

Virtualization:

Taking the Wireless World Beyond Basic Access

...and providing flexibility limited only by network requirements and imagination

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

HiPath Wireless Convergence Software Siemens Enterprise-Class Wireless LAN Management

Executive Summary

HiPath Wireless is designed for real-world, available and manageable enterprise and carrier-class, mission-critical deployments. Such installations place special demands upon network management systems, and the need for a fundamentally new approach here has resulted in the development of Siemens HiPath Wireless Convergence Software. Through the use of virtualization, which allows an unprecedented degree of flexibility in managing both the WLAN infrastructure and specific users and mobile devices, HiPath Wireless Convergence Software allows a highly-dynamic set of services to be provided to users grouped by policy class. The dynamic nature of WLANs themselves is thus optimized. Variables such as time of day and the physical location of a given user can be used to define specific services. Applicable in convention centers, sports arenas, hotels, campus settings, hospitals, and many other venues, HiPath Wireless Convergence Software provides the provisioning, monitoring, and control that allows a WLAN infrastructure to meet the needs of diverse constituencies with appropriate efficiency, performance, and security.

Introduction

Anyone who has ever installed and managed a large wireless LAN network understands the problem: with so many network components, wireless options, access and control decisions, and security concerns, the job is tough. Part of the reason is that most contemporary wireless LANs are still better thought of as a collection of independent network components, rather than a single system designed for integration within the enterprise network. Those now deploying public-space WLANs are having a similar experience: distributed operations mean managing multiple subnetworks rather than a unified system.

The challenge is even more complex than this, however. Managing a wireless LAN network of necessity means that one must be concerned with not just infrastructure, but also mobile clients, both devices and users. After all, the WLAN exists to serve this constituency, and good wireless management focuses on what users need to do at least as much, if not more, than simply configuring, securing, and monitoring the infrastructure itself. However, most wireless LAN management strategies pay little attention to client devices and users, leaving this problem as an exercise for the network manager.

In designing HiPath Wireless, we looked beyond radio and network hardware and carefully examined how wireless LANs are and will be used, and what facilities would be required to close the loop with the client. This led us to a new way of looking at network resources and utilization, and to the concept of virtualization. Virtualization is not new — it has been a fixture and core element of much of computing and communications for more than 30 years, with concepts and capabilities like “virtual memory” and “virtual machines” now common. But the concept of virtualizing network facilities in wireless LAN networks has not been previously applied; it is an important, new innovation and the subject of this white paper.

HiPath Wireless Convergence Software provides the provisioning, monitoring, and control that allows a WLAN infrastructure to meet the needs of diverse constituencies with appropriate efficiency, performance, and security.

What is Virtualization?

In a nutshell, virtualization is the separation of the physical structure of a given object and what can be done with it. Virtual memory, for example, is a way of mapping physical memory to a much larger logical address space, and then using this construct as if it were physically real memory. In the case of networking, the physical structure of the network is usually quite simple — client devices and network elements (like routers and Ethernet switches) connected together with a given topological and geographic relationship between them. In general, any data can be sent from any node to any other node.

However, although networks can allow any device to access any data, this is seldom required or even desired. Rather, a key element of network management is to define what traffic flows are legitimate, and which must be prevented. The most common technique for this is network policy management, which defines the sets of network services or policies available to given groups of users. In many cases, however, these capabilities are simply defined by the network address or location or point of interconnect of a given client. Because wireless LANs allow this physical relationship to vary in the course of normal operations, static policies are clearly an unsatisfactory approach. Network management schemes designed for a wired environment simply do not carry over to wireless.

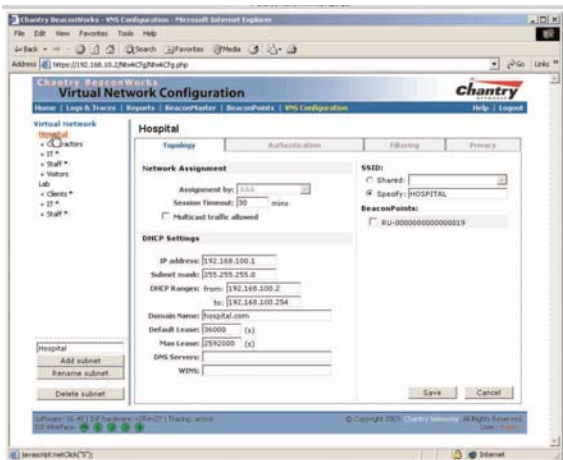
Virtualization allows individual network clients and other network elements to be managed and grouped exclusively by policy rather than their physical network location. Typical network management items such as access control and other security elements, traffic management including defining and managing quality-of-service (QoS), and packet filtering, can be assigned to policies and applied to devices and users on a unit-by-unit and user-by-user basis. But, again, given the dynamic relationship between clients and the wireless network, such variables as time of day or (current) physical location within the wireless infrastructure can also be used as the basis of policies, and provide great flexibility beyond static assignments.

We call this enhanced set of policy-based network management capabilities HiPath Wireless Convergence Software. Administered via a Web-based interface, HiPath Wireless Convergence Software provides unprecedented network configuration, management, security and control possibilities that are essential in WLAN deployments. HiPath Wireless Convergence Software provides a degree of flexibility not available in any other wireless network management approach — it even allows network management decisions to be made dynamically based on time and location.

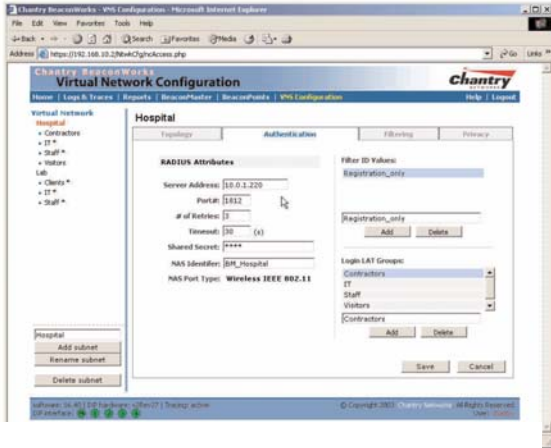
Factors, Policies and Policy Groups

To provide a logical view of the many otherwise disparate elements of HiPath Wireless Convergence Software, we have grouped these elements into three categories: Factors, Policies and Policy Groups.

- **Factors** – these can be thought of as “input” to HiPath Wireless Convergence Software; they are variables that feed the HiPath Wireless Convergence Software decision engine. Factors are discovered by HiPath Wireless Convergence Software at various points during the life of a given client session. These include the 802.11 Service Set Identifier (SSID, which can also be thought of as a wireless LAN’s “network name”), the specific Access Point that a client is connected to, and the MAC address



Administered via a Web-based interface, HiPath WirelessConvergence Software provides unprecedented network configuration, management, security and control possibilities that are essential in large-scale WLAN deployments.



HiPath Wireless Convergence Software can use 802.1x for authentication, and also provide a captive portal (or URL re-direct) mechanism that directs unauthenticated users to a Web page so they can provide login information.

of the client. In addition, client type or capability set can also be a factor, such as whether or not a client has specific service needs. This could be the case, for example, with voice-over-IP (VoIP) devices or with specific security capabilities — most production enterprise environments will enforce some form of authentication to ensure that users that gain access to the network are, in fact, permitted (by policy) to connect. HiPath Wireless Convergence Software can use 802.1x for authentication, and also provide a captive portal (or URL re-direct) mechanism that directs unauthenticated users to a Web page so they can provide login information. HiPath Wireless Convergence Software allows both authentication mechanisms to be deployed on the same physical infrastructure based on the needs or capabilities of the client device.

Finally, a unique property of HiPath Wireless Convergence Software is its ability to take into account factors that vary over time or location (i.e., to which HiPath Wireless Access Point the mobile unit is connected). We'll provide examples of the use of these two factors below.

- Policies** – these elements can be thought of as the “output” of HiPath Wireless Convergence Software. The value of Policies is determined based on the value of Factors. As seen in Figure 1, some policies are typically set once during a session as the user is authenticated. These include the authentication mechanism and the selection of an IP address for the user from a specific IP address pool. It is also possible to define an accounting mechanism for the user, which can be either RADIUS accounting or call-detail recording (CDR) records, and to set traffic steering policies. Examples include forcing traffic to a particular physical port (known within HiPath Wireless Convergence Software as an Egress Interface), and directing traffic to particular industry-standard virtual LANs (VLANs) or virtual private networks (VPNs) — both referred to as Virtual Router interfaces.

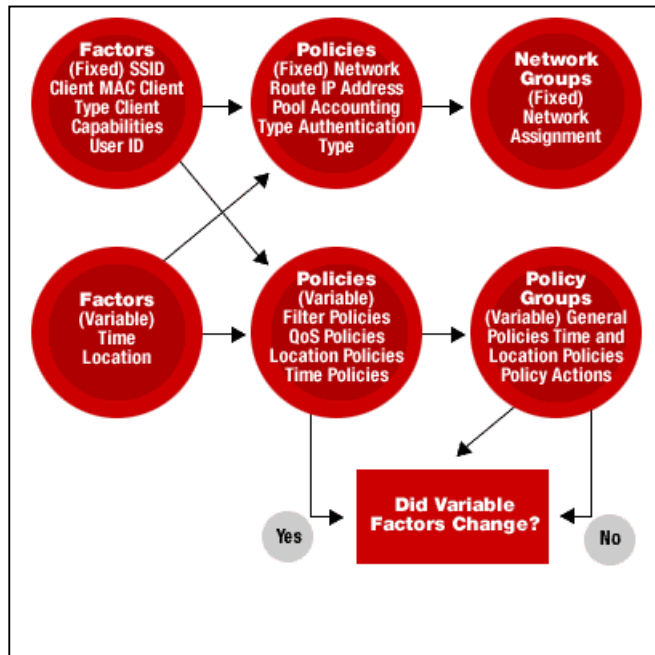


Fig. 1: A unique property of HiPath Wireless Convergence Software is its ability to take into account factors that vary over time or location.

A number of policies can also change once a session is established. Examples include packet filters, account policy, and QoS. Packet filters prevent specific types of traffic from reaching certain locations. The extreme case of packet filtering is the implementation of a *Walled Garden* where all traffic for a given user is directed to a particular default server based on authentication information or, more likely, the lack thereof in the case of general Internet access. Account Policy can also be changed, allowing charging mechanisms to vary, for example, based on location or time. And traffic prioritization can be used to set a QoS policy on a user-by-user basis. This could allow, for example, certain classes of users to receive greater responsiveness from the network based on their relative importance as determined by the network management staff.

Each policy has an action. For example, fixed policies make a decision based on how, when and where the user is connecting, then take the action to assign the user to a specific network with a specific accounting type. A packet filter policy makes a decision based on the contents of the packet, and then takes an action to permit or deny the packet. The output of an individual policy, and of policy groups, is the action that they take.

- **Policy Groups** – Policy Groups combine Policies into a cohesive user service and experience. Individual users are assigned to groups by the network management staff. Note, however, that membership in a given Policy Group can vary over time due to changes in Factors and thus Policies.

There are three types of Policy Groups: Network Assignment, General Policies and Time and Location Based.

1. *Network Assignment* is based on the IP Address Pool and Egress Interface or Virtual Router policies. Membership in this Group is assigned when a session is created and does not change.
2. *General Policies* are based on the Accounting Mechanism, QoS, and Packet Filters policies. Various combinations of these can be used to provide great flexibility in network and user management. Note that these Policies can change over time, allowing a significant degree of dynamic behavior.
3. *Time and Location-Based Policies* allow the integration of user/device location and time into network behavior; allowing network managers to customize access in ways never before possible (see the Examples section, below).

While all Policy Groups have default settings, the real value of HiPath Wireless Convergence Software is in its ability to vary network behavior based on elements that have not been considered in current network management architectures and products. Again, the key is *virtualization* — separating users and devices from their physical relationship with the network. Siemens will continue to evolve the services models over time to consider new factors and define new policies, along with developing APIs to allow integration into new models.

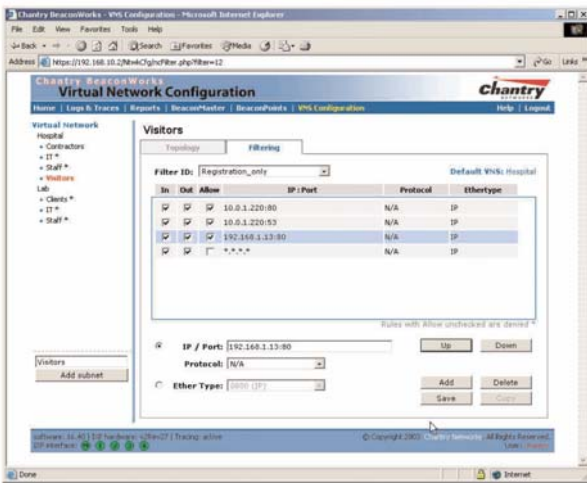
HiPath Wireless Convergence Software Samples

It's easiest to understand what HiPath Wireless Convergence Software can do via specific examples. What follows is designed to illustrate various possibilities — the objective of HiPath Wireless Convergence Software is to provide flexibility limited only by network requirements and imagination.

Example 1 — Visitor Access within the Enterprise

It's increasingly common for businesses to offer visitors wireless LAN-based access to the Internet and the Web. Sometimes visitors just want to check email (a real convenience while waiting for a meeting to begin or while sitting in the lobby), but occasionally they need critical information from their own company intranet. Perhaps they need the latest presentation file, or new product specifications, or sales numbers. There's always an excellent chance that the contents of the visitor's hard drive is out of date. Of course, an enterprise would be foolish to run an open shop, allowing anyone with a wireless LAN card to connect. Indeed, it's likely that all employees would need to authenticate with the network (through RADIUS or some other mechanism), and that encryption would be used for all of their traffic. In addition, certain employees would have access to specific resources on the network, such as servers and printers, while others would not.

Regardless, HiPath Wireless Convergence Software can assign the visitor to a group that only allows direct access to the Internet, with no access to any part of the enterprise network. It's assumed that the visitor would then establish their own VPN connection to their enterprise network, securing their information while using the wireless network on a guest basis. In addition, via the use of location data, a visitor would be prohibited from accessing the network except in certain parts of the building—a lobby or conference room, for example. And, guest traffic could be prioritized below most enterprise traffic to assure responsiveness for key staff that need it the most. Finally, using captive portal, certain guest users could be given access to a Walled Garden allowing limited use of network resources — a printer, for example. And detailed session ("CDR") records can provide a history for tracking unauthorized traffic, attempts at hacking, and access to RADIUS accounting information to enable the option for individual departments to be charged for the access provided to their visitors.



HiPath Wireless Convergence Software can assign the visitor to a group that only allows direct access to the Internet, with no access to any part of the enterprise network

Example 2 — Shopping Mall

It seems only natural that shopping malls, like most other public spaces attracting a potentially large number of people, will eventually provide WLAN access to the Internet. Using HiPath Wireless Convergence Software, the services provided can go far beyond simple Internet access. With respect to basic Internet access, services could be provided:

1. On an open-systems basis at no charge,
2. Free for "preferred shoppers,"
3. At a nominal charge (via credit card) to others.

But the possibilities get very interesting when location and time are introduced. For example, a given user would receive "mall news" on their "home page." This information would change as a user roams through the mall, highlighting specials and other attractions based on location. Time can also be an element — the home page could inform the user that the mall is closing shortly, or that specials might be available from a given merchant for a limited period of time. Walled Garden functionality can be used to easily implement a variety of access scenarios. At the same time secure access can be provided to mall employees, with different access privileges and policies than the public users without requiring the deployment of different physical infrastructure.

Example 3 — Sports Venue

A stadium or arena is a natural venue for HiPath Wireless because of the size of the facility (which demands a large-scale WLAN solution) and the requirement to provide services based on the needs of

a very diverse set of constituencies. Consider the following:

- The venue could provide basic access, on an unauthenticated, open-systems basis, to anyone with a client device. In this case, traffic will be directed to a Walled Garden site that provides basic information, such as upcoming events, recent score information, and a venue directory (food vendors, phones, restrooms, etc.).
- The Captive Portal facility could be used to authenticate premium users, or allow the entry of credit-card information for premium content (interviews with players, game highlights, or Internet access).
- Patrons in club box or premium seats would get higher quality-of-service (network responsiveness), with the ability to contact housekeeping, restaurant services, etc. VPN access could be configured for corporate boxes, and special services or even dedicated HiPath Wireless Access Points could be provided for the media.
- Service could be discontinued entirely within a certain number of minutes at the end of an event, to encourage attendees to leave in a timely manner, while service for club-box patrons and the media could be extended for a longer period.

Example 4 — Voice over IP on a WLAN

Voice services via wireless LANs are expected to grow in importance over the next few years, as the utility of wireless LANs expands to meet new opportunities. The key challenge in handling voice traffic on a WLAN is that such service must be time-bounded — only minimal latency is acceptable if usable voice service is to be provided. Such a service guarantee can be achieved via the prioritization of packets containing voice (or other time-bounded communications) ahead of other traffic. This is easily accomplished within HiPath Wireless Convergence Software by assigning voice users to a group with high quality-of-service. Such traffic is handled ahead of traffic with a greater tolerance for latency. Moreover, voice traffic can be secured separately from other traffic, again thanks to the facilities in HiPath Wireless Convergence Software.

Example 5 — Convention Center

Like stadiums and arenas, convention centers need a wireless LAN solution that is designed for large-scale deployment. Again, the diverse nature of the user community demands the ability to handle many different types of service. Consider the following scenarios:

- Access to general conference information could be provided via a Walled Garden.
- Certain organizers and other key staff would be given general access to the Internet to reach sponsors, suppliers, and key contacts. These users would also get higher-priority access to the wireless LAN and they would be able to use printers and servers not available to the general attendee.
- General access to the Internet would be provided only in certain locations to encourage attendees to focus their time on the conference.
- Information supplied in specific conference rooms would be tailored to a particular session.
- Careful accounting records could be kept to get an idea of the level of interest for particular sessions.
- WLAN service to exhibitors' booths could be tailored by creating separate, protected virtual networks quickly and with minimal overhead, particularly important in temporary and frequently-changing installations.

Example 6 — University Campus

Similarly, a campus setting is an excellent opportunity for the flexibility of a wireless LAN, with many colleges and universities now “unwiring” access to both the Internet and the campus intranet.

Differing levels of service could be offered to faculty and students. Guest access could be granted to visitors, while denying them the use of specific resources. Certain research projects and other sensitive information could be restricted to authorized users. During exams, access to the Internet could be restricted, but service could be provided for authorized access to information on an FTP server. Access to printers could be restricted to students from particular schools within the university. And, specific services could be based upon an individual student's specific location and/or time of day.

Example 7 — Hospital

Hospitals represent essentially all of the challenges of security and services in a wireless LAN environment. While hospitals have been using WLANs for many years, such networks have been suspect with respect to security — a problem now of paramount concern with the implementation of new legal requirements such as HIPAA. HiPath Wireless Convergence Software allows patient data to be secured using 802.11i-based wireless security as well as utilizing existing VPN services to provide security over the wired network. Access to sensitive information could be restricted to certain parts of the facility, and the disposition of this type of data could also be restricted by preventing access to certain sites or servers by users without access rights to this information. This ensures that data which belongs on the network and is subject to hospital control stays on the network and isn't subject to compromise. At the same time, paid or free Internet access could be provided to patients and visitors using the HiPath Wireless Captive Portal solution, and staff could simultaneously have access to wireless VoIP services throughout the entire facility. In this way, sensitive information can be protected while allowing casual or unauthenticated traffic to exist simultaneously on the same wireless infrastructure.

Example 8 — Hotel

Finally, the hospitality industry is adopting high-speed Internet access as a competitive differentiator. Hotel-based meetings can benefit in much the same way as convention centers.

Access can be provided in the lobby (for guest services and even Internet access), in guest rooms, and for staff use as well. A user registered for Internet access in their room could, of course, get access anywhere guests are allowed. Different charging mechanisms can be used based on time of day, traffic volume, or guest location. Hotel business centers could make their printing and fax services available to authorized users anywhere in the facility, boosting both revenue and guest convenience.

Conclusion

In addition to client access and services, HiPath Wireless Convergence Software provides a complete set of tools to manage the infrastructure. But the real value of a virtualized approach to network management is in the flexibility it brings — the ability to modify policies on the fly, and to take into account variables natural to the wireless environment, such as location and time. HiPath Wireless Convergence Software has been designed as an extensible platform for centralized management of the inherently fluid wireless environment. As outlined in this white paper, a wireless LAN is a valuable addition to many networked environments. HiPath Wireless Convergence Software completes the wireless LAN, allowing provisioning and management facilities that significantly increase the value of the WLAN with benefits for network managers and users alike.

© 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.