Lab 8.6.2 Configure VLANs on the AP

Estimated Time: 40 minutes

Number of Team Members: Students will work in teams of two.

Objective

The student will extend VLANs into a WLAN.

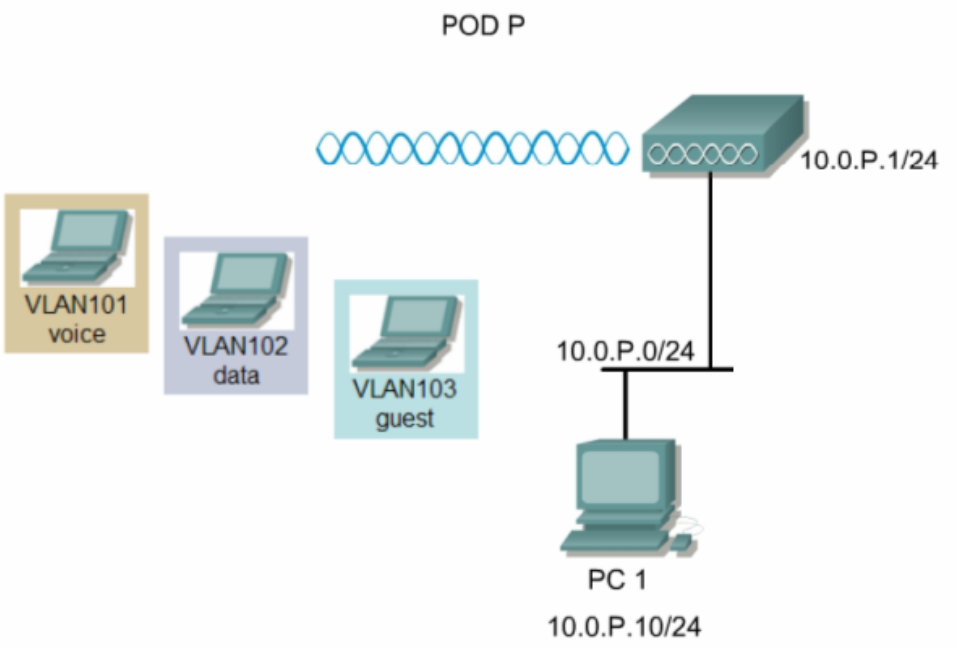
Scenario

VLANs can be extended into a WLAN by adding IEEE 802.11Q tag awareness to the AP. Frames destined for different VLANs are transmitted by the AP wirelessly on different SSIDs with different WEP keys. Only the clients associated with that VLAN receive those packets. Conversely, packets coming from a client associated with a certain VLAN are 802.11Q tagged before they are forwarded onto the wired network.

The basic wireless components of a VLAN consist of an AP and a client associated to it using wireless technology. The AP is physically connected through a trunk port to the network VLAN switch on which the VLAN is configured. The physical connection to the VLAN switch is through the AP Ethernet port. A router is also necessary to route between the different VLANs. Up to 16 SSIDs can be configured on the AP, hence 16 VLANs are supported. Configuring the AP to support VLANs is a three-step process:

1. Create SSIDs and assign authentication settings to SSIDs.
2. Assign SSIDs to VLANs and enable the VLAN on the radio and Ethernet ports.

Topology



Preparation

Team	Access Point Name	SSID	VLAN	Authentication	Bridge group	BVI Address
1	PodP	management voice data guest	10 101 102 103	Network EAP Shared Network EAP Open	1 101 102 103	10.0.P.1/24

Reset the AP to the default configuration.

Tools and Resources

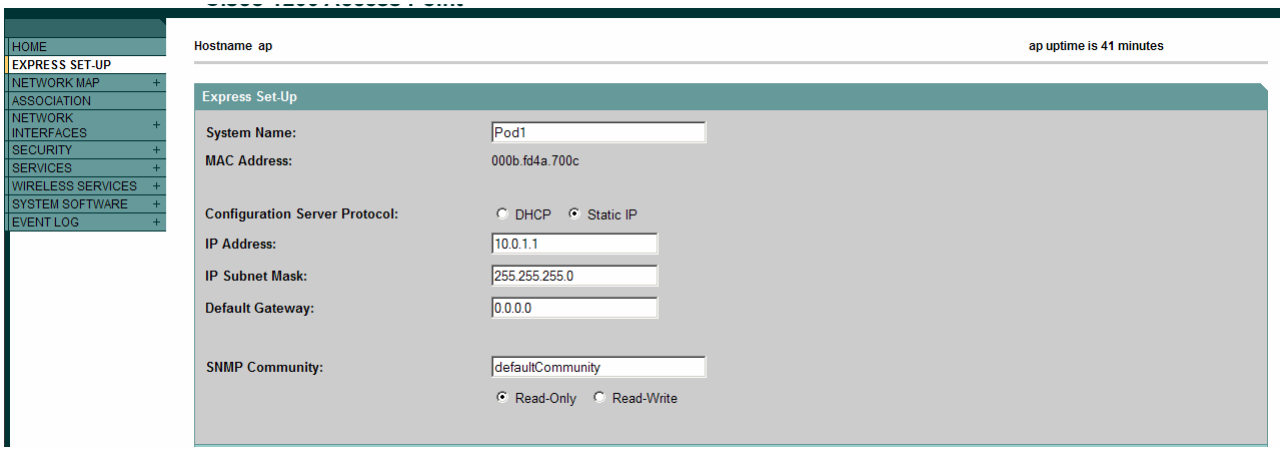
Each team will need:

- 1 AP
- 2 PCs or laptop
- Console cable

Additional Materials

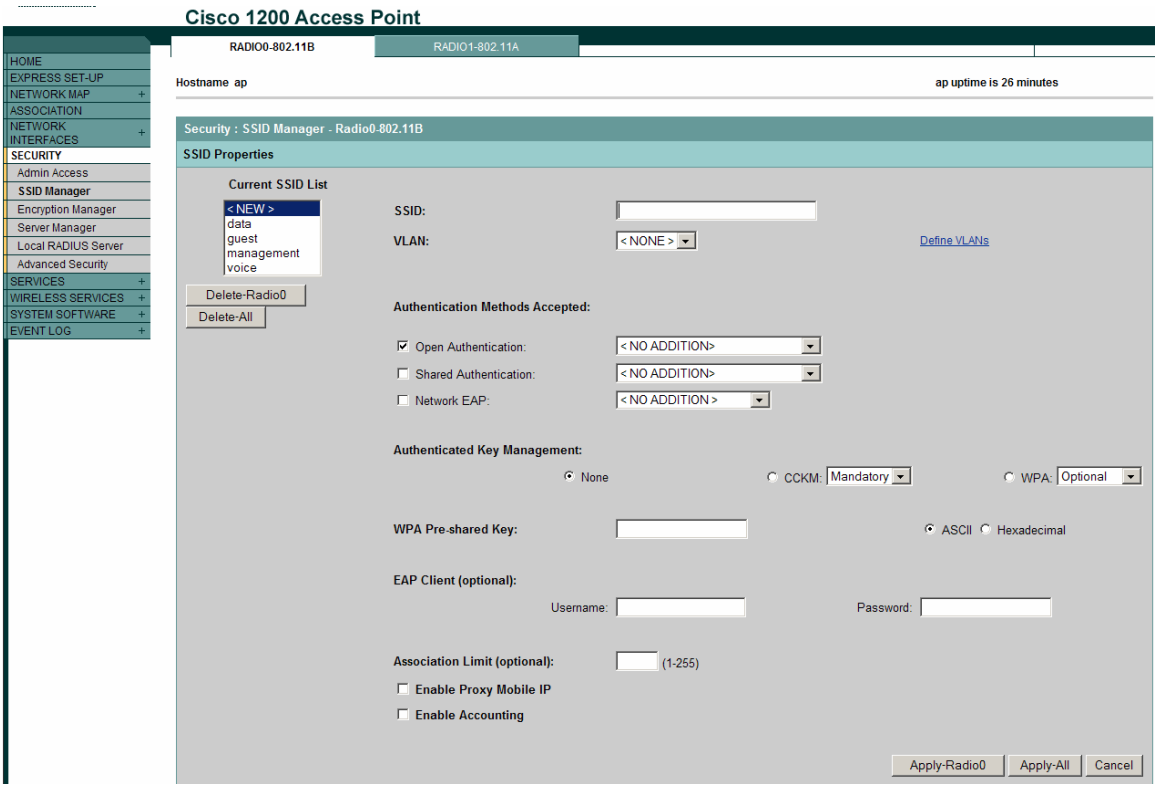
http://www.cisco.com/en/US/products/hw/wireless/ps430/products_installation_and_configuration_guide_book09186a0080147d69.html

Step 1 Configure the System Name and BVI address



From the **EXPRESS SET-UP** page, configure the System Name and BVI address.

Step 2 Define the SSIDs and Authentication Type



From the **SECURITY>SSID Manager** page, configure the 802.11b radio management, voice, data, and guest SSIDs, and authentication type according to the Preparation table.

a. Enter the *management* SSID in the SSID: box.

b. Select the authentication method.

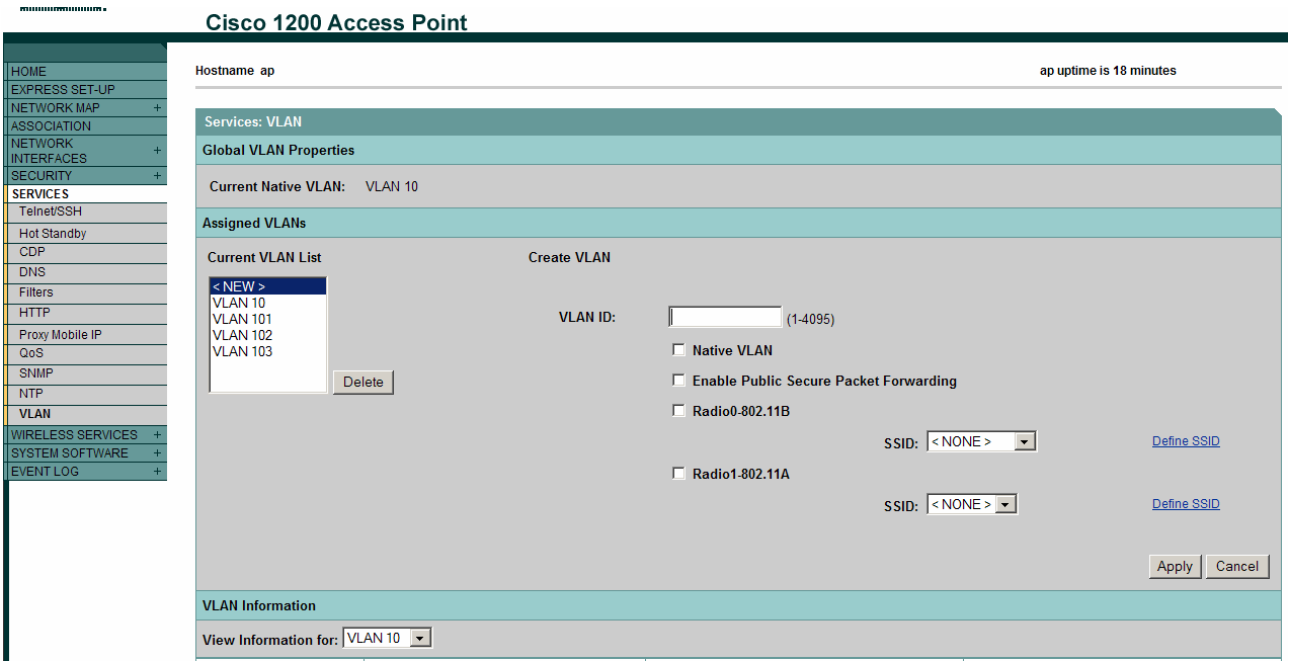
c. Click **Apply**.

d. Repeat the steps for the voice, data, and guest SSIDs.

1. Why is VLAN ID 10 used for the management VLAN instead of VLAN ID 1?

_____

Step 3 Define the VLANs



From the **SERVICES>VLAN** page, configure the 802.11b radio for management, voice, data, and guest VLANs according to the Preparation table.

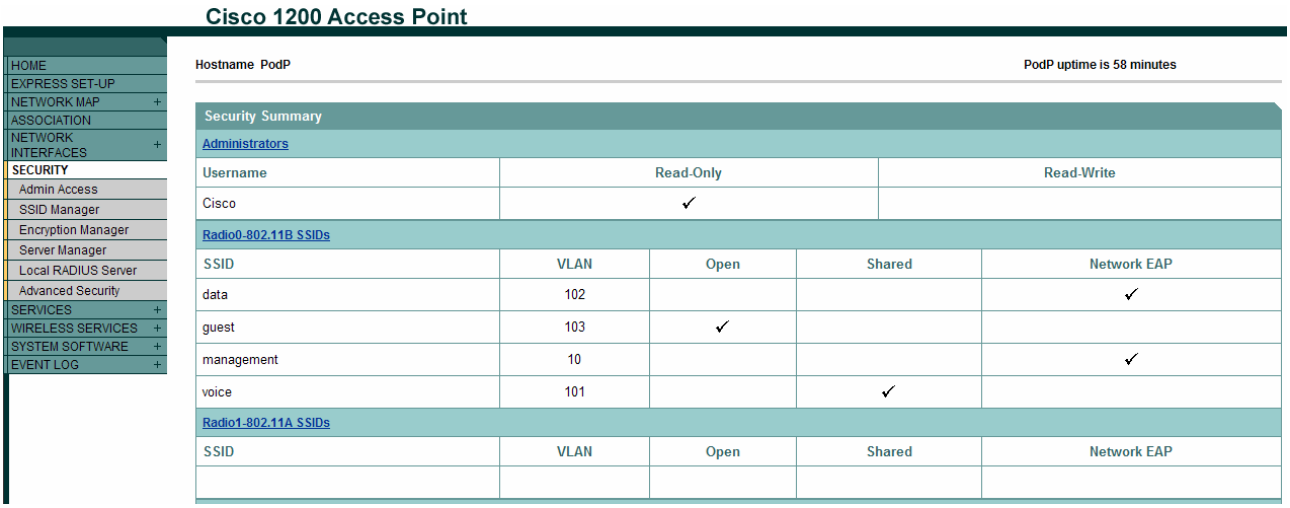
a. Enter VLAN ID *10* in the **VLAN ID**: box. Since this is the management VLAN, check the Native VLAN box. Also, check the Radio0-802.11B.

b. Choose the *management* SSID from the **SSID** drop down box.

c. Click **Apply.**

d. Repeat the steps for the voice, data, and guest VLANs.

Step 4 Verify the Configuration through GUI



From the **SECURITY** home page

a. Verify the VLAN configuration through the GUI

Step 5 Verify the Configuration through the IOS CLI

Telnet or Console into the AP.

a. Verify the configuration through IOS CLI.

```
PodP#show run
Building configuration...

Current configuration : 3167 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname PodP
!
enable secret 5 $1$N46P$W9Eb.bK3xvfZ1XgDmRXDZ1
!
username Cisco password 7 01300F175804
ip subnet-zero
!
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 ssid data
    vlan 102
    authentication network-eap eap_methods
 !
 ssid guest
    vlan 103
    authentication open
 !
 ssid management
    vlan 10
    authentication network-eap eap_methods
 !
 ssid voice
    vlan 101
    authentication shared
 !
 speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
 rts threshold 2312
 station-role root
!
interface Dot11Radio0.10
 encapsulation dot1Q 10 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 Dot11Radio0.101
 encapsulation dot1Q 101
 no ip route-cache
 bridge-group 101
 bridge-group 101 subscriber-loop-control
 bridge-group 101 block-unknown-source
 no bridge-group 101 source-learning
 no bridge-group 101 unicast-flooding
 bridge-group 101 spanning-disabled
!
interface Dot11Radio0.102
 encapsulation dot1Q 102
 no ip route-cache
 bridge-group 102
 bridge-group 102 subscriber-loop-control
 bridge-group 102 block-unknown-source
 no bridge-group 102 source-learning
 no bridge-group 102 unicast-flooding
 bridge-group 102 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 Dot11Radio1
 no ip address
 no ip route-cache
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 rts threshold 2312
 station-role root
 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 FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
!
interface FastEthernet0.10
 encapsulation dot1Q 10 native
 no ip route-cache
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface FastEthernet0.101
 encapsulation dot1Q 101
```



```
 no ip route-cache
 bridge-group 101
 no bridge-group 101 source-learning
 bridge-group 101 spanning-disabled
!
interface FastEthernet0.102
 encapsulation dot1Q 102
 no ip route-cache
 bridge-group 102
 no bridge-group 102 source-learning
 bridge-group 102 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 BVI1
 ip address 10.0.P.1 255.255.255.0
 no ip route-cache
!
ip http server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/
prodconfig/help/eag/ivory/1100
bridge 1 route ip
!
!
line con 0
line vty 0 4
 login local
line vty 5 15
 login
!
end

PodP#
```

Step 6 Configure PCs and connect to the AP

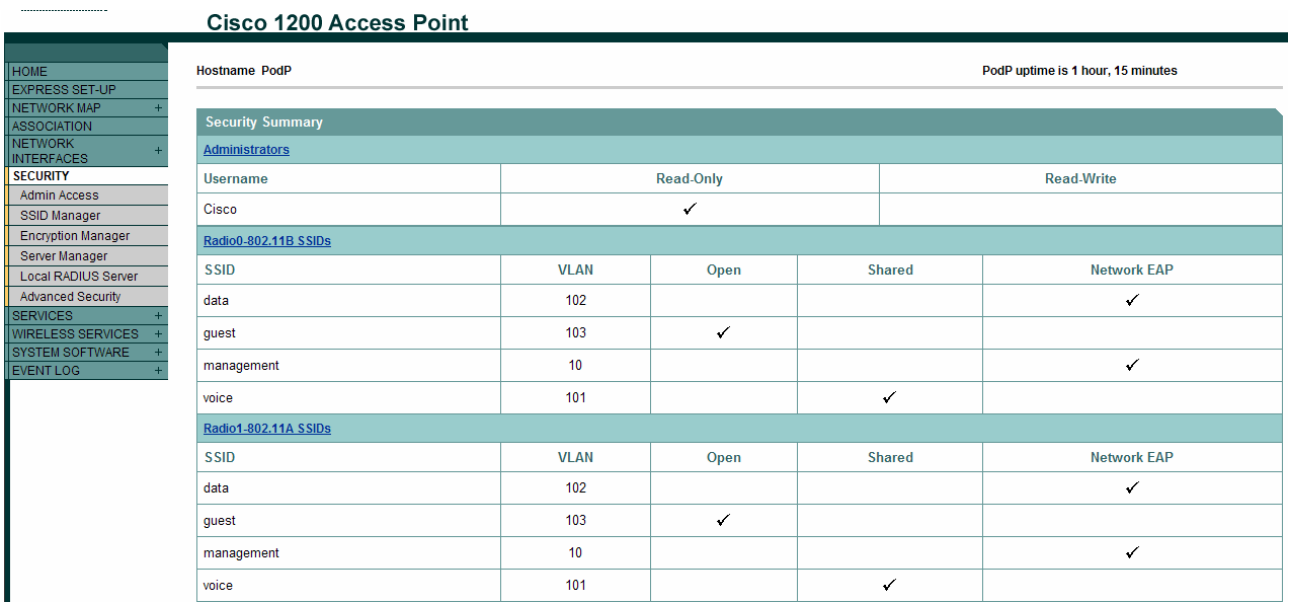
a. Now configure 2 wireless PCs.

- PC 1 with Open Authentication with a SSID of guest
- PC2 with Shared Authentication with a SSID of voice

b. Verify the connection through the **ASSOCIATION** page.

Note	Cisco recommends not using shared keys due to inherent security flaws with the technology

Step 7 Configure 802.11a VLANs (optional)



a. Now create the SSIDs for the 802.11a radio and apply to the existing VLANs .

b. Verify the settings afterwards through the **SECURITY** home page.

c. Verify the setting through IOS CLI.

d. Return to Step 6 and configure 2 802.11a clients. Verify the connections.

e. Save the configuration to a text file.

Step 7 Configure 802.11a VLANs through IOS CLI (Optional Challenge)

From the IOS CLI:

a. Erase the existing startup configuration and reload the AP.

b. Configure the SSIDs and VLANs for the 802.11b radio.

c. Verify the configuration by comparing to Step 5.

d. Configure the SSIDs and VLANs for the 802.11a radio.

e. Compare to the text file saved from Step 6d.

Step 7 Configure PCs and connect to the AP

a. Now configure 2 wireless PCs for the guest VLAN (Client and TCP/IP setting).

Can the PCs ping each other? _____

b. Now change the PC2 to the Voice VLAN.

Hint: Remember this VLAN has WEP Mandatory.

Can the PCs ping each other? _____

c. Finally, change the PC1 to the Voice VLAN.

Can the PCs ping each other? _____

d.

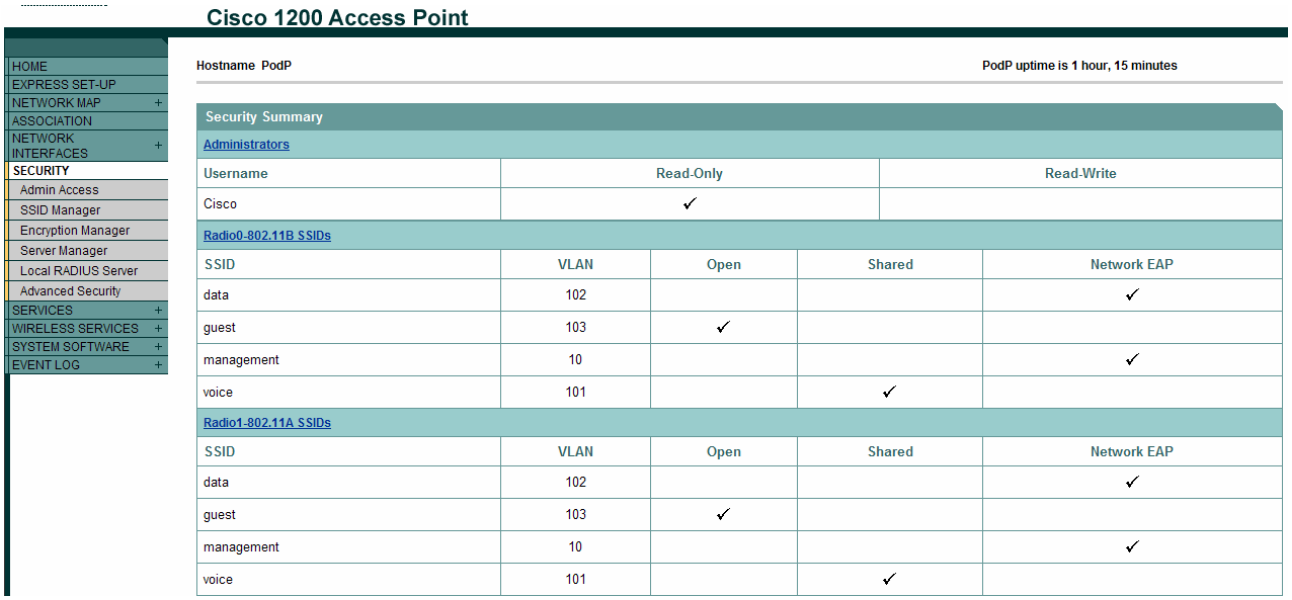
- PC 1 with Open Authentication with a SSID of guest

- PC2 with Shared Authentication with a SSID of voice

e. Verify the connection through the **ASSOCIATION** page.

Note	Cisco recommends not using shared keys due to inherent security flaws with the technology

Step 8 Configure 802.11a VLANs (Optional)



a. Now create the SSIDs for the 802.11a radio and apply to the existing VLANs.

b. Verify the settings afterwards through the **SECURITY** home page.

c. Verify the setting through IOS CLI.

d. Return to Step 6 and configure 2 802.11a clients. Verify the connections.

e. Save the configuration to a text file.

Step 9 Trunk AP to AP (Optional Challenge)

In this optional step, create a trunk between Pod APs through one of the following methods:

- On a 802.1q enabled switch, connect each APs to a switch with 802.1q trunking enabled on the port connecting each AP.
- Use a crossover cable between both APs

a. Change the BVI address to a 16 bit mask.

b. Configure the IP addresses on the wireless PCs with a 16 bit mask

c. Test connectivity between the PCs in VLAN 103.

d. Attempt to connect to the BVI address from the wireless PCs located in VLAN 103. Notice there is no connectivity between VLANs, only within VLANs.

e. Configure LEAP authentication for the data VLAN and test connectivity between pods PCs which are connecting through Data profiles.

f. Notice that there in no connectivity between VLANs. If time permits, configure a “router on a stick” to route between the VLANs. If using an enterprise 3550 or routing capable switch, inter VLAN routing can be configured without using a router.

Step 10 Configure 802.11a VLANs through IOS CLI (Optional Challenge)

From the IOS CLI:

a. Erase the existing startup configuration and reload the AP.

b. Configure the SSIDs and VLANs for the 802.11b radio

c. Verify the configuration by comparing to Step 5

d. Configure the SSIDs and VLANs for the 802.11a radio.

e. Compare to the text file saved from Step 6d.

f. Return to Step 6.

