



Interlink Networks Secure.XS and Cisco Wireless Deployment Guide

(An AVVID certification required document)

Overview

This document is intended to serve as a guideline to setup Interlink Networks Secure.XS Wireless LAN Security (RADIUS) Server and Cisco Access Points (AP) to authenticate wireless local area network (WLAN) clients that use Cisco's LEAP protocol. The scenarios covered in the document include LEAP/EAP authentication and MAC address authentication in separate VLANs configured on a dot1q AP. Accurately configuring the APs and the RADIUS server in each case is important. For non-dot1q configurations, the security related configuration remains the same while the "Radio to VLAN-mapping" configurations change.

For in depth configuration guidance, refer to the user guides for each product:

Cisco AP user guides can be found on: www.cisco.com .

Interlink Networks Secure.XS user guides can be found on: www.interlinknetworks.com .

Scope of the Document

This document accurately reflects configurations for the APs and Interlink's Secure.XS servers for the software versions below. Any future enhancements and changes to the user interfaces in the above products would require the document to be updated accordingly.

Hardware and Software Versions:

Item #	Item Description	Software Revisions
1	Interlink Secure.XS (Linux)	6.1
2	Interlink Secure.XS (Windows)	6.1
3	Cisco AP350	12.01T1
4	Cisco AP1100	12.2-8.JA
5	Cisco AP1200	12.01T1
6	Cisco Aironet Client Utility (Win XP)	5.05.001

Document Revisions:

Revision	Date	History
1	3/6/03	First release
2	3/21/03	Modifications include, formatting and adding AP configuration guidelines.
3	7/9/03	Added VLAN configuration instructions.

Co-authored by:

Cisco Systems, Inc.
and
Interlink Networks

Contents

Interlink Networks Secure.XS - Cisco LEAP Deployment Guide

- I. Interlink Secure.XS Installation on Linux**
- II. Secure.XS for Windows Installation**
- III. Configuring Secure.XS for LEAP authentication**
- IV. Configuring Secure.XS for MAC Address Authentication**
- V. Adding Support for VLANs**
- VI. Cisco AP1100 Configuration**
- VII. Cisco AP 350 and AP 1200 Configuration**
- VIII. Cisco Aironet Client Utility Configuration**

Interlink Secure.XS Server

1. Interlink Secure.XS Installation on Linux

1. Purchase a copy of Secure.XS (<http://www.interlinknetworks.com/products/on2-4.htm>). You will Select Linux as the desired OS.

2. Run the Installer. You will need root access in order to install Secure.XS.

Secure.XS.6.x.x.linux.bin (x's will be replaced by version downloaded.)

3. Install server components. Install the following components.

- 1- Server Binary Components
- 2- Server Configuration Files
- 3- Server Manager
- 4- Remote Control

ENTER A COMMA-SEPARATED LIST OF NUMBERS REPRESENTING THE COMPONENTS TO BE INSTALLED: 1,2,3,4

4. Accept the Defaults. Press enter (about nine times) to accept all the default settings. You can change them all later if you like. The installer will take several minutes to install of the selected components. Installation should complete without errors.

5. Set a path to the server library. (Later, you should add this to your startup scripts.)

```
# export LD_LIBRARY_PATH=/opt/aaa/lib
```

6. Start the server.

```
# /opt/aaa/bin/radiusd
```

6. Test your installation. 'radpwstst' is a testing tool that acts like a RADIUS client.

```
# /opt/aaa/bin/radpwstst -s localhost -w password test_user
```

The response should be:

```
'test_user' authentication OK
```

If you get this response you have a running server that is correctly configured for RADIUS authentication. If you do not get this response, something is wrong. If the server is not authenticating the test user, it won't do much good to continue beyond this point.

If your server is authenticating the test user, you should proceed. There is some additional configuration required to get LEAP working.

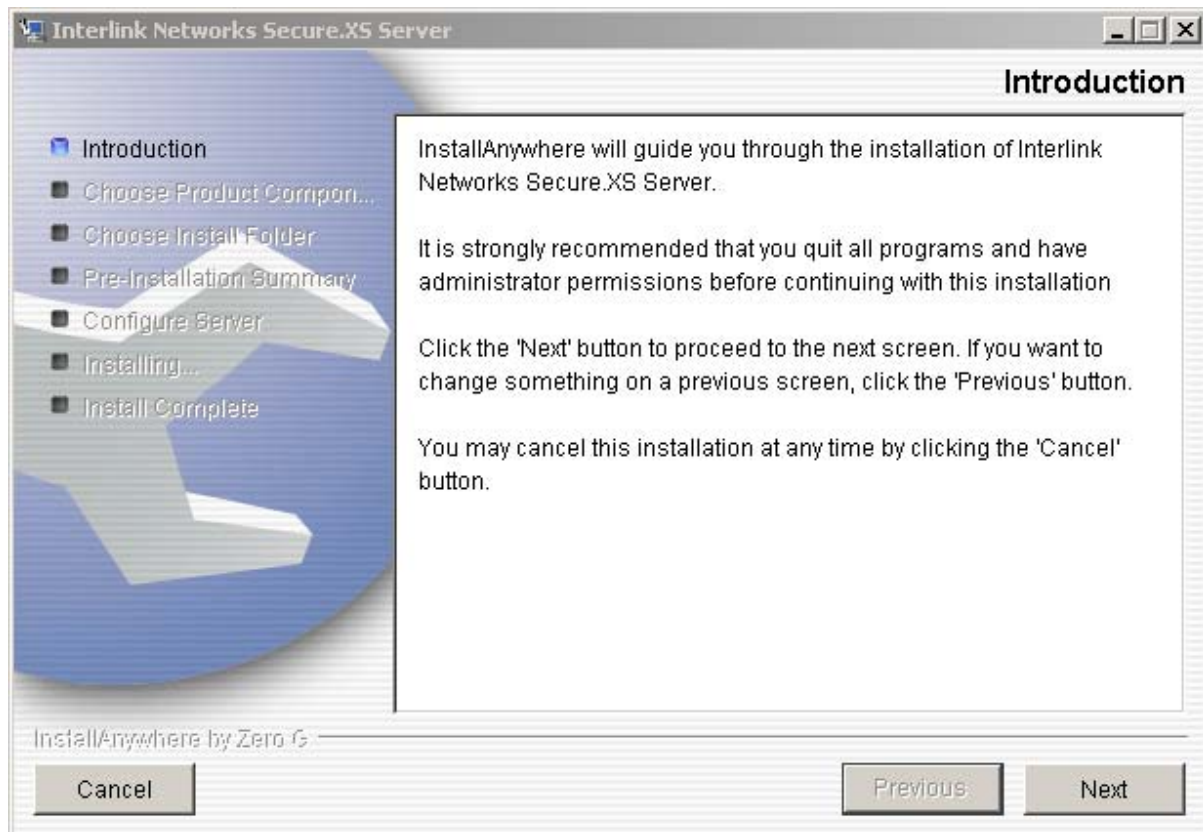
7. Start the Server Manager GUI. The Server Manager GUI runs from a tomcat web server. Start it with the following command:

```
# /opt/tomcat/bin/startup.sh
```

You should now be able to point your web browser to `http://<ip_address>:8080/aaa` to bring up the web GUI. Use the username and password that you setup earlier (adminaaa, adminaaa) to login to the GUI.

II. Secure.XS for Windows Installation

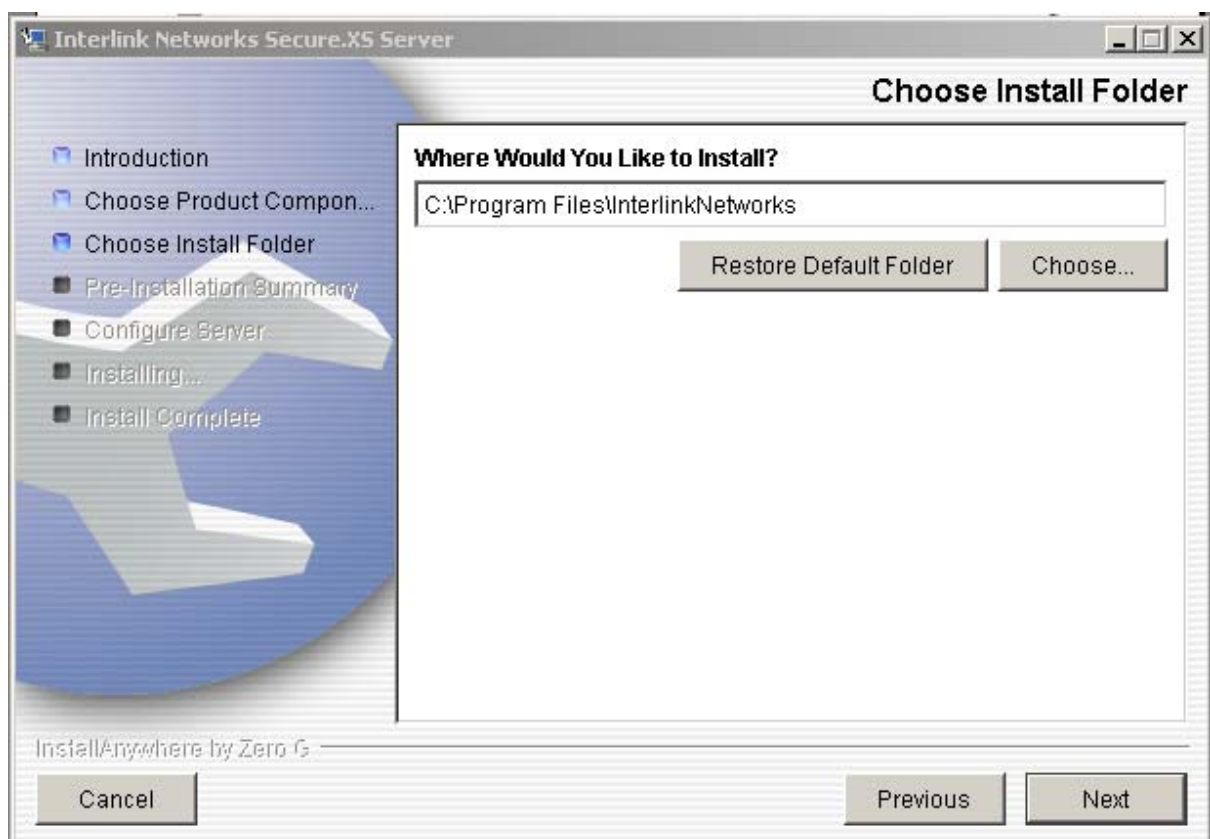
1. Get a copy of Secure.XS (<http://www.interlinknetworks.com/products/on2-4.htm>). Select Windows as the desired OS. Download the installer file to the computer where the server will be installed.
2. Locate the directory where the installer resides. Double-click on Secure.XS.6.1.x.windows.exe. The installer will begin the installation process.



3. Select Product Components - Install the Authentication Server, Server Configuration Files, Binary Components, and Server Manager. These are the default options.



4. Choose Install Folder - Install Secure.XS into the default folder.

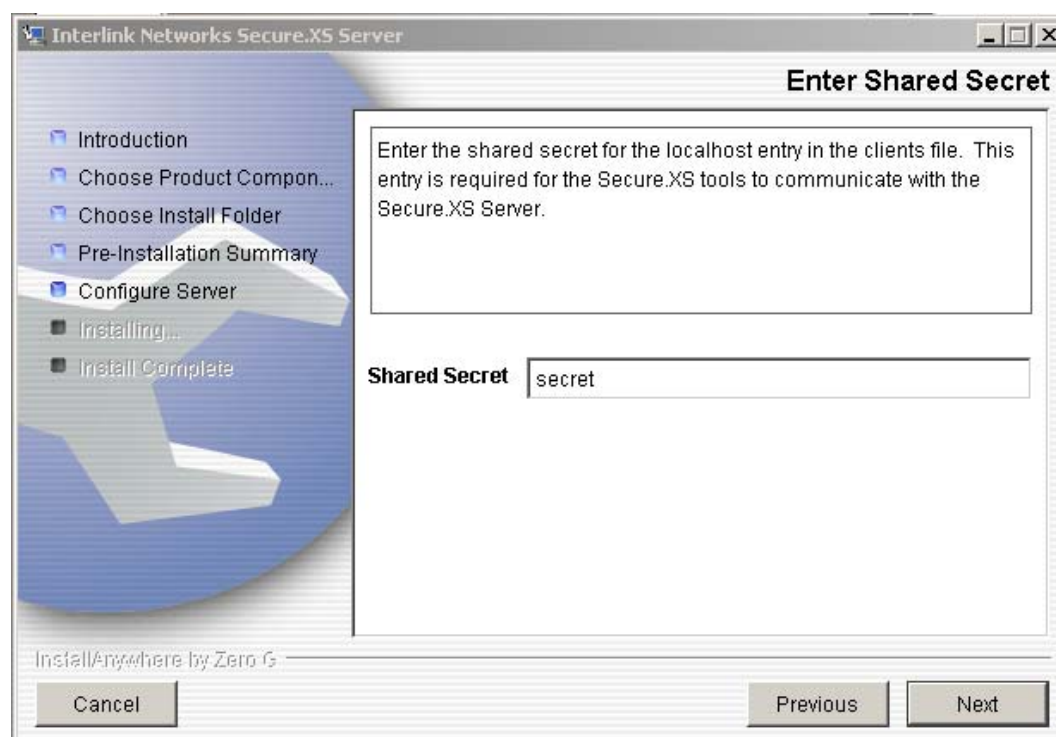


5. Pre-Installation Summary - The next screen shows a summary of components to be installed.

Choosing the defaults will result in the correct setup.



6. Additional Configuration Information - There are some additional items that need to be configured. Enter each one in turn and click "Next" in between each entry. To simplify the installation, select the default values.



7. Installation Complete - The installer will indicate that the installation is complete. Click "Done" to complete the installation process.



8. Test the Installation - Verify that the installation and configuration is complete and correct. This is done by running the Secure.XS Test Tool from the Start->Interlink Networks menu. Click on "Test Authentication" to start the server and send a test request. Enter the test username and password that you configured in the installation (test_user, password).

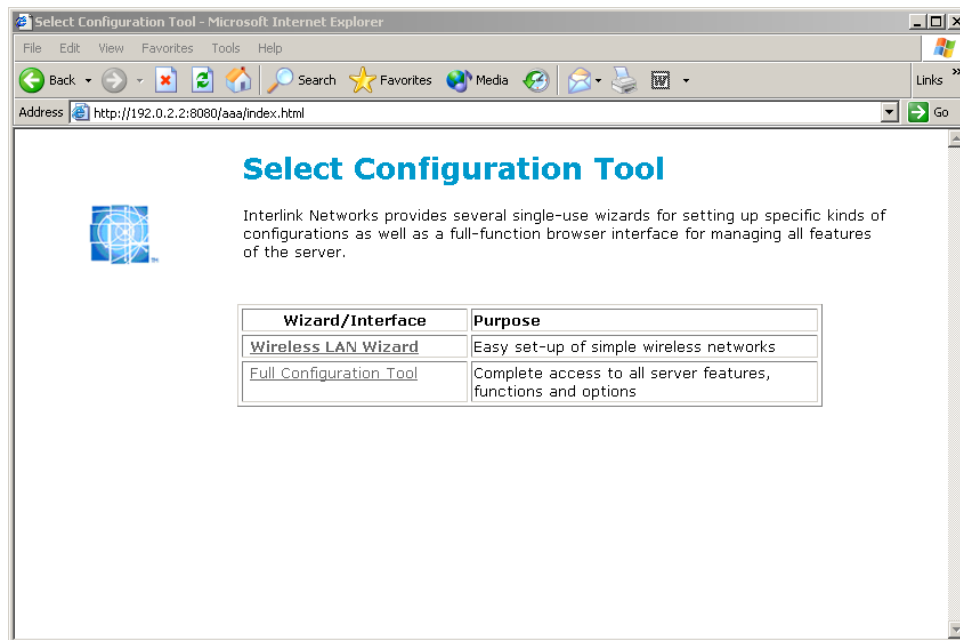


If the "Test Authentication" returns successfully, you have a server running correctly. Now, click on "Launch Server Manager" to begin configuring Secure.XS for LEAP authentication.

III. Configuring Secure.XS for LEAP Authentication

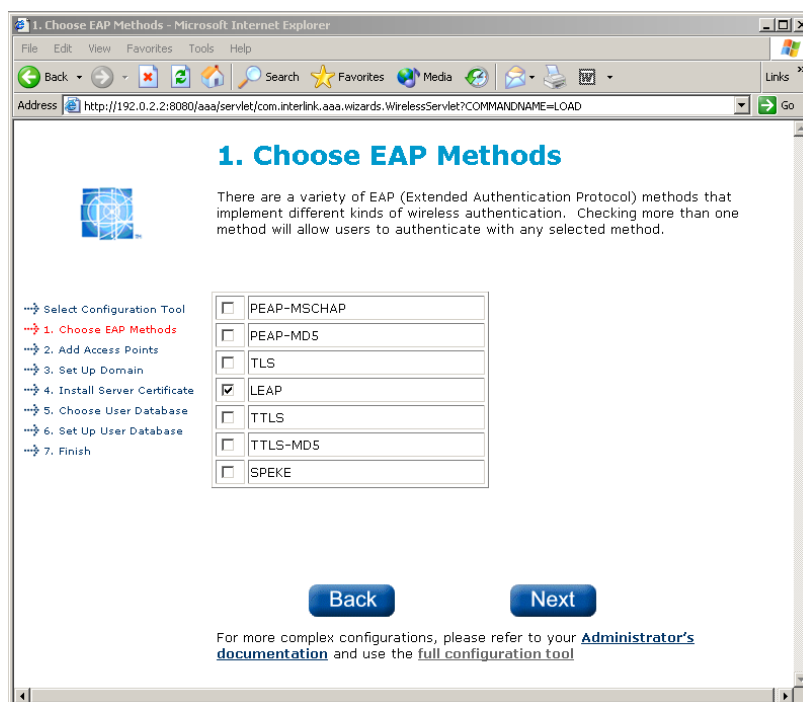
This section focuses on configuring Secure.XS using the Wireless LAN Wizard configuration tool. As the Server Manager is web-based, this will be identical for both Windows and Linux installations.

1. Point your web browser to the Secure.XS Server Manager. If you installed the server on <ip_address> then the URL is http://<ip_address>:8080/aaa. The following screen will appear:



Select "Wireless LAN Wizard" to use the Wizard to configure Secure.XS. The WLAN Wizard consists of six steps necessary to configure WLAN security.

1, Choose EAP Method. The following screen will allow you to select from a variety of EAP methods. Since we are focusing on LEAP authentication, select "LEAP" only from the list:



2. Add Access Points. Now you will need to add the access points that will be secured by

Secure.XS. By default, you can add four access points here. You can also click on "Click here to add more APs..." to add additional blanks for more APs. You will also need to specify a shared secret for each of the access points that you enter. This is the RADIUS shared secret that you entered during the server installation (default was "secret").

2. Add Access Points

RADIUS servers must know the network address and unique shared secret of each Access Point that requests security services. Each of the Access Points configured on this screen must be set up to use the 802.1x protocol.

Access Point IP or DNS Address	Shared Secret
192.0.2.1	secret
192.0.2.5	secret

[Click to add more APs...](#)

[Back](#) [Next](#)

For more complex configurations, please refer to your [Administrator's documentation](#) and use the [full configuration tool](#)

3. Set up Domain. This step allows you to configure a domain from which you would accept certificates. Since we are not configuring any certificate-based authentication methods, click on the "Next" button without any changes.

4. Install Server Certificate. This step allows you to install the server certificate that is required for certificate-based authentication methods. Since we are not configuring any certificate-based authentication methods, click on the "Next" button without any changes.

5. Choose User Database. This step allows you to select the user repository where your user profiles are stored. Select "User File". This will allow the configuration of users stored in a local database on Secure.XS. Click "Next".

5. Choose User Database

User names and passwords are stored in a user database or directory. You may keep your user names and passwords on this server (in a "user file") or point to a directory that serves many applications (such as LDAP or Active Directory).

User Database or Directory Type

☒ User File

☐ LDAP

[Back](#) [Next](#)

For more complex configurations, please refer to your [Administrator's documentation](#) and use the [full configuration tool](#)

6. Add Users. This step allows you add users to the internal Secure.XS database. Since the installation created test_user with password of "password", we can use that user for simple verification of LEAP functionality.

6. Add Users

Each user needs a unique user name and password.

User Name	Password	Confirm Password
test_user	*****	*****

[Click to add more users...](#)

[Back](#) [Next](#)

For more complex configurations, please refer to your [Administrator's documentation](#) and use the [full configuration tool](#)

7. Finish. This last screen displays a summary of the WLAN Wizard Configuration. Click "Done" to complete the Wizard and save the configuration.

7. Finish

You have now defined the following configuration for your Secure.XS Server. Clicking **DONE** will save your configuration and exit this wizard. You can make changes with the **BACK** button or by clicking on the navigation steps to the left. Closing your browser will discard all changes.

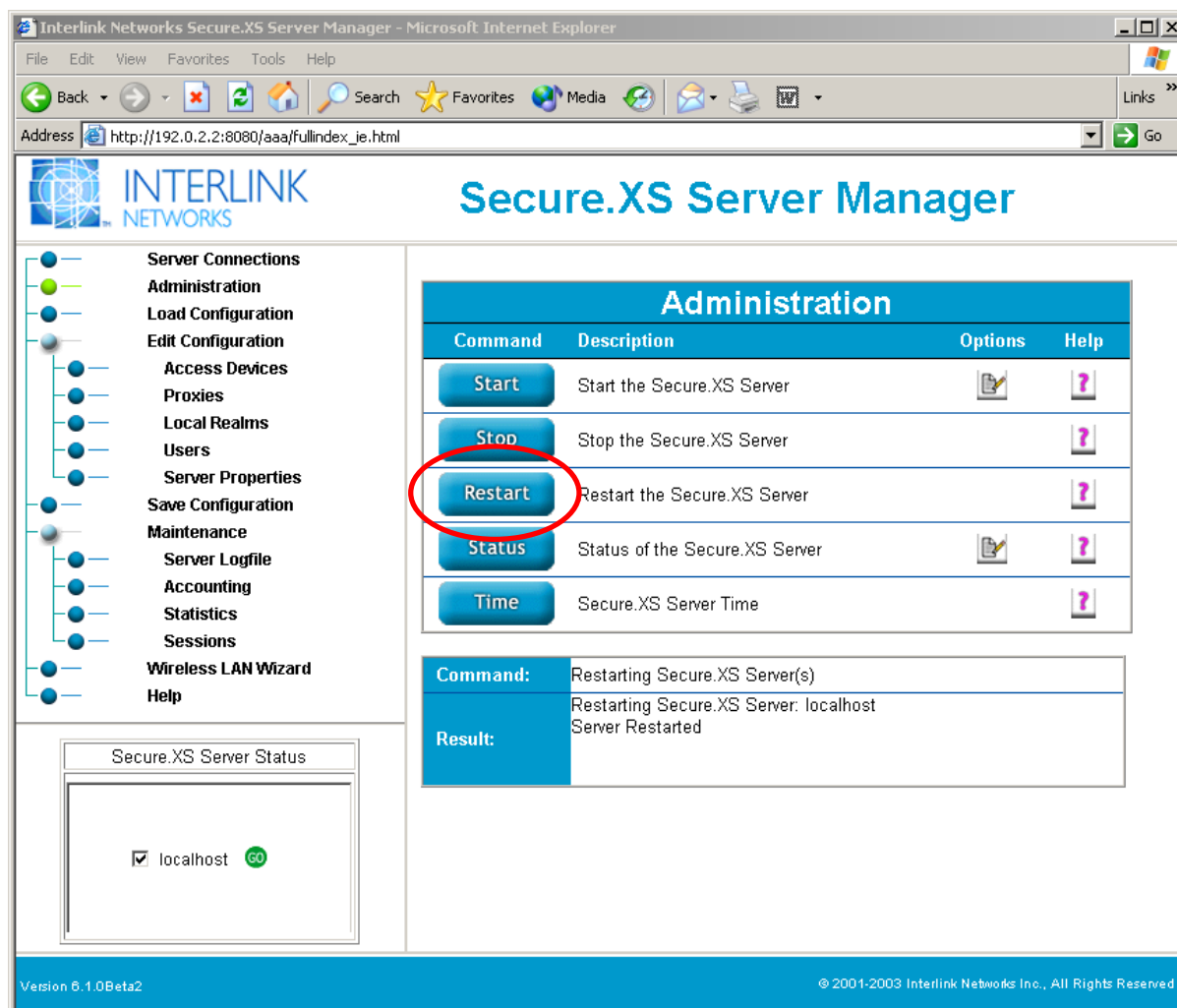
You have configured:

- EAP Method(s): LEAP
- 2 access device(s) configured
- 1 user(s) configured
- No server certificate installed

[Back](#) [Done](#)

8. Restart the Server. Once the Wireless LAN Wizard finishes saving the configuration, you will be redirected to the "Administration" screen in the Full Configuration tool.

Click on "Restart" to load the configuration changes that you just finished. Notice that you can click on "Wireless LAN Wizard" to rerun the wizard.

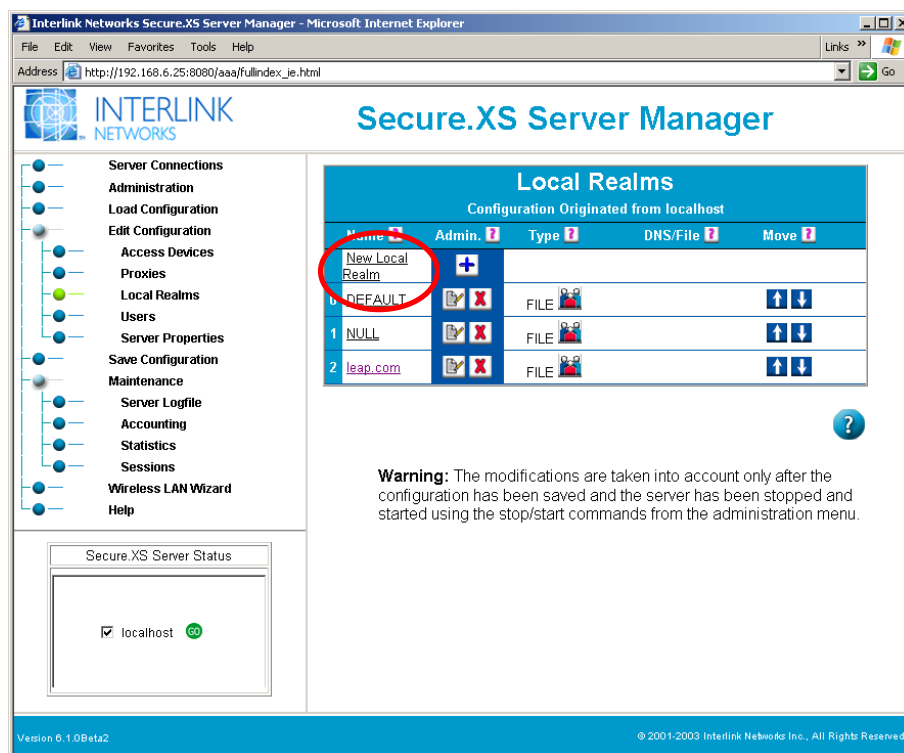


At this point, the server is running (notice the green "GO" symbol). Secure.XS is ready to authenticate LEAP users.

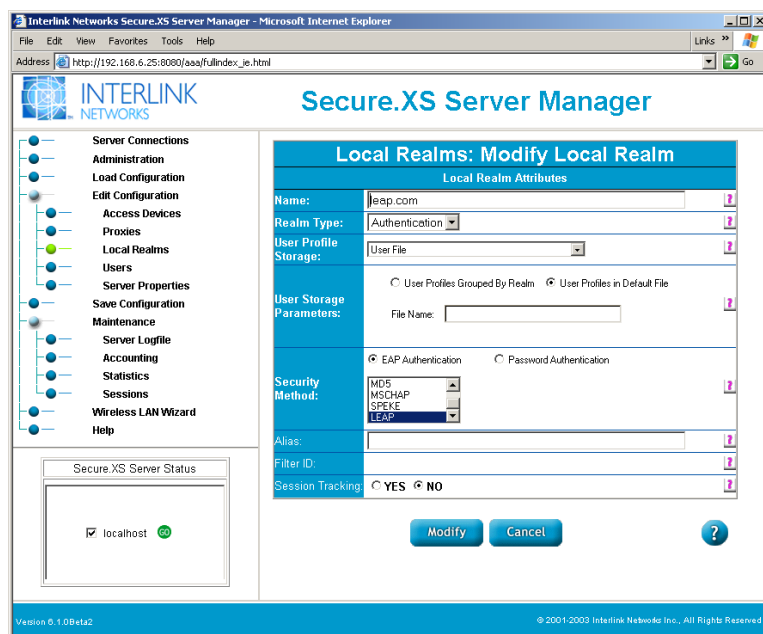
IV. Configure Secure.XS for MAC Authentication

Configuring Secure.XS to perform both MAC address and LEAP authentication requires using the Secure.XS Full Configuration tool. You will need to create a new "realm" for your LEAP users and enter the MAC addresses of those devices that will authenticate using their MAC Addresses.

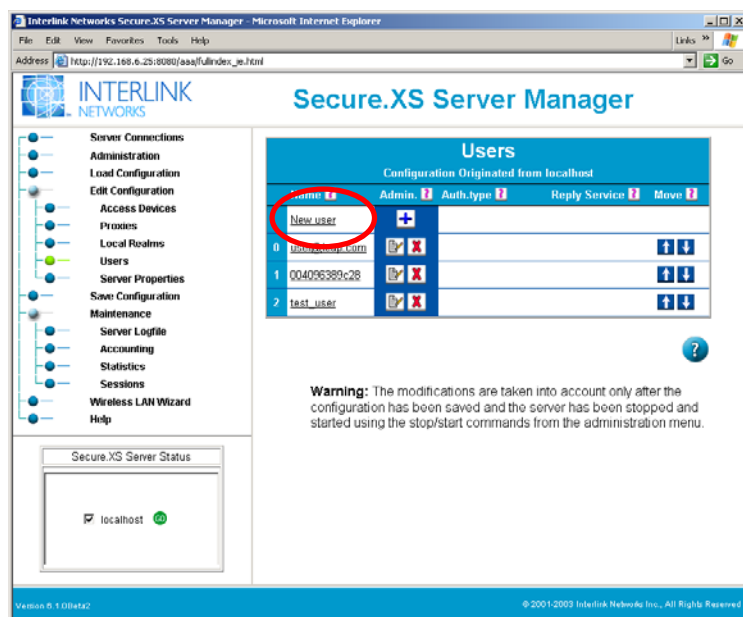
1. From the Full Configuration Tool main screen, click on "Local Realms". Click on "New Local Realm" to add the new realm as shown below.



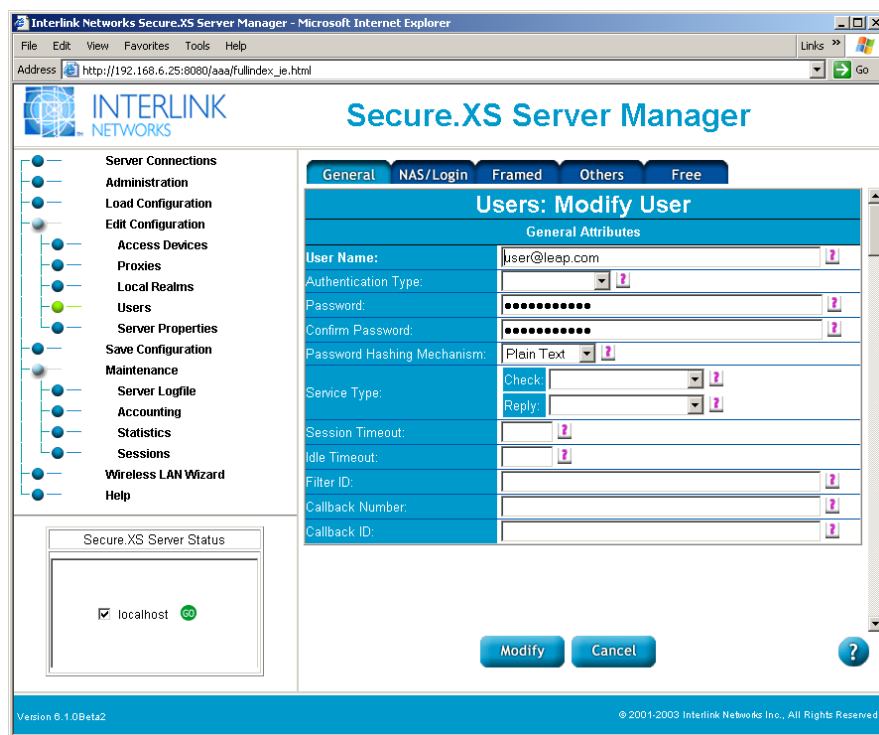
2. Add the realm "leap.com". The name of the realm is not important. But all LEAP users will use the realm as a postfix to identify them to Secure.XS. Configure the realm for LEAP authentication as shown below.



3. Add the user to be authenticated using LEAP. This is done by clicking on "Users" from the configuration menu and then clicking on "New User".



4. Add the LEAP user as shown below. Note that the user must have the user@realm form where "realm" is the LEAP realm that was configured above. Click "Modify" when you are done.



5. Modify the NULL realm to authenticate the MAC address devices. Click on "Local Realms" from the Secure.XS configuration screen. Edit the NULL realm to authenticate using passwords as shown below:

The screenshot shows the 'Secure.XS Server Manager' web interface in Microsoft Internet Explorer. The left sidebar contains a navigation menu with options like 'Server Connections', 'Administration', 'Load Configuration', 'Edit Configuration', 'Access Devices', 'Proxies', 'Local Realms', 'Users', 'Server Properties', 'Save Configuration', 'Maintenance', 'Server Logfile', 'Accounting', 'Statistics', 'Sessions', 'Wireless LAN Wizard', and 'Help'. The 'Local Realms' option is highlighted. The main content area is titled 'Local Realms: Modify Local Realm' and contains the following fields:

- Name:** NULL
- Realm Type:** Authentication
- User Profile Storage:** User File
- User Storage Parameters:**
 - ☐ User Profiles Grouped By Realm
 - ☒ User Profiles in Default File
 - File Name:** (empty field)
- Security Method:**
 - ☐ EAP Authentication
 - ☒ Password Authentication
 - PEAP-MSCHAP
 - PEAP-MD5
 - MD5
 - MSCHAP
- Alias:** (empty field)
- Filter ID:** (empty field)
- Session Tracking:** ☐ YES ☒ NO

At the bottom of the form are 'Modify' and 'Cancel' buttons, and a help icon. The footer shows 'Version 6.1.0Beta2' and '© 2001-2003 Interlink Networks Inc., All Rights Reserved'.

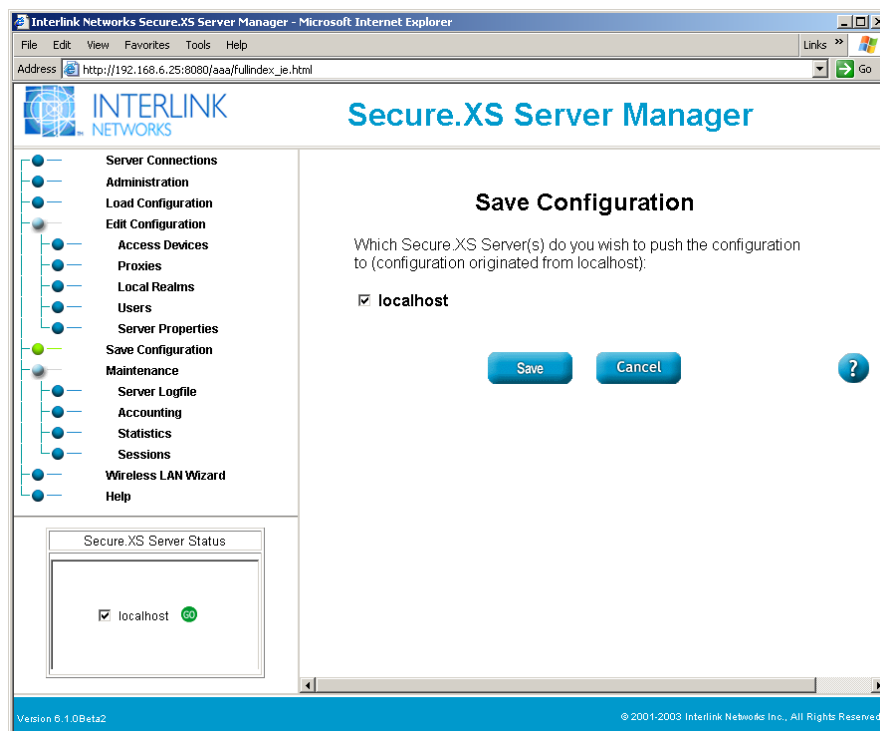
6. Add MAC Addresses. You can do this by adding a user with both username and password set to the device MAC address as shown below:

The screenshot shows the 'Secure.XS Server Manager' web interface in Microsoft Internet Explorer. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Users: Modify User' and has tabs for 'General', 'NAS/Login', 'Framed', 'Others', and 'Free'. The 'General' tab is selected, showing the following fields:

- User Name:** D04096389c28
- Authentication Type:** (dropdown menu)
- Password:** (masked with dots)
- Confirm Password:** (masked with dots)
- Password Hashing Mechanism:** Plain Text
- Service Type:**
 - Check:** (dropdown menu)
 - Reply:** (dropdown menu)
- Session Timeout:** (empty field)
- Idle Timeout:** (empty field)
- Filter ID:** (empty field)
- Callback Number:** (empty field)
- Callback ID:** (empty field)

At the bottom of the form are 'Modify' and 'Cancel' buttons, and a help icon. The footer shows 'Version 6.1.0Beta2' and '© 2001-2003 Interlink Networks Inc., All Rights Reserved'.

7. Save the configuration and restart Secure.XS. At this point you should save your configuration changes by selecting "Save Configuration" from the menu. Once the configuration is saved, restart the server and everything should be ready.



V. Adding Support for VLANs

Cisco Aironet Access Points support 802.1Q for VLANs. One flexible method for assigning VLANs involves assigning a VLAN ID using RADIUS attributes.

Secure.XS can assign VLANs on a per-user basis. In order to enable this, some attributes must be added to the Secure.XS dictionary file.

On Linux systems, this is

```
/etc/opt/aaa/dictionary.
```

On Windows, the file is

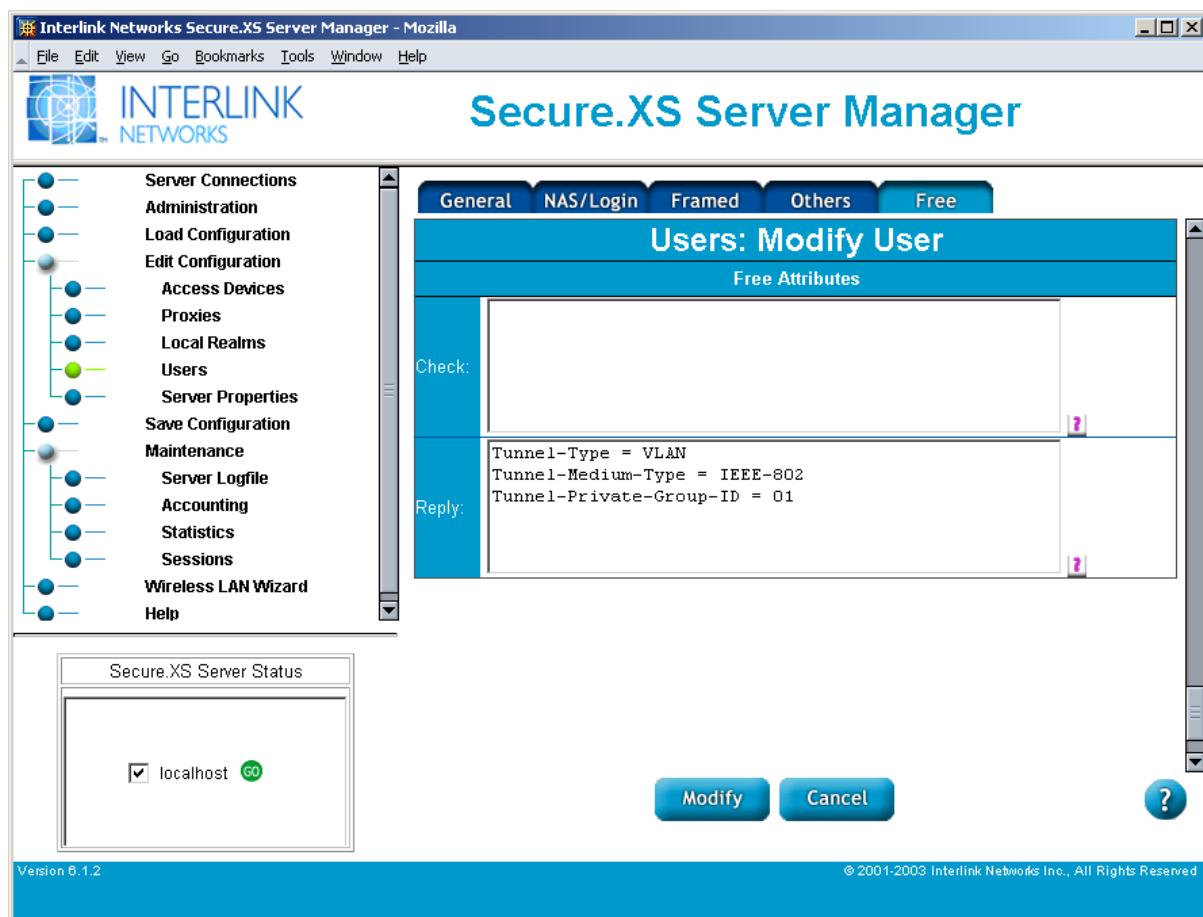
```
C:\Program Files\InterlinkNetworks\AAAServer\raddb\dictionary.
```

Add the following dictionary entries:

```
Tunnel-Type=VLAN 13  
Tunnel-Medium-Type=802
```

(On Secure.XS 6.1.2 and newer, these attributes are already defined).

In order to enable VLAN tagging for a user, add the attributes into the users profile using the Secure.XS Server Manager. The following screenshot shows an example.



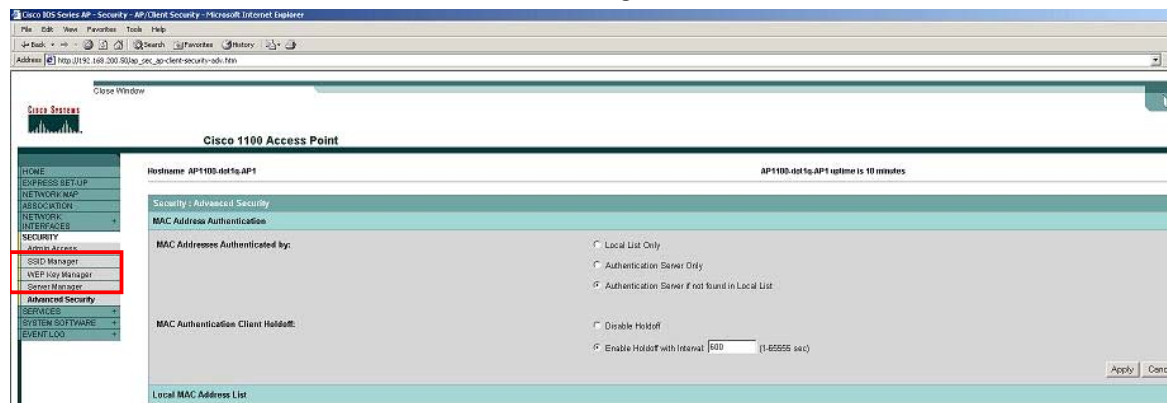
Cisco Access Point Configuration

Cisco AP1100

NOTE: The content provided in this document is not intended to be a step-by-step configuration guide. Please refer to appropriate AP's configuration guide for detailed steps. After configuring APs, use the screen-shots below to verify accuracy of configuration.

1. Log into the Access Point by pointing your browser it IP address. Go to the 'Security' menu on the left side of the page. There are four configuration screens to complete. They are "SSID Manager", "WEP Key Manager", "Server Manager" and "Advanced" (can be found in the area shown).

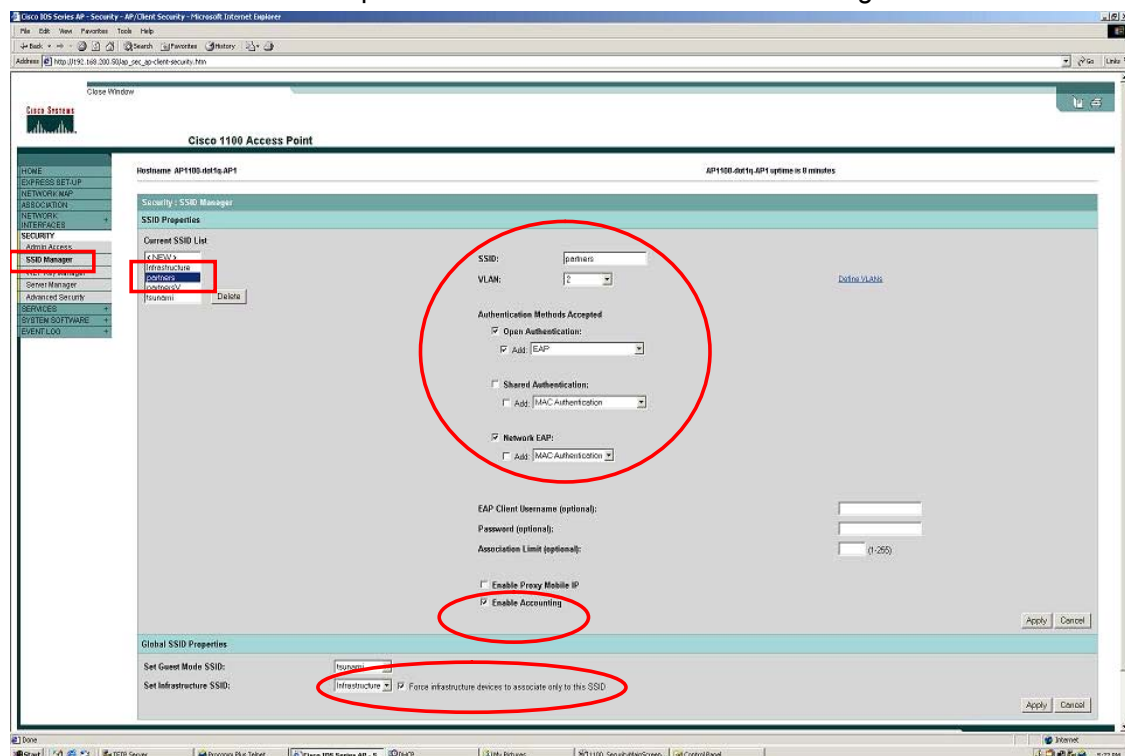
AP1100: Configuration



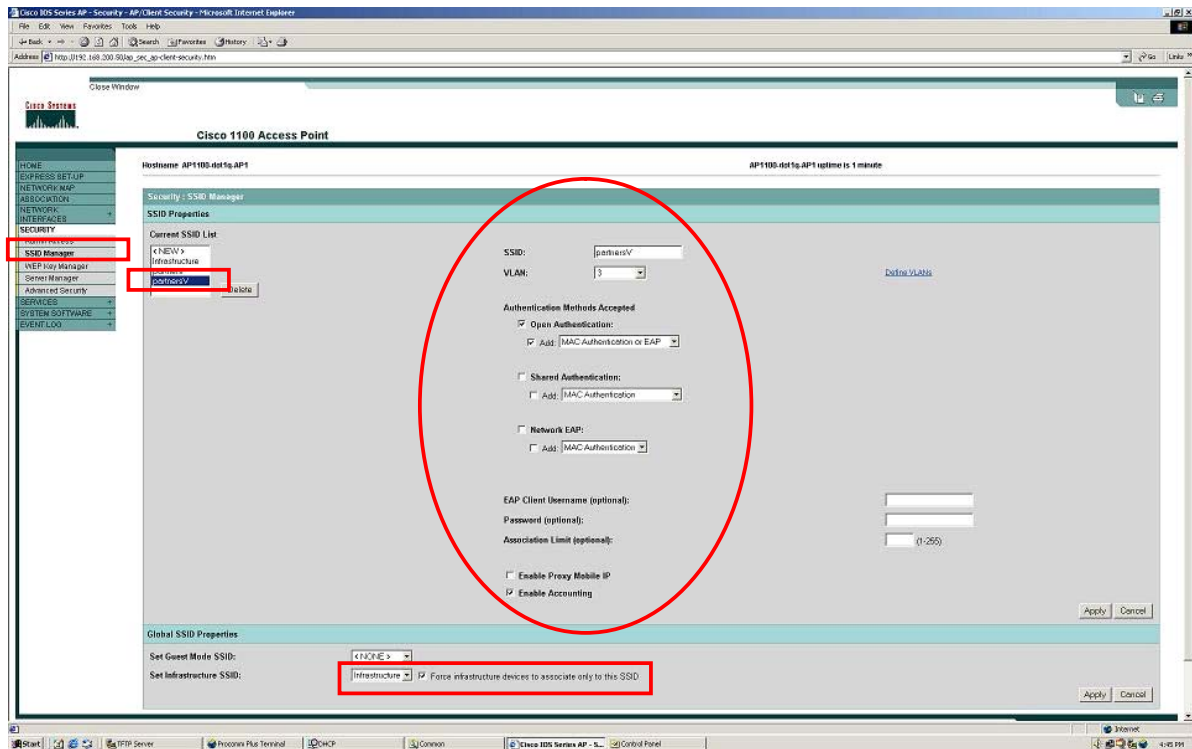
2. Configure SSID Managers

The SSID Manager configures the authentication methods allowed for each SSID. Multiple SSIDs can be added and each can be related to a different VLAN.

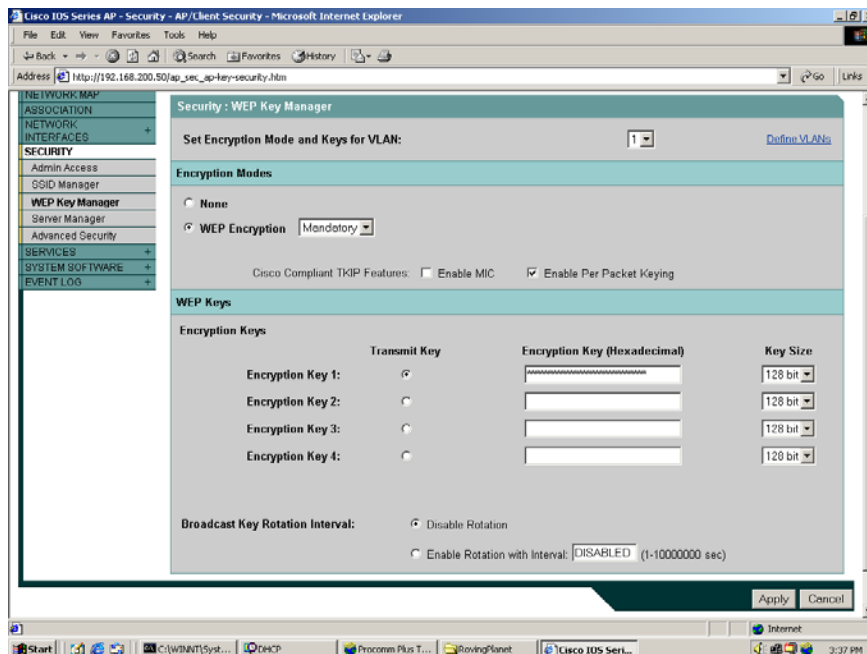
AP1100: "partners" SSID EAP/Network EAP Configuration



AP1100: "partnersV" SSID AAA-based MAC Authentication Configuration

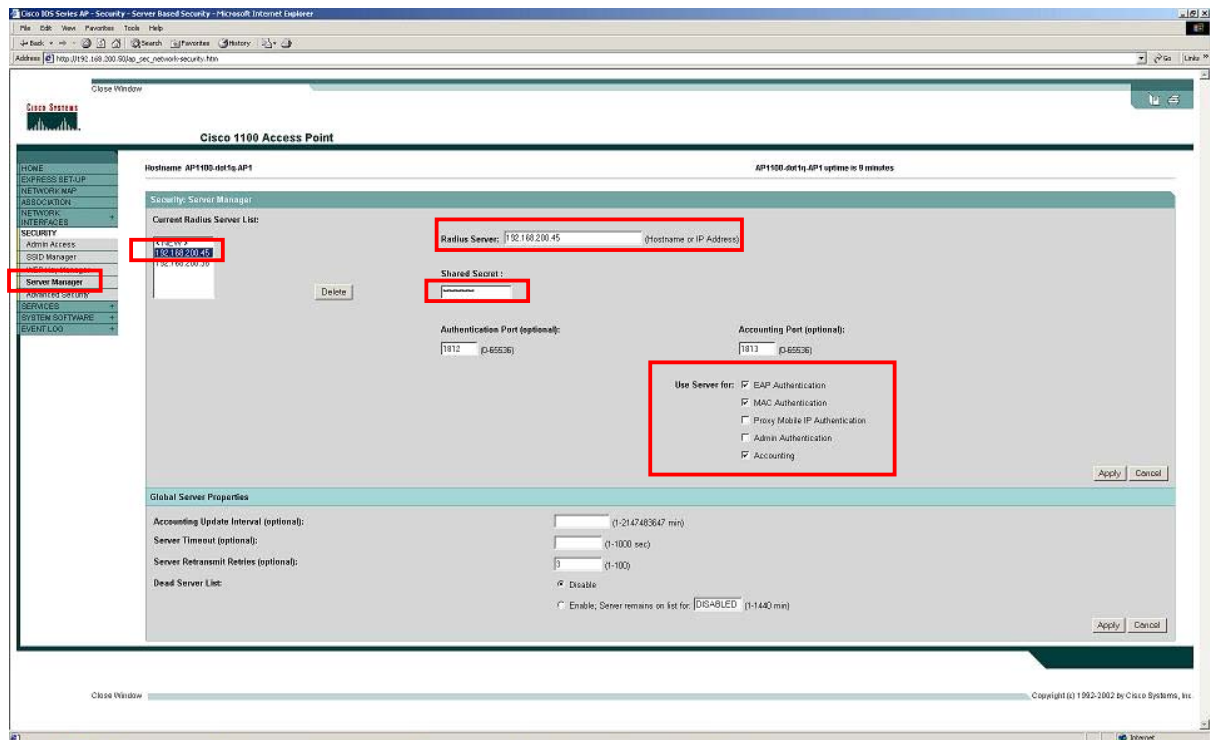


Configure WEP Key Manager - The WEP Key Manager configures the encryption modes for the WLAN. Configure "Mandatory" WEP Encryption as shown below:



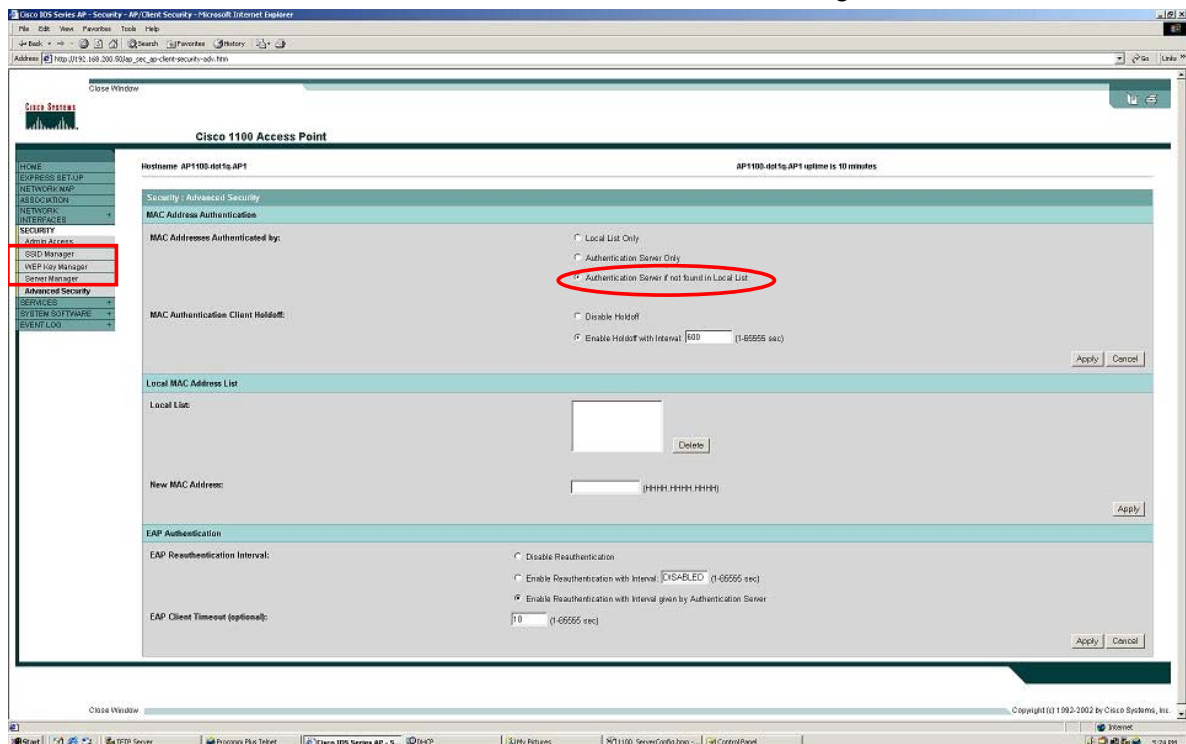
4. Server Manager - The Server Manager configures that Authentication Server that will be used. This should point to the Secure.XS installation. The RADIUS shared secret that was configured during the Secure.XS setup will also be entered here. The default Authentication and Accounting Ports are 1812 and 1813, respectively. Select "EAP Authentication" and "MAC Authentication" to accept both types of authentication.

AP1100: AAA Server Setup



5. Advanced Security – On the “Advanced Security” page, set the MAC address authentication setting

AP1100: MAC Address Authentication Configuration



to as shown.

6. Final configuration check on AP1100

AP1100: Dot1q Configuration Final Check

The screenshot shows the Cisco IOS Security AP configuration page for AP1100-dot1q AP1. The page is titled 'Cisco 1100 Access Point' and 'AP1100-dot1q AP1 uptime is 7 minutes'. The 'Security Summary' section shows the 'Admin Address' and 'SSID' configuration. The 'Server-Based Security' section shows the 'Server Name/IP Address' and 'EAP' configuration. The 'VLAN' column in the SSIDs table is highlighted with a red circle. The 'EAP' and 'MDC' columns in the Server-Based Security table are highlighted with a red circle. The 'Network EAP' and 'Accounting' checkboxes are highlighted with red circles.

Security Summary		Read Only		Read Write	
Username					
SSID					
SSID		VLAN	Open	Shared	Network EAP
Infrastructure		1	✓		
partners		2	✓		
partnersV		3	✓		
tsunami		none	✓		
Server-Based Security					
Server Name/IP Address	EAP	MDC	Proxy Mobile IP	Admin	Accounting
192.168.200.45	✓	✓			
192.168.200.38	✓	✓			

Cisco AP350 and AP1200

The user interfaces of the Cisco AP350 and AP1200 are nearly identical. Screenshots are presented from the AP350.

1. Select Security from the Setup Menu

AP1200/350: Main Setup

AP1200-dot1q-AP1 **Setup**

Cisco 1200 Series AP 12.01T

Home Map Network Associations **Setup** Logs Help

Uptime: 00:02:18

Express Setup

Associations			
Display Defaults	Address Filters	Protocol Filters	Port Assignments
		VLAN	Advanced
			Service Sets

Event Log

Display Defaults	Event Handling	Notifications
------------------	----------------	---------------

Services

Console/Telnet	Boot Server	Routing	Name Server
Time Server	FTP	Web Server	SNMP
Cisco Services	Security	Accounting	Proxy Mobile IP

Network Ports

Network Ports		Diagnostics	
Ethernet	Identification	Hardware	Filters
AP Radio: Internal	Identification	Hardware	Filters

[Home][Map][Login][Network][Associations][Setup][Logs][Help]

Cisco 1200 Series AP 12.01T © Copyright 2002 Cisco Systems, Inc. credits

2. Multiple SSID configuration – For e.g. SSID partners – shows a typical EAP setup, while partnersV – shows a MAC authentication setup, while tsunami (primary) is mapped to NATIVE VLAN. Verify your configuration with the ones shown below.

AP1200/350: Dot1q setup

AP1200-dot1q-AP1 **AP Radio: Internal Service Sets**

Cisco 1200 Series AP 12.01T

Home Map Network Associations **Setup** Logs Help

Uptime: 00:02:22

Service Set Summary Status

Device: AP Radio: Internal

SSID for use by Infrastructure Stations (such as Repeaters): 3

Disallow Infrastructure Stations on any other SSID: ☒ yes ☐ no

Service Set ID(SSID): Add New

Existing SSIDs:

[0]	tsunami(primary)
[1]	partners
[2]	partnersV
[3]	native

Edit Remove

Apply OK Cancel RestoreAll

AP1200/350: "partners" SSID configuration

AP1200-dot1q-AP1 AP Radio: Internal SSID #1

Cisco 1200 Series AP 12.01T

Uptime: 00:03:06

Device: AP Radio: Internal

Service Set ID (SSID): partners

Current Number of Associations: 0

Maximum Number of Associations: 0

Proxy Mobile IP is enabled: ☐ yes ☒ no

Default VLAN ID: 100 (GATA)

Default Policy Group ID: 100 (None)

Accept Authentication Type: ☒ Open ☐ Shared ☐ Network-EAP

Require EAP: ☒

Default Unicast Address Filter: Allowed

To require static or server-based MAC-Address authentication, set "Default Unicast Address Filter" to "Disabled"

Apply OK Cancel Restore Defaults

Map Login Help

Cisco 1200 Series AP 12.01T © Copyright 2002 Cisco Systems, Inc. credits

AP1200/350: "partnersV" SSID configuration for MAC Authentication

AP1200-dot1q-AP1 AP Radio: Internal SSID #2

Cisco 1200 Series AP 12.01T

Uptime: 00:04:19

Device: AP Radio: Internal

Service Set ID (SSID): partnersV

Current Number of Associations: 0

Maximum Number of Associations: 0

Proxy Mobile IP is enabled: ☐ yes ☒ no

Default VLAN ID: 100 (VOICE)

Default Policy Group ID: 100 (Voice Over IP)

Accept Authentication Type: ☒ Open ☐ Shared ☐ Network-EAP

Require EAP: ☒

Default Unicast Address Filter: Disabled

To require static or server-based MAC-Address authentication, set "Default Unicast Address Filter" to "Disabled"

Apply OK Cancel Restore Defaults

Map Login Help

Cisco 1200 Series AP 12.01T © Copyright 2002 Cisco Systems, Inc. credits

2. From the Security setup screen, select "Authentication Server". Configure the IP Address and shared secret for the Authentication Server to be used. In addition, select "User server for: EAP Authentication and MAC Authentication" as shown below. When complete, click "OK".

AP1200/350: AAA server configuration

AP1200-dot1q-API Authenticator Configuration - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://192.168.200.40/SetAuthenticatorConfig.cfm?referenceid=http://192.168.200.40/Setup.cfm

AP1200-dot1q-API Authenticator Configuration

Cisco 1200 Series AP 1201T

Stop Help

Uptime: 00:06:49

SO2 TX Protocol Version (for EAP Authentication): 802.1x-2001

Primary Server Retry Period (Min.): 0

Server Name/IP	Server Type	Port	Shared Secret	Retran Int (sec)	Max Retran
192.168.200.35	RADIUS	1812		5	3
	RADIUS	1812		5	3
	RADIUS	1812		5	3
	RADIUS	1812		5	3

Use server for: ☒ EAP Authentication ☒ MAC Address Authentication ☐ User Authentication ☐ MIP Authentication

Use server for: ☒ EAP Authentication ☐ MAC Address Authentication ☐ User Authentication ☐ MIP Authentication

Use server for: ☒ EAP Authentication ☐ MAC Address Authentication ☐ User Authentication ☐ MIP Authentication

Use server for: ☒ EAP Authentication ☐ MAC Address Authentication ☐ User Authentication ☐ MIP Authentication

Note: For each authentication function, the most recently used server is shown in green text.

Apply OK Cancel Restore Defaults

3. Accounting server setup screen, define the RADIUS server ip, port #, shared secret and enable the service. Select both EAP and non-EAP for MAC authentication stations to take advantage of accounting.

AP1200/350: AAA server for Accounting

AP1200-dot1q-API Accounting Setup - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://192.168.200.40/SetAccounting.cfm

AP1200-dot1q-API Accounting Setup

Cisco 1200 Series AP 1201T

Stop Help

Uptime: 00:07:55

Enable accounting: ☒ Enabled ☐ Disabled

Enable delay to report STOP: ☒ Enabled ☐ Disabled

Minimum delay time to report STOP (sec): 2

Server Name/IP	Server Type	Port	Shared Secret	Retran Int (sec)	Max Retran	Enable Update	Update Delay (sec)
192.168.200.35	RADIUS	1813		5	3	<input checked="" type="checkbox"/>	600
	RADIUS	1813		5	3	<input type="checkbox"/>	600
	RADIUS	1813		5	3	<input type="checkbox"/>	600
	RADIUS	1813		5	3	<input type="checkbox"/>	600

Use accounting server for: ☒ EAP authentication ☒ non-EAP authentication

Use accounting server for: ☐ EAP authentication ☐ non-EAP authentication

Use accounting server for: ☐ EAP authentication ☐ non-EAP authentication

Use accounting server for: ☐ EAP authentication ☐ non-EAP authentication

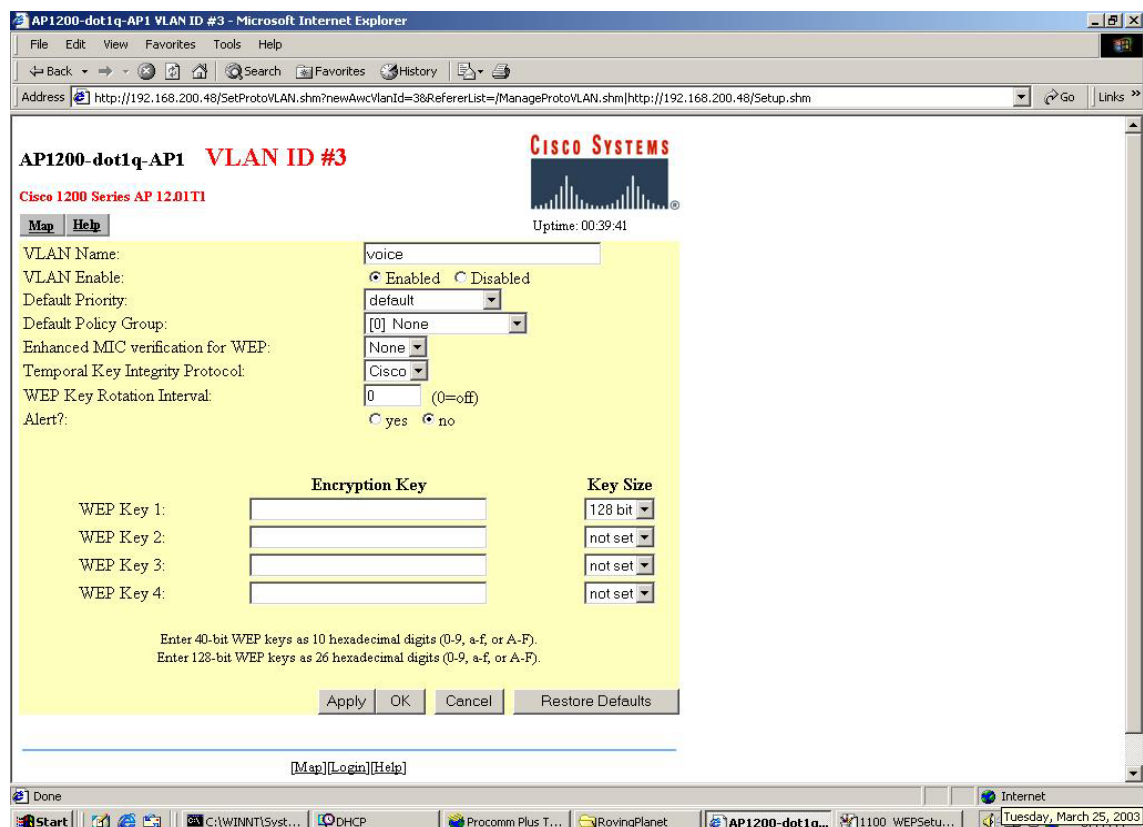
Use accounting server for: ☐ EAP authentication ☐ non-EAP authentication

Apply OK Cancel Restore Defaults

Map/Logout/Help

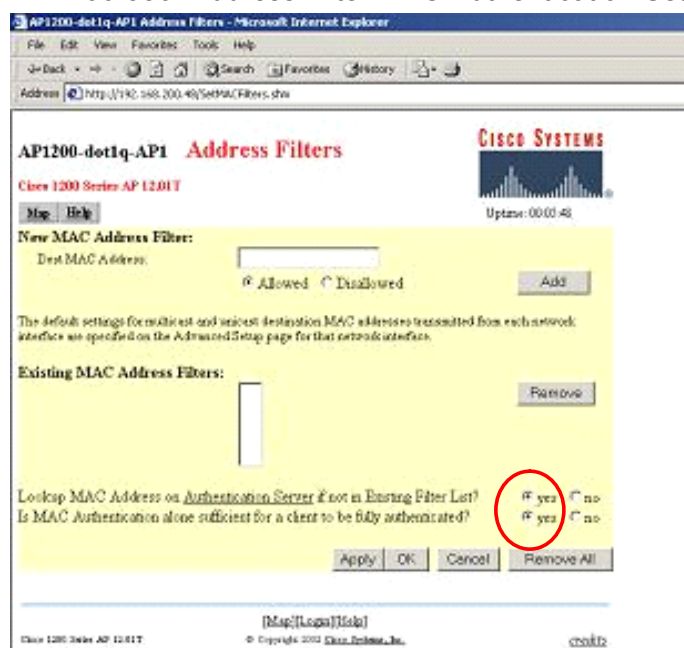
Cisco 1200 Series AP 1201T © Copyright 2002 Cisco Systems, Inc. credits

4. WEP setup - select "Radio Data Encryption (WEP)".



5. Enable MAC Authentication - Click on the "Address Filters" link from the "Setup" Menu. On the Address Filters page, enable "Lookup MAC Address on Authentication Server if not in Existing List?" and "Is MAC Authentication alone sufficient for a client to be fully authenticated?" as shown below.

AP1200/350: Address Filter/MAC Authentication Setup



Cisco-Aironet Client Utility Configuration

You can configure the ACU by creating two separate profiles, one for MAC authentication and one for LEAP authentication. For LEAP profile, follow the user guide to set the client for "LEAP". For the MAC authentication, follow the user guide to set the client for static WEP, 128 bit (that matches that set in the AP).

Once you have configured these profiles, you should be able to authenticate using either one. Each profile will cause the AP350 to generate a RADIUS request to authenticate the user.



Interlink Networks is a leading developer of access control and security software for wired and wireless networks. The company's standards-based solutions enable secure wireless LAN networks through strong 802.1x authentication. Interlink Networks provides software solutions for OEMs that scale from SOHO to enterprise to carrier-class platforms.

For more information, please call (734) 821-1200 or visit www.interlinknetworks.com.