

## WLAN Architectures:

A closer look at the core differences between traditional AP, switched, and routed WLAN architectures.

A white paper by Chantry Networks Corp., an affiliate of Siemens Communications, Inc.

## Routed WLANs: Siemens Solution for Enterprise-Class Wireless LANs

HiPath Wireless is designed for real-world, scalable, available and manageable enterprise-class installations.

### Executive Summary

With the increasing standardization of basic wireless-LAN (WLAN) functionality, the core differences between different WLAN system implementations are now embodied in architecture. Traditional WLAN architectures, based on a network of interconnected access points (or APs) suffer from the high expense required both to acquire and manage that WLAN network. This situation has motivated the development of switched WLANs, but these in turn are proprietary, closed systems that introduce concerns about reliability and management. Switches still live at the edge of the network, and managing a large number of switches is almost as challenging as managing distinct access points.

What's required is a routed WLAN architecture, as is embodied in the HiPath Wireless System. Using a router in place of a switch allows a WLAN to be a full member of an enterprise network and leverages the investment already made in an IP-based infrastructure. Distance and configuration limitations are eliminated. Scalability is a core benefit, along with the flexibility that's required as networks grow and adapt to new enterprise challenges. Availability is also a key element of the routed approach, as fault-tolerant architectures — even spanning large geographies — fit naturally into a routed environment. And, Siemens extends the power of the routed architecture with HiPath Wireless Convergence Software, which is designed for large-scale deployments and even allows specific user functionality to be based on such variables as geographic location and time of day.

HiPath Wireless is designed for real-world, scalable, available, and manageable enterprise-class installations. The architectural innovations in HiPath Wireless bring valuable cost and performance benefits to WLAN deployments across a broad range of industries and applications.

### Introduction

Wireless LANs have arrived. They've gone from an interesting experiment to essential applications in enterprises of all sizes and types in what seems like record time. It's now clear that the benefits of mobile, *anytime/anywhere* access to information make a significant difference in productivity and the ability of an enterprise to respond quickly, accurately, and effectively to customers, competitors, and rapidly-changing market conditions and opportunities. *WLANs are playing a key role in this reality*, across the entire enterprise, both in the office and, via public-access WLANs, on the road as well.

The challenge is not *whether* an enterprise should consider a WLAN installation; the timeframe for that debate is now long past. Rather, given the fluidity of the market, WLAN technology, and the rapid rate at which new wireless-LAN products are being introduced, the decision needs to revolve around *how well* a given WLAN solution meets the needs of your enterprise. Successful WLANs must offer the best combination of *coverage, capacity, management, and growth potential* to enable the enterprise to optimize each of these factors as corporate requirements evolve. Because standards so strongly influence the functionality of a WLAN, the real value of a particular WLAN product is more likely to be defined in capabilities above the 802.11 MAC layer. In short, today's WLAN installation decision revolves more around architecture than any other element.

Just as the 802.11 standard defines the fundamental capabilities of a WLAN, the architecture of a given product that embodies this technology defines how (and how well) the product will address real-world application requirements. Let's consider the evolution of WLAN architectures as an illustration of this point.

The traditional WLAN architecture uses bridges (typically called access points or APs) to interconnect (typically mobile) wireless clients with a wired backbone, thus providing access to other network elements and resources. As a user roams out of the radio coverage range of one access point and into the range of another, the connection is automatically handed off via a dialog between the access points themselves. Higher levels of the protocol stack are completely unaware of this handoff, and coverage can be arbitrarily extended by adding more APs. Note that each AP is independent of the others, and must be configured and managed individually.

It is now obvious that this architecture is fundamentally flawed for large enterprise installations, particularly where the number of client connections is now reaching proportions that could only have been imagined until recently. Despite falling prices, enterprise-class APs remain expensive, and not just to acquire—the costs associated with maintaining and managing a large number of APs can be a significant operational expense. And, the possibility for disruptions to the existing network resulting from changes and additions to an AP-based installation needs to be carefully considered.

Very obvious functional holes also exist in the AP-centric architecture, in the areas of *security* and *mobility*. It's clear from the well-publicized problems with 802.11's Wired Equivalent Privacy (WEP) security that a more sophisticated solution is required, and roaming across subnets is complex to administer if one is brave enough to attempt it at all. These issues have been addressed with "enhancer" or "completer" products from a number of firms – but these enhancements for security, mobility, and management are usually implemented as additional expensive hardware boxes with their own set of operational issues and other constraints. This approach clearly moves in the wrong direction, creating complexity rather than eliminating it.

The new *switched WLAN* architectures are based on a central controller (usually called a *WiFi switch*) that interconnect "lightweight" or "thin" access points. These APs are much simpler (and much less expensive) than traditional APs. The brains of the installation reside centrally in the wireless switch, so acquisition and management costs are lower in installations that would otherwise involve more than a few APs as the cost of the switch is amortized across the entire installation. And, the operations staff deals with a single unit (the switch) via a single IP address rather than a large number of individual access points—a much more reasonable approach especially in large-scale deployments.

But switches have their own set of fundamental architectural flaws. First, the lightweight APs are proprietary, with similarly proprietary protocols between them and the switch. There are issues with availability—the switch is a single point of failure, and fault-tolerant switch configurations, which are available from some vendors, can get complex and very expensive. More importantly, the switches themselves are designed to be isolated Layer-2 subnets, distinct from the rest of the network and required direct connection to all APs in the subnet. As a result, each switch manages a small subnet of APs (typically less than six) whose reach is limited by the 100 meter maximum length of Ethernet (Category 5) cable. Mobility across these subnets can range from very difficult to essentially impossible, depending upon the implementation. The WLAN is literally an appendage hanging off the corporate network, rather than a full

member of it. And, if one has many switches, the network management problem quickly returns—except that instead of managing a large number of APs, one is managing a large number of switches.

All of this begs the question: how can we solve the WLAN architecture challenge once and for all?

At Siemens, *we have*. But the solution has required yet another step in the evolution of WLAN architecture: to truly address the requirements of a large-scale wireless deployment, the WLAN needs to be a *full member* of a standards-based, *routed* network architecture—a fully integrated extension of the enterprise network—not simply another Ethernet segment that happens to be implemented via radio.

### Introducing Routed WLAN

A router is a core element of almost every network configuration. The router provides a broad range of services from inter-networking to essential network monitoring, management, and control. The power of the router lies in its ability to deal with network issues and opportunities at Layer 3 of the OSI model which is, after all, the network layer. In designing our architecture, we began by considering the IP routed networks that most enterprises already have in place. By leveraging ubiquitous IP networks, we have designed a routed WLAN architecture that augments and extends our customers' networks, rather than simply adding new functionality at the edge (whether based on distinct APs or switched implementations).

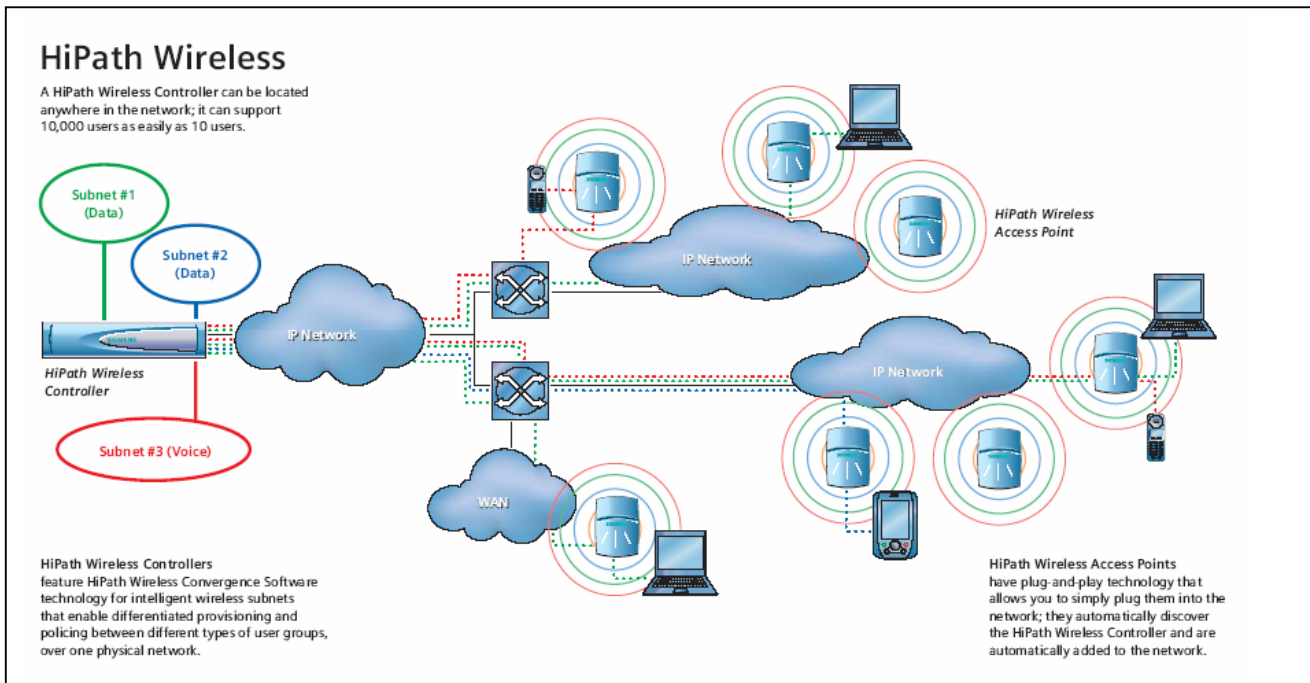
In a switched wireless architecture, the physical layer (the radio itself) is located in a lightweight AP; and the features of the medium-access control layer, where most 802.11 functionality resides, reside in the switch. The Siemens routed architecture keeps both 802.11 MAC and PHY functionality in our HiPath Wireless Access Point, allowing the highly-integrated 802.11 chipsets to work as intended. We move all higher-level functionality, such as authentication and IP address management, to our HiPath Wireless Controller. Because our architecture leverages the routed IP network, the HiPath Wireless Controller can be located essentially anywhere in a network, across multiple switch or router hops or even across WAN links, rather than being bound by the 100 meter limitation of switched architectures. The HiPath Wireless Access Point communicates with the HiPath Wireless Controller via standard IP protocols. This means that, by its very nature, the Siemens architecture is designed to address large-scale deployments, capable of growing to meet wireless networking challenges of any size, starting (if desired) small but growing to configurations that can handle large, distributed environments with ease.

The Siemens routed architecture was designed with the needs of large, multi-location enterprises in mind. It is also highly applicable to public-access WLAN installations that can cover multiple locations of varying sizes and capacity demands.

As we will explore in this white paper, routing is the best metaphor for a wireless LAN architecture. While the IEEE 802.11 standard defines core functionality, so much of what makes WLANs valuable exists above the MAC layer. Security, for example, is best implemented as an end-to-end service using such tools as RADIUS and virtual private networks (VPNs) that transcend the WLAN alone. Quality of service (QoS) similarly is also best managed as an end-to-end service, because so much of the responsiveness depends upon traffic management all the way back to the server. These are just a couple of the reasons why routed architectures are the best approach to implementing WLANs—WLANs that are *full peers* in an enterprise or other large-scale network. While almost any wireless-LAN

The HiPath Wireless Controller can be located essentially anywhere in a network, across multiple switch or router hops or even across WAN links, rather than being bound by the 100 meter limitation of switched architectures.

## The HiPath Wireless Architecture



architecture can move data and provide satisfactory connectivity for most users, the real difference between Siemens' approach and other architectures can be seen in three key areas: *scalability*, *availability* and *virtualization*. We believe these three elements, which we will explore in detail below, will be what defines the success of *enterprise-class* and *carrier-class* WLAN systems moving forward. Indeed, the ability of a WLAN architecture to grow and adapt to changing requirements with minimal (if any) interruption to or reconfiguration of the rest of the network, and the resilience of the architecture in day-to-day networking challenges, will be the key differentiators in an era otherwise dominated by standards.

### Scalability

Network configurations seldom remain static for long—in fact, *they only grow*. In the case of WLANs, growth occurs for reasons of both *coverage* (providing basic radio service in a given area) and *capacity* (providing the performance users really need to be productive). It's also worth mentioning here that the ongoing evolution of the 802.11 standard may dictate growth as well—capacity can be added via radios compatible not only with 802.11b, but also the faster 802.11a and 802.11g, and with various combinations of these physical-layer standards to meet specific requirements.

This means that a successful WLAN architecture *must allow users to plan for growth and change without knowing exactly what growth and change will be required*. And that's another benefit of a router-based architecture. *Siemens' WLAN implementation has no fundamental limitations*. A Siemens WLAN can consist of literally *thousands* of HiPath Wireless Access Points and *thousands* of mobile users. Because mobile users are homed to a HiPath Wireless Controller instead of physically connected to a WLAN switch, roaming across router boundaries is handled transparently without requiring Mobile IP or a similar complex solution.

# Scalability

WLANs are seeing huge applications in universities and other large campus settings. Nothing enhances the educational experience like the ability to access information from libraries, shared class projects, and, of course, the Internet, whenever and wherever the need arises. Productivity, even on campus, depends on getting what's required when it's required. Like in many other venues, having a broadly deployed WLAN infrastructure is becoming a competitive differentiator among universities everywhere.

Of course, universities can (and typically do) cover a huge amount of geography—from individual classrooms to labs, dorms, common areas, and even outdoor spaces. Providing such pervasive coverage with traditional WLAN access points can be daunting, given the expense involved to install, configure, manage, and upgrade the infrastructure on what may be a continual basis. It gets even more challenging when one considers that the density of WLAN users can be highly variable as well—for example, there could be many students actively using the WLAN in a lecture hall for relatively brief periods during the day, and then this traffic load might disperse to many other parts of the campus after class.

Siemens network architecture makes the work of designing, deploying, managing, and growing a WLAN infrastructure of this type much less demanding. Rather than adding dedicated wireless switching gear in every wiring closet, a HiPath Wireless Access Point can simply attach to the existing IP backbone network just like any other networked device. The HiPath Wireless Controller can similarly be located anywhere it's convenient, but will typically be in a physically secure server room or network equipment rack. Adding new HiPath Wireless Access Points for more coverage, capacity, or new technology is fast and easy. With HiPath Wireless Access Point's plug and play technology, HiPath Wireless Access Points automatically discover the HiPath Wireless Controller, and are automatically registered and configured (with appropriate notification to network management staff, of course). HiPath Wireless Access Points also support load balancing, allowing large numbers of users to be handled with improved throughput resulting for each user.

Scalability also means flexibility. It's critical for an enterprise-class implementation to place as few limitations on users and network managers. Deployments, both initial and incremental, must be accomplished with minimal (if any) disruption to the existing infrastructure, including minimal (if any) installation of new cabling. HiPath Wireless Access Points can be interconnected over an existing Ethernet infrastructure, minimizing the cost to install and deploy and making the best use of the current physical plant. And finally, scalability must allow investment protection and lower total cost of ownership. Growth must be smooth and non-disruptive to both wired and wireless network segments, and additional coverage and capacity must be provided through low-cost HiPath Wireless Access Points while taking advantage of the centralized power and performance of the HiPath Wireless Controller. In large configurations the cost of deploying traditional access points or WLAN switches will be significantly higher for both equipment and ongoing operational expense.

## Availability

The Siemens HiPath Wireless WLAN solution is also designed for high availability under varying network and traffic conditions. The reason is the routed nature of the architecture. The Internet, after all, is based on routers, and designed for availability and, indeed, *survivability* under a wide variety of interruption and even damage scenarios. An enterprise-class or carrier-class WLAN system requires the same degree of availability as the Internet – *it must keep operating no matter what*.

Unfortunately, the AP-based and switched-based architectures cannot meet this challenge. Each AP is a single point of failure and APs cannot cover for one another unless the infrastructure is sufficiently (and expensively) overbuilt. Likewise, the switch itself is a single point of failure, and unless an expensive redundant switch is

installed (and this is not even possible with many switched products), the switch-based architecture cannot provide sufficient redundancy. Moreover, a large-scale WLAN architecture must be self-discovering, self-configuring, and self-healing according to *policies* set by network management. And, an enterprise-class carrier-class architecture must be able to adapt to both changing network conditions and unit failures, should they occur.

# Availability

While the network might not be the computer, a computer without a network is of little value today. One of the nice features of WLANs is that they can be more reliable than a wired infrastructure – while interruptions to a wired physical plant are relatively common, the airwaves themselves never “break.” This is not to say that the vagaries of wireless communications have vanished from this planet – interference, multipath, and fading are still facts of life in the radio world. But the right architecture can compensate for these problems and, more importantly, problems that can occur at higher levels of the protocol stack.

Consider a large-scale enterprise WLAN. Operation of this network is critical to the enterprise with finance, marketing, engineering, and executive use on a near constant basis. High availability is critical. Now suppose this installation is built from traditional access points – and suppose one of these access points fails. Coverage and capacity are immediately reduced. If another access point is not within range of the failed unit, coverage will be lost until the unit can be replaced. There might be a small-scale crisis under these circumstances, but.... it gets worse.

To wit: if this enterprise is using a switched architecture and the switch itself fails, there is a “major event”. The APs serviced by the wireless switch will be down. Of course, fault-tolerant configurations are possible for some switched products, but they

require another switch in a hot-standby configuration. And this would be true for every switch in the enterprise’s network, resulting in significant capital outlay and management expense.

The Siemens architecture takes a very different approach to solving this problem. Since HiPath Wireless Access Points connect to HiPath Wireless Controllers over IP, rather than over a single physical Ethernet cable as in a switched architecture, the one-to-one relationship between a switched wireless subnet and the wireless switch itself no longer exists. A HiPath Wireless Controller can control and manage many subnets transparently and efficiently. And fault tolerance can be obtained simply by designating another HiPath Wireless Controller elsewhere in the network as a backup unit. So, in the very unlikely event that a HiPath Wireless Controller fails (perhaps due to a power interruption or the inadvertent unplugging of precisely the wrong cable), failover is transparent and operations continue. Should a HiPath Wireless Access Point fail, Siemens’ automatic load sharing will move traffic automatically to another HiPath Wireless Access Point—*transparently*.

Finally, Siemens architecture even supports fully-redundant networks. Imagine two co-located WLAN subnetworks, each with their own HiPath Wireless Controller and HiPath Wireless Access Points. If this were a switched architecture, traffic would remain distinct between the two. Siemens routed architecture allows users to move between these two subnets transparently, in response to changes in wireless network loading, user roaming, or a variety of other (not always welcome) conditions.

*The Siemens architecture is designed for high availability. Should a HiPath Wireless Access Point fail, nearby HiPath Wireless Access Points can be automatically re-configured to pick up the load, without losing user traffic or dropping user sessions. HiPath Wireless Controllers can be similarly configured for redundancy. One HiPath Wireless Controller can automatically pick up the load from another HiPath Wireless Controller regardless of where they are located (they don’t even have to be near one another). Every element of the Siemens architecture is designed for reliability. Even software images stored in HiPath Wireless Access Points and HiPath Wireless Controllers are redundant, allowing them to revert to previous loads if there is any doubt about the integrity of the latest release.*

## Virtualization

The concept of network virtualization is not new—indeed, *virtual* has been part of the IT lexicon for years. For purposes of this document and Siemens’ implementation of virtualization, we’ll use this term to

define a *decoupling of the physical nature of a given WLAN installation and the services provided on it*. We call this capability *Virtual Network Services*, and it's available via our *HiPath Wireless Convergence Software*. HiPath Wireless Convergence Software is actually a set of networking capabilities that allow network managers to provision user capabilities on a user-by-user or user-group basis. To keep things simple (and powerful), classes of capabilities (*policies*) can be defined and individual users assigned to these classes. The nature of specific classes can even change over time in response to user mobility, changing network conditions, and even time of day.

All mobile units and users are subject to individual (or group) security policies. Some users will be allowed full access to the corporate network, while others may be given Internet access only. Similarly, user security and billing policies can be assigned and traffic can be routed or prioritized based on their virtual network assignment; policies can even be assigned according to such parameters as time of day or specific location. Some users might, for example, be given access to information resources during normal working hours, but cut off from even reaching certain information at other times—or denied access if they are in a part of the building where they are unauthorized. HiPath Wireless Convergence Software is designed to provide far greater flexibility than traditional network-management approaches, with the added benefit of centralization, and without the need to configure virtual LANs (VLANs) throughout your network. All policies can be defined at the HiPath Wireless Controller, and automatically propagated to affect HiPath Wireless Access Points and users across the network without additional work on the part of network managers.

## Virtualization

Public-space WLAN deployments are one of the hottest applications for WLAN technology—and with good reason. With so many WLAN-equipped products now on the market, from PDAs to notebooks to even more options (like voice) in the near future, users are seeking uniformity of their network connections whether in the office, the home, or on the road via the rapidly-expanding “hot-spot” services. Thanks to 802.11, this objective is now easy to accomplish, and public-access WLANs are appearing in ever-greater numbers.

Today's public-access WLAN services, however, are really quite rudimentary, providing no security and fundamentally undifferentiated services to users. It is clear to us at Siemens that the requirements for hot-spots go far beyond this state of affairs.

Consider, for example, WLAN access in a convention center. Such facilities are usually quite large (both in terms of geography and network traffic load) and must serve many diverse communities. Such deployments can be quite challenging, but the power of HiPath Wireless Convergence Software greatly simplifies deployment and operations:

- Our *Walled Garden* facility can be used to provide location- and event-specific information as a default, for all users and at no charge.
- General Internet access can be provided to conference visitors on a paid basis, charged either via pre-subscribed service or per use (or based on time of connection or volume of data transferred).
- Wireless access for convention participants can be provided with inherent security, allowing secure connections to the Internet or VPN access to corporate intranets.
- Wireless Voice over IP services for conference organizers or specific classes of users can be provided network-wide with necessary traffic prioritization and without jeopardizing the security of the wired intranet or requiring new WLAN hardware.

HiPath Wireless Convergence Software provides a very broad range of possibilities and options for security and traffic management, and the definition of services to meet the needs of any venue and all using the same wireless infrastructure.

### The Next Step in the Evolution of Wireless LANs

Siemens HiPath Wireless is designed for real-world, scalable, available and manageable enterprise-class installations. Finally, the WLAN is a full peer with the rest of the network, functioning as a Layer-3 router rather than a Layer-2 switch, and providing capabilities far beyond those of architectures based on access points or WiFi switches. With unprecedented configuration possibilities, scalability from simple to global configurations, availability matching the requirements of enterprise-class and carrier-class applications, and security and management techniques possible only through the virtualization capabilities of our unique HiPath Wireless Convergence Software, Siemens is leading the evolution of WLANs to opportunities undreamed of only a few years ago. And we're not stopping here—because architectures aren't designed to be ends in themselves. We're working on additions, enhancements, and new capabilities that will continue to increase the value of routed architectures in the future and continue to deliver on the promise of true wireless mobility.

© Siemens Communications, Inc. 2005; All rights reserved.

The information provided in this whitepaper contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of the contract. Availability and technical specifications are subject to change without notice.