Allied Telesis™

Extricom Series

WLAN System

- AT-EXMS-1000
- AT-EXLV-2000
- AT-EXLS-3000
- AT-EXMS-500
- AT-EXRP-22n/32n/22En/32EOn

Installation and User Guide

the solution : the network

613-002102 Rev. C

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis, Inc. has been advised of, known, or should have known, the possibility of such damages.

Disclaimer and Safety

Note
Important: Read this guide, safety instructions, and the release notes for your switch firmware, before installing and operating the Extricom Series WLAN System.

This chapter includes the following:

❐ “Disclaimer Statements” on page 3

❐ “Federal Communication Commission and Industry Canada Interference Statement” on page 4

❐ “FCC and IC Radiation Exposure Statement” on page 5

❐ “Translated Safety Statements” on page 5

Disclaimer Statements

Allied Telesis makes no representations or warranties whether expressed or implied, that the Extricom Series wireless local area network (WLAN) system or any component thereof shall meet the purchaser’s operating requirements or that system operation will be uninterrupted or error-free. All WLANs, including the Extricom Series WLAN System, can potentially be affected by outside sources of interference such as other broadcasting devices, radiation, device immunity level, and other external sources of interference.

⚠ **Warning**
This equipment has been approved for mobile applications where the equipment is to be used at distances greater than 20cm from the human body (with the exception of hands, wrists, feet and ankles). Operation at distances of less than 20 cm is strictly prohibited.

Changes or modification to equipment not expressly approved by Allied Telesis, Inc. is strictly prohibited and could void the user's license to operate the equipment. 🙤 **E108**

Note
AT-EXRP-22n, AT-EXRP-32n, and AT-EXRP-22En access points are for indoor use only.

Note
The maximum antenna gain is 4dBi.

Note
An Extricom Series access point includes multiple WLAN radio modules; each radio module is configured separately and serves a different set of clients. There is no relation between transmissions on different radio modules, hence in a single AP:

Radio modules cannot transmit simultaneously over the same radio channel.

A client device may transmit and receive data through one radio module.

Note
Please check the release notes for your version of Extricom Series firmware before installing or operating the system. The relevant release notes supersede this user guide.

The availability of some specific channels and/or operational frequency bands is country-dependent, and the firmware is programmed at the factory to match the intended destination. This firmware setting is not accessible by the end user.

Federal Communication Commission and Industry Canada Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC and IC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses 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 of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- 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

⚠ **Caution**
FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate this equipment. **E80**

This device complies with Part 15 of the FCC & IC Rules. Operation is subject to the following two conditions:

- ❐ This device may not cause harmful interference
- ❐ This device must accept any interference received, including interference that may cause undesired operation.

FCC and IC Radiation Exposure Statement

This equipment complies with FCC and IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Operations in the 5.15-5.25 GHz band are restricted to indoor usage only, to reduce potential for harmful interference to co-channel satellite systems.

The maximum antenna gain permitted (for devices in the 5725-5825 MHz band) must comply with the EIRP limits specified for point-to-point and non point-to-point operation as appropriate, as stated in section A9.2(3).

Sec. A9.2 (3): For the band 5725-5825 MHz, the maximum conducted output power shall not exceed 1.0 W or 17 + 10 log10 B, dBm, whichever power is less. The power spectral density shall not exceed 17 dBm in any 1.0 MHz band. The maximum EIRP shall not exceed 4.0 W or 23 + 10 log10 B, dBm, whichever power is less. B is the 99% emission bandwidth in MHz.

Fixed point-to-point devices for this band are permitted up to 200 W EIRP by employing higher gain antennas, but not higher transmitter output powers. Point-to-multipoint systems, Omni-directional applications and multiple co-located transmitters transmitting the same information are prohibited under this high EIRP category. However, remote stations of point-to-multipoint systems shall be permitted to operate at the point-to-point EIRP limit provided that the higher EIRP is achieved by employing higher gain directional antennas and not higher transmitter output powers.

Translated Safety Statements

Important: The 👓 indicates that a translation of the safety statement is available in a PDF document titled *Translated Safety Statements* on the Allied Telesis website at **www.alliedtelesis.com/support**.

Contents

Disclaimer and Safety 3
Disclaimer Statements 3
Federal Communication Commission and Industry Canada Interference Statement 4
FCC and IC Radiation Exposure Statement 5
Translated Safety Statements 5

Preface 13
Document Conventions 14
Contacting Allied Telesis 15

Chapter 1: Introduction to the Extricom Series WLAN System 17
Extricom Series WLAN System Solution 18
Product Naming Conventions 19
Switches, Range Extender, and Media Converter 19
Access Points 20
Overview of the Extricom Series WLAN System 21
Feature Highlights 23
Overview of the Switch Platforms 29
Overview of the Extricom Series Access Points 31
Access Points with Internal Integrated Antennas 31
Access Points with Connectors for External Antennas 32
Outdoor Access Points with Connectors for External Antennas 33
A Typical Extricom Series Wireless Network Topology 34
Switch Cascade 35
AT-EXLS-3000 38

Chapter 2: Installation 39
Reviewing Safety Precautions 40
Unpacking the Extricom Series WLAN System 42
Switches 42
Access Points 42
AT-EXRE-1000 Range Extender 42
AT-EXMC-1000 Media Converter 42
Additional Equipment 43
Cables for Connecting Two Switches in Switch Cascade 43
Cable for Connecting the AT-EXLS-3000 to AT-EXMS-1000s 43
Determining the Location of the Extricom Series Access Points 44
Extricom Series Switches 45
AT-EXRP-22n, AT-EXRP-32n, AT-EXRP-22En, AT-EXRP-32EOn Access Points 49
Access Point Connectors and LEDs 51
Mounting the Switches (Optional) 53
Mounting the Access Points (Optional) 54
Connecting the Switch and the Access Points 56
Connecting the AT-EXLS-3000 Switch 60
Range Extenders and Media Converters 62
AT-EXRE-1000 Range Extender 62
AT-EXMC-1000 Media Converter 62

Chapter 3: Configuring Extricom Series WLAN System 63
Accessing the Extricom Series Switch GUI 64
Using the Extricom Series Web Configuration Pages 66
Overview of the Configuration 68
Configuring LAN Parameters 70
Configuring WLAN Settings 72
Configuring ESSID Definition 72
Configuring WLAN Radios 88
ESSID Assignment 95
Access Points 96
System Tools Configuration 99
Apply 99
Reboot 99
Maintenance 100
Time & Date 101
Passwords 102
Upgrade 104
Certificate 105
Application 106
License 106
Advanced Configuration 107
Cascade Resiliency 107
Rogue 110
System Logging 110
SNMP 112
IDS 114
Portal (Captive Portal) 116
Multicast 119
LBS 120
Expert 120
Others 120
Viewing Events and Reports 123
System Events 123
Clients Events 123
Events Filter 124
Reports 124
Diagnostics 125

Chapter 4: Configuring AT-EXLS-3000 System 129
Powering Edge Switches 130
Advanced Configuration – AT-EXLS-3000 Differences 132
Redundancy 132
Redundancy Fields for Primary Switch 133

Chapter 5: Configuring AT-EXLV-2000 System 135
Advanced Configuration – AT-EXLV-2000 Differences 136
Enabling Large Public Venue 136
Configuring Honeypot 136
Configuring Access Point Parameters 138
Switch Load Balancing 139

Chapter 6: Troubleshooting 141

Chapter 7: Northbound SNMP Traps 145

Appendix A: Internal Access Point Mounting Template 155

Appendix B: Certifications 157

Figures

Figure 1: Switch, Range Extender, Media Converter Naming Convention 19
Figure 2: Access Point Naming Convention 20
Figure 3: Three-Channel Blanket Coverage 21
Figure 4: AT-EXMS-1000 29
Figure 5: AT-EXLV-2000 29
Figure 6: AT-EXLS-3000 30
Figure 7: AT-EXMS-500 30
Figure 8: AT-EXRP-22n and AT-EXRP-32n APs 31
Figure 9: AT-EXRP-22En AP........ 32
Figure 10: AT-EXRP-32EOn AP........ 33
Figure 11: Typical Extricom Series Topology 34
Figure 12: Switch Cascade Topology 35
Figure 13: Uplink Redundancy in Switch Cascade Topology 36
Figure 14: Full Redundancy in Switch Cascade Topology 37
Figure 15: AT-EXLS-3000 Topology........ 38
Figure 16: AT-EXMS-1000 and AT-EXLV-2000 Switches........ 45
Figure 17: AT-EXLS-3000 Switch........ 45
Figure 18: AT-EXMS-500 Switch........ 46
Figure 19: AT-EXRP-22n and AT-EXRP-32n........ 49
Figure 20: AT-EXRP-22En 49
Figure 21: AT-EXRP-32EOn........ 50
Figure 22: Switch Mounting Bracket........ 53
Figure 23: AP Mounting Bracket........ 54
Figure 24: AP Drilling Card........ 55
Figure 25: Login Page 65
Figure 26: Typical Web Configuration Page........ 66
Figure 27: Configuration Overview of AT-EXLV-2000 68
Figure 28: LAN Settings Page 70
Figure 29: WLAN ESSID Definition Page - ESSID Settings Tab........ 73
Figure 30: MAC ACL Configuration Tab........ 84
Figure 31: MAC ACL Scheduler Configuration Tab........ 85
Figure 32: RADIUS Configuration Tab 86
Figure 33: WLAN Wizard Configuration Page 88
Figure 34: Radios Configuration Page........ 92
Figure 35: WMM Configuration Tab........ 93
Figure 36: ESSID Assignment Page........ 95
Figure 37: Access Points PoE & Radio Controls Page........ 96
Figure 38: Port Naming Window........ 97
Figure 39: Access Points Status Page 97
Figure 40: Access Point Configuration Window - Secondary Switch........ 98
Figure 41: System Tools Configuration Page........ 99
Figure 42: Maintenance Configuration Tab 100
Figure 43: Pop-up Window - Configuration Elements to Upload 101
Figure 44: Pop-up Window - Configuration Elements to Restore 101
Figure 45: Time & Date Configuration Tab........ 102
Figure 46: Upgrade Configuration Tab 104
Figure 47: Certificate Configuration Tab........ 105
Figure 48: Application Configuration Tab 106
Figure 49: License Configuration Tab........ 106

Figure 50: Resiliency Configuration Tab 107
Figure 51: Rogue Configuration Tab 110
Figure 52: System Logging Configuration Tab 111
Figure 53: SNMP Configuration Tab 113
Figure 54: IDS Configuration Tab 115
Figure 55: Captive Portal Configuration Tab 117
Figure 56: Extricom Series Default Captive Portal Web Page 119
Figure 57: Multicast Configuration Tab 120
Figure 58: LBS Configuration Tab 120
Figure 59: Expert Configuration Tab 120
Figure 60: Others Configuration Tab 121
Figure 61: Band Steering Operational Flow 121
Figure 62: Events & Reports - Client Events Tab 123
Figure 63: Events Filter Configuration Tab 124
Figure 64: Reports Tab 124
Figure 65: Diagnostics Tab 126
Figure 66: Access Points PoE & Radio Controls Page 130
Figure 67: Redundancy Configuration Tab 132
Figure 68: LV Settings 136
Figure 69: Honeypot 136
Figure 70: LV Access Point Parameters 138
Figure 71: LV Switch Load Balancing 140
Figure 72: Internal Access Point Mounting Template 155

Tables

Table 1. Switch, Range Extender, Media Converter Model Nomenclature 19
Table 2. Access Point Model Nomenclature 20
Table 3. Extricom Series Switch Connectors 46
Table 4. Extricom Series Switch LEDs 47
Table 5. Extricom Series AP Connectors 51
Table 6. AT-EXRP-22En, AT-EXRP-32n, AT-EXRP-22En, AT-EXRP-32EOn AP LEDs 51
Table 7. Cat5e/6 100/1000Mbps Cable 58
Table 8. Fiber Media cable 58
Table 9. Mixed Media Types 58
Table 10. Mixed Media Types 59
Table 11. Overview Page 68
Table 12. LAN Configuration Parameters 70
Table 13. ESSID Parameter Descriptions 73
Table 14. Security Definition Parameters 79
Table 15. MAC ACL Scheduler Parameters 85
Table 16. RADIUS Configuration Parameters 87
Table 17. Radio Configuration Parameters 89
Table 18. WMM Parameters Description 93
Table 19. WMM Standard Prioritization 94
Table 20. Maintenance Configuration Tab 100
Table 21. Default Passwords 103
Table 22. Resiliency Configuration Tab Parameters for a Primary Cascade Switch 108
Table 23. Switch Cascade Failover Behavior 108
Table 24. Rogue Configuration Tab Rogue AP White List Parameters 110
Table 25. IDS Configuration Parameters 115
Table 26. Captive Portal Configuration Parameters 117
Table 27. Reports Tab Fields 124
Table 28. Diagnostics Tab Parameters and Tests 126
Table 29. Redundancy Configuration Tab Parameters for a Primary Cascade Switch 133
Table 30. Honeypot configuration 137
Table 31. Honeypot ESSID Configuration 137
Table 32. Rate Stickiness Configuration 139
Table 33. LV Switch Load Balancing 140
Table 34. Troubleshooting 141
Table 35. SNMP Traps 145
Table 36. Certifications 157

Preface

This preface contains the following sections:

❒ "Document Conventions" on page 14

❒ "Contacting Allied Telesis" on page 15

This guide provides detailed instructions for installing, configuring, and troubleshooting the AT-EXMS-500, AT-EXMS-1000, AT-EXLV-2000, and AT-EXLS-3000 WLAN switches, AT-EXRP-22n, AT-EXRP-32n, AT-EXRP-22En, and AT-EXRP-32EOn UltraThin™ access points (APs), AT-EXRE1000 range extender, and AT-EXMC1000 media converter.

Document Conventions

This document uses the following conventions:

Note
Notes provide additional information.

⚠ **Caution**
Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

⚠ **Warning**
Warnings inform you that performing or omitting a specific action may result in bodily injury.

Contacting Allied Telesis

If you need assistance with this product, you may contact Allied Telesis technical support by going to the Support & Services section of the Allied Telesis web site at **www.alliedtelesis.com/support**. You can find links for the following services on this page:

- 24/7 Online Support — Enter our interactive support center to search for answers to your product questions in our knowledge database, to check support tickets, to learn about RMAs, and to contact Allied Telesis technical experts.
- USA and EMEA phone support — Select the phone number that best fits your location and customer type.
- Hardware warranty information — Learn about Allied Telesis warranties and register your product online.
- Replacement Services — Submit a Return Merchandise Authorization (RMA) request via our interactive support center.
- Documentation — View the most recent installation and user guides, software release notes, white papers, and data sheets for your products.
- Software Downloads — Download the latest software releases for your managed products.

For sales or corporate information, go to **www.alliedtelesis.com/purchase** and select your region.

Chapter 1

Introduction to the Extricom Series WLAN System

This chapter contains the following sections:

❒ "Extricom Series WLAN System Solution" on page 18

❒ "Product Naming Conventions" on page 19

❒ "Overview of the Extricom Series WLAN System" on page 21

❒ "Feature Highlights" on page 23

❒ "Overview of the Switch Platforms" on page 29

❒ "Overview of the Extricom Series Access Points" on page 31

❒ "A Typical Extricom Series Wireless Network Topology" on page 34

❒ "AT-EXLS-3000" on page 38

Extricom Series WLAN System Solution

A Wireless Local Area Network (WLAN) based on the IEEE 802.11 standard enables laptops, PDAs, phones, and other Wi-Fi equipped devices to wirelessly connect to the enterprise network.

However, large-scale deployments of traditional cell-based WLANs, in which each access point (AP) operates on a different channel than that of adjacent APs, have been hindered by issues such as poor coverage, low capacity, high-latency mobility, and expensive interference analysis or site survey and maintenance costs.

The Extricom Series WLAN, on the other hand, takes a different solution approach, by avoiding the coverage and capacity trade-offs of traditional cell-based WLAN architecture. In addition, the need for cell planning and interference analysis, a highly expensive aspect of owning a WLAN, is also eliminated. Finally, the Extricom Series WLAN approach eliminates most WLAN maintenance tasks. The Extricom Series WLAN System is specifically designed to provide increased network capacity, seamless mobility, high level of security, and easy installation and configuration.

Product Naming Conventions

Extricom Series WLAN products include wireless switches and access points (APs). Optional Extricom products include a range extender and media converter. The following lists the naming conventions of these products.

Switches, Range Extender, and Media Converter

The AT-EXMS-1000 switch is used as an example for the naming convention shown in Figure 1.

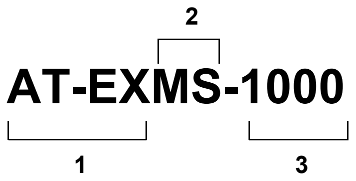


Figure 1. Switch, Range Extender, Media Converter Naming Convention

Table 1 identifies the numbers corresponding to the model name.

Table 1. Switch, Range Extender, Media Converter Model Nomenclature

Convention	Definition
1	Allied Telesis - Extricom
2	Identifies switch type or if range extender or media converter: ❒ MS - Multi Series ❒ LV - Large Venue ❒ LS - Large Scale ❒ RE - Range Extender ❒ MC - Media Converter
3	Deployment size: 500, 1000, 2000, 3000, in which 500 is the smallest and 3000 is the largest.

Access Points

The AT-EXRP-32EOn access point is used as an example for the naming convention shown in Figure 2.

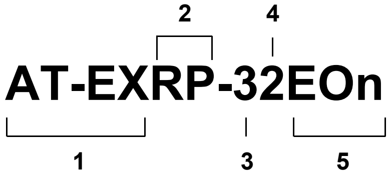


Figure 2. Access Point Naming Convention

Table 2 identifies the numbers corresponding to the model name.

Table 2. Access Point Model Nomenclature

Convention	Definition
1	Allied Telesis - Extricom
2	Radio point (access point)
3	Number of radios in unit: ❐ 2 - AT-EXRP-22n, AT-EXRP-22En ❐ 3 - AT-EXRP-32n, AT-EXRP-32EOn
4	Number of spatial streams - 2
5	Type of antenna: ❐ n - internal (AT-EXRP-22n, AT-EXRP-32n) ❐ En - external (AT-EXRP-22En) ❐ EOn - external outdoor (AT-EXRP-32EOn)

Overview of the Extricom Series WLAN System

The Extricom Series WLAN consists of a wireless switch (AT-EXMS-500 / AT-EXMS-1000 / AT-EXLV-2000 and sometimes, also the AT-EXLS-3000) connected to a set of UltraThin™ APs (AT-EXRP-22n, AT-EXRP-32n, AT-EXRP-32EOn and AT-EXRP-22En). The Extricom Series WLAN System eliminates the concept of cell planning and replaces it with the “Channel Blanket” topology. In this topology, each Wi-Fi radio channel is used on every access point to create continuous “blankets” of coverage. By using multi-radio APs, the Extricom Series System is able to create multiple overlapping Channel Blankets from the same physical set of devices, as illustrated in Figure 3.

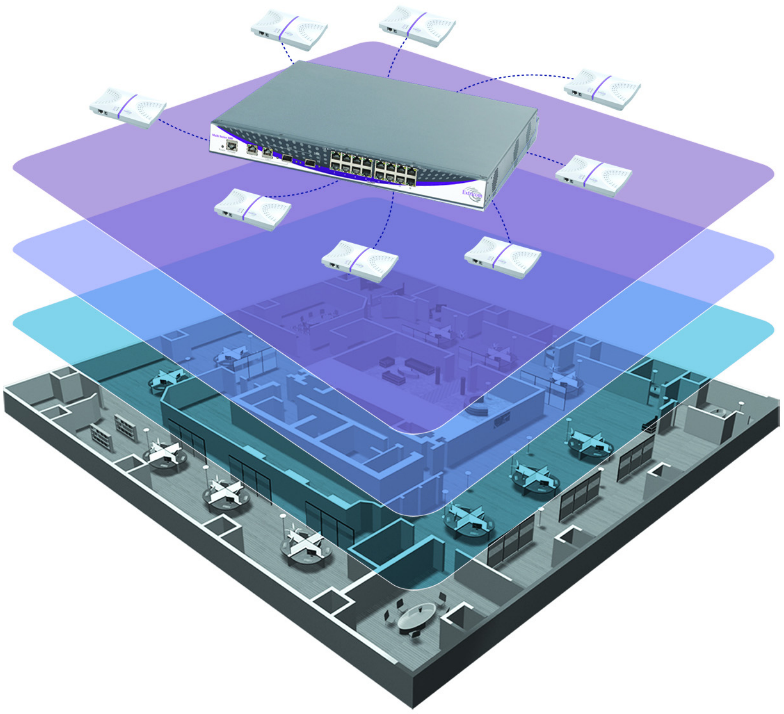


Figure 3. Three-Channel Blanket Coverage

The Extricom Series solution is based on a fully centralized WLAN architecture, in which the switch makes all the decisions for packet delivery on the wireless network. In this configuration, the access points (APs) simply function as radios, with no software, storage capability, or IP addresses. Even the basics of connecting are different: clients associate directly with the switch, not with the APs. The APs act as RF conduits to rapidly funnel traffic between the clients and the switch. The Extricom Series architecture has essentially centralized the 802.11 logic in the switch, while distributing the wireless electronics in the APs.

Centralization of the Wi-Fi environment enables enterprises to deploy 802.11a/b/g/n channels at every AP, creating multiple overlapping Channel Blankets that leverage each of the radios in the multi-radio UltraThin AP. Each channel's bandwidth is delivered across the blanket's service area (that is, the combined coverage of all APs connected to the switch), with interference-free operation and consistent capacity throughout.

As the client moves through the coverage blanket, different APs take over the communication with it, depending on which AP is in the best position to serve the client at the time. The switch always uses the optimal uplink and downlink path. While this goes on "behind the scenes," the client never detects an AP-to-AP hand-off (that is, de-association and re-association), thus experiencing seamless mobility.

Within each Channel Blanket, the switch avoids co-channel interference by permitting multiple APs to simultaneously transmit on the same channel only if they will not interfere with each other: This is the essence of the TrueReuse™ functionality.

The Extricom Series supports the 802.11n standard, which builds upon existing 802.11 standards. 802.11n can be used in both the 5 GHz and 2.4 GHz frequency bands, introduces enhancements to the MAC and the PHY layer, and makes use of multiple-input multiple-output (MIMO) technology. MIMO is a technology that employs multiple transmitter and receiver antennas to support simultaneous data streams. Such technology is capable of increasing data throughput via enhancements such as spatial multiplexing (data streams), 40MHz channel bonding, block acknowledgment and frame aggregation, and use of spatial diversity to increase range.

Feature Highlights

The Extricom Series WLAN System solution offers the following features:

Ease of deployment - no cell planning

The Extricom Series architecture requires no cell planning and experiences no constraints due to RF interference or channelization. Consequently, Extricom Series APs can be deployed wherever needed, in any density or even varying density, to meet the end-client's desired level of service (stipulated in terms of connection rate). The traditional site survey is therefore reduced to simple examination of the space in order to plan the location of the physical equipment.

Multi-Layer WLAN

Using multiple radio access points (APs), a single set of APs enables deployment of multiple high-data-rate Channel Blankets with overlapping coverage, resulting in multiplied aggregate capacity. Separate Channel Blankets also offer the unique ability to guarantee Quality of Service by physically segregating different types of traffic (based on service class, user type, and administrative privileges) onto different channels.

Same-band operation

The Extricom Series WLAN System enables WLAN channels, in the same band (for example, Channel 1, 6, and 11 in 2.4 GHz), to be simultaneously used within the same AP, to form overlapping Channel Blankets using the same physical set of APs.

TrueReuse bandwidth

TrueReuse technology multiplies the bandwidth of a standard 802.11 channel by dynamically optimizing the reuse of each frequency. Within a Channel Blanket, up to three APs are permitted to simultaneously transmit on the same channel, when the TrueReuse algorithm determines that they can do this without causing each other co-channel interference.

Zero-latency mobility

In an Extricom Series WLAN, a wireless device remains on the same channel everywhere within the Channel Blanket. Inter-AP hand-off delays or packet loss does not occur as the client moves across the range of different APs.

Wi-Fi Collaboration

The Extricom Series patented Wi-Fi Collaboration technology, in which all APs are able to receive on the same channel, provides uplink path diversity for client transmissions, making the system highly resistant to RF instabilities and outside interference.

Dense AP deployment

In an Extricom Series WLAN, APs can be deployed in any density convenient to the enterprise, to achieve both blanket coverage and a guaranteed communications rate to all users. In fact, while cell-based solutions shy away from dense deployments because of their inherent RF obstacles, the Extricom Series System performance actually increases with AP density.

Wire-line quality VoWLAN

The Extricom Series interference-free architecture is perfectly suited for VoWLAN providing zero latency mobility, voice and data separation, reduced power consumption, and high RF resiliency, all together resulting in superior voice performance.

Frame aggregation

With MAC-layer aggregation, a station with a number of frames to send can combine them into an aggregate frame (MAC MPDU). The resulting frame contains fewer headers in the overhead than would be the case without aggregating, and because fewer, larger frames are sent, the contention time on the wireless medium is reduced.

Block acknowledgment

Block acknowledgment works in conjunction with frame aggregation, allowing the transmitter to request a block acknowledgment for a multiple frame, thus improving overall performance.

Operating modes

Extricom Series products support Legacy, Mixed, and HT Only modes. HT stands for high throughput. HT Only is a mode in which a specific Channel Blanket can be configured so that only 802.11n clients (working in mixed mode) can associate with it. This enables support of co-existence of ‘n’ and ‘b/g’ clients, from the same set of APs, but separated on different channels, so there is no mixed-mode throughput degradation.

Channel bonding

All earlier versions of 802.11 have used 20 MHz wide channels, defined in the 2.4 GHz and 5 GHz bands. 802.11n- Draft 2.0 specifies operation in the same 20 MHz channels used by 802.11b/g in the 2.4 GHz and 802.11a in the 5 GHz bands, but adds a mode in which a full 40 MHz wide channel can be used. This offers approximately twice the throughput of a 20 MHz channel. Extricom Series products support 20 and 40 MHz channels both in 2.4 GHz and 5 GHz.

IEEE 802.11i support

Extricom Series products support WEP-64, WEP-128, WPA-TKIP, WPA2-AES (CCMP) encryption. The authentication modes supported include: RADIUS (802.1x) and WPA Pre Shared Key (PSK).

Power save

Full power-conservation management is enabled for associated mobile devices over unicast, multicast, and broadcast frames. This is based on various IEEE 802.11 standard power-save specifications, such as, PS-Poll and U-APSD for 802.11a/b/g devices, and SM & U-PSMP power save for 802.11n devices.

System redundancy

The Extricom Series System enables full redundancy by connecting two switches in a cascade or hot-standby topology. The switchover parameters are user-configurable.

Dynamic VLAN (Subnet roaming)

Dynamic VLAN enables VLAN and subnet assignments, access-control lists, authentications, QoS levels, and other policies to remain with users over the wired-to-wireless transition, regardless of where the user roams in the network. A tunnel is created for a user that roams to a different VLAN while currently communicating with the original VLAN to enable uninterrupted communication.

Inter-switch hand-off/Fast roaming

The Extricom Series enables mobile voice clients to roam seamlessly by supporting fast hand-offs between multiple APs and switches in the network. This enables the client to roam back to a previously authenticated AP with no delay.

Multiple RADIUS servers & RADIUS server redundancy

The Extricom Series System supports multiple RADIUS servers per Extended Service Set Identifier (ESSID), enabling the user to set redundancy between these RADIUS servers. RADIUS is a common authentication protocol utilized under the 802.1x security standard (often used in wireless networks). It improves the WEP encryption key standard, when used in conjunction with other security methods such as EAP-PEAP. In an enterprise environment, several RADIUS servers may be used for backup and also for serving different geographical locations. Up to four different RADIUS servers can be defined for each ESSID. RADIUS redundancy is based on the assumption that the user database is identical in all RADIUS servers and that users are listed in all servers with the same credentials. Switchover from one RADIUS server to another takes place after consecutive failures of the server. The order of priority is 1 to 4.

Network Time Protocol (NTP)

The Extricom Series System supports synchronization of the system clock over the network, thereby ensuring accurate local time-keeping with reference to radio and atomic clocks located on the Intranet and/or Internet.

Fast Hand-off (Opportunistic Key Caching)

WLAN clients roaming between APs of the same Channel Blanket within a single switch's coverage area experience zero-latency mobility. Clients roaming between different Extricom Series WLAN switches use the standard 802.11 hand-off mechanism, which is further facilitated by the opportunistic key-caching mechanism in the 802.11i standard. In addition to this, the Extricom Series System speeds up 802.11i hand-off between Extricom Series switches by use of Extricom's inter-switch protocol. This permits the client to avoid repetitive 802.1x authentications, thereby enabling faster transition between access points connected to different switches, with minimal session interruption.

Real-time location services

Based on AeroScout or Ekahau technology, Real-Time Location Services (RTLS) technology provides the ability to locate and position mobile wireless network devices (or any user equipment specifically equipped with an AeroScout or Ekahau active RFID tag device) within the Extricom Series wireless network infrastructure. Extricom Series products are enhanced to provide support for RTLS by integration with AeroScout and Ekahau active RFID technology. Generally, device location is determined based on several APs picking up a radio transmission attribute from an AeroScout or Ekahau Tag device or any Wi-Fi client, performing measurements and reporting the measurements to an AeroScout or Ekahau Location Engine. AeroScout and Ekahau positioning algorithms use Received Signal Strength Indicator (RSSI) to determine object location.

Captive Portal

The Captive Portal technique compels any HTTP client to view a special web page (usually for authentication purposes) before accessing the rest of the network. Captive Portal turns a web browser into a secure authentication device. This is done by intercepting an Internet access request and redirecting it to an Extricom local logging web page which may require authentication, or simply display an acceptable use policy and require the user to agree.

MAC authentication

MAC authentication enables the Extricom Series switch to authenticate WLAN devices via RADIUS server even if they have no native support for 802.1x. This mechanism is normally used in "dumb" device WLAN topology (such as barcode readers) in which WLAN client authentication must be managed via a central RADIUS server.

WMM

Wi-Fi Alliance WMM is an 802.11 Quality of Service (QoS) implementation based on a subset of the draft 802.11e standard supplement. The WMM specification provides basic prioritization of data packets based on four categories - voice, video, best effort, and background.

Prioritization is based on the original Carrier Sense Multiple Access/ Collision Avoidance Protocol in the 802.11 standard. In 802.11, the Distributed Coordination Function (DCF) mechanism uses a simple listen-before-talk algorithm to minimize the chance of packet collisions caused by more than one device accessing the wireless medium at the same time. A client must wait for a randomly selected time period and then "listen" to find whether any other device is communicating before starting to transmit. The random back-off period gives all devices a fair opportunity to transmit.

WMM (based on 802.11e standard) enhances the DCF by defining an Enhanced Distributed Channel Access (EDCA). EDCA specifies different fixed and random wait times for the four prioritization categories to provide more favorable network access for applications that are less tolerant of packet delays. Devices that have less time to wait have a better chance of being able to transmit than those that have a longer wait. In order of highest priority, the access prioritization categories are voice, video, best effort and background.

By default, these four WMM prioritization categories are statically mapped to Ethernet 802.1p prioritization tags to allow consistent QoS across wireless and wired network segments. Flow arriving from the wired network tagged with 802.1p priority is mapped to the appropriate Access category, while WMM flow arriving from the wireless medium is encapsulated and tagged with the appropriate 802.1p priority.

The back-off timing for each access category consists of a fixed period called the Arbitrary Inter-Frame Space Number (AIFSN) followed by a random period called the Contention Window (CW), both specified in multiples of the slot time. The CW maintains the DCF random back-off component to help avoid collisions of packets from the same access category. The CW range doubles each time there is a collision (starts CWmin up to CWmax) and is reset to its minimum value after a successful transmission.

EDCA uses a mechanism called a Transmit Opportunity (TXOP) – a bounded time interval during which a station can send as many frames as possible, but the transmission time must not extend beyond the maximum duration of the TXOP. Each priority level is assigned a TXOP, and this mechanism prevents low-speed stations from spending too much time using the media when other clients (including those with traffic in higher priority queues) are waiting.

Another mechanism introduced by WMM is per-access category Acknowledgment policy (Normal or No ACK). Normal means that an acknowledge packet is returned for every packet received. This provides a more reliable transmission, but increases traffic load, which decreases performance. However, one may choose to cancel the acknowledgment by selecting “No ACK” for each access category. This can be useful for voice, for example, where speed of transmission is important, and packet loss is tolerable to a certain degree.

IPv6 support

The Extricom Series Switch family supports IPv6 pass-through. For example, DHCP requests in IPV6 format are passed between the WLAN and the LAN.

Blanket balancing

The switches automatically perform load balancing, distributing the traffic evenly over the different channels.

Low-density parity-check (LDPC)

Extricom Series access points support LDPC which improves reception of packets over a noisy channel.

Space–time block coding (STBC)

Extricom Series access points support STBC which improves the ability to transmit packets over a noisy channel.

Overview of the Switch Platforms

The Extricom Series WLAN switches are connected to Extricom Series APs to form an Extricom WLAN. The Extricom Multi Series (MS) is a high-performance switch hardware platform, and is software-configurable to support a range of wireless and networking functions in an Extricom WLAN System.

The AT-EXMS-1000 is equipped with 2 RJ45/SFP GbE Combo port uplinks and 16 GbE Power over Ethernet (PoE) edge-side ports. The AT-EXMS-1000 is capable of performing different wireless and networking functions, depending on the firmware installed on it. The AT-EXMS-1000 is shown in Figure 4.

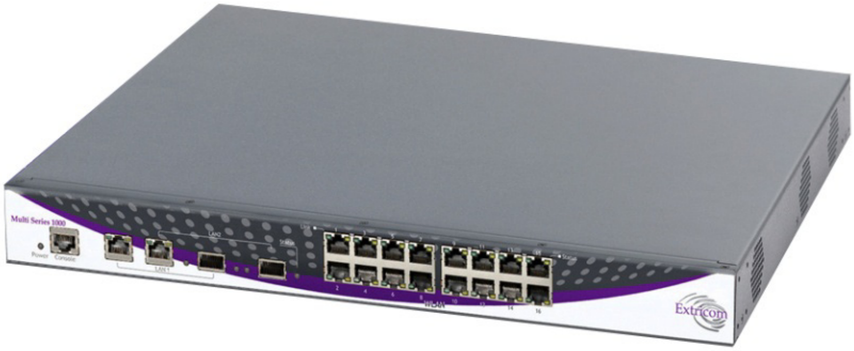


Figure 4. AT-EXMS-1000

The AT-EXLV-2000 is equipped with 2 RJ45/SFP GbE Combo port uplinks and 16 GbE PoE edge-side ports. The AT-EXLV-2000 is specifically designed to provide wireless access in large-venue environments. The AT-EXLV-2000 is shown in Figure 5.

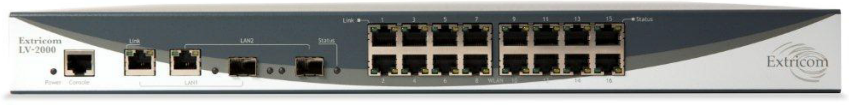


Figure 5. AT-EXLV-2000

The AT-EXLS-3000 is equipped with 2 RJ45/SFP GbE Combo port uplinks and 8 GbE ports to connect AT-EXMS-1000 edge switches. The AT-EXLS-3000 controls up to 8 edge switches to provide a Channel Blanket of up to 128 APs. The AT-EXLS-3000 is shown in Figure 6.

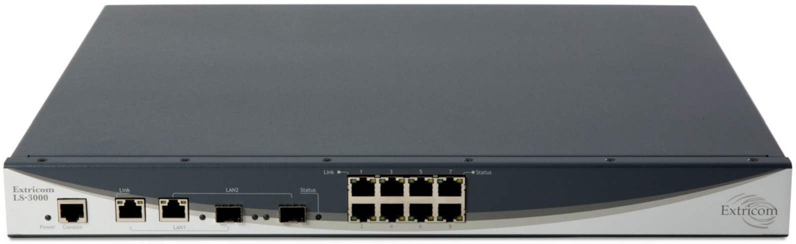


Figure 6. AT-EXLS-3000

The AT-EXMS-500 is equipped with 2 RJ45/SFP GbE Combo port uplinks and 8 GbE PoE edge-side ports. The AT-EXMS-500 is capable of performing different wireless and networking functions, depending on the firmware installed in it. The AT-EXMS-500 is shown in Figure 7.

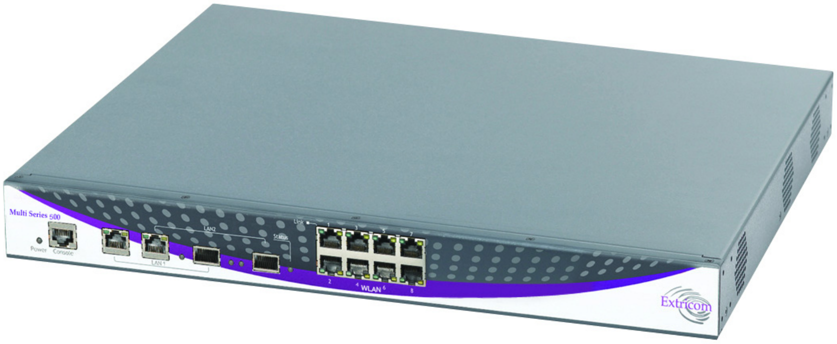


Figure 7. AT-EXMS-500

Configuring a switch and its associated set of APs is as simple as configuring a single traditional AP, greatly reducing the effort required to deploy and maintain the WLAN. Configuration is done via a dedicated, secured web interface that comes standard with every switch.

Note
SFP modules are not shipped with the AT-EXMS-500 or AT-EXMS-1000. To use the SFP ports, you must use Class 1 laser certified SFP modules according to IEC/EN 60825-1 and /or CDRH.

Overview of the Extricom Series Access Points

Access Points with Internal Integrated Antennas

The two-radio AT-EXRP-22n and three-radio AT-EXRP-32n are 802.11n access points with internal antennas for maximum throughput and easy deployment of 802.11n with or without legacy Wi-Fi. The AT-EXRP-22n is equipped with two, and the AT-EXRP-32n - with three, dual-stream radios, each of which can be operated on the 2.4 GHz or 5 GHz band. Each radio has a 2x2 MIMO antenna configuration for an air rate of up to 300 Mbps.

The APs do not require configuration, enabling plug-and-play installation. If stolen, the APs do not pose a security risk, because all encryption is performed in the switch.

With all intelligence residing in the WLAN switch, APs may be placed as close together as necessary to provide high-quality, high-speed connectivity from all locations within the enterprise.

Extricom Series APs are connected to the Extricom Series WLAN Switch via standard Cat5e/6 cables. The APs are powered by the standard 802.3af Power over Ethernet (PoE), and only a single Cat5e/6 cable connection is required to support all radios in an Extricom Series AP.

An AT-EXRE-1000 range extender can be used between the AP and the switch, for extended reach.

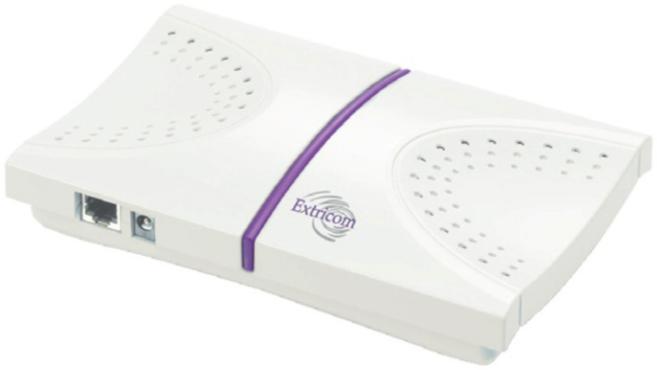


Figure 8. AT-EXRP-22n and AT-EXRP-32n APs

Access Points with Connectors for External Antennas

Some applications may require an access point capable of connecting to external antenna(s): The AT-EXRP-22En accommodates this requirement. The AT-EXRP-22En contains two dual-stream 802.11a/b/g/n radios and four external antenna connectors.

An external antenna may be desired to make the AP less visible by mounting it in the plenum. The situations may arise, in which to ensure connectivity and service levels within a complex coverage environment, directional antennas may be needed, rather than the omni-directional antennas that are standard inside Extricom Series integrated antenna APs. In such cases, the antennas may also be located at some distance from the AP in order to cover a specific area.

The AT-EXRP-22En is shown in Figure 9.

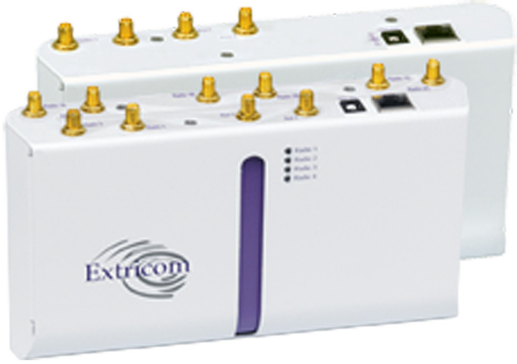


Figure 9. AT-EXRP-22En AP

The AT-EXRP-22En AP is connected to the Extricom Series WLAN Switch via standard Cat5e/6 cables, in exactly the same manner as integrated antenna AP models. The APs are powered by the standard 802.3af Power over Ethernet (PoE), but can be powered by an external power supply if desired.

An antenna with an RP-SMA plug (male) connector can be connected to the AT-EXRP-22En. For purposes of product homologation testing, a “Rubber Duck” type antenna was used, specifically the Netgate 2.4-2.5 / 5.1-5.9 GHz Dual Band Rubber Duck RP-SMA (part number: ANT-2458-5RD-RSP). More specifications on this antenna can be found at **http://www.netgate.com/product_info.php?products_id=386**.

Note
With AT-EXRP-22En: Use only xPVC or similar jacket cable which is NEC Article 725 and 444 Compliant and plenum rated per NFPA 262 (UL 910) standard.

Outdoor Access Points with Connectors for External Antennas

Outdoor applications may require rugged, waterproof access points: The AT-EXRP-32EOn accommodates this requirement. The AT-EXRP-32EOn features a waterproof IP67-rated rugged die-cast aluminum enclosure with N-type connectors for external antennas, ensuring it performs flawlessly in outdoor weather and in harsh indoor conditions. The AT-EXRP-32EOn contains three 802.11a/b/g/n radios. The AT-EXRP-32EOn has six external antenna connectors.

The AT-EXRP-32EOn is shown in Figure 10.

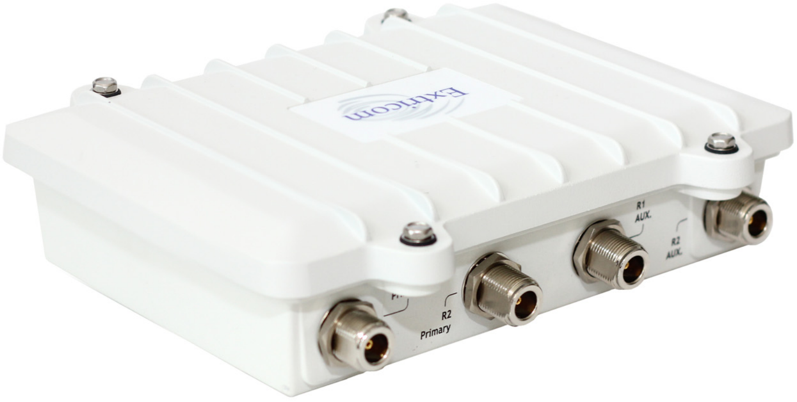


Figure 10. AT-EXRP-32EOn AP

The AT-EXRP-32EOn connects to the Extricom Series WLAN Switch via standard Cat5e/6 cables, in exactly the same manner as integrated antenna AP models. The APs are powered by the standard 802.3af Power over Ethernet (PoE), but can be powered by an external power supply if desired.

An antenna with an N-type plug (male) connector can be connected to the AT-EXRP-32EOn.

A Typical Extricom Series Wireless Network Topology

An Extricom Series WLAN switch is connected to the wired LAN and the APs distributed throughout the enterprise. Figure 11 shows a typical Extricom Series enterprise topology, consisting of an Extricom Series switch and eight APs.

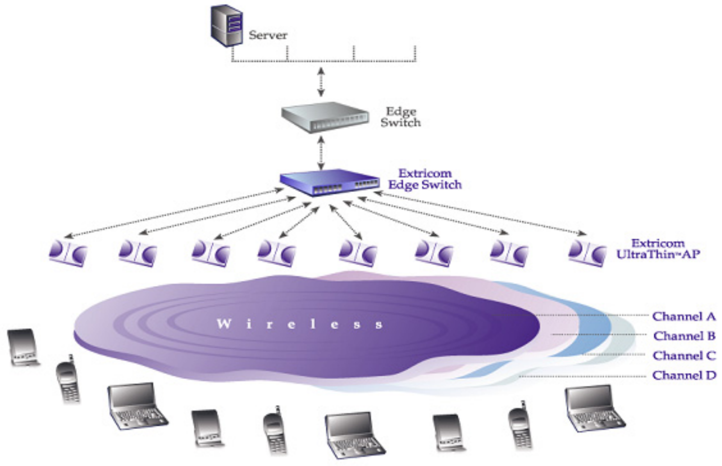


Figure 11. Typical Extricom Series Topology

The Extricom Series uses standard WLAN protocols (IEEE 802.11). As a result, any 802.11a/b/g/n standard wireless device can work seamlessly with the Extricom Series System.

Note
Mixing different types of Extricom Series APs on the same switch is only permitted with the following: AT-EXRP-22n, AT-EXRP-32n, AT-EXRP-22En, and AT-EXRP-32EOn. While these AP configurations are possible, it should be noted that this may result in a heterogeneous wireless coverage between the different Channel Blankets throughout the deployment area.

Note
Extricom Series APs must be directly connected to the switch to function.

Note
An Extricom range extender or media converter may be used between the AP and the switch, when extra range is required.

Switch Cascade

Switch Cascade is an Extricom Series topology in which two AT-EXMS-1000 or AT-EXLV-2000 switches are interconnected together to create one larger logical switch with optional enhanced redundancy capabilities. One AT-EXMS-1000 switch serves as the primary, and the other AT-EXMS-1000 switch serves as the secondary. A diagram of the Cascade topology is shown below, in its standard configuration:

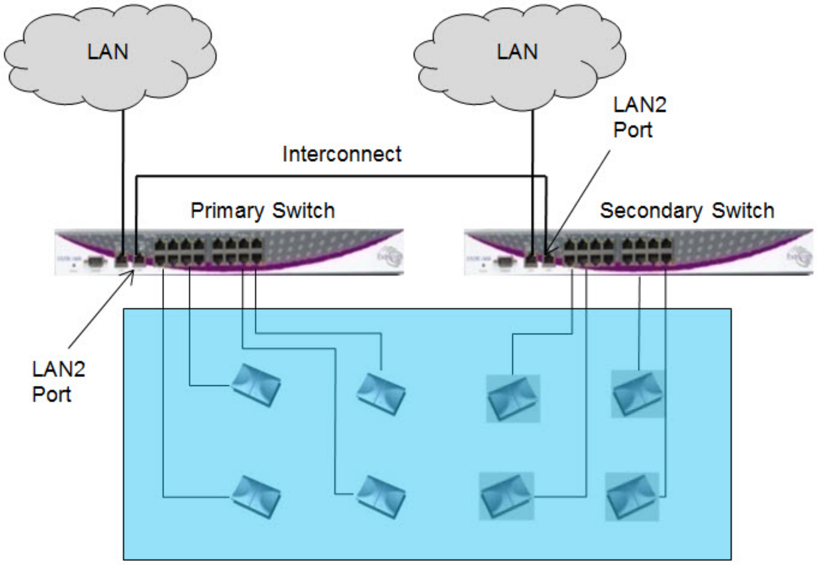


Figure 12. Switch Cascade Topology

The interconnect hardware is connected to the LAN2 port of each switch. Refer to “Connecting the Switch and the Access Points” on page 56 for more details about the interconnect hardware and maximum distance between cascaded switches.

The APs of both switches together form a seamless Channel Blanket. Up to 3 seamless Channel Blankets can be deployed. Up to 32 APs can be deployed in a cascade topology.

In Figure 12 above, a basic Switch Cascade configuration is depicted.

In a switch cascade, the secondary switch routes all of the traffic from its APs to the primary switch over the interconnect cable. The primary switch performs the full set of Extricom edge switch functions on the secondary switch’s traffic, as well as on the traffic from its own APs. It determines to which AP to transmit each incoming packet, while the secondary switch forwards the traffic it receives to the correct AP.

Resiliency in Switch Cascade

Note
Switch Cascade Resiliency applies only to the AT-EXMS-1000 and AT-EXLV-2000 switches.

The optional Resiliency licensed feature provides enhanced redundancy capabilities. Switch Cascade in Resiliency mode can overcome failures in uplink, switches, or the interconnection between the switches. See the following examples:

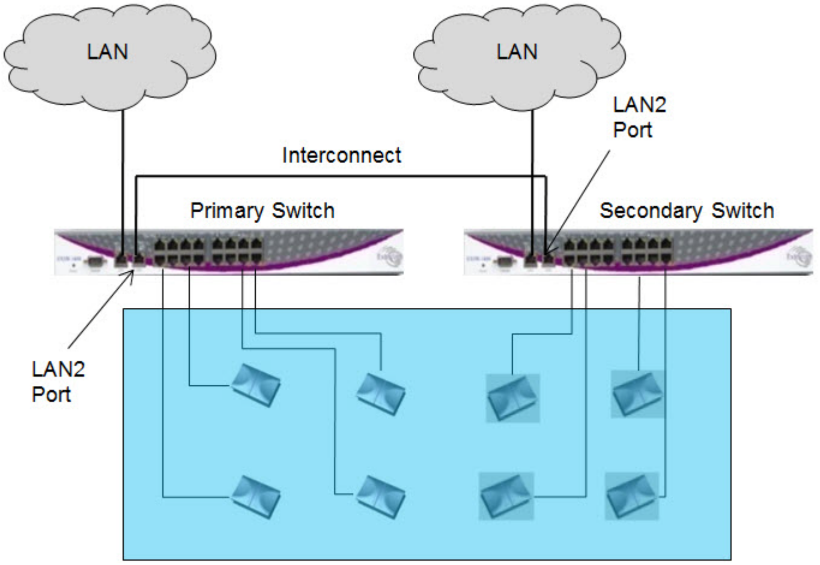


Figure 13. Uplink Redundancy in Switch Cascade Topology

In Figure 13 above, the switch configuration provides uplink redundancy - if the primary switch uplink connectivity is lost for some reason, the secondary switch takes over the primary switch and replaces its functionality with no loss of wireless service. In this configuration, there is no redundancy in the APs' deployment, and each AP covers a specific area uniquely.

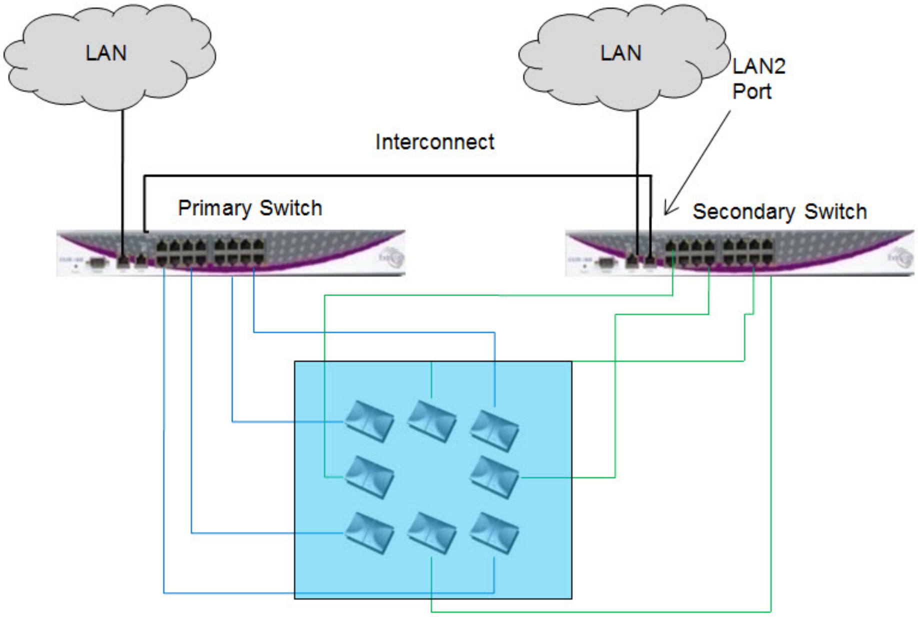


Figure 14. Full Redundancy in Switch Cascade Topology

In Figure 14 above, a full redundancy configuration is shown, where it is possible to deploy APs interleaved, depending on the degree of service robustness required in the event of a failure. In an AP interleaved deployment, APs are deployed as in Figure 14, with one or more APs from the primary switch placed in the coverage area of the secondary switch, and vice versa. Such cross-connect provides necessary redundancy and prevents failure in wireless coverage when one of the switches, primary or secondary, or the interconnect fails. Refer to “Cascade Resiliency” on page 107 for further information.

AT-EXLS-3000

The AT-EXLS-3000 topology consists of two tiers with up to 128 APs connected via 8 edge AT-EXMS-1000 switches to a single AT-EXLS-3000 switch. All 128 APs are interconnected to the AT-EXLS-3000 to create one very large logical switch. A diagram of the AT-EXLS-3000 topology is shown below.

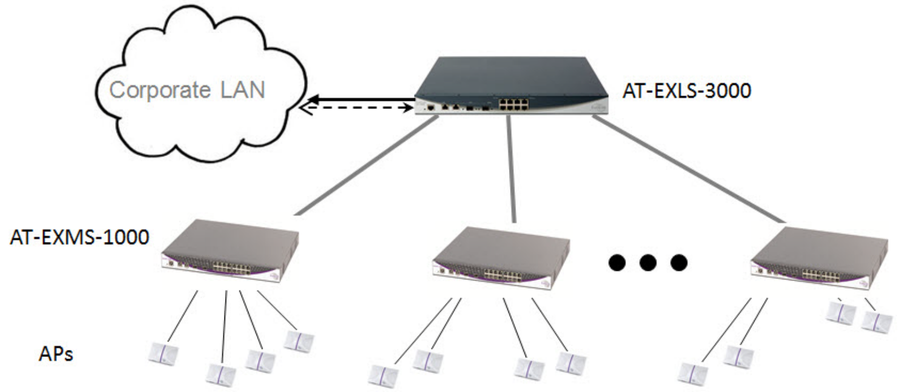


Figure 15. AT-EXLS-3000 Topology

The interconnect hardware is connected to the LAN2 port of each edge switch. Refer to “Connecting the AT-EXLS-3000 Switch” on page 60 for more details about the interconnect hardware and maximum distance between AT-EXLS-3000 and edge switches.

In the AT-EXLS-3000 topology, the edge switches route all of the traffic from their APs to the AT-EXLS-3000 switch over the interconnect cables. The AT-EXLS-3000 switch performs the full set of Extricom switch functions on the edge switches’ traffic. It determines to which AP to transmit each incoming packet, while the edge switches forward the traffic they receive to the correct AP.

Chapter 2

Installation

The installation process is described in the following sections:

- “Reviewing Safety Precautions” on page 40
- “Unpacking the Extricom Series WLAN System” on page 42
- “Additional Equipment” on page 43
- “Determining the Location of the Extricom Series Access Points” on page 44
- “Extricom Series Switches” on page 45
- “AT-EXRP-22n, AT-EXRP-32n, AT-EXRP-22En, AT-EXRP-32EOn Access Points” on page 49
- “Access Point Connectors and LEDs” on page 51
- “Mounting the Switches (Optional)” on page 53
- “Mounting the Access Points (Optional)” on page 54
- “Connecting the Switch and the Access Points” on page 56
- “Connecting the AT-EXLS-3000 Switch” on page 60
- “Range Extenders and Media Converters” on page 62

This chapter provides instructions for unpacking and installing the Extricom Series WLAN System.

Reviewing Safety Precautions

Review the following safety precautions before you begin the installation.

Note
The ☞ indicates that a translation of the safety statement is available in a PDF document titled *Translated Safety Statements* on the Allied Telesis website at **www.alliedtelesis.com/support**.

Follow the instructions in the guide to ensure proper installation and operation of the switch and access points (APs).

Note
The use of wireless devices is subject to the constraints imposed by local laws.

- Operate the switch and APs (apart from AT-EXRP-32EOn) in an indoor environment.
- Disconnect the switch and APs from power sources before servicing.
- The switch and AP enclosure must not be opened by anyone other than an authorized service representative.
- To comply with FCC RF exposure compliance requirements, maintain a minimal separation distance of at least 20 cm (8 inches) between the AP and all persons.
- The power cable included should not be used with any other electrical equipment other than Extricom Series switches.
- The switch contains an internal battery.

⚠ **Warning**
This equipment has been approved for mobile applications where the equipment is to be used at distances greater than 20cm from the human body (with the exception of hands, wrists, feet and ankles). Operation at distances of less than 20 cm is strictly prohibited.

Changes or modification to equipment not expressly approved by Allied Telesis, Inc. is strictly prohibited and could void the user's license to operate the equipment. ☞ **E108**

⚠ **Caution**

Risk of explosion if battery is replaced by an incorrect type. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer’s instructions. 👓 **E22**

⚠ **Caution**

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate this equipment. 👓 **E80**

⚠ **Caution**

A switch reboot will cause a temporary loss of WLAN service until the reboot process is complete. 👓 **E109**

⚠ **Caution**

Once the changes are made, you must click **Save**, then go to System Tools and apply changes as described in the Apply section, in order for them to take effect. The changes will be discarded if the unit is rebooted before the changes are applied. 👓 **E110**

⚠ **Caution**

For security purposes, it is important that all the passwords (including operator and root passwords) be changed from the default values when the switch is first installed, as well as periodically updated. 👓 **E111**

⚠ **Caution**

Record all passwords and store them in a safe location. 👓 **E112**

Unpacking the Extricom Series WLAN System

The Extricom Series WLAN System is shipped depending on the customer order.

- Refer to “Switches” for switch shipping box contents.
- APs are shipped as part of the overall order (APs are shipped in separate boxes, and the number of APs depends on the customer order). Refer to “Access Points” for AP shipping box contents.
- If extra range is required between the AP and switch, an Extricom range extender (100 and 150 meters from the switch) or media converter (over 150 meters from the switch) may be used between the AP and the switch. Refer to “AT-EXRE-1000 Range Extender” for range extender shipping box contents or “AT-EXMC-1000 Media Converter” for media converter shipping box contents.
- The AT-EXLS-3000 switch is also shipped with AT-EXMS-1000 edge switches shipped as part of the overall order (AT-EXMS-1000 edge switches are shipped in separate boxes, and the number of AT-EXMS-1000 edge switches depends on the customer order).

Switches

Extricom Series WLAN switches shipping boxes include the following:

- One switch
- Two 19 inch rack installation brackets
- One cable, Ferrite EMI/RFI
- Four bumpers (feet)
- Eight bracket screws
- One AC power cable

Access Points

Extricom AP shipping boxes include one AP.

AT-EXRE-1000 Range Extender

The AT-EXRE-1000 range extender shipping box includes one AT-EXRE-1000 range extender.

AT-EXMC-1000 Media Converter

The AT-EXMC-1000 media converter shipping box includes the following:

- One AT-EXMC-1000
- One EXPA-48 AC/DC Adapter

Additional Equipment

The following additional equipment is required for installing the Extricom Series WLAN System:

- ❐ One Cat5e/6 cable for each AP.
- ❐ Cat5e/6 cable(s) for connecting the WLAN switch uplink to the LAN switch. A pair of fiber optic pigtails with LC connectors may be used (may be multi-mode or single-mode according to the SFP module in use).
- ❐ A range Extender (AT-EXRE-1000) is required for any AP that will be located between 100 and 150 meters from the WLAN switch.
- ❐ For cabling distances over 150 meters, AT-EXMC-1000 media converters and optical fiber cables must be used.
- ❐ Two stainless-steel pan-head 8 x 1-1/4” self-tapping Phillips screws for wall or ceiling mounting each AP (optional).

Cables for Connecting Two Switches in Switch Cascade

The following additional equipment is required for connecting two AT-EXMS-1000 or two AT-EXLV-2000 switches:

- ❐ One Cat5e/6 cable.
- ❐ A pair of fiber optic pigtails with LC connectors may be used (may be multi-mode or single-mode according to the SFP module in use).

Cable for Connecting the AT-EXLS-3000 to AT-EXMS-1000s

One Cat5e/6 cable is required for connecting the AT-EXLS-3000 to each AT-EXMS-1000 switch.

Determining the Location of the Extricom Series Access Points

Before installing the switch and the APs, create a plan for the placement of the APs. Before permanently mounting the APs, it is recommended to test the network (using a laptop client) to identify potential coverage holes. If such a problem exists, relocate an AP or add more APs to eliminate the holes in the coverage. To find the best location for the required coverage, the Extricom Deployment Tool may be used.

The APs should be placed in a stable, secure location, such as mounted on a wall or ceiling.

The switch should be placed near the distribution point of the LAN line. This is usually in the communications closet of your enterprise.

Extricom Series Switches

The AT-EXMS-1000 and AT-EXLV-2000 switches have 21 connectors (see Figure 16).

The AT-EXLS-3000 switch has 13 connectors (see Figure 17).

The AT-EXMS-500 switch has 13 connectors (see Figure 18 on page 46).

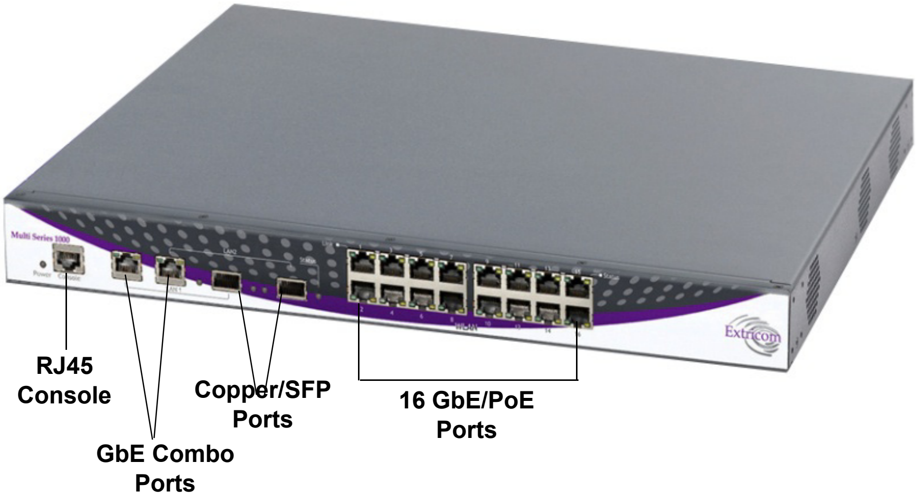


Figure 16. AT-EXMS-1000 and AT-EXLV-2000 Switches

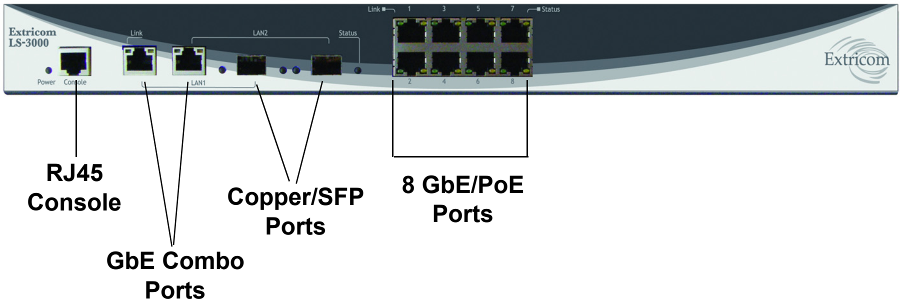


Figure 17. AT-EXLS-3000 Switch

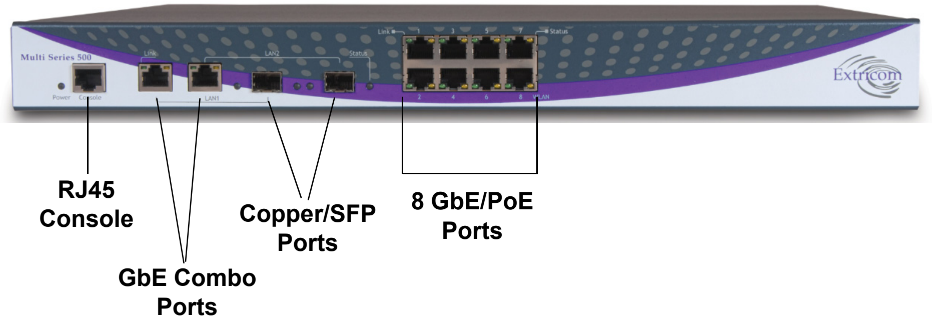


Figure 18. AT-EXMS-500 Switch

Table 3 below describes the front panel and connectors of Extricom Series switches.

Table 3. Extricom Series Switch Connectors

Connectors	Description
Console	Serial connector - only to be used for troubleshooting, support, or maintenance by, or as instructed by, Allied Telesis personnel. Refer to “Troubleshooting” on page 141 for console cable pin-out and serial parameters.
LAN1, LAN2	2 GbE RJ45, 2 GbE SFP combo ports - used to connect the switch to the wired LAN. Use only GbE or SPF. The rules for using the combo port pairs are as follows: ❐ You may use either the twisted pair port or SFP slot of a combo port pair, but not both at the same time. ❐ If you connect both the twisted pair port and SFP slot of a combo port pair to network devices, the SFP slot takes priority, and the twisted pair port is blocked. ❐ The SFP slot becomes active when the SFP transceiver establishes a link to a network device. ❐ The twisted pair port and SFP slot of a combo port pair share the same settings, such as VLAN assignments, access control lists, and spanning tree.

Table 3. Extricom Series Switch Connectors (continued)

Connectors	Description
WLAN Ports	RJ45 connectors - used to connect Extricom Series APs or (in the case of the AT-EXLS-3000) edge switch to the switch. ❐ These ports provide 802.3AF PoE compatible power. ❐ Maximum current: 270 mA, 48 volts. ❐ Do not connect any non-Extricom Series device to the WLAN ports.

Table 4 below describes the front panel LEDs of Extricom Series Switches.

Table 4. Extricom Series Switch LEDs

LED	Color	Description
Power	None	No power
	Green	❐ Blinking - system is loading, final loading phase ❐ Solid On - switch is ready/ operational
	Red	On - loading error or secondary switch not connected
	Red-Orange	Alternating - system is loading, initial loading phase
	Green-Orange	Alternating - the license is not loaded onto the switch
LAN, LAN1, LAN2 Ports		
Act/Link	Green	❐ Solid On - operational connection ❐ Blinking - activity over connection
	Orange	❐ On - LAN connection is operational at 1000 Mbps ❐ Off - LAN connection is operational at 100 Mbps
Status (SFP links)	Green	❐ Solid On - 1000 Mbps full-duplex SFP connection ❐ Off - no SFP connection

Table 4. Extricom Series Switch LEDs (continued)

LED	Color	Description
WLAN Ports		
Link	Green	❐ Solid On - operational connection ❐ Blinking - activity over connection ❐ Off - no connection
Status	Orange	❐ Solid On - LAN connection is operational at 1000 Mbps ❐ Off - LAN connection is operational at 100 Mbps

AT-EXRP-22n, AT-EXRP-32n, AT-EXRP-22En, AT-EXRP-32EOn Access Points

All Extricom Series access points (APs) have two connectors on the front panel of the device: the WLAN connector and the Power connector. The AT-EXRP-22En and AT-EXRP-32EOn have external antenna connectors. The APs have an LED located near the LAN port on the front face of the device. This LED functionality can be enabled or disabled in the web configuration GUI, and when enabled, indicates the status of the AP (refer to the tables which follow for details).

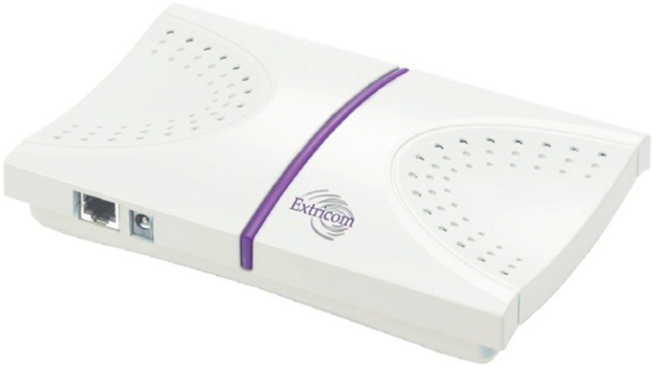


Figure 19. AT-EXRP-22n and AT-EXRP-32n

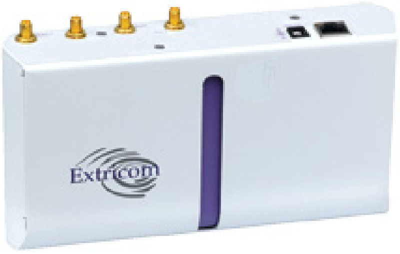


Figure 20. AT-EXRP-22En

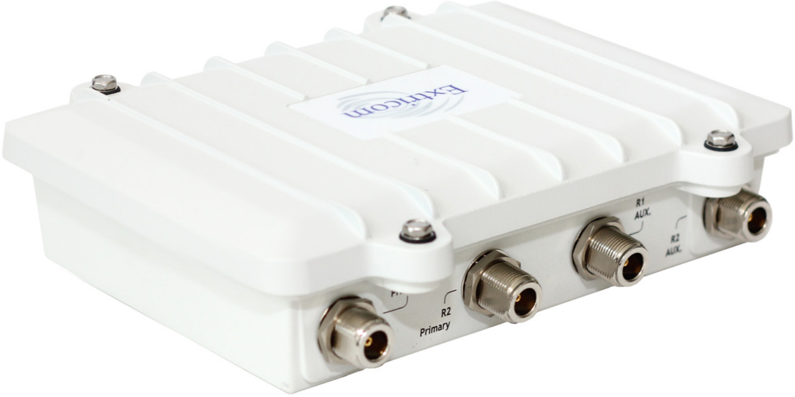


Figure 21. AT-EXRP-32EOn

Access Point Connectors and LEDs

Table 5 and Table 6 below describe the Extricom Series access point connectors and LEDs.

Table 5. Extricom Series AP Connectors

Connectors	Description
Power	Note: External power is not required for most applications. Power is supplied via the Ethernet cable (PoE). In the case of an external power requirement (e.g., when media converters are used, and POE is blocked), use a UL Listed Limited Power Source (LPS) or NEC Class II power adapter. Rating - Input: 90-240VAC, 0.8A max. Output: 48VDC, 0.56A max. The DC output plug of the power supply must be a standard round DC plug with 5.5mm outer-ring diameter and 2.5mm inner-ring diameter. Plug polarity: Outer (-), Inner (+).
WLAN	RJ45 connector – used to connect the Extricom Series AP to the Extricom Series switch. Power is provided by the Extricom Series switch to the AP when directly connected to it.

Table 6. AT-EXRP-22En, AT-EXRP-32n, AT-EXRP-22En, AT-EXRP-32EOn AP LEDs

LED	Color	Description
Left	Green	❒ Blinking - normal system operation ❒ Off - error on one or more radios
Right	Orange	❒ On - error on one or more radios ❒ Off - normal system operation

Note

When LED functionality is disabled, the green LED should still blink for a few seconds when it goes through the initialization process after which both LEDs turn off.

Mounting the Switches (Optional)

Extricom Series WLAN switches can be rack mounted. Two 19 inch rack installation brackets are shipped with the switches. The bracket is shown in Figure 22.

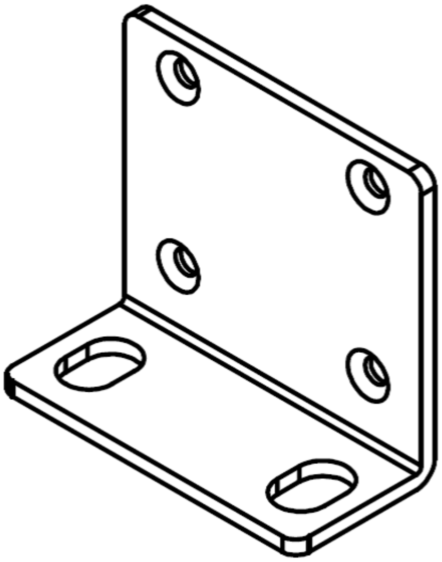


Figure 22. Switch Mounting Bracket

Mounting the Access Points (Optional)

The AT-EXRP-22En and AT-EXRP-32EOn APs can be mounted on a wall or ceiling. For this purpose, a separate mounting bracket is provided for ease of installation. The bracket has two holes for mounting to the wall and one hole for a screw that mounts the AP to the bracket. The mounting bracket is shown in Figure 23.

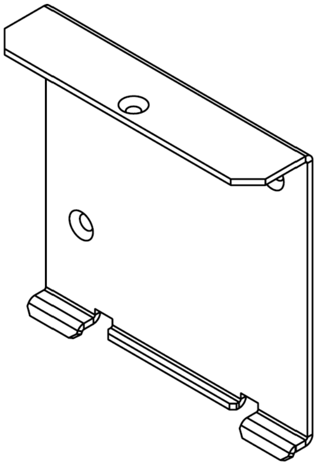


Figure 23. AP Mounting Bracket

The AT-EXRP-22n and AT-EXRP-32n APs can be mounted on a wall or ceiling without additional mounting brackets. To mount these APs, you will need two stainless-steel pan-head 8 x 1-1/4” self-tapping Phillips screws (not supplied).

To mount the AT-EXRP-22n and AT-EXRP-32n APs:

1. Place the installation template on the wall where you want to mount the AP: use the drilling card included with the AP (see Figure 24 on page 55), or refer to Appendix A, “Internal Access Point Mounting Template” on page 155.

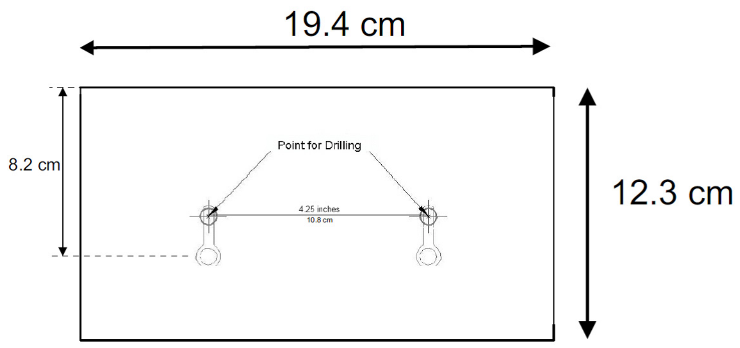


Figure 24. AP Drilling Card

2. Mark the “Point for Drilling” locations on the wall.

3. Screw the two stainless-steel pan-head 8 x 1-1/4” self-tapping Phillips screws into the wall, leaving enough of the screws protruding to enable you to hook the AP over the screws.

4. Align the holes on the back of the AP with the screws and slip the AP into place.

Connecting the Switch and the Access Points

The Extricom Series switch is connected to the wired LAN and to the APs that are located throughout the enterprise.

To connect a switch and access points:

1. Using a Cat5e/6 100/1000Mbps cable, connect the RJ45 LAN1 connector located on the front panel of the switch (refer to Figure 16 on page 45) to the LAN switch.

2. Using a Cat5e/6 cable, connect each AP to one of the switch's RJ45 WLAN connectors.

Note
If an AP must be located over 100 meters from the switch, an Extricom range extender must be used, which allows up to an additional 50m, for a total switch-to-AP distance of up to 150m.

Switch-to-AP distances of up to 400 meters can be supported on GbE connections by using Extricom AT-EXMC-1000 media converters.

3. Connect the power cable to the power connector located on the rear panel of the switch and plug the other end of the power cable into a power source.

4. Verify that the Power LED on the switch is green.

Note
Additional APs can be connected or disconnected while the switch is active.

Note
If using fiber media converters (ATI/100Mbps, CTC/1000Mbps) to extend switch-to-AP distance:

The switch-side media converter is powered via PoE from the WLAN switch or optional external power supply.

Once all cables are connected (switch – copper – converter – fiber – converter – copper – AP), perform a port power down/up in the web GUI of the switch to renew switch awareness of the AP connection.

Fiber mode is Multi for 100Mbps.

Fiber mode can be Multi or Single for 1000Mbps per the SFP module selected. Both ends of the fiber termination must be in the same (SFP) mode.

To connect a switch cascade (AT-EXMS-1000 and AT-EXLV-2000):

1. Connect the primary and secondary switch to the LAN (via the LAN1 port) and to its APs (via WLAN ports), as directed in "To connect a switch and access points:" on page 56.

2. Verify that both switches are running the same firmware release, and that this is the newest release that supports Switch Cascade.

3. Refer to "Switch interconnect guidelines" for important switch interconnect guidelines.

4. Connect the switch interconnect cable to the LAN2 port of the primary switch and to the LAN2 port of the secondary switch.

The secondary switch remains inactive until it is synchronized with the primary switch. When the primary switch is rebooted, its configuration GUI will be in read-only mode, until the secondary switch is synchronized.

Switch interconnect guidelines

The maximum length, in meters, of the primary-to-secondary (AT-EXLS-3000-to-AT-EXMS-1000) switch interconnect is computed according to the following tables:

If using Cat5e/6 100/1000Mbps cable, refer to Table 7:

Table 7. Cat5e/6 100/1000Mbps Cable

Distance Between Secondary Switch and Its Farthest AP	**Max. Switch Interconnect Distance (Copper Interconnect Cable)**
150 (with EXRE)	50

Note
Beyond 100 m, copper-based cables require a range extender (EXRE).

If using fiber media cable, refer to Table 8:

Table 8. Fiber Media cable

Distance Between Secondary Switch and Its Farthest AP*	**Max. Switch Interconnect Distance (Fiber Interconnect Cable)**
400 (with EXMC)	50
50 (with EXRE)	450
*The total length of the copper-based cable to/from EXMC must be less than 2m.	

If using mixed media types, refer to Table 9 and Table 10 on page 59:

Table 9. Mixed Media Types

Distance Between Secondary Switch and Its Farthest AP (Copper Cable)	**Max. Switch Interconnect Distance (Fiber Interconnect Cable)**
100	400
150 (with EXRE)	300

Table 10. Mixed Media Types

Distance Between Secondary Switch and Its Farthest AP (Fiber Cable) *	Max. Switch Interconnect Distance (Copper Interconnect Cable)
400 (with EXMC)	50

*The total length of the copper-based cable to/from EXMC must be less than 2m.

Note
EXMC and EXRE are not to be used with uplink ports, for example, in the case of interconnect.

Connecting the AT-EXLS-3000 Switch

The AT-EXLS-3000 Switch is designed to greatly increase the coverage area of the Extricom Series solution. The Large Scale solution is a/b/g/n Wi-Fi-compliant.

The Extricom Large Scale (LS) switch is typically connected to the wired LAN and to between 4 and 8 edge switch devices. Each edge switch connects up to 16 APs that are located throughout the enterprise.

The Extricom Large Scale switch (AT-EXLS-3000) attaches to the network via the IEEE802.3ad link aggregation ports. Network configuration details such as security profile, SSIDs, assigned channels to blankets, VLAN assignments, are maintained in the AT-EXLS-3000 switch, not by the edge switches.

To connect an AT-EXLS-3000 switch to the edge switches and access points:

1. Using a Cat5e/6 100/1000Mbps cable, connect the RJ45 LAN1 connector located on the front panel of the switch to the LAN switch.
2. Using a Cat5e/6 100/1000Mbps cable, connect the RJ45 LAN1 connector located on the front panel of each edge switch to one of the AT-EXLS-3000 switch's RJ45 WLAN connectors.
3. Using a Cat5e/6 cable, connect each AP (see Figure 16 on page 45) to one of the edge switch's RJ45 WLAN connectors.

Note
If an AP must be located over 100 meters from the switch, an Extricom range extender must be used, which allows up to an additional 50m, for a total switch-to-AP distance of up to 150m.

Note
AP distances of up to 400m can be supported on GbE connections by using Extricom AT-EXMC-1000 media converters.

4. Connect the power cable to the power connector located on the rear panel of the AT-EXLS-3000 switch and plug the other end of the power cable into a power source.
5. Connect the power cables to the power connectors located on the rear panel of the edge switches and plug the other end of the power cables into a power source.

6. Verify that the Power LEDs on all the switches are green.

Note
Additional APs can be connected or disconnected while the switch is active.

If using fiber media converters (ATI/100Mbps, CTC/1000Mbps) to extend switch-to-AP distance:

- ❒ The switch-side media converter is powered via PoE from the WLAN switch or optional external power supply.
- ❒ Once all cables are connected (switch – copper – converter – fiber – converter – copper – AP), perform a port power down/up in the web GUI of the switch to renew switch awareness of the AP connection.
- ❒ Fiber mode is Multi for 100Mbps.
- ❒ Fiber mode can be Multi or Single for 1000Mbps per the SFP module selected. Both ends of the fiber termination must be in the same (SFP) mode.

Primary-to-secondary switch interconnect computation

Refer to "Switch interconnect guidelines" on page 57 for the maximum length, in meters, of the primary-to-secondary switch interconnect computation.

To connect an AT-EXLS-3000 pair for redundancy:

1. Verify that both switches are running the same firmware release and that it is the newest release that supports Resiliency.

2. Verify both switches have a valid AT-EXLS-3000 Redundancy license.

3. Connect the interconnect cable to the LAN2 port of the AT-EXLS-3000 primary switch and to the LAN2 port of the AT-EXLS-3000 secondary switch.

4. A direct cable connection between a redundant AT-EXLS-3000 pair is not mandatory: Any L2 or L3 connection is sufficient as long as each one of the switches can ping a common reference IP address.

Range Extenders and Media Converters

AT-EXRE-1000 Range Extender

The AT-EXRE-1000 Power Over Ethernet Gigabit (PoE) range extender doubles the standard range of PoE, from the baseline 100 meters to a full 150 meters, all while enabling full gigabit speed. It can be used both as a standalone product, to extend the reach of PoE installations, and as a complement to the Extricom Series WLAN System.

When used in WLAN implementations, the AT-EXRE-1000 enables any Extricom UltraThin™ AP to be connected using standard Cat5e/6 cable up to 150 meters from the Extricom Series WLAN Switch. The range extender sits in-line on the Ethernet cable and does not require an external power feed. The range extender receives its power from the original PoE injector in the switch or from a PoE injector/power supply, while it simultaneously injects PoE to the extended cable segment.

AT-EXMC-1000 Media Converter

The AT-EXMC-1000 media converter allows users to extend the size of their WLAN with the use of fiber cabling. The AT-EXMC-1000 functions as a GbE range extender, providing fiber connectivity to Extricom Series access points and Extricom Series WLAN switches at distances of up to 400 meters, assuming that the switches and the APs are GbE-enabled. The AT-EXMC-1000 can be installed in any implementation and is connected to the WLAN switch, edge switch, or AP with Cat-5e/6 cable through a standard RJ45 port.

The AT-EXMC-1000 provides an extended level of deployment flexibility for large-scale Channel Blanket deployments, because it does not need the power infrastructure normally required for fiber deployments. The switch-side media converter is powered via PoE from the WLAN switch or optional external power supply; the AP-side media converter is powered via external power supply and provides PoE to the AP. Effectively, a 400-meter fiber run to an AP will require only a single power supply.

Chapter 3

Configuring Extricom Series WLAN System

This chapter contains the following sections:

- “Accessing the Extricom Series Switch GUI” on page 64
- “Using the Extricom Series Web Configuration Pages” on page 66
- “Overview of the Configuration” on page 68
- “Configuring LAN Parameters” on page 70
- “Configuring WLAN Settings” on page 72
- “Access Points” on page 96
- “System Tools Configuration” on page 99
- “Advanced Configuration” on page 107
- “Viewing Events and Reports” on page 123

This chapter provides instructions for configuring the Extricom Series WLAN System.

Accessing the Extricom Series Switch GUI

After connecting the switch and APs, configure the Extricom Series WLAN System through the Extricom Series web configuration GUI using a terminal or PC connected to the same LAN as the switch.

To access the Extricom Series web-based configuration tool:

1. In your web browser, enter the following: `https://<IP address of the switch>`

   where `<IP address of the switch>` is the IP address of the switch provided with your purchase. Note that https must be used, not http, in order to initiate a secure browsing session (SSL) with the switch.

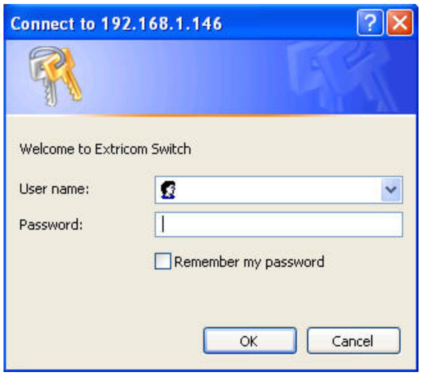
   Note
   Prior to opening the configuration tool, make sure your console PC is configured with an IP address in the same subnet as the switch.

   Note
   If you did not receive a switch IP address with the switch, the factory default value for the switch IP address is 192.168.1.254.

   Note
   If you are using the default IP settings, do not place a router between the user PC and the switch.

2. On the first login, you will receive a notice in your browser that there is a problem with the website’s security certificate. Click on **Continue to this website (not recommended)**.

3. The Login page appears, as shown in Figure 25 on page 65:



Connect to 192.168.1.146

Welcome to Extricom Switch

Figure 25. Login Page

4. Enter the user name and password of the system integrator and click **OK**. The Summary page appears.

Note
If you did not receive a user name and password with your switch, use the following factory default user name and password:

user name: admin
password: Switch1

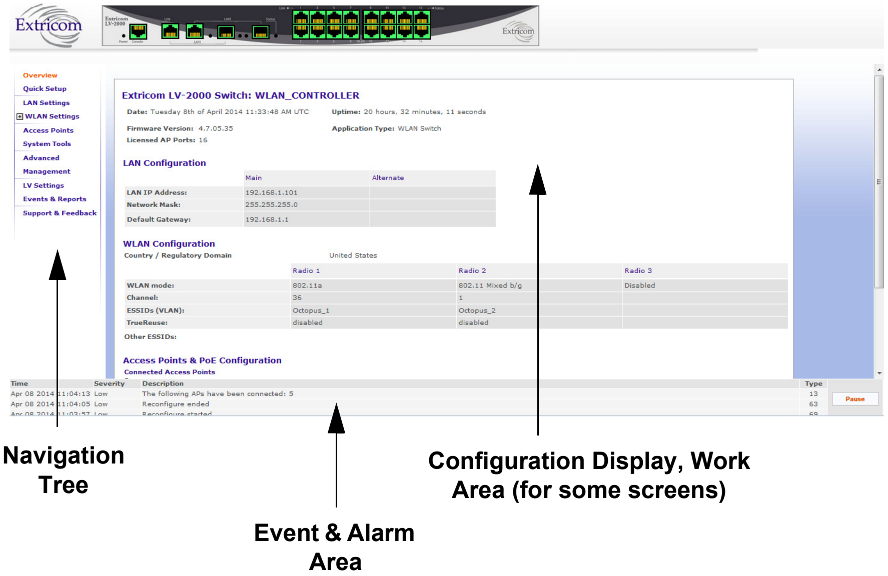
The user name and password are case-sensitive.

Note
If you use Internet Explorer 8 web browser to configure the switch, you will receive a notice in a pop-up window stating that there is a problem with the website’s security certificate: Press the tab key on your keyboard until you see the link **Continue to this website (not recommended)**, then click on it.

Using the Extricom Series Web Configuration Pages

The Extricom Series Web Configuration pages have four main areas:

- Switch image – The Extricom Series Web configuration page displays an image of the configured switch at the top of the page; the image shows dynamic status of the PoE of each AP port (gray = PoE off, green = PoE on).
- Navigation tree.
- Configuration display and editable work area (for some screens).
- Event and alarm area.



Extricom LV-2000 Switch: WLAN_CONTROLLER

Date: Tuesday 8th of April 2014 11:33:48 AM UTC **Uptime:** 20 hours, 32 minutes, 11 seconds

Firmware Version: 4.7.05.35 **Application Type:** WLAN Switch

Licensed AP Ports: 16

LAN Configuration

	Main	Alternate
LAN IP Address:	192.168.1.101	
Network Mask:	255.255.255.0	
Default Gateway:	192.168.1.1	

WLAN Configuration

Country / Regulatory Domain United States

	Radio 1	Radio 2	Radio 3
WLAN mode:	802.11a	802.11 Mixed b/g	Disabled
Channel:	36	1	
ESSIDs (VLAN):	Octopus_1	Octopus_2	
TrueReuse:	disabled	disabled	

Other ESSIDs:

Access Points & PoE Configuration

Connected Access Points

Time	Severity	Description	Type
Apr 08 2014 11:04:13	Low	The following APs have been connected: 5	13
Apr 08 2014 11:04:05	Low	Reconfigure ended	63
Apr 08 2014 11:03:57	Low	Reconfigure started	69

Figure 26. Typical Web Configuration Page

The navigation tree provides access to the Overview display, as well as the following Extricom Series Web configuration pages:

- Quick Setup – wizard used to quickly set up a basic switch configuration.
- LAN Settings – configure LAN parameters.
- WLAN Settings – configure WLAN parameters including ESSID-related configuration and Radio configuration.
- Access Points – view ports in use and activate/deactivate PoE.
- System tools – configure general system parameters such as passwords, time & date, firmware upgrade.
- Advanced – configure advanced features such as redundancy, TrueReuse, 802.11d, IDS, and SNMP.

- Management – configure the switch to be managed by the CloudBlanket NMS.
- LV Settings – only available on the AT-EXLV-2000. Configure additional features related to large venues.
- Events & Reports – view system events and performance reports.
- Support & Feedback.

The work area displays the configuration settings corresponding to the category selected in the navigation tree. Use this area to configure Extricom system parameters, where applicable. Web configuration pages may include a **Save** button; when this is selected, the configuration changes are applied to the off-line configuration file. If you wish to apply these parameters, click **Apply** in the System Tools configuration section; this starts the reconfiguration process.

Note
If you do not select **Apply** (in the System Tools configuration section) after clicking **Save**, the configuration change will not take effect.

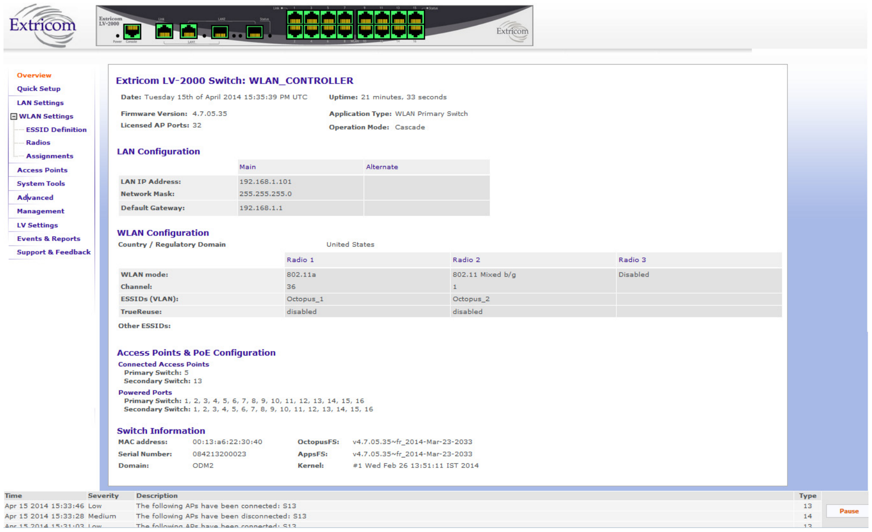
Note
If you change the IP address of the switch, and the new IP address is accessible from your computer, you will not lose the connection session. If however, the new IP address is on a different subnet which is inaccessible from your computer, the connection session will be lost. In this case, you will have to configure your PC with a new IP address that is in the same subnet as the switch and start a new https session.

The Event and Alarm area displays real-time SNMP trap messages. You can pause the traps by selecting **Pause**.

Please see "Northbound SNMP Traps" on page 145 for more details.

Overview of the Configuration

The Overview page, shown in Figure 27, provides a summary of the current configuration. To get to it, click **Overview** in the navigation tree.



Extricom LV-2000 Switch: WLAN_CONTROLLER

Date: Tuesday 15th of April 2014 15:35:39 PM UTC
Uptime: 21 minutes, 33 seconds
Firmware Version: 4.7.05.35
Licensed AP Ports: 32
Application Type: WLAN Primary Switch
Operation Mode: Cascade

LAN Configuration

	Main	Alternate
LAN IP Address:	192.168.1.101	
Network Mask:	255.255.255.0	
Default Gateway:	192.168.1.1	

WLAN Configuration

Country / Regulatory Domain United States

	Radio 1	Radio 2	Radio 3
WLAN mode:	802.11a	802.11 Mixed b/g	Disabled
Channel:	36	1	
ESSIDs (VLAN):	Octopus_1	Octopus_2	
TrueReuse:	disabled	disabled	

Other ESSIDs:

Access Points & PoE Configuration

Connected Access Points
Primary Switch: 5
Secondary Switch: 13

Powered Ports
Primary Switch: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16
Secondary Switch: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16

Switch Information

MAC address:	00:13:a6:22:30:40	**OctopusFS:**	v4.7.05.35~fr_2014-Mar-23-2033
Serial Number:	084213200023	**AppsFS:**	v4.7.05.35~fr_2014-Mar-23-2033
Domain:	ODM2	**Kernel:**	#1 Wed Feb 26 13:51:11 IST 2014

Time	Severity	Description	Type
Apr 15 2014 15:33:46	Low	The following APs have been connected: S13	13
Apr 15 2014 15:33:28	Medium	The following APs have been disconnected: S13	14
Apr 15 2014 15:31:03	Low	The following APs have been connected: S13	13

Figure 27. Configuration Overview of AT-EXLV-2000

Table 11 provides a summary of the Overview page.

Table 11. Overview Page

Field	Description
Date	Displays the date and time the summary was created
Uptime	Displays the amount of time the switch has been up since the last reboot
Firmware Version	Displays the firmware version number installed
Licensed AP ports	Displays the number of licensed ports configured
Application Type	Displays one of the switch configuration options: ❐ WLAN Switch ❐ WLAN Secondary Switch ❐ WLAN Primary Switch

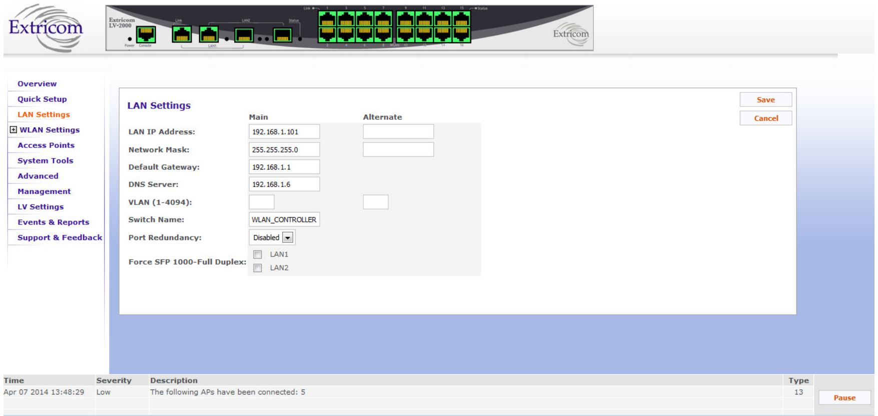
Table 11. Overview Page (continued)

Field	Description
LAN Configuration	
Main	IP address of the switch
	Network mask
	IP address of the default gateway
WLAN Configuration	
Country/ Regulatory Domain	Displays the regulatory domain name currently in use by the switch
WLAN mode	Displays the WLAN mode for each radio (Disabled, 802.11a, 802.11b, 802.11g, 802.11b/g, 802.11n/a, 802.11n/g, 802.11n/b/g, or Rogue)
Channel	Displays the channel for each radio
ESSIDs (VLAN)	Displays the ESSIDs and their related VLANs, defined and assigned to each radio
TrueReuse	Shows whether TrueReuse is enabled or disabled for each radio
Other ESSIDs	Displays other ESSIDs that are defined, but are not assigned to any specific radio
Access Points & PoE Configuration	
Connected Access Points	List of the active APs
Powered Ports	List of WLAN ports that have PoE enabled
Switch Information	
MAC address	Displays the base MAC address of the switch
Serial Number	Displays a unique serial number of the switch
Domain	RF localization indication
OctopusFS	Extricom Series firmware application version and build date
AppsFS	Third-party software application version and build date
Kernel	Extricom Series-specific Linux kernel build date

Configuring LAN Parameters

To configure LAN parameters:

1. Click **LAN Settings** in the navigation tree. The LAN Settings page appears (see Figure 28).



LAN Settings

	Main	Alternate
LAN IP Address:	192.168.1.101	
Network Mask:	255.255.255.0	
Default Gateway:	192.168.1.1	
DNS Server:	192.168.1.6	
VLAN (1-4094):		
Switch Name:	WLAN_CONTROLLER	
Port Redundancy:	Disabled	
Force SFP 1000-Full Duplex:	□ LAN1 □ LAN2	

Time	Severity	Description	Type
Apr 07 2014 13:48:29	Low	The following APs have been connected: 5	13

Figure 28. LAN Settings Page

2. Configure the LAN parameters. Refer to Table 12 for a description of the LAN parameters.

Table 12. LAN Configuration Parameters

Field	Description
LAN IP Address	LAN IP address used for the switch management. You may add an alternate IP address if you wish to manage the switch from a different network. In that case, enter the value in the Alternate field.
Network Mask	Network mask for the LAN 1 IP address. You may also add an alternate network mask in the Alternate field for the alternate IP address defined.
Edge’s Subnet	Subnet of a redundant pair (Primary - Secondary or Main - Standby). Only appears if the switch is defined as a part of a redundant pair, i.e., in a cascade configuration.
Default Gateway	IP address of the default gateway.
DNS server	IP address of the DNS server.

Table 12. LAN Configuration Parameters (continued)

Field	Description
VLAN	Tag ID for the VLAN used for the switch management. You may add two VLAN tag IDs: one for the LAN 1 IP address in the Main field, and an alternate one for the alternate IP address, using the Alternate field.
Switch Name	Alphanumeric descriptor of the switch. Maximum length is 64 characters.
Port Redundancy	Drop-down menu with the following options: ❒ Disabled ❒ Enabled When enabled, the GbE RJ45/SFP combo ports function as a redundant pair, consisting of the primary SFP port and the secondary RJ45 port. During normal operation, only the primary port is active. If a failure occurs on the primary port, the secondary port becomes active and remains active, even when the primary port recovers. If failures occur on both ports, the first port that recovers becomes the active port.
Force SFP 1000-Full Duplex	When using an SFP to connect to the LAN, you might need to force the link to 1000 full duplex to work with certain LAN switches.

3. Click Save to save the configuration.

Note
IMPORTANT! The changes made to the configuration will be lost if you do not click **Apply** in the System Tools configuration section after clicking **Save** on one or several configuration pages. Refer to “Reboot” on page 99.

Configuring WLAN Settings

The WLAN Settings section is subdivided into three menu subsections:

- ❒ ESSID Definition – refer to “Configuring ESSID Definition” on page 72.
- ❒ Radios – refer to “Configuring WLAN Radios” on page 88.
- ❒ Assignments – refer to “ESSID Assignment” on page 95.

Configuring ESSID Definition

An Extended Service Set Identifier (ESSID) is a name of a network, which is defined by a set of privileges, settings, and limitations (such as security definitions, access privileges, VLAN assignments). Each wireless device must connect to a specific ESSID. Each channel can support multiple ESSIDs, thus creating “virtual” networks on the same channel.

The following is the data structure used by the Extricom Series systems:

- ❒ Each radio is assigned one channel.
- ❒ Each channel can support up to 8 different ESSIDs.

Note
Up to 7 ESSIDs are allowed on channel 1, and up to 8 ESSIDs are allowed on each of the remaining channels.

- ❒ Each ESSID can be associated with a VLAN tag.
- ❒ The same ESSID name can be repeated for different channels.

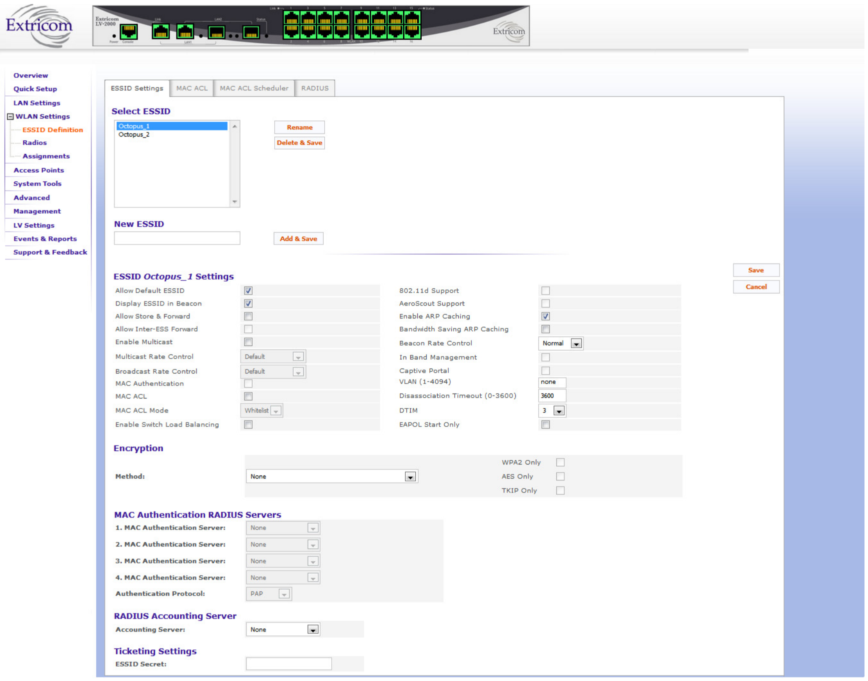
In the ESSID web page, there are the following four configuration tabs:

- ❒ ESSID Settings
- ❒ MAC ACL
- ❒ MAC ACL Scheduler
- ❒ RADIUS

ESSID Settings

Click **ESSID Definitions** in the navigation tree. The ESSID Settings page appears (see Figure 29 on page 73).

Under this tab you may add a new ESSID, as well as rename or delete an existing ESSID. You can configure ESSID parameters; refer to Table 13 on page 73 for a description of the available parameters.



Select ESSID

Octopus_1
Octopus_2

New ESSID

ESSID *Octopus_1* Settings

Allow Default ESSID	☑	802.11d Support	□
Display ESSID in Beacon	☑	AeroScout Support	□
Allow Store & Forward	□	Enable ARP Caching	☑
Allow Inter-ESS Forward	□	Bandwidth Saving ARP Caching	□
Enable Multicast	□	Beacon Rate Control	Normal
Multicast Rate Control	Default	In Band Management	□
Broadcast Rate Control	Default	Captive Portal	□
MAC Authentication	□	VLAN (1-4094)	none
MAC ACL	□	Disassociation Timeout (0-3600)	3600
MAC ACL Mode	Whitelist	DTIM	3
Enable Switch Load Balancing	□	EAPOL Start Only	□

Encryption

Method: None

WPA2 Only □
AES Only □
TKIP Only □

MAC Authentication RADIUS Servers

1. MAC Authentication Server: None
2. MAC Authentication Server: None
3. MAC Authentication Server: None
4. MAC Authentication Server: None
Authentication Protocol: PAP

RADIUS Accounting Server

Accounting Server: None

Ticketing Settings

ESSID Secret:

Figure 29. WLAN ESSID Definition Page - ESSID Settings Tab

Table 13. ESSID Parameter Descriptions

Field	Description
ESSID	
Select ESSID	Select an ESSID from the list. Once selected (highlighted), you may add or rename it by clicking on either the **Rename** or the **Delete & Save** button on the right.
New ESSID	Type in the new ESSID name string and click on the **Add & Save** button on the right.
ESSID <ESSID name> Settings	
Allow Default ESSID	If this option is enabled, a wireless device will be allowed to connect to the Extricom Series WLAN without requesting a specific ESSID (i.e., “default” or “any” ESSID). If this option is disabled, a wireless device must connect to a specific ESSID in the Extricom Series WLAN.

Table 13. ESSID Parameter Descriptions (continued)

Field	Description
Display ESSID in Beacon	This option provides an additional (though limited) level of security. The AP sends out a beacon with information about the network. If this option is enabled, the ESSID appears in the beacon. If disabled, the ESSID does not appear in the beacon.
Allow Store & Forward	If this option is enabled, two wireless devices connected to the Extricom Series WLAN with the same ESSID can communicate and transfer data to each other. Traffic between wireless devices will not be forwarded to the LAN switch. If this option is disabled, all traffic goes through the LAN switch. This could be used by IT managers to apply security settings or various policies on the LAN network. Note: Disabling Allow Store & Forward disables the Allow Inter-ESS Forward option.
Allow Inter-ESS Forward	If this option is enabled, two wireless devices connected to the Extricom Series WLAN with different ESSIDs will be able to communicate with each other without going through a router. Traffic between wireless devices will not be forwarded to the LAN switch. ❒ This option must be enabled on both ESSIDs. ❒ In order for wireless devices, associated to different ESSIDs, to be able to communicate with each other, the ESSIDs must be defined on the same VLAN (or no VLAN). If this option is disabled, all traffic goes through the LAN switch. This could be used by IT managers to apply security settings or various policies on the LAN network.

Table 13. ESSID Parameter Descriptions (continued)

Field	Description
Multicast Rate Control	This option, when enabled, provides support of multicast and broadcast packets for the selected ESSID. Multicast and/or broadcast packets shall be transmitted from all APs. Once this feature is enabled, Multicast Rate Control and Broadcast Rate Control may be left as default, or changed to Rate Optimized or Range Optimized. ❒ If **Rate Optimized** is selected, multicast packets are sent using the highest enabled data rate in legacy (MCS7 in High Throughput (HT) mode). ❒ If **Range Optimized** is selected, multicast packets are sent using the lowest enabled data rate in legacy (MCS3 in HT mode).
MAC Authentication	Select this option if you wish to impose MAC authentication on this ESSID. MAC authentication enables a user to authenticate WLAN clients using RADIUS server, even if they do not support 802.1 x authentications. Note that when using this option, the security setting does not allow you to select any 802.1x methods. (To enable this option go to the Advanced → Others tab.)
MAC ACL	This option, when enabled, allows a user to add a MAC access list to the specific ESSID. Only clients with a MAC address included in this list are allowed to access the network if the MAC ACL mode is set to Whitelist. Conversely, if the MAC ACL mode is set to Blacklist, then these clients are not allowed to use the network. (Use the MAC ACL tab on this page to add MAC ACL lists.)
Enable Switch Load Balancing	Enables or disables load balancing of the switch. Refer to “Switch Load Balancing” on page 139 for configuration information of this feature.

Table 13. ESSID Parameter Descriptions (continued)

Field	Description
802.11d Support	Enables support of the 802.11d standard. The purpose of this standard is to provide regulation domains for each country in a predefined list. The regulation domains and country information are provided as part of the Beacons & Probe response. To use this feature, 802.11d support per ESSID must first be enabled (under the Others tab on the Advanced page).
AeroScout Support	Enables support for AeroScout location services. To use this feature, AeroScout support must be enabled in the Location-Based Service tab on the Advanced page.
Enable ARP Caching	This option, when enabled, provides an immediate response to ARP requests directed towards WLAN stations associated with the selected ESSID. The switch answers on behalf of the WLAN stations. Note: ARP Caching is enabled by default.
Bandwidth Saving ARP Caching	Reduces the number of ARP packets sent over the wireless medium.
Beacon Rate Control	Use this option if you wish to tune the beacon distribution mechanism. You can tune the system to provide customized beacon coverage. The higher the rate, the more beacons shall be distributed on this SSID. Select one of the five rates available in the drop-down menu: ❒ Basic: 0% beacon rate control ❒ Normal (default): 33% beacon rate control ❒ Increased: 66% beacon rate control ❒ High: 80% beacon rate control ❒ Full: 100% beacon rate control (To enable this option go to the Advanced → Others tab.)

Table 13. ESSID Parameter Descriptions (continued)

Field	Description
In Band Management	Select this option if you wish to allow management of the switch via the wireless media through this ESSID. In-band management ESSIDs are assigned to the same VLAN as the VLAN that has been set up for the switch management. Once you set this option, the VLAN setting will be automatically updated to the management VLAN as set in the LAN Configuration web page. If In Band Management ESSID is enabled, only the following security settings are permitted (this should be set from the Others Tab on the Advanced page): ❐ WPA/WPA2 personal (TKIP/AES & Pre Shared Key Authentication) ❐ WPA/WPA2 Enterprise (TKIP/AES & 802.1x Authentication)
Captive Portal	Select this option if you wish to set this ESSID to be captive-portal restricted. If you set this option, the ESSID VLAN ID is automatically assigned with the VLAN ID specified in the Portal tab in the Advanced page.
VLAN	Enter a VLAN tag to assign to the ESSID. Assigning a VLAN to an ESSID enables you to control a wireless device’s privileges through the existing wired network definitions.
Disassociation Timeout	Enter the amount of time (in seconds) a wireless device can remain inactive (no data sent to or from the wireless device) before automatically disconnecting it from the network.

Table 13. ESSID Parameter Descriptions (continued)

Field	Description
DTIM	Delivery Traffic Indication Message (DTIM) is the period of time after which broadcast and multicast packets are transmitted to mobile clients in the Active Power Management mode. Select the DTIM period from the drop-down menu. This is relevant for clients that want to utilize the power management capability. The possible values are 1-5. The default is 3. Note: A high DTIM value may cause these clients to lose connection with the network.
EAPOL Start Only	EAPOL stands for Extensible Authentication Protocol (EAP) over LAN. Select this option if you want the switch to only connect to clients that require the switch to wait for an EAPOL Start. Note: When this option is selected, clients that do not send an EAPOL start will not be able to connect to this ESSID.

Configuring Security Definitions

In the Encryption section of the ESSID Settings configuration page, the following security definitions can be configured:

- ❐ Method of encryption
- ❐ Type of authentication

Note
With some configurations, you can use encryption without authentication. For a higher level of security, however, it is recommended to use both encryption and authentication. The Extricom Series WLAN makes configuration of ESSID security parameters easier by listing available combinations of Encryption and Authentication protocols.

Security definitions are configured for each ESSID individually.

To configure the security definitions:

1. Click on the ESSID for which you want to configure the security definitions in the Select ESSID field.

2. Configure the security definitions for the selected ESSID. Refer to Table 14 below for a description of Security parameters.

Table 14. Security Definition Parameters

Field	Description
Encryption	Choose the method of encryption with or without authentication. A combination of encryption and authentication methods may be selected from the Method drop-down list. There are eight options available: ❐ None – no authentication. ❐ WEP64 – Wired Equivalent Privacy (802.11 encryption protocol). This is a very basic encryption level. (Also known as WEP40.) ❐ WEP128 – This encryption is similar to WEP64, but the WEP keys are longer. (Also known as WEP104.) ❐ WEP64 & 802.1x Authentication – WEP key used for authentication and encrypting the data frames. ❐ WEP128 & 802.1x Authentication – analogous to WEP 64 & 802.1x Authentication, but with WEP 104. ❐ WPA/WPA2 Personal – Wi-Fi Protected Access/Wi-Fi Protected Access 2. Also referred to as WPA-PSK (Pre-shared key) mode, it is designed for home and small office networks and does not require an authentication server. Each wireless network device authenticates with the access point using the same 256-bit key generated from a password or passphrase.

Table 14. Security Definition Parameters (continued)

Field	Description
Encryption (continued)	❐ WPA/WPA2 Enterprise – Also referred to as WPA-802.1X mode, and sometimes, just WPA (as opposed to WPA-PSK). It is designed for enterprise networks and requires a RADIUS authentication server. This requires a more complicated setup, but provides additional security (for example, protection against dictionary attacks on short passwords). An Extensible Authentication Protocol (EAP) is used for authentication, which comes with different types. ❐ WPA/WPA2 – Enterprise & Personal enables the wireless client to choose from either of the two methods on a single ESSID. In addition, there are two types of encryption ciphers available: ❐ AES – Advanced Encryption Standard (Cipher Block Chaining Message Authentication Code Protocol) is currently the most advanced and secured method of Wi-Fi encryption and is part of 802.11i (WPA2) standard. ❐ TKIP – Temporal Key Integrity Protocol. This is a more secure and more advanced method of encryption as a part of the WPA standard. When the WPA2 Only box is checked, only clients with WPA2 support are allowed to access the WLAN. When the AES Only box is checked, only clients with AES support are allowed to access the WLAN. Cisco LEAP protocol (not CMIC & CKIP) is supported under WEPxxx & 802.1x Authentication.

Table 14. Security Definition Parameters (continued)

Field	Description
Encryption (continued)	Authentication is used to identify if a wireless device is authorized to connect to the WLAN and verify the wireless device's identity. Authentication methods (such as specific EAP methods available in the WPA/WPA2 enterprise option) also verify that the association process is secured. Authentication utilizing WPA/WPA2 (enterprise) can also support encryption key changes. The following methods are available: ❐ 802.1x – if the cipher is WEP40 or WEP104 ❐ WPA/WPA2 enterprise – if the cipher is TKIP or AES ❐ Supported protocols: EAP, TLS, TTLS, PEAP, LEAP and MD5 Note: When choosing an encryption cipher and authentication method, make sure it is compatible with the wireless devices' capabilities. Note: The Extricom Series System supports WPA2 Mixed Mode. This mode permits the coexistence of WPA and WPA2 clients on the same ESSID. WPA2 Mixed Mode allows old WLAN clients with new WLAN clients on the same ESSID during the transition period. Any security combination (Encryption and Authentication) can be selected from the list and the checkboxes.

Table 14. Security Definition Parameters (continued)

Field	Description
WEP Keys	The WEP Keys area is only enabled if the cipher selected in the Method field of the Encryption area is either WEP64, WEP128, WEP64 & 802.1X Authentication, or WEP128 & 802.1X Authentication. In the WEP Keys area, you define the WEP Transmission Key that is used for encrypting or decrypting. You can define a single WEP key. For the transmission key you define, select the input format (ASCII or HEX), and enter the key according to the following: ❒ Cipher - WEP64 (or WEP64+802.1x) – ASCII: 5 characters – HEX: 10 digits ❒ Cipher - WEP128 (or WEP128+802.1x) – ASCII: 13 characters – HEX: 26 digits
WPA	The WPA area is only enabled if the cipher selected in the Method field of the Encryption area is either WPA/WPA2 Personal, WPA/WPA2 Enterprise, or WPA/WPA2 Personal & Enterprise. If WPA/WPA2 Personal or WPA/WPA2 Personal & Enterprise with Pre-Shared key authentication method is used, the WPA PSK field is enabled. In this case, select one of the following input formats, and enter the corresponding key listed: ❒ For ASCII, enter 8-63 characters. ❒ For HEX, enter 64 digits. You may select to either show or hide the key characters by either clicking the **Show Key** or **Hide Key** button to the right of the Key field. For all WPA/WPA2 encryption methods, you may specify **Group Rekey Interval**, which is the amount of time (in seconds) that elapses before the Group Key is changed.

Table 14. Security Definition Parameters (continued)

Field	Description
MAC Authentication RADIUS Server	This configuration option becomes available when encryptions with no RADIUS server are selected. The allowed encryption methods are: None, WEP64,WEP128, WPA/WPA2 Personal. The MAC authentication option must be checked to select a RADIUS server from a drop-down list. Define the MAC Authentication RADIUS Server by selecting one from the drop-down list.
RADIUS Authentication Servers	Define the RADIUS Authentication Server(s) by selecting one (or more, up to four) from the drop-down list if: ❒ The WEP64/WEP128 encryption with the 802.1x authentication method is selected, or ❒ The WPA/WPA2 - Enterprise or WPA/ WPA2 - Enterprise & Personal authentication method with the TKIP/AES cipher is selected. Note: Use Server # 1 if only one server is used. Use consecutive servers if several servers are used.
RADIUS Accounting Server	Select the RADIUS accounting server from the drop-down list of RADIUS servers.
Ticketing Settings	If one-use authentication tickets are used on this SSID, this is where the ESSID secret used to create the tickets is configured.

RADIUS Accounting Server

The RADIUS Accounting Server option enables the administrator to forward information about clients connected to a specific ESSID to an accounting server: Once enabled, the Extricom Series Switch forwards to the accounting server.

To configure the RADIUS accounting server:

1. Define the accounting server in the RADIUS list tab.

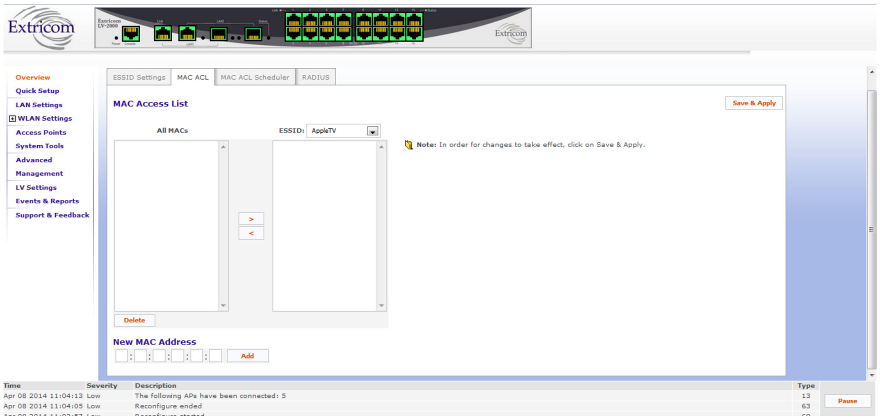
2. Click the **ESSID Settings** tab.

3. In the RADIUS Accounting Server section, choose the Accounting server from the drop-down list.

> **Note**
> The RADIUS Accounting Server option can be configured and enabled without a RADIUS Authentication server.

Configuring MAC ACL

To configure a per-ESSID MAC ACL, click the **MAC ACL** tab in the ESSID Definition configuration screen.



ESSID: AppleTV

Note: In order for changes to take effect, click on Save & Apply.

Time	Severity	Description	Type
Apr 08 2014 11:04:13	Low	The following APs have been connected: 5	13
Apr 08 2014 11:04:05	Low	Reconfigure ended	63

Figure 30. MAC ACL Configuration Tab

1. Select one of the configured ESSIDs from the ESSID drop-down list.

2. Select a MAC address from the list in the All MACs field.

3. Use the right arrow to add this MAC address to the ESSID field (use the left arrow to remove a MAC address from the ESSID field).

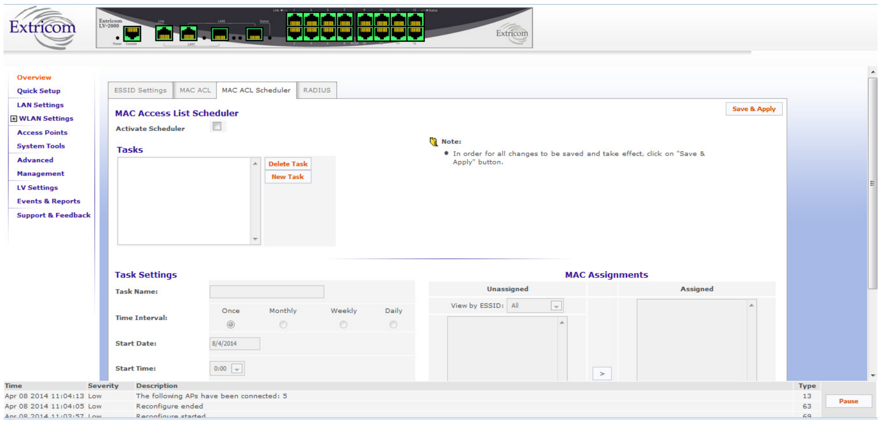
4. You may add a new MAC address to the All MACs list by inserting it manually in the New MAC Address field, then clicking **Add**. It is also possible to add a new MAC address to the All MACs table from the Event menu. When a new event message notification appears informing you of a new client, it will have a + button in the Add field. Once you click this button, the MAC address of the new client is automatically added to the All MACs list.

5. You may also remove a MAC address from the All MACs list by highlighting it and clicking **Delete** below the All MACS field.

6. Click **Save & Apply** to save the configuration and apply it immediately. It is not necessary to use the main Apply page.

Configuring MAC ACL Scheduler

The MAC ACL scheduler allows you to customize ACL configuration to allow various ACLs be activated at various times. To schedule ACL tasks, click the **MAC ACL Scheduler** tab in the ESSID Definition configuration section.



MAC Access List Scheduler

Activate Scheduler □

Tasks

Note:

- In order for all changes to be saved and take effect, click on "Save & Apply" button.

Task Settings

Task Name:

Time Interval: Once ● Monthly ○ Weekly ○ Daily ○

Start Date: 8/4/2014

Start Time: 0:00

MAC Assignments

Unassigned: View by ESSID: All

Assigned

Time	Severity	Description	Type
Apr 08 2014 11:04:13	Low	The following APs have been connected: 5	13
Apr 08 2014 11:04:05	Low	Reconfigure ended	63
Apr 08 2014 11:03:57	Low	Reconfigure started	69

Figure 31. MAC ACL Scheduler Configuration Tab

MAC ACL schedule may be activated by selecting the **MAC Access List Scheduler** checkbox at the top of the work area. Also:

1. To add a new ACL schedule, click **New Task**. An entry named New Task will appear in the Tasks field. You may also delete a schedule by selecting it from the list in the Tasks field and clicking **Delete Task**.

2. To configure the newly added schedule, or to modify an existing one, select it from the list in the Tasks field, then proceed to the Task Settings area of the configuration, as described in Table 15:

Table 15. MAC ACL Scheduler Parameters

Field	Description
Task Name	Assign a name to a selected schedule by entering an alphanumeric string in this field.
Time Interval	You may assign periodicity of an ACL by selecting one of the following radio buttons: ❒ Once ❒ Monthly ❒ Weekly ❒ Daily

Table 15. MAC ACL Scheduler Parameters (continued)

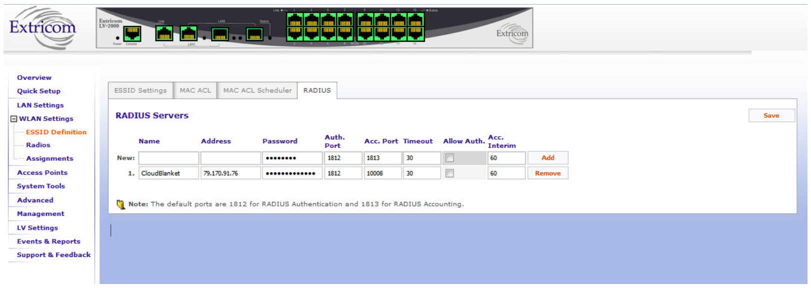
Field	Description
Start Date	Click inside the date field and navigate to the desired start date in the pop-up calendar.
Start Time	Select the start time from the drop-down menu. The options range from 0:00 to 23:00 in increments of one hour.
Duration	Select the time interval during which the ACL will be activated. The values in the drop-down menu are Continuous, 1 hour, 2 hours through 24 hours.

3. To apply the selected ACL task to the specified MAC addresses, proceed to the MAC Assignments area of the configuration screen. Here, you may move various MAC addresses between the Unassigned and Assigned fields by using the left and right arrow keys. You may either display all ACLs or only those associated with specific ESSIDs by selecting the specific ESSID or **All** from the Viewed by ESSID drop-down menu.

> **Note**
> The one or more MAC addresses selected will be activated via the Scheduler only if the relevant MAC address is assigned. If MAC ACL mode is set to Whitelist, only assigned MAC addresses will be scheduled activated. If MAC ACL mode is set to Blacklist, only assigned MAC addresses will NOT be scheduled activated.

Configuring RADIUS

To configure the RADIUS server option, select the RADIUS tab in the ESSID Definition configuration section. The RADIUS Servers work area displays the already configured RADIUS servers in the system RADIUS server bank. Here, you may also configure new RADIUS servers, as well as delete entries that are no longer needed.



RADIUS Servers

	Name	Address	Password	Auth. Port	Acc. Port	Timeout	Allow Auth.	Acc. Interim	
New:			••••••••	1812	1813	30	□	60	Add
1.	CloudBlanket	79.170.91.76	•••••••••••••	1812	10008	30	□	60	Remove

Note: The default ports are 1812 for RADIUS Authentication and 1813 for RADIUS Accounting.

Figure 32. RADIUS Configuration Tab

1. You may remove a RADIUS server from the list by clicking **Remove** next to the server definition line.

2. To modify an existing server, or to configure the new one, specify the following parameters as listed in Table 16:

Table 16. RADIUS Configuration Parameters

Field	Description
Name	ASCII string for the name of the RADIUS server.
Server Address	IP address of the RADIUS server.
Password	RADIUS server password.
Auth. Port	RADIUS authentication port number. The default value is 1812.
Acc. Port	RADIUS accounting port number. The default value is 1813.
Timeout	The time (in seconds) during which the Extricom Series switch will wait for the RADIUS server response, before it stops transmitting and switches to the next failover RADIUS server (if configured).
Allow Auth.	Click to allow the RADIUS attributes to determine the length of time a user can be connected to the wireless network. Multiple RADIUS servers can be used to authenticate on a single ESSID; if using RADIUS authorization, check the box on all of the servers. The order of priority is configured in the ESSID page. Only the first server is used, unless it is non-responsive, in which case, the switch would use the second configured server on the list, then the third, and so on.
Acc Interim	Interval (in seconds) to send accounting information. The default value is 60.

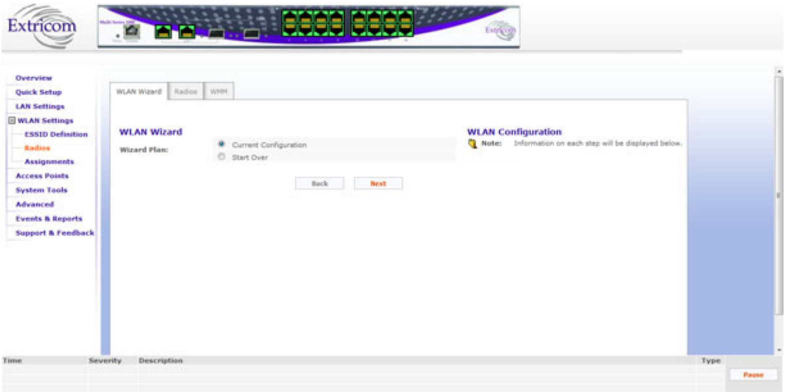
To save the configuration, click **Save**. At the end of the configuration, you must apply the configuration in the System Tools section.

Configuring WLAN Radios

To configure the WLAN radios, select **Radios** under WLAN Settings in the navigation tree. On this configuration page, you will find the following three configuration tabs:

- ❒ WLAN Wizard
- ❒ Radios
- ❒ WMM

Configuring Radios Using WLAN Wizard



WLAN Wizard

Wizard Plan: ● Current Configuration ○ Start Over

WLAN Configuration

Note: Information on each step will be displayed below.

Figure 33. WLAN Wizard Configuration Page

Using the step-by-step WLAN Wizard facility, and starting with either the **Current Configuration** or a new one (**Start Over**), you may simplify the process of configuring the radios, following the five pre-determined steps below.

1. Access Point Type
2. Rogue AP Detection Blanket
3. Blanket Types
4. TrueReuse
5. Additional Parameters

At each step, a corresponding entry is displayed on the right side of the configuration screen. For details on the configuration parameters, refer to Table 17 on page 89.

Table 17. Radio Configuration Parameters

Field	Description
Channel Options	
WLAN Mode	Select the WLAN mode from the drop-down menu. Options are: ❐ Disable - choose this option to disable the radio ❐ 802.11a ❐ 802.11b ❐ 802.11g ❐ 802.11 Mixed b/g ❐ 802.11n/a ❐ 802.11n/g ❐ 802.11n/g/b ❐ Rogue detection Note: Not all same-band configurations are possible, depending on the type of AP connected, the configured radio state, and whether TrueReuse is configured across the switch. See the Release Notes for possible configuration scenarios. Refer to "Feature Highlights" on page 23 for a description of same-band operation.
Select Channel	Select the channel from the drop-down menu. The options available are based on the country and WLAN mode.
Enable TrueReuse	Enable the TrueReuse function on the selected radio. Requires a TrueReuse License. Note: Not all TrueReuse configuration scenarios are available. This depends on which bands are configured on all other radios, the type of access point in use, and the configured radio state. See the Release Notes for possible configuration scenarios.
More/Less Options	Click to hide or reveal additional configuration options.

Table 17. Radio Configuration Parameters (continued)

Field	Description
Max Retries	Select the number of times that the switch tries to resend a packet if the transmission of that packet fails. Available values are 0 to 14.
Enable Short Preamble	This option becomes available only when 802.11b is selected as the WLAN mode. In this case, mark the checkbox to allow a short preamble.
Publish 802.11b rates	Only available in 802.11g or 802.11n/g modes. If this checkbox is selected, the switch will publish support of 802.11b data rates in the beacon. This is required by some older clients to operate.
Enable Load Balancing	Check this box if you want to enable load balancing. By using load balancing, mobile devices connect to the least-loaded Basic Service Set Identifier (BSSID) among all BSSIDs sharing the mobile devices' SSID. The number of connected users defines the metric that is used to determine the load.
The following parameters are available if one of the 802.11n-WLAN modes has been selected.	
Select Width	Click the appropriate radio button to select the width of the 802.11n channel, either **20MHz** or **20/40MHz**.
Secondary Channel	If 20/40MHz channel width is selected via the Select Width option, the system automatically configures the second 20MHz channel to be used for bonding as either above (Upper) or below (Lower) the primary 20MHz channel.
Select 802.11n Mode	Two blanket operational modes are supported: ❒ Mixed – In this mode, the Channel Blanket is available to all WLAN clients, for example, clients operating in 802.11a, 802.11b, 802.11g modes. ❒ HT Only – High throughput only. In this mode, the Channel Blanket is available to 802.11n clients only. Note: In this mode, the 802.11n devices are in fact working in a mixed mode, but the switch will not allow a/b/g devices to connect.

Table 17. Radio Configuration Parameters (continued)

Field	Description
Select Guard Interval	Guard interval can be configured to short (400 nanoseconds) or long (800 nanoseconds). Note: When a 20MHz channel is configured, it is not possible to configure short guard interval.
Spatial Streams	Select the number of spatial data streams for each AP. (Signals transmitted simultaneously from multiple antennas.)
802.11a/b/g Rate Configuration	Data rate configuration is only applicable to 802.11a/b/g Channel Blankets. For each of the data rates listed, select whether the rate is **Basic**, **Optional**, or **Disabled**. When configuring the data rates, you should consider the data rate capabilities of the wireless devices in your enterprise. ❐ Basic – The Basic data rates are usually the data rates that the vast majority of your wireless devices can support. Only wireless devices that support all the Basic data rates will be connected to the WLAN system. Therefore, it is recommended that you configure a minimal number of Basic data rates that the vast majority or all your wireless devices can support. When working in mixed mode, there should be at least one Basic data rate from the 802.11b rates. ❐ Optional – If you configure a data rate as Optional, the network will provide that data rate to wireless devices that can support it. ❐ Disabled – Disabled data rates are not available to wireless devices. Note: Because the Extricom Series WLAN system allows for dense deployment of APs, it is recommended, where applicable, to disable low data rates. Not doing so could possibly lead to an “edge user” effect, in which a client reduces aggregate network throughput by moving to the edge of the coverage area.

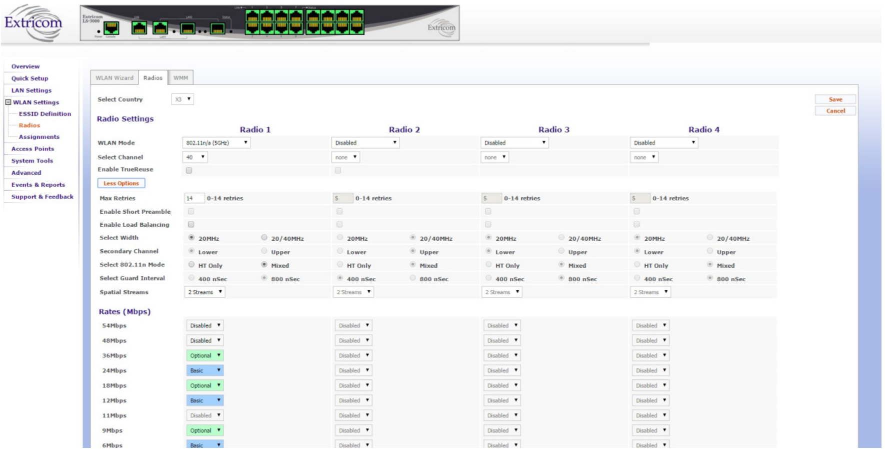
Configuring Radios Manually

To configure each radio manually, click on the **Radios** tab to access the Radios configuration screen.

The radio settings configured on the Radios tab apply to all access points connected to the switch. That is, each radio can be configured differently in the Radios tab on a switch; however, these radio settings will be the same on each access point connected to the switch.

When the Radios page is initially displayed, it appears in its abridged form. To see all of the configuration options, click the **More Options** button. The window shown in Figure 34 appears.

> **Note**
> When configuring 802.11a/b/g radios, the 802.11n displayed parameters cannot be configured and are grayed out.



Select Country: X3

Radio Settings

	Radio 1		Radio 2		Radio 3		Radio 4	
WLAN Mode	802.11n/a (5GHz)		Disabled		Disabled		Disabled	
Select Channel	40		none		none		none	
Enable TrueReuse	☐		☐					
Max Retries	14 0-14 retries		5 0-14 retries		5 0-14 retries		5 0-14 retries	
Enable Short Preamble	☐		☐		☐		☐	
Enable Load Balancing	☐		☐		☐		☐	
Select Width	● 20MHz	○ 20/40MHz	○ 20MHz	● 20/40MHz	● 20MHz	○ 20/40MHz	● 20MHz	○ 20/40MHz
Secondary Channel	● Lower	○ Upper	○ Lower	● Upper	● Lower	○ Upper	● Lower	○ Upper
Select 802.11n Mode	○ HT Only	● Mixed	○ HT Only	● Mixed	○ HT Only	● Mixed	○ HT Only	● Mixed
Select Guard Interval	○ 400 nSec	● 800 nSec	● 400 nSec	○ 800 nSec	○ 400 nSec	● 800 nSec	○ 400 nSec	● 800 nSec
Spatial Streams	2 Streams		2 Streams		2 Streams		2 Streams	

Rates (Mbps)

	Radio 1	Radio 2	Radio 3	Radio 4
54Mbps	Disabled	Disabled	Disabled	Disabled
48Mbps	Disabled	Disabled	Disabled	Disabled
36Mbps	Optional	Disabled	Disabled	Disabled
24Mbps	Basic	Disabled	Disabled	Disabled
18Mbps	Optional	Disabled	Disabled	Disabled
12Mbps	Basic	Disabled	Disabled	Disabled
11Mbps	Disabled	Disabled	Disabled	Disabled
9Mbps	Optional	Disabled	Disabled	Disabled
6Mbps	Basic	Disabled	Disabled	Disabled

Figure 34. Radios Configuration Page

The configuration parameters of each radio are arranged in a column. There are up to four columns, each of which is clearly identified with the corresponding title, for example, Radio 1, Radio 2. Refer to Table 17 on page 89 to set up the configuration parameters.

Configuring WMM

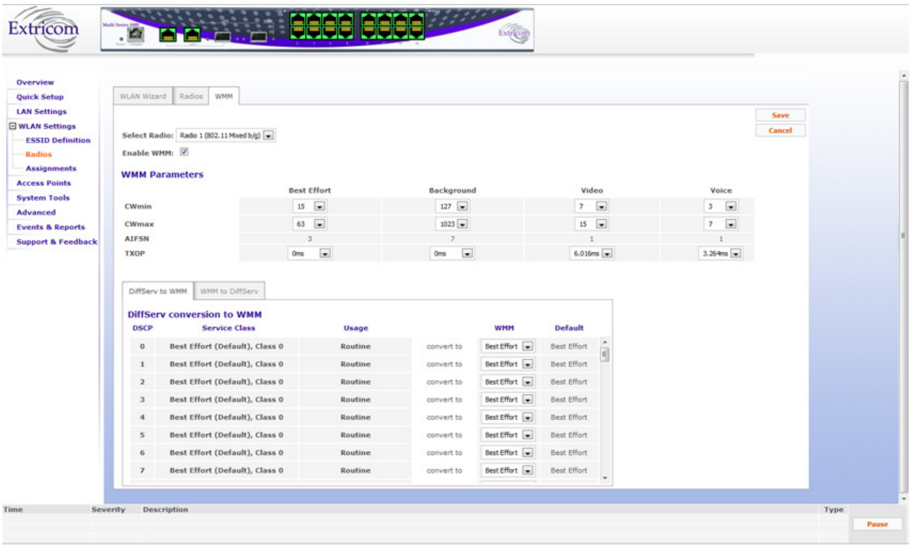
To configure WMM, click on the **WMM** tab.

> **Note**
> WMM is configured per radio.

1. Select the radio from the drop-down list.

2. Enable WMM by marking the **Enable WMM** checkbox.

3. Configure the appropriate WMM parameters as described in Table 18.



Select Radio: Rado 1 (802.11 Mixed b/g)

Enable WMM: ☑

WMM Parameters

	Best Effort	Background	Video	Voice
CWmin	15	127	7	3
CWmax	63	1023	15	7
AIFSN	3	7	1	1
TXOP	0ms	0ms	6.016ms	3.264ms

DiffServ conversion to WMM

DSCP	Service Class	Usage		WMM	Default
0	Best Effort (Default), Class 0	Routine	convert to	Best Effort	Best Effort
1	Best Effort (Default), Class 0	Routine	convert to	Best Effort	Best Effort
2	Best Effort (Default), Class 0	Routine	convert to	Best Effort	Best Effort
3	Best Effort (Default), Class 0	Routine	convert to	Best Effort	Best Effort
4	Best Effort (Default), Class 0	Routine	convert to	Best Effort	Best Effort
5	Best Effort (Default), Class 0	Routine	convert to	Best Effort	Best Effort
6	Best Effort (Default), Class 0	Routine	convert to	Best Effort	Best Effort
7	Best Effort (Default), Class 0	Routine	convert to	Best Effort	Best Effort

Time	Severity	Description	Type

Figure 35. WMM Configuration Tab

Table 18. WMM Parameters Description

Field	Description
CWmin	From the drop-down menu, select the minimum contention window (time slots) for each access category. Available values are: 3, 7, 15, 31, 63, 127, 255, 511, and 1023. The default values for the following categories are: ❒ **Voice** – 3 ❒ **Video** – 7 ❒ **Best Effort** – 15 ❒ **Background** – 127
CWmax	From the drop-down menu, select the maximum contention window for each access category. Available values are: 3, 7, 15, 31, 63, 127, 255, 511, and 1023 (time slots). The default values for the following categories are: ❒ **Voice** – 7 ❒ **Video** – 15 ❒ **Best Effort** – 63 ❒ **Background** – 1023

Table 18. WMM Parameters Description (continued)

Field	Description
AIFSN	Arbitration Inter Frame Spacing Number - predetermined and fixed for each access category and may not be changed.
TXOP	Transmit opportunity. Interval (in milliseconds) during which a station can send as many frames as possible. Available values are: 0, 1.504, 3.008, 3.264, and 6.016.

The DiffServ to WMM tab maps packets, which arrive on the wired interface of the switch, into WMM Access Categories, according to the Differentiated Service Code Point (DSCP) field in the IP header (Layer 3).

If the packets are tagged on the wire using 802.1p, the 802.11 QoS priority code is determined from the maximum between the priority code derived from the WMM static mapping value (2, 0, 5, or 7) and the 802.1p priority code. Refer to Table 19.

Table 19. WMM Standard Prioritization

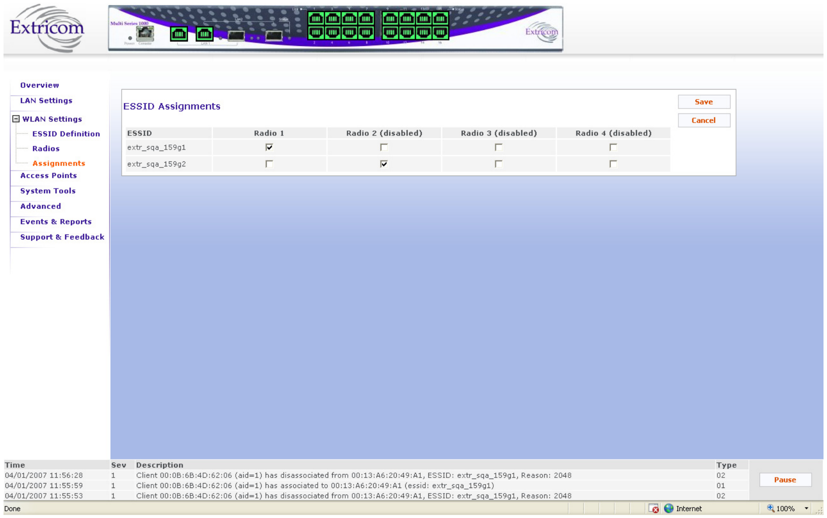
WMM Access Category	Static 802.11 QoS Value	Priority
Background	2	Lowest
Best Effort	0	
Video	5	
Voice	7	Highest

The **WMM to DiffServ** tab maps the WMM AC of packets, which arrive from wireless clients, into DSCP codes in the IP header (Layer 3). If the packet is tagged, that is, the ESSID is assigned a VLAN, the 802.11 QoS priority code is also written into the 802.1p field (three bits).

Note
These mapping options are available only when Expert mode is enabled in the Advanced settings.

ESSID Assignment

To assign specific radios to individual ESSIDs, select **Assignments** under WLAN Settings in the navigation tree.



ESSID Assignments

ESSID	Radio 1	Radio 2 (disabled)	Radio 3 (disabled)	Radio 4 (disabled)
extr_sqa_159g1	☑	☐	☐	☐
extr_sqa_159g2	☐	☑	☐	☐

```
Time                 Sev  Description                                                                                         Type
04/01/2007 11:56:28  1    Client 00:0B:6B:4D:62:06 (aid=1) has disassociated from 00:13:A6:20:49:A1, ESSID: extr_sqa_159g1, Reason: 2048   02
04/01/2007 11:55:59  1    Client 00:0B:6B:4D:62:06 (aid=1) has associated to 00:13:A6:20:49:A1 (essid: extr_sqa_159g1)                    01
04/01/2007 11:55:53  1    Client 00:0B:6B:4D:62:06 (aid=1) has disassociated from 00:13:A6:20:49:A1, ESSID: extr_sqa_159g1, Reason: 2048   02
```

Figure 36. ESSID Assignment Page

The web page displays a cross-reference table of previously defined ESSIDs and radios (up to 4). Check the box for each ESSID you wish to assign to any of the four radios.

Access Points

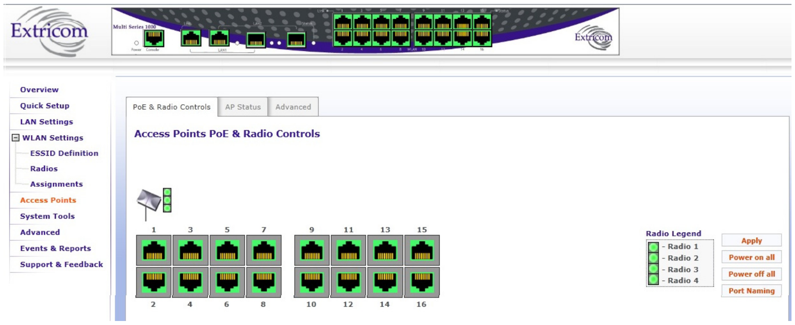
The only AP configuration required in the Extricom Series WLAN architecture is powering of the AP ports on or off.

To configure AP PoE status:

Click on **Access Points** in the navigation tree. Under the PoE & Radio Controls tab:

- ❒ Toggle an individual AP PoE on or off by clicking on its RJ45 connector image. The RJ45 connector image will turn either green or gray, depending on whether it has been powered on or off, respectively. To immediately activate your selection, click the **Apply** button on the right side of the configuration screen.
- ❒ An image of an AP connected to the RJ45 connector will appear if an AP is powered on and connected to the port.
- ❒ To power on all of the APs with PoE, click the **Power on all** button on the right side of the screen.
- ❒ To power off all of the APs with PoE, click the **Power off all** button on the right side of the screen.

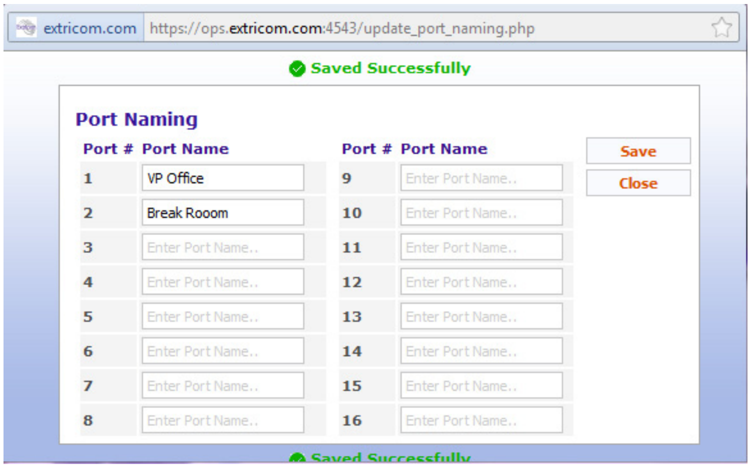
Note
The image of the switch on top of the page also color-illustrates the PoE status of the APs.



Access Points PoE & Radio Controls

Figure 37. Access Points PoE & Radio Controls Page

You may choose to assign names to the ports. If you do, click the **Port Naming** button on the right side of the screen. The Port Naming window pops up.



Saved Successfully

Port Naming

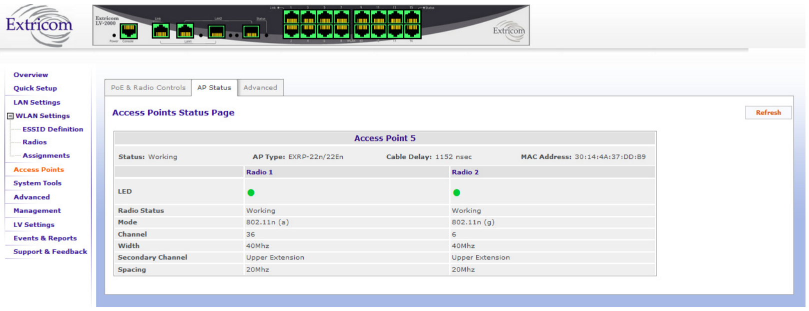
Port #	Port Name	Port #	Port Name
1	VP Office	9	Enter Port Name..
2	Break Rooom	10	Enter Port Name..
3	Enter Port Name..	11	Enter Port Name..
4	Enter Port Name..	12	Enter Port Name..
5	Enter Port Name..	13	Enter Port Name..
6	Enter Port Name..	14	Enter Port Name..
7	Enter Port Name..	15	Enter Port Name..
8	Enter Port Name..	16	Enter Port Name..

Saved Successfully

Figure 38. Port Naming Window

Type in the names for the ports, click **Save**, then **Close**.

To see which ports of the AP are up or down, click the **AP Status** tab. To display the most up-to-date information, click the **Refresh** button on the right side of the screen.



Access Points Status Page

Access Point 5

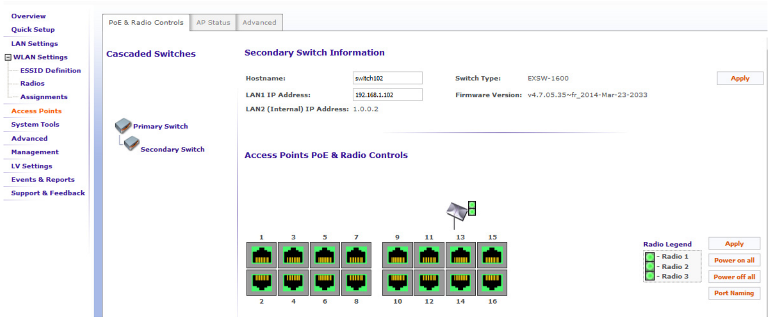
Status: Working AP Type: EXRP-22n/22En Cable Delay: 1152 nsec MAC Address: 30:14:4A:37:DD:B9

	Radio 1	Radio 2
LED	●	●
Radio Status	Working	Working
Mode	802.11n (a)	802.11n (g)
Channel	36	6
Width	40Mhz	40Mhz
Secondary Channel	Upper Extension	Upper Extension
Spacing	20Mhz	20Mhz

Figure 39. Access Points Status Page

APs of Cascaded Switches

When two switches have been cascaded together as primary and secondary (refer to "Switch Cascade" on page 35 for details about Switch Cascade configuration), the Access Point window is somewhat different. A tree of the two switches appears on the left to allow the user to easily toggle between views of the APs of each cascaded switch. The secondary switch is shown below the primary one in the tree:



Secondary Switch Information

Hostname: switch102

LAN1 IP Address: 192.168.1.102

LAN2 (Internal) IP Address: 1.0.0.2

Switch Type: EXSW-1600

Firmware Version: v4.7.05.35~fr_2014-Mar-23-2033

Access Points PoE & Radio Controls

Figure 40. Access Point Configuration Window - Secondary Switch

Selective Radio Activation

Toggle an individual radio in a specific AP on or off by clicking on its image. The radio image will turn either green or gray, depending on whether it has been powered on or off, respectively. To immediately activate your selection, click the **Apply** button on the right side of the configuration screen.

Note
The image of the switch on the top of the page, also colored, illustrates the PoE status of the APs.

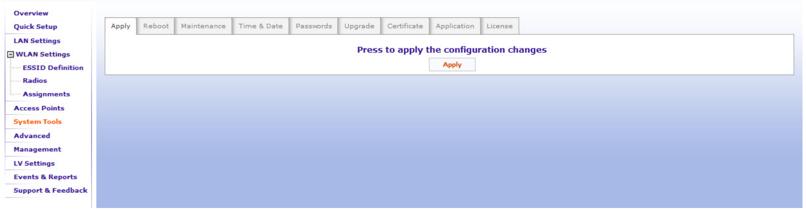
System Tools Configuration

Apply

Use this tab to apply the new configuration changes. In some cases, after using the **Apply** button, a system reboot is required, however, most parameters can be changed, and the changes take effect immediately. A system reboot is required after a change in the application type or firmware and license upgrades.

The **Apply** button:

- ❒ Checks whether a full reboot is required. If a reboot is not required, the updates will take effect immediately.
- ❒ Applies the configuration changes contained in the shadow configuration file (created when clicking the **Save** button on a Configuration page) to the new, active configuration file.



Press to apply the configuration changes

Figure 41. System Tools Configuration Page

Reboot

Use this tab to reboot the system and save the configuration changes created when clicking the **Save** button on a Configuration page. In some cases, such as upgrading or downgrading the firmware, or returning the Switch Cascade from failover to normal operation, a system reboot is required. Refer to the specific configuration update sections to see if the reboot is needed in order for the changes to take effect.

⚠ **Caution**
A switch reboot will cause a temporary loss of WLAN service until the reboot process is complete. ✍ **E109**

To reboot the Extricom Series switch:

1. Select the **Reboot** configuration tab and click **Reboot**.

   A new screen opens, prompting you "Are you sure you want to reboot?"

2. Click **Reboot** to proceed.

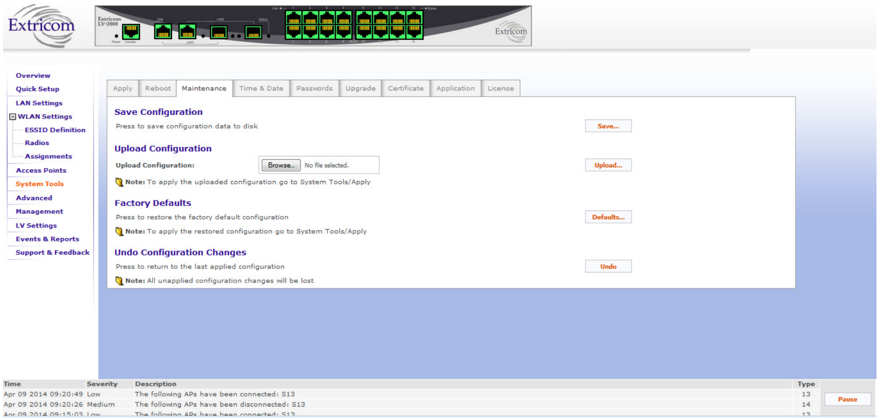
Caution

Once the changes are made, you must click **Save**, then go to System Tools and apply changes as described in the Apply section, in order for them to take effect. The changes will be discarded if the unit is rebooted before the changes are applied. ☞ **E110**

Maintenance

Use the Maintenance tab to:

- Save the current configuration to a disk.
- Upload a configuration to the switch.
- Restore the switch to factory default configuration.
- Undo configuration changes and return to the last applied configuration.



Save Configuration

Press to save configuration data to disk

Upload Configuration

Upload Configuration: No file selected.

Note: To apply the uploaded configuration go to System Tools/Apply

Factory Defaults

Press to restore the factory default configuration

Note: To apply the restored configuration go to System Tools/Apply

Undo Configuration Changes

Press to return to the last applied configuration

Note: All unapplied configuration changes will be lost

Time	Severity	Description	Type
Apr 09 2014 09:20:49	Low	The following APs have been connected: S13	13
Apr 09 2014 09:20:26	Medium	The following APs have been disconnected: S13	14
Apr 09 2014 09:15:03	Low	The following APs have been connected: S13	13

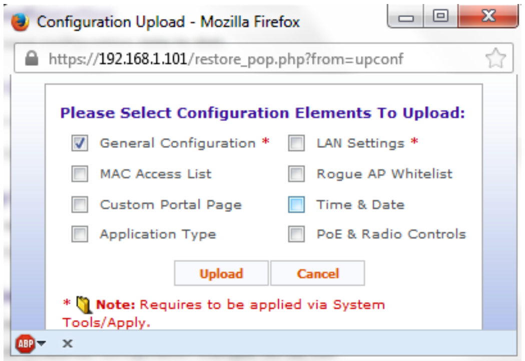
Figure 42. Maintenance Configuration Tab

Table 20. Maintenance Configuration Tab

Field	Description
Save Configuration	Save the active configuration to an off-line disk.
Upload Configuration	Upload a configuration from an off-line disk to the switch. Use the browse field to locate the configuration file. You will see a pop-up window stating “Please select configuration elements to upload”.
Factory Defaults	Restore factory default configuration. You will see a pop-up window stating “Please select configuration elements to Restore”.
Undo Configuration Changes	Return to the last applied configuration. All configuration changes not applied will be lost.

To save the active configuration, click on the **Save** button and specify the off-line location where you wish to save the file.

To upload a configuration, check the appropriate configuration elements in the Browse pop-up window, then click **Upload**:



Configuration Upload - Mozilla Firefox

https://192.168.1.101/restore_pop.php?from=upconf

Please Select Configuration Elements To Upload:

☑ General Configuration * ☐ LAN Settings *

☐ MAC Access List ☐ Rogue AP Whitelist

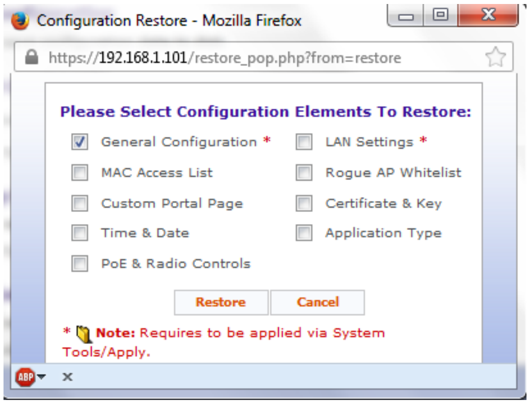
☐ Custom Portal Page ☐ Time & Date

☐ Application Type ☐ PoE & Radio Controls

* **Note:** Requires to be applied via System Tools/Apply.

Figure 43. Pop-up Window - Configuration Elements to Upload

To restore the factory default parameters, check the appropriate boxes in the Browse pop-up window, then click **Restore**:



Configuration Restore - Mozilla Firefox

https://192.168.1.101/restore_pop.php?from=restore

Please Select Configuration Elements To Restore:

☑ General Configuration * ☐ LAN Settings *

☐ MAC Access List ☐ Rogue AP Whitelist

☐ Custom Portal Page ☐ Certificate & Key

☐ Time & Date ☐ Application Type

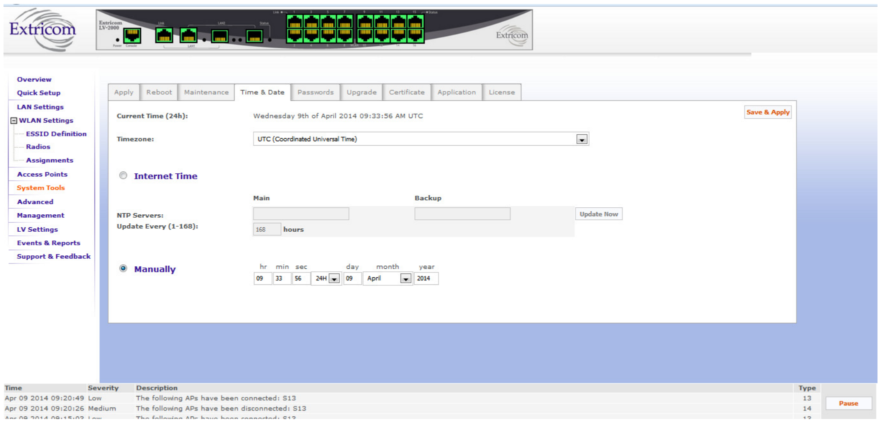
☐ PoE & Radio Controls

* **Note:** Requires to be applied via System Tools/Apply.

Figure 44. Pop-up Window - Configuration Elements to Restore

Time & Date

Use this configuration tab to set the time and date on the switch. The Extricom Series System supports two ways of setting the time and the date - manually or using the NTP protocol.



Current Time (24h): Wednesday 9th of April 2014 09:33:56 AM UTC

Timezone: UTC (Coordinated Universal Time)

○ Internet Time

NTP Servers: Main Backup

Update Every (1-168): 168 hours

● Manually

hr 09 min 33 sec 56 24H day 09 month April year 2014

Time	Severity	Description	Type
Apr 09 2014 09:20:49	Low	The following APs have been connected: S13	13
Apr 09 2014 09:20:26	Medium	The following APs have been disconnected: S13	14

Figure 45. Time & Date Configuration Tab

To manually set the time and date on your Extricom Series Switch:

1. Select the **Manually** radio button.
2. Enter the time and the date in the corresponding fields.
3. Click **Save and Apply**.

To set the time and date on your Extricom Series Switch using NTP protocol:

1. Select the **Internet Time** radio button.
2. Select the time zone from the drop-down menu.
3. Specify custom main and backup servers by entering their IP addresses in the **Custom Server IP** fields.
4. Specify the NTP update interval (in hours) in the **Update Every (1-168)** field.
5. Click **Save & Apply** to immediately start the NTP process.
6. Click **Update Now** to synchronize the system clock with the NTP server.

Passwords

Use this tab to set or change passwords. Passwords are set according to the user access privileges. Refer to Table 21 on page 103 for default passwords according to the user access levels.

Table 21. Default Passwords

User Access Level	Privileges	Default Password
admin	Accessing the web configuration	Switch1
operator	User account, SSH access	12345
root	Super user	octopus

Note
The “operator” and “root” passwords are used when accessing the switch for maintenance and service purposes. Changing these passwords should be performed only by an Allied Telesis-authorized engineer.

Caution
For security purposes, it is important that all the passwords (including operator and root passwords) be changed from the default values when the switch is first installed, as well as periodically updated. ✍ **E111**

Caution
Record all passwords and store them in a safe location. ✍ **E112**

To set and change a password on an Extricom Series switch:

1. Select the **Passwords** tab.
2. Select the user category from the drop-down list.
3. Enter the current password.
4. Enter the new password.
5. Retype the new password.
6. Click **Apply**.

Upgrade

Use the **Upgrade** tab to upgrade the Extricom Series switch firmware as follows:

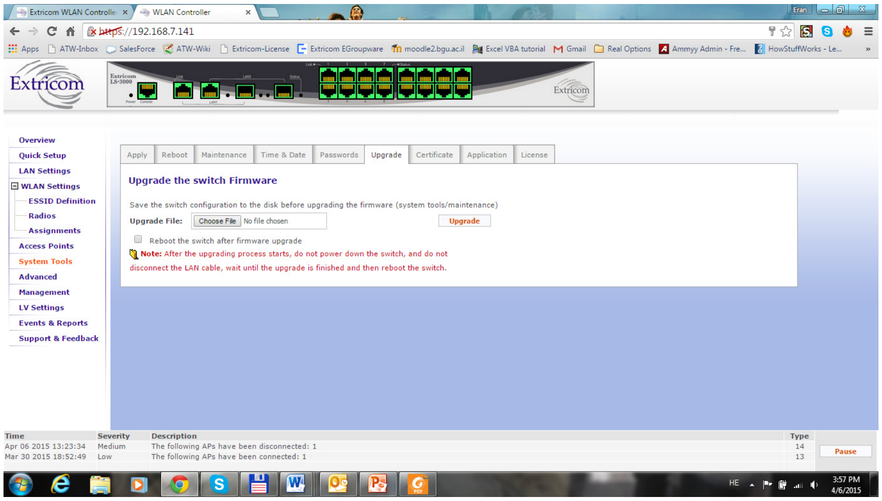
1. Download the upgrade file to your computer from the CD supplied with your purchase.

   OR

   Obtain an upgrade file from your authorized Allied Telesis reseller or distributor.

2. Create a backup of the current configuration as described under the **Save** option of the Maintenance configuration section.

3. Select the **Upgrade** tab to access the page shown in Figure 46.



Upgrade the switch Firmware

Save the switch configuration to the disk before upgrading the firmware (system tools/maintenance)

Upgrade File: Choose File No file chosen Upgrade

□ Reboot the switch after firmware upgrade

Note: After the upgrading process starts, do not power down the switch, and do not disconnect the LAN cable, wait until the upgrade is finished and then reboot the switch.

Time	Severity	Description	Type
Apr 06 2015 13:23:34	Medium	The following APs have been disconnected: 1	14
Mar 30 2015 18:52:49	Low	The following APs have been connected: 1	13

Figure 46. Upgrade Configuration Tab

4. Click **Choose File** and navigate to the location of the firmware upgrade file. The file’s name with the full path appears in the Upgrade File field.

5. You can check the **Reboot the switch after firmware upgrade** box for the switch to automatically reboot at the end of the upgrade process, or you can manually reboot the switch at a later time.

6. Click **Upgrade** to upgrade the firmware and wait for the upgrade process to end.

7. If you did not check the **Reboot the switch after firmware upgrade** box, manually reboot the switch as described in “Reboot” on page 99.

Note
The firmware upgrade file is GNU zipped (gzip). Some Internet browsers are configured to automatically unzip files when downloading. Verify that this function is disabled so that the upgrade file remains zipped after downloading.

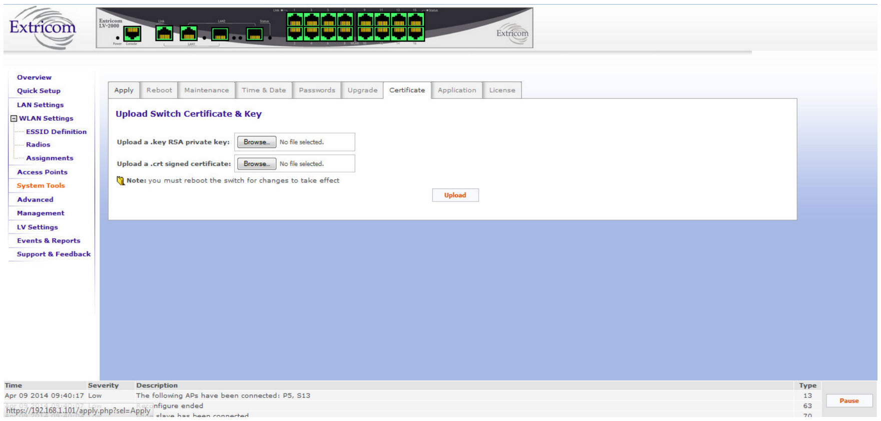
Note
Upgrading a Switch Cascade pair is done via the primary switch GUI.

Certificate

The first time that a Captive Portal user logs into the SSL (https) version of the portal from his browser, he receives a notice about a problem with the switch security certificate, such as "There is a problem with the website's security certificate". At that point, the user clicks on **Continue to this website (not recommended)**.

To avoid this error message, the WLAN operator can purchase a signed certificate and the RSA private key from an issuing authority. Once these are available, to install them on the switch:

1. Select the **Certificate** configuration tab.
2. Browse to the location of each file. Once located, the name and the path of the RSA private key file and the signed certificate file will appear in the corresponding fields.
3. Click **Upload** to complete the installation.



Upload Switch Certificate & Key

Upload a .key RSA private key: No file selected.

Upload a .crt signed certificate: No file selected.

Note: you must reboot the switch for changes to take effect

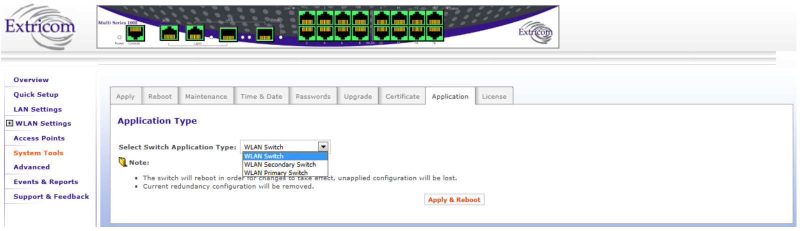
```
Time                  Severity  Description                                          Type
Apr 09 2014 09:40:17  Low       The following APs have been connected: P5, S13        13
                                nfigure ended                                         63
                                slave has been connected                              70
https://192.168.1.101/apply.php?sel=Apply
```

Figure 47. Certificate Configuration Tab

Application

In the Application configuration screen, you can change the role of a switch by selecting one of the Switch Application Types from the drop-down list. The options you will see depend on the License you have, but include:

- WLAN Switch - refers to a device in standalone mode.
- WLAN Secondary Switch - refers to the backup role of the switch in a switch cascade.
- WLAN Primary Switch - refers to the primary role of the switch in a switch cascade.



Application Type

Select Switch Application Type: WLAN Switch

Note:

- The switch will reboot in order for changes to take effect, unapplied configuration will be lost.
- Current redundancy configuration will be removed.

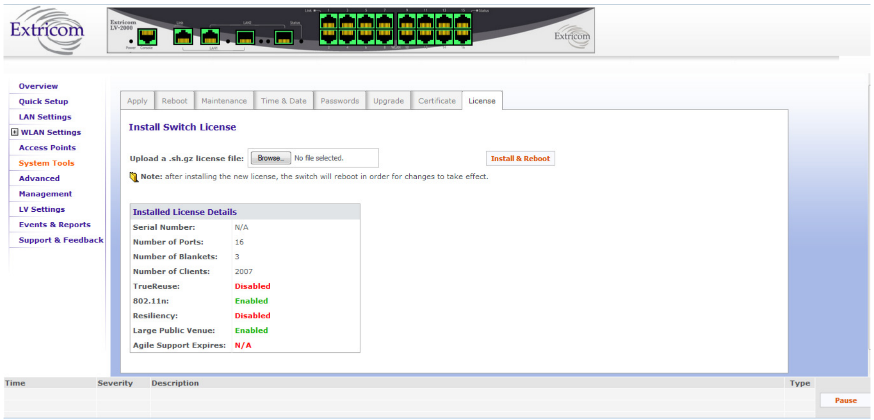
Figure 48. Application Configuration Tab

License

To install the license and activate the switch, click the **License** configuration tab.

1. Browse to the location of the License file on your computer.
2. Click **Install & Reboot** to finish activating the switch.

The switch reboots, and the license details are displayed in the Installed License Details section of the License Configuration tab.



Install Switch License

Upload a .sh.gz license file: No file selected.

Note: after installing the new license, the switch will reboot in order for changes to take effect.

Installed License Details	
Serial Number:	N/A
Number of Ports:	16
Number of Blankets:	3
Number of Clients:	2007
TrueReuse:	Disabled
802.11n:	Enabled
Resiliency:	Disabled
Large Public Venue:	Enabled
Agile Support Expires:	N/A

Figure 49. License Configuration Tab

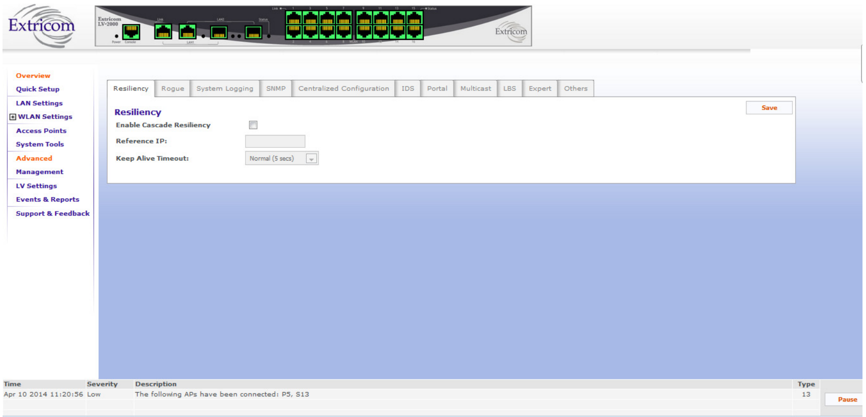
Advanced Configuration

To configure advanced features, select **Advanced** from the navigation tree. The configuration tabs under this configuration category are described below.

Cascade Resiliency

The Resiliency tab will only appear on a switch that has the Resiliency parameter on the license installed.

The Resiliency feature provides enhanced redundancy capabilities through several layers – switches and APs and combined. Cascade Resiliency supports redundancy between cascaded switches. Both switches serve a single BSSID until any of them is at fault. As soon as one of the switches fails, the operational switch serves mobile devices by itself with no human intervention. The eventual replacement of the faulty switch does not necessitate any interruption in service, while returning to a fully redundant mode.



Resiliency

Enable Cascade Resiliency ☐

Reference IP:

Keep Alive Timeout: Normal (5 secs)

Time	Severity	Description	Type
Apr 10 2014 11:20:56	Low	The following APs have been connected: P5, S13	13

Figure 50. Resiliency Configuration Tab

Resiliency Fields for Primary Switch

Table 22 on page 108 lists all the available parameters under the Resiliency configuration screen fields for a switch that has been set up as a primary cascade switch. The secondary switch GUI will not display the fields listed below.

Table 22. Resiliency Configuration Tab Parameters for a Primary Cascade Switch

Field	Description
Enable Cascade Resiliency	Check the box to enable Cascade Resiliency.
Reference IP	IP address of a reference device on the LAN. This is used to test connectivity to the LAN. The reference device must be operational and respond to pings.
Keep Alive Timeout	Interval in seconds between keep-alive packets sent to the reference IP.

The Keep Alive Timeout parameter defines the amount of time that the switch will wait before initiating the failover procedure. Configuring a shorter timeout decreases the amount of time in detecting a failure, but also increases the amount of false alarms.

⚠ **Caution**

Once the changes are made, you must click **Save**, then go to System Tools and apply changes as described in the Apply section, in order for them to take effect. The changes will be discarded if the unit is rebooted before the changes are applied. ✍ **E110**

When a switch or link failure is detected, a failover occurs, and the cascaded switch that remains fully operational goes into primary mode.

Table 23 indicates which cascaded APs provide service in the event of a failover.

Table 23. Switch Cascade Failover Behavior

Failure Type	Primary APs	Secondary APs	Comments
Switch Interconnect	√	√[1]	Primary and secondary switches failover to standalone mode. Even though APs of both switches are functioning, there is no seamless mobility between the switches.

Table 23. Switch Cascade Failover Behavior (continued)

Failure Type	Primary APs	Secondary APs	Comments
Primary LAN Link	X	√1	Secondary switch takes control and becomes primary.
Secondary LAN Link	√	√	No switch failover. Seamless mobility between switches. Secondary switch heartbeat checks if the primary switch is turned off.
Primary Switch Failure	X	√1	Secondary switch failover to Primary mode.
Secondary Switch Failure	√	X	
√ = Full service X = Not in service			

Notes:

- Traffic interruption time during a failover depends on the link and switch core monitoring parameters chosen (refer to Table 23 above).
- The cascaded switches contain the same configuration file, so in the event of a primary or secondary failure, the same configuration file is used by the operational switch.
- A primary switch can function as a standalone edge switch without requiring a failover (an edge switch being an AT-EXMS-1000 connected to, and managed by, an AT-EXLS-3000).
- Once the fault that caused the switchover has been resolved, both switches automatically return to normal cascade operation.

GUI Operation in Normal Cascade and Failover Operation

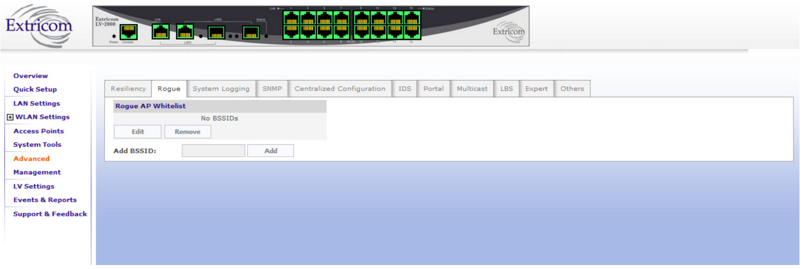
The primary switch GUI is fully operational if the primary switch is interconnected to a functional secondary switch. The secondary switch GUI is always read-only, except for the following menus: Reboot, Application, LAN Settings, Upgrade, and License. If the primary switch is not interconnected to a functioning secondary switch, the GUI will behave identical to a secondary switch (read-only apart from the specific above-mentioned menus).

Rogue

Rogue APs represent a threat to LAN security. Rogue APs are unauthorized APs that are physically connected to the wired Ethernet LAN.

The Rogue mechanism implemented in the Extricom Series switches requires a dedicated radio to scan the wireless media and detect Rogue APs. Therefore, one of the radios must be defined as “Rogue” in the Radio Settings page.

The Rogue tab folder allows you to edit a “white list” of independent APs that you allow to operate in your environment.



Rogue AP Whitelist

No BSSIDs

Add BSSID:

Figure 51. Rogue Configuration Tab

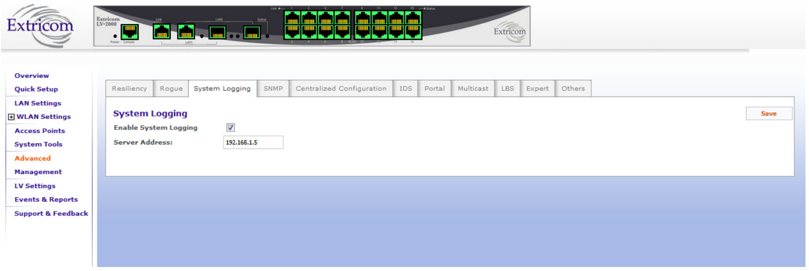
Table 24. Rogue Configuration Tab Rogue AP White List Parameters

Field	Description
Add BSSID	Add a BSSID (MAC address) of an AP that you permit to operate in your network.
Edit	Edit the list of legal BSSIDs.
Remove	Remove a BSSID from the white list.

System Logging

By default, the event logging is turned off. You may turn it on using the System Logging configuration tab in the Advanced section. To do this:

1. Click the **Enable System Logging** checkbox.
2. Enter the IP address of the server on which the Syslog protocol log will be stored.
3. Click **Save**.



System Logging

Enable System Logging ☑

Server Address: 192.168.1.5

Figure 52. System Logging Configuration Tab

The following lists events that are logged (refer to "Northbound SNMP Traps" on page 145 for definitions of the events below):

- AP connected
- AP disconnected
- AP malfunction
- AP reset
- Changed wireless status (On/Off)
- Client association
- Client disassociation
- Client ignore MTU
- EAPOL key error
- Edge connected
- Edge disconnected
- Edge mode switchover
- Firmware Upgrade done
- Firmware Upgrade failed
- Firmware Upgrade progress
- Firmware Upgrade startup
- Intrusion detection association flood attack
- Intrusion detection disassociation flood attack
- Intrusion detection authentication failure attack
- Intrusion detection authentication flood attack
- Intrusion detection de-authentication broadcast
- Intrusion detection de-authentication flood attack
- Intrusion detection EAPOL logoff attack
- Intrusion detection EAPOL start attack
- Intrusion detection RF jamming attack
- Last RADIUS failed

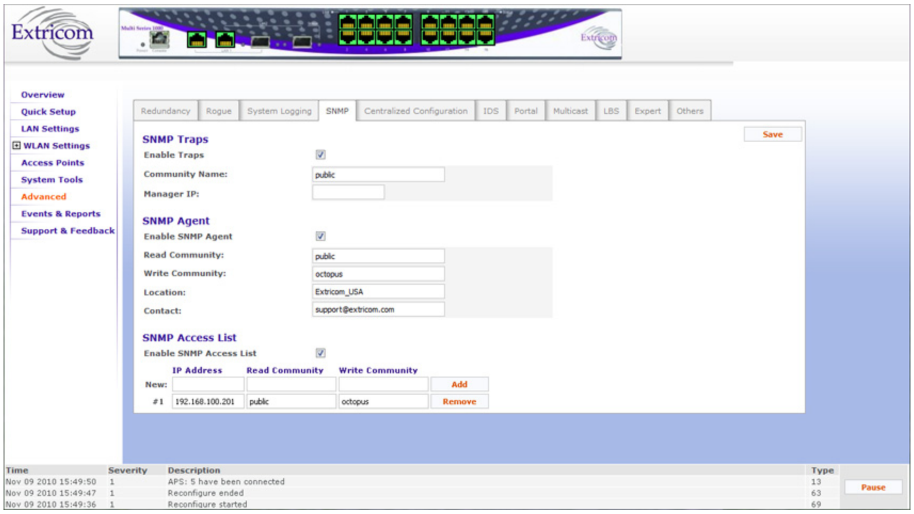
- License failed
- PoE reset
- RF localization failed
- Radio is functioning normally in all APs
- Radio is not functioning in APs
- Radio malfunction
- Radio reset
- RADIUS changed selection
- RADIUS timeout
- Reconfigure ended
- Reconfigure started
- Redundancy Keep alive Connection Down
- Redundancy Keep alive Connection Up
- Redundancy Peer Connection Down
- Redundancy Peer Connection Up
- Redundancy Status Down
- Redundancy Status Up
- Rogue AP Found
- Rogue AP Lost
- Rogue AP Update
- Set Client IP
- Start.sh Ended
- Start.sh Started
- Starting Boot

SNMP

Extricom Series switches generate a wide variety of traps to describe events occurring on the WLAN. In general, these traps can be categorized as follows:

- AP events (for example, connections, disconnections)
- Client events (for example, associations, disassociations)
- Switch events
- Configuration events
- RADIUS events
- Redundancy events (for Switch Cascade)
- Security events (for example, intrusion detection, rogue AP detection)

Traps are displayed in the Events and Alarms area at the bottom of the web interface (see Figure 53 below) as well as in the Events & Reports menu (refer to "Viewing Events and Reports" on page 123).



SNMP Traps

Enable Traps ☑

Community Name: public

Manager IP:

SNMP Agent

Enable SNMP Agent ☑

Read Community: public

Write Community: octopus

Location: Extricom_USA

Contact: support@extricom.com

SNMP Access List

Enable SNMP Access List ☑

	IP Address	Read Community	Write Community	
New:				Add
#1	192.168.100.201	public	octopus	Remove

Time	Severity	Description	Type
Nov 09 2010 15:49:50	1	APS: 5 have been connected	13
Nov 09 2010 15:49:47	1	Reconfigure ended	63
Nov 09 2010 15:49:36	1	Reconfigure started	69

Figure 53. SNMP Configuration Tab

SNMP Traps

Traps can be sent by the switch over its northbound interface to network management devices. To begin sending SNMP traps over the northbound interface, configure the SNMP Traps section under the SNMP tab as follows:

1. Check the **Enable Traps** box.
2. Enter the desired name in the **Community Name** field.
3. Enter the IP address of the manager device in the **Manager IP** field.

Refer to "Northbound SNMP Traps" on page 145 for a complete list of SNMP traps that may be sent by an Extricom Series switch.

SNMP Agent

You may configure the switch to respond to SNMP queries from various management systems on the network. To do this:

1. Enable the function by checking the **Enable SNMP Agent** box.
2. Set the password for SNMP Get-Requests by entering it in the **Read Community** field.
3. Set the password for SNMP Set-Requests by entering it in the **Write Community** field.

4. Enter the location of the switch in the **Location** field.

5. Enter the contact information in the **Contact** field.

SNMP Access List

To tighten security of your wireless LAN, you may decide to configure specific access lists (ACLs) to grant SNMP access to specific devices. To do this:

1. Enable the SNMP ACL function by checking the **Enable SNMP Access List** box.

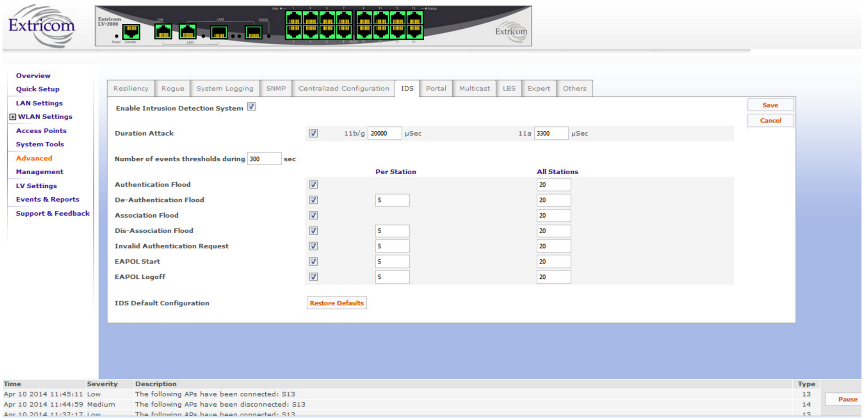
2. Enter the IP address of a device, along with the Get-Request and Set-Request passwords in the **Read Community** and **Write Community** fields, respectively.

3. Click **Add**.

Enter as many ACLs as needed. Before navigating away from this configuration screen, do not forget to save the changes you made by clicking the **Save** button on the right. To start generating SNMP traps, you must apply the configuration.

IDS

IDS stands for intrusion detection system. Malicious WLAN clients can cause a denial-of-service condition by flooding the WLAN network. A denial-of-service condition is identified through attack signatures or other factors, most of which are well-known. The IDS tab allows the user to enable this mechanism, set thresholds for identifying an attack, and choose the types of attacks to be detected. The IDS mechanism detects 802.11 duration attacks and 802.11 management message flooding attacks. Upon attack detection, the system sends a Trap message notifying of the event, and when applicable, provides the attacker’s details (for example, MAC address). Network administrators can use this information to take action and block malicious users. To configure IDS services, refer to Table 25 on page 115 for the specific parameters.



Enable Intrusion Detection System ☑

Duration Attack ☑ 11b/g 20000 µSec 11a 3300 µSec

Number of events thresholds during 300 sec

		Per Station	All Stations
Authentication Flood	☑		20
De-Authentication Flood	☑	5	20
Association Flood	☑		20
Dis-Association Flood	☑	5	20
Invalid Authentication Request	☑	5	20
EAPOL Start	☑	5	20
EAPOL Logoff	☑	5	20

IDS Default Configuration

Time	Severity	Description	Type
Apr 10 2014 11:45:11	Low	The following APs have been connected: S13	13
Apr 10 2014 11:44:59	Medium	The following APs have been disconnected: S13	14
Apr 10 2014 11:37:17	Low	The following APs have been connected: S13	13

Figure 54. IDS Configuration Tab

Table 25. IDS Configuration Parameters

Field	Description
Enable	Enables Intrusion detection
Duration Attack	
	WLAN devices reserve the channel for a particular period of time and then start using the radio channel. This time period is the Network Allocation Vector (NAV) in 802.11. By using high NAV values, an attacker can prevent other WLAN devices from utilizing the wireless network.
Enable	Mark the checkbox to enable this feature.
11b/g, 11a box	Define the Max NAV period (in µsec), after which the attack is detected.
Flood attacks	
	Malicious users can flood the WLAN with 802.11 management messages
Number of Events Thresholds During xx Sec.	Time window (in seconds)
Per station	Number of times a specific event is allowed during the event threshold. Each of the possible attack types listed below this parameter is assigned a limit per station.

Table 25. IDS Configuration Parameters (continued)

Field	Description
All station	Number of times a specific event is allowed during the event threshold. Each possible attack type listed below this parameter is assigned with a limit to all stations.
Authentication Flood	Flooding the WLAN with authentication requests
De-Authentication Flood	Flooding the WLAN with de-authentication requests
Association Flood	Flooding the WLAN with association requests
Dis-Association Flood	Flooding the WLAN with dis-association requests
Invalid Authentication Request	Flooding the WLAN with invalid authentication requests
EAPOL Start	Flooding the WLAN with EAP authentication “EAPOL Start”
EAPOL Logoff	Flooding the WLAN with EAP authentication “EAPOL Logoff”
Defaults	
Restore defaults	IDS Default Configuration

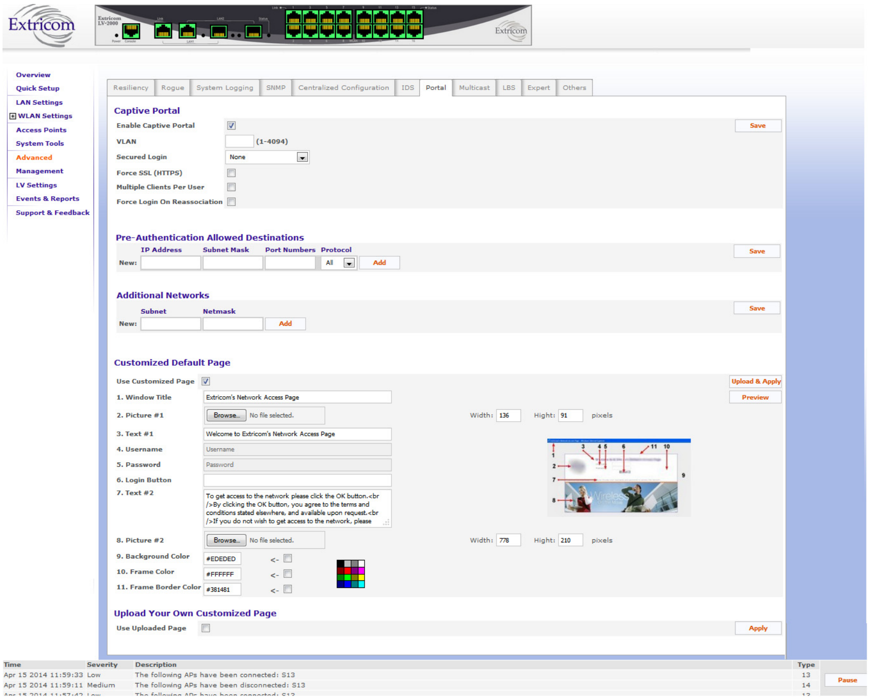
Portal (Captive Portal)

The Captive Portal mechanism restricts user Internet access by redirecting user web access requests to a Captive Portal web page.

There are two Captive Portal web page types:

- SSL-based Secured Logging: In Secured Logging, a user is initially authenticated before allowed Internet access. The user enters the username and the password using SSL. The switch then authenticates the user via RADIUS Server. Secured Logging is used for applications that require authentication-based access, such as hotels and guest access.
- Open Access: In an Open Access model, a user trying to access the web is redirected to a welcome web page, which might, for example, contain Terms of Use to which the user must agree before being allowed Internet access. Open Access is used for applications that enable open access, such as free airport networks.

The Portal Configuration tab is shown in Figure 55.



Captive Portal

Enable Captive Portal ☑

VLAN (1-4094)

Secured Login: None

Force SSL (HTTPS) □

Multiple Clients Per User □

Force Login On Reassociation □

Pre-Authentication Allowed Destinations

	IP Address	Subnet Mask	Port Numbers	Protocol
New:				All

Additional Networks

	Subnet	Netmask
New:		

Customized Default Page

Use Customized Page ☑

1. Window Title: Extricom's Network Access Page
2. Picture #1: No file selected. Width: 136 Hight: 91 pixels
3. Text #1: Welcome to Extricom's Network Access Page
4. Username: Username
5. Password: Password
6. Login Button
7. Text #2: To get access to the network please click the OK button.<br />By clicking the OK button, you agree to the terms and conditions stated elsewhere, and available upon request.<br />If you do not wish to get access to the network, please
8. Picture #2: No file selected. Width: 778 Hight: 210 pixels
9. Background Color: #EDEDED <- □
10. Frame Color: #FFFFFF <- □
11. Frame Border Color: #381481 <- □

Upload Your Own Customized Page

Use Uploaded Page □

Time	Severity	Description	Type
Apr 15 2014 11:59:33	Low	The following APs have been connected: S13	13
Apr 15 2014 11:59:11	Medium	The following APs have been disconnected: S13	14

Figure 55. Captive Portal Configuration Tab

Use the Portal tab to configure the Captive Portal settings described in Table 26.

Table 26. Captive Portal Configuration Parameters

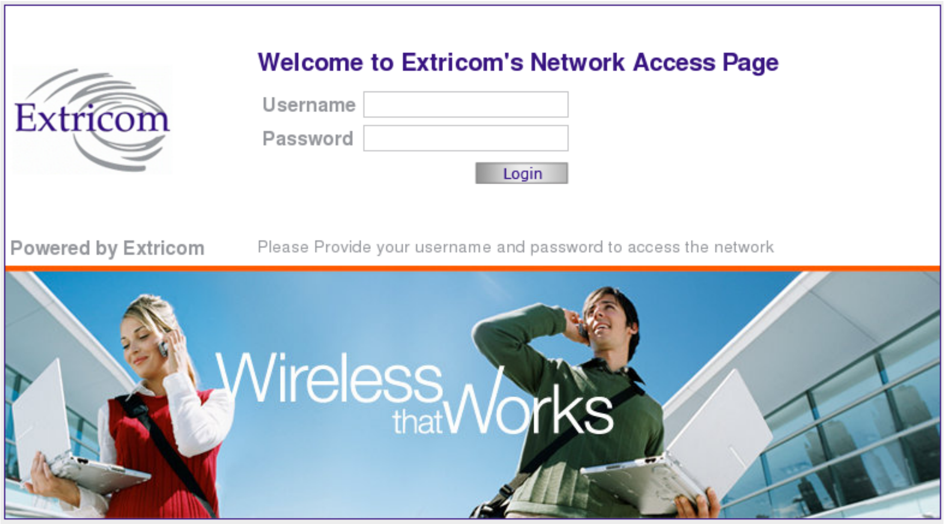
Field	Description
Enable captive portal	You must enable this option system-wide if you want to configure Captive Portal on any ESSID.
VLAN	Set the captive-portal VLAN. When ESSID is set to be captive-portal restricted, the ESSID VLAN is automatically set to this VLAN.
Secured Login	Set the type of authentication - either None, Remote, or Local. None enables Captive Portal without authentication of the client. Remote authentication requires selection of a RADIUS server and an authentication protocol (PAP or CHAP).

Table 26. Captive Portal Configuration Parameters (continued)

Field	Description
Force SSL (HTTPS)	When this option is selected, any client that attempts to connect using http: will be redirected to SSL (https:) communication. If this feature is not activated, the type of session will depend solely on the protocol (http:// or https://) specified at the beginning of the URL string entered into the client's browser.
Multiple Clients Per User	Enables multiple simultaneous client connections with the same user name and password via the portal.
Force Login on Re-association	Configure login without authentication on re-association.
Pre-Authentication Allowed Destination (Walled Garden)	You can define a list of up to 10 free-access network destinations (10 rules). WLAN clients associated to the captive-portal restricted ESSID can reach these destinations without going through the captive-portal authentication process. A network destination (a rule) is defined by an IP address, subnet mask, port numbers, and an Internet Protocol (TCP, UDP, ICMP). It is advised to define free access to the DHCP server on port 67 using broadcast and to the DNS server on port 53 using unicast, as in the following example: ❐ DHCP server – IP Address: 0.0.0.0 – Subnet Mask: 0.0.0.0 – Port Number: 67 – Protocol: All ❐ DNS server – IP Address: 192.168.1.5 – Subnet Mask: 255.255.255.255 – Port Number: 53 – Protocol: All

Table 26. Captive Portal Configuration Parameters (continued)

Field	Description
Additional Networks	You may add trusted networks by specifying a subnet along with its netmask for each such network. It is advised to define the network used by the ESSID with the Portal authentication, as in the following example: Subnet: 192.168.1.0 Netmask: 255.255.255.0
Customize Default Page	If you do not check the **Use Customized Page** box, the captive portal web page will be set to the Extricom Series default web page. If you check the **Use Customized Page** box, follow the instructions to customize the page.
Upload Your Own Customized Page	Allows you to upload your own captive portal web page. Use the instruction link to build your web page.



Welcome to Extricom's Network Access Page

Username

Password

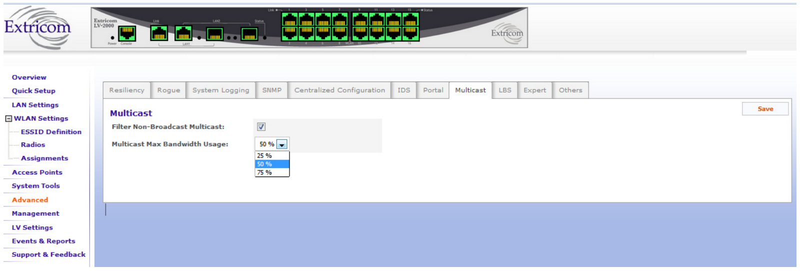
Please Provide your username and password to access the network

Figure 56. Extricom Series Default Captive Portal Web Page

Multicast

Under the Multicast configuration tab, you may limit the amount of time the system is busy with sending multicast traffic: this feature mostly applies to specific applications communicating mostly via multicast traffic.

Note
The Multicast tab is available only when Expert mode is enabled from the Advanced settings.



Multicast

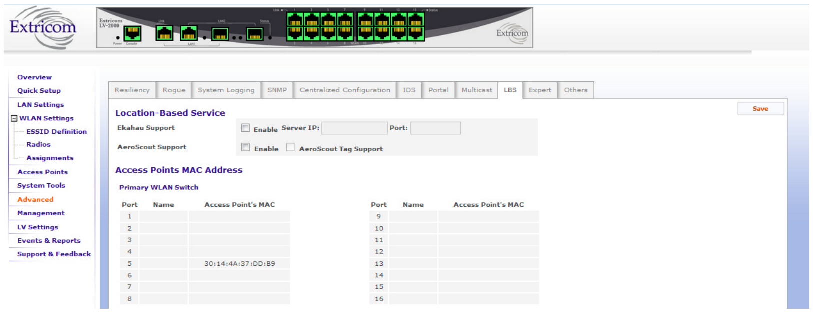
Filter Non-Broadcast Multicast: ☑

Multicast Max Bandwidth Usage: 50 % (25 %, 50 %, 75 %)

Figure 57. Multicast Configuration Tab

LBS

Location-Based Service (LBS) tab: Real Time Location Services (RTLS) support third-party RTLS solution vendors to provide high-accuracy location-based services for WLAN mobile clients.



Location-Based Service

Ekahau Support ☐ Enable Server IP: Port:

AeroScout Support ☐ Enable ☐ AeroScout Tag Support

Access Points MAC Address

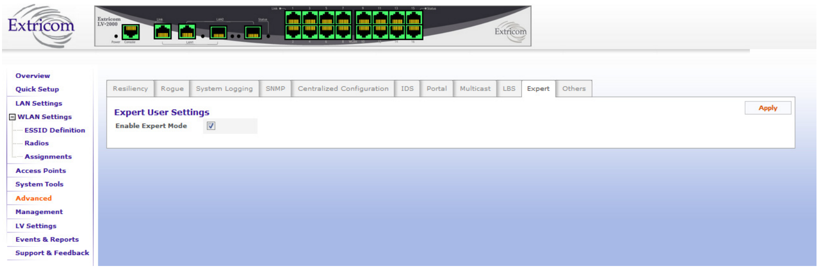
Primary WLAN Switch

Port	Name	Access Point's MAC	Port	Name	Access Point's MAC
1			9		
2			10		
3			11		
4			12		
5		30:14:4A:37:DD:B9	13		
6			14		
7			15		
8			16		

Figure 58. LBS Configuration Tab

Expert

Under the Expert tab, Expert User mode provides advanced configuration options which are not visible via the basic settings. To activate Expert User mode, check the **Enable Expert Mode** box and click **Apply**.



Expert User Settings

Enable Expert Mode ☑

Figure 59. Expert Configuration Tab

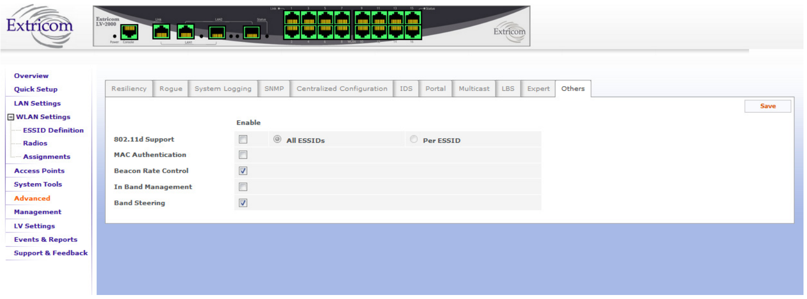
Others

Under the Others tab, a number of advanced configuration options, such as 802.11d, are provided.

- Check the **802.11d Support** box if you wish to enable this option. You can enable it per ESSID or for all ESSIDs.
- Check the **MAC Authentication** box if you wish to enable this option.

- Check the **Beacon Rate Control** box if you wish to enable this option.
- Check the **In Band Management** box if you wish to enable this option (this is a general enabling of the option and requires per ESSID configuration).
- Check the **Band Steering** box if you wish to enable this option.

To activate these options per ESSID, after selecting the above checkboxes, refer to "Configuring WLAN Settings" on page 72.



	Enable		
802.11d Support	☐	● All ESSIDs	○ Per ESSID
MAC Authentication	☐		
Beacon Rate Control	☑		
In Band Management	☐		
Band Steering	☑		

Figure 60. Others Configuration Tab

Band Steering

A technique called Band Steering is used to divert 802.11 clients to the 5 GHz band. Band Steering works by recognizing that a client is 5GHz capable and then responding to its association requests only in the 5 GHz band and not the 2.4 GHz band. The client then associates in the 5 GHz band.

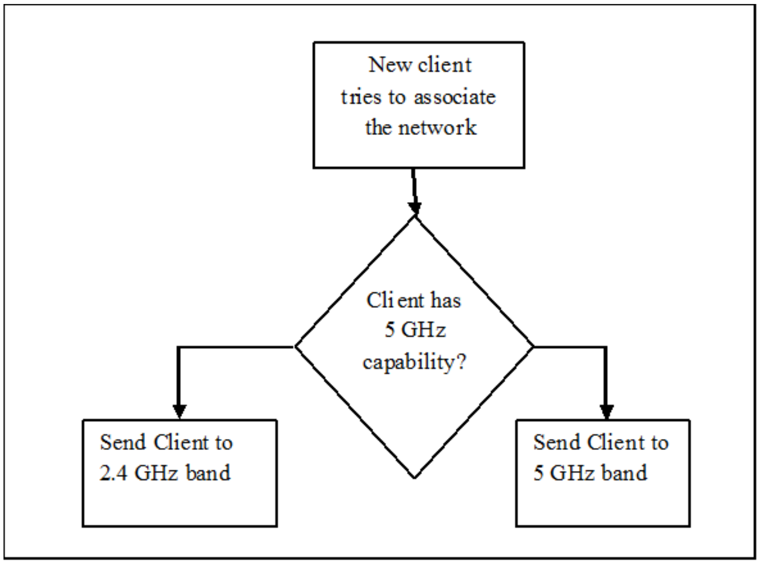

New client tries to associate the network
Client has 5 GHz capability?
Send Client to 2.4 GHz band
Send Client to 5 GHz band

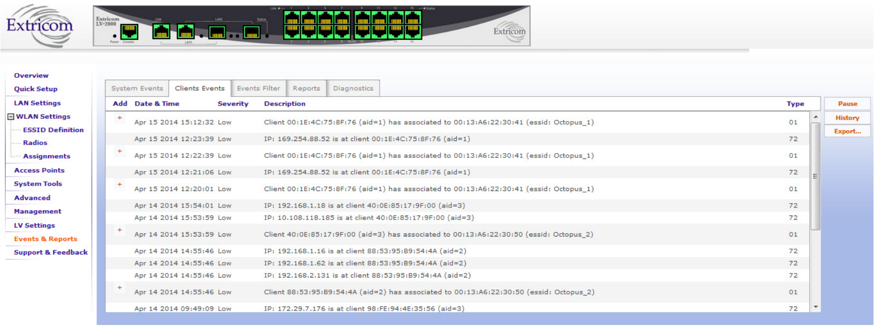
Figure 61. Band Steering Operational Flow

Band Steering only works if the Wi-Fi network has at least two radios: one for the 2.4 GHz band and one for the 5 GHz band.

Viewing Events and Reports

The Events & Reports page provides performance reports and lists various system events. To access this page, click **Events & Reports** in the navigation tree. Within the page, you will find the following configuration tabs:

- System Events
- Clients Events
- Events Filter
- Reports
- Diagnostics



Add	Date & Time	Severity	Description	Type
+	Apr 15 2014 15:12:32	Low	Client 00:1E:4C:75:8F:76 (aid=1) has associated to 00:13:A6:22:30:41 (essid: Octopus_1)	01
	Apr 15 2014 12:23:39	Low	IP: 169.254.88.52 is at client 00:1E:4C:75:8F:76 (aid=1)	72
+	Apr 15 2014 12:22:39	Low	Client 00:1E:4C:75:8F:76 (aid=1) has associated to 00:13:A6:22:30:41 (essid: Octopus_1)	01
	Apr 15 2014 12:21:06	Low	IP: 169.254.88.52 is at client 00:1E:4C:75:8F:76 (aid=1)	72
+	Apr 15 2014 12:20:01	Low	Client 00:1E:4C:75:8F:76 (aid=1) has associated to 00:13:A6:22:30:41 (essid: Octopus_1)	01
	Apr 14 2014 15:54:01	Low	IP: 192.168.1.18 is at client 40:0E:85:17:9F:00 (aid=3)	72
	Apr 14 2014 15:53:59	Low	IP: 10.108.118.185 is at client 40:0E:85:17:9F:00 (aid=3)	72
+	Apr 14 2014 15:53:59	Low	Client 40:0E:85:17:9F:00 (aid=3) has associated to 00:13:A6:22:30:50 (essid: Octopus_2)	01
	Apr 14 2014 14:55:46	Low	IP: 192.168.1.16 is at client 88:53:95:B9:54:4A (aid=2)	72
	Apr 14 2014 14:55:46	Low	IP: 192.168.1.62 is at client 88:53:95:B9:54:4A (aid=2)	72
	Apr 14 2014 14:55:46	Low	IP: 192.168.2.131 is at client 88:53:95:B9:54:4A (aid=2)	72
+	Apr 14 2014 14:55:46	Low	Client 88:53:95:B9:54:4A (aid=2) has associated to 00:13:A6:22:30:50 (essid: Octopus_2)	01
	Apr 14 2014 09:49:09	Low	IP: 172.29.7.176 is at client 98:FE:94:4E:35:56 (aid=3)	72

Figure 62. Events & Reports - Client Events Tab

System Events

The System Events tab lists system messages that were generated by the switch as event notifications. The date and time of occurrence, as well as the severity of the event, are also displayed.

Clients Events

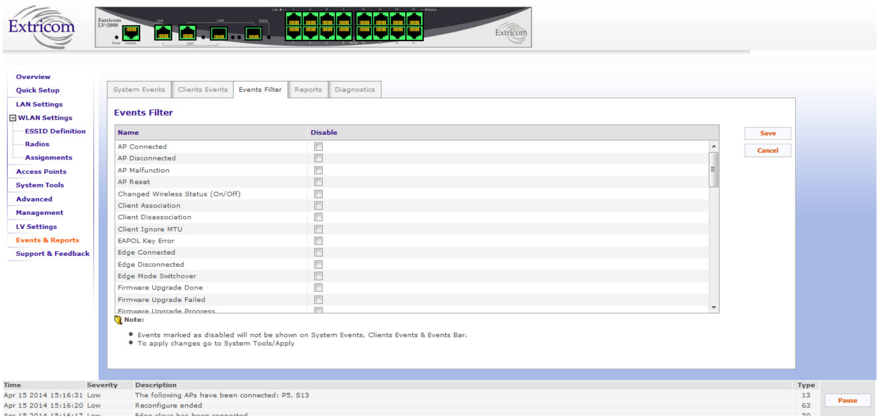
The Clients Events tab lets you view client association and disassociation events only. As in the case with the System Events tab, each client event is displayed with the corresponding date and time of its occurrence and level of severity.

On both the System Events page and Clients Events page, there are three buttons on the right side of the screen: **Pause/Continue** toggle, which lets you stop or start the flow of the events; **History**, which brings up the list of the most recent past events (up to 1000); and **Export**, which lets you save an event log into an HTML file on your computer.

If a message has a plus sign in the **Add** field, by clicking on this message, the MAC address associated with the message user will be automatically inserted into the MAC ACL list.

Events Filter

You may exclude some of the events from your reports, using the Events Filter configuration tab. Select the checkbox(es) corresponding to those events, then click **Save**.



Events Filter

Name	Disable
AP Connected	□
AP Disconnected	□
AP Malfunction	□
AP Reset	□
Changed Wireless Status (On/Off)	□
Client Association	□
Client Disassociation	□
Client Ignore MTU	□
EAPOL Key Error	□
Edge Connected	□
Edge Disconnected	□
Edge Mode Switchover	□
Firmware Upgrade Done	□
Firmware Upgrade Failed	□
Firmware Upgrade Progress	□

Note:

- Events marked as disabled will not be shown on System Events, Clients Events & Events Bar.
- To apply changes go to System Tools/Apply

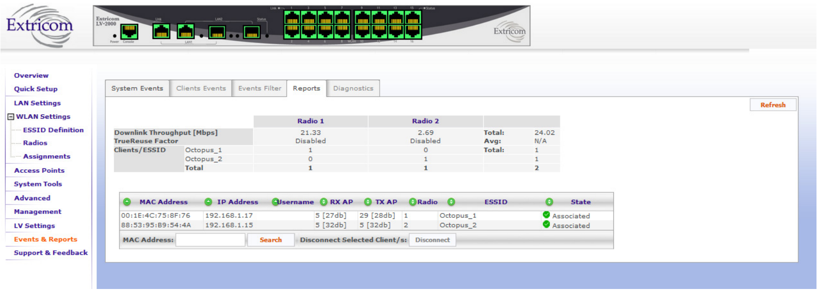
Time	Severity	Description	Type
Apr 15 2014 15:16:31	Low	The following APs have been connected: P5, S13	13
Apr 15 2014 15:16:20	Low	Reconfigure ended	63
Apr 15 2014 15:16:17	Low	Edge slave has been connected	70

Figure 63. Events Filter Configuration Tab

Refer to “Northbound SNMP Traps” on page 145 for event descriptions.

Reports

The Reports tab, shown below, provides a wide range of per-radio-channel-based and per-switch-based statistics.



		Radio 1	Radio 2		
Downlink Throughput [Mbps]		21.33	2.69	Total:	24.02
TrueReuse Factor		Disabled	Disabled	Avg:	N/A
Clients/ESSID	Octopus_1	1	0	Total:	1
	Octopus_2	0	1		1
	Total	1	1		2

MAC Address	IP Address	Username	RX AP	TX AP	Radio	ESSID	State
00:1E:4C:75:8F:76	192.168.1.17		5 [27db]	29 [28db]	1	Octopus_1	✓ Associated
88:53:95:B9:54:4A	192.168.1.15		5 [32db]	5 [32db]	2	Octopus_2	✓ Associated

MAC Address: [ ] Search Disconnect Selected Client/s: Disconnect

Figure 64. Reports Tab

Table 27 describes the information available on this page:

Table 27. Reports Tab Fields

Field	Description
Downlink Throughput [Mbps]	A one-second snapshot of the data volume carried by all downlinks on a particular radio channel (Channel Blanket).
Total	Total downlink throughput of the switch, based on a one-second snapshot of data volume.

Table 27. Reports Tab Fields (continued)

Field	Description
TrueReuse Factor	Available only if TrueReuse is enabled. Ranges from 1-3. Indicates the current downlink throughput relative to what the downlink throughput would have been if TrueReuse were not enabled. Computes the average number of downlinks transmitting simultaneously per radio channel. The average is computed based on several snapshots taken during several one-second time intervals. Example: a value of 3 means that downlink throughput with TrueReuse is currently 3 times higher on average on that radio channel than if TrueReuse had been disabled.
Avg.	TrueReuse Factor average over all radio channels.
Clients/ESSID	Number of clients connected per ESSID per radio channel.
Clients/ESSID Total	Total number of clients per ESSID per radio channel, over all channels, per switch.
MAC Address	Used to search for a MAC address on the page. Any matching MAC address in the list of clients’ MAC addresses will be highlighted.
Disconnect Selected Client/s	Used to reset a client connection, in order to help a client establish a working connection. The client must then re-authenticate to reconnect to the WLAN.

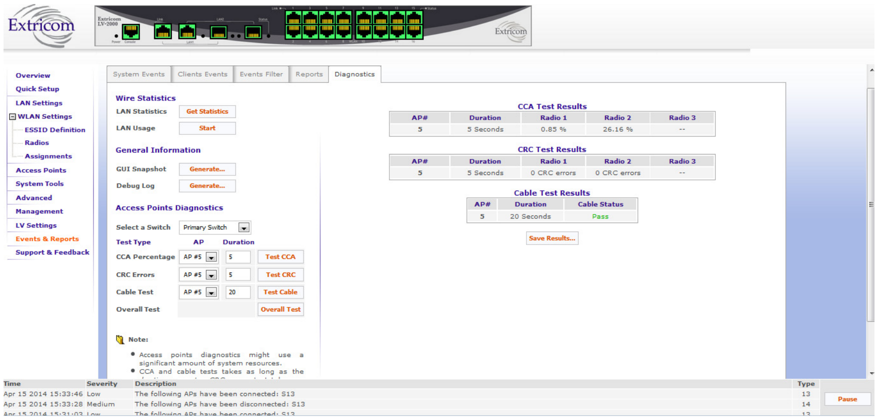
Note
The statistics window does not get updated automatically. Click **Refresh** to update the statistics.

At the bottom of the screen in this tab folder, the clients are listed, along with the following information: MAC Address, IP Address, Username, RX and TX AP, Channel, ESSID and current State.

Diagnostics

In this section, you may collect various media usage, traffic, network health, and other relevant statistics, as well as initiate various real-time tests. The area for data requests and test initiating is located in the left section of the configuration screen. The results are displayed in the right portion of the screen and may also be downloaded to your computer.

Refer to Table 28 below for the details on diagnostics parameters and types of tests available.



Wire Statistics

LAN Statistics: Get Statistics

LAN Usage: Start

General Information

GUI Snapshot: Generate...

Debug Log: Generate...

Access Points Diagnostics

Select a Switch: Primary Switch

Test Type	AP	Duration	
CCA Percentage	AP #5	5	Test CCA
CRC Errors	AP #5	5	Test CRC
Cable Test	AP #5	20	Test Cable
Overall Test			Overall Test

Note:

- Access points diagnostics might use a significant amount of system resources.
- CCA and cable tests takes as long as the

CCA Test Results

AP#	Duration	Radio 1	Radio 2	Radio 3
5	5 Seconds	0.85 %	26.16 %	--

CRC Test Results

AP#	Duration	Radio 1	Radio 2	Radio 3
5	5 Seconds	0 CRC errors	0 CRC errors	--

Cable Test Results

AP#	Duration	Cable Status
5	20 Seconds	Pass

Save Results...

Time	Severity	Description	Type
Apr 15 2014 15:33:46	Low	The following APs have been connected: S13	13
Apr 15 2014 15:33:28	Medium	The following APs have been disconnected: S13	14
Apr 15 2014 15:31:03	Low	The following APs have been connected: S13	13

Figure 65. Diagnostics Tab

Table 28. Diagnostics Tab Parameters and Tests

Field	Description
Wire Statistics	
LAN Statistics	Click **Get Statistics** to get information about the transmit (TX) and receive (RX) traffic on the LAN, in packets and in bytes. You also receive information on traffic, such as, errors, drops, and overruns. Click **Save Results** below the table in the right portion of the screen to export those results into an HTML file.
LAN Usage	Click **Start** to begin collecting the LAN data on receive (RX/Downlink) and transmit (TX/Uplink) traffic in real time (in Mbps). To terminate data gathering click **Stop**.
General Information	
GUI Snapshot	Clicking **Generate** begins generating a series of statistics snapshots which are organized into a series of files and packaged into a compressed archive of HTML files.
Debug Log	Click **Generate** to save a log to a .log file.

Table 28. Diagnostics Tab Parameters and Tests (continued)

Field	Description
Access Points Diagnostics	
CCA Percentage	Clear Channel Assignment result in 0-100%. A higher value indicates there is more medium consumption. Duration is measured in seconds. This function impacts the WLAN service. Select an AP from the drop-down list, specify the duration of the test in seconds, and click **Test CCA**.
CRC Errors	Cyclic Redundancy Check (CRC) errors indicate the number of frames received with errors (accidental changes to raw data). Select an AP from the drop-down list, specify the duration of the test in seconds, and click **Test CRC**. The CRC errors test takes as long as the duration parameter multiplied by the number of radios.
Cable Test	Initiates a data transfer to measure the drop-packets threshold. The recommended duration for the cable test is 1200 seconds.
Overall Test	Initiates all three tests - CCA Percentage, CRC Errors, and Cable Test. The results are displayed in the right portion of the screen.

Chapter 4

Configuring AT-EXLS-3000 System

This chapter contains the following sections:

- “Powering Edge Switches” on page 130
- “Advanced Configuration – AT-EXLS-3000 Differences” on page 132

This chapter provides instructions for configuring the AT-EXLS-3000 System.

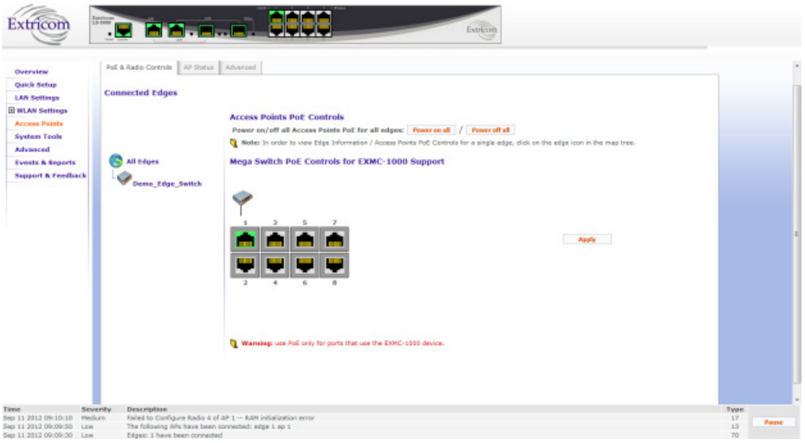
Powering Edge Switches

The Edge switches are independently powered and supply power to the access points via PoE. The PoE output from the AT-EXLS-3000 unit provides the power for the AT-EXMC-1000 media converters, which can be used to provide a fiber optical connection between the AT-EXLS-3000 and the AT-EXMS-1000 switches.

Click **Access Points** in the navigation tree. Under the PoE & Radio Controls tab:

- ❒ Toggle an individual Edge PoE on or off by clicking on its RJ45 connector image. The RJ45 connector image will turn either green or gray depending on whether it has been powered on or off, respectively. To immediately activate your selection, click the **Apply** button on the right side of the configuration screen.
- ❒ An image of an AT-EXMS-1000 switch connected to the RJ45 connector will appear if an Edge switch is powered on and connected to the port.
- ❒ To power on all of the Edge Switches with PoE, click the **Power on all** button on the right side of the screen.
- ❒ To power off all of the APs with PoE, click the **Power off all** button on the right side of the screen.

Note
The image of the switch on top of the page also color-illustrates the PoE status of the APs.



Access Points PoE Controls

Power on/off all Access Points PoE for all edges: Power on all / Power off all

Note: In order to view Edge Information / Access Points PoE Controls for a single edge, click on the edge icon in the map tree.

Mega Switch PoE Controls for EXMC-1000 Support

Warning: use PoE only for ports that use the EXMC-1000 device.

Time	Severity	Description	Type
Sep 11 2012 09:10:10	Medium	Failed to Configure Radio 4 of AP 1 -- RAM initialization error	17
Sep 11 2012 09:09:50	Low	The following APs have been connected: edge 1 ap 1	13
Sep 11 2012 09:09:30	Low	Edges: 1 have been connected	70

Figure 66. Access Points PoE & Radio Controls Page

Note
In the above image, the AT-EXLS-3000 is displayed as “Mega Switch”.

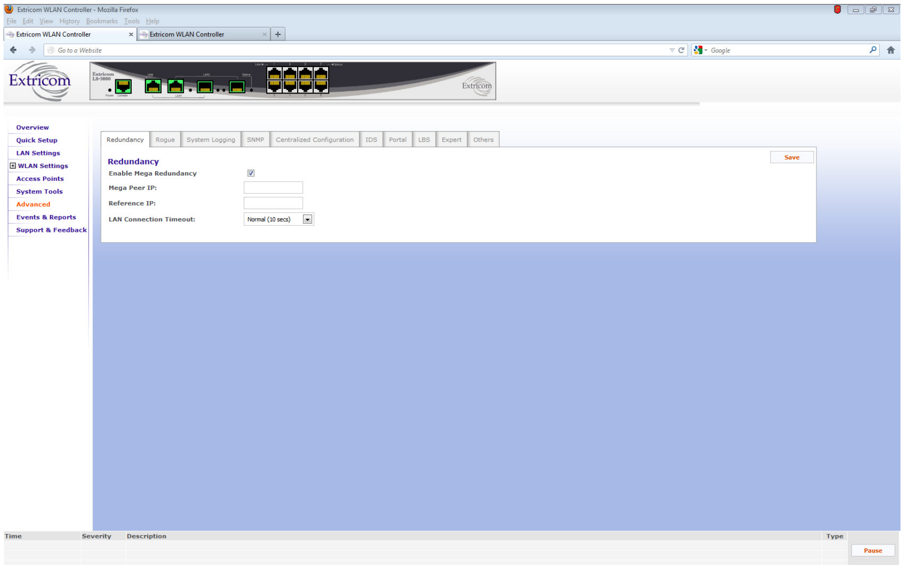
For information on configuring the system tools, refer to “System Tools Configuration” on page 99.

Advanced Configuration – AT-EXLS-3000 Differences

To configure advanced features, select **Advanced** from the navigation tree. For more detailed information, refer to “Advanced Configuration” on page 107.

Redundancy

Switch redundancy refers to redundancy over wired LAN media and provides the master-to-backup auto fall-back functionality. Both switches serve a single BSSID until either of them is at fault. As soon as one of the switches fails, the operational switch serves mobile devices by itself with no human intervention. The eventual replacement of the faulty switch does not necessitate any interruption in service, while returning to a fully redundant mode.



Redundancy

Enable Mega Redundancy ☑

Mega Peer IP:

Reference IP:

LAN Connection Timeout: Normal (10 secs)

Figure 67. Redundancy Configuration Tab

Note
Redundancy is only available if the appropriate license is installed. To check whether redundancy has been installed, refer to “License” on page 106. If it is not available, contact your Allied Telesis distributor.

Redundancy Fields for Primary Switch

Table 29 lists all available options under the Redundancy configuration screen fields.

Table 29. Redundancy Configuration Tab Parameters for a Primary Cascade Switch

Field	Description
Enable Mega Redundancy	Select this field to enable redundancy.
Mega Peer IP	IP address of the AT-EXLS-3000 device on the LAN.
Reference IP	IP address of a reference device on the LAN. This is used to test connectivity to the LAN. The reference device must be operational and respond to pings.
LAN Connection Timeout	Interval in seconds before a timeout state occurs. The default is 10 seconds.

Once the changes are made, you must click **Save**, then go to System Tools and apply changes as described in “Apply” on page 99, in order for them to take effect.

When a switch failure or a link failure has been detected, a failover occurs, and the switch that remains fully operational goes into standalone mode.

Note
Once the fault that caused the switchover has been resolved, both switches must be rebooted in order for them to return to normal cascade operation. Otherwise, they will continue to operate in standalone mode.

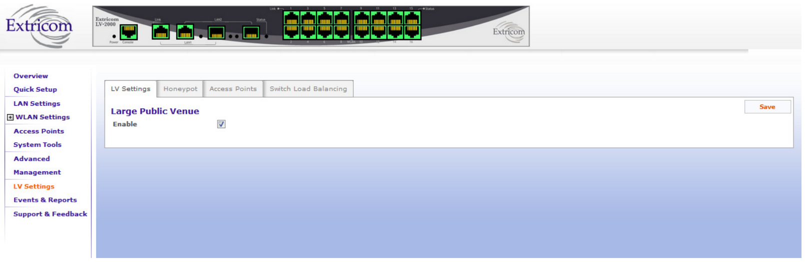
Chapter 5

Configuring AT-EXLV-2000 System

This chapter provides instructions for configuring the AT-EXLV-2000 System.

Advanced Configuration – AT-EXLV-2000 Differences

To configure advanced features, select **Advanced** from the navigation tree. For more detailed information, refer to “Advanced Configuration” on page 107.



Large Public Venue

Enable ☑

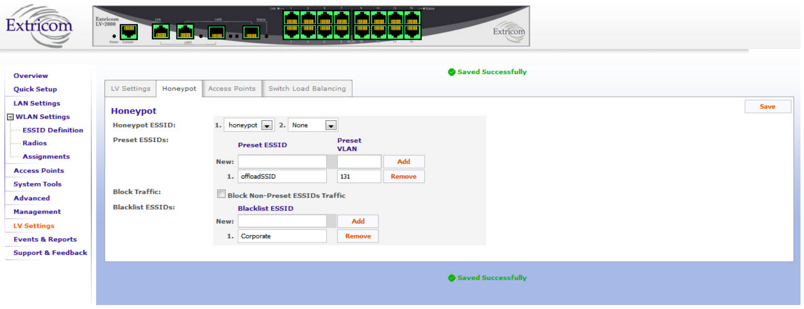
Figure 68. LV Settings

Enabling Large Public Venue

Enabling this option provides for the enhanced functionality to provide the IEEE 802.11 service within large public venue sites.

Configuring Honeypot

The Honeypot configuration provides for reducing the RF level at the site, by providing response to mobile devices that are probing the air and keep trying to reconnect their last location, such as: Home WLAN network, Office WLAN network, or any other WLAN service. The mobile devices that get stuck to the Honeypot will stop probing, thus allowing the air for real network traffic.



Saved Successfully

Honeypot

Honeypot ESSID: 1. honeypot 2. None

Preset ESSIDs:

	Preset ESSID	Preset VLAN
New:		
1.	offloadSSID	131

Block Traffic: □ Block Non-Preset ESSIDs Traffic

Blacklist ESSIDs:

	Blacklist ESSID
New:	
1.	Corporate

Saved Successfully

Figure 69. Honeypot

Table 30. Honeypot configuration

Field	Description
Honeypot ESSID	Select one ESSID from the drop-down menu: ❒ None – if there is no need for Honeypot on the configured WLAN switch. ❒ 'Honeypot-Name' – Select the ESSID, which has been configured to be the honeypot. Refer to Table 31 for honeypot ESSID configuration.
Preset ESSIDs	Allows configuring certain SSIDs within the honeypot to be assigned unique VLANs.
Block Traffic	If checked, client traffic (apart from DHCP) on this SSID will not be passed on to the LAN.
Blacklist ESSIDs	Add all the ESSIDs that serve real traffic and MUST NOT get stuck in the Honeypot.

The Honeypot ESSID should be configured as listed in Table 31:

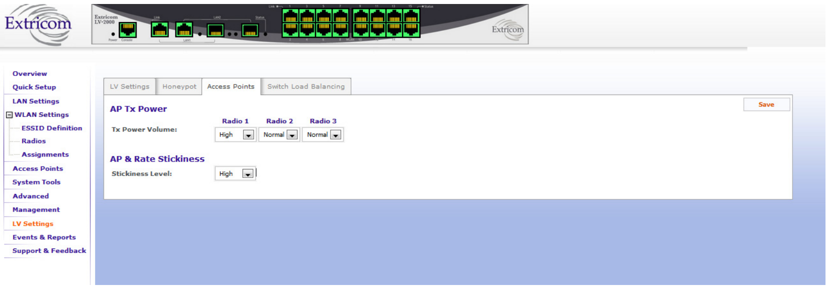
Table 31. Honeypot ESSID Configuration

Field	Value	Description
ESSID Name	<Name>	Any alphanumeric name
Allow Default ESSID	Enable	Allow connection without requesting specific ESSID
Display ESSID in Beacon	Disable	ESSID does not appear in Beacon
Allow Store & forward	Disable	All traffic goes through the WLAN switch
Allow Inter-ESS forward	Disable	All traffic goes through the WLAN switch
Enable Multicast	Disable	Multicast is not supported
MAC ACL	Disable	MAC Access List is not supported
802.11d support	Disable	802.11d is not supported

Table 31. Honeypot ESSID Configuration (continued)

Field	Value	Description
Enable ARP Caching	Enable	Provide immediate response to ARP request directed toward the WLAN stations. The switch answers on behalf of the WLAN stations.
Bandwidth Saving ARP Caching	Enable	Reduce the number of ARP packets sent over the wireless medium
VLAN	<Tag>	Any number with the 1 – 4096 range
Disassociation Timeout	3600	The amount of time in seconds that a mobile device can remain inactive before automatically disconnecting it from the network
Encryption	None	

Configuring Access Point Parameters



AP Tx Power

	Radio 1	Radio 2	Radio 3
Tx Power Volume:	High	Normal	Normal

AP & Rate Stickiness

Stickiness Level: High

Figure 70. LV Access Point Parameters

Configure Tx power for the AT-EXLV-2000 to streamline the large-venue deployment in terms of user density and capacity: By increasing and decreasing Tx power, the large-venue deployment can be fine-tuned.

Select the Tx power of all the radios at all the access points from the drop-down menu:

- Highest: Highest available power of the radio (15 dBm).
- High: Lower (3 db) power mode of the radio (12 dBm).
- Normal: Lower (3 db) power mode of the radio (9 dBm).

Tx Power should be configured according to the WLAN design consideration:

- ❒ Comply with local EIRP regulation, taking into consideration the configured directional antenna.
- ❒ Calculate the link budget to allow for the maximum rate for the mobile devices around the site.
- ❒ Reduce the power level in order to reduce the overall noise and interference levels at the site.

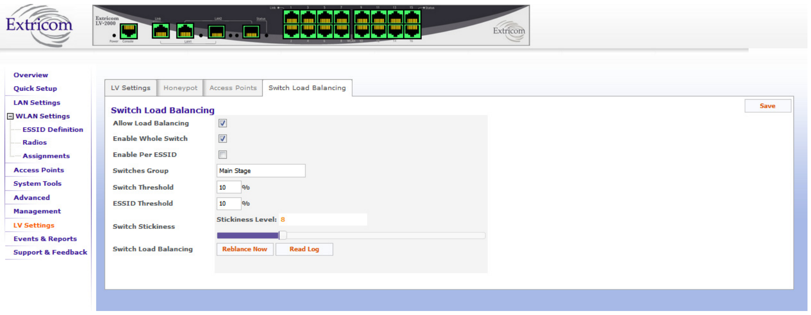
Select the AP and Rate Stickiness from the drop-down menu:

Table 32. Rate Stickiness Configuration

Value	Description
Normal	The mobile device is served by the optimized access point. This configuration applies to cases in which the mobile devices are moving most of the time, such as, convention centers, casinos, and concourses at arenas or stadiums.
High	The mobile device is served by the optimized access point, however, the decision to be served by another access point is evaluated more carefully by the switch, and frequent roaming between access points is eliminated. This configuration applies to cases in which the mobile devices are at the same location along with the event, but can move, such as, the bowl at the arena or open-air stadiums.
Fixed	The mobile device is served by fixed access point.

Switch Load Balancing

Large-venue environments typically have multiple overlapping AT-EXLV-2000 switches in order to provide increased throughput. By utilizing switch load balancing, these switches share client information in order to optimally load balance, as well as minimize client roaming. Switch load balancing can be configured between switches that are defined in the same group. The exchange of information between group switches uses the Inter-Switch Link (ISL) standard protocol.



Switch Load Balancing

Allow Load Balancing	☑
Enable Whole Switch	☑
Enable Per ESSID	□
Switches Group	Main Stage
Switch Threshold	10 %
ESSID Threshold	10 %
Switch Stickiness	Stickiness Level: 8
Switch Load Balancing	Reblance Now Read Log

Figure 71. LV Switch Load Balancing

Table 33. LV Switch Load Balancing

Field	Description
Allow Load Balancing	Enables the Switch Load Balancing feature on this switch.
Enable Whole Switch	Configures the load is balanced for the entire switch.
Enable Per ESSID	Configures the load is balanced per SSID.
Switches Group	Name of the group within the load will be balanced. All switches to be load balanced must have the same group name.
Switch Threshold	Load threshold above the average of the group that triggers this switch to stop accepting new connections.
ESSID Threshold	Load threshold above the average of the group that triggers this switch to stop accepting new connections per ESSID.
Switch Stickiness	If a client that is already associated to another switch in the group attempts to associate with this switch, how much stronger (in dB) the client signal must be for the switch to accept the client.
Rebalance Now	Initiates a load re-balance.
Read Log	Shows load data per switch/ESSID for the switch group.

Chapter 6

Troubleshooting

This chapter contains information on how to troubleshoot the Extricom Series WLAN System in the event a problem occurs.

Note
If after following the instructions in this chapter you are unable to resolve the problem, contact Allied Telesis Technical Support for assistance. Refer to “Contacting Allied Telesis” on page 15 for information on how to contact our Technical Support Department.

Table 34 lists problems you may encounter with your WLAN and provides possible solutions.

Table 34. Troubleshooting

Problem	Solution
The AP Power LED is not lit	❒ Verify that the AP Ethernet cable is connected to the switch and to the AP. The APs get PoE from the switch. ❒ Verify that the AP is not turned off in the Access Points configuration page (refer to “Access Points” on page 96).

Table 34. Troubleshooting (continued)

Problem	Solution
A wireless device cannot associate with a specific ESSID	❒ Verify that the wireless device supports the same 802.11 standard as configured for the ESSID (802.11/a/b/g). ❒ Verify that the wireless device is set to connect to the specific ESSID. ❒ Verify that the wireless device supports the security standard used by the ESSID, e.g., WEP. ❒ Verify that the security settings are configured to use the same authentication method. ❒ If the RADIUS Server is used, verify that the wireless device is registered and has the necessary authorization.
Cannot connect to the Extricom Series web configuration pages	❒ Verify that the switch is connected to the LAN. ❒ Verify that the correct IP address is used.
Low data rates	❒ Verify that the switch was not mistakenly configured to use low data rates. ❒ Verify that there is no additional cause of interference (e.g., an additional WLAN network in the same proximity using the same frequencies as the Extricom Series WLAN, that there are no cordless phones using the same frequencies, or microwave oven interference).
Wireless devices disconnect in a specific location	❒ Verify that there is no additional cause of interference (e.g., an additional WLAN network in the same proximity using the same frequencies as the Extricom Series WLAN, that there are no cordless phones using the same frequencies, or microwave oven interference). ❒ Add an additional AP to cover the area. Plug another AP into the switch, or relocate an existing AP.

Table 34. Troubleshooting (continued)

Problem	Solution
Cannot access the switch's web configuration GUI	❐ Verify that the workstation on which the web browser is running is connected to the same LAN as the switch. ❐ Verify that the URL entered for the switch begins with https.

Chapter 7

Northbound SNMP Traps

This chapter lists and describes the SNMP traps sent by the Extricom Series switch over the northbound interface.

SNMP traps will only be sent if enabled in the switch configuration. Furthermore, some traps will only be sent if a specific feature is configured (for example, traps 28-30 will only be sent if Rogue AP Detection is configured on the switch).

All SNMP traps are sent according to RFC 1157 SNMPv1.

Table 35. SNMP Traps

Trap No.	Trap Name	Description
1	Client Association	This trap is sent whenever a client successfully associates with the switch. The trap includes the client MAC address and AID, as well as the BSSID and ESSID, to which the client is associated.
2	Client Disassociation	This trap is sent whenever a client disassociates from the switch. The trap includes the client MAC address and AID, as well as the BSSID and ESSID, to which the client is disassociated. The disassociation reason code is also sent.

Table 35. SNMP Traps (continued)

Trap No.	Trap Name	Description
4	EAPOL Key Error	A client attempted to associate using WPA, but there was an error with the EAPOL key. The trap details which of the following errors occurred: the key does not exist, there is a timeout, the key does not match, or the cypher does not match.
13	AP Connected	One or more APs have been connected to the switch (AP has been physically connected via Ethernet cable, or it was already connected, and PoE has been enabled). The AP number corresponds to the port number on the switch to which the AP is connected. Upon switch startup or reconfiguration, this trap is sent listing all the APs connected.
14	AP Off	One or more APs have been disabled. The AP Ethernet cable has either been physically disconnected from the switch or PoE has been turned off. The AP number corresponds to the port number on the switch to which the AP is connected.
19	Redundancy peer connection up	When using Normal (not Cascade) redundancy, this switch has regained connectivity with the peer switch.
20	Redundancy peer connection down	When using Normal (not Cascade) redundancy, this switch has lost connectivity with the peer switch.
21	Redundancy keepalive connection up	When using Normal (not Cascade) redundancy, the switch regained connectivity to the Reference IP.
22	Redundancy keepalive connection down	When using Normal (not Cascade) redundancy, the switch lost connectivity to the Reference IP.

Table 35. SNMP Traps (continued)

Trap No.	Trap Name	Description
25	Redundancy status up	When using Normal (not Cascade) redundancy, this switch has taken over the wireless responsibility. If the secondary switch is issuing this trap, it is because it detected a failure in the primary switch. If the primary switch is issuing this trap, it has recovered from an error and is now resuming wireless responsibility.
26	Redundancy status down	When using Normal (not Cascade) redundancy, this switch has relinquished wireless responsibility. If the primary switch is issuing this trap, it discovered an error (for example, connectivity to the Reference IP is lost), in which case, the trap specifies what the error is. If the secondary switch is issuing this trap, the primary switch has recovered from an error, and the secondary switch is transferring wireless responsibility back to it.
28	Rogue AP lost	Available only when Rogue AP Detection is enabled. This trap indicates that a previously discovered rogue network has stopped transmitting. The trap details if the rogue network was an AP or ad-hoc, the relevant BSSID and ESSID, on which channel the rogue was transmitting, which Extricom Series AP on the switch was closest to the rogue AP, and approximately how far the rogue AP was from the Extricom Series AP.

Table 35. SNMP Traps (continued)

Trap No.	Trap Name	Description
29	Rogue AP found	Available only when Rogue AP Detection is enabled. This trap indicates that a rogue network has been detected. The trap details if the rogue network is an AP or ad-hoc, the relevant BSSID and ESSID, on which channel the rogue is transmitting, which Extricom Series AP is closest to the rogue AP, and approximately how far the rogue AP is from the Extricom Series AP.
30	Rogue AP update	Available only when Rogue AP Detection is enabled. This trap indicates that the status of a rogue AP has been updated. This trap always comes after trap 29. This trap details if the rogue network is an AP or ad-hoc, the relevant BSSID and ESSID, on which channel the rogue is transmitting, which Extricom Series AP is closest to the rogue AP, and approximately how far the rogue AP is from the Extricom Series AP.
43	Intrusion detection Duration attack	Available only when Intrusion Detection is enabled. Indicates that the switch has detected a Duration attack. The trap details the duration length, as well as the transmitting MAC address.
44	Intrusion detection Association Flood attack	Available only when Intrusion Detection is enabled. Indicates that the switch has detected an Association Flood attack. The trap details how many associations were received and within what time interval.

Table 35. SNMP Traps (continued)

Trap No.	Trap Name	Description
45	Intrusion detection Disassociation Flood attack	Available only when Intrusion Detection is enabled. Indicates that the switch has detected a Disassociation Flood attack. The trap details how many disassociations were received and within what time interval. If the event was triggered from a per-station limitation, the trap also includes the client MAC address.
46	Intrusion detection Authentication Failure attack	Available only when Intrusion Detection is enabled. Indicates that the switch has detected an Authentication Flood attack. The trap details how many associations were received and in what time interval.
48	Intrusion detection Authentication Flood attack	Available only when Intrusion Detection is enabled. Indicates that the switch has detected an Authentication Flood attack. The trap details how many authentications were received and in what time interval.
49	Intrusion detection De-Authentication Flood attack	Available only when Intrusion Detection is enabled. Indicates that the switch has detected a De-Authentication Flood attack. The trap details how many de-authentications were received and in what time interval. If the event was triggered from a per-station limitation, the trap also includes the client MAC address.
50	Intrusion detection RF Jamming attack	Available only when Intrusion Detection is enabled. Indicates that the switch has detected an RF Jamming attack.

Table 35. SNMP Traps (continued)

Trap No.	Trap Name	Description
51	Intrusion detection EAPOL Start attack	Available only when Intrusion Detection is enabled. Indicates that the switch has detected an EAPOL Start Flood attack. The trap details how many EAPOL Start packets were received and in what time interval. If the event was triggered from a per-station limitation, the trap also includes the client MAC address.
52	Intrusion detection EAPOL Logoff attack	Available only when Intrusion Detection is enabled. Indicates that the switch has detected an EAPOL Logoff Flood attack. The trap details how many EAPOL Logoff packets were received and in what time interval. If the event was triggered from a per-station limitation, the trap also includes the client MAC address.
53	Intrusion detection De-Authentication Broadcast	Available only when Intrusion Detection is enabled. Indicates that the switch has detected a De-Authentication Broadcast.
54	Radius Timeout	A client attempted to associate to an ESSID using 802.1x authentication. A timeout was reached when attempting to contact the RADIUS server. If the ESSID has a secondary RADIUS server configured, the switch attempts to authenticate the client using this server. The trap details on which ESSID the authentication attempt occurred.
55	Radius Changed selection	This trap will occur after trap 54, if the ESSID has multiple RADIUS servers configured. The trap details from which RADIUS server it is changing and to which server it is changing.

Table 35. SNMP Traps (continued)

Trap No.	Trap Name	Description
56	Last Radius Failed	This trap will occur after traps 54 and 55. If the switch was unable to contact all RADIUS servers, it will try again from the beginning of the RADIUS server list.
57	RF localization failed	The switch localization lock is missing or corrupt: Contact an Allied Telesis representative.
59	Firmware upgrade startup	Switch firmware upgrade has started.
60	Firmware upgrade done	Switch firmware upgrade has ended.
61	Firmware upgrade progress	This trap is sent with a progress update during the switch firmware upgrade.
62	Firmware upgrade failed	Switch firmware upgrade has failed.
63	Reconfigure ended	Switch reconfigure has ended.
65	Radio is not functioning in access points	One or more of the radios in a Channel Blanket is not functioning. The trap details which radio in which AP is not functioning.
66	Radio is functioning normally in all access points	All radios in a Channel Blanket are now functioning normally. Will be sent after all of the errors causing trap number 65 have been fixed.
67	Client Ignore MTU	The client has been sending packets that are larger than the switch MTU, even though the switch has sent several adjust MTU packets to the client.
68	Edge Mode Switchover	The secondary switch in a switch cascade is changing to standalone mode. This trap is sent from the secondary switch and details the reason for the switchover.
69	Reconfigure started	Switch reconfiguration has started.

Table 35. SNMP Traps (continued)

Trap No.	Trap Name	Description
70	Edge Connected	A secondary switch of a switch cascade has connected and synchronized with the primary switch. This trap is sent from the primary switch.
71	Edge Disconnected	A secondary switch of a cascade has been disconnected from the primary switch. This trap is sent from the primary switch. This trap is sent if the link between the primary switch and the secondary switch is down or if the secondary switch is non-responsive
72	Set Client IP	The client now has an IP address set. The trap details the client MAC address, AID, and the IP address it is set to use. The IP address was either received via DHCP or statically set and is being used by the client.
73	Start.sh Started	Start.sh is being run on the switch.
74	Start.sh ended	Start.sh has finished running on the switch.
75	Starting Boot	The switch is being rebooted.
76	Changed Wireless Status (On/Off)	The wireless has been enabled or disabled on the switch. The trap indicates if the wireless has been turned on or off and includes the reason for the change. If the wireless was turned off, all radio LEDs on the APs will be constant red. The wireless on a switch can be turned off or on manually or automatically in case of a switch cascade redundancy event.
77	Radio reset	A problem at the radio required a warm reset. The trap details which radio in which AP required the warm reset.
78	AP reset	A radio required multiple warm resets and was still not working properly, so the whole AP was reset. The trap details which AP was reset.

Table 35. SNMP Traps (continued)

Trap No.	Trap Name	Description
79	POE reset	An AP was reset, but is still not working properly. The AP was power-booted via PoE. The trap details which AP was PoE reset.

Appendix A

Internal Access Point Mounting Template

Figure 72 depicts the internal access point mounting template for mounting the AT-EXRP-22n and AT-EXRP-32n access points. This template can be used as an alternative to the drilling card included with the access point.

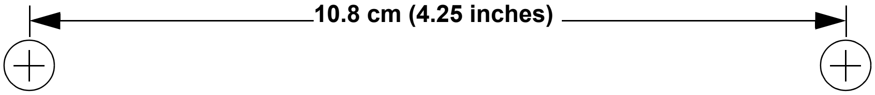


Figure 72. Internal Access Point Mounting Template

Note
Due to variations in printers, when printing this page, printer Page Scaling should be set to “None”, otherwise the diagram may be automatically reduced in size. As a double-check, make sure the distance between drill points is as indicated above.

Appendix B

Certifications

Table 36 lists compliance certifications of Extricom Series access points and switches.

Table 36. Certifications

Access Points	
EMC	ETSI EN 301 489-1V1.9.2:2011 FCC Part 15 Class B
Safety	EN 60950-1:2006+A11+A12+A1 UL 60950-1 IEC 60950-1
RoHS	ROHS2 2011/65/EU
Radio	FCC Part 15 Class C and Part 15 Class E VCCI Technical Requirements V-3/2001.04 EN 300 328 (V1.8.1) EN 301 893 (1.7.1)
Switches	
EMC	ETSI EN 300 386 V1.4.1: 2008-04 ETSI EN 55024:98+A1:2001+A2:2003 ETSI EN 55022:2006 + A1:2007 FCC Part 15 Class B
Safety	EN 60950-1:2006+A11+A12+A1 UL 60950-1 IEC 60950-1
RoHS	ROHS2 2011/65/EU