White Paper

Practical Considerations for Deploying 802.11n

A white paper from Siemens Enterprise Communications
February 2008

Communication for the open minded

Siemens Enterprise Communications
www.siemens.com/open

SIEMENS

Executive Summary

There is a lot of confusion surrounding the capabilities and status of the new 802.11n WiFi standard. The confusion is understandable since the standard is very broad and has been slow to develop, and even slower to finalize. (Full ratification is not expected until mid 2009). However, this glacial pace has changed in response to the 2007 announcement by the WiFi Alliance (WFA) to launch a compatibility testing and certification program for 802.11n infrastructure and clients based on the Draft 2 standard. The WFA Draft-N certification program has removed much of the deployment risk and accelerated the 802.11n market. Wireless hardware based on Draft 2 of the 802.11n standard is ready for deployment from a technical, interoperability and cost perspective, but there are some key issues to consider when planning your 802.11n network.

Two of the major issues to consider when planning for 802.11n are power consumption and WLAN architecture. 802.11n hardware from many vendors requires significantly more than the 12.95 Watts guaranteed by the current PoE standard, 802.3af. Their solution is to reduce the capabilities of their 11n AP to save power, or to force expensive upgrades to your network. It is important to select an 802.11n solution that operates at full dual-concurrent 3x3 MIMO when using 12.95 Watts. This is the only way to ensure that your company can take advantage of the full speed and reliability of 802.11n without requiring dramatic upgrades to your existing network or PoE infrastructure. Siemens is the only vendor supporting fully functional 802.11n within the 802af PoE standard.

Note: For third-party validation of this claim please refer to 802.11n Access Points and Power over Ethernet: Key Considerations by Craig Mathias at the Farpoint Group, February 2008 – www.siemens.com/us/open/802.11n/report

The second major issue to consider is the increased traffic on your core network arising from high-throughput 11n WLANs. It is important that your WLAN solution provide flexibility for traffic forwarding and network segmentation. HiPath Wireless' VNS architecture and intelligent traffic forwarding provide the required flexibility. Traffic can be forwarded locally using bridge mode, or managed at the controller using tunnelled mode. HiPath Wireless provides the best migration path to 802.11n, as customers are not obligated to upgrade their core network infrastructure.

As with any new technology, there are plenty of issues and caveats, but 802.11n is definitely ready for enterprise deployment today. It provides the WLAN performance and reliability that supplement the existing security standard (802.11i) and QoS standard (802.11e) and make WLAN as fast, secure and reliable as wired LAN.

802.11n will enable pervasive wireless deployment in the enterprise and may eventually become the dominant enterprise local area network (LAN) technology...Pervasive 802.11n deployment will also accelerate the growth of the enterprise Voice over WLAN (VoWLAN) market.

Source: The Burton Group, Paul DeBeasi – July 2007

Table of Contents

1.0 Getting Ready for the New Wireless

It is clear that WiFi is rapidly becoming ubiquitous in workplaces around the world. Tri-mode WiFi (802.11 a/b/g) is already standard on notebook computers, while more and more PDAs and Smartphones include 802.11 radios. According to Arizona market research firm In-Stat, WiFi chipset sales are likely to reach 300 million units in 2007, up 41% from 2006 when 213 million chipsets were shipped. However, for a number of reasons, until now WiFi deployments have been broad, but not deep. In their 2007 Wireless LAN State-of-the-Market Report (www.webtorials.com), authors Joanie Wexler and Steven Taylor found that although WLANs had been deployed by at least 86 percent of those companies surveyed globally, the majority of implementations were incomplete. The survey reveals that almost all companies have installed WLAN in common areas such as meeting rooms, lobbies and cafeterias, but only about half had installed WLAN into offices, cubicles and other work areas, and even less had deployed enterprise-wide WLAN.

Up until recently, there have been many reasons that companies were reluctant to deploy an enterprise-wide WLAN. Early wireless solutions had flawed security, poor reliability and relatively low data throughput. However, in the last few years, new standards for WLAN Security (802.11i) and Quality of Service (802.11e) have all but eliminated security concerns and doubts about the WLAN's ability to prioritize voice and video traffic. These days, companies can easily deploy an enterprise-wide WLAN that is as secure and reliable as a conventional wired LAN. In addition there is a new wireless standard in the works, 802.11n, which promises much higher data throughput and increased wireless range and reliability. The increased performance from 802.11n WLANs should eliminate the last roadblock to enterprise-wide WLAN deployment.

This document explains the new 802.11n technology, describes its strengths and weaknesses, and gives some advice on how best to migrate to 802.11n.

In-Stat believes that 802.11g will continue to dominate the Wi-Fi chipset market in 2007 and 2008, with 802.11n not reigning supreme until 2009.

Source: In-Stat, The Wi-Fi Chipset Market: Portable Connectivity Applications Drive Volumes, May 2007

2.0 What is 802.11n?

802.11n is an enhancement to the IEEE 802.11 wireless network standard that includes many new features to increase transmission speeds, range and reliability compared to 802.11a/b/g. The enhancements translate to 300 Mbps of raw data throughput and/or double the range compared to current 802.11a/g technology.

(Note that 802.11n can only achieve higher speed and reliability OR longer range, and, the recommendation is to deploy 802.11n for higher speed / reliability because most enterprises are focused on enhancing their mobile user experience.)

The 802.11n standard was first proposed in late 2003, but an early disagreement between the two different camps impeded the process considerably. Despite the politics involved, an early draft of 802.11n was released in late 2004. The "Pre-N" release provided higher network performance but offered very poor interoperability, and limited market acceptance. The lack of success in the important enterprise market, and the disproportionate number of issues arising from the half-baked standard prevented widespread adoption.

In late 2005, the warring camps put aside their differences and worked together to release an official 802.11n Draft 1.0 specification. Draft 1, released in March 2006 was an important political milestone for the standards committee, as it showed a commonality of purpose and willingness to work together and move forward.
However, technically it was less of a success. Wireless products based on Draft 1 suffered from poor performance, lack of vendor interoperability and weak backwards compatibility with 802.11 a/b/g hardware. Hardware based on the Draft 1 standard showed some success in the less demanding consumer market, but completely flopped in the important enterprise market. To many it seemed that the only way that 802.11n hardware was ever going to sell into the enterprise market was after the standard was finalized.

Then in late 2006, the WiFi Alliance (WFA) stepped forward to announce a certification program for products based on the upcoming Draft 2.0 standard. The WFA has a history of taking steps to facilitate the ratification and market acceptance of important wireless standards. They had introduced WiFi Protected Access (WPA) as an intermediate solution for wireless security while waiting for final ratification of the 802.11i standard and WiFi Multimedia (WMM) as an interim standard for 802.11e. The WFA Draft-N certification program was designed to ensure vendor interoperability between Draft 2 based products and to provide backwards compatibility with existing 802.11 a/b/g hardware. This certification program should be a tremendous boost to hardware vendors that have released early 802.11n Draft 2 product.

WiFi Alliance (WFA) Certified Draft 802.11n Label

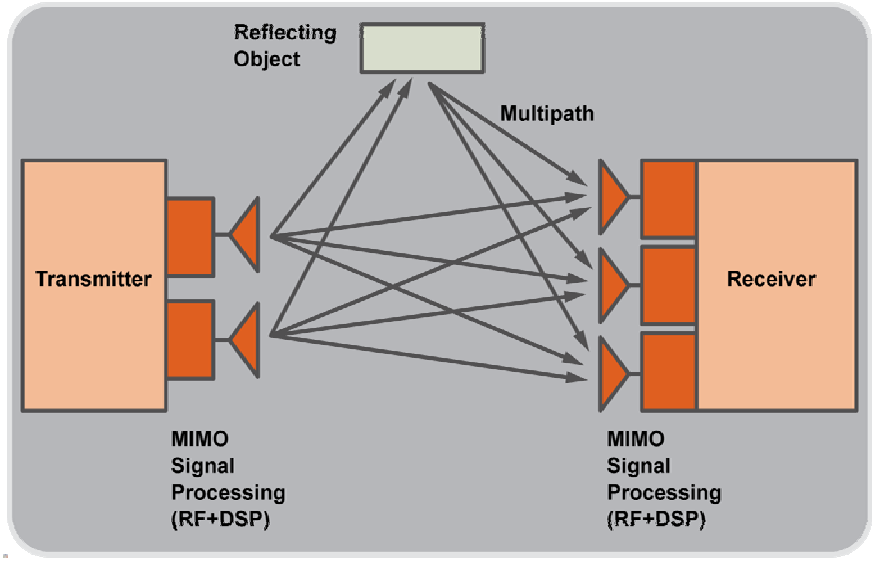
2.1 802.11n Technology Overview

Current wireless solutions operate in the 2.4 GHz radio frequency band (802.11g and 802.11b) or the 5 GHz radio band (802.11a). 802.11n can operate on the 2.4 GHz and/or 5 GHz bands. 802.11n provides backwards compatibility by supporting simultaneous 802.11a and 802.11n (802.11n/a) at 5 GHZ and/or simultaneous 802.11b, 802.11g and 802.11n (802.11n/b/g) at 2.4 GHz. However, in greenfield deployments an 802.11n AP can be configured to not be backward compatible with 802.11a or 802.11b/g. For simultaneous 2.4 GHz and 5 GHz support, two radios must be available on the AP. The 802.11n standard makes use of several innovative technologies to improve the range, throughput, and reliability of wireless LANs. The three primary innovations are Multiple Input Multiple Output (MIMO) technology, packet aggregation and channel bonding (40 MHz Channels). Together, these techniques

allow 802.11n solutions to achieve an approximate fivefold performance increase over current 802.11a/b/g networks.

Multiple Input Multiple Output (MIMO) technology

The heart of the new 802.11n standard is a technique called MIMO, or Multiple Input - Multiple Output. On the transmission side, MIMO uses Space Division Multiplexing (SDM) to transmit multiple data streams on the same frequency but over different spatial channels, increasing the transmission power and data that can be sent over the air. MIMO on the receiving end allows multiple signals to be combined, increasing signal strength and eliminating the effects of multipath fading. While previous wireless technologies had problems dealing with multipath signal reflections and attenuation, MIMO actually uses these reflections to increase the range and reliability over the wireless coverage area.



802.11n using Multiple Input - Multiple Output (MIMO) with Spatial Division Multiplexing (SDM).

Channel Bonding (40MHz Channels)

Normal 802.11a/g only supports 20 MHz channels that can carry a maximum of 54 Mbps of raw data per channel. 802.11n increases that throughput to 150 Mbps per channel, but also employs a technique called channel bonding to combine two adjacent 20 MHz channels into a single 40 MHz channel. The technique more than doubles the channel bandwidth to 300 Mbps throughput. Channel bonding is most effective in the 5 GHz frequency given the far greater number of available channels, while the 2.4 GHz frequency has only three non-overlapping 20 MHz channels.

Comparison of different 802.11 transfer rates (source: Intel Labs)

IEEE WLAN Standard	Over-the-Air (OTA) Estimates	Media Access Control Layer, Service Access Point (MAC SAP) Estimates
802.11b	11 Mbps	5 Mbps
802.11g	54 Mbps	25 Mbps (when .11b is not present)
802.11a	54 Mbps	25 Mbps
802.11n	**300 Mbps**	**150 Mbps**

Packet Aggregation

There are many MAC enhancements to 802.11n. Packet aggregation increases efficiency by aggregating multiple packets of application data into a single transmission frame. 802.11n networks can send multiple data packets with the fixed overhead cost of just a single frame. Packet aggregation is more beneficial for data applications such as file transfers. However, real-time applications (e.g. voice) do not benefit from packet aggregation. For voice, it is better to minimize the number of “packed” packets to reduce latency and eliminate jitter contentions.

2.2 802.11n Caveats

It is important to understand the potential downsides to any exciting new technology and 802.11n is no different. Later in this whitepaper we will present a list of practical issues to consider when migrating to 802.11n. However, there are a couple of basic issues to take into account when considering an 802.11n deployment, Power over Ethernet (PoE) and Traffic Forwarding.

Power over Ethernet

Power over Ethernet (PoE) is a technology used on wired Ethernet LANs (Local Area Networks). PoE is defined by the IEEE 802.3af specification and allows the electrical current necessary for the operation of a remote device to be carried over the Ethernet LAN cables rather than by power cords. PoE reduces network cost and complexity by reducing the number of wires that must be pulled to install a network. The 802.3af standard states exactly how much power is to be provided via the Ethernet cable. The specification guarantees 12.95 Watts of power to a remote device (at a maximum distance of 100 meters). A new PoE proposal, 802.3at, also called POE Plus, promises to double the raw wattage of 802.3af, to 30 watts, while also facilitating more dynamic power management. Unfortunately, 802at is still not finalized, nor is it expected to be before late 2008, if at all. In addition, 802.3at will require expensive upgrades to network switches or use of power injectors to facilitate the additional power being transmitted over the Ethernet lines. Furthermore, installation of 802at may actually void warranties on some network products designed to the 802af specification.

Given the advanced capabilities of 802.11n Access Points – MIMO, SDM, and multiple antennae – it is easy to see that the components may be very power hungry. This is especially true when running in full 3x3 MIMO mode, or when using two radios to support simultaneous 2.4 GHz and 5 GHz operation. Until recently, non-power optimized releases of 802.11n chips were unable to function in 3x3 MIMO using conventional 802.3af PoE. They need to operate off a wall plug, or step down to 2x2 MIMO and use a single radio, which has a dramatic impact on performance. Even more drastic measures like pulling a second Ethernet cable, or using short cable runs, have been promoted by some vendors.

Traffic Forwarding (Centralized, Distributed, Intelligent)

Another important issue to consider when planning for 802.11n is how much traffic your wireless network is going to generate on your wired LAN. Many enterprise WLAN architectures require APs to "backhaul" their traffic to a centralized controller, which then routes it across the network; multiple 802.11n APs can produce a significantly higher load on your LAN than legacy 802.11a/b/g APs. Depending on the size of the WLAN deployment, and how much application data is forwarded to the centralized controller, significant congestion may occur. The last thing any CIO wants to do is to build out a Gigabit Ethernet LAN – or 10 Gigabit network core – just to support their new 802.11n WLAN.

The central opportunity—and challenge—associated with 11n is higher performance. With APs capable of offering at least five times greater throughput, users are sure to be impressed ... provided your overall architecture can support the additional traffic.

Source: Dave Molta, Network Computing - October 2007

3.0 Migrating to 802.11n

The path to 802.11n can be easy and economical, but poor planning can result in less than satisfactory performance for both your new 802.11n WLAN and your legacy 802.11a/b/g WLAN. One of the toughest decisions facing the CIO is whether it is the right time to consider an 802.11n deployment.

3.1 Do You Need 802.11n?

Everyone wants more bandwidth, better reliability, more capacity and lower latency for their wireless network. Sensitive applications like VoWLAN are extremely susceptible to low bandwidth and high latency. However, the reality is that the vast majority of today's WLANs are under-utilized – typical Radio Frequency (RF) utilization is less than 20%. If you are considering using WLAN for simple data applications, then perhaps you can wait. If however, you need to accommodate high-bandwidth wireless data applications such as real-time medical imagery, or mobile PLC for manufacturing; or if you are currently in the process of evaluating and deploying an enterprise wide WLAN and do not want the expense of another upgrade cycle, then moving to 802.11n may be the right move.

3.2 Plan your Radio Spectrum

One of the first issues to consider is radio spectrum and transmission frequency. The 2.4 GHz spectrum is congested. It supports 802.11b/g Access Points, Bluetooth®, cordless phones, microwave ovens, industrial, medical, and scientific (ISM) equipment, and other licensed systems. The 5 GHz spectrum is less congested, but it has issues of its own. First, there are licensing issues in some countries that have to be considered. Another issue when selecting a spectrum is what type of legacy 802.11 network is currently in place. Usually it is 802.11 b/g running at 2.4 GHz. When deploying your new WLAN, you need to consider whether you want the 802.11n APs to support the legacy WLAN, or to operate independently.

To properly deploy 802.11n and take advantage of the wide channels (40 MHz) for improved data throughput, you need to channel bond. This could prove difficult for 2.4 GHz environments as there are only three non-overlapping channels to begin with, and bonding two of them would leave only one available non-overlapping channel. An 802.11n AP running 2.4 GHz and trying to use wide channels will surely cause disruption with existing legacy devices. 802.11n Draft 2 provides mechanisms to ensure backward compatibility and prevent co-channel interference. However, these mechanisms would prevent the establishment of 40 MHz wide channels when operating at 2.4 GHz and only allow 20 MHz channels (e.g. 1, 6, 11 in North America). This would defeat the major purpose of deploying 802.11n by reducing its bandwidth significantly. The 5 GHz spectrum provides many non-overlapping channels (23 in North America). An 802.11n AP running 5 GHz could dynamically change channels until two adjacent channels are clear to allow channel bonding while allowing coexistence with 802.11a and 802.11b/g APs and clients alike.

3.3 Suggested Migration Planning

1. You should seriously consider deploying 802.11n now if you are in the process of evaluating and deploying WLAN for the first time, upgrading to a controller based system from a fat AP solution, or significantly expanding your WLAN coverage area. You should also consider deploying 802.11n if you have reliability issues with your existing WLAN or your current or near future applications require more bandwidth.
2. It is highly recommended to deploy concurrent 2.4GHz and 5 GHz 802.11n APs, where the Access Point supports both 2.4 GHz and 5 GHz 802.11n simultaneously. Chances are that wireless clients will not all be upgraded to 802.11n at the same time. This makes it likely that by the end of deployment, the WLAN will need to support both legacy (802.11a/bg) and 802.11n clients for both 2.4 GHz and 5 GHz. This is especially true when you are overlaying 802.11n onto a legacy 2.4 GHz network. For 802.11n client purchases, it is best to purchase dual mode clients (2.4 and 5 GHz), or

at a minimum, 5 GHz clients. Ensure that your legacy clients and your client purchasing strategy are in harmony with the complete migration plan.

3. For customers with existing 802.11a/b/g networks, you should add 802.11n APs where needed as a replacement to an existing 802.11a/b/g AP. Configure both bands for 802.11n support to achieve ideal performance and reliability, while providing backward compatibility to legacy 802.11a/b/g clients. Note that in dense AP deployments, channel bonding for the 2.4 GHz band should be disabled, since it will cause channel interference.
4. For greenfield customers, a dual mode 802.11n AP (2.4 GHz and 5 GHz) is highly recommended. One must take care that the client strategy also supports this approach because in protection mode (support of legacy clients using 802.11a/b/g), the performance gain may become negligible.
5. Note that VoWLAN clients will remain 802.11g or 802.11a for a number of years because of their power consumption, but voice quality and reliability will improve with 802.11n.

802.11n AP Placement Considerations

RF Planning software is an important tool when planning any WLAN deployment. This is especially true for 802.11n APs. Some of the limitations of legacy WLAN technologies, i.e. channel conflicts, hidden nodes, and multipath attenuation, are no longer a concern because 802.11n makes it much easier to plan for AP placement. Remember to include power issues when you are planning for 802.11n. The ability to reuse existing PoE connections and simply replace existing APs at their existing locations can save significant dollars when upgrading to 11n networks.

Another key benefit of 802.11n is its extended range. However, when doing a site survey it is important that one does not rely on this extended range to cut corners and decrease AP density. Decreasing AP density can cause oversubscription and degraded performance for all connected clients. For the enterprise, it is more advantageous to focus on the improved bandwidth capability instead of increased range.

Good Neighbor, Bad Neighbor

Today's 802.11a/b/g technology uses a single channel, and does not provide channel bonding. For the 2.4 GHz spectrum, since there are only three non-overlapping 20 MHz channels, turning on channel bonding will reduce the number of channels to one, and reduce the overall performance of your network and by increasing interference with neighboring APs. For the 5 GHz spectrum, this is less of an issue. For example, since there are 23 non-overlapping channels available in the North America, even with channel bonding there will be 11 non-overlapping 40 MHz channels. It is recommended to implement 802.11n at 5 GHz if possible or if 2.4 GHz is required, to be friendly with neighbors by not enabling 40 MHz (channel bonding).

Wireless Intrusion Detection and Prevention

Wireless Intrusion Detection and Prevention Systems (WIDS/WIPS) also need to be updated to work with 802.11n. It is very important to detect 802.11n rogue APs even on your legacy 802.11 a/b/g network. Customers that have already deployed 802.11a/b/g APs with dedicated sensor software should try to leverage those to detect rogue 802.11n APs on the 2.4 GHz and 5 GHz bands if possible.

Client Selection

There are a wide variety of 802.11n clients available. Performance, power management and interoperability are the three main considerations when purchasing an 802.11n client. Clients will benefit the most from MIMO and packet aggregation for file transfers and data backups. Interestingly, with channelization and MIMO power-conservation, which enable multiple spatial streams only when they are needed, 802.11n performance features may end up saving power in some cases because a client is active on the WLAN for shorter durations. Finally, the most important element is client compatibility with your Access Point. It is highly recommended to purchase WFA 802.11n Draft 2 certified clients.

4.0 HiPath Wireless and 802.11n

The HiPath Wireless product family includes wireless Controllers, Access Points and management software. A HiPath Wireless network is extremely scaleable as it can support thousands of APs and tens of thousands of client devices. High-availability features in the controllers and dynamic RF compensation in the APs create a robust, fault tolerant WLAN infrastructure for mission critical enterprise solutions.

4.1 Advanced Power Management

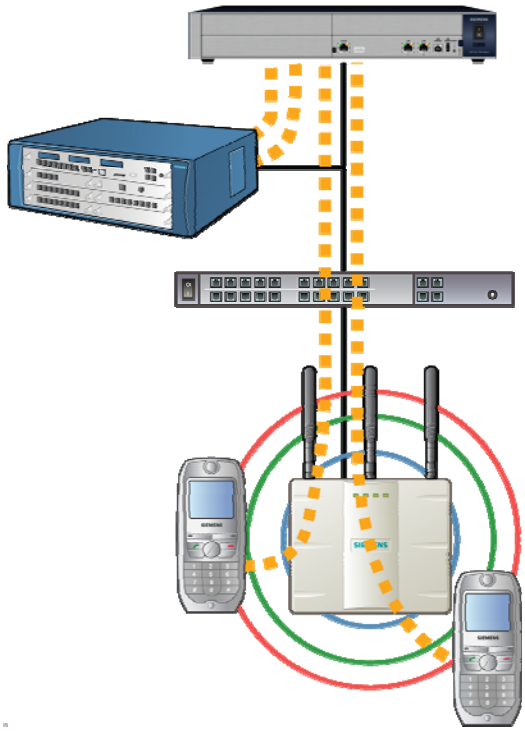
In many WLAN deployments, power to distributed APs is provided by PoE (802.3af). For legacy APs running an 802.11 a/b/g network, the guaranteed 12.95 Watts is ample for full operation. However, depending on how they are manufactured and configured, 802.11n Access Points can be power hungry. Depending on which Draft 2 chipset is included, and how power conscious the manufacturer is, an 802.11n AP running dual radios in 3x3 MIMO can consume upwards of 18 Watts. To allow these power hungry APs to work using PoE, they need to either step down their operational capability (MIMO 2x2, and/or single radio), or if present, they can use dual Ethernet connections and manage two 802.3af PoE connections to provide the required power. The last choice, and probably the most distasteful, is to upgrade the wiring closet to 802.3at, the proposed next-generation PoE specification.

By waiting for the latest 802.11n Draft 2 chipset and implementing a number of innovative power optimizations, HiPath Wireless APs can run full 3x3 MIMO using just over 12 Watts of power. This means that HiPath Wireless 802.11n APs are the only products on the market today that can operate at full 3x3 MIMO dual band and utilize existing 802.3at PoE connections. They do not force network reconfiguration and re-wiring or expensive upgrading. To date, Siemens is the only vendor supporting fully functional 802.11n within the 802af PoE standard.

4.2 Virtual Network Services (VNS) Architecture

HiPath Wireless uses a unique Virtual Network Services (VNS) Architecture to segment and map wireless networks to the topology of an existing wired network. A VNS is a policy-based virtual network that controls traffic flow, wireless policies (security, mobility, QoS) and administrative domains for the wireless network without requiring any changes to the wired IP network. Each VNS can be dynamically configured to groups of wireless devices based on organization, security profile, applications, traffic patterns, geographic location or any other grouping. A VNS can be deployed transparently to the existing wired network, allowing customers to securely provide a variety of unique services using the same WLAN infrastructure. The chief advantages of VNS over conventional segmentations schemes like VLANs is that all segments and policies are centrally defined and configured at the controller just once. The configurations are then pushed out across the entire network; there is no need to re-configure multiple switches each time a change is required, and the wired network can remain untouched.

With the VNS architecture, network traffic flow is defined on a per-segment basis. There are two forwarding modes possible; tunnel mode and bridge mode. When using tunnel mode, all access and usage policies are applied at the central controller. All wireless traffic is forwarded to the controller, which in turn routes the traffic to its destination on the wired or wireless network. In bridge mode, the central controller still provisions access and usage policies, but some functions are now performed at the AP.



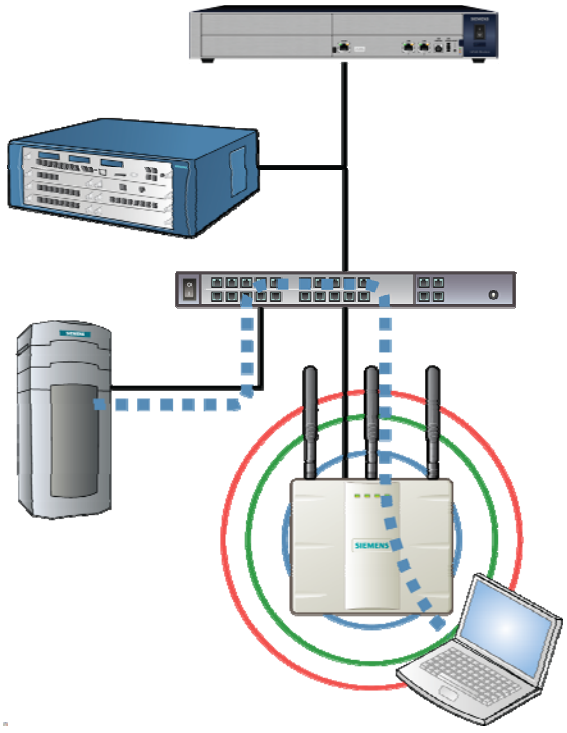
Network Traffic Flow – Tunnelled Mode

All traffic routed through WLAN Controller. Traffic stays near central resources

Best suited for:

- Low bandwidth
- Frequent roaming
- "Skinny" apps
- Low latency networks

The advantages of the VNS architecture are the virtualization of both user groups and traffic flows – central vs. distributed traffic management. This allows IT managers to dynamically select the best configuration without having to change any hardware. Since multiple VNS's can be supported on a single controller, both types of architecture can co-exist on the same WLAN infrastructure. For example, peer-to-peer traffic and high bandwidth applications such as video are better served with a VNS segment configured in bridge mode, whereas guest access may be better served in tunnelled mode to provide strict centralized network security policies (run through a wired IDS system, etc.). HiPath Wireless's VNS architecture supports the best of both worlds.



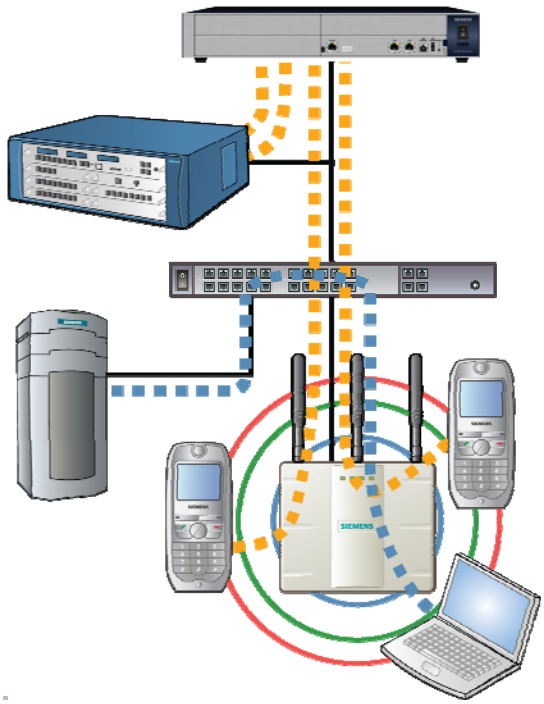
Network Traffic Flow – Bridge Mode

Management traffic routed to WLAN Controller. All other traffic routed at the AP.

Best suited for:

- High bandwidth
- Portability, not mobility
- Application resiliency
- Decentralized networks

With the advent of 802.11n, wireless architecture and traffic forwarding capabilities become strategic decision points. The high data throughput of 802.11n will generate much higher traffic flow, which is best served by locally bridging the traffic from the AP directly to the Ethernet at the edge so that the core is not taxed with double traffic to and from the controller. Deploying your 802.11n WLAN should not require a LAN upgrade to Gigabit or 10 Gigabit Ethernet. For applications like VoWLAN that require seamless call roaming, or guest access that demands centralized security, traffic should be tunneled directly to the controller. Because of its VNS architecture, HiPath Wireless provides the best migration path to 802.11n.



Network Traffic Flow – The Best of Both Worlds; Bridge & Tunnelled

Because of its VNS architecture, HiPath Wireless provides the best migration path to 802.11n.

4.3 The Real Cost of Upgrading

Early adopters of 802.11n should be aware of the potential higher costs associated with early 802.11n APs. It is estimated that early Draft 2 solutions can cost as much as 100% more than mature Draft 2 solutions. Table 2 provides a comparison of HiPath's 802.11n AP with other leading solutions.

Feature Comparison Checklist	HiPath Wireless AP3600	Other 802.11n APs
Radio Operation	Dual concurrent 802.11n radios	Operation limited to a single 802.11n radio
Power Requirements	802.3af – allows use of existing PoE implementations	802.3at – not yet standardized specification – requires new PoE wiring closet switches
10GE on the Controller	Not required	Required for most solutions; this may require upgrading backbone also depending on AP traffic distribution

5.0 Conclusion

Over time, 802.11n will become the dominant enterprise LAN technology – not just the dominant wireless LAN technology. From a technical, interoperable and cost effective perspective, 802.11n is ready to go today. However, enterprises interested in 802.11n should think carefully about the long-term strategic implications of their network architecture, as well as cost implications that could be borne by something as seemingly innocuous as power consumption. 802.11n is not just an Access Point replacement decision; it may have implications throughout the entire wired network. In the worst case scenario, the enterprise may be forced to upgrade their corporate LAN to 10Gigabit Ethernet or their PoE infrastructure to 802.3at to compensate for poorly designed 802.11n products or a poorly executed deployment. Now is the perfect time to plan your migration strategy and evaluate the architectural impact and the available products.

Siemens HiPath Wireless provides a complete portfolio of wireless products for your WLAN deployment. The addition of the new 802.11n wireless Access Point to their award winning line-up makes HiPath Wireless the only vendor in the market with a product supporting fully functional 802.11n within the 802af PoE standard. In addition, HiPath Wireless' innovative VNS architecture and intelligent traffic forwarding is ideally suited for 802.11n in either greenfield or backward-compatibility deployment. Because of its VNS architecture, HiPath Wireless provides the best migration path to 802.11n.

Siemens Enterprise Communications is a thought leader and innovator in the enterprise communications industry. We are one of the leading players in the market with full coverage of all the relevant markets from a strong European base with global reach. Our people have the passion, commitment, skills and know-how to deliver a broad range of cutting-edge technologies, outstanding products and professional services. All with the support of an enterprise that has the financial strength to outperform the rest in this competitive and consolidating market.

... .11n is going to shake up the WLAN space perhaps like no development ever has before. And it's all going to happen with unprecedented market velocity.

Source: Craig Matthias, Principal, Farpoint Group - 2007

Munich-based Siemens Enterprise Communications GmbH & Co. KG, a wholly owned subsidiary of Siemens with more than 15,000 employees, is one of the world's leading vendors of Open Communications solutions for enterprises of all sizes. Our products, solutions and services make business processes more productive, faster and more secure - with any device, network or IT infrastructure.

Communication for the open minded

Siemens Enterprise Communications
www.siemens.com/open

Printed in Germany.