IT@Intel White Paper

Intel Information Technology
Business Solutions
April 2010

Managing a Global Wireless LAN

Mike Mauch
IT Manager, Intel IT

Gary Veum
Network Specialist, Intel IT

Mario Vallejo
WLAN Service Owner, Intel IT

Executive Overview

Intel IT developed a new management and support structure for wireless LANs (WLANs). We consolidated first-level support and centralized the WLAN engineer workgroup as well as device management. We manage the WLAN as an integrated service that enables centralized control of the WLAN, using global tools for centralized monitoring, reporting, and configuration. This approach provides all stakeholders with a common view of the components of the WLAN service and the network.

The combination of central IT engineering expertise, a set of global guidelines, and a centralized management platform allows us to deliver a highly available service with minimal support staff.

Our centralized WLAN management system offers several benefits to IT.

- **Increases efficiency.** Previously, local WLAN configuration changes required five minutes per access point; the central WLAN management system reduces this to just five minutes per building. Replicated across 150 sites, we can greatly improve efficiency.
- **Uses global configuration templates.** Common templates apply to the entire global network, which enables us to efficiently make configuration changes, verify configurations, and monitor for unauthorized configuration changes.
- **Enables reporting.** Provides useful information, such as WLAN device inventories and wireless adoption trends, to IT and other Intel groups, supporting informed business decisions.
- **Enables us to be supplier-independent.** The system's simple user interface allows non-specialists to monitor and diagnose simple WLAN problems without learning supplier- and equipment-specific commands. We can add new equipment and OS versions with minimal retraining of personnel.

Our WLAN management system is the first wholly centralized managed service within Intel IT. The combination of central IT engineering expertise, a set of global guidelines, and a centralized management platform allows us to deliver a highly available service with minimal support staff.

Contents

IT@INTEL

IT@Intel is a resource that enables IT professionals, managers, and executives to engage with peers in the Intel IT organization—and with thousands of other industry IT leaders—so you can gain insights into the tools, methods, strategies, and best practices that are proving most successful in addressing today's tough IT challenges. Visit us today at www.intel.com/IT or contact your local Intel representative if you'd like to learn more.

BACKGROUND

Over the past decade, Intel has increasingly adopted Wi-Fi* technology to support a highly mobile global workforce, and employees have become reliant on it for office network connectivity. From an initial installation of 250 access points (APs) in 2001, the Intel network now includes wireless LANs (WLANs) at 150 sites in 63 countries. While some sites have as few as two APs, one of our main campuses has 480 APs that provide continuous coverage over 2.6 million square feet.

Intel's WLAN currently supports about 80,000 employees worldwide, with more than 32,000 individual clients connecting simultaneously every day. Employees appreciate how easy and convenient it is to connect to the Intel network through the WLAN.

Although WLANs are an excellent productivity tool, they present several unique technical management challenges compared to LANs:

- Intel IT must support multiple WLAN generations, architectures, and suppliers.
- As WLAN clients move, they must be able to seamlessly connect on different floors and in different buildings and Intel locations.
- WLAN connectivity is dependent on user authentication with our Remote Authentication Dial-In User Service (RADIUS) system and corporate directory services, which adds a layer of complexity.
- Disturbances in radio signal propagation cannot be easily seen or measured, but instantly affect users. Calls to the Service Desk are often the first indication that a problem exists.
- We cannot track WLAN clients by the port to which they connect, as their connection points change as they roam. Therefore, the traditional method of LAN management—managing ports—is not sufficient for WLANs.

WLANs also pose some human-factor management issues. First, Intel IT has a relatively small number of people with WLAN expertise; however, this small group must manage globally deployed devices. Also, we have traditionally monitored WLANs by region, with each site managing its own WLAN—which can lead to non-standard configurations and an unreliable user experience. Finally, our traditional approach to configuration and maintenance, which involves updating or configuring each device individually, is labor-intensive and prone to user errors.

We needed a new approach to WLAN management that enabled us to efficiently deal with the technical challenges while making the best use of our WLAN engineering resources.

SOLUTION

Intel IT has implemented a distributed wireless infrastructure that uses multiple designs and suppliers. To support this infrastructure, we developed a new philosophy focused on managing the WLAN as a service, not as a collection of disparate components. Our WLAN management system is the first wholly centralized managed service within our organization.

Because WLAN expertise is a highly specialized skill, building a central monitoring and management structure makes the best use of our WLAN resources while also cutting support costs. Our WLAN engineers can quickly view deployed WLAN devices and specific details on individual users worldwide.

Implementing a Central WLAN Management System

Our central WLAN management system uses a main console and management server clusters to monitor and control our global WLAN, as shown in Figure 1.

Central access to the WLAN management Web interface allows valuable WLAN expertise to be applied across the entire network. Because the WLAN depends on many technologies and components, it is critical to give support engineers an end-to-end view of all functionality.

INDEPENDENT OF SUPPLIERS, EQUIPMENT MODELS, AND ARCHITECTURES

Our central WLAN management system can accommodate multiple connectivity standards, suppliers, generations of equipment, and architectures, as shown in Figure 2.

Because our central WLAN management system is supplier-independent, if we determine that a new supplier's WLAN equipment offers advantages, we can add that new equipment with minimal retraining of those responsible for monitoring or troubleshooting the WLAN. The management view of the network remains unchanged for the support engineers.

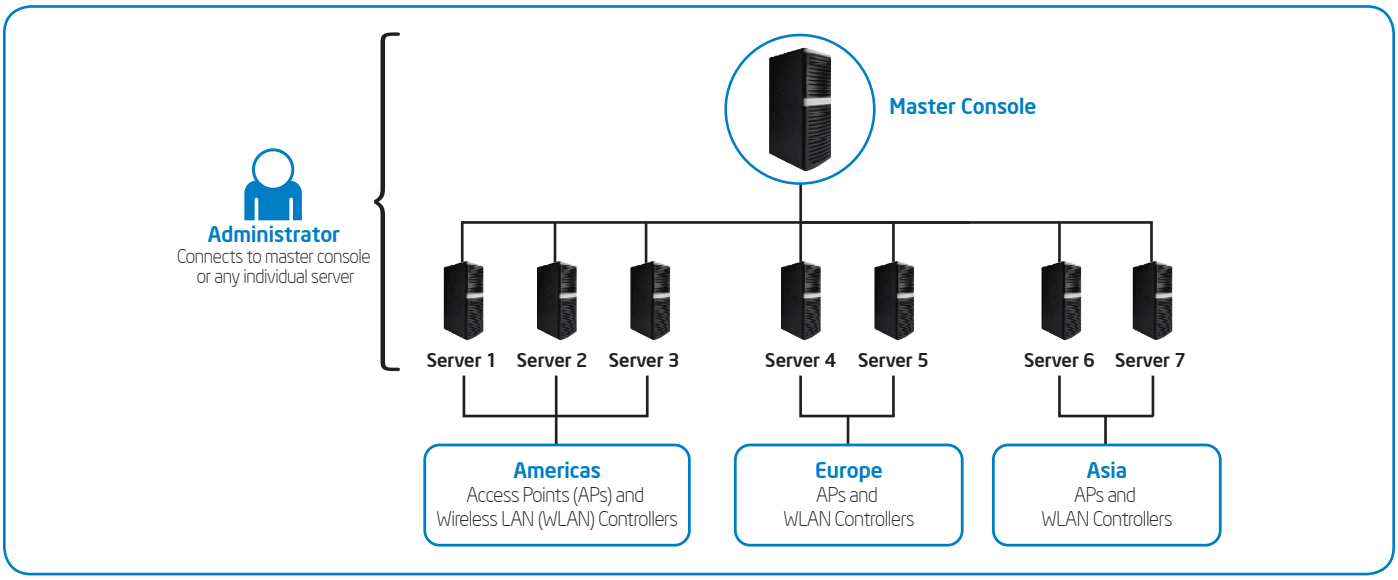

Figure 1. All network functions are routed through management server clusters to the central wireless LAN (WLAN) console.

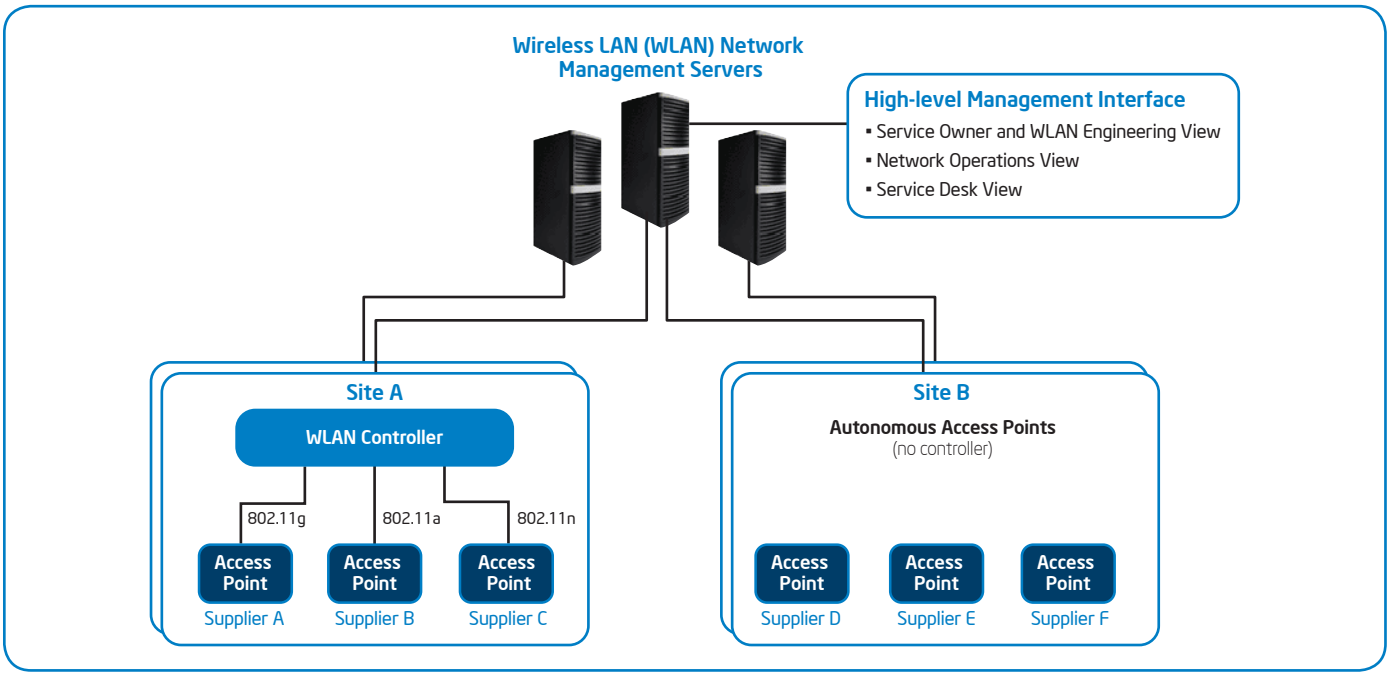

Figure 2. Our system supports multiple suppliers, architectures, and connectivity standards. All network activity is routed to a single set of management servers.

DEVICE CONNECTION

Each WLAN device on the network is connected to the network manager using Simple Network Management Protocol (SNMP), Telnet, and/or Secure Shell (SSH), and sends status updates through SNMP trap alerts. We use SNMP to retrieve most software and configuration information, although some information requires using SSH and a command-line interface (CLI). Software upgrades and configuration changes use the same combination of CLI and SNMP.

SERVER REQUIREMENTS

WLAN management software is processor- and RAM-intensive, so we refreshed our management servers to use Intel® Xeon® processor X5570. Taking advantage of this processor's built-in intelligent performance and power management features enables us to regulate power consumption and minimize the number of servers needed to run the management software.

Managing a Global Network

The WLAN is Intel IT's only centrally managed global network service. Other services have local management systems or none at all. Additionally, the WLAN is the only service that provides an instant inventory, with all components, switches, and APs enumerated on one screen and easily available for detailed reports.

Role-based administration of the central WLAN manager allows for multiple views of the WLAN:

- Global Service Desk engineers
- Regional network engineers, who provide installation, day-to-day support, and alert consolidation
- High-level users, including the WLAN management group, WLAN engineering, and the service owner

The central WLAN management system organizes geographic sites into folders. It is possible to set permissions so that some regional network engineers can make changes to only certain sites, although they can see all sites.

If the Service Desk's first-level support team cannot resolve a problem they feel resides in the WLAN infrastructure, the team escalates a trouble ticket to the network operations group—a team of individuals who are the point people for day-to-day WLAN installations, management, and troubleshooting. If network operations needs assistance, they in turn escalate to the service owner, who is also responsible for training, planning, and new deployments. The WLAN engineering team is the final step within Intel IT; however both the service owner and WLAN engineering can open tickets with WLAN suppliers if necessary.

On average, from the almost 200 trouble tickets that the Service Desk opens annually, only 3 to 5 percent are escalated to the service owner and WLAN engineering. Out of this 3 to 5 percent, we further escalate about 5 percent of tickets to suppliers for additional support.

SERVICE DESK

From the global scope and comprehensive network view that the central WLAN management system provides, Service Desk engineers can determine whether their current ticket is an isolated instance or part of a wider pattern.

Additionally, the system's global search engine and graphical data representation help engineers identify a user's location, media access control (MAC) address, client machine information, current AP and roaming history, and other relevant information. The ability to capture this information quickly, with a minimum of user interaction, has improved the ability of Service Desk engineers to troubleshoot issues. Previously, identifying a user's WLAN controller and AP could take 15 minutes or more when the support engineers had to connect to WLAN devices directly, but with the central WLAN management system it takes just a minute or two.

Support engineers can also use the WLAN management tools to isolate issues for more accurate escalation. For example, a problem with authentication may involve the client, a configuration issue, RADIUS, or even the WAN. Support engineers can now diagnose the problem's subsystem and subsequently escalate the problem to the correct specialist support group.

The system also helps first- and second-level support engineers close the greatest number of tickets possible, rather than escalate. Tool usage data indicates that support engineers, as well as the service owner and WLAN engineering team involved in escalations, now depend on the WLAN central management to view user connection details and historical associations when dealing with a new problem—a trend that does not occur for all Intel IT management consoles.

We plan to enhance the interface to the trouble ticket system by providing a quick method to cut and paste information for use in trouble tickets.

Solving connectivity issues

The most common WLAN-related Service Desk calls at Intel are related to connectivity issues. The central WLAN management system is especially helpful in diagnosing WLAN connectivity problems, as it provides a view of all supporting systems. Figure 3 shows an example of a diagnostic screen after a user reported poor performance. The root cause was initially unclear, and neither the client software nor the WLAN controllers were able to provide any data pointers to help with troubleshooting.

However, the WLAN central management system showed the client AP association history and the low signal levels at which the user was connecting. The support engineer was then able to recommend that the radio frequency (RF) power levels of the existing APs needed to be increased and that 802.11a radios needed to be added to the existing APs due to the excessive interference in the 2.4 GHz band from APs in surrounding buildings.

Managing rogue access points

Rogue APs—users turning on unauthorized APs within an Intel building or plugging into an Ethernet wall jack—are also a significant problem.

Most enterprise WLAN equipment can be set up to detect rogue APs, but several issues make removing these information security threats time-consuming. First, many false alerts are generated in cases where smaller Intel offices are adjacent to other buildings in which tenants run their own WLANs. Also, several Intel development and quality-assurance groups use Wi-Fi in the course of their daily work but outside Intel IT's control.

Our solution is to apply a set of tests to determine whether the unknown AP is indeed connected to an Intel LAN and to filter out authorized equipment. To assist in this process, we use an Intel intranet site that allows lab Wi-Fi users to register a cohabitation agreement, allowing them to use certain RF channels and service set identifiers (SSIDs). Local support engineers validate cohabitation agreements, which are valid for 12 months, and the appropriate information is electronically exported to the central WLAN management system.

Once the rogue AP list has been limited to suspicious devices, the central WLAN management system applies simple filtering rules, such as signal strength levels, and identifies the source of transmissions on a building floor plan, which is then e-mailed to a local support engineer, who must find the rogue AP. The accurate location on a floor plan of each rogue AP helps the local person, who may not be an IT engineer and therefore may not readily recognize Wi-Fi devices, find the offending APs.

Managing alerts

Because the WLAN is dependent on so many subsystems, such as RADIUS, Dynamic Host Configuration Protocol (DHCP), and our Domain Name System (DNS), it is often difficult to determine the root cause of problems. In many cases, a single problem causes multiple alerts that obscure the original outage, and false alerts are also a problem. The central WLAN management screen consolidates related alerts so they can be double-checked for accuracy.

Diagnostics for **00:21:5C:85:BD:0B**

Possible Issues

Issue	Ideal	Actual
Low signal quality:	>=20	27
Excessive roaming in last two hours:	<=10 roams	0
High user bandwidth:	<=50% of radio capacity	318 kbps (0.13%)
Unauthenticated user:	Authenticated	EAP
High user load on AP/radio:	<=15	14
High AP/radio bandwidth:	<=75% of radio capacity	1670 kbps (0.67%)
802.11b users associated to 802.11bg radio:	None	**1**
802.11bg or 802.11a users associated to 802.11n radio:	None	**1**
High FCS error rate:	<=100	0

Diagnostic Summary

	Current	Last Hour	Last 2 Hours	Last 4 Hours
User Bandwidth	318 kbps (0.13%)	318 kbps (0.13%)	318 kbps (0.13%)	318 kbps (0.13%)
Radio Bandwidth	1670 kbps (0.67%)	1722 kbps (0.69%)	2533 kbps (1.02%)	3314 kbps (1.34%)
AP Bandwidth	1672 kbps (0.34%)	1724 kbps (0.35%)	2535 kbps (0.51%)	3315 kbps (0.67%)
Radio User Count	6	7	7	8
AP User Count	14	14	14	14
Signal Quality	**27**	36	**38**	51

Current User Counts

	User Count on AP	User Count on Radio
802.11g	6	0
802.11n (5 GHz)	5	5
802.11a	1	1
802.11b	1	0
Total	13	6

AP Information

Name:	AL1
Uptime:	10 days 21 hrs 20 mins
Location:	-
Type:	Model X
Controller IP Address:	XX.X.X.XXX

Figure 3. The wireless LAN (WLAN) management system diagostics screen enables Service Desk engineers to quickly pinpoint the cause of connectivity problems.

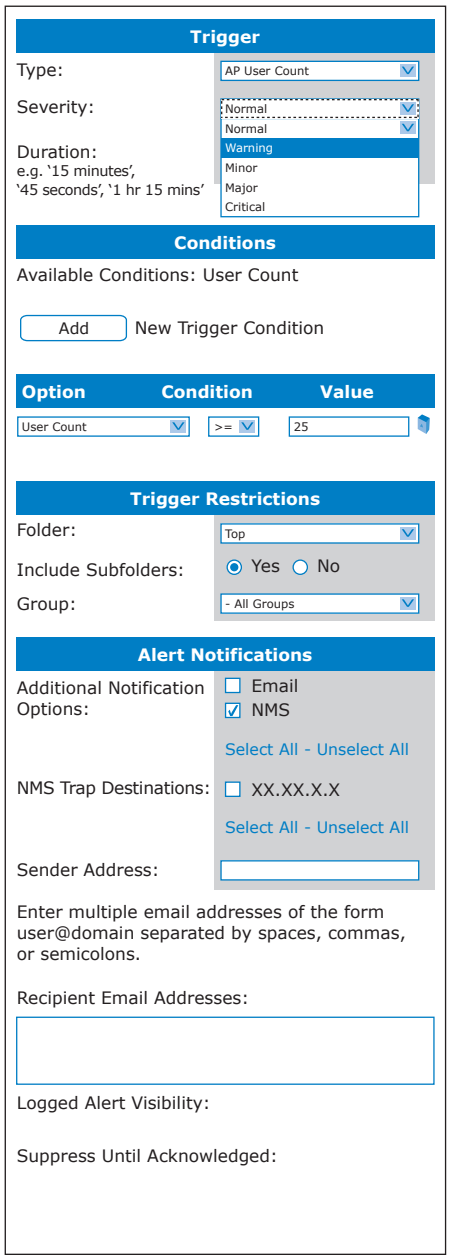

Figure 4. Specific situations trigger the wireless LAN (WLAN) management system to generate automatic alerts, supporting proactive problem management.

Alerts are escalated from the central WLAN management system to the Service Desk central event console—the point at which LAN, WAN, RADIUS, DHCP, WLAN, and other alerts are consolidated and parsed.

WLAN alerts are crucial to enabling the WLAN support engineers to respond to WLAN issues before they affect users. For example, if too many users are connected to one AP, performance can degrade rapidly. To avoid this scenario, the central WLAN management system can send out an alert if more than 25 users connect to an AP, as shown in Figure 4. The network team can then evaluate AP coverage in that area and add an additional AP if needed. This proactive approach minimizes support calls and increases user confidence in the WLAN.

Another important type of alert relates to information and network security. Our central WLAN management system collects WLAN user information that is then stored in our configuration management database. If suspicious activity is detected on the network, operations can monitor the time and origin of connection. If the suspicious activity is related to a specific file, the user's historical record shows the amount of data downloaded, which can then be tied to the size of the suspicious file.

STANDARD SITE DESIGN AND CHANGE MANAGEMENT

A global management system is a requirement not just for our global WLAN support organization, but for revision and configuration control and global inventory management as well.

Limiting the number of standard designs

Our WLAN design was developed by the WLAN engineering group and is based on four evolving WLAN generations. Limiting the number of standard designs allows the engineering team to thoroughly test and understand each design prior to site installations. Troubleshooting is easier, too, because we have instituted a global set of configuration parameters.

Table 1 summarizes our current WLAN design. Although we are transitioning to the 802.11n standard, we manage the current three designs simultaneously because it would be cost prohibitive to upgrade all sites whenever a new design is introduced. Our central WLAN management system enables us to efficiently and successfully manage several designs because it provides a consolidated view of the entire WLAN, including all equipment and software.

Centralizing revision control

Managing three designs at the same time can cause difficulties, because each design is subject to its own operational bugs, upgrade requirements, and hardware revisions. Centralizing revision control allows at-a-glance verification of the many different components underlying each configuration model, whether we are installing a new WLAN site or making revisions to an existing site.

Table 1. Standard Intel IT Wireless LAN (WLAN) Designs

Generation	Variations
2	▪ Supplier A's autonomous access point (AP) model using 802.11g with 802.1x, with no WLAN controller
3	▪ Supplier A's AP model using 802.11a/g with WLAN controller ▪ Supplier B's AP model using 802.11a/g with WLAN controller
4	▪ Supplier A's AP model using 802.11a/g/n with WLAN controller

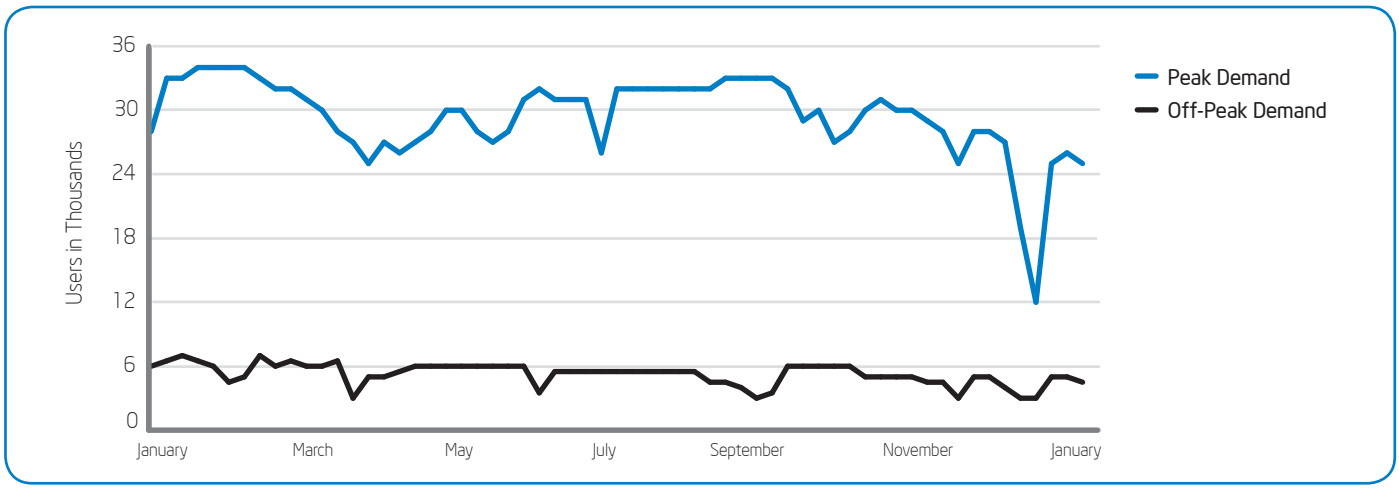

Figure 5. Usage reports can highlight where the wireless LAN (WLAN) is congested. For illustrative purposes only.

- **New WLAN sites.** The final step in commissioning a new WLAN site is to add the devices to the central WLAN management system. Registration with and verification by the central WLAN management system allows the WLAN service owner to check the configuration against the standardized configuration and design. The system flags discrepancies for correction. Registration is the critical difference between autonomous and central control, and forces compliance checks that might otherwise be circumvented.
- **Existing WLAN sites.** We manage software revisions centrally, using the network manager's subsystem to schedule and update each site and deliver reports showing snapshots of all sites and current revisions. This has allowed revision management to become a routine, controlled process rather than a highly cumbersome engineer-intensive and error-prone exercise.

Prior to implementing the central WLAN management system, even a minor configuration update could take five minutes per AP. But our central WLAN configuration reduced this to only five minutes per building. Replicated over 150 sites, this represents a considerable potential for savings.

Centralized WLAN management has also enabled us to implement standard templates for operational configuration. Rather than setting parameters locally at the AP, the template resides on the central WLAN management server and all changes are programmed and enforced network-wide. The system's auto-repair application runs overnight, checking that site configurations have not been changed locally. This synchronizes sites with the templates and discourages local reconfiguration; changes not made through the central management system are automatically reversed.

TRAINING SUPPORT ENGINEERS

We offer in-house training to support engineers and also encourage them to take training courses from suppliers.

We developed a two-hour, self-paced, Web-based course for people who use the WLAN management system infrequently and don't need comprehensive information. This course is targeted for management station views of the network rather than the intricacies of each WLAN controller or AP type. The course uses an intuitive user interface and a simple conceptual management model independent of the underlying hardware generation.

Engineers who spend more time trouble-shooting WLAN issues take the WLAN supplier's, installer's, or maintainer's courses, as appropriate. They also receive a four-hour, instructor-led course on the central WLAN management system.

Both training courses specifically address two issues that can be problematic:

- **Timestamps.** To provide global support, all timestamps must be consistent. The system sets all timestamps to Greenwich Mean Time (GMT), which can be confusing to local support teams at first.
- **Mindset.** Engineers need to become accustomed to using a remote network manager to obtain information from a local WLAN controller

Providing Reports and Statistics

The central WLAN management system collects and summarizes WLAN usage statistics, allowing support engineers to easily prepare reports on bandwidth utilization, simultaneous users, and usage trends. One trend is shown in Figure 5.

WLAN statistics are also useful to other groups at Intel:

- Several teams have asked for wireless adoption trends, turning to Intel IT for indicative statistics.
- Site inventory reports are used frequently, providing the number of APs or controllers of a particular type or model.
- When planning upgrade cycles, the service owner can determine how many sites are running each WLAN model, allowing each site to make informed financial decisions and use their resources effectively.
- Inventory reports provide a list of equipment in service, helping to identify equipment that has been replaced and can be removed from the appropriate supplier maintenance contract.

Results

Our central WLAN management system has the potential to significantly reduce the time and effort we spend on WLAN configuration updates—from five minutes per AP previously to five minutes per building now. We can realize substantial savings by replicating this efficiency across 150 sites.

Other benefits of the central WLAN management system include:

- Supplier independence—we can add new equipment with minimal retraining of engineers.
- Ability to push equipment configuration changes globally.
- Ability to track WLAN assets by serial numbers and locations, which helps maintain accurate inventory data.
- Improved network security with easy access to user connection data.
- Ability to quickly troubleshoot WLAN issues, regardless of where they occur geographically.
- Ability to proactively resolve WLAN issues before they affect WLAN users.
- Ability to obtain a holistic view of overall WLAN health.

CONCLUSION

From just a few access points in 2001, Intel's WLAN has grown to support about 80,000 mobile employees at 150 sites worldwide. We manage the WLAN as an integrated service characterized by a set of global tools, centralized monitoring and reporting, and centralized control of the WLAN, which provides all stakeholders with a common view of the components of the WLAN service and the network

To support this service model, we rigorously centralized management of all WLAN installations and adopted enforceable global templates for configuration models. The system's simple user interface allows non-specialists to monitor and diagnose simple WLAN problems without learning supplier- and equipment-specific commands.

The combination of central IT engineering expertise, a set of global guidelines, and a centralized management platform allows us to deliver a highly available service with minimal support staff.

ACRONYMS

AP	access point
CLI	command-line interface
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
GMT	Greenwich Mean Time
MAC	media access control
RADIUS	Remote Authentication Dial-In User Service
RF	radio frequency
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSID	Service Set Identifier
WLAN	wireless LAN

Printed in USA
0410/JLG/KC/PDF

Please Recycle
322971-001US