SMART MOBILE™: NEXT-GENERATION WLAN ARCHITECTURE FOR HIGH PERFORMANCE NETWORKS

TRAPEZE smart mobile™

EXECUTIVE SUMMARY

The evolution of wireless local area networking (WLAN) is facing a new set of requirements, driven by a number of technology and business trends. One is the imminent arrival of the 802.11n standard, which will increase wireless traffic loads by more than 10 times—far exceeding the throughput capacity of today's wireless switches. Another trend is the acceleration in enterprise adoption of voice over IP that is dramatically cutting phone costs. Enterprises are eager to extend VoIP over wireless, but current generation WLANs cannot support voice at enterprise-wide scale. Additional trends include the need to extend wireless service outdoors throughout the campus, quad and warehouse, as well as the need to maintain state-of-the-art wireless security and minimize management and operations costs as wireless networks increase in size, criticality, and pervasive use.

Today's WLAN architectures fall under one of two approaches—distributed or centralized. A distributed architecture places all the intelligence in the network access points. This approach is also known as "fat AP." A centralized architecture places all the intelligence in one or more WLAN controllers rather than the AP. This approach is also known as "thin AP." Neither of today's approaches provides the traffic optimization necessary to handle the emerging requirements for next generation WLANs, including cost-effective implementation of 802.11n networks and large-scale voice over WLAN deployments, while retaining centralized control and management.

Recognizing the limitations of current approaches, Trapeze Networks has developed a new WLAN architecture called Smart Mobile™. Smart Mobile introduces an innovative breakthrough called "intelligent switching," which combines the advantages of both centralized and distributed approaches. As a result, Smart Mobile allows organizations to adopt high-performance 802.11n networks, deliver high-quality voice for hundreds of users, and scale their WLANs across the enterprise indoors and outdoors, without compromising security or manageability and without having to upgrade their existing switching or WLAN controller infrastructures.

INTRODUCTION

Over the last few years, enterprises have increasingly deployed wireless local area networks (WLANs) to drive productivity, reduce cost, and improve work quality. While the return on investment has been substantial, enterprises recognize they have reaped only a fraction of the potential benefits. Today, they are looking to leverage wireless technology for even greater value, by extending it to more users and by expanding the scope of wireless services and applications.

At the same time, a number of business and technology trends are creating a new set of requirements for wireless networks that can deliver the increased value that enterprises are demanding. Emerging developments such as the high-throughput 802.11n standard hold the promise of providing significantly more powerful WLANs. But current WLAN architectures stand in the way of realizing those benefits. Consequently, a new approach is needed to deliver the next generation of high performance wireless networks.

This paper identifies the requirements for next-generation WLANs, examines the limitations of existing approaches, and describes an innovative WLAN architecture from Trapeze Networks called Smart Mobile™, which overcomes those limitations.

FIVE REQUIREMENTS FOR NEXT GENERATION WLANS

As enterprises develop their strategies for deploying new WLANs or evolving existing ones, five key requirements must guide their evaluation. The choices they make today will profoundly impact their ability to maximize value from their WLAN investments and minimize their costs throughout the WLAN life cycle.

- **802.11n.** The IEEE 802.11n standard, which is more than ten times faster than 802.11b/g or 802.11a, is expected to be ready for enterprise deployment in the second half of 2007. Any new WLAN investments must support 802.11n when it's available. For existing investments, the enterprise must examine whether its WLAN infrastructure will be crippled by the 10-fold increase in throughput that 802.11n will bring and whether it can move to 802.11n without exorbitant upgrade costs.
- **Voice over WLAN.** Enterprises have accelerated their adoption of voice over IP to dramatically reduce phone costs, and they are eager to extend VoIP to wireless. But voice over WLAN (VoWLAN) has had limited enterprise adoption, because current generation WLANs cannot deliver toll-quality service to large numbers of users. Next generation WLANs must overcome this limitation to support hundreds of roaming users with clear, reliable service.
- **Seamless indoor and outdoor coverage.** Enterprises want to extend mobility services across their campuses, including outdoor and unwired areas such as shop floors and warehouses. Enterprise users require the same, consistent enterprise feature set whether indoors or out. To get maximum functionality at the lowest cost of operation, enterprises need a single wireless data/voice infrastructure that covers indoors and outdoors.
- **Comprehensive security.** Security remains the top concern for enterprises deploying WLANs. To meet their business continuity and data privacy requirements, enterprises need a strong multi-layer approach, including state-of-the-art technologies for endpoint security such as Microsoft Network Access Protection (NAP) or the Trusted Computing Groups' Trusted Network Computing (TNC); advanced Wireless Protected Access (WPA2) authentication and encryption; and Federal Information Processing Standards (FIPS) compliant wireless intrusion detection (WIDS) and prevention (WIPS).
- **Centralized management.** A large WLAN may comprise thousands of access points (APs), tens or hundreds of switches, and tens of thousands of mobile users who need constant connectivity to their critical data and voice applications. As wireless networks continue to increase in size, and as mobility becomes pervasive, the ability to efficiently manage the WLAN becomes absolutely critical.

CURRENT APPROACHES TO WLAN ARCHITECTURES: WHY DISTRIBUTED OR CENTRALIZED ALONE CANNOT MEET THE NEW REQUIREMENTS

Current approaches to WLAN architectures follow two fundamental models:

- In a *distributed* architecture, the access points are highly intelligent—each AP acts as a self-contained router, equipped with all the intelligence required to associate with client devices and manage traffic flow. This approach is also known as the “fat AP” model. Cisco’s Aeronet products are a prime example of this architecture.
- In a *centralized* architecture, the APs have minimal or no intelligence and are instead connected to a WLAN controller that controls the AP and its associated client traffic. This approach is also known as the “thin AP” model. Aruba Networks is a prime example of this architecture, as is Cisco’s Airespace product line.

Each architecture has its advantages and disadvantages but neither alone addresses the complete requirements for next generation WLAN performance.

Distributed (“Fat AP”) Architecture: Pros and Cons

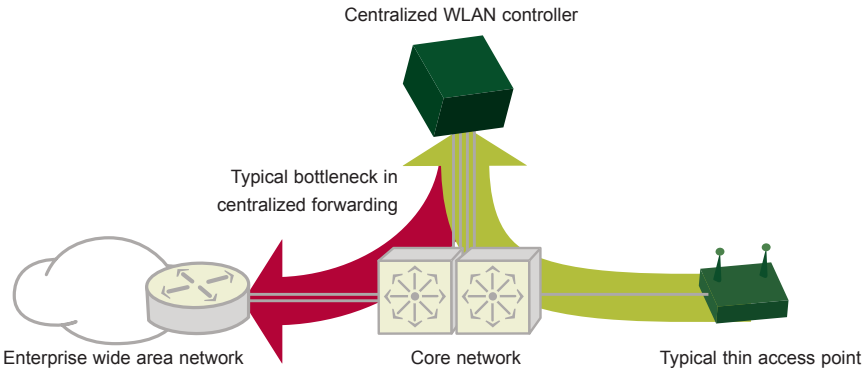
Fat APs were the first generation of WLAN products. Many organizations initially used fat APs to add wireless to their wired networks. The fat AP model was simple to implement, because fat APs could be easily and quickly connected as standalone devices. Many IT organizations liked the ability to optimize traffic flows, enforce firewall policies such as packet filtering and prioritization, and distribute cryptography operations at the AP. But fat APs operate independently of each other—requiring individual software, configuration and management—and the operation of any one AP can impact others. So as more are added to the network, IT discovered it was very difficult and expensive to manage numerous fat APs in a coordinated fashion.

Centralized (“Thin AP”) Architecture: Pros and Cons

The need to deploy wireless more broadly and cost-effectively led to the rise of the centralized WLAN architecture. In this model, one or more WLAN controllers in the data center handle the intelligence for thin APs placed throughout the enterprise network. Centralizing the intelligence created possibilities for centralized software and configuration management, as well as sophisticated controls for co-ordinated operations such as RF AutoTune and WIDS/WIP, allowing IT to manage all of the WLAN switches as a single entity, while the switches manage the individual APs. Traffic encryption and decryption, traffic forwarding, and policy enstantiation, such as packet filtering and prioritization, are handled by the central WLAN controller.

A centralized architecture improves control and management and lowers operational costs, but it is highly inefficient in forwarding traffic. Thin APs forward all traffic to the central WLAN appliance, which then forwards it to its ultimate destination (in contrast to taking the more direct data path to the destination in a distributed or "fat AP" architecture).

Centralized Only Architectures Cannot Support Next-Generation Wireless Applications

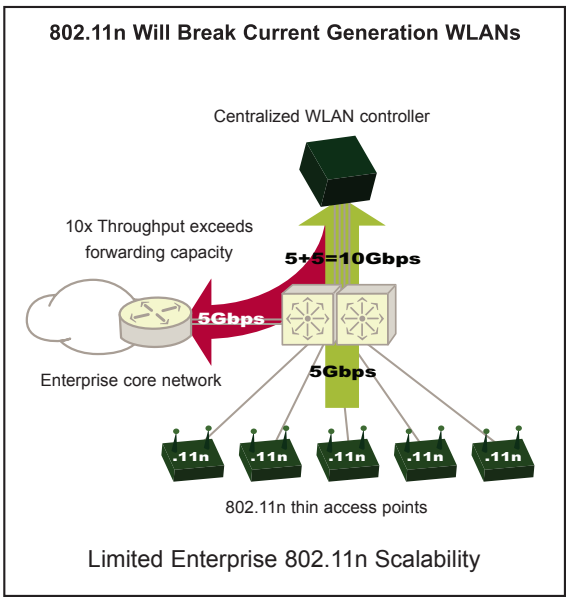


Centralized network forces the applications to adapt to the network

As a result, wireless traffic on the wired network is doubled, because every wireless packet takes a longer-than-necessary, indirect path to its destination, traversing the wired infrastructure twice—once to the WLAN controller, then again to the desired destination.

Centralized WLANs Cannot Handle 802.11n without Costly Upgrades

This doubling of wireless traffic may be acceptable at today's peak rates of 54Mbps, but with the 10-fold increase in throughput that 801.11n will bring, a centralized-only architecture becomes impractical, even in the most high performance campus Ethernet infrastructures. Additionally, the need to handle all of the WLAN encryption centrally will overwhelm current generation WLAN controllers. At a minimum, enterprises deploying a centralized-only architecture will have to double their switching power and upgrade the WLAN controllers to handle 802.11n, which negates the attractive simplicity and economics of an overlay WLAN.



Limited Enterprise 802.11n Scalability

Centralized WLANs Cannot Support Large-scale Voice Deployments

In addition to its traffic handling inefficiencies, a centralized architecture does not easily scale voice service beyond a handful of roaming users. The time it takes for traffic to go from the client to AP through the central controller and out to its destination increases latency and jitter. Voice quality is further impacted when the WLAN spans multiple buildings and many APs are physically located across the campus switching infrastructure far from the WLAN controllers, compounding the centralized forwarding problem.

BEYOND ONE SIZE FITS ALL: A NEW APPROACH IS NEEDED

The limitations of both fat AP and thin AP models clearly indicate that a new approach is required. It is also clear that a "one size fits all" approach is not optimal, because different applications can have different needs. For example, voice over wireless requires very low latency and jitter, but centralized forwarding cannot provide the traffic optimized packet flow required to deliver toll-quality voice at scale. In contrast, security-sensitive applications like guest access benefit from centralized forwarding, by consolidating traffic to a secured segment outside the enterprise firewall and adjacent to the internet services that guests are likely to seek first. Control can be maintained at the WLAN switch, ensuring that guest traffic remains strictly segregated from the internal network.

What's needed is a WLAN architecture that is not restricted to either a centralized or distributed forwarding model but instead is optimized to support different application requirements. In response, Trapeze Networks developed Smart Mobile™—a next-generation WLAN architecture designed specifically to overcome the limitations of both distributed and centralized architectures.

HOW SMART MOBILE WORKS

Smart Mobile significantly evolves today's current approaches by merging the advantages of both centralized and distributed architectures. In contrast to both centralized and distributed architectures, Smart Mobile does not restrict intelligence to either the center or the edge of the network. Instead, intelligence exists throughout the network, at both the center and at the edge. This allows the network to adapt to the needs of the underlying application so that performance is optimized based on the application's requirements.

Key elements of the Smart Mobile architecture, which will be discussed in more detail below, include:

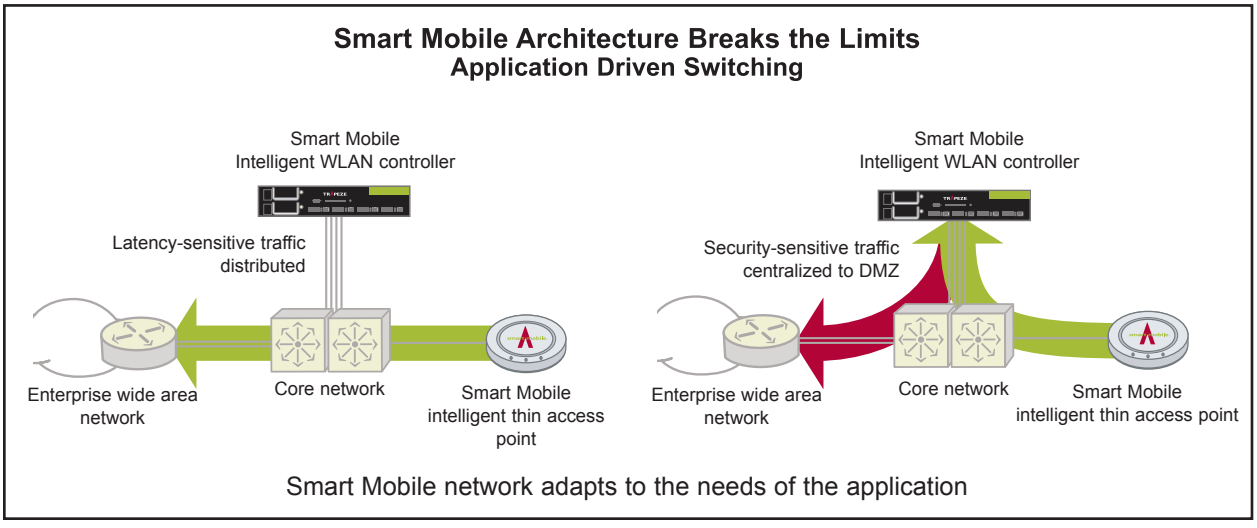
- **Application optimized intelligent switching**: Smart Mobile is built on the principle that the application requirements should drive the WLAN architecture, resulting in a flexible switching model. Traffic can be

forwarded at the controller (centralized) or at the AP (distributed), depending on the type of traffic and the enterprise's policies and preferences.

- **Distributed cryptography.** Smart Mobile enables network managers to centrally define policies for authentication, encryption, and packet filtering based on users' identities, but these policies can be enforced at the AP once the data flow is decrypted. This approach maximizes scalability, both because WLAN controllers do not experience an increase in encryption load when there is an increase in the number of APs or when aggregate throughput requirements increase substantially (e.g., due to 802.11n), and because cryptographic performance is increased with each additional AP installed.
- **Enterprise-wide extensibility.** Smart Mobile delivers a comprehensive architecture to support consolidated operations for indoor/outdoor application mobility throughout the enterprise, by deploying technologies such as wireless back-haul, as well as mesh-portal and mesh-point services.
- **Comprehensive security.** Smart Mobile delivers a cohesive strategy to support all the critical elements of a comprehensive security model, including endpoint assurance, advanced authentication and encryption, application-optimized traffic flow, firewall policy enforcement, and uncompromising intrusion protection.
- **Centralized management.** Smart Mobile retains fully centralized WLAN management and control, integrating complete lifecycle management functionality in a single management console.

APPLICATION-OPTIMIZED INTELLIGENT SWITCHING

Today, organizations must choose a WLAN architecture—either distributed (fat AP) or centralized (thin AP)—and force-fit their applications to that architecture's needs. Smart Mobile eliminates this either/or compromise. With the Smart Mobile architecture, the APs are neither thin nor fat. They are "smart." Smart Mobile APs have sufficient intelligence to perform cryptography and policy enforcement, as well as data forwarding, throughout the distributed WLAN, at the point closest to the wireless client. Enterprises can configure the Smart Mobile WLAN to specify which data gets forwarded centrally and which gets forwarded on a distributed basis.



Smart Mobile network adapts to the needs of the application

Centralized Forwarding in Smart Mobile: The WLAN Controller Forwards the Data

As in a typical centralized only WLAN, client data traffic can be delivered directly to the WLAN controller, with the WLAN controller forwarding it through the network. The return traffic is also forwarded through the WLAN controller, which then forwards it to the AP and on to the client station. Local file, print and application traffic would take a similar path configured for centralized forwarding.

Centralized QoS and Firewall Policy Enforcement
When wireless to wireless traffic is forwarded centrally, Smart Mobile ensures quality of service (QoS) for applications like voice. It uses Wi-Fi Multimedia (WMM) over-the-air, mapped to DiffServ and 802.1p for traffic prioritization and management, enforcing QoS throughout the core network. QoS is enforced as part of the design of the forwarding plane of the Mobility Exchange. The Mobility Exchange also enforces the firewall and location policy for strong security and control.

Distributed Forwarding in Smart Mobile: The AP Forwards the Data

In distributed forwarding, the access point forwards the traffic without having to send it through a WLAN controller. This makes it possible to deploy voice over WLAN on a massive scale, because voice packets travel the shortest path possible, thus minimizing latency. Distributed forwarding also enables migration to 802.11n without having to upgrade existing WLAN controllers, because it reduces the offered data forwarding load on the controller.

"Station Switching Records" Enable AP-based Distributed Forwarding
To enable distributed forwarding, Smart Mobile introduces the distribution of switching data learned by the central WLAN controller to the AP in the form of a "station switching record" (SSR). The Mobility Exchange controller distributes a SSR to the AP for each associated client. The SSR is distributed after the endpoint client station is validated and the client is authenticated, which ensures a secure session. The SSR contains the station address, VLAN, subnet and gateway data, tag and local switch flags, firewall and QoS policy, and broadcast suppression information.

Once the AP has the SSR for an authenticated client, the client traffic is delivered directly from the AP and no longer needs to go through the Mobility Exchange controller. The AP forwards the traffic through the network as directly to the destination as the attached network segment allows. The return traffic follows the same path through the AP. Local file, print and application traffic follow a similar path.

Distributed QoS and Firewall Policy Enforcement
When wireless to wireless traffic is forwarded on a distributed basis, Smart Mobile ensures quality of service (QoS) for applications like voice. Just as with centralized wireless to wireless QoS, Smart Mobile uses Wi-Fi Multimedia (WMM) over-the-air, mapped to DiffServ and 802.1p, enforcing QoS throughout the core network. But in the case of distributed wireless to wireless, QoS is enforced in the Mobility Point based on the SSR data provided by the Mobility Exchange distributing QoS policy enforcement. In addition, the Mobility Point enforces the firewall and location policy for distributed forwarding.

DISTRIBUTED CRYPTOGRAPHY

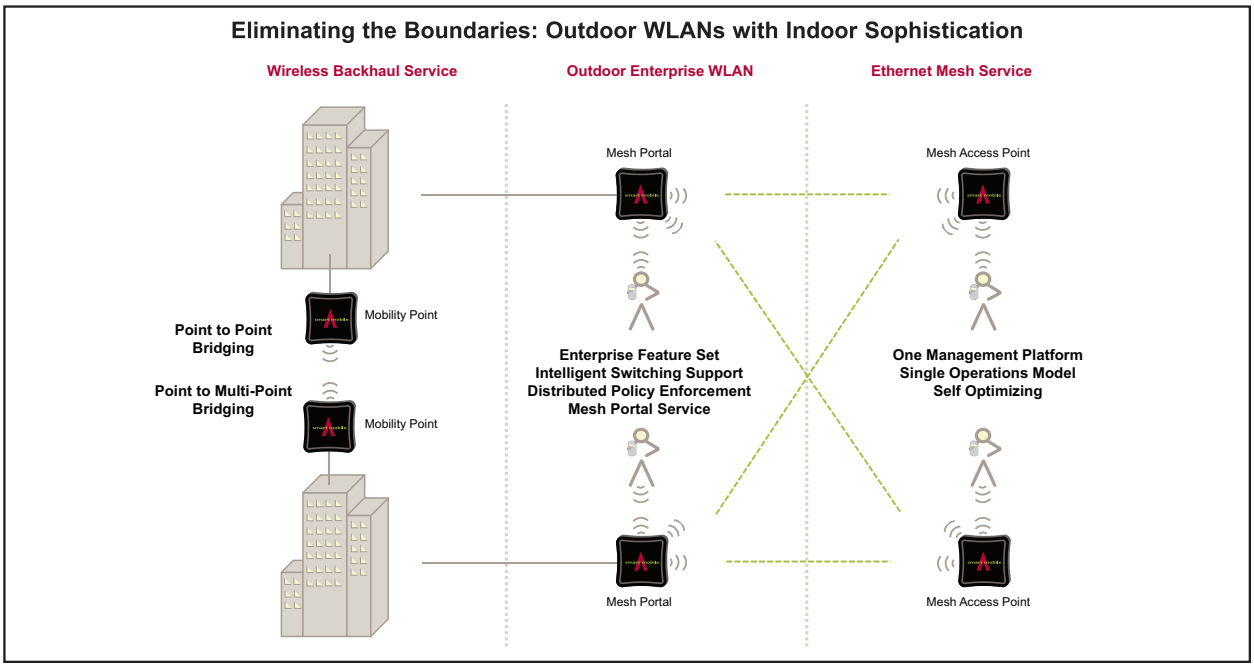
Smart Mobile's distributed cryptography approach is critical to enabling distributed forwarding. As noted above, Smart Mobile provides centralized security policy definition, but policy enforcement can be distributed or centralized based on application needs. Mobility Point access points perform 802.11 packet decryption and encryption, which ensures that encryption performance scales as network usage grows. In contrast, centralized encryption creates a bottleneck at the WLAN controller. The inherent performance and scalability advantages of distributed forwarding and policy enforcement are not possible under a centralized cryptography model.

Increased Performance and Scalability
The distributed cryptography model delivers greater performance because it leverages the processing power in the AP silicon for encryption. Ultimately, it delivers greater scalability at less cost. In addition, this approach can facilitate rapid implementation of emerging wireless standards by deploying more capable APs instead of bigger, more expensive WLAN controllers. Organizations will naturally add more APs as they expand WLAN coverage, and the encryption power and emerging standards availability in the AP will scale in conjunction. Adding APs as the user base grows is far less costly than upgrading expensive WLAN controllers to handle the load centrally.

ENTERPRISE-WIDE EXTENSIBILITY: EXTENDING COVERAGE OUTDOORS

Distributed data forwarding plays a key role in extending enterprise WLAN service to outdoor and unwired areas using enterprise mesh technologies like mesh point and mesh portal services. Distributed forwarding eliminates the need to backhaul traffic to the central WLAN controller to make policy determinations. Instead, the policies

are enforced in the mesh by the mesh point and mesh portal APs. This is critically important because over-the-air bandwidth is very limited, so reducing the need to backhaul traffic to the wired network helps to conserve and optimize usage of scarce bandwidth.



Optimal Path Selection

Smart Mobile uses optimal path selection through mesh portals, which is an enabling technology for enterprise outdoor and un-carpeted coverage requirements. The mesh portal is selected by wireless link quality or by switched path cost. The mesh portal uplink can change while the client service is simultaneously preserved. This optimal path selection also routes around uplink failures, while preserving client service. The Smart Mobile intelligent switching model optimizes traffic flows for the applications throughout the WLAN, and is more scalable than a generalized routing protocol.

Native Mobility across the Entire Network

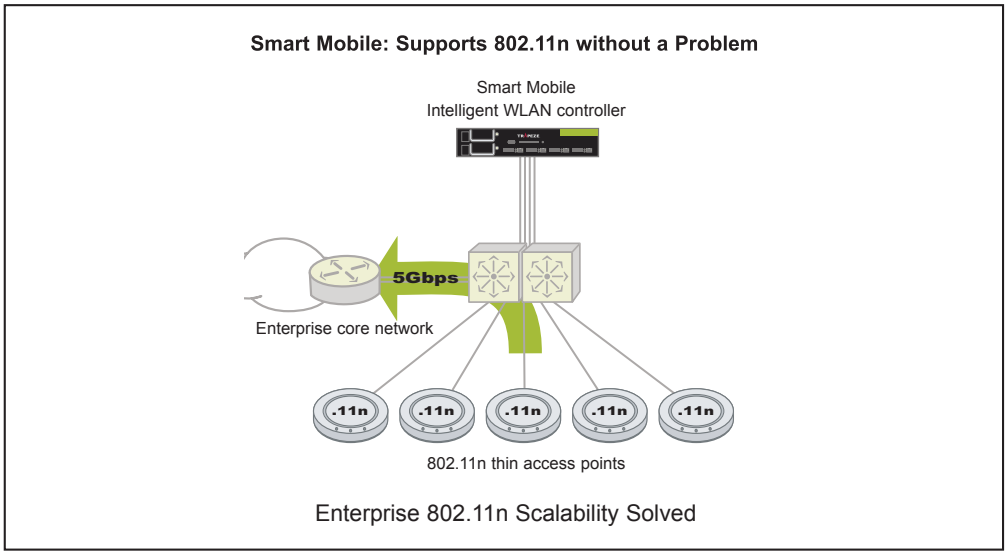
Smart Mobile's distributed forwarding model continues support for native mobility. The Mobility Domain (a group of up to 32 Mobility Exchanges) knows all of its Mobility Domain peers in the network through inter-Mobility Exchange peer communications with Mobility Domain "seeds." The "seed" informs each Mobility Exchange of every other Mobility Exchange in the domain, every Mobility Exchange VLAN instance, and every associated client's Mobility Point VLAN instance. The Station Switching Record supports tunnel endpoints, so Smart Mobile can establish dynamic tunnel end-points based on SSRs, to any Mobility Exchange or Mobility Point AP in the Mobility Domain. When a tunnel endpoint is specified, a tunnel is established between the client-hosting Mobility Point and any other Mobility Exchange or Mobility Point.

Intelligent Switching in Smart Mobile: Optimized for Performance and Scalability

With Smart Mobile, IT managers determine what traffic should be centrally forwarded and what traffic should be forwarded on a distributed basis. The IT manager sets up service profiles as part of the Smart Mobile network configuration. IT can set up different service profiles to fit the requirements of different applications. For instance, IT may choose to tunnel all guest traffic to a centrallized or segregated controller, but use distributed forwarding for all the employee traffic. Or IT may use distributed forwarding for all the voice traffic, but centrally forward all other traffic. The switching model can be configured to fit the specific application requirements.

High Performance Investment Protection for 802.11n

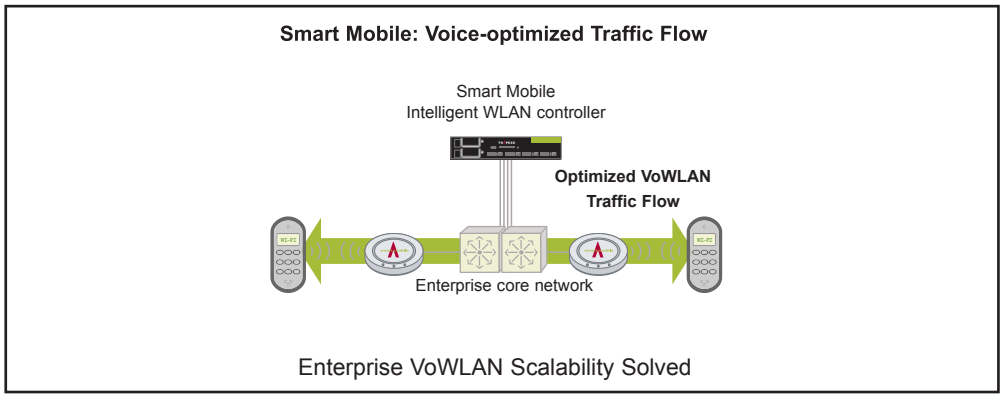
Distributed forwarding provides investment protection for 802.11n because it takes the load off the WLAN switches and eliminates the 10/100 Mbps bottleneck. Enterprises can deploy 802.11n without having to replace their Mobility Exchange WLAN controllers. But IT does not sacrifice control and security to gain a high bandwidth advantage. Policies in Smart Mobile are distributed and enforced at the AP, whether that policy describes encryption, quality of service, firewalls, location or many other parameters.



Enterprise 802.11n Scalability Solved

Enabling VoWLAN on a Massive Scale

For many years the VoIP community has been perfecting Session Initiation Protocol (SIP) and User Datagram Protocol (UDP) for optimized transport of VoIP, bringing VoIP technology to its current pervasive deployability. Establishing a VoIP call includes both handsets negotiating the call with the central SIP server. Conducting a call requires the SIP-negotiated UDP call transport mechanism flow from handset to handset directly. Smart Mobile distributed forwarding resembles the SIP/UDP VoIP architecture and supports optimized traffic flow for voice applications. Once the central WLAN controller assures the handset and authenticates the caller, the VoIP handsets talk to each other as peers. In essence, distributed forwarding in Smart Mobile allows voice traffic to take the shortest path through the network, with the lowest possible latency and jitter, which ensures the highest quality voice call. While current-generation WLAN architectures cannot support voice service for more than a handfull users, Smart Mobile can deliver toll-quality voice service to hundreds of users.



Enterprise VoWLAN Scalability Solved

UNCOMPROMISED SECURITY

Smart Mobile delivers uncompromised protection of business continuity and data privacy by incorporating four tiers of security:

- **Endpoint integrity assurance.** With endpoint integrity assurance, SmartMobile prevents misconfigured or infected devices from accessing the network by checking for the latest security patches and service packs, personal firewall and routing policy, anti-virus and anti-spyware software.
- **Industry-leading (802.1X) authentication and encryption.** Strong authentication, authorization, accounting, coupled with advance wireless protected access (WPA2) encryption prevents misuse and eavesdroppers, isolating traffic between private users and groups, and ensuring data privacy.
- **Application-based firewall policy enforcement.** Smart Mobile provides per user, per station, per group policy enforcement for QoS scheduling, location and security filtering that is application aware. Policy is enforced at the point in the network that is closest to the end station, preserving network bandwidth and improving performance throughout.
- **Comprehensive intrusion protection.** Trapeze partnered with AirDefense, the pioneer and leader in wireless intrusion prevention systems, to deliver the industry's only fully integrated IPS. The Trapeze/AirDefense solution defends against rogue devices, denial-of-service attacks, Evil Twins that spoof legitimate hotspots, misconfigured machines, and many other threats. An integrated IPS reduces configuration efforts in comparison with deploying a separate IPS overlay, and simplifies administration.

CENTRALIZED MANAGEMENT

Smart Mobile retains centralized management, providing IT managers with complete lifecycle control over the WLAN from a single console. The ability to centrally plan, configure, deploy, and manage the WLAN improves overall visibility into the network, reduces operational costs and total cost of ownership, and lets organizations deliver a broad range of services to their users with minimal burden on IT.

Trapeze RingMaster™ is recognized as the industry's leading centralized lifecycle management suite. RingMaster has an integrated 3D planner to help organizations plan their WLAN deployment, both indoors and outdoors. RingMaster enables network managers to efficiently configure, deploy, monitor and optimize a WLAN that supports tens of thousands of users. IT can set policies for users based on their identities, so that no matter where they roam on the wired or wireless network, they have consistent access to their resources—and IT has control.

Mobility Point access points are plug-and-play, and are configured and controlled by the Mobility Exchange switches. This increases management efficiency as well as security.

GETTING READY FOR TOMORROW, TODAY

Making a strategic investment in WLANs today requires organizations to be prepared to support tomorrow's requirements, which can be full of unknowns. As organizations begin to plan for the next phase of their WLAN deployment, they should ask themselves several key questions:

- **Where can you use high-speed wireless?** The high-performance 802.11n opens the doors of mobility to new classes of users. Users of bandwidth-intensive applications, such as enterprise collaboration and teleconferencing applications, computer aided design or software development tools, no longer have to sacrifice performance for the convenience of pervasive enterprise-wide mobility. Smart Mobile is the only 802.11n ready enterprise wireless LAN.

RECOMMENDATION: Notebooks shipping in Q1 2007 will include 802.11n. Upgrade the heaviest users first to the new standard. Ensure that your switches are Smart Mobile capable.

- **What are your plans for VoIP?** Sales of IP PBXs have surpassed traditional PBXs, and employees will naturally want to go mobile with their VoIP handsets and soft phones. As a result, Wi-Fi phones will have strong growth in 2007 and 2008,

and with the promise of convergence and the penetration of multimode Wi-Fi/cellular phones will be even higher. Smart Mobile can support hundreds of VoWLAN handsets because distributed forwarding delivers the lowest latency, period.

RECOMMENDATION: Create a pilot for VoWLAN to discover how employees view the productivity benefits and experience.

- **How will you support user demand for wireless service across the campus and in other outdoor locations?** Today, organizations are forced to choose between indoor and outdoor wireless solutions. A single seamless, best-in-class solution for both indoors and outdoors will provide the richest service set and the most efficient operations models. With the addition of mesh portal and mesh point service supporting Mobility Points, you can extend your Smart Mobile network outdoors, giving you outdoor reach with indoor sophistication.

RECOMMENDATION: Explore applications and enterprise wireless services supported by an outdoor mesh.

- **How will you enforce a multi-tiered security model across your next-generation, high-performance WLAN?** As wireless service becomes pervasive, organizations will want to maintain the highest security levels to keep out intruders and prevent potential attacks. In addition to effective methods for endpoint assurance, authentication, encryption, and firewall policy enforcement, organizations will need increasingly sophisticated defenses against intrusion threats.

RECOMMENDATION: Evaluate the cost and complexity of deploying a separate IDS/IPS overlay versus an integrated IDS solution.

- **How will you manage your next-generation, indoor-outdoor WLAN to minimize IT burden and operating costs?** As wireless networks increase in size, number of users, and scope of services provided, manageability of the network is an increasingly critical requirement.

RECOMMENDATION: Determine whether your vendor's approach to WLAN management requires multiple components or is supported through a single, integrated management console that allows network-wide planning, configuration, and operational control.

WIRELESS WITHOUT LIMITS

Smart Mobile from Trapeze Networks was designed specifically to optimize traffic flows in an extensible WLAN capable of scaling throughout the enterprise, overcoming the limits of today's approaches to WLAN architectures. By combining the best aspects of both distributed and centralized architectures, Smart Mobile enables organizations to meet the business and application requirements for the next generation of wireless networks.

Smart Mobile eliminates the boundaries between indoors and outdoors, giving organizations outdoor reach with indoor sophistication. Smart Mobile WLANs are ready for 802.11n today, and allow organizations to deploy high performance and latency sensitive applications such as VoWLAN on an enterprise scale, without compromising security or manageability and without having to upgrade their existing switching or WLAN controller infrastructures.

Americas | 5753 W. Las Positas Blvd. | Pleasanton, CA 94588 | Phone 925.474.2200 | Fax 925.251.0642
EMEA | Olympia 10c | 1213 NP Hilversum | The Netherlands | Phone +31 (0) 35.64.64.420 | Fax +31 (0) 35.64.64.429
Asia-Pacific | 275A, 2/F, Sui On Centre | 8 Harbour Road | Wanchai, Hong Kong | Phone +852.2824.8691 Fax +852.2824.8381
Japan | ARK Mori Bldg., West Wing 12F | 12-32, Akasaka 1-chome | Minato-ku, Tokyo 107-6024 | Phone +81 (0) 3.4360.8400 | Fax +81 (0) 3.4360.8447

WP001-11/06