

Application Note: Example Scenarios for AeroGuard™ MIMO Solutions

Introduction

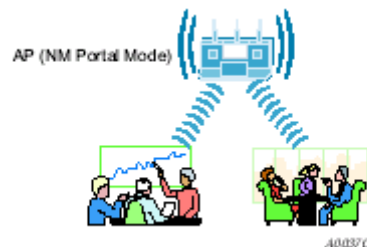
This document describes five application scenarios that cover the entire gamut of network configuration most encountered in any small, medium or even a large distributed enterprise business. Each scenario is described followed by a summary of network requirements, easy to follow configuration steps and a complete list of network equipment required to realize the network.

The scenario clearly demonstrate the power of the AeroGuard™ MIMO Solution in terms of its versatility, scalability, security, and ease of management.

Scenario 1: Small office, single AP, possible future growth

Acme Works begins as a small company with 20 users. The office is at a single location served by one access point connected to the wired backbone. The elements of the network are shown below.

Example 1 Network Requirements



One AP is able to meet current coverage and capacity needs. The AP is configured as a network management 'Portal' to assure that the appropriate network management structure will be in place in the event that the business expands and additional APs are required. Since the user base is small, there is no need for an external RADIUS authentication infrastructure. The security mode is WPA with pre-shared keys (PSK) and AES encryption. A single SSID is in place, and the default VLAN, QoS, and service profiles are used.

Example 1 Feature Decisions

Physical Network	<input checked="" type="checkbox"/> One AP	<input type="checkbox"/> Multiple APs	<input type="checkbox"/> Wireless Backhaul
Network Management	<input checked="" type="checkbox"/> NM Portal	<input type="checkbox"/> NMS PRO	
User Authentication	<input type="checkbox"/> Built-In Security Portal	<input type="checkbox"/> External RADIUS Server	
Security Modes	<input checked="" type="checkbox"/> WPA (default)	<input type="checkbox"/> Open	<input type="checkbox"/> WEP
VLAN	<input checked="" type="checkbox"/> Default VLAN	<input type="checkbox"/> Multiple VLANs	
SSID	<input checked="" type="checkbox"/> Single SSID (default)	<input type="checkbox"/> Multiple SSIDs	
Quality of Service (Class of Service - COS)	<input checked="" type="checkbox"/> Default COS Mappings	<input type="checkbox"/> Custom COS Mappings	
Service Profile	<input checked="" type="checkbox"/> Default Service Profile	<input type="checkbox"/> Custom Service Profiles	
Guest Access	<input checked="" type="checkbox"/> Disabled (default)	<input type="checkbox"/> Enabled	

400264

The above table lists the tasks required for configuration and provides pointers to the detailed instructions in this guide.

Example 1 Configuration Tasks

1. Bring up the first (or only) SOHOfware AeroGuard AP:
 - Make sure a DHCP server is available on the network, and create a DHCP reservation for the MAC address of this AP.
 - Have the information sheet shipped with the AP available.
 - Bootstrap the AP as an NM Portal. Defaults are acceptable for most settings.
 - Choose an SSID (wireless network name).
 - Choose an administrative password and WPA pre-shared key.
 - Configure clients with compatible WPA security using the same pre-shared key.

2. Confirm that the network is up:
 - Open the IP Topology panel in NM Portal to confirm that the AP is listed as discovered.
 - Open the Station Management panel at any time to view a list of client stations associated to the AP.

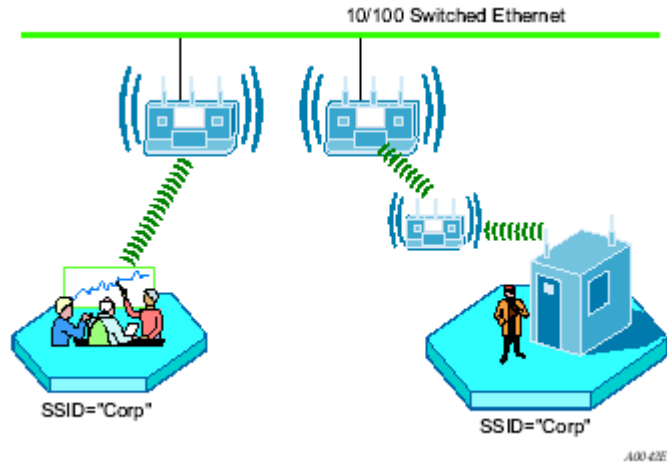
Network Equipment List

- AeroGuard™ MIMO 1202 AP
- Client Cards AeroGuard 1023CB or any Wi Fi compliant client device

Scenario 2: Small to mid-size business with wireless backhaul

Acme Works has now grown to 70 users. The site is the same as in Example 1; however Acme wants to provide coverage to a temporary building that has no wired connection. An additional AP is added to provide user access via a wireless backhaul.

Example 2 Network Requirement



The table below summarizes the feature decisions for this example. The security portal capability within NM Portal provides authentication for the backhaul AP. The security mode is WPA with pre-shared keys (PSK). A single SSID is in place, and the default VLAN, QoS, and service profiles are used.

Example 2 Feature Decisions

Physical Network	<input type="checkbox"/> One AP	<input checked="" type="checkbox"/> Multiple APs	<input checked="" type="checkbox"/> Wireless Backhaul
Network Management	<input checked="" type="checkbox"/> NM Portal	<input type="checkbox"/> NMS PRO	
User Authentication	<input type="checkbox"/> Built-In Security Portal	<input type="checkbox"/> External RADIUS Server	
Security Modes	<input checked="" type="checkbox"/> WPA (default)	<input type="checkbox"/> Open	<input type="checkbox"/> WEP
VLAN	<input checked="" type="checkbox"/> Default VLAN	<input type="checkbox"/> Multiple VLANs	
SSID	<input checked="" type="checkbox"/> Single SSID (default)	<input type="checkbox"/> Multiple SSIDs	
Quality of Service (Class of Service - COS)	<input checked="" type="checkbox"/> Default COS Mappings	<input type="checkbox"/> Custom COS Mappings	
Service Profile	<input checked="" type="checkbox"/> Default Service Profile	<input type="checkbox"/> Custom Service Profiles	
Guest Access	<input checked="" type="checkbox"/> Disabled (default)	<input type="checkbox"/> Enabled	

A00366

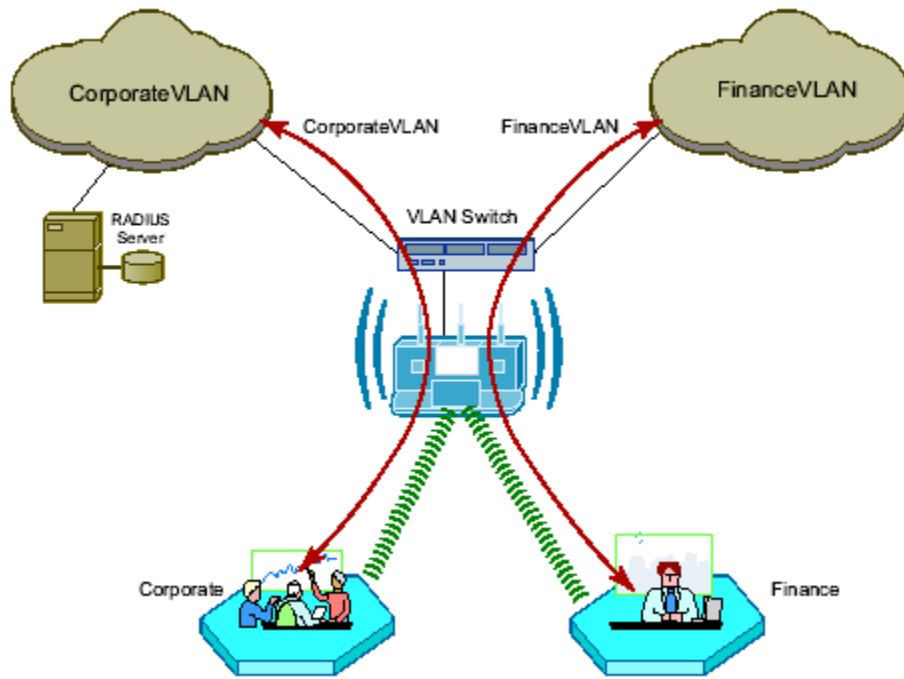
Scenario 3: Mid-size business, multiple SSIDs, multiple VLANs

Now a successful business, the management at Acme Works wants to position the company for continued growth. The company decides to deploy an external RADIUS server to manage user authentication centrally for the entire company. The RADIUS authentication infrastructure works well for a changing user population (employees joining, leaving, or moving to new departments) and readily supports further network service enhancements.

The company creates two SSIDs as a way to separate the Finance department network traffic from the main corporate network traffic. Two RADIUS servers are configured, each in its own authentication zone. To separate Finance department traffic from the overall network traffic, a Finance VLAN is created. A Finance service profile is also created and bound to the Finance SSID. The service profile is configured to include the Finance VLAN, high security and higher-than-normal COS. Once this structure is in place and a member of the Finance group is authenticated by way of the RADIUS server, the Finance group tag is passed to the SOHware AeroGuard AP, and the Finance service profile is applied to the user.

The network configuration for this example is shown below in the figure and table.

Example 3 Network Requirement



Example 3 Feature Decisions

Physical Network	<input type="checkbox"/> One AP	<input checked="" type="checkbox"/> Multiple APs	<input checked="" type="checkbox"/> Wireless Backhaul
Network Management	<input checked="" type="checkbox"/> NM Portal	<input type="checkbox"/> NMS PRO	
User Authentication	<input type="checkbox"/> Built-in Security Portal	<input checked="" type="checkbox"/> External RADIUS Server	
Security Modes	<input checked="" type="checkbox"/> WPA (default)	<input type="checkbox"/> Open	<input type="checkbox"/> WEP
VLAN	<input type="checkbox"/> Default VLAN	<input checked="" type="checkbox"/> Multiple VLANs	
SSID	<input type="checkbox"/> Single SSID (default)	<input checked="" type="checkbox"/> Multiple SSIDs	
Quality of Service (Class of Service - COS)	<input type="checkbox"/> Default COS Mappings	<input checked="" type="checkbox"/> Custom COS Mappings	
Service Profile	<input type="checkbox"/> Default Service Profile	<input checked="" type="checkbox"/> Custom Service Profiles	
Guest Access	<input checked="" type="checkbox"/> Disabled (default)	<input type="checkbox"/> Enabled	

A00264

The above table lists the tasks required to link to an external RADIUS server and add multiple VLANs, and provides pointers to the detailed instructions in this guide.

Example 3 Configuration Tasks

1. Add authentication servers and zones
 - Identify the RADIUS server for each authentication zone.
 - Select the authentication option for the SSID, with reference to the defined authentication zone.
2. Set up VLANs
 - Choose the VLAN structure for the network.
 - Configure the VLANs.
3. Add VLANs to the service profiles
 - Define or modify service profiles to include VLAN selection.
 - Bind each profile to an SSID with an existing or new user group.

Scenario 4: Large business, guest access, extended network services

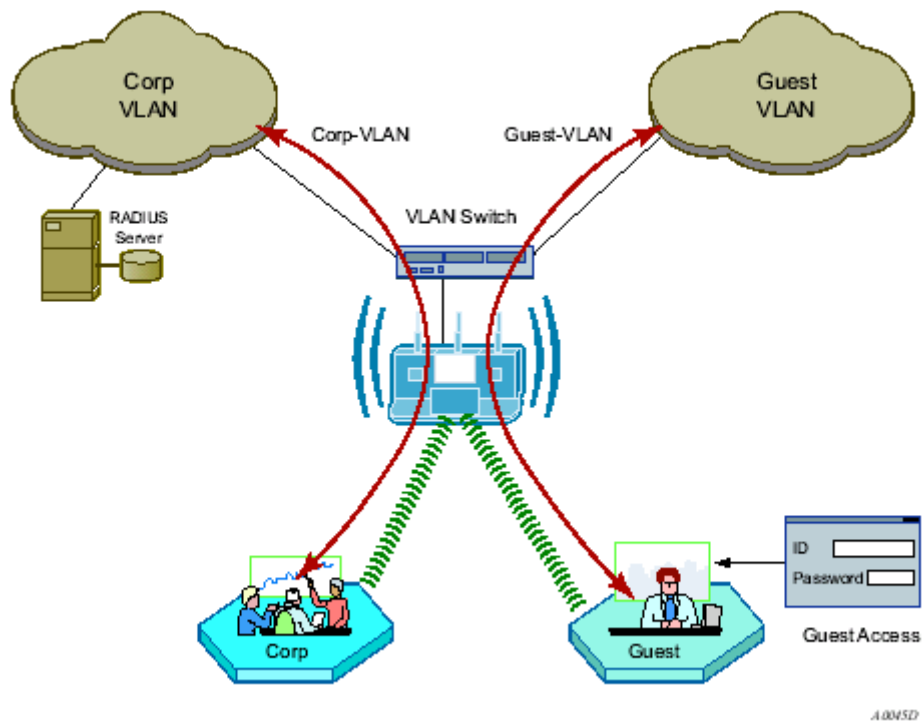
Acme Works is now a widely known and successful enterprise. With an ever increasing number of visitors requiring network access, the network administrator decides to implement a corporate guest access solution.

A guest VLAN and service profile are created and bound to the Corporate SSID, and a guest password is created. Guests can now visit Acme Works, log in using the guest password through a web browser, and obtain access to the resources available on the guest VLAN.

As additional needs arise, the network administrator can easily add new VLANs and service profiles, and change the available levels of service. New VLANs are created to segregate traffic for the Manufacturing and Engineering departments, and new service profiles are created to accommodate members of those departments. Special classes of service are assigned for applications sensitive to interruption or bandwidth fluctuation, such as voice over IP, and low priority, bandwidth-intensive applications such as FTP transfers.

The network configuration for this example is shown in Figure 11, and the feature decisions are shown in the figure and table below.

Example 4 Network Requirements



Example 4 Feature Decisions

Physical Network	<input type="checkbox"/> One AP	<input checked="" type="checkbox"/> Multiple APs	<input checked="" type="checkbox"/> Wireless Backhaul
Network Management	<input checked="" type="checkbox"/> NM Portal	<input type="checkbox"/> NMS PRO	
User Authentication	<input type="checkbox"/> Built-In Security Portal	<input checked="" type="checkbox"/> External RADIUS Server	
Security Modes	<input checked="" type="checkbox"/> WPA (default)	<input checked="" type="checkbox"/> Open	<input type="checkbox"/> WEP
VLAN	<input type="checkbox"/> Default VLAN	<input checked="" type="checkbox"/> Multiple VLANs	
SSID	<input type="checkbox"/> Single SSID (default)	<input checked="" type="checkbox"/> Multiple SSIDs	
Quality of Service (Class of Service - COS)	<input type="checkbox"/> Default COS Mappings	<input checked="" type="checkbox"/> Custom COS Mappings	
Service Profile	<input type="checkbox"/> Default Service Profile	<input checked="" type="checkbox"/> Custom Service Profiles	
Guest Access	<input type="checkbox"/> Disabled (default)	<input checked="" type="checkbox"/> Enabled	

A028/4

The above table lists the tasks required to configure guest access and provides pointers to the detailed instructions in this guide.

Example 4 Configuration Tasks

1. Set up guest VLANs
 - Configure a VLAN for guest access.
2. Create guest service profile
 - Add a guest service profile with the guest VLAN and desired COS and open security.
3. Configure landing page
 - Choose an internal or external landing page.
 - Assign guest password.

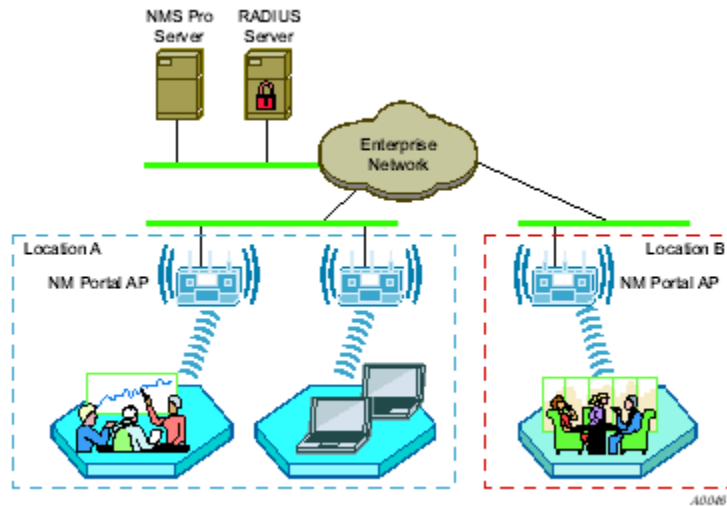
Scenario 5: Large Campus with Branch Offices

With continued growth, the original Acme Works building is now surrounded by multiple buildings within a large campus setting. The company also has two branch offices in neighboring communities. The decision is made to implement SOHware NMS-Professional for enterprise class network management. This solution will provide network administrators with extensive control and oversight, centralized monitoring, and fault management.

The campus buildings and branch offices lend themselves to a hierarchical management structure in which an NM Portal AP is configured in each building. Each NM Portal AP handles policy distribution and software upgrades at its location as directed by SOHware NMS-Professional. The NM Portal AP also serves as a backup security portal in the event that another RADIUS authentication server in its zone becomes unavailable.

The network configuration for this example is shown in Figure 13, and the feature decisions are shown below.

Example 5 Network



Example 5 Feature Decisions

Physical Network	<input type="checkbox"/> One AP	<input checked="" type="checkbox"/> Multiple APs	<input checked="" type="checkbox"/> Wireless Backhaul
Network Management	<input checked="" type="checkbox"/> NM Portal	<input checked="" type="checkbox"/> NMS PRO	
User Authentication	<input checked="" type="checkbox"/> Built-In Security Portal	<input checked="" type="checkbox"/> External RADIUS Server	
Security Modes	<input checked="" type="checkbox"/> WPA (default)	<input checked="" type="checkbox"/> Open	<input type="checkbox"/> WEP
VLAN	<input type="checkbox"/> Default VLAN	<input checked="" type="checkbox"/> Multiple VLANs	
SSID	<input type="checkbox"/> Single SSID (default)	<input checked="" type="checkbox"/> Multiple SSIDs	
Quality of Service (Class of Service - COS)	<input type="checkbox"/> Default COS Mappings	<input checked="" type="checkbox"/> Custom COS Mappings	
Service Profile	<input type="checkbox"/> Default Service Profile	<input checked="" type="checkbox"/> Custom Service Profiles	
Guest Access	<input type="checkbox"/> Disabled (default)	<input checked="" type="checkbox"/> Enabled	

A00264

The above table summarizes the tasks required to provide network management for the campus installation:

Example 5 Configuration Tasks

1. Install SOHware NMS-Professional
2. Enroll APs
 - Use the NM Portal in the local building or the campus SOHware NMS system to enroll additional APs.
3. Create and distribute policies
 - Use SOHware NMS-Professional to create configuration policies and distribute them to APs across the network.