the Sensor table data stored on the Access Point. That data changes only when the *Apply* command is used.)
- *Populate* – queries (discovers) the network for Sensors and adds the Sensor IDs to the window. This function is helpful when initially defining Sensors.

3.10.2.3 Adding a Dot Configuration Entry

Table entries can be added manually, or via the *Populate* menu command.

1. Fill the *DotId16* column for each Sensor to be defined.

   Use *Populate* to direct TrafficDOT to acquire the ID values of the Sensors recognized by the Access Point or type a type a 4-character hex ID of the Sensor.

   Note: this is the value displayed in the *Sensor ID* column on the *Access Point Main window*.

2. Type into the *Lane* field a short text description of the lane in which the Sensor resides.

3. Type into the *Position* field an integer *between 0 and 2* that indicates the Sensor's relative position in the lane.

   Note: Positions are determined by counting up from zero in the direction of the traffic's travel. That is, a vehicle will first drive over Sensor zero, then Sensor one and then Sensor two.

   There is a maximum of three Sensors per lane. The Sensor in position zero must be defined before the Sensor in position one, and position one must be defined before position two.

4. Apply an optional channel extension per Sensor by supplying a value to the *CC Extension* column.
5. Apply an optional channel delay per Sensor by supplying a value to the *CC Delay* column.
6. Supply an optional description string to the *Description* column.
7. If the Sensor is used with a traffic controller, supply the card address in the column *Address 170*. If the Sensor is not used with a signal controller, type a zero into the field.

   Specify up to three additional channel assignments using fields *Address 170 2*, *Address 170 3*, and *Address 170 4*.

8. The check box at the left edge of the row designates the Sensor as being included (or ignored) by statistical or other applications. The check box is filled by default which indicates the Sensor will be included.
9. Click *Apply* from the *Operations* menu to add the entry.

3.10.2.4 Changing a Dot Configuration Entry

Edit the Sensor table entry directly in the table cells adhering to the cell content rules described above. A Sensor may be hidden from statistics generation and other reporting by clearing the check box at the left edge of the row. Click the check box to clear it or to fill it. Click *Apply* from the *Operations* menu to apply the change.

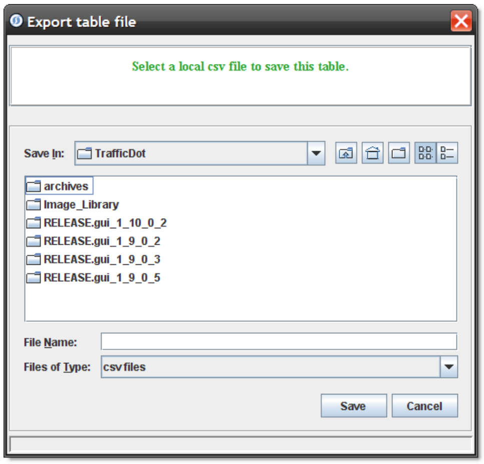
3.10.2.5 Deleting a Dot Configuration Entry

Deleting an entry permanently removes the Sensor's entry from the configuration. Note, however, that deleting a table entry has *no impact* on the actual physical Sensor and its event detection and RF functions.

To delete an entry, right click anywhere in the row. Click *Delete* on the pop-up menu to remove the entry. Click *Apply* from the *Operations* menu to save the changes.

3.10.2.6 Exporting a Dot Table

The contents of a dot configuration table can be exported to a comma separated value (CSV) text file. Click *Export* from *Operations* menu to invoke the *Export Table File* window.



Select a local csv file to save this table.

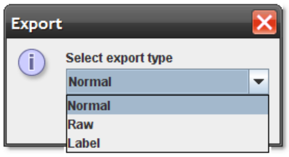
Save In: TrafficDot

File Name:

Files of Type: csv files

Figure 3.68: Export Dot Table to File

Supply a name for the file and click *Save*. The *Export* window appears to acquire the scope of the data exported.



Select export type

Normal

Figure 3.69: Export Type

Select one of the export types and click *OK*. The export types are described in the table below.

Export Type	Data Elements Included in the Exported File
Normal	Enabled,Dot Id 16, Lane, Position, CC Extension, CC Delay, Description, Address 170, Address 170 2, Address 170 3, Address 170 4
Raw	Enabled, Dot Id 16, Dot Id 64, Time Slot, Lane, Position, CC Extension, CC Delay, Description, Address 170, Address 170 2, Address 170 3, Address 170 4
Label	Dot Id 16, Lane, Position

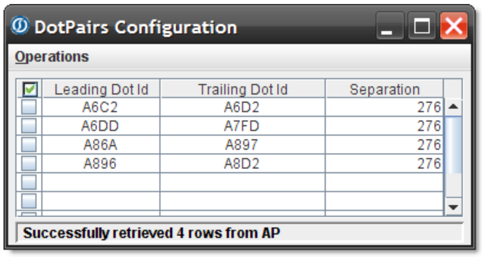
Table 33: Dot (Sensor) Table Export Options

3.10.2.7 Printing Sensor Labels

The file created with an *Label* export type can be used as input to any label-making application that supports CSV files. This allows Sensor labels to be printed and affixed prior to Sensor installation.

3.10.3 Working With the Dot Pairs Table

The *Dot Pairs Configuration* window provides display and maintenance of the Sensor pairs of the network. Sensor pairs – also known as dot pairs or speed pairs – are essential to producing value added information from detection events. For example, speed, length, gap and other values can be derived only by knowing the relative position and distance between two Sensors.



☑	Leading Dot Id	Trailing Dot Id	Separation
☐	A6C2	A6D2	276
☐	A6DD	A7FD	276
☐	A86A	A897	276
☐	A896	A8D2	276
☐			
☐			

Successfully retrieved 4 rows from AP

Figure 3.70: Dot Pairs Configuration window

3.10.3.1 Understanding the Window Contents

The window displays one Sensor pair per row using the following columns:

Column Name	Description
<check-box>	Logical 'toggle' switch representing whether the Sensor pair is enabled for event reporting.
Leading Dot Id	The factory assigned hardware device identifier of a leading Sensor. This column displays the least significant 16 bits as a 4-character HEX string.
Trailing Dot Id	The factory assigned hardware device identifier of a following Sensor. This column displays the least significant 16 bits as a 4-character HEX string.
Separation	The distance between the leading and trailing Sensors in millimeters.

Table 34: Columns of the DotPairs Configuration window

Entries are added, revised or deleted directly in the table. The *Operations* menu provides a set of commands that act on the table data.

3.10.3.2 Operations Menu Commands

The Operations menu provides a means to acquire the current Sensor pair table information from an Access Point, save changes to the table, and perform other tasks.

- *Refresh* – reads the current Sensor pair table data from an Access Point. (*Note*: this operation reads stored table data only – it does not query the network for actual Sensors.)
- *Apply* – saves the table data displayed on the window to the Access Point.
- *Import* – reads a CSV formatted file and adds the contents to the window.
- *Export* – reads the window contents and saves the entries to a CSV formatted file.

- *Clear* – empties the window of all entries. (*Note*: this command does not change the Sensor table data stored on the Access Point. That data changes only when the *Apply* command is used.)
- *Populate* – queries the *Dot* table and and adds the Sensor pairs to the window. This function is helpful when initially defining the Sensors to the table. (*Note*: you must first define Sensors to the *Dot* table and assign relative positions[21] to benefit from this command.)

3.10.3.3 Adding a DotPairs Configuration Entry

To add a new entry, do the following:

1. Position the cursor in the *Leading Dot Id* column on a blank row. Type a 4-character hex Id of a Sensor.

   Note: a "leading" Sensor is the Sensor that a vehicle first passes over when traveling in the direction of normal traffic flow. This is the value displayed in the *Sensor ID* column on the *Access Point Main window*.

2. Type into the *Trailing Dot Id* field a 4-character hex Id of a Sensor.

   Note: a "trailing" Sensor is the Sensor that a vehicle passes over second when traveling in the direction of normal traffic flow.

3. Type into the *Separation* field a decimal value (in millimeters) specifying the physical distance between the leading and trailing Sensors.
4. The check box at the left edge of the row designates the Sensor pair as being included (or ignored) by statistical or other applications. The check box is filled by default which indicates the Sensor will be included.
5. Click *Apply* from the *Operations* menu to add the entry.

3.10.3.4 Changing a DotPairs Configuration Entry

Edit a Sensor pair table entry directly in the table cells adhering to the cell content rules described above. A Sensor pair may be hidden from statistics generation and other reporting by clearing the check box at the left edge of the row. Click the check box to clear it or to fill it. Click *Apply* from the *Operations* menu to apply the changes.

3.10.3.5 Deleting a DotPairs Configuration Entry

Deleting an entry permanently removes a Sensor pair entry from the configuration. Note, however, that deleting a table entry has *no impact* on the actual physical Sensors and their event detection and RF functions.

---

[21] Where applicable you must declare Sensors as *leading, trailing* or *second trailing* Sensors in a lane.

To delete an entry, right click anywhere in the row. Click *Delete* on the pop-up menu to remove the entry. Click *Apply* from the *Operations* menu to save the changes.

3.10.3.6 Saving Changes

Changes to the Dots and DotPairs tables are saved only when the *Apply* command from the *Operations* menu is clicked.

3.11 Updating Device Firmware

Firmware updates are transmitted to Sensors and Repeaters from the Access Point via the wireless communication channel. The update procedure is a two-part process, with the first activity performed on the Access Point and the second on the Sensors and/or Repeaters.

Firmware updates become operational immediately and are not reversible. It is not necessary to reconfigure devices after updating their firmware, although in many cases, new firmware enables additional device functionality that may require initial configuration.

Note: Access Point firmware updates do not occur over the wireless radio; AP firmware is updated over an IP network connection. (See the section *Updating Access Point Firmware* for more information.)

3.11.1 Performing a Sensor or Repeater Firmware Update

Firmware updates are started from the *Tools* menu option *Start Broadcasting Sensor or Repeater Firmware*.

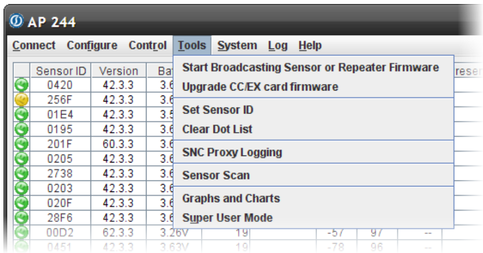


Figure 3.71: Tools menu

Step-by-step procedures for updating Sensor and Repeater firmware are described in the following sections:

- *Updating Sensor Firmware*
- *Updating Repeater Firmware*

3.12 Setting Sensor Ids

Beginning with VDS version 1.8, 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.

3.12.1 Considerations for Setting Sensor IDs

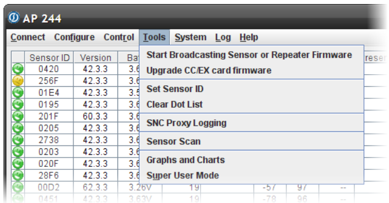
Consider the following when setting Sensor Ids to user-defined strings:

- 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 *Set 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 *Set 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 appears 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.)

3.12.2 Procedure

To set a Sensor Id, do the following:

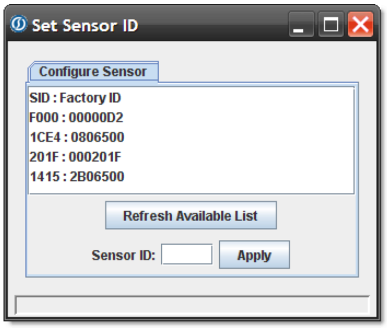
1. Connect to the target Access Point.
2. From the *Tools* menu, click *Set Sensor Id*.



Sensor ID	Version
0420	42.3.3
256F	42.3.3
01E4	42.3.3
0195	42.3.3
201F	60.3.3
0205	42.3.3
2738	42.3.3
0203	42.3.3
020F	42.3.3
28F6	42.3.3
00D2	62.3.3
0451	42.3.3

Figure 3.72: Tools menu

The *Set Sensor ID* command opens the *Set Sensor ID* window which, in turn, requires the Access Point and the other network devices to be in *discover* mode. A window appears allowing you to enable discover mode if it is not enabled.



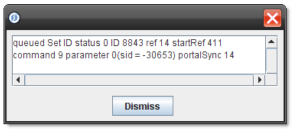
```
SID : Factory ID
F000 : 00000D2
1CE4 : 0806500
201F : 000201F
1415 : 2B06500
```

Figure 3.73: Set Sensor ID window

> *Note*: the *Set Sensor ID* window shows only Sensors running a VDS firmware version that supports aliasing Sensors. Therefore, the window may not display all Sensors in your network.

3. From the *Configure Sensor* list, click a Sensor to select it.
4. Type a new device identifier string into the *Sensor ID* field and click *Apply*. The string must be four characters in length and may consist only of hexadecimal characters.

   A command progress window appears; click *Dismiss* to close it.



```
queued Set ID status 0 ID 8843 ref 14 startRef 411
command 9 parameter 0(sid = -30653) portalSync 14
```

Figure 3.74: Command progress

The *Set Sensor ID* command opens the *Set Sensor ID* window which, in turn, requires the Access Point and the other network devices to be in *discover* mode. A window appears allowing you to enable discover mode if it is not enabled.

5. Close the *Set Sensor ID* window.
6. Return to the TrafficDOT *Main* window and monitor the operation.

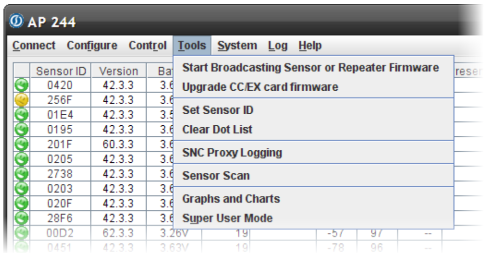
   While the command is executed, the row representing the original Sensor depicts a loss of contact to the Access Point. A new row appears representing the Sensor under its new ID value. Depending on the time slot of the Sensor, it may take a moment for these changes to be observed.

7. After the row representing the Sensor appears on the *Main* window, select from the *Tools* menu the command *Clear Dot List*.

This directs TrafficDOT to refresh its display of network devices with the most recent information. Do this to remove the row representing the Sensor under its original ID.

3.13 Refreshing the Main Display

On occasion, it may be necessary to refresh the data displayed in TrafficDOT's *Main* window. This is done from the *Tools* menu by clicking *Clear Dot List*.



Sensor ID	Version
0420	42.3.3
256F	42.3.3
01E4	42.3.3
0195	42.3.3
201F	60.3.3
0205	42.3.3
2738	42.3.3
0203	42.3.3
020F	42.3.3
28F6	42.3.3
00D2	62.3.3
0451	42.3.3

Figure 3.75: Tools menu

The data is refreshed as it is received by the Access Point according to the time slot of each device. Depending on the number of devices in the network, it may take a moment for the window to refresh fully.

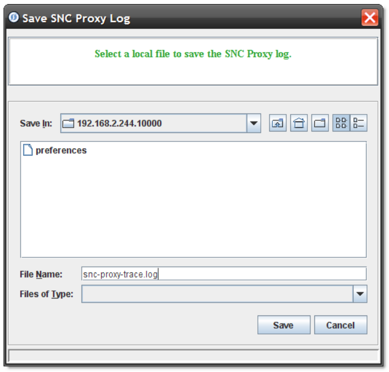
3.14 Enabling Logging for the SNC Proxy Process

On occasion, it may be necessary to log the operations of the SNC Proxy process executing on the Access Point. (The SNC Proxy process provides an interface to the Access Point that supports remote administration and data archiving operations.)

Enabling logging results in the creation of a log file in a user specified folder and writing log transactions to the file. A menu option is provided to enable logging; a command button is provided to terminate a logging session.

To enable SNCProxy logging, do the following:

8. From the *Tools* menu, click *SNC Proxy Logging*. The *Save SNC Proxy Log* window appears.



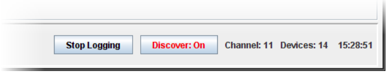
Select a local file to save the SNC Proxy log.

Save In: 192.168.2.244.10000

File Name: snc-proxy-trace.log

Figure 3.76: Save SNC Proxy Log window

9. Type a file name for the log file, giving it a file extension of "`.log`". Optionally, navigate to a different folder to store the file. Click Save. The *Stop Logging* button appears at the bottom of the *Main* window; logging starts immediately.



Channel: 11 Devices: 14 15:28:51

Figure 3.77: SNC Proxy logging enabled

To terminate SNC Proxy logging, click the *Stop Logging* command button.

3.15 Scanning RF Channels for Sensys Devices

The *Sensor Scan* utility on the *Tools* menu provides a way to automatically scan the RF channels of the Access Point and report Sensys devices communicating on those channels. Use the utility to identify what RF channel a particular device has been configured to use – such as may be the case when working with replacement parts or devices held in stock.

Note: the factory default RF channels for Sensys equipment are as follows: (*i*) Access Points – channel 0 (zero), (*ii*) Sensors – channel 0 (zero), and (*iii*) Repeaters – to Access Point, channel 0 (zero); to Sensors, channel 1.

3.15.1 Considerations for Scanning RF Channels

3.15.1.1 Basic Operation

The channel scan tool surveys a minimum of one channel (the channel on which the Access Point is transmitting), up to the full 16 channels available to VDS systems from Sensys Networks. Sensys devices found transmitting on the scanned channels are reported in a results window. The results window displays information only; the results cannot be operated on.

3.15.1.2 Order of Channels Scanned

The Access Point's channel is always scanned first. It is followed by the next highest numbered channel, relative to the Access Point's and subject to the channels specified in the scan request. (As circumstance warrant, the scan process when completing the scan of channel 15 “loops” back to channel 0 (zero) and continues.) Because of this, the results reported from the scan may not appear in strict numerical order by channel.

3.15.1.3 Limiting the Scan

The channel scan can be limited in any of the following ways:

- *by device* – directs the scan to report only specified devices (multiple device IDs may be specified). The scan terminates when all specified devices are found or all channels have been scanned.
- *include Repeaters* – directs the scan to report Repeaters in addition to Sensors (*Note*: the default is to scan for Sensors only.)
- *include 2nd-tier Repeaters* – directs the scan to include tandem Repeaters (that is, a Repeater downstream of a Repeater) in addition to Sensors.
- *by channel* – directs the scan to survey only the selected channel(s). If no channel selection is made, the scan is confined to the channel of the Access Point. Multiple channels can be selected.

- *by duration* – the element *scan interval* dictates how many minutes the scan process spends on each requested channel. The higher the number supplied as the interval, the longer the overall process will take but there will be less chance of scanning error resulting from dropped packets or retries. A lower number results in less overall time devoted to the operation, but a greater chance that a scanning inaccuracy may result due to RF communications errors. Site circumstances should be taken into account when setting the interval. Additionally, the available interval values are automatically adjusted when either of the Repeater settings are enabled.

The filters noted above are optional and can be combined in any fashion.

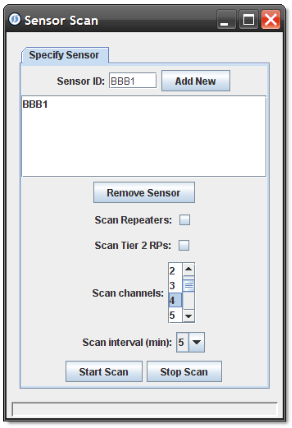
3.15.1.4 Scanning for Repeaters

When Repeaters are included, the Access Point pauses its scan until all Repeaters have completed their scan. When Tier 2 Repeaters (tandem Repeaters) are included, the parent Repeater pauses its scan until its child Repeater has completed its scan. Repeaters at the same tier level (peers) perform scans simultaneously. When scanning detector networks using Repeaters and/or Tandem Repeaters, using the highest scan interval will result in the most accurate scan.

3.15.2 Procedure

To scan RF channels for Sensys devices, do the following:

10. From the *Tools* menu, click *Sensor Scan*. The *Sensor Scan* window appears.



Sensor ID: BBB1

BBB1

Scan Repeaters: ☐

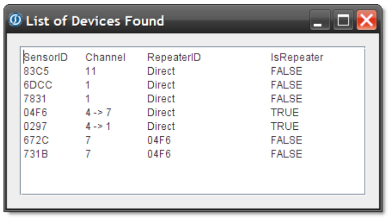
Scan Tier 2 RPs: ☐

Scan channels: 2 3 4 5

Scan interval (min): 5

Figure 3.78: Sensor Scan window

11. Specify the requirements for the channel scan (See *Considerations for Scanning RF Channels* above.) Click *Start Scan* to imitate the operation. The *List of Devices Found* window appears.



```
SensorID   Channel   RepeaterID         IsRepeater
83C5       11        Direct             FALSE
6DCC       1         Direct             FALSE
7831       1         Direct             FALSE
04F6       4 -> 7    Direct             TRUE
0297       4 -> 1    Direct             TRUE
672C       7         04F6               FALSE
731B       7         04F6               FALSE
```

Figure 3.79: List of Devices Found window

The columns displayed in the window are described below:

Column Name	Description
Sensor ID	The factory assigned hardware device identifier. Repeaters are identified by the value TRUE in the *isRepeater* column.
Channel	The RF channel(s) on which the device is transmitting. A value formatted as "**#>#**" indicates a Repeater where the left-most number is the Access Point channel and the right-most number is the Sensor channel.
RepeaterID	The device ID of the Repeater through which the device is transmitting; the value "Direct" indicates that the device communicates directly with the Access Point.
isRepeater	Indicates the device is a Repeater; a value of "FALSE" denotes a Sensor.

Table 35: List of Devices Found Window Contents

12. Terminate the scan before its conclusion by clicking *Stop Scan*. Alternatively, wait for the message "*Scan finished*" in the window area and close both the *List of Devices Found* and the *Sensor Scan* windows.

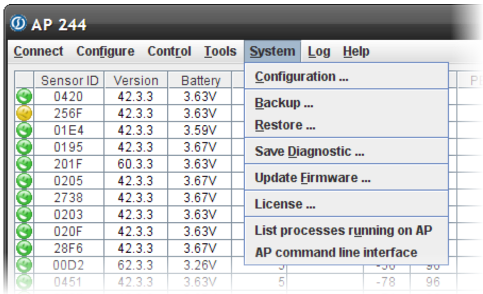
3.16 Configuring and Managing System Parameters

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
- Marksman output attributes
- Advanced settings
- Other properties

3.16.1 Starting Work

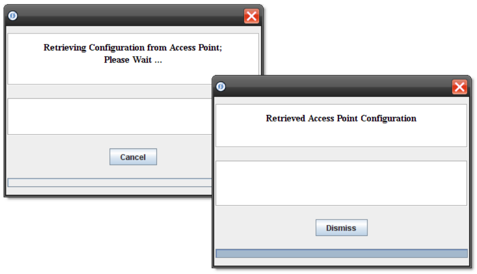
Each of the collections of system parameters is implemented as a tab on TrafficDOT's *System Configuration* window.



Sensor ID	Version	Battery
0420	42.3.3	3.63V
256F	42.3.3	3.63V
01E4	42.3.3	3.59V
0195	42.3.3	3.67V
201F	60.3.3	3.63V
0205	42.3.3	3.67V
2738	42.3.3	3.67V
0203	42.3.3	3.63V
020F	42.3.3	3.63V
28F6	42.3.3	3.67V
00D2	62.3.3	3.26V
0451	42.3.3	3.63V

Figure 3.80: System menu

Click *Configuration* from TrafficDOT's *System* menu to read the Access Point's configuration file.


Retrieving Configuration from Access Point;
Please Wait ...

Retrieved Access Point Configuration

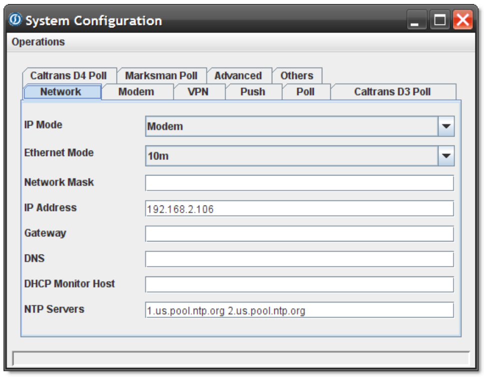
Figure 3.81: Reading AP configuration file

Click *Dismiss* to work on the configuration.

> *Note*: the configuration data displayed on the System Configuration window is an editable copy of the configuration. After editing the data, use the *Save* command from the *Operations* menu to write the configuration to the Access Point. Failing to save changes preserves the original Access Point's configuration.

3.16.2 Working 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	Modem
Ethernet Mode	10m
Network Mask	
IP Address	192.168.2.106
Gateway	
DNS	
DHCP Monitor Host	
NTP Servers	1.us.pool.ntp.org 2.us.pool.ntp.org

Figure 3.82: Network tab

3.16.2.1 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 appears only when the *IP Mode* element is set to *Modem*.

3.16.2.2 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.

3.16.2.3 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.

3.16.2.4 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.

3.16.2.5 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.

3.16.2.6 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.

3.16.2.7 Designating the DHCP Monitor Host

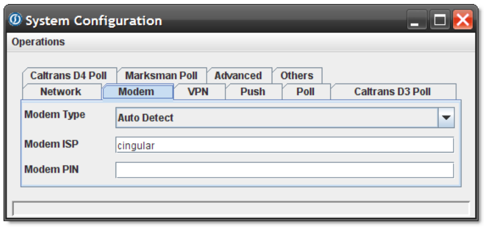
DHCP Monitor Host identifies by IP address a network node used by the Access Point to evaluate its connection to a host providing Dynamic Host Control Protocol services. Typically, the device used as the monitoring host is the DHCP server itself.

3.16.2.8 Specifying the Network Time Sources

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

3.16.3 Working With Modem Properties

Modem properties define the settings necessary to conduct IP communications with the Access Point over a cellular data network.



Modem Type: Auto Detect

Modem ISP: cingular

Modem PIN:

Figure 3.83: Modem tab (Optional)

3.16.3.1 Setting the Modem Type

Modem Type specifies the type of cellular data modem (if any) used by the Access Point to make a back haul connection to an enterprise network. The system default Auto Detect directs the system to automatically query the modem and determine its type. Other values include:

- CDMA
- Dual Band GPRS
- Edge GPRS
- Quad Band GPRS (U.S. standard)
- Quad band GPRS (International standard)

An Access Point is ordered as being equipped with a CDMA modem, GPRS modem, or without a modem. Ensure to set this element correctly for your circumstances.

3.16.3.1.1 Matching the Modem Type to the Access Point's Modem

Select from the drop-down list the modem type that is appropriate to your site. Failure to select the proper type may impede back haul communications.

3.16.3.1.2 Configuring Access Points With No Modem

Accept the default value Auto Detect when configuring an Access Point that does not use a cellular modem.

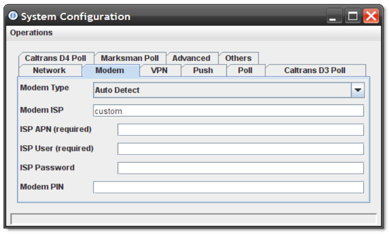
3.16.3.2 Defining the Modem ISP

Modem ISP names the cellular data service carrier. Type the name of one of the carriers from the list below:

- alltel
- caltrans
- cmnet
- cingular
- knp
- telenor
- telia
- telstra

- telus
- tmobile
- verizon
- wyless

Additionally, typing the string `"custom"` opens additional fields to describe the data service carrier.



Modem Type: Auto Detect
Modem ISP: custom
ISP APN (required):
ISP User (required):
ISP Password:
Modem PIN:

Figure 3.84: Custom ISP Properties

3.16.3.3 Defining the ISP Descriptors

Complete the fields for the carrier's access point name (APN), user and password according to the requirements of the carrier. Leave the fields blank if they a re not required by the carrier.

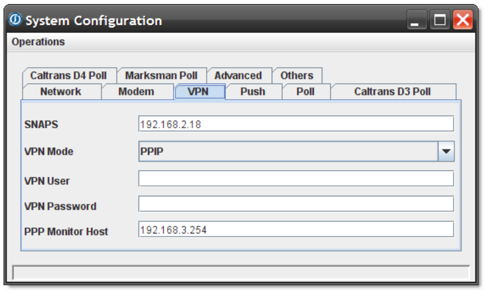
3.16.3.4 Defining the Modem PIN

Modem PIN defines an authentication string if required by the wireless data service carrier. Leave the field blank if a PIN is not required.

3.16.4 Working With 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 Sensys 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: 192.168.2.18
VPN Mode: PPIP
VPN User:
VPN Password:
PPP Monitor Host: 192.168.3.254

Figure 3.85: VPN tab (Optional)

3.16.4.1 Specifying the Sensys Management Server

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

3.16.4.2 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.

3.16.4.3 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.

3.16.4.4 Specifying the Host to Monitor for VPN Communications

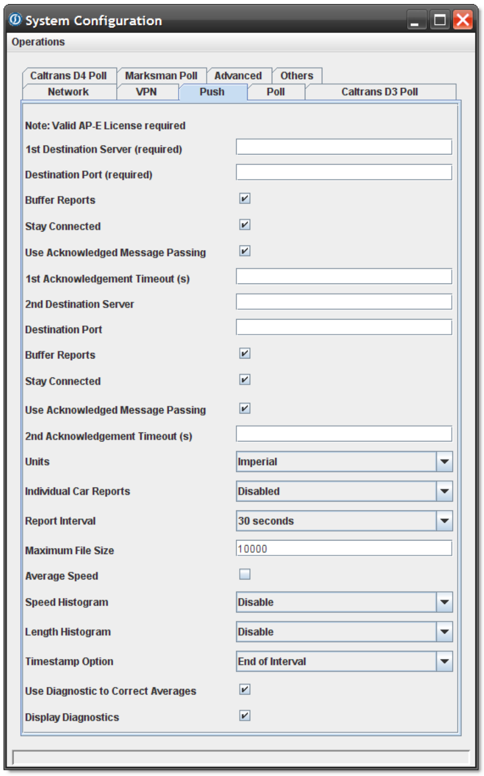
PPP Monitor Host names the host used by the Access Point to maintain the VPN connection. If the Access Point cannot contact this host for a duration of one minute or more, it drops the VPN connection and attempts to reconnect. Typically, this entry points to the VPN server itself. Type a host name or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

3.16.5 Working With 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 Points push process.

Note: use of this feature requires an appropriate license.



Note: Valid AP-E License required

1st Destination Server (required)	
Destination Port (required)	
Buffer Reports	☑
Stay Connected	☑
Use Acknowledged Message Passing	☑
1st Acknowledgement Timeout (s)	
2nd Destination Server	
Destination Port	
Buffer Reports	☑
Stay Connected	☑
Use Acknowledged Message Passing	☑
2nd Acknowledgement Timeout (s)	
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 3.86: Push tab (Requires license)

3.16.5.1 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. The elements for a destination server are described below.

3.16.5.1.1 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.

3.16.5.1.2 Destination Port

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

3.16.5.1.3 Buffer Reports

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

3.16.5.1.4 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.

3.16.5.1.5 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.

3.16.5.1.6 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.

3.16.5.2 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).

3.16.5.3 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 Network's default format
- *Marksman* – produces output that complies with the Marksman specification

3.16.5.4 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

3.16.5.5 Maximum File Size

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

3.16.5.6 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.

3.16.5.7 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

3.16.5.8 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

3.16.5.9 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*

3.16.5.10 Use Diagnostic 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.

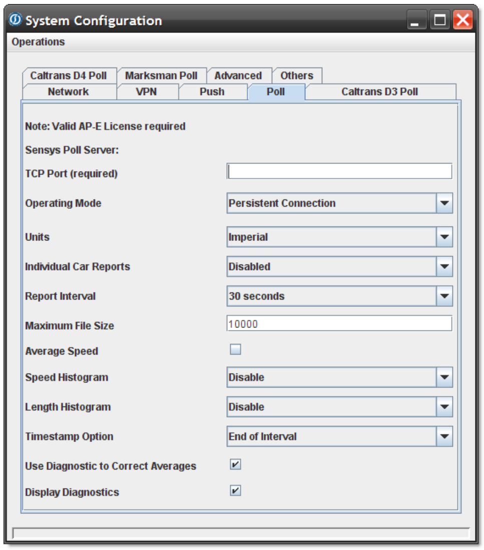
3.16.5.11 Display Diagnostics

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

3.16.6 Working with 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

Sensys Poll Server:

TCP Port (required)	
Operating Mode	Persistent Connection
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 3.87: Poll tab (Requires license)

3.16.6.1 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.

3.16.6.2 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. Rports 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.

3.16.6.3 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).

3.16.6.4 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 Network's default format
- *Marksman* – produces output that complies with the Marksman specification

3.16.6.5 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

3.16.6.6 Maximum File Size

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

3.16.6.7 Average Speed

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

3.16.6.8 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

3.16.6.9 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

3.16.6.10 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*

3.16.6.11 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.

3.16.6.12 Dsiplay Diagnostics

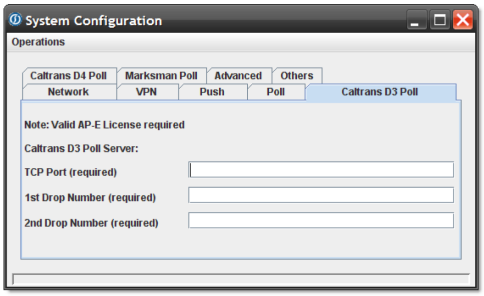
Enables/disables inclusion of the Sensor diagnostic values in the output data collection.

3.16.7 Working with California DOT District 3 Poll Servers

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 Sensys Networks polling interface developed for CalTrans D3 Poll Servers.

Note: use of this feature requires an appropriate license.



Note: Valid AP-E License required

Caltrans D3 Poll Server:

Figure 3.88: CalTrans D3 Pool tab (Requires license)

3.16.7.1 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.

3.16.7.2 1st Drop Number

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

3.16.7.3 2nd Drop Number

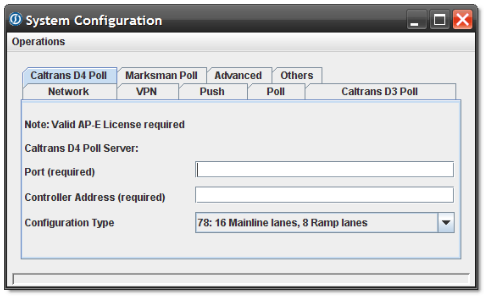
A required value originated by the polling client used by the statistical server to formulate a response message.

3.16.8 Working with California DOT District 4 Poll Servers

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 Sensys Networks polling interface developed for CalTrans D4 Poll Servers.

Note: use of this feature requires an appropriate license.



Note: Valid AP-E License required

Caltrans D4 Poll Server:

Port (required)

Controller Address (required)

Configuration Type: 78: 16 Mainline lanes, 8 Ramp lanes

Figure 3.89: CalTrans D4 Poll tab (Requires license)

3.16.8.1 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.

3.16.8.2 Controller Address

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

3.16.8.3 Configuration Type

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

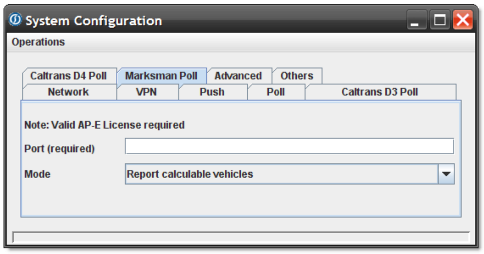
- 71: 8 Mainline lanes, 0 Ramp lanes
- 72: 8 Mainline lanes, 4 Ramp lanes

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

3.16.9 Working with 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.

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



Note: Valid AP-E License required

Port (required)

Mode: Report calculable vehicles

Figure 3.90: Marksman Poll tab (Requires license)

3.16.9.1 Designating the Port Number

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

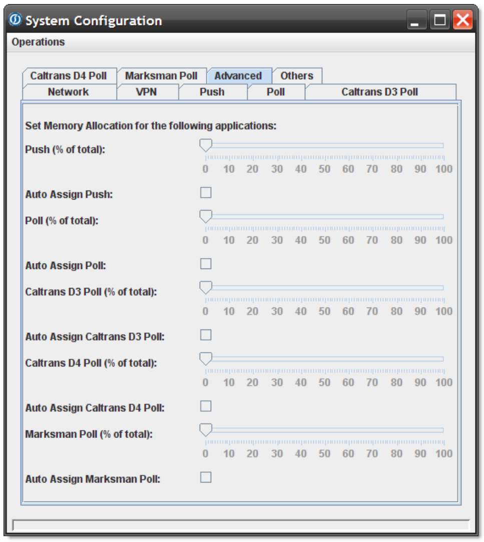
3.16.9.2 Selecting a Reporting Mode

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

- Report only calculable vehicles
- Report all

3.16.10 Configuring Advanced 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 of the *System Configuration* window. A total of **500KB** of memory is allocated to local applications. The memory allocation is configured via the *Advanced* tab.



Set Memory Allocation for the following applications:

Push (% of total):

Auto Assign Push: ☐

Poll (% of total):

Auto Assign Poll: ☐

Caltrans D3 Poll (% of total):

Auto Assign Caltrans D3 Poll: ☐

Caltrans D4 Poll (% of total):

Auto Assign Caltrans D4 Poll: ☐

Marksman Poll (% of total):

Auto Assign Marksman Poll: ☐

Figure 3.91: Advanced tab

3.16.10.1 Window Contents and Operation

The tab displays a slidebar and check box related to memory allocation to the application processes that may execute on an Access Point. The slidebar 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.

3.16.10.2 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(s) to specify this.

3.16.10.3 Manually Allocating Memory to the Processes

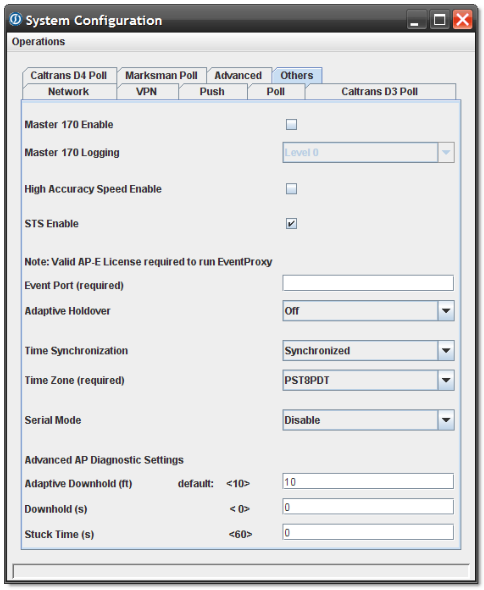
To manually set the memory allocated to one or more of the processes, do the following:

1. Locate the the slidebar related to the desired application and move it to indicate the desired percentage of application memory (500 KB) allocated to that process.
2. From the *Operations* menu, click *Save*. 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.

3.16.11 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 AP diagnostics settings



Master 170 Enable ☐
Master 170 Logging: Level 0
High Accuracy Speed Enable ☐
STS Enable ☑

Note: Valid AP-E License required to run EventProxy
Event Port (required):
Adaptive Holdover: Off

Time Synchronization: Synchronized
Time Zone (required): PST8PDT

Serial Mode: Disable

Advanced AP Diagnostic Settings
Adaptive Downhold (ft) default: <10> 10
Downhold (s) < 0> 0
Stuck Time (s) <60> 0

Figure 3.92: Others tab

3.16.11.1 Enabling the Master 170 Interface for Traffic Signal Controllers

Sensys 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 network to a traffic signal controller.

3.16.11.2 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.

3.16.11.3 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**. See the section *Configuring Sensors* for more information.

3.16.11.4 Enabling the Interface to Siemens Traffic Systems

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.

3.16.11.5 Direct Access to Sensor Event Data

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.

Note: use of this feature requires an appropriate license.

3.16.11.6 Adaptive Holdover

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

3.16.11.7 Time Synchronization Settings

Time is used throughout Sensys 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.

3.16.11.7.1 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 (specified on the *Network* tab of TrafficDOT's *System Configuration* window) and distributed throughout the network by the Access Point
- *Free Running* – each device uses its own internal clock.

3.16.11.7.2 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.

3.16.11.8 Serial Port 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.

3.16.11.8.1 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.

3.16.11.9 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.

3.16.11.9.1 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.

3.16.11.9.2 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.

3.16.11.9.3 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.

3.17 Rebooting an Access Point

Access Points are self-contained computing platforms executing a distribution of the Linux operating system and, as such, may host any process that is compatible with that environment. It is common in such environments to start applications as part of the OS boot process.

Therefore, configuring an Access Point to run a new application will typically require a restart (reboot) to get the application up and running. (*Note*: making entries on many of the tabs of the *System Configuration* window results in the addition of applications to the Access Point.)

Rebooting an Access Point is done via TrafficDOT's *Control* menu.

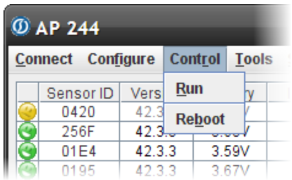


Figure 3.93: Control menu

Click *Reboot* to restart the Access Point, reload its configuration from flash memory and launch applications designated to run on the Access Point.

3.18 Updating Access Point Firmware

Access Point firmware updates are made over the IP network connection with TrafficDOT. Be sure to have the firmware image available to the computer hosting TrafficDOT before beginning.

Note: Access Point firmware can also be updated via a Sensys Management server. Refer to Sensys documents SNAPS Professional Setup & Operations Guide (P/N 152-240-001-005)or Sensys System Manager Setup & Operations Guide (P/N 152-240-001-026) for information regarding performing Access Point firmware updates in that way.

3.18.1 Understanding the Steps in a Firmware Update

Each Access Point firmware update operation consists of the following steps:

- Connecting to the Access Point
- Designating the new firmware image file
- Transferring the new image file to the Access Point
- Verifying the integrity of the image file (*This step occurs automatically*.)
- Updating the Access Point firmware (*This step occurs automatically*.)
- Rebooting the Access Point (*This step occurs automatically*.)
- Confirming the Access Point firmware update

3.18.2 Pre-Update Considerations

Consider these ramifications of firmware update operations before proceeding:

1. *Effect on vehicle detection* – during a firmware update operation all Access Point processes and capabilities are suspended.
2. *Importance of uninterrupted power* – it is essential that power to the Access Point is not interrupted during the firmware update process. Serious damage to the Access Point may result if this consideration is not observed.
3. *Effect on signal control channels* – CC and EX cards receiving detections through the Access Point will receive a constant call for the duration of the update operation.

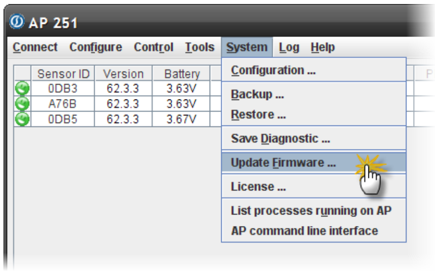
Note: Sensys Networks recommends applying firmware updates first to Sensors, then to Repeaters, and then to the Access Point.

3.18.3 Performing an Access Point Firmware Upgrade

Follow these steps to perform a firmware update:

1. Connect to the target Access Point and start TrafficDOT. (Refer to the section *Connecting to an Access Point* above for more information.)

2. From the *System* menu, click *Update Firmware*. The *Firmware VDS240* window opens.

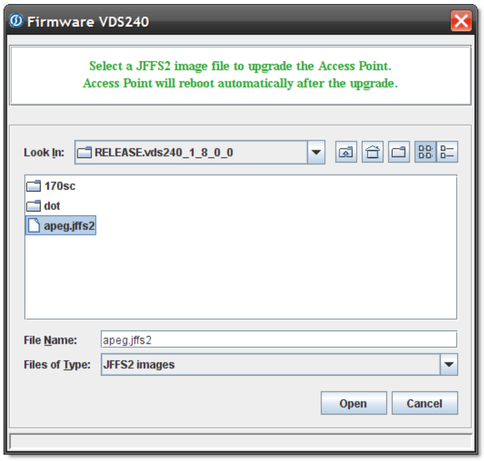


Sensor ID	Version	Battery
0DB3	62.3.3	3.63V
A76B	62.3.3	3.63V
0DB5	62.3.3	3.67V

Figure 3.94: System menu

The window shows the hard disk storage of the computer which is running TrafficDOT.

3. Navigate to the folder that contains the new Access Point firmware image and select the image file by clicking it. Make a note of the VDS version number to which the image corresponds.



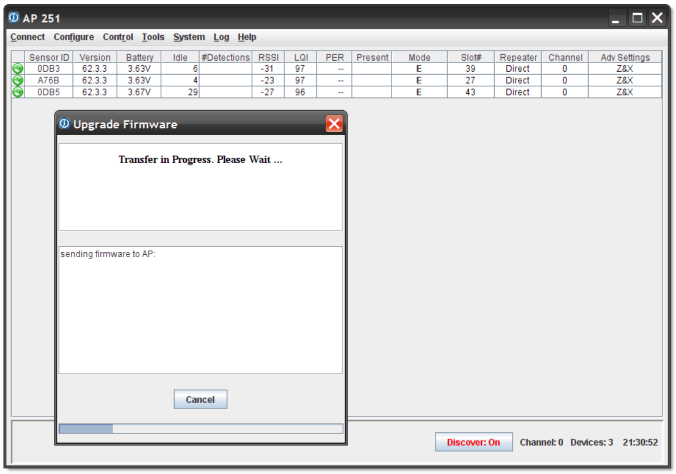
Select a JFFS2 image file to upgrade the Access Point.
Access Point will reboot automatically after the upgrade.

Look In: RELEASE.vds240_1_8_0_0
File Name: apeg.jffs2
Files of Type: JFFS2 images

Figure 3.95: Firmware VDS240 window

Note: Access Point images from Sensys Networks are named *apeg.jffs2*. Never attempt to use a file with a file extension other than JFFS2.

4. Click *Open* to send the firmware image to the Access Point. The *Upgrade Firmware* window opens.



	Sensor ID	Version	Battery	Idle	#Detections	RSSI	LQI	PER	Present	Mode	Slot#	Repeater	Channel	Adv Settings
●	0DB3	62.3.3	3.63V	6		-31	97	--		E	39	Direct	0	Z&X
●	A76B	62.3.3	3.63V	4		-23	97	--		E	27	Direct	0	Z&X
●	0DB5	62.3.3	3.67V	29		-27	96	--		E	43	Direct	0	Z&X

Transfer in Progress. Please Wait ...

```
sending firmware to AP:
```

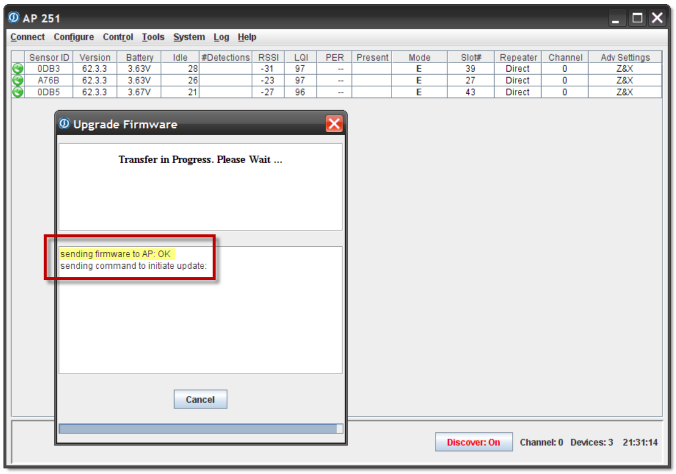
Channel: 0 Devices: 3 21:30:52

Figure 3.96: Downloading Firmware to Access Point

This operation may take a few moments. When connected to the Access Point over cellular data networks or other wide-area topologies, be certain to provide a longer time for the download file transfer to complete. Track progress via the progress bar at the bottom of the *Upgrade Firmware*.

The *Cancel* button can be used to terminate the operation without impacting the Access Point or the detector network.

5. Confirm that a message appears verifying the file was successfully sent to the Access Point as shown below.



	Sensor ID	Version	Battery	Idle	#Detections	RSSI	LQI	PER	Present	Mode	Slot#	Repeater	Channel	Adv Settings
●	0DB3	62.3.3	3.63V	28		-31	97	--		E	39	Direct	0	Z&X
●	A76B	62.3.3	3.63V	26		-23	97	--		E	27	Direct	0	Z&X
●	0DB5	62.3.3	3.67V	21		-27	96	--		E	43	Direct	0	Z&X

Transfer in Progress. Please Wait ...

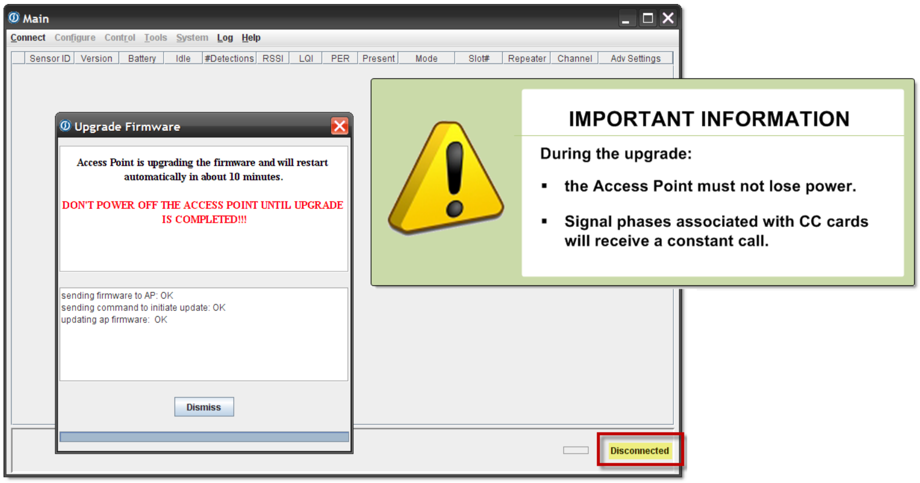
```
sending firmware to AP: OK
sending command to initiate update:
```

Channel: 0 Devices: 3 21:31:14

Figure 3.97: Image file transfer status

When the file was been successfully transferred to the Access Point, the command to commit the image is automatically issued.

6. Confirm that the automatic upgrade process begins by inspecting the *Upgrade Firmware* and *Main* windows.



Access Point is upgrading the firmware and will restart automatically in about 10 minutes.

DON'T POWER OFF THE ACCESS POINT UNTIL UPGRADE IS COMPLETED!!!

```
sending firmware to AP: OK
sending command to initiate update: OK
updating ap firmware:  OK
```

IMPORTANT INFORMATION

During the upgrade:

- **the Access Point must not lose power.**
- **Signal phases associated with CC cards will receive a constant call.**

Figure 3.98: Access Point disconnects during reboot

The upgrade process is active when the message area displays the message "*updating ap firmware: OK*". During the upgrade process the Access Point disconnects itself from TrafficDOT, applies the new firmware image, and restarts. During that time do not interrupt the supply of power to the Access Point. Additionally, note that signal phases associated with the Access Point's CC cards (if any) will receive a constant call.

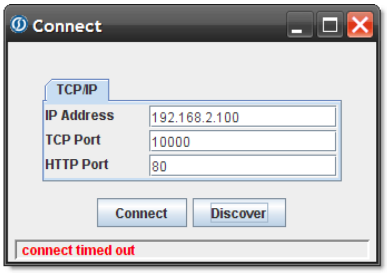
7. Confirm the disconnect of the Access Point by inspecting the connection status monitor at the lower right corner of the *Main* window. Additionally, note the device display table is suppressed. Click the *Dismiss* button on the *Upgrade Firmware* window.

   The upgrade may take up to 10 minutes. The upgrade process completes automatically by rebooting the Access Point. However, a connection to TrafficDOT is not re-established.

8. After approximately 10 minutes, attempt to reconnect to the Access Point using the *Connect* option from the *Connect* menu.

   If a connection is made, the Access Point has rebooted; continue to the next step. However, a connection timeout, shown below, indicates that the Access Point has not completed the upgrade and reboot.

   Note: it is normal for the Access Point to connect and disconnect during the process. Simply wait a few more minutes and attempt to connect to the Access Point again.



IP Address 192.168.2.100
TCP Port 10000
HTTP Port 80

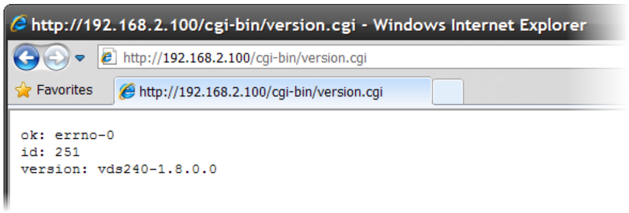
connect timed out

Figure 3.99: Connect window

9. When a connection can be made to the Access Point, verify the VDS240 version identifier.

   Open a browser window with Internet Explorer, Firefox, or other browser. Go to the following URL and inspect the results.

   ```
   http://192.168.2.100/cgi-bin/version.cgi
   ```

   
   http://192.168.2.100/cgi-bin/version.cgi - Windows Internet Explorer
   http://192.168.2.100/cgi-bin/version.cgi
   Favorites
   http://192.168.2.100/cgi-bin/version.cgi

   ```
   ok: errno-0
   id: 251
   version: vds240-1.8.0.0
   ```

   Figure 3.100: Display VDS version id via http command

   Confirm that the *version* identifier string matches the expected version VDS level. A match indicates a successful and complete Access Point firmware upgrade.

10. Disconnect from the Access Point and exit TrafficDOT.

3.19 Checking the VDS Version of an Access Point

The version of the VDS240 software running on an Access Point can be verified by executing a script on the Access Point.

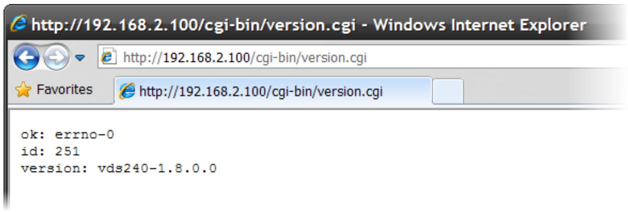
Follow the steps in the section to verify the VDS240 software version:

13. Connect to the target Access Point.
14. Open a browser window with Internet Explorer, Firefox, or other browser. Go to the following URL.

    ```
    http://192.168.2.100/cgi-bin/version.cgi
    ```

> *Note*: the example in this section uses the default IP address of an Access Point. Replace the IP address shown above with any valid IP address of an Access Point.

15. Review the results returned to the browser window.


http://192.168.2.100/cgi-bin/version.cgi - Windows Internet Explorer
http://192.168.2.100/cgi-bin/version.cgi
Favorites
http://192.168.2.100/cgi-bin/version.cgi

```
ok: errno-0
id: 251
version: vds240-1.8.0.0
```

Figure 3.101: Display VDS version level with http command

Ensure the first line includes the string "ok"; if it does not contact Sensys Networks. The text following the label *version:* is the installed VDS240 software level.

16. Close the browser window.

3.20 Backup / Restore an Access Point's Configuration

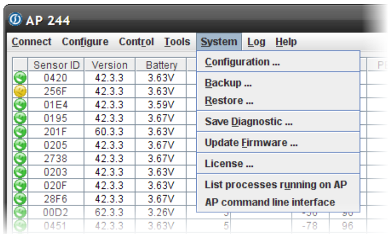
Sensys Networks recommends backing up the configuration of an Access Point once it has been finalized, as well as immediately before and after any significant changes are made.

By default, backups are stored on the file system of the platform that hosts TrafficDOT, but any accessible network file system will suffice. backup files are formatted as Linux "`tar`" files – a file format designed for archiving computer data of all sorts.

Note: these functions are disabled when TrafficDOT connects to an Access Point through a proxy server.

3.20.1 Backup Procedure

Backup activities are initiated from the *System* menu.

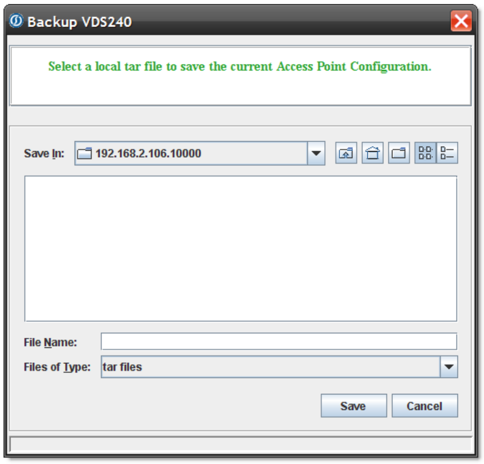


Sensor ID	Version	Battery
0420	42.3.3	3.63V
256F	42.3.3	3.63V
01E4	42.3.3	3.59V
0195	42.3.3	3.67V
201F	60.3.3	3.63V
0205	42.3.3	3.67V
2738	42.3.3	3.67V
0203	42.3.3	3.63V
020F	42.3.3	3.63V
28F6	42.3.3	3.67V
00D2	62.3.3	3.26V
0451	42.3.3	3.63V

Figure 3.102: System menu

To backup the current Access Point configuration, do the following.

1. Click *Backup* from the *System* menu. The *Backup VDS240* window appears.



Select a local tar file to save the current Access Point Configuration.

Save In: 192.168.2.106.10000

File Name:

Files of Type: tar files

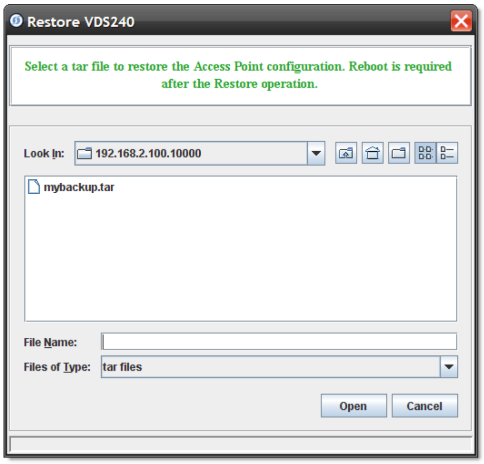
Figure 3.103: Backup VDS240 window

2. Name the file to store the backup. Optionally, store the file to a different folder than the default. Click *Save* to backup the Access Point.

3.20.2 Restore Procedure

Restoring an Access Point's configuration and data from a prior backup is also initiated from the *System* menu. To restore an Access Point configuration and data, do the following.

1. Click *Restore* from the *System* menu. The *Restore VDS240* window appears.



Select a tar file to restore the Access Point configuration. Reboot is required after the Restore operation.

Look In: 192.168.2.100.10000

mybackup.tar

File Name:

Files of Type: tar files

Figure 3.104: Restore VDS240 window

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. Click *Open* to restore the Access Point from the file.

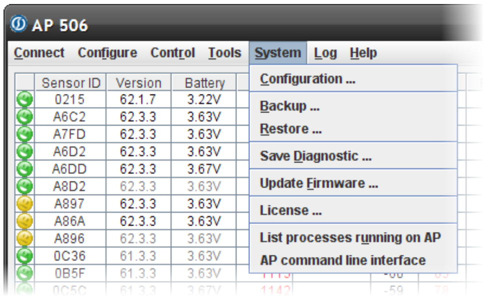
3.20.3 Creating a Diagnostic File

On rare occasions, Sensys Network's 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 performed from the *System* menu and 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.

3.21 Reviewing Processes Executing on an Access Point

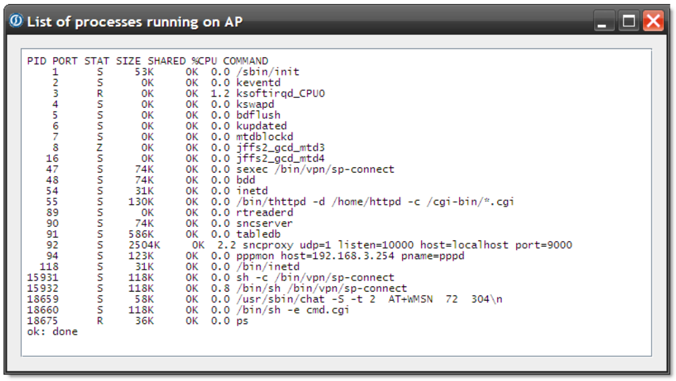
Occasionally, there is a need to review the list of processes that are hosted on an Access Point. You may be directed to inspect this information at the request of Sensys Networks or you may wish to confirm that a process you have configured is actually hosted on the Access Point. A process list is initiated from the *System* menu.



Sensor ID	Version	Battery
0215	62.1.7	3.22V
A6C2	62.3.3	3.63V
A7FD	62.3.3	3.63V
A6D2	62.3.3	3.63V
A6DD	62.3.3	3.67V
A8D2	62.3.3	3.63V
A897	62.3.3	3.63V
A86A	62.3.3	3.63V
A896	62.3.3	3.63V
0C36	61.3.3	3.63V
0B5F	61.3.3	3.63V
0C5C	61.3.3	3.67V

Figure 3.105: System menu

From the *System* menu, click *List processes running on AP*. The process list window appears.



```
PID PORT STAT SIZE SHARED %CPU COMMAND
    1       S     53K      0K  0.0 /sbin/init
    2       S      0K      0K  0.0 keventd
    3       R      0K      0K  1.2 ksoftirqd_CPU0
    4       S      0K      0K  0.0 kswapd
    5       S      0K      0K  0.0 bdflush
    6       S      0K      0K  0.0 kupdated
    7       S      0K      0K  0.0 mtdblockd
    8       Z      0K      0K  0.0 jffs2_gcd_mtd3
   16       S      0K      0K  0.0 jffs2_gcd_mtd4
   47       S     74K      0K  0.0 sexec /bin/vpn/sp-connect
   48       S     74K      0K  0.0 bdd
   54       S     31K      0K  0.0 inetd
   55       S    130K      0K  0.0 /bin/thttpd -d /home/httpd -c /cgi-bin/*.cgi
   89       S      0K      0K  0.0 rtreaderd
   90       S     74K      0K  0.0 sncserver
   91       S    586K      0K  0.0 tabledb
   92       S    2504K      0K  2.2 sncproxy udp=1 listen=10000 host=localhost port=9000
   94       S    123K      0K  0.0 pppmon host=192.168.3.254 pname=pppd
  118       S     31K      0K  0.0 /bin/inetd
15931       S    118K      0K  0.0 sh -c /bin/vpn/sp-connect
15932       S    118K      0K  0.8 /bin/sh /bin/vpn/sp-connect
18659       S     58K      0K  0.0 /usr/sbin/chat -S -t 2  AT+WMSN  72  304\n
18660       S    118K      0K  0.0 /bin/sh -e cmd.cgi
18675       R     36K      0K  0.0 ps
ok: done
```

Figure 3.106: List of Processes Running on AP window

The window displays a list of all processes executing on the Access Point. The display is includes the following columns; note that some lines in the sample above “wrap” to occupy more than a single line.

Element	Description
PID	The process id number. Each process is assigned a unique identifier by the Linux operating system.
PORT	<not displayed>
STAT	The state of the process. A value of “R” indicates a running process; a value of “S” indicates a suspended (sleeping) process.
SIZE	The amount of memory being consumed by the process.
SHARED	The amount of shared memory used by the process.
% CPU	The approximate percentage of time spent running during the entire lifetime of a process.
COMMAND	The command and parameters used to initiate the process.

Table 36: Process List Elements

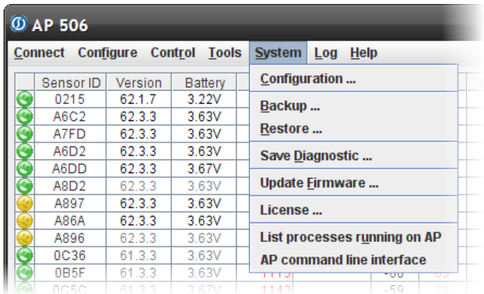
Note: it may be helpful to select all of the text in the display and perform a *copy-and-paste* operation into an application such as MS Excel to format the columns. Click the close window control in the upper right-hand corner to close the window.

3.22 Updating an Access Point's 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.

Note: in the event of a corrupted license file or license key, Access Points recognize a maximum of 12 Sensors. Contact Sensys Networks for assistance.

License file operations are initiated from the *System* menu. (*Note*: you must have a license file on the platform hosting TrafficDOT or another available file system before completing this operation.)

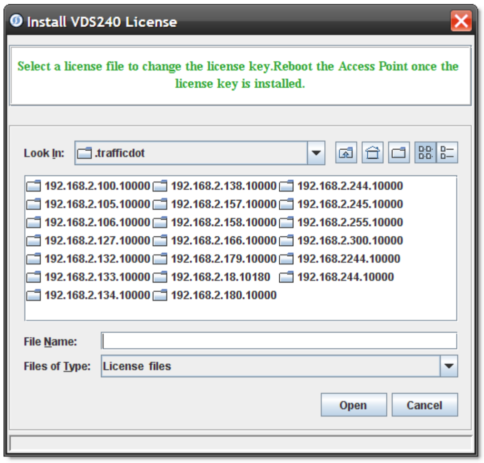


Sensor ID	Version	Battery
0215	62.1.7	3.22V
A6C2	62.3.3	3.63V
A7FD	62.3.3	3.63V
A6D2	62.3.3	3.63V
A6DD	62.3.3	3.67V
A8D2	62.3.3	3.63V
A897	62.3.3	3.63V
A86A	62.3.3	3.63V
A896	62.3.3	3.63V
0C36	61.3.3	3.63V
0B5F	61.3.3	3.63V
0C5C	61.3.3	3.67V

Figure 3.107: System menu

To install/update an Access Point license file, do the following:

1. From the *System* menu, click *License*. The *Install VDS240 License* window appears.



Select a license file to change the license key.Reboot the Access Point once the license key is installed.

Look In: .trafficdot

192.168.2.100.10000
192.168.2.105.10000
192.168.2.106.10000
192.168.2.127.10000
192.168.2.132.10000
192.168.2.133.10000
192.168.2.134.10000
192.168.2.138.10000
192.168.2.157.10000
192.168.2.158.10000
192.168.2.166.10000
192.168.2.179.10000
192.168.2.18.10180
192.168.2.180.10000
192.168.2.244.10000
192.168.2.245.10000
192.168.2.255.10000
192.168.2.300.10000
192.168.2244.10000
192.168.244.10000

File Name:

Files of Type: License files

Figure 3.108: Install VDS240 License

2. Select the file that contains the license for the Access Point. Optionally, navigate to a different folder than the default. Click *Open* to install or update the license file.

3. 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.)

4 Glossary

A

Access Point

A hardware device that collects event data from wireless Sensors and Repeaters, optionally aggregates it, and forwards it to local signal control equipment, traffic management systems or a 3rd party application server.

Access Point proxy

A software process executing on an Access Point or centralized server that brokers requests made of the Access Point. A proxy manages and ultimately reduces the load on the Access Point resulting from upstream applications. (See *Sensys management server*.)

advance detection

Determining the presence of vehicles (in terms of count, classification and speed) as they approach a specified location of interest, such as an intersection.

alert

An activity associated with a detection event (ON/OFF) such that the activity is triggered by each occurrence of the detection event.

AP

A natural abbreviation for the Sensys Networks Access Point. (See also Access Point)

AP240

Wireless vehicle detection system Access Point from Sensys Networks. (See also *Access Point*.)

APDIAG

A utility software program from Sensys Networks. APDIAG produces statistics that characterize SNP connection integrity and Sensor detection differences for a specified period (typically one day). Results are stored in an external file suitable for further analysis, display or processing.

apegid

The unique, 64-bit identifier for an , commonly represented as a HEX string made of the 16 least significant bits.

APPOLLSTAT

A Sensys Networks software application that facilitates transferring event reports from an to a Type 170 signal controller using CalTrans SDRMS formatted packets.

APPOLLSTAT_TCP

A Sensys Networks software application that facilitates transferring event reports from an to a generalized external poll server using Sensys Networks formatted packets.

APPUSHSTAT

A Sensys Networks software application used to intelligently move Sensor data between designated hosts.

APSTAT

A Sensys Networks software program that processes detection event data to produce per vehicle and per lane statistics.

APSTATRECV

A Sensys Networks software application that receives data packets sent by APOLLSTAT or APPOLLSTAT_TCP enabling a distributed network of poll servers.

APTABLE

An internal Sensys Networks software application that reports or updates the databases of Sensor locations and Sensor pairs. This tool is not intended for customer use.

arterial count

Refers to the act of tallying the number of vehicles that pass a designated point on a significant road or thoroughfare. This is a common application for the Sensys Wireless Detection Network.

arterial count station

The location and equipment used to tally vehicles that pass a designated point on a specific road or thoroughfare. (See also *count station*.)

AustRoads specification

Australian Roads specification; *Austroads* is the association of Australian and New Zealand road transport and traffic authorities whose purpose is to contribute to the achievement of improved Australian and New Zealand road transport outcomes.

B

(no entries)

C

CDMA

Code Division Multiple Access, a cellular phone technology used to send data and voice based on a scheme where each transmitter/receiver is assigned a unique code.

Contact Closure cards

Hardware cards that interface a Sensys Networks to a traffic signal controller.

coring

Refers to drilling a small, shallow circular hole in the roadway surface to hold wireless Sensors.

count station

The location and equipment used to tally vehicles that pass a designated point on a road or thoroughfare. (See also *arterial count station*.)

D

default gateway

A node on a computer network that serves as an entry point to another network.

destination server

Names the target of a statistics data file transfer initiated by APPUSHSTAT.

Detect Z Threshold

In regard to the Z axis of the Earth's magnetic field, the magnitude of change from a baseline value necessary to declare a detection event. Detection events are declared as a result of such changes persisting for a predetermined duration.

detection

The activity of measuring changes in the local magnetic field and comparing them to a baseline value to infer presence/absence of vehicles.

detection threshold

Detection is governed by thresholds (defining the degree of change necessary to signal a possible detection) and durations (defining the amount of time the change must last).

Detection zone

An abstract space around a Sensor in which vehicle detection occurs with high probability and accuracy. Beyond the detection zone are the *intermediate* zone and *non-detection* zone.

DHCP

Dynamic Host Control Protocol. An industry standard protocol for automatically assigning IP addresses to network nodes based on a predetermined IP address range and a trusted server. Using DHCP frees network administrators from having to maintain and pre-assign IP addresses.

directional antenna

An antenna that concentrates transmission power into a direction such that coverage distance increases at the expense of coverage angle. The Sensys wireless Sensor, Access Point, and Repeater all use the same type of microstrip patch antenna. The antenna is oriented parallel to and beneath the top surface of the wireless Sensor, while it is oriented parallel to and behind the front face of the and Repeater.

dot

A Sensys wireless Sensor.

DOT

Department of Transportation, a municipal, state, federal or private organization responsible for traffic system design, management, maintenance and operations.

dot pair

Refers to a set of two Sensors, both of which reside in the same lane, from whose event data speed and length measurements are derived.

dot pair table

A database stored on the that holds entries that describe dot pairs.

dot table

A database stored on the that holds entries that describe the Sensors in a given network.

DSSS

Direct Sequence Spread Spectrum. One of two types of spread-spectrum radio technology used in wireless LAN (WLAN) transmissions. To increase a data signal's resistance to interference, the signal at the sending station is combined with a higher-rate bit sequence that spreads the user data in frequency by a factor equal to the spreading ratio.

E

event server

A computer host that tracks detection events and responds to requests related to the events.

EVENTPROXY

A Sensys Networks software application that provides a text/line-oriented interface into raw event data.

Expect Acks

A configuration option of Sensor event reporting such that a Sensor reports only events and expects an acknowledgment of each transmission.

extension

Refers to an amount of time used to adjust the system's interpretation of the falling edge of the waveform associated with an event. (See also *Holdover*.)

extra latency

A fixed amount of latency optionally added by an Access Point to event reporting for the purposes of achieving the most accurate waveform associated with event detection. Using this element normally results in the most accurate count, occupancy and speed calculations at the cost of some degree of responsiveness.

F

Fedora Linux

A distribution of the Linux operating system that is sponsored by the Fedora Project, an undertaking of Red Hat Linux, a commercial provider of Linux tools and support.

freeway count station

See c*ount station*.

ftp

File Transfer Protocol. A common file transfer tool that operates on computer networks. By default, it is unsecured and does not guarantee delivery.

G

GPRS

A standard for wireless communications which runs at speeds up to 115 kilobits per second, compared with GSM (Global System for Mobile Communications) system's 9.6 kilobits. GPRS, which supports a wide range of bandwidths, is an efficient use of limited bandwidth and is particularly suited for sending and receiving small bursts of data.

GPS

A worldwide MEO (medium or middle, earth orbit) satellite navigational system formed by 24 satellites orbiting the earth and their corresponding receivers on the earth. The satellites orbit the earth at approximately 12,000 miles above the surface and make two complete orbits every 24 hours. Devices that use the GPS provide precise co-ordinates for latitude and longitude.

H

holdover

A means of delaying the recognition of the end of a detection event. *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.

I

IEEE 802.15.4

IEEE 802.15 is the 15th working group of the IEEE 802 which specializes in Wireless PAN (Personal Area Network) standards. It includes five task groups (numbered from 1 to 5). Group 4 (Low Rate WPAN) concentrates on low data rate but very long battery life (months or even years) and very low complexity. The specification for the physical layer of the radio used by the Sensys Wireless Vehicle Detection system is based on this standard. This specification has also been adopted by the Zigbee Standard.

individual car reports

Designates a type of statistical output wherein data is reported for individual vehicles as events occur as opposed to aggregated over a period of time. Also known as *real-time reporting*.

IP

Network layer protocol in the TCP/IP stack offering a best-efforts, connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly and security.

IP address

A unique number assigned to any node connected to an IP-based network.

ISM band, ISM channel

Industry, Scientific and Medical Band. A range of unlicensed radio frequencies that include 902 - 928 MHz, 2.4 - 2.4835 GHz and 5.725 - 5.850 GHz with RF power up to 1 watt. Frequency hopping or direct sequence transmission is allowed. Sensys networks operate in the 2.4 GHz ISM band.

ISP

Internet Service Provider. An entity, normally for-profit, that sells a connection to the broader IP-based network commonly known as the Internet. ISP's typically offer a range of value-added services to their clients including infrastructure services (IP addressing, security, bandwidth management), data/file transmission services, and applications (email, messaging, web site development, etc.)

L

latency

Generally, latency refers to the time delay resulting from sending packets across a network. In regard to a Sensys network, latency is usually thought of as the difference between when an event is detected by a Sensor and when that event is received by the .

LQI

A metric of Sensys Networks, LQI is an indicator of the signal-to-noise ratio (SNR). LQI will be affected by both RF signal strength and local RF interference. TrafficDOT displays LQI as a number between 40 and 99, with 99 representing optimal quality. LQI values above 95 are considered “good”; LQI values around 90 are considered “adequate”.

M

master mode

A configuration option controlling when an Access Point begins transmitting. In prior releases, Access Points put into master mode begin transmitting immediately upon receiving power. This behavior is now the default system state.

maximum reporting latency

The maximum amount of time that may pass between successive transmissions from a given Sensor. Alternatively, it can be described as the maximum period during which events will be queued prior to reporting.

microstrip patch antenna

The type of directional antenna used in Access Points, Sensors and Repeaters. These antennas conduct RF energy in a non-uniform pattern.

mode

In regard to Sensors, a mode dictates the type of detection behavior exhibited. Different modes require different packet sizes which, in turn, may impact time slot assignment.

N

NAT

Network Address Translation. A network service that involves re-writing the source and/or destination addresses of IP packets as they pass through a router or firewall. An important result is the hiding of IP addresses.

network mask

Determines what computers can be accessed locally without using a gateway, and what computers can only be reached through a gateway. The bits in the network mask determine what is a network and what is a computer.

NEVENTS / Near full

These parameters set 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. When the “near full” state is reached, the Sensor transmits data at its next opportunity (its next time slot) without regard to how much time is left in the *Max. Reporting Latency* counter.

ntp

Network Time Protocol. A protocol to exchange and synchronize time between hosts on computer networks.

O

Onset filter

A means to delay the recognition of the start of a vehicle detection. Specifies the number of consecutive samples for which the ON condition must be true before a detection event is true.

Overhead

Framing, error control, addressing, idle code, or any other characters or bit sequences in a data transmission other than actual end-user data.

P

PeMS

Performance Monitoring System. Server software from Berkeley Transportation Systems, Inc. that uses statistical algorithms to extract information from an existing Sensor system to compute long-term performance measures over a freeway system.

permanent count station

See *count station*.

port

A logical connecting point for a process. Data is transmitted between processes through ports (or sockets). Each port provides queues for sending and receiving data.

port number

See *port*.

PPTP

Point-to-Point Tunneling Protocol. Point-to-Point Tunneling Protocol (PPTP) is a protocol (set of communication rules) that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. Effectively, a corporation uses a wide-area network as a single large local area network. This kind of interconnection is known as a virtual private network (VPN).

primary DNS

The host on a computer network that first responds to a request for domain name resolution. Typically, there are primary and secondary DNS servers designated for every site.

pulse mode

A type of event reporting where only the leading edge of the detection pulse is reported. This is implemented via the property *Report only ON events*.

R

RADIUS server

Remote Authentication Dial In User Service.   A host offering an industry standard authentication, authorization and accounting protocol for applications such as network access or IP mobility.

reboot

Restarting a hardware device resulting in a full cycle of post-on self-testing, reinitialization of operating system software and other start-up processes. Rebooting an results in it reacquiring its license file and launching any new application instances that have been defined.

reference value

With regard to Sensors, this value is the baseline value of the local magnetic field to which detected changes are compared. Sensors automatically rebaseline themselves through a process called recalibration.

Repeater

An optional system component that extends the range of an by receiving and forwarding RF communications between the and Sensors that would otherwise be out of signal range.

Repeater coverage area

A physical area approximately corresponding to the beam pattern of a Repeater such that Sensors located in the coverage area attain acceptable RF performance with the Repeater.

RF

Radio frequency. Sensys networks operate in the 2.4 GHz ISM band.

RF channel

A discrete radio frequency range within the unlicensed ISM band in which Sensys networks operate.

RP

A natural abbreviation for the Sensys Networks Repeater. (See also *Repeater*.)

RP240-B

Wireless vehicle detection system Sensor signal Repeater from Sensys Networks. (See also *Repeater*.)

RP240-B-LL

Wireless vehicle detection system Sensor signal Repeater from Sensys Networks equipped with extended life battery pack. (See also *Repeater*.)

RPM

Redhat Package Manager. RPM Package Manager (originally Red Hat Package Manager, abbreviated RPM) is a package management system. The name RPM refers to two things: a software package file format, and a free software tool which installs, updates, uninstalls, verifies and queries software packaged in this format. RPM is used in conjunction with the Linux operating system that operates on Sensys Networks's Access Points.

RSSI

A metric used by Sensys Networks, Received Signal Strength Indicator, expresses signal strength. RSSI is measured in dBm, dB relative to 1 mW into a 50 Ohm impedance. Typical RSSI numbers will range from -50dBm (for Sensors very close to a receiver) to -95dBm (the far edge of RF coverage).

RSSI threshold

A user configurable value to which actual RSSI measurements are compared for the purpose of visually highlighting poor radio signal strength on the *Access Point Main window*.

S

San Diego Ramp Metering System (SDRMS)

The most widely used ramp metering control algorithm used in California.

Sensor

A sensitive magnetometer capable of low-power radio communications packaged in a small, hardened plastic case suitable for pavement mounting.

Sensor channel

The RF channel (frequency) used by a Sensys Repeater to communicate with the Sensors serviced by the Repeater. The Sensor channel must be distinct from the Repeater's channel to avoid RF interference.

Sensor coverage area (SCA)

An imaginary area of physical space that approximates the area of acceptable RF performance for a given or Repeater. Sensors within a given device's SCA will operate with significantly better RF quality than Sensors that are outside of the SCA.

Sensor pair

(See *dot pair*.)

SensorID

A unique, 64-bit identifier assigned to each Sensor at the factory. Typically, this value is represented as a 4-character HEX string.

Sensys Management server

An application server that combines services essential to management of large wireless Sensor networks. Services include diagnostic and health monitoring, remote maintenance and configuration, vehicle data archiving, statistical processing and output display, and other functions.

Signal to noise ratio (SNR)

A term for the power ratio between a signal (meaningful information) and the background noise. The higher the ratio, the less the noise impedes communications.

SIM card

Subscriber Identity Module card; a small printed circuit board installed in a GSM terminal to enable operations on a network. The card contains subscription details, security information and a variable amount of memory for user data. Sensys Access Points support SIM cards for use with cellular data services.

slot

A column heading on the *Access Point Main window* that displays the time slot used by a Sensor or Repeater. Design rules of the SNP protocol require that no two devices transmit to the same receiver via the same time slot.

SNCPROXY

A utility software application developed by Sensys Networks providing a proxy services for Access Points. In large installations, SNCPROXY is used to reduce (*i*) the work load of the processors on the Access Points and (*ii*) the overall bandwidth necessary to manage the system.

SNP

Sensys Nano-Power protocol. A proprietary network protocol developed by Sensys Networks that enables reliable data communications between a Sensys wireless Sensor and its communicating or Repeater with very low latency and extremely low power consumption.

statistics server

A host computing platform that compiles statistics from raw Sensor event data and responds to requests for the statistics.

stop bar

A solid white line, normally 12 to 24 inches wide, extending across all approach lanes to a STOP sign or traffic signal, placed parallel to the centerline of the intersecting street.

stuck high

A momentary state of a Sensor wherein detection is suspended. Typically resetting the Sensor clears this condition.

superuser

A term commonly found in Unix/Linux environments that refers to a computer user account with unrestrained access permissions.

sync packet

A management packet broadcast by Access Points for the purposes of time synchronization and device transmission coordination.

synchronized reporting

A mode of Sensor event data reporting where reports are made at predetermined, fixed intervals relative to a uniform network time. This mode of reporting can be thought of as “time driven” reporting.

T

TDMA

Time division multiple access. A channel access method for shared medium (usually radio) networks. It allows several users to share the same frequency channel by dividing the signal into different time slots. Users transmit in rapid succession, one after the other, each using their own time slot. This allows multiple stations to share the same transmission medium (e.g. radio frequency channel) while using only the part of its bandwidth they require. The SNP protocol is a TDMA-based protocol.

time slot

A section or “slice” of a transmission frame that provides an opportunity for a node to transmit. Time slots sequentially order and coordinate transmissions in a TDMA based environment. The SNP protocol prohibits multiple devices from transmitting in the same time slot.

TrafficDOT

A Java-based software application developed by Sensys Networks, that enables real-time configuration, management and monitoring of a network and all of its associated devices (Sensors, Repeaters and Contact Closure cards).

transmit interval

Defines how often any particular device is allowed to transmit on an SNP network, and as such, influences the number of devices in a given network. The transmit interval is configured on the *Event* tab of the *Access Point Configuration* window.

TTI specification

Data specification and format guide from the Texas Transportation Institute (TTI), a department at Texas A&M University that does research on transportation to increase the safety and efficiency of vehicles (as well as roads and rails, in the case of ground transport).

tunneling

A network communications technique where a given protocol is used to encapsulate a second protocol for transport. Tunneling can be used to carry a payload over an incompatible delivery network, or to provide a secure path through an untrusted network.

U

undetect

Refers to an observation of the local magnetic field such that the change relative to the baseline value has subsided, which in turn, infers that a vehicle is no longer present.

Undetect X Threshold

An element that determines how far the measured value for the X axis must fall before a detection event is deemed to be over.

Undetect Z Threshold

An element that determines how far the measured value for the Z axis must fall before a detection event is deemed to be over.

V

VDS240

Wireless vehicle detection system from Sensys Networks.

VPN

Virtual Private Network. A virtual private network is a communications network tunneled through another network and dedicated for a specific use. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. Access Points can establish a VPN connection to a Sensys management server to facilitate remote management and other functions.

VSN240

Wireless vehicle detection Sensor from Sensys Networks. (See also *Sensor*.)

W

watchdog timeout

An interval after which the Sensor makes a transmission without regard to whether an event detection has occurred. Typically watch dog timeout values are 30 seconds; longer intervals will preserve battery life.

workingFile

The name of the temporary, output file used by APSTAT (and other applications) as it generates statistics; this file is subsequently renamed with the timestamp of the last entry in the file.

X

X mode

An operating mode supported by Sensys Contact Closure Master and Extension cards that directs the card to display Card ID values set by the circuit-board switch SW2.

Y

(no entries)

Z

Zone of detection

(See *detection zone*.)

5 Appendixes

5.1 TrafficDOT Menu Hierarchy

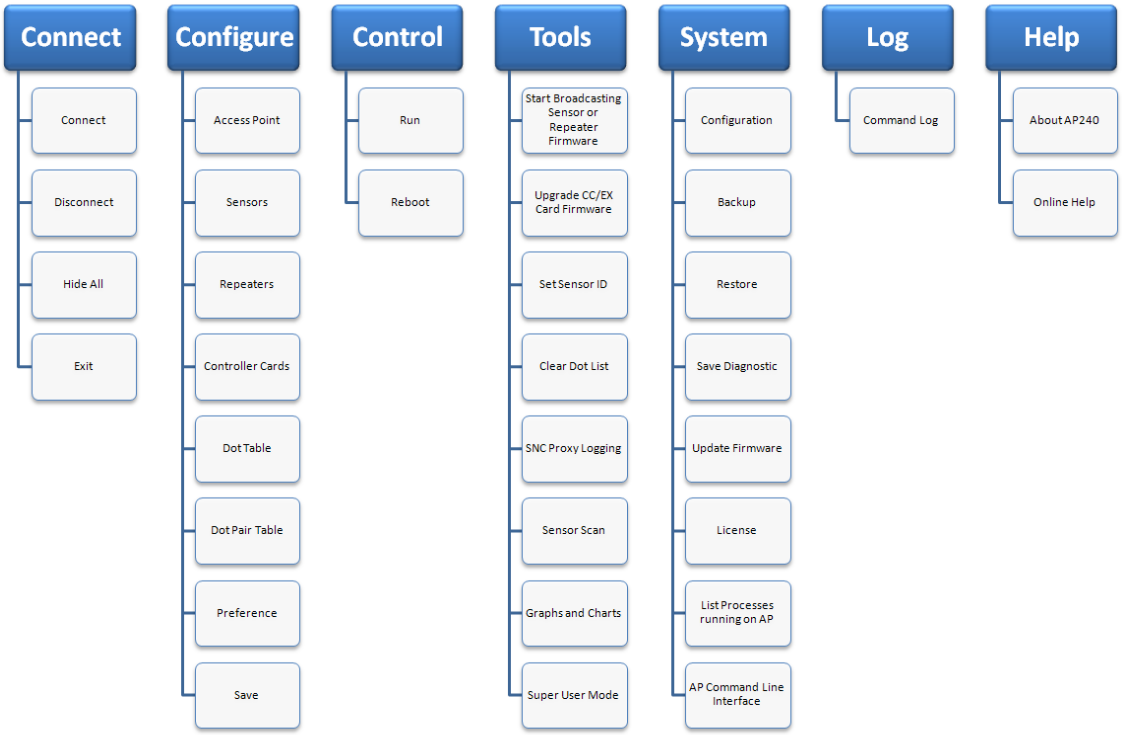


Figure 5.1: TrafficDOT (v1.10) Menus and Commands

5.2 Contact Closure Card External Interfaces

This appendix shows the connector pin assignments for the external interfaces of Sensys Contact Closure Master and Expansion cards.

5.2.1 Backplane Edge Connections

Pin	Function (TS1 mode)	Function (TS2 mode)
1	Not connected	Channel 1 Delay enable
2	Not connected	Channel 2 Delay enable
3	Address 3	Address 3
4	Daisy chain RS485 Uplink +	Daisy chain RS485 Uplink +
5	Daisy chain RS485 Uplink -	Daisy chain RS485 Uplink -
6	Address 0	Address 0
7	Not connected	Channel 1 status
8	Daisy chain RS485 Downlink +	Daisy chain RS485 Downlink +
9	Daisy chain RS485 Downlink -	Daisy chain RS485 Downlink -
10	Address 1	Address 1
11	AC power neutral	AC power neutral
12	AC power line	AC power line
13	Not connected	Not connected
14	Not connected	Not connected
15	Address 2	Address 2
16	Not connected	Channel 3 status
17	Not connected	Not connected
18	Not connected	Not connected
19	Not connected	Not connected
20	Not connected	Channel 2 status
21	Not connected	Not connected
22	Not connected	Channel 4 status
A	GND	GND
B	24V	24V
C	Reset input	Reset input
D	Not connected	Not connected
E	Not connected	Not connected
F	Channel 1 collector	Channel 1 collector
H	Channel 1 emitter	Channel 1 emitter
J	Not connected	Not connected
K	Not connected	Not connected

Table 37: Backplane edge connections (continued on following page)

(Note: Backplane edge connection table, continued from prior page).

Pin	Function (TS1 mode)	Function (TS2 mode)
L	Chassis Ground	Chassis Ground
M	AC power neutral	AC power neutral
N	AC power line	AC power line
P	Not connected	Not connected
R	Not connected	Not connected
S	Channel 3 collector	Channel 3 collector
T	Channel 3 emitter	Channel 3 emitter
U	Not connected	Not connected
V	Not connected	Not connected
W	Channel 2 collector	Channel 2 collector
X	Channel 2 emitter	Channel 2 emitter
Y	Channel 4 collector	Channel 4 collector
Z	Channel 4 emitter	Channel 4 emitter

Table: (continued from prior page) Backplane edge connections

5.2.1.1 Notes

1. Pins G, I, O, and Q are not implemented.

5.2.2 IN RJ45 Connector Pin Assignments

Pin	Function on CC Card	Function on EX Card
1	Not connected	Daisy Chain RS485 Downlink +
2	Not connected	Daisy Chain RS485 Downlink -
3	Not connected	Daisy Chain Uplink +
4	RS485+	Not connected
5	RS485-	Not connected
6	Not connected	Daisy Chain RS485 Uplink -
7	+48V	Not connected
8	48V Return	Not connected

Table 38: IN RJ45 connector pin assignments

5.2.3 OUT RJ45 Connector Pin Assignments

Pin	Function on CC and EX Cards
1	Daisy Chain RS485 Downlink +
2	Daisy Chain RS485 Downlink -
3	Daisy Chain RS485 Uplink +
4	Not connected
5	Not connected
6	Daisy Chain RS485 Uplink +
7	Not connected
8	Not connected

Table 39: OUT RJ45 connector pin assignments

5.3 Marksman Protocol Specification

The Marksman protocol is defined as a set of ASCII text delimited by commas. A sample of the output is given below as used for the TransActive interface.

```
0024a4dc000000b4,1,201109,1049,07,105,0,0,1,2.726,2.546,-1,-1,,0.320,0.220
0024a4dc000000b4,2,201109,1049,09,011,0,0,1,1.751,1.531,-1,-1,,0.227,0.375
0024a4dc000000b4,3,201109,1049,11,542,0,0,1,2.641,2.266,-1,-1,,0.259,0.266
0024a4dc000000b4,4,201109,1049,13,503,0,0,1,2.000,1.734,-1,-1,,0.211,0.227
0024a4dc000000b4,5,201109,1049,15,387,0,0,1,1.875,1.648,-1,-1,,0.258,0.234
0024a4dc000000b4,6,201109,1049,17,098,0,0,1,1.711,1.477,-1,-1,,0.227,0.234
0024a4dc000000b4,7,201109,1049,18,879,0,0,1,1.789,1.555,-1,-1,,0.234,0.227
0024a4dc000000b4,8,201109,1049,20,723,0,0,1,1.883,1.656,-1,-1,,0.281,0.188
0024a4dc000000b4,9,201109,1049,22,424,0,0,1,1.719,1.531,-1,-1,,0.227,0.171
0024a4dc000000b4,10,201109,1049,24,339,0,0,1,1.836,1.665,-1,-1,,0.164,0.250
0024a4dc000000b4,11,201109,1049,26,261,0,0,1,1.984,1.734,-1,-1,,0.242,0.188
```

Figure 5.2: Marksman output sample

The format is described in the table below:

Field	Element	Sample	Notes
1	ApegID	0024a4dc000000b4	
2	Record Number	1	From 0 to 999,999, then wrapping
3	Date of Record	201109	DDMMYY format
4	Time	1049	Hours and minutes
5	Seconds	11	
6	Milliseconds	339	
7	(Ignored)	0	Not used
8	Lane Identifier	1	Starting with one (1)
9	Direction	1	Sensys alarms on change of direction
10	Headway	2.73	Time in seconds between the front of successive vehicles
11	Gap	2.55	Time in seconds between the front of this vehicle and the rear of the previous vehicle
12	Speed	-1	Kilometers per hour
13	Vehicle Length	-1	Expressed in centimeters
14	Vehicle Class	<blank>	Not used
15	Vehicle Duration (Leading)	0.156,	Vehicle duration over leading sensor; expressed in seconds to three decimal places.
16	Vehicle Duration (Trailing)	0.180	Vehicle duration over trailing sensor; expressed in seconds to three decimal places.

Table 40: Marksman Protocol Element Description

5.4 Index of Tables

5.5 Index of Figures