1. CISCO

1.1 Product Description

Because Cisco Systems is a major supplier of enterprise level wireless products, which meet the benchmark requirements for the high sensitivity environment, this section will address this vendors' wireless solution in greater detail than the other product sections. This is not an endorsement but is provided as an example of the integrated solution required for implementation of a secured WLAN in an enterprise. Other vendors such as 3COM have been invited to contribute similar solutions for this benchmark level and those inputs will be added in upcoming versions.

Cisco Systems advocates an integrated wired/wireless architecture called the Structured Wireless-Aware Network (SWAN). Cisco provides a variety of wireless products such as APs, point-to-point bridges, management and authentication appliances, and network interfaces for client devices. The SWAN solution uses the Cisco IOS, which is familiar to most network administrators and provides advanced features such as Quality of Service (QoS), Multicast, Voice, and VLAN capabilities. Refer to Cisco's website for the most recent information in this fast changing market sector (http://www.cisco.com).

1.1.1 Security

The integrated model will provide the following capabilities:

- Industry standard wireless layer 2 encryption of the user traffic as defined in the IEEE 802.11i standard

- Industry standard authentication for the wireless user groups as well as the wired user groups via IEEE 802.1x protocol and the Extensible Authentication Protocol allowing for integration with DOD PKI infrastructure.

- Industry standard FIPS certified layer 3 VPN IPSec services through the use of VPN 3000 concentrators or VPN Services Modules in the Catalyst 6500

- Intrusion protection via wireless and wired integrated tools

- Application protection from malicious viral or lack of system patch incidences through Network Admission Control for wireless and wired clients

- Traffic/user class separation for user groups

- Infrastructure protection through rogue AP prevention, detection, suppression, and AP Authentication.

1.1.2 End User Applications

An integrated solution will provide the end users with as consistent experience regardless as they use both the wired and the wireless infrastructure. Their applications will continue to work as they roam throughout the wireless architecture. Leveraging your

existing installed base, this solution provides for FIPS secure Voice, Video, and Data traffic from the wireless edge through the core of your network.

At the heart of the Cisco SWAN solution are the Cisco Aironet APs. The APs provide MAC layer intelligent functions such as NIST approved AES encryption, mutual authentication, QoS, Multicast and up to 16 separate VLANs per AP. By performing encryption and authentication at the edge, Cisco APs ensure that no unauthenticated and unencrypted traffic traverses the network beyond the AP. Different levels of security are placed at various points of control in the network and WLAN security policies are reinforced at the access and distribution layer levels.

WLAN encryption is a critical component to any WLAN deployment. Standards based Wireless Devices from Cisco and Cisco Compatible Partners (CCX) will be able to provide a scalable enterprise Layer 2 FIPS certifiable wireless encryption. This security method also allows port based, 802.1x authentication for both wired and wireless users, thus unifying security schemes while enhancing network security. This security scheme will also provide the customer with a forward migration path to 802.1x based Network Admission Control (NAC) mechanisms for day zero protection from viruses etc. Moreover, this security mechanism secures the infrastructure at layer 2 mitigating layer 2 attack susceptibility, while layer 3 VPN's can be added for an extra layer of risk mitigation and protection.

The Cisco SWAN Architecture can fully meet FIPS 140-2 security requirements employing either a layer 3 VPN solution where the APs are placed on networks that are "outside the enterprise firewall" or using the layer 2 AES encryption available from 802.11i compliant software. Cisco APs themselves will be FIPS 140-2 certified, this alternative architecture will place the APs "inside the enterprise firewall" would then be possible in highly sensitive environments. Cisco is currently pursuing such certification based on the 802.11i standard and FIPS 140-2 capable APs may be available at the time this benchmark is published.

1.1.3 Solution Components

The proposed solution will be an integration of Cisco's Structured Wireless Aware Network SWAN architecture with the current network infrastructure – components include:

- Cisco dual mode 802.11 a/b/g APs and sensors

- Cisco 802.11i Compliant client cards (CB21ag or PC21ag) or partners' Cisco Compatible eXtensions (CCX) client cards/devices

- Simplified and centralized management and configuration using Cisco's Wireless LAN Solutions Engine (WLSE)

- Integrated wired and wireless LAN services (Wireless Domain Services) using Cisco infrastructure and Cisco IOS software across multiple platforms, starting with the Catalyst 6500 based Wireless LAN Services Module (WLSM)

- Cisco Wireless Security Suite (standards based IEEE 802.11i/WPAv2 security protocols)

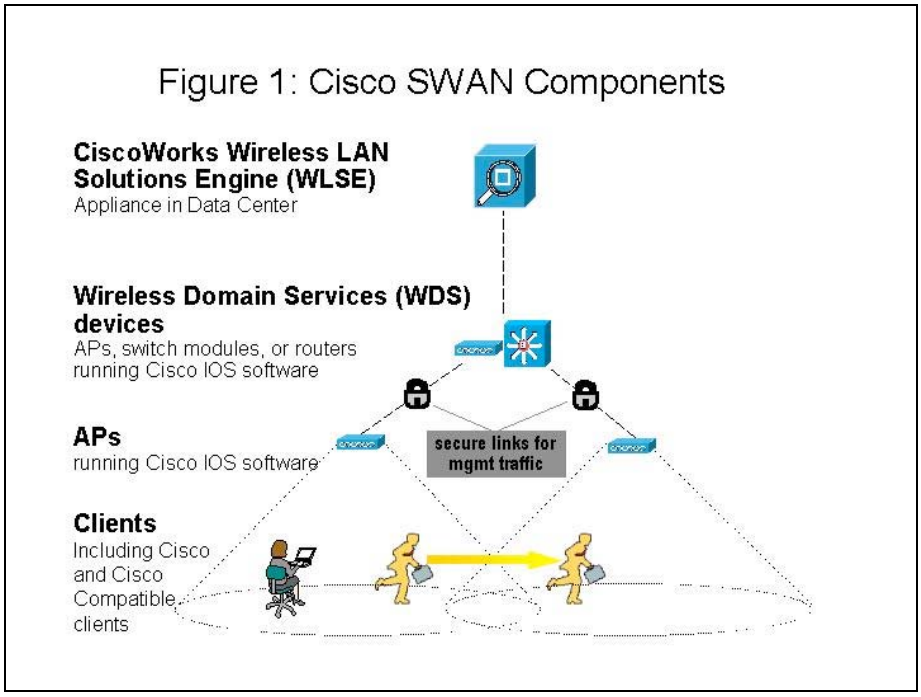

Figure 1-1. Cisco SWAN Components

1.1.3.1 Wireless LAN Solutions Engine

The WLSE is a systems level device with advanced RF and WLAN management features that ensures centralized deployment and configuration of APs (up to 2500 per WLSE), simplifying everyday operation of WLANs. WLSE also enhances security, and maximizes network availability, while reducing deployment and operating expense. WLSE is the management platform from which an administrator can:

Identify and contain potential rogue APs. WLSE generates alerts and displays information on the AP such as the location of potential rogue APs. Administrator can either classify the AP as friendly or disable the APs switch port if it is determined to be a rogue.

Detect potential WLAN intruders. Clients that are active but not associated with a trusted AP can be detected with alerts allowing the network administrator to take appropriate action. Furthermore, Cisco is enhancing WLAN IDS function such as detecting and reporting incorrectly configured clients. Operated in conjunction with the AirDefense IDS/IPS solution, a complete end-to-end Secure wireless solution can be achieved.

View RF interference sources. With knowledge of interference sources, an administrator can change AP settings to mitigate the effects of the interference.

Have an optimal AP deployment with minimal effort. The Assisted Site Survey feature uses a combination of AP scans and client walkabout procedure to measure real-time RF environmental data. The measured RF data is used to tune and optimize WLAN deployment parameters such as channel settings and power settings on the APs.

Ensure complete RF coverage. AP coverage areas are shown in graphical form (store floor, etc.). An administrator can quickly spot coverage gaps or channel overlap by using this information. AP settings, such as radio output power, can then be changed automatically to optimize the AP coverage patterns for self-healing features for robust RF coverage in the event of AP failure.

1.1.3.2 Wireless Domain Services

Positioned between WLSE and the APs are a set of network devices that act as logical AP controllers. These devices, which today can be an AP, Cisco ISR router, or WLAN Solutions Module (WLSM) run a set of Cisco IOS Software® services called Wireless Domain Services (WDS). These services include radio measurements (RM) aggregation, fast, secure roaming and a secure hierarchy of infrastructure based authentication:

RM Aggregation: An AP routes the RMs gathered by it and associated clients to the WDS device. The WDS device then aggregates the RMs, eliminating redundant information. The WDS device then sends the condensed RM information to WLSE for analysis.

Fast, Secure Roaming: Roaming is the process of a client moving from one AP to another. Latency-sensitive applications such as wireless VoIP, enterprise resource planning (ERP), and Citrix based solutions require that roaming occur as quickly and seamlessly as possible. Some applications such as VoIP can be disrupted if roaming takes longer than 150 milliseconds (ms).

As part of the roaming process, the client associates to the new AP and, if 802.1X is being used, performs an 802.1X re-authentication. Ordinarily, the new AP would act as the 802.1X authenticator, and the re-authentication process could take 1,000 ms or longer. To speed the re-authentication, the WDS device acts as the 802.1X authenticator and uses the Cisco Centralized Key Management (CCKM) protocol to provide complete re-authentication without communication to an authentication server. As a result, secure roaming occurs in less than 150 ms. after a client is disconnected from the network, a new 802.1X authentication to an authentication server is required for each new session assuring the security of the WLAN.

1.1.3.3 Wireless LAN Services Module

The Cisco Catalyst 6500 Series WLSM can be flexibly deployed anywhere in the network-from the wiring closet to the core, to the data center to the WAN edge, or as a

services switch. Figure 1-2, *WLSM Enterprise Campus Deployment*, illustrates the Cisco Catalyst 6500 Series WLSM can be deployment in an enterprise campus environment. An access point can connect to the Catalyst 6K on any subnet. Upstream switches or routers do not have to be configured, and no specific assignment or trunks are required. Once the AP is registered and has received its configuration through the CiscoWorks WLSE, fast secure roaming tunnels (FSRT) are established between the AP and the Catalyst 6K WLSM. WLAN users are thus provided fast secure roaming both within and across subnets. No special client software is required, which gives network administrators flexibility on network access policies. Clients can be authenticated and placed in mobility groups accessing network resources. WLAN client handoff between APs, including re-authentication and re-keying (if used) occurs in sub 150 ms timeframes.

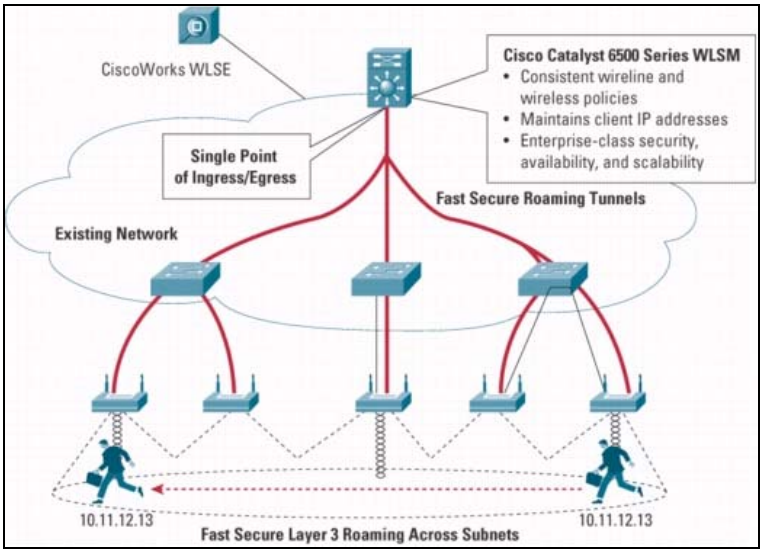

Figure 1-2. WLSM Enterprise Campus Deployment

The Catalyst 6K preserves the client IP address regardless of the AP association; any established VPNs or open connections can function despite roams. The Catalyst 6K WLSM provides the following benefits:

- Uses existing network infrastructure investments that do not force changes to the wireline infrastructure and do not require special client devices, greatly simplifying deployment, and management, lowering TCO

- Enables fast secure campus wide Layer 3 mobility for mobile users registered with the WLSM, especially critical for real time latency sensitive applications like VoWLAN

- Increased scalability, supporting up to 300 Access Points and 6000 Mobile Users throughout the campus using a single Catalyst 6500 WLSM located anywhere in the network

- Simplified management and deployment of wireless networks by unifying wireless networks, providing consistent application of policies for all wireless traffic via a single point of ingress and providing ‘out of box’ access point configuration

- Unified QoS and security policy application for groups of wireless users using a centralized point of ingress in the network (via multipoint GRE tunnel application on the supervisor)

- Wireless Traffic Segregation through the support for multiple VLANs on the AP mapping to multiple ‘mobility groups’. Allows network managers to segment and individually authenticate, control access and manage disparate wireless user groups such as ‘guest’ and ‘employee’ by enabling mobility groups.

- Hardware based DoS protection mechanisms such as control path limiters and Unicast Reverse Path Forwarding (uRPF)

- Service Module chaining: extends Catalyst 6500 Series intelligent network services to the wireless network including enterprise class security (DoS) prevention, Access Control, Firewall, IDS, and VPN. See Figure 1-3, *Secure Module Chaining*.

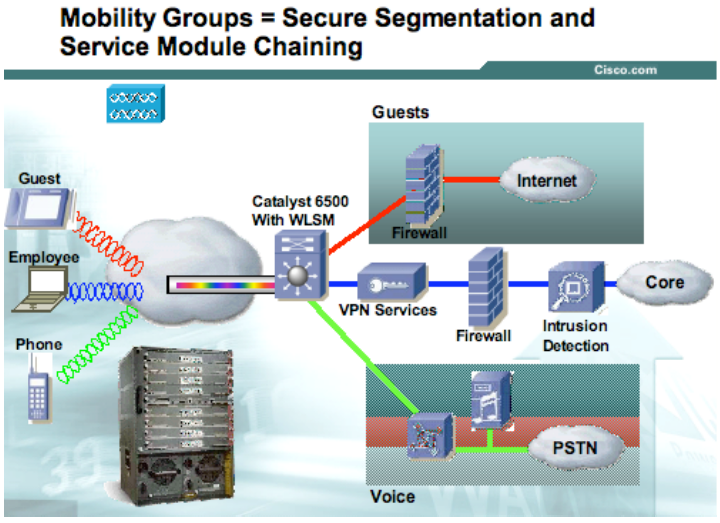

Figure 1-3. Secure Module Chaining

Access points, a key component of wireless networks, can be configured in several ways. Three common ways are the command line interface (CLI), web page or via the Wireless LAN Solution Engine. Configurations here are shown as web pages for clarity. There are over 55 Cisco configuration web pages with many parameters. Not all pages or parameters are discussed in the following screen shots.

1.2 Configuration of Recommended Security Policies

The following are device specific configuration settings for the CISCO AP and other network products used in this test.

Architecture Component	Cisco Implementation
AP	Model 1200 with 802.11g radio [IOS firmware v12.3(2)JA2]
AP Manager	Wireless LAN Solution Engine (WLSE v2.7)
RADIUS	Authentication Control Server (ACS v3.2)
Wireless Domain Services (WDS)	WDS services running on designated primary and backup Cisco APs (radios turned off) or WDS running on the Wireless LAN Solutions Module for the Catalyst 6500

2.3.1.010	Use layer 2 or 3 encryption with AES

Some basic parameters required to configure an AP as part of a WLAN are shown in the following screen print. Configure the following:

- System Name: device-group-name such as “ap-cis-benchmark”.
- IP Address: choose non-routable static IP for security and ease of management. Choose IP appropriate for OOB management VLAN discussed below).
- IP Subnet Mask: Choose appropriately for your network.

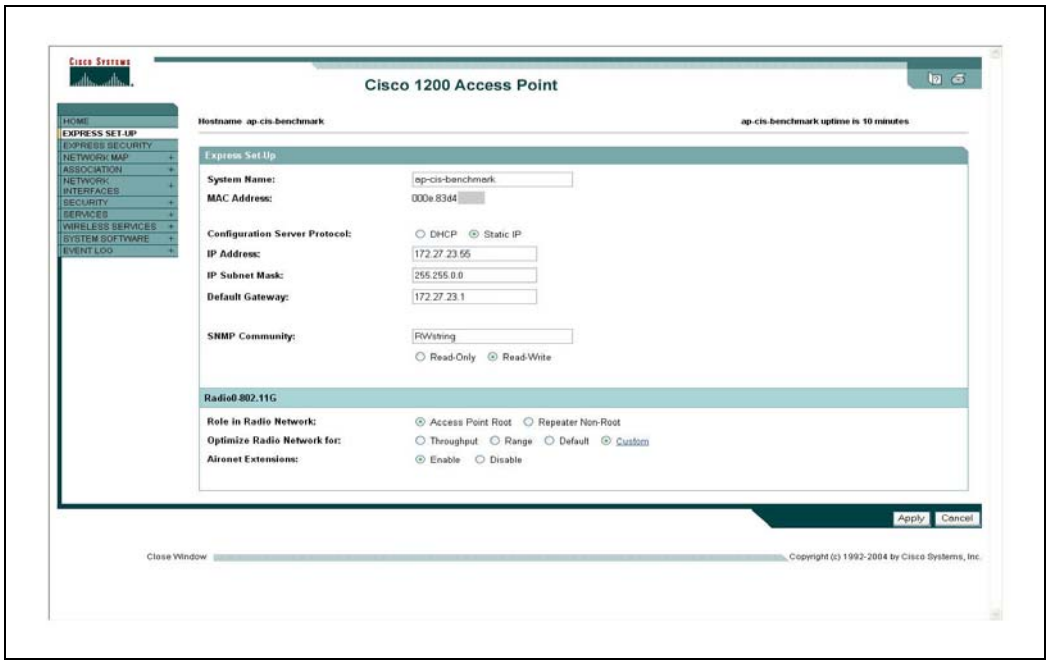

Figure 1-4. Cisco: Express Setup Screen

Figure 1-5, *Encryption Configuration*, shows the initial configuration of encryption on the wireless link, as follows:

- EAP Authentication – Enable EAP-PEAP and set Radius server and secret. Secret must be consistent with organization's password policy. Mutual authentication process between client and network is protected with PEAP.

- WPA or WPAv2– Should be enabled in conjunction with Layer 3 VPN services. Security at layer 2 should be required; if Layer 2 Encryption is not used, the wireless and wired infrastructure is potentially vulnerable from the AP to the VPN concentrator. Packet sniffing of the L3 IKE negotiation process is possible.

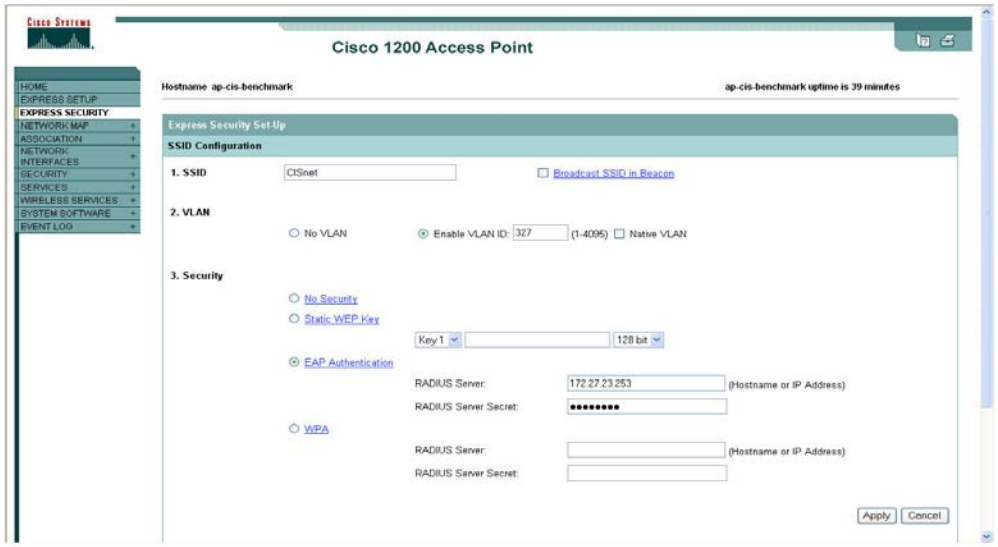

Figure 1-5. Cisco: Encryption Configuration

2.3.1.020	Choose products that support a network level security management solution.
This product supports network level security management solutions.	

2.3.1.030	Disable management ports on network devices when not in use.

The following are recommended settings for the services and ports available:

- Telnet/SSH: Enabled – Enables secure shell tunneling to AP for management purposes (CLI). For secure deployments, SSH should be enabled and Telnet should be disabled.
- CDP: Disable Cisco Discovery Protocol. CDP can be disabled, but may adversely impact Power over Ethernet negotiation with the AP, as well as limit the ability for Switch port shutdown of rogue AP's.
- Filters: Enabled (optionally, these can be individually enabled if needed). See Figure 1.7 for configuration options. Filters/Access lists can be enabled on the AP to only allow critical services such as DHCP, DNS and VPN services to further control traffic.
- Filters: Enabled (optionally, these can be individually enabled if needed). See Figure 1.7 for configuration options.
- SNMP: Enabled – Allows network management and monitoring devices to access the AP (but over an OOB management VLAN described later).
- VLAN: Enabled – Allows multiple virtual LANs to be configured to the AP from network.
- Hot Standby: Disabled
- DNS: Disabled
- HTTP: Enabled – Allows browser access to the AP for configuration. Caution, this access should only be allowed over a secure channel, since the communication is not HTTPS.
- QoS: Disabled (unless applications require this feature)
- NTP: Enable – for network Managements best practice – this will provide a way to help correlate events if the need arises for Network Troubleshooting.
- ARP Caching: Disabled (enable to decrease wireless broadcast traffic and increase security)

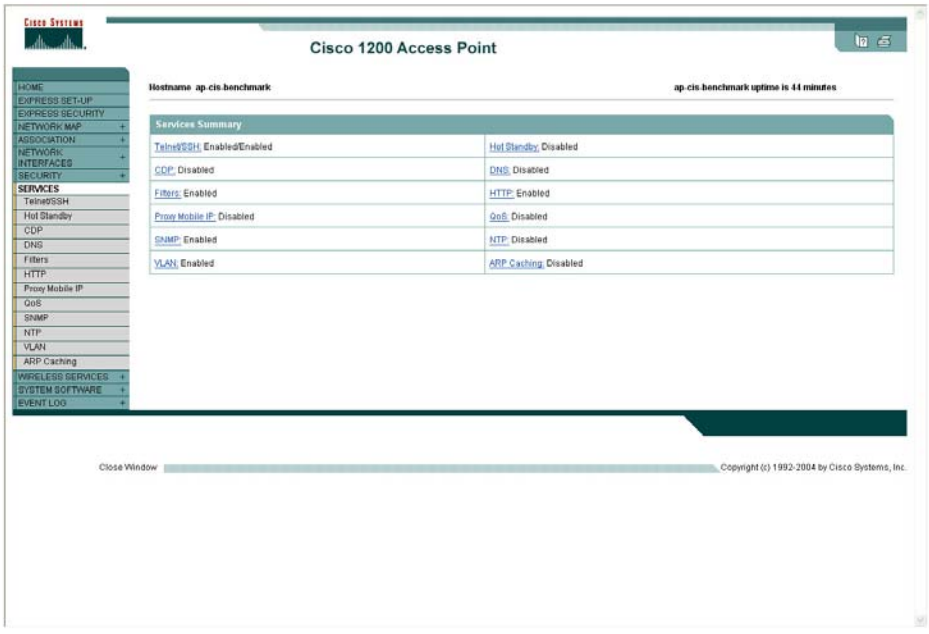

Figure 1-6. Cisco: Configuring Management Ports and Services

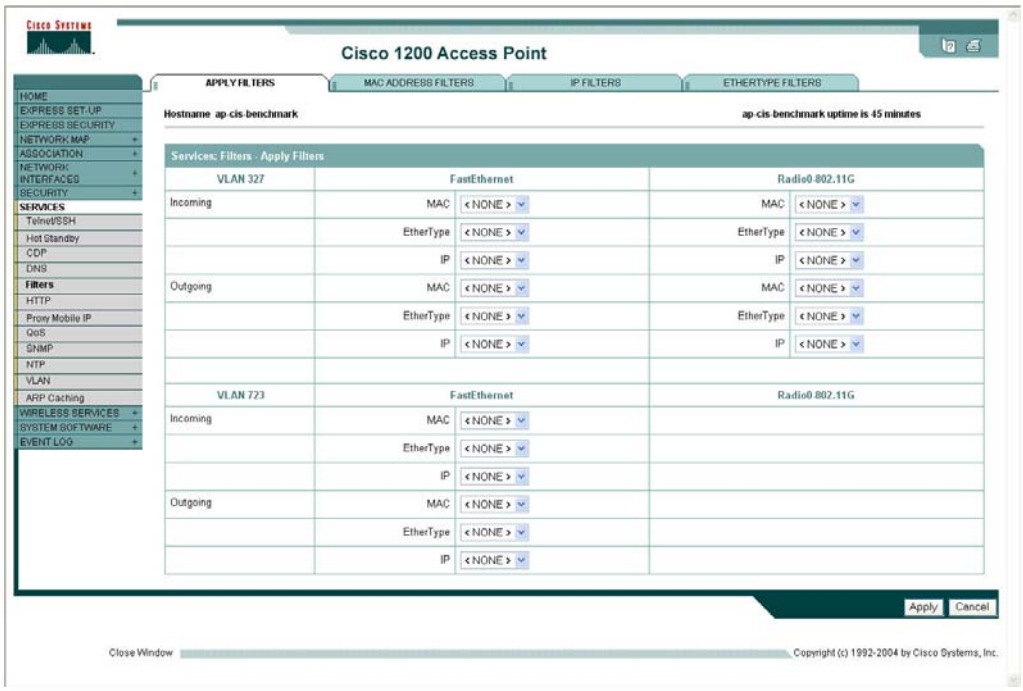

Figure 1-7. Cisco: Filters

2.3.1.040	Use OOB management across a specially configured VLAN for network administration/management

The following screen prints show the configuration of VLANs. Figure 1-8 shows a security summary with both VLANs, one for management and one for wireless users.

- **Services > VLAN** – OOB VLAN
- VLAN ID: choose a number within the range and enter
- Native VLAN: check this box for the OOB management network only
- SSID: <none> none associated with management VLAN; only wireless user VLANs have associated SSIDs

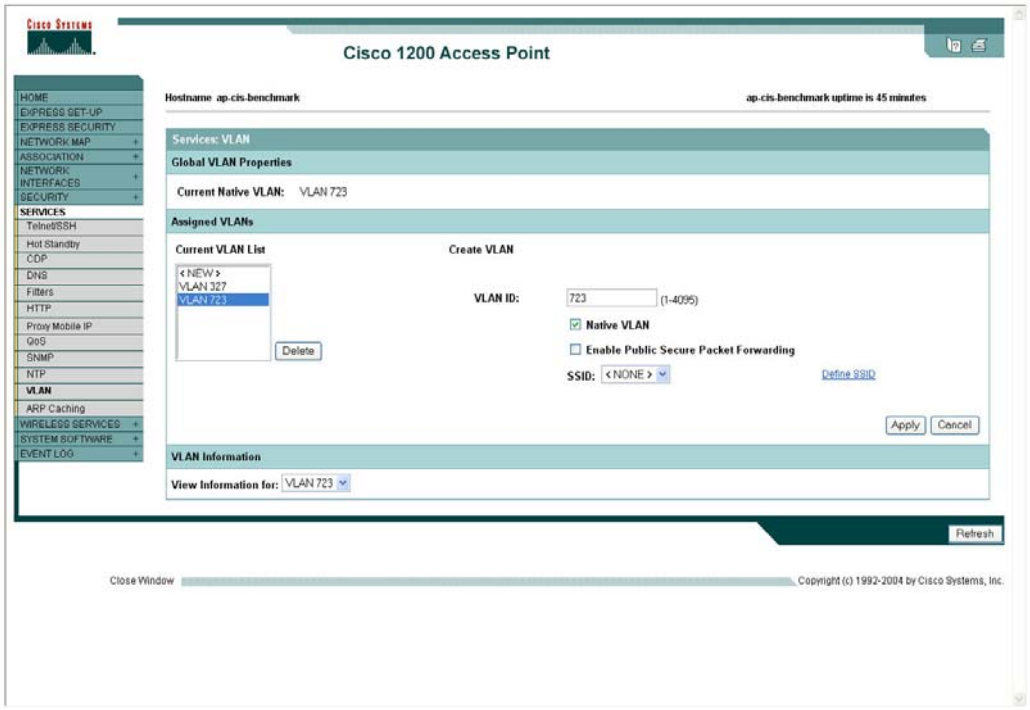

Figure 1-8. Cisco: VLAN Summary Screen

The following screen print shows the configuring of VLANs for wireless user traffic.

- **Services > VLAN** – wireless user VLAN
- VLAN ID: choose a number within the range and enter. For example, 327 is shown.
- Native VLAN: uncheck this box. 327 VLAN is intended for wireless user traffic.
- SSID: Choose the SSID entered earlier in configuration process (e.g., CISnet).

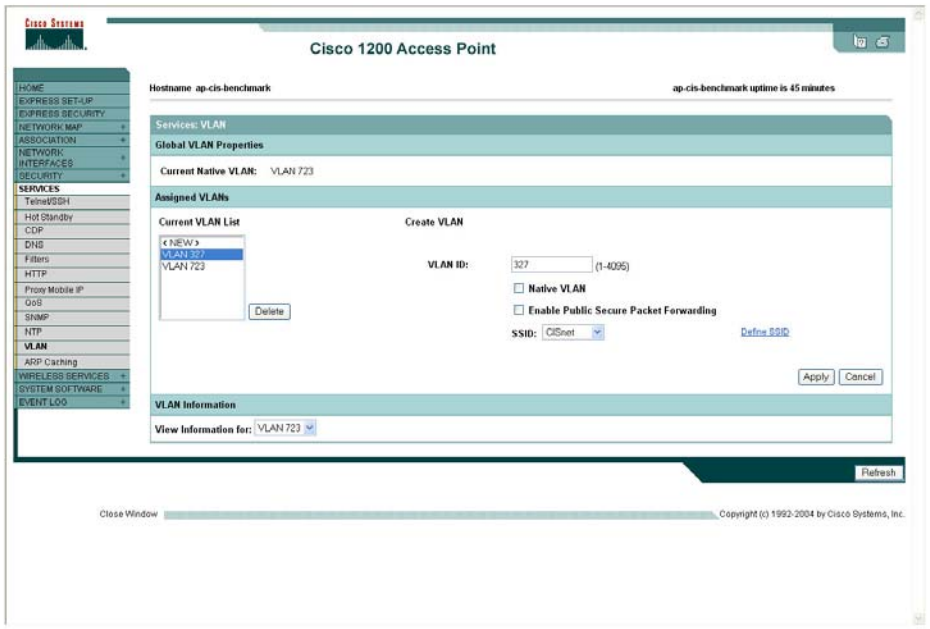

Figure 1-9. Cisco: VLAN User Configuration

2.3.1.050	WLAN must have session timeout capability and must be set to 15 min or less

Set client station to chosen number of minutes less than 15 minutes (in seconds).

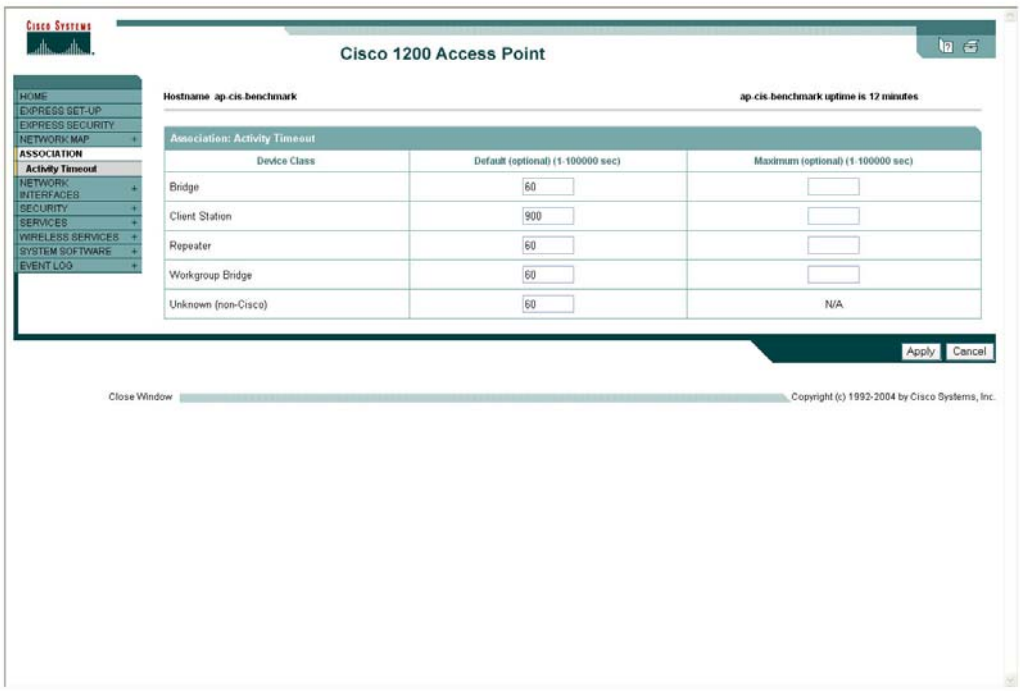

Figure 1-10. Cisco: Timeout Setting

2.3.1.060	Set AP transmit power to lowest possible to attain signal strength required

- Go to **Settings** tab, select **Network Interfaces**
- CCK Transmitter Power (mW): click desired power setting
- OFDM Transmitter Power (mW): click desired power setting

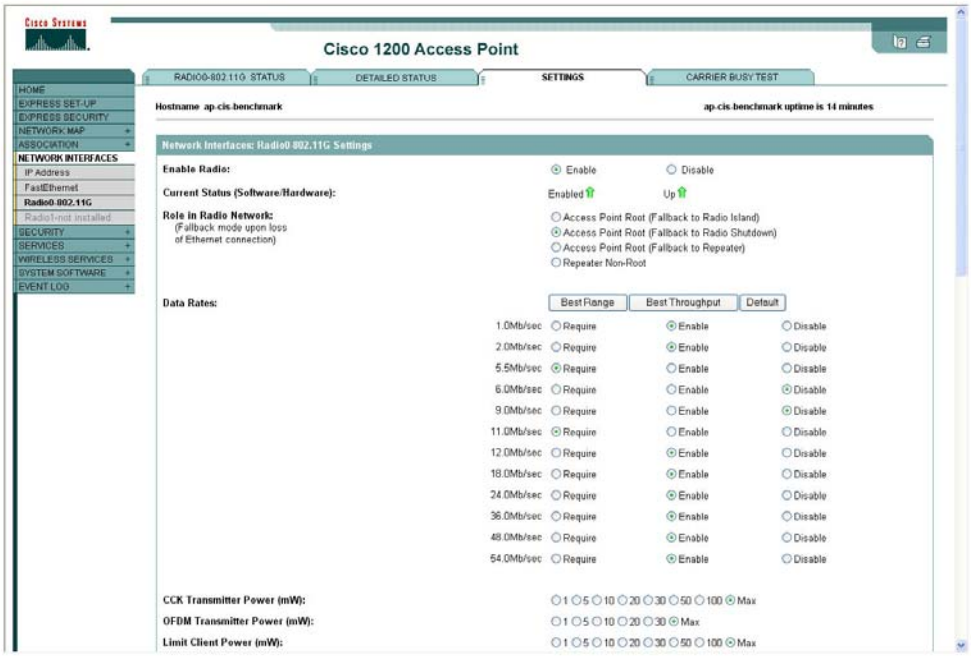

Figure 1-11. Cisco: Transmit Power Settings

2.3.1.070	Password-protect AP and bridges beyond manufacturer's default setting

Preferred Method: Use Authentication server for Administrator access to provide an additional layer of security (RADIUS or TACACS).

Less secure method: **Administrator Authenticated By: Local User List Only (Individual Passwords)**.

Password: Set password per organizational password policy.

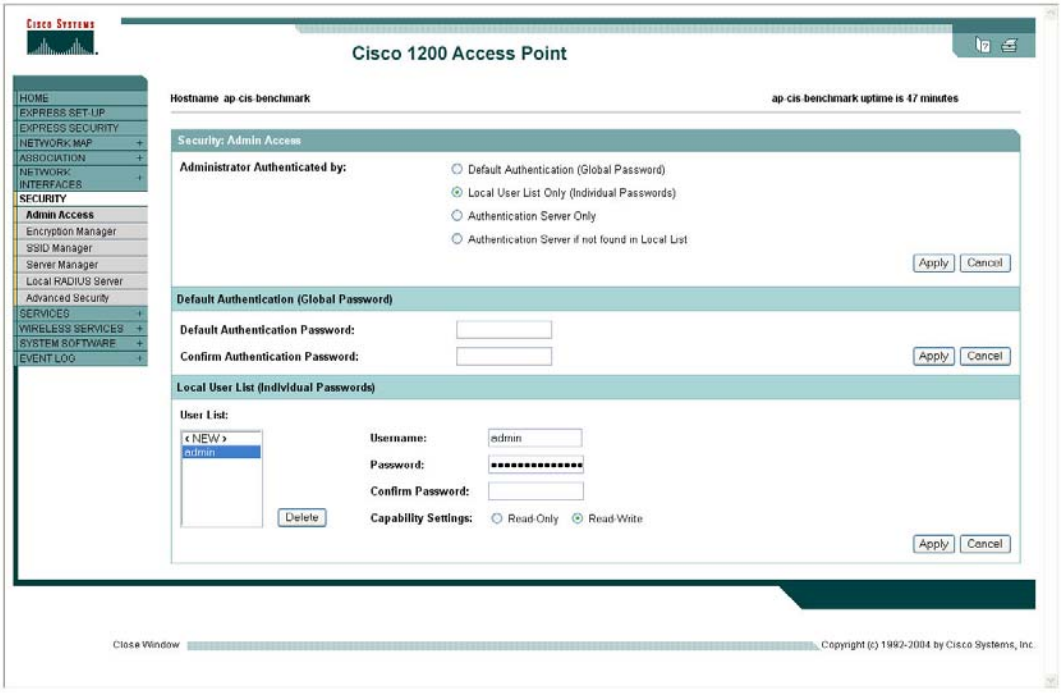

Figure 1-12. Cisco: Passwords Configuration

2.3.1.080	Change default SSID
SSID was set as part of Express Security page as shown in Figure 1-4.	

2.3.1.090	Disable SSID broadcast mode
SSID broadcast is disabled by default.	

2.3.1.100	Enable MAC address filtering
Enable MAC address filtering from a central server if automatic device network registration is operational within the enterprise. If automatic network registration is not operational, manual registration for an enterprise probably not justified for wireless devices. **Caution** – MAC Address filtering may adversely impact Fast Secure Layer 3 Roaming due to the large list of MAC addresses that will have to be maintained on the RADIUS server.	

2.3.1.110	Backup system configuration settings
Backup and restore AP configurations – The WLSE can be used to automatically update AP configurations (individually or in groups) and check for changes in any AP configuration.	

2.3.1.120	Enable Wireless Client Isolation
Restrict client-to-client traffic – Access points can be configured to restrict client-to-client traffic on the AP and client-to-client traffic between different APs on the same network.	

2.3.1.130	Enable and configure logging
This feature may be configured by selecting the **Event Log** button.	