


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	<p>Check this box if you want to enable rate adaptation.</p> <div>  <ul style="list-style-type: none"> 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) </div>
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	<p>Two modes are supported:</p> <ul style="list-style-type: none"> 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.

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

By default, these four WMM prioritization categories are statically mapped to Ethernet 802.1p prioritization tags to allow consistent QoS across wireless and wired network segments. Flow arriving from the wired network tagged with 802.1p priority is mapped to the appropriate Access category, while WMM flow 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 1. 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 CW_{min} up to CW_{max}) 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.

WMM Parameters

	Background	Best Effort	Video	Voice
ACK Policy	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
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	convert to	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 1: 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 2: 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 3: VPT To WMM Destination

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

Table 4: 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:

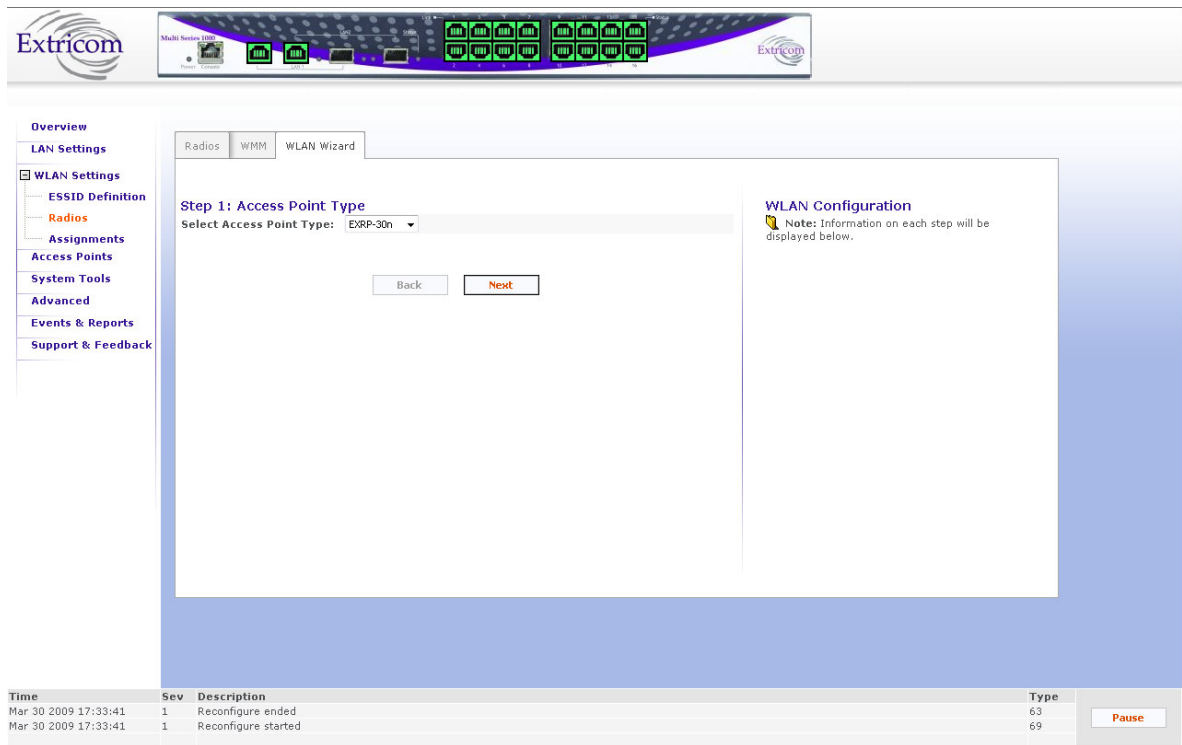


Figure 2: WLAN Wizard

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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
extr_sqa_159g2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Log

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 3: 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.

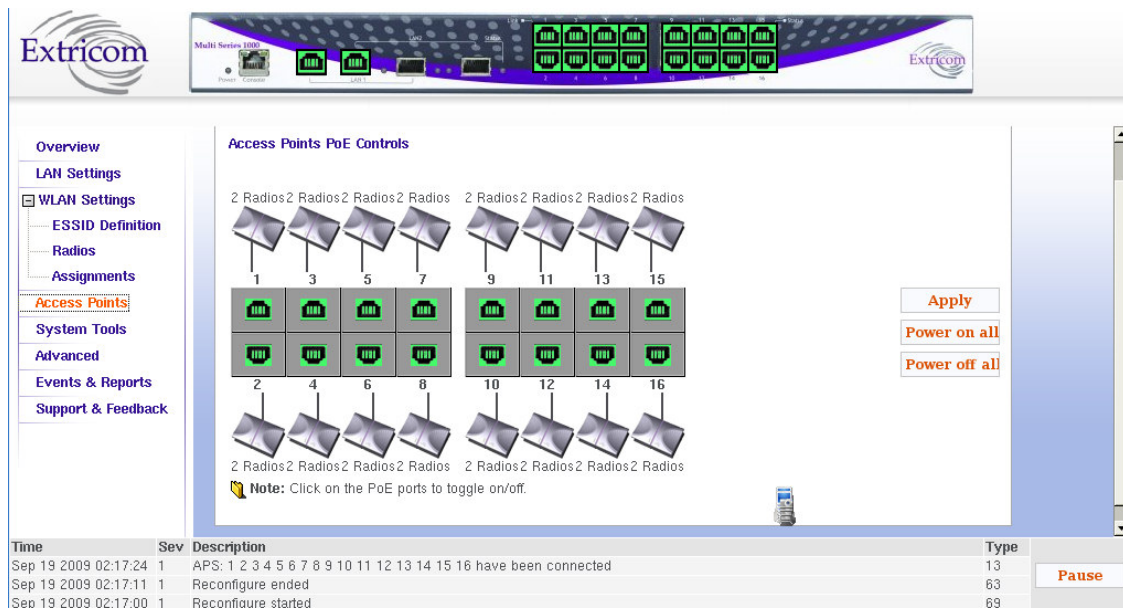


Figure 4: Access Point Configuration Window

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. **Error! Bookmark not defined.**, 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:

Extricom

Multi System 1000

Extricom

Overview

LAN Settings

WLAN Settings

Access Points

System Tools

Advanced

Events & Reports

Support & Feedback

Cascaded Switches

Primary Switch

Secondary Switch

Edge Information

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

Save

Access Points PoE Controls

Click to toggle:

17 19 21 23

25 27 29 31

18 20 22 24

26 28 30 32

Apply

Power on all

Power off all

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	3	APS: 11 have been disconnected	14

Pause

Figure 5: 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)

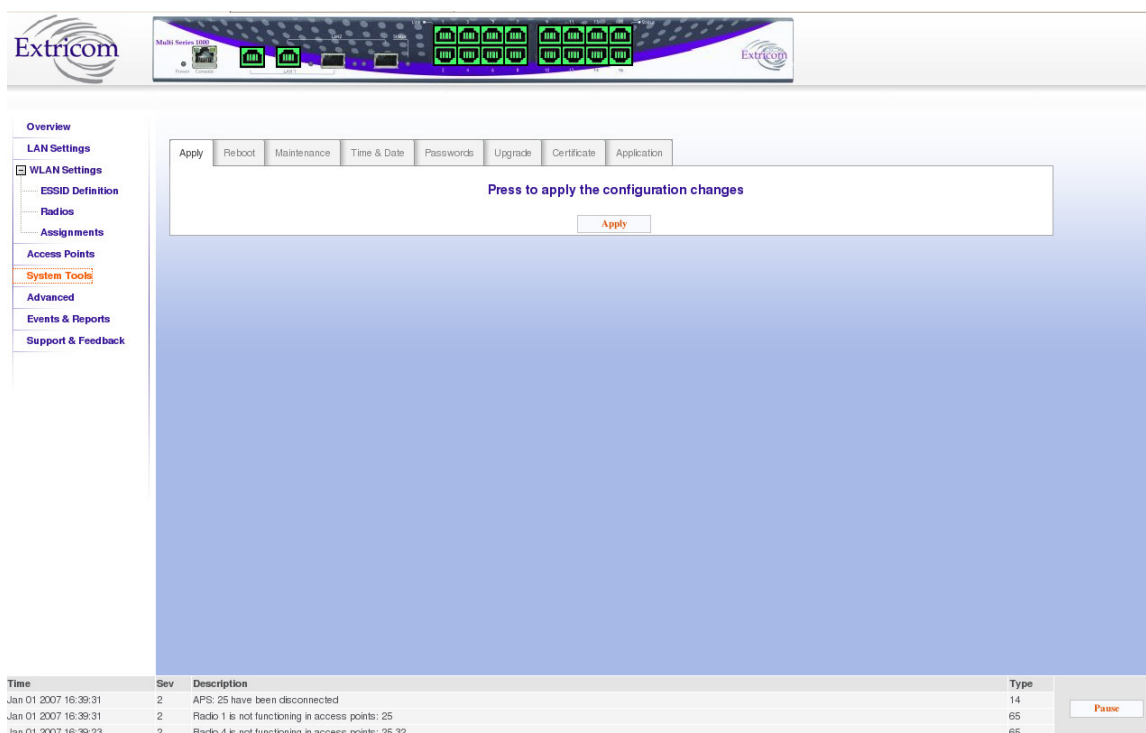


Figure 6: System Tools Configuration Page

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

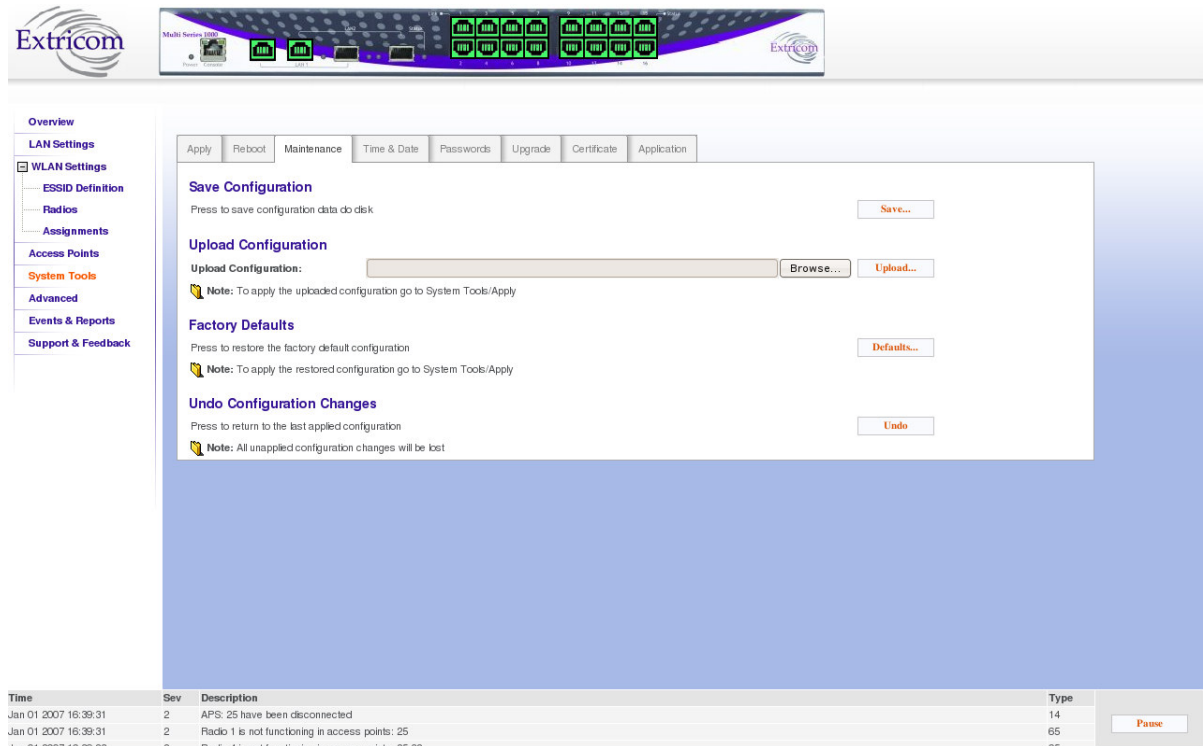


Figure 7: Maintenance Configuration Page

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. <div>  All unapplied configuration changes will be lost. </div>

Table 5: Maintenance Configuration Tab

Time & Date Setting

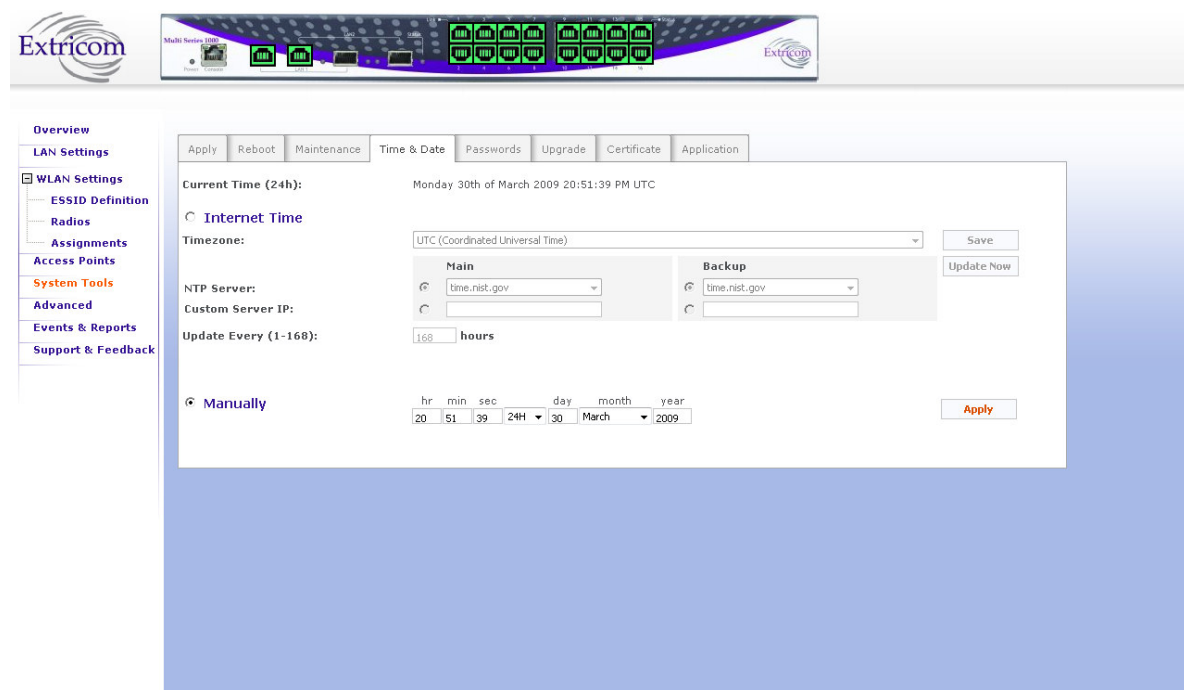


Figure 8: Time & Date Configuration Page

The Extricom system supports two ways of setting Date and Time (refer to Figure 8)

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 6 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 6: 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 the 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:

The screenshot displays the Extricom web interface. At the top, there's a header with the Extricom logo and a navigation bar with tabs: Apply, Reboot, Maintenance, Time & Date, Passwords, Upgrade, Certificate, and Application. The Application tab is selected. On the left, a sidebar menu shows various configuration options: Overview, LAN Settings, WLAN Settings (selected), ESSID Definition, Radios, Assignments, Access Points, System Tools, Advanced, Events & Reports, and Support & Feedback. The main content area is titled 'Application Type' and contains a dropdown menu for 'Select Switch Application Type:' set to 'WLAN Primary Switch'. Below this, a note states: 'Note: the switch will reboot in order for changes to take effect, unapplied configuration will be lost'. An 'Apply & Reboot' button is visible. At the bottom, there's a table with columns: Time, Sev, Description, and Type. The table contains three rows of log entries. A 'Pause' button is located to the right of the table.

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 16:39:31	2	Radios 4 is not functioning in access points: 25, 32	65

Figure 9: 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 7: 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 10 below appears:

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 16:39:31	2	Radio 1 is not functioning in access points: 25	65

Figure 10: 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: <ul style="list-style-type: none">• 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 8: 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 9: Switch Cascade Failover Behavior

Notes:

1. Traffic interruption time during a failover depends on the link and switch core monitoring parameters chosen (see Table 9 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:

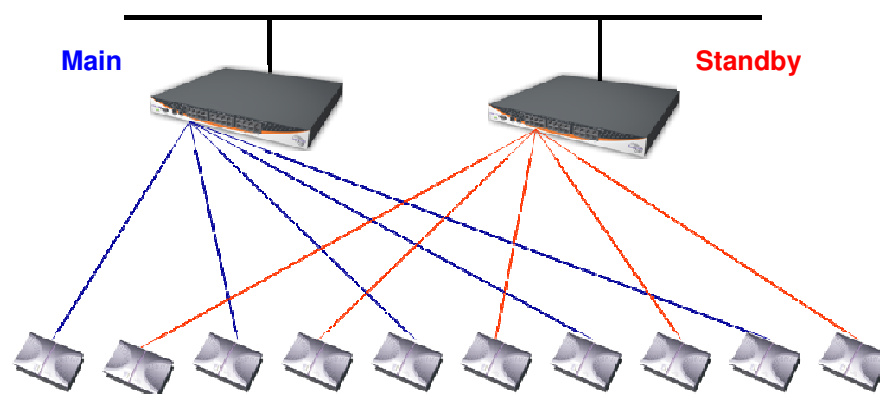


Figure 11: Normal Redundancy Deployment

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: <ul style="list-style-type: none"> • 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 10: 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.

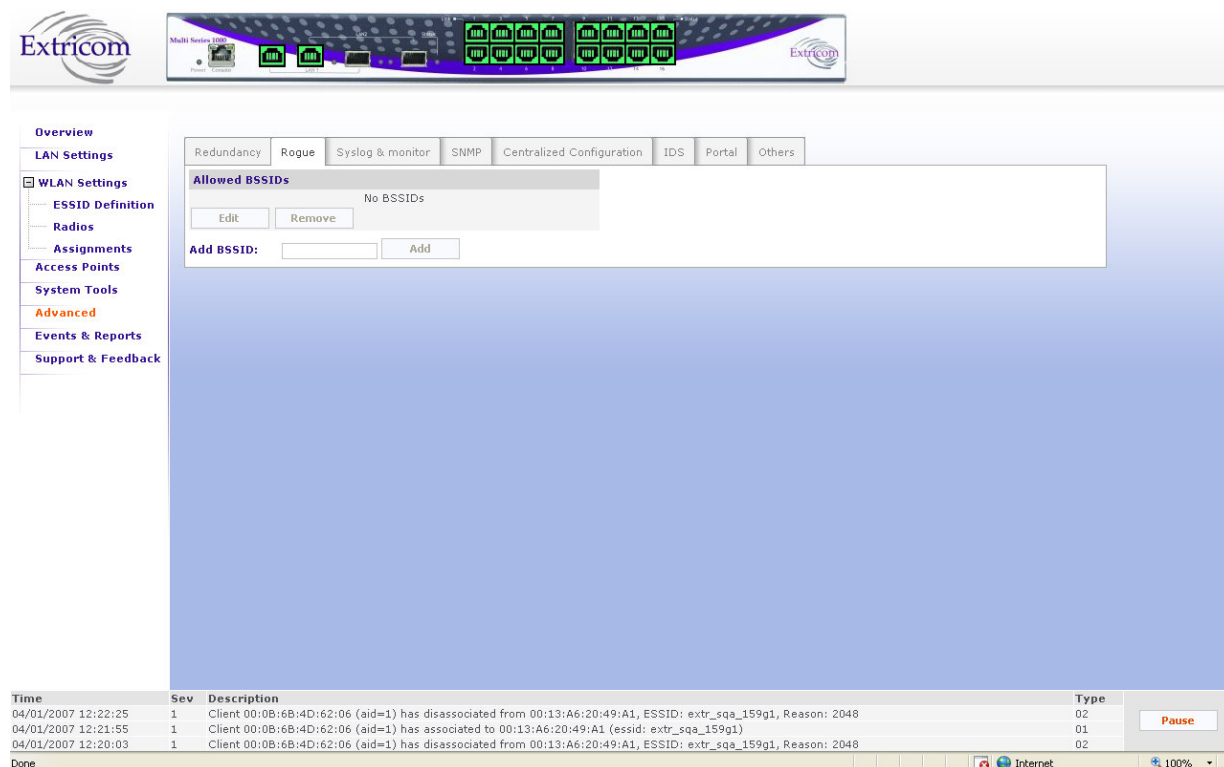


Figure 12: Syslog & Monitor Tab

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 11: 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.

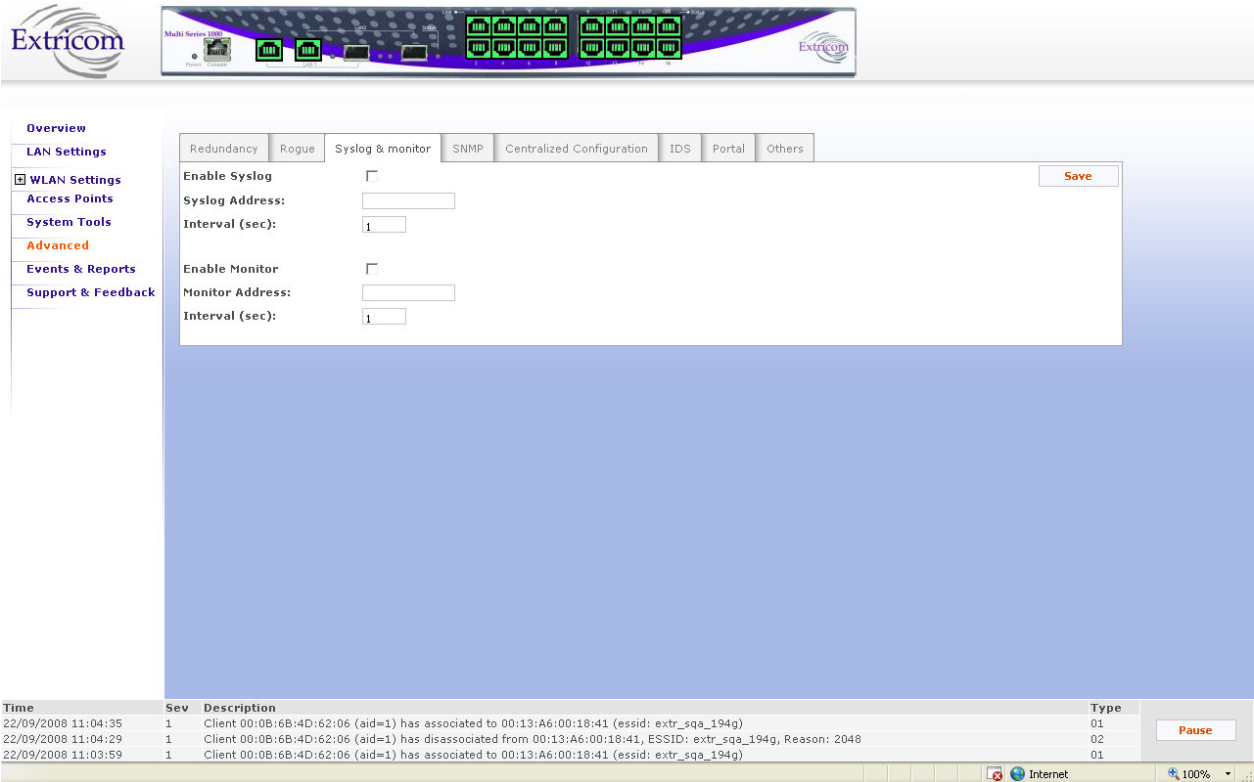



Figure 13: Syslog & Monitor Tab

Field	Description
Enable Syslog	Check to record system information in the System Log.
<div><div>In most common operational scenarios, this option should be unchecked (unless used for troubleshooting).</div></div>	
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	<p>The Monitor Log is only relevant if using Extricom's dedicated network status monitoring tool (not provided with the switch.)</p> <p>By default, this option is not checked.</p> <div>  Check this option only if you are using the Extricom dedicated network monitoring tool, otherwise unnecessary data packets are sent through the Ethernet. </div>
Monitor Address	Enter the address of the Monitor Log if using the Extricom dedicated network monitoring tool.
Interval (sec)	<p>Specifies how often information is sent to the Monitor Log. The default setting is 1 second and this is the recommended interval.</p> <div>  Configure this parameter only if using the dedicated network monitoring tool. </div>

Table 12: 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 14 below.

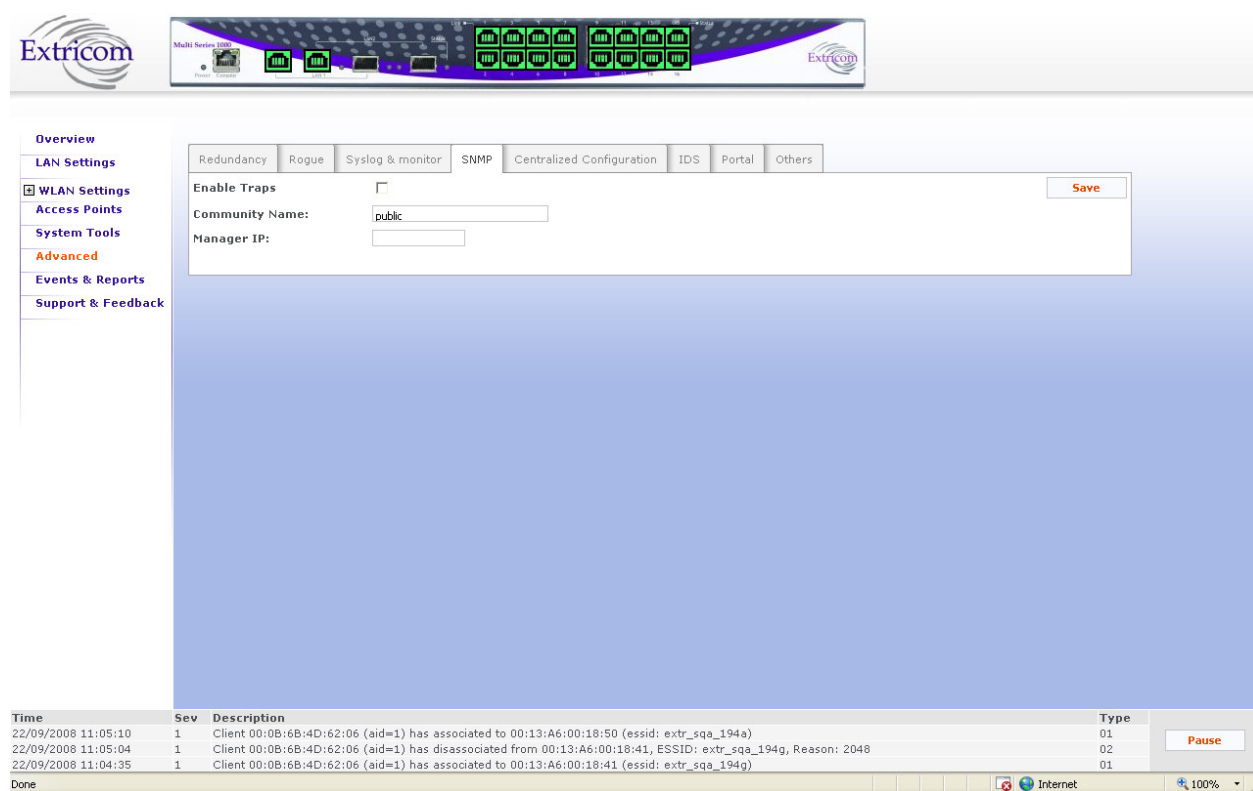


Figure 14: SNMP Configuration Tab

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 13: SNMP Configuration Features

The following is a subset of the traps that are sent northbound from the Extricom switch when Enable Traps is checked:

1. **Client <Client MAC> has associated to <ESSID>** - This trap is sent after successful association with the client MAC address and the ESSID the client associated to.
2. **Client <Client MAC> has disassociated from <ESSID>. Reason: <Reason>** - This trap is sent after client disassociation/disconnection from an ESSID. The reason code is an 802.11 reason code.
3. **Client: <Client MAC> - ESSID: <ESSID> - Cipher suite: <Cipher>** - This trap is sent in case of any key error during four-way handshake (MIC error) or as a result of any key error when receiving data from client.
4. **New Rogue Detected <BSSID><Port><Radio><Channel><RSSI>** - This trap is sent when a new Rogue AP is detected. The trap includes the AP's BSSID, the switch port which detected the Rogue AP, the channel of the Rogue AP and the Rogue AP signal level (RSSI).
5. **Rogue Updated <BSSID><Port><Radio><Channel><RSSI>** - This trap is sent when an existing previously detected Rogue AP is re-detected with change in one of its parameters. The trap includes the AP's BSSID, the switch port which detected the Rogue AP, the channel of the Rogue AP and the Rogue AP signal level (RSSI).
6. **Rogue Removed <BSSID><Port><Radio><Channel><RSSI>** - This trap is sent when a new Rogue AP is detected. The trap includes the AP's BSSID, the switch port which detected the Rogue AP, the channel of the Rogue AP and the Rogue AP signal level (RSSI).
7. **RADIUS Timeout <ESSID><# of timeouts>** - This trap is sent when the RADIUS timeout had elapsed and includes the ESSID and the number of timeouts that occurred.
8. **RADIUS Redundancy Selection Changed <ESSID><#of RADIUS>to<# of RADIUS>** - This trap is sent when the RADIUS selection has been changed from one server to another, and includes the ESSID, the number of the previous server and the number of the new server.
9. **No RADIUS <ESSID>** - This trap is sent when the last RADIUS server failed and includes the ESSID.
10. **Configured and connected APs of channel [<channel number>]** - This trap provides a summary of all APs and their status. This trap is typically sent after an event of AP removal or connection from/to the switch.
11. **AP <ap number in hex base> has been connected** - This trap is typically sent after an event of connecting an AP to the switch.
12. **AP <ap number in hex base> has been disconnected** - This trap is typically sent after an event of disconnecting an AP from the switch.
13. **Reference Host is up** - This trap is sent when the Reference host is up and active. Sent by the Main switch.
14. **Reference Host is down** - This trap is sent when the Reference host is down. Sent by the Main Switch.
15. **Standby Switch is up** - This trap is sent when the Standby Switch is up & active.

16. ***Standby Switch is down*** - This trap is sent when the Standby Switch is down.
17. ***Inactive - Reference Host is down*** - This trap is sent when the Reference host is down, and hence the Main switch becomes inactive.
18. ***Inactive Standby Switch - Main Switch is up*** - This trap is sent when the Main Switch becomes active again and hence the Standby Switch becomes inactive (Switch over).
19. ***Main Switch is active again*** - This trap is sent when the Main Switch changes status from inactive to active and regains the Main switch status.
20. ***Failure detected in Main Switch - Switching Over.*** - This trap is sent when the Main Switch is about to go down and the Standby Switch is becoming Active.

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*.

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 15: 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.

Figure 16: 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.

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

Figure 17: 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.

Attack Type	Per Station	All Stations
Authentication Flood	<input checked="" type="checkbox"/>	20
De-Authentication Flood	<input checked="" type="checkbox"/> 5	20
Association Flood	<input checked="" type="checkbox"/>	20
Dis-Association Flood	<input checked="" type="checkbox"/> 5	20
Invalid Authentication Request	<input checked="" type="checkbox"/> 5	20
EAPOL Start	<input checked="" type="checkbox"/> 5	20
EAPOL Logoff	<input checked="" type="checkbox"/> 5	20

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 18: 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 μ sec 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 14: 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

The screenshot displays the Extricom Multi Series 1000 web interface. The top navigation bar includes tabs for Redundancy, Rogue, Syslog & monitor, SNMP, Centralized Configuration, IDS, Portal, and Others. The left sidebar lists various configuration sections: Overview, LAN Settings, WLAN Settings (with sub-items for ESSID Definition, Radios, Assignments, Access Points, System Tools, Advanced, Events & Reports, and Support & Feedback), and others. The main content area is the 'Portal' configuration page. It features a 'Enable Captive Portal' checkbox (checked), a 'VLAN' field set to 1, and a 'Secured Login' checkbox (unchecked). Below these are options for 'Force SSL (HTTPS)' and 'Multiple Clients Per User'. A 'Pre-Authentication Allowed Destinations' table is present, with columns for IP Address, Subnet Mask, Port Numbers, and Protocol. At the bottom, there is a 'Customized Default Page' section with a 'Use Customized Page' checkbox. A status bar at the very bottom shows a log entry: 'Sep 13 2009 19:51:08' with a severity of 1 and a description 'APS: 5 have been connected'.

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

Figure 19: 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)	<p>When this option is activated, any client that attempts to connect using http: will be redirected to SSL (https:) communication.</p> <p>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.</p>
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)	<p>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.</p> <p>A network destination (a rule) can be composed of any IP address/Sub Net mask, Port number and IP protocol type.</p>
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 15: Captive Portal Fields



Welcome to Extricom's Network Access Page

Username

Password

[Login](#)

Powered by Extricom

Please Provide your username and password to access the network



Wireless
that Works

Figure 20: 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.
- 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.

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 21: 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 22: Event Log Page

Reports Window - Details

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

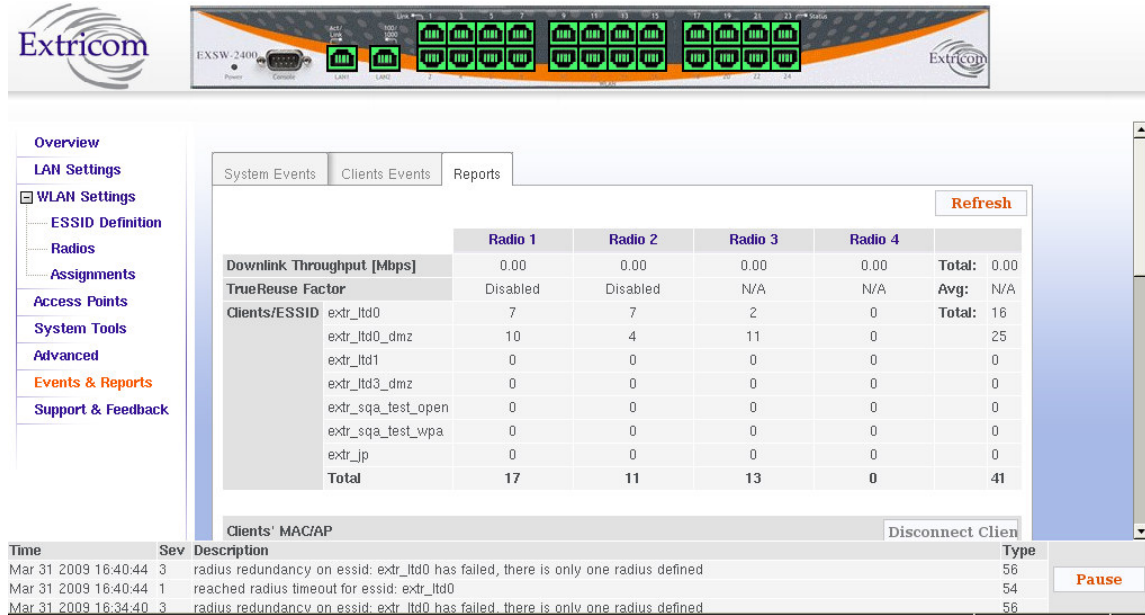


Figure 23: Reports Window – Top

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: <ul style="list-style-type: none"> 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 16: 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:

Extricom Multi Series 1000

Overview

LAN Settings

WLAN Settings

ESSID Definition

Radios

Assignments

Access Points

System Tools

Advanced

Events & Reports

Support & Feedback

Clients' MAC Address/Access Point

MAC Address: **Search** Display IP Address: **Show** Disconnect Selected Client/s: **Disconnect**

AP #	MAC Address	IP Address
AP #1	00:21:6A:1B:DF:56	
AP #2	00:0E:8E:19:CE:E9	00:16:6F:C2:D1:86
AP #3	00:80:46:4F:49:81	00:0E:8E:15:7B:C7
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
AP #8	00:13:E8:92:E2:51	00:11:F5:48:AF:D4
AP #9	00:0E:8E:20:01:70	00:0E:8E:20:01:75
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

Pause

Figure 24: 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.

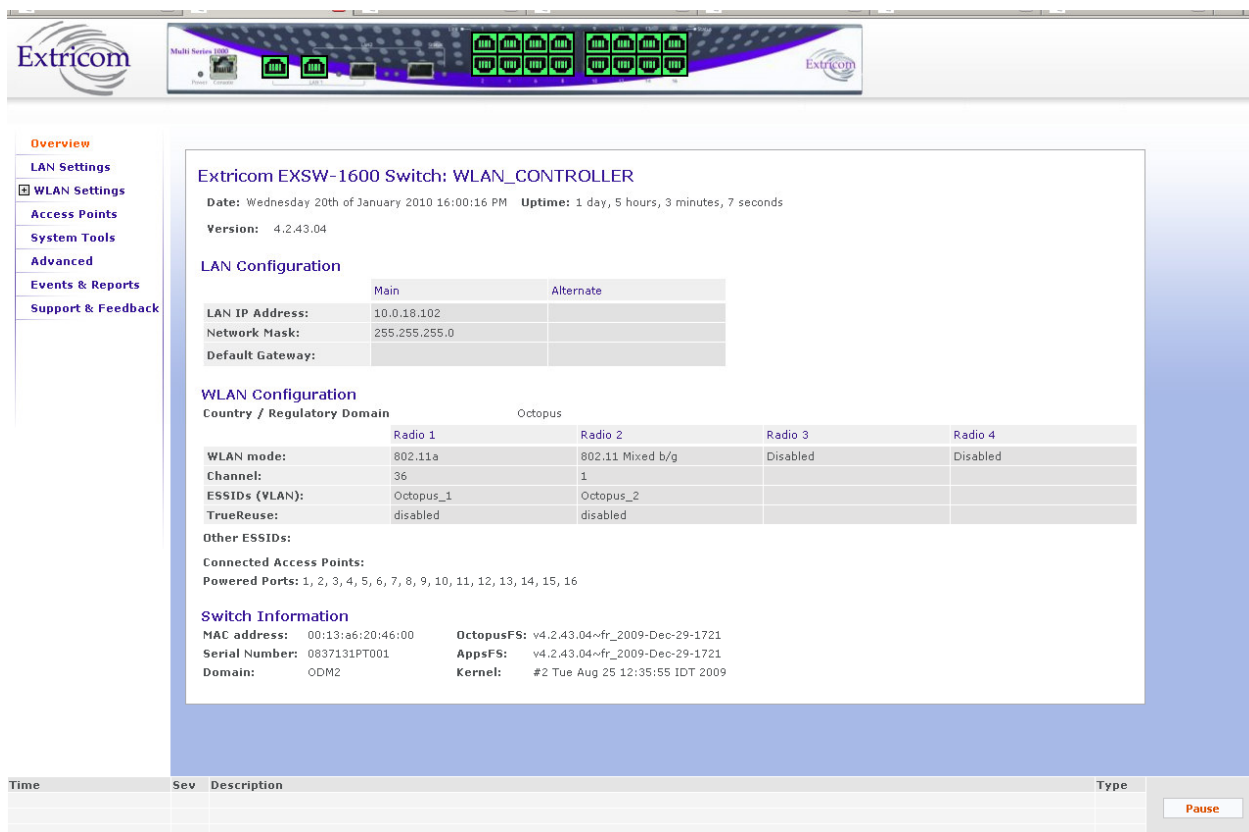


Figure 25: Configuration Overview

Refer to Table 17 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 17: Summary Page Features

Troubleshooting

Table 18 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.	<ul style="list-style-type: none"> • 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 <i>Access Points Web</i> configuration page (refer to <i>page 44</i>).
A wireless device can't associate with a specific ESSID	<ul style="list-style-type: none"> • Verify that the wireless device supports the same 802.11 standard as configured for the ESSID (802.11a/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	<ul style="list-style-type: none"> • Verify that the switch is connected to the LAN. • Verify that the correct IP address is used.
Low data rates	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 <code>https</code>.

Table 18: Troubleshooting

Internal Access Point Mounting Template

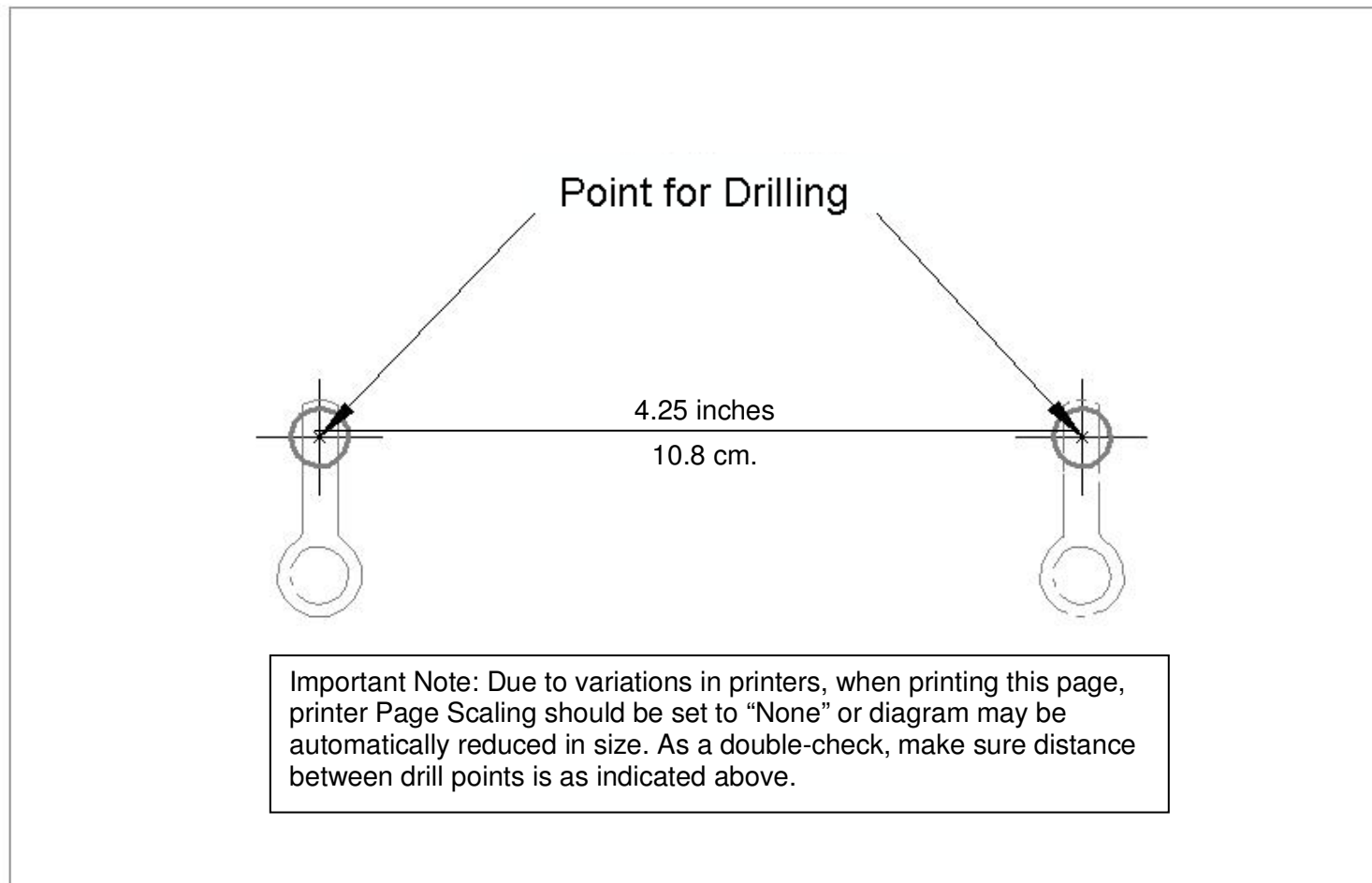


Figure 26: Access Point Mounting Template