White Paper
November 2014

IT@Intel
Wireless Infrastructure Implementation: Best Practices

Our exclusive use of a wireless infrastructure helps us improve employee mobility, job satisfaction, and productivity—as well as deliver LAN access in new construction faster and at lower cost.

Omri Barkay
WLAN Engineer, Intel IT

Avigail Garti
Network Engineer, Intel IT

Liran Klein
Network Specialist, Intel IT

Tim Verrall
Senior Principal Engineer, Intel IT

Executive Overview

Intel IT is enabling business transformation on Intel campuses around the world by standardizing on Wi-Fi* for LAN access. Our exclusive use of a wireless infrastructure helps to improve employee mobility, job satisfaction, and productivity—as well as deliver LAN access in new construction faster and at lower cost.

Our transition to a wireless infrastructure began with wireless LAN (WLAN) to provide on-premises mobility to employees with mobile business PCs. Over time, this infrastructure's importance increased as more wireless devices entered the enterprise, including employee-owned devices, smartphones, PC-based softphones, and wireless displays.

Today at Intel, the wireless office is a reality. In reaching this goal, Intel IT developed best practices for setting up a robust, secure wireless infrastructure. These practices improve quality of service (QoS) for voice and video applications and enable new services, such as cellular voice over Wi-Fi and location-based services.

Several benefits come from following these practices:

- Easier adoption of innovative, time-saving mobile services that enhance employee productivity
- Consistent wireless performance and user experiences, including enhanced telephony and video performance over Wi-Fi
- Improved mobility and less expensive office changes for employees throughout each campus and across Intel sites
- Better support of devices dependent on wireless connectivity for LAN and external displays
- Reduced equipment costs since we no longer issue desk phones and do not require as many network backend switch ports

Contents

Acronyms

AP	access point
BKM	best-known method
PoC	proof of concept
QoS	quality of service
RADIUS	Remote Authentication Dial-In User Service
RF	radio frequency
VoIP	voice over IP
WiDi	wireless display
WLAN	wireless local area network

Moving forward, we will continue advancing our WLAN's capabilities and services using these best practices. A future addition to these practices will be best-known methods (BKMs) for enhancing the ability to dynamically adjust the level of network authorization when connections, devices, or user identities change.

Background

Intel IT operates a worldwide computing environment that supports over 100,000 Intel employees. Many employees collaborate on teams across countries, time zones, and campuses. Employees connect to IT services through more than 160,000 devices. While the majority of these devices are wireless mobile business PCs, more than 70,000—nearly half—are wireless handheld devices. Visitor wireless handheld devices can add up to another 20,000.

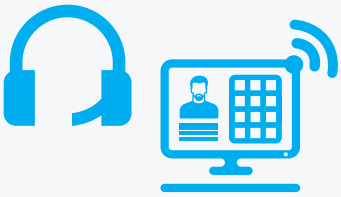
Recognizing the business transformation potential of wireless technologies, Intel IT has experimented and deployed wireless technologies over the last 10 years for employee LAN, Internet, and telecommunications services. Today, on our wireless-only campuses, we make it easier to adopt new wireless form factors, deliver innovative time-saving mobile services, and adapt existing space to new uses. By implementing a robust wireless infrastructure and making it our networking standard rather than a supplementary network, we help ensure the ability to handle high demand and deliver high performance. We also provide a solid foundation for adding transformative wireless applications, such as wireless display sharing for conference rooms.

Our experiences demonstrate that enabling mobile devices with a reliable, scalable, and robust wireless LAN (WLAN) and encouraging employees to carry wireless mobile business PCs on and off premises delivers more than just convenience; it also creates savings. Telecommuting and other alternative workplace options reduce office space requirements. Wireless voice over IP (VoIP)-based softphones reduce the need for a costly traditional telecommunications infrastructure. Mobile business PCs and other mobile computing platforms use less energy than desktop PCs. Supporting 15–20 employees with a single access point (AP) is less expensive than cabling each cubicle and providing one or two dedicated wired ports on a LAN switch per employee.

Wireless infrastructure delivers many other benefits:

- A more flexible work style that promotes collaboration across global teams and greater productivity, according to Intel IT user surveys and observational studies
- Improved business continuity as employees take work computers home and have these computers with them when natural disasters or other events prevent them from coming into the office
- Easier, faster, less expensive employee office changes within a campus or to another campus
- Simpler conference room display connections as wireless connections minimize the need to support such wired display ports as HDMI, DVI, and VGA
- Easier future adoption of innovative mobile technologies, such as GPS and near-field communications (NFC) that will enable everything from location-based services to wireless "smart" payments

Relying completely on WLAN to connect employees and implement new technologies can present some challenges. Enterprise adoption requires a wireless infrastructure that can deliver the performance (connection speed, bandwidth, and quality of service [QoS]), security, manageability, and redundancy necessary for reliable day-in, day-out business use. The Infrastructure must be versatile enough to provide wireless services for different classes of mobile devices, including enterprise mobile business PCs with softphones, employee-owned devices (including cellular-based smartphones and tablets), and visitors' mobile devices. The infrastructure must also provide solutions for a wide range of use models, such as connecting to display devices in conference rooms and accommodating thin-form-factor mobile devices that lack ports but need to connect to larger screens and other peripherals.



What Is a Softphone?

A softphone is a software program for making telephone calls over the Internet using a computer rather than a wired desk phone connected to a telecommunications network. Supporting voice over wireless infrastructure unifies communications on a single device, helping to minimize the cost of wired desk phones and allowing employees to use and take their "office" phones anywhere on campus.

Most softphones operate like a traditional telephone, sometimes appearing as an image of a phone with a display panel and buttons with which a user can interact. Intel employees use a headset with a built-in microphone that is connected to the sound port on the computer. A typical softphone has all standard telephony features (such as hold, transfer, conference) and often additional features typical of online messaging, such as user-status indication, video, and wide-band audio.

Best Practices

To set up a successful enterprise WLAN, Intel IT has developed a set of best practices. By following these practices, we can quickly and efficiently replace wired LAN access services in existing workspaces and implement WLAN in new buildings. This provides employees with secure, reliable connections for current and future mobile devices, technologies, and applications. In this section, we discuss our best practices and best-known methods (BKMs) for architecting our wireless infrastructure and providing a robust, forward-looking design that is adaptable to a wide range of users, manageable, and secure.

Provide employees with secure, reliable connections for current and future mobile devices, technologies, and applications.

5 best practices to planning and building a robust WLAN

1. Start incrementally
2. Design for performance
3. Employ redundancy
4. Perform WLAN site surveys
5. Enable QoS for voice and video

Best Practice 1: Plan and Build a Robust, Forward-Looking WLAN

Wireless technologies are more recent than wired infrastructure and continue to evolve. In planning and developing a reliable enterprise WLAN, it is important to develop a robust wireless infrastructure that can easily adopt new and updated technologies and handle continued growth in Wi-Fi* services consumption. We focus on performance, connection speed, bandwidth, redundancy, and QoS.

BKM 1: Start Incrementally with Proofs of Concept (PoCs), Staged Deployments, and Standardized Components

Before introducing a new wireless technology or service, we devise and perform a PoC. For our initial WLAN, we performed a PoC in 2007 to determine whether a WLAN could serve as our primary network. Since then, we have used PoCs to test new services, such as softphones, as well as new equipment and technologies to improve performance.

If a PoC is successful, we stage a pilot installation on a single floor, building, or campus and make any necessary adjustments before deploying a technology across the enterprise. Our trial stage includes training support staff, communicating with users, and defining detailed quality indicators to show whether we met our target.

Standardization on proven components is essential to our success in staged deployments. While we architect different setups depending on the size of the deployment, within each setup we use the same APs, WLAN controllers, firmware, software, and other components. This approach allows us to engineer a setup once, copy exactly at multiple locations, and maintain consistency in the services we provide.

Some elements standardize more easily than others. For example, mobile devices use several operating systems (OSs). Rather than dictate a single OS or version of OS, we design our WLAN to handle any OS that supports industry-standard Wi-Fi, QoS, common drivers, and the ability to push policies.

BKM 2: Design for Performance

To ensure excellent performance, we use 802.11n throughout our WLAN. This version of 802.11 employs two data channels simultaneously to deliver faster data transfer speeds and better video and multicast streaming performance. It also provides the latest security measures and experiences less interference with other wireless devices.

To achieve maximum performance, we set all devices to use the higher frequency 5 GHz band because it delivers more bandwidth and many more nonoverlapping channels for less interference and greater cumulative bandwidth (total data transferred over the total transfer period). We also space our APs approximately 45 feet apart. This decision was based on

tests showing that APs spaced 60 feet apart provided inferior performance with location-based services, VoIP, and other services. We also found that smaller devices, which generally use smaller antennas, benefit from greater AP density. In addition, real-time services, such as VoIP, require dense AP deployments to deliver a strong signal (-67 dBm or better).

For performance, we favor "thin" APs controlled by a WLAN controller rather than "fat" APs. Thin APs rely on a WLAN controller for centralized management and security while fat APs include everything needed to handle wireless clients. In large office settings, the combination of thin APs and WLAN controllers offers several performance advantages:

- The AP manages timing-dependent operations (beacons, probe response, buffering, and radio monitoring) locally to reduce latency.
- The WLAN controller reduces the complexity of the AP by managing more complex, less time-dependent operations (association, 802.11 authentication, 802.1X processing, and bridging).
- With WLAN controllers acting as a central point, receiving information from multiple APs and concentrating radio frequency (RF) allocation, APs in different environments do not compete for the same RF channels. Providing centralized monitoring at a single location, the WLAN controller can automatically place neighboring APs on separate channels and allocate the proper power level to each AP for best roaming results and the least co-channel interference.

BKM 3: Employ Redundancy to Ensure Reliability, Availability, and Coverage

For better coverage and more reliable performance, we use a dual-redundant infrastructure that includes two clouds, two WLAN controllers per building, and two APs to cover every physical point in a building (Figure 1). This infrastructure gives us more APs per location and fewer users per AP. It also provides greater reliability and availability since there is no single point of failure. If any infrastructure component fails, any connecting wireless device will automatically roam to a neighboring AP, minimizing interruption to the user.

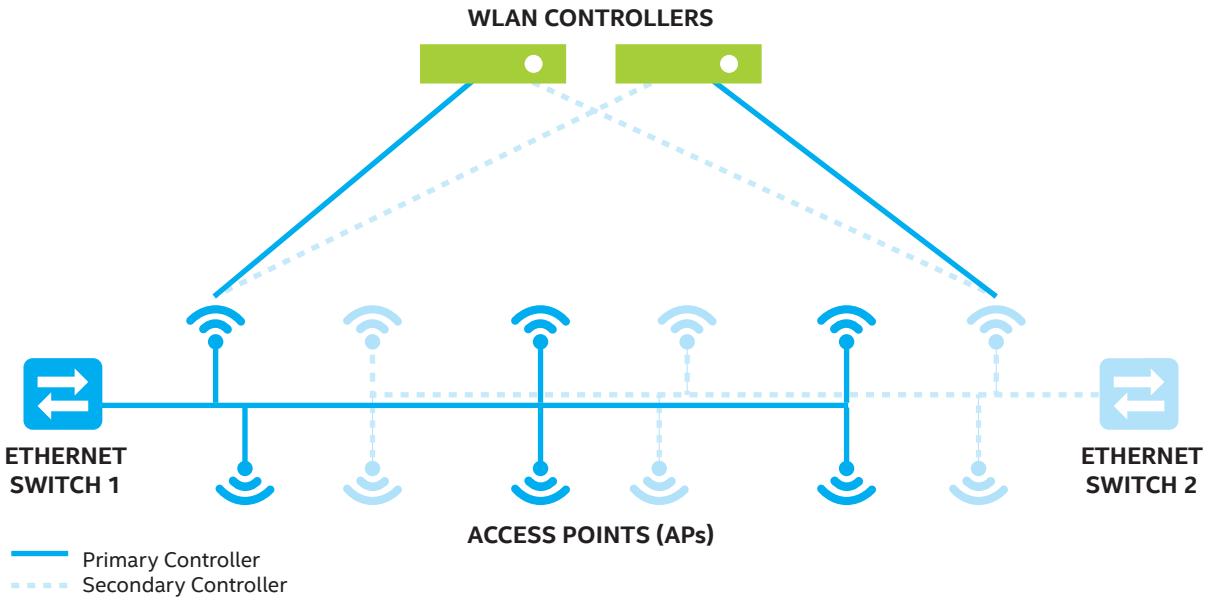


Figure 1. Intel IT uses two controllers per building and covers each physical location with two access points (APs) to help ensure redundancy.

BKM 4: Perform WLAN Site Surveys and Verify Coverage in the Field

To adapt our solution to different types and sizes of buildings, we use a third-party automated WLAN planning tool. This tool helps us meet the following goals and criteria:

- Enable a 15–20 percent AP overlap
- Locate APs for redundancy and dynamic power allocation
- Serve 15–20 users per AP
- Ensure small cells for VoIP service
- Provide excellent coverage of conference rooms and shared areas separate from employee office APs

After a floor or building is connected, we verify coverage in the field. We test each grid separately. Based on the results, we install additional APs where needed to meet our coverage and service goals. We also periodically physically recheck AP locations, correcting inaccuracies in our maps, and moving APs as needed to improve performance.

BKM 5: Enable QoS for Voice and Video

Our first PoC trial of softphones over our wireless infrastructure revealed quality issues for VoIP due to latency. As the technology matured, we experimented to improve performance. We found that through frame aggregation, 802.11n provided more throughput, but this aggregation degraded call quality.

ZERO

Number of traditional desk phones we now issue.

To solve this problem, we adjusted the media access control (MAC) layer, aggregating frames only for non-real-time data and disabling aggregation to prioritize latency-sensitive voice traffic. Using IP header marking to identify the voice traffic packets and classify them to low-latency queues throughout the infrastructure, we provided a “fast lane” for voice traffic that enabled more consistent performance across clients and networks. We also increased AP density by about 25 percent (from 60 feet to 45 feet) to create smaller coverage cells and decrease the number of users sharing resources.

After we made these improvements, our PoC provided positive results. We are now 12 months into our latest round of improvements and have stopped issuing traditional desk phones.

In parallel, we made additional MAC and IP layer changes to prioritize video traffic. These changes provided the necessary QoS improvements to ensure good streaming video and multicast performance. Unlike unicast traffic, multicast performance suffers over WLANs because of the lack of error correction in the WLAN MAC layer. To enable multicast traffic, we convert multicast to unicast over the WLAN, marking the traffic and ensuring that it is handled in a separate fast lane after the voice packets.

Best Practice 2: Use Centralized Management

Before the introduction of WLAN controllers, overall WLAN management proved difficult since each AP operated as a separate node, autonomously configured with channel and power settings from a static RF plan. Deploying WLAN controllers enabled us to bring enterprise-quality centralized management to wireless infrastructure.

BKM 1: Base Wireless Infrastructure on WLAN Controllers

WLAN controllers allow administrators to create AP groups for geographical management and security as well as to implement special features. If a change needs to be made to the wireless configuration of an entire building—such as adding an SSID (service set identifier)—the administrator can simply apply that change to the group through the WLAN controller.

WLAN controllers are also valuable for implementing features not available to a standard decentralized wireless network, such as enabling centralized RF management. In this case, a controller that detects radio interference at one AP could maintain local performance by automatically boosting the power of nearby APs.

Benefits of centralized management through WLAN controllers

1. Enhance security
2. Check logs
3. Set multiple security settings
4. Easily detect rogue APs
5. Lower TCO and management costs

Implementing centralized management through WLAN controllers also enhances security. WLAN controllers can enable administrators to check logs, configure security settings, and implement group policies for wireless users all from one location. WLAN controllers also make it easier to detect rogue APs and determine whether the AP is a trusted device.

Centralized management through WLAN controllers can help lower total cost of ownership. While thin APs may initially cost more than fat APs, the ability to centrally configure and administer the APs through the WLAN controller rather than individually can help reduce management costs.

BKM 2: Follow the ISO FCAPS Model

To monitor and manage our wireless infrastructure, we use the FCAPS (fault, configuration, accounting, performance, and security) network management model:

- **Fault.** For IT notifications of errors (faults), we use a management solution that parses, classifies, and forwards Simple Network Management Protocol (SNMP) traps and event messages based on severity.
- **Configuration.** To reduce configuration time and effort, we use a generic global configuration template supplemented with a local configuration template where necessary. For simple, global updates, we standardize as much as possible on a single firmware solution for APs across the enterprise.
- **Accounting/performance.** For network health, we monitor coverage, load, utilization, and uptime. Our troubleshooting capabilities include addressing single and multiple clients, depending on the extent of the issue.
- **Security.** To enhance security, we configure the system to identify and alert us to rogue devices using unauthorized networks.

Best Practice 3: Provide Services for Each Class of User

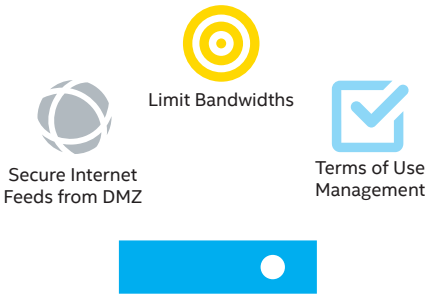
To serve an enterprise, wireless infrastructure must provide services geared for each class of user. These classes include employees using corporate-issued mobile business PCs and employee-owned devices, contractors, and visitors.

BKM 1: Set Up a Dedicated Enterprise WLAN for Employees

The wireless infrastructure described so far enables employees to use Wi-Fi to connect securely to the corporate network and the Internet anywhere on campus. A key part of this wireless infrastructure is the corporate-issued mobile business PC. We configure this PC with advanced security features and remote platform management and supplement these features with the granular trust model we use for enterprise security.[1]

BKM 2: Set Up a Separate WLAN for Internet/Intranet Access by Employee-Owned Devices

Employees want the flexibility to perform their jobs using the platforms, applications, online tools, and services they use on their consumer devices. To enable employee-owned devices in the enterprise, we use Internet feeds from our demilitarized zone—a subnet protected from the Internet by a firewall and separated from the intranet by a different set of firewalls. These feeds enable us to provide 2.4-GHz and 5-GHz Wi-Fi Internet access.



Benefits of using WLAN with Employee-Owned Devices

For security, we tunnel Internet traffic from campuses to demilitarized zones using generic routing encapsulation over WAN. To add another level of security and improve performance, we use a transparent proxy to filter and cache traffic. In places where we do not want employee-owned devices to consume more than a predetermined amount of bandwidth to or from the site, we also apply a bandwidth limitation.

For provisioning we use tools created for account management (password creation, reset, and deletion). We require employees to accept terms of use by filling out a web form. This process helps ensure that they understand their responsibilities and our privacy policy. We use a third-party application for device security, including a remote wipe feature for managed devices that are lost or stolen.

BKM 3: Employ Centralized Authentication, Authorization, and Accounting to Control Access from Corporate-Issued and Employee-Owned Devices

Employee WLAN connectivity is dependent on user authentication with our Remote Authentication Dial-In User Service (RADIUS) system and corporate directory services. RADIUS provides the following centralized services:

- Authentication (confirming that the user is indeed the user)
- Authorization (determining what the user is entitled to)
- Accounting (collecting records of connection usage)

[1] For more on this approach to information security and the way we implement it with managed PCs, see our white paper, "Granular Trust Model Improves Enterprise Security."

In some use cases, we permit only one account per device and use corporate domain accounts for our corporate-issued mobile business PCs and a separate account with more circumscribed privileges for employee-owned devices (Figure 2).

RADIUS supports many authentication protocols. Different protocols are used based on the requested connection, security level, purpose, and inherent support by the client device and network access device. For authentication, we use the 802.1X Extensible Authentication Protocol (EAP)—specifically EAP-PEAP-MSCHAPv2, EAP-TLS, and EAP-FAST.

BKM 4: Set Up a Separate Wi-Fi Network for Contractors and Visitors

Using an overlay network, Intel IT provides contractors and visitors with a separate wireless service outside our firewall, enabling them to access the Internet using their devices. VPN access is available to their home sites but not to the Intel intranet.[2]

BKM 5: Provide Cellular Over Wi-Fi Service for Employees

Nearly all Intel employees use cell phones (smartphone and traditional cell phones). Some use corporate-issued phones, some use personal phones, and some use both. Although still in the trial stage, we see two primary benefits for cellular over Wi-Fi services:

- Cellular over Wi-Fi enables all voice calls, texting, and data over Wi-Fi instead of expensive cellular services.
- Since cellular signals are typically weak inside large buildings, bringing cellular over Wi-Fi into the enterprise allows employees and visitors with specific phone types to use onsite Wi-Fi for more reliable voice reception and coverage. Data transmission is faster and more reliable as well.

For security, we implement two levels of trust: fully trusted and partially trusted/untrusted. Fully trusted smartphones, generally corporate-issued, have their own wireless network providing access to Intel corporate services and resources. Partially trusted and untrusted smartphones have access to Wi-Fi to connect to the Internet and limited or no access to corporate services and resources. We plan to increase the number of phone types we support.

BKM 6: Provide Separate Wi-Fi Network for Test and Lab Devices that Require Partial Network Access

For testing and development purposes, test and lab devices may need network access to intranet resources. In some cases, the devices may not be completely trusted, and their access must be limited to network areas of a single lab or secured network. We address these situations by using AAA RADIUS (described above) to determine which network to use for a specific lab device account. We send this information back to the WLAN controllers so that they can place the device on the appropriate secured network.

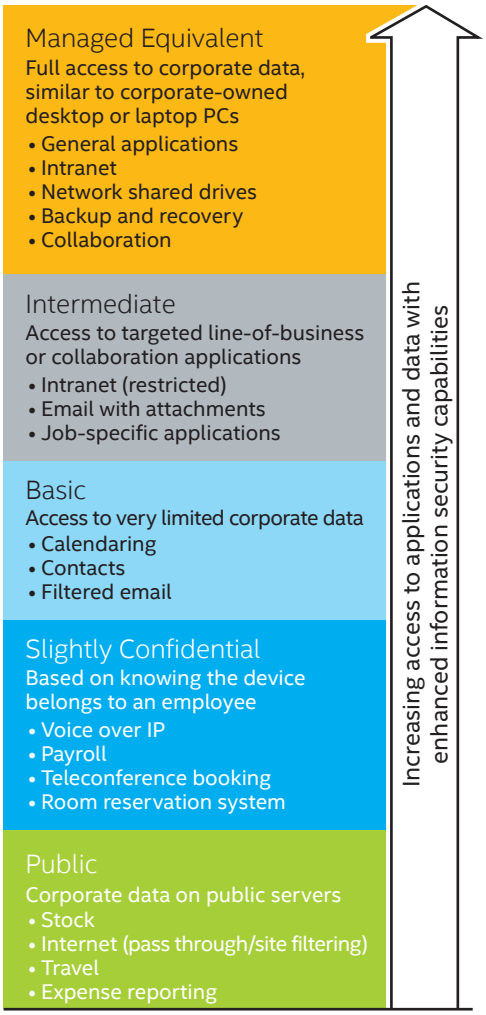


Figure 2. We control levels of access depending on user authentication and device type to protect corporate data while providing employees with flexibility in the mobile devices they use.

[2] Learn more in our white paper, "Evolving the Mobile Employee Hotspot for IT Consumerization."

Best Practice 4: Use Best-in-Class Security to Protect the WLAN and Intellectual Property

Security is a top concern for Intel to protect both intellectual property and employees' personal identifiable information. The 802.11n standard specifies Wi-Fi Protected Access 2 (WPA2) and allows for the data to be encrypted using the NIST Advanced Encryption Standard (AES). In addition to these industry-standard security measures, we also implement several of our own.

Security is a top concern for Intel to protect both intellectual property and employees' personal identifiable information.

BKM 1: Define and Control Access by User Type

In providing the right level of access for each user type (employee using a corporate-issued mobile business PC, employee using an employee-owned device, and visitor), we use different Wi-Fi networks and standards. Nearly all employees have corporate-issued devices to access the WLAN on-premises. Off-premises access of the corporate network is by remote access technologies such as VPN.

Employees electing to use an employee-owned device in addition to their corporate-issued mobile business PC can choose the WLAN-connection solution designed to fit their use case and work environment. Solutions range from basic browser connections for when the employee-owned device is a secondary device, to special Intel IT builds and virtualization solutions when the employee-owned device is used as a primary compute device. The solution selected provides the necessary security and other functionality for the level of access required by the employee for their device.[3]

Contractors and visitors connect to the Internet through an open Wi-Fi network outside our firewalls. Sponsors (for example, managers) create temporary self-expiring accounts for these groups, who must accept our terms of use and acceptable use policy. Access requires compliance with our policies, such as specific antivirus DAT files and patch levels.

BKM 2: Control Access to Data with Authentication and Role-Based Trust

We make all access to the WLAN as secure as possible. We use technologies such as federation, multifactor authentication, and certificate services to control access to data by performing role-based trust calculations and managing access privileges appropriately. Only the office WLAN provides full access to Intel network. Our lab WLAN provides partial access to allow testing of less secure devices without compromising the Intel network.

Our various WLANs include the following access controls:

- Machine authentication and domain identity to access the office WLAN
- User authentication and user domain identity for access to our design facilities
- User authentication and alternate credential store for access by employee-owned devices

[3] Learn more in our white paper, "Improving Security and Mobility for Personally Owned Devices."

- User authentication, user domain identity, and user alternate credential store for mobile WLAN access through a smartphone to the Wi-Fi network for data and calling
- Web portal user authentication for visitors who access our open network

BKM 3: Detect and Control Camera-Equipped Phones to Protect Against Intellectual Property Theft

Smartphones provide valuable mobility and productivity benefits, but their cameras present a potential security issue when carried by our employees into sensitive or restricted areas. In a successful PoC, we provided a solution to enable Intel's factory workers to bring smartphones with cameras into sensitive areas of our operations. This solution is now in use in our new factories.[4]

When a device is about to enter the factory environment, this solution performs three main functions:

- It detects whether the device is IT-managed (Figure 3).
- If the device is IT-managed, the solution deploys over-the-air technology to remotely disable features such as Wi-Fi connectivity and the camera.
- If the device is not IT-managed, the solution alerts the floor supervisor and provides the location of the device. (Sensors and triangulation pinpoint the exact location of unauthorized devices on the factory floor.) The supervisor can then enforce standard security policies and address the violation.

[4] Learn more in our white paper, "Enabling Smart Phones in Intel's Factory Environment."

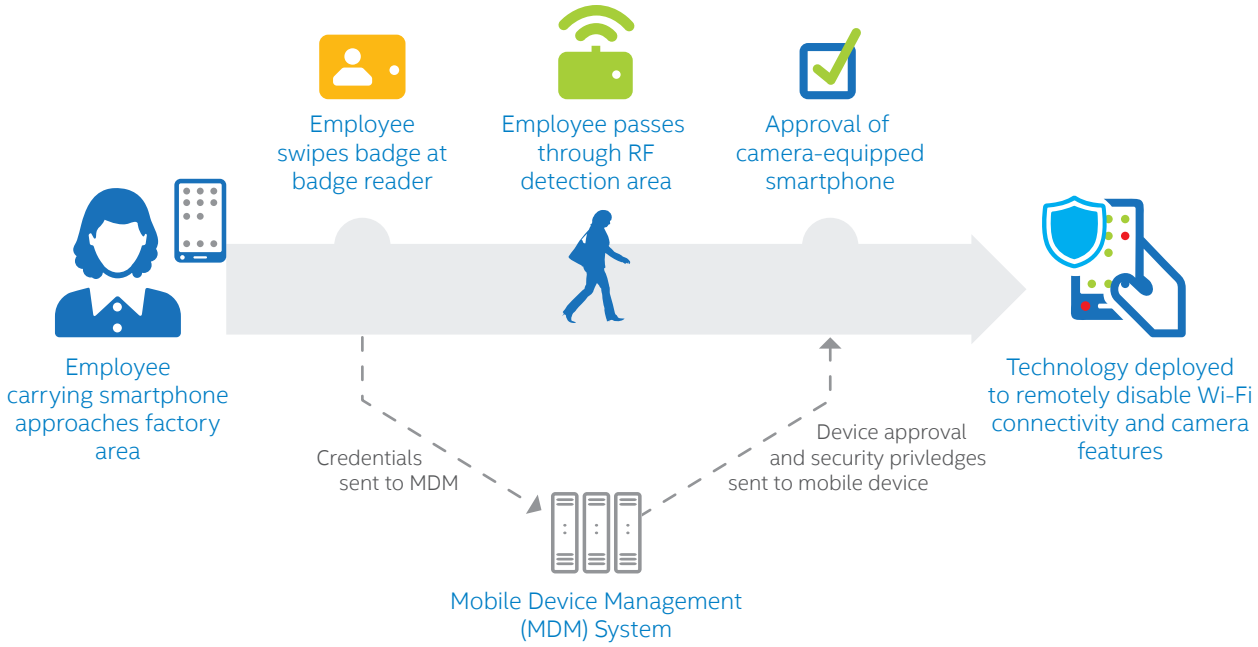


Figure 3. Our security policy for camera-equipped phones includes detection at the factory entrance to identify whether a device is managed by IT.

Best Practice 5: Make the Wireless Experience Satisfying and Rewarding

From an employee point of view, the greatest advantage and benefit of a wireless infrastructure is mobility. Intel IT also recognizes that an enterprise-wide WLAN can further satisfy and reward employees through new applications and services that enhance productivity, increase convenience, and even surmount office space limitations.

Time-Savings Benefits of Softphones

1. Device independence
2. No-dial phone conferences
3. Content and video link sharing
4. Dial by name
5. Call availability times

BKM 1: Provide Time-Saving Applications to Enhance Productivity

One time-saving technology Intel IT continues to experiment with is location-based services for wireless devices.[5] Using device location information gathered from the Wi-Fi network, location-based services help employees find cafeterias, available conference rooms, labs, PC service centers, printers, and other on-site services. We also provide interactive maps that allow employees to mark locations so they don't have search for the same conference room or other resource on future visits.

To provide extra value in addition to mobility to our softphones, we provide solutions that improve the user experience, save time, and reduce frustration. For phone conferences, users can click a link in their calendar application and automatically join a conference—no dialing required. To enhance collaboration, we aggregate features on the same interface that help enable successful sharing, such as being able to provide content links and video links.

To make it easier to call a fellow Intel employee, we make employee names the dialing mechanism. Instead of searching for person's number, employees can click on the name in their directory and the application calls the person's specified devices. Users can customize this solution, selecting which mobile devices ring when someone attempts to contact them from within the Intel WLAN as well as the days and times those devices accept calls.

BKM 2: Use Wireless Infrastructure to Provide Greater Convenience

To bring greater convenience to conference rooms and cubicles where employees need large screens, we are performing trials with Intel® Pro Wireless Display (Intel® Pro WiDi), a product of a collaboration between Intel IT and Intel's product development team. Trading a cable or swapping seats to display content frustrates users and wastes time. Intel Pro WiDi enables fast handoffs by providing a wireless receiver that establishes a peer-to-peer Wi-Fi Direct* connection using HDMI* and the Miracast* standard.

This approach allows content sharing while maintaining the existing Wi-Fi connection for accessing the WLAN. It also provides security by isolating the wireless content sharing to a peer-to-peer network (essentially a wireless personal area network, or WPAN), blocking bridging to the corporate WLAN.

[5] Learn more in our white paper, "Getting a Headstart on Location-based Services in the Enterprise."

Intel Pro WiDi offers other advantages as well. It enables sharing content on conference room screens from wireless devices that lack wired external display capabilities. It also eliminates the expense of cabling and switch equipment.[6]

BKM 3: Use Wireless Infrastructure to Overcome Space Limitations

Intel IT recently introduced the wireless "lab in a cube." This innovation reduces the need for expensive laboratory real estate in our design facilities by offering chip designers access to a virtual lab from a cubicle or anywhere on campus through a secure, wireless connection to the lab network.

Results

Through successful implementation of our best practices for enterprise-wide wireless infrastructure, Intel IT is realizing the long-sought business goal of the wireless office. We are also delivering consistent wireless performance and user experiences, including enhanced telephony and video performance.

Wireless infrastructure frees employees from their desks, enabling them to use their wireless computing devices—including their softphones—anywhere on campus. This infrastructure also enables us to better support a wide range of corporate-issued and thin-form factor employee-owned devices and innovative time-saving mobile services that enhance employee productivity.

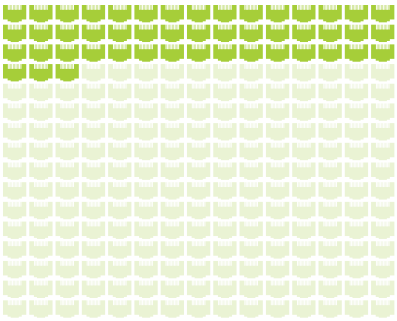
From an IT perspective, relying completely on wireless infrastructure frees us from having to install, manage, maintain, and secure two forms of employee LAN connectivity—wired and wireless. We can focus our efforts and investments exclusively on a wireless network.

Our WLAN and softphone strategy helps provide considerable cost savings over wired LAN and traditional wired telecommunications in the following ways:

- We can connect 15 users to a single AP instead of using 15 ports on a switch.
- We can service a floor with just 48 ports in a closet compared to requiring 250 ports in a closet for wired LAN services.
- Instead of spending money on desk phones and the accompanying switching hardware, we can include softphone capabilities in our mobile business PCs.

48

NUMBER OF WLAN PORTS NEEDED PER FLOOR



Using WLAN and softphones provides considerable cost savings over wired LAN services by reducing our port usage by 202 ports per floor.

[6] Learn more in our white paper, "Evaluating Intel® Pro Wireless Display for Enterprise Use."

Conclusion

Intel IT's best practices for wireless infrastructure enable us to quickly and securely bring new office space online, help Intel better use existing space, accommodate new wireless form factors, and deliver new services throughout Intel's global operations.

We want our WLAN to serve as the access network for any service or use case in the future. We plan to implement a differentiated network that will provide access only to areas that the specific connection requires, including the ability to adjust the level of network authorization dynamically when a connection, device, or user identity changes. By consistently implementing our best practices, Intel IT will be prepared to take advantage of everything a wireless infrastructure has to offer.

For more information on Intel IT best practices, visit www.intel.com/IT.

IT@Intel

We connect IT professionals with their IT peers inside Intel. Our IT department solves some of today's most demanding and complex technology issues, and we want to share these lessons directly with our fellow IT professionals in an open peer-to-peer forum.

Our goal is simple: improve efficiency throughout the organization and enhance the business value of IT investments.

Follow us and join the conversation:

- Twitter
- #IntelIT
- LinkedIn
- IT Center Community

Visit us today at intel.com/IT or contact your local Intel representative if you would like to learn more.

Related Content

Visit intel.com/IT to find content on related topics:

- A Roadmap for Connecting Smart Phones to the Intel Wi-Fi* Network paper
- Accelerating the Enterprise Network Using 802.11n Wireless paper
- Enabling Smart Phones in Intel's Factory Environment paper
- Evaluating Intel® Pro Wireless Display for Enterprise Use paper
- Evolving the Mobile Employee Hotspot for IT Consumerization paper
- Getting a Headstart on Location-based Services in the Enterprise paper
- Granular Trust Model Improves Enterprise Security paper
- Improving Security and Mobility for Personally Owned Devices paper
- Managing a Global Wireless LAN paper
- Refresh Cycle Still Relevant as the IT Landscape Evolves paper