S3100 User Manual

VERINT

POWERING ACTIONABLE INTELLIGENCE™

S3100

Firmware Release 3.30

User Manual

Verint Video Solutions

By providing this document, Verint Systems Inc. is not making any representations regarding the correctness or completeness of its contents and reserves the right to alter this document at any time without notice.

Published by:

Verint Video Solutions
1800 Berlier Street
Laval (Quebec)
Canada
H7L 4S4
www.verint.com/smartsight

Publication date: February 10, 2005

Contents

Preface

The *S3100 User Manual* presents the information and procedures on installing and configuring the SmartSight® S3100 outdoor wireless bridge.

Who Should Read this Manual

This manual is intended for engineers and technicians who will install the S3100 units. It provides conceptual information on how to configure, install, and operate the units.

This manual assumes that you are familiar with:

- Installation and manipulation of electronic equipment
- General use of computers
- Microsoft Windows operating systems
- Local area networks (LANs) and basic IP data communication concepts and practices
- Radio frequency (RF) regulations

How to Use this Manual

This manual contains all the information needed to install and configure an S3100 unit.

Contents

The *S3100 User Manual* is divided into the following chapters:

1. **Overview**—Provides a brief description of the features of the S3100 unit and illustrations of its casing.
2. **System and RF Planning**—Lists the available frequency bands and describes planning operations relative to system setup and radio frequency (RF).
3. **Configuring and Installing the Unit**—Presents the configuration and installation procedures for the S3100 unit.
4. **Setting Parameters with the CLI**—Explains how to program the S3100 unit using the SmartSight command line interface.

The manual also includes the following appendixes:

A. **Factory Default Configuration**—Lists the default parameter values of the S3100 unit.

B. **RJ-45 Ethernet Cables**—Presents the pinouts of the straight-through and crossover Ethernet cables.

C. **Pole Mounting of the Antennas**—Shows how to install on a pole the antennas supplied by Verint Video Solutions.

D. **DHCP Support and APIPA Service**—Explains how the dynamic host configuration protocol server and the Microsoft APIPA service work.

E. **Surge Protection**—Describes how to protect the S3100 unit from voltage and current surges.

F. **RF Contact between Masters**—Explains how to ensure that two master units “see” each other.

G. **Separation Between Units Using Adjacent Channels**—Lists the minimum distances between units using adjacent frequency channels.

H. **Technical Specifications**—Lists the complete technical specifications of the S3100 units.

A glossary, an index, and compliance information complete the manual.

Conventions

The following typographic conventions are used throughout this manual:

Visual cue	Meaning
Connect	The name of an interface element you have to act on. A key to press. The value of an interface element.
Advanced > **VSIP**	Any sequence of steps (in the menu structure of a graphical application, in the navigation structure of a web site, and so on).
connection_name	Text that must be replaced by a user-supplied value. Text representing variable content.
`S3100.xh`	The name of a command, file, or directory. Text that appears on the screen. Examples of user-supplied values.

Related Documentation

In addition to this manual, the following documentation is also available:

- *S3100 Installation Guide*—Contains the configuration steps and the installation procedure for the S3100 unit.
- *SConfigurator User Manual*—Presents the instructions on how to use a proprietary Verint Video Solutions software to configure the unit, connect it to other units, and update its firmware.
- *Release Notes*—Contain information about S3100 upgrades and known issues still under investigation, as well as a description of features not covered in this version of the documentation.

All these documents are contained on the *SmartSight Utilities* CD shipped with the unit. Furthermore, a paper copy of the installation guide is included with your order.

Related Verint Video Solutions Products

You can use the S3100 units with the S1100 wireless systems, the S1100w wireless video transmitters, and the S1500e series and S1600e Ethernet video servers.

For more details about any of these products, visit our web site. For pricing information, call your dealer.

About Us

Verint Systems (NASDAQ: VRNT) is a leading global provider of video security, surveillance and business intelligence solutions. Verint Video Solutions transform digital video into actionable intelligence: timely, mission-critical insights for faster, more effective decisions.

Today, more than 1000 companies in 50 countries use Verint Systems solutions to enhance security, boost operational efficiency, and fuel profitability.

Web Site

For information about the SmartSight line of products, visit www.verint.com/smartsight. To download the product specifications, application notes, and user documentation, as well as to request the latest versions of firmware and software, use the following links:

To access	Visit
Complete selection of what is available:	www.verint.com/smartsight/support
User documentation:	www.verint.com/smartsight/manuals
Various tools and demos:	www.verint.com/smartsight/tools
Firmware upgrade requests:	www.verint.com/smartsight/firmware_upgrade

Support

If you encounter any type of problem after reading this manual, contact your local distributor or Verint Video Solutions representative. You can also use the following sections on our web site to find the answers to your questions:

To access	Visit
Technical support request form:	www.verint.com/smartsight/request
Solution database (FAQ):	www.verint.com/smartsight/faq
Login to our customer service system:	www.verint.com/smartsight/account

Verint Video Solutions technical support personnel is available to help you use your SmartSight units and the related software:

- On the web: www.verint.com/smartsight/request
- By phone: 1 888 494-7337 (North America) or +1 450 686-9000 Monday to Friday, from 8:30 to 17:30 EST
- By fax: +1 450 686-0198

Warranty

Each product manufactured by Verint Systems is warranted to meet all published specifications and to be free from defects in material and workmanship for a period of two (2) years from date of delivery as evidenced by the Verint Systems packing slip or other transportation receipt. Products showing damage by misuse or abnormal conditions of operation, or which have been modified by Buyer or repaired or altered outside Verint Systems factory without a specific authorization from Verint Systems shall be excluded from this warranty. Verint Systems shall in no event be responsible for incidental or consequential damages including without limitation, personal injury or property damage.

The warranty becomes void if the product is altered in any way.

Verint Systems responsibility under this warranty shall be to repair or replace, at its option, defective work or returned parts with transportation charges to Verint Systems factory paid by Buyer and return paid by Verint Systems. If Verint Systems determines that the Product is not defective within the terms of the warranty, Buyer shall pay all handling and transportation costs. Verint Systems may, at its option, elect to correct any warranty defects by sending its supervisory or technical representative, at its expense, to customer’s plant or location.

Since Verint Systems has no control over conditions of use, no warranty is made or implied as to suitability for customer’s intended use. There are no warranties, expressed or implied, except as stated herein. This limitation on warranties shall not be modified by verbal representations.

Equipment shipped ex works Verint Systems factory shall become the property of Buyer, upon transfer to the common carrier. Buyer shall communicate directly with the carrier by immediately requesting carrier’s inspection upon evidence of damage in shipment.

Buyer must obtain a return materials authorization (RMA) number and shipping instructions from Verint Systems prior to returning any product under warranty. Do not return any Verint Systems product to the factory until RMA and shipping instructions are received.

1

Overview

The S3100 is the latest addition to the SmartSight family of outdoor, wireless, digital video bridging products. It covers the 2.4 GHz and 5 GHz frequency bands in North America and Europe.

Note: The S3100 units require professional installation.

About the S3100

The S3100 license-free video bridge has many uses, including:

- Point-to-multipoint application—One S3100 bridge and multiple S1100w units
- Point-to-point repeater—Two S3100 units acting as a range extender for one or many pairs of S1100 units
- Point-to-multipoint repeater—Two S3100 units acting as a range extender for multiple S1100w units
- Wireless bridge—Two S3100 units linking two networks (wired or wireless)

To cover these application types, the following S3100 models are available:

- *S3100-RP*: A repeater device made up of two units
- *S3100*: A single unit for the other applications

Unless otherwise specified, the word *S3100* refers to any of these units.

Every S3100 unit comes with the following security features:

- SSL—Every unit is shipped with a unique SSL (secure sockets layer) certificate for securing its IP link. SSL is a commonly used protocol for managing the security of IP message transmission. Therefore, the connections between two units or between a unit and the SConfigurator tool can be secured.

  The SSL protocol secures the VSIP communication data. It does not apply to audio and video transmission.

  Once a unit is in secure mode, you cannot access it anymore with Telnet and you cannot perform firmware updates through the IP network on it. However, you can configure it with SConfigurator.

  For more information about this security feature, refer to the *SConfigurator User Manual*.

- SPCF/SDCF—These proprietary MAC (media access control) protocols use AES encryption (with key rotation) over the wireless link to secure communication between the units. They secure VSIP communication as well as audio and video data. For more information, see page 12.

Shipment

Your shipment contains the following items:

- The requested outdoor wireless bridge
- For an *S3100* unit:
  - A power-over-Ethernet kit (injector and power cord)
  - An 82-foot (25-meter) straight-through outdoor Ethernet cable (may be replaced by the optional *ECAB-50* cable)
- For an *S3100-RP* unit:
  - A 3-foot (1-meter) outdoor crossover Ethernet cable
  - Two 30-foot (10-meter) 24V AC outdoor power cords
- A wall mount bracket set, already installed on the unit
- One or two pole mount bracket sets, including stainless steel clamps
- The *SmartSight Utilities* CD containing the release notes and documentation for the unit as well as the SConfigurator application
- The *S3100 Installation Guide*

The shipment may also contain the following options:

- One or two high-gain antennas

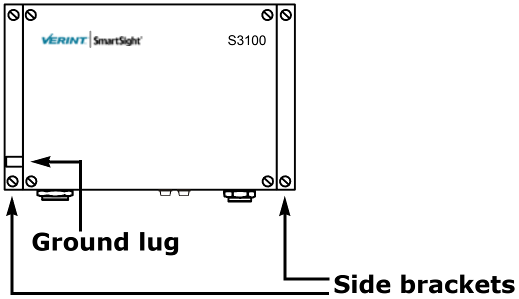
  Warning: When choosing antennas, you must ensure that the combined transmission power of the unit and antenna does not exceed the maximum value established by your country's regulations. For more information, see page 28.

- For an *S3100* unit:
  - A 164-foot (50-meter) straight-through outdoor Ethernet cable (*ECAB-50*)
- For an *S3100-RP* unit:
  - One or two 24V AC external power supplies (*PS2440*)

  Note: If you are using power supplies other than those supplied by Verint Video Solutions, you need to ensure that they have a minimum capacity of 30 VA.

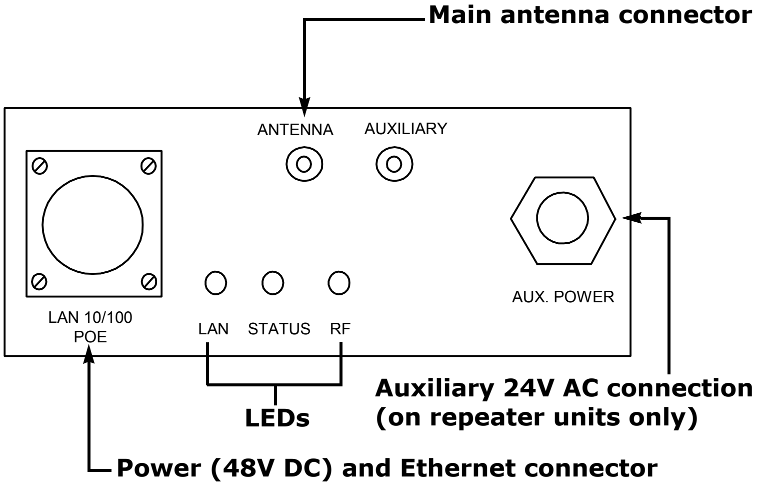
Casing Description

The S3100 electronics are enclosed in a weather-tight cast aluminum module. All cable entries are mounted on the underside of the unit to maintain its weatherproof properties. Here is the S3100 casing:



The unit underside integrates:

- A power and Ethernet connector
- Three LEDs
- Two female antenna connectors (the auxiliary connector is for future development)
- An optional 2-pin 24V AC auxiliary power connector (on the repeater units only)



2

System and RF Planning

To allow optimal configuration, you must properly plan your network, especially configuration layout and RF (radio frequency). Planning is especially required if you want to install many systems in the same area, in order to prevent radio interference between the *colocated* units and to select the appropriate antennas. In all cases, follow the recognized RF installation practices.

Available Frequency Bands and Channels

The S3100 supports communications in the following frequency bands, in North America and Europe:

- 2.4 GHz OFDM, also known as 802.11g
- 5 GHz OFDM, also known as 802.11a

2.4 GHz Band

The 2.4 GHz band provides 11 channels in North America and 13 in Europe. In these two regions, only channels 1, 6, and 11 are non-overlapping. All these channels are for indoor or outdoor use. The center frequencies of the channels are:

Channel	Frequency (GHz)	Channel	Frequency (GHz)
1	2.412	8	2.447
2	2.417	9	2.452
3	2.422	10	2.457
4	2.427	11	2.462
5	2.432	12	2.467 (Europe only)
6	2.437	13	2.472 (Europe only)
7	2.442		

5 GHz Band

In the 5 GHz band, the number of available channels and sub-bands vary depending on the country of operation.

Most European countries adhere to the DFS (dynamic frequency selection) and TPC (transmit power control) regulations established by the European Telecommunications Standards Institute (ETSI); these regulations apply to the 5 GHz frequency band only. To know which bands are available in your country of operation and whether your country adheres to DFS and TPC, refer to the *Wireless Frequency Plan* document located on our web site (Tools & Demos section).

In North America, nine channels are available in the 5 GHz band, all non-overlapping and for indoor or outdoor use. The center frequencies of these channels are:

Channel	Frequency (GHz)	Channel	Frequency (GHz)
52	5.26	149	5.745
56	5.28	153	5.765
60	5.30	157	5.785
64	5.32	161	5.805
		165	5.825

In Europe, the 11 non-overlapping channels, for indoor or outdoor use, are:

Channel	Frequency (GHz)	Channel	Frequency (GHz)
100	5.50	124	5.62
104	5.52	128	5.64
108	5.54	132	5.66
112	5.56	136	5.68
116	5.58	140	5.70
120	5.60		

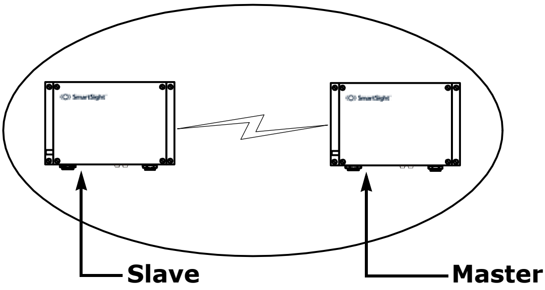
Wireless Cells

A wireless network is designed such that information can travel back and forth between two points without the need for wires. Wireless devices are grouped into *wireless cells*. The devices in a cell communicate together on the same frequency channel and share the same wireless passkey (described on page 49).

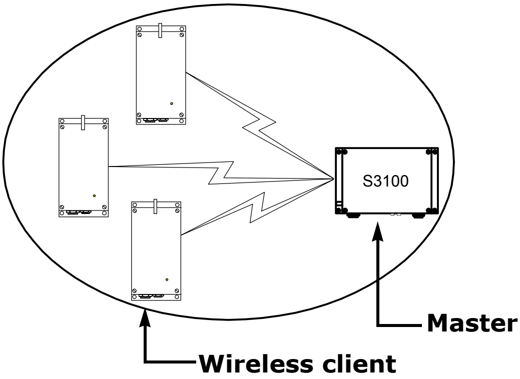
Roles

An S3100 can have two MAC (media access control) roles, according to its function in the wireless cell: master or slave. The other wireless units (S1100, S1100w) that are connected to S3100 bridges are *clients*. Clients always connect to a master S3100.

In this first example of a wireless cell, two S3100 units, a master and a slave, form a wireless bridge:



The second example shows three wireless clients associated to an S3100 master unit:



You can colocate many wireless cells if you respect certain conditions (see page 20).

Compatibility Issues

When planning your wireless systems, you have to take into account the firmware versions of the involved units. It is recommended that the S3100 units have the same firmware versions as their associated slaves and clients. Use the following matrix to ensure complete compatibility between your units:

		Slaves and clients					
		V2.55	**V2.56**	**V2.60**	**V3.10**	**V3.20**	**V3.30**
Master S3100	**V2.55**	yes	yes	no	no	no	no
	V2.56	yes	yes	no	no	no	no
	V2.60	no	no	yes	yes	yes	yes
	V3.20	no	no	yes	yes	yes	yes
	V3.30	no	no	yes	yes	yes	yes

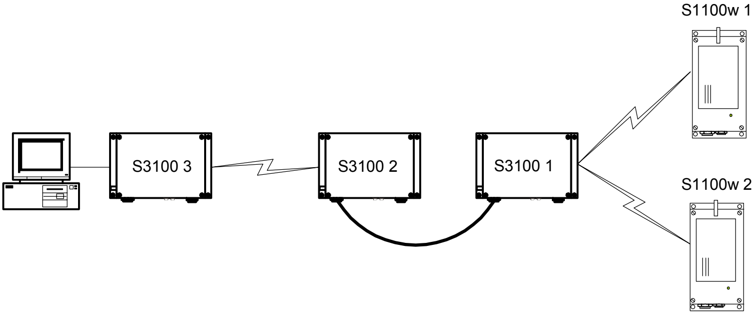
In a wireless cell involving S1100w units, the order in which you configure the units (either the first time or later when they are installed in the field) or update their firmware is critical if you do not want to lose access to them. You should then:

1. Update or configure the units starting with the farthest (in terms of number of RF hops) from the computer running the upgrade procedure.
2. One step at a time, get closer to the host computer.

In a point-to-point repeater, you should:

1. Update the firmware of all S1100 pairs, starting with the remote unit.
2. Change the IP address of the computer running SConfigurator (see page 40).
3. Update the firmware of the two S3100 units.

For example, consider the following wireless cell:



You should update or configure the units in the following order:

1. S1100w 1—You then lose contact with S1100w 1.
2. S1100w 2—You then lose contact with S1100w 2.
3. S3100 1—You can then reach all units.
4. S3100 2—You then lose contact will all units except master S3100 3.
5. S3100 3—You can then reach all units.

For the complete firmware update procedure, refer to the *SConfigurator User Manual*.

Video Bit Rate and Data Throughput

You can connect up to 16 client and 7 slave units to a master bridge in a wireless cell. However, video quality, frame rate, and system layout can limit the number of units that a single master bridge can support.

Furthermore, video quality and frame rate influence the required data throughput. Therefore, you need to carefully plan the number of cameras that will work on a link. Data throughput is influenced by the MAC protocol used; for more information about the protocols, see page 12. The following figures were measured in typical setup situations. They may vary depending on your configuration.

The total data throughput for the SPCF protocol in the 5 GHz band, in a unidirectional UDP link setup, is:

Physical bit rate	Throughput for a 3 mile (5 km) distance	Throughput for a 15.5 mile (25 km) distance
6 Mbps	3.5 Mbps	3.3 Mbps
9 Mbps	4.6 Mbps	4.3 Mbps
12 Mbps	5.5 Mbps	5.1 Mbps
18 Mbps	6.9 Mbps	6.2 Mbps
24 Mbps	7.7 Mbps	6 Mbps
36 Mbps	8.9 Mbps	8 Mbps
48 Mbps	9.7 Mbps	8.6 Mbps
54 Mbps	10 Mbps	8.8 Mbps

The throughput values for the SDCF protocol in the 5 GHz band, in a unidirectional UDP link setup, are:

Physical bit rate	Throughput for a 3 mile (5 km) distance	Throughput for a 15.5 mile (25 km) distance
6 Mbps	4.1 Mbps	3.7 Mbps
9 Mbps	5.8 Mbps	4.9 Mbps
12 Mbps	7.1 Mbps	5.9 Mbps
18 Mbps	9.3 Mbps	7.3 Mbps
24 Mbps	10.9 Mbps	8.3 Mbps
36 Mbps	13.3 Mbps	9.6 Mbps
48 Mbps	14.9 Mbps	10.4 Mbps
54 Mbps	15.6 Mbps	10.7 Mbps

For the bit rate requirements of the video servers to which the cameras are connected, consult the *Bit Rate Settings for Video Servers* document located on the Verint Video Solutions web site (Tools & Demo section).

System Planning

The grouping of units in each wireless cell is determined by their respective locations with respect to one another and by the available outdoor wireless bridges. As a rule of thumb, each client or slave unit must have a clear RF line of sight with its master bridge within each cell. However, the client and slave units can be completely hidden from one another. For more information about the RF line of sight, see page 26.

MAC Protocols

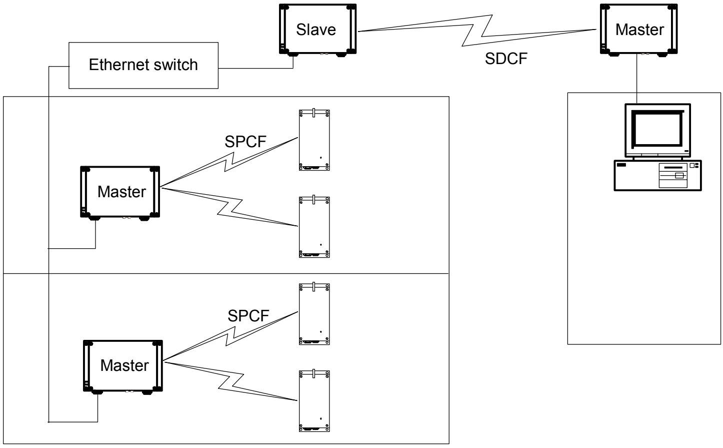
Depending on the type of applications, an S3100 unit uses one of the two proprietary MAC protocols that solve problems inherent to 802.11 wireless networking products.

The SPCF (SmartSight point coordination function) protocol resolves the “hidden node,” quality of service, range, and security problems. SPCF is used in point-to-multipoint applications and in repeater contexts. With this protocol, a master S3100 has total control over the radio frequency used; therefore, in an RF line-of-sight context, you cannot install two cells sharing the same frequency channel.

You use the SDCF (SmartSight distributed coordination function) protocol in point-to-point systems with a high volume of video transmission, typically over long distances or when a remote site is hard to reach. SDCF optimizes the RF link by providing more data throughput. It also resolves the range and security problems of the 802.11 standard. However, SDCF does not manage the hidden node issue.

These two protocols are designed to work with SmartSight units; they cannot work with wireless units from other vendors.

Here is a typical context of use showing the two protocols. A point-to-multipoint system is installed on every floor of a multistorey parking building. The surveillance station is in another building. The SDCF cell acts as a wireless bridge between the two sites.



TPC

If the country of operation of the S3100 unit requires conformity to the TPC (transmit power control) regulations, the transmission power of its radio is automatically reduced by 3 dB before leaving the Verint Video Solutions factory. However, in case of a weak wireless link (that is, a link with an RF margin of less than 15 dB), you have the opportunity to use the maximum transmission power (see page 69).

DFS

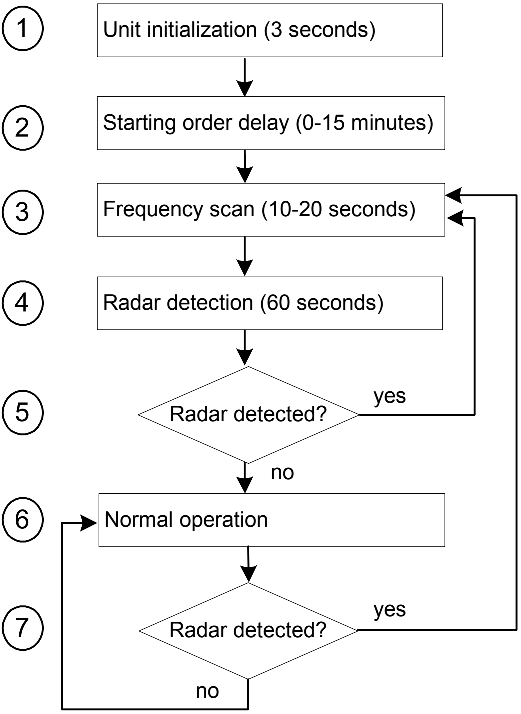
To follow the DFS (dynamic frequency selection) regulations specified by ETSI for the selected country, it is the master unit that performs the tasks relative to frequency channel selection and radar detection. In other words, you cannot choose the frequency channel on which the unit will run.

The automatic selection of the frequency channel limits the number and the configuration of the wireless cells. Furthermore, when colocating many cells, all masters must "see" each other.

Note: DFS is required only in the 5 GHz band.

You should start the master first, then power the client or slave when the other unit is in normal operation.

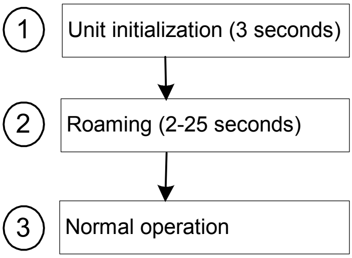
A master unit in DFS mode goes through the following sequence when booting up:


1
Unit initialization (3 seconds)
2
Starting order delay (0-15 minutes)
3
Frequency scan (10-20 seconds)
4
Radar detection (60 seconds)
5
Radar detected?
yes
no
6
Normal operation
7
Radar detected?
yes
no

1. The unit goes through the standard startup procedure.
2. The starting order delay ensures that colocated masters will not select a frequency channel at the same time, therefore minimizing the possibility that they choose the same one. For more information about the starting order, see page 69.

3. The unit scans the available frequencies (based on the selected country) and automatically selects a channel. In the selection process, channels already used by colocated masters will be discarded at first.
4. The unit listens for 60 seconds on the selected channel to detect possible radar interference.
5. If a radar is detected on the channel, the unit returns to the scan process. Otherwise, it continues its bootup procedure.
6. The unit runs normally.
7. If a radar is detected, the unit immediately goes back to the scan process to select another channel.

The boot sequence of client or slave units is:



1. The unit goes through the standard startup procedure.
2. The unit roams through the channels in the available frequency bands to locate its master.
3. When the master is located, the client or slave unit runs normally on the selected frequency channel.

Application Types

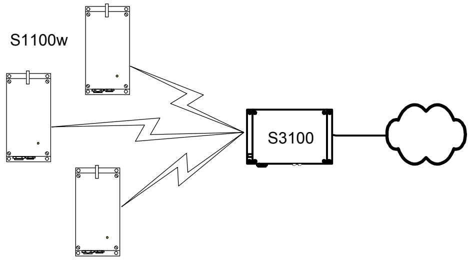
The S3100 units are used in many types of applications, including:

- Point-to-multipoint application—One S3100 bridge linking multiple S1100w units to a LAN
- Point-to-point repeater—Two S3100 units acting as a range extender for one or many pairs of S1100 units
- Point-to-multipoint repeater—Two S3100 units acting as a range extender for multiple S1100w units

- Wireless bridge—Two S3100 units linking two networks (wired or wireless)

Point-to-Multipoint

A point-to-multipoint application is a wireless cell made up of an S3100 bridge (the *S3100* product code, called the *master*) and several S1100w transmitters (the *clients*). The MAC protocol for the master unit is SPCF. Here is a typical point-to-multipoint system:



To install a single wireless cell made up of three S1100w units and one bridge, you have to:

1. Assign the same wireless passkey to the S1100w and S3100 units.
2. In a non-DFS context, assign a frequency channel to the S3100 unit. In a DFS context, the master unit will automatically select a channel.

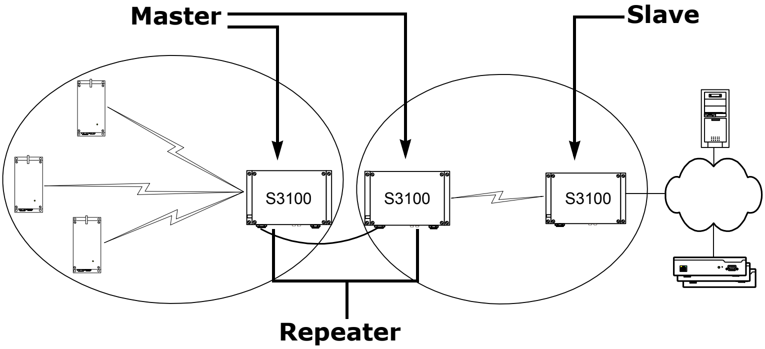
   The associated S1100w units will automatically use their master’s channel.
3. Install the S1100w units such that each one has a clear RF line of sight with the S3100 bridge.

For the complete configuration and installation procedures, see page 33.

Point-to-Multipoint Repeater

A point-to-multipoint repeater is used as a range extender for wireless links, when you need a device to retransmit the signals coming from S1100w units towards the Ethernet LAN. A typical context is when you cannot obtain an RF line of sight between the transmitters and the S3100 connected to the wired LAN.

A point-to-multipoint repeater (the *S3100-RP* product code) is made up of two S3100 units separated into two colocated cells. For example:



To operate the two cells forming the repeater, you have to:

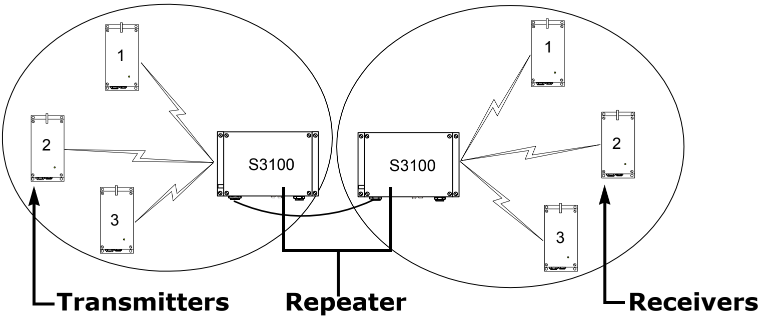
1. In each cell, assign the same wireless passkey to all the units. The wireless passkey must be different from that of the other cell.
2. Always connect the S1100w units to a master S3100, never to a slave.
3. Set the MAC mode of the S3100 in Cell1 to SPCF.
4. Set the MAC mode of the two S3100 units in Cell2 to SDCF.
5. In a non-DFS context, assign a frequency channel to the master S3100 unit in each cell. For better isolation, use different frequency bands.
6. In a DFS context, set a different starting order for each master S3100. Ensure that the two masters see each other.
7. Install the S1100w and slave S3100 units such that each one has a clear RF line of sight with its associated master.

For the complete configuration and installation procedures, see page 34.

Point-to-Point Repeater

A point-to-point repeater is used as a range extender for wireless links, when you need a device to retransmit the signals coming from one or many S1100 transmitters to their corresponding receivers. A typical context is when you cannot obtain an RF line of sight between the transmitters and the receivers.

A point-to-point repeater (the *S3100-RP* product code) is made up of two master S3100 units, separated into two colocated cells. For example, with three pairs of S1100 units:



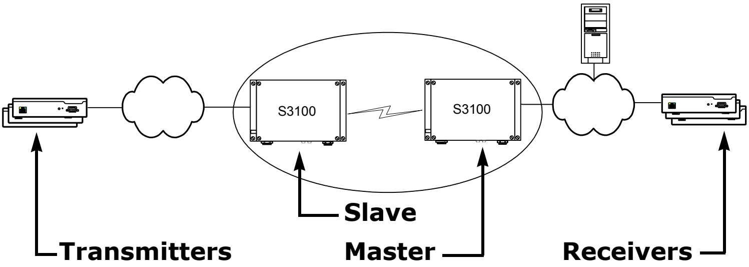
To operate the two cells forming the repeater, you have to:

1. In each cell, assign the same wireless passkey to all the units. The wireless passkey must be different from that of the other cell.
2. Set the MAC mode of the two S3100 units to SPCF.
3. In a non-DFS context, assign a frequency channel to the master S3100 unit in each cell. For better isolation, use different frequency bands.
4. In a DFS context, set a different starting order for each master S3100. Ensure that the two masters see each other.
5. Install the S1100 units such that each one has a clear RF line of sight with its associated master.

For the complete configuration and installation procedures, see page 32.

Wireless Bridge

You can use two S3100 units (the *S3100* product code)—a master and a slave—to access remote or hard to reach video servers, or to send video through a long distance link. For instance, a wireless bridge application can connect remote S1500e series or S1600e video servers (the following illustration) or wireless units without an RF line of sight.



To create a wireless bridge application, you have to:

1. Assign the same wireless passkey to the two S3100 units.
2. In a non-DFS context, assign a frequency channel to the master S3100 unit.
3. Set the MAC mode of the two S3100 units to SDCF.
4. Install the S3100 units such that there is a clear RF line of sight between the two antennas.

For the complete configuration and installation procedures, see page 36.

Colocated Cells

You can operate many wireless cells in the same location, provided you follow guidelines relative to frequency band and channel, distance, wireless passkey, and location.

Distance Limitations

The distance limitations between units are:

- To avoid material damages, you must never power any two units while their antennas are facing one another with a distance of less than 10 feet (3 meters).
- If using adjacent channels, see page 87 for the recommendations on the minimum distances to respect.
- When setting SDCF cells using the same frequency channel, there is no limitation if the maximum distance between any two colocated units is less than 6 miles (10 km). For a longer distance, you must carefully plan the maximum link distances of the cells (see page 70).
- With different frequency bands or with non-adjacent channels in the same band, two units can be side by side with no minimum distance between them.

General Guidelines

Regarding frequency channel, you cannot manually select one in the 5.40–5.725 GHz band in Europe; for the detailed procedure, see page 22. In the 5 GHz band in North America and the 2.4 GHz band everywhere, the channel selection guidelines vary depending on the MAC protocol:

- When at least one SPCF cell is involved, you cannot use the same frequency channel.
- Two SDCF cells can use the same frequency channel. They will share the available bandwidth.

The wireless passkeys of colocated cells must be different from one another, regardless of their MAC protocols or frequency channels.

5 GHz Band in North America and 2.4 GHz Band

In the 2.4 GHz band in North America and Europe, you can use the three non-overlapping channels (channels 1, 6, and 11) to colocate wireless cells. In the 5 GHz band, all channels are non-overlapping.

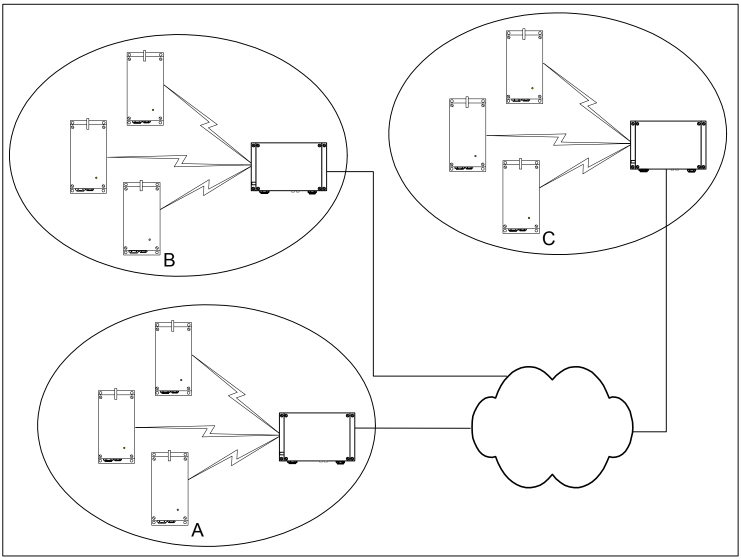
A typical colocation example is three point-to-multipoint applications, each one made up of three S1100w units and one bridge. To install such a system, you have to:

1. In each cell, assign the same wireless passkey to the S1100w units and the S3100 bridge. The wireless passkey must be different from that of the other cells.
2. Assign a different frequency channel to each S3100 master unit; the associated S1100w units will automatically use their master's channel. For better isolation, use different frequency bands for adjacent cells. For example:

Unit	Cell	Channel	Wireless Passkey
S3100_A	A	52	ertynmbvcxzapoiu
S1100w_A1	A	52	ertynmbvcxzapoiu
S1100w_A2	A	52	ertynmbvcxzapoiu
S1100w_A3	A	52	ertynmbvcxzapoiu
S3100_B	B	149	PUK98rewq4123qzx
S1100w_B1	B	149	PUK98rewq4123qzx
S1100w_B2	B	149	PUK98rewq4123qzx
S1100w_B3	B	149	PUK98rewq4123qzx
S3100_C	C	64	987123jkl456wert
S1100w_C1	C	64	987123jkl456wert
S1100w_C2	C	64	987123jkl456wert
S1100w_C3	C	64	987123jkl456wert

3. In each cell, install the S1100w units such that each one has a clear RF line of sight with its associated S3100 bridge.

This application can be illustrated this way, where the three cells are in the same location:



Installing more than three cells in the 2.4 GHz band or more than nine cells in the 5 GHz band requires more RF planning. In such a context, you should contact the Verint Video Solutions project engineering group for assistance.

5 GHz Band in Europe

The maximum number of colocated cells corresponds to the number of channels in the available frequency bands that can be used outdoors. For instance, in most countries of Western Europe, you can have up to 11 colocated cells in the 5.40–5.725 GHz band. However, because the master units must see each other in a DFS context, the variety of supported setups is limited.

In this context, you can easily install up to five cells. By respecting the following steps, you can assume that the cells will not share the same frequency channel, making the complete bandwidth available for each one. You have to:

1. Assign a different wireless passkey to each cell.
2. Ensure that all S3100 masters “see” one another. For the procedure, see Appendix F on page 83.

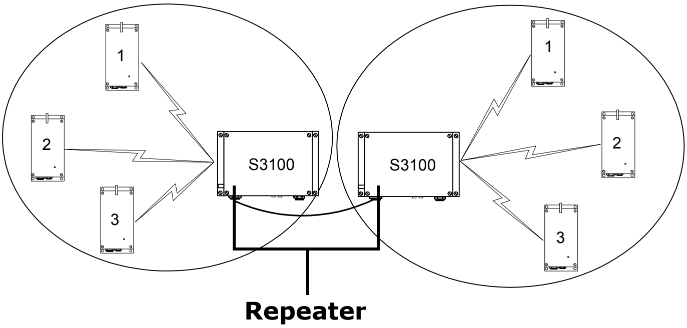
3. Position the units so that there is at least 3 feet (1 meter) between each antenna.
4. In each master unit, set a different starting order: 1 for the first unit, 2 for the unit next to it, 3 for the third one, and so on.

Installing more than five cells in the 5.40–5.725 GHz band requires the use of adjacent channels. This situation demands greater distances between the antennas to reduce potential radio interference. Therefore, you should contact the Verint Video Solutions project engineering group for assistance.

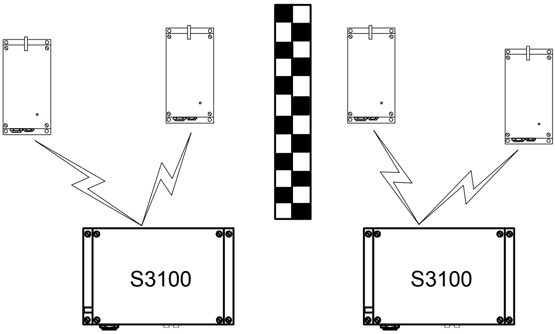
Supported Setups

The following colocated systems are supported in the 5.40–5.725 GHz band:

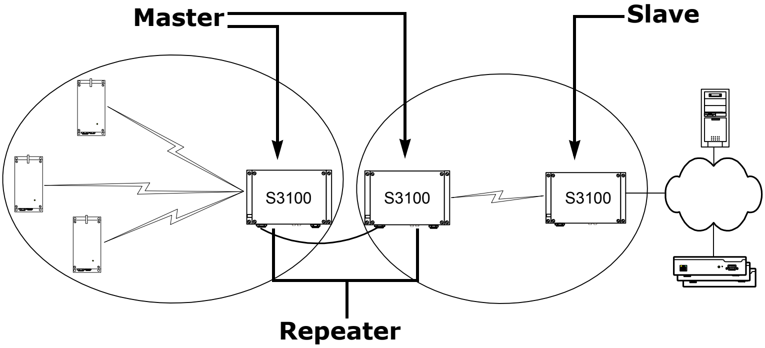
- A point-to-point repeater for one or more pairs of S1100 units, with or without hidden nodes. The two S3100 master units see each other.



- Two point-to-multipoint applications, in which the transmitters from one system do not see the transmitters from the other cell. The two S3100 master units see each other.



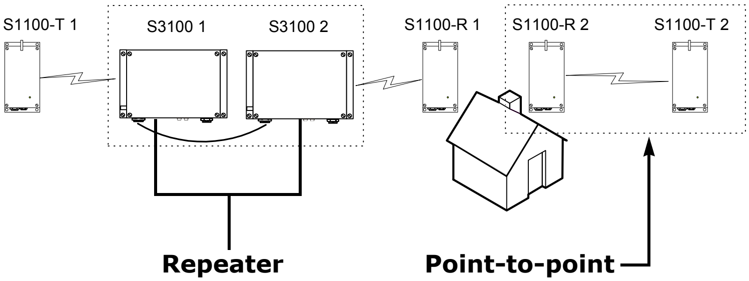
- A point-to-multipoint repeater. The two S3100 master units see each other.



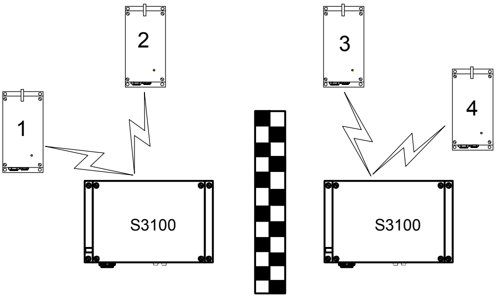
Unsupported Setups

You cannot install the following colocated systems in the 5 GHz band in Europe:

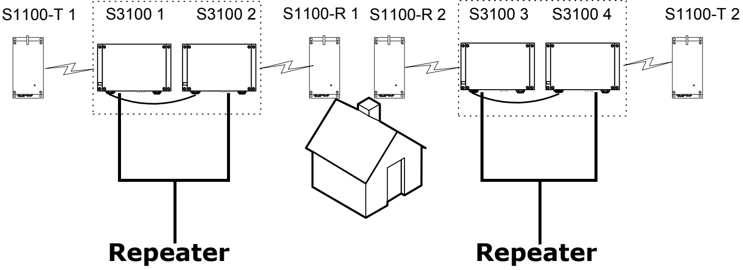
- A point-to-point repeater with a point-to-point link. In this setup, there are two masters that do not see each other, S3100 2 and S1100-R 2, while the two receivers do.



- Point-to-multipoint applications with hidden masters. In this context, the two S3100 masters do not see each other, while transmitters 2 and 3 do.



- Multiple point-to-point repeaters. The S3100 2 and S3100 3 masters do not see each other, while the two receivers do.



RF Planning

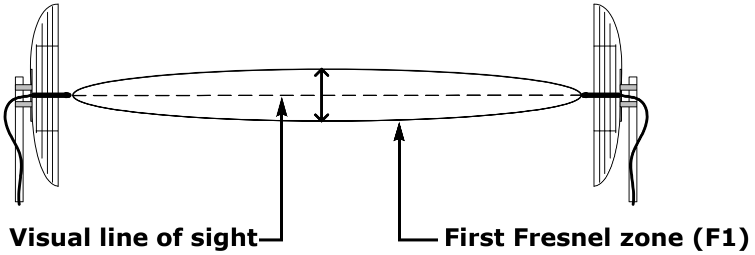
Successful operation of a wireless link depends on proper RF path planning and antenna installation. You have to install the units in such a way that there is a clear RF line of sight between the two antennas.

Location Evaluation

The path between the two antennas must be free of obstacles that could disturb propagation. For very short link distances—less than 500 feet (152 meters)—you may be able to establish a working link despite partial path obstruction. However, radio waves will be in part absorbed and in part diffracted by the obstacles, therefore affecting link reliability. Because the reliability of such an installation is highly unpredictable, Verint Video Solutions does not recommend it. A path free of any obstacle is called an *RF line-of-sight path*.

To establish an RF line-of-sight path, you must take into account the beam width of the radio signal transmitted between the two antennas. This beam width is an elliptical area immediately surrounding the visual line of sight. It varies in thickness depending on the length of the signal line of sight; the longer the length, the thicker the beam width becomes.

The region outlined by the signal beam width is known as the *first Fresnel zone*. The Fresnel zone is always thicker at the mid-point between the two antennas. Therefore what appears to be a perfect line-of-sight path between the base and a remote station may not be adequate for a radio signal; this is the difference between “visual” and “RF” line of sight.



In practice, it has been determined that a radio path can be considered an RF line-of-sight path if it has a clear opening through 60% of the first Fresnel zone (or *0.6 F1*). Here are values for 0.6 F1 for various signal path distances and frequency bands:

Distance (mi./km)	**2.45 GHz (feet/m)**	**5.3 GHz (feet/m)**	**5.8 GHz (feet/m)**	**Earth curvature effect (feet/m)**
1 / 1.6	14 / 4.2	9.5 / 2.9	8.9 / 2.7	0
4 / 6.5	27 / 8.4	18.7 / 5.7	18 / 5.5	2 / 0.6
7 / 11.3	37 / 11	25 / 7.6	23.6 / 7.2	6 / 1.8
15 / 24	53 / 16	36.4 / 11.1	35 / 10.6	29 / 8.8

For distances under seven miles, the earth curvature effect is negligible. However, for greater distances, you need to consider it in your calculations; for instance, for a 15-mile link in the 2.4 GHz band, the two antennas must be located 82 feet higher than the highest obstacle in the RF line of sight between them (that is, 53 feet for the Fresnel zone plus 29 feet for the earth curvature effect). For help, consult the Verint Video Solutions project engineering group.

A common problem encountered in the field and related to the 0.6 F1 clearance rule is building obstruction. The proposed visual path may just barely clear a building but the RF line of sight will not. In such a case, the signal will be partially absorbed and diffracted. Increasing the height of the two antennas or the gain of the antennas are the only alternatives to improve the link quality.

Note: At 2.4 and 5 GHz, radio waves are highly attenuated by dense foliage. A link established in the fall or winter season may be adversely affected in the spring and summertime, if it is established below tree level.

Antenna Requirements

Verint Video Solutions offers many antennas to meet various distance requirements.

You have to consider many factors when choosing an antenna, including the distance to cover, the RF bit rate, the radiated power (EIRP), and the frequency band used. For systems located in North America on the 5 GHz band, you can use the *Wireless Distance Calculator* located on our web site (Tools & Demos section).

The combined transmission power of the unit and antenna must not exceed the maximum value established by your country's regulations. To ensure that this maximum is not exceeded, enter the gain of the chosen antenna in the CLI (Wireless Communication menu) or SConfigurator (Wireless pane). The unit will automatically take it into account and adjust its own transmission power accordingly at startup.

To know the maximum antenna gain you can use, subtract a value from the maximum EIRP allowed (in dBm):

Frequency band	**Value to subtract from EIRP**
2.4 GHz in North America	11 dB
2.4 GHz in Europe	11 dB
5 GHz with DFS/TPC	12 dB
5 GHz without DFS/TPC	6 dB

The maximum EIRP varies depending on your country and band; for more information, refer to the *Wireless Frequency Plan* document located on our web site (Tools & Demos section). In North America for instance:

Frequency band	**Maximum transmitted power of the unit**	**Maximum radiated power (EIRP)**
2.4 GHz	18 dBm	30 dBm
5.3 GHz	17 dBm	30 dBm
5.8 GHz	17 dBm	36 dBm in point to multipoint 53 dBm in point to point

For example, consider a unit running in the 5.3 GHz band in North America. Since the maximum EIRP allowed in this area is 30 dBm, you should not install an antenna whose gain is greater than 24 dBi (that is, 30 dBm - 6 dB).

Note: Connecting an antenna with a gain higher than the calculated value contravenes your country's regulations. It is your responsibility to ensure that you respect the regulations in place.

Interference

In most countries, the 2.4 GHz band is not regulated by a government agency; this absence of frequency coordination can result in interference between various systems. For instance, if a link with an RF line of sight is subject to excessive video delay and very low frame rate (or possibly breakdown of video images), it could be due to interference.

Fortunately, you have ways of adapting your setup to avoid interference:

- RF channel selection—In the 2.4 GHz band, the S3100 has 11 or 13 channels to choose from. In case of interference, it is recommended to change channel until you find a clean one.
- Antenna selection—Using a 16-dBi gain antenna instead of an 8.5-dBi one can significantly lower interference from other radio systems. Replace the antenna if switching channels does not correct the problem or if all channels must be used to colocate several systems.

The 5 GHz band is less cluttered than the 2.4 GHz band, resulting in less potential interference from other wireless systems.

RF Exposure Considerations

In order to comply with the RF exposure requirements of CFR 47 part 15 in North America, the units must be installed in such a way as to allow a minimum separation distance of 12 inches (30 cm) between antennas and persons nearby.

3

Configuring and Installing the Unit

You can set up the S3100 units for point-to-multipoint, repeater, or wireless bridge applications.

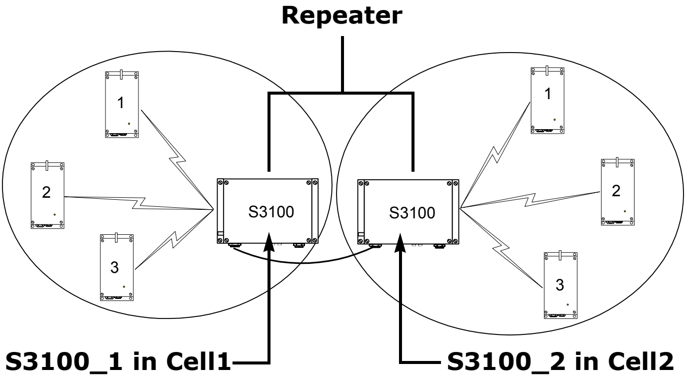
Computer Requirements

The minimum software and hardware requirements for the host computer needed to configure the unit are:

- Windows 2000 Service Pack 2 or higher, or Windows XP
- An Ethernet network card
- A serial port (not through a USB converter)

Point-to-Point Repeater Application

A point-to-point repeater is used as a range extender for wireless links, when you need a device to retransmit the signals coming from one or many S1100 transmitters to their corresponding receivers. A repeater is made up of two S3100 units.



To set up such an application, you have to follow a series of steps, in the following order:

1. Configuring the S1100 pairs in repeater mode. For the procedure, refer to the *S1100 Installation Guide*.

   Warning: You must complete the configuration of the S1100 units before powering up an S3100 bridge.

2. Assembling the power devices (see page 39).

3. Configuring the two S3100 units, one at a time (see page 39). You have to shut down the first unit when configuring the second one.

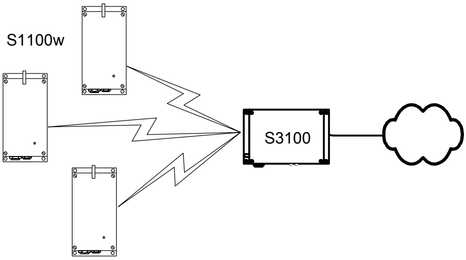
The wireless parameters to apply are:

Parameter	**S3100_1**	**S3100_2**
MAC mode	SPCF	SPCF
Role	Master	Master
Band	*Band1*	*Band1*
Channel	In a non-DFS context: *ChannelA*	In a non-DFS context: *ChannelB*
Bit rate	N/A	N/A
Starting order	In a DFS context: 1	In a DFS context: 2
Wireless passkey	*Passkey1* common to all units in Cell1	*Passkey2* common to all units in Cell2

4. Installing the S3100 units (see page 51).

Point-to-Multipoint Application

A point-to-multipoint application is a wireless system made up of a master S3100 (the *S3100* product code) and several S1100w clients.



To set up such an application, you have to follow a series of steps, in the following order:

1. Configuring the S1100w transmitters. For the procedure, refer to the *S1100w Installation Guide*.

2. Connecting power and Ethernet (see page 37).

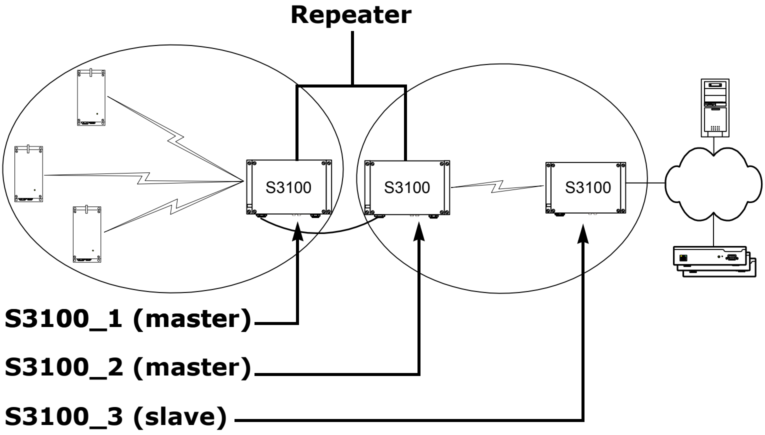
3. Configuring the S3100 unit (see page 39). The wireless parameters to apply are:

Parameter	S3100
MAC mode	SPCF
Role	Master
Band	Manual selection (the same as in the S1100w units)
Channel	In a non-DFS context: manual selection
Bit rate	N/A
Starting order	In a DFS context, if other colocated cells are present: a value different from that of the other cells
Wireless passkey	A passkey common to all units in the cell

4. Installing the S3100 unit (see page 51).

Point-to-Multipoint Repeater Application

A point-to-multipoint repeater is used as a range extender for wireless links, when you need a device to retransmit the signals coming from S1100w transmitters towards the Ethernet LAN. A repeater is made up of two S3100 units.



All devices in this setup must be in the same IP subnet.

To set up such an application, you have to follow a series of steps, in the following order:

1. Assembling the power devices (see page 37 for the slave and page 39 for the two repeater units).
2. Configuring the two S3100 units part of the repeater, one at a time (see page 39). You have to shut down the first unit when configuring the second one.

   The wireless parameters to apply are:

Parameter	**S3100_1**	**S3100_2**
MAC mode	SPCF	SDCF
Role	Master	Master
Band	The same band as in the S1100w units	*Band2*
Channel	In a non-DFS context: *ChannelA*	In a non-DFS context: *ChannelB*
Bit rate	N/A	N/A
Starting order	In a DFS context: 1	In a DFS context: 2
Wireless passkey	*Passkey1* common to all units in Cell1	*Passkey2* common to all units in Cell2

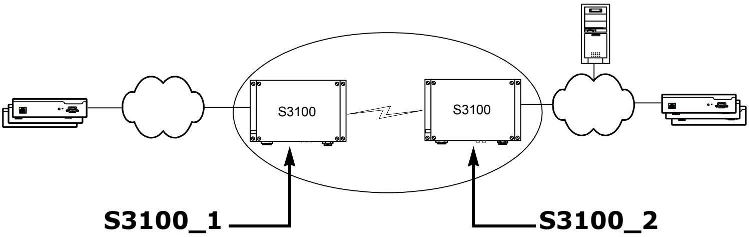
3. Configuring the slave S3100 unit connected to the LAN (see page 39). The wireless parameters to apply are:

Parameter	**S3100_3**
MAC mode	SDCF
Role	Slave
Band	*Band2*
Channel	N/A
Bit rate	Manual selection
Starting order	N/A
Wireless passkey	*Passkey2* common to all units in Cell2

4. Installing the repeater units (see page 51).
5. Installing the slave S3100 (see page 51).

Wireless Bridge Application

You can use two S3100 units (the *S3100* product code) to access remote or hard to reach video servers, or to send video through a long distance link. Any of the two bridges can act as the master.



To set up such an application, you have to follow a series of steps, in the following order:

1. Connecting power and Ethernet on the two units (see page 37).
2. Configuring the two S3100 units one at a time; always start with the master (see page 39). You have to shut down the first unit when configuring the second one.

   The wireless parameters to apply are:

Parameter	S3100_1	S3100_2
MAC mode	SDCF	SDCF
Role	Slave	Master
Band	*Band1*	*Band1*
Channel	N/A	In a non-DFS context: manual selection
Bit rate	Manual selection	N/A
Starting order	N/A	In a DFS context: a value different from that of the other wireless cells, if applicable
Wireless passkey	*Passkey1*	*Passkey1*

3. Installing the S3100 units (see page 51).

Power and Ethernet Connections

Depending on the S3100 unit used, the power connections are different:

- The *S3100* model (one unit) uses power over Ethernet (PoE).
- The *S3100-RP* model (two units) comes with two 24V AC power supplies.

You have to assemble these devices prior to installing them on the units. It is strongly recommended to execute these tasks in a lab.

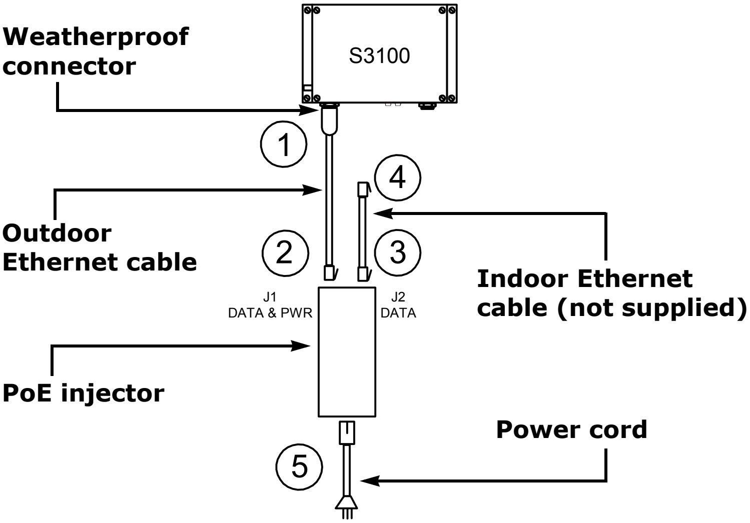
The maximum length of outdoor Ethernet cables is 164 feet (50 meters). The maximum length of indoor cables is 82 feet (25 meters).

Power over Ethernet

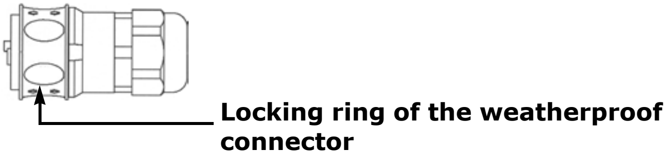
With the *S3100* model, you use the supplied PoE kit to power the unit and establish the Ethernet connection. In addition to the kit, your shipment includes an Ethernet cable with a weatherproof connector at one end that will go directly on the unit.

The PoE kit contains two items: an injector and a power cord.

To assemble the PoE kit:



1. Plug the supplied outdoor Ethernet cable (the end with the weatherproof connector) into the PoE receptacle of the S3100 unit. Lock the weatherproof connector by pushing forward the locking ring.

   You unlock the connector by pulling back the locking ring, then withdrawing the plug.

2. Plug the other end of the outdoor Ethernet cable into the DATA & PWR port of the injector.

3. Connect one end of your Ethernet cable—straight-through or crossover, depending on your installation (see page 44)—into the DATA port of the injector.

   Note: The maximum length of this cable is 82 feet (25 meters).

4. Connect the other end of your Ethernet cable into an Ethernet device or your computer.

   Warning: To avoid damaging your equipment, ensure that your cable is connected into the DATA port of the PoE injector, and not in the DATA & PWR port.

5. Power the S3100 unit by connecting the electric plug of the power cord into the outlet.

Power Devices for the Repeater

Prior to configuring the two S3100 units making up the repeater, you need to assemble their power cord and power supply.

To assemble a power device:

1. Plug the weatherproof connector of the supplied power cord into the auxiliary 24V AC power connector of the unit.
2. Connect the loose end of the power cord into a 24V AC power supply.

Configuration

To configure an S3100 unit, you need SConfigurator, a proprietary tool included on the *SmartSight Utilities* CD. You can also find its latest version on the Verint Video Solutions web site (Firmware Upgrades section). You have to copy its executable file to the hard disk of your computer.

Configuring an S3100 unit involves a series of steps, in the following order:

1. In a point-to-point repeater context, changing the IP address of the computer running SConfigurator (see page 40).
2. Preparing the unit (see page 44).

   Warning: Never power more than one S3100 unit at a time during the configuration process.

3. Setting the IP parameters of the unit (see page 44).
4. Setting the country of operation and the unit name (see page 47).

5. Setting the wireless parameters (see page 48).
6. Checking the communication between the units (see page 51).
7. In a point-to-point repeater context, putting back the original IP address of the computer.

For any other configuration task or for more information about the parameters, refer to the *SConfigurator User Manual*.

Write down the final values of the configuration parameters (especially the IP address and VSIP port) in the form located at the end of the *S3100 Installation Guide*.

Changing the IP Address of the Computer

To change the parameters of the S3100 units in a point-to-point repeater context, you need to temporarily change the IP address of your computer. The temporary address must be in the 192.168.135.255 subnet. The procedure varies depending on your operating system (Windows 2000 or Windows XP).

The recommended temporary IP settings are:

- IP address: 192.168.135.2
- Subnet mask: 255.255.255.0
- Default gateway: 192.168.135.1

To change the IP address under Windows 2000:

1. From the desktop, right-click **My Network Places**, then choose **Properties**.

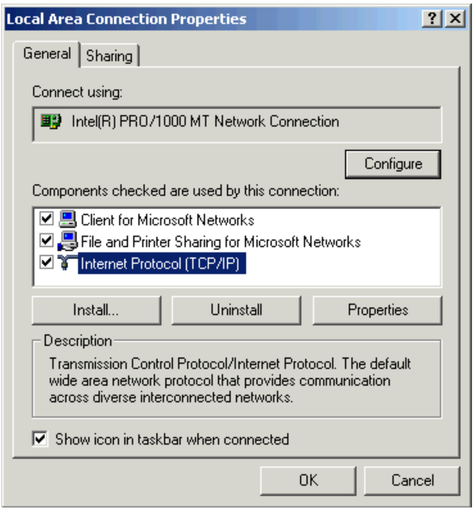
   The Network and Dial-up Connections window appears.

2. Double-click **Local Area Connection**.

   The Local Area Connection Status window appears.

3. Click **Properties**.

The Local Area Connection Properties window appears.



Local Area Connection Properties

Connect using:

Intel(R) PRO/1000 MT Network Connection

Components checked are used by this connection:

☑ Client for Microsoft Networks

☑ File and Printer Sharing for Microsoft Networks

☑ Internet Protocol (TCP/IP)

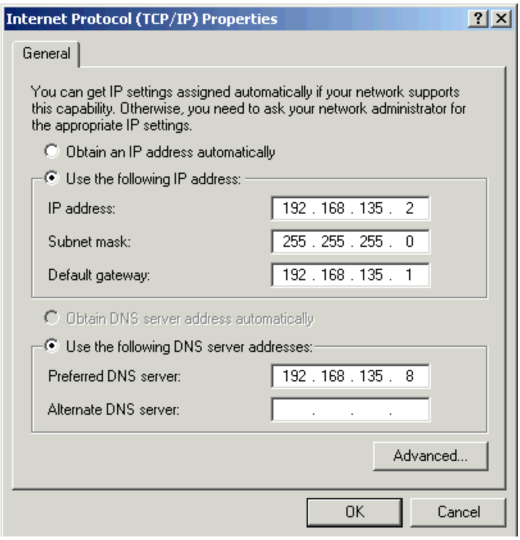
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in taskbar when connected

4. In the component list, select **Internet Protocol (TCP/IP)**, then click **Properties**.

The Internet Protocol (TCP/IP) Properties window appears.



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 135 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 135 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 135 . 8

Alternate DNS server: . . .

5. If **Use the following IP address** is selected, write down the information displayed in the box: the IP address, the subnet mask, and the default gateway.

   You will need these addresses to put back your computer in its initial state once the configuration process is completed.

6. If **Obtain an IP address automatically** is selected, click **Use the following IP address**.

7. Enter the desired IP settings (temporary or initial).

8. Click **OK** to close all windows.

To change the IP address under Windows XP:

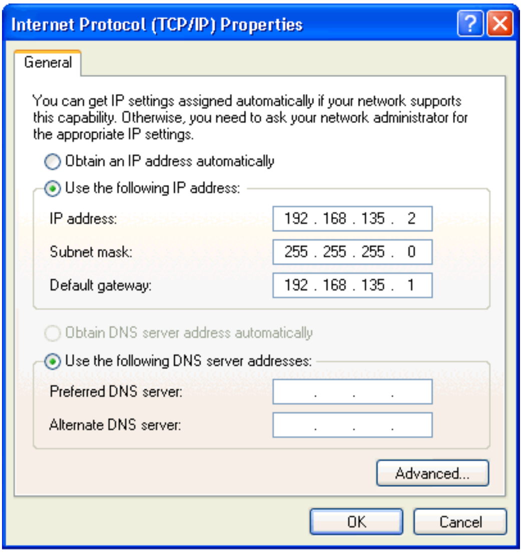
1. In the Windows Start menu, choose **Control Panel**.

2. If the classic view is enabled, choose **Network Selection**. In the category view, select **Network and Internet Connections**, then **Network Connections**.

3. Double-click your active LAN or Internet connection.

4. Click **Properties**.

   A Properties window appears.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 135 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 135 . 1

○ Obtain DNS server address automatically

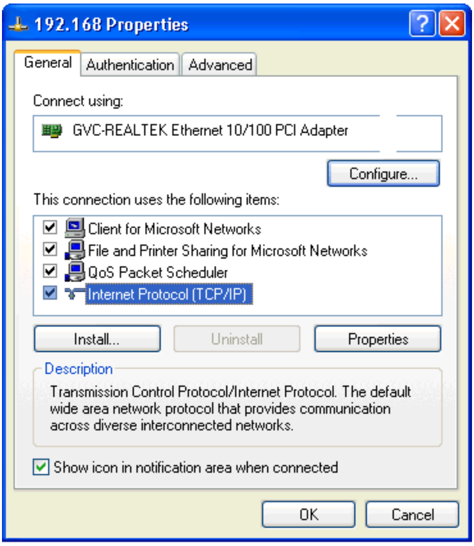
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

5. In the General tab, select the **Internet Protocol (TCP/IP)** item, then click **Properties**.

   The Internet Protocol (TCP/IP) Properties window appears.



Connect using:

GVC-REALTEK Ethernet 10/100 PCI Adapter

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected

6. If **Use the following IP address** is selected, write down the information displayed in the box: the IP address, the subnet mask, and the default gateway.

   You will need these addresses to put back your computer in its initial state once the configuration process is completed.

7. If **Obtain an IP address automatically** is selected, click **Use the following IP address**.

8. Enter the desired IP settings (temporary or initial).

9. Click **OK** to close all windows.

Unit Preparation

To configure the unit, you need a crossover or straight-through Ethernet cable. The crossover cable is to directly connect the unit to a computer; the straight-through cable is to integrate the S3100 on a network. For their detailed pinouts, see page 75.

To prepare an S3100 unit for configuration:

1. Plug the external antenna on the main antenna connector of the unit.
2. Power up the S3100 unit.
3. Connect the unit to the network or a computer using the proper Ethernet cable.

IP Parameters

Before installing the S3100 unit, you need to change its IP address to ensure compatibility with an existing network. The default IP addresses of all units are based on the APIPA service and will be in the range 169.254.*X*.*Y*, where *X* and *Y* are relative to the MAC address of the individual unit; for more information about the APIPA service, see page 79.

To work properly, units on the same network must have unique IP addresses. The unit will not prevent you from entering a duplicate address. However, its three status LEDs will turn to flashing red; then the unit will use an APIPA address.

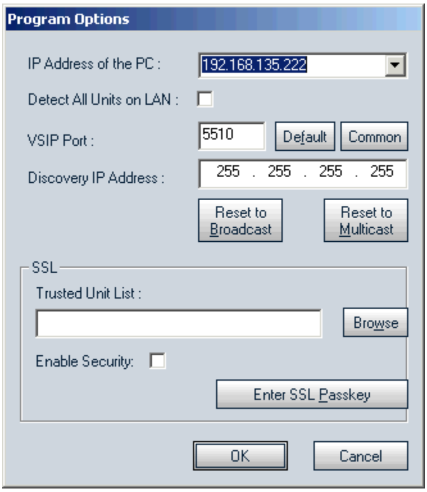
To set the initial IP parameters:

1. Start SConfigurator.

   The SConfigurator window appears.

2. From the General tab, click **Program Options**.

The Program Options window appears.



Program Options

IP Address of the PC : 192.168.135.222

Detect All Units on LAN : □

VSIP Port : 5510

Discovery IP Address : 255 . 255 . 255 . 255

SSL

Trusted Unit List :

Enable Security: □

3. Check **Detect All Units on LAN**.

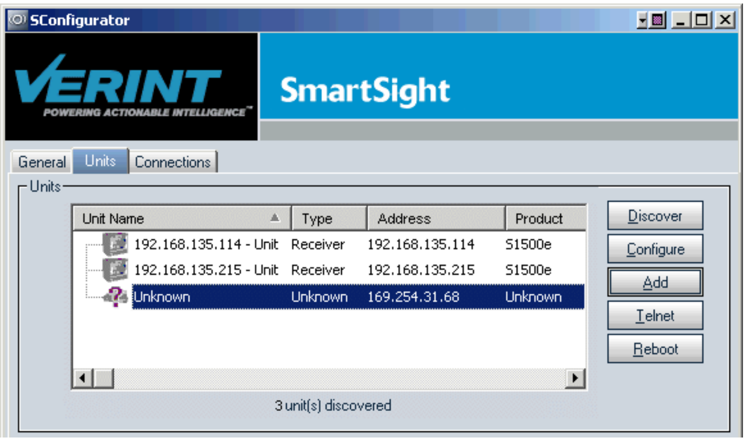
4. Ensure that the VSIP Port value is 5510; otherwise, click **Default**.

5. Ensure that the Discovery IP Address is 255.255.255.255; otherwise, click **Reset to Broadcast**.

6. Click **OK**.

7. Choose the **Units** tab, then click **Discover**.

A unit of type "Unknown" with a 169.254.*X*.*Y* address appears in the Units box; it corresponds to your new unit.

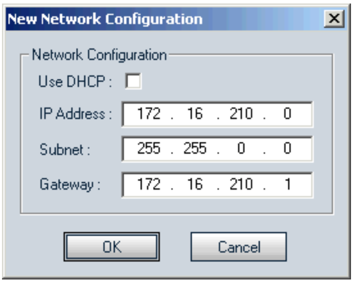


Unit Name	Type	Address	Product
192.168.135.114 - Unit	Receiver	192.168.135.114	S1500e
192.168.135.215 - Unit	Receiver	192.168.135.215	S1500e
Unknown	Unknown	169.254.31.68	Unknown

3 unit(s) discovered

8. Select the unknown unit, then click **Configure**. In the Reconfigure unit? confirmation window, click **Yes**.

The New Network Configuration window appears.



Use DHCP : □

IP Address : 172 . 16 . 210 . 0

Subnet : 255 . 255 . 0 . 0

Gateway : 172 . 16 . 210 . 1

9. Enter the IP information for the unit.

- For an S3100 in a point-to-point repeater, enter the following information:
  - Use DHCP: do not check this box
  - IP address: 192.168.135.51 for the S3100 on the transmitter side and 192.168.135.52 for the S3100 on the receiver side
  - Subnet: 255.255.255.0
  - Gateway: 192.168.135.1

- For an S3100 in another context:
  - To use DHCP (dynamic host configuration protocol) in the other application types, check **Use DHCP**.

    For more information about DHCP, see page 79.
  - Otherwise, enter the IP address, subnet mask, and gateway of the unit, as provided by your network administrator.

10. Click **OK**.

The S3100 unit reboots with its new network configuration.

11. In SConfigurator, choose the **Units** tab, then click **Discover**.

The new outdoor wireless bridge appears in the Units list.

12. Select the new S3100, then click **Configure**.

The Unit Configuration window appears.

Country Selection and Unit Name

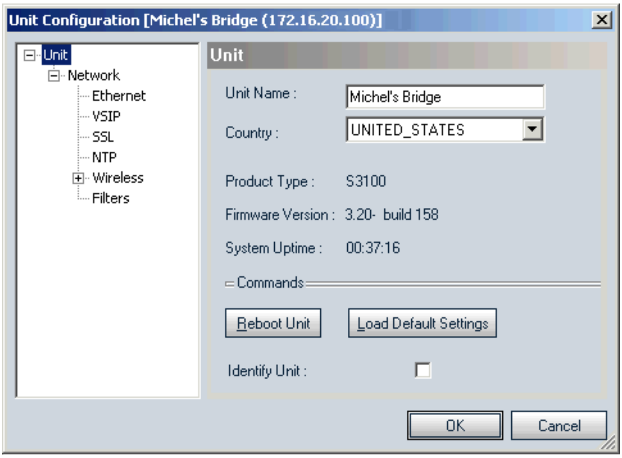
You must assign the proper country of operation to the unit, so that it will:

- Comply to the DFS/TPC regulations, if applicable
- Respect the EIRP rules
- Use the proper set of frequency channels

It is recommended to give a meaningful name to each unit, to help maintenance and debugging.

To set the country of operation and the name of the unit:

1. In the parameter tree of the Unit Configuration window, click **Unit**.



Unit Configuration [Michel's Bridge (172.16.20.100)]

Unit

Unit Name : Michel's Bridge

Country : UNITED_STATES

Product Type : S3100

Firmware Version : 3.20- build 158

System Uptime : 00:37:16

Identify Unit : □

2. In the Unit Name field, assign a meaningful name to the unit.
3. Select the country of operation of the unit.
4. Click **OK**.

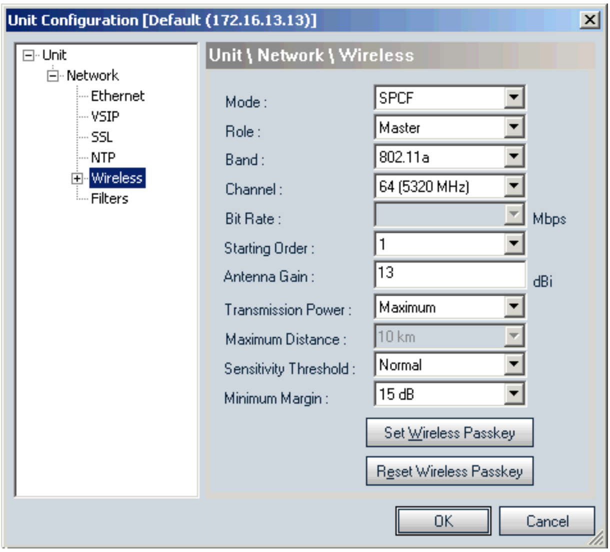
The unit reboots.

Wireless Parameters

Depending on the type of application involved, you have to assign a different set of parameters. Furthermore, the configuration steps vary with the MAC role (master or slave). Use the values supplied in the description of the applications (from page 32 to page 36).

To set the wireless parameters for a master unit:

1. In the parameter tree of the Unit Configuration window, expand the **Network** structure, then click **Wireless**.



Mode : SPCF
Role : Master
Band : 802.11a
Channel : 64 (5320 MHz)
Bit Rate : Mbps
Starting Order : 1
Antenna Gain : 13 dBi
Transmission Power : Maximum
Maximum Distance : 10 km
Sensitivity Threshold : Normal
Minimum Margin : 15 dB

2. Set the parameters, as required. For the wireless passkey procedure, see page 50.
3. Click **OK**.

The unit reboots.

To set the wireless parameters of a slave unit:

1. In the parameter tree of the Unit Configuration window, expand the **Network** structure, then click **Wireless**.
2. In the Role field, select **Slave**.
3. Click **OK** to save the settings.

   The unit reboots.
4. In the Units tab, click **Discover**.
5. Select the slave unit, then click **Configure**.
6. In the parameter tree of the Unit Configuration window, expand the **Network** structure, then click **Wireless**.

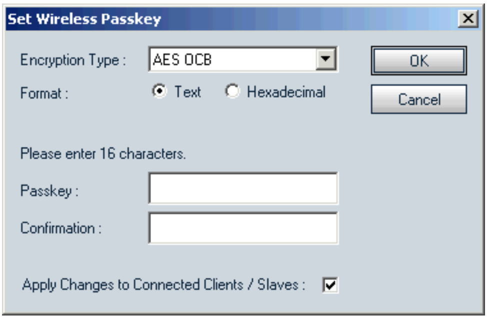
7. Set the parameters, as required.
8. Click **OK**.

   The slave unit reboots.

To set the wireless passkey:

1. In the Wireless pane, click **Set Wireless Passkey**.

   The Set Wireless Passkey window appears.



Set Wireless Passkey

Encryption Type : AES OCB

Format : ● Text ○ Hexadecimal

Please enter 16 characters.

Passkey :

Confirmation :

Apply Changes to Connected Clients / Slaves : ☑

2. Select the format of the passkey.
3. In the Passkey field, enter the passkey (case-sensitive).

   The passkey must have exactly 16 characters if the format is Text, or 32 digits if Hexadecimal.

   For the wireless connection to be secure, do no enter a known name (like a street name), but instead use a mix of digits and letters. Furthermore, do not disclose the passkey. The connection security is based on the secrecy and uniqueness of the passkey.
4. In the Confirmation field, enter again the passkey.
5. Clear **Apply Changes to Connected Stations**.
6. Click **OK**.

Communication Checking

Using SConfigurator, ensure that the master S3100 and its clients and slaves communicate well together.

To check the communication:

1. If required, power up all the units making up the system.
2. In the Units tab, the associated units should be hierarchically positioned under the S3100.
3. In the Link Status pane of the S3100, the units should be in the Clients/Slaves list.
4. Ensure that there is end-to-end video transmission in the lab before installing the units in their final location.

Installation

After ensuring that all units are communicating properly in a lab, you can install the S3100 units in their final location. You can install them either on a wall or on a pole.

Warning: When installing colocated wireless systems, you have to take into account the distance limitations listed on page 20.

Warning: Always mount the unit with the mating connectors pointing downwards. Otherwise moisture may penetrate the unit; the associated repair costs are not covered by the warranty.

Installation of the Repeater Units

A repeater (the *S3100-RP* product code) is made up of two units connected together with an outdoor Ethernet cable.

To install the repeater units:

1. Install the two units back to back in their final location:

- □ On a wall—Put four screws on the two side brackets and fix the unit at the desired location.
- □ On a pole—Screw the pole mount brackets (supplied with your shipment) in the back of the unit; then attach the brackets on the pole with the stainless steel clamps.

2. To enable the built-in surge protection, connect each unit to the ground using the grounding lug on its left side.

Use a large diameter wire (minimum AWG 10), and make it as short as possible.

3. If the S3100 units will be directly exposed to the sun in an environment likely to reach 122°F (50°C), install sun shields.

4. Install the antennas (see page 54).

5. Connect the supplied crossover Ethernet cable between the two units.

6. Power the units using the assembled power devices.

Installation of the Single Unit

The *S3100* product code corresponds to a single outdoor wireless bridge.

To install the S3100:

1. Plug the assembled PoE injector on the unit.

2. Connect your Ethernet cable in the PoE injector.

3. Install the S3100 in its final location:

- □ On a wall—Put four screws on the two side brackets and fix the unit at the desired location.
- □ On a pole—Screw the pole mount brackets (supplied with your shipment) in the back of the unit; then attach the brackets on the pole with the stainless steel clamps.

4. If you are installing the S3100 unit in a lightning prone environment or in a site where large AC mains power fluctuations are a common occurrence, add additional external surge protection to the PoE injector.

For more information, see page 81.

5. To enable the built-in surge protection, connect the unit to the ground using the grounding lug on its left side.

Use a large diameter wire (minimum AWG 10), and make it as short as possible.

6. If the S3100 unit will be directly exposed to the sun in an environment likely to reach 122°F (50°C), install a sun shield.

7. Install the antennas (see page 54).

8. Connect the loose end of your Ethernet cable into an Ethernet device or your computer.

Warning: To avoid damaging your equipment, ensure that the Ethernet cable is connected into the DATA port of the PoE injector, and not in the DATA & PWR port.

9. Power the unit by connecting the electric plug of the PoE injector into the outlet.

Installation of the Antenna

You install the antenna after the S3100 unit is in place. The antennas provided by Verint Video Solutions are designed to be mounted on a mast or pole of 2–3 inch (5–7.5 cm) diameter.

To install the antenna:

1. Install the antenna above the S3100 unit. If you bought your antenna from Verint Video Solutions, use the supplied pole mount bracket.

For illustrations of pole mount installations, see page 77.

2. Screw the SMA connector of the antenna cable to the S3100 main antenna port and tighten it with a 0.25-inch (0.6 cm) wrench.

Warning: Do not over-tighten to avoid damaging the connector. The recommended torque is 8 lb.-in. (100 N-cm). You could use a calibrated SMA torque wrench (for instance, from the Pasternack company, available at www.pasternack.com).

Warning: Do not use the auxiliary antenna connector and do not remove its termination cap.

3. Apply two or three layers of electrical tape around all RF connections.

The antenna cable and connectors are weather-tight; however, vibration caused by the wind will over time loosen the connectors and reduce the efficiency of the gaskets. The electrical tape will prevent this situation.

4. Carefully align the antenna with those of the other units (S1100w clients or S3100) so that they have a clear RF line of sight.

5. To improve the signal level between two units, use the antenna alignment utility from SConfigurator.

LEDs

The S3100 unit comes with three bicolor (green-red) LEDs that provide detailed information on the unit activity.

- LAN—For the Ethernet network (802.3) status:

Condition	Indication
Steady green	The unit is connected to the Ethernet network.
Flashing green (1-sec. flash every 3 sec.)	The unit is in normal operation but is not connected to the network.
Flashing green (0.1 sec. off for each packet)	A packet is received or transmitted.
Red blink (0.1 sec.)	There is a communication error.
Flashing red (0.1 sec. intervals)	The unit is being identified.
Flashing red (1 sec. intervals) happening simultaneously on all LEDs	On a master unit: There is another master currently running on the same frequency channel; for more information, see page 57.

- RF—For the wireless LAN (802.11) status:

Condition	Indication
Flashing green (1-sec. flash every 3 sec.)	The unit is in normal operation without any connected client/slave.
Steady green	The unit is in normal operation with at least one connected client/slave.
Flashing green (0.1 sec. off for each packet)	A packet is received or transmitted.
Red blink (0.1 sec.)	There is a communication error.
Flashing red (0.1 sec. intervals)	The unit is being identified.
Flashing red (1 sec. intervals) happening simultaneously on all LEDs	On a master unit: There is another master currently running on the same frequency channel; for more information, see page 57.

- System status—For the general unit status, similar to the single status LED on the other SmartSight units:

Condition	Indication
Steady red (1 sec.)	The unit is powering up.
Steady green (3 to 5 sec.)	The unit is loading its firmware.
Flashing green (1 sec. intervals)	The unit is in normal operation.
Flashing red (1 sec. intervals)	The IP address of the unit is already assigned to another unit in the network. or On a master unit: There is another master currently running on the same frequency channel; for more information, see page 57. This condition happens simultaneously on all LEDs.
Flashing green-red (1 sec. intervals)	The unit is undergoing a firmware update.
Flashing red (0.1 sec. intervals)	The unit is being identified.

The following power-up conditions on the system status LED are abnormal:

- LED not lit—Check the power supply and cabling. If power is available and the LED stays off, call Verint Video Solutions technical support for assistance.
- Steady red LED—There is an internal error that prevents the unit from starting normally. Power down, then power back up the unit once. If the condition persists, proceed to a firmware update (for details, refer to the *SConfigurator User Manual*). If the update fails or the condition persists after the update, call Verint Video Solutions technical support.
- Flashing red LED (2-second intervals)—There is an internal error that prevents the unit from operating normally. This situation may happen after a firmware update or after the first boot-up. Power down the unit and call Verint Video Solutions technical support.
- Flashing green-red LED not during a firmware update—The unit is in backup mode. You will need to start the firmware update procedure.

Duplicate Master Detection

The duplicate master detection problem occurs when two S3100 master units—with at least one using the SPCF mode—are using the same frequency channel and are seeing each other.

More specifically, the problem is detected when the second S3100 is booting up. This bridge refuses to start its wireless operations (to prevent any interference with the working setup) and makes its three LEDs flash red (1-second intervals). In the CLI of the unit, the Current SPCF Connection Status parameter turns to **Duplicate master detected** (accessed through **Advanced > Communication Status and Statistics > Wireless Status**). Furthermore, an error message is logged in the unit.

The already running master will not change its behavior.

Finding a “Lost” S3100

Since the S3100 does not have a serial port, you may have difficulty accessing it if you do not remember its IP address or VSIP port. For instance, if you enabled security on the unit, you cannot access it with Telnet; if you lost its VSIP port, you cannot locate it with SConfigurator.

To find a “lost” S3100 unit, you need to use SConfigurator and the common VSIP port.

To find a lost S3100:

1. Open SConfigurator.
2. From the General tab, click **Program Options**.
3. Click **Common** to set the common VSIP port, then **OK**.
4. Click the **Units** tab.

5. Click **Discover**.

All units on the network, regardless of their configurable VSIP ports, appear in the Units list. Locate the lost S3100 and write down its VSIP port and IP address in the form located at the end of the *S3100 Installation Guide*.

4

Setting Parameters with the CLI

The S3100 units come with a simple command line interface (CLI) for configuration purposes. The CLI is hierarchically organized, with menus, sub-menus, and individual options representing configuration parameters. Only the parameters that you are likely to change are described.

Getting Started

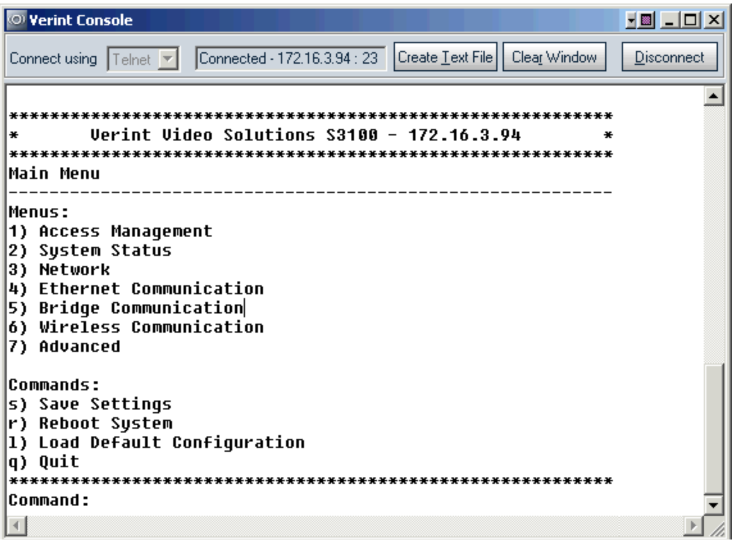
You can use the Telnet utility, through SConfigurator, to open the command line interface of the unit.

Note: Ensure that your computer and the S3100 unit are in the same IP subnet.

To enter the CLI with Telnet:

1. Open SConfigurator.
2. In the Units tab, discover the units.
3. Select the desired unit, then click **Telnet**.

   The CLI main menu appears in the Verint Console window.



```
***********************************************************
*       Verint Video Solutions S3100 - 172.16.3.94       *
***********************************************************
Main Menu
-----------------------------------------------------------
Menus:
1) Access Management
2) System Status
3) Network
4) Ethernet Communication
5) Bridge Communication
6) Wireless Communication
7) Advanced

Commands:
s) Save Settings
r) Reboot System
l) Load Default Configuration
q) Quit
***********************************************************
Command:
```

   The CLI has a timeout that is triggered after three minutes of inactivity. When the timeout occurs:

   - You lose access to the command line.
   - The “Thank you for using the Verint Video Solutions CLI” message appears at the command line.
   - The Verint Console window becomes disabled.
   - The Disconnect button switches to Connect.

4. To reactivate the CLI after a timeout, click **Connect**.

5. To work through the CLI menu structure, follow these guidelines:

- To execute a command or open a menu, type in the corresponding letter or number, then press **Enter**.
- To return to the previous menu, enter **p**.

6. To end the CLI work session:

a. Save the settings by entering **s** at the main menu, then pressing **Enter**.

b. Exit the CLI by entering **q** at the main menu, then pressing **Enter**.

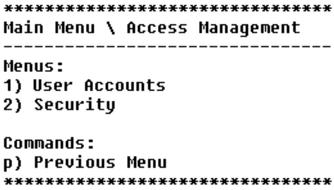
Depending on the changed settings, the unit may perform a soft boot.

c. Close the Verint Console window.

Warning: Do not use the Disconnect button to exit the CLI. Clicking it does not free the RS-232 connection and does not save your settings.

Access Management

The Access Management menu takes care of user accounts (user names and passwords) and unit security.

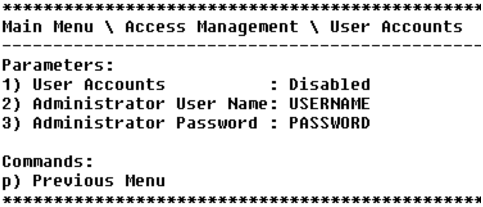


```
********************************
Main Menu \ Access Management
--------------------------------
Menus:
1) User Accounts
2) Security

Commands:
p) Previous Menu
********************************
```

User Accounts

The User Accounts menu enables you to protect the configuration of the unit by restricting its access with a user name and a password. Once the user account mode is activated, you need the user name/password combination to access the CLI through a Telnet session.

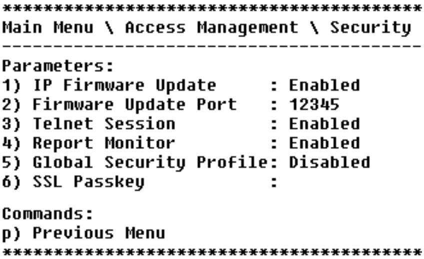


```
**********************************************
Main Menu \ Access Management \ User Accounts
----------------------------------------------
Parameters:
1) User Accounts          : Disabled
2) Administrator User Name: USERNAME
3) Administrator Password : PASSWORD

Commands:
p) Previous Menu
**********************************************
```

Security

The Security menu holds commands relative to the protection of the unit.



```
****************************************
Main Menu \ Access Management \ Security
----------------------------------------
Parameters:
1) IP Firmware Update     : Enabled
2) Firmware Update Port   : 12345
3) Telnet Session         : Enabled
4) Report Monitor         : Enabled
5) Global Security Profile: Disabled
6) SSL Passkey            :

Commands:
p) Previous Menu
****************************************
```

It allows you to control:

- Firmware updates through the IP network
- Access to Telnet
- SSL

IP Firmware Update

You can prevent firmware updates to be performed on your unit through the IP network. By default, this type of update is allowed. Be aware that it is the only available update method for the S3100, since it does not have a serial port.

For more information about firmware updates, refer to the *SConfigurator User Manual*.

Telnet Session

By default, you can use Telnet to access the CLI of your unit. To improve the security of your system, you may prohibit such an access. In this case, you will not have access to the unit CLI anymore.

Global Security Profile

This command is available if the unit has an SSL certificate. If you activate the global security profile, the unit will only accept secure SSL connections. It also means that you cannot access the unit anymore with Telnet and you cannot perform firmware updates through the IP network on it.

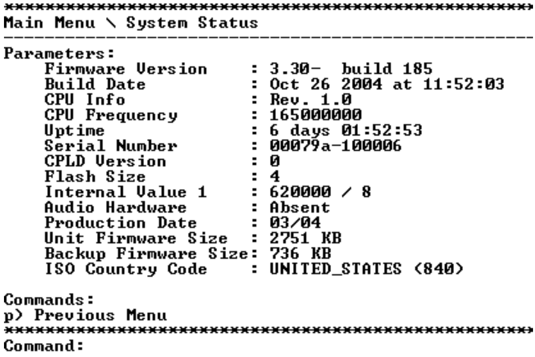
SSL Passkey

To secure a unit with SSL, provided of course it has an SSL certificate, you need to provide a passkey. This passkey must be the same for all units and the software tools to allow proper secure communication between them.

It is recommended to perform this operation in SConfigurator (version 2.55 or higher for the tool and the unit).

System Status

The system status information indicates the current values of internal S3100 parameters, including the firmware version.

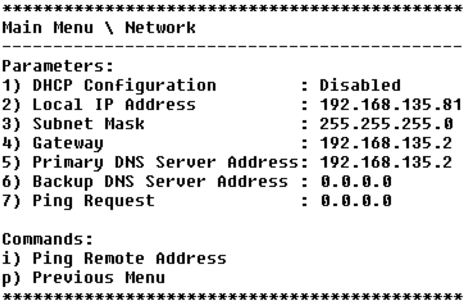


```
****************************************************
Main Menu \ System Status
----------------------------------------------------
Parameters:
    Firmware Version    : 3.30-  build 185
    Build Date          : Oct 26 2004 at 11:52:03
    CPU Info            : Rev. 1.0
    CPU Frequency       : 165000000
    Uptime              : 6 days 01:52:53
    Serial Number       : 00079a-100006
    CPLD Version        : 0
    Flash Size          : 4
    Internal Value 1    : 620000 / 8
    Audio Hardware      : Absent
    Production Date     : 03/04
    Unit Firmware Size  : 2751 KB
    Backup Firmware Size: 736 KB
    ISO Country Code    : UNITED_STATES (840)

Commands:
p> Previous Menu
****************************************************
Command:
```

Network

The Network menu allows you to configure several parameters to ensure the compatibility between the S3100 and its IP network.



```
********************************************
Main Menu \ Network
-------------------------------------------
Parameters:
1) DHCP Configuration        : Disabled
2) Local IP Address          : 192.168.135.81
3) Subnet Mask               : 255.255.255.0
4) Gateway                   : 192.168.135.2
5) Primary DNS Server Address: 192.168.135.2
6) Backup DNS Server Address : 0.0.0.0
7) Ping Request              : 0.0.0.0

Commands:
i) Ping Remote Address
p) Previous Menu
********************************************
```

For more information about these settings, contact your network administrator.

DHCP Configuration

DHCP (dynamic host configuration protocol) allows devices and computers connected to a network to automatically get a valid network configuration from a server. For more information about DHCP, see Appendix D on page 79.

You can set this option only if the S3100 is connected to a network that uses a DHCP server.

Local IP Address

The IP address is the identifier of the S3100 on the network. The IP address format is a 32-bit numeric address written as four numbers separated by periods. Each number is in the 0–255 range. Each device on a network must have a unique IP address.

Write down the final IP address in the form located at the end of the *S3100 Installation Guide*.

Subnet Mask

The subnet mask is the binary configuration specifying in which subnet the IP address of the unit belongs. A subnet is a portion of a network that shares a common address component. On TCP/IP networks, a subnet is defined as a group of devices whose IP addresses have the same prefix. Unless otherwise specified by your network administrator, it is recommended to use a subnet mask of 255.255.255.0.

Gateway

The gateway represents a network point that acts as an entrance to another network.

Warning: Never use the IP address of the unit as the gateway value.

Ping Request

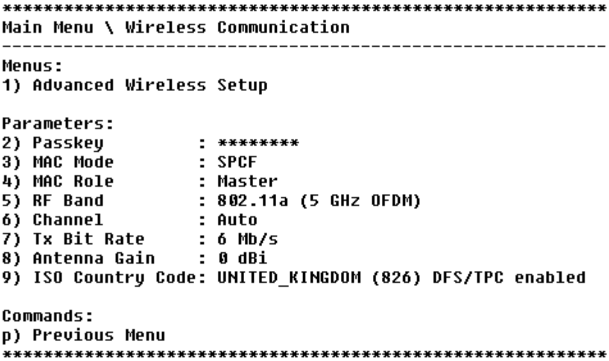
Ping is a basic Internet program that allows you to check that a particular IP address exists and can accept requests.

To ping a specific unit:

1. In the Ping request parameter, enter its IP address.
2. Execute the **Ping Remote Address** command.

Wireless Communication

The Wireless Communication menu contains a set of parameters relative to radio frequency (RF).



```
***********************************************************
Main Menu \ Wireless Communication
-----------------------------------------------------------
Menus:
1) Advanced Wireless Setup

Parameters:
2) Passkey         : ********
3) MAC Mode        : SPCF
4) MAC Role        : Master
5) RF Band         : 802.11a (5 GHz OFDM)
6) Channel         : Auto
7) Tx Bit Rate     : 6 Mb/s
8) Antenna Gain    : 0 dBi
9) ISO Country Code: UNITED_KINGDOM (826) DFS/TPC enabled

Commands:
p) Previous Menu
***********************************************************
```

Basic Parameters

Passkey

The wireless passkey is a unique case-sensitive identifier enabling secure and encrypted RF communication in a wireless cell (that is, with the other slave bridges and S1100w units). The passkey length varies depending on the key entry format (presented on page 68):

- 32 digits if hexadecimal
- 16 characters if string (default)

For the wireless connection to be secure, do no enter a known name (like a street name), but instead use a mix of digits and letters. Furthermore, do not disclose the passkey. The connection security is based on the secrecy and uniqueness of the passkey.

It is a good practice to change the default passkey during the configuration process.

MAC Mode

The two available MAC (media access control) modes are **SDCF** and **SPCF**. For more information, see page 12.

MAC Role

The MAC role represents the function of the unit in the wireless system. Possible values are: **Master** (default) and **Slave**. For more information, see page 8.

RF Band

The following frequency bands are available:

- 802.11a (5 GHz OFDM)
- 802.11g (2.4 GHz OFDM)

Channel

If your units are operating in a DFS environment, you cannot manually select the frequency channel; in this context, the displayed value of the Channel parameter is **Auto**.

On a master bridge in a non-DFS environment, you can either specify an RF channel manually or use the automatic channel selection. On a slave bridge, you can specify an initial value for the *roaming* process by which the unit will find its master; however, this initial channel may not be the one used by the master bridge.

The channels available in North America are:

- 1 to 11 in the 2.4 GHz band
- 52, 56, 60, and 64 in the 5.3 GHz band
- 149, 153, 157, 161, and 165 in the 5.8 GHz band

To know which channels are available elsewhere, refer to the *Wireless Frequency Plan* document located on our web site (Tools & Demos section).

Tx Bit Rate

The transmission bit rate is the data rate at which the unit operates. A high bit rate reduces the effective distance between two functional units.

You can set the bit rate in slave S3100 units only.

When a slave unit connects to its master for the first time, it automatically receives the best possible value (the **Auto** value), with a default RF margin set to 15 dB (to change the margin, see page 70).

Once the unit is operating properly, Verint Video Solutions strongly recommends to change the configured bit rate from Auto to the actual bit rate of the connection. This way, the wireless communication will be more stable in the presence of changing atmospheric conditions or other RF interferers. To know the actual bit rate of the connection, look in the **Advanced > Communication Status and Statistics > Wireless Status** menu. If the quality of the RF link degrades severely, the actual bit rate could be lower that the manually configured one.

The available bit rates for the slave S3100 unit are 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

Antenna Gain

If you enter the gain of the antenna you install on the unit, the S3100 will be able to automatically change its transmission power so that the total power (unit and antenna) does not exceed the maximum value established by your country’s regulations. For more information about the maximum antenna gain you can use, see page 28.

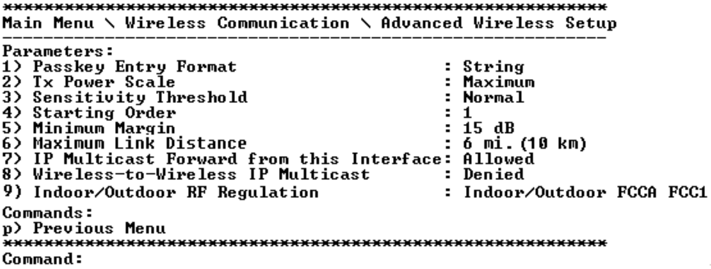
ISO Country Code

You must assign the proper country of operation to the unit, so that it will:

- Comply to the DFS/TPC regulations, if applicable
- Respect the EIRP rules
- Use the proper set of frequency channels

Advanced Parameters

The Advanced Wireless Setup menu contains specialized RF features.



```
**********************************************************
Main Menu \ Wireless Communication \ Advanced Wireless Setup
----------------------------------------------------------
Parameters:
1) Passkey Entry Format                     : String
2) Tx Power Scale                           : Maximum
3) Sensitivity Threshold                    : Normal
4) Starting Order                           : 1
5) Minimum Margin                           : 15 dB
6) Maximum Link Distance                    : 6 mi. (10 km)
7) IP Multicast Forward from this Interface: Allowed
8) Wireless-to-Wireless IP Multicast        : Denied
9) Indoor/Outdoor RF Regulation             : Indoor/Outdoor FCCA FCC1
Commands:
p) Previous Menu
**********************************************************
Command:
```

Passkey Entry Format

The wireless passkey can have two formats: string (default) or hexadecimal.

Tx Power Scale

The transmission power scale indicates the level of emitting power of the unit radio. The available values are:

- Maximum—The maximum allowed.
- 50%—The power is reduced by 3 dB.
- 25%—The power is reduced by 6 dB.
- 12.5%—The power is reduced by 9 dB.
- Minimum—The power is set at 3 dBm.

By default, the transmission power scale of a unit subject to the TPC regulations is set to 50%.

Sensitivity Threshold

The sensitivity threshold is the minimum signal level perceived by the radio of the unit.

Reducing the sensitivity of the radio enables unwanted “noise” to be filtered out. A safe value is 10 dB below the current received signal level (displayed in the **Advanced > Communication Status and Statistics > Wireless Status** menu). The default value, **Normal**, represents the most sensitive context. You must be careful not to reduce the sensitivity to a level where the unit would not “hear” its legitimate correspondent.

Starting Order

The starting order is a sequence number, used during the boot-up process of a master unit in a DFS context, to delay its startup. The purpose of this parameter is to ensure that colocated master units will not start at the same time. The default starting order is 1. Every colocated cell should have a different starting order: It should be incremented by 1 in each system.

At the beginning of the boot sequence, the master unit waits a specific number of seconds based on the value of this parameter. This wait period will ensure that no two masters will start at the same time and select the same frequency channel. This delay is: (*order* - 1) multiplied by 80 seconds.

The starting order has an impact only when the channel selection is automatic.

Minimum Margin

The minimum margin is used when the transmission bit rate is set to Auto. It represents the difference (in dB) between the actual signal received by the unit and the minimum signal required by a given bit rate to correctly receive data on the RF link. The default minimum margin is 15 dB. You can change it only on slave units.

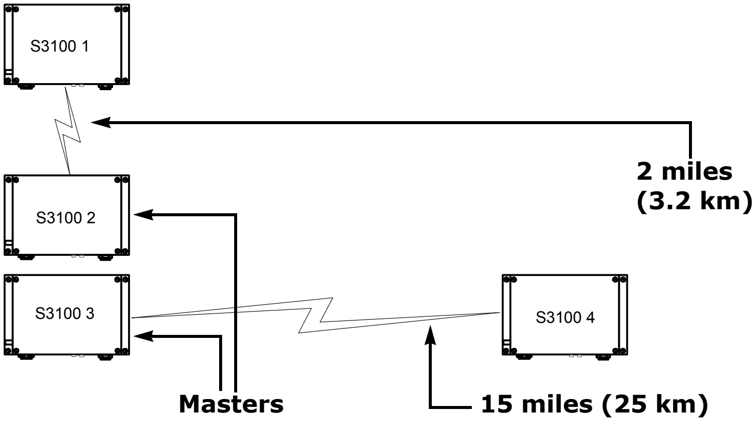
Maximum Link Distance

The maximum link distance parameter appears when the MAC mode is SDCF. It specifies the maximum transmission distance, between any two units, in all wireless cells present in the same geographical region and sharing the same frequency channel.

The two S3100 units making up an SDCF wireless cell must have the same value for this parameter. Possible values are:

- 3 miles (5 km)
- 6 miles (10 km)—default
- 9 miles (15 km)
- 12 miles (20 km)
- 15 miles (25 km)

For instance, consider the following setup, where the two wireless cells use the same frequency channel:



Since the two masters are in RF line of sight, all units must set their maximum link distance values to 15 miles (25 km). Otherwise packet collisions may occur, resulting in lost data.

Indoor/Outdoor RF Regulation

Depending on the country of operation and the chosen frequency band, the unit is allowed to operate indoors only, outdoors only, or either indoors or outdoors. The frequency channels available in the indoor-only regulation are different from those assigned to indoors/outdoors; the same goes for the outdoor-only channels.

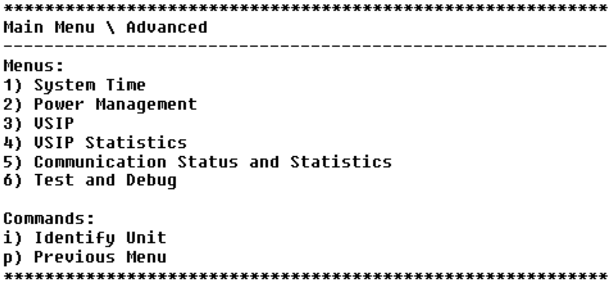
Note: Under the RF regulation, a unit programmed to be used only indoors must not be installed outdoors, and vice versa.

To know which frequency channels are available in your country of operation in each of the three operation modes, refer to the *Wireless Frequency Plan* document located on our web site (Tools & Demos section).

The default factory value for most countries is indoor/outdoor.

Advanced

The Advanced menu holds a series of advanced setups mainly used by Verint Video Solutions technical support. Some of these parameters are available through SConfigurator or a video management software.



```
***********************************************************
Main Menu \ Advanced
-----------------------------------------------------------
Menus:
1) System Time
2) Power Management
3) VSIP
4) VSIP Statistics
5) Communication Status and Statistics
6) Test and Debug

Commands:
i) Identify Unit
p) Previous Menu
***********************************************************
```

To recognize an S3100 among a large set of units, you can make its three LEDs flash red rapidly.

To identify an S3100 unit:

1. From the main menu, choose **Advanced**, then press **Enter**.
2. Enter **i** to make the LEDs flash red. Re-enter **i** to set the LEDs to their previous state.
3. Enter **p** until you are in the main menu.
4. Enter **q** to exit.

Load Default Configuration

The Load Default Configuration command, located in the main menu, resets all user parameters to their factory settings (described in Appendix A on page 73). All user-defined values will be lost.

Following a reset, you will need to reprogram the S3100 unit (for instance, its IP address and VSIP port) for proper operation within its network.

Reboot System

The Reboot System command, located in the main menu, performs a soft boot on the S3100. A system reboot clears all unsaved changes in the CLI and returns to your preset configuration.

A

Factory Default Configuration

The S3100 is programmed at the factory with the following configuration:

Type	Configuration
Access management	■ User name: USERNAME ■ Password: PASSWORD ■ User accounts: Disabled ■ Telnet sessions: Enabled ■ IP firmware update: Enabled ■ Global security profile: Disabled ■ SSL passkey: <empty>
Network	■ DHCP configuration: Disabled ■ IP address: 169.254.*.* (MAC address of the unit) ■ Subnet mask: 255.255.0.0 ■ Gateway: 169.254.*.* (MAC address of the unit)
Wireless Communication (North America)	■ Wireless passkey: ABCDEFGHIJKLMNOP ■ Frequency band: 802.11a (5 GHz OFDM) ■ Channel: Auto ■ Tx bit rate: Auto ■ Antenna gain: 13 dBi ■ Country: USA ■ Tx power scale: Maximum
Wireless Communication (Europe)	■ Wireless passkey: ABCDEFGHIJKLMNOP ■ Frequency band: 802.11a (5 GHz OFDM) ■ Channel: Auto ■ Tx bit rate: Auto ■ Antenna gain: 13 dBi ■ Country: United Kingdom ■ Tx power scale: 50% (-3 dB)
VSIP	■ VSIP Port: 5510 ■ VSIP multicast IP address: 224.16.32.1 ■ VSIP discovery IP address: 255.255.255.255

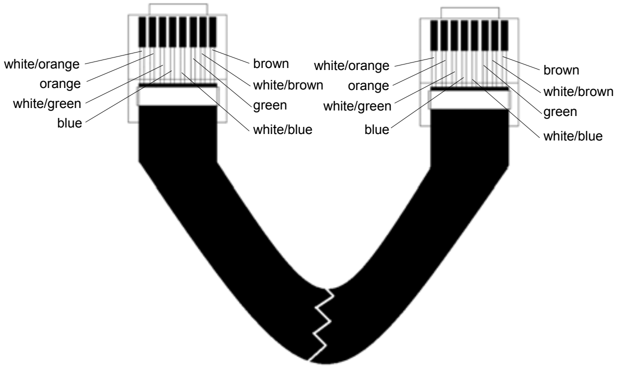
B

RJ-45 Ethernet Cables

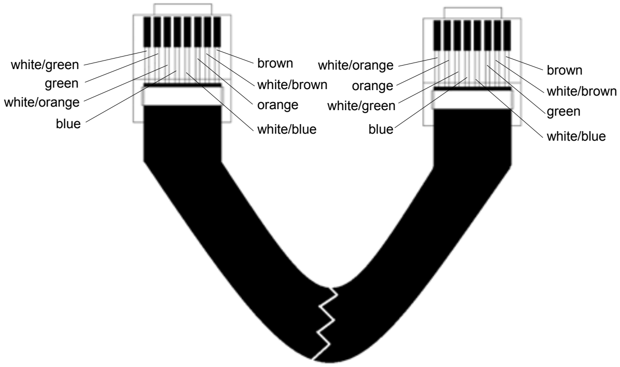
Depending on whether the S3100 unit is integrated on a network or not, the Ethernet cable varies:

- If on a network, use a straight-through cable.
- To link it directly to a computer, use a crossover cable.

Here is the bottom view of the RJ-45 connectors on a straight-through cable:



Here is the bottom view of the RJ-45 connectors on a crossover cable:



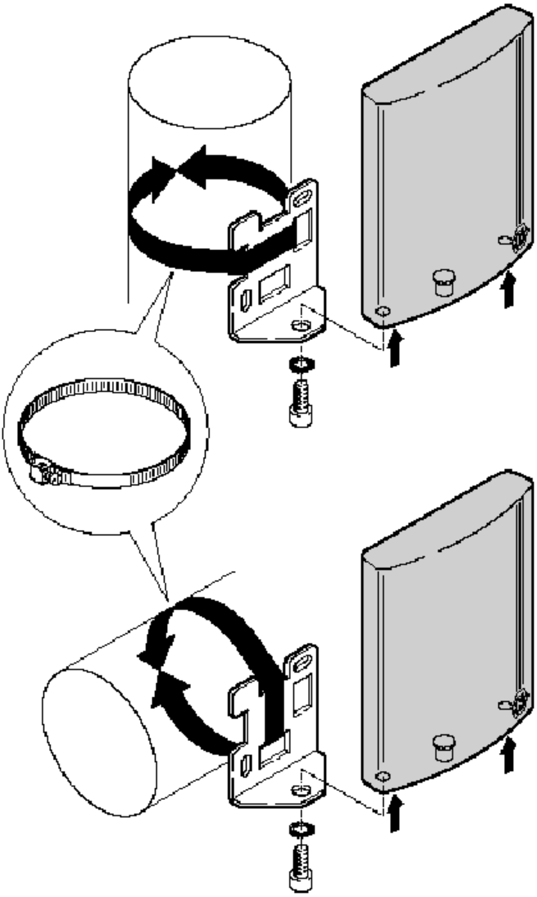
C

Pole Mounting of the Antennas

The installation procedure for the external antenna varies depending on the model.

ANT-WP13-5x/S Antenna

Here is the way to install the 13-dBi antenna to be used in the 5 GHz band:



D

DHCP Support and APIPA Service

DHCP (dynamic host configuration protocol) allows devices and computers connected to a network to automatically get a valid IP configuration from a dedicated server.

The APIPA (automatic private IP addressing) service, available on the Windows operating systems, enables a device to assign itself a temporary IP address.

At startup, a unit searches for a valid IP network configuration. The unit requires this configuration prior to starting its functions. The network configuration for SmartSight units consists of:

- An IP address
- A subnet mask
- A gateway

The unit first looks in its local memory. If no configuration is found, it tries to contact a DHCP server. If DHCP configuration fails—if the unit does not find a server or if it cannot get a configuration from it within one minute—the unit assigns itself temporary network settings based on the APIPA service. This service allows a unit to find a unique IP address until it receives a complete network configuration, either manually or from a DHCP server.

A unit in APIPA mode does not reside on the same subnet as the other devices on the IP network; therefore, it may not be able to see them or be visible to them. Units use the following temporary APIPA configuration:

- IP address: 169.254. *. *
- Subnet mask: 255.255.0.0
- Gateway: 169.254. *. *

The *. * portion is based on the MAC address of the unit.

A unit is in APIPA mode:

- The first time it boots up
- After receiving a duplicate IP address
- After a factory reset
- When the DHCP server does not have any available IP addresses

DHCP configuration is disabled:

- After a firmware upgrade
- After a factory reset

E

Surge Protection

Voltage and current surges can be induced by lightning strikes or power line transients. In the real world, under the right circumstances, these surges can reach sufficiently high levels to damage almost any electronic equipment. Therefore you need to add protection to your units.

The S3100 provides built-in surge protection on the Ethernet/PoE and 24V AC power connectors. The antenna connectors do not have surge protection; this situation should not cause problems as long as you keep the antenna cable short—that is, below 6.6 feet (2 meters).

If you are installing an S3100 unit (*S3100* model) in a heavy lightning environment, or in a site where large AC mains power fluctuations are a common occurrence, Verint Video Solutions recommends that you add surge protection on the DATA & PWR port of the PoE injector. It will protect your equipment and the power inserter from surges coming down from the Ethernet cable.

Using a surge protector is strongly recommended if the Ethernet cable runs outside the building for more than 82 feet (25 meters). This device should be installed at the entry point of the cable inside the building. To be effective, this protection equipment must be properly grounded.

PoE protectors recommended by Verint Video Solutions include:

Company	**Part number**	**Web site**
Citel	MJ8-505-24D3A60	www.citelprotection.com
Transtector Systems	1101-693 TSJ POE-48	www.transtector.com

For the curious mind, a surge protector helps to clamp the surge to safe levels and divert its energy to the earthing point, preventing device damage. Experienced installers know that an effective surge protection must be installed with proper earthing and grounding.

F

RF Contact between Masters

If the country of operation of your units requires DFS compliance, you must ensure that the master units (S3100 and S1100-R) in colocated cells “see” one another in their permanent location. Such a contact means that RF communication can be performed between each pair of masters, therefore preventing them to choose the same frequency channel.

Apply the following procedure to ensure that *MasterA* sees *MasterB*. You will have to access the command line interface (CLI) of at least one master. For more information about the CLI, refer to Chapter 4 in the *S3100 User Manual* or to Chapter 4 in the *S1100 User Manual*.

To ensure that two master units see each other:

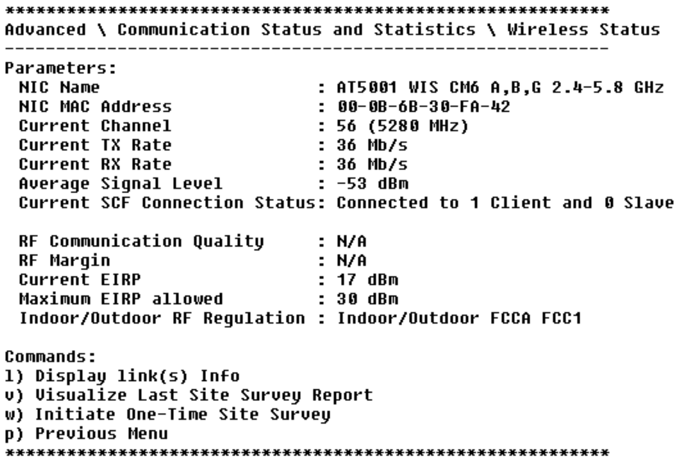
1. Take down the unit name of MasterB.

The unit name is displayed in SConfigurator's Units tab, in the Unit Information pane of the Configuration Assistant, or in the **Advanced > VSIP** menu of the CLI.

2. Shut down MasterB, then power it up.

3. Wait until MasterB has selected a frequency channel. To ensure that a channel is selected:

□ If MasterB is an S3100, go in the **Advanced > Communication Status and Statistics > Wireless Status** menu of the CLI. Wait until the value of Current SCF Connection Status is **Connected to *X* Clients and *Y* Slaves**.

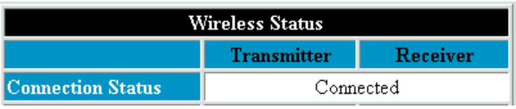


```
***********************************************************
Advanced \ Communication Status and Statistics \ Wireless Status
-----------------------------------------------------------
Parameters:
  NIC Name                     : AT5001 WIS CM6 A,B,G 2.4-5.8 GHz
  NIC MAC Address              : 00-0B-6B-30-FA-42
  Current Channel              : 56 (5280 MHz)
  Current TX Rate              : 36 Mb/s
  Current RX Rate              : 36 Mb/s
  Average Signal Level         : -53 dBm
  Current SCF Connection Status: Connected to 1 Client and 0 Slave

  RF Communication Quality     : N/A
  RF Margin                    : N/A
  Current EIRP                 : 17 dBm
  Maximum EIRP allowed         : 30 dBm
  Indoor/Outdoor RF Regulation : Indoor/Outdoor FCCA FCC1

Commands:
l) Display link(s) Info
v) Visualize Last Site Survey Report
w) Initiate One-Time Site Survey
p) Previous Menu
***********************************************************
```

- □ If MasterB is an S1100, go in the **Wireless Status** window of the Configuration Assistant. Wait until the connection status is **Not Connected** or **Connected**; these statuses occur after **Radar Detection**.



Wireless Status		
	Transmitter	Receiver
Connection Status	Connected	

- □ If you do not have access to the connection status of MasterB, wait for the following time period: (starting order of MasterB - 1) multiplied by 80 seconds.

4. Perform a site survey in MasterA:

a. Open the CLI of the unit.

a. Go in the **Advanced > Communication Status and Statistics > Wireless Status** menu.

b. Execute the **Initiate One-Time Site Survey** command.

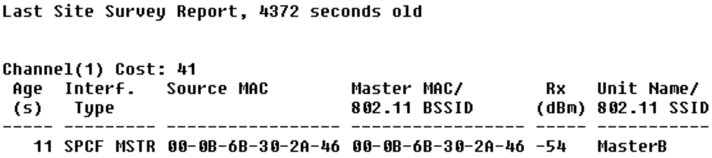
c. To see the progress of the operation, press **Enter** every second.

The site survey is completed when the value of Current SCF Connection Status returns to **Connected to *X* Clients and *Y* Slaves**, after having gone to **Site survey (100% completed)**.

d. Execute the **Visualize Last Site Survey Report** command.

e. Check that the MasterB name is listed as the Unit Name of one of the channels. You may have to scroll up the CLI window to see the beginning of the survey data.

For example, in the following site survey, MasterB has a visual connection with the MasterA unit. If the MasterB name is not displayed in the site survey, it means that the two masters cannot see each other.



```
Last Site Survey Report, 4372 seconds old


Channel(1) Cost: 41
 Age  Interf.   Source MAC         Master MAC/        Rx    Unit Name/
 (s)   Type                        802.11 BSSID      (dBm) 802.11 SSID
----- --------- ----------------- ----------------- ----- -----------
   11 SPCF MSTR 00-0B-6B-30-2A-46 00-0B-6B-30-2A-46 -54   MasterB
```

G

Separation Between Units Using Adjacent Channels

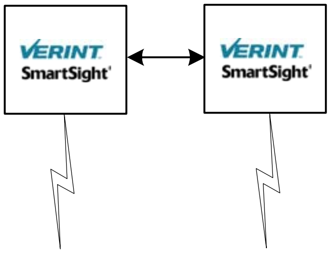
If using adjacent frequency channels in a non-DFS environment, you should respect guidelines relative to the minimum separation between unit antennas. The guidelines apply to the S1100, S1100w, and S3100 units.

In the 2.4 GHz band, the *adjacent channel* term applies only to the three non-overlapping channels (1, 6, and 11).

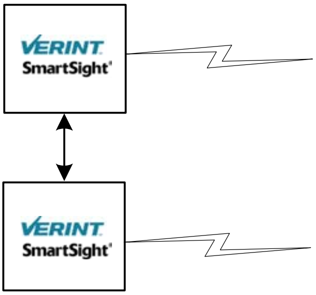
The presented figures represent worse case scenarios. By respecting them, you can assume that there will not be radio interference between the units.

Three physical setups are covered:

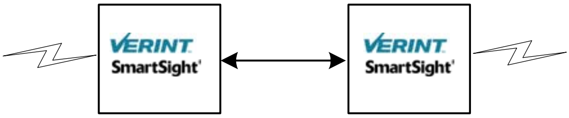
Side by side:



On top:



Back to back:



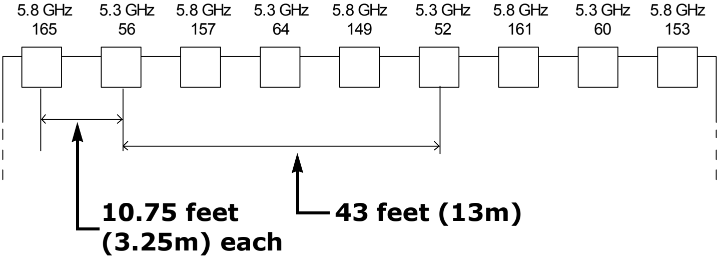
The minimum separation between units using adjacent channels are:

Setup	5 GHz (13-dBi antenna with 40º beam width)	2.4 GHz (8.5-dBi antenna with 60º beam width)
Side by side	43 feet (13m)	55.8 feet (17m)
On top	13 feet (4m)	6.2 feet (1.9m)
Back to back	7.8 feet (2.4m)	15.7 feet (4.8m)

If you are using other antennas with narrower beam widths, the distances may be reduced. For assistance, contact the Verint Video Solutions project engineering group.

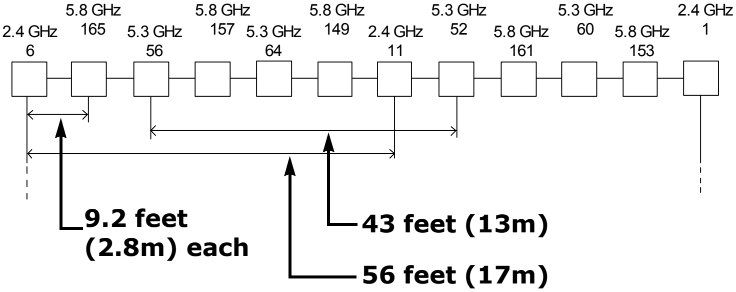
To help you plan your systems, here are installation scenarios that respect the limitations. These scenarios include the frequency band and channel.

- Using only 5 GHz channels, all on the same side of a building:



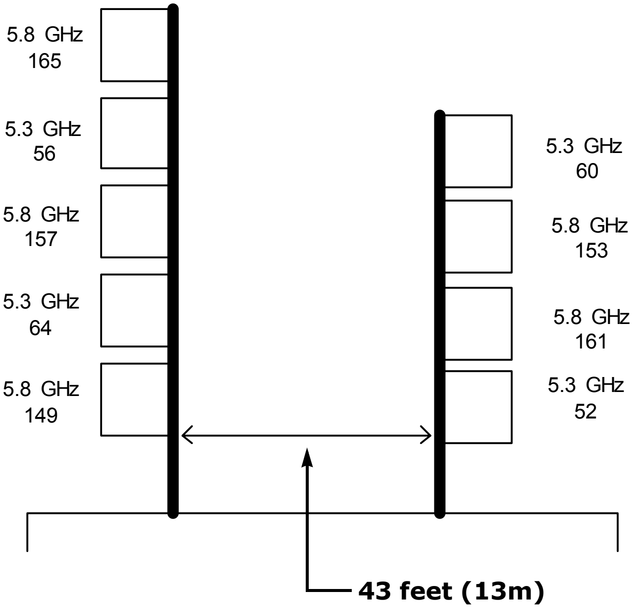
Notice that the units using the adjacent channels 52 and 56 are separated by the prescribed 43 feet (13m). However, you can intersperse other units in-between, as long as they do not use adjacent channels. This way, you can increase the unit density without encountering interference problems.

- Using 5 GHz and 2.4 GHz channels, all on the same side of a building:

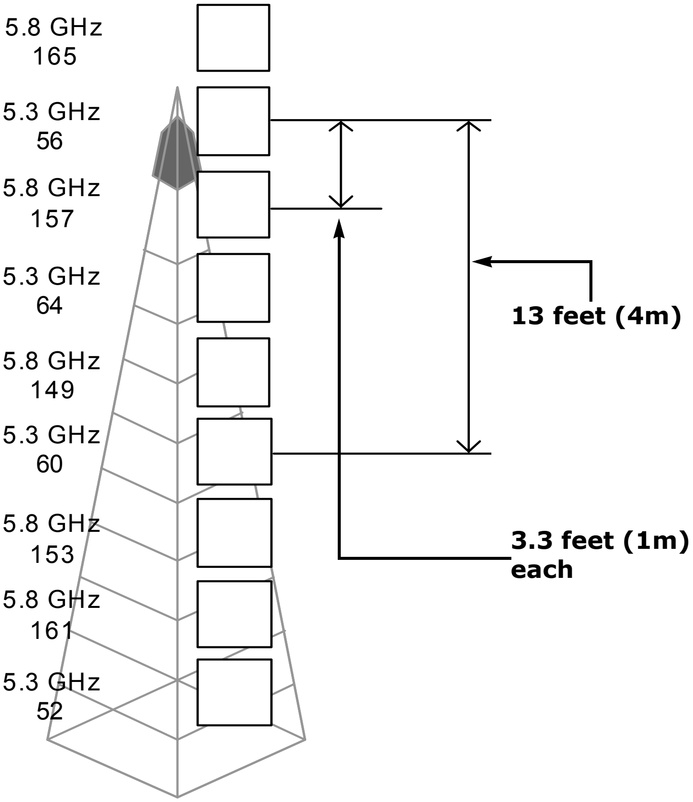


The units using the adjacent channels 6 and 11 in the 2.4 GHz are separated by the prescribed 56 feet (17m).

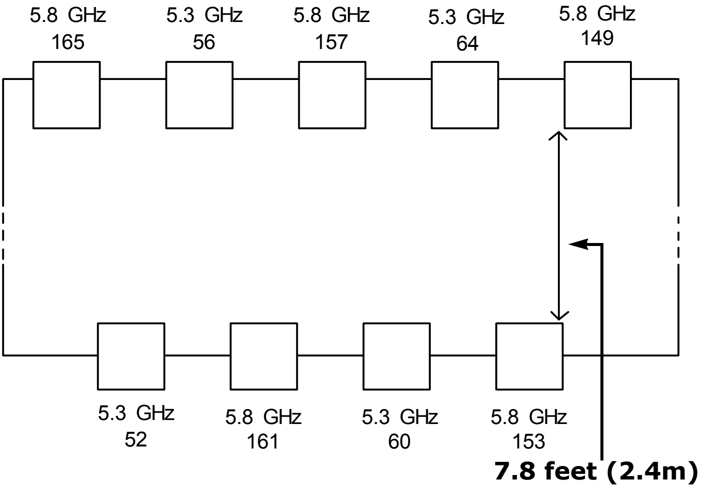
- Using only 5 GHz channels, all pointing in the same direction on two poles. There is no minimum separation between any two adjacent units sharing a pole, since they do not use adjacent channels:



- Using only 5 GHz channels, all on the same side of a tower. The minimum separation between units using adjacent channels—for example, 56 and 60—is the prescribed 13 feet (4m):



- Using only 5 GHz channels, on two sides of a building. There is no separation limitation between any two adjacent units, since they do not use adjacent channels. The minimum separation of 7.8 feet (2.4m) between back-to-back units is respected:



H

Technical Specifications

Here are the S3100 technical specifications:

Network	RF interface	SmartSight SPCF and SDCF
	Modulation	OFDM
	Encryption	128-bit AES
	Data rate (max. burst rate)	6, 9, 12, 18, 24, 36, 48, and 54 Mbps
	Ethernet connector	Weatherproof 10/100Base-T (RJ-45)
	Protocols	Transport: RTP/IP, UDP/IP, TCP/IP, or multicast IP Others: DNS and DHCP client
	Security	SSL-based authentication
Power	Input voltage	S3100: 48V DC PoE S3100-RP: 24V AC +/- 10%
	Consumption	12W (250 mA at 48V DC) 25 VA at 24V AC
	Connector	Weatherproof circular
Physical	Enclosure	NEMA 4X/IP 66 powder coat painted die-cast aluminum with wall mounting brackets
	Size	8.1L x 5.5W x 4.1H in. (205L x 140W x 105H mm)
	Weight	2.0 lb. (0.90 kg)
	Environment	-22ºF to 122ºF (-30ºC to 50ºC)
	Humidity	95% non condensing at 122°F (50°C)
	LED indicators	Status, wireless activity, LAN activity
	Antenna connectors	SMA female
Certification/ Regulation	USA	FCC part 15 (subparts B, C, and E)
	Canada	Industry Canada RSS-210 and ICES-003
	Europe	CE marked EN 300 328-2 V1.2.1 (2001-12) EN 301 893 V1.2.3 (2003-08) EN 301 489-01 V1.4.1 (2002-08) EN 301 489-17 V1.2.1 (2002-08) EN 60950:2000

Glossary

This glossary is common to the SmartSight line of products.

Access Point A device acting as a communication switch for connecting wireless units to a wired LAN. Access points are mainly used with wireless transmitter units to transfer wireless content onto the wired IP network.

APIPA (Automatic Private IP Addressing) A feature of Windows-based operating systems that enables a device to automatically assign itself an IP address when there is no dynamic host configuration protocol (DHCP) server available to perform that function. Also known as *AutoIP*.

Bridge A unit linking a wireless network to a wired Ethernet network. The newest SmartSight bridge is the S3100.

CCTV (Closed Circuit Television) A television system in which signals are not publicly distributed; cameras are connected to television monitors in a limited area such as a store, an office building, or on a college campus. CCTV is commonly used in surveillance systems.

CIF (Common Image Format) A video format that easily supports both NTSC and PAL signals. Many CIF flavors are available, including CIF, QCIF, 2CIF, and 4CIF. Each flavor corresponds to a specific number of lines and columns per video frame.

CLI (Command Line Interface) A textual user interface in which the user responds to a prompt by typing a command.

Codec (Coder/Decoder) A device that encodes or decodes a signal.

Configuration Assistant A proprietary graphical program used to configure and update the firmware of the S1100 units.

DCE (Data Communication Equipment) In an RS-232 communication channel, a device that connects to the RS-232 interface. SmartSight units and modems are DCE.

Decoder See *Receiver*.

DHCP (Dynamic Host Configuration Protocol) A communication protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in a network.

DTE (Data Terminal Equipment) In an RS-232 communication channel, the device to which the RS-232 interface connects. Computers, switches, multiplexers, cameras, and keyboards are DTE.

DVR (Digital Video Recorder) A device (usually a computer) that acts like a VCR in that it has the ability to record and play back video images. The DVR takes the feed from a camera and records it into a digital format on a storage device which is most commonly the hard drive.

Encoder See *Transmitter*.

Ethernet A local-area network (LAN) architecture using a bus or star topology and supporting data transfer rates of 10 Mbps. It is one of the most widely implemented LAN standards. The 802.11 protocols are often referred to as "wireless Ethernet."

Firmware Software stored in read-only memory (ROM) or programmable ROM (PROM), therefore becoming a permanent part of a computing device.

IP (Internet Protocol) The network layer for the TCP/IP protocol suite widely used on Ethernet networks.

LAN (Local Area Network) A computer network that spans a relatively small area. A LAN can connect workstations, personal computers, and surveillance equipment (like video servers). See also *WAN*.

MPEG-4 A graphics and video lossy compression algorithm standard that is derived from MPEG-1, MPEG-2, and H.263. MPEG-4 extends these earlier algorithms with synthesis of speech and video, fractal compression, computer visualization, and artificial intelligence-based image processing techniques.

Multicast Communication between a single sender and multiple receivers on a network; the devices can be located across multiple subnets, but not through the Internet. Multicast is a set of protocols using UDP/IP for transport.

nDVR The SmartSight video management and storage software. This graphical product is used in conjunction with wired and wireless video servers.

NTSC (National Television Standards Committee) The North American standard (525-line interlaced raster-scanned video) for the generation, transmission, and reception of television signals. In addition to North America, the NTSC standard is used in Central America, a number of South American countries, and some Asian countries, including Japan. Compare with *PAL*.

NTP (Network Time Protocol) A protocol designed to synchronize the clocks of devices over a network.

OSD (On-Screen Display) Status information displayed on the video monitor connected to a receiver unit.

PAL (Phase Alternation by Line) A television signal standard (625 lines, 50 Hz, 220V primary power) used in the United Kingdom, much of western Europe, several South American countries, some Middle East and Asian countries, several African countries, Australia, New Zealand, and other Pacific island countries. Compare with *NTSC*.

PTL (Push-to-Listen) In a two-way system, the communication mode in which the listener must push a button while listening.

PTT (Push-to-Talk) In a two-way system, the communication mode in which the talker must push a button while talking.

PTZ Camera (Pan-Tilt-Zoom) An electronic camera that can be rotated left, right, up, or down as well as zoomed in to get a magnified view of an object or area. A PTZ camera monitors a larger area than a fixed camera.

Receiver A device converting a digital video signal into an analog form. Also called *decoder*.

Repeater A range extender for wireless links. The SmartSight repeater is made up of two S3100 bridges.

RF (Radio Frequency) Any frequency within the electromagnetic spectrum associated with radio wave propagation. When a modulated signal is supplied to an antenna, an electromagnetic field is created that is able to propagate through space. Many wireless technologies are based on RF field propagation.

RS-232 A standard interface approved by the Electronic Industries Alliance (EIA) for connecting serial devices.

RS-422 A standard interface approved by the Electronic Industries Alliance (EIA) for connecting serial devices, designed to replace the older RS-232 standard because it supports higher data rates and greater immunity to electrical interference.

RS-485 An Electronics Industry Alliance (EIA) standard for multipoint communications.

S1000 Series The SmartSight series of secure outdoor wireless video systems (one receiver and one transmitter per system). The series covers the 2.4 GHz band in North America and Europe and the 5 GHz band in North America. Starting with firmware release 3.20, the S1000 series is replaced by the new S1100 units.

S1000w The SmartSight outdoor wireless video transmitter operating on the 2.4 GHz frequency band.

S1100 The newest series of secure outdoor wireless video systems (one receiver and one transmitter per system) covering the 2.4 and 5 GHz bands in North America and Europe.

S1100w The multiband (2.4 and 5 GHz) SmartSight outdoor wireless video transmitter operating in North America and Europe.

S1500e Series The SmartSight series of wired video servers (receivers and transmitters) designed for video monitoring and surveillance over IP networks. The transmitters in the series offer from one to eight video inputs; the series proposes two receivers with one and four video outputs.

S1600e The SmartSight high-resolution wired video server (receiver and transmitter) providing point-to-point analog extension with web access.

S1700e Series The newest SmartSight series of wired video transmitters designed for video monitoring and surveillance over IP networks, offering DVD-quality video and power over Ethernet. The transmitter in the series offers one video input and web access.

S1708e Series The newest SmartSight series of wired video transmitters designed for a variety of video monitoring and surveillance applications in which a high concentration of cameras terminates within the same area. The transmitters in the series offer 8, 12, or 24 video inputs.

S3100 The outdoor, wireless, digital SmartSight video bridging unit. It has many uses, including linking video servers (wireless or wired) to an Ethernet LAN and acting as a range extender.

SConfigurator A proprietary graphical program used to configure and update the firmware of video server and outdoor wireless bridge units.

Serial Port An interface that can be used for serial communication, in which only one bit is transmitted at a time. A serial port is a general-purpose interface that can be used for almost any type of device.

SSL (Secure Sockets Layer) A commonly used protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection. The SSL protocol secures the following data: I/O, serial port, and VSIP communication; it does not apply to audio and video transmission.

Transceiver (Transmitter/Receiver) A device that both transmits and receives analog or digital signals.

Transmitter A device sending video signals captured with a connected camera or dome to a receiver. The transmitter converts the analog signal into a digital form before transmitting it. Also called *encoder*.

Video Server A unit transmitting or receiving video signals through an IP network. The SmartSight wireless servers are the S1000w and S1100w units; the wired servers are the S1500e series, S1600e, S1700e series, and S1708e series units.

VSIP (Video Services over IP) A proprietary communication protocol for sending messages between a computer and a SmartSight unit, or between two units.

WAN (Wide Area Network) A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local area networks (LANs).

WEP (Wired Equivalent Privacy) A security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. It is designed to afford wireless networks the same level of protection as a comparable wired network.

Wireless Cell A group of wireless devices that communicate together on the same radio frequency channel and share the same wireless passkey.

Wireless Transmission A technology in which electronic devices send information to receivers using radio waves rather than wiring.

Index

Compliance

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the effective isotropic radiated power (EIRP) is not more than that required for successful communication.

Note: The S3100 units require professional installation. They should be installed in a location that would prevent the general population from approaching from 3 feet (1 meter) of the radiating element.

USA

This device complies with part 15 of the FCC (Federal Communications Commission) rules (see http://www.fcc.gov/).

Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation of the device.

This equipment has been tested and found to comply with the limits for Class B Digital Device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in residential installation. This equipment generates and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and the S3100 unit
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

Any changes or modifications not expressly approved by Verint Video Solutions could void the user’s authority to operate the equipment.

Canada

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that required for successful communication.

Italia

L'uso di questo apparato in Italia è regolamentato da:

- D.Lgs 1.8.2003, n.259, articoli 104 (attività soggette ad autorizzazione generale) e 105 (libero uso), per uso privato;
- D.M. 28.5.03, per la fornitura al pubblico dell'accesso alle reti e ai servizi di telecomunicazioni (R-LAN or R-LAN and Hiperlan).

Europe

Declaration of Conformity

Manufacturer:

Verint Systems Inc.
1800 Berlier
Laval, Québec
H7L 4S4
Canada

Declares under sole responsibility that the product:

Product name: Outdoor wireless bridge
Model number: S3100-CE, S3100-CE-RP

To which this declaration relates is in conformity with the following standards or other documents:

R&TTE Directive 1999/5/EC

EN 300 328-2 V1.2.1 (2001-12)
EN 301 893 V1.2.3 (2003-08)
EN 301 489-01 V1.4.1 (2002-08)
EN 301 489-17 V1.2.1 (2002-08)
EN 60950:2000

I, the undersigned, hereby declare that the equipment specified above conforms to the above Directive(s) and Standard(s).

May 6th, 2004
Laval, Canada

Willie Kouncar
Vice President, Product development
Verint Video Solutions

Turkey

Declaration of Conformity

Manufacturer:

Verint Systems Inc.
1800 Berlier
Laval, Québec
H7L 4S4
Canada

Declares under sole responsibility that the product:

Product name: Outdoor wireless bridge
Model number: S3100-TR-24, S3100-TR-RP-24

To which this declaration relates is in conformity with the following standards or other documents:

R&TTE Directive 1999/5/EC

EN 300 328-2 V1.2.1 (2001-12)
EN 301 489-01 V1.4.1 (2002-08)
EN 301 489-17 V1.2.1 (2002-08)
EN 60950:2000

I, the undersigned, hereby declare that the equipment specified above conforms to the above Directive(s) and Standard(s).

December 14th, 2004
Laval, Canada

Willie Kouncar
Vice President, Product development
Verint Video Solutions

Verint Video Solutions
1800 Berlier Street
Laval (Quebec)
Canada
H7L 4S4

VERINT
POWERING ACTIONABLE INTELLIGENCE™