

Avaya Conference Phones

คุณสมบัติอันหลักหลายที่มีให้เลือกในชุดผลิตภัณฑ์ โทรศัพท์ สำหรับการประชุมของวิชาชีวะ ที่เป็นที่ต้องการ สำหรับองค์กรที่ได้รับประโยชน์อย่างมากจากการทำงานร่วมกัน

ด้วยคุณภาพเสียงคมชัด การขจัดเสียงรบกวนที่เป็น สิทธิบัตรเฉพาะ และการออกแบบที่กันสนิม ดูดีในทุก มุมมอง โทรศัพท์สำหรับการประชุมของวิชาชีวะ ที่เป็น ตัวเลือกที่สมบูรณ์แบบสำหรับการทำงานร่วมกัน และ การทำงานภายในตัวสากล แวดล้อมเสมือนในปัจจุบัน



Avaya B179 SIP
Conference Phone

AVAYA
The Power of We™

ກາງເລື່ອກທີ່ເຫັນຈາດ ເຊີຍຮັກເມືອງຮົມເຫັຕີ ແລະ ປຣະກຍັດ ຄ່າໃຊ້ຈ່າຍໃນການເດີນກາງ



Avaya 159
Conference Phone

ເນື່ອຄຸນຈຳເປັນຕົວການຕິດຕ່ອງກັບໂຄຣສັກຄົມໄດ້ອ່າງຮວດເຮົວແລະຈ່າຍຕ່າຍ
ເພື່ອເປີດຕົວໂຄຮງການ ການຂອນຕີ ພຣີການຕັດສິນໃຈໃນເຊີງສຶກ ການປະໜຸມກາງ
ໂໂຣຄັພົກໄດ້ຮັບການພິສູງນີ້ແລ້ວວ່າເປັນວິທີທີ່ມີປະສິກົນກາພໃນການຂັບເຄລື່ອນຮຸຮົກຈົ
ໃຫ້ກ້າວໄປບ້າງໜ້າ ແລະເປັນສິ່ງທີ່ອົງຄົກຕ່າງໆ ທີ່ສິ່ງນີ້ມີຫວ່າງຈາກການຫຼາຍໆ ແກ່ງ
ແລະວູ້ໃນສົການການຄົມທີ່ພັນການຈາກຕົວການມີສ່ວນຮ່ວມໃນການກຳຈານຮ່ວມກັນ
ໄດ້ອ່າງຮວດເຮົວແລະຈ່າຍຕ່າຍ

ຈາດ ຮວດເຮົວ ແລະເປັນມີຕຣກັບສິ່ງແວດລ້ອມມາກກວ່າການເດີນກາງໄປປະໜຸມ
ແບບພບໜ້າກັນຈົງ ສາມາດຄົປົບໃຫ້ເຂົາກັບເວລາຂອງທຸກຄົນໄດ້ດີກວ່າ ພຣ້ອມກັ້ງ
ເຊີຍປຣະກຍັດຄ່າໃຊ້ຈ່າຍໄດ້ເປັນຍ່າງດີ ແລະກຳໃຫ້ຄຸນມີສ່ວນເຊີຍລົດກາວະໂລກຮ້ອນ



ອວຍ່ານໍາເສັນໂໂຣຄັພົກສໍາຫັກການປະໜຸມເພື່ອ¹
ໃຫ້ໃນສົການການພູ້ນັກທີ່ສົການພູ້ນັກທີ່ສົການພູ້ນັກທີ່
ພັບກັນປະໜຸມ ແລະສົການທີ່ພັບກັນປະໜຸມ

- **Avaya B100 Series Conference Phones:** ໃຫ້ຄຸນກາພເສີຍທີ່ເຢືຍມຍອດ
ກັ້ນຮຸນ SIP ແລະແບບອະນາສືອກມາພຮອມກັບ
ຄຸນສົມບັດບັນສູງ

ຄຸນກາພເສີຍສຸດຍວດ

ຄຸນກາພເສີຍຈັນເຊີຍມີຄ້ອງຈຸດເດັ່ນຂອງໂໂຣຄັພົກ
ສໍາຫັກການປະໜຸມຂອງອວຍ່າຖຸກຮຸນ:

- **Avaya B100 Series Conference Phones:** ປະກອບຕົວຍຸດຄຸນສົມບັດ Avaya
OmniSound 2.0 ເກໂນໂລຢີຕ້ານເສີຍທີ່ມີ
ສິກົນບັດຮັບເພາະເຊື່ອກອກແບບເພື່ອສົ່ງພ່ານເສີຍ
ທີ່ຜົດໃສ ນອກຈາກນີ້ຢັງມີຮບບໍຂັດເສີຍຮບກວນ
ທີ່ເຊີຍລົດເສີຍຮບກວນເບື້ອງຫລັງໃຫ້ວູ້ໃນຮະຕັບ
ທ່ານສຸດ ແລະສົ່ງພ່ານເສີຍຢ່ານຄວາມກົດວ້າງ ຫົ່ງໃຫ້
ສົກົນບານເສີຍທີ່ 7 ກໂລເອຣຕະ ສໍາຫັກການ
ໂໂຣຄັພົກພ່ານ VoIP

จัดประชุมทางโทรศัพท์ได้ง่าย และมีประสิทธิภาพยิ่งขึ้น

โทรศัพท์สำหรับการประชุมของอวาย่าถูกออกแบบมาเพื่อช่วยให้ผู้ใช้งานสามารถติดต่อสื่อสาร และทำงานร่วมกันได้ง่ายขึ้นไม่ว่าพิภพเดียวจะอยู่ที่ไหน:

การเข้าถึงผู้ฟังจำนวนมาก: โทรศัพท์สำหรับการประชุมของอวาย่าสามารถดำเนินการครอบคลุมห้องขนาดมาตรฐาน (เพิ่มพื้นที่ได้ถึง 300 ตารางฟุต) นอกจากนี้ยังสามารถติดตั้งในโถไฟเพิ่มอีก 2 ตัว ซึ่งจะเพิ่มพื้นที่การดำเนินการเป็นสองเท่า (มากกว่า 700 ตารางฟุต) และรองรับผู้เข้าร่วมประชุมได้มากกว่า 12 คน เมื่อใช้เข้าถึงผู้ฟังได้กว้างขึ้นยังสามารถเชื่อมต่อ Avaya B100 Series Conference Phones เข้ากับระบบกระจายเสียงได้

จัดการประชุมได้อย่างง่ายดาย: โทรศัพท์สำหรับการประชุมของอวาย่าได้รับการออกแบบสำหรับการตั้งค่าการโทรได้อย่างง่ายดาย และรวดเร็ว Avaya B100 Series Conference Phone สามารถสร้างกลุ่มการประชุมไว้ล่วงหน้า เมื่อโทรศัพท์ไปยังกลุ่มที่กำหนดไว้ได้อย่างรวดเร็ว และมีประสิทธิภาพ รวมถึงความสามารถในการสร้างสมุดโทรศัพท์ของตัวเอง พร้อมกับคุณสมบัติการสร้างกลุ่มผู้ใช้ได้ถึง 1,000 รายซึ่งต่อตอกสู่ โดยสามารถส่งออกและนำเข้ารายชื่อผ่านทางเว็บ

การเชื่อมต่อ: ด้วยโทรศัพท์สำหรับการประชุมของอวาย่า ผู้ใช้ร่วมประชุมสามารถเชื่อมต่อคอมพิวเตอร์ (สำหรับการโทรศัพท์ระบบ VoIP) โทรศัพท์มือถือ โทรศัพท์ไร้สาย สำหรับใช้งานภายในอาคาร และโทรศัพท์ตั้งโต๊ะ รวมถึงเข้ากับโทรศัพท์สำหรับการประชุมโดยตรง เทคโนโลยีในการสนับสนุนการใช้งานระหว่างโทรศัพท์ประเภทต่างๆ และการเชื่อมต่อแบบพสมพานิชทำให้สัญญาณโทรศัพท์ระบบ VoIP ใช้การส่งผ่านเสียงย่านความถี่ได้กว้างถึง 7 กิกะเฮิรตซ์

นำเสนอผ่านอุปกรณ์ไร้สาย: การประชุมทางโทรศัพท์ที่เกี่ยวข้องกับการนำเสนอผ่านอุปกรณ์ไร้สายมักสร้างเป็นทางให้กับผู้ฟังผู้นำเสนอ และผู้ฟังที่อยู่ในระยะใกล้ Avaya B100 Series Conference Phones ช่วยแก้ปัญหาดังกล่าวด้วยการจัดเตรียมการเชื่อมต่อกับบุคคลอุปกรณ์ สวนศรีษะแบบไร้สาย ซึ่งทำให้ทุกคนได้ยินเสียงของผู้นำเสนออย่างทั่วถึง และต่อเนื่อง ซึ่งคุณสมบัติตั้งกล่าวเนี่ยหมายความว่าอย่างยิ่งสำหรับการบรรยายในห้องประชุม

บันทึกการประชุม: เมื่อมีสาระสำคัญที่ต้องบันทึก และจัดเก็บในระหว่างการประชุม ตัวอย่าง เช่น สิ่งที่ต้องนำมาบากบogene ในภายหลัง เพื่อส่งให้กับเพื่อนร่วมงาน หรือเพื่อคัดลอกสำเนาเสียงโดยบันทึกบน SD Card ที่เสียบลงในช่องบันทึก เครื่องโทรศัพท์ สามารถเก็บรายละเอียดของ การประชุมเป็นไฟล์เสียง และ/หรือใช้โทรศัพท์สำหรับการประชุมเป็นอุปกรณ์บันทึกเสียง

เลือกโทรศัพท์สำหรับการประชุมที่เหมาะสม

Avaya B179: จัดการโทรศัพท์ SIP-based

การใช้งาน: ห้องประชุมผู้บริหาร และห้องประชุมขนาดใหญ่

โทรศัพท์แบบ SIP-based ที่ประกอบด้วยคุณสมบัติหลากหลาย รองรับการโทรศัพท์ระบบ VoIP และทำงานร่วมกับ Avaya Aura Communication Manager สามารถนำเข้า/ส่งออกรายละเอียดของรายชื่อผู้ติดต่อ ผ่านทางเว็บ

Avaya B159: เชื่อมต่อได้อย่างง่ายดาย

การใช้งาน: ห้องประชุมผู้บริหาร และห้องประชุมขนาดใหญ่

เพิ่มการเชื่อมต่อสำหรับโทรศัพท์มือถือ โทรศัพท์ไร้สาย โทรศัพท์ตั้งโต๊ะ และโทรศัพท์ไร้สาย ไฟเบอร์ อีก 2 ตัว รองรับการเชื่อมต่อหลายระบบ บริจจ์ติดตั้งไว้ภายในเพื่อรองรับการเชื่อมต่อหลายๆ รูปแบบได้พร้อมกัน

Avaya B149: เรียบง่าย และมีคุณภาพ

การใช้งาน: สำนักงานส่วนตัว และห้องประชุมขนาดกลางและขนาดย่อม

พสมพานิชคุณภาพเสียงชั้นยอดเข้ากับการตั้งค่าที่ง่ายดายผ่านทางคู่มือการประชุม และสนับสนุนโทรศัพท์





Compare Avaya Conference Phones

	B149	B159	B179
			
Participants	<10	>10	>10
Size of Room (sq. meters/feet)	30/320	30/320	30/320
Protocol	Analog	Analog	SIP
Sound Technology	OmniSound. 2.0	OmniSound. 2.0	OmniSound. 2.0
Display (pixels)	128 x 64	128 x 64	128 x 64
Keypad	Yes	Yes	Yes
USB Connection	NA	Yes	NA
Conference Guide	Yes	Yes	Yes
Audio Connectivity for mobile, cordless, DECT	NA	Yes	NA
Call Recording	Yes	Yes	Yes

เกี่ยวกับอา耶่า

อา耶่าคือบริษัทัญห์นำเสนอโซลูชันด้านการติดต่อสื่อสาร และการทำงานร่วมกันระดับโลกที่ได้รับตราโซลูชันด้านการสื่อสารแบบเบ็ดเสร็จ ครอบคลุม

เซ็นเตอร์ ข้อมูล และบริการที่เกี่ยวเนื่องให้กับองค์กรทุกภาคทั่วโลก สามารถเข้าไปดูรายละเอียดเพิ่มเติมได้ที่เว็บไซต์ www.avaya.com

AVAYA
The Power of We™

สนใจข้อมูลติดต่อได้ที่

Sierra Asia Pacific Inc., (Thailand branch)

55 อาคารเวย์เพลส ชั้น 10 ถนนวิภาวดี แขวงจุฬาลงกรณ์ กรุงเทพฯ 10330

โทร. 0-2655-4400, 0-2655-4791

แฟกซ์ 0-2655-4402

e-mail : marketingth@avaya.com

Avaya WLAN 2300 Series

The Avaya WLAN 2300 Series is a complete 802.11 solution for enterprises wishing to deploy widespread wireless coverage for today's business, IP Telephony and converged multimedia applications. The solution combines the latest industry standards with a centralized architecture and advanced features to create a secure, cost-effective and highly scalable WLAN infrastructure. The WLAN 2300 Series includes the tools and features required for successful planning and implementation, whether deploying a first-time WLAN using a quick and simple approach, or graduating to a precisely engineered mobile infrastructure as part of a global enterprise mobility strategy.

The WLAN 2300 Series features a centralized wireless LAN deployment model with "thin" access points controlled and managed by a central WLAN Security Switch (Refer Figure 1). The series is comprised of four primary elements:

- WLAN Access Points
- WLAN Security Switches
- WLAN Management Software system
- WLAN Location Engine

Each plays a key role in the complete mobility solution.

- The **Avaya WLAN 2300 Series Access Points** perform 802.11a/b/g mobile connectivity, encryption/ decryption for wireless traffic, priority queuing and radio frequency (RF) monitoring, including rogue access point identification and containment. Access points exchange control and data traffic with their associated WLAN Security Switch.
- The **Avaya WLAN 2300 family of security switches** controls the access points and performs key functions such as security, networking, quality of service (QoS) and roaming for mobile users. The WLAN Security Switch also correlates radio frequency data from multiple access points and coordinates their response to changing RF conditions and RF attacks.

- The **Avaya WLAN Management Software** system is a comprehensive design and management tool that identifies ideal access point locations on detailed floor plans, configures all devices with a single click and provides granular monitoring and reporting for complete visibility and control over the entire system.
- The **Avaya WLAN Location Engine** is an optional element that adds integrated location services to any WLAN 2300 installation enabling new applications and services such as location-based security policies, content delivery or asset locating and tracking.

Support for 802.11n

The introduction of WLAN 802.11n into the marketplace represents an exciting time for customers due to its greatly enhanced capabilities over the existing 802.11 a/b/g standards, in terms of capacity, range and reliability. Refer to Figure 2 for an 802.11 a/b/g/n comparison. Avaya offers a number of 802.11n Trapeze branded products that work seamlessly with the WLAN 2300 series. This includes two 802.11n APs (Trapeze MP-432 and Trapeze MP-82) and a new high capacity switch (Trapeze MX-2800). The Trapeze MP-432/MP-82 will run on existing WLAN 23xx security switches. These are optional products, intended for those customers with an immediate need for 802.11n.

Avaya's recommendation is that before installing any new technology, it is important for customers to first consider all of the implications and create an approach that meets the needs and business goals of your organization.

Deploying 802.11n involves much more than just an exchange of hardware and software. A wide range of issues need to be carefully considered, such as AP powering, LAN considerations, support strategy for clients and controller processing. Developing a comprehensive plan spanning applications, clients and infrastructure is recommended.

Avaya's WLAN 2300 Series advantage

A better user experience

The WLAN 2300 Series provides best-in-class performance to support delay-sensitive applications like voice and multimedia. Seamless, fast roaming among all access points, dynamic RF management and QoS policy enforcement means that users get the highest quality WLAN experience possible — a must for IP Telephony and multimedia applications.

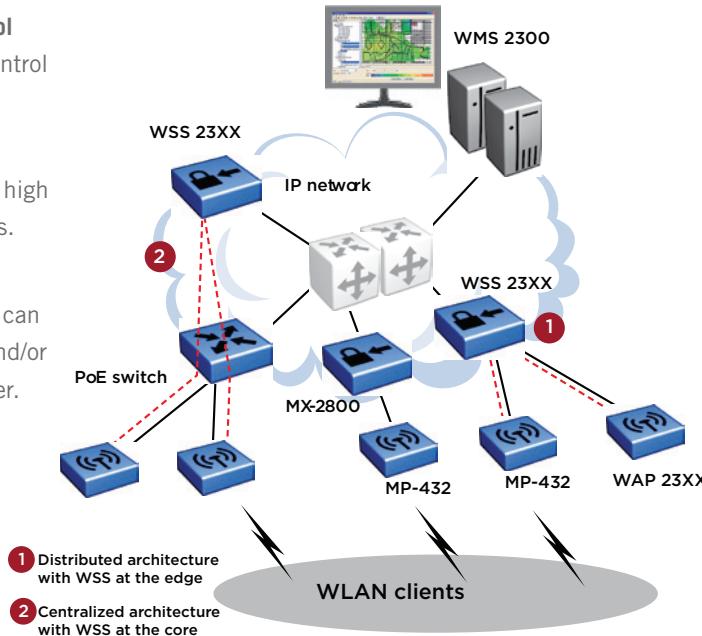
A better administrative experience

The WLAN 2300 Series makes life easier for administrators by automating tasks

Figure 1. WLAN 2300 Centralized WLAN System

Access Points are dependant on WLAN Security Switch for operation

- **Control and Provisioning Protocol (CAPP)** establishes a secure control plane between a WSS and its managed WAPs.
- **Trapeze MX-2800 controller** for high capacity 802.11n deployments.
- **Trapeze MP-432** provides the 802.11n wireless interface. It can run on a WLAN 23xx switch and/or the Trapeze MX-2800 controller.



- **WLAN Management System (WMS) 2300** for system-wide planning, configuration and management
- **WLAN Security Switch (WSS) 23XX** controls the access points and can be deployed either at the edge of the network (1) to support directly connected APs, or elsewhere in the network (2) to support indirectly connected APs across the LAN.
- **WLAN Access Point (WAP) 23XX** provides the 802.11 a/b/g wireless interface and can be directly connected to either a PoE switch, or a WSS. Each WAP is dependant on a WSS for operation.

throughout the entire implementation and operations life cycle. The WLAN Management Software system provides an analytical site survey that considers three-dimensional RF attenuation characteristics of all elements that will impact WLAN coverage. Competing approaches often apply open-air scenarios to indoor floor plans without any adjustment for structure and materials.

The broad family of WLAN Security Switches means that the right model can be deployed for any scenario. The access points automatically find and connect to WLAN Security Switches, and flexible AAA, QoS and security enforcement options allow for a seamless fit with existing policy structures and security equipment. The WLAN Management Software system also adopts new access points and WLAN Security Switches into an updated Wireless LAN topology.

Real-time RF management handles unpredictable user loads and interference

without the need for administrator intervention, and unlike competing solutions, the WLAN 2300 Series puts client performance first so that channel and power adjustments don't disconnect active users. And extending the architecture to remote branch offices couldn't be easier. WLAN Security Switches self-configure and ensure that WLAN service stays up even if WAN links fail. The WLAN 2300 Series even makes visitor-based networking a breeze. A unique streamlined application designed for front-desk personnel can be used to generate temporary guest IDs with expiration times and pre-configured access controls.

As for security, the WLAN 2300 Series goes beyond the latest industry security standards with built-in wireless threat protection that guards against RF-based attacks and vulnerabilities. The advanced RF scanning and control capability protects against unauthorized access points and

ad-hoc users. Even the WLAN components themselves are authenticated before they're accepted into the system and all subsequent control traffic is encrypted. And to make sure that the WLAN doesn't add another layer of policy administration, the system will pull user policies directly from existing backend AAA servers, and bind those policies to users as they roam. Working together, the vast range of security capabilities ensures that user mobility doesn't compromise the integrity of your network services.

A better return on your mobility investment

The number one expected benefit from WLAN investments is improved user productivity — which can only be realized if the WLAN service and supported applications perform to the user's expectations. And usage patterns are changing quickly. Users are connecting

Figure 2. 802.11a,b/g,n comparison

	802.11b	802.11g	802.11a	802.11n*
Compatibility	802.11b	802.11b,g	802.11a	802.11a,b,g,n
Number of channels	3 non-overlapping	3 non-overlapping	Up to 15 nonoverlapping channels (country specific)	Same as 802.11 a/b/g using 20 MHz channels. Restricted to 1 in 2.4 GHz and 3 in 5 GHz using 40 MHz channels
Typical Indoor range	100 ft - 300 ft	100 ft - 300 ft	40 ft - 300 ft	Expected to be 2X range of 802.11a/b/g
Typical outdoor range (Line of sight)	400 ft - 1500 ft	400 ft - 1500 ft	100 ft - 1000 ft	N/A
Data rates	11, 5.5, 2 and 1 Mbps	54, 48, 36, 24, 18, 12, 9 and 6 Mbps	54, 48, 36, 24, 18, 12, 8 and 6 Mbps	Up to 600 Mbps (up to 300 Mbps in WLAN 2300 R7)
Wireless medium	DSSS, 2.4 GHz	OFDM, 2.4 GHz	OFDM, 5 GHz	OFDM-MIMO in 2.4 and/or 5 GHz

* Ratification of standard expected 2H 2009

more frequently with WLAN and staying connected longer than ever before. Add to this a parallel investment in IP Telephony and converged applications, combined with convenient desktop videoconferencing and the onslaught of new and embedded 802.11 clients, including dual-mode cellular/ Wi-Fi® phones, and it's clear that demand for voice and multimedia over WLAN is imminent.

Whether you're planning to adopt Voice over Wireless LAN today, or tomorrow, the WLAN 2300 Series is designed to deliver high-quality voice and converged services that are necessary to achieve real user productivity improvements. The system offers multiple levels of redundancy not found in competing solutions — access points can be dual-homed to find a backup connection should one fail, and WLAN Security Switches can be deployed in an active-standby configuration with n+1 redundancy and offer dual power supplies as well. Dynamic RF management, rogue access point protection and wireless threat protection will keep today's mobile services and applications up

and running during worst-case scenarios. Even the granular monitoring and reporting tools have been specifically designed for administrators who need to support business-critical services.

WLAN Security Switch 2300 Series

The WLAN 2300 Series includes a family of security switches, each designed to meet specific needs of enterprise-wide deployments. The portfolio breadth, combined with advanced features and a common management system, provides unparalleled deployment flexibility and scalability to meet the growing demands of mobile professionals. Each switch can be deployed and managed independently, or can participate with other 2300 Security Switches in large enterprise network deployments. In multiple switch architectures, client information and policies are shared among switches to permit fast roaming among all access points. Regardless

of network size or topology, the WLAN Security Switch 2300 family can lower equipment costs substantially by offering the right-sized product for any deployment scenario.

- **Avaya WLAN Security Switch 2350**

The WLAN Security Switch 2350 is the smallest switch in the 2300 Series and is ideally suited for extending WLAN services to small or branch office environments. The WLAN Security Switch 2350 auto-configures when first connected to the network and can control up to three access points. It offers the same features as the larger 2300 switches but in a smaller package.

- **Avaya WLAN Security Switch 2360**

The WLAN Security Switch 2360 is ideally suited for mid-size office sites or wiring closet deployments and can control up to 12 access points that can be either connected directly to one of the eight Ethernet ports or indirectly through a

Layer 2 or 3 network. The WLAN Security Switch 2361 is identical to the 2360, but adds a second power supply for improved wireless service resiliency.

- **Avaya WLAN Security Switch 2382**

The largest switch in the 2300 series features Gigabit connectivity and is designed for large deployments and data center installations. The WLAN Security Switch 2382 can be licensed to control up to 128 distributed access points. Dual power supplies provide superior resiliency for voice and business applications.

User-based policies for enhanced security

WLAN Security Switches can enforce security and QoS policies based on the individual user or group identity — not their device, initial access point or physical port. These policy assignments can be maintained locally, or pulled from central AAA servers during authentication. The latter approach allows for massive scale

and stronger security by centralizing policy management and mitigating the need to update and synchronize multiple policy databases. Subsequent to authentication, user policies are propagated to other WLAN Security Switches to allow for fast, secure roaming with consistent QoS levels. The WLAN Security Switch tracks and maintains records of user location, roaming history, data transferred and other activity for accounting and billing purposes.

Mobility domains for “free” roaming

Each WLAN Security Switch controls a specified number of access points which in turn creates an 802.11 service domain where mobile users can roam freely. Multiple WLAN Security Switches can work together to create large mobility domains that can span multiple floors, an entire building or campus. Within the mobility domain, each user's security, QoS and access policies follow them as they roam from access point to access point. Regardless of where a user roams, their traffic will always be tunneled back to the WLAN Security Switch

that can put them on to the appropriate network VLAN and subnet. This roaming architecture ensures a symmetrical data flow and won't break multi-cast memberships like competing solutions.

Virtual service groups for management flexibility

Each WLAN Security Switch can support up to 32 independent virtual WLANs over a single infrastructure. Each virtual WLAN can be set up as a unique service group that can be assigned its own VLAN, subnet and AAA server(s), along with specific security and QoS policies. In shared environments or managed services implementations, each virtual service group can have its own Web authentication page to request usernames and passwords or display instructions, welcome banners, corporate identities or advertisements.

AAA management/offloading offers authentication options

WLAN Security Switches are capable of enforcing multiple authentication options

Figure 3. WLAN Security Switch options

					
	WSS 2350	WSS 2360	WSS 2361	WSS 2382	MX-2800
Number of Fast Ethernet ports/Power over Ethernet	2/1	8/6	8/6	1/0 (Mgt)	1/0 (Mgt)
Number of Gigabit Ethernet ports	—	—	—	2 x 1-Gbps (SFP)	8 x 1-Gbps (RJ-45 or SFP) 2 x 10-Gbps (XFP)
Number of access points supported	3	12	12	Licensed N x 32 128 max	Licensed N x 64 512 max
Third-party AP support	Yes	Yes	Yes	Yes	Yes
Form factor	Small table mount	1U rack mount	1U rack mount	1U rack mount	1U rack mount
Power supply	Single	Single	Dual-redundant	Dual-redundant	Optional Dual-redundant
Application	SMB/branch office	Mid-size office/wiring closet	Mid-size office/wiring closet	Data center	Data center

including client MAC address, 802.1X or Web-based authentication, and can map any SSID or virtual service group to a primary and backup AAA server, or load balance requests among multiple AAA servers for service resiliency. The WLAN Security Switch offloads back-end AAA servers by terminating and processing Extensible Authentication Protocol (EAP) for 802.1X users, including key generation and management functions for EAP-TLS, EAP-MD5 and PEAP. The WLAN Security Switch will also offload Transport Layer Security (TLS) processing, including X.509 certificate generation and management.

Centralized access point management provides simplified administration

Each WLAN Security Switch provides centralized management for the access points under its control. Firmware updates,

configuration changes and RF management can all be performed by the WLAN Security Switch through a management interface or via Wireless Management Software. The WLAN Security Switch management system provides administrators with detailed tracking and reporting of activity on all access points.

Dynamic RF management ensures optimal coverage

The WLAN Security Switch continually receives RF data from associated access points and processes important information such as traffic load, interference from nearby devices, noise levels, client signal strength and signal-to-noise ratios. Using this data, the WLAN Security Switch calculates the optimal 802.11 channel assignments and radio power transmission levels for all associated access points. The WLAN Security Switch can automatically apply these settings to the respective access points and keep the WLAN system operating

at peak performance and efficiency even when adverse or unexpected conditions arise such as outages, interference or radio jamming attacks.

User RF optimization provides personalized performance

The WLAN Security Switch 2300 Series takes RF management to a new level by assimilating client RF data and client usage patterns, in addition to the basic RF data received from access points. The result is an auto-tuned RF environment that is optimized for user performance and usable capacity rather than blind approaches that achieve a theoretical balance among access points. By focusing on user performance, the WLAN 2300 keeps access points optimized for voice, multimedia and business applications.

Plug-n-Play/Plug-n-Grow

Traditional standalone WLAN deployments require careful planning and time-consuming

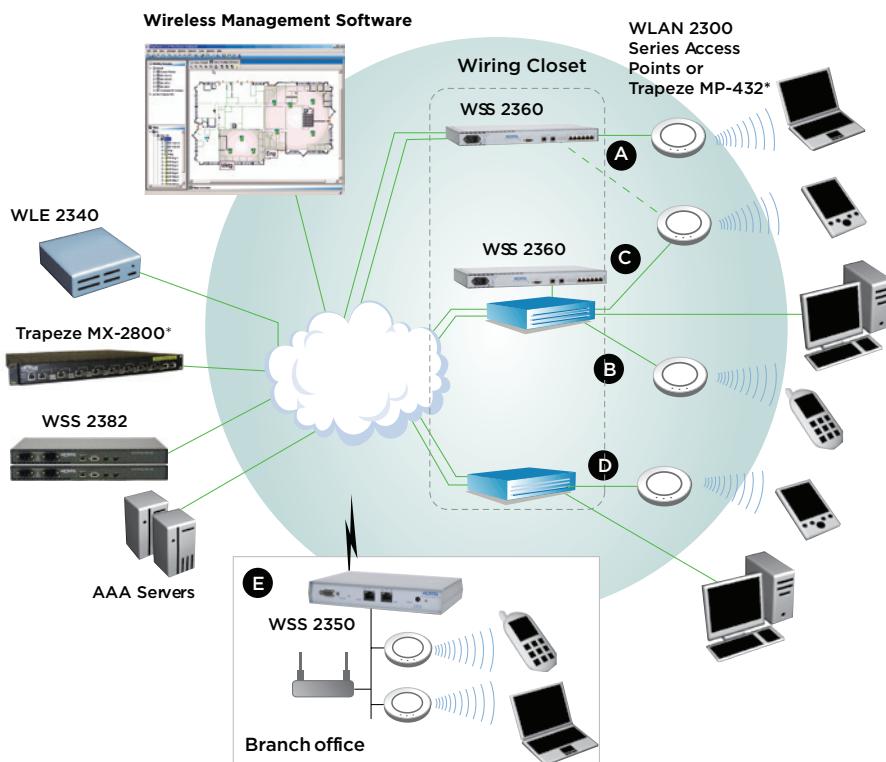


Figure 4. Multiple deployment options

Seamless integration with existing networks

WAP-WSS configurations

- A Directly connected to WSS 2300
- B Indirectly connected to WSS (in wiring closet) through edge PoE switch
- C Redundant connection using dual-Ethernet ports
- D Indirectly connected to WSS (in data center) through PoE switch
- E Branch office deployment using WSS 2350

* Trapeze MP-432 and MX-2800 hardware requires WLAN 2300 Release 7 software.

reconfigurations of nearby access points whenever new ones are added to the network. The WLAN 2300 Series greatly simplifies this process by immediately recognizing new access points and dynamically incorporating them into the WLAN system with greatly minimized administrator intervention.

Rogue access point protection contains threats

WLAN Security Switches continually monitor RF activity and can identify unauthorized access points and clients that are broadcasting in the 802.11 radio spectrums. The system can identify and locate rogues, alert administrators, monitor the access point's activity and even contain the threat by launching containment measures from neighboring access points. The system can also mirror suspicious wireless traffic on a user or group basis for security scanning.

Enhanced wireless threat protection goes beyond standards

Most of the recently introduced WLAN security standards like WPA2 and 802.11i address concerns relating to user authentication and data confidentiality/integrity, but have done little to protect against RF-based attacks that focus on

the WLAN infrastructure itself. The WLAN Security Switch 2300 series can protect against such attacks by comparing current RF activity to a built-in signature database and alerting administrators of a threat and location of the threatening device.

Control of third-party access points

WLAN Security Switches have the unique capability of being able to control popular standalone access points from other vendors. This allows IT departments to keep their existing access points and upgrade to a centralized architecture with many of the benefits of a complete WLAN 2300 system, including user-based policy enforcement and fast roaming.

User load balancing for best performance

Large-scale WLANs can present mobile clients with multiple points of connectivity at any given time. If too many users connect to a particular access point, individual performance suffers and system capacity is reduced significantly. The WLAN 2300 Series continually monitors user load and will automatically redirect new users to alternative access points and deliver the best possible user performance for given conditions.

Seamless fast roaming enables uninterrupted voice and multimedia services

The WLAN 2300 Series allows seamless roaming between all access points. Mobile clients can roam between access points belonging to different subnets and even between those managed by a different WLAN Security Switch. Additionally, each user's authentication information and associated policies are shared with other 2300 Series Security Switches so that the delay of re-authentication during roaming is eliminated. This allows users to maintain a voice quality connection while roaming within a particular area, between floors and even building-to-building.

Self-healing, resilient design minimizes service disruption

Each WLAN Security Switch maintains a map of RF characteristics within its service domain. In the event of an access point failure, the WLAN Security Switch will immediately recognize the change in RF patterns and respond by increasing transmission power levels of surrounding access points to fill the coverage hole. Similarly, if an access point is temporarily handicapped by a physical obstruction, the system will respond to minimize service disruption. The WLAN Security Switch hardware is also designed for resiliency with dual power supplies, Multi-Link Trunking, active-standby architecture options and n+1 redundancy for access point connectivity to eliminate any single points of failure within the system.

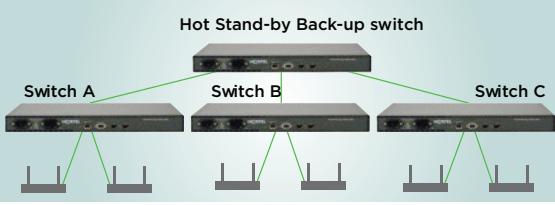
Figure 5.
WLAN Access Points

Feature	Avaya WAP 2332	Trapeze MP-432/MP-82
Dual radio 802.11n	No	Yes
Dual radio 802.11a/b/g	Yes	Yes
P-MP Wireless Bridging	Yes	Yes
Dual Ethernet ports	Yes	Yes
Local traffic forwarding	Yes	Yes
Fully compatible with existing WLAN 2300 systems	Yes	Yes

Clustering Support

Security switches can be configured in a cluster allowing them to act as a single virtual switch for wireless configurations and AP load balancing, which provides for automatic redundancy. This makes it easier to scale and improves resiliency. This capability solves most of the problems often faced by large-scale enterprises by providing a single point of

Figure 6. Clustering diagram

Today's limited approach	Clustered approach
	
Discrete switches operate independently	► Clustered switches — act collectively as single virtual switch
Harder to scale	► Easy to scale — Capacity can be added in chunks, anywhere in the network
Limited resiliency — APs mapped directly to switch	► Highest resiliency — APs dynamically map to switches —optimized, auto AP load balancing
Difficult to manage, highest cost of ownership	► Easiest to manage, lowest cost of ownership

configuration, automatic AP failover without client connection loss and AP load balancing.

WLAN 2300 Series

Access Points

The WLAN Access Point 2332 is a multi-mode, dual-radio 802.11 a/b/g unit. It is controlled by the WLAN Security Switches and can be deployed in large numbers without creating a management burden. The APs are plenum-rated for ceiling installations and feature an attractive enclosure that resembles a common smoke detector to blend in with office environments. The Trapeze MP-432 is a dual-radio 802.11n unit. It is fully compliant with the 802.11n Draft 2 standard.

Simple installation

The WLAN Management Software system can be used to map the location of access points based on the expected number of users and type of applications being accessed. The WLAN Management Software system will also calculate each access point's ideal configuration and push it out to the WLAN Security Switches which

automatically configure the access points upon installation. The access points can connect directly to an Ethernet port on the WLAN Security Switch, or indirectly across a Layer 2 or 3 network and receive 803.3af Power over Ethernet (PoE) from a WLAN Security Switch, a PoE capable Layer 2/3 switch or PoE injector.

Resiliency and QoS for voice and multimedia applications

The WLAN 2300 series Access Points are designed to deliver reliable service for voice and multimedia applications and feature redundant Ethernet ports that allow for a backup network connection if the primary port fails for any reason. To deliver the best user experience, the access point classifies traffic into multiple user and group queues based on AAA-defined QoS policies, SVP or DiffServ classifications. The access point does not store any sensitive security information locally, making it safe for unsecured areas, and if theft is still a concern, then each access point can be physically locked down using the Kensington™ lock interface. To prevent tampering, each access point is authenticated

to a WLAN Security Switch upon installation and all subsequent control traffic is encrypted.

RF scanning to prevent unauthorized activity

The WLAN 2300 series Access Points can perform scheduled or automated RF scans to search for unauthorized 802.11 devices and detect RF attacks. Access Points can run periodic sweeps of all channels in the active radio band while simultaneously providing mobile connectivity, or they can act as dedicated RF monitors and scan all bands and channels continuously. Any unauthorized activity or unexpected change in RF conditions is reported to the WLAN Security Switch, which determines if a rogue access point has been identified or if channel or power level adjustments are required.

Flexible antenna options for customizing signal patterns

The WLAN 2300 series Access Points are equipped with dual internal radios, omnidirectional dual diversity antennas with external antenna connectors that allow enterprises to customize signal patterns and match particular deployment requirements.

Figure 7. Wireless backhaul

The WLAN Access Point 2332 can create wireless backhaul links with its neighbors for simpler installations and bridging applications.

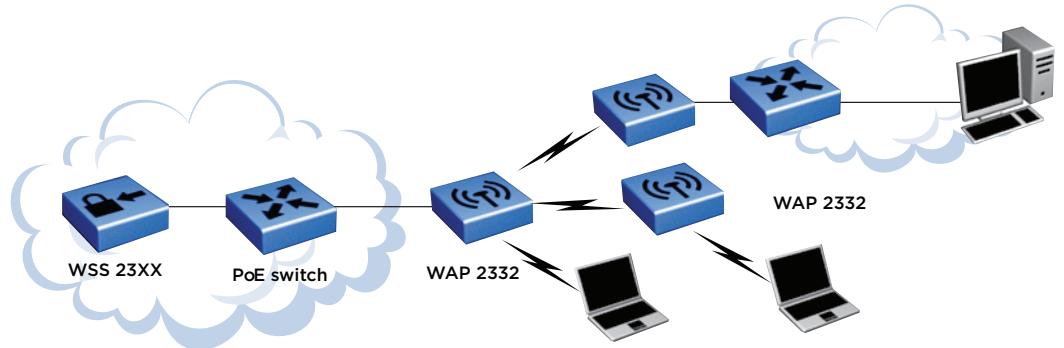
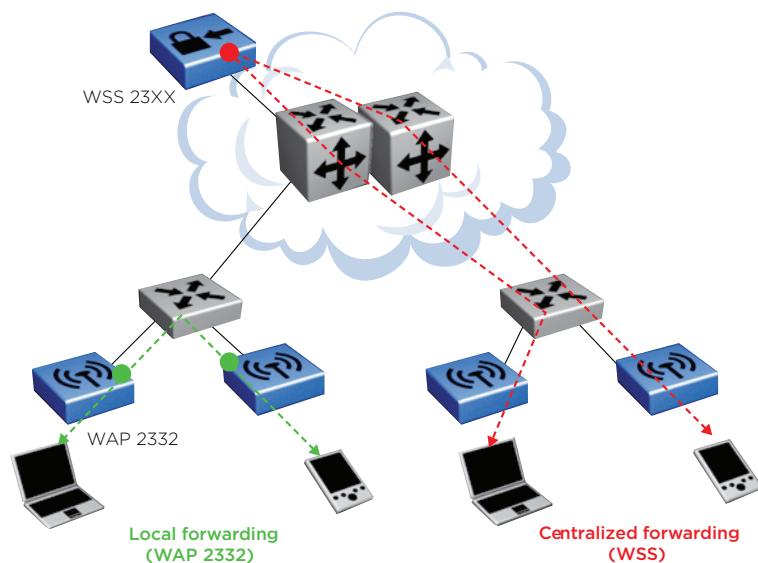


Figure 8. Local traffic forwarding

The WAP 2332 has the unique ability to import a user's policies from the WSS and forward traffic locally, outside of the WSS tunnel. This option can improve system capacity by offloading the WSS of excessive data traffic and can improve performance by creating shorter data paths.



WLAN Management Software system

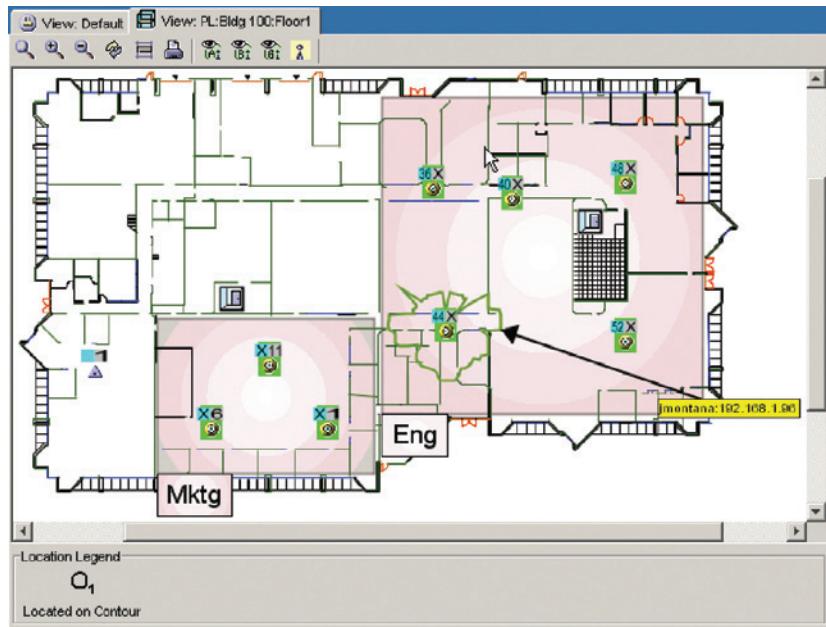
The WLAN Management Software system is much more than a management application — it is an integrated tool suite that helps administrators through every phase of the project cycle from initial planning, deployment and configuration through ongoing operations support, troubleshooting and reporting. WLAN Management Software runs on common server platforms including Windows 2000, Windows XP and LINUX, and can support hundreds of individual WLAN Security Switches and

thousands of access points. The WLAN Management Software system lets administrators perform system-wide updates with a single key stroke and “see” what’s happening at any moment with the rich graphical interfaces. The WLAN Management Software system is a client/server application and can support up to four simultaneous administrators, each with individual access levels and authorizations.

Painless planning and deployment
Prior to deployment, the WLAN Management

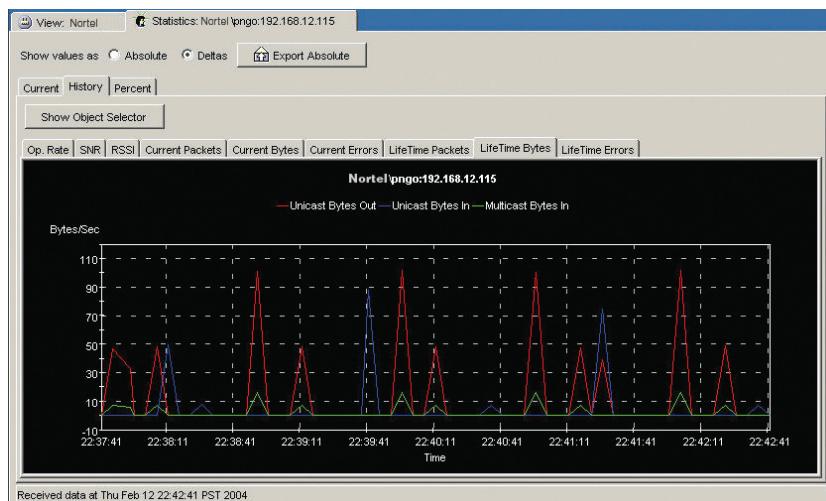
Software system can act as a powerful standalone analytical site survey and planning tool that can import AutoCAD DXF™, AutoCAD DWG, JPEG or GIF floor plan files and apply attenuation characteristics to walls, doors, ceilings and other RF obstacles. The system can then design the ideal WLAN network including topology, equipment counts and radio channel and power settings. It even considers minimum user throughput levels, user volumes, failover and peak capacity scenarios to help engineers build service-ready WLANs for voice and converged

Figure 9. Client and Rogue Access Point Location



The WLAN Management Software system accurately locates clients and rogue access points on imported floor plans.

Figure 10. Detailed Monitoring



The WLAN Management Software system provides an intuitive dashboard for monitoring and troubleshooting. The system provides WLAN topology, element status, RF and client performance information, historical data and more.

applications. The WLAN Management Software system will map the access point's physical location on floor plans and produce an accurate bill of materials to make installation as simple as possible, and once access points are installed, it can push configurations out to thousands of devices with a single key stroke to get the WLAN up and running as quickly as possible.

The system can also import RF maps from an Ekahau™ site survey tool and overlay them on top of existing floor plans for an exact RF topology and more accurate rogue access point and user location. An open API can be used to export user location to third-party applications.

Ongoing operations

The WLAN Management Software system is designed to equip administrators with the powerful tools required to support wireless voice and converged services. The visual interface presents a top-level floor plan view that includes RF topology, access point, rogue access point and user location mapping with configurable alarms for ongoing monitoring of the WLAN. Should an event occur, administrators can troubleshoot by drilling down to a granular level and see user roaming and usage history, RF and network statistics and hierarchical maps. The threat of rogue access points and ad-hoc users is mitigated through immediate identification, location and containment. All user, network and RF data, statistics and history can be captured in customizable reports and the planning tool can also be used on an ongoing basis to support configuration updates and new equipment deployments as the network grows. The WLAN Management Software system also features an HP OpenView plug-in to integrate with existing management systems.

SECURITY CAPABILITIES OF THE WLAN 2300 SYSTEM

Security standards/authentication

- WPA/WPA2
- 802.11i/802.1x
- EAP-TLS, EAP-TTLS, EAP-MD5, EAP w/MS CHAP v2 and PEAP, PEAP-TLV
- MAC authentication
- X.509 certificates
- RADIUS AAA
- RADIUS Extensions
- Local AAA
- Web-based AAA

Cryptography

- WEP, dynamic WEP, TKIP: RC4 40/108 bit
- SSL, TLS: RC4 128 bit
- CCMP: AES 128 bit
- Public key cryptography RSA 1024/2048 bit

Wireless threat protection

- Flood attack detection
- RF jamming protection

- AP MAC address masquerading detection
- Weak WEP IV detection
- Spoof attack detection
- Rogue AP protection

Access control

- User/group identity
- Multiple SSID
- MAC filtering
- Layer 3 deny filters
- Layer 4 deny filters
- Time-of-day restrictions
- Day-of-week restrictions
- Location-based policies
- Client blacklisting
- Subnet classification
- VLAN assignments
- Roaming restrictions

ROGUE ACCESS POINT PROTECTION WITH THE WLAN 2300 SERIES

- Rogue access point detection — Unauthorized access point is detected during an RF scan.
- Rogue access point alert — Notifies the appropriate administrator of the event.
- Rogue access point classification—Analyzes and classifies the threat based on behavior.
- Rogue access point location — Identifies access point location on the floor map.
- Rogue access point monitoring — Records behavior and usage.
- Rogue access point containment — Threatening access point is crippled by an RF attack.

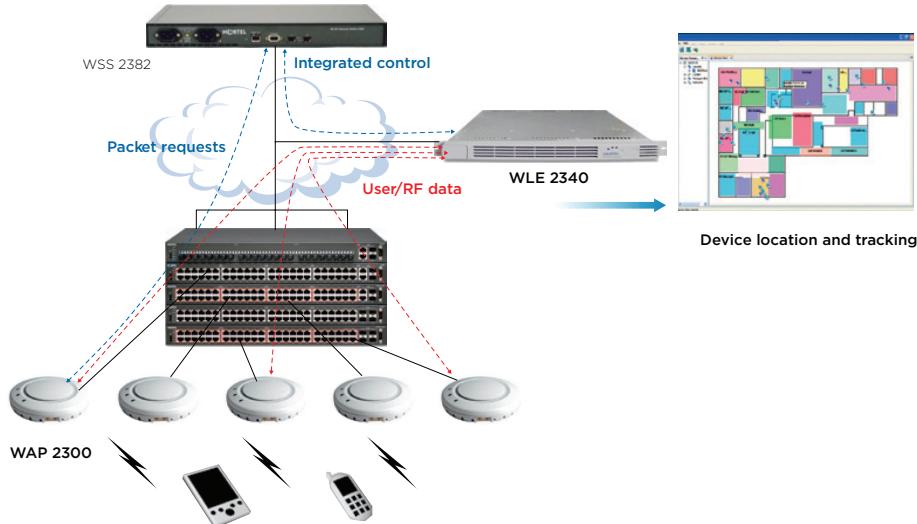
WLAN Location Engine

The WLAN Location Engine 2340 is an integrated location services solution that uses the RF and user data captured by the WLAN 2300 access points to resolve the location of thousands of mobile stations or asset tags simultaneously.

Security standards/authentication

- | | |
|---|---|
| <ul style="list-style-type: none"> • WPA/WPA2 • 802.11i/802.1x • EAP-TLS, EAP-TTLS, EAP-MD5, EAP w/MS CHAP v2 and PEAP, PEAP-TLV • MAC authentication | <ul style="list-style-type: none"> • X.509 certificates • RADIUS AAA • RADIUS Extensions • Local AAA • Web-based AAA |
|---|---|

Figure 11. WLAN Location Engine 2340



Integrated location services allow the WLAN 2300 system to locate and track any mobile station with high-resolution accuracy for applications such as location-based policies, content delivery or asset locating and tracking.

Cryptography

- WEP, dynamic WEP, TKIP: RC4 40/108 bit
- SSL, TLS: RC4 128 bit
- CCMP: AES 128 bit
- Public key cryptography RSA 1024/2048 bit

Wireless threat protection

- Flood attack detection
- RF jamming protection
- AP MAC address masquerading detection
- Weak WEP IV detection
- Spoof attack detection
- Rogue AP protection

Access control

- User/group identity
- Multiple SSID

- MAC filtering
- Layer 3 deny filters
- Layer 4 deny filters
- Time-of-day restrictions
- Day-of-week restrictions
- Location-based policies
- Client blacklisting
- Subnet classification
- VLAN assignments
- Roaming restrictions

Rogue access point protection with the WLAN 2300 Series

- **Rogue access point detection** — Unauthorized access point is detected during an RF scan.

- **Rogue access point alert** — Notifies the appropriate administrator of the event.
- **Rogue access point classification** — Analyzes and classifies the threat based on behavior.
- **Rogue access point location** — Identifies access point location on the floor map.
- **Rogue access point monitoring** — Records behavior and usage.
- **Rogue access point containment** — Threatening access point is crippled by an RF attack.

This capability can be used to strengthen security with zone-based access controls, enable new services such as location-specific content delivery, or as the foundation for new applications like asset tagging, locating and tracking. An application programming interface makes the location information accessible for any business application that can benefit from user location.

WLAN 2300 Accessories

The WLAN 2300 series supports a range of antennas for both indoor and outdoor use. This allows for improved deployment flexibility where planners can choose an antenna pattern that meets coverage requirements while allowing for convenient AP placement and installation. Customers may use outdoor antennas for fringe coverage around and between buildings on an enterprise campus. This allows customers to extend their wireless LAN services outdoors, allowing them to enjoy the benefits of a single management system for outdoor use in courtyards, parking lots, the exteriors of a warehouse for shipping and control applications. Other applications include outdoor Internet access, security cameras, facilities dispatch and environmental controls. Optional power supplies are also available.



Trapeze Networks MP-432



Trapeze Networks MX-2800

Optional 802.11n hardware

Trapeze Networks MP-432 (802.11n Access Point)

The Trapeze Networks indoor MP-432 is a high-performance 802.11n (3x3) Multiple Input/Multiple Output (MIMO), dual radio access point, with maximum aggregate data rates of up to 600 Mbps. One radio operates in the 2.4 GHz band and one in the 5 GHz band. The MP-432 is backwards compatible with legacy 802.11 a/b/g clients in the 2.4 GHz and 5 GHz bands to provide investment protection without the need for a second overlay networks. It is compliant with the IEE 802.11n Draft 2.0 standard. In most deployment scenarios, the MP-432 operates in full functionality 3 x 3 MIMO dual radio mode with the existing IEEE 802.3af. The MP-432 is compatible with the Avaya WLAN 23xx Security Switches and Trapeze Networks MX-2800 Controller.

Trapeze Networks MP-82 (802.11n Access Point)

The Trapeze Networks Mobility Point 82 is an 802.11n (2x3) Multiple Input / Multiple Output (MIMO), dual radio access point, designed for high density deployments requiring maximum capacity. The MP-82 is compatible with Avaya's WLAN 23xx Security Switches and Trapeze Networks MX-2800 Controller. The MP-82 is backwards compatible with legacy 802.11 a/b/g clients providing investment protection. It is compliant with the IEE 802.11n Draft 2.0 standard.

Trapeze Networks MX-2800 (High Capacity Controller)

The Trapeze Mobility Exchange MX-2800

is the next-generation WLAN controller for medium to large-size enterprise WLAN deployments. It offers 28 Gbps of throughput and supports up to 512 802.11n APs, while providing always-on availability and hitless failover with no service interruption.

Key features include:

- 28Gbps Ethernet switching capacity
- 2 10-Gbps ports; 8 1-Gbps ports
- Line-rate speed and throughput
- Industry's only hardware-switched wired and wireless
- 512 active AP's (Note: max 256 AP with software version 7.0; max 512 AP with software version 7.2 or later)
- 12,000 active clients per switch

Why you should choose Avaya's WLAN 2300 Series

Built to support voice and multimedia applications in today's networks

The WLAN 2300 Series is designed for voice, multimedia and business-critical applications; it adheres to the latest QoS standards and minimizes the performance impact of today's strong security standards by offloading back-end AAA servers of many cryptographic processing functions. This architecture allows fast secure roaming among all access points with the minimal latency and jitter needed to support time-sensitive applications. Dynamic RF management ensures service resiliency by protecting against unexpected interference, obstructions, outages and weak coverage

zones that can have a significant impact on performance and user experience. The system can also be deployed with full redundancy of all network components to protect against service interruption.

Mobility management keeps control over roaming users

The WLAN 2300 Series takes mobility to a higher level by allowing security and QoS policies to follow users as they roam anywhere on the WLAN network. Access controls, VLAN/subnet assignments, bandwidth rate, QoS priorities and multicast memberships are enforced even if the user roams between floors and buildings. Administrators can assign time-of-day restrictions and even location-based restrictions that block access from specific areas like parking lots or exam and emergency rooms.

Easy implementation — from planning to production

The WLAN Management Software system helps network administrators through every phase of a WLAN project from planning and configuration through to monitoring, reporting, expansion and ongoing operations. Beginning with a basic floor plan, WLAN Management Software builds a visual map of the ideal WLAN network, including radio coverage, physical topology and access point locations. The tool then produces a bill of materials for your implementation and once the equipment is installed, configurations can be pushed out to all system elements with a single key stroke. Granular monitoring and customizable reporting keeps administrators on top of all activity and provides everything they need to handle troubleshooting and support calls for enterprise-wide converged mobile services.

Extend your LAN to wireless with seamless deployment in any network

The WLAN 2300 Series is designed to operate as an overlay to existing IP networks without the need for network reconfigurations or expensive upgrades to core switch infrastructure. The solution can be configured to enforce existing authentication policies and extensions; it does not introduce any new protocols that will impact other devices. The access points can be installed on any subnet or in any wiring closet, allowing the placement to be simple, convenient and focused on providing optimal wireless coverage. Once in place, the access points attach to their controllers across the network, and provide seamless roaming for mobile users, regardless of what subnets the access

points are attached to. The mobile user's IP address doesn't change, and applications keep working. For installations that support multiple user types such as hospitals, multi-tenant buildings, airports and college campuses, one WLAN infrastructure can be securely partitioned to form up to 32 unique service groups, each with their own Web-portal, security and QoS policies.

Standards-based/open client approach for user and application compatibility

The WLAN 2300 Series adheres to the latest IEEE and de-facto industry standards to ensure strong security and QoS while maintaining compatibility with user devices. The system supports security standards such as WPA, WPA2, 802.11i/802.1x with

WEP, Dynamic WEP, TKIP, CCMP, EAP-TLS, TTLS and PEAP, PEAP-TLV and QoS standards including 802.1p and DiffServ, WMM and SVP. Advanced features such as dynamic RF management, fast roaming and user policy management do not carry any client prerequisites other than the 802.11a or b/g standards present on all adapters and Centrino™ enabled devices. The WLAN Management Software system makes work easy during the planning phase by recognizing floor maps in all common formats, including AutoCAD® DXF™, AutoCAD DWG, JPEG or GIF file types. Avaya's WLAN 2300 Series is the ideal choice for customers seeking the performance, management tools and resiliency required for delivering high-quality voice and multimedia applications over a wireless network.

About Avaya

Avaya is a global leader in enterprise communications systems. The company provides unified communications, contact centers, and related services directly and through its channel partners to leading businesses and organizations around the world. Enterprises of all sizes depend on Avaya for state-of-the-art communications that improve efficiency, collaboration, customer service and competitiveness. For more information please visit www.avaya.com.



INTELLIGENT COMMUNICATIONS

© 2009-2010 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. and are registered in the United States and other countries.

All trademarks identified by ®, TM or SM are registered marks, trademarks, and service marks, respectively, of Avaya Inc.

All other trademarks are the property of their respective owners. Avaya may also have trademark rights in other terms used herein.

12/09 • DN5014

avaya.com



Avaya Wireless LAN 8100 Series

The Avaya WLAN 8100 Series combines the latest 802.11n wireless standard with a new and truly integrated wireless/wired architecture for a stellar result - an advanced solution that delivers wired performance to wireless users at a lower total cost of ownership.

Optimized Support for Real Time Applications

With the explosion of mobile devices such as smart-phones and tablets within the enterprise, it is imperative that WLAN networks can handle this rapid growth. At the same time, networks must meet the stringent requirements that real time applications, such as video and voice, place on the Wi-Fi infrastructure. Avaya has designed the WLAN 8100 Series from the ground up to provide optimized support for real time applications and to provide anytime, anywhere access for the full breadth of enterprise applications. The series includes three primary components: WLAN Access Points, WLAN Controllers and the WLAN Management Software.

WLAN Access Points provide wireless access to mobile devices and perform encryption/decryption for wireless traffic, priority queuing and radio frequency (RF) monitoring, including rogue access point identification and containment.

Features include:

- One to three 802.11a/b/g/n radios
- Two spatial streams over integrated MIMO Antennas (2.4 GHz and 5 GHz)
- Integrated and external antenna options
- Simultaneous dual band operation (2.4 GHz and 5 GHz)
- Adaptive frame aggregation
- One GigE uplink port
- Full performance with current 802.3af Power over Ethernet standard

The New Era of Wireless Connectivity

The market is embarking on a new era where an enterprise's wireless network will deliver services at levels equivalent to wired LANs. This will enable office environments to be entirely wireless and integrated with existing fixed and cellular wide area networks, giving workforces seamless universal mobility both in and out of the office. This will require a true wireless broadband infrastructure capable of supporting all communications needs, including voice, video, unified communications, and other real-time applications. With the Avaya next generation WLAN 8100, the freedom of true high-speed wireless can transform the office environment.

WLAN Controllers control the access points and perform key centralized functions such as security, networking, quality of service (QoS), and roaming for mobile users. Controllers can be deployed as either standalone wireless controllers or integrated into the Avaya wired portfolio with the control capability running as a virtual machine on a server.

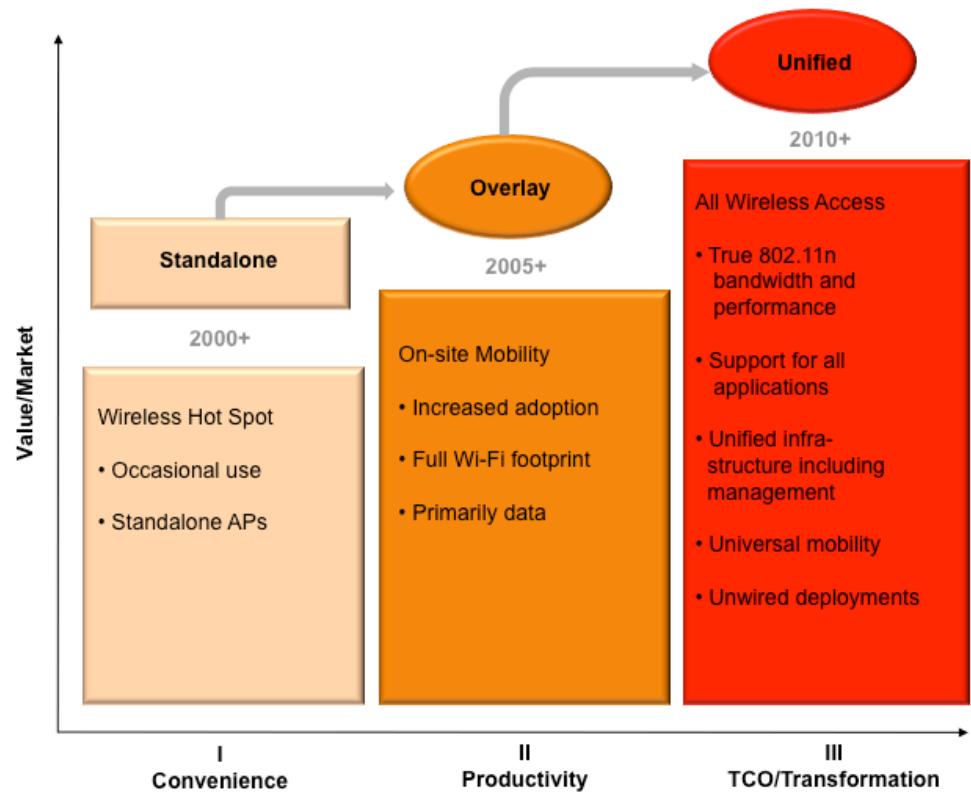
Features include:

- Support for up to 512 access points
- Scalable architecture with separate data and control planes, each of which can scale independently
- Expansion module for further scalability
- Ability to move data plane and/or control plane to core/edge switches

The WLAN Management Software

is a comprehensive design and management tool that provides granular monitoring and reporting for complete visibility and control over the entire system. It integrates with Avaya Unified Communications Management.

By offering centralized management and eliminating the need to support multiple overlay networks—including LAN, WLAN, VPN, voice and network management—the WLAN 8100 Series can lead to significant operational cost savings. The series simplifies surveying, configuring, deployment, monitoring and reporting functions, and also includes self-diagnosing and self-healing capabilities to support mainstream WLAN applications as efficiently as possible.



New Architecture for a New World

To help WLANs reach the speeds of wired LANs, Avaya has developed a new approach to solve old wireless traffic bottlenecks.

Traditional centralized architectures route all wireless control and data traffic through a wireless controller before forwarding it to its final destination. As more users join the network, traffic increases. Bandwidth-heavy applications such as video add to this congestion. Because everything on the network is forced through the same gate, the wireless controller becomes an unavoidable bottleneck and degrades performance.

Avaya next generation WLAN architecture decouples wireless control traffic from wireless data (application) traffic, enabling increased resilience and performance, without sacrificing the ability to quickly increase network capacity.

By separating the control and data functions, the Wireless Control Point can run on virtual servers rather than dedicated network hardware. This not only increases network performance; it can reduce hardware costs and network complexity.

For enterprises using Avaya LAN Switching products, wireless switching will be implemented as a software function in Avaya-enabled core or access switches upon availability of next generation stackable Ethernet Routing Switches.

Key benefits of the Avaya split-plane architecture include:

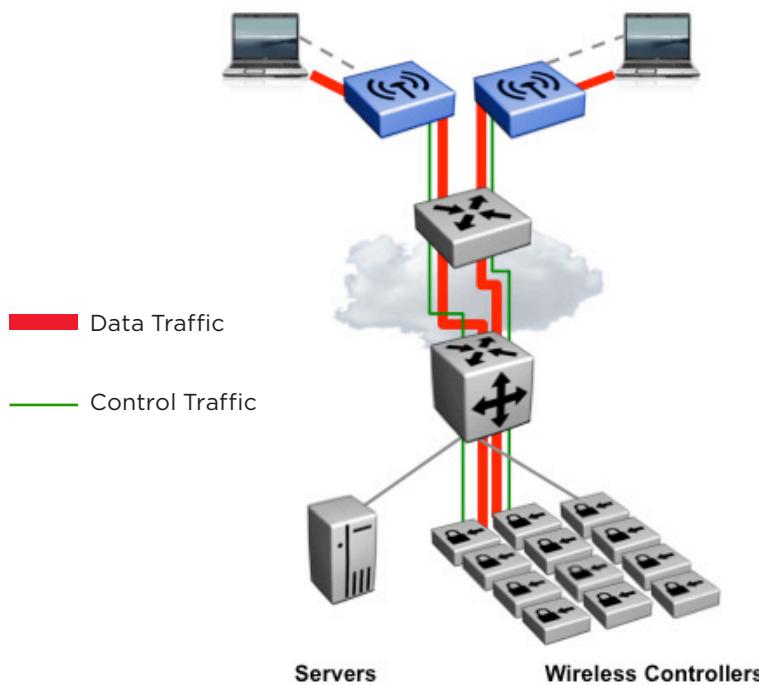
- Optimized performance allowing wireless data to take the most efficient path through the LAN switches directly from source to destination, helping reduce latency and jitter to create a better user experience for real time traffic, such as voice
- Improved network resilience and flexibility through virtualization of the wireless control function

- Easy, independent scalability for wireless application and control traffic, allowing businesses to scale bandwidth in a sensible and efficient way, and enterprises to load services (such as mobility roaming) without limiting the domain size
- Reduced hardware and equipment costs through switch virtualization and more efficient data flow

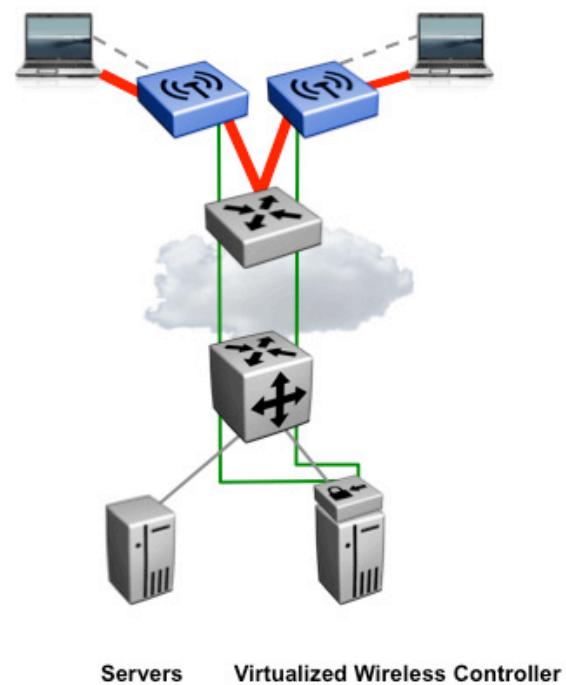
Advanced Services for an Advanced Network

For wireless to truly become an end user's primary means of network access, it must be able to support the same applications that run over a wired LAN infrastructure. The WLAN 8100 provides optimized support for every aspect of an enterprise network including voice, unified communications, video, E-911, location tracking, guest management and advanced security, all with unprecedented reliability and resilience.

Traditional Centralized Model



Avaya 'Split-Plane' Solution



Video

An increasing number of enterprises are relying on video to facilitate communication and reduce travel expenses. While video already represents a major driver of bandwidth consumption, this is expected to grow more rapidly in the next five years, placing increasing demands on the network in the process.

The WLAN 8100 Series split-plane architecture efficiently routes high bandwidth video traffic and can quickly scale to meet the increased demand without additional hardware investment.

Voice

The WLAN 8100 delivers high-quality voice and converged services to achieve measurable user productivity improvement. By offering a single turnkey end-to-end mobility solution that includes a WLAN infrastructure, Voice over WLAN, converged LAN/WAN, IP PBX systems and voice handsets and clients, Avaya can truly unify enterprise communications.

The Avaya VoWLAN solution includes:

- High voice call density per access point for more cost effective AP deployments
- VIEW certification with Avaya Wireless Handsets for proven Wi-Fi interoperability and maximum performance
- VoWLAN clients offering full interoperability with Avaya IP PBX systems
- Voice calling from PCs with Avaya one-X® Softphone
- Advanced Call Admission Control (CAC) algorithms to help ensure excellent voice quality

Instead of simply counting calls like most competitive solutions, the Avaya Dynamic CAC solution takes into account bandwidth usage and changes in the RF environment. This allows more calls to be admitted while preserving optimum call quality. Three key parameters allow Avaya CAC to preserve optimum quality:

Media Measurement gives a holistic understanding of resource consumption for all sessions in progress, including RF bandwidth consumption, interference and other factors. The product of these measurements constitutes a “utilization factor” that helps estimate traffic and call flow.

New-Flow Estimation lets new calls send mobile signals to the AP that specifies the traffic attributes and QoS requirements for a session. The New-Flow Estimator combines the resource requirements for the call with available resources in the network to estimate the total new resource usage.

Admission Decision decides whether or not to admit the new call based on the New-Flow Estimation. If enough resources are not available, Admission Decision can borrow bandwidth from other applications, enabling powerful resource sharing possibilities.

Emergency Support

While mobile communications offer many advantages, an emergency offers a unique challenge. E-911 tracking systems can be ineffective for WLAN handsets since a user with a Wi-Fi mobile handset can call from anywhere.

Traditionally, call locations were mapped to an originating static line. Since the advent of mobile phones and IP telephony, 911 emergency response systems have had to adapt to an environment where calls can be placed from almost anywhere and change at a moment's notice.

A number of solutions have tried to solve this problem with limited success. Most have been undermined by a presumption that a network's wiring structure doesn't change. While they allow for instantaneous identification of a call's origin, the entire network database must be updated the moment a single cable is moved or changed for the system to continue functioning.

With the WLAN 8100 Series, Avaya supports full E-911 VoWLAN integration. The WLAN 8100 Controller interfaces with the Avaya Communication Server 1000 call server or Avaya Aura® architecture to precisely identify the location of an emergency call. This is made possible by allowing the mobile handset or client application to communicate with the nearest AP to establish an emergency response location (ERL). In the event of an E-911 call, the ERL is relayed to emergency dispatchers. If the call location changes, dispatchers are updated in real-time.

ERLs are mapped to APs, thus covering the entire wireless network area. Because they are rarely moved, mapping devices to access points is an efficient and reliable way to establish their location and is resistant to disruption by future technological changes.

Guest Access and Management

Enterprise networks must be open enough to allow easy access for guests and temporary users, but secure enough to prevent these same users from accessing restricted information.

Guest access is one of the most pervasive applications of wireless networking, but most solutions require dedicated resources, such as front desk and IT personnel, in order to provision accounts. Privileged access to infrastructure devices can also open the core network to potential security risks.

The WLAN 8100 Guest Management solution provides enterprises with 24/7 guest network access without requiring the overhead of an IT helpdesk. The Avaya IDEngine Guest Manager generates a unique user ID and password for each visitor, providing secure, convenient network connectivity for guests and temporary users. User IDs come with specific security profiles that enable access only for specific resources and a limited amount of time. Guest provisioning can be generated automatically, or customized by front desk or IT personnel. Once a user has been provisioned, they have seamless controlled access through either wired and/or wireless infrastructures.

Avaya Guest Management solutions include:

- Authenticated wireless access using captive-portal for guest users and temporary staff with notebook PCs, tablets, PDAs or smart phones
- Simplified guest user provisioning by corporate end-users, which offloads the task of creating and managing guest user accounts from front desk personnel or IT staff
- The ability to allow partial access to specific parts of the network based on different guest user classes



802.11n: A Truly Wireless Standard

The 802.11n standard brings wireless networking greater range and penetration than ever before. The standard adds multiple-input multiple-output (MIMO) antennas to wireless devices. In addition, with bandwidth up to 300 megabits per second, 802.11n is up to five times faster than the previous wireless standard for a true broadband experience.

Location Tracking

More businesses are embracing location tracking as a means to improve productivity and reduce costs. In certain environments, such as hospitals, knowing the location of a staff member or a specific piece of equipment can literally be the difference between life and death. For other enterprises, tracking equipment location can be a significant driver for cost savings.

Enterprises can implement location tracking for all 802.11 devices using active RFID tags and their existing WLAN infrastructure. Avaya Real Time Location Services (RTLS) allows enterprises to track personnel and assets as they move within the Avaya WLAN 8100 Series network. Easy to use, cost effective and accurate, Avaya location tracking is interoperable with any Wi-Fi-enabled device in the WLAN 8100 coverage area. To track non-Wi-Fi assets, Avaya offers battery-powered RFID tags that interact with RTLS servers and applications for comprehensive, real-time tracking.

Network Security

As with any network, security is a top priority for the Avaya WLAN 8100 Series. A holistic approach addresses security in a number of ways:

Authentication and Encryption

keep user data secure and confidential. Built around the 802.11i standard, the WLAN 8100 Series supports WPA2, WEP, 802.1X and Proactive Key Caching; security measures that are more robust than most wired networks.

Wireless Intrusion Detection (WID)

provides RF surveillance to detect rogue network activity and malicious attacks. WLAN 8100 provides basic WID capabilities and an advanced Wireless Intrusion Detection System / Wireless Intrusion Prevention System option for enterprises requiring greater security.

Secure Network Access delivers protection from infected clients. Because most Wi-Fi devices are also mobile, they can connect to hundreds of networks in their lifetime, incurring a significant risk of virus infection. The WLAN 8100 Series supports 802.1X Port-Based Network Access Control for identifying users for authentication and authorization to an assigned virtual LAN. The physical or virtual WLAN Controller works closely with the AAA server to offload the 802.1X EAP protocol processing, reducing the burden on the AAA server. In addition, Avaya IDEngines Ignition Server provides centralized authentication and authorization for wired, wireless and VPN network devices, including:

- AAA identity-based network access control
- Easy-to-use standards-based policy engine
- RADIUS integration with all enterprise network equipment
- Quick and deep integration with major directories

Unauthorized Access Point Protection

Protection finds and contains unauthorized wireless activity. The WLAN 8100 Series scans and maps the RF neighborhood, monitoring activity to help ensure only authorized access points are granted network access. Any unauthorized wireless paths into the network, such as peer-to-peer sharing programs, are isolated and contained.

Always-On Architecture

Next generation WLAN solutions require high resiliency and ubiquitous WLAN coverage. The Avaya always-on architecture features a number of capabilities that maximize network uptime:

- Hitless failover without service interruption
- APs that dynamically map to controllers, optimizing auto-AP load balance
- AP/controller clustering support, many-to-many redundancy and the addition of new switches without needing to configure changes and with zero network downtime

Each WLAN Controller 8180 comes with 16 or 64 AP licenses, with more available for purchase as needed. When fully operational, the WLAN controllers automatically load balance the APs. If a controller fails, licenses on that controller automatically shift to another. In the event of a hardware failure, this provides license failover and eliminates the need to purchase additional licenses. To get the same level of resiliency from other solutions, enterprises would have to purchase licenses on both controllers, doubling the cost.

WLAN 8100 – A Wireless Solution for a Wireless World

The WLAN 8100 offers the speed and security of a wired LAN with increased scalability, flexibility and resilience. A next generation solution that offers common policies and tools for security, guest access and network management, the WLAN 8100 is the cornerstone to a truly wireless environment. The Avaya WLAN 8100 Series leverages the rich heritage of carrier-grade voice and more than a decade of wireless innovation. A unique, wireless architecture allows the WLAN 8100 Series to adapt to enterprise needs as they arise using fewer components and more affordable hardware investments.

Move to the next generation of wireless without compromising speed, security or performance, all for a lower total cost of ownership.



WLAN AP 8120
Indoor, high performance, 802.11n, dual radio access point with integrated antenna.



WLAN AP 8120-E
Plenum-rated, two radio, 802.11n access point for use with external antennas.



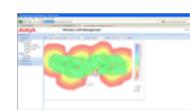
Omni directional external antenna
External dual band MIMO antenna 180° for WLAN AP 8120-E (6 element).



Directional external antenna
External dual band MIMO antenna 70° for WLAN AP 8120-E (3 element).



WLAN Controller 8180
Two models: WC 8180: 64 license controller and WC 8180 -16L: 16 license controller.



WLAN Management System 8100
Comprehensive design and management tool license controller.

Top 10 WLAN 8100 Differentiators

- 1. Optimized support for Business Applications**
 - More than just web or email access, Avaya WLAN excels at voice, video and data
- 2. Support for Advanced Wireless Applications**
 - Out-of-the-box E-911 location tracking helps reduce integration costs
- 3. Availability**
 - Avaya WLAN supports load balancing, controller clustering and license pooling, delivering higher availability at a lower cost
- 4. Scalability**
 - Scale users or data paths independently as needed
- 5. Performance**
 - Avaya WLAN supports a high number of active Wi-Fi calls per access point
- 6. Security**
 - Much more than just WLAN security standards, Avaya provides full centralized (unified) network access control for both wired and wireless
- 7. Network Management/Administration**
 - Manage the ecosystem, not the box with integrated wired, wireless and voice network management from Avaya
- 8. Architecture**
 - Users receive equal levels of service whether running wired or wireless
- 9. Total Cost of Ownership**
 - Unified approach removes not only performance boundaries but also CAPEX and OPEX versus the overlay model
- 10. Full Solution Provider**
 - Avaya offers a true and proven end-to-end ecosystem, from critical unified communications applications through the access technologies, management and services

About Avaya

Avaya is a global provider of business collaboration and communications solutions, providing unified communications, contact centers, data solutions and related services to companies of all sizes around the world. For more information please visit www.avaya.com.

Learn More

To learn more and to obtain additional information such as white papers and case studies about Avaya Wireless LAN contact your Avaya Account Manager or Authorized Partner or visit us online at www.avaya.com.

© 2011 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. and are registered in the United States and other countries. All trademarks identified by ®,™, or SM are registered marks, trademarks, and service marks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. Avaya may also have trademark rights in other terms used herein. References to Avaya include the Nortel Enterprise business, which was acquired as of December 18, 2009.
08/11 • DN5110

สำนักงานที่ครบครันความทันสมัย สร้างสรรค์เพื่อธุรกิจของท่าน

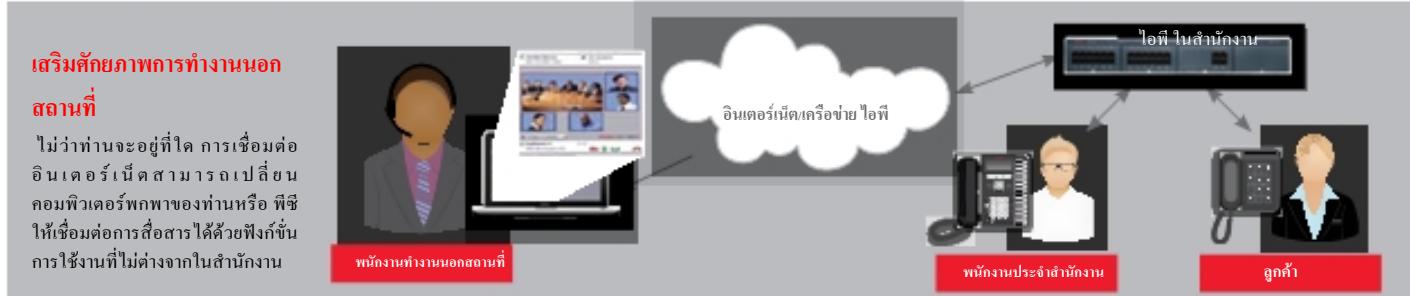
อาว่าย่า ไอพี ออฟฟิศ สร้างสรรค์เพื่อธุรกิจขนาดเล็กและขนาดกลางเพื่อรองรับและตอบสนองความต้องการของลูกค้าได้มากยิ่งขึ้น ในขณะที่ท่านสามารถประหยัดค่าใช้จ่ายในการสื่อสาร

เรียนรู้เกี่ยวกับ
อาว่าย่า ไอพี ออฟฟิศ
ให้มากยิ่งขึ้น

- ชัมการสาชิต
- คำนวนผลตอบแทนในการลงทุนใน 5 นาที
- ชัมเรื่องราวของลูกค้า
- ไปที่ avaya.com/ไอพี ออฟฟิศ



ยกระดับระบบการสื่อสารที่ท่านมีให้มีประสิทธิภาพยิ่งขึ้น



គំរាប់រាជការពីរាជធានីភ្នំពេញទៅភ្នំពេញ និងត្រូវបានដោះស្រាយជាការងាររបស់ខ្លួន

อาว่า ไอโฟนฟีสแลนบลูบุนราชาใช้งานโทรศัพท์ในระบบของจีอ่า ซึ่งประกอบด้วยไอโฟนรุ่น 9600 และรุ่น 1600 คิจิตอลไฟน์รุ่น 9500 และ 1400 และโทรศัพท์ระบบเบสต์ไอโอพีในรุ่นต่างๆ ของโทรศัพท์มือถือ



ຄັກໜະຈຳພາຍ

รุ่น	ไฮไฟ ออฟฟิศ 500 สามารถทำงานด้วยไฟจ้านในระบบได้มากถึง 384 คันต่อห้องระบบเครือข่ายจ้างงาน สูงสุด 32 แห่งและสามารถเลื่อนท่อภายในสูงสุดถึง 1000 หมาเมลต่อเครื่อง
ขนาดต่อหน่วย	ไฮไฟ ออฟฟิส 500: กว้าง 445 x สูง 73 x หนา 365 (มม.); ระยะห่างต่อสุดด้านหน้าและด้านหลัง: 75 มม. เพิ่มน้ำหนัก: กว้าง 445 x สูง 71 x หนา 245 (มม.); ระยะห่างต่อสุดด้านหน้าและด้านหลัง: 75 มม.

ຄມຄັກໝາຍເດືອນ

การเข้มต่อ	<ul style="list-style-type: none"> ความสามารถในการใช้งาน : อนาคต, คิดbold, ใจที่, เสือไอพี ไฟฟ้า โทรศัพท์ทางไกล : อนาคต, ทีวี/อีวี/พาร์วีโอ, โทรศัพท์ทางไกลเดล้อไอพี 	<ul style="list-style-type: none"> เครื่องเข้า - เครื่องเข้า คิวบิก ก้อน ที่ 1 ใจ และไอพี - ใช้งานได้ในสถานที่ต่างๆ ด้วยเครื่องเข้าขนาดเล็ก (ไปจนถึงผู้ใช้งาน 1000 ราย ใน 32 แห่ง) หัวข้อมูลนับค่าการใช้งานที่สำนักตรวจสอบอย่างไร
คุณสมบัติทั่วไป	<ul style="list-style-type: none"> แสดง功用ของโทรศัพท์ให้ด้านมา การพัฒนา การรับสาย การต่อสาย การเปลี่ยนชื่อเครื่อง โทรศัพท์ที่มีเสียงภาษา การรับสาย ระบบเข็มบอก การสนับสนุนภาษา <p>(สูงคงที่ 64 คู่สายรวมทั้งสิ้น 128 พอร์ต)</p>	<ul style="list-style-type: none"> การโอนสาย ระบบเข็มบอกด้านมือถือ (สายไปร่วม, ไม่มีชื่อรับสาย, ไม่สามารถอธิบายได้) ระบบติดตาม ระบบโทรศัพท์ด้านมือถือ ห้ามรบกวน เสียงดนตรีที่ตัดสิ้นเชิงความหลากหลาย บันทึกเสียงฝ่ายต่อคู่ร่วมงาน ระบบเข็มบอกสามารถเปลี่ยนแปลงได้ การทดสอบผลเรื่องความเสียงไปร่วมอีเมล์
คุณสมบัติขั้นสูง	<ul style="list-style-type: none"> การบันทึกสายสนับสนุน ความสามารถในการเข้าใช้งานในโทรศัพท์เครื่องอื่นๆ (ในสถานที่ที่ขาดแคลนหรือต้องการสถานที่) ให้ผลการใช้งานที่ปรับเปลี่ยนได้ในสถานที่ต่างๆ คู่สายโทรศัพท์เคลื่อนที่ที่ขยายความสามารถของโทรศัพท์ การใช้งานร่วมกันในระบบการสนับสนุนแบบสามภาษา (ต้องระบบที่ป้องกันการต่อสาย) ระบบรวมเข็มบอกที่ส่งกันเดียวที่ต่างๆ ไปเป็นหนึ่งเดียว 	<ul style="list-style-type: none"> อ่านเข็มบอกเป็นสิ่งพุ่ง ระบบบริการเข็มบอกจากฐานข้อมูลเป็นเรื่อง สูญเสียการติดต่อ <ul style="list-style-type: none"> - เสียงที่ สต็อก, เริ่มใหม่, คิดใหม่, การลดลงของผู้คนคุณ - เอเชียคัมเบอร์, อุปกร์ร์รายงานฟังก์ชันการทำงาน, การบันทึก - บันทึกประวัติการใช้งาน ฯลฯ

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับอฟฟิศ "ไอพี 祚ไห" ท่านติดต่อผู้จัดการฝ่ายบริการลูกค้าข้างหน้าของเว็บไซต์ด้านบนที่ได้รับการแต่งตั้งขึ้นของอواญา หรือเข้ายังเว็บไซต์ของเราราคาที่ avaya.com

อย่างไรก็ตามเทคโนโลยีการสื่อสารและระบบโทรศัพท์อันดับหนึ่งของโลก

รายงานข้อมูลการประกอบธุรกิจโทรศัพท์ของกลุ่มบริษัท เดลโอยอิป ไตรมาสที่ 4 10 กุมภาพันธ์ 2554

เกี่ยวกับอาชญา

อาชญากรรมทางการสื่อสารในธุรกิจ บริษัทให้บริการด้านการรวมระบบการสื่อสารในองค์กร สูนย์กลางการติดต่อสื่อสาร การพัฒนาเครือข่ายด้านข้อมูลและบริการที่เกี่ยวข้องโดยตรง และการบริการชั้นสูงของอาชญากรรม

ในการต่อоворือเพื่อพัฒนาประสิทธิภาพในการบริการด้านลูกค้าและเพื่อความล้ำหน้าในการแข่งขันไม่เป็นหนึ่งเดียวท่านสามารถอยู่ในชุมชนฯ ได้ที่ www.avaya.com.

ชื่อ อาชยาและเครื่องหมายของ อากาฯ เป็นเครื่องหมายการค้าของบริษัท อากาฯ จำกัด และได้จดทะเบียนในประเทศไทย
สำหรับอุปกรณ์และในประเทศไทยต่างๆ เกี่ยวกับงานการค้าทั่วทั้งประเทศที่แสวงค์เครื่องหมาย TM หรือ SM เป็นเครื่องหมายด้วย เครื่องหมาย
การค้า และเครื่องหมายการค้าที่จดทะเบียนแล้วของอากาฯ
เจ้าของน้ำคราฟ อากาฯ ซึ่งมีเครื่องหมายลิขสิทธิ์เดียวกันอีกด้วยที่รับใช้ลูกค้า ควบคู่กับเครื่องหมายน้ำคราฟ อากาฯ

เพื่อลงนามเข้าร่วมในนั้น ที่ที่ใช้ในที่นี้ การอ้างอิงถึง

AVAYA
The Power of We™