EXTRICOM WLAN SYSTEM USER GUIDE

EXSW-400/800
EXSW-1200/2400
MULTI SERIES 1000
EXRP-20/40/30N
EXRP-20E/40E/40EN

For System Firmware Release 4.2
Document Version 4.1

Copyright

Important Notice:
Read this user manual, safety instructions, and the release notes for your switch firmware, before installing and operating the Extricom WLAN system.

Disclaimer

Extricom makes no representations or warranties whether express or implied, that the Extricom 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 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.

> **!** ***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 Extricom Ltd. is strictly prohibited and could void the user's license to operate the equipment.***

> ✍
>
> - ***Extricom access points are for indoor use only.***
> - ***The maximum antenna gain is 4dBi***
> - ***An Extricom 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 :***
>   - ***The same information cannot be transmitted over separate Radio modules***
>   - ***Radio modules cannot transmit simultaneously over the same radio channel***
>   - ***Client can transmit and receive data through one Radio module.***

> **!** ***Please check the release notes for your version of Extricom 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 are country dependent and the firmware 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

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.

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

1) This device may not cause harmful interference
2) This device must accept any interference received, including interference that may cause undesired operation.

Important Note:

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 e.i.r.p. 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 e.i.r.p. 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 e.i.r.p. 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 e.i.r.p. category. However, remote stations of point-to-multipoint systems shall be permitted to operate at the point-to-point e.i.r.p. limit provided that the higher e.i.r.p. is achieved by employing higher gain directional antennas and not higher transmitter output powers.

Table of Contents

About This Guide

This guide provides detailed instructions for installing, configuring, and troubleshooting the Extricom EXSW-400/800/1200/2400 and Multi Series 1000 WLAN switches and Extricom EXRP-20/40/30n and 20E/40E/40En UltraThin™ Access Points (APs).

This version of the user guide has been updated to include product changes up to and including switch version 4.2.43.04.

Audience

This guide is intended for enterprise IT managers and system installers who are familiar with installing and configuring networks.

Conventions

✍	This is a note. It emphasizes important information to users.

-	***This is a caution. A caution warns of possible damage to the equipment if a procedure is not followed correctly.***

!	***A warning alerts you to important operating instructions.***

Safety Precautions

Follow the instructions in the guide to ensure proper installation and operation of the switch and APs.

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

- Operate the switch and APs 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 equipments other than Extricom switches.
- The switch contains an internal battery.

!

- ***CAUTION - Always replace the battery with the same type to avoid the risk of explosion.***
- ***Dispose of used battery according to the instructions provided with the new battery.***

Chapter 1

Introduction to the Extricom Wireless LAN System

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.

Extricom’s WLAN, on the other hand, takes a different and novel 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, Extricom’s innovative approach does away with most WLAN maintenance tasks. Extricom’s WLAN System is specifically designed to provide increased network capacity, seamless mobility, high level of security, and easy installation and configuration.

Overview of the Extricom WLAN System

The Extricom WLAN consists of a wireless switch (EXSW-400/800/1200/2400, &EXSW-1600 based on the Multi Series 1000 platform) connected to a set of UltraThin™ APs (EXRP-20/40/30n and EXRP-20E/40E/40En). The Extricom 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 system is able to create multiple overlapping Channel Blankets from the same physical set of devices, as illustrated in Figure 1.

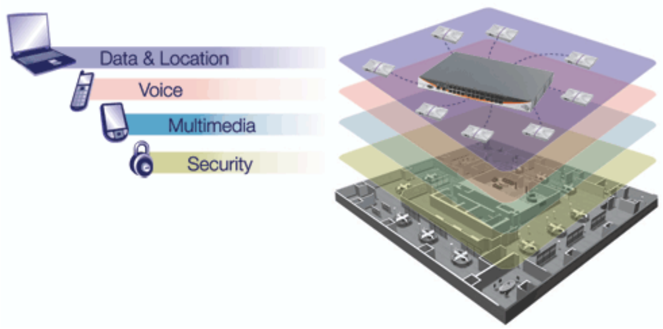


Figure 1: Four Channel Blanket Coverage

The Extricom solution is based on a fully centralized WLAN architecture, in which the switch makes all of 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 address. Even the basics of connecting are different: clients associate directly with the switch, not with the AP. The AP acts as an "RF conduit" to rapidly funnel traffic between the clients and the switch. The Extricom 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 (i.e. the combined coverage of all APs connected to the switch), with interference-free operation and consistent capacity throughout.

As the client moves throughout the blanket, different APs will be in the best position to serve the client at different times. The switch always uses the uplink and downlink path that is optimal to serve the client. While this is going on "behind the scenes," the client never experiences an AP-to-AP handoff (i.e. de-association and re-association), resulting in 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 won't interfere with each other. This is the essence of the TrueReuse™ functionality.

Extricom supports the 802.11n standard. 802.11n 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.

Features and Benefits

Extricom's WLAN system solution offers the following features:

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

- **Multi-Layer WLAN**
  Using multiple radio Access Points, 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 user types, traffic, and roles onto different channels.

- **Same band operation**
  The Extricom WLAN system enables WLAN channels, in the same band (e.g. 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. It is possible to configure up to four channels of same band when using EXRP-40/40E/40En 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 WLAN, wireless device remains on the same channel everywhere within the Channel Blanket. Inter-AP handoffs delays or packet loss do not occur as the client moves across the range of different APs.

- **Wi-Fi Collaboration**
  Extricom's 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 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, Extricom's system performance actually increases with AP density.

- **Wire-line quality VoWLAN**
  Extricom's 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.

- **IEEE 802.11n**
  Extricom architecture supports 802.11n both in the 2.4 GHz and in the 5GHz bands, using both 20MHz and 40MHz wide channels. The advantages of Extricom's architecture are numerous in the 802.11n setting. Among them is the unique ability to deliver full-bandwidth performance in the 2.4GHz band, to both 802.11n and 802.11b/g devices. By contrast, cell-planning architectures cannot be used with 802.11n 40MHz channel-bonding, since the number of non overlapping channels is insufficient for this.

- **IEEE 802.11i support**
  Extricom's 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.

- **Centralized configuration**
  New switches are added to the network via a single Web interface either manually by the user, or automatically using an Extricom protocol.

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

- **SNMP**
  The Extricom system supports SNMP V2 based on standard and private MIBs, enabling the user to configure the switch using SNMP Set operations, read switch status using SNMP Get operation and determine the status of the system, including the status of APs and Redundancy, using SNMP Traps. SNMP is provided for customers wishing to use their existing network management system to administer multiple Extricom switches. Alternatively, the Extricom EXNM-2000 network management software platform is available as a dedicated centralized Extricom WLAN management system.

- **Multiple RADIUS & RADIUS Redundancy**
  The Extricom system supports multiple RADIUS servers per ESSID, enabling the user to set redundancy between these RADIUS servers.

- **Network Time Protocol (NTP)**
  The Extricom 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 Handoff (Opportunistic Key Caching)** - WLAN clients roaming between APs of the same channel blanket within a single switch's coverage area will experience zero-latency mobility. Clients roaming between different Extricom WLAN switches use the standard 802.11 handoff mechanism, which is further facilitated by the opportunistic key caching mechanism in the 802.11i standard. In addition to this, the Extricom system speeds up 802.11i handoff between Extricom 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

- **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 technique enables the Extricom 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) where WLAN client authentication is to be managed via a central RADIUS server.

Overview of the Extricom Switches

The Extricom WLAN switches are connected to Extricom APs to form an Extricom WLAN.

The Extricom EXSW-400, EXSW-800, EXSW-1200, and the EXSW-2400 switches are Fast-Ethernet capable; the EXSW-1600 and EXSW-800G are GbE-capable switches based on the Extricom Multi Series 1000 platform.

The EXSW-400 and EXSW-800 can connect to EXRP-20/40 or EXRP-20E/40E APs to provide legacy 802.11a/b/g service with up to 4 or 8 APs respectively. Alternatively, these switches can connect to EXRP-30n or EXRP-40En APs to provide 802.11n and 802.11a/b/g service. However, both switches can support up to a maximum of two channel blankets, regardless of the Extricom AP model that is being used.

The EXSW-1200 and EXSW-2400 can connect to EXRP-20/40 or EXRP-20E/40E APs to provide legacy 802.11a/b/g service. Alternatively, these switches can connect to EXRP-30n or EXRP-40En APs to provide 802.11n and 802.11a/b/g service; the EXSW-1200 can connect to up to 12 APs and the EXSW-2400 switch can connect to up to 24 APs.

When deployed with EXRP-20/20E access points, the EXSW-1200/2400 switches support up to two channel blankets, and when they are connected to EXRP-40/40E/40En access points, the EXSW-1200 and 2400 switches support up to four channel blankets. When deployed with EXRP-30n access points, the EXSW-1200/2400 can support up to three channel blankets, two with 802.11a/b/g/n support, and one with 802.11a/b/g support.

EXSW-1200/2400 switches are equipped with hardware for two LAN ports with 100 Mbps Ethernet line speed. However, only one uplink port is used currently; the second port is reserved for future port redundancy development. AP connectivity is also 100 Mbps.

The EXSW-800G and EXSW-1600 provide GbE speeds (1,000 Mbps) on both the AP ports and LAN uplink port. The 800G and 1600 can connect to EXRP-20/40 or EXRP-20E/40E APs to provide legacy 802.11a/b/g service. Alternatively, these switches can connect to EXRP-30n or EXRP-40En APs to provide 802.11n and 802.11a/b/g service; the EXSW-800 can connect up to 8 APs and the EXSW-1600 can connect up to 16 APs.

When deployed with EXRP-20/20E access points, the EXSW-800G and 1600 switches support up to two channel blankets, and when they are connected to EXRP-40/40E/40En access points, the EXSW-800G and 1600 switches support up to four channel blankets. When deployed with EXRP-30n access points, these switches can support up to three channel blankets, two with 802.11a/b/g/n support, and one with 802.11a/b/g support.

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, or via the optional EXNM-2000 Network Management System.

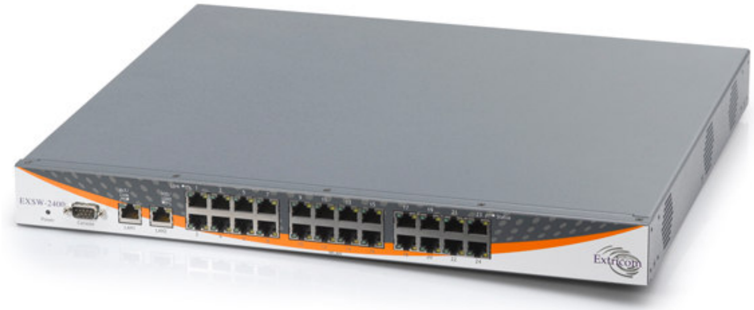


Figure 2: Extricom EXSW-2400 Switch

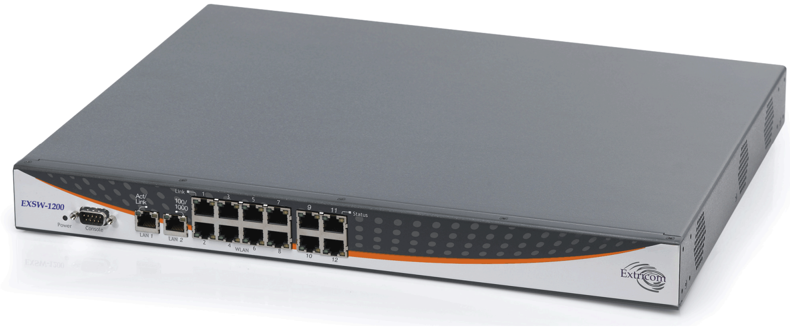


Figure 3: Extricom EXSW-1200 Switch

The Extricom EXSW-1200 is derived from the EXSW-2400, with the same hardware and firmware. The only difference between the two models is the number of WLAN ports supported.

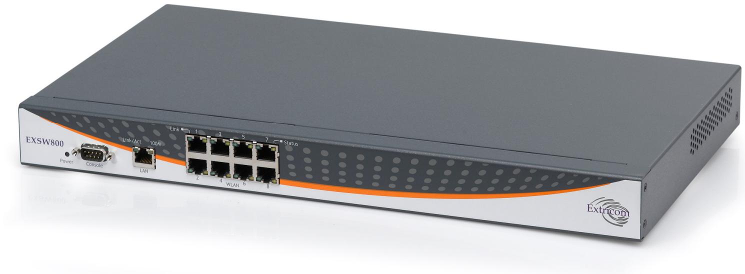


Figure 4: Extricom EXSW800 Switch

The EXSW800 switch only supports two channels, so when it is connected to EXRP-40, only two radios will operate.

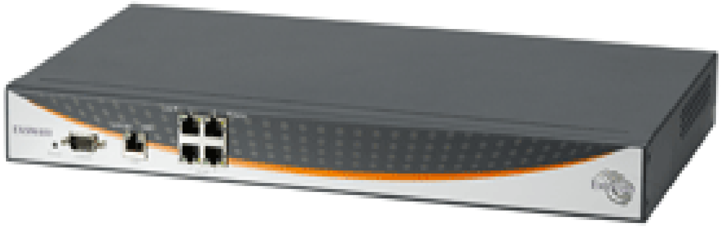


Figure 5: Extricom EXSW-400 Switch

The EXSW400 switch only supports two channels, so when it is connected to EXRP-40, only two radios will operate.

Overview of the Multi Series 1000 Appliance Platform

Figure 6: Extricom Multi Series 1000

The Extricom Multi Series 1000 is a high-performance hardware platform, and is software-configurable to support a range of wireless and networking functions in an Extricom WLAN System.

The Multi Series 1000 is equipped with two RJ45/SFP GBE Combo port uplinks, and 16 GBE PoE edge-side ports. The Multi Series 1000 is therefore capable of performing different wireless and networking functions, depending on the firmware installed on it,

In the current release, the Multi Series 1000 platform is used to support the EXSW-1600, EXSW-1600C, and EXSW-800G. The EXSW-1600, EXSW-1600C, and EXSW-800G are the ultimate platforms for full 802.11n implementation.

The EXSW-1600C is a special version of the EXSW-1600. The EXSW-1600C is designed and licensed for use only as part of a Switch Cascade pair.
The EXSW-1600 can be used as a standalone edge switch or as part of a Switch Cascade pair.

✍ ***SFP modules are not shipped with the Multi Series 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 Access Points

Access Points with Internal Integrated Antennas

Extricom's EXRP-20, EXRP-40 and EXRP-30n UltraThin APs are high-bandwidth devices. The EXRP-20 contains two 802.11a/b/g radios, the EXRP-40 contains four 802.11a/b/g radios, and the EXRP-30n contains two 802.11a/b/g/n and one 802.11a/b/g radio.

The EXRP-20 and EXRP-40 APs have internal diversity antennas – one diversity antenna for each radio. The EXRP-30n possesses three (3) antennas per 802.11a/b/g/n radio (for supporting 3x3 MIMO).

The APs do not require configuration, enabling plug-and-play installation. If stolen, the APs do not pose a security risk, since 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 APs are connected to the Extricom 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 AP.

An EXRE-10 or 1000 range extender can be used between the AP and the switch, for extended reach.

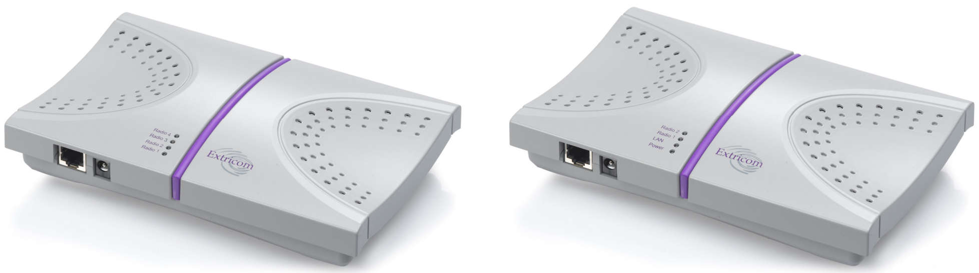


Figure 7: Extricom EXRP-20 and EXRP-40 AP

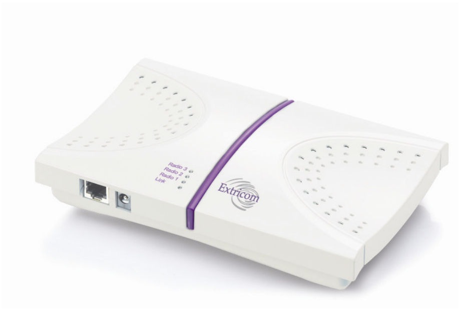


Figure 8: Extricom EXRP-30n AP

Access Points with Connectors for External Antennas

Some applications may require an access point capable of connecting to external antenna(s). The EXRP-20E/EXRP-40E, and EXRP-40En accommodate this requirement. The EXRP-20E/EXRP-40E have the same electronics as the EXRP-20/40 (respectively), but with a metal, plenum-rated casing, and connectors for attaching external antennas. The EXRP-20E contains two 802.11a/b/g radios and has four external antenna connectors. The EXRP-40E contains four 802.11a/b/g radios and has eight external antenna connectors. The EXRP-40En contains two 802.11a/g/n radios and two 802.11a/b/g radios. The EXRP-40En has ten external antenna connectors.

An external antenna may be desired to make the AP less visible by mounting it in the plenum. There may also arise situations where, 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 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.

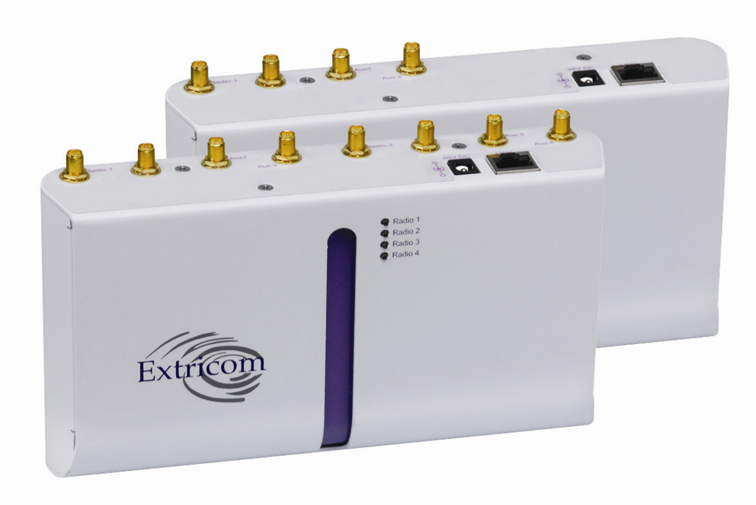


Figure 9: EXRP-20E/40E access points

The EXRP-20E/40E and EXRP-40En APs are connected to the Extricom 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 EXRP-20E/40E and EXRP-40En . For purposes of product homologation testing, Extricom used a "Rubber Duck"-type antenna, 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.

!	With EXRP-20E/40E/40En - Use only xPVC or similar jacket cable which is NEC Article 725 and 444 Compliant and plenum rated per NFPA 262 (UL 910) standard

A Typical Extricom Wireless Network Topology

An Extricom WLAN switch is connected to the wired LAN, and the APs distributed throughout the enterprise. Figure 10 shows a typical Extricom enterprise topology, consisting of an Extricom switch and eight APs.

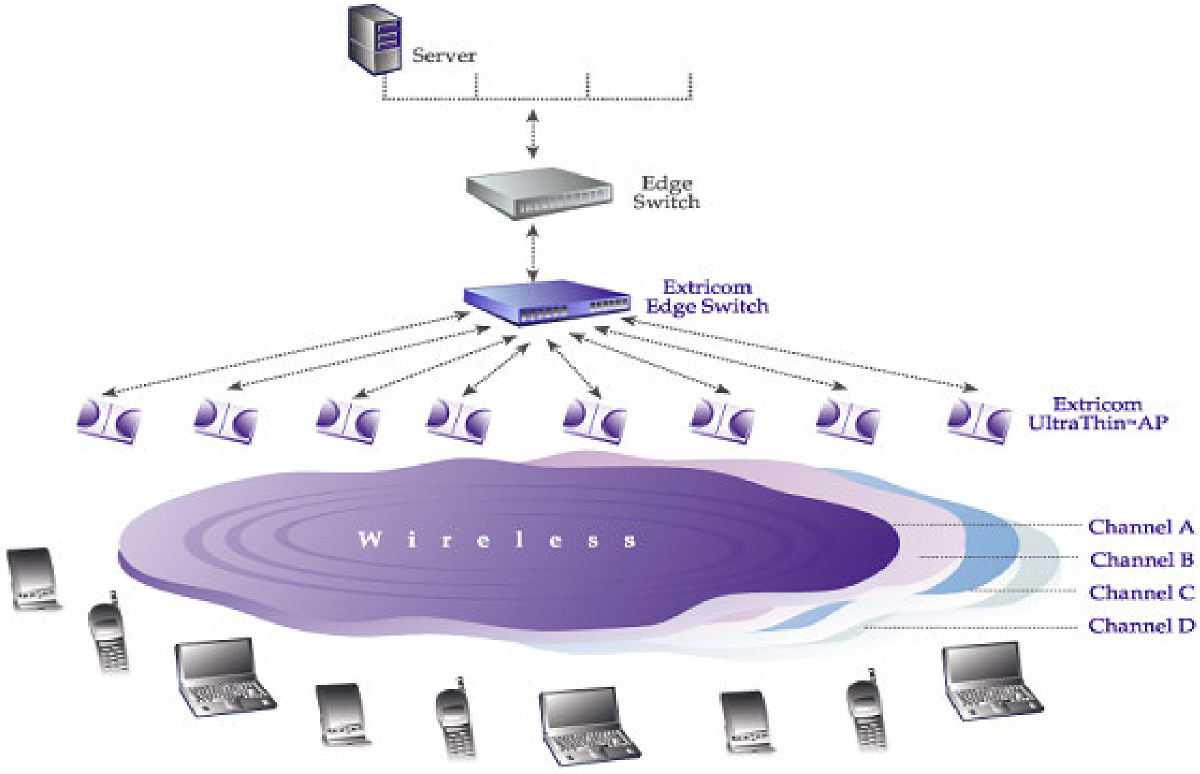


Figure 10: Typical Extricom Typology

Extricom 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 system.

- **Mixing different types of Extricom AP's on the same switch is not permitted, except for EXRP-20 and 20E AP's or EXRP-40 and 40E AP's.**
- **When using the EXSW-400/800 with EXRP-40, EXRP-30n, or EXRP-40En, only two radios will operate.**
- **Extricom APs must be directly connected to the switch to function.**
- **An Extricom range extender or media converter, may be used between the AP and the switch, when extra range is required.**

Switch Cascade (Multi Series 1000 Platform Only)

Switch Cascade is a new Extricom topology in which two Multi Series 1000 switches are interconnected together to create one larger logical switch with enhanced redundancy. One Multi Series 1000 switch serves as the primary, and the other Multi Series 1000 switch serves as the secondary. A diagram of the Cascade topology is shown below, in its standard configuration:

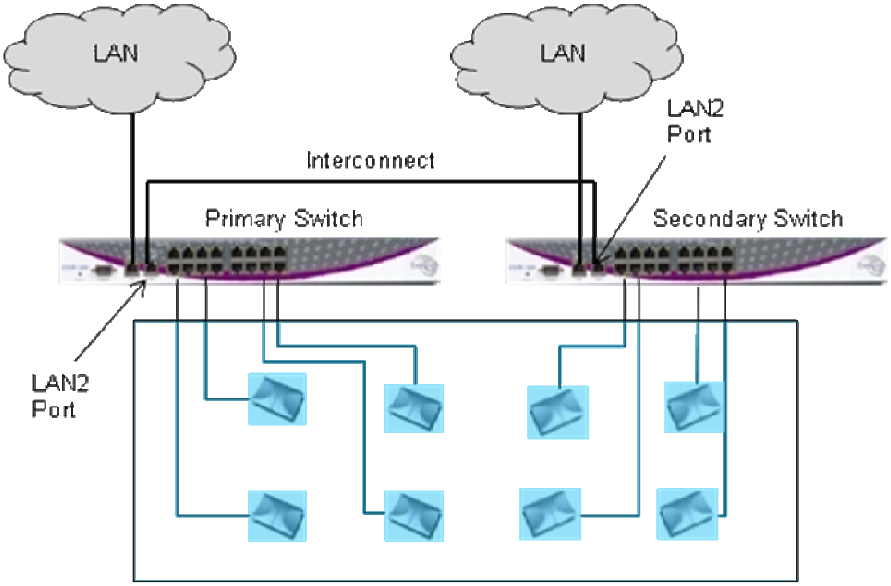


Figure 11: Switch Cascade Topology

The interconnect is connected to the LAN2 port of each switch. See page 26 for more details about the interconnect hardware and maximum length.

The APs of each switch form a seamless channel blanket that extends across the APs of both switches. Up to 4 seamless channel blankets can be deployed. Up to 32 APs can be deployed in the cascade topology.

In the above topology, the switch configuration is redundant, but the APs are not. To achieve AP redundancy, the APs from each switch should be deployed in a mesh configuration, as illustrated below:

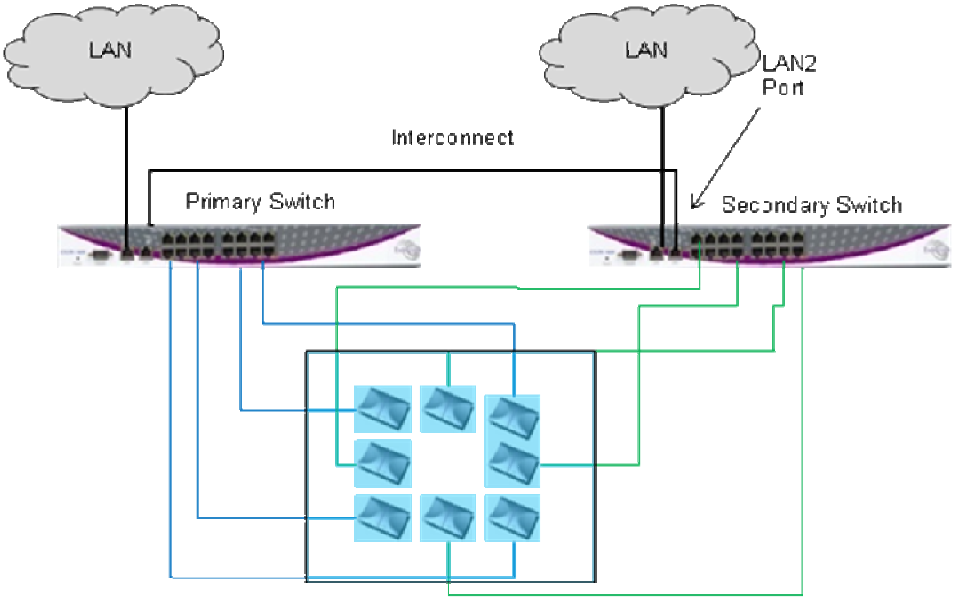


Figure 12: Switch Cascade With AP Redundancy

It is also possible to deploy the APs in a semi-mesh, according to the degree of service required in the event of a failover. In a semi-mesh deployment, most APs are configured as in Figure 12, but one or more APs from the Primary are placed in the coverage area of the secondary, or vice versa.

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 traffic from its own APs. The same is true for traffic downloaded to the APs: the primary switch performs the Extricom edge switch functions, such as determining to which AP to transmit each packet, and the secondary switch routes the traffic it receives to the correct AP.

Heartbeat checks are performed over the LAN links. A failover takes place if there is a critical failure of one of the switches, one of the LAN links, or in the interconnect.

Extricom Support for 802.11n

802.11n is a breakthrough technology that enables Wi-Fi networks to do more, faster, over a larger area. 802.11n Wi-Fi provides optimized connectivity for enterprise computer networking, delivering the range, bandwidth, and performance that multimedia applications and products demand.

For 802.11n deployment, Extricom offers the EXRP-30n, and EXRP-40En APs. The EXRP-30n contains two 802.11a/b/g/n radios and one 802.11a/b/g radio, and the EXRP-40En contains two 802.11a/b/g/n radios and two 802.11a/b/g radios.

All current Extricom switches support 802.11n. However, for new 802.11n deployments, the Multi Series 1000 platform (EXSW-1600/800G) is recommended because of its GbE capability which takes full advantage of the GbE capability of the EXRP-30 and 40En.

Brief Overview of 802.11n

The following section describes at a high level the main features and terms of 802.11n. It also outlines which features of the standard are supported by Extricom products at this time. This section is provided to give customers using Extricom's 802.11n products an overview of 802.11n technology, and to help them understand what parameters need to be to configured on the Extricom switch in order to support 802.11n.

802.11n is a member of the 802.11 family of standards; it can function in both the 2.4 GHz and 5GHz bands using OFDM transmission (as with 802.11a and 802.11g). The emphasis in 802.11n design was mainly on increasing bandwidth, range and performance of the 802.11 protocol itself. This was largely achieved by using multiple transmitters/receivers (MIMO) and enhancements to the OFDM PHY and 802.11 MAC layers.

MIMO

Definition: 802.11a/b/g devices used SISO architecture (single input, single output) for transmitter and receiver paths. 802.11n uses MIMO (Multiple inputs / multiple outputs) architecture. That is, multiple transmitter and multiple receiver antennas **(NxM)** are used to support multiple, simultaneous data streams**.**

Extricom 802.11n: Extricom Access Points are equipped with three receivers and three transmitters, so as to make 3x3 MIMO possible. Initially, however, the firmware in the radio chipset will operate in a 3x2 MIMO configuration. This will be firmware upgradeable when the chipset manufacturer makes this enhancement available.

Data Streams

Definition: Spatial multiplexing divides data into multiple streams and sends it simultaneously over multiple paths using the multiple transmitters (antenna) over the channel. These streams are recombined by the multiple receivers to get the original data.

Extricom 802.11n: Extricom Access Points support two data streams over the 3x3 transmitter/ receivers.

Channel Bonding

Definition: 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 where a full 40-MHz wide channel can be used. This offers approximately twice the throughput of a 20-MHz channel.

Extricom 802.11n: Extricom products support 20 and 40MHz channels *both* in 2.4GHz and 5GHz.

Guard Interval

Definition: In OFDM, inter-symbol interference occurs when the delay between different RF paths to the receiver exceeds the guard interval, causing a reflection of the previous symbol to interfere with the strong signal from the current symbol: a form of self-interference. 802.11n allows a shorter guard interval to increase PHY performance.

Extricom 802.11n: Extricom supports configurable guard interval (400 or 800 ns). However, short guard interval is only supported with 40MHz channel.

Frame Aggregation

Definition: 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 overhead than would be the case without aggregating, and because fewer, larger frames are sent, the contention time on the wireless medium is reduced.

Extricom 802.11n: Extricom supports frame aggregation.

Block Acknowledgment

Definition: Block Acknowledgment works in conjunction with frame aggregation, allowing the transmitter to request a block ACK for a multiple frame improving overall performance.

Extricom 802.11n: Extricom supports block acknowledgment.

Operating Modes

Definition: 802.11n defines three modes of operation for 802.11n devices:

1. Legacy mode – In this mode, the 802.11n radio works in legacy 802.11a/b/g mode only.
2. Mixed mode – In this mode the 802.11n radio can work with both 802.11n & 802.11a/b/g clients
3. Greenfield mode – In this mode the 802.11n radio works only with 802.11n clients.

Extricom 802.11n: Extricom products support both Legacy and Mixed modes. Currently there is no support for Greenfield mode. With this release, however, Extricom is introducing a unique feature, the "**HT Only**" blanket in which a specific Channel Blanket can be configured so that only 802.11n clients (working in mixed mode) can associate to it. This enables a deployment to support 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 occurs.

Coexistence

Definition: 802.11n is designed to operate with backward compatibility for 802.11b/g/a devices—the method of operation known as mixed mode that was previously described. 802.11b/g/a, on the other hand, does not have forward compatibility with 802.11n. Therefore 802.11n must protect 802.11b/g/a stations from 802.11n transmissions that may be interpreted as interference

Extricom 802.11n: Extricom supports PHY layer protection (L_SIG protection) for OFDM transmissions (802.11a/g clients). MAC layer protection is supported (Dual CTS protection) for non-OFDM (802.11b) clients.

MCS

Definition: The complexity of 802.11n rate adaptation has given birth to the concept of Modulation Coding Scheme (MCS). MCS includes variables such as the number of spatial streams, modulation, and the data rate on each stream.

Extricom 802.11n: Extricom supports two data streams; therefore MCS 0 to 15 can be configured.

SM Power Save

Definition: The basic 802.11n power save mode is based on the earlier 802.11 power save function. Power save in 802.11n is enhanced for MIMO operation with SM power save mode. Since MIMO requires maintaining several powered-up receiver chains, standby power draw for MIMO devices is likely to be considerably higher than for earlier 802.11 equipment. A new provision in 802.11n allows a MIMO client to power-down all but one RF chain when in power save mode. When a client is in the 'dynamic' SM power save state, the AP sends a wake-up frame, usually an RTS/CTS exchange, to give it time to activate the other antennas and RF chains. In static mode, the client decides when to activate its full RF chains, regardless of traffic status.

Extricom 802.11n: Extricom supports SM power save mode static mode.

Chapter 2

Installing the Extricom WLAN System

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

Unpacking the Extricom WLAN System

The Extricom WLAN system is shipped with the following:

- One Extricom switch.
- CD which contains The Extricom WLAN System User Guide, Release Notes and EULA
- APs (the number of APs is based on customer order and provided in separate boxes) are shipped as part of the overall order.
- One power cable.

Additional Equipment

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

- One CAT-5e/6 cable for each AP.
- One CAT-5e/6 cable(s) for connecting the WLAN switch uplink to the LAN switch.
- A range Extender (EXRE) is required for any AP that will be located between 100 and 200 meters from the WLAN switch.
- For cabling distances over 200 m, media converters must be used.
- Two (EXRP-20/40/30n) stainless steel pan head 8x1-1/4" self-tapping Phillips screws for wall or ceiling mounting each AP (optional).

Determining the Location of the Extricom Access Points

Before installing the switch and access points, plan the placement of the APs. Before permanently mounting the APs, Extricom recommends testing the network (using a laptop client) to identify potential coverage holes. If such a problem exists, relocate an AP or add additional APs to resolve the coverage hole. 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 on top of a closet or bookshelf, or mounted on a wall.

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

EXSW-400/800/1200/2400/Multi Series 1000 Switch (EXSW-800G, EXSW-1600)

The Extricom EXSW-400 switch has 6 connectors and 4 LED types on the front panel (refer to Figure 13).

The Extricom EXSW-800 switch has 10 connectors and 4 LED types on the front panel (refer to Figure 14).

The Extricom EXSW-1200 switch has 15 connectors and 4 LED types on the front panel (refer to Figure 15).

The Extricom EXSW-2400 switch has 27 connectors and 4 LED types on the front panel (refer to Figure 16).

The Extricom Multi Series 1000 Appliance Platform has 21 connectors (refer to Figure 17).

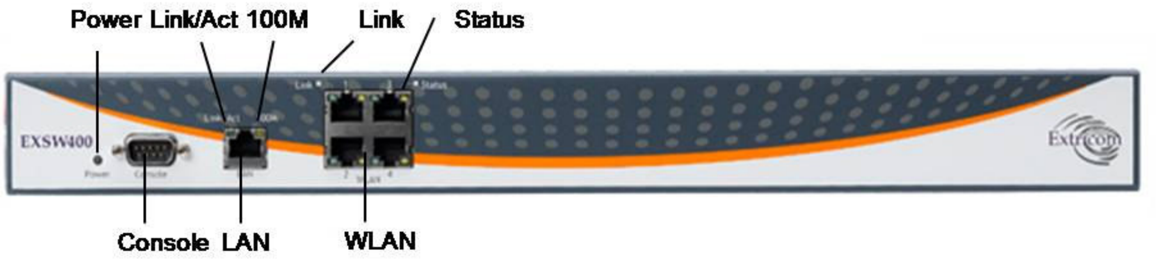


Figure 13: Extricom EXSW-400 Switch

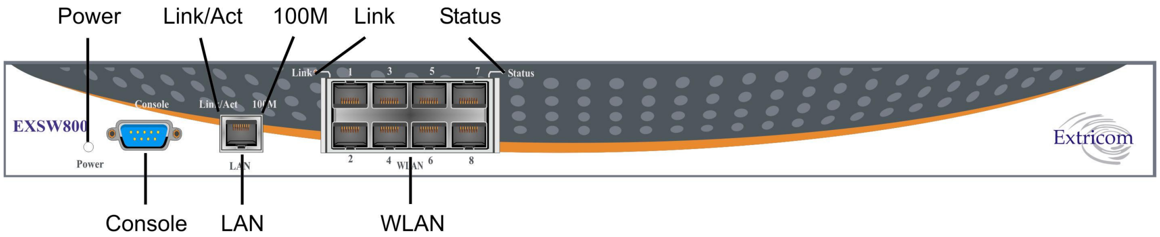


Figure 14: Extricom EXSW-800 Switch

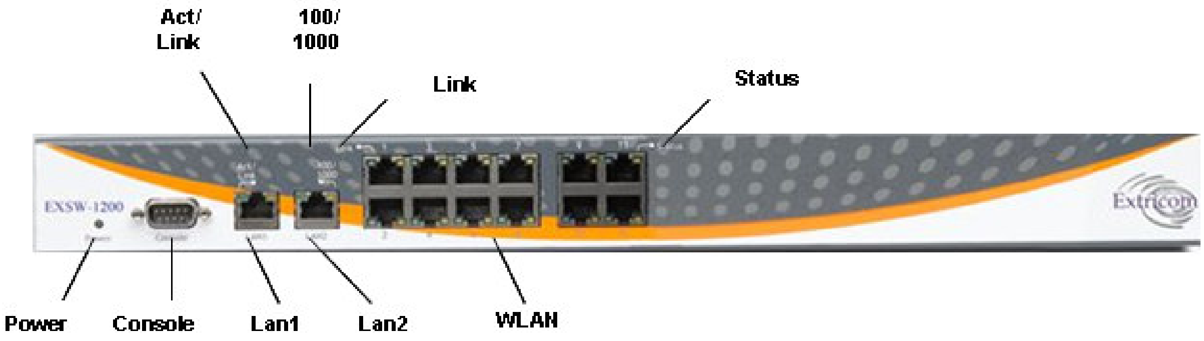


Figure 15: Extricom EXSW- 1200 Switch

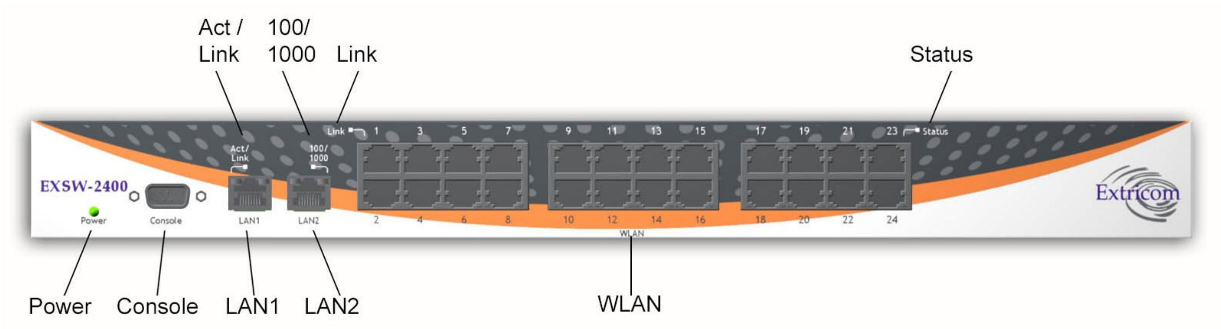


Figure 16: Extricom EXSW-2400 Switch

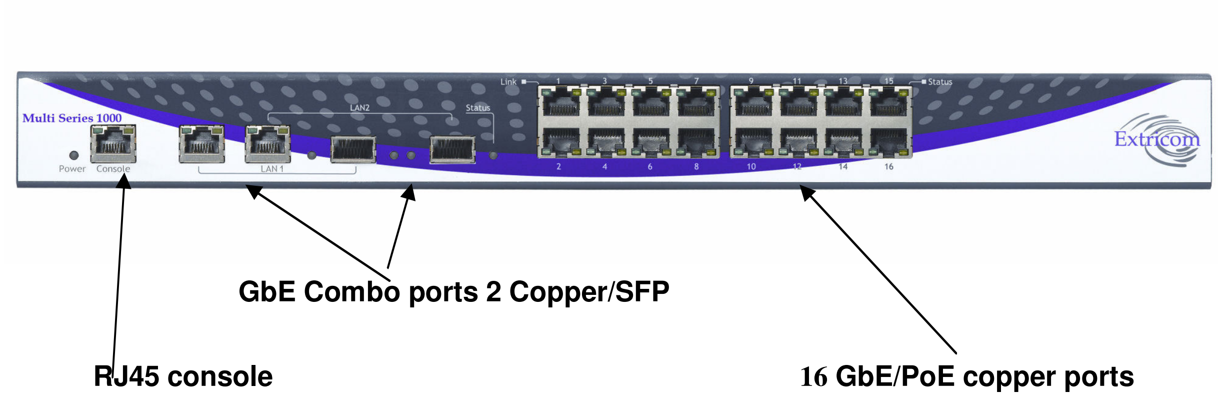


Figure 17: Extricom Multi Series 1000

Table 1 below describes the front panel and connectors of Extricom EXSW-400/800/1200/2400/Multi Series 1000 switches.

Connectors	Description
Console	Serial connector – only to be used by, or as instructed by, Extricom personnel for troubleshooting, support, or maintenance. Can be accessed using a Null modem cable.
LAN	2 Fast Ethernet RJ-45 ports – used to connect the switch to the wired

Connectors	Description
(EXSW-400/800) LAN1, LAN2 (EXSW- 1200/2400)	LAN. ✍ Only LAN1 is used for connection to the wired LAN. LAN2 on EXSW-1200/2400 is currently not in use.
LAN1,LAN2 (Multi Series 1000)	2 GbE RJ-45, 2 GbE SFP combo ports – used to connect the switch to the wired LAN. Use only GbE or SPF. ✍ Only LAN1 is used for connection to the wired LAN. LAN2 is used for Switch Cascade interconnect only.
WLAN (AP) Ports	RJ-45 connectors – used to connect Extricom APs to the switch. These ports provide 802.3AF PoE compatible power. Maximum current: 270 mA, 48 volts. - ***Do not connect any device other than Extricom APs to the WLAN ports.***

Table 1: Extricom EXSW-400/800/1200/2400/1600 Switch Connectors

Table 2 below describes the front panel LEDs of Extricom EXSW-400/800/1200/2400 and Multi Series 1000 Appliance Platform.

LED	Color	Description
Power	None	● No power
	Green	● *Blinking* - switch is loading ● *On* - switch is ready/operational
	Red	● *On* - Error after loading
	Green-Orange	● *Blinking* - RF localization error
LAN, LAN1, LAN2 Ports		
Act/Link	Green	● *On* - connection ● *Blinking* - activity over connection ● *Off* - no connection
100 (EXSW-400/800 only)	Orange	● *On* - 100 Mbps full duplex connection ● *Off* - 10Mbps full duplex or no connection
100 /1000 (EXSW-1200/2400 only)	Orange	● *On* - 100 Mbps full duplex connection ● *Off* - No connection ✍ Only a 100 Mbps LAN connection is supported.

LED	Color	Description
(1000) (Multi Series 1000 only)	Orange	• Not in use. Only a 1000 Mbps LAN connection is supported. In v4.2, Orange LED is not used.
Status (SFP links) (Multi Series 1000 only)	Green	• *On* - 1000 Mbps full duplex SFP connection • *Off* - no SFP connection
WLAN (AP) Ports		
Link	Green	• *On* - connection • *Blinking* - activity over connection • *Off* - no connection
Status (EXSW-400/800/1200/2400 only)	Orange	• *On*- 100 Mbps full duplex connection • *Off* - no connection
Status (Multi Series 1000 only)	Orange	• *On* - 1000 Mbps full duplex connection • *Off* -100 Mbps full duplex or no connection

Table 2: Extricom EXSW-400/800/1200/2400/1600 Switch LEDs

Extricom EXRP-20/20E/40/40E/30n/40En Access Points

Extricom EXRP-20/40/30n APs have two connectors (AP to WLAN switch communication, power) located on the side of the device and four LEDs located on the top of the device (see Figure 18).

In addition to these two connectors, the EXRP-20E/40E APs also have four or eight external antenna connectors respectively (see Figure 19). The EXRP-40En has 10 external antenna connectors.

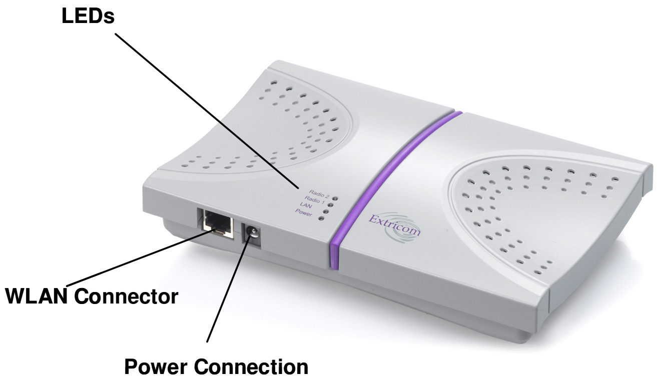


Figure 18: Extricom Integrated Antenna AP

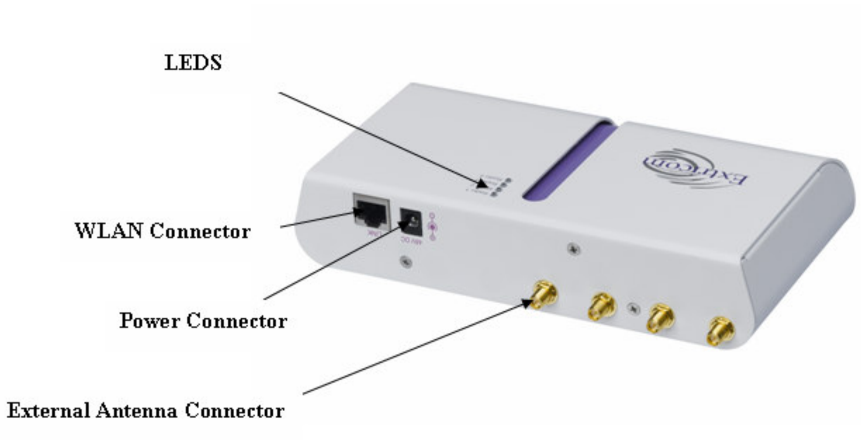


Figure 19: Extricom External Connector Antenna AP (EXRP-20E shown)

Table 3 below describes the Extricom Access Point connectors.

Connectors	Description
Power	✎ External power is not required for most applications. Power is supplied via the Ethernet cable (PoE). In case of an external power requirement (e.g. when media converters are used and POE is blocked), use a UL Listed LPS (Limited Power Source) 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 (+). - ***Due to regulatory requirements in Europe (CE) and the pending certification process for the power supply connector, an external power supply should not be used with EXRP20/40/20E/40E.***
WLAN	RJ-45 connector – used to connect the Extricom AP to the Extricom switch. Power is provided by the Extricom switch to the AP when directly connected to it.

Table 3: Extricom AP Connectors

LEDs	Color	Description
Radio 1	Green	1st Radio is active
	Red	1st Radio is malfunctioning
	Off	1st Radio is off
Radio 2	Green	2nd Radio is active
	Red	2nd Radio is malfunctioning
	Off	2nd Radio is off
LAN	Green (flashing)	Connection to Extricom switch is active
	Off	Not active
Power	Green	On/Off

Table 4: Extricom EXRP-20/EXRP-20E AP LEDs

LEDs	Color	Description
Radio 1	Green	1st Radio is active
	Red	1st Radio is enabled with no assigned ESSID, or malfunctioning
	Off	1st Radio is off
Radio 2	Green	2nd Radio is active
	Red	2nd Radio is enabled with no assigned ESSID, or malfunctioning
	Off	3rd Radio is off
Radio 3	Green	3rd Radio is active
	Red	3rd Radio is enabled with no assigned ESSID, or malfunctioning
	Off	3rd Radio is off
Radio 4	Green	4th Radio is active
	Red	4th Radio is enabled with no assigned ESSID, or malfunctioning
	Off	4th Radio is off

Table 5: Extricom EXRP-40/EXRP-40E/En AP LEDs

LEDs	Color	Description
Radio 1	Green	1st Radio is active
	Red	1st Radio is malfunctioning
	Off	1st Radio is off
Radio 2	Green	2nd Radio is active
	Red	2nd Radio is malfunctioning
	Off	2nd Radio is off
Radio 3	Green	2nd Radio is active
	Red	2nd Radio is malfunctioning
	Off	2nd Radio is off
LAN	Green (flashing)	Connection to Extricom switch is active
	Off	Not active

Table 6: Extricom EXRP-30n LEDs

Connecting the Switch and Access Points

The Extricom 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 CAT-5e/6 100/1000Mbps cable, connect the RJ-45 LAN1 connector located on the front panel of the switch (refer to Figure 16) to the LAN switch.
2. Using a CAT-5e/6 cable, connect each AP (refer to Figure 16) to one of the switch's RJ-45 WLAN connectors.

> If an AP must be located over 100 meters from the switch, an Extricom Range Extender must be used, which enables up to an additional 100m, for a total switch to AP distance of up to 200m.
>
> Switch to AP distances of up to 700m can be supported on GbE connections by using Extricom 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 LEDs on both the switch and connected APs are green.

> Additional APs can be connected /disconnected while the switch is active.

Mixing AP types in the same deployment is not permitted, except for EXRP-20 and 20E APs, or EXRP-40 and 40E APs.

When using the EXSW400/800 with EXRP-30n/40E/40En APs, only two radios will operate.

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

- Each converter requires external power
- 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. Note both ends of the fiber termination must be in the same (SFP) mode.

To connect a switch cascade:

1. Connect the primary and secondary switch to the LAN and to its APs, as directed in the section above.
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 the chart on the following page for important switch interconnect guidelines
4. Connect the switch interconnect from the LAN2 connector located on the front panel of the primary switch, (refer to Figure 17) to the LAN2 connector located on the front panel of the secondary switch.

✍ The maximum length of the primary to secondary switch interconnect is computed according to the following tables: (all distances in meters)

Interconnect Using CAT-5e/6 100/1000Mbps Cable:

Distance Between Secondary Switch and Its Farthest AP	Max. Switch Interconnect Distance (Copper Interconnect Cable)
50	150
100	100
150	50
175	25
190	10

Interconnect Using Fiber Media Cable:

Distance Between Secondary Switch and Its Farthest AP	Max. Switch Interconnect Distance (Fiber Interconnect Cable)
50	500
100	300
150	150
175	75

Note: Beyond 100 m, copper-based cables require a range extender.

Mounting the Access Points (Optional)

Extricom EXRP-20E/40E/40En APs can be mounted on the 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.

Extricom EXRP-20/40/30n APs can be mounted on the wall or ceiling. To mount the APs, you will need two stainless steel pan head 8x1-1/4" self-tapping Phillips screws.

To mount the EXRP-20/40/30n Access Points:

1. Place the installation template (refer to *Internal Access Point Mounting* Template in this Guide) on the wall where you want to mount the AP.
2. Mark the "Point for Drilling" locations on the wall.
3. Screw the two stainless steel pan head 8x1-1/4" self-tapping Phillips screws into the wall leaving enough of the screws protruding to enable you to hook the AP over the screw.
4. Align the holes on the back of the AP with the screws and slip the AP into place.

✍ Position the EXRP-20/40 AP so that the connectors are on the bottom left corner of the AP.

The EXRP-20 and EXRP-40 are similar in appearance. Please double-check the LED titles or label on the underside of the unit to make sure you have the right type of AP for your deployment.

The EXRP-20E, EXRP-40E, and EXRP-40En resemble each other but have a different number of external antenna connectors.

Chapter 3

Configuring the Extricom WLAN System

Accessing the Extricom Switch GUI

After connecting the switch and AP, configure the Extricom WLAN system through Extricom's web configuration GUI using a terminal or PC connected to the same LAN as the switch.

To access the Extricom web configuration pages:

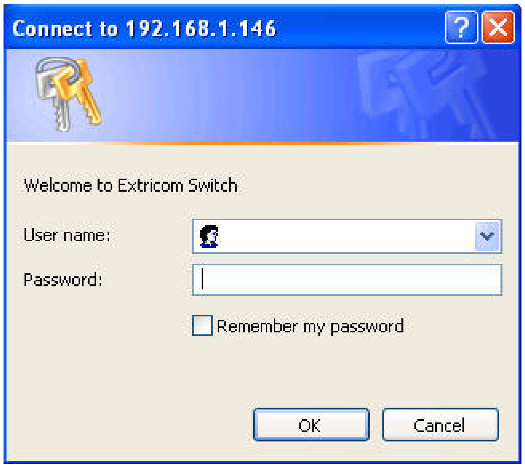
1. In your Web browser, enter the following: **`https://<IP address of the switch>`** where **`<IP address of the switch>`** is the IP address of the switch provided with your purchase (for example, the URL should be https://1.2.3.4 if the IP address of the switch is 1.2.3.4). Note that **https** must be used, *not* http, in order to initiate a secure browsing session. **https** initiates an SSL session with the switch.

> ✍ 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.

> ✍ 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 below in Figure 20:



Connect to 192.168.1.146

Welcome to Extricom Switch

Figure 20: Login Page

4. Enter your user name and password (as provided by your system installer) and click **OK**. The *Summary* page appears.

> 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.

When System Pop-up Windows Appear In Explorer 8

1. You will receive a notice in the pop-up window that there is a problem with the website's security certificate.
2. Press the **tab key** on your keyboard until you see the link "**Continue to this website (not recommended)**"
3. Click on it.

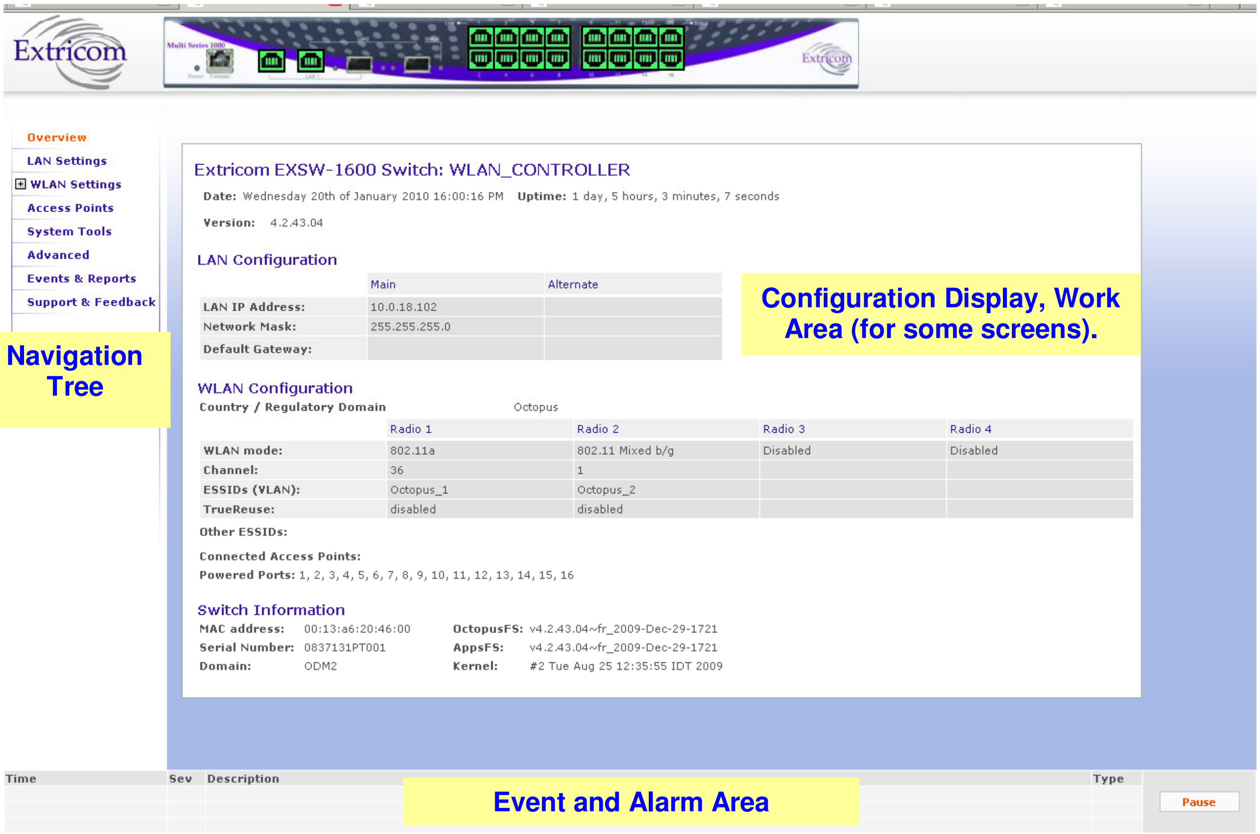
System pop-up windows are used in only a few situations, for example, when clicking on System Tools \Maintenance \Factory Defaults button.

Using the Extricom Web Configuration Pages

The Extricom Web Configuration pages have four main areas:

- Switch image – The Extricom Web configuration page displays an image of the configured switch (the EXSW400, EXSW800, EXSW-1200, Multiseries 1000, or the EXSW-2400); the image shows dynamic status of the PoE of each AP port (grey= PoE off , green=PoE on).
- Navigation tree

- Configuration display, and editable work area (for some screens)
- Event and alarm area



Extricom EXSW-1600 Switch: WLAN_CONTROLLER

Date: Wednesday 20th of January 2010 16:00:16 PM **Uptime:** 1 day, 5 hours, 3 minutes, 7 seconds

Version: 4.2.43.04

LAN Configuration

	Main	Alternate
LAN IP Address:	10.0.18.102	
Network Mask:	255.255.255.0	
Default Gateway:		

WLAN Configuration

Country / Regulatory Domain Octopus

	Radio 1	Radio 2	Radio 3	Radio 4
WLAN mode:	802.11a	802.11 Mixed b/g	Disabled	Disabled
Channel:	36	1		
ESSIDs (VLAN):	Octopus_1	Octopus_2		
TrueReuse:	disabled	disabled		

Other ESSIDs:

Connected Access Points:

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

Switch Information

MAC address:	00:13:a6:20:46:00	**OctopusFS:**	v4.2.43.04~fr_2009-Dec-29-1721
Serial Number:	0837131PT001	**AppsFS:**	v4.2.43.04~fr_2009-Dec-29-1721
Domain:	ODM2	**Kernel:**	#2 Tue Aug 25 12:35:55 IDT 2009

Time	Sev	Description	Type

Figure 21: Typical Web Configuration Page

The *navigation tree* provides access to the following Extricom Web configuration pages:

- *LAN* Settings – used for configuring LAN parameters.
- *WLAN Settings* – used for configuring WLAN parameters including ESSID-related configuration and Radio configuration.
- *Access Points* – used for viewing ports in use, and activating/deactivating PoE.
- *System tools* – used for configuring general system parameters such as passwords, time & date, firmware upgrade, etc.
- *Advanced*– used for configuring advanced features such as redundancy, TrueReuse, 802.11d, IDS, SNMP, and Centralized Configuration parameters.
- *Events & Reports* – used for viewing system events and performance reports.
- *Support & Feedback*

The *work area* displays the information 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 offline configuration file. If you wish to apply these parameters, select the **Apply** option in the **System Tool** web page; this will start the reconfiguration process.

The *event and alarm* area will display real time SNMP trap messages, you can pause the traps by selecting **Pause**.

Please see page 92 for more details.

> ✍ If you do not select **Apply** option (in the **System tool** web page) after clicking **Save**, the new configuration will only take effect after rebooting the switch

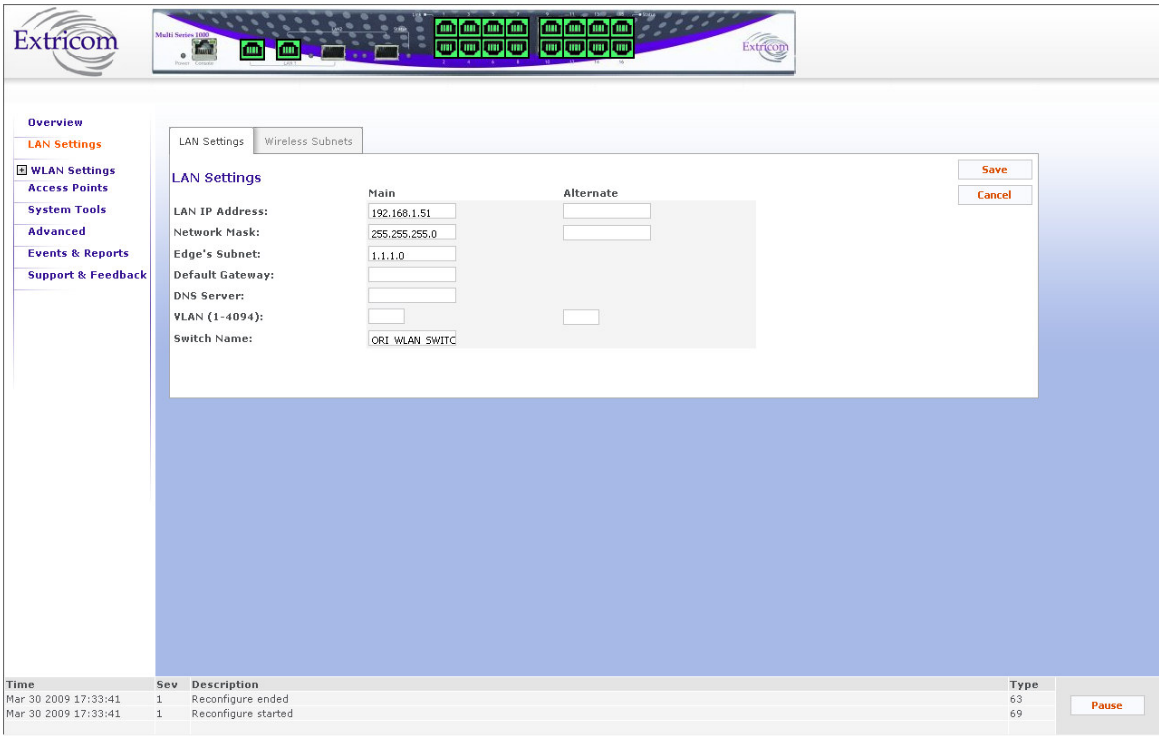
Configuring LAN Parameters

In the *LAN Configuration* page, you can configure the following:

- The LAN ports' IP address and network mask, as well as a backup address and mask.
- The LAN interface and management VLAN tag IDs.
- The default gateway.
- Wireless subnet tab – Configures all wireless subnets (SSID subnets) controlled by the IT manager. This may be required when Captive Portal is enabled.

To configure LAN parameters:

1. Click **LAN Configuration** in the navigation tree. The *LAN Configuration* page appears (refer to Figure 22).



LAN Settings

	Main	Alternate
LAN IP Address:	192.168.1.51	
Network Mask:	255.255.255.0	
Edge's Subnet:	1.1.1.0	
Default Gateway:		
DNS Server:		
VLAN (1-4094):		
Switch Name:	ORI WLAN SWITC	

Time	Sev	Description	Type
Mar 30 2009 17:33:41	1	Reconfigure ended	63
Mar 30 2009 17:33:41	1	Reconfigure started	69

Figure 22: LAN Configuration Page

2. Configure the LAN parameters. Refer to Table 7 for a description of the LAN parameters.

Field	Description
LAN IP Address	Enter LAN IP address used for the switch management. You can add an alternate IP address if you wish to manage the switch from a different network; enter the value in the **alternate** field.
Network Mask	Enter the network mask for the LAN 1 IP address and you can also add an alternate network mask for the alternate IP address defined, enter the value in the **alternate** field.
Edge's Subnet	Subnet of a redundant pair (Primary - Secondary or Main - Standby). Only appears if switch defined as part of a redundant pair.
Default Gateway	Default gateway address.
DNS server	Add the DNS server IP address
VLAN	Management VLAN tag ID for VLAN access to manage the switch. You can add two: one for the LAN 1 IP address through the **Main** field, and an alternate VLAN id for the **Alternate IP** address defined (using the alternate field).
Switch name	A textual descriptor of the switch. Maximum length is 64 characters.

Table 7: LAN Configuration Parameters

3. Click **Save** to save the configuration.
4. When using Captive Portal, if any Captive Portal ESSID has an associated VLAN, you need to enter the IP subnet that you are planning to assign to this VLAN.

> ✍ If you do not select Apply (in the **System tool**s web page) after selecting **Save on one page or more**, when you reboot the switch the new configuration is lost. (refer to Rebooting the Switch on page 62).

Configuring WLAN Parameters

The *WLAN Configuration* page contains three sub-menu pages:

- ESSID definition
- Radios
- Assignments

Configuring ESSIDs

An *ESSID* (Extended Service Set Identifier) is the name of the network. Wireless devices must connect to a specific ESSID which determines the pre-defined set of privileges, settings, and limitations (such as security definitions, access privileges, VLAN assignments, etc.) of the network. Each channel can support multiple ESSIDs, thus creating "virtual" networks on the same channel.

The following is the data structure used by the Extricom system:

- Each radio is assigned *one* channel.
- Each channel can support up to *8-16* different ESSIDs (see note below).
- Each ESSID can be associated with a VLAN tag.
- The same ESSID name *can* be repeated for different channels;

> ✍ On the EXSW-1200, EXSW-2400, and Multi Series 1000, up to 7 ESSIDs are allowed on channel 1, and up to 8 ESSIDs are allowed on each of the remaining channels.
>
> On the EXSW-400 and EXSW-800, up to 15 ESSIDs are allowed on channel 1, and up to 16 ESSIDs are allowed on channel 2.
>
> There is a maximum of 31 ESSIDs per system.

Table 8 below shows an example of possible channel, ESSID and VLAN tag assignments for the EXSW-400 and EXSW-800 switches.

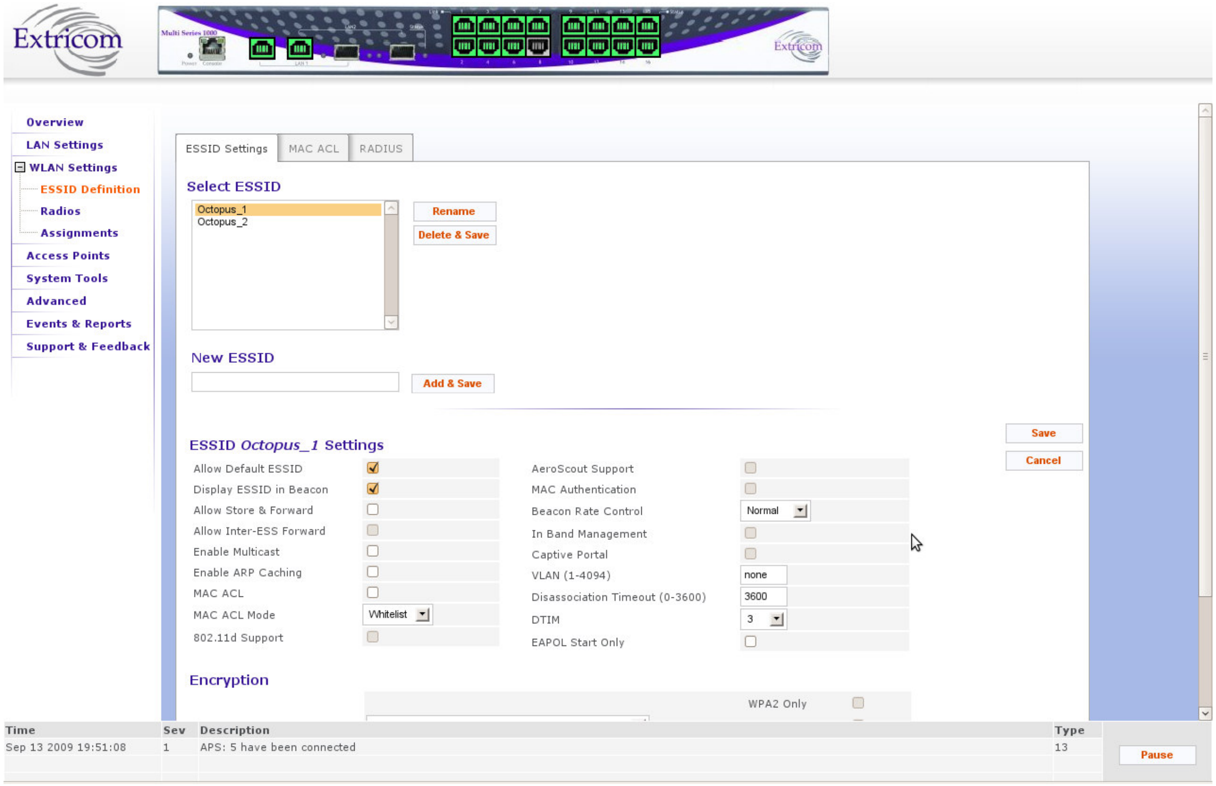
Access Point	Channel	ESSID	VLAN tag
First Radio	1	Network1	1
		Network2	2
		…	…
		…	…
		Network15	15
Second Radio	6	Network16	16

Access Point	Channel	ESSID	VLAN tag
		Network17	17
		Network18	18
		…	…
		…	…
		Network31	31

Table 8: ESSID per channel Example

In the *ESSID* web page, it is possible to **Add** a new ESSID, and to **Rename** or **Delete** an existing ESSID. For a selected ESSID it is possible to configure the following features:

- Allow Default ESSID
- Display ESSID in Beacon
- Allow Store & Forward
- Allow Inter-Ess Store & Forward
- Enable Multicast
- Enable ARP Caching
- Enable MAC ACL
- Enable 802.11D support
- Enable AeroScout
- MAC authentication
- Beacon Rate Control
- In-Band Management
- Captive Portal
- Assign a VLAN to the ESSID
- Set a disassociation timeout
- Set DTIM period
- Encryption parameters
- MAC ACL (in MAC ACL tab) / RADIUS server (in RADIUS tab)



Select ESSID

Octopus_1
Octopus_2

New ESSID

ESSID *Octopus_1* Settings

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

Encryption

WPA2 Only □

Time	Sev	Description	Type
Sep 13 2009 19:51:08	1	APS: 5 have been connected	13

Figure 23: WLAN Configuration Page

When configuring ESSID parameters, refer to the following table for a description of the available parameters:

Field	Description
ESSID	
Select ESSID	Select an ESSID from the dropdown list. To **Add/Delete/Rename ESSIDs** from this list, use the **Add/Delete/Rename** field in the web page.
ESSID option	
Allow Default ESSID	If this option is *enabled*, a wireless device will be allowed to connect to the Extricom WLAN without requesting a specific ESSID (i.e., “default” or “any” ESSID). If this option is *disabled*, then a wireless device needs to connect to a specific ESSID in the Extricom WLAN.
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.

Field	Description
Allow Store & Forward	If this option is *enabled*, two wireless devices connected to the Extricom 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 in the LAN network. ✍ 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 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 at all). 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 in the LAN network.
Enable Multicast	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.
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.
MAC ACL	This option, when enabled, allows a user to add a MAC access list to the specific ESSID. Only clients with MAC address included in this list are allowed to access the network if the ACL mode is Whitelist. If the ACL mode is Blacklist, then these clients are not allowed to use the network. Use the MAC ACL tab to add the MC ACL list
MAC ACL Mode	Select Whitelist or Blacklist. Whitelist mode means that the MAC addresses listed can access the network. Blacklist mode means that the MAC addresses listed cannot access the network.

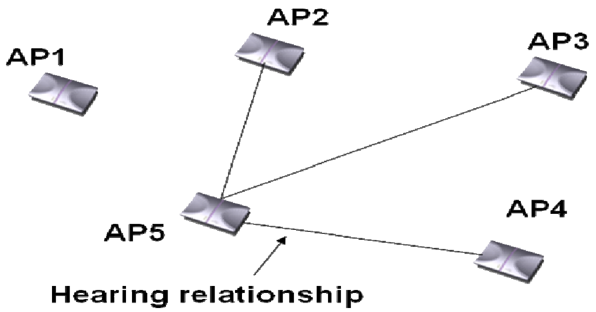
Field	Description
802.11d Support	Enables support of the 802.11d standard.The purpose of this standard is to provide regulation domains for each country in a predefined list. The regulation domains and country information are provided as part of Beacons & Probe response. To use this feature, 802.11d support per ESSID must first be enabled using the Advanced/Others tab folder.
Enable AeroScout	Enable location based services for the ESSID, based on the Aeroscout platform. To use this feature, Aeroscout support per ESSID must first be enabled using the Advanced/Others tab folder. Requires Aeroscout hardware.
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.
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 802.1x authentication. Note that when using this option, the security setting does not allow you to select any 802.1x methods.
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, more beacons shall be distributed on this SSID. 5 levels are available in the pull-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
In Band Management	Select this option if you wish to allow management of the switch through the wireless media through this ESSID. In band management ESSIDs have the same VLAN as set for the switch management VLAN. Once you set this option, the VLAN setting will be automatically updated to the management VLAN as set in the **LAN Configuration** web page. In band management SSID if enabled shall only allow the following security Settings (This should be set from the **Others Tab** in the **Advanced** page): • WPA/WPA2 personal (TKIP/AES & Pre Shared Key Authentication) • WPA/WPA2 Enterprise (TKIP/AES & 802.1x Authentication)

Field	Description
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.
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 from the network.
DTIM Period	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 for the selected ESSID. This is relevant for clients that want to utilize the power management capability. The possible values are 1-5. The default is 3. ✍ A high DTIM value may cause these clients to lose connection with the network.
EAPOL Start Only	Select this option if you want the switch to connect only clients that require the switch to wait for an EAPOL Start. ✍ When this option is selected, clients that do not send an EAPOL start will not be able to connect to this ESSID.

Table 9: ESSID Parameter Descriptions

Beacon Rate Control

The EXSW creates a hearing relationship table between APs. It forms an AP Bundles group (Bundle of APs – group of APs, each bundle can include 1 or more APs). The total number of bundles is equal to the number of APs. Each bundle can send a Beacon at the same time interval. Then a transmission occurs based on round-robin between bundles (every 100msec). In order to compensate sensitive clients for a lost beacon, it is possible to set (per SSID) the Beacon rate control at a higher threshold. Although the feature minimizes the possibility of clients receiving duplicate beacons, there is no guarantee of zero duplicate/missed beacons.



*** Clients near AP1 hear only 1 beacon out of 5, therefore Hearing % is 20%.**

Figure 24: Hearing Topology Example

The following table shows the hearing % of each AP in the diagram above:

AP	Receiving APs	Hearing %
1	1	20
2	2,5	40
3	3,5	40
4	4,5	40
5	2,3,4,5	80

Table 10: Hearing %

Beacon transmission prior to switch s/w v3.4 would have followed the legacy pattern below:

Bundle/Interval	BC1	BC2	BC3	BC4	BC5
1	AP1				
2		AP2			
3			AP3		
4				AP4	
5					AP5

Table 11: Legacy Pattern

However, from v3.4 and later, a Smart Beacon mechanism was implemented, so that the beaconing in the example is actually as shown below (BC rate control of 80%):

Bundle/Interval	BC1	BC2	BC3	BC4	BC5
1	AP1,AP5				
2		AP1,AP2			
3			AP1,AP3,AP5		
4				AP5,AP4	
5					AP1,AP5

Table 12: Smart Beaconing

Configuring Security Definitions

In the *ESSID* page *Encryption* section the following security definitions can be configured:

- Type of encryption.
- Type of authentication.

> 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 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. Select the ESSID for which you want to configure the security definitions from the **ESSID** dropdown list.
2. Configure the security definitions for the selected ESSID. Refer to Table 13 for a description of Security parameters.

Field	Description
Encryption & Authentication	
Choose method	Define the method of encryption and authentication. A combination of encryption and authentication methods may be selected from the options detailed in the drop-down list. **Encryption cipher** There are three types of encryption ciphers available: • *WEP64* – Wired Equivalent Privacy (802.11 encryption protocol). This is a very basic encryption level. (AKA WEP40) • *WEP128* – This encryption is similar to WEP64, but the WEP keys are longer. (AKA WEP104) • *TKIP* – Temporal Key Integrity Protocol. This is a more secure and more advanced method of encryption as a part of the WPA standard. • *AES (CCMP)* – 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. **Authentication method** Authentication is used to identify if a wireless device is authorized to connect to the WLAN, and verifies 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 WEP or WEP104 • *WPA/WPA2 enterprise* – if the cipher is TKIP or AES • *Supported protocols: EAP, TLS, TTLS, PEAP, LEAP and MD5* When choosing an encryption cipher and authentication method, make sure it is compatible with the wireless devices' capabilities. The Extricom 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 transition period. Any security combination (Encryption and Authentication) can be selected from the list and the check boxes.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td><em>WEP Keys</em></td><td>The <em>WEP Keys</em> area is only enabled if the cipher selected in the <strong>Choose Method</strong> field is WEP or WEP104. In the <em>WEP Keys</em> area, you define the WEP Key that is used for encrypting or decrypting.
You can define all four WEP keys. For each key you define, select the input format (ASCII or HEX) and enter the key according to the following table:
<table>
<tr><th>Cipher</th><th>ASCII</th><th>HEX</th></tr>
<tr><td>WEP64
(or WEP64+802.1x)</td><td>5 characters</td><td>10 digits</td></tr>
<tr><td>WEP128
(or WEP128+802.1x)</td><td>13 characters</td><td>26 digits</td></tr>
</table></td></tr>
<tr><td>Transmission Key</td><td>Select the WEP64/WEP128 key to be used for transmitting data from the AP.</td></tr>
<tr><td><em>WPA</em></td><td>The WPA area is only enabled if the cipher selected in the <strong>Choose Method</strong> field is WPA/WPA2 personal</td></tr>
<tr><td>WPA-PSK</td><td>If WPA/WPA2 Personal with Pre-Shared key authentication 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.</td></tr>
<tr><td><em>WPA/RADIUS</em></td><td></td></tr>
<tr><td>Re-key Interval</td><td>Enter the amount of time (in seconds) that elapses before the Group Key is changed.</td></tr>
<tr><td><strong>RADIUS Servers</strong></td><td>Define the RADIUS servers list if:
• The cipher is WEP64/WEP128, and the 802.1x authentication method is selected.
• The cipher is TKIP/AES, and the WPA/WPA2 Enterprise authentication method is selected.
✍ Use Server # 1 if only one server is used. Use consecutive servers if several servers are used.</td></tr>
<tr><td>RADIUS Server-1</td><td>Select the RADIUS server #1 from the dropdown list of RADIUS servers</td></tr>
<tr><td>RADIUS Server-2</td><td>Select the RADIUS server #2 from the dropdown list of RADIUS servers</td></tr>
<tr><td>RADIUS Server-3</td><td>Select the RADIUS server #3 from the dropdown list of RADIUS servers</td></tr>
<tr><td>RADIUS Server-4</td><td>Select the RADIUS server #4 from the dropdown list of RADIUS servers</td></tr>
</table>

Table 13: Security Definition Parameters

Encryption and Authentication methods.

The **Choose Method** dropdown list in **Encryption & Authentication** displays the following options:

- None
- WEP64 (Open)
- WEP128 (Open)
- WEP64 & 802.1x Authentication
- WEP128 & 802.1x Authentication
- WPA/WPA2 personal (TKIP/AES & Pre Shared Key Authentication)
- WPA/WPA2 Enterprise (TKIP/AES & 802.1x Authentication)

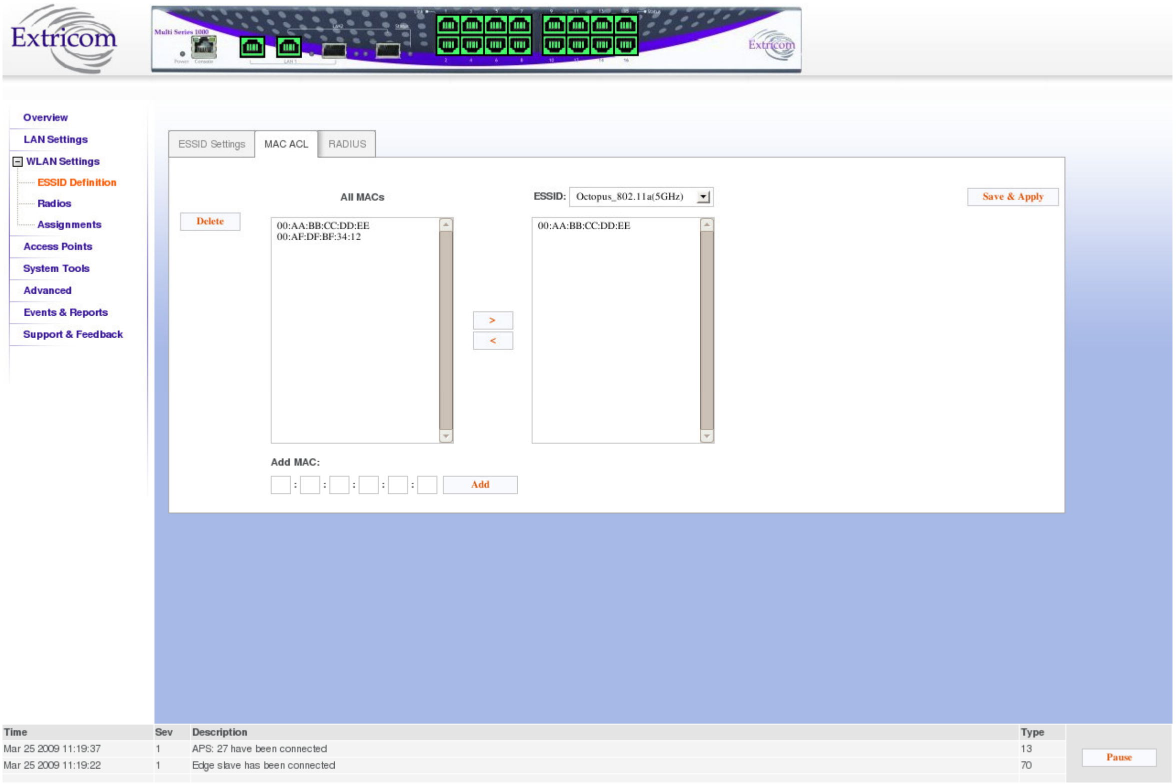
When the “WPA2 Only” is checked, only Clients with WPA2 support are allowed to access the WLAN.

When the “AES Only” 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*”.

Configuring MAC ACL

To configure a per-ESSID MAC ACL, select the MAC ACL tab. In this sub-page, select the ESSID you wish to set MAC ACL for.



ESSID: Octopus_802.11a(5GHz)

All MACs:
00:AA:BB:CC:DD:EE
00:AF:DF:BF:34:12

00:AA:BB:CC:DD:EE

Add MAC: □:□:□:□:□:□

Time	Sev	Description	Type
Mar 25 2009 11:19:37	1	APS: 27 have been connected	13
Mar 25 2009 11:19:22	1	Edge slave has been connected	70

Figure 25: MAC ACL configuration Tab

To configure MAC ACL per ESSID

1. Select an ESSID from a list of configured ESSIDs by selecting it from the dropdown list.
2. Select a MAC address from the **All MACs** list.
3. Use the Right Arrow/Left Arrow to insert/remove this MAC to/from the selected ESSID.
4. You can add a new MAC address to the **All MACs** list by inserting it manually in the **Add MAC** field, then selecting **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 notifies you of a new client , the event message will has a + sign in the **Add** field , once you press it, it is automatically added to the **All MACs** list.
5. Click **Save & Apply** to save the configuration and apply it immediately. There is no need to use the main Apply page.

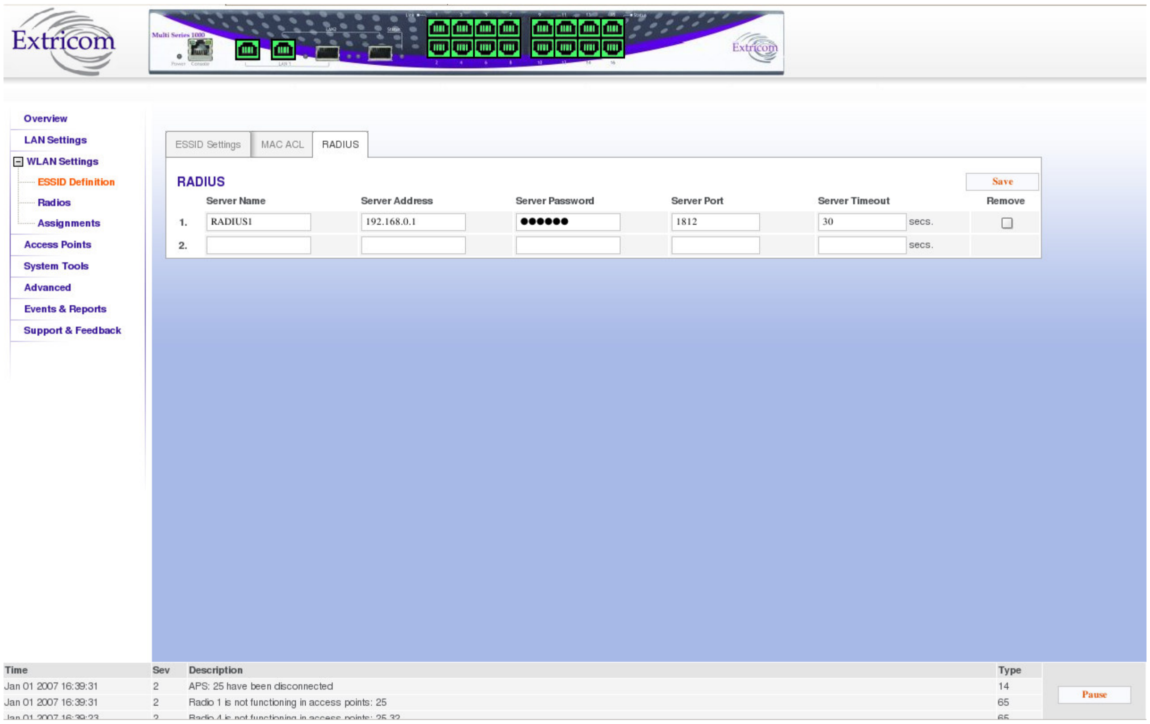
Configuring RADIUS

RADIUS is a common authentication protocol utilized under the 802.1x security standard (often used in wireless networks). Although RADIUS was not initially intended to be a wireless security authentication method, 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.

To configure the RADIUS server option, select the RADIUS tab. The RADIUS tab displays the already configured RADIUS servers and allows you to configure new RADIUS servers in the system RADIUS server bank, and also delete entries no longer needed.



RADIUS

	Server Name	Server Address	Server Password	Server Port	Server Timeout	Remove
1.	RADIUS1	192.168.0.1	●●●●●●	1812	30 secs.	□
2.					secs.	

```
Time                  Sev  Description                                        Type
Jan 01 2007 16:39:31  2    APS: 25 have been disconnected                     14
Jan 01 2007 16:39:31  2    Radio 1 is not functioning in access points: 25    65
Jan 01 2007 16:39:23  2    Radio 4 is not functioning in access points: 25,32 65
```

Figure 26: Radius Configuration Tab

Field	Description
Server Name	Enter the name of the RADIUS server.
Server Address	Enter the address of the RADIUS server.

Field	Description
Server Port	Enter the RADIUS server port.
Server Password	Enter the RADIUS server password.
Server Timeout	Enter the time which the Extricom switch will wait for the RADIUS server response.

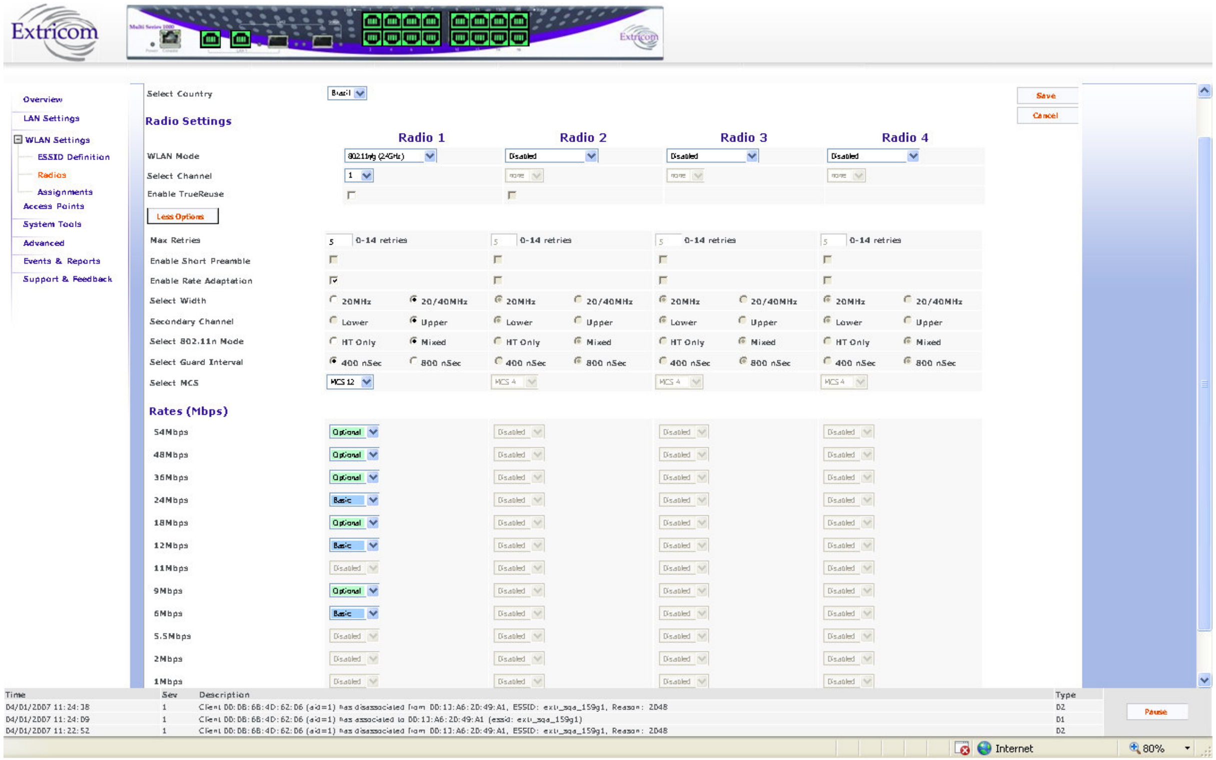
Table 14: Radius Configuration Parameters

Configuring WLAN Radios

To configure the WLAN radios, use the Radios web page. The Radios web page provides the options available for configuring the radios.

When the Radios page is initially displayed, it appears in abridged form. To see all of the configuration options, you must click on the "More Options" button. Then, the window as shown in Figure 27 below appears.

Note that when configuring 802.11a/b/g radios, the 802.11n displayed parameters cannot be configured and are greyed-out.



Select Country: Brazil

Radio Settings

	Radio 1	Radio 2	Radio 3	Radio 4
WLAN Mode	802.11n/g (2.4GHz)	Disabled	Disabled	Disabled
Select Channel	1	none	none	none
Enable TrueReuse	□	□		
Max Retries	5 0-14 retries	5 0-14 retries	5 0-14 retries	5 0-14 retries
Enable Short Preamble	□	□	□	□
Enable Rate Adaptation	☑	□	□	□
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
Select MCS	MCS 12	MCS 4	MCS 4	MCS 4

Rates (Mbps)

	Radio 1	Radio 2	Radio 3	Radio 4
54Mbps	Optional	Disabled	Disabled	Disabled
48Mbps	Optional	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
5.5Mbps	Disabled	Disabled	Disabled	Disabled
2Mbps	Disabled	Disabled	Disabled	Disabled
1Mbps	Disabled	Disabled	Disabled	Disabled

```
Time                 Sev  Description                                                                                      Type
04/01/2007 11:24:38  1    Client 00:0B:6B:4D:62:D6 (aid=1) has disassociated from 00:13:A6:20:49:A1, ESSID: exti_sqa_159g1, Reason: 2048   02
04/01/2007 11:24:09  1    Client 00:0B:6B:4D:62:D6 (aid=1) has associated to 00:13:A6:20:49:A1 (essid: exti_sqa_159g1)                     01
04/01/2007 11:22:52  1    Client 00:0B:6B:4D:62:D6 (aid=1) has disassociated from 00:13:A6:20:49:A1, ESSID: exti_sqa_159g1, Reason: 2048   02
```

Figure 27: Radio Configuration Page

Configuring Radio Parameters

To configure specific radio parameters, select the appropriate Radio tab (Radio1-Radio4) on the **Radios** web page.

Field	Description
Channel Options	
Disable	Use the **WLAN Mode** dropdown checkbox to disable the radio.
WLAN Mode	Select the WLAN mode. Possible options are: ● **Disable** - choose this option to disable the radio ● 802.11a ● 802.11b ● 802.11g ● 802.11b/g ● 802.11n/a ● 802.11n/g ● 802.11n/g/b ● Rogue detection ✍ Not all Same Band configurations are possible, depending on type of Access point connected, the configured radio state and whether TrueReuse is configured across the switch. See the Release Notes for possible configuration scenarios.
Channel	Select the channel. The options available are based on the country and WLAN mode.
Enable TrueReuse	Enable the TrueReuse function on the selected radio. ✍ Not all TrueReuse configuration scenarios are available. This depends on what 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	Press this to maximize/minimize option display Channel Blanket

Field	Description
Maximum Retries	Select the number of times to try to resend a packet if the transmission of the packet fails.
Enable Short Preamble:	This option becomes available only when selecting **802.11b** as the WLAN mode. In this case, mark the checkbox to allow a short preamble.
Enable Rate Adaptation	Check this box if you want to enable rate adaptation. ✍ • For 802.11a/b/g, **all enabled** rates participate in the rate adaptation. • For 802.11n devices, rate adaptation will not change the number of data streams .(MCS 0 to 7, or MCS 8 to 15)
The following parameters are available if one of the 802.11n-WLAN modes has been selected.	
Select 802.11n Channel Width	Select the width of the 802.11n channel , 20MHz or 40MHz
Select 802.11n Secondary Channel	If 20/40MHz channel width is selected using the **Select Width** option, the system automatically configures the second 20MHz channel that will be used for bonding as either above (Upper) or below (Lower)the primary 20MHz channel that is was chosen by the Select channel option).
Select 802.11n Blanket operational Mode	**T**wo modes are supported: • **Mixed mode –** In this mode, the Channel Blanket is available to all WLAN clients (802.11a/b/g/n) where 802.11n clients are working in mixed mode • **HT only –** In this mode, the Channel Blanket is available for 802.11n clients only. Note that 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.
Select 802.11n Guard Interval	Guard interval can be configured to short (400 nano seconds) or long (800 nano seconds). Note that when a 20MHz channel is configured, it is not possible to configure short guard interval.
Select 802.11n MCS	Selecting the MCS is equivalent to setting the rate in legacy radios; MCS 0-7 use one data stream, while MCS 8-15 use two data streams.

Field	Description
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. ✍ Since the Extricom 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.

Table 15: Radio Configuration Parameters

Configuring 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 DCF 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 a 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*.

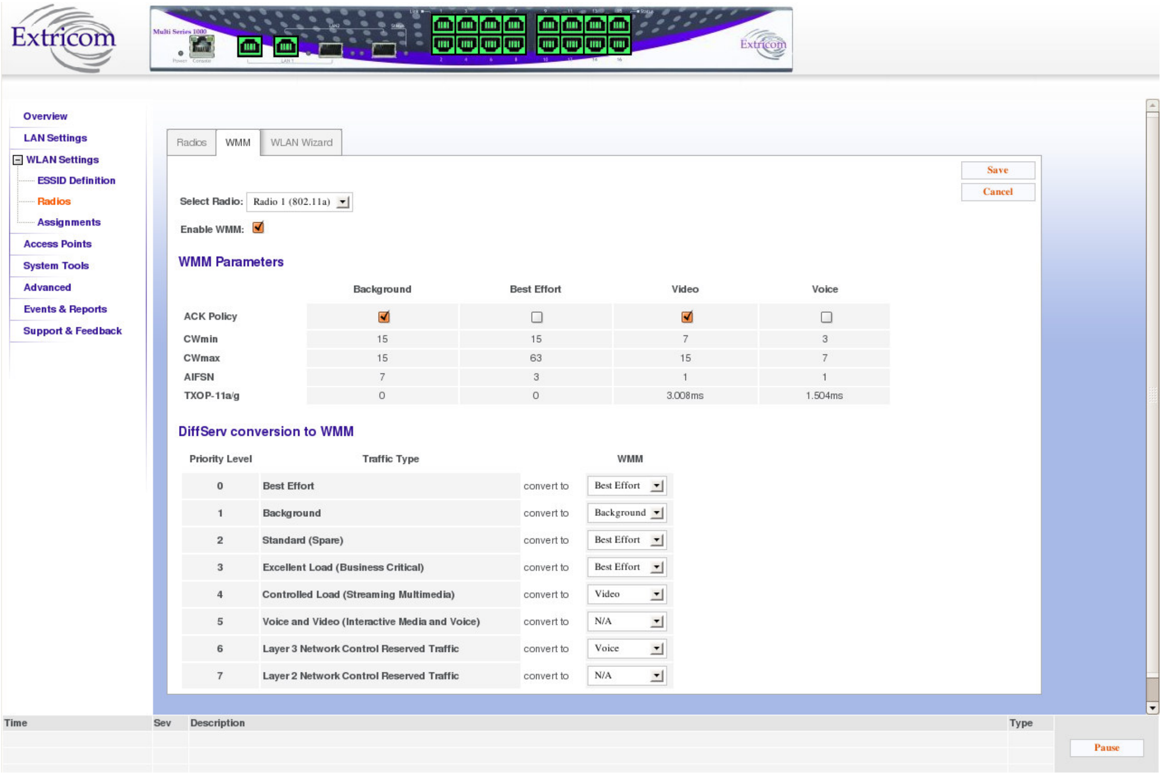
By default, these four WMM prioritization categories are statically mapped to Ethernet 802.1p prioritization tags to allow consistent QoS across wireless and wired network segments. Flow arriving from the wired network tagged with 802.1p priority is mapped to the appropriate Access category, while WMM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

The default mappings can be changed by using the pull-down menus that appear under DiffServe conversion to WMM, in Figure 28. Options are **Video**, **Voice**, **Best Effort**, and **Background**.

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 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 acknowledgement 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.



Select Radio: Radio 1 (802.11a)

Enable WMM: ☑

WMM Parameters

	Background	Best Effort	Video	Voice
ACK Policy	☑	□	☑	□
CWmin	15	15	7	3
CWmax	15	63	15	7
AIFSN	7	3	1	1
TXOP-11a/g	0	0	3.008ms	1.504ms

DiffServ conversion to WMM

Priority Level	Traffic Type		WMM
0	Best Effort	convert to	Best Effort
1	Background	convert to	Background
2	Standard (Spare)	convert to	Best Effort
3	Excellent Load (Business Critical)	convert to	Best Effort
4	Controlled Load (Streaming Multimedia)	convert to	Video
5	Voice and Video (Interactive Media and Voice)	convert to	N/A
6	Layer 3 Network Control Reserved Traffic	convert to	Voice
7	Layer 2 Network Control Reserved Traffic	convert to	N/A

Figure 28: WMM Configuration Tab

WMM is configured per radio; all parameters are displayed only in this stage.

Field	Description
ACK policy	Configurable per access category, when this option is set, the switch will ask WMM stations NOT to send ACK for WMM flow of this category
CWmin	Min Contention window for the Access category
CWmax	Maximum Contention window
AIFSN	Arbitration Inter Frame Spacing Number
TXOP-11a/g	Interval during which a station can send as many frames as possible

Table 16: WMM Parameter Descriptions

Configuring WMM Parameters

1. Select the radio for which you want to define WMM parameters
2. Enable or disable WMM
3. If you have enabled WMM, select the appropriate WMM parameters.

The following values are mapped for a marked Ethernet frame:

1	Background
2	
0	Best Effort
3	
4	Video
5	
6	Voice
7	

Table 17: VPT To WMM Destination

0x08	Background
0x20	
0x28	Video
0xa0	
0x30	Voice
0xe0	
0x88	
0xb8	
Other	Best Effort

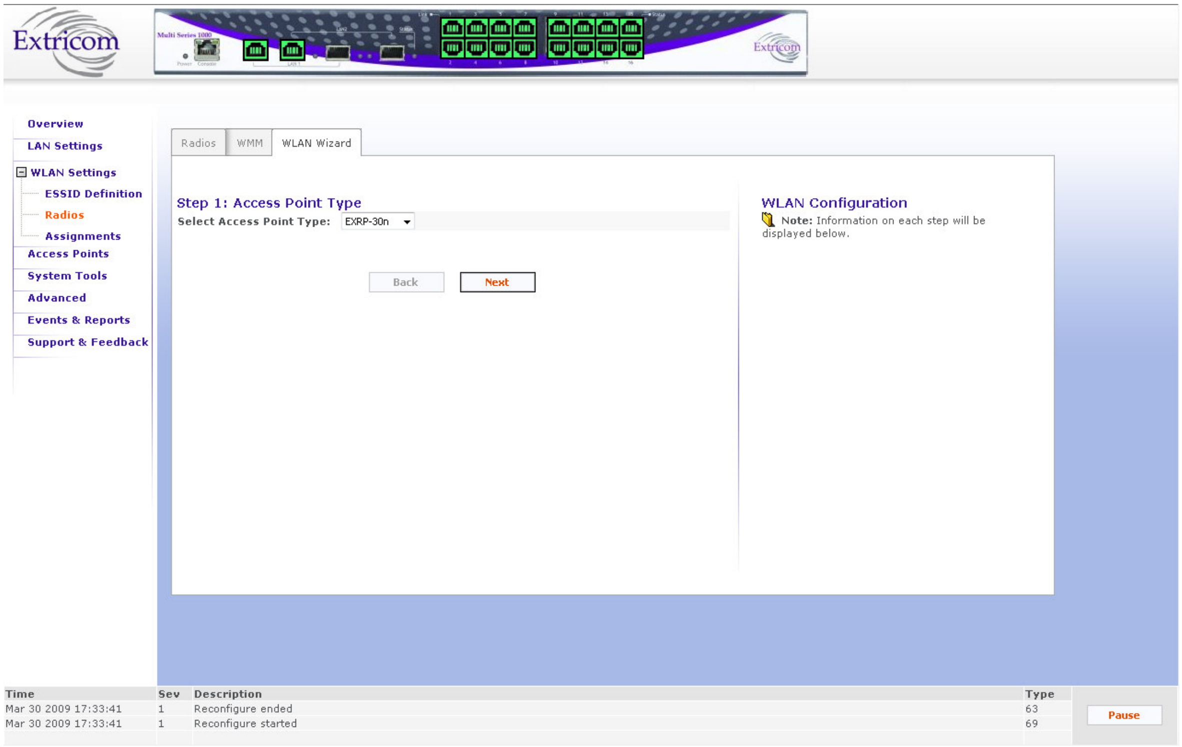
Table 18: ToS To WMM Destination

WLAN Wizard

The 'WLAN Wizard' tab folder provides a convenient tool that simplifies the radio configuration for the user by serializing the following steps:

- Access point type selection
- Rogue AP detection presence (yes/no)
- Blanket type selection
- True Reuse selection (yes/no)
- Summary and confirmation

The Wizard tab folder is shown below, at step 1:



Step 1: Access Point Type

Select Access Point Type: EXRP-30n

WLAN Configuration

Note: Information on each step will be displayed below.

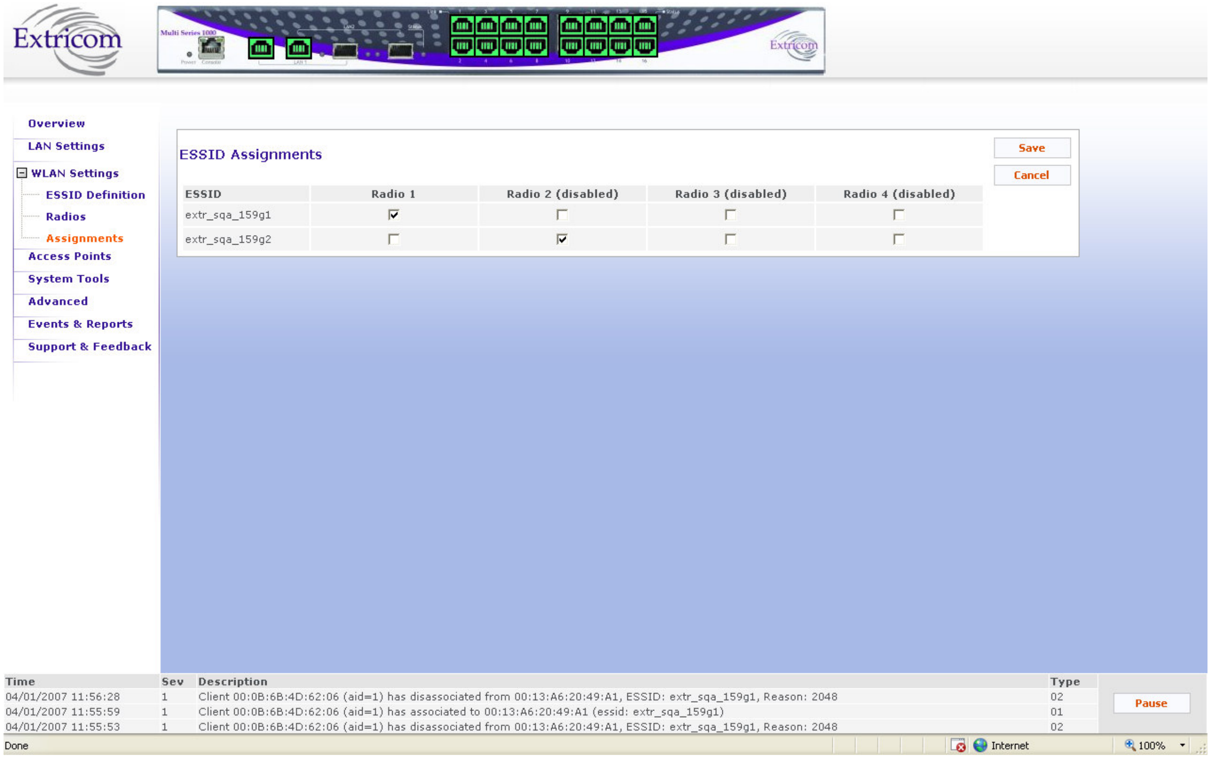
Time	Sev	Description	Type
Mar 30 2009 17:33:41	1	Reconfigure ended	63
Mar 30 2009 17:33:41	1	Reconfigure started	69

Figure 29: WLAN Wizard

As selections are made, they are listed on the right side of the screen under WLAN configuration.

ESSID Assignment

Use the **ESSID Assignment** web page to assign ESSID to a specific radio (Radio 1 to 4).



ESSID Assignments

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

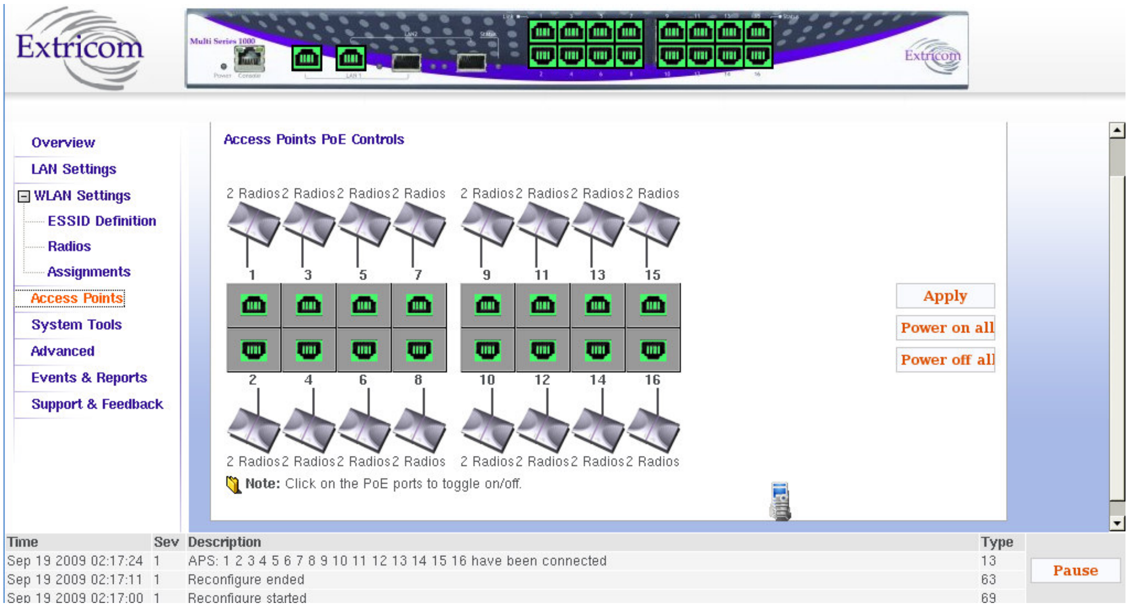
Time	Sev	Description	Type
04/01/2007 11:56:28	1	Client 00:0B:6B:4D:62:06 (aid=1) has disassociated from 00:13:A6:20:49:A1, ESSID: extr_sqa_159g1, Reason: 2048	02
04/01/2007 11:55:59	1	Client 00:0B:6B:4D:62:06 (aid=1) has associated to 00:13:A6:20:49:A1 (essid: extr_sqa_159g1)	01
04/01/2007 11:55:53	1	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 30: ESSID Assignment Page

The web page displays a cross-reference table of previously defined ESSIDs and Radios (1 to 4). Check the box for each ESSID you wish to assign to any of the four radios.

Powering Access Points

The only AP configuration required in the Extricom WLAN architecture is activation or deactivation of AP ports.



Note: Click on the PoE ports to toggle on/off.

Time	Sev	Description	Type
Sep 19 2009 02:17:24	1	APS: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 have been connected	13
Sep 19 2009 02:17:11	1	Reconfigure ended	63
Sep 19 2009 02:17:00	1	Reconfigure started	69

Figure 31: Access Point Configuration Window

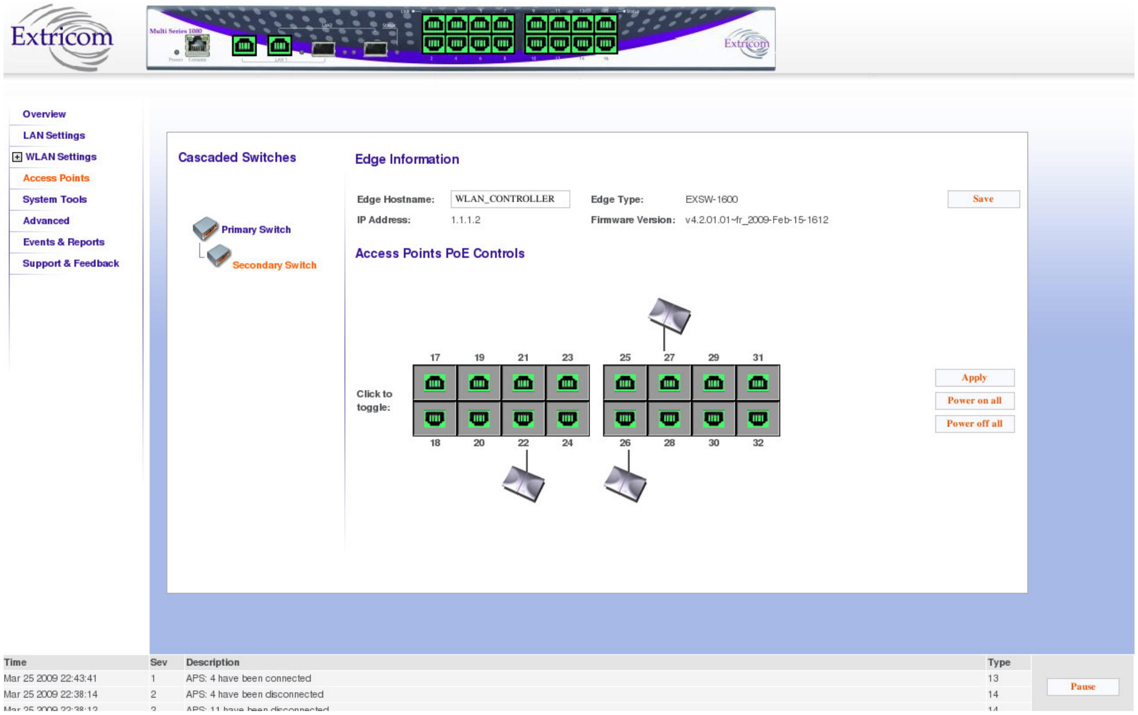
To configure AP PoE status:

- Toggle an individual APs PoE state by clicking on the RJ45 connector image of the access point. The RJ45 connector image will change colors (to grey or green). You need to click the **Apply** button to immediately activate your selection.
- Green indicates that PoE is active. Grey indicates that PoE is off.
- A graphic 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 APs with PoE, select **Power on all**.
- To power-off PoE to all APs, select **Power off all**.

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

Cascaded APs

When two switches have been cascaded together as Primary and Secondary (see Chapter 1, Switch Cascade section on p. 14, for details about Switch Cascade) 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 AP Configuration window is shown below:



Edge Hostname: WLAN_CONTROLLER
Edge Type: EXSW-1600
IP Address: 1.1.1.2
Firmware Version: v4.2.01.01~fr_2009-Feb-15-1612

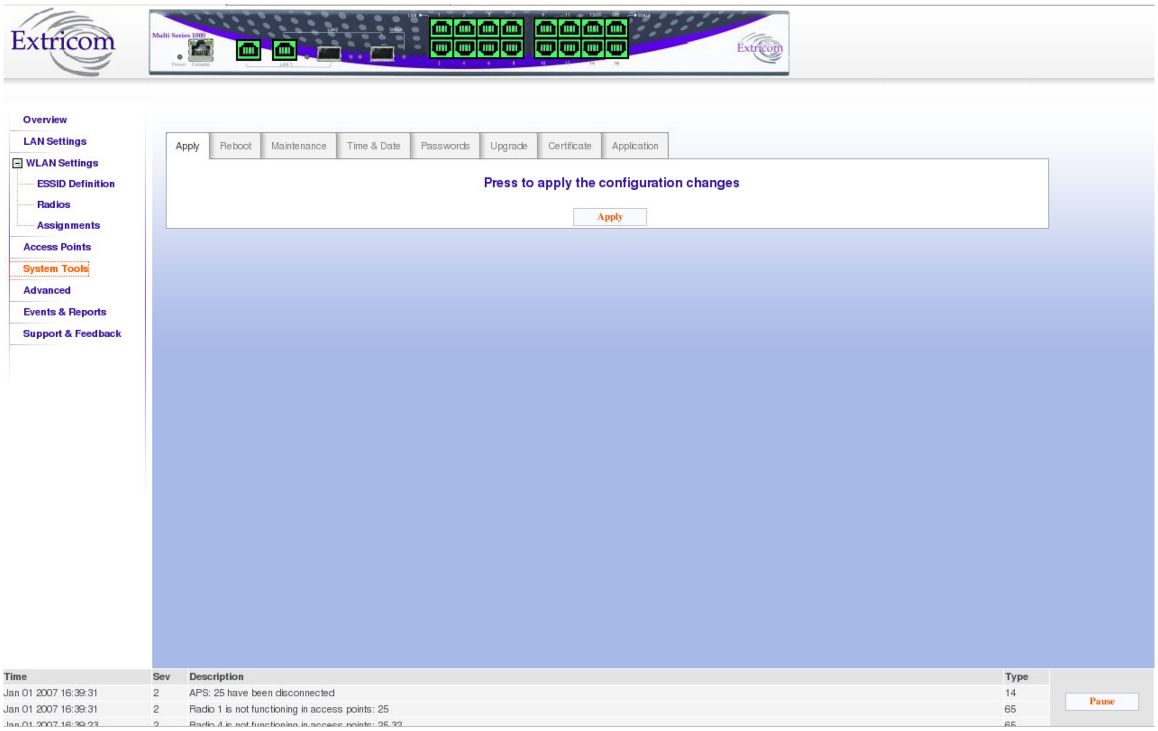
```
Time                  Sev  Description                        Type
Mar 25 2009 22:43:41  1    APS: 4 have been connected         13
Mar 25 2009 22:38:14  2    APS: 4 have been disconnected      14
Mar 25 2009 22:38:12  2    APS: 11 have been disconnected     14
```

Figure 32: Access Point Configuration Window Secondary Switch

System Tools Configuration

This web page includes the following system tools tabs:

- Apply – Use this Web page to start the reconfigure process
- Reboot –Use this Web page to reboot the system.
- Maintenance
- Time & Date – Use this Web page to set time and date
- Password
- Upgrade
- Certificate (Multi Service 1000 platform only)
- Application (Multi Service 1000 platform only)



Press to apply the configuration changes

Time	Sev	Description	Type
Jan 01 2007 16:39:31	2	APS: 25 have been disconnected	14
Jan 01 2007 16:39:31	2	Radio 1 is not functioning in access points: 25	65
Jan 01 2007 16:39:23	2	Radio 4 is not functioning in access points: 25,32	65

Figure 33: System Tools Configuration Page

Applying Saved Changes

Not every change in an Extricom switch's configuration requires system reboot. Some parameters can be changed and the changes will take effect immediately. The **Apply** button checks whether a full reboot is required. In case reboot is not required, the update will take effect immediately.

Rebooting the Switch

You must reboot the switch after upgrading/downgrading the firmware, and in some other cases such as returning a Switch Cascade from failover to normal operation. Situations in which a reboot is required are indicated in the User Guide.

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

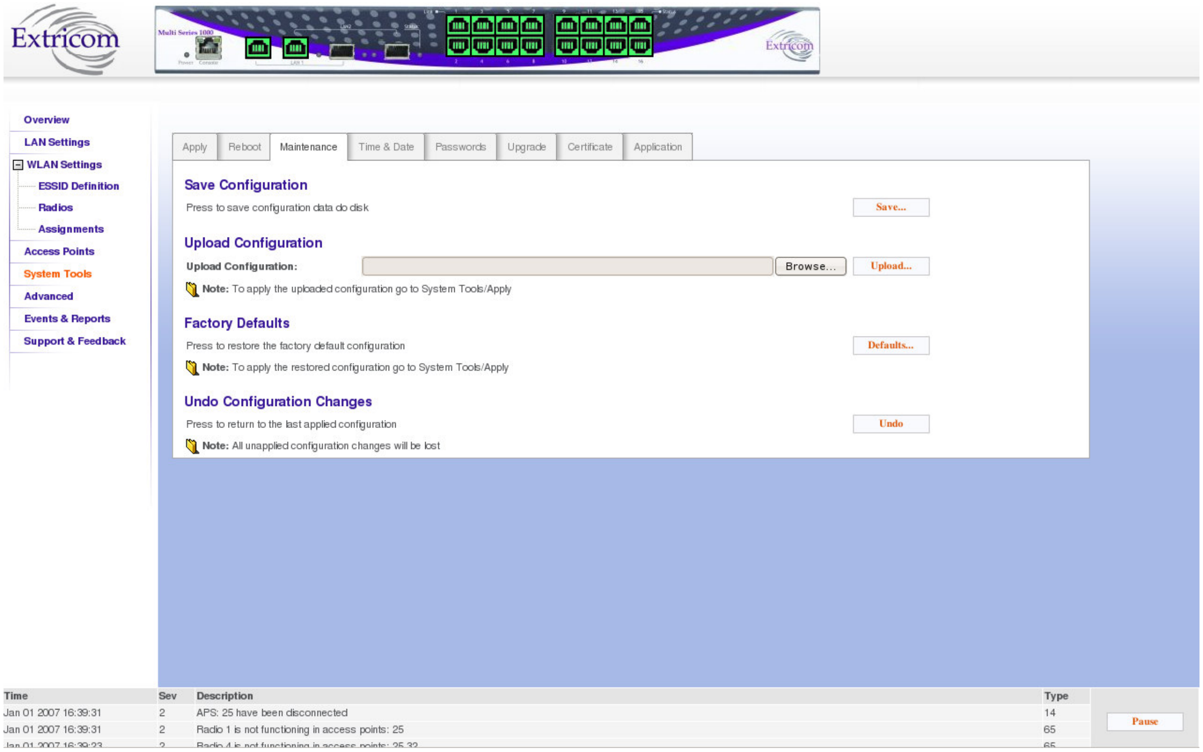
To reboot the Extricom switch:

1. In the **Reboot** tab, click **Reboot**.
2. A new screen opens, prompting you "Are you sure you want to reboot?"
3. Click **Reboot** to reboot.
4. **Note**: rebooting before applying saved changes will discard the saved changes.

Maintenance tab

Use the maintenance tab to:

- Save current configuration to a disk
- Upload configuration (Switch , MAC ACL , Allowed ESSID)
- Reset to factory defaults
- Undo configuration changes



Save Configuration

Press to save configuration data do disk

Upload Configuration

Upload Configuration:

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	Sev	Description	Type
Jan 01 2007 16:39:31	2	APS: 25 have been disconnected	14
Jan 01 2007 16:39:31	2	Radio 1 is not functioning in access points: 25	65
Jan 01 2007 16:39:23	2	Radio 4 is not functioning in access points: 25,32	65

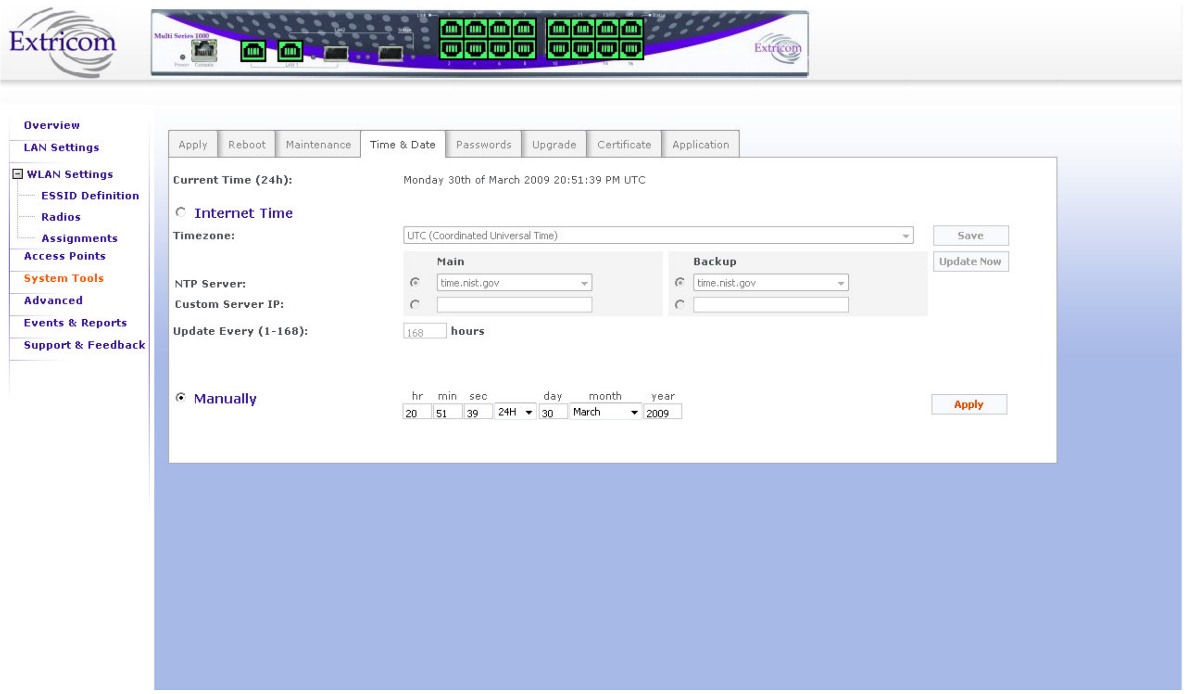
Figure 34: Maintenance Configuration Page

Field	Description
Save	Save current configuration to an offline disk
Upload	This is used to upload configuration from an offline disk (Use the browse field to locate file). You will see a popup window stating “Please select configuration elements to upload”; you can select a Switch , MAC ACL, or Allowed ESSID configuration file
Factory Defaults	Restore factory default configuration. You will see a popup window stating “Please select configuration elements to upload”. You can select Switch, MAC ACL, Allowed ESSID configuration file, and/or Captive Portal Custom page

Field	Description
Undo Configuration Changes	Returns to the last applied configuration. ✍ All unapplied configuration changes will be lost.

Table 19: Maintenance Configuration Tab

Time & Date Setting



Current Time (24h): Monday 30th of March 2009 20:51:39 PM UTC

○ Internet Time

Timezone: UTC (Coordinated Universal Time)

	Main	Backup
NTP Server:	● time.nist.gov	● time.nist.gov
Custom Server IP:	○	○

Update Every (1-168): 168 hours

● Manually

hr	min	sec		day	month	year
20	51	39	24H	30	March	2009

Figure 35: Time & Date Configuration Page

The Extricom system supports two ways of setting Date and Time (refer to Figure 35)

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

1. Select **manually** radio button.
2. Enter the time and date in the format hh:mm:ss dd-mm-yy.
3. Click **Apply** to set the time.

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

1. Select **Internet Time** radio button.
2. Select the **Timezone**.
3. Select **NTP server** (main and backup) You can enter Custom IP address using (in the **Custom Server IP:** field)

4. Add the NTP update interval (hour based) by updating the **Update Every (1-168): hours** field.

5. Click **Save** to save the configuration and start the NTP process.

6. Click **Update now** to start NTP time-setting immediately.

Setting Passwords for the Extricom Switch

Passwords are set according to user levels. Refer to Table 20 for a description of the user access levels and their default passwords.

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

Table 20: Default Passwords

✍ 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 Extricom-authorized engineer.

! ***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.***

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

To set and change a password for the Extricom switch:

1. Select the **Passwords** tab.

2. Enter the user access level whose password you want to change.

3. Enter the current password.

4. Enter the new password.

5. Re-type the new password.

Upgrading Extricom Firmware

Extricom firmware can be upgraded using *Upgrade* tab.

To upgrade Extricom firmware:

1. Download the upgrade to your computer from the CD supplied with your purchase.
   or
   Obtain an upgrade file from your authorized Extricom reseller or distributor.
2. Create a backup of the configuration file that contains the current configuration.
3. In the *Upgrade* tab, click **Browse** and browse to the location of the upgraded firmware. The file's path appears in the **Upgrade Firmware** field.
4. Click **Update** to upgrade the firmware and wait for the upgrade process to end. A message will appear when the upgrade ended and will ask you to reboot he switch.
5. Reboot the switch (use the Reboot tab)

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

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

Upload a Switch Certificate and Key

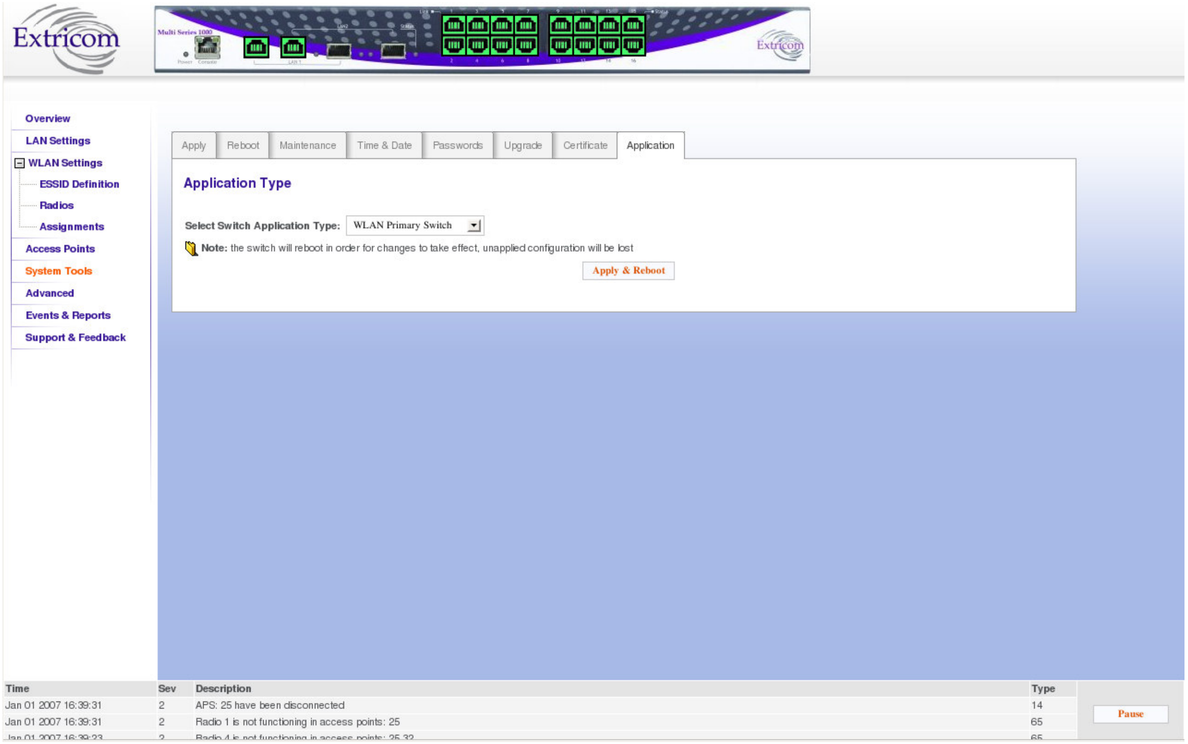
The first time that a Captive Portal user logs in from his browser, he/she will receive a notice about the switch security certificate such as "There is a problem with the website's security certificate. Click on "Continue to this website (not recommended)".

To avoid this, the WLAN operator can purchase a signed certificate from an issuing authority.

Signed certificates are installed on the switch using the Certificate tab folder.

Application

The Application tab folder brings up the following window:



Application Type

Select Switch Application Type: WLAN Primary Switch

Note: the switch will reboot in order for changes to take effect, unapplied configuration will be lost

Time	Sev	Description	Type
Jan 01 2007 16:39:31	2	APS: 25 have been disconnected	14
Jan 01 2007 16:39:31	2	Radio 1 is not functioning in access points: 25	65
Jan 01 2007 16:39:23	2	Radio 4 is not functioning in access points: 25 32	65

Figure 36: Application Type Window

> The Application window is the first window to use when configuring a switch cascade (see Chapter 1, Switch Cascade section, for details about Switch Cascade). After the Application window must be used to define the switch roles before accessing the Redundancy window in the System Tools to complete the configuration.

"Application Type" refers to the role of the switch currently being accessed by the web interface. The available application types are as follows:

Application Type	Description	Switch Types That Support This Mode
WLAN Switch	Standalone edge switch	EXSW-1600
WLAN Primary Switch	Primary switch in a Cascade configuration	EXSW-1600, EXSW-1600C
WLAN Secondary Switch	Secondary switch in a Cascade configuration	EXSW-1600, EXSW-1600C

Table 21: Application Types

Steps To Installing A Switch Cascade

1. Referring to the instructions in Chapter 2 above, connect each switch to the LAN and connect each switch to its AP’s. Do not interconnect the switches yet.
2. Ensure that you have the latest available version of switch firmware with Switch Cascade support.
3. Read the release notes for that firmware version, and follow the installation instructions.

Advanced Configuration of the Extricom WLAN

The **Advanced** configuration page of the Extricom WLAN includes the following tabs:

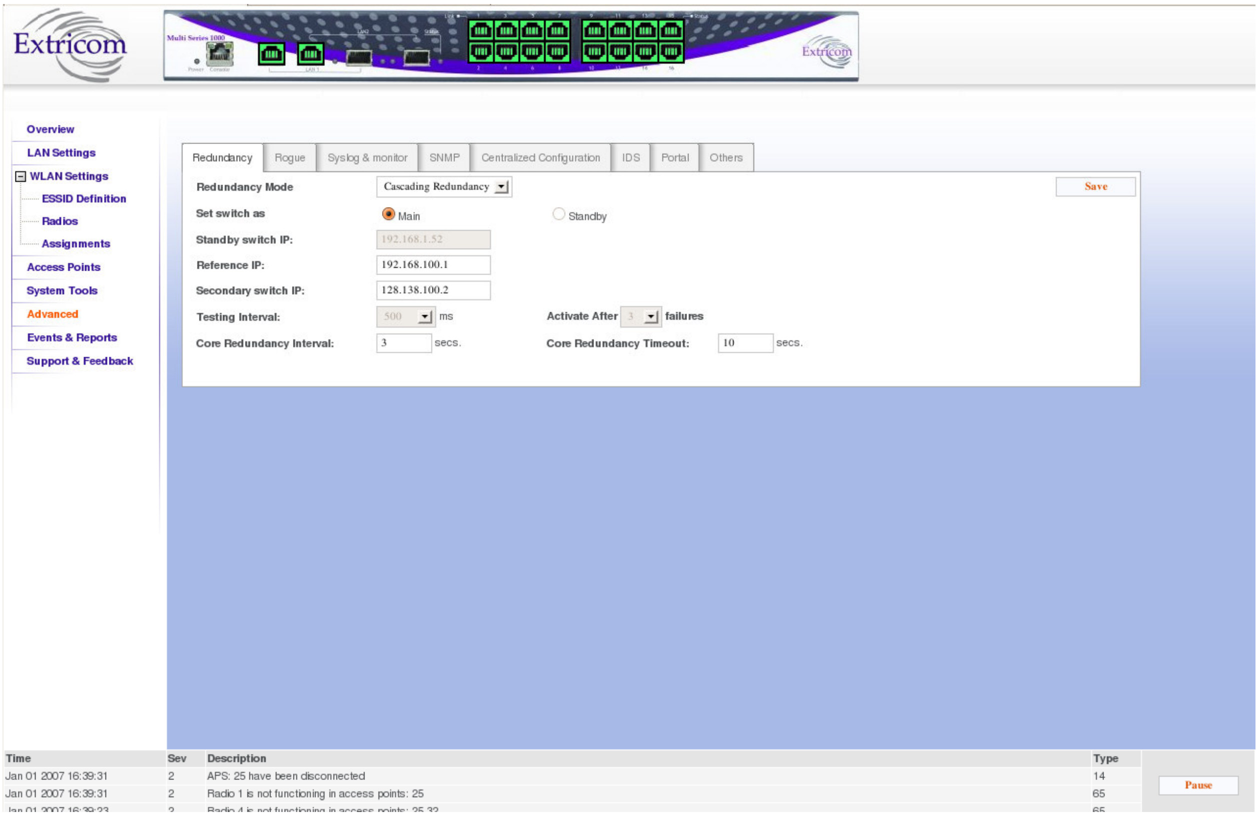
- Redundancy
- Rogue
- Syslog &Monitor
- SNMP parameters.
- Centralized configuration
- IDS
- Captive Portal
- Others

To configure the Advanced Features parameters:

1. Click **Advanced** in the navigation tree. The **Redundancy** configuration page appears.
2. Select the **appropriate** tab for configuring Redundancy, Syslog & Monitor ,SNMP parameters, Centralized configuration, IDS, Captive Portal, or other features.

Configuring Redundancy

When clicking on the Redundancy tab folder, the window in Figure 37 below appears:



Redundancy Mode	Cascading Redundancy
Set switch as	● Main ○ Standby
Standby switch IP:	192.168.1.52
Reference IP:	192.168.100.1
Secondary switch IP:	128.138.100.2
Testing Interval:	500 ms
Activate After	3 failures
Core Redundancy Interval:	3 secs.
Core Redundancy Timeout:	10 secs.

Time	Sev	Description	Type
Jan 01 2007 16:39:31	2	APS: 25 have been disconnected	14
Jan 01 2007 16:39:31	2	Radio 1 is not functioning in access points: 25	65
Jan 01 2007 16:39:23	2	Radio 4 is not functioning in access points: 25 32	65

Figure 37: Redundancy Window

The fields available in the Redundancy tab folder change depending on whether the switch has been set to function as a primary switch in a cascade topology, or has been set to function as a standalone edge switch.

> **!** To activate a switch cascade, one switch must be set as the Primary, and another switch set as the Secondary, using the Application Type tab folder in the System Tools (see page 64). Then, in the Redundancy tab folder, the Redundancy Mode of the Primary switch must be set to Cascade. Please refer to the release notes for your firmware version of Switch Cascade.

Redundancy Fields For Primary Switch

The following table lists the available fields when the switch is functioning as a Primary switch. When a secondary switch is being viewed, the same fields will be visible but they will be read-only.

Field	Description
Redundancy Mode	Select redundancy mode. Possible options are: ● Disable - no switch redundancy. A cascaded pair will still provide seamless channel blanket(s) extending across the two switches, but the cascade pair will not have LAN redundancy. ● Cascade – Switch Cascade with LAN redundancy ● Normal – do not use this setting
Set Switch As	(Not relevant for Cascade)
Standby Switch IP	(Not relevant for Cascade)
Reference IP	IP address of a reference network element. This is used to test connectivity to the LAN. The reference element must be operational and respond to pings.
Secondary Switch IP	IP address of the Secondary switch in the cascade pair.
Testing Interval	Interval in msec between keep-alive packets sent to Reference IP.
Activate After XX failures	The number of lost keep-alive packets before activating failover
Core Redundancy Interval	Interval in seconds between heartbeats sent from switch to switch, across the switch interconnect.
Core Redundancy Timeout	Elapsed time before activating failover. Resets every time there is heartbeat.

Table 22: Redundancy Tab Folder Fields When Switch Set As Primary

The Testing Interval and Activate After XX failures parameters monitor LAN link and switch interconnect health.

The Core Redundancy Interval and Core Redundancy Timeout monitor the health of the cascaded switches.

After making these changes, you must click “Save”, then go to System Tools and click on “Apply Changes” in order for them to take effect.

! To activate a switch cascade, one switch must first be designated as the Primary, and another switch designated as the Secondary, using the Application Type tab folder in the System Tools. Then, in the Redundancy tab folder, the Redundancy Mode of the Primary switch must be set to Disable or Cascade.

When a switch failure or link failure has been detected, a failover occurs and the cascaded switch that remains fully operational goes into standalone mode. In two cases below, both switches remain fully operational so they both go into standalone mode. A switch that goes into standalone mode continues to provide switching service to its APs only.

The following table indicates which cascaded APs provide service in the event of a failover, assuming Redundancy mode is set to "Cascade":

Failure Type	Primary APs	Secondary APs	Comments
Switch Interconnect	√	√[1]	Primary and secondary switch failover to standalone mode. Even though APs of both switches are functioning, there is no seamless mobility between the switches.
Primary LAN Link	X	√[1]	Secondary switch failover to standalone mode.
Secondary LAN Link	√	√	No switch failover. Seamless mobility between switches. Secondary switch heartbeat checks of Primary switch are turned off.
Primary Switch Failure	X	√[1]	Secondary switch failover to standalone mode.
Secondary Switch Failure	√	X	

Table 23: Switch Cascade Failover Behavior

Notes:

1. Traffic interruption time during a failover depends on the link and switch core monitoring parameters chosen (see Table 23 above).
2. √ = Full service
3. X = Not in service

4. 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 remaining switch.
5. A Primary switch can function as standalone edge switch without requiring a failover.

> **!** 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.

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. Otherwise, it is read-only, except for the "Reboot" function and the Application tab folder.

The Secondary switch GUI is always read-only, except for the "Reboot" function and the Application tab folder, regardless of whether the Secondary switch is operating as a secondary switch or standalone switch.

Normal Redundancy Mode

This is a legacy redundant mode which has been superseded by Switch Cascade. In normal redundancy mode, one switch functions as the main switch while the second switch functions in a hot standby mode ("Standby" switch) only. The second switch and all of its APs do not carry any traffic while the standby switch is running in hot standby. When one of the switchover conditions are met, the standby switch and its APs carry traffic. A Normal Redundancy topology is illustrated below:

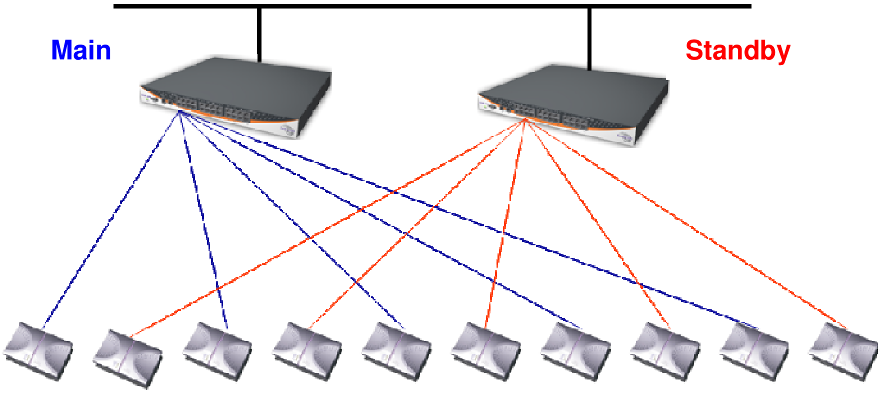


Figure 38: Normal Redundancy Deployment

Redundancy Fields For Standalone Edge Switch

The following table lists the available fields when switch is functioning as a standalone edge switch:

Field	Description
Redundancy Mode	Select redundancy mode. Possible options are: ● Disable - switch operates as a standalone edge switch ● Normal redundancy – switch operates as part of a hot standby configuration
Set switch as	Designate the switch as a **Main** switch or a **Standby switch.**
Standby switch IP	IP address of the standby switch.
Reference IP	IP address of a reference network element. This is used to test connectivity to the LAN.
Testing Interval	Interval in msec between keep-alive packets sent to Reference IP.
Activate After XX failures	The number of lost keep-alive packets before activating failover

Table 24: Redundancy Tab Folder Fields When Switch Set As a Standalone Edge

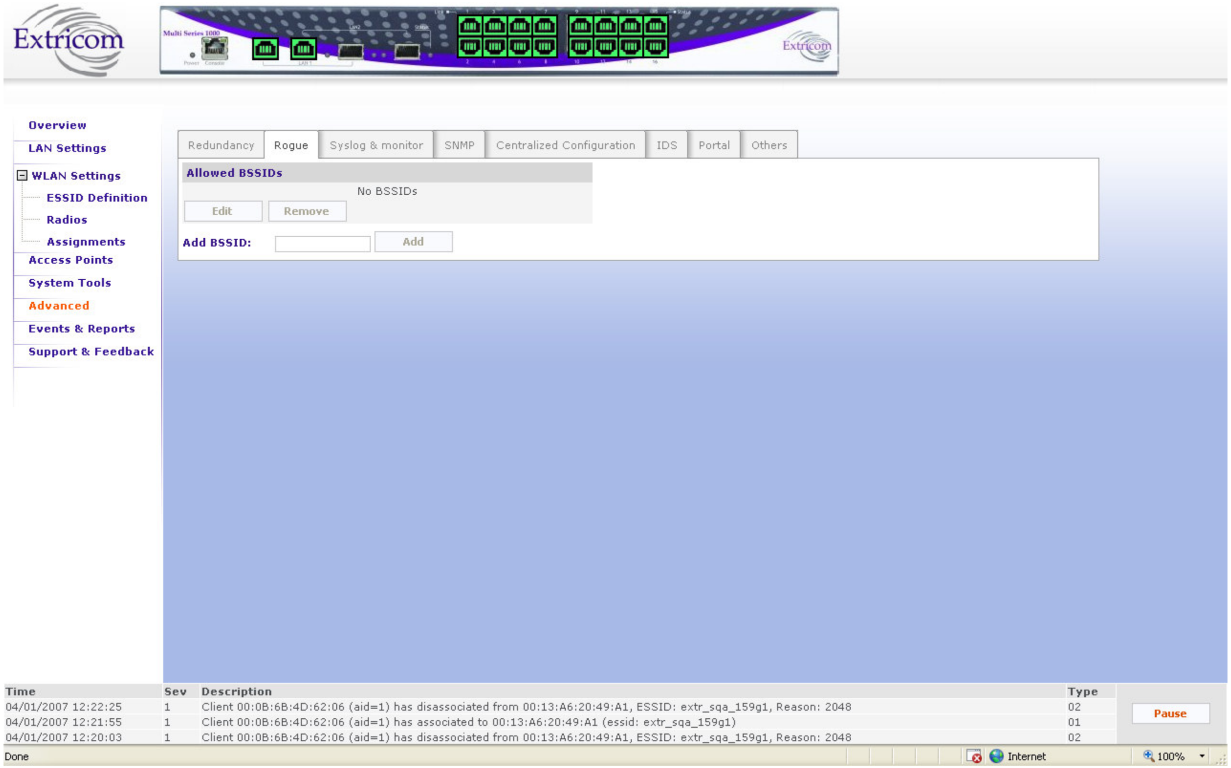
If “Disable” is chosen in the Redundancy Mode field, all other fields in this tab folder are inactive.

Configuring Rogue

Rogue access points represent the biggest threat to Wi-Fi security. Rogue APs are unauthorized APs that are physically connected to the wired Ethernet LAN.

The Rogue mechanism implemented in the EXSW 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.



Allowed BSSIDs

No BSSIDs

Add BSSID:

```
Time                 Sev  Description                                                                                      Type
04/01/2007 12:22:25  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 12:21:55  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 12:20:03  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
```

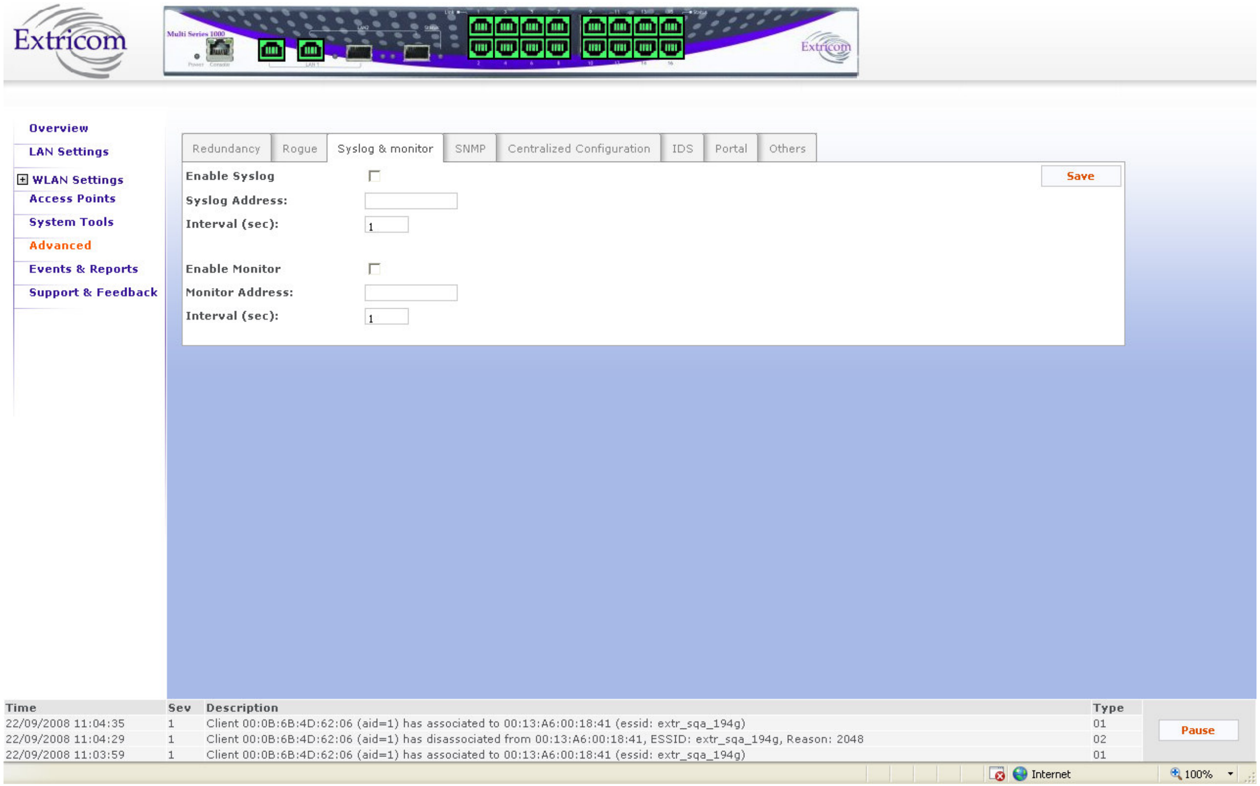
Figure 39: Syslog & Monitor Tab

Field	Description
Allowed BSSIDs	
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

Table 25: Redundancy Tab Folder Fields When Switch Set As Primary

Configuring Syslog & Monitor

Currently, in most common operational scenarios, Syslog and monitor utilities should not be used (unless used for troubleshooting). The Monitor utility can be used only if Extricom's dedicated network monitoring tool is enabled; otherwise do not enable this feature.



Enable Syslog □
Syslog Address:
Interval (sec): 1

Enable Monitor □
Monitor Address:
Interval (sec): 1

Time	Sev	Description	Type
22/09/2008 11:04:35	1	Client 00:0B:6B:4D:62:06 (aid=1) has associated to 00:13:A6:00:18:41 (essid: extr_sqa_194g)	01
22/09/2008 11:04:29	1	Client 00:0B:6B:4D:62:06 (aid=1) has disassociated from 00:13:A6:00:18:41, ESSID: extr_sqa_194g, Reason: 2048	02
22/09/2008 11:03:59	1	Client 00:0B:6B:4D:62:06 (aid=1) has associated to 00:13:A6:00:18:41 (essid: extr_sqa_194g)	01

Figure 40: Syslog & Monitor Tab

Field	Description
Enable Syslog	Check to record system information in the System Log. In most common operational scenarios, this option should be unchecked (unless used for troubleshooting).
Syslog Address	Enter the IP address of the computer to which to send the System Log.

Field	Description
Interval (sec)	Specifies how often information is sent to the System Log. The default is 1 second, and this is the recommended setting.
Enable Monitor	The Monitor Log is only relevant if using Extricom's dedicated network status monitoring tool (not provided with the switch.) By default, this option is not checked. ✍ Check this option only if you are using the Extricom dedicated network monitoring tool, otherwise unnecessary data packets are sent through the Ethernet.
Monitor Address	Enter the address of the Monitor Log if using the Extricom dedicated network monitoring tool.
Interval (sec)	Specifies how often information is sent to the Monitor Log. The default setting is 1 second and this is the recommended interval. ✍ Configure this parameter only if using the dedicated network monitoring tool.

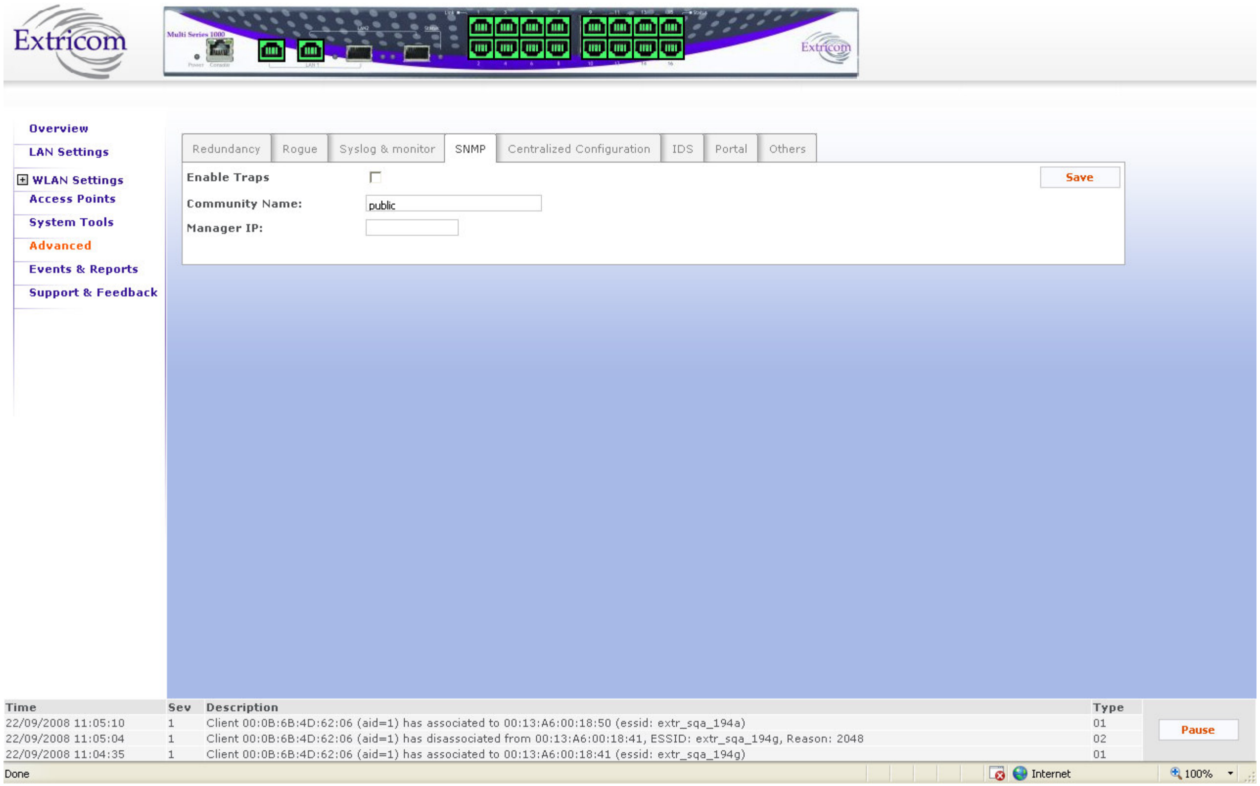
Table 26: Syslog & Monitor Configuration Parameters

Configuring SNMP

The Extricom switch generates a rich variety of traps to describe events occurring within the WLAN. In general, the traps can be categorized as follows:

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

Traps are displayed at the bottom of the web interface, as illustrated in Figure 41 below.



Enable Traps □

Community Name: public

Manager IP:

```
Time                 Sev  Description                                                                                          Type
22/09/2008 11:05:10  1    Client 00:0B:6B:4D:62:06 (aid=1) has associated to 00:13:A6:00:18:50 (essid: extr_sqa_194a)          01
22/09/2008 11:05:04  1    Client 00:0B:6B:4D:62:06 (aid=1) has disassociated from 00:13:A6:00:18:41, ESSID: extr_sqa_194g, Reason: 2048   02
22/09/2008 11:04:35  1    Client 00:0B:6B:4D:62:06 (aid=1) has associated to 00:13:A6:00:18:41 (essid: extr_sqa_194g)          01
```

Figure 41: SNMP Configuration Tab

Traps can also be sent over a northbound interface to network management devices, such as Extricom's EXNM-2000. The northbound interface is enabled using the SNMP configuration tab, as described below:

Field	Description
Enable Traps	Check this option to enable SNMP traps over the northbound interface.
Community name	Enter the community name.
Manager IP	Enter the manager's IP address.

Table 27: SNMP Configuration Features

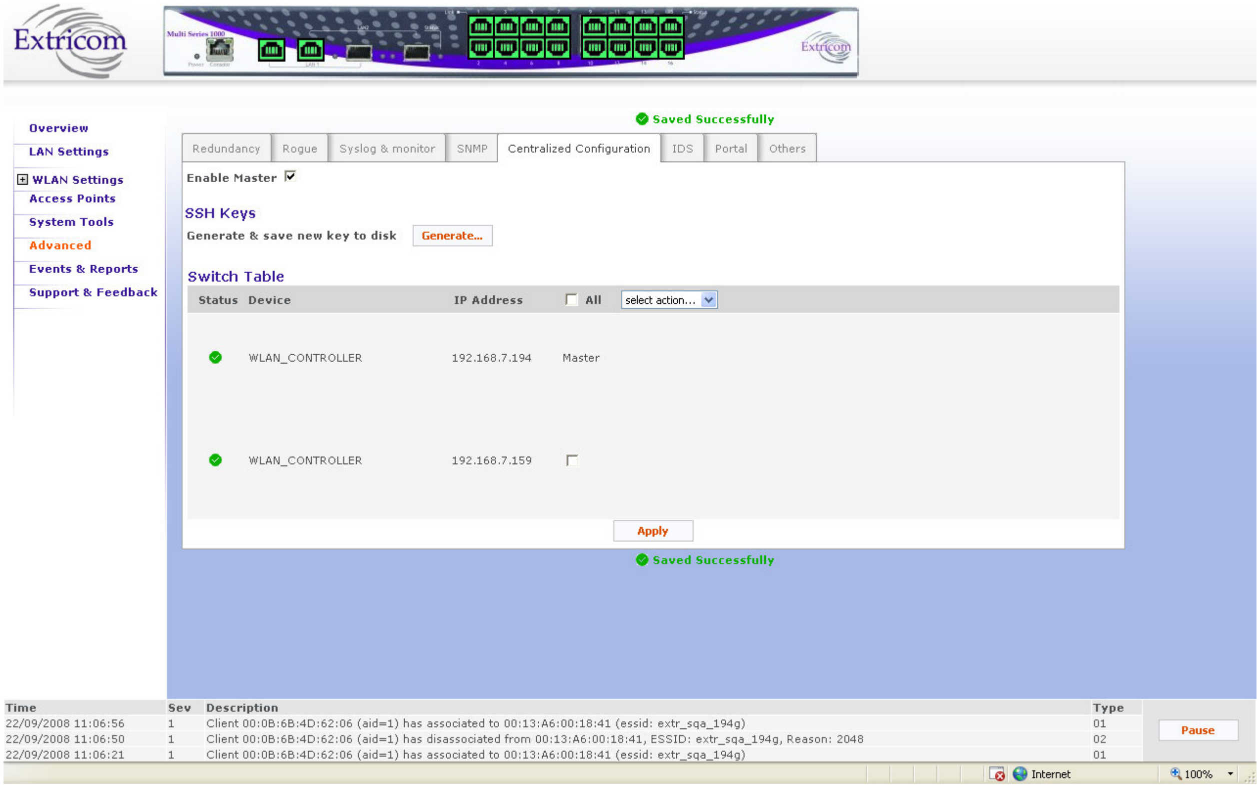
Please see Chapter 5 for a list of SNMP traps that may be sent by the switch.

Centralized Configuration Tab

Centralized Configuration allows you to manage a group of identical Extricom switches (*slaves*) from one single *master* switch. You should decide which switch will act as *master*. Extricom switches have a built-in mechanism to discover the presence of other Extricom switches.

> Note: from version 4.1, only autodiscovery of potential slave switches is supported. Manual addition of slave switches is no longer supported.

Configuration changes on the *master* switch are propagated to the *slave* switches via a secured mechanism. For this authentication scheme to work, the *slave switches* need to obtain a copy of the *master*'s public key prior to the centralized configuration. This is done in the initial phase of the switch's configuration by first retrieving the *master*'s public key and then uploading it to the designated *slave switches*.



Enable Master ☑

SSH Keys

Generate & save new key to disk

Switch Table

Status	Device	IP Address	□ All
✓	WLAN_CONTROLLER	192.168.7.194	Master
✓	WLAN_CONTROLLER	192.168.7.159	□

```
Time                 Sev  Description                                                                                        Type
22/09/2008 11:06:56  1    Client 00:0B:6B:4D:62:06 (aid=1) has associated to 00:13:A6:00:18:41 (essid: extr_sqa_194g)         01
22/09/2008 11:06:50  1    Client 00:0B:6B:4D:62:06 (aid=1) has disassociated from 00:13:A6:00:18:41, ESSID: extr_sqa_194g, Reason: 2048  02
22/09/2008 11:06:21  1    Client 00:0B:6B:4D:62:06 (aid=1) has associated to 00:13:A6:00:18:41 (essid: extr_sqa_194g)         01
```

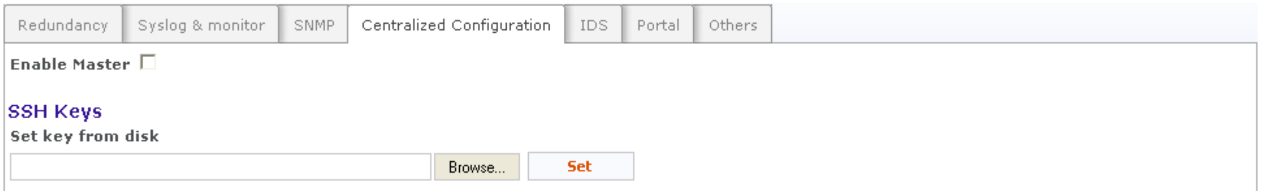
Figure 42: Centralized Configuration Master Page

To configure Centralized Configuration parameters:

Initial Setup

1. Configure the LAN settings on the *Master* switch.

2. Generate an SSH key pair on the *Master* switch (select master first). This is done by clicking on the **Generate** button.
3. Retrieve the SSH public key from the *Master* switch and save it in a file on your PC.
4. Manually configure each of the *Slave* switch's LAN settings, and continue by uploading the previously saved master's public key on every *Slave* you wish to manage. This allows the *Slave* switch to be configured only by the *Master* switch which generated the public key.



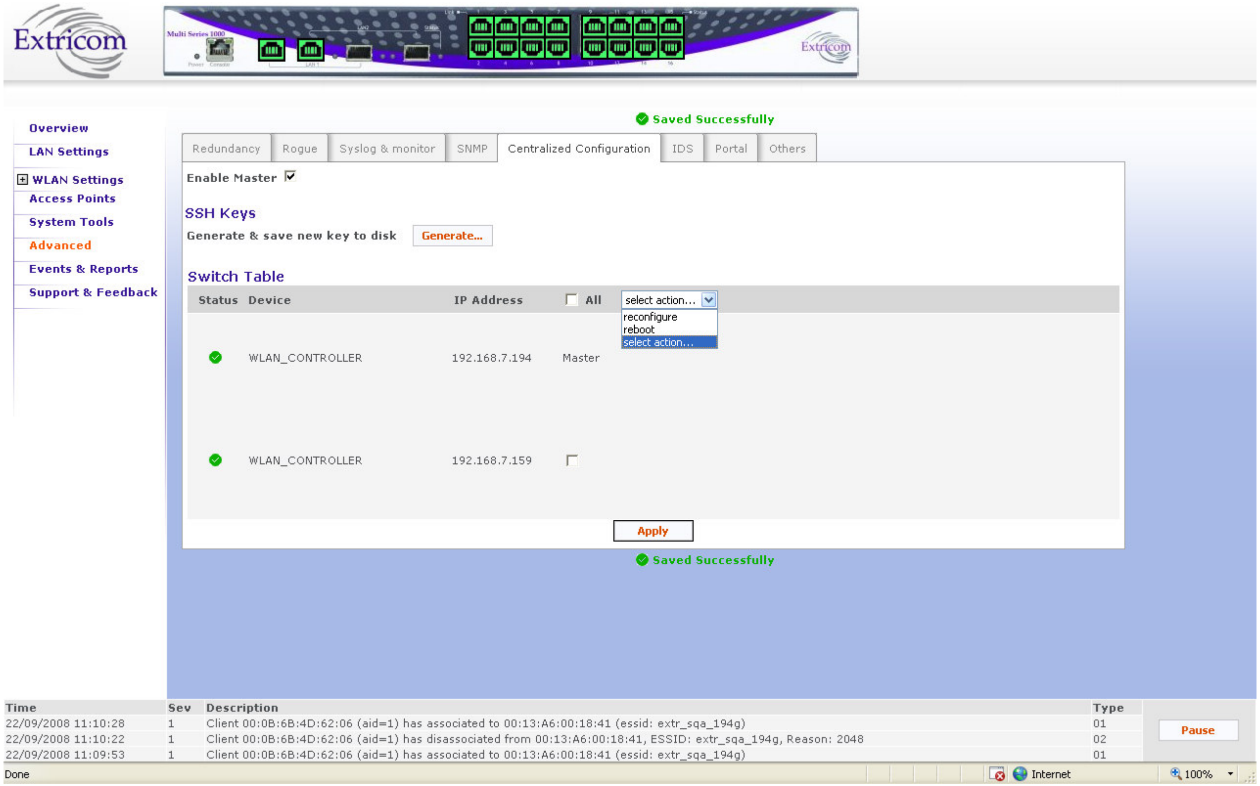
Enable Master □

Set key from disk

Figure 43: Centralized Configuration Slave Page

Slave Switch Configuration

1. On the *Master* switch, open the Centralized Configuration web page and click on the **Update** button in the **Switches Table** section. This will retrieve and generate the *Slave* switches' information and all the relevant dialog boxes will be populated with data.
2. Configure the slave switch, i.e. copy the configuration file of the master with appropriate changes to the slave.



Saved Successfully

Enable Master ☑

Generate & save new key to disk

Status	Device	IP Address	□ All
●	WLAN_CONTROLLER	192.168.7.194	Master
●	WLAN_CONTROLLER	192.168.7.159	□

Saved Successfully

Time	Sev	Description	Type
22/09/2008 11:10:28	1	Client 00:0B:6B:4D:62:06 (aid=1) has associated to 00:13:A6:00:18:41 (essid: extr_sqa_194g)	01
22/09/2008 11:10:22	1	Client 00:0B:6B:4D:62:06 (aid=1) has disassociated from 00:13:A6:00:18:41, ESSID: extr_sqa_194g, Reason: 2048	02
22/09/2008 11:09:53	1	Client 00:0B:6B:4D:62:06 (aid=1) has associated to 00:13:A6:00:18:41 (essid: extr_sqa_194g)	01

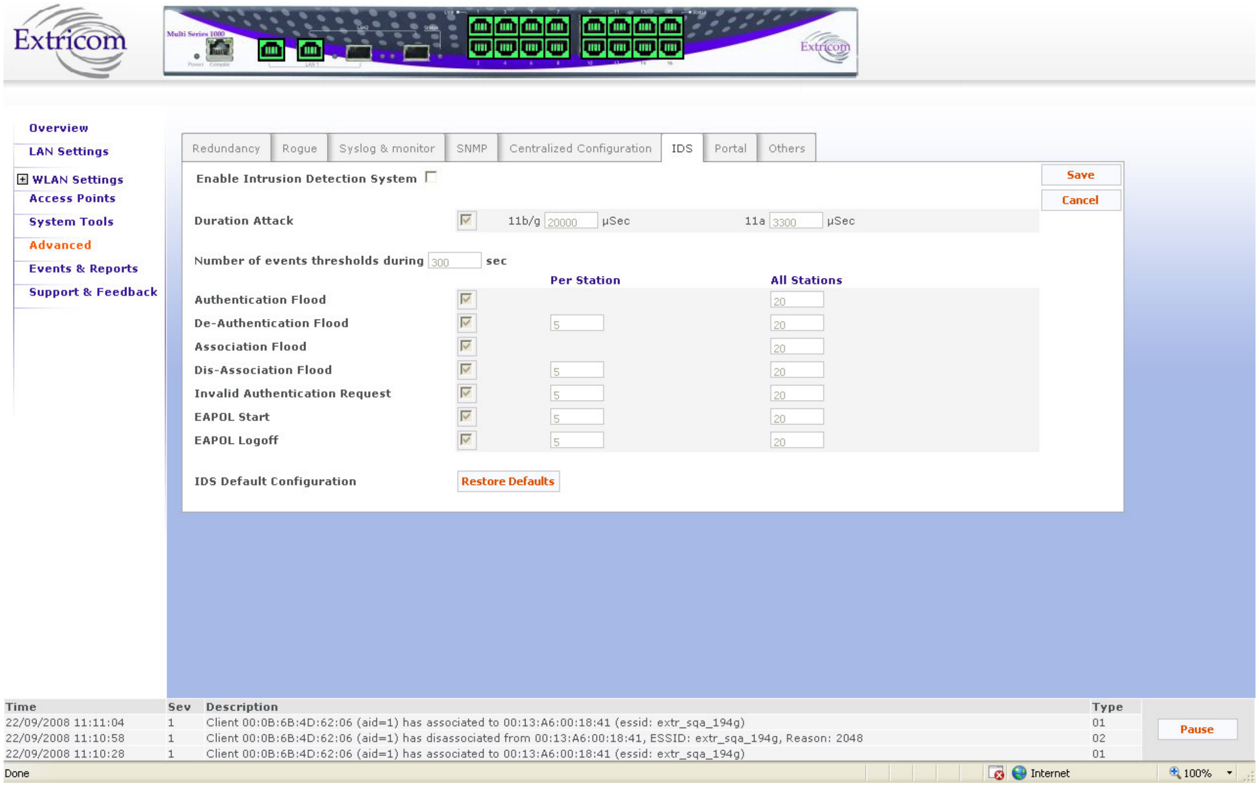
Done

Figure 44: Action Options

3. Reboot the *Slave* switches.

IDS Tab

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 type of attack 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 attacker details (i.e. MAC address). Network administrators can use this information to take action and block malicious users.



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 Restore Defaults

Time	Sev	Description	Type
22/09/2008 11:11:04	1	Client 00:0B:6B:4D:62:06 (aid=1) has associated to 00:13:A6:00:18:41 (essid: extr_sqa_194g)	01
22/09/2008 11:10:58	1	Client 00:0B:6B:4D:62:06 (aid=1) has disassociated from 00:13:A6:00:18:41, ESSID: extr_sqa_194g, Reason: 2048	02
22/09/2008 11:10:28	1	Client 00:0B:6B:4D:62:06 (aid=1) has associated to 00:13:A6:00:18:41 (essid: extr_sqa_194g)	01

Figure 45: IDS Configuration Tab

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	Select check box to enable this feature
11b/g , 11a µsec box	Define the Max NAV period after which attack is discovered
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 is assigned a limit **per station**
All station	Number of times a specific event is allowed during the event threshold. Each of the possible attack types listed below 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

Table 28: IDS Configuration Features

Portal Tab (Captive Portal)

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

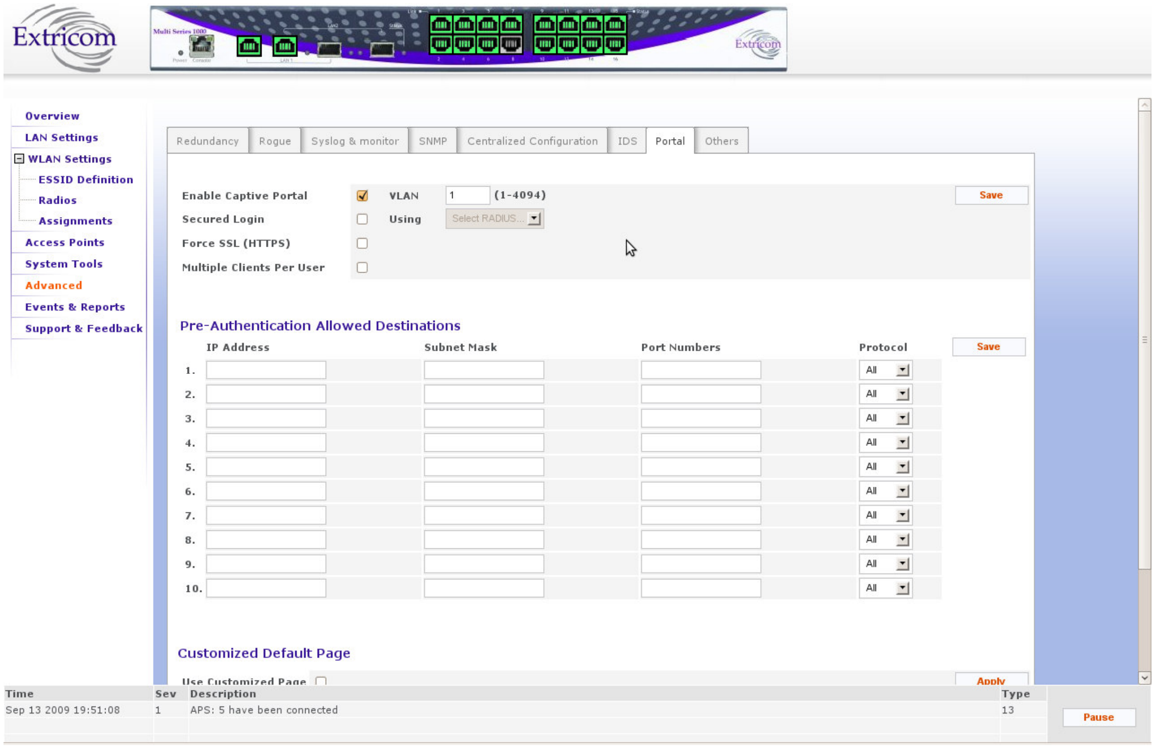
There are two Captive Portal web page types:

- **SSL-based Secured Logging**: In Secured Logging, a user is initially authenticated before they are allowed internet access. The user enters their username and 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, guest access, etc.

- **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, etc.

The **Portal** tab allows you to configure the following Captive Portal settings:

- Enable/Disable Captive Portal
- Set Captive Portal parameters
- Set Walled Garden configuration(Pre-authentication allowed destinations)
- Define a customized Captive Portal web page
- Upload a customized Captive Portal web page



Enable Captive Portal ☑ VLAN 1 (1-4094)

Secured Login □ Using Select RADIUS...

Force SSL (HTTPS) □

Multiple Clients Per User □

Pre-Authentication Allowed Destinations

	IP Address	Subnet Mask	Port Numbers	Protocol
1.				All
2.				All
3.				All
4.				All
5.				All
6.				All
7.				All
8.				All
9.				All
10.				All

Customized Default Page

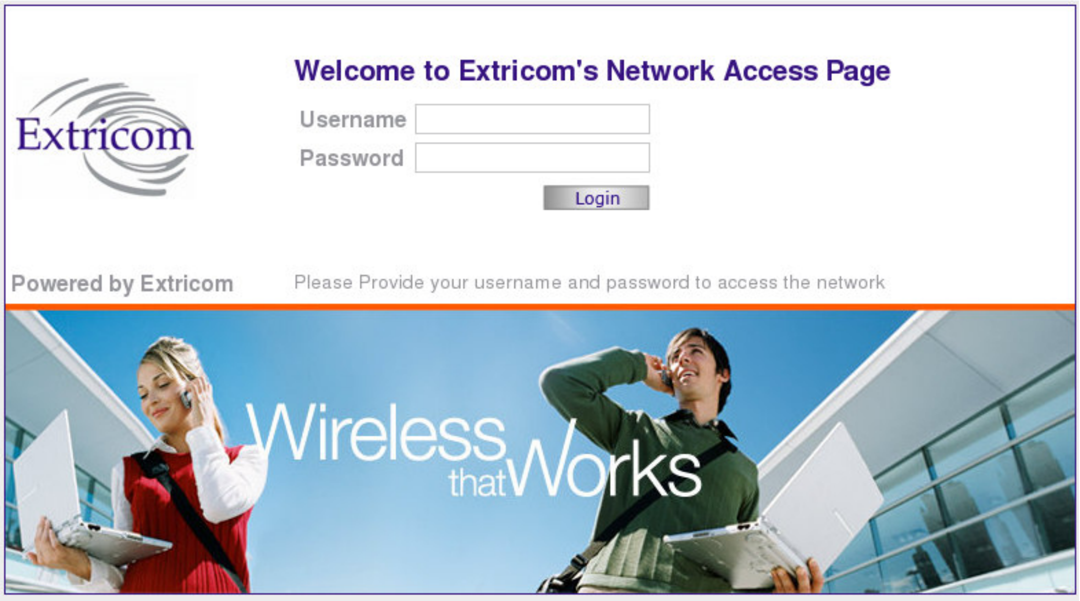
Use Customized Page □

Time	Sev	Description	Type
Sep 13 2009 19:51:08	1	APS: 5 have been connected	13

Figure 46: Captive Portal Configuration

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 the Captive portal web page, either required authentication via RADIUS server, or Open Access login.
Using RADIUS	Set the RADIUS server used for Secured Logging
Force SSL (HTTPS)	When this option is activated, 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 additional clients to connect via the portal, when they are using the same user name and password of an already connected client.
Walled Garden (pre-authentication allowed destination)	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) can be composed of any IP address/Sub Net mask, Port number and IP protocol type.
Customize default page	If you don't check the "Use Customized Page" check box , then the captive portal web page will be set to Extricom default web page, otherwise follow the instructions to customize the page
Use Upload page	Allows you to upload your own captive portal web page. Use the **instruction** link to build your web page.

***Table 29:* Captive Portal Fields**



Welcome to Extricom's Network Access Page

Username

Password

Powered by Extricom

Please Provide your username and password to access the network

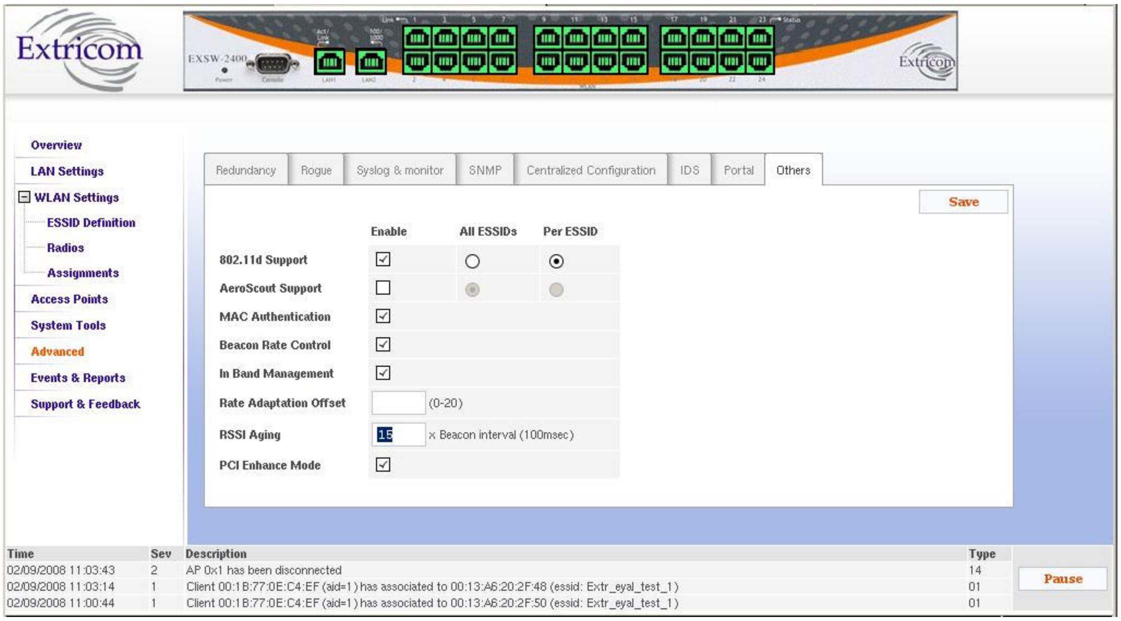
Figure 47: Extricom Default Captive Portal Web Page

Others Tab

This tab provides other advanced configuration functions such as AeroScout and 802.11d.

- Select the **802.11d Support** check box if you wish to enable this option. You can enable it per ESSID or for all ESSIDs.
- Select the **AeroScout Support** check box if you wish to enable this option. You can enable it per ESSID or for all ESSIDs.
- Select the **In Band management** check box if you wish to enable this option (This is a general enable for the option and requires per ESSDI configuration).
- Rate Adaptation algorithm fine-tuning
  - Set **Rate adaptation offset** [0-20] (default is 0) – The Rate adaptation algorithm is based on received RSSI values. This parameter will change the sensitivity of the effect of RSSI value changes on the rate adaptation. The higher the value the less sensitive it will be.
  - Set **RSSI aging** (default is 15) - This parameter determines the period of time to wait before switching to the lowest rate if no RSSI information is received from a client. This is measured in multiplication of 100msec (every beacon interval)
- Select **PCI enhanced mode (**Checked by default) – This is related to different HW versions of the EXRP boards. If the Access Points don't function , uncheck this selection (notify the Extricom support team)

To activate these options per ESSID, after selecting the above check boxes go to the **WLAN Settings** page.



	Enable	All ESSIDs	Per ESSID
802.11d Support	☑	○	●
AeroScout Support	☐	●	○
MAC Authentication	☑		
Beacon Rate Control	☑		
In Band Management	☑		
Rate Adaptation Offset		(0-20)	
RSSI Aging	15	x Beacon interval (100msec)	
PCI Enhance Mode	☑		

```
Time                 Sev  Description                                                                                Type
02/09/2008 11:03:43  2    AP 0x1 has been disconnected                                                               14
02/09/2008 11:03:14  1    Client 00:1B:77:0E:C4:EF (aid=1) has associated to 00:13:A6:20:2F:48 (essid: Extr_eyal_test_1)  01
02/09/2008 11:00:44  1    Client 00:1B:77:0E:C4:EF (aid=1) has associated to 00:13:A6:20:2F:50 (essid: Extr_eyal_test_1)  01
```

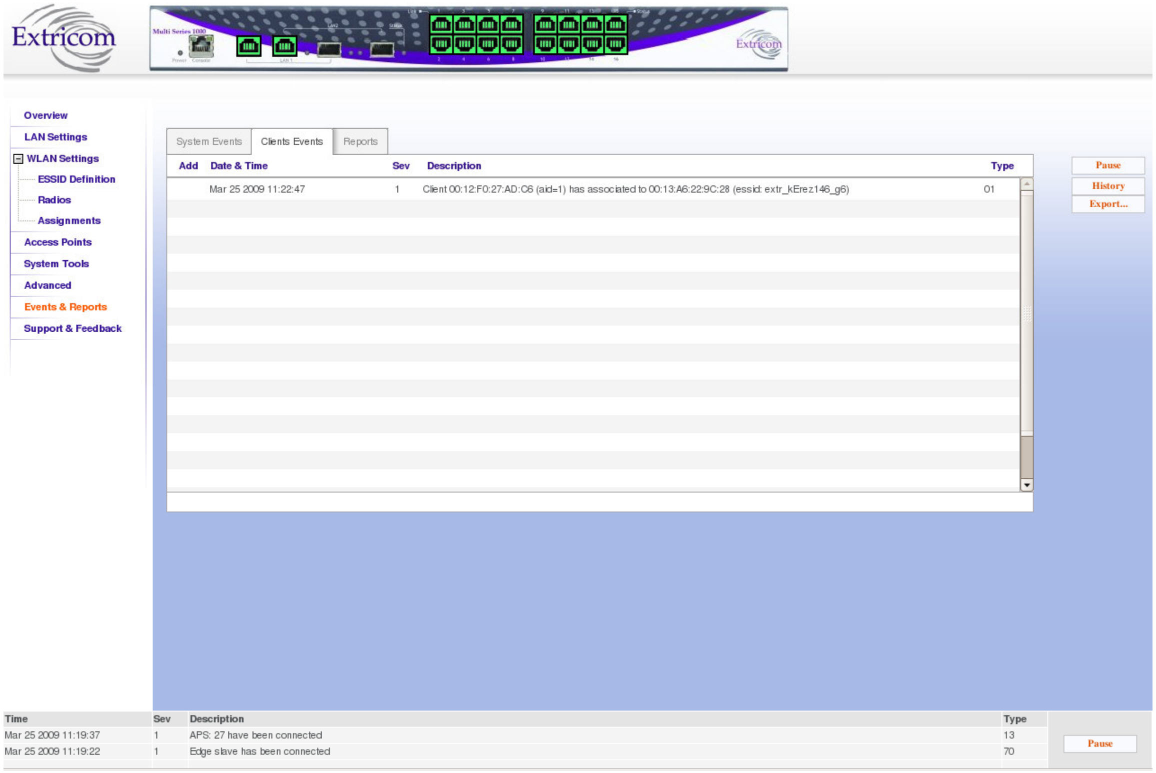
Figure 48: Other Configuration Tab

Viewing Events and Reports

The *Events & Reports* page provides performance reports and list of events.

To view Reports & Events:

1. Click **Events & Reports** in the navigation tree.
2. Select the **Reports** tab to view TrueReuse performance and downlink throughput. The screen updates every few seconds.
3. Select the **System Events** tab to view system alarms and events.
4. Select the **Clients Events** tab to view client association and disassociation events only.
5. Select **Pause /Continue** if you wish to stop/start the events flow.
6. If a message is signed with the sign in the **Add** field, by clicking this message (of an associated user), the user's MAC address will be automatically inserted into the MAC ACL list.
7. Press **History** to see past events (up to a maximum of 1000 most recent events).
8. Press **Export** to export the alarms and events to a .CSV file.



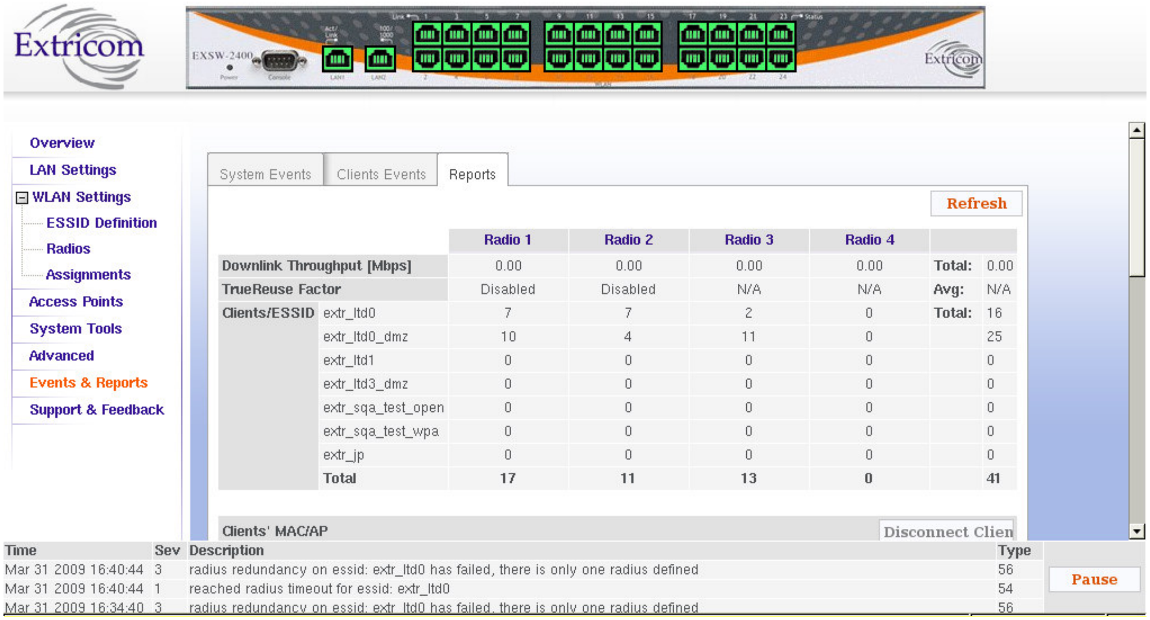
Add	Date & Time	Sev	Description	Type
	Mar 25 2009 11:22:47	1	Client 00:12:F0:27:AD:C6 (aid=1) has associated to 00:13:A6:22:9C:28 (essid: extr_kErez146_g6)	01

Time	Sev	Description	Type
Mar 25 2009 11:19:37	1	APS: 27 have been connected	13
Mar 25 2009 11:19:22	1	Edge slave has been connected	70

Figure 49: Event Log Page

Reports Window - Details

The Reports window, shown below, provides a wide range of statistics:



		Radio 1	Radio 2	Radio 3	Radio 4		
Downlink Throughput [Mbps]		0.00	0.00	0.00	0.00	Total:	0.00
TrueReuse Factor		Disabled	Disabled	N/A	N/A	Avg:	N/A
Clients/ESSID	extr_ltd0	7	7	2	0	Total:	16
	extr_ltd0_dmz	10	4	11	0		25
	extr_ltd1	0	0	0	0		0
	extr_ltd3_dmz	0	0	0	0		0
	extr_sqa_test_open	0	0	0	0		0
	extr_sqa_test_wpa	0	0	0	0		0
	extr_jp	0	0	0	0		0
	Total	17	11	13	0		41

Clients' MAC/AP

```
Time                  Sev  Description                                                                    Type
Mar 31 2009 16:40:44  3    radius redundancy on essid: extr_ltd0 has failed, there is only one radius defined  56
Mar 31 2009 16:40:44  1    reached radius timeout for essid: extr_ltd0                                    54
Mar 31 2009 16:34:40  3    radius redundancy on essid: extr_ltd0 has failed, there is only one radius defined  56
```

Figure 50: Reports Window – Top

Statistics are available on a per radio channel basis, as well as per switch. The following table describes the information that is available on this page:

Field	Description
Downlink Throughput	Mbps. Based on a 1 second snapshot of data volume carried by all downlinks on a particular radio channel (channel blanket).
Total	Total downlink throughput of the switch, based on a 1 second snapshot of data volume.
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 was not enabled. Computes the average no. of downlinks transmitting simultaneously per radio channel. The average is computed based on several snapshots taken during a 1 second time interval. Example: a value of 3 means that downlink throughput with TrueReuse is currently 3x higher on average on that radio channel than if TrueReuse had been disabled.
Avg.	TrueReuse Factor averaged over all radio channels

Field	Description
Clients /ESSID	# of clients connected per ESSID per radio channel
Clients/ESSID Totals	Total 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.
Display IP Address	Hide or display the IP address of each client.

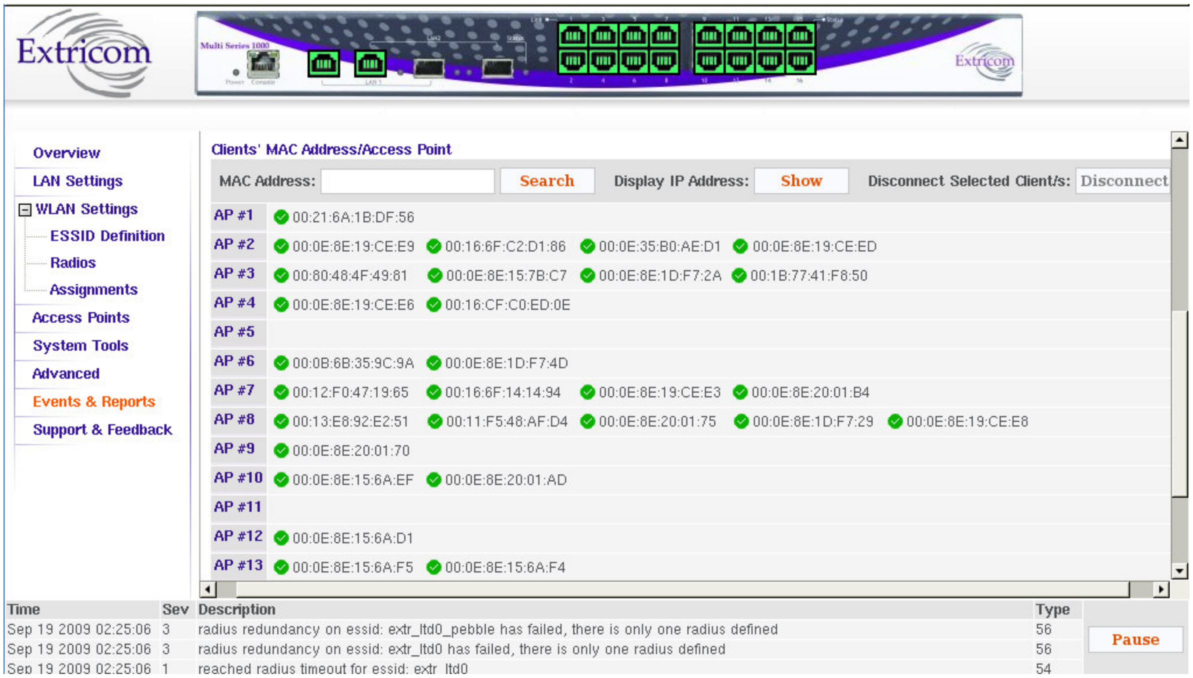
Colored Status Icon	Green = client connected to AP.
	Red = client connection problem
	Notes:
	1. "Client connection problem" means a client that for too long, is in an interim state between disconnected and connected. For example, a client that is associated but not authenticated. After the disassociation timeout (default 1 hour), the switch will disconnect such a client.

Disconnect Selected Client/s	Used to reset a client connection, in order to help a client establish a working connection.

Table 30: Reports Window Fields

✍ Note: the statistics window does not refresh automatically. Click on **Refresh** to update the statistics.

Further down the screen in this tab folder, the clients (MACs) per AP are listed:



Clients' MAC Address/Access Point

MAC Address: | Display IP Address: | Disconnect Selected Client/s:

AP #1	✓ 00:21:6A:1B:DF:56				
AP #2	✓ 00:0E:8E:19:CE:E9	✓ 00:16:6F:C2:D1:86	✓ 00:0E:35:B0:AE:D1	✓ 00:0E:8E:19:CE:ED	
AP #3	✓ 00:80:48:4F:49:81	✓ 00:0E:8E:15:7B:C7	✓ 00:0E:8E:1D:F7:2A	✓ 00:1B:77:41:F8:50	
AP #4	✓ 00:0E:8E:19:CE:E6	✓ 00:16:CF:C0:ED:0E			
AP #5					
AP #6	✓ 00:0B:6B:35:9C:9A	✓ 00:0E:8E:1D:F7:4D			
AP #7	✓ 00:12:F0:47:19:65	✓ 00:16:6F:14:14:94	✓ 00:0E:8E:19:CE:E3	✓ 00:0E:8E:20:01:B4	
AP #8	✓ 00:13:E8:92:E2:51	✓ 00:11:F5:48:AF:D4	✓ 00:0E:8E:20:01:75	✓ 00:0E:8E:1D:F7:29	✓ 00:0E:8E:19:CE:E8
AP #9	✓ 00:0E:8E:20:01:70				
AP #10	✓ 00:0E:8E:15:6A:EF	✓ 00:0E:8E:20:01:AD			
AP #11					
AP #12	✓ 00:0E:8E:15:6A:D1				
AP #13	✓ 00:0E:8E:15:6A:F5	✓ 00:0E:8E:15:6A:F4			

```
Time                  Sev  Description                                                                           Type
Sep 19 2009 02:25:06  3    radius redundancy on essid: extr_ltd0_pebble has failed, there is only one radius defined  56
Sep 19 2009 02:25:06  3    radius redundancy on essid: extr_ltd0 has failed, there is only one radius defined         56
Sep 19 2009 02:25:06  1    reached radius timeout for essid: extr_ltd0                                               54
```

Figure 51: Reports Window – Bottom

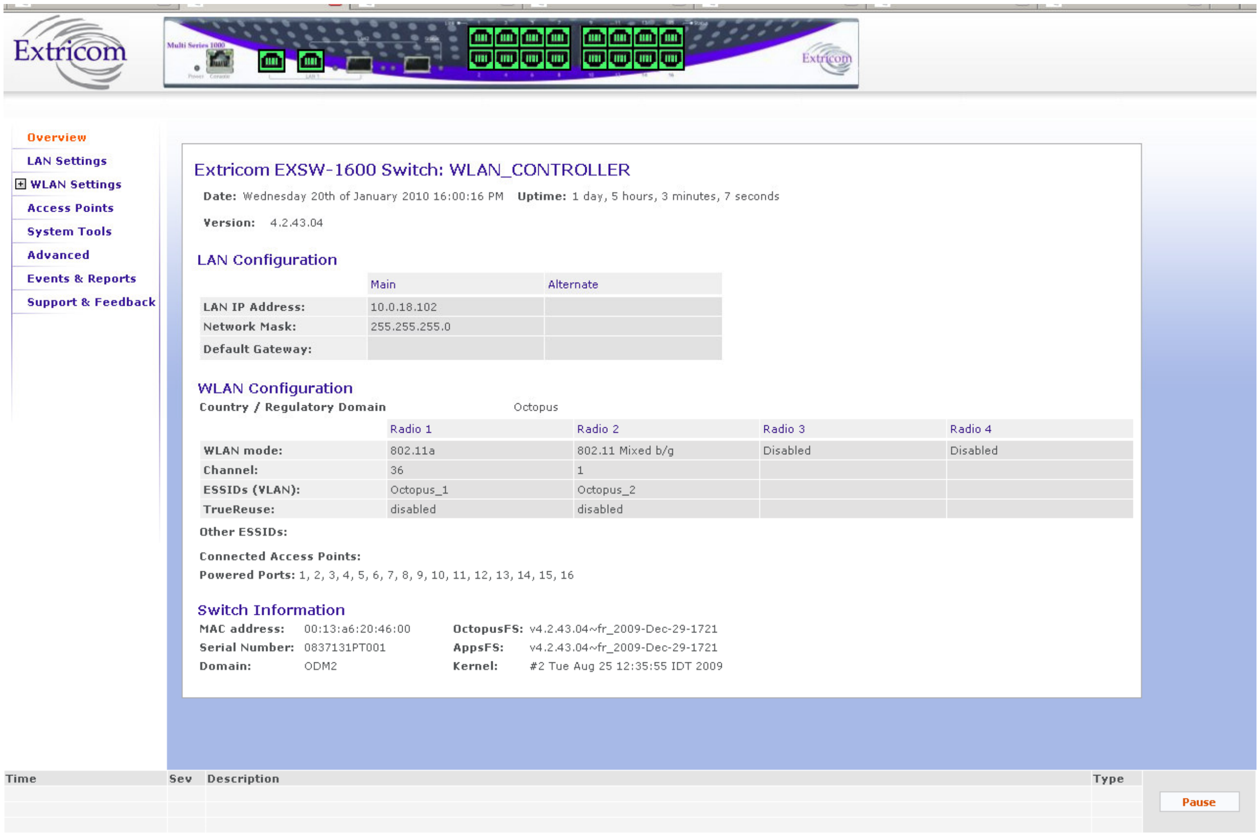
A client can be temporarily disconnected using the **Disconnect** button. The client must then reauthenticate to reconnect to the WLAN.

Viewing an Overview of the Configuration

The **Overview** page provides a summary of the current configuration.

To view a summary of the updated configuration:

1. Click **Overview** in the navigation tree.



Extricom EXSW-1600 Switch: WLAN_CONTROLLER

Date: Wednesday 20th of January 2010 16:00:16 PM **Uptime:** 1 day, 5 hours, 3 minutes, 7 seconds

Version: 4.2.43.04

LAN Configuration

	Main	Alternate
LAN IP Address:	10.0.18.102	
Network Mask:	255.255.255.0	
Default Gateway:		

WLAN Configuration

Country / Regulatory Domain Octopus

	Radio 1	Radio 2	Radio 3	Radio 4
WLAN mode:	802.11a	802.11 Mixed b/g	Disabled	Disabled
Channel:	36	1		
ESSIDs (VLAN):	Octopus_1	Octopus_2		
TrueReuse:	disabled	disabled		

Other ESSIDs:

Connected Access Points:

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

Switch Information

MAC address:	00:13:a6:20:46:00	**OctopusFS:**	v4.2.43.04~fr_2009-Dec-29-1721
Serial Number:	0837131PT001	**AppsFS:**	v4.2.43.04~fr_2009-Dec-29-1721
Domain:	ODM2	**Kernel:**	#2 Tue Aug 25 12:35:55 IDT 2009

Time	Sev	Description	Type

Figure 52: Configuration Overview

Refer to Table 31 for a description of the summary information.

Field	Description
Date	Displays the date and time the summary was created.
Uptime	Displays the amount of time the switch has been active.
LAN Configuration	
Main	IP address of the switch.
	Network mask
	Default gateway
WLAN Configuration	
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)

Field	Description
Channel	Displays the channel for each radio (1 – 4,Rogue)
ESSIDs (vlan)	Displays the ESSIDs and their related VLANs, defined and assigned to each radio (1-4, Rogue)
TrueReuse	Displays TrueReuse status for each radio
Other ESSIDs	Displays other ESSIDs that are defined but are not assigned to a specific radio.
Connected Access Points	List of the active APs.
Powered Ports	List of WLAN ports which have PoE enabled.
Switch Configuration	
MAC address	Displays the base MAC address of the switch near the MAC address.
Serial Number	Displays the switch unique serial number
Domain	RF localization indication
OctopusFS:	Extricom firmware application version and build date
AppsFS	Third-party software application version and build date
RootFS	Linux file system build date
Kernel	Extricom-specific Linux kernel build date
Redboot	Linux redboot build date

***Table 31:* Summary Page Features**

Chapter 4

Troubleshooting

Table 32 lists problems you may encounter with your WLAN and provides possible solutions. If after trying the solutions you are still experiencing difficulties, contact Extricom Customer Support.

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* Web configuration page (refer to *page 94*).
A wireless device can't 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 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 WLAN, or 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 WLAN, or 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 Access Point.

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`.

Table 32: Troubleshooting

Chapter 5

Northbound SNMP Traps

The table below lists and describes the SNMP Traps sent by the Extricom 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 (e.g. 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.

Trap No.	Trap Name	Description	Version
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 that the client is associated to.	4.1 or above
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 that the client disassociated from. The disassociation reason code is also sent.	4.1 or above
4	EAPOL Key Error	A client attempted to associate using WPA but there was an error with the EAPOL key. The trap will detail 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.	4.1 or above

Trap No.	Trap Name	Description	Version
13	AP Connected	One or more APs has been connected to the switch (AP has been physically connected via Ethernet cable, or it was already connected and PoE has been enabled). Tthe AP number corresponds to the port number on the switch that the AP is connected to. Upon switch startup or reconfigure, this trap will be sent listing all the APs connected.	4.1 or above
14	AP Off	One of more APs has been disabled. The AP Ethernet cable has either been physically disconnected from the switch or PoE has been turned off. Tthe AP number corresponds to the port number on the switch that the AP is connected to.	4.1 or above
19	Redundancy peer connection up	When using "Normal" (not "Cascade") redundancy, this switch has regained connectivity with the peer switch.	4.1 or above
20	Redundancy peer connection down	When using "Normal" (not "Cascade") redundancy, this switch has lost connectivity with the peer switch	4.1 or above
21	Redundancy keepalive connection up	When using "Normal" (not "Cascade") redundancy, the switch regained connectivity to the Reference IP.	4.1 or above
22	Redundancy keepalive connection down	When using "Normal" (not "Cascade") redundancy, the switch lost connectivity to the Reference IP.	4.1 or above
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 will have done so because it detected a failure in the primary switch. If the Primary switch is issuing this trap it means it has recovered from an error and is now resuming wireless	4.1 or above

Trap No.	Trap Name	Description	Version
		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 means it discovered an error (for example connectivity to Reference IP is lost) in which case the trap will specify what the error is. If the Secondary switch is issuing this trap it means that the Primary has recovered from an error and the secondary is transferring wireless responsibility back to it.	4.1 or above
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 will detail if the rogue network was an AP or ad-hoc, the relevant BSSID and ESSID, what channel the rogue was transmitting on, which Extricom AP on the switch was closest to the rogue AP, and approximately how far the rogue AP was, from the Extricom AP.	4.1 or above
29	Rogue AP found	Available only when Rogue AP Detection is enabled. This trap indicates that a rogue network has been detected. The trap will detail if the rogue network is an AP or ad-hoc, the relevant BSSID and ESSID, what channel the rogue is transmitting on, which Extricom AP is closest to the rogue AP, and approximately how far	4.1 or above

Trap No.	Trap Name	Description	Version
		the rogue AP is from the Extricom 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 will always come after trap 29. This trap will detail if the rogue network is an AP or ad-hoc, the relevant BSSID and ESSID, what channel the rogue is transmitting on, which Extricom AP is closest to the rogue AP, and approximately how far the rogue AP is from the Extricom AP.	4.1 or above
43	Intrusion detection Duration attack	Available only when Intrusion Detection is enabled. Indicates that the switch has detected a Duration attack.The trap will detail the duration length as well as the transmitting MAC address.	4.1 or above
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 will detail how many associations were received and within what time interval.	4.1 or above
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 will detail how many disassociations were received and within what time interval. If the event was triggered from a per station limitation, the trap will also include the client MAC address.	4.1 or above

Trap No.	Trap Name	Description	Version
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 will detail how many associations were received and in what time interval.	4.1 or above
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 will detail how many authentications were received and in what time interval.	4.1 or above
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 will detail how many de-authentications were received and in what time interval. If the event was triggered from a per station limitation the trap will also include the client MAC address.	4.1 or above
50	Intrusion detection RF Jamming attack	Available only when Intrusion Detection is enabled. Indicates that the switch has detected an RF Jamming attack	4.1 or above
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 will detail how many EAPOL Start packets were received and in what time interval. If the event was triggered from a per station limitation, the trap will also include the client MAC address.	4.1 or above

Trap No.	Trap Name	Description	Version
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 will detail how many EAPOL Logoff packets were received and in what time interval. If the event was triggered from a per station limitation, the trap will also include the client MAC address.	4.1 or above
53	Intrusion detection De-Authentication Broadcast	Available only when Intrusion Detection is enabled. Indicates that the switch has detected a De-Authentication Broadcast	4.1 or above
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 will attempt to authenticate the client using this server. The trap details which ESSID the authentication attempt occurred on.	4.1 or above
55	Radius Changed selection	This trap will occur after trap 54, if the ESSID has multiple RADIUS servers configured. The trap will detail which RADIUS server it is changing from and to which server it is changing to.	4.1 or above
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.	4.1 or above
57	RF localization failed	The switch localization lock is missing or corrupt. Contact an Extricom representative.	4.1 or above
59	Firmware upgrade startup	Switch firmware upgrade has started.	4.2.42.2 or above

Trap No.	Trap Name	Description	Version
60	Firmware upgrade done	Switch firmware upgrade has ended.	4.2.42.2 or above
61	Firmware upgrade progress	This trap is sent with a progress update during the switch firmware upgrade.	4.2.42.2 or above
62	Firmware upgrade failed	Switch firmware upgrade has failed.	4.2.42.2 or above
63	Reconfigure ended	Switch reconfigure has ended.	4.2.42.2 or above
65	Radio is not functioning in access points	One or more of the radios in a channel blanket is not functioning. The trap will detail which radio in which AP is not functioning.	4.1 or above
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.	4.1 or above
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.	4.2.42.2 or above
68	Edge Mode Switchover	The secondary switch in a switch cascade is changing to standalone mode. This trap will be sent from the secondary switch. The trap will detail the reason for the switchover.	4.2.42.2 or above
69	Reconfigure started	Switch reconfigure has started.	4.2.42.2 or above
70	Edge Connected	A secondary switch of a switch cascade has connected and synchronized with the primary switch. This trap will be sent from the primary switch.	4.2.42.2 or above

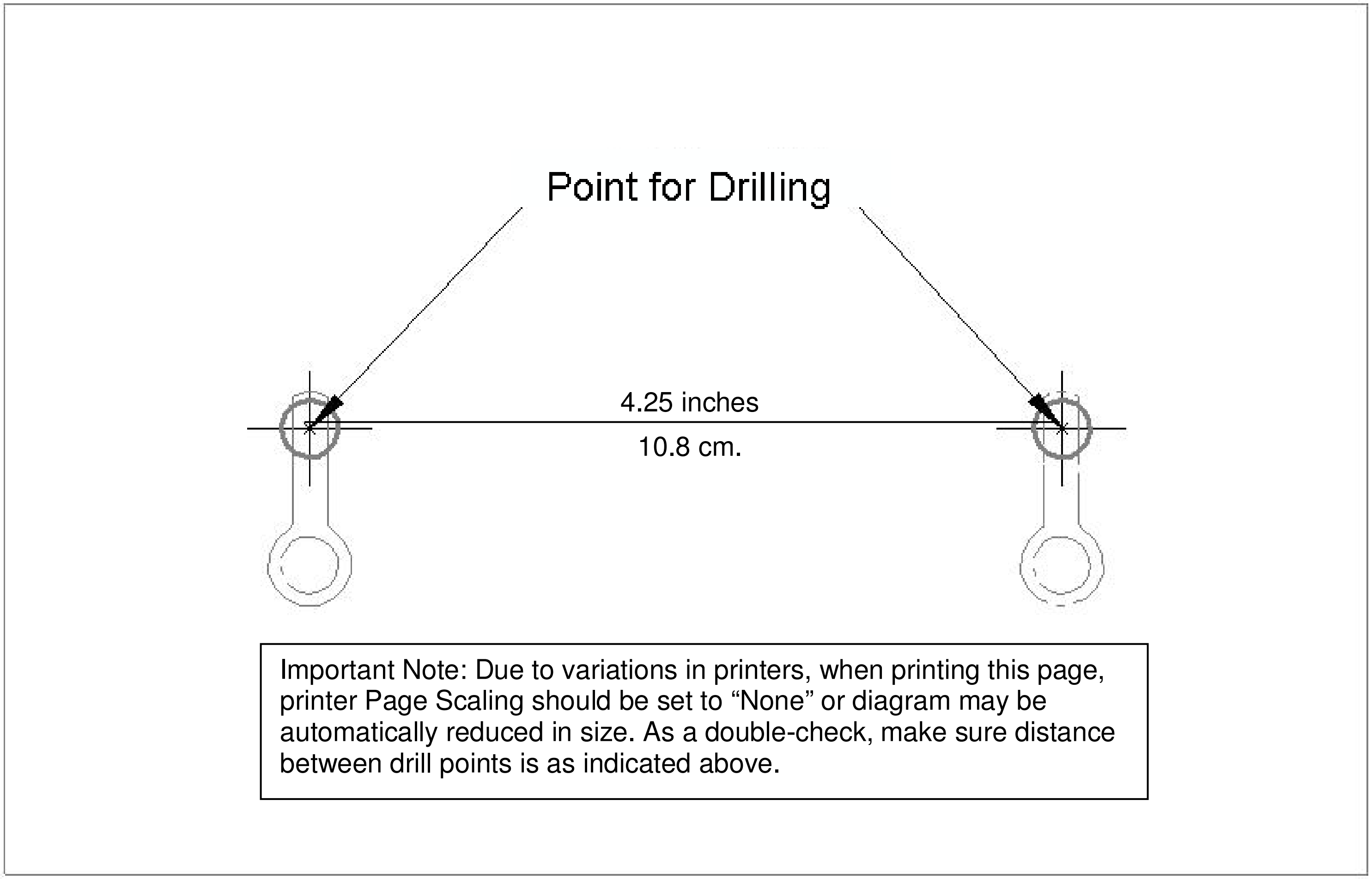
Trap No.	Trap Name	Description	Version
71	Edge Disconnected	A secondary switch of a cascade has been disconnected from the primary switch. This trap will be sent from the primary switch. This trap will be sent if the link between the primary switch and the secondary is down or if the secondary switch is non-responsive	4.2.42.2 or above
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.	4.1 or above
73	Start.sh Started	Start.sh is being run on the switch.	4.2.42.2 or above
74	Start.sh ended	Start.sh has finished running on the switch.	4.2.42.2 or above
75	Starting Boot	the Switch is being rebooted.	4.2.42.2 or above
76	Changed Wireless Status (On/Off)	The wireless has been enabled or disabled on the switch. The trap will say if the wireless has been turned "ON" of "OFF" and will include the reason for the change. In case 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.	4.2.42.2 or above
77	Radio reset	A problem at the radio required a warm reset. The trap details which radio in which AP required the warm reset.	4.1 or above

Trap No.	Trap Name	Description	Version
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.	4.1 or above
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.	4.1 or above

Table 33: SNMP Traps

Appendix A

Internal Access Point Mounting Template



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

Figure 53: Access Point Mounting Template