SPECIAL REPORT

The New Wireless LAN Architecture

By Jim Metzler

Sponsored Exclusively By:

Colubris NETWORKS™

This Special Advertising Section Produced By:

NETWORKWORLD®
www.networkworld.com

Table of Contents

Organizations of all types and sizes are under relentless pressure to become continually more agile. An agile organization is an organization that can efficiently respond in real-time to any factor in the environment that significantly impacts the health and well being of the organization and its stakeholders.

The requirement to be agile applies at different, but related levels inside of an organization. For example, an organization must be agile to respond to shifts in the business environment, such as the emergence of a new competitor or the opening of new markets. In addition, the IT function within that organization must be agile in its ability to incorporate new technologies, as well as its ability to respond to, or even anticipate, changes in the expectations of the company's business unit managers.

The purpose of a network architecture is to ensure the agility of the network organization in a cost-effective manner. Without an effective network architecture, networks typically evolve by deploying a new solution for each new business requirement. This approach leads to a network infrastructure that is comprised of a wide range of technologies, and which is both expensive and time consuming to maintain and modify.

However, just having a network architecture is not sufficient to ensure the agility of the network organization. To be effective, a network architecture must provide a clear linkage between an organization's business objectives and the services that are provided by the organization's network infrastructure. In addition, the network architecture must drive decisions around the acquisition and deployment of products and technologies.

This special report is focused on the wireless LAN (WLAN) component of an organization's overall network architecture. This report should help you create an outline of a WLAN architecture that tightly integrates with the existing LAN architecture and which enhances the agility of the network organization. This report will briefly analyze the shift in LAN architectures that occurred in the late 1990s, and will demonstrate how those shifts were in response to specific business and technology trends. As part of this analysis, this report will highlight some key principles relative to the development of an effective LAN architecture. This report then will highlight some of the primary business and organizational trends that are impacting the LAN and suggest a network architecture that enables network organizations to respond to those trends.

About the Author

Jim Metzler is is a principal in Ashton, Metzler & Associates, a consulting firm that focuses on leveraging technology for business success. During his career, he has worked in virtually every major segment of the IT industry.

The 1990s LAN architecture

An architecture is intended to be relevant for a number of years. However, on a periodic basis, changes in the environment are significant enough to justify modifying an existing architecture. In most cases these environmental changes involve a shift in business requirements combined with the development of new technologies. This section follows the fundamental shift in LAN architecture that occurred in the 1990s and will highlight some key principles relative to developing an effective LAN architecture.

One of the most common LAN designs in the early 1990s consisted of shared Ethernet workgroups interconnected by FDDI. However, the mid 1990s marked the beginning of a fundamental shift in business requirements. In that timeframe companies began to deploy increasingly faster PCs to respond to the movement to client server computing. As a result, network organizations began to reduce the number of users that they assigned to an Ethernet segment.

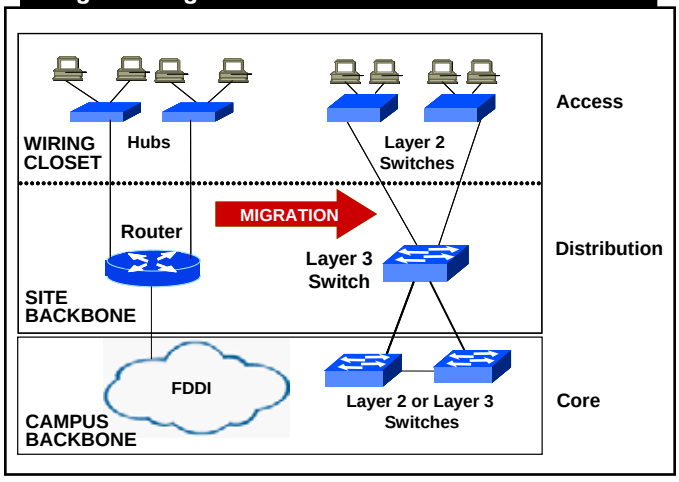
At the same time that shifting requirements were driving the movement toward having fewer users on an Ethernet segment, there was an increased focus on the operational efficiency of the LAN infrastructure. In particular, driven by the desire to reduce the complexity associated with server management, IT organizations began the process of centralizing servers. The process of server consolidation underscores an important architecture principle.

Architecture Principle #1: Centralized management is a requirement for a network to scale.

As organizations began to consolidate servers, there was a series of technological advances that led to the deployment of the first generation of LAN switches. These LAN switches made it economically feasible to dedicate an Ethernet segment to an individual user.

This combination of shifting requirements, an increased focus on operational efficiency, and the deployment of LAN switching led to both the need and the ability to migrate the enterprise LAN architecture away from one based on shared media, and towards one based on switching. Figure 1 depicts the migration that most companies went through in this time frame.

Figure 1: Migration to The Switched LAN Architecture



The architecture that is depicted on the right of Figure 1 is The Switched LAN Architecture. The Switched LAN Architecture is comprised of a hierarchical three-tier design that corresponds to the physical topology of a company's wiring closet, site backbone and campus backbone. Note that the three tiers of The Switched LAN Architecture are often referred to as access, distribution, and core.

While it is possible to put Layer 3 switches in the wiring closets, that results in significantly increasing the complexity of ongoing management. Driven by the previously mentioned principle of reducing complexity, virtually all companies populate their wiring closets with Layer 2 switches.

A key characteristic of first generation LAN switches is that similar to the shared hubs that they were replacing, these switches were designed primarily to provide raw connectivity and not to provide any significant value-added functionality. This changed quickly. In particular, companies soon adopted a LAN architecture that called for deploying switches that supported advanced functionality by incorporating the ability to process packets at layers 4 and higher. This allows a LAN to implement value-added services such as QoS.

Architecture Principle #2: A network architecture needs to be able to support enhanced services in addition to just raw connectivity.

It would have been possible to implement processing at Layer 4 and above only in Layer 3 switches in the distribution and core layers. However, driven by the need to support demanding applications such as VoIP, the vast majority of companies have implemented a LAN architecture that calls for the Layer 2 switches in the wiring closet to be able to process at Layer 4 and above. Hence, while architecture principle No.1 called for the centralization of management functionality, the deployment of sophisticated functionality in wiring closet switches leads to a complementary architecture principle.

Architecture Principle #3: Distributed processing is required both for scalability and for the ability to support enhanced services.

Like all network technologies, the first generation of LAN switches was relatively expensive and lacked high throughput. For example, first generation LAN switches typically provided a small number of ports, most of which were running at 10M bit/sec. In addition, most of these switches could not support all of the ports running at wire speed. However, within a couple of years, the per-port prices dropped, and LAN switches began to support a large number of ports running at wire speeds up to a gigabit per second.

Architecture Principle #4: Networks in general, and LANs in particular, need to be able to scale to support continually increasing levels of throughput.

While today's switched LANs are comprised almost exclusively of Ethernet, it is important to realize that in the mid 1990s there were a number of switched LAN technologies. In addition to some proprietary technologies, these technologies included Ethernet, Token Ring, FDDI, ATM and 100VGAnyLAN.

Architecture Principle #5: Network architectures tend to focus on a small set of standards-based technologies and industry standard practices.

The challenging business environment

The requirement for agility, combined with the growing need to support a mobile workforce, has spawned the requirement for companies to provide employees access to corporate applications, whether the employee is at his usual workspace, at another office in his primary place of employment, or at an airport or hotel.

The need for agility is driven in part by the relentless pressure of competition, which has reduced most business's ability to raise prices. This has led to the general business requirement to control costs in general, and IT costs in particular.

While these trends apply to virtually all organizations, each industry segment has its own unique challenges. An example of that is the medical industry. Over the last few years there has been increased public awareness of the need to improve the quality of medical care. This awareness typically comes from incidents that are reported on the evening news, and backed up by studies of the healthcare industry.

For example, a 1999 report from the Institute of Medicine (IOM) highlighted the seriousness of the issue. The IOM report quoted studies that indicated that medical errors in U.S. hospitals result in the death of 44,000 to 98,000 people each year.

The healthcare industry also is in the midst of an ongoing labor shortage. One component of this labor shortage

involves nurses. More than 126,000 nursing positions are unfilled today and that number is expected to increase significantly just as the Baby Boomers begin to place even more demands on the system.

The myriad challenges that every company faces have resulted in intense pressure on the IT organization to demonstrate its business value. This pressure to demonstrate the business value of IT is summarized in a story entitled "IT Doesn't Matter"[1]. Author Nicholas Carr suggests that IT has become a commodity and hence no longer provides an organization with a strategic advantage. Based on this assumption, Carr urges organizations to reduce how much they spend on IT.

Carr's story has encouraged IT organizations to focus on providing value-added services and not just commodity technologies. The creation of a network architecture enables IT organizations to establish a clear linkage between business requirements and the services that the IT organization provides.

The need for services

Background

One of the techniques that IT organizations can use to provide business value and yet control costs is to deploy a single network infrastructure over which they create multiple virtual networks. For example, many companies use MPLS WAN services from one or more service providers. These MPLS WAN services offer multiple service classes that are engineered to support disparate traffic types.

For the sake of example, assume that a service provider's MPLS network offers four service classes. The enterprise IT organization may use these four classes to offer the following services:

- Voice
- Video
- High priority data transport
- Low priority data transport

This approach is in close alignment with the need to be able to layer value-added services on top of basic connectivity. However, this requirement is not limited to the WAN, it extends also to the LAN. One of the implications of this requirement is that IT organizations need to deploy a WLAN architecture that facilitates the ongoing deployment of value-added services.

Another implication of this requirement is that IT professionals must acquire WLAN equipment from a vendor that provides a wide range of services. However, it is just as important that IT professionals acquire WLAN equipment from a vendor that supports an open environment that enables third parties to develop additional services.

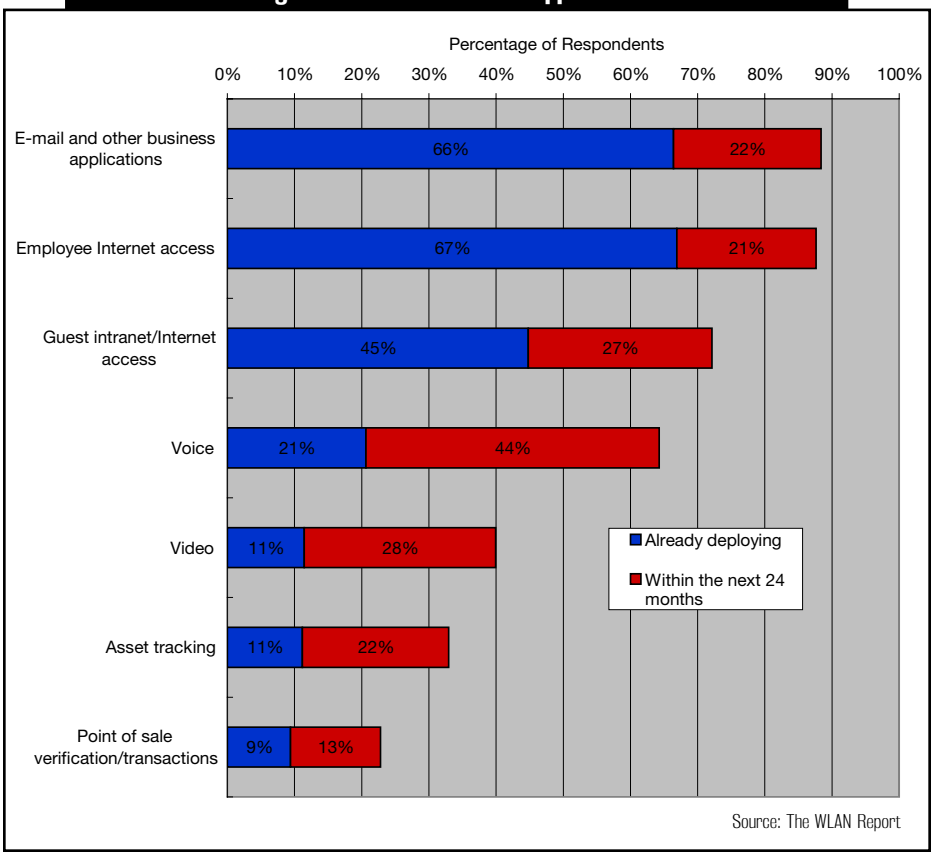
The purpose of this section is to provide some examples of possible services to be layered on top of an organization's WLAN. This is not intended to be an exhaustive list of possible services.

To demonstrate the recognition in the marketplace of the need for services, this special report will refer to market research contained in the document "Wireless LAN State-of-the-Market Report" that was authored by Joanie Wexler (www.webtorials.com). Throughout this special report, that document will be referred to as The WLAN Report.

[1] *IT Doesn't Matter, Nicholas Carr, Harvard Business Review, 2003*

To create The WLAN Report, Wexler asked the subscribers to Webtorials a number of questions relative to their current and planned use of WLANs. For example, Wexler asked the survey respondents about the applications that they intended to run over their WLANs. Their responses are shown in Figure 2.

Figure 2: Plans for WLAN Applications



Legacy services

While it is critically important that the new WLAN architecture enable IT organizations to offer new value-added services, it is also extremely important that the new WLAN architecture support any existing services. This requirement is demonstrated in Figure 2. In that figure, 66% of companies already use their WLANs to provide access to e-mail and other business applications. An additional 22% of companies intend to provide this service within the next 24 months. There were 419 respondents to the survey.

One industry segment where creating linkages with legacy systems is critical is the medical industry. As mentioned, two challenges facing the medical industry are increasing the quality of medical care and leveraging an increasingly scarce supply of nurses.

To respond to these challenges, hospitals and other care facilities are providing wireless devices to their nurses. By using WLAN technology, these devices are linked to clinical information systems. One of the goals of establishing this linkage is to inform a nurse in advance of any potential adverse consequence that might result because of administering a drug or other form of treatment.

Value-added services

Guest services

This class of service is targeted at visitors to a building or campus complex. As is shown in Figure 2, 45% of companies already offer this service and an additional 27% of companies intend to provide this service within the next 24 months.

A major part of the challenge in providing guest services is that there is a wide range of types of guests that must be accommodated. Because of that, it is critical to authenticate all guests.

For example, the authentication process may determine that the guest is an employee of the organization who normally works at another location. In this case, it might be desirous to provide the employee access to corporate applications and to ensure that the employee's traffic gets the appropriate QoS treatment. However, if the authentication process determines that the guest is a contractor or someone who is there to make a sales call or apply for a job, it may be desirous to tightly constrain the resources to which the guest

has access. In some cases, the guest may be constrained to only have Internet access.

VoWi-Fi

Another service that is beginning to be widely deployed is transporting voice over a WLAN. This service is commonly referred to as VoWi-Fi. As is shown in Figure 2, 21% of companies already offer this service and an additional 44% of companies intend to provide this service within the next 24 months.

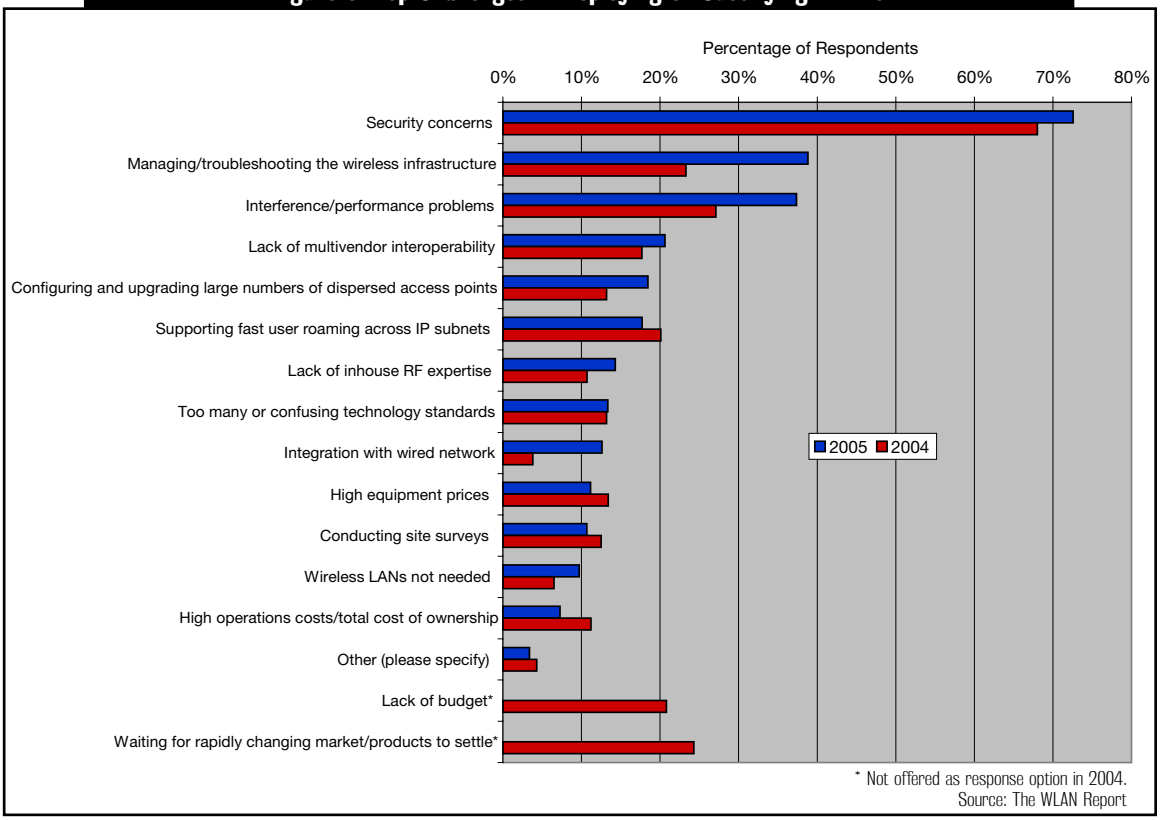
To ensure acceptable voice quality, VoWi-Fi requires QoS. In a growing number of cases, these VoWi-Fi deployments also include Session Initiation Protocol because of the broad range of applications that can be enabled in a SIP-based solution.

One application of VoWi-Fi is for people who want to have one phone to use both in fixed locations, such as their home or office, as well as while they are traveling. To provide this service, the phone call must seamlessly switch between the WLAN in the building and the person's cell phone service provider outside of the building.

Security

Security can be viewed both as a service unto itself as well as a service that enhances the value of other services. In either case, security is a top of mind issue for virtually all IT professionals no matter what technology is being discussed. In particular, as shown in Figure 3, for the last two years security is far and away the most significant challenge impacting the deployment and justification of WLANs.

Figure 3: Top Challenges in Deploying or Justifying WLANs



The IEEE is addressing security through a variety of new standards. One such standard, 802.1X, is focused on port based network access control and provides an authentication framework that is applicable in both wired and wireless environments. A key concept within the 802.1X standard is identity. In this context, identity refers to the accurate and positive identification of network users, hosts, applications, services and resources. As part of the 802.1X standard, a server will verify a client's identity to ensure that authorized users gain access to the appropriate enterprise computing resources, while unauthorized users are denied access.

The recently adopted IEEE 802.11i standard uses 802.1X for user authentication and key distribution. For encryption, the 802.11i standard requires the implementation of Advanced Encryption Standard-Counter-Mode Cipher Block Chaining Message Authentication Code Protocol. This protocol not only encrypts the packet payload, but it also protects selected packet header fields.

Emerging services

While it is critical that IT organizations deploy a WLAN architecture that can support these existing services, it is also critical that the WLAN architecture support services that are likely to emerge over the next few years.

To exemplify this concept, the following highlights some WLAN-based services and service enhancements that could emerge and become mainstream over the next few years.

- Power management

  The goal of power management is to optimize battery life for handheld devices. This service puts to sleep either the entire WLAN device, or just the WLAN interfaces.

- Location services

  These services are intended to identify the location of a piece of equipment or a person within a building or campus complex. Organizations such as hospitals could use this service to keep track of life-saving equipment as it moves throughout the hospital. A service that locates people could be used to support the E911 requirement that when someone calls 911, both the calling number and the location of the caller, must be available to the 911 operator.

- Dynamic allocation of capacity

  In many cases it is useful to allocate WLAN capacity to users when they authenticate themselves using protocols such as 802.1X. This allows an IT organization to assign different amounts of bandwidth to users based on the identity of the users and the overall utilization of the WLAN.

- Meshing protocols

  In most current WLAN deployments, each access point is connected to some form of WLAN switch and not to another access point. WLAN meshing protocols allow for direct connectivity between access points. These links between access points increase both the availability of the WLAN as well as the number of possible design options.

- Advanced security on the controller

  Two forms of security that are getting a lot of attention are intrusion-detection systems (IDS) and intrusion-protection systems (IPS). An IDS is intended to protect the IT infrastructure by detecting inappropriate, incorrect or anomalous activity as it is happening. Alternatively, an IPS is intended to prevent any form of wireless attack or intrusion.

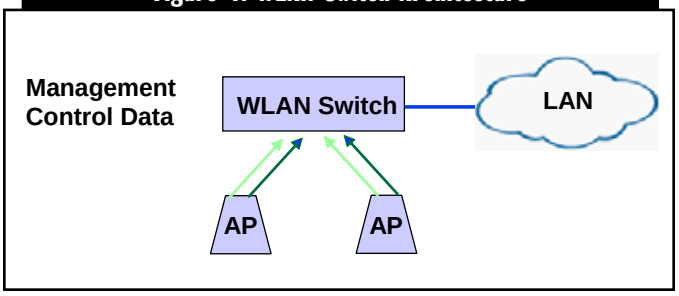
The new WLAN architecture

When The Switched LAN Architecture was developed WLANs were not a reality. As such, support for WLANs was not included in the architecture. Given the broad-based momentum to deploy WLANs a new architecture needs to be developed. This architecture must closely integrate WLANs with the existing LAN architecture and must adhere to the architecture principles developed in section two of this document.

Some of the initial deployments of WLANs were based on simply installing one or more access points. While this solution scaled relatively well, it did not allow for any coordination among the access points.

Figure 4 depicts the WLAN Switch Architecture that many companies currently implement. Throughout this document, this architecture will be referred to as the WSA. As can be seen in Figure 4, within the WSA a proprietary WLAN switch is the central point for control, management and data traffic.

Figure 4: WLAN Switch Architecture



The WSA has many advantages. One of these advantages is security. The WSA provides for strong access control and privacy and also allows for secure roaming. This architecture also reduces the burden of configuration management and ongoing operations.

However, the WSA also has many disadvantages. For example, the WLAN switch is a single point of failure for all of the access points that are attached to it. In addition, because all of the traffic from the access points transits the WLAN switch, this switch becomes a performance bottleneck and adds significant cost for simple data pass through traffic.

Another limitation of the WSA is that it is not easily adapted to accommodate new technologies or service offerings. For example, the IEEE is working on a new WLAN standard 802.11n. This standard will support real data throughput of at least 100 M bit/sec, which may well require an even higher raw data rate. To support this standard, the WSA would require a forklift upgrade. In addition, based on the proprietary nature of the WLAN switch, it is not easy for third parties to add any services, such as the type discussed in section four of this document, to the WSA.

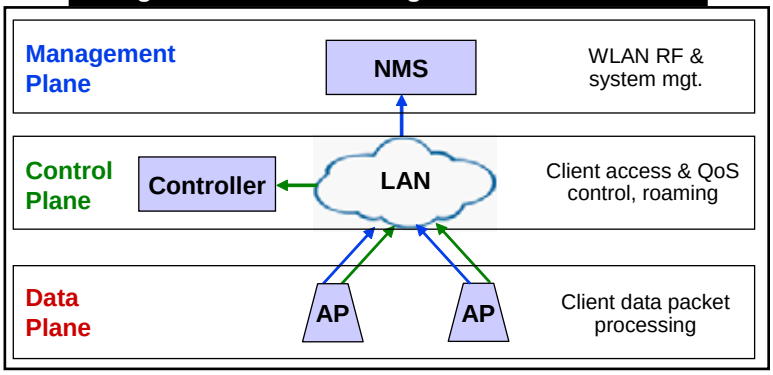
What is needed is a WLAN architecture that preserves the advantages of the WSA while overcoming its disadvantages. Table 1 lists some of the architectural aspects of the WSA that lead to its disadvantages. The table also indicates how those architectural deficiencies could be remedied.

Table 1: Remedying the WSA

Architectural Deficiency of the WSA	Remedy
The WLAN Switch is a bottleneck	Eliminate the WLAN switch
A single plane for control, management and data	Separate control, management and data planes
Data processing is centralized	Data process is distributed
Proprietary interfaces	Open interfaces

The Distributed Intelligent WLAN Architecture depicted in Figure 5 incorporates the remedies suggested in Table 1. Throughout this document, this architecture will be referred to as the DIWA.

Figure 5: Distributed Intelligent WLAN Architecture



A critical aspect of the DIWA is that it supports the concept of a "multi-service virtual access point". This enables IT organizations to offer a variety of services over a WLAN.

The DIWA also supports packet processing in access points. This approach allows IT organizations to enforce security and

Table 2: Evaluating the Distributed Intelligent WLAN Architecture

Architectural Principle	Conformance
Centralized management is a requirement for a network to scale.	Both the management and the control of the WLAN are centralized.
Network architectures tend to focus on a small set of standards-based technologies and industry standard practices.	The management, control and data planes are kept separate as is the case with all contemporary architectures. The functionality is packaged into a single piece of equipment for use in small sites.
Networks in general, and LANs in particular, need to be able to scale to support continually increasing levels of throughput.	There is not a single performance or availability bottleneck.
A network architecture needs to be able to support services in addition to just raw connectivity.	Open APIs enable third parties to have access to information pertaining to security, location and QoS.
Traffic processing intelligence needs to be as close to the user as possible.	Traffic processing occurs in access points.

bandwidth management at the network edge. This approach also contributes to the overall scalability and performance of the WLAN.

Similar to The Switched LAN Architecture, the DIWA as shown in Figure 5 is intended to be deployed in large sites. To conform to standard industry practices, the bulk of the functionality contained in the DIWA needs to be contained in a single piece of equipment for use in small sites.

To evaluate the viability of any new architecture such as the DIWA, it is important to determine if that architecture conforms to the architecture principles that are highlighted in section two of this document. As can be seen in Table 2, the DIWA is in tight conformance with those principles.

Deployment options

To minimize complexity, an architecture must be able to be deployed across a range of sites, from a large headquarters facility to a small branch office.

Figure 6 shows how the DIWA would be deployed inside a large site in which there are LAN switches on each of the floors (such as the distribution network) that are connected by a single core switch. In this case, the Network Management System and the controller, or possibly a cluster of controllers, is attached to the core LAN switch. Also attached to the core switch would be other relevant servers, such as servers to provide Authentication, Authorization, and Accounting, VPN and DHCP services to both wired and wireless users.

However, the functionality contained in the DIWA needs to be integrated into a single piece of equipment for use in small sites. Figure 7 shows how an integrated device that functions both as a multi-service controller as well as an access point would be deployed. In conformance with architecture principle No.1, the management of the network is centralized.

Figure 6: Large Site Deployment

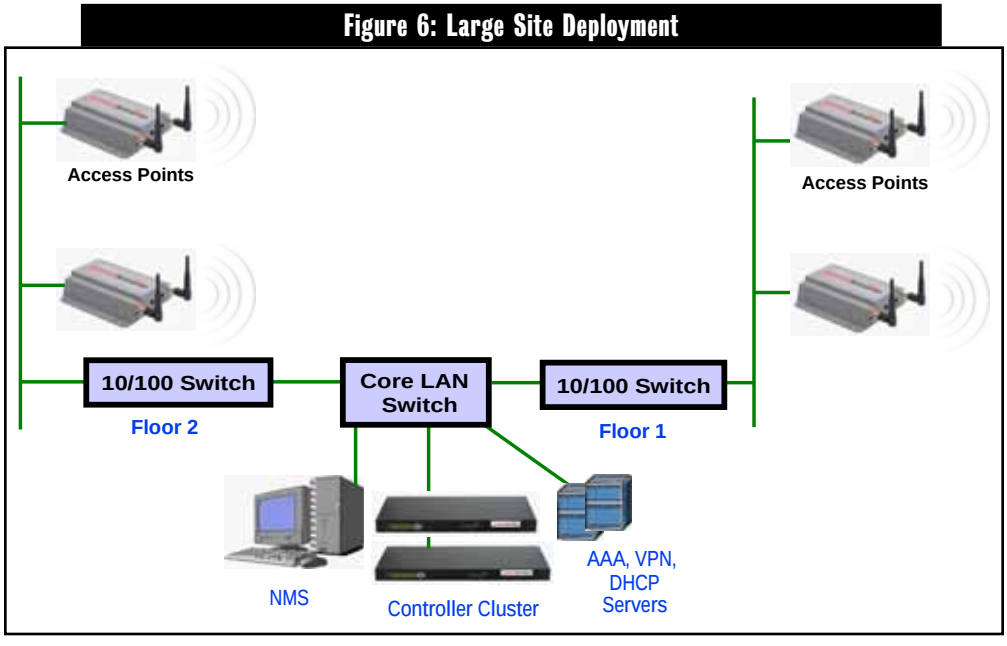
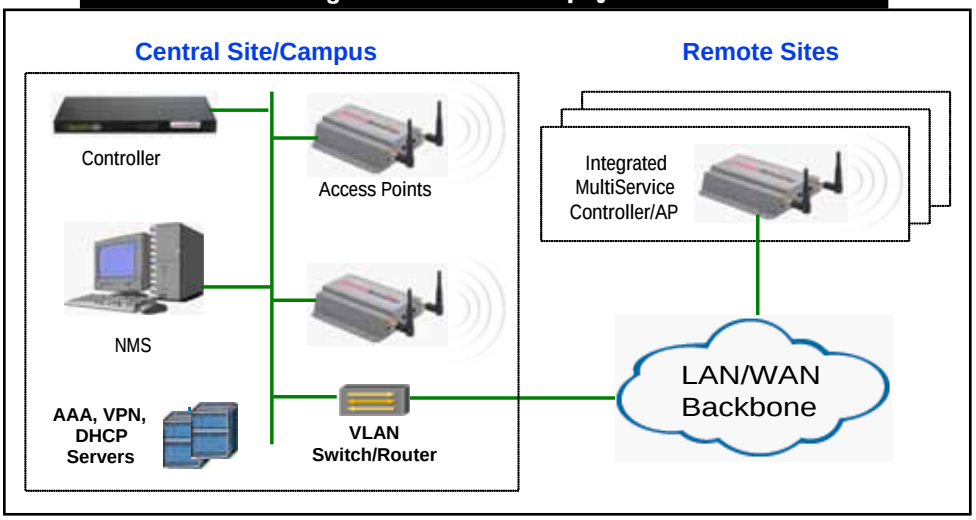


Figure 7: Remote Site Deployment



Call to action

An IT architecture is intended to be relevant for a number of years. However, on a periodic basis, changes in the environment are significant enough to justify modifying the architecture. In addition to the changing business requirements outlined in this document, there are a number of specific IT initiatives that should cause IT organizations to consider changing their WLAN architecture. These initiatives include the IT organization's desire to:

- Expand the current deployment of WLANs
- Deploy services such as VoWi-Fi and hence need intelligence in the access point
- Avoid Single Points of Failure
- Create an integrated wired and wireless LAN infrastructure
- Deploy centralized management of remote sites
- Implement an open environment to efficiently support applications developed by third parties
- Reduce capital expenditures and operational expenses
- Deploy a network that is large scale, broadly distributed, and which has sites of all sizes
- Deploy policy management and enforcement

Given the IT organization's responsibility to leverage its investments, the most effective and efficient way to implement a change in architecture is through a process of "cap and grow". In this case, "cap and grow" means that IT organizations should no longer invest in the WLAN Switch Architecture but should continue to use the equipment that is already deployed.

Cap and grow also means that on an ongoing basis, IT organizations should deploy the Distributed Intelligent WLAN Architecture as shown in Figure 5. This architecture, which conforms to a broad set of widely accepted architecture principles, exhibits two key attributes. The first of these attributes is that the DIW is focused on providing a wealth of services from both the equipment supplier as well as from third parties that leverage the architecture's open interfaces. The second key attribute is that within the DIWA, management and service creation are centralized while packet processing is distributed.