

Deploying Wireless as a Base Building Service

Advances in technology incorporated into the Cisco wireless access points makes it feasible to deploy wireless as a base building service. In this deployment model wireless is part of the building and is shared among the tenants. Using VLANs we can ensure that a tenant is connected to their own corporate network regardless of which access point they associate with. This design also allows for simple coverage of common areas such as courtyards, restaurants and cafes.

1. Introduction

This document provides a technical overview of a solution to allow wireless services to be offered by building owners as part of the base services just like water, power, and air conditioning.

1.1. Office Buildings Today

When a tenant moves into a building they expect access to certain common services such as electricity, water, air-conditioning, and waste-disposal. It would be unthinkable if each new tenant came and installed their own water and sewer piping only to have it ripped out and replaced the next tenant when they leave. That is not to say there are not exceptions. Some tenants have exceptional power requirements, for example, and so bring in some of their own equipment. However, for the majority of tenants the power that comes with the building is sufficient.

Buildings are pre-fitted to supply all the basic services that most tenants require. A notable exception though is wireless data communications services. Yet this is an area where planning is essential because the wireless spectrum within a building is inherently shared. If each individual tenant installs their own wireless networks without any centralized planning there will inevitably be channel conflicts between tenants as the wireless signals leak through walls and floors. Of course the tenants can reduce power on the wireless access points to limit the leakage, but this means they may not be using enough power to ensure complete coverage of their own workplace resulting in dead zones.

1.2. A Better Building

For wireless services a better approach is to have a centrally planned and deployed network. This spectrum planning could be done by the architects, the building managers, or by the building owners. Once the site survey is completed then a single wireless network can be deployed that is then used by all the tenants. Each tenant will be able to lock onto the wireless network from anywhere in the building and their data will be forwarded to their own corporate network.

1.3. Roles and responsibilities in buildings with wireless as a base service

This document describes a business model where wireless data infrastructure is owned and managed. This may be done by the building owner, but it is more likely that installation and service will be outsourced to specialist companies. In this document the following terms are used to describe the various partners in the solution:

- **Building owner** – This could be an individual company or may be a property trust.
- **Systems Integrator** – This is the company responsible for the initial design and deployment of the wireless infrastructure. This may include site surveys, installation, design and test.



- **Wireless Service Manager** – This is the company that manages the wireless network. This will include making necessary configuration changes to access points and RADIUS servers as tenants move in and out of the building. Depending on configuration it may also mean adding and deleting user accounts in the RADIUS servers for tenant employees. If this were a corporate deployment this role would be assumed by the IT administrator.
- **Tenant** – A company that rents space within the building.
- **Guest** – A user working temporarily in the building. A guest may be working in one of the tenancies or may be a casual user in a public part of the building such as a café. In either case, guests do not have access to tenant networks they will only have access to the Internet on a restricted basis.
- **Building manager** – The company that manages the building for all the traditional services. This may or may not be the same as the Wireless Service Manager or they may act as a first point-of-call for support which is then handed off to the Wireless Service Manager.
- **Internet Service Provider (ISP)** – Provides connectivity to the Internet for guest and tenant access.
- **HotSpot Operator** – If guest access is billed the HotSpot operator provides hot-spot portal web pages and billing services.

2. Solution Goals and Requirements

2.1. Users have complete mobility within the building

The key difference between an enterprise WLAN deployment and a building service style deployment is that several tenants can share the same access point. This is actually an advantage to the design. If each tenant deploys their own solution they must be very careful not to interfere with WLAN deployments above, below or to the side of their offices. This usually means tuning down the power to ensure that there is no leakage into adjacent offices. With a shared design the access points can be tuned for optimum floor coverage rather than for minimized conflicts. It does not matter if someone in an adjacent office locks onto an access point on another floor because the use of VLANs ensures their data ends up on the correct network.

2.2. Guests have access to wireless network

When tenants have guests come to the building for meetings it is very useful if these guests can use the wireless network for Internet access and VPN access to their corporate networks. This allows customers, suppliers and others to immediately complete tasks rather than waiting until they are back in their own offices. For this reason the design includes an unsecured guest VLAN for casual users. Restaurants and cafes can use the guest VLAN to create a wireless hotspot. The design allows for either free access or paid access to the Internet. The building owner will need to decide on the charging model.

2.3. Bandwidth use is controlled

Using switches that support rate limiting means that we can restrict the amount of bandwidth used by any one tenant. In most cases we would do this for the guest VLAN to control download costs, but it could be extended to other VLANs if required.

2.4. Access is controlled

With the current version of code all access points will refer to a RADIUS server for user authentication before someone is allowed to access the network. This means that no one can access a tenant VLAN without first passing a login verification. The guest VLAN would not require this authentication. The user names and passwords can either be stored directly in the RADIUS server or the access points can request authentication from the different tenant owned login servers. The choice of which method to use will depend on what kind of tenants occupy the building. Larger tenants with their own IT infrastructure will probably want to have their own access control server do the authentication, smaller tenants may prefer to use the building's ACS server.

2.5. Design is Secure



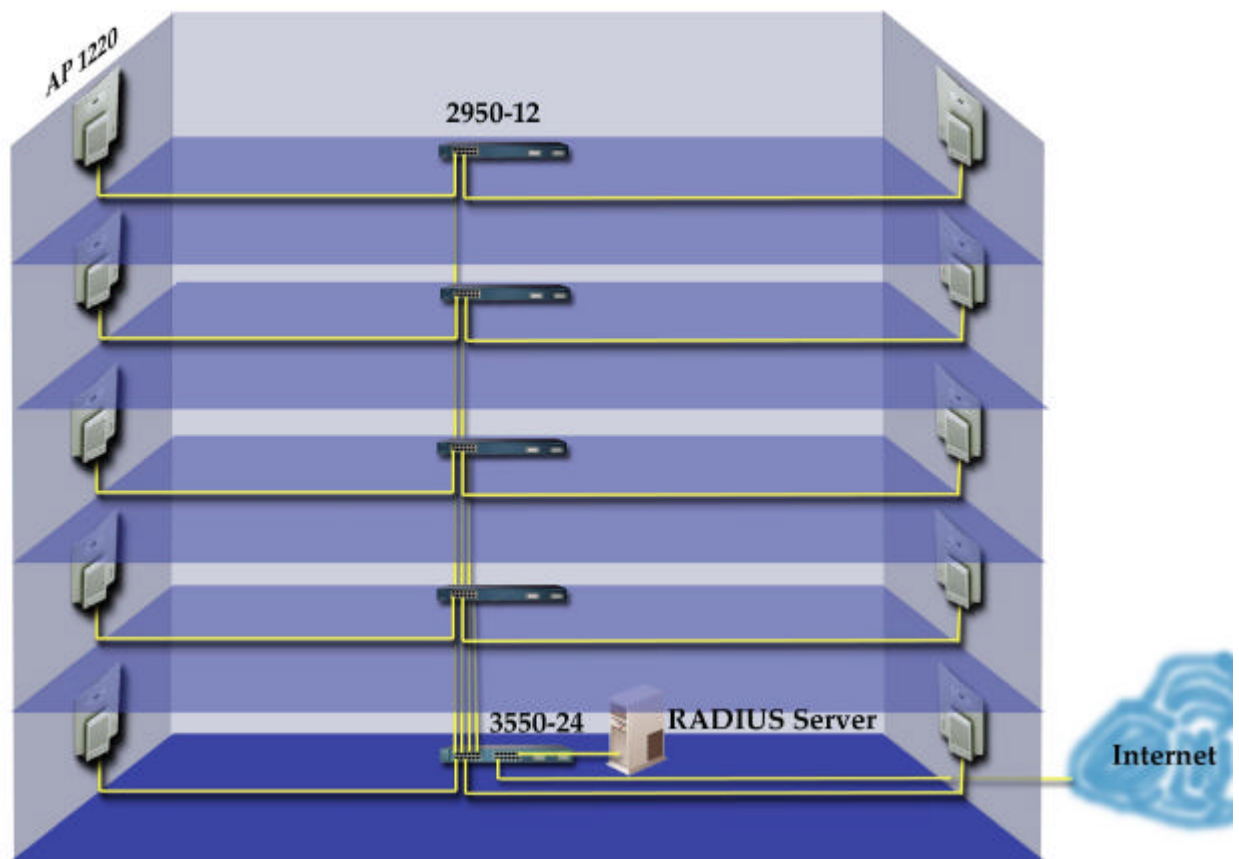
Although Cisco has corrected the security problems of the initial versions of the Wired Equivalent Privacy (WEP) standard many organizations still today deploy wireless networks insecurely. Typically this would be in small companies that do not have specialist IT staff.

In a building offering wireless as a base service the wireless security design is done by a certified integration partner. This means that all tenants get the benefits of a professionally designed security solution even if they are not big enough to have in-house IT staff. Using a building-owned RADIUS server we can offer LEAP (and later WPA) secured wireless connections even for companies that have no internal network authentication mechanisms.

2.6. Solution is flexible

The entire reason for wireless as a base building service is to make the property more attractive to potential tenants. For a building owner one key factor of any communication solution is that it never creates a problem for a potential tenant which would mean that the building become more difficult to lease to certain kinds of tenants. We can certainly imagine that some larger organizations will already have in place guidelines for wireless deployments. These organizations may not want to use network equipment that they don't themselves manage. This is the reason to have switches on each floor. This allows certain access points to be disconnected from the building systems so they can be managed by an individual tenant.

3. Solution Components



The solution has four major components. The components are shown in the diagram above. Specific products are labeled as these are the products used during testing in the proof-of-concept labs. The generic requirements are described below.



- Access Points (AP 1230) – The 1230 Access Points allow for both 802.11b and 802.11a networks. This allows for an upgrade path if the wireless network becomes congested. As a minimum any access point that can run IOS version 12.2.4-JA or later and supports VLANs and 801.1Q trunking could be used.
- Layer-2 Switches (2950-12) – The switches used in the tenancies need only Layer-2 capability and the required number of ports. The ports must support 802.1Q wherever they attach to an access point.
- Layer-3 Switch (3550-24) – The main (basement) switch is a layer three switch. This switch needs layer three capabilities because routing is required to support some authentication models. Also the switch should support rate limiting so that per-tenant bandwidth can be controlled if necessary. Access lists are needed to prevent unwanted traffic from hopping from one VLAN to another. Currently the 3550 is a good choice for this function, but other Layer-3 switches could be used.
- RADIUS Server – This RADIUS server allows us to authenticate users and permits the use of the best security, LEAP, even for tenant that don't have their own authentication mechanisms for LAN access. Some other useful features in the RADIUS server is the ability to proxy authentication to other servers. If RADIUS proxy will be used then routing must be enabled to allow traffic from the native VLAN to the tenant VLAN and access lists must be put in place to limit traffic to only the proxy traffic. While it is more work to put the proxy in place it makes it easier for the tenant to manage user accounts and password to allow access to the building wireless network.

4. VLAN Design

Much of this section is based on the *Wireless Virtual LAN Deployment Guide* (see References section for URL). That guide is designed for enterprises who wish to use VLANs to segment different parts of their corporate LAN. Although the technology is the same the way it is used is different. In our case it is much more of a service provider style of deployment because we are using a common infrastructure to support many different customers. Also, this guide does not deal with the use of wireless bridges as this would be very uncommon in a building deployment. Readers looking for information about wireless VLANs and bridging should refer to the aforementioned guide.

4.1. Wireless VLAN Overview

The concept of Layer-2 wired VLANs is extended to the wireless LAN (WLAN) with wireless VLANs. As with wired LANS, wireless VLANs define broadcast domains and segregate broadcast/multicast traffic between VLANs. If VLANs are not used, a building owner would have to install additional Wireless LAN infrastructure to segment traffic between tenants. Consider the case with common areas. Since 802.11b only offers three non-overlapping channels, without VLANs only three tenants in a building could directly use the common areas of their building.

With all IOS firmware releases for the access points, an 802.1Q trunk can be terminated on an access point (AP1200, AP1100, AP350, and AP340) or on a bridge (BR350), allowing access up to 16 wired VLANs. A unique Service Set Identifier (SSID) defines a wireless VLAN on the access point and the bridge. Each SSID is mapped to a VLAN-id on the wired side (default SSID to VLAN-id mapping).

Additionally, with wireless LANs, a per-VLAN security policy can be defined on the Access Point and on the bridge by the Wireless Service Manager. This means that one tenant can decide to use standard WEP because they will always use an encrypted VPN to connect to corporate resources and another can use Cisco LEAP authentication for strong security without the overhead of a VPN solution. Both these tenant can use the same access point simultaneously even though their security policies are different. This will be discussed in detail in section 6 Security Design.

4.2. Wireless VLAN Deployment

A wireless LAN deployment scenario is shown in Figure 1. Each tenant uses a different SSID when they associate with an access point. This SSID will then, after authentication by the RADIUS server, force them onto the VLAN which corresponds to their own enterprise network. For simplicity in the example we assume that Tenant N uses SSID called "Tenant N" which is mapped to VLAN N. Also each wireless VLAN is configured with an appropriate security policy and mapped to a wired VLAN. The Guest VLAN allows access to the



internet for users who do not normally work in the building. There is no wireless security applied so these users will need to use an encrypted VPN solution on their PCs if they want secure data over the wireless link.

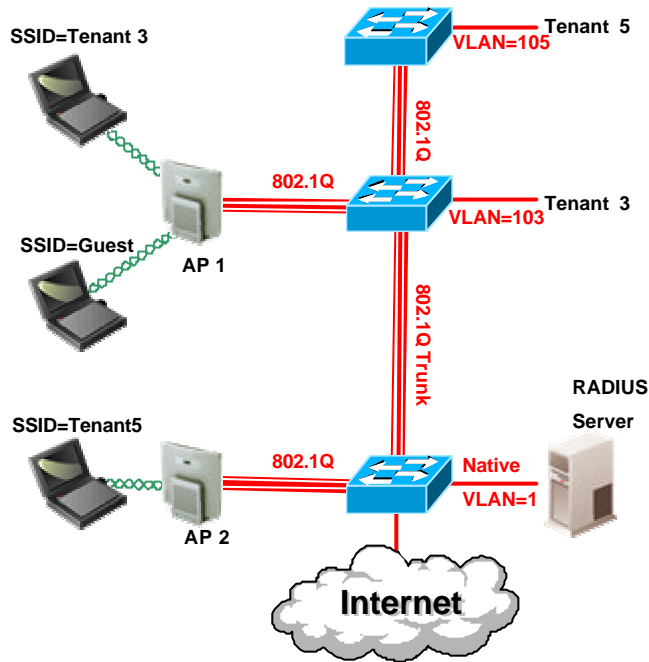


Figure 1 Wireless VLAN deployment model

Table 1 SSID to VLAN to Security Policy Mappings

SSID	VLAN-id	Security Policy
Tenant3	3	802.1x with Dynamic WEP + TKIP
Tenant5	5	802.1x with Dynamic WEP + TKIP
Guest	1	Open/no WEP

When the tenant moves into the building they work with the Wireless Service Manager to determine the most appropriate security policy for their company. The Wireless Service Manager then enforces the appropriate security policies within the wired network for all the different tenants.

4.3. Wireless VLANs: Detailed Feature Description

This section details the VLAN features available with IOS firmware starting from release 12.2.4-JA. With this release, an 802.1Q trunk can be enabled between the access point/bridge and the wired infrastructure allowing up to 16 wired VLANs to be extended to the WLAN.

4.3.1. Configuration parameters per VLAN

As discussed in section 4.2, a per VLAN security policy can be defined on the access point to allow the Wireless Service Manager to define appropriate restrictions per VLAN. The following parameters are configurable on the SSID (wireless VLAN):



- SSID name: Configures a unique name per wireless VLAN
- Default VLAN ID: Default VLAN-ID mapping on the wired-side
- Authentication types: Open, Shared, and Network-EAP types
- MAC authentication: Under Open, Shared, and Network-EAP
- EAP authentication: Under Open and Shared authentication types.
- Maximum number of Associations: Ability to limit maximum number of WLAN clients per SSID.

The following parameters are configurable on the wired VLAN-side:

- Encryption key: This is the key used for broadcast/multicast traffic segmentation per VLAN. It is also used for static Wired Equivalent Privacy (WEP) clients (for both unicast and multicast traffic). The Wireless Service Manager must define a unique encryption key per VLAN.
- Enhanced MIC Verification for WEP: Enables MIC per VLAN.
- Wi-Fi Protected Access (WPA) required parameters.
- Temporal Key Integrity Protocol (TKIP): Enables per-packet key hashing per VLAN.
- WEP (Broadcast) Key rotation Interval: Enables Broadcast WEP key rotation per VLAN. This is only supported for wireless VLANs with 802.1X protocols enabled (such as LEAP, EAP-TLS, PEAP, EAP-SIM, etc.)
- Default Policy Group: Applies policy-group (set of Layer-2, 3, and 4 filters) per VLAN. Each filter (within a policy group) is configurable to allow or deny certain type of traffic.
- Default Priority: Applies default CoS priority per VLAN.

With an encryption key configured, the VLAN supports standardized WEP. However, Cisco TKIP/MIC/Broadcast key rotation features are optionally configurable as noted above. Table 2 below lists the SSID and VLAN-ID configuration parameters.

Table 2: SSID and VLAN-ID Configuration Parameters

	SSID parameter	VLAN-id parameter
Authentication Types	X	
Maximum number of Associations	X	
Encryption key (Broadcast Key)		X
TKIP/MIC		X
WEP (Broadcast) Key rotation Interval		X
Policy Group		X
Default Priority (CoS mapping)		X

4.3.2. Broadcast Domain Segmentation

All Layer-2 broadcast and multicast messages are propagated over the air. Thus, each WLAN client receives broadcast/multicast traffic belonging to different VLANs. This is different from wired VLAN broadcast/multicast traffic. With wired LANs, a wired client receives Layer-2 broadcast/multicast traffic for its own VLAN only. Thus, a unique encryption (broadcast/multicast) key per VLAN is used to



segment the Layer-2 broadcast domains on the wireless LAN. This unique encryption key must be configured during initial VLAN setup. If Broadcast Key rotation is enabled, this encryption key is generated dynamically and delivered to WLAN clients in 802.1X messages.

The requirement to segment broadcast domains on the wireless-side restricts the use of unencrypted-VLAN per WLAN Extended Sub System (ESS). Some early software IOS version supported a maximum of one VLAN can be unencrypted per WLAN ESS. This restriction is removed in later versions.. Also, the behavior of a WLAN client on an encrypted VLAN should be to discard unencrypted Layer-2 broadcast/multicast traffic.

4.3.3. Native (Default) VLAN Configuration

The access point's (or the bridge's) native VLAN (i.e. default VLAN) must be set to the native VLAN of the wired trunk. This allows the access point or bridge to receive and communicate using the Inter-Access Point Protocol (IAPP) with other access points or bridges in the same wireless LAN ESS. It is a requirement that all access points and bridges in an ESS must use the same native VLAN-ID. All Telnet and http management traffic as well as the RADIUS traffic is routed to the access point via the native VLAN. Cisco recommends that Wireless Service Managers restrict user access to the native/default VLAN of the access points and bridges (with the use of Layer-3 access control lists (ACLs) and policies on the wired infrastructure side).

In the case of a combined deployment of infrastructure devices (such as workgroup bridges, non-root bridges, and repeaters) along with non-infrastructure devices (such as WLAN clients) in an enterprise WLAN the native VLAN of the access point is mapped to the "Infrastructure" SSID. WEP Encryption along with TKIP (at least per-packet Key hashing) should be turned-on for the "Infrastructure" SSID. Configuration of a secondary SSID as the "Infrastructure" SSID is also recommended. The concepts of primary and secondary SSIDs are explained in the next section.

4.3.4. Primary (Guest) and Secondary SSIDs

When enabling multiple wireless VLANs on the access point or bridge, multiple SSIDs are created with each SSID mapping to a default VLAN-ID on the wired side. However, as per 802.11 specifications, only one SSID can be broadcast in the beacons. The Wireless Service Manager defines a primary (Guest) SSID that is broadcast in the 802.11 beacon management frames. All other SSIDs are secondary SSIDs and are not broadcast in the 802.11 beacon management frames.

If a client or infrastructure device (such as a workgroup bridges) is to send a probe request with a secondary SSID, the access point or bridge will respond with a probe response with that secondary SSID.

A Wireless Service Manager can also map the primary SSID to the VLAN-ID on the wired infrastructure in different ways. For example the primary SSID could be mapped to the unencrypted VLAN on the wired-side to provide "Guest" VLAN access.

4.4. Wireless VLAN Deployment Example

This section discusses the elements of configuration for the access points and the switches to implement the wireless service. In section 11 you will find complete configurations for the devices used in this example. This section shows the IOS CLI commands for both the switches and the access points. In practice it is easier to use the GUI on the access points for initial configuration. The access point commands shown in this section were generated using the HTML GUI built into the access points. The AP CLI was only used for particular commands outside of a typical configuration. These are discussed in the section on authentication. The following diagram will be used as a reference for the configuration examples in this section.

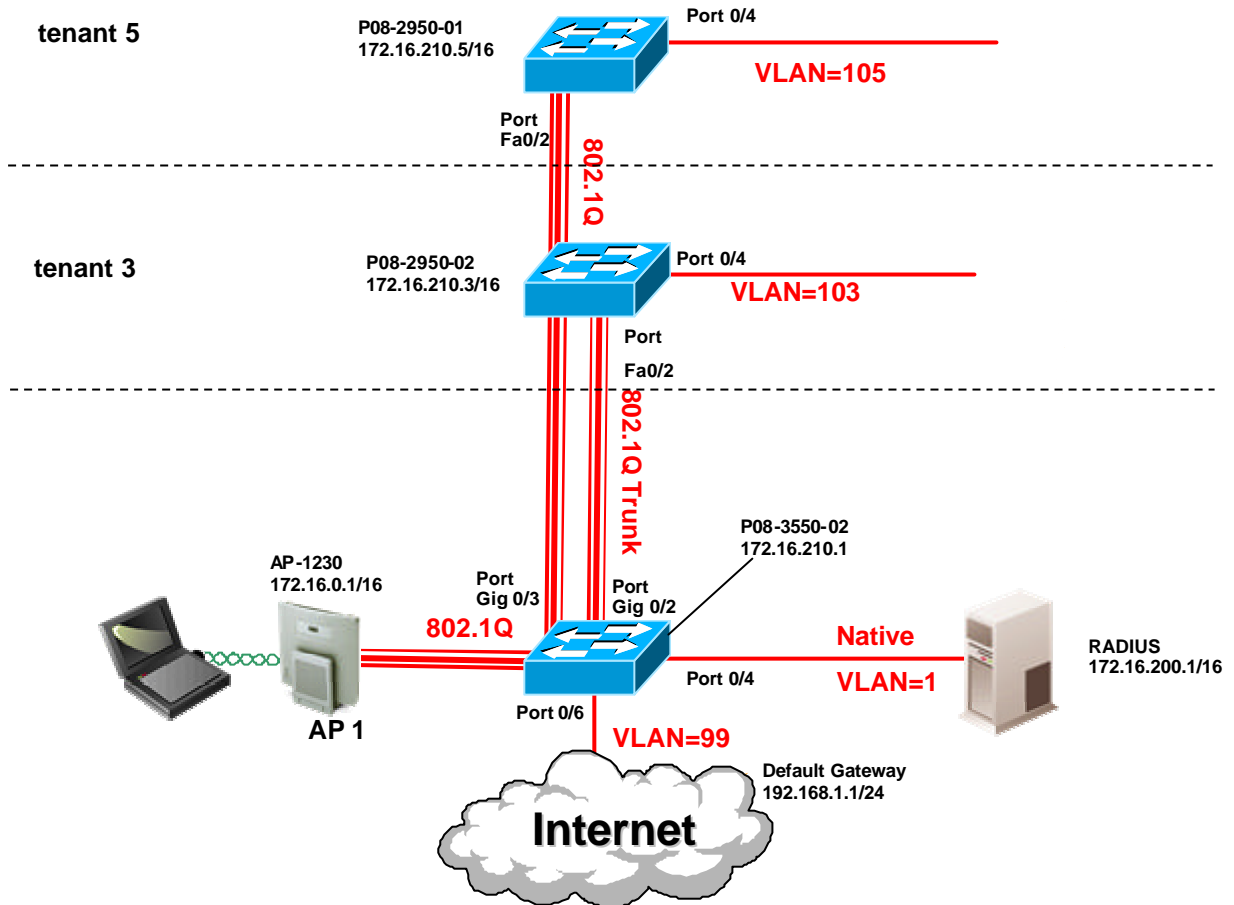


Figure 2 : Example architecture for access point and switching configurations

4.4.1. Configurations to map SSID to VLAN

The first step in creating the wireless service is to map wireless SSIDs to VLANs. In our example we have tenants 3 and 5. We use the simple rule that the VLAN for tenant N is VLAN number (100 + N). This allows for a simple naming structure while avoiding VLAN 1 which is the native VLAN. The SSID to VLAN mapping is done on each access point in the system. In the configuration fragment shown we also set the authentication methods for tenant 3. Complete discussion of authentication can be found in section 7 *User Authentication Procedures*. The commands to set up SSID and VLANs for tenant 3 would be:



```
ssid tenant3
  vlan 103
  authentication network-eap eap_methods

interface Dot11Radio0.103
  encapsulation dot1Q 103
  no ip route-cache
  bridge-group 103
  bridge-group 103 subscriber-loop-control
  bridge-group 103 block-unknown-source
  no bridge-group 103 source-learning
  no bridge-group 103 unicast-flooding
  bridge-group 103 spanning-disabled
```

4.4.2. Mapping guest access to a VLAN

One VLAN is nominated as the Guest VLAN. This VLAN is used to allow people in the building to get out to the Internet without giving them access to any of the tenant VLANs. In the example here we chose VLAN 99 to be the guest VLAN. The things that are special about the guest VLAN are that traffic is only allowed out to the Internet and the guest VLAN uses open access (no encryption). The guest-mode command allows clients without any SSID to associate with the access point. The commands on the access point to set up the guest VLAN are as follows.

```
ssid guest
  vlan 99
  authentication open
  guest-mode

interface Dot11Radio0.99
  encapsulation dot1Q 99
  no ip route-cache
  bridge-group 99
  bridge-group 99 subscriber-loop-control
  bridge-group 99 block-unknown-source
  no bridge-group 99 source-learning
  no bridge-group 99 unicast-flooding
  bridge-group 99 spanning-disabled
```

4.4.3. Configuring the native VLAN

The native VLAN is used for communication between the access points and the primary RADIUS server. It is also used for communication between the access points to handle client hand-offs. The native VLAN is tied to a bridge group which has the IP address used to manage the access point. The primary RADIUS server should be on the same subnet on the native VLAN as the access points.



```
interface FastEthernet0.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
 !
interface BV11
 ip address 172.16.0.1 255.255.0.0
 no ip route-cache
 !
```

4.4.4. Mapping a port to a VLAN on a switch

This is the simplest way to configure a port to be in a particular VLAN. The VLAN is created automatically, although it would make sense to create the VLANs you want to use explicitly and give them a name. The following fragment configures port 4 on the 2950 shown in the diagram that connects to tenant 3.

```
interface FastEthernet0/4
 switchport access vlan 103
 switchport mode access
 no ip address
```

4.4.5. Configuration a port to trunk to an AP

The following configuration fragment shows how the trunk port connecting the 3550 to the access point would be configured.

```
interface GigabitEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
```

4.5. Summary of Rules for Wireless VLAN Deployment

This section summarizes the VLAN rules and guidelines discussed in this document:

1. 802.1Q VLAN trunking (hybrid mode only) supported between the Switch and the access point or bridge.
2. A maximum of 16 VLANs per ESS are supported with each wireless VLAN represented with a unique SSID name.
3. Wireless Service Manager must configure a unique encryption key per VLAN.
4. A maximum of one unencrypted VLAN per ESS is supported.
5. A maximum of one primary/guest SSID per ESS is supported.
6. TKIP, MIC, and Broadcast key rotation can be enabled per VLAN.
7. Open, Shared-Key, MAC, network-EAP (LEAP), and EAP authentication types are supported per SSID.



8. Shared-Key Authentication is supported only on the SSID mapped to the native VLAN (this is most likely to be the “Infrastructure” SSID).
9. One unique policy group (set of L2/L3/L4 filters) is allowed per VLAN.
10. Each SSID is mapped to a default wired VLAN where the ability to override this default SSID to VLAN-ID mapping is provided via RADIUS-based VLAN access control mechanisms.
11. RADIUS-based VLAN-ID assignment per user is supported
12. RADIUS-based SSID access control per user is supported
13. The ability to assign a CoS mapping per VLAN with 8 different levels of priorities is supported
14. The ability to control number of clients per SSID is supported
15. All access points and bridges in the same ESS must use the same native VLAN-ID to facilitate IAPP communication between access points and bridges.
16. All wireless LAN security policies should be mapped to the wired LAN security policies on the switches and routers.

5. Switching Design

One of the design criteria is that the building wireless system must not cause problems for companies that already have wireless deployment guidelines in place and choose to manage their own wireless equipment. In this case the Wireless Service Manager will disconnect the access points that serve that tenant and allow the tenant to use and manage those APs. The APs should continue to use channels that conform to the building spectrum plan that was established by the site survey.

In the design we use an appropriate number of switches to allow a set of access points to be privately managed. The building owner will have to set a rental fee for the equipment during the tenancy. Once the tenant leaves the building the switches will be re-connected to the building wireless system.

Companies that choose to privately manage the access points will reduce the value of the whole system so it is encouraged that they remain on the building system if possible.

5.1. Best-Practices for the Wired Infrastructure

The way wireless VLANs work lends itself to two different architectures within the building switching infrastructure: a pure layer-2 design and a combination Layer-2/Layer-3 implementation. Each approach is valid and viable, but have different capabilities. The merits of the two options are outlined in the following sections.

5.1.1. Pure Layer-2 Design

The simplest design is a pure Layer-2 design. In this model all authentication is done by the building RADIUS server. The access points and the building RADIUS server all sit on the native VLAN and have IP addresses on the subnet assigned to that VLAN. Once a user logs into the system successfully they have access to their corporate VLAN. IP address assignment and any further login procedures are left to the tenant to organize. The building switches do not need to know anything about the IP addressing schemes of the tenants so they do not have to have routing enabled. The tenants addresses schemes can have overlap, but because there is no traffic between VLANs this is never an issue. The switching design inherently blocks inter-VLAN traffic because there is no routing between VLANs.

On the down side, we lose the ability for single sign on in some cases. The building RADIUS server must have an entry for every user for every tenant in the building. As employees come and go this database must be updated. If the RADIUS server does not allow for user changeable passwords then the Wireless Service Manager must do this on behalf of users.



5.1.2. Combination Layer-2/Layer-3 Design

If we want tenant to do their own authentication and manage their own user databases then we need to use routing. This is because the access points need to communicate directly with the tenant's authentication servers, yet the access points do not have direct access to the tenant's networks. Access points only have the ability to drop user data on a tenant VLAN, but they do not have an IP address on each VLAN. In this case any communication with tenant authentication servers is sent to a Layer-3 switch which does have access to the VLAN.

The layer3 capable switch becomes the default gateway for the access points. This switch will have an IP address on the tenant VLAN. Because this switch will have visibility into several subnets these subnets cannot have overlapping address spaces. Since this switch will have IP routing enabled we will have to implement access control lists to prevent traffic from going from one tenant VLAN to another.

Although a Layer-3 design is more complex it does offer greater flexibility. Some of the advantages are:

- Allows flexibility in authentication as authentication servers can communicate between each other.
- Rate limiting at Layer-3 is possible to control bandwidth usage.
- Layer-3 access control lists can be used to enhance security.
- DHCP servers can supply addresses to multiple VLANs.

5.1.3. Wired Infrastructure Recommendations

The following best practices are recommended for the wired infrastructure when 802.1Q trunking is extended to the access points and bridges:

1. Limit broadcast/multicast traffic to the access point and bridge by enabling VLAN Filtering and IGMP snooping on the switch ports. On the 802.1Q trunks to the access point and bridge, filter to allow only active VLANs in the ESS. Enabling IGMP snooping prevents the switch from flooding all switch ports with Layer-3 multicast traffic.
2. Map Wireless Security Policies to the wired infrastructure with Access Control Lists (ACLs) and other mechanisms
3. The access point does not support VTP/GVRP protocols for dynamic management of VLANs because the access point acts as a "stub" node. The Wireless Service Manager must use the wired infrastructure to maintain and manage the wired VLANs.
4. Enforce security policies via Layer-3 ACLs on the "guest" and management VLANs (recommended).
 - The Wireless Service Manager could implement ACLs on the wired infrastructure to force all "guest" VLAN traffic to the Internet Gateway.
 - The Wireless Service Manager should restrict user access to the native/default VLAN of the access points and bridges with the use of Layer-3 ACLs and policies on the wired infrastructure.
 - Example: Traffic to access points and bridges via the native/default VLAN is only allowed to and from the management VLAN where all the management servers including the RADIUS server reside.

6. Security Design

6.1. Introduction

This section on security is taken from the "*SAFE: Wireless Security in Depth*" whitepaper with some small modifications for this system. The URL for the complete paper can be found in the References section.

6.2. SAFE Wireless Security Recommendations



The Cisco Wireless Security Suite provides robust wireless security services for Cisco Aironet® wireless products. The Cisco Wireless Security Suite is an 802.1X-based security solution that closely parallels the security available in a wired local area network (LAN). This enterprise-class solution provides scalable, centralized security management with support for dynamic per-user, per-session Wired Equivalent Privacy (WEP) encryption keys to protect the privacy of transmitted data. Other features include mutual authentication taking advantage of Extensible Authentication Protocol (EAP) types such as EAP Cisco Wireless or LEAP, Protected EAP (PEAP), EAP-Transport Layer Security (EAP-TLS) and prestandard Temporal Key Integrity Protocol (TKIP) features such as message integrity check (MIC) and per-packet keying to ensure that every data packet is encrypted with a different key.

Organizations should choose to deploy either IPsec or 802.1X/EAP with TKIP or Cisco TKIP, but generally not both. Specific designs using both at the same time were tested in the SAFE lab and are discussed in the "Alternatives" sections of the following designs. Organizations should use IPsec when they have the utmost concern for the sensitivity of the transported data, but remember that this solution is more complex to deploy and manage than 802.1X/EAP with TKIP. The 802.1X/EAP with TKIP should be used when an organization wants reasonable assurance of confidentiality and a transparent user security experience. The basic WEP enhancements can be used anywhere WEP is implemented. For the vast majority of networks, the security provided by 802.1X/EAP with TKIP is sufficient. Table 3 below gives a detailed view of the pros and cons of IPsec and EAP authentication protocols in WLAN designs:

EAP provides three significant benefits over basic 802.11 security:

- The first benefit is the mutual authentication scheme, as described previously. This scheme effectively eliminates "man-in-the-middle (MITM) attacks" introduced by rogue access points and RADIUS servers.
- The second benefit is a centralized management and distribution of encryption keys. Even if the WEP implementation of RC4 had no flaws, there would still be the administrative difficulty of distributing static keys to all the access points and clients in the network. Each time a wireless device was lost, the network would need to be rekeyed to prevent the lost system from gaining unauthorized access.
- The third benefit is the ability to define centralized policy control, where session time-out triggers reauthentication and new key derivation.

6.3. EAP Authentication Protocols

Numerous EAP types are available today for user authentication over wired and wireless networks. Current EAP types include:

- EAP-Cisco Wireless (LEAP)
- EAP-Transport Layer Security (EAP-TLS)
- Protected EAP (PEAP)
- EAP-Tunneled TLS (EAP-TTLS)
- EAP-Subscriber Identity Module (EAP-SIM)

In the Cisco SAFE wireless architecture, LEAP, EAP-TLS, and PEAP were tested and documented as viable mutual authentication EAP protocols for WLAN deployments.

6.4. Cisco LEAP

Cisco LEAP is the widely deployed EAP type in use today in WLANs. LEAP supports all three of the 802.1X and EAP elements mentioned previously. With LEAP, mutual authentication relies on a shared secret, the user's logon password, which is known by the client and the network. As shown in Figure 3, the RADIUS server sends an authentication challenge to the client. The client uses a one-way hash of the user-supplied password to fashion a response to the challenge and sends that response to the RADIUS server. Using information from its user database, the RADIUS server creates its own response and compares that to the response from the client. When the RADIUS



server authenticates the client, the process repeats in reverse, enabling the client to authenticate the RADIUS server. When this is complete, an EAP-Success message is sent to the client and both the client and the RADIUS server derive the dynamic WEP key.

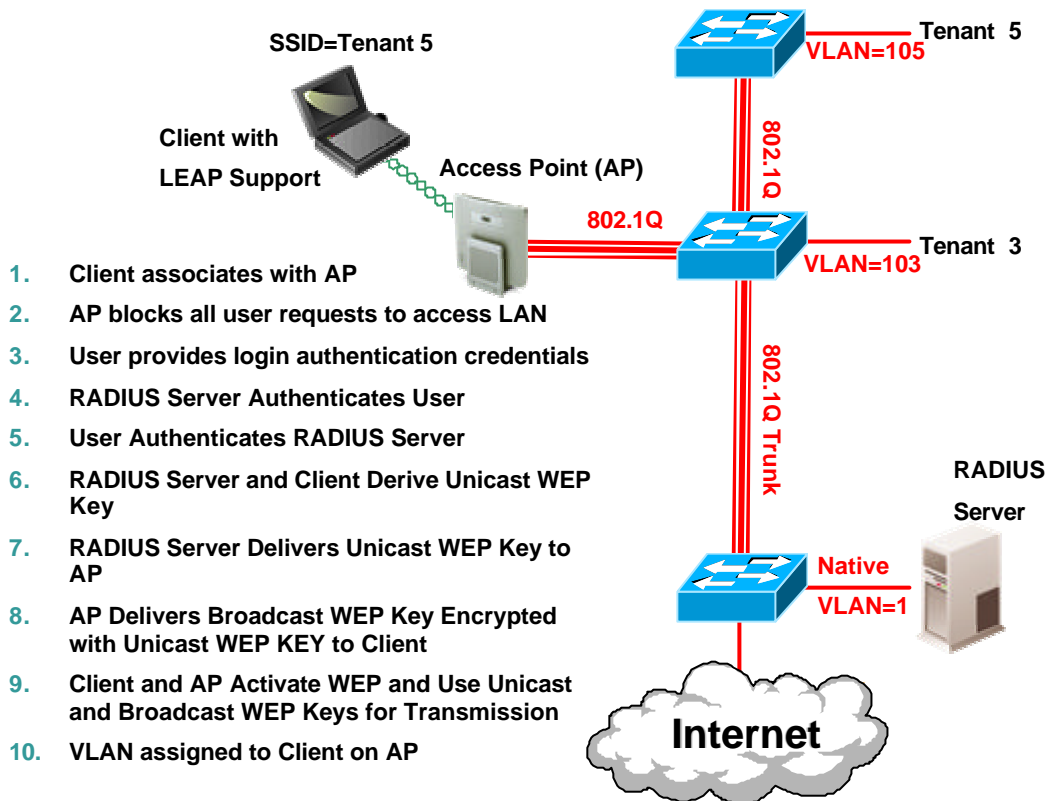


Figure 3 : LEAP Authentication process

6.5. Standard VPN WLAN Design Guidelines

WLAN access points connect to Layer-2 switches in the building module on a dedicated wired VLAN and forward IPsec traffic from the WLAN client. The traffic is kept separate from normal wired traffic until it is decrypted by the VPN termination device. It is important to point out that WEP is not enabled in this design. The wireless network itself is considered an untrusted network, suitable only as a transit network for IPsec traffic. In order to isolate this untrusted network, administrators should not mix the VLAN for the WLAN users with a wired network. This configuration would allow hackers on the wireless network to potentially attack users on the wired network. The WLAN clients associate with a wireless access point to establish connectivity to the building network at Layer-2. The wireless clients then use DHCP and DNS services in the server module to establish connectivity to the building network at Layer-3. After the initial Layer-3 configuration, the VPN tunnel authenticates to the VPN gateway. The VPN gateway can use digital certificates or preshared keys for wireless device authentication. If the VPN gateway uses preshared keys for authentication, then OTPs are recommended to authenticate users to it. Without OTP, the VPN gateways are open to brute-force login attempts by hackers who have obtained the shared IPsec key used by the VPN gateway. The VPN gateway takes advantage of RADIUS services, which in turn contact the OTP server for user authentication. The VPN gateway uses DHCP for IP address configuration in order for the WLAN client to communicate through the VPN tunnel. Security in the design is maintained by preventing network access if a VPN gateway or RADIUS service fails. Both services are required in order for the client to reach the wired network with production traffic. It should be noted that when the wireless client is communicating with the building network, but before the IPsec tunnel is established, the client traffic is not considered secure. All the noted WLAN security issues are still present until the wireless client can secure communications with an IPsec VPN. Therefore, three mitigation techniques are recommended:



First, the access point should be configured with EtherType, protocol, and port filters based on a company's wireless usage policy. SAFE WLAN recommends restrictive filters that allow only the necessary protocols required for establishing a secure tunnel to a VPN gateway. These protocols include DHCP for initial client configuration; DNS for name resolution of the VPN gateways; the VPN-specific protocols, IKE (User Datagram Protocol [UDP] port 500) and ESP (IP Protocol 50), and ICMP for troubleshooting purposes. Even with this filtering, the DNS and DHCP servers are still open to direct attack on the application protocols themselves. Extra care should be taken to ensure that these systems are as secure as possible at the host level. This includes keeping them up-to-date with the latest OS and application patches and running a host-based intrusion detection system (HIDS). Additionally, recent models of access layer switches have the capability to implement a technology called VLAN ACL (VACL). Implementing VACLs for VPN-related protocols and specific IP addresses of the VPN concentrators can provide an additional layer of filtering to guarantee that only IPsec traffic destined for the appropriate enterprise VPN concentrators crosses the switch. The DNS traffic is optional, dependent on whether the VPN client needs to be configured with a DNS name for the VPN gateway or if only an IP address is suitable. It is recommended that ICMP be allowed only to the outside interface of the VPN concentrator for troubleshooting purposes and path maximum-transmission-unit (MTU) discovery.

Secondly, a VPN client feature automatically establishes a tunnel when the correct WLAN IP address is received from DHCP. This feature eliminates the need for the end user to manually establish the VPN tunnel after the computer startup. Third, personal firewall software is included on the wireless client to protect the client while it is connected to the untrusted WLAN network without the protection of IPsec. In general terms, the VPN gateway delineates between the trusted wired network and the untrusted WLAN. The wireless client establishes a VPN connection to the VPN gateway to start secure communication to the corporate network. In the process of doing so, the VPN gateway provides device and user authentication via the IPsec VPN. Split tunneling by the client should be disabled—all traffic must traverse the tunnel.

Table 3 : Wireless Encryption Technology Comparison

	Cisco LEAP with TKIP	EAP-TLS with TKIP	EAP-PEAP with TKIP	IPsec-based VPN
Key length (in bits)	128	128	128	168/128, 192, 256
Encryption algorithm	RC4	RC4	RC4	3DES or AES
Packet integrity	CRC-32/MIC	CRC-32/MIC	CRC-32/MIC	MD5-HMAC/ SHA-HMAC
Device authentication	No	Certificate	No	Pre-shared secret or certificates
User authentication	Username/ password	Certificate	Username/ password or OTP	Username/ Password or OTP
Certificate requirements	None	RADIUS server/ WLAN client	RADIUS server	Optional
User differentiation¹	Group	Group	Group	User
Single sign-on support	Yes	Yes	No	No
ACL requirements	Optional	Optional	Optional	Required
Additional hardware	No	Certificate server	Certificate server	IPsec Concentrator
Per-user keying	Yes	Yes	Yes	Yes
Protocol support	Any	Any	Any	IP unicast
Client OS support	Wide range	Wide range	Wide range	Wide range
Open standard	No	Yes	IETF draft RFC	Yes



7. User Authentication Procedures

One of the major design aspects of wireless as a base building service is login security. This section describes the issues and options for how tenants log into the building wireless system and subsequently connect to their corporate network. Authentication is also closely related to IP address assignment with DHCP and logging in to a Windows Primary Domain Controller (PDC). The different scenarios that have been tested in the Cisco Proof-of-Concept labs are:

- Tenant has no authentication servers.
- Tenant uses Windows Primary Domain Controller for authentication
- Tenant has their own RADIUS server for authentication.
- Authentication services for Guest Users

The following diagram will be used as a reference for the different options described. In the appendices you will find a complete example of these deployment scenarios including configuration for the switches, the access point, and the RADIUS server.

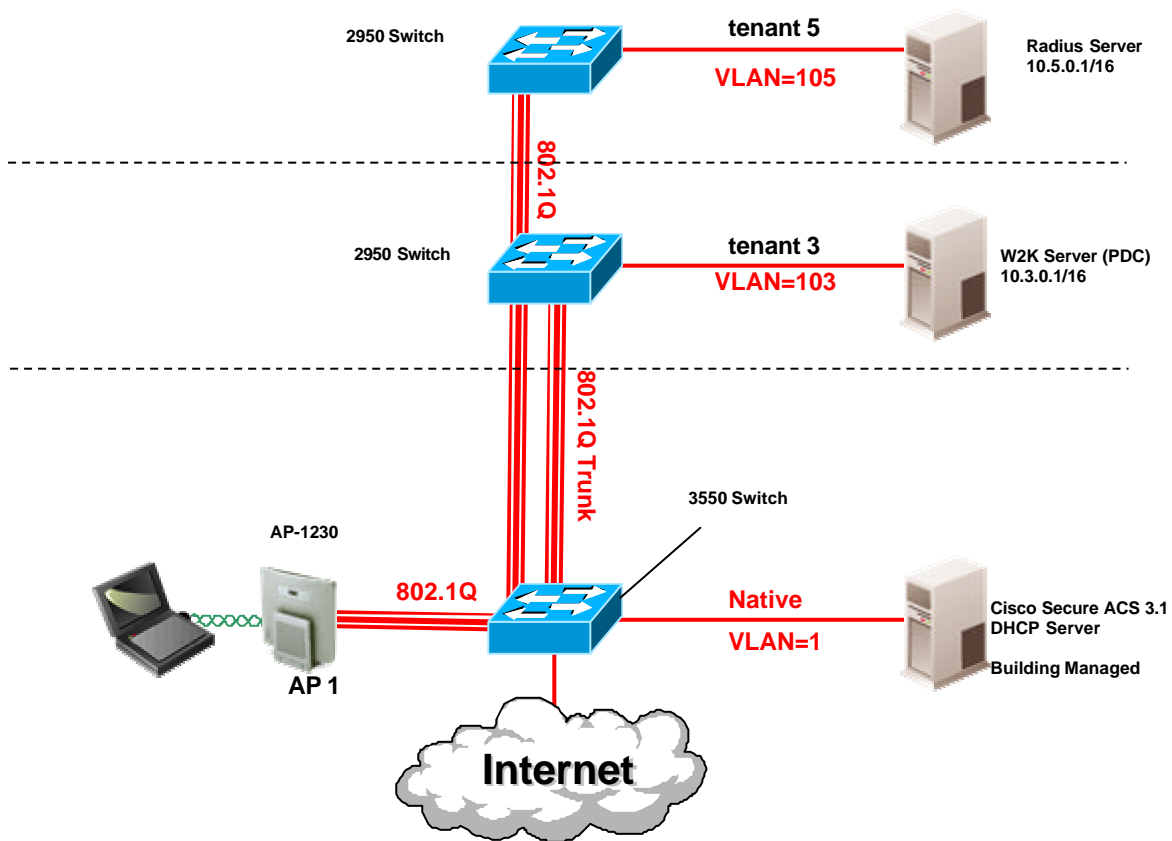


Figure 4 :Network with differing types of authentication servers

7.1. Tenant has no authentication servers

In this case a smaller tenant has no authentication mechanism in their network. Typically the network would be used to access printers and get out onto the Internet. With the building wireless system a user needs to prove they have the right to access a certain VLAN before we allow them on the system. For this the building has it's own RADIUS server that is LEAP compatible. This allows even tenants that do not have their own security systems to benefit from the strongest wireless security protocol available.



To provide this service the access point talks to the building managed RADIUS server on the native VLAN (VLAN 1 in the above diagram). The RADIUS server stored the user names and passwords. Once the user has been authenticated they will simply be on their own VLAN.

Consider just the initial authentication portion for Tenant 3 in the above diagram (that is authenticating to the building RADIUS server ignoring the authentication to the Window PDC). We need the following configuration elements on the access point. First, under the Dot11Radio0 interface and then under the tenant3 ssid we assign the vlan to use and the method to authenticate for LEAP access. In this case we use a method list called **eap_methods**. This method list is used for login under **the aaa authentication** statement and is referred to the **rad_eap** group. The **rad_eap** group will be used for any tenant that needs to use the building RADIUS server for initial authentication. In the **aaa group server** statement we give the IP address of the server. The AP has a direct connection (no routing required) to the building RADIUS server because it is on the native VLAN and so is the AP.

```
aaa group server radius rad_eap server 172.16.200.1 auth-port 1645 acct-port 1646

aaa authentication login eap_methods group rad_eap

interface Dot11Radio0
  ssid tenant3
  vlan 103
  authentication network-eap eap_methods
```

7.2. Tenant has their own RADIUS server

If a tenant has their own Radius server which they want to use in place of the building RADIUS server we can use a separate aaa group server statement to allow the AP to point directly to the tenant RADIUS server for authentication for that particular SSID. This is the case in the example diagram for tenant 5. The authentication statements mirror those for the building RADIUS server.

```
aaa group server radius rad_tenant5 server 10.5.0.1 auth-port 1645 acct-port 1646

aaa authentication login tenant5_methods group rad_tenant5

interface Dot11Radio0
  ssid tenant5
  vlan 105
  authentication network-eap tenant5_methods
```

There are a few additional consequences of using a tenant RADIUS server.

- Because the AP needs to be able to communicate with the tenant RADIUS server we must configure a default gateway to which we will send packets to be routed. This default gateway will generally be the 3550 switch because it will be configured for routing. It could, however, be any device that has the ability to forward packets to the tenant RADIUS server. The command to set the default gateway is global on the AP.

```
ip default-gateway 172.16.210.1
```

- The tenant RADIUS server will need to know who to send the response packets back to. For this it is easier to design the system so that the access points use a single, consistent address as their source address in the RADIUS protocol exchange. This will be the address they use on the native VLAN (VLAN 1 in the diagram). The command to set this is



ip radius source-interface BV11

- Routing must be turned on in the 3550 and the tenant VLAN subnet must not conflict with any other subnets that the 3550 must route to. If two tenants choose the same private address space then IOS will not allow them to both be configured for routing.
- Because routing has been enabled on the 3550 we must add appropriate access lists and other security mechanisms so that packets cannot pass from one tenant VLAN to another. See the appendices for examples of such access lists.
- Once the user is authenticated by the tenant RADIUS sever they will be assigned to the appropriate VLAN. Now routing is no longer an issue. The user machine will make a broadcast request to find a DHCP server. This DHCP server must be present on the tenant VLAN to respond to the request. Normal configuration rules for DHCP apply.

7.3. Tenant uses a Windows PDC for authentication

The LEAP login process has several phases. First there is user authentication, then the user obtains an IP address with DHCP, finally the user will log into a Window PDC if that has been configured in the ACU. If the user wants to log in to the local machine then this final step will be skipped (it will also not apply to non-Windows machines such as Apple OS-10 and Linux machines running the ACU). There exist two variants on this scenario: First, the tenant does not have a RADIUS authenticator and second, the tenant has their own RADIUS authenticator.

The Windows PDC is used only for access to resources in the Windows network. It has nothing to do with authentication for access to the building wireless network. This is why these two authentications are really separate, but we may want to make them look like single login for user convenience.

7.3.1. Tenant does not have a RADIUS sever

In this case no routing is required. Once the user is authenticated by the building RADIUS server the user is dropped into their own VLAN. This also means there are no restrictions on IP addressing for the tenant VLAN. The tenant would have to provide their own DHCP server to hand out IP addresses to clients as they connect. One key element is if we want a transparent login process then the windows user name and password must be the same in the PDC and on the building RADIUS server. If the Windows password is modified without changing the one in the building's RADIUS server then the user will see that they can log in when they are connected to wired LAN, but not when they try to log into the wireless system..

7.3.2. Tenant provide their own RADIUS server

If the tenant provides their own RADIUS and DHCP servers then we do not have the issue of keeping the building RADIUS server database synchronized with the Windows PDC. However, since we are requiring the access points to send RADIUS authentication requests directly to a tenant server we have to comply with all the rules described in section 7.2.

7.4. Authentication for Guest users

Often the guest VLAN will be administered by a HotSpot provider. This provider will typically put a Linux or other box on the connection to the Internet. This will stop users and let them provide their login credentials or payment details before the user gets access to the Internet. This machine will usually supply IP addresses to guest users using DHCP. If this is the case there is no special configuration required. The guest VLAN uses open authentication as far as wireless goes. Users who need data privacy will need to use a VPN client to connect to their corporate network.

In the case where the guest VLAN needs the building to provide an IP address the building RADIUS server can be configured to also be a DHCP server. There is no authentication on the guest VLAN so users are immediately dropped into the VLAN (VLAN 99 in our example). The user's machine will send a broadcast out to find a DHCP server. Since there is no DHCP server on VLAN 99 the 3550 will need to forward the DHCP request to the RADIUS server, on the native VLAN (VLAN 1), using a DHCP helper command. The 3550 will need



routing enabled so that DHCP responses can be passed back to the guest user's machine. If access lists are being used to prevent inter-VLAN traffic then an exception will have to be made for DHCP to permit it between the native and guest VLANs.

8. Provisioning and Management

The Wireless Service Manager will need to change the configurations of access points and, in some cases, switches as tenants move in and out. This is to ensure that only authorized tenants can access the building wireless system. If some tenants do not have their own authentication mechanism, but still want strong security procedures then the Wireless Service Manager may need to manage a database of users for that tenant. This database will need to be updated as employees of the tenant change. The following sections outline the procedures that may be necessary are tenant and tenant employees change.

8.1. Tenant Provisioning

Adding or removing a tenant from the system will require the changes listed below. Note that one could easily design management systems and procedures to automate these changes or even render them unnecessary.

- Add a new SSID and VLAN for the tenant in all the access points.
- Assign ports in floor switches to the new VLAN
- Turn off ports that are not required.
- Create an authentication policy.
- Configure access points to implement the authentication policy.
- Configure routing rules in the routing switches to allow the authentication policy.
- Add appropriate access lists to implement security for the new VLAN

It is recommended that when a tenant leaves that access to the unused VLAN is disabled.

8.2. User Provisioning

If the building RADIUS server is used by a tenant for user authentication then a new users will have to be added when a new employee arrives. There will need to be a mechanism for the employee to change their password. A user will need to be deleted from the system when the employee leaves.

8.3. Large Scale Deployments

For small deployments standard network management tools such as Cisco Works may be sufficient. However, to manage large numbers of access points it may be useful to deploy specialized WLAN management tools. Cisco has released such a tool under the name CiscoWorks Wireless LAN Solution Engine. Tools may also become available from other software vendors.

There are three main areas that need to be addressed when managing large numbers of access points: configuration management, fault reporting, and report generation. For interested readers, the following section is derived from the CiscoWorks WLSE data sheet and give an idea of the types of functions typically used for large scale deployments. The mapping of the features to these three key management areas is shown. A link to the complete documentation can be found in the References section.

8.3.1. CiscoWorks WLSE overview

Automation of Access Point Configuration - The CiscoWorks WLSE provides centralized template-based configuration for a large number of Cisco Aironet access points and bridges. Hierarchical, user-defined groups can be created in a flexible manner that can span multiple subnets to suit user needs. A configuration template with user-specified parameters can be applied to a group of access points and bridges on demand, or scheduled to run later. It supports an "undo" of the last configuration change. Configuration templates may be created using the CiscoWorks WLSE GUI or imported from a previously configured access point or bridge. Configuration parameter support can be



verified against different access point and bridge firmware releases. Customer defined configurations may be applied automatically to access points and bridges as soon as they are deployed on the network.

Access Point Performance and Fault Monitoring - The CiscoWorks WLSE provides centralized firmware updates to facilitate firmware changes on large numbers of access points and bridges. Access point and bridge images may be imported from Cisco.com and the CiscoWorks WLSE can be used as a central repository. Firmware updates can be initiated on demand, or scheduled to run later. Firmware can be updated using HTTP and SNMP protocols. The CiscoWorks WLSE generates alerts for security policy misconfigurations on Cisco Aironet access points and bridges, reducing potential security vulnerabilities.

The CiscoWorks WLSE configures and monitors VLANs on access points, allowing customers to differentiate LAN policies and services, such as security and QoS, for different users.

The CiscoWorks WLSE provides proactive fault and performance monitoring of Cisco Aironet access points, bridges, the ACS authentication server, and the switches connected to the access points. For access points and bridges, both Ethernet and radio ports can be monitored for availability, errors, and usage. The CiscoWorks WLSE also monitors the authentication response time from the ACS server by performing synthetic authentication transactions. For switches connected to access points, availability, port use, CPU, and memory use can be monitored. Filtering and sorting by fault priority is available to view and act upon selected faults.

The CiscoWorks WLSE provides a flexible way to define and clear fault conditions for monitored attributes and provides sufficient information for operational staff to easily pinpoint a problem source. Administrators can set up fault and performance thresholds for the monitored attributes with specified actions and fault priorities. Fault forwarding and notification can be done via syslog message, SNMP trap or e-mail. Group level polling enables users to have different policies and polling profiles for different sets of devices.

The CiscoWorks WLSE has a flexible, role-based user access model. Pre-defined and administrator defined access roles control user feature access on the CiscoWorks WLSE. For example, help desk personnel can be limited by access role to only view reports and faults. Authorized users can configure, monitor, and generate reports for the WLAN infrastructure, even through firewalls.

Historical Trend and Performance Reporting -The CiscoWorks WLSE offers many predefined reports for access points and bridges. This includes summary reports (IP address, SSID, firmware version, number of clients and, etc., detailed reports (Ethernet or Radio port status, errors, encryption details, etc.), ACS authentication reports (server, port, and server priority), client association reports, and usage reports. Reports are available at both the group level and the individual access point or bridge level. Group usage reports show bandwidth and client association for access points. These reports can be used for capacity planning by monitoring which access points are consuming the most bandwidth and have the largest number of clients. Historical packet and error reports for access points and bridges are also provided.

The CiscoWorks WLSE provides current and historical client association reports accessible by client Media Access Control (MAC) address and name. Since wireless clients can be anywhere, these reports assist in troubleshooting by providing historical access point associations for the client. Client detail reports (MAC address, IP address, state, type, and associated access point), and client statistics reports (errors, packets, signal strength and quality, etc.) are also provided. Reports can be scheduled to be periodically emailed.

9. Solution Design Limitations

9.1. Large Buildings

Problem: For a small building you can easily assign one VLAN per tenant. The 16 VLAN limitation on the access points makes this solution difficult to scale to a large building. The most difficult areas are common areas (gardens, restaurants, cafes) where tenants from any floor may want to work.

Workarounds: cover each area with two or more access points each of which services 16 tenants. For .11b based systems with three channels available this means that a common area can support up to 44 tenants and a guest VLAN. One VLAN is reserved for the native VLAN on each access point. This is used for management. For .11a systems with eight channels this would permit 119 tenants and guest access. If both are used then we have a maximum of 164 tenants and guest (assuming guest access uses a single .11b VLAN).



9.2. Roaming

Problem: This design does not provide for VPN services. It would be a logical extension to the mobility concept have a VPN server, but this requires much more management and integration with the tenant authentication servers.

Workarounds: Tenants or the building provide VPN services.

10. Further Reading

Wireless Quality-of-Service Deployment Guide

http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_technical_reference09186a0080144498.html

Wireless Virtual LAN Deployment Guide

http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_technical_reference09186a00801444a1.html

Cisco Aironet 1200 Series – Configuring VLANS

http://www.cisco.com/en/US/products/hw/wireless/ps430/products_installation_and_configuration_guide_chapter09186a00801486a1.html

SAFE: Wireless LAN Security in Depth

http://www.cisco.com/en/US/netsol/ns110/ns129/ns131/ns128/networking_solutions_implementation_white_paper09186a008009c8b3.shtml

Configuration Guides for VLANs on the 3550

http://www.cisco.com/en/US/products/hw/switches/ps646/products_configuration_guide_chapter09186a00800c6f52.html

Configuring Network Security with Access Control Lists on the 3550

http://www.cisco.com/en/US/products/hw/switches/ps646/products_configuration_guide_chapter09186a00800c6f59.html

Configuring VLANs on the 2950

http://www.cisco.com/en/US/products/hw/switches/ps628/products_configuration_guide_chapter09186a008007e91e.html

CiscoWorks Wireless Lan Solutions Engine

<http://www.cisco.com/warp/public/cc/pd/cxsr/1105/ps3915/index.shtml>

Many of the configuration guides will change with software versions. Check the URLs above to make sure they match the software version you are using on the access points and switches.



11. Appendix A: VLAN Configuration Example for Aironet IOS Software Release 12.2.4-JA for Cisco Aironet 1230 Series Access Points

11.1. Reference Diagram

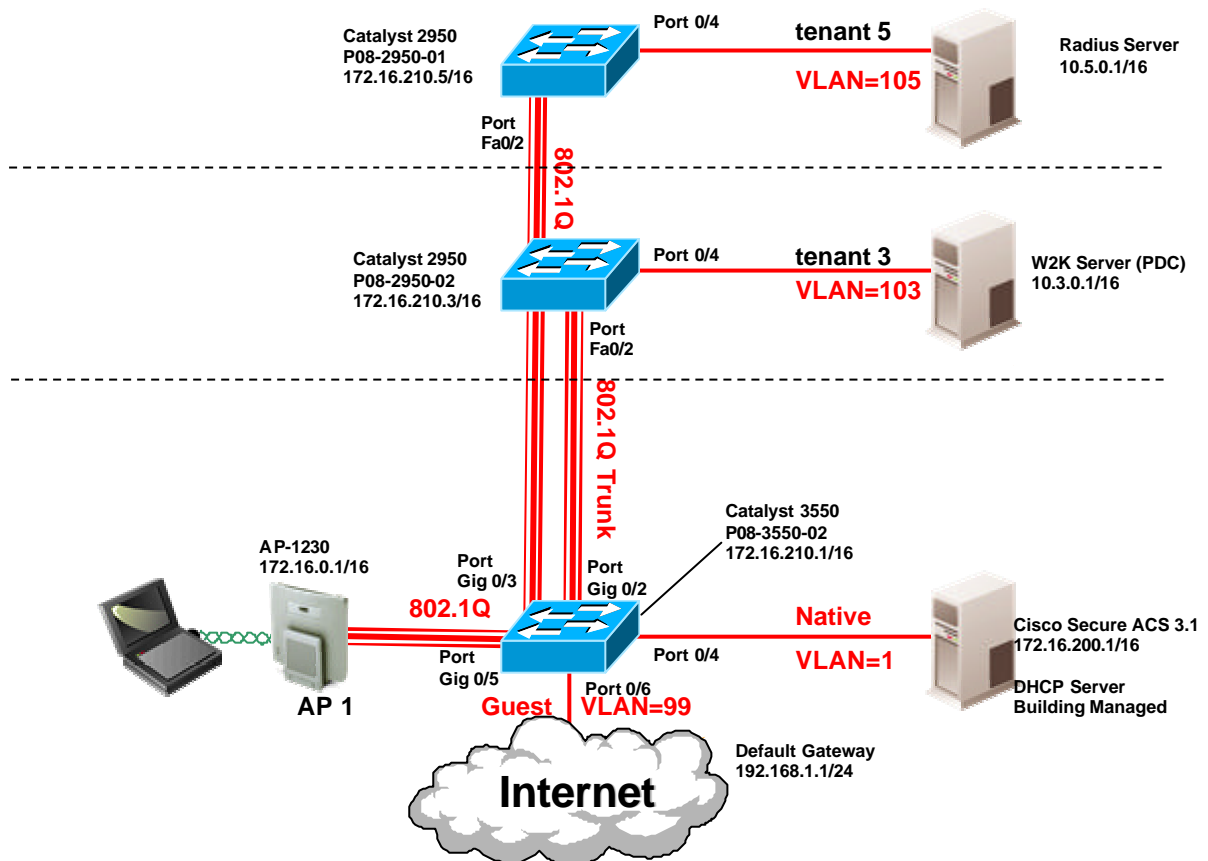


Figure 5 : Reference network for extracted configuration files

11.2. Access Point Configuration

```
AP1230-1#sh run
Building configuration...

Current configuration : 4318 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname AP1230-1
!
aaa new-model
!
!
```



```
aaa group server radius rad_eap server 172.16.200.1 auth-port 1645 acct-port 1646
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin server 172.16.200.1 auth-port 1645 acct-port 1646
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius rad_tenant5 server 10.5.0.1 auth-port 1645 acct-port 1646
!
aaa authentication login default local group tac_admin group rad_admin
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authentication login tenant5_methods group rad_tenant5
aaa authorization exec default local group tac_admin group rad_admin
aaa authorization ipmobile default group rad_pmip
aaa accounting network acct_methods start-stop group rad_acct
aaa session-id common
!
username Cisco password 7 14341B180F0B
username admin privilege 15 password 7 01100F175804
ip subnet-zero
!
dot11 holdoff-time 600
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 encryption vlan 103 key 1 size 128bit 7 79D43D513A6A68F60FE65FD36A5E transmit-key
 encryption vlan 103 mode wep mandatory mic key-hash
!
 encryption vlan 105 key 1 size 128bit 7 FD494BE43EC57CF2595C25382FE2 transmit-key
 encryption vlan 105 mode wep mandatory mic key-hash
!
 broadcast-key vlan 103 change 3600
 broadcast-key vlan 105 change 3600
!
 ssid guest
  vlan 99
  authentication open
  guest-mode
!
 ssid tenant3
  vlan 103
  authentication network-eap eap_methods
!
```



```
ssid tenant5
  vlan 105
  authentication network-eap tenant5_methods
!
speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
rts threshold 2312
station-role root
no cdp enable
!
interface Dot11Radio0.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio0.99
 encapsulation dot1Q 99
 no ip route-cache
 bridge-group 99
 bridge-group 99 subscriber-loop-control
 bridge-group 99 block-unknown-source
 no bridge-group 99 source-learning
 no bridge-group 99 unicast-flooding
 bridge-group 99 spanning-disabled
!
interface Dot11Radio0.103
 encapsulation dot1Q 103
 no ip route-cache
 bridge-group 103
 bridge-group 103 subscriber-loop-control
 bridge-group 103 block-unknown-source
 no bridge-group 103 source-learning
 no bridge-group 103 unicast-flooding
 bridge-group 103 spanning-disabled
!
interface Dot11Radio0.105
 encapsulation dot1Q 105
 no ip route-cache
 bridge-group 105
 bridge-group 105 subscriber-loop-control
 bridge-group 105 block-unknown-source
 no bridge-group 105 source-learning
 no bridge-group 105 unicast-flooding
 bridge-group 105 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
!
```



```
interface FastEthernet0.1
  encapsulation dot1Q 1 native
  no ip route-cache
  bridge-group 1
  no bridge-group 1 source-learning
  bridge-group 1 spanning-disabled
!
interface FastEthernet0.99
  encapsulation dot1Q 99
  no ip route-cache
  bridge-group 99
  no bridge-group 99 source-learning
  bridge-group 99 spanning-disabled
!
interface FastEthernet0.103
  encapsulation dot1Q 103
  no ip route-cache
  bridge-group 103
  no bridge-group 103 source-learning
  bridge-group 103 spanning-disabled
!
interface FastEthernet0.105
  encapsulation dot1Q 105
  no ip route-cache
  bridge-group 105
  no bridge-group 105 source-learning
  bridge-group 105 spanning-disabled
!
interface BVI1
  ip address 172.16.0.1 255.255.0.0
  no ip route-cache
!
ip default-gateway 172.16.210.1
ip http server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
/ivory/1100
ip http authentication aaa
ip radius source-interface BVI1
radius-server host 172.16.200.1 auth-port 1645 acct-port 1646 key 7 02050D480809
radius-server host 10.5.0.1 auth-port 1645 acct-port 1646 key 7 070C285F4D06
radius-server retransmit 3
radius-server attribute 32 include-in-access-req format %h
radius-server vsa send accounting
bridge 1 route ip
!
line con 0
line vty 5 15
!
end
```

11.3. Routing Switch Configuration

```
p08-3550-2#sh run
```



Building configuration...

Current configuration : 1834 bytes

```
!  
version 12.1  
no service pad  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname p08-3550-2  
!  
!  
ip subnet-zero  
ip routing  
ip dhcp excluded-address 192.168.1.254  
ip dhcp excluded-address 192.168.1.253  
ip dhcp excluded-address 192.168.1.1 192.168.1.29  
!  
!  
spanning-tree extend system-id  
system mtu 1550  
!  
!  
interface GigabitEthernet0/1  
  no ip address  
!  
interface GigabitEthernet0/2  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
  no ip address  
!  
interface GigabitEthernet0/3  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
  no ip address  
!  
interface GigabitEthernet0/4  
  switchport mode access  
  no ip address  
!  
interface GigabitEthernet0/5  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
  no ip address  
!  
interface GigabitEthernet0/6  
  no ip address  
!  
interface GigabitEthernet0/7  
  switchport mode access  
  no ip address  
!  
interface GigabitEthernet0/8  
  switchport access vlan 103
```



```
switchport mode access
no ip address
!
interface GigabitEthernet0/9
no ip address
!
interface GigabitEthernet0/10
no ip address
!
interface GigabitEthernet0/11
no ip address
!
interface GigabitEthernet0/12
no ip address
!
interface Vlan1
ip address 172.16.210.1 255.255.0.0
ip access-group 100 in
!
interface Vlan99
ip address 192.168.1.254 255.255.255.0
ip access-group 100 in
ip helper-address 172.16.200.1
!
interface Vlan103
ip address 10.3.0.254 255.255.255.0
ip access-group 100 in
!
interface Vlan105
ip address 10.5.0.254 255.255.255.0
ip access-group 100 in
!
ip classless
ip http server
!
!
!
access-list 100 permit udp 172.16.0.0 0.0.255.255 any eq 1645
access-list 100 permit udp any eq 1645 172.16.0.0 0.0.255.255
access-list 100 permit udp any any eq bootps
access-list 100 permit udp any any eq bootpc
!
line con 0
line vty 5 15
!
end
```

11.4. Layer-2 switch configurations

```
p08-2950-2#sh run
Building configuration...
```



```
Current configuration : 1540 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname p08-2950-2
!
!
ip subnet-zero
!
spanning-tree extend system-id
!
!
interface FastEthernet0/1
  no ip address
!
interface FastEthernet0/2
  switchport mode trunk
  no ip address
!
interface FastEthernet0/3
  no ip address
!
interface FastEthernet0/4
  switchport access vlan 103
  switchport mode access
  no ip address
!
!
interface Vlan1
  ip address 172.16.210.3 255.255.0.0
  no ip route-cache
!
ip http server
!
!
line con 0
line vty 5 15
!
end

p08-2950-2#
```

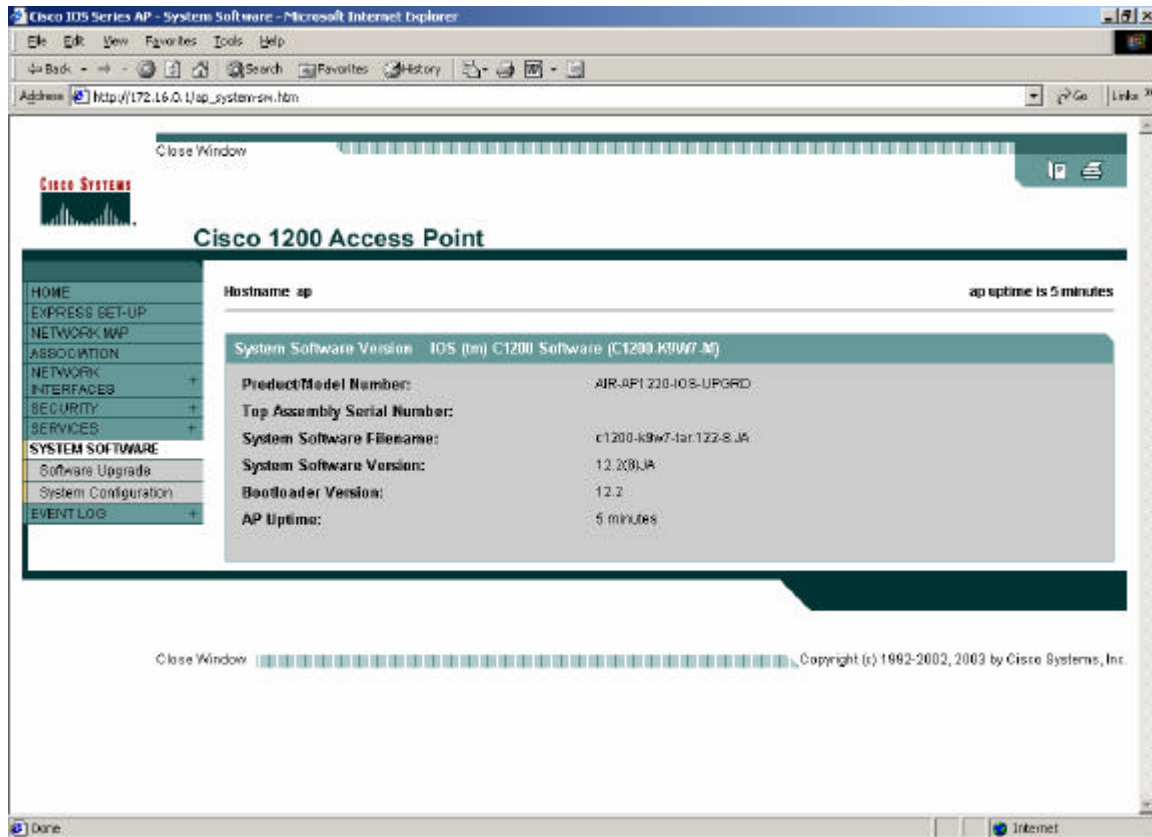


11.5. Using the Access Point Graphical User Interface

This section shows some of the key screens used to configure the VLANs for the guest VLAN (99) and the tenant 3 VLAN (103). The GUI was used to generate the configuration for the access point shown in section 11.2.

11.5.1. Checking the Software Version Numbers

The following screen is found under the **System Software** header on the left side. It shows the software version. This is the version used for the labs from which this design guide was created.

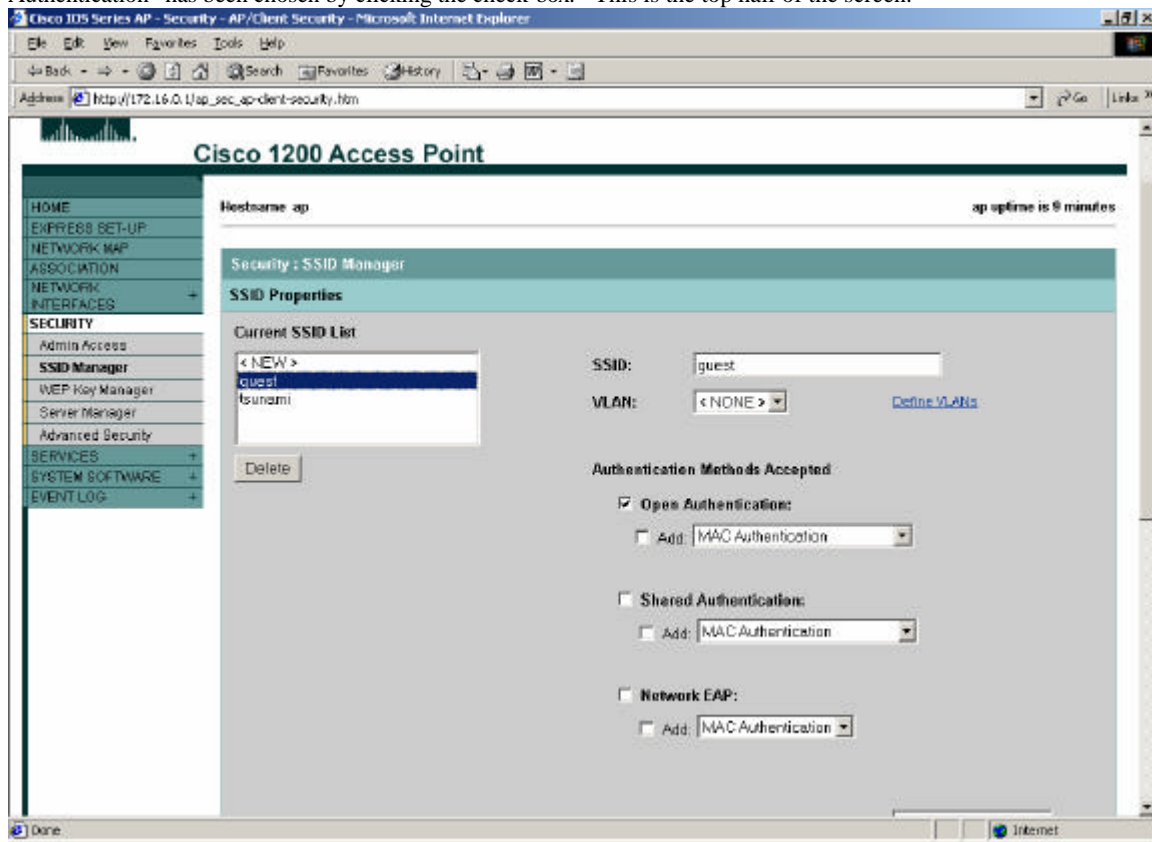


11.5.2. Configuring the Guest VLAN

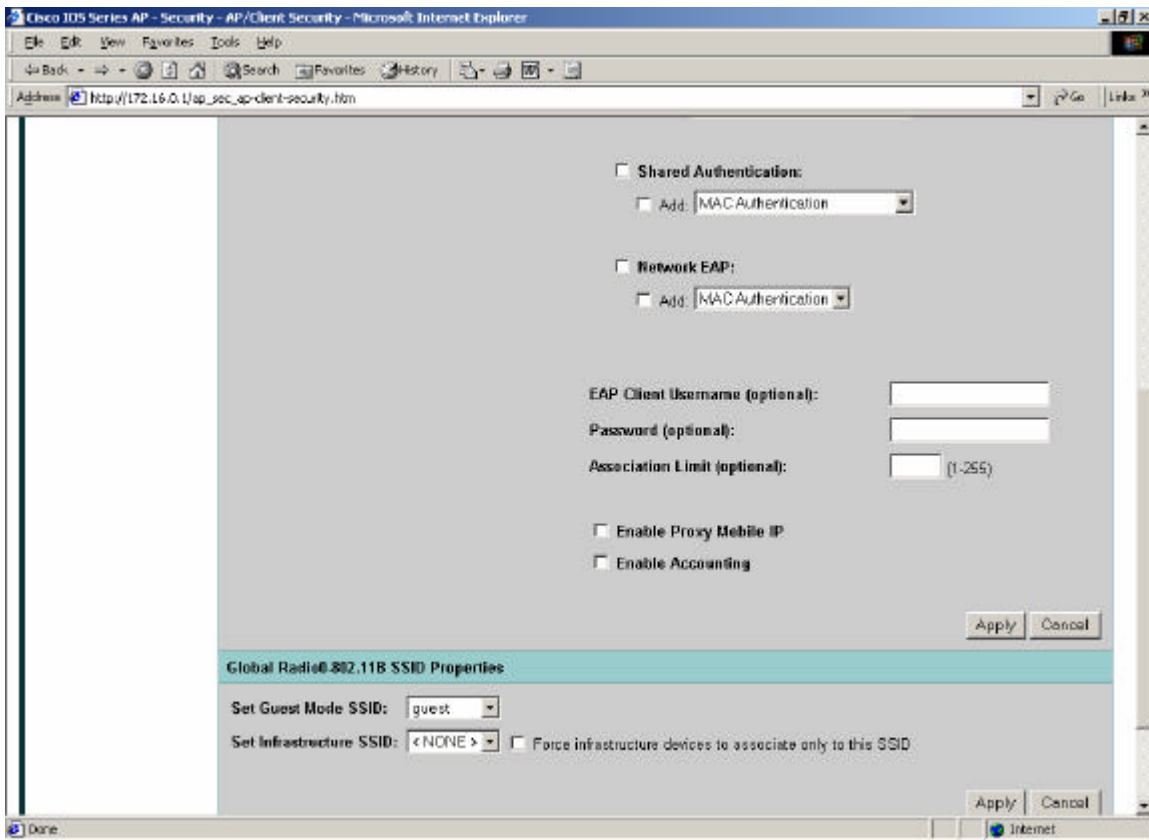
The guest VLAN has two special characteristics: it uses Open authentication and has "guest-mode" enabled so that clients can associate even if they do not have an SSID configured.



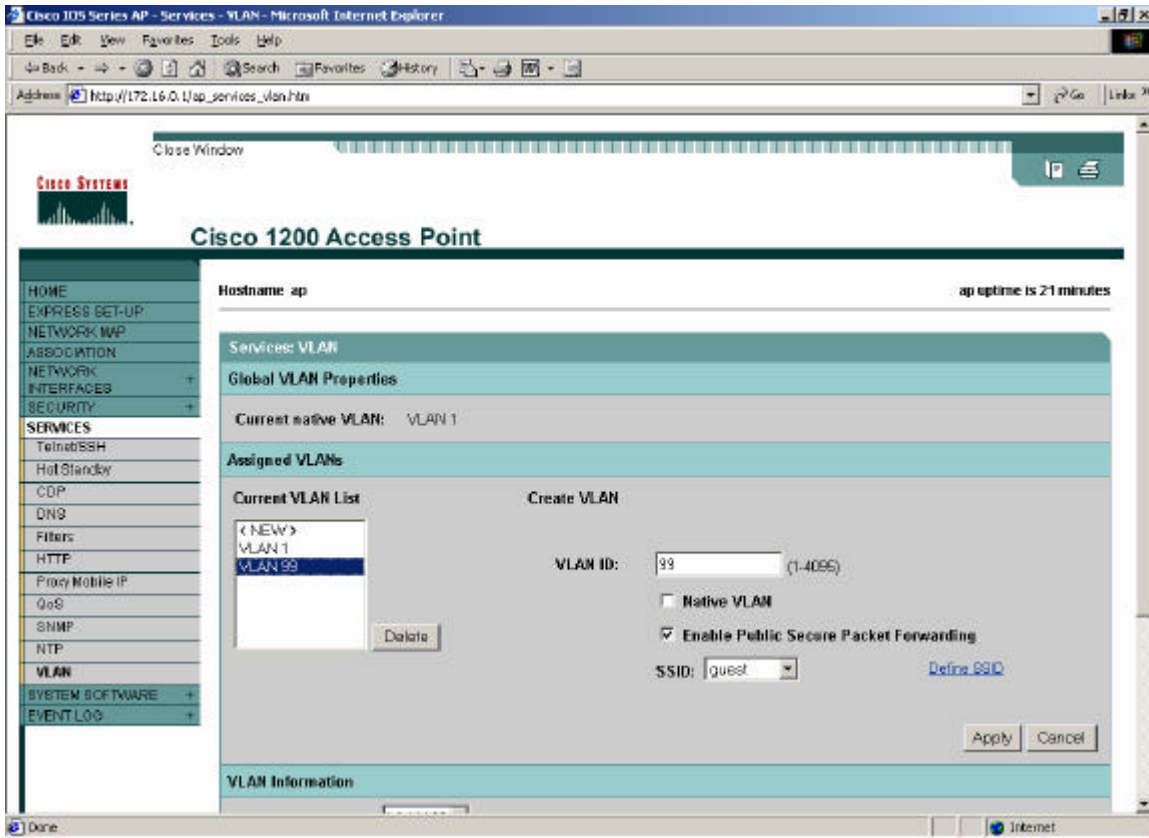
The following screen shows the **SSID Manager** screen under the **Security** header. It shows the guest SSID and that “Open Authentication” has been chosen by clicking the check-box. This is the top half of the screen.



The bottom half of the screen has the drop menu where we can set the “guest mode” option as shown.

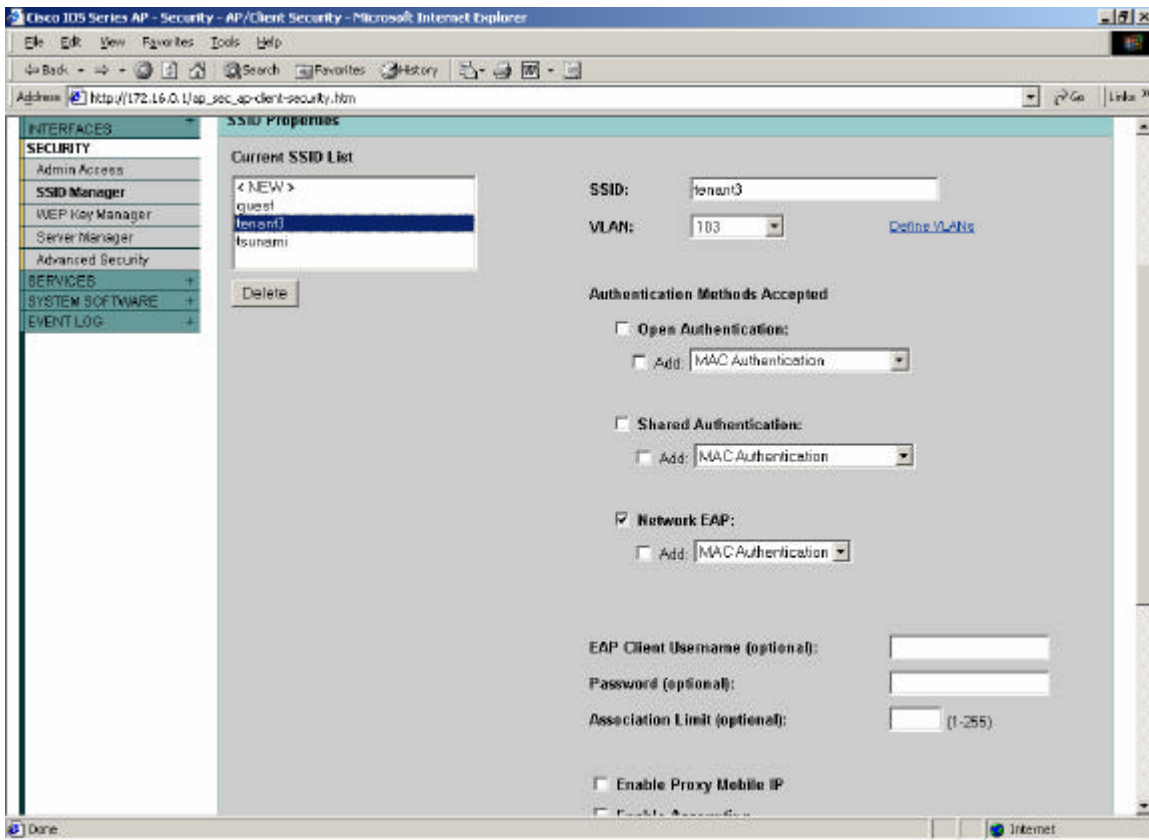


Under the Services header with the VLAN screen we are able to associate the VLAN number 99 with the SSID “guest” that we have set up. The “Enable Public Secure Packet Forwarding” prevents clients from talking directly to each other, but did interact with the bridging and routing configuration so should be tested before use. Actual configuration used for this document did not use this option.

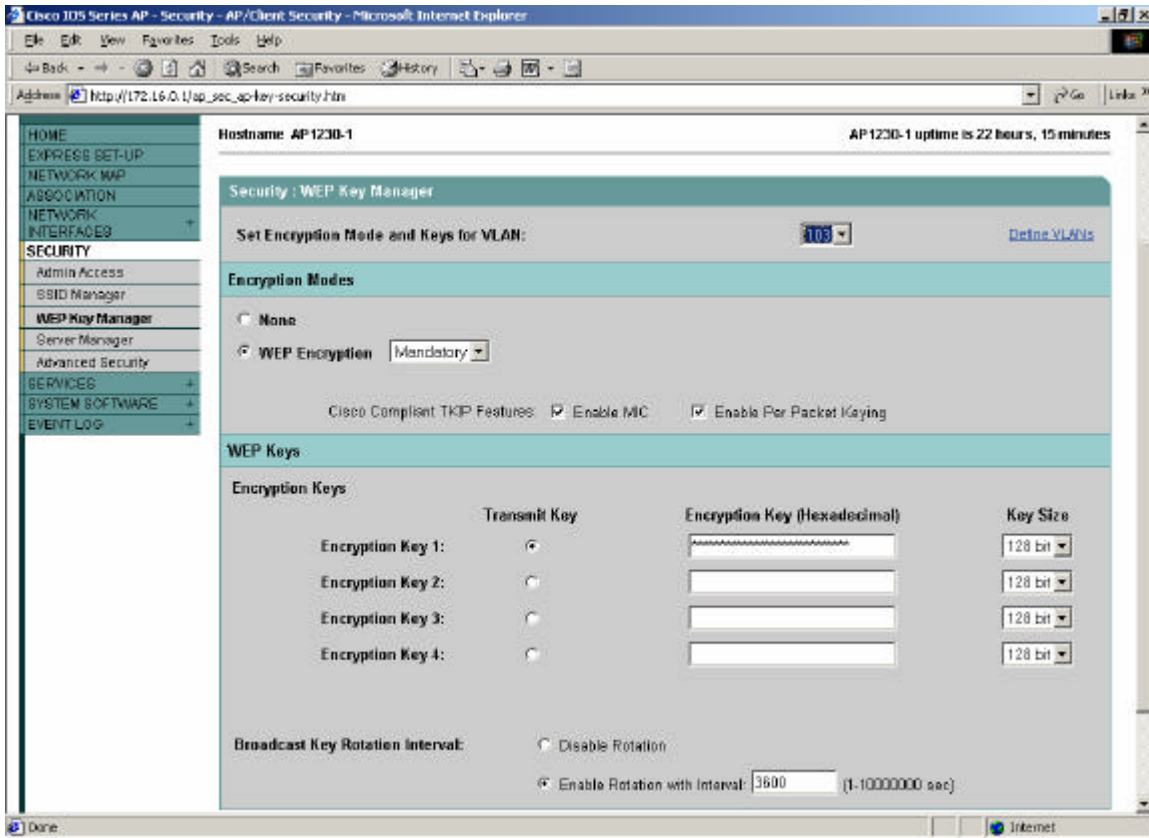


11.5.3. Configuring the VLAN for tenant 3

The following screen shows the mapping of the tenant 3 SSID to their VLAN (103). This tenant uses Cisco LEAP for authentication so we check the **Network EAP** authentication method.



Even though we are using LEAP which creates dynamic encryption keys we need to set a WEP key in the configuration. This key can be an arbitrary value. In the following screen we also enable broadcast key rotation every hour.



11.5.4. Configuring a Building Managed RADIUS Server

The following screen configures the AP to talk to the building RADIUS server.



Cisco IOS Series AP - Security - Server Based Security - Microsoft Internet Explorer

Address: http://172.16.0.1/ap_sec_network-security.htm

Security: Server Manager

Current Server List:

< NEW >	Server: 172.16.200.1 (Hostname or IP Address)	
Delete	Server Type: RADIUS	Shared Secret: *****
	Authentication Port (optional): (0-65535)	Accounting Port (optional): (0-65535)

Use Server for:

- EAP Authentication
- MAC Authentication
- Proxy Mobile IP Authentication
- Admin Authentication
- Accounting

Apply Cancel

Global Server Properties

Accounting Update Interval (optional): (1-2147483647 min)

TACACS+ Server Timeout (optional): DISABLED (1-1000 sec)

RADIUS Server Timeout (optional): DISABLED (1-1000 sec)

**Corporate Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright 2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0301R)