

Pick the Right WLAN Architecture for Your Organization

There are two types of architecture for large-scale wireless local area networks: centralized and decentralized. It is vital to select the right one, because this determines which vendors and products you can use.

Core Topic

Enterprise Networking Equipment: Wireless LAN Systems

Key Issue

How will wireless LAN technologies and architectures evolve in the next five years?

Many solutions exist for deploying large-scale enterprisewide wireless local-area networks (WLANs). However, the basic architecture components of all solutions are the same.

There are two basic architectural components or devices that can be used to create an enterprisewide wireless network: access points and controllers. Access points have antennas and radios and vary in capability based on the amount and the type of intelligence that reside in them. Controllers, as the name suggests, are dedicated network devices for controlling the access points. Controllers can be classified depending on whether wired networking capability is included (integrated switch approach) or functionality is limited to managing the wireless networking environment (appliance approach).

Controllers are often tasked with management (radio strength, frequency and channel selection), authentication (access, authorize and authenticate) and security features (rogue access point detection, security tunnels and network layer encryption) of the wireless network. Access points can be further classified as:

- *Thick*: Fully functional WLAN with LAN bridging capability
- *Thin*: Only containing radios and antennas
- *Coordinated*: Limited intelligence to perform certain local radio frequency (RF) functions but dependent on its central controller for operations

Using these basic components, access points and controllers, two types of wireless network architectures exist for large-scale WLAN deployments: centralized and decentralized.

Centralized Architecture

Gartner

In a centralized approach, a controller is deployed in the distribution or the core of the network. It controls the core functions of a wireless network. Coordinated access points are deployed at the edge of the network and provide services enforced by the central controller.

In a centralized architecture, all traffic passes through the controller to allow the controller to police the wireless traffic and balance the load on access points. Access points provide RF access and implement policies enforced by its controller. Both components (access points and controller) are constantly in communication for traffic delivery and management.

There are no standard ways of distributing the wireless functions between coordinated access points and the wireless controller. Each vendor has made a different choice about distribution of functions between access points and controllers. Some vendors have chosen to move all functionality except RF access to the controller, while others have implemented data encryption and access control functions in the access points. In solutions where data encryption is not implemented in access points, a direct connection between access points and controllers or a dedicated tunnel is maintained.

Some examples of centralized architecture are Airespace 4000, Aruba 5000, Cisco WLSM on Catalyst 6500 and Symbol WS 5000.

Decentralized Architecture

In a decentralized architecture, the core wireless functions are distributed and available independently at every access point. Access points are responsible for maintaining an interconnected communication topology for exchanging information with other access points within the wireless network and may also communicate with central device for user policies. For smaller networks, access points can be deployed in a stand-alone mode. In bigger networks (more than 10 access points), constant communication between access points adds unnecessary RF management load on the access points and thus a controller should be deployed for load balancing and allowing for efficient subnet roaming.

Some examples of decentralized architecture are Cisco Aironet AP 1200, 3Com AP 8750 and Proxim ORiNOCO AP 4000.

Architecture Selection

Several factors must be considered when choosing the most-suitable architecture for an enterprise. The main difference

between the two architectures lies in their approach of handling the functions of wireless network. Table 1 compares the two architectures based on the issues that are important to most enterprises and how they are addressed in both architectures.

Table 1
Comparison of Centralized and Decentralized Architecture

	Centralized Architecture	Decentralized Architecture
Throughput	Throughput is determined by the processing power of the central controller. A controller must be capable of processing packets at line rate, otherwise latency may occur in the network as traffic passes through the controller. Throughput will vary depending on the location of the controller in the network.	As packets are processed by access points, throughput is directly proportionate to the number of users connected to that access point.
Authentication	Authentication is handled via a controller (WLAN appliance or WLAN switch) in conjunction with an AAA back-end server (for example, RADIUS). When users roam, reauthentication is not needed.	Authentication is done at the access point or in the RADIUS server when using 802.1x authentication. While roaming within the subnet, the authentication information is handed off between access points. Out of subnet, reauthentication is required.
Key Generation and Management	Key generation is usually performed at the controller. Keys are managed at the controller and cached at the access point. Keys do not survive access point reboots.	Key generation is performed at the AAA server. The user's master session key for encryption is generated at the end of the EAP/802.1X authentication simultaneously by the client and RADIUS server. In the case of WPA, the data encryption keys are generated by the access point and WLAN client using WPA key management.
Redundancy	Most of the products require another switch or appliance for central controller redundancy. If access point fails, most products are capable of adjusting power output on adjacent access points to account for the loss.	Access point placement should provide enough cell overlap in coverage to avoid disruption in service if access point fails.
Network Management	Central controller handles access point configurations, load balancing, error reporting and security policy enforcement.	In some decentralized solutions, each access point may need to be managed as a separate entity. Separate management components may need to be added for different types of management functions.

Source: Gartner Research (June 2004)

(Some vendors may have implemented some of the features in Table 1 slightly differently, but the information is generally true for most of the products in each category.)

In addition to the differences pointed out in Table 1, other considerations may be specific to enterprise environments and influence the selection of WLAN architecture. Some other factors include:

- Established wired network design
- Incumbent vendor for the wired network (whether the enterprise has standardized on a particular vendor or has a mix of vendors in its established LAN)
- Area to be serviced by wireless network
- Types of services required (data, voice over wireless)
- Types of clients to be supported (laptops, desktops and handheld devices)
- Types of users (employees, guests and contractors)
- Application that will be run on the wireless network

For example, if an organization considers providing WLAN in multiple buildings within the office campus, planning to support voice over WLAN, where usage patterns vary significantly at different times of the day and provide services to guests and regular employees, then centralized architecture is a better choice.

Centralized architecture offers better connectivity and security while roaming — the two most important attributes of a large-scale wireless network. Most of the WLAN deployments before 2004 used decentralized architecture. Enterprises must carefully evaluate the centralized architecture solutions and weigh the pros and cons of their established architecture against the centralized approach before making a decision about enterprisewide wireless roll-up.

In "greenfield" deployments, a centralized approach should be considered in any installation where more than five access points are required.

Acronym Key

AAA	authentication, authorization and accounting
EAP	extensible authentication protocol
RADIUS	remote access dial-in user services
RF	radio frequency
WLAN	wireless local-area network
WPA	Wireless Fidelity protected access

Bottom Line: Wireless local-area network architecture drives the choice of vendor and product selection. Architecture contributes to the manner in which certain wireless functionality is implemented. Centralized architecture certainly has advantages over decentralized architecture, especially for a large-scale enterprisewide WLAN deployment. In addition to flexible implementation, which depends on an enterprise's unique

requirements, products are available from many vendors that support a much wider variety of applications and provide better user mobility and security.