

Nextiva S3100 Series User Guide

Covering the S3100, S3100-BR, and
S3100-RP

Firmware Release 4.12

October 2007

Nextiva S3100 Series

Covering the S3100, S3100-BR, and S3100-RP

Firmware Release 4.12

User Guide

This document contains confidential and proprietary information of Verint Systems Inc. and is protected by copyright laws and related international treaties. Unauthorized use, duplication, disclosure or modification of this document in whole or in part without the written consent of Verint Systems Inc. is strictly prohibited.

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.

All marks referenced herein with the ® or TM symbol are registered trademarks or trademarks of Verint Systems Inc. or its subsidiaries. All rights reserved. All other marks are trademarks of their respective owners.

© 2007 Verint Systems Inc. All rights reserved.

www.verint.com/videosolutions

Publication date: October 10, 2007

Contents

Preface	vii
Who Should Read this Guide	viii
How to Use this Guide	viii
Conventions	viii
Related Documentation	viii
Related Products	ix
About Us	ix
Warranty	x
Chapter 1 ■ Overview	1
About the S3100 Series	2
Shipment	2
Casing Description	3
S3100	4
S3100-BR and S3100-RP	4
Chapter 2 ■ System and RF Planning	5
Available Frequency Bands and Channels	6
2.4 GHz Band	6
4.9 GHz Band	6
5 GHz Band	7
Wireless Cells	8
Roles	8
Compatibility Issues	8
Video Bit Rate and Data Throughput	10
System Planning	12
MAC Protocols	13
TPC	13
DFS	14
Application Types	15
Access Point	16
Point-to-Multipoint Repeater	16
Point-to-Point Repeater	17
Wireless Bridge	18
Wireless Bridge Repeater	19
Colocated Cells	20
Distance Limitations	20
General Guidelines	20
4.9 GHz Band in North America	20
5 GHz Band in North America and 2.4 GHz Band	21
5 GHz Band in Europe	22
RF Planning	25
Location Evaluation	25
Antenna Requirements	26
Interference	27
RF Exposure Considerations	27

Chapter 2 ■ Configuring and Installing the Device	29
Computer Requirements	30
Point-to-Point Repeater	30
Access Point	31
Point-to-Multipoint Repeater	32
Wireless Bridge	33
Wireless Bridge Repeater	34
Power Connections	35
Power over Ethernet	36
24V DC Power	37
Configuration	37
Changing the IP Address of the Computer	37
Device Preparation	41
IP Parameters	41
Country Selection and Device Name	43
Wireless Parameters	44
Communication Checking	47
Installation	47
Installation of the S3100-RP Devices	47
Installation of the S3100-BR Devices	48
Installation of the S3100 Access Point Device	49
Installation of the Antenna	50
Firmware Update	50
Quality of Service	51
LEDs	51
Duplicate Master Detection	52
Finding a “Lost” S3100	53
Chapter 4 ■ Setting Parameters with the CLI	55
Getting Started	56
Access Management	57
User Accounts	57
Security	57
System Status	59
Network	59
Wireless Communication	60
Basic Parameters	61
Advanced Parameters	63
Advanced	65
Identifying a Device	65
Conducting Site Surveys	66
Load Default Configuration	66
Reboot System	67
Appendix A ■ Factory Default Configuration	69
Appendix B ■ RJ-45 Ethernet Cables	71
Appendix C ■ Pole Mounting of the Antennas	73
Appendix D ■ DHCP Support and APIPA	75
Appendix E ■ Surge Protection	77
Appendix F ■ RF Contact between Masters	79

- Appendix G ■ Separation Between Devices Using Adjacent Channels83**
 - Performing a Site Survey 84
 - Minimum Distances 87
- Appendix H ■ DFS and False Radar Detection91**
- Appendix I ■ S3100 Technical Specifications93**
- Glossary95**
- Index101**
- Compliance 107**

Preface

The *Nextiva S3100 Series User Guide* presents the information and procedures on installing and configuring the Nextiva™ S3100 series multipurpose outdoor wireless device.

Who Should Read this Guide

This guide is intended for managers, IT system administrators, engineers, and technicians who will use the S3100 series edge devices. It provides conceptual information on how to configure, install, and operate the devices.

This guide assumes that you are familiar with:

- Installation and manipulation of electronic equipment
- General use of computers
- Local area networks (LANs) and basic IP data communication concepts and practices
- Radio frequency (RF) platforms
- Pan-tilt-zoom (PTZ) platforms (cameras and keyboards)
- Microsoft Windows operating systems

How to Use this Guide

This guide contains all the information needed to install and configure an S3100 series device.

Conventions

The following typographic conventions are used throughout this guide:

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.
<i>connection_name</i>	Text that must be replaced by a user-supplied value. Text representing variable content.
SConfigurator.exe	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 guide, the following documentation is also available:

- *Nextiva S3100 Installation Guide*
- *Nextiva S3100-BR Installation Guide*
- *Nextiva S3100-RP Installation Guide*
- *SConfigurator User Guide*
- *Release Notes*

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

Related Products

You can use the S3100 series devices with the Nextiva S1100 wireless systems, the S1100w wireless video transmitters, and the wired Ethernet edge devices.

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

About Us

Verint® Systems Inc. (NASDAQ: VRNT) is a leading global provider of analytic software-based solutions for security and business intelligence. Verint solutions help organizations make sense of the vast voice, video, and data available to them, transforming this information into actionable intelligence for better decisions and highly effective performance.

Since 1994, Verint has been committed to developing innovative solutions that help global organizations achieve their most important objectives. Today, organizations in over 50 countries use Verint solutions to enhance security, boost operational efficiency, and fuel profitability.

Web Site

For information about the Nextiva line of products, visit www.verint.com/videosolutions.

To request the latest versions of firmware and software or to download other product-related documents, you need access to the Verint Video Intelligence Solutions partner extranet. To register, go to <http://vvs.verint.com>.

Support

If you encounter any type of problem after reading this guide, contact your local distributor or Verint representative. You can also use the following sections on the partner extranet to find the answers to your questions:

- Knowledge Base
- FAQ
- My Account

For assistance with the Nextiva edge devices and the related software, contact the customer service team:

- By phone: 1 888 747-6246 or 631 962-9202
- By email: vvssupport@verint.com

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 series is a multipurpose, outdoor, wireless, digital video product covering the 2.4 GHz and 5 GHz frequency bands in North America and Europe, and the 4.9 GHz public safety band in North America.



Note: The S3100 series devices require professional installation.

About the S3100 Series

The S3100 series has many uses, including:

- Access point application—A communication hub for multiple S1100w devices
- Point-to-point repeater—A range extender for one or many pairs of S1100 devices
- Point-to-multipoint repeater—A range extender for multiple S1100w devices
- Wireless bridge—A link between two networks (wired or wireless)
- Wireless bridge repeater—A range extender for a wireless bridge

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

- S3100—A single device for access point applications
- S3100-BR—Two devices for wireless bridge applications
- S3100-RP—Two devices for repeater applications

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

Every S3100 device comes with the following security features:

- SSL—Every edge device 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 with another device or the SConfigurator tool can be secured.

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

Once a device 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 Guide*.

- SPCF/SDCF—These proprietary MAC (Media Access Control) protocols use AES encryption (with key rotation) over the wireless link to secure communication between the devices. They secure VSIP communication as well as audio and video data. For more information, see page 13.

Shipment

Your shipment contains the following items:

- The requested S3100 series product, with wall mount brackets already installed
- One or two pole mount bracket sets, including stainless steel clamps
- For an S3100 device:
 - 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 device:
 - Two 30-foot (10-meter) 24V AC outdoor power cords
 - A 3-foot (1-meter) outdoor crossover Ethernet cable
- For an S3100-BR device:
 - Two 30-foot (10-meter) 24V AC outdoor power cords
 - Two 82-foot (25-meter) outdoor straight-through Ethernet cables
- The *Utilities* CD containing the release notes and documentation for the device as well as the SConfigurator application
- An S3100 installation guide (varies depending on the model)

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 device and antenna does not exceed the maximum value established by your country's regulations. For more information, see page 26.

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

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

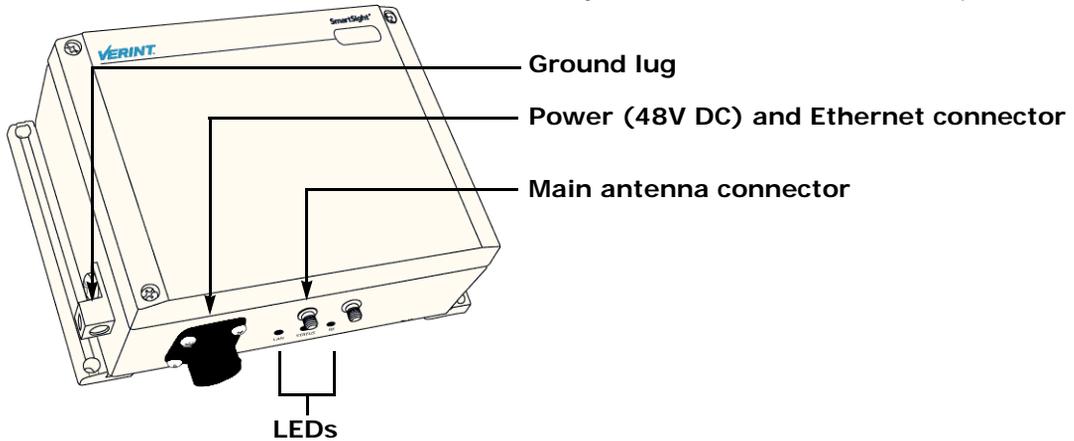
Casing Description

The S3100 electronics are enclosed in a weather-tight cast aluminum module. All cable entries are mounted on the underside of the device to maintain its weatherproof properties. The connectors vary depending on the model.

S3100

The device underside integrates:

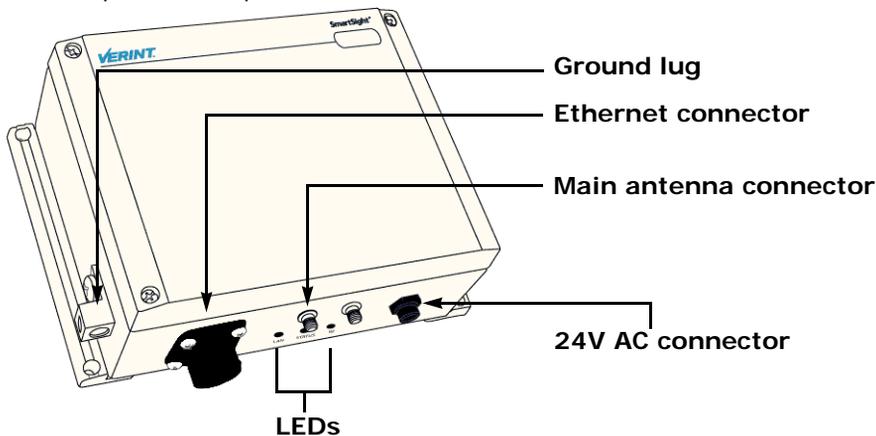
- A power and Ethernet connector
- Three LEDs
- A ground lug
- Two female antenna connectors (the auxiliary connector is for future development)



S3100-BR and S3100-RP

The device underside integrates:

- An Ethernet connector
- Three LEDs
- A ground lug
- Two female antenna connectors (the auxiliary connector is for future development)
- A 2-pin 24V AC power connector



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* devices 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
- 4.9 GHz OFDM, a public safety band available in North America only
- 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 independent (that is, 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		

4.9 GHz Band

The 4.9 GHz band is a licensed band for entities providing public safety services focused on the protection of life, health, or property in North America. This band provides license holders with an interference-free, secure channel for robust and secure broadband technologies, including wireless video surveillance systems.

For more detailed information concerning the regulations governing licensing and use of frequencies in the 4.9 GHz band, see Subpart Y of the FCC document, Memorandum Opinion and Order and Third Report and Order at:

http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-99A1.pdf

The 4.9 GHz band has a width of 50 MHz (4940 to 4990 MHz). Since the standard channel width is 20 MHz, only two independent channels can co-exist in the band. However, the S3100 supports channel fragmentation, allowing narrower channels of 5 MHz and 10 MHz. You can have up to four independent channels with a 10 MHz width, and up to 10 with a 5 MHz width. All these channels are for indoor or outdoor use. For more information about channel fragmentation, see page 45.

The available channels are:

Channel	Frequency (GHz)	Channel width
3	4.9425	5 MHz
6	4.9475	5 MHz
7	4.9525	5 MHz or 10 MHz
7	4.950	20 MHz
8	4.9575	5 MHz
9	4.9625	5 MHz or 10 MHz
10	4.9675	5 MHz
11	4.9725	5 MHz or 10 MHz
11	4.970	20 MHz
12	4.9775	5 MHz
13	4.9825	5 MHz or 10 MHz
16	4.9875	5 MHz

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 the Verint Video Intelligence Solutions extranet (Technical Support, then Downloads, then Utilities and Tools).

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

Channel	Frequency (GHz)
149	5.745
153	5.765
157	5.785
161	5.805
165	5.825

In Europe, the 11 independent 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		

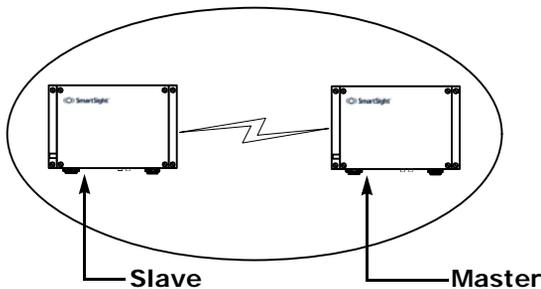
Wireless Cells

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 46).

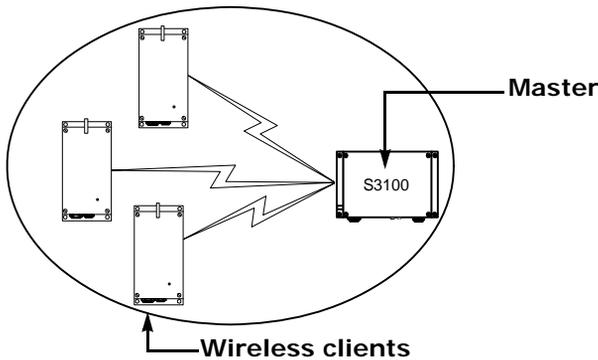
Roles

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

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



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



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

Compatibility Issues

When planning your wireless systems, you need to take into account the firmware versions of the involved devices. It is recommended that the S3100 devices have the same firmware versions as their associated slaves and clients; however, from version 2.60 and up, the devices are fully compatible (for example, an S3100 at version 3.20 with an S1100w at version 3.60).

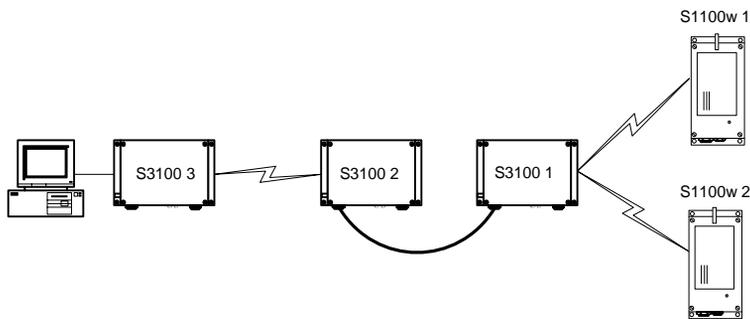
In a wireless cell involving S1100w transmitters, the order in which you configure the devices (either the first time or later when they are installed in the field) or update their firmware is critical if you do not want to lose access to them. You should then:

1. Update or configure the devices 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 device.
2. Change the IP address of the computer running SConfigurator (see page 37).
3. Update the firmware of the two S3100 devices.

For example, consider the following wireless cell:



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

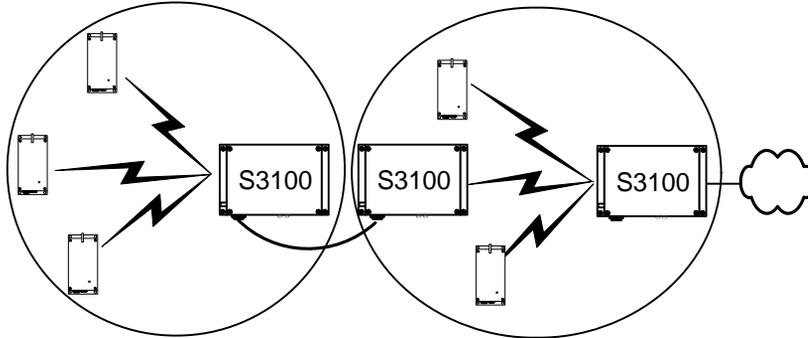
1. S1100w 1—You then lose contact with S1100w 1.
2. S1100w 2—You then lose contact with S1100w 2.
3. S3100 1—You can then reach all devices.
4. S3100 2—You then lose contact will all devices except master S3100 3.
5. S3100 3—You can then reach all devices.

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

Video Bit Rate and Data Throughput

You can connect up to 16 client and 7 slave devices to a master S3100 in a wireless cell. However, video quality, frame rate, and system layout can limit the number of devices that a single master device can support.

Each time multiple client or slave devices are connected to a master S3100, the available bandwidth is divided equally between the connections. In the following example, two S1100w clients and one slave S3100 connected to a master on a 6 Mbps link each have 2 Mbps throughput.



Note: In that context, you must ensure that all devices connected to a slave S3100 do not require more than the available bandwidth. Otherwise video packets may be lost.

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.

The following figures were measured in typical setup situations. They may vary depending on your configuration. The total data throughput in a unidirectional UDP link setup varies depending on two factors:

- The MAC protocol. For more information about SPCF and SDCF, see page 13.
- The frequency channel width: 20 MHz in all available bands, or 5 MHz and 10 MHz in the 4.9 GHz frequency band.

SPCF

The throughput for a 20 MHz channel for the SPCF protocol is:

Physical bit rate	Throughput for a 3 mile (5 km) distance	Throughput for a 9.3 mile (15 km) distance	Throughput for a 15.5 mile (25 km) distance
6 Mbps	3.5 Mbps	3.4 Mbps	3.3 Mbps
9 Mbps	4.7 Mbps	4.5 Mbps	4.4 Mbps
12 Mbps	5.6 Mbps	5.4 Mbps	5.2 Mbps
18 Mbps	7.0 Mbps	6.6 Mbps	6.3 Mbps
24 Mbps	8.1 Mbps	7.5 Mbps	7.1 Mbps
36 Mbps	9.1 Mbps	8.6 Mbps	8.1 Mbps
48 Mbps	10.0 Mbps	9.3 Mbps	8.7 Mbps
54 Mbps	10.1 Mbps	9.5 Mbps	9.0 Mbps

The throughput for a 10 MHz channel for the SPCF protocol is:

Physical bit rate	Throughput for a 3 mile (5 km) distance	Throughput for a 9.3 mile (15 km) distance	Throughput for a 15.5 mile (25 km) distance
3 Mbps	2.0 Mbps	1.9 Mbps	1.9 Mbps
4.5 Mbps	2.8 Mbps	2.7 Mbps	2.7 Mbps
6 Mbps	3.5 Mbps	3.4 Mbps	3.3 Mbps
9 Mbps	4.5 Mbps	4.4 Mbps	4.3 Mbps
12 Mbps	5.4 Mbps	5.1 Mbps	5.0 Mbps
18 Mbps	6.7 Mbps	6.3 Mbps	6.0 Mbps
24 Mbps	7.4 Mbps	7.1 Mbps	6.8 Mbps
27 Mbps	7.7 Mbps	7.4 Mbps	7.0 Mbps

The throughput for a 5 MHz channel for the SPCF protocol is:

Physical bit rate	Throughput for a 3 mile (5 km) distance	Throughput for a 9.3 mile (15 km) distance	Throughput for a 15.5 mile (25 km) distance
1.5 Mbps	1.1 Mbps	1.1 Mbps	1.1 Mbps
2.25 Mbps	1.5 Mbps	1.5 Mbps	1.5 Mbps
3 Mbps	1.9 Mbps	1.9 Mbps	1.8 Mbps
4.5 Mbps	2.6 Mbps	2.6 Mbps	2.5 Mbps
6 Mbps	3.2 Mbps	3.2 Mbps	3.1 Mbps
9 Mbps	4.2 Mbps	4.1 Mbps	3.9 Mbps
12 Mbps	4.9 Mbps	4.7 Mbps	4.6 Mbps
13.5 Mbps	5.1 Mbps	5.0 Mbps	4.8 Mbps

SDCF

The throughput for a 20 MHz channel for the SDCF protocol is:

Physical bit rate	Throughput for a 3 mile (5 km) distance	Throughput for a 9.3 mile (15 km) distance	Throughput for a 15.5 mile (25 km) distance
6 Mbps	4.5 Mbps	4.2 Mbps	4.0 Mbps
9 Mbps	6.3 Mbps	6.1 Mbps	5.3 Mbps
12 Mbps	7.8 Mbps	7.6 Mbps	6.7 Mbps
18 Mbps	10.5 Mbps	10.1 Mbps	8.4 Mbps
24 Mbps	12.7 Mbps	12.2 Mbps	9.8 Mbps
36 Mbps	15.9 Mbps	15.0 Mbps	11.7 Mbps
48 Mbps	17.9 Mbps	16.5 Mbps	12.7 Mbps
54 Mbps	18.9 Mbps	17.7 Mbps	13.2 Mbps

The throughput for a 10 MHz channel for the SDCF protocol is:

Physical bit rate	Throughput for a 3 mile (5 km) distance	Throughput for a 9.3 mile (15 km) distance	Throughput for a 15.5 mile (25 km) distance
3 Mbps	2.3 Mbps	2.3 Mbps	2.2 Mbps
4.5 Mbps	3.4 Mbps	3.2 Mbps	3.1 Mbps

Physical bit rate	Throughput for a 3 mile (5 km) distance	Throughput for a 9.3 mile (15 km) distance	Throughput for a 15.5 mile (25 km) distance
6 Mbps	4.3 Mbps	4.1 Mbps	3.9 Mbps
9 Mbps	6.0 Mbps	5.6 Mbps	5.2 Mbps
12 Mbps	7.5 Mbps	6.9 Mbps	6.3 Mbps
18 Mbps	9.9 Mbps	8.9 Mbps	7.8 Mbps
24 Mbps	11.8 Mbps	10.3 Mbps	8.9 Mbps
27 Mbps	12.6 Mbps	10.9 Mbps	9.5 Mbps

The throughput for a 5 MHz channel for the SDCF protocol is:

Physical bit rate	Throughput for a 3 mile (5 km) distance	Throughput for a 9.3 mile (15 km) distance	Throughput for a 15.5 mile (25 km) distance
1.5 Mbps	1.2 Mbps	1.2 Mbps	1.1 Mbps
2.25 Mbps	1.7 Mbps	1.7 Mbps	1.7 Mbps
3 Mbps	2.3 Mbps	2.2 Mbps	2.1 Mbps
4.5 Mbps	3.2 Mbps	3.0 Mbps	2.9 Mbps
6 Mbps	4.1 Mbps	3.8 Mbps	3.7 Mbps
9 Mbps	5.5 Mbps	5.1 Mbps	4.8 Mbps
12 Mbps	6.7 Mbps	6.1 Mbps	5.6 Mbps
13.5 Mbps	7.1 Mbps	6.5 Mbps	5.9 Mbps

The S3100 automatically adjusts the transmission speed with the current RF conditions.

For the bit rate requirements of the edge devices to which the cameras are connected, consult the *Bit Rate Settings for Video Servers* document located on the Verint Video Intelligence Solutions extranet (Technical Support, then Downloads, then Utilities and Tools).

System Planning

The grouping of devices in each wireless cell is determined by their respective locations with respect to one another and by the available S3100 devices. As a rule of thumb, each client or slave device must have a clear RF line of sight with its master device within each cell. However, the client and slave devices can be completely hidden from one another. For more information about the RF line of sight, see page 25.

MAC Protocols

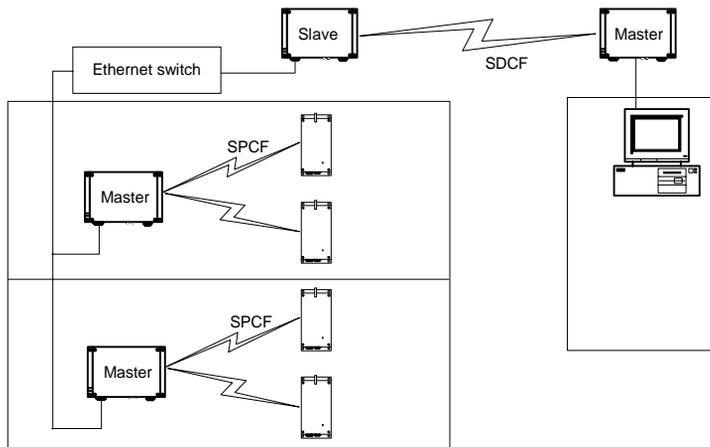
Depending on the type of applications, an S3100 device uses one of the two proprietary MAC protocols that solve problems inherent to 802.11 wireless networking products:

- The SPCF (SmartSight Point Coordination Function) protocol resolves the “hidden node,” quality of service, range, and security problems. SPCF is used in access point 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—and in wireless bridge applications. 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 Nextiva devices; they cannot work with wireless devices from other vendors.

Here is a typical context of use showing the two protocols. A access point 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 device 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 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 63).

DFS

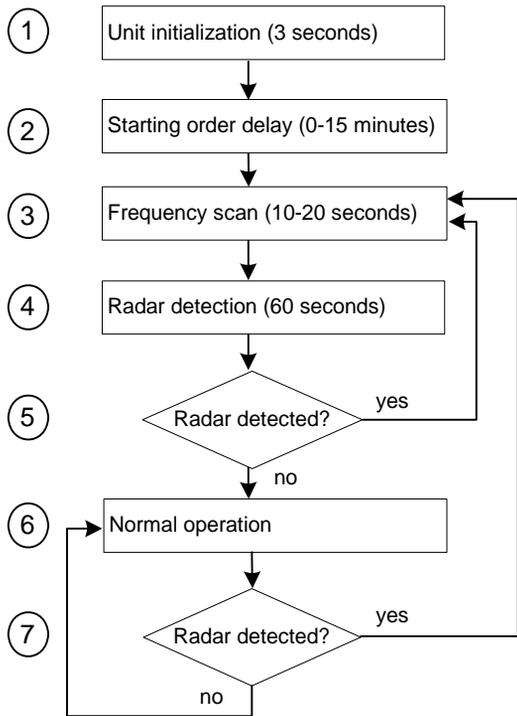
To follow the DFS (Dynamic Frequency Selection) regulations specified by ETSI for the selected country, it is the master device that performs the tasks relative to frequency channel selection and radar detection. In other words, you cannot choose the frequency channel on which the edge device will run.

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.

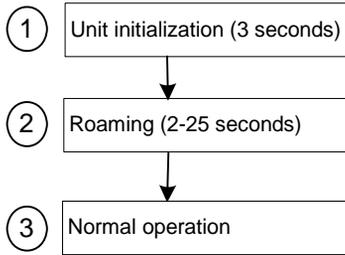
You should start the master first, then power the client or slave when the other device is in normal operation.

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



1. The device 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 64.
3. The device 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 device listens for 60 seconds on the selected channel to detect possible radar interference.
5. If a radar is detected on the channel, the device returns to the scan process. Otherwise, it continues its bootup procedure.
6. The device runs normally.
7. If a radar is detected, the device immediately goes back to the scan process to select another channel.

The boot sequence of client or slave devices is:



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

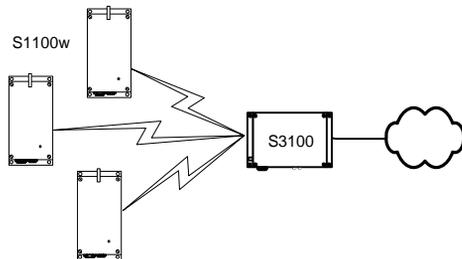
Application Types

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

- Access point—One S3100 device linking multiple S1100w transmitters to a LAN (the S3100 model)
- Point-to-point repeater—Two S3100 devices acting as a range extender for one or many pairs of S1100 transmitters (the S3100-RP model)
- Point-to-multipoint repeater—Two S3100 devices acting as a range extender for multiple S1100w transmitters (the S3100-RP model)
- Wireless bridge—Two S3100 devices linking two networks, wired or wireless (the S3100-BR model)
- Wireless bridge repeater—Two S3100 devices acting as a range extender for a wireless bridge (the S3100-RP model)

Access Point

An access point application is a wireless cell made up of an S3100 device (the S3100 product code, called the *master*) and several S1100w transmitters (the *clients*). The MAC protocol for the master device is SPCF. Here is a typical access point system:



To install a single wireless cell made up of three S1100w transmitters and one S3100, you need to:

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

The associated S1100w transmitters will automatically use their master's channel.

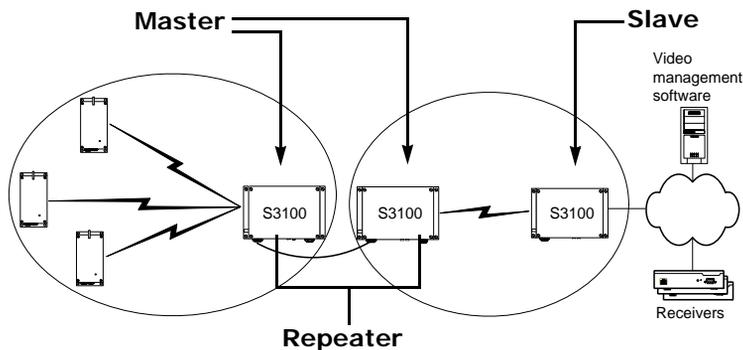
3. Install the S1100w transmitters such that each one has a clear RF line of sight with the S3100 device.

For the complete configuration and installation procedures, see page 31.

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 transmitters 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 devices separated into two colocated cells. For example:



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

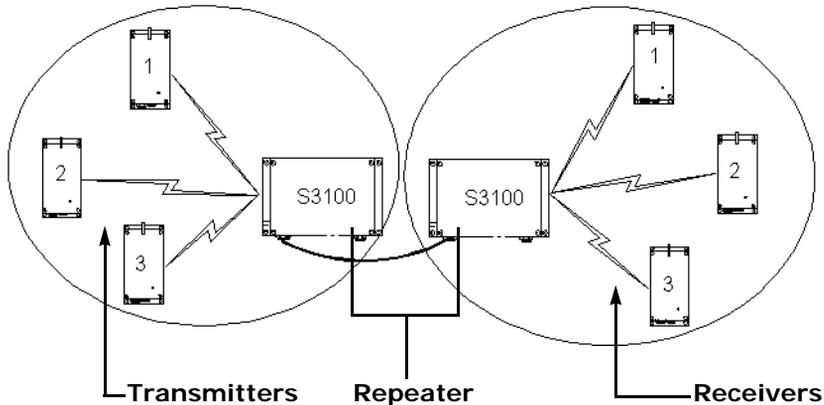
1. In each cell, assign the same wireless passkey to all the devices. The wireless passkey must be different from that of the other cell.
2. Always connect the S1100w transmitters to a master S3100, never to a slave.
3. Set the MAC mode of the S3100 in Cell1 to SPCF.
4. Set the MAC mode of the two S3100 devices in Cell2 to SDCF.
5. In a non-DFS context, assign a frequency channel to the master S3100 device 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 devices 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.

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 devices, separated into two colocated cells. For example, with three pairs of S1100 devices:



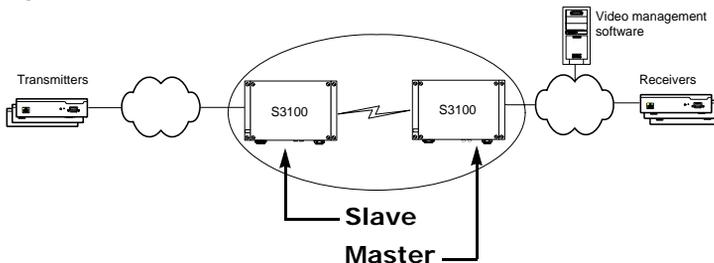
To operate the two cells forming the repeater, you need to:

1. In each cell, assign the same wireless passkey to all the devices. The wireless passkey must be different from that of the other cell.
2. Set the MAC mode of the two S3100 devices to SPCF.
3. In a non-DFS context, assign a frequency channel to the master S3100 device 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 devices such that each one has a clear RF line of sight with its associated master.

For the complete configuration and installation procedures, see page 30.

Wireless Bridge

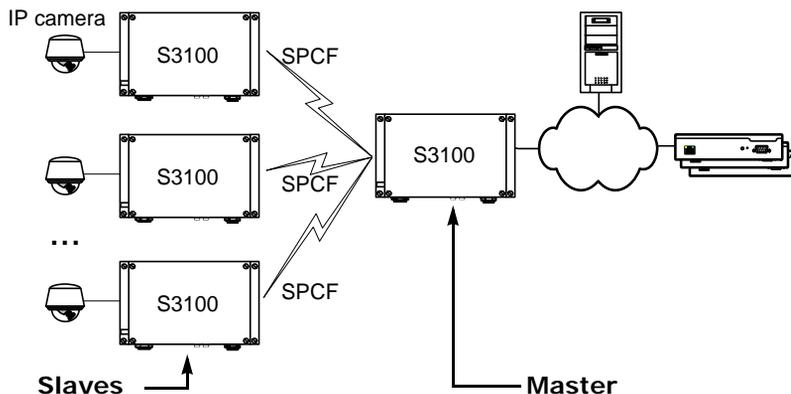
You use two S3100 devices (the S3100-BR product code)—a master and a slave—to transfer video surveillance data between two LANs when a wired connection is not available or too costly to install. For instance, a wireless bridge application can connect remote S1900e-AS edge devices (the following illustration) or wireless devices without an RF line of sight.



To create a wireless bridge application, you need to:

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

You can also use the S3100-BR product in point-to-multipoint wireless bridges, to transmit video coming from IP cameras:



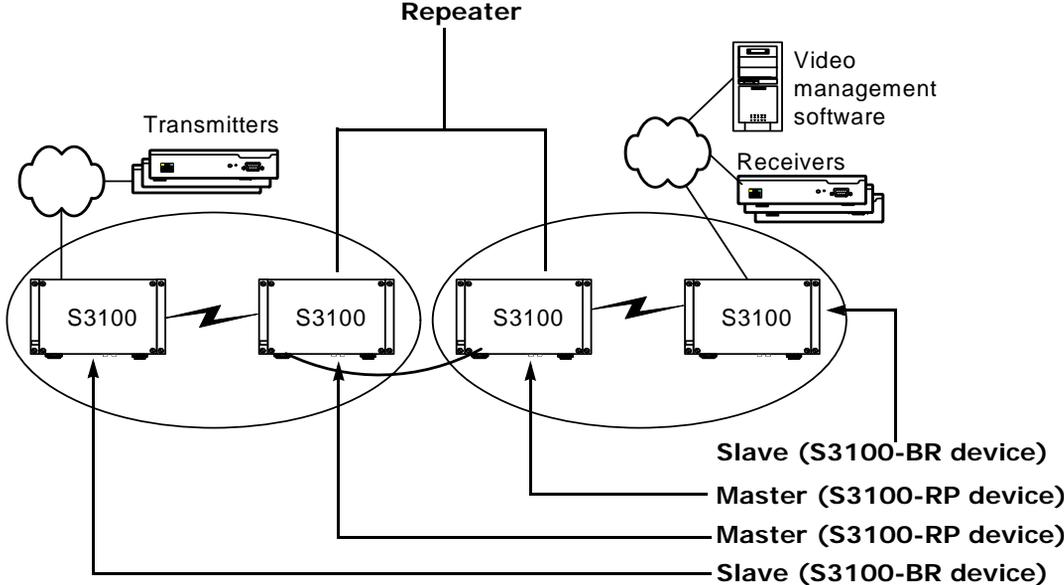
All slaves (you can install up to seven of them) must be S3100-BR devices. The configuration of such an application is very similar to that of a standard wireless bridge, except that the MAC role of the devices is SPCF instead of SDCF.

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

Wireless Bridge Repeater

A wireless bridge repeater is used as a range extender to retransmit the signals exchanged by the two devices forming a wireless bridge. A typical context is when you cannot obtain an RF line of sight between the two devices forming the wireless bridge.

A wireless bridge repeater (the *S3100-RP* product code) is made up of two master devices, separated into two colocated cells. For example:



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

1. In each cell, assign the same wireless passkey to the two devices. The wireless passkey must be different from that of the other cell.
2. Set the MAC mode of all four S3100 series devices to SDCF.
3. In a non-DFS context, assign a frequency channel to the master S3100 device 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 S3100 series devices such that each one has a clear RF line of sight with its corresponding counterpart.

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

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 devices are:

- The minimum distance between two devices is 3 feet (1 meter), regardless of the band or channel used.
- To avoid material damages, you must never power any two devices while their antennas are facing one another with a distance of less than 10 feet (3 meters).
- In an SDCF cell, if the maximum distance between two devices is longer than 6 miles (10 km), you must adjust the maximum link distance parameter; for more information, see page 64.
- If using adjacent channels, see page 83 for the recommendations on the minimum distances to respect.
- To reduce radio interference possibilities between two adjacent frequency channels, ensure that the maximum margin between the emission of the two wireless cells is 25 dB; for more information, see Appendix G on page 83.

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 4.9 GHz and 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.

4.9 GHz Band in North America

Depending on the channel width (20, 10, or 5 MHz), you can colocate 2, 4, or 10 wireless cells respectively. For the available channels in each of the three scenarios, see page 7.

The following example presents three wireless cells with 10-MHz channels. To install such a system, you have to:

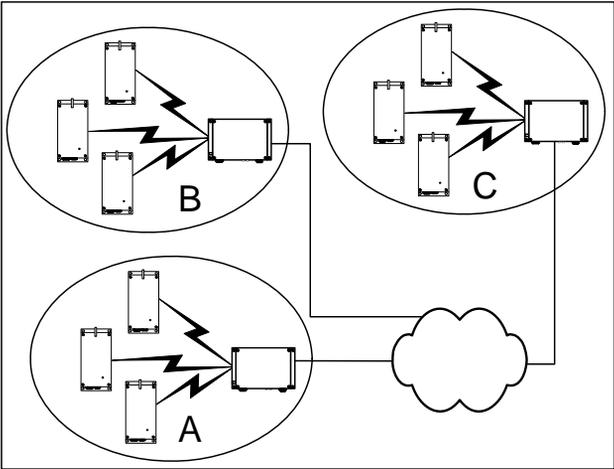
1. In each cell, assign the same wireless passkey to the S1100w transmitters and the S3100 access point. The wireless passkey must be different from that of the other cells.

- 2. Assign a different frequency channel to each S3100 device; the associated S1100w devices will automatically use their master's channel:

Device	Cell	Channel	Wireless Passkey
S3100_A	A	7	ertymbvcxzapoIU
S1100w_A1	A	7	ertymbvcxzapoIU
S1100w_A2	A	7	ertymbvcxzapoIU
S1100w_A3	A	7	ertymbvcxzapoIU
S3100_B	B	13	PUK98rewq4123qzx
S1100w_B1	B	13	PUK98rewq4123qzx
S1100w_B2	B	13	PUK98rewq4123qzx
S1100w_B3	B	13	PUK98rewq4123qzx
S3100_C	C	11	987123jkl456wert
S1100w_C1	C	11	987123jkl456wert
S1100w_C2	C	11	987123jkl456wert
S1100w_C3	C	11	987123jkl456wert

- 3. In each cell, install the S1100w devices such that each one has a clear RF line of sight with its associated S3100 access point.

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



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 independent channels (channels 1, 6, and 11) to colocate wireless cells. In the 5 GHz band, all channels are independent.

A typical colocation example is three access point applications, each one made up of three S1100w transmitters and one S3100. To install such a system, you need to:

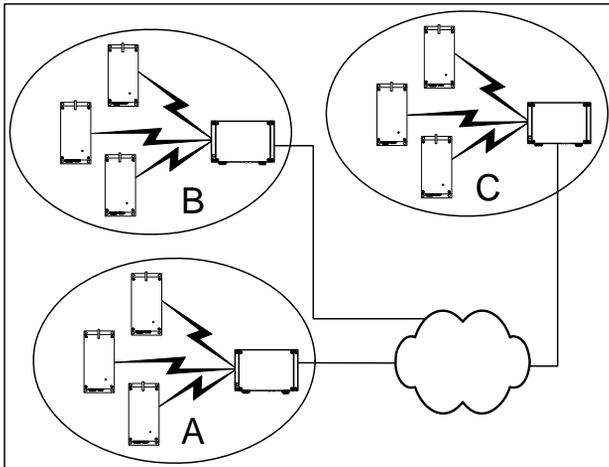
- 1. In each cell, assign the same wireless passkey to the S1100w transmitters and the S3100 device. The wireless passkey must be different from that of the other cells.

- Assign a different frequency channel to each S3100 master device; the associated S1100w transmitters will automatically use their master’s channel. For example:

Device	Cell	Channel	Wireless Passkey
S3100_A	A	149	ertymbvcxzapoIU
S1100w_A1	A	149	ertymbvcxzapoIU
S1100w_A2	A	149	ertymbvcxzapoIU
S1100w_A3	A	149	ertymbvcxzapoIU
S3100_B	B	165	PUK98rewq4123qzx
S1100w_B1	B	165	PUK98rewq4123qzx
S1100w_B2	B	165	PUK98rewq4123qzx
S1100w_B3	B	165	PUK98rewq4123qzx
S3100_C	C	157	987123jkl456wert
S1100w_C1	C	157	987123jkl456wert
S1100w_C2	C	157	987123jkl456wert
S1100w_C3	C	157	987123jkl456wert

- In each cell, install the S1100w transmitters such that each one has a clear RF line of sight with its associated S3100 device.

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 Intelligence 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 devices 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:

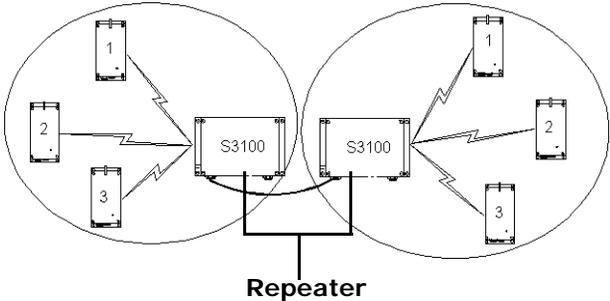
- 1. Assign a different wireless passkey to each cell.
- 2. Ensure that all S3100 masters “see” one another. For the procedure, see Appendix F on page 79.
- 3. Position the devices so that there is at least 3 feet (1 meter) between each antenna.
- 4. In each master device, set a different starting order: 1 for the first device, 2 for the device 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 Intelligence Solutions project engineering group for assistance.

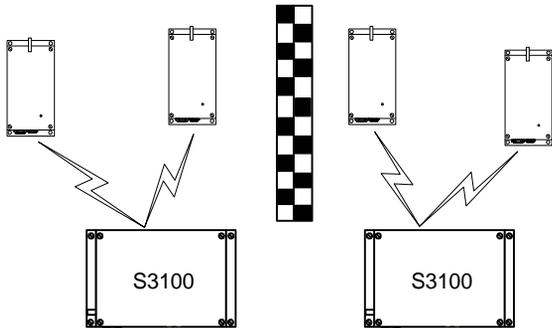
Supported Setups

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

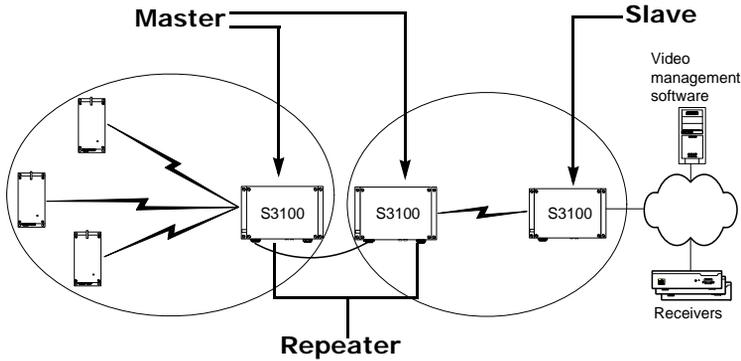
- A point-to-point repeater for one or more pairs of S1100 devices, with or without hidden nodes. Both master devices see each other.



- Two access point applications, in which the transmitters from one system do not see the transmitters from the other cell. Both master devices see each other.



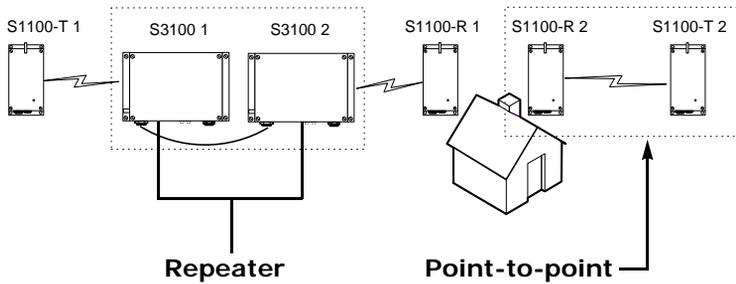
- A point-to-multipoint repeater. Both master devices see each other.



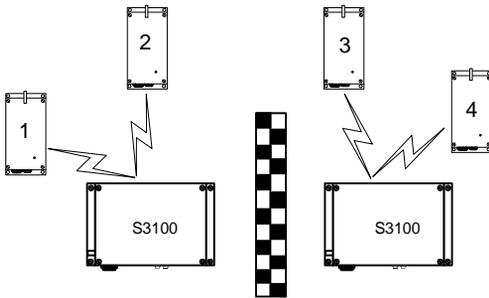
Unsupported Setups

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

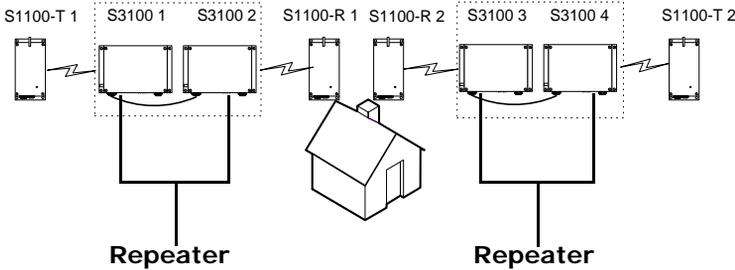
- A point-to-point repeater with a point-to-point link. In this setup, two masters do not see each other, S3100 2 and S1100-R 2, while the two receivers do.



- Access point 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

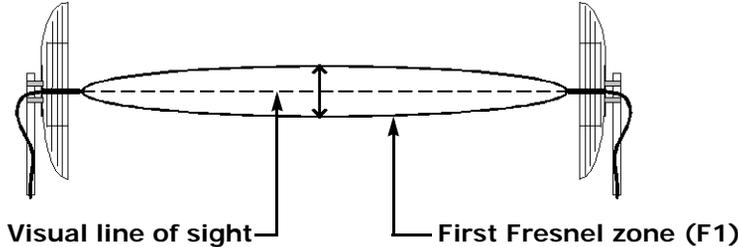
Successful operation of a wireless link depends on proper RF path planning and antenna installation. You have to install the devices in such a way that there is a clear RF line of sight between the two antennas.

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 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 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)	4.9 GHz (feet/m)	5.3 GHz (feet/m)	5.8 GHz (feet/m)	Earth curvature effect (feet/m)
1 / 1.6	14 / 4.2	9.8 / 3.0	9.5 / 2.9	8.9 / 2.7	0
4 / 6.5	27 / 8.4	19.5 / 5.9	18.7 / 5.7	18 / 5.5	2 / 0.6
7 / 11.3	37 / 11	25.8 / 7.9	25 / 7.6	23.6 / 7.2	6 / 1.8
15 / 24	53 / 16	37.8 / 11.5	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 Intelligence Solutions Support 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, 4.9, 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 offers many antennas to meet various distance requirements. You need 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. For systems located in North America on the 5 GHz band, you can use the *Wireless System Margin Calculator* located on the Verint Video Intelligence Solutions extranet (Technical Support, then Downloads, then Utilities and Tools).

The combined transmission power of the device 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 device will automatically take it into account and adjust its own transmission power accordingly at startup.

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. You can only use antennas certified by Verint.

The maximum antenna gain supported to meet local regulations are:

Location	Band	Antenna gain	Comment
Europe	2.4 GHz	8.5 dBi	
	5 GHz	13 dBi	
North America	2.4 GHz	16 dBi	
	4.9 GHz	13 dBi	To be used only with the S3100-49, S3100-BR-49, and S3100-RP-49
	5 GHz	19 dBi	

The antennas certified by Verint are:

- ANT-WP8-24/S: 8.5 dBi gain, 2.4 GHz band, 65° beamwidth, patch antenna with 3-foot (1-meter) SMA-SMA cable
- ANT-WP13-5x/S: 13 dBi gain, 5.25-5.85 GHz band, 40° beamwidth, patch antenna SMA/F connector
- ANT-WP13-49-5x/S: 13 dBi gain, 4.9-5.85 GHz band, 40° beamwidth, patch antenna SMA/F connector
- ANT-WP16-24/S: 16dBi gain, 2.4 GHz band, 27° beamwidth, patch antenna with 3-foot (1-meter) SMA-N cable
- ANT-WP19-5x/S: 19 dBi gain, 5.25-5.85 GHz band, 18° beamwidth, patch antenna with 3-foot (1-meter) SMA-N cable

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—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—Replacement of the integrated antenna by a higher gain one can significantly lower the interference from other radio systems. Replace the antenna if switching channels does not correct the problem or if all channels must be used to collocate several systems.

There should not be any interference in the 4.9 GHz band, since it is a licensed band with limited usage to public safety.

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 devices must be installed in such a way as to allow a minimum separation distance of 12 inches (30 cm) between antennas and persons nearby.

2

Configuring and Installing the Device

You can set up the S3100 devices for access point, repeater, or wireless bridge applications.

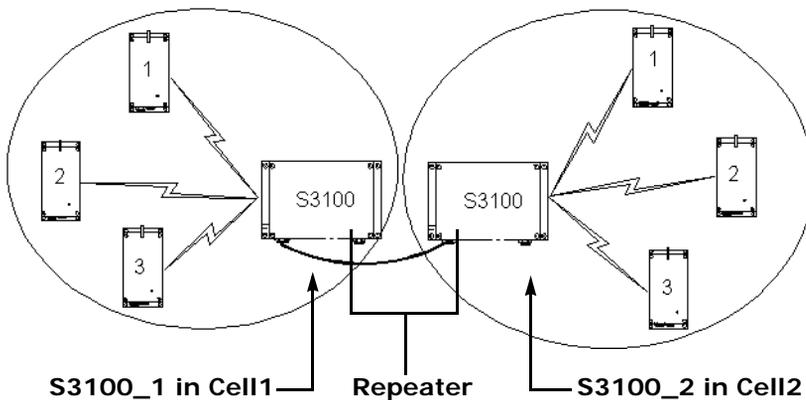
Computer Requirements

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

- An Ethernet network card
- Windows 2000 Service Pack 2 or higher, or Windows XP Service Pack 2

Point-to-Point Repeater

A point-to-point repeater is 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. You use the S3100-RP (made up of two S3100 devices) to create this repeater.



The steps required to prepare your devices for this type of application are:

1. Configuring the S1100 pairs in repeater mode. For the procedure, refer to the *Nextiva S1100 User Guide*.
Warning: You must complete the configuration of the S1100 devices before powering up an S3100 device.
2. Assembling the 24V DC power devices (see page 37).
3. Configuring the two S3100 devices, one at a time (see page 37). You need to shut down the first device before configuring the second one.

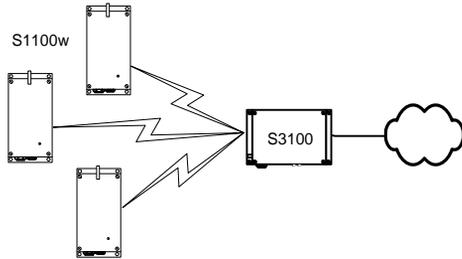
The wireless parameters to apply are:

Parameter	S3100_1	S3100_2
MAC mode	SPCF	SPCF
Role	Master	Master
Band	<i>Band1</i> ; if necessary in the 4.9 GHz band, change the channel bandwidth	<i>Band1</i> ; if necessary in the 4.9 GHz band, change the channel bandwidth
Channel	In a non-DFS context: <i>ChannelA</i>	In a non-DFS context: <i>ChannelB</i>
Bit rate	N/A	N/A
Starting order	In a DFS context: 1	In a DFS context: 2
Wireless passkey	<i>Passkey1</i> common to all devices in Cell1	<i>Passkey2</i> common to all devices in Cell2

4. Installing the S3100 devices (see page 47).

Access Point

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



The steps required to prepare your devices for this type of application are:

1. Configuring the S1100w transmitters. For the procedure, refer to the *Nextiva S1100w Installation Guide*.
2. Connecting power and Ethernet (see page 36).
3. Configuring the S3100 device (see page 37).

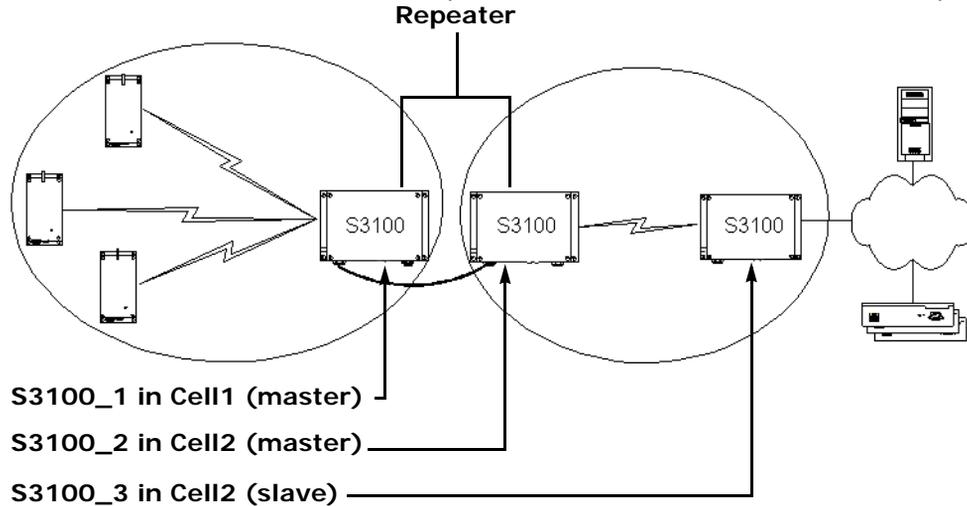
The wireless parameters to apply are:

Parameter	S3100
MAC mode	SPCF
Role	Master
Band	Manual selection (the same as in the S1100w transmitters); if necessary in the 4.9 GHz band, change the channel bandwidth
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 devices in the cell

4. Installing the S3100 device (see page 47).

Point-to-Multipoint Repeater

A point-to-multipoint repeater is a range extender for wireless links, when you need a device to retransmit the signals coming from S1100w transmitters towards the Ethernet LAN. You use the S3100-RP (made up of two S3100 devices) to create this repeater.



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

The steps required to prepare your devices for this type of application are:

1. Assembling the power devices (see page 36 for the slave and page 37 for the two repeater devices).
2. Configuring the two S3100 devices part of the repeater, one at a time (see page 37). You need to shut down the first device before 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 transmitters; if necessary in the 4.9 GHz band, change the channel bandwidth	<i>Band2</i> ; if necessary in the 4.9 GHz band, change the channel bandwidth
Channel	In a non-DFS context: <i>ChannelA</i>	In a non-DFS context: <i>ChannelB</i>
Bit rate	N/A	N/A
Starting order	In a DFS context: 1	In a DFS context: 2
Wireless passkey	<i>Passkey1</i> common to all devices in Cell1	<i>Passkey2</i>

- 3. Configuring the slave S3100 device connected to the LAN (see page 37).

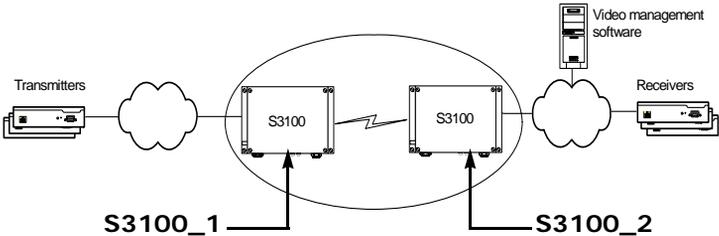
The wireless parameters to apply are:

Parameter	S3100_3
MAC mode	SDCF
Role	Slave
Band	<i>Band2</i> ; if necessary in the 4.9 GHz band, change the channel bandwidth
Channel	N/A
Bit rate	Manual selection
Starting order	N/A
Wireless passkey	<i>Passkey2</i>

- 4. Installing the repeater devices (see page 47).
- 5. Installing the slave S3100 (see page 47).

Wireless Bridge

You use a wireless bridge to access remote or hard to reach wired edge devices, or to send surveillance video data through a long distance link. You use the S3100-BR (made up of two devices, one master and one slave) to create this bridge. Any of the two devices can act as the master.



The steps required to prepare your devices for this type of application are:

- 1. Assembling the 24V DC power devices (see page 36).

2: Configuring and Installing the Device

2. Configuring the two S3100 devices one at a time; always start with the master (see page 37). You need to shut down the first device before configuring the second one.

The wireless parameters to apply are:

Parameter	S3100_1	S3100_2
MAC mode	SDCF	SDCF
Role	Slave	Master
Band	<i>Band1</i> ; if necessary in the 4.9 GHz band, change the channel bandwidth	<i>Band1</i> ; if necessary in the 4.9 GHz band, change the channel bandwidth
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	<i>Passkey1</i>	<i>Passkey1</i>

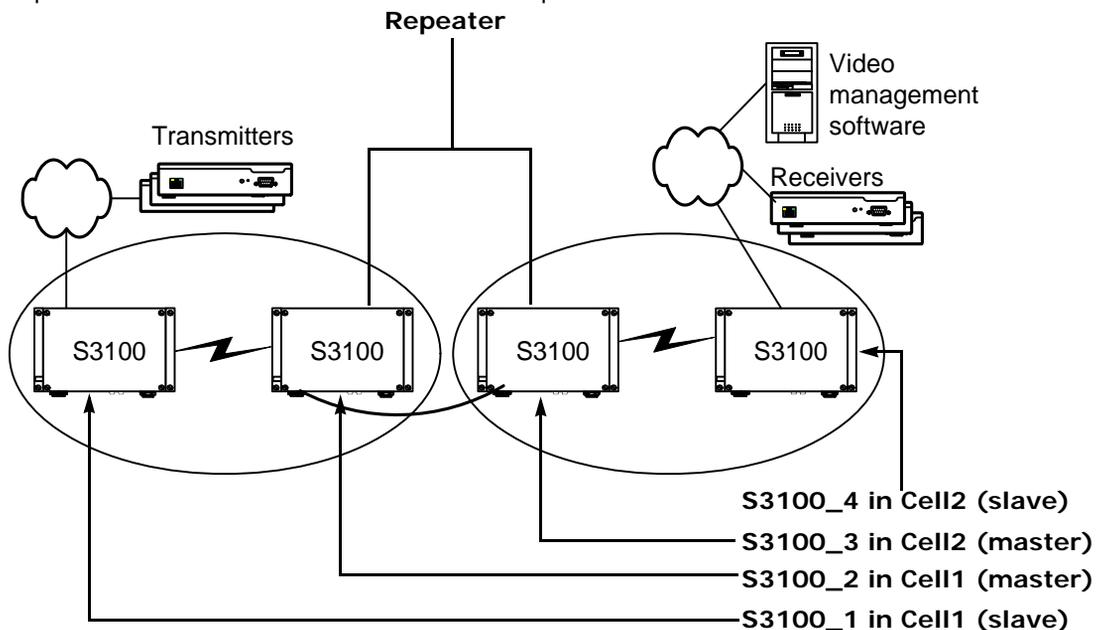
For a point-to-multipoint wireless bridge (for the description, see page 18), the only difference is that the MAC mode is SPDF for all devices.

3. Installing the S3100 devices (see page 47).

Wireless Bridge Repeater

A wireless bridge repeater is used as a range extender to retransmit the signals exchanged by the two devices forming a wireless bridge. A typical context is when you cannot obtain an RF line of sight between the two devices forming the wireless bridge.

A wireless bridge repeater (the *S3100-RP* product code) is made up of two master devices, separated into two colocated cells. For example:



The steps required to prepare your devices for this type of application are:

1. Assembling the 24V DC power devices (see page 36).
2. Configuring the four S3100-RP and S3100-BR devices one at a time; always start with the masters (see page 37). At any time there must be only one S3100 device powered.

The wireless parameters to apply to the devices in Cell1 are:

Parameter	S3100_1	S3100_2
MAC mode	SDCF	SDCF
Role	Slave	Master
Band	<i>Band1</i> ; if necessary in the 4.9 GHz band, change the channel bandwidth	<i>Band1</i> ; if necessary in the 4.9 GHz band, change the channel bandwidth
Channel	N/A	In a non-DFS context: <i>ChannelA</i>
Bit rate	Manual selection	N/A
Starting order	N/A	In a DFS context: 1
Wireless passkey	<i>Passkey1</i>	<i>Passkey1</i>

The wireless parameters to apply to the devices in Cell2 are:

Parameter	S3100_3	S3100_4
MAC mode	SDCF	SDCF
Role	Master	Slave
Band	<i>Band2</i> ; if necessary in the 4.9 GHz band, change the channel bandwidth	<i>Band2</i> ; if necessary in the 4.9 GHz band, change the channel bandwidth
Channel	In a non-DFS context: <i>ChannelB</i>	N/A
Bit rate	N/A	Manual selection
Starting order	In a DFS context: 2	N/A
Wireless passkey	<i>Passkey2</i>	<i>Passkey2</i>

3. Installing the S3100 devices (see page 47).

Power Connections

Depending on the S3100 device used, the power connection is different:

- The S3100 model uses power over Ethernet (PoE).
- The S3100-BR and S3100-RP models come with two 24V AC power supplies.

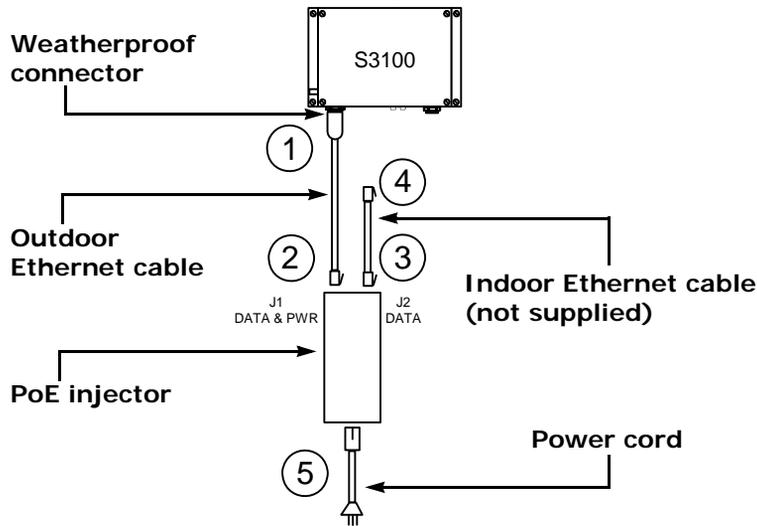
You need to assemble these devices prior to installing them on the devices. It is strongly recommended to execute these tasks in a lab.

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

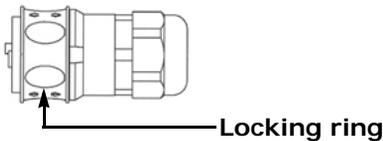
Power over Ethernet

With the S3100 model, you use the supplied PoE kit to power the device and establish its 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 device. The PoE kit sold by Verint contains two items: an injector and a power cord. The connection procedure may vary if you use another PoE kit.

To connect the PoE kit sold by Verint:



1. Plug the supplied outdoor Ethernet cable (the end with the weatherproof connector) into the PoE receptacle of the S3100. 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 the indoor Ethernet cable—straight-through or crossover, depending on your installation—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 the indoor 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 by plugging the power cord between the injector and the outlet.

24V DC Power

Prior to configuring the two S3100 devices making up the repeater or wireless bridge, you need to assemble their power cord and power supply.

To assemble the power device:

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

Configuration

To configure an S3100 device, you need SConfigurator, a proprietary tool included on the *Utilities* CD. You can also find its latest version on the Verint Video Intelligence Solutions extranet (Technical Support, then Downloads, then Firmware Upgrades). You copy its executable file to the hard disk of your computer.

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

Warning: For the S3100-BR and S3100-RP products, you need to shut down the first device before configuring the second one.

1. In a point-to-point repeater context, changing the IP address of the computer running SConfigurator (see page 37).
2. Preparing the device (see page 41).

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

3. Setting the IP parameters of the device (see page 41).
4. Setting the country of operation and the device name (see page 43).
5. Setting the wireless parameters (see page 44).
6. Checking the communication between the devices (see page 47).
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 Guide*.

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 *Nextiva S3100 Installation Guide*.

Changing the IP Address of the Computer

To change the parameters of the S3100 devices 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).

2: Configuring and Installing the Device

The recommended temporary IP settings are:

- IP address: 192.168.135.2
- Subnet mask: 255.255.0.0
- 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**.

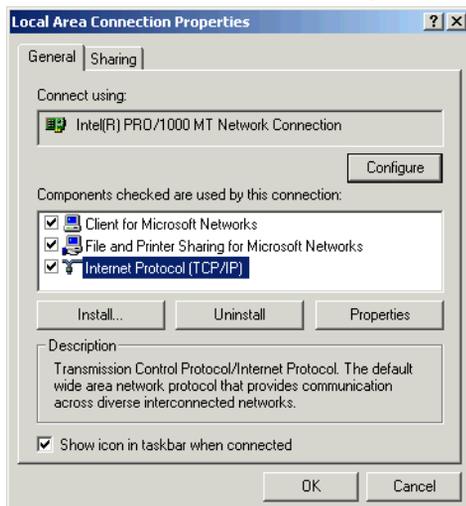
The Network and Dial-up Connections window appears.

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

The Local Area Connection Status window appears.

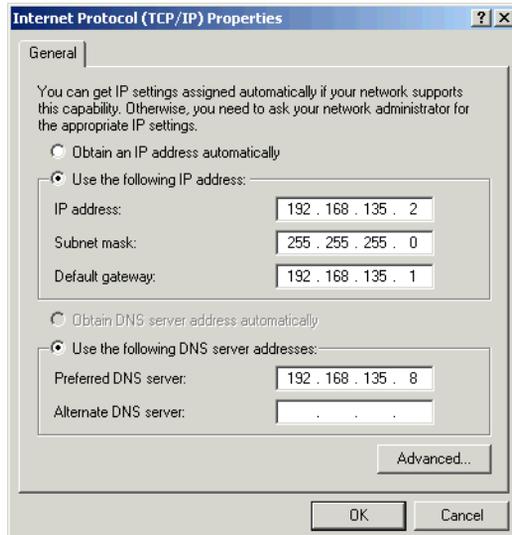
3. Click **Properties**.

The Local Area Connection Properties window appears.



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

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



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.

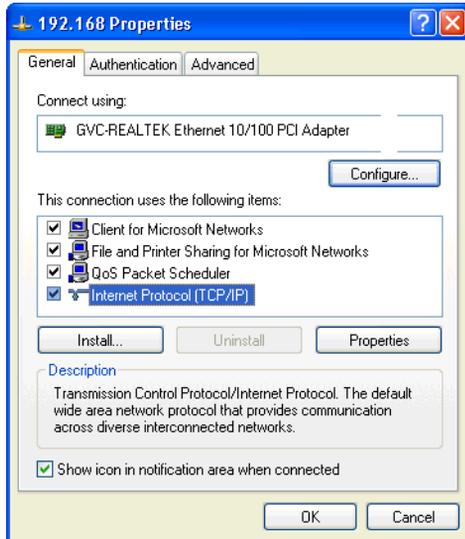
To change the IP address under Windows XP:

1. In the Windows Start menu, select **Control Panel**.
2. If the classic view is enabled, select **Network Selection**. In the category view, select **Network and Internet Connections**, then **Network Connections**.
3. Double-click your active LAN or Internet connection.

2: Configuring and Installing the Device

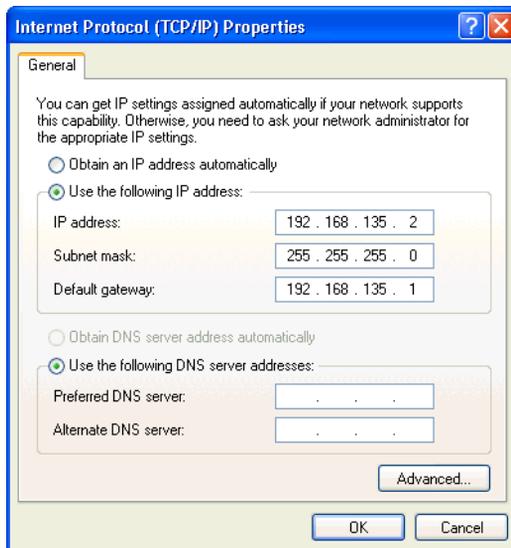
4. Click **Properties**.

A Properties window appears.



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

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



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.

Device Preparation

To configure the device, you need a crossover or straight-through Ethernet cable. The crossover cable is to directly connect the device to a computer; the straight-through cable is to integrate the device on a network.

Note: The maximum length of outdoor Ethernet cables is 164 feet (50 meters). The maximum length of indoor cables (crossover or straight-through) is 82 feet (25 meters).

To prepare a device for configuration:

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

IP Parameters

The first step in installing an S3100 device is to change its IP address to ensure compatibility with an existing network. The default IP addresses of all devices are based on the APIPA addressing scheme and will be in the range 169.254.X.Y, where X and Y are relative to the MAC address of the individual device; for more information about APIPA, see page 75.

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

To set the initial IP parameters:

1. Start SConfigurator.
The SConfigurator window appears.

2: Configuring and Installing the Device

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

The Program Options window appears.

The Program Options dialog box contains the following fields and controls:

- IP Address of the PC: 172.16.11.1
- Detect All Units on LAN:
- VSIP Port: 9515 (with Default and Common buttons)
- Discovery IP Address: 255 . 255 . 255 . 255 (with Reset to Broadcast and Reset to Multicast buttons)
- SSL section:
 - Trusted Unit List: (empty text box with Browse button)
 - Enable Security:
 - Enter SSL Passkey: (text box)
- OK and Cancel buttons at the bottom.

3. Check **Detect All Units on LAN**.
4. Ensure that the **VSIP Port** 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. In the New settings have been applied window, click **OK**.
8. Select the **Units** tab, then click **Discover**.

A device of type "Unknown" with a 169.254.X.Y IP address appears in the list; it corresponds to your new device.

The Units tab shows a table of discovered units:

Unit Name	Type	Address	Product
192.168.135.114 - Unit	Receiver	192.168.135.114	51500e
192.168.135.215 - Unit	Receiver	192.168.135.215	51500e
Unknown	Unknown	169.254.31.68	Unknown

Buttons on the right: Discover, Configure, Add, Telnet, Reboot.

3 unit(s) discovered

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

The New Network Configuration window appears.

10. Enter the IP information for the device.

- 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: 255.255.0.0
 - Gateway: 192.168.135.1
- For an S3100 in another context:
 - To use DHCP (Dynamic Host Configuration Protocol), check **Use DHCP**. For more information about DHCP, see page 75.
 - Otherwise, enter the IP address, subnet mask, and gateway of the device, as provided by your network administrator.

11. Click **OK**.

The device reboots with its new network configuration.

12. In the Units tab, click **Discover**.

The new S3100 device appears.

13. Select the device, then click **Configure**.

The Unit Configuration window appears.

Country Selection and Device Name

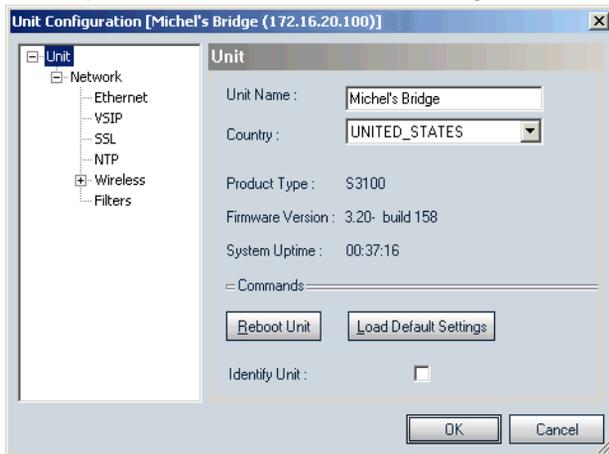
You must assign the proper country of operation to the device, so that it will:

- 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 device, to help maintenance and debugging.

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

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



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

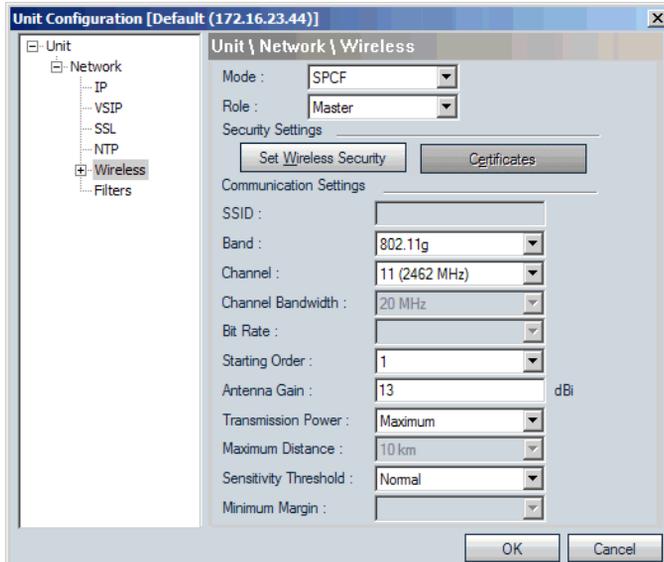
The device reboots.

Wireless Parameters

Depending on the type of application involved, you need to assign a different set of parameters. Use the values supplied in the description of the applications (from page 30 to page 35).

To set the wireless parameters:

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



2. In the Role field, select the function of the device (**Master** or **Slave**).
3. Set the parameters as required. For the wireless passkey procedure, see next.
4. Click **OK**.

The device reboots.

2: Configuring and Installing the Device

To set the wireless passkey:

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

The Set Wireless Security window appears.

The screenshot shows the 'Set Wireless Security' dialog box. It is divided into two main sections: 'Authentication' and 'Encryption'.
In the 'Authentication' section:
- 'WPA Authentication Method' is set to 'WPA-PSK'.
- 'WPA Negotiation Timeout' is set to '45 second(s)'.
- 'WPA Reauthentication Period' is set to '1 day(s)'.
- 'WPA EAP Login Name' is 'stef'.
- 'WPA EAP Password' and 'Confirmation Password' fields are empty.
In the 'Encryption' section:
- 'Encryption Type' is set to 'AES-OCB'.
- 'Format' has two radio buttons: 'Text (ASCII)' (selected) and 'Hexadecimal'. A 'Reset' button is next to it.
- 'Passkey' and 'Confirmation' fields are empty.
- A note below the fields states: 'The key must contain exactly 32 hexadecimal digits (0-9 and A-F)'.
- There is a checkbox labeled 'Apply changes to connected clients / slaves' which is currently unchecked.
At the bottom of the dialog are 'OK' and 'Cancel' buttons.

2. In the Encryption group box, select the format of the passkey: **Text (ASCII)** or **Hexadecimal**.
3. In the Passkey box, enter the new 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 not 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 box, enter again the passkey.
5. To set the wireless passkey to its default value, click **Reset**.
6. On a master S3100, to apply the new password to all associated devices:
 - a. Ensure that **Apply changes to connected clients/slaves** is checked.
 - b. Click **OK**.

*Note: The wireless passkey of the S3100 series device will be changed only when you click **OK** in the Unit Configuration window.*

The Changing Wireless Passkey window appears.

- c. When the procedure is finished, click **Close**.
7. Click **OK**.

Communication Checking

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

To check communication:

1. If required, power up all the devices making up the system.
2. In the Units tab in SConfigurator, ensure that the associated devices are hierarchically positioned under the master.
3. In the Network > Wireless > Link Status pane of the Unit Configuration window of the master, ensure that the associated devices are in the Clients/Slaves list.
4. Ensure that there is end-to-end video transmission in the lab before installing the devices in their final locations.

Installation

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

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

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

Installation of the S3100-RP Devices

The S3100-RP model is made up of two devices connected together with an outdoor Ethernet cable.

To install the devices:

1. Install the two devices back to back in their final location:
 - On a wall—Put four screws on the two side brackets and fix the device at the desired location.
 - On a pole—Screw the pole mount brackets (supplied with your shipment) in the back of the device; then attach the brackets on the pole with the stainless steel clamps.
2. To enable the built-in surge protection, connect each device to the ground using the ground lug on its left side.

Use a large diameter wire (minimum AWG 10), and make it as short as possible.
3. If the devices 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 50).

2: Configuring and Installing the Device

5. Apply silicone grease on the female contact of each power cord and on the 24V AC connector on the device. For the detailed procedure, refer to the leaflet shipped with the power cords.

Warning: Failure to apply the grease will void the warranty.

6. Power the devices using the assembled power devices.
7. Connect the supplied crossover Ethernet cable between the two devices.

Installation of the S3100-BR Devices

A wireless bridge is made up of two devices, each connected to a network or an IP camera with a straight-through cable.

To install the devices:

1. Install each device in its final location:
 - On a wall—Put four screws on the two side brackets and fix the device at the desired location.
 - On a pole—Screw the pole mount brackets (supplied with your shipment) in the back of the device; then attach the brackets on the pole with the stainless steel clamps.
2. To enable the built-in surge protection, connect each device to the ground using the ground lug on its left side.

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

3. If the devices 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 50).
5. Apply silicone grease on the female contact of each power cord and on the 24V AC connector on the device. For the detailed procedure, refer to the leaflet shipped with the power cords.

Warning: Failure to apply the grease will void the warranty.

6. Power the devices using the assembled power devices.
7. Connect each device to the network or an Ethernet equipment (for example, switch or IP camera) using a supplied straight-through Ethernet cable.
8. If you need to connect directly one of the devices to an IP camera that does not have automatic MDI/MDI-X capability, change the supplied straight-through cable the following way:
 - a. Install the supplied cables on the S3100 and on the camera.
 - b. Remove their standard Ethernet connectors.
 - c. Properly connect the two cables together to form a cross-connect Ethernet cable.

Alternatively, you can also convert the straight-through cable to a crossover cable by either:

- Connecting an Ethernet crossover adapter to the Verint-supplied Ethernet straight-through cable, then plugging the adaptor into the IP camera.
- Converting the RJ-45 end of the Verint-supplied cable from a standard straight-through cable to a crossover one by modifying the wire locations and installing a new RJ-45 connector.

Note: Ensure that you follow the IP camera installation recommendation concerning the use of outdoor rated connectors.

Installation of the S3100 Access Point Device

The S3100 model, used for access point applications, is a single device.

To install the S3100:

1. Apply silicone grease inside the weatherproof connector of the outdoor Ethernet cable, including on the o-ring, and on the LAN 10/100 POE connector on the device. For the detailed procedure, refer to the leaflet shipped with the cable.

Warning: Failure to apply the grease will void the warranty.

2. Connect the PoE kit (see page 36).
3. Install the S3100 in its final location:
 - On a wall—Put four screws on the two side brackets and fix the device at the desired location.
 - On a pole—Screw the pole mount brackets (supplied with your shipment) in the back of the device; then attach the brackets on the pole with the stainless steel clamps.
4. If you are installing the device 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 77.

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

Use a large diameter wire (minimum AWG 10), and make it as short as possible.
6. If the device will be directly exposed to the sun in an environment likely to reach 122°F (50°C), install a sun shield.
7. Install the antenna (see page 50).
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 device by connecting the electric plug of the PoE injector into the outlet.

Installation of the Antenna

You install the antenna after the S3100 device is in place. The antennas provided by Verint 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 device. If you bought your antenna from Verint, use the supplied pole mount bracket.

For illustrations of pole mount installations, see page 73.

2. Screw the SMA connector of the antenna cable to the 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 devices (S1100w clients or S3100) so that they have a clear RF line of sight.
5. To improve the signal level between two devices, use the antenna alignment utility from SConfigurator.

Firmware Update

You can update the firmware of the S3100 devices with the SConfigurator utility or a video management software; for the detailed procedure, refer to the documentation of the software. The latest firmware files are available on the Verint Video Intelligence Solutions extranet (Technical Support, then Downloads, then Firmware Upgrades).

Warning: Firmware downgrade is not supported on any device. If you perform a downgrade, any problem encountered will not be covered by your product warranty.

The only method to update the firmware is through an IP network connection. If this update procedure fails:

1. Restart the same procedure immediately.
2. If the problem persists, move the device so that it is in the same IP subnet as the host computer, reboot it, then restart the procedure.

You should take into consideration the following facts regarding firmware update using the IP network:

- It can be deactivated in the command line interface (CLI).

- Ensure that the IP link is stable before starting the procedure; therefore it is not recommended to perform it over the Internet.

Quality of Service

Quality of Service (QoS) is a set of low-level networking protocols giving higher priority to more important data flows while ensuring that the less important ones do not fail. QoS is an essential technology for organizations rolling out a new generation of network applications such as real-time voice communications and high-quality video delivery.

In the Nextiva edge devices, the two available QoS flavors are Type of Service (ToS) and Differentiated Service Code Points (DSCP).

For QoS to be taken into account, the network infrastructure equipment (switches and routers) must support one of these protocols. If any of these devices does not support QoS, the QoS data will simply be processed as traditional non-QoS data. Furthermore, all Nextiva edge devices on a network must support the same QoS protocol (or no protocols at all).

You can set a priority flag to three data types coming out of an edge device: video, audio, and control. A QoS-enabled switch (or router) uses this flag to determine how the current data compares to what is currently going through it.

To set the QoS values, you need to go in the command line interface (CLI) of the device, access the Advanced > Quality of Service menu. For the procedure to access the CLI, see page 55.

LEDs

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

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

Condition	Indication
Steady green	The device is connected to the Ethernet network.
Flashing green (1-sec. flash every 3 sec.)	The device 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 device is being identified.
Flashing red (1 sec. intervals)	On a master device: There is another master currently running on the same frequency channel; for more information, see page 52.

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

Condition	Indication
Flashing green (1-sec. flash every 3 sec.)	The device is in normal operation without any connected client/slave.
Steady green	The device 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 device is being identified.
Flashing red (1 sec. intervals) happening simultaneously on all LEDs	On a master device: There is another master currently running on the same frequency channel; for more information, see page 52.

- System status—For the general device status:

Condition	Indication
Steady red (1 sec.)	The device is powering up.
Steady green (3 to 5 sec.)	The device is loading its firmware.
Flashing green (1 sec. intervals)	The device is in normal operation.
Flashing red (1 sec. intervals)	The IP address of the device is already assigned to another device on the network. or On a master device: There is another master currently running on the same frequency channel; for more information, see page 52. This condition happens simultaneously on all LEDs.
Flashing green-red (1 sec. intervals)	The device is undergoing a firmware update or is in backup mode.
Flashing red (0.1 sec. intervals)	The device 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 Intelligence Solutions technical support for assistance.
- Steady red LED—There is an internal error that prevents the device from starting normally. Power down the device, wait 30 seconds, then power it up. If the condition persists, call Verint Video Intelligence Solutions technical support.
- Flashing green-red LED not during a firmware update—The device 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 devices—with at least one in 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 device 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 device, 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 device.

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 device, you cannot access it with Telnet; if you lost its VSIP port, you cannot locate it with SConfigurator.

To find a “lost” S3100 device, 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 devices 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 its installation guide.

4

Setting Parameters with the CLI

The S3100 devices 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

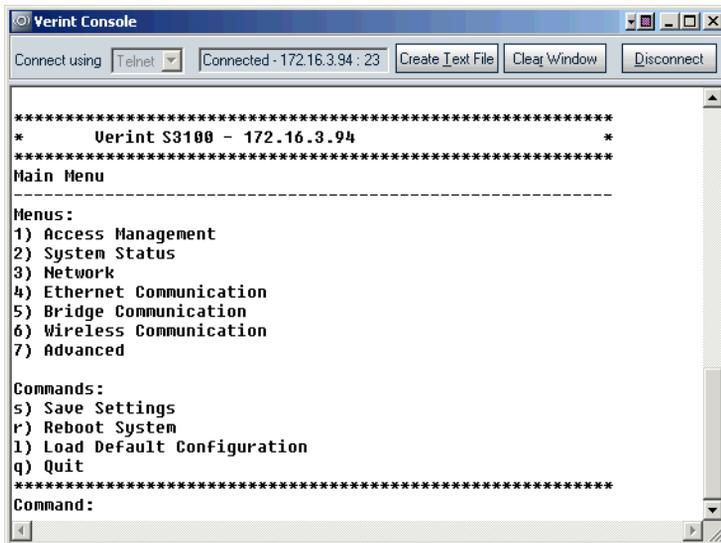
You can use the Telnet utility, through SConfigurator, to open the command line interface of the device.

To enter the CLI with Telnet:

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

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

The CLI main menu appears in the Verint Console window.



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 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 device may perform a soft boot.
 - c. Close the Verint Console window.

Warning: Do not use the Disconnect button to exit the CLI, since it does not save your settings.

Access Management

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

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

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

4: Setting Parameters with the CLI

It allows you to control:

- Firmware updates through the IP network
- Access to Telnet
- Global security profile
- SSL

IP Firmware Update

You can prevent firmware updates to be performed on your device 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 Guide*.

Telnet Session

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

Global Security Profile

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

SSL Passkey

To secure a device with SSL, provided of course it has an SSL certificate, you need to provide a passkey. This passkey must be the same for all devices 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 device).

System Status

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

```
*****
Main Menu \ System Status
-----
Menus:
1) Storage

Parameters:
  Firmware Version   : 4.00a build 247
  Build Date        : Feb 6 2007 at 16:59:19
  CPU Info          : Rev. 1.0
  CPU Frequency     : 165000000
  Uptime            : 00:50:05
  Serial Number     : 00079a-10000c
  CPLD Version      : 1
  Internal Value 1  : 1320000 / 8
  Audio Hardware    : Absent
  Production Date   :
  Unit Firmware Size : 2559 KB
  Backup Firmware Size: 742 KB
  ISO Country Code  : UNITED_STATES (840)

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

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        : 172.16.23.200
3) Subnet Mask             : 255.255.0.0
4) Gateway                 : 172.16.23.200
5) Primary DNS Server Address : 0.0.0.0
6) Backup DNS Server Address  : 0.0.0.0
7) Ping Request Target     : 0.0.0.0
8) Ping Request Send Buffer Size: 32

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 75.

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. Its 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 installation guide of your product.

Subnet Mask

The subnet mask is the binary configuration specifying in which subnet the IP address of the device 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 255.255.0.0.

Gateway

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

Warning: Never use the IP address of the device 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 device:

1. In the **Ping Request Send Buffer Size** parameter, enter the buffer size (in bytes).
2. In the **Ping Request Target** parameter, enter the IP address of the device.
3. 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         : Client
5) RF Band          : public safety (4.9GHz OFDM)
6) Channel          : Auto
7) Channel Bandwidth: 20MHz channel
8) Tx Bit Rate      : 54 Mb/s
9) Antenna Gain     : 13 dBi
10) ISO Country Code : UNITED_STATES (840)

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 devices and S1100w transmitters). The passkey length varies depending on the key entry format (presented on page 63):

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

For the wireless connection to be secure, do not 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 device 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)
- public safety (4.9 GHz OFDM)

Channel

If your devices 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 S3100 device in a non-DFS environment, you can either specify an RF channel manually or use the automatic channel selection. On a slave device, you can specify an initial value for the *roaming* process by which the device will find its master; however, this initial channel may not be the one used by the master device.

The channels available in North America are:

- 1 to 11 in the 2.4 GHz band
- 3, 6, 7, 8, 9, 10, 11, 12, 13, and 16 in the 4.9 GHz band (list varies depending on the channel bandwidth)
- 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 the Verint Video Intelligence Solutions extranet (Technical Support, then Downloads, then Utilities and Tools).

Channel Bandwidth

In the 4.9 GHz band, the bandwidth can be fragmented to allow 5- and 10-MHz channels; the default channel width is 20 MHz. This parameter only appears if the RF band is 4.9 GHz. The list of available channels varies depending on the chosen bandwidth; for more information, see page 7.

Tx Bit Rate

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

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

When a slave device 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 64).

Once the device is operating properly, Verint 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 than the manually configured one; when the quality improves later on (it is evaluated periodically), the bit rate will be automatically updated.

The available bit rates for the slave S3100 device are:

Band	Channel width	Bit rates (Mbps)
2.4 GHz	N/A	6, 9, 12, 18, 24, 36, 48, and 54
4.9 GHz	5 MHz	1.5, 2.25, 3, 4.5, 6, 9, 12, and 13.5
	10 MHz	3, 4.5, 6, 9, 12, 18, 24, and 27
	20 MHz	6, 9, 12, 18, 24, 36, 48, and 54
5 GHz	N/A	6, 9, 12, 18, 24, 36, 48, and 54

Antenna Gain

If you enter the gain of the antenna you install on the device, the S3100 will be able to automatically change its transmission power so that the total power (edge device 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 26.

ISO Country Code

You must assign the proper country of operation to the device, 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) Physical Error Rate Threshold : 5000
8) IP Multicast Forward from this Interface: Allowed
9) Wireless-to-Wireless IP Multicast : Denied
10) Indoor/Outdoor RF Regulation : Indoor Only FCCA FCC1
*****
```

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 device 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.

Sensitivity Threshold

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

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 device would not “hear” its legitimate correspondent.

Starting Order

The starting order is a sequence number, used during the boot-up process of a master S3100 in a DFS context, to delay its startup. The purpose of this parameter is to ensure that colocated master devices 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 device 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 device 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 S3100 devices.

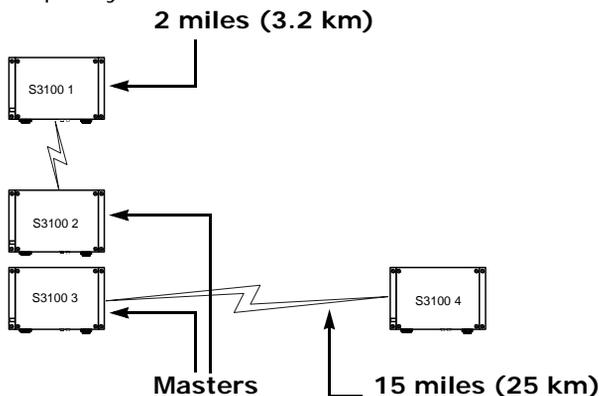
Maximum Link Distance

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

The two S3100 devices 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 devices 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 S3100 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 device 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 the Verint Video Intelligence Solutions extranet (Technical Support, then Downloads, then Utilities and Tools).

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 Intelligence Solutions customer service. Some of these parameters are available through SConfigurator or a video management software.

```
*****
Main Menu \ Advanced
-----
Menus:
1) System Time
2) System Time Stats
3) USIP
4) USIP Statistics
5) License Management
6) Communication Status and Statistics
7) Quality of Service
8) Test and Debug

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

Identifying a Device

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

To identify an S3100 device:

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.

Conducting Site Surveys

The S3100 device allows you to perform site surveys on your RF network. A site survey scans all frequency channels, evaluate the interference level in each channel, and allows you to choose the channel with the less interference.

```
*****
Advanced \ Communication Status and Statistics \ Wireless Status
-----
Parameters:
NIC Name           : AT5006X DCMA-82 A,B,G 2.4,4.9,5.x GHz
NIC MAC Address   : 00-0B-6B-2F-F8-E5
Current Channel    : 7 (4950 MHz) 20 MHz channel bandwidth
Current TX Rate    : 6 Mb/s
Current RX Rate    : 6 Mb/s
Average Signal Level : -65 dBm
Current SCF Connection Status: Connected to 1 Client and 1 Slave

RF Communication Quality : N/A
RF Margin                : N/A
Current EIRP              : 34 dBm
Maximum EIRP allowed     : 42 dBm
Indoor/Outdoor RF Regulation : Indoor/Outdoor FCCA FCC1
1) Site survey iteration  : 1
```

```
Commands:
1) Display link(s) Info
s) Start/Stop Site Survey
v) Visualize Last Site Survey Report
r) Reset Site Survey data base
p) Previous Menu
*****
```

You can perform the following operations relative to RF site surveys:

- Specify the number of consecutive surveys to perform
- Start and stop a site survey
- Look at the last survey report
- Reset the survey database

To conduct site surveys:

1. From the main menu, choose **Advanced > Communication Status and Statistics > Wireless Status**, then press **Enter**.
2. Perform the required operations.

Note: During the site survey execution, the RF link will be momentarily broken (duration varies depending on the number of iterations). The link is automatically restored when the survey is finished.

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 69). All user-defined values will be lost.

Following a reset, you will need to reprogram the S3100 device (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

A: Factory Default Configuration

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

Type	Configuration
Access management	<ul style="list-style-type: none">■ User name: USERNAME■ Password: PASSWORD■ User accounts: Disabled■ Telnet sessions: Enabled■ IP firmware update: Enabled■ Global security profile: Disabled■ SSL passkey: <empty>
Network	<ul style="list-style-type: none">■ DHCP configuration: Disabled■ IP address: 169.254.*.* (MAC address of the device)■ Subnet mask: 255.255.0.0■ Gateway: 0.0.0.0
Wireless Communication (North America)	<ul style="list-style-type: none">■ 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)	<ul style="list-style-type: none">■ 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	<ul style="list-style-type: none">■ VSIP Port: 5510■ VSIP multicast IP address: 224.16.32.1■ VSIP discovery IP address: 255.255.255.255

B

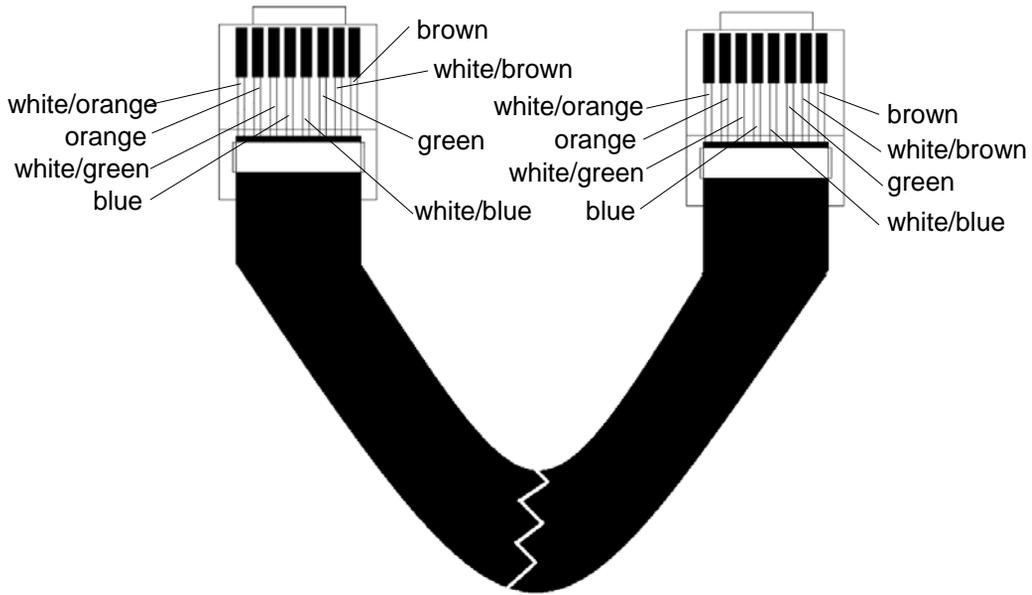
RJ-45 Ethernet Cables

B: RJ-45 Ethernet Cables

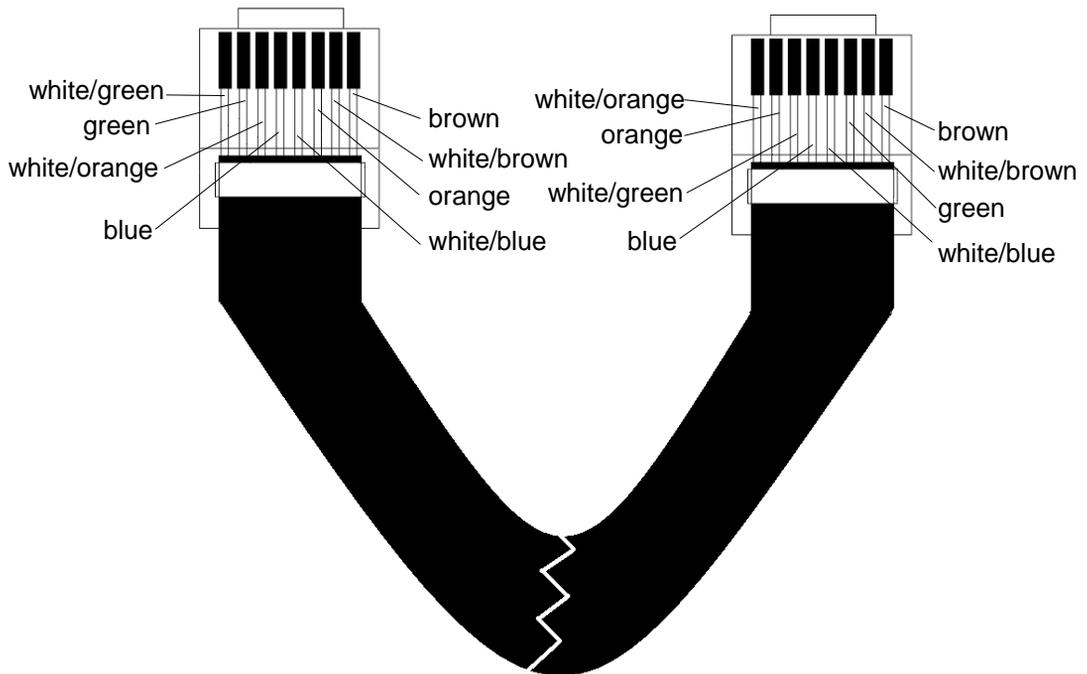
Depending on whether the device is integrated on a network or not, the Ethernet cable varies:

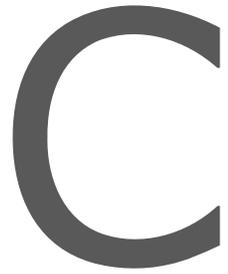
- If on a network, use a straight-through cable.
- To link it directly to a computer, use a crossover cable.

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:



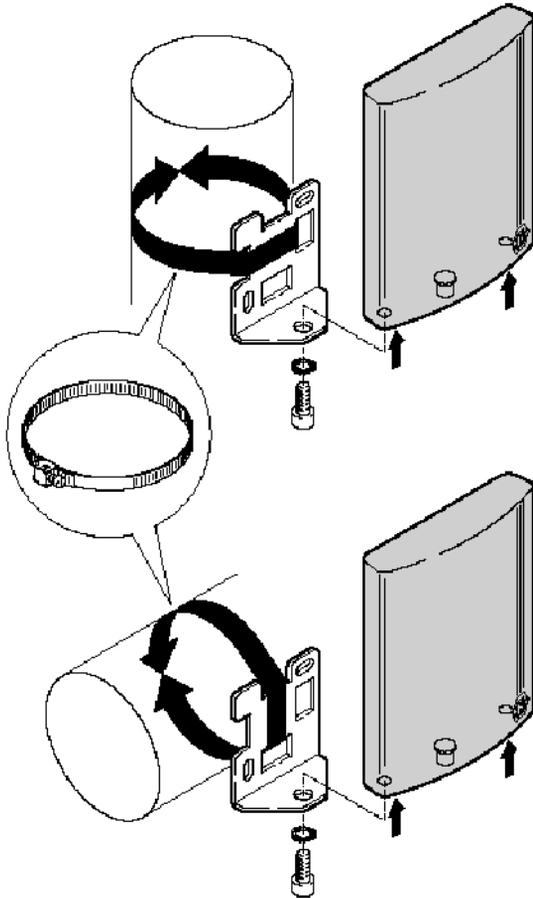


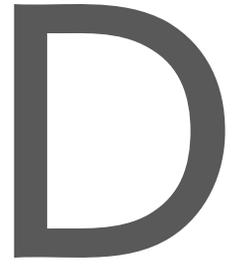
Pole Mounting of the Antennas

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:





DHCP Support and APIPA

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) scheme, available on the Windows operating systems, enables a device to assign itself a temporary IP address.

At startup, an edge device searches for a valid IP network configuration. The device requires this configuration prior to starting its functions. The network configuration for Nextiva devices consists of:

- An IP address
- A subnet mask
- A gateway

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

A device 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. Devices use the following temporary APIPA configuration:

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

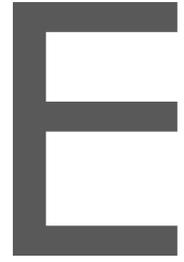
The *. * portion is based on the MAC address of the device.

A device is in APIPA mode:

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

DHCP configuration is automatically disabled:

- After a firmware upgrade
- After a factory reset



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 devices.

E: Surge Protection

VerintThe 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).

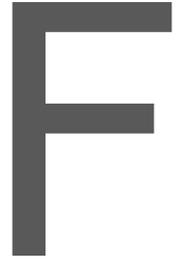
If you are installing an S3100 model in a heavy lightning environment, or in a site where large AC mains power fluctuations are a common occurrence, Verint recommends that you add surge protection on the DATA & PWR port of the PoE injector. It will protect your equipment and the power inserter from surges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



RF Contact between Masters

If the country of operation of your devices requires DFS compliance, you must ensure that the master devices (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 *Nextiva S3100 Series User Guide* or to Chapter 4 in the *Nextiva S1100 User Guide*.

To ensure that two master devices see each other:

1. Take down the device name of MasterB.

This name is displayed in the SConfigurator 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:
1) 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	
	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 device.
 - 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 need 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 device. 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      Source MAC      802.11 BSSID     (dBm) 802.11 SSID
-----
  11 SPCF MSTR 00-0B-6B-30-2A-46 00-0B-6B-30-2A-46 -54  MasterB
```




Separation Between Devices Using Adjacent Channels

Wireless interference can occur between wireless cells using adjacent frequency channels (for example, channels 149 and 153 in the 5 GHz band). Therefore, it is preferable to avoid using adjacent channels. However, if your setup requires you to, you must follow specific guidelines regarding minimum distances between antennas and signal level margin.

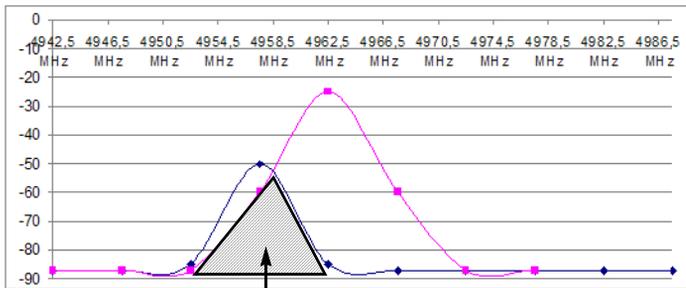
Note: In the 2.4 GHz band, the adjacent channel term applies only to the three independent channels (1, 6, and 11).

If using adjacent frequency channels in a non-DFS environment, you should respect guidelines relative to the minimum separation between device antennas, to avoid interference.

To reduce radio interference possibilities between two adjacent channels, you should ensure that the maximum margin between the emission of the two wireless cells is 25 dB. To meet this objective, perform a site survey and apply minimum distance guidelines.

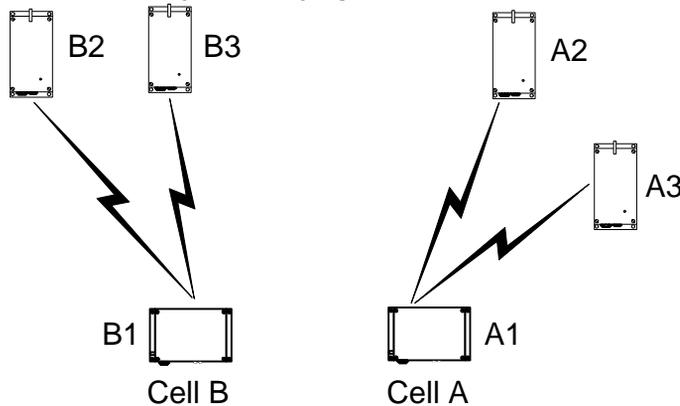
Performing a Site Survey

The difference in signal level between two adjacent cells must be less than or equal to 25 dB. If this margin is higher than 25 dB, there will be too much interference in the two adjacent wireless cells. To calculate this margin, you need to perform a site survey; for more information, see page 66. Here is an example of a 25 dB margin between channels 8 and 9 in the 4.9 GHz band:



Interference between the two channels

Consider the following setup in the 4.9 GHz band with 5-MHz bandwidth, where Cell B uses channel 6 and you are trying to add Cell A on channel 3 (adjacent to channel 6):



To determine if this setup is feasible, you need to conduct a site survey on device A1 (the master device in Cell A), then calculate the margin between the two cells. During the site survey, device A1 will find the other five devices. With the provided signal levels, you need to check if $S_2 - S_1 \leq 25$ dB, where:

- S1 is the lowest signal level in the wireless cell of the device performing the site survey (A1 in the example).
- S2 is the highest signal level in the adjacent cell (Cell B in the example).

To calculate the emission margin between two adjacent wireless cells:

1. Open SConfigurator, then go to the **Units** tab.
2. Select the master device in the wireless cell you are adding, then click **Telnet**.
3. From the main menu of the command line interface (CLI), choose **Advanced > Communication Status and Statistics > Wireless Status**, then press **Enter**.

```
*****
Advanced \ Communication Status and Statistics \ Wireless Status
-----
Parameters:
  NIC Name           : AT5006X DCMA-82 A,B,G 2.4,4.9,5.x GHz
  NIC MAC Address    : 00-0B-6B-2F-F8-E5
  Current Channel     : 7 (4950 MHz) 20 MHz channel bandwidth
  Current TX Rate     : 6 Mb/s
  Current RX Rate     : 6 Mb/s
  Average Signal Level : -65 dBm
  Current SCF Connection Status: Connected to 1 Client and 1 Slave

  RF Communication Quality : N/A
  RF Margin                : N/A
  Current EIRP              : 34 dBm
  Maximum EIRP allowed     : 42 dBm
  Indoor/Outdoor RF Regulation : Indoor/Outdoor FCCA FCC1
  1) Site survey iteration  : 1

Commands:
1) Display link(s) Info
s) Start/Stop Site Survey
v) Visualize Last Site Survey Report
r) Reset Site Survey data base
p) Previous Menu
*****
```

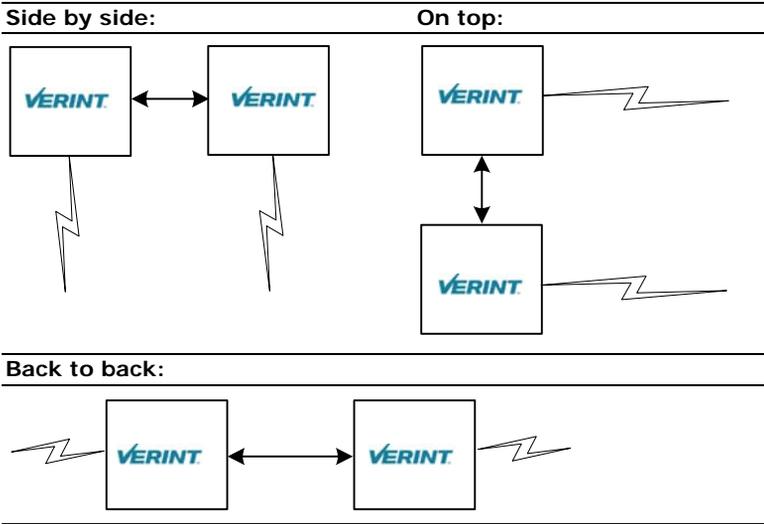
4. For a thorough scan, specify 60 site survey iterations.
5. Start the site survey operation.

Note: During the execution, the RF link will be momentarily broken (duration varies depending on the number of iterations). The link is automatically restored when the survey is finished.

Minimum Distances

To respect the 25 dB margin between two adjacent channels, in addition to performing a site survey, you can use guidelines relative to minimum distances between the wireless devices. By respecting them, you can assume that there will not be radio interference between the devices.

Three physical setups are covered:



The minimum separation between devices using adjacent channels is:

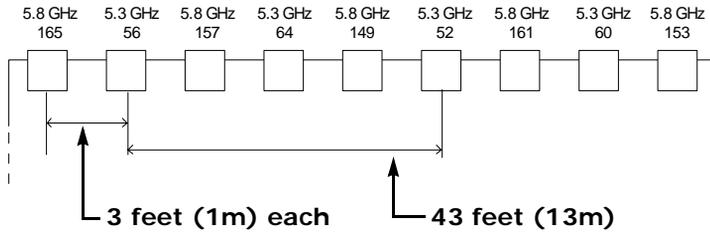
Setup	5 GHz (13-dBi antenna with 40° beam width)	4.9 GHz (13-dBi antenna with 40° beam width)	2.4 GHz (8.5-dBi antenna with 60° beam width)
Side by side	43 feet (13m)	36.1 feet (11m)	55.8 feet (17m)
On top	13 feet (4m)	6.6 feet (2m)	6.2 feet (1.9m)
Back to back	7.8 feet (2.4m)	13.1 feet (4m)	15.7 feet (4.8m)

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

G: Separation Between Devices Using Adjacent Channels

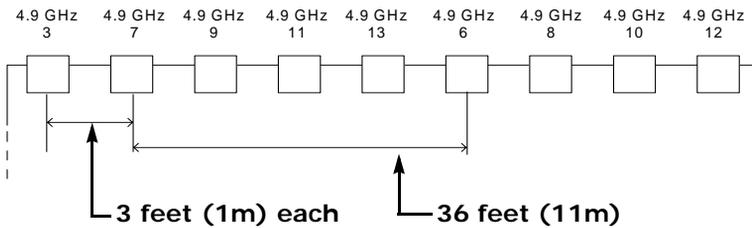
The following deployment scenarios respect these limitations:

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



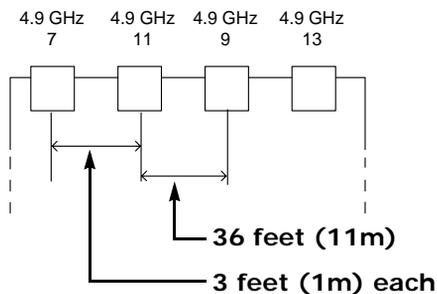
Notice that the devices using the adjacent channels 52 and 56 are separated by the prescribed 43 feet (13m). However, you can intersperse other devices in-between, as long as they do not use adjacent channels. This way, you can increase the device density without encountering interference problems.

- In the 4.9 GHz band, using only 5 MHz channels, all on the same side of a building:



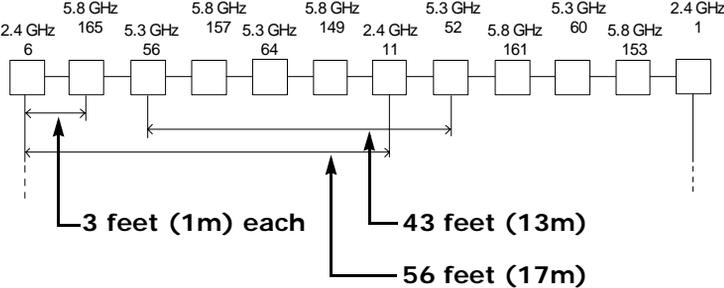
Notice that the devices using the adjacent channels 7 and 6 are separated by the prescribed 36 feet (11m). However, you can intersperse other devices in-between, as long as they do not use adjacent channels. This way, you can increase the device density without encountering interference problems.

- In the 4.9 GHz band, using only 10 MHz channels, all on the same side of a building:

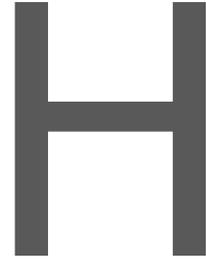


Since only four channels are available, it is unavoidable that two adjacent channels are positioned next to each other.

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



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



DFS and False Radar Detection

Nextiva wireless devices operating in the European Union must adhere to the Dynamic Frequency Selection (DFS) standard; this standard forces any RF transmitter to change frequency channels if radar activity is detected on the current operating channel. If two colocated wireless cells are communicating on adjacent channels, it is possible that the interference between the two systems causes false radar detections. This side-effect is a well-known industry-wide problem. New features in the wireless devices help minimize the occurrence of false detection events.

To avoid false radar detection caused by an adjacent channel, the signal level of an potential interfering device on the first adjacent channel must not exceed -50 dB, -36 dB on the second channel, and -32 dB on the third channel; for example, if you use channel 100, 104 is the first adjacent channel, 108 the second channel, and 112 is the third channel.

The design of wireless systems in a DFS context becomes difficult because not only can the master devices cause an interference, but the clients and slaves on an adjacent channel can also generate interferences that can cause false radar detection. There should be a reduced number of cells available to limit the amount of possible false radar detections; it is strongly suggested to limit the number of colocated cells to six.

The new features that help reduce the possibility of false detection events are:

■ **Half Channel Selection**

This new parameter of the command line interface (CLI) eliminates the possibility of using adjacent channels. Enable this feature on all masters (S3100, S1100-R) in a new installation to avoid the potential conflict of having two masters on adjacent channels. By default this feature is disabled.

If this option is enabled, the channel list becomes:

100(DFS), 108(DFS), 116(DFS), 124(DFS), 132(DFS), 140(DFS), 254(Auto DFS/TPC)

The full channel list is:

100(DFS), 104(DFS), 108(DFS), 112(DFS), 116(DFS), 120(DFS), 124(DFS), 128(DFS), 132(DFS), 136(DFS), 140(DFS), 254(Auto DFS/TPC)

In the CLI: Wireless Communication > Advanced Wireless Setup > DFS/TPC Adjacent Channel Removal

■ **Slave Radar Detection Management**

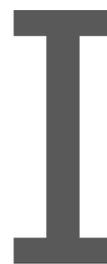
A new CLI parameter allows you to disable radar detection on slave or client devices, therefore reducing the number of nodes that can detect radars. In a typical DFS environment, the slave or client can detect a radar and alert its master to change the frequency channel. This situation can cause a major problem because it increases the number of nodes that can detect radars.

The default value is Disabled, meaning that the slave/client does not detect radars; in this case, the slave/client EIRP is reduced from 30 to 23 dBm.

In the CLI: Wireless Communication > Advanced Wireless Setup > Enable Radar Detection on Slave

■ **Manual Channel Selection**

You can now select the initial frequency channel that will be used by the master, with SConfigurator or the CLI. This new feature does not disable radar detection on master devices. This process will still take place and if a radar is detected, the device will go through the regular DFS process (stop transmission on the channel, block this channel for 30 minutes, and select a new channel in the available channel list).



S3100 Technical Specifications

Here are the S3100 technical specifications:

Network	RF interface	Proprietary 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
Power	Security	SSL-based authentication
	Input voltage	S3100: 48V DC PoE S3100-BR, 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	-22°F to 122°F (-30°C to 50°C)
	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 Directive 2002/95/EC of the European Parliament and of the Council of 27 January 2003 (RoHS)

Glossary

This glossary is common to the Nextiva line of edge device products.

Access Point A communication hub for connecting wireless edge devices (S1100w) to a wired LAN. The Nextiva access point is the S3100 product.

AES (Advanced Encryption Standard) An encryption standard used in the WPA2 authentication method.

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 See *Wireless Bridge*.

Camera, IP See *S2500e, S2600e Series, or S2700e Series*.

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 Intermediate 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 edge devices.

DCE (Data Communication Equipment) In an RS-232 communication channel, a device that connects to the RS-232 interface. Nextiva edge devices 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.

Edge Device A Nextiva device transmitting or receiving video signals through an IP network. The devices can be wireless or wired; some transmitters are IP cameras.

Encoder See *Transmitter*.

Ethernet A local area network (LAN) architecture using a bus or star topology and supporting data transfer rates of 10, 100, and 1000 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.

IP Camera See *S2500e*, *S2600e Series*, or *S2700e Series*.

LAN (Local Area Network) A computer network that spans a relatively small area. A LAN can connect workstations, personal computers, and surveillance equipment (like edge devices). 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 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.

Multiport S17XXe Series The 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 4, 8, 12, or 24 video inputs. Some models offer onboard video analytics capabilities.

nDVR A video management and storage software sold by Verint. This graphical product is used in conjunction with wired and wireless edge devices.

Nextiva The powerful, enterprise-class video management platform and suite of applications from Verint that helps enhance security and improve performance. Nextiva simplifies the management of large scale, distributed video operations and promotes efficient use of network resources.

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 edge device.

PAL (Phase Alternation by Line) A television signal standard (625 lines) 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*.

PEAP (Protected Extensible Authentication Protocol)—A method to securely transmit authentication information, including passwords, over a wireless network.

PSK (Pre-Shared Key) A mode of the WPA and WPA2 security protocols, designed for home and small office networks that cannot afford the cost and complexity of an authentication server. It is also known as *personal mode*.

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.

QoS (Quality of Service) A set of low-level networking protocols giving higher priority to more important data flows while ensuring that the less important ones do not fail.

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

Repeater A range extender for wireless links. The Nextiva repeater is the S3100-RP product, made up of two devices.

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.

S1100 The 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, and the public safety 4.9 GHz band in North America.

S1100w The outdoor wireless video transmitter covering the 2.4 and 5 GHz bands in North America and Europe, and the public safety 4.9 GHz band in North America.

S1500e Series The series of wired edge devices (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.

S1700e Series The 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.

S17XXe Series (Multiport) The 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 4, 8, 12, or 24 video inputs. Some models offer onboard video analytics capabilities.

S1900e Series The highly compact, single-input video transmitter designed for video monitoring and surveillance over IP networks, offering various video qualities and functionality sets, as well as web access for configuration and live viewing. The series includes one receiver, the S1970e-R (displaying up to four video streams), and three transmitters, the S1900e-AS (with onboard analytics capabilities), the S1950e (a cost optimized solution), and the S1970e (for better video performance).

S1900e-Vicon The board holding the S1900e compact IP technology, to be included into Vicon SurveyorVFT dome cameras.

S2500e The MPEG-4-compliant professional IP camera integrating a video sensor and an Ethernet encoder in the same compact enclosure.

S2600e Series The set of professional IP cameras with a super wide range for excellent quality in high-contrast environments. These MPEG-4-compliant cameras integrate a video sensor and an Ethernet encoder in the same compact enclosure. The series includes color, day/night, and analytics-ready cameras. All models provide web access for configuration and live viewing.

S2700e Series The set of high-resolution, IP mini-dome cameras with triple axis lens rotation for flexible installation, and low lux sensitivity for crisp clear images in a variety of lighting conditions. The S2700e cameras offer DVD-quality video and web access for configuration and live viewing. The models are separate for NTSC and PAL; for each video standard, there are two models: indoor and vandal-resistant.

S3100 Series The set of multipurpose outdoor, wireless, digital video products. The series includes the S3100 (for access point systems), S3100-BR (for wireless bridge applications), and S3100-RP (for point-to-point, point-to-multipoint, and wireless bridge repeaters). The S3100 series covers the 2.4 and 5 GHz bands in North America and Europe, and the public safety 4.9 GHz band in North America

SConfigurator A proprietary graphical program used to configure and update the firmware of edge devices.

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 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.

TKIP (Temporal Key Integrity Protocol)—A security protocol used in the WPA authentication method.

TLS (Transport Layer Security)—A cryptographic protocol that provide secure communications on a wireless network.

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 to a receiver. The transmitter converts the analog signal into a digital form before transmitting it. Also called *encoder*.

TTLS (Tunneled Transport Layer Security)—A cryptographic protocol that creates a secure TLS tunnel.

VSIP (Video Services over IP) A proprietary communication protocol for sending messages between a computer and a Nextiva edge device, or between two devices.

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 Bridge A link between two networks, wired or wireless. The Nextiva wireless bridge is the S3100-BR product, made up of two devices.

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.

WPA (Wi-Fi Protected Access version 1) An authentication method to secure wireless systems. It is the successor of WEP. WPA implements the majority of the IEEE 802.11i standard.

WPA2 (Wi-Fi Protected Access version 2) An authentication method that implements the full 802.11i standard, but will not work with some older network cards. It is also known as *802.11i*.

Index

Numerics

- 0.6 F1 25
- 2.4 GHz frequency band. *See* frequency band.
- 4.9 GHz frequency band. *See* frequency band.
- 5 GHz frequency band. *See* frequency band.
- 802.11a. *See* frequency band.
- 802.11g. *See* frequency band.

A

- abnormal power-up condition 52
- Access Management menu 57
- access point application
 - configuration 31
 - defined 16
 - installation 49
- account, user 57
- address, IP. *See* IP address.
- adjacent channel 23, 83–89
- administrator account 57
- Advanced menu 65
- allocation of frequency bands 7
- antenna
 - choosing 26
 - gain 26, 62
 - installation 50, 73
 - location, for Fresnel zone 26
 - requirements 26
 - separation, in colocated systems 20, 83–89
- APIPA addressing scheme 41, 75
- application types 15–19

B

- band, frequency. *See* frequency band.
- bandwidth, channel 6, 62
- bit rate
 - dynamic 12
 - RF 62
 - video 10
- boot sequence 14
- boot, soft 67
- bridge application, wireless
 - configuration 33
 - defined 18
 - installation 48

C

- cable, Ethernet. *See* Ethernet cable.
- casing of the device 3
- CD, Utilities viii

- cell, wireless. *See* wireless cell.
- certificate, SSL 2, 58
- channel, RF
 - automatic selection with DFS 14
 - available 6, 61
 - fragmenting 6, 62
 - manual selection 45, 61
 - selecting the location 65
 - usage, in relation to the MAC protocol 20
- characteristics of the device 2
- CLI (command line interface)
 - access with Telnet 56
 - menus 59–67
- client
 - boot sequence with DFS 15
 - communication with master 47
 - defined 8
 - maximum number in a cell 10
- colocated cell 20–22
- command line interface. *See* CLI (command line interface).
- common VSIP port 53
- communication between master, clients, and slaves 47
- compatibility of firmware versions 8
- compliance 105
- computer requirements 30
- computer, changing the IP address 37
- configuration
 - default 66, 69
 - device 37–47
 - order, in the wireless cell 9
- connection
 - Ethernet 41
 - Ethernet cable 71
 - grounding 49
 - PoE 36
 - power 35
- connectors on the device 4
- constraints in Europe 13–15, 22–25
- contact between two masters 23, 79–81
- country
 - available frequency bands 7
 - selecting 43, 63
- crossover Ethernet cable
 - for configuring the device 41
 - pinout 72
 - supplied 2
- customer service ix

D

data throughput 10
 default configuration 66, 69
 detecting duplicate masters 52
 DFS (Dynamic Frequency Selection)
 boot sequence 14–15
 defined 7
 setups in Europe 22–25
 DHCP (Dynamic Host Configuration Protocol) 43,
 59, 75
 distance
 between antennas 20, 87–89
 between antennas and persons 27
 between collocated devices 20, 87–89
 maximum link 64
 downgrade of firmware 50
 DSCP (Differentiated Service Code Points) 51
 duplicate IP address 41
 duplicate master detection 52
 dynamic bit rate control 12
 Dynamic Frequency Selection. *See* DFS (Dynamic
 Frequency Selection).

E

EIRP 26
 emitting power. *See* transmission power.
 enclosure of the device 3
 equipment list 2
 Ethernet cable
 for configuration 41
 connection 41
 maximum length 35, 41
 pinouts 71
 supplied 2
 Ethernet network LED 51
 ETSI (European Telecommunications Standards
 Institute) 7
 Europe
 colocation in the 2.4 GHz band 21–22
 colocation in the 5 GHz band 22–25
 DFS context 7, 14–15
 TPC context 7, 13
 evaluating the location 25
 exposure, RF 27
 external antenna. *See* antenna.
 extranet, Verint Video Intelligence Solutions ix

F

factory default configuration 66, 69
 features of the device 2
 finding a lost device 53
 firmware update
 downgrading 50
 performing 50
 preventing 58

firmware update (*cont'd*)
 without losing devices 9
 firmware version
 compatibility between devices 8
 displayed 59
 first Fresnel zone 25
 frequency band
 available 6
 distance limitations 83–89
 licensed 6
 public safety 6
 selecting, in the CLI 61
 frequency channel
 automatic selection with DFS 14
 available 6, 61
 fragmenting 6, 62
 manual selection 45, 61
 selecting the location 65
 usage, in relation to the MAC protocol 20
 Fresnel zone 25

G

gain of an antenna 26, 62
 gateway 60
 global security profile 58
 grounding connection 49

H

hidden node problem 13

I

identifying a device 65
 indoor/outdoor RF regulation 65
 injector, PoE 36
 installation
 antenna 50, 73
 device 47–49
 interference, RF 27, 83
 IP address
 APIPA 75
 changing, for the computer 37
 duplicate 41
 setting 41, 59
 temporary 75

L

LAN LED 51
 LED 4, 51–52
 length of Ethernet cable 35, 41
 licensed band. *See* frequency band.
 limitations
 collocated systems 20
 distance 20, 87–89
 Europe 13–15, 22–25

line-of-sight path 25
 link distance, maximum 64
 link speed 62
 loading default configuration 66, 69
 location evaluation 25
 login name. *See* user name.
 lost device 53

M

MAC protocol 13, 61
 MAC role 8, 18
 margin between adjacent channels 84
 margin, minimum RF 64
 mask, subnet 60
 master
 boot sequence with DFS 14
 communication with clients and slaves 47
 constraint in DFS 14
 defined 8
 duplicate 52
 ensuring RF contact 23, 79–81
 maximum gain of an antenna 26
 maximum length of Ethernet cable 35, 41
 maximum link distance 64
 maximum number of devices in a cell 10
 maximum transmission power. *See* transmission power.
 Media Access Control (MAC). *See the “MAC” entries.*
 menus in the CLI 59–67
 minimum RF margin 64

N

network
 menu in the CLI 59
 planning 5–18
 settings in SConfigurator 43

O

options, when ordering a device 2
 order in the configuration and update process 9
 order, starting 14, 64

P

passkey
 SSL 58
 for Telnet connection 57
 wireless. *See* wireless passkey.
 password. *See* passkey.
 ping request 60
 pinout, Ethernet cable 71
 planning
 RF 25–27
 wireless cell 12–18

PoE (power-over-Ethernet) injector 36
 point-to-multipoint repeater
 configuration 32
 defined 16
 installation 47
 point-to-multipoint wireless bridge
 configuration 34
 defined 18
 point-to-point repeater
 configuration 30
 defined 17
 installation 47
 power connection 35
 power requirement 3, 4
 power, transmission. *See* transmission power.
 power-over-Ethernet (PoE) injector 36
 power-up condition, abnormal 52
 preparation of the device 41
 preventing, firmware update 58
 protection
 device configuration 57
 surge 49, 77
 protocol, MAC 13, 61
 public safety band. *See* frequency band.

Q

Quality of Service (QoS) 51

R

radar detection 14
 radio frequency. *See* RF (radio frequency).
 radio transmission power. *See* transmission power.
 reboot, soft 67
 recognizing a device 65
 repeater
 installation 47
 point-to-multipoint 16, 32
 point-to-point 17, 30
 wireless bridge 19, 34
 requirements
 antenna 26
 computer 30
 power 3, 4
 video bit rate 12
 reset to factory default 66, 69
 RF (radio frequency)
 channel. *See* frequency channel.
 contact between two masters 23, 79–81
 exposure considerations 27
 global spectrum allocation 7
 LED 52
 line of sight 25
 menu in the CLI 60
 parameters 44–46, 60
 planning 25–27

RF (radio frequency) (*cont'd*)

See also the "wireless" entries.

RJ-45 Ethernet cable. *See* Ethernet cable.

RoHS 109

role, MAC 61

S

S1100

checking communication with master 47

compatibility with S3100 8

maximum number in a cell 10

role in a wireless cell 8, 17

S1100w

checking communication with master 47

compatibility with S3100 8

maximum number in a cell 10

role in a wireless cell 8, 16

S3100

in an access point application 16

casing 4

configuration 31

installation 49

S3100-BR

casing 4

configuration 33

installation 48

in a wireless bridge application 18

S3100-RP

casing 4

configuration 30, 32, 34

installation 47

in a point-to-multipoint repeater 16

in a point-to-point repeater 17

in a wireless bridge repeater 19

scanning for a frequency channel 14

SConfigurator 41–47

SDCF

in the CLI 61

defined 13

maximum link distance 64

security features 2

Security menu 57

sensitivity threshold 63

separation between antennas 87–89

sequence of boot 14

setups in Europe 23–25

shipment list 2

site survey

adjacent channels 84

CLI commands 66

RF contact between masters 80

slave

boot sequence with DFS 15

communication with master 47

defined 8

maximum number in a cell 10

soft reboot 67

software reset 66

SPCF 13, 61

specifications, technical 91

spectrum allocation 7

speed of the wireless link 62

SSL (Secure Sockets Layer) 2, 58

starting order 14, 64

status LED 52

status, system 57

straight-through Ethernet cable

for configuring the device 41

pinout 72

supplied 2

subnet mask 60

support, technical ix

surge protection 49

survey, site

adjacent channels 84

CLI commands 66

RF contact between masters 80

system planning 12–18

system reboot 67

system status 57

system status LED 52

T

technical specifications 91

technical support ix

Telnet, preventing access 58

temporary IP address 75

threshold, sensitivity 63

throughput, data 10

ToS (Type of Service) 51

TPC (Transmit Power Control) 7, 13

transmission distance, maximum 64

transmission power

when choosing an antenna 26

in the CLI 63

reducing, for TPC 13

U

user account 57

user name 57

Utilities CD viii

V

Verint web site ix

version of firmware

compatibility between devices 8

displayed 59

VSIP port 53

W

- warranty x
- web site, Verint ix
- width, channel 6, 62
- wireless bridge
 - configuration 33
 - defined 18
 - installation 48
- wireless bridge repeater
 - configuration 34
 - defined 19
 - installation 47
- wireless cell 8, 12–18
- wireless Ethernet LED 52
- wireless frequency plan 7
- wireless parameters 44–46, 60–65
- wireless passkey
 - in the CLI 61
 - in colocated cells 20
 - in SConfigurator 46
 - in a single cell 8

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 devices 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

The FCC IDs are VKHCM9S3100 and NKRDCMA82 (for the S3100-49, S3100-BR-49, and S3100-RP-49 only).

This device complies with parts 15 and 90 (for the S3100-49, S3100-BR-49, and S3100-RP-49 only) 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 device
- 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 Systems Inc. could void the user's authority to operate the equipment.

Canada

The IC ID is 7286A-CM9S3100.

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.

This device has been designed to operate with the antennas listed below, and having a maximum gain of 16 dBi for the 2.4 GHz band and 19 dBi for the 5 GHz band. Antennas not included in this list or having a gain greater than 16 dBi for the 2.4 GHz band and 19 dBi for the 5 GHz band are strictly prohibited for use with this device. The required antenna impedance is 50 ohms. The certified antennas are:

- ANT-WP8-24/S: 8.5 dBi gain, 2.4 GHz band, 65° beamwidth, patch antenna with 3-foot (1-meter) SMA-SMA cable
- ANT-WP13-5x/S: 13 dBi gain, 5.25-5.85 GHz band, 40° beamwidth, patch antenna SMA/F connector
- ANT-WP13-49-5x/S: 13 dBi gain, 4.9-5.85 GHz band, 40° beamwidth, patch antenna SMA/F connector
- ANT-WP16-24/Sio: 16dBi gain, 2.4 GHz band, 27° beamwidth, patch antenna with 3-foot (1-meter) SMA-N cable
- ANT-WP19-5x/S: 19 dBi gain, 5.25-5.85 GHz band, 18° beamwidth, patch antenna with 3-foot (1-meter) SMA-N cable

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 device
Model number: S3100, S3100-BR, S3100-RP

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

R&TTE Directive 1999/5/EC

EN 301 489-17 V1.2.1 (2002-08)
EN 301 489-1 (V1.5.1) (2004-09)
EN 60950-1:2001, A11:2004 First Edition
EN 300 328, V1.6.1 (2004-11)
ETSI EN 301 893 V1.3.1 (2005-03)
EN 50385:2002

Verint hereby declares that the equipment specified above conforms to the above Directive(s) and Standard(s).

September 17th, 2007
Laval, Canada

For the official signed declaration of conformity, visit

http://www.verint.com/video_solutions/section2a.cfm?article_level2_category_id=17&article_level2a_id=289.

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 device
Model number: S3100, S3100-BR, S3100-RP

To which this declaration relates is in conformity with the following standards or other documents:**R&TTE Directive 1999/5/EC**

EN 301 489-17 V1.2.1 (2002-08)
EN 301 489-1 (V1.5.1) (2004-09)
EN 60950-1:2001, A11:2004 First Edition
EN 300 328, V1.6.1 (2004-11)
ETSI EN 301 893 V1.3.1 (2005-03)
EN 50385:2002

Verint hereby declares that the equipment specified above conforms to the above Directive(s) and Standard(s).

September 17th, 2007
Laval, Canada

For the official signed declaration of conformity, visit

http://www.verint.com/video_solutions/section2a.cfm?article_level2_category_id=17&article_level2_a_id=289.

RoHS Declaration of Compliance

June 14th, 2006

Verint believes in the importance of conducting our business in a manner that will help protect the environment as well as our employees, customers, and the public.

To that end, we are committed to bringing our existing and future product lines into EU RoHS Directive compliance.

Thus, as of July 1 2006, the following products, S3100, S3100-BR, and S3100-RP, will comply with the DIRECTIVE 2002/95/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 January 2003 (RoHS) regarding the restriction of the use of certain hazardous substances in electrical and electronic equipment.

The S3100, S3100-BR, and S3100-RP products will not exceed the maximum concentrations of 0.1% by weight in homogenous materials for lead, hex chrome, mercury, PBB, PBDE, and 0.01% for cadmium. In addition, the S3100, S3100-BR, and S3100-RP products will qualify for the "lead in servers solders" exemption as set forth in the Directive.

This declaration is provided based on reasonable inquiry of our suppliers and represents our actual knowledge based on the information provided by our suppliers.

AMERICAS

info@verint.com

www.verint.com/videosolutions

EMEA

marketing.emea@verint.com

www.verint.com/videosolutions

APAC

marketing.apac@verint.com

www.verint.com/videosolutions