IT@Intel White Paper
Intel IT
IT Best Practices
Employee Productivity and IT Consumerization
June 2011

A Roadmap for Connecting Smart Phones to the Intel Wi-Fi* Network

As smart phone technology supports better encryption, network authentication, and other important security and manageability requirements, we anticipate more widely deploying our smart phone Wi-Fi connectivity model throughout the enterprise.

Jim Baca
Principal Engineer, Intel IT

Roy Beiser
Network Specialist, Intel IT

Executive Overview

To take advantage of the consumerization of IT and better manage the proliferation of smart phone use at Intel—without compromising Intel's security and manageability requirements—Intel IT has developed a roadmap for connecting smart phones to the enterprise Wi-Fi* network.

Many current smart phone models don't meet our security and manageability requirements. Because our Wi-Fi infrastructure cannot control which models access Intel resources, smart phones, whether employee- or corporate-owned, must use the 3G/4G cellular network for voice calls. Smart phones must also use the cellular network when accessing resources such as e-mail, calendars, or contact information.

However, we anticipate that allowing smart phones to connect to Intel's enterprise Wi-Fi network could offer several potential advantages over using the cellular network:

- Avoidance of costly cellular usage fees
- More reliable voice reception and coverage, supporting enhanced mobility and productivity
- Faster and more reliable data transmission

To achieve these benefits while still protecting Intel data, we developed a secure Wi-Fi connectivity model for smart phones that uses virtual Wi-Fi networks built on our existing Wi-Fi infrastructure. We control which corporate resources a device can access based on three levels of trust—fully trusted, partially trusted, and non-trusted.

We began our phased plan for introducing Wi-Fi connectivity for smart phones with evaluation and analysis, including several proofs of concept. We are currently transitioning to Phase 2, to expand these early projects and continue testing the model.

As smart phone technology matures to support better encryption, network authentication, and other important security and manageability requirements, we anticipate more widely deploying our smart phone Wi-Fi connectivity model throughout the enterprise. In the future, we also anticipate using this same model for other devices across the Compute Continuum, such as tablets and laptop PCs.

Contents

IT@INTEL

The IT@Intel program connects IT professionals around the world with their peers inside our organization – sharing lessons learned, methods and strategies. Our goal is simple: Share Intel IT best practices that create business value and make IT a competitive advantage. Visit us today at www.intel.com/IT or contact your local Intel representative if you'd like to learn more.

BACKGROUND

In response to the continuing consumerization of IT, Intel IT has defined new policies that allow employee-owned smart phones to access limited corporate resources such as e-mail, calendars, and contact information. This gives Intel's highly mobile employees the flexibility to use their own smart phones as companion devices to their mobile business PCs, enhancing collaboration with global teams, business partners, and customers from home or on the road.

Intel employees have increased their use of handheld devices, including smart phones, by 94 percent since 2009, as shown in Figure 1. But as handheld devices have proliferated in our environment, so too have issues surrounding security and network connectivity.

Current Smart Phone Usage and Connectivity Models at Intel

Smart phones in use on Intel campuses—both employee- and corporate-owned—are allowed to connect only to the cellular network for voice calls or when accessing corporate data. (See the sidebar "How Smart Phones Work.") We do not allow them to connect to the enterprise Wi-Fi network due to security concerns over separating corporate and personal use:

- Corporate use. Employees use a personal or corporate-owned smart phone to access corporate data—such as business-related e-mail on a corporate-owned smart phone or synchronizing a calendar on a personal smart phone.
- Personal use. Employees use a personal smart phone for activities not related to business, such as downloading music.

Existing smart phone technology does not support the secure partitioning of corporate and private data; therefore, we require employees to use the cellular network to establish an Internet connection while onsite at an Intel campus. Intel corporate data such as e-mail messages are then "pushed" to the device through a secure application gateway.

When at home or on the road, employees can use a public Wi-Fi network or the cellular network to access limited Intel resources through the Internet. This does not pose a security risk to Intel because the connection is made through an Internet connection with a firewall, and is not a direct, unlimited connection to Intel's enterprise network.

Limitations of the Current Connectivity Model

Limiting smart phone users to cellular connectivity while onsite at an Intel campus

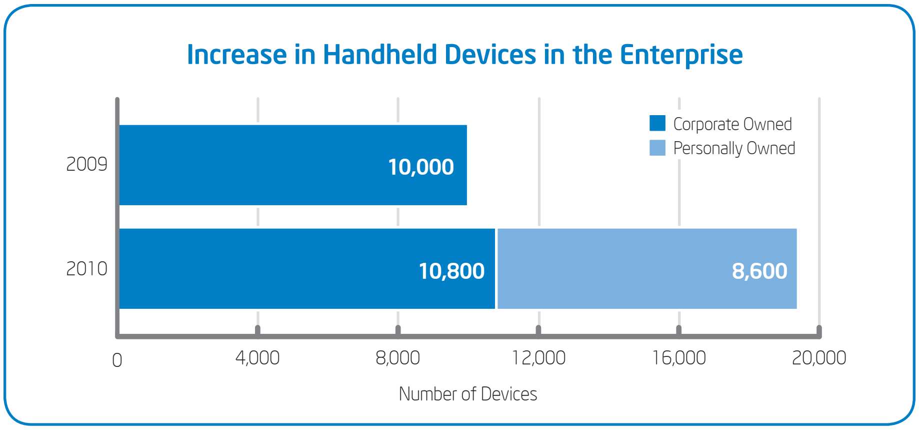

Figure 1. The number of handheld devices accessing corporate data on the Intel network grew by 94 percent from 2009 to 2010, primarily due to increased use of employee-owned smart phones.

effectively protects Intel's corporate data. However, Wi-Fi connectivity can be faster and more reliable than cellular connectivity, assuming enough wireless access points (APs) exist. Wi-Fi connectivity also helps Intel and employees avoid recurring cellular usage fees.

Intel's smart phone users are cognizant of these advantages and have been requesting Wi-Fi connectivity. In particular, some Intel labs that test new devices would like to connect to the Internet using Wi-Fi, and employees who own certain smart phone models do not have reliable cellular reception at some Intel locations.

To meet these needs, Intel IT has developed a roadmap for connecting smart phones to our Wi-Fi enterprise network that meets our requirements for security and manageability.

SOLUTION

We are taking a phased approach to implementing Wi-Fi connectivity for smart phones. This approach accommodates both corporate and personal use cases without compromising information security. Although the current solution is for smart phones, in the future, we can also apply it to other devices across the Compute Continuum, such as to tablets or laptops, as we continue to respond to the consumerization of IT.

We have developed a new smart phone connectivity model, which includes proofs of concept (PoCs) and pilot projects for evaluation and testing. We will expand the scope to move toward global deployment.

New Smart Phone Wi-Fi Connectivity Model

In order to protect our network and intellectual property, we developed a network connectivity model based on levels of trust to manage employee- and corporate-owned devices.[1]

How Smart Phones Work

Most current smart phones are "dual mode," supporting two interfaces that can transmit both voice and data.

3G/4G cellular interface. Powered by the network of cell phone towers across a region.

Wireless LAN (WLAN) interface. Uses one or more of the Wi-Fi* communication protocols—802.11a, 802.11g, or 802.11n—to transmit voice and data.

Dual-mode smart phones can switch back and forth between the two interfaces, or even use them simultaneously, depending on the connection type available and the application in use.

We defined three levels of trust:

- **Fully trusted.** A trusted or fully managed device—such as an Intel-owned mobile business PC—poses very low risk to the network. Currently, only a few smart phone models fall into this category. These devices would be allowed access to every host and server at Intel, with full Wi-Fi network connectivity.
- **Partially trusted.** Also referred to as partially managed, these devices—such as certain smart phone models—have some support for security measures, including remote wipe, screen lock passcode, or secure storage. We would allow them access to Wi-Fi connectivity, which would in turn provide access to the Internet as well as limited Intel corporate services and resources.
- **Non-trusted.** Employees could use their non-managed, personally owned devices on an Intel campus, but could not access corporate data. We would provide these devices with access to a Wi-Fi-based Internet connection, similar to Intel's current guest network. However, this Internet connection would not provide access any Intel corporate services or resources; it would merely support Internet services like Web browsing.

Because these levels of trust—and the network access afforded to each of them—are valid for all types of computing devices, we would be able to apply our connectivity model to additional classes of devices, such as tablets or laptops, as the need arises.

EXPOSED SERVICES

We call the services accessible to partially trusted devices "exposed services" because we expose them to the Internet using special application gateways located in the demilitarized zone (DMZ)—the portion of the network connecting the enterprise network to the Internet, as shown in Figure 2. With our current cellular-based connectivity model, exposed services include e-mail, calendar, and contacts.

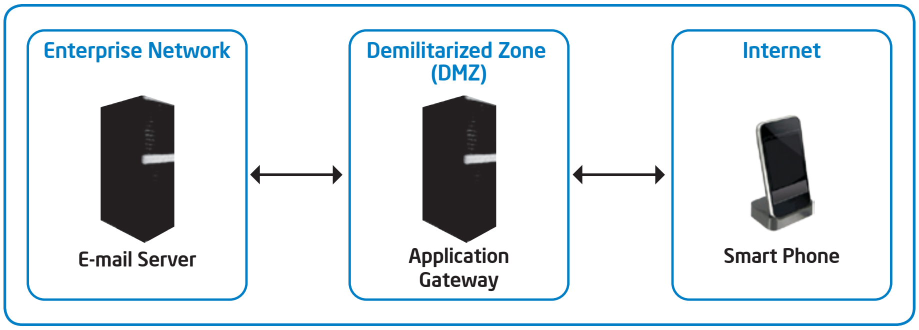

Figure 2. Exposed services are provided to partially trusted devices by using special application gateways, which connect the enterprise network to the Internet.

[1] These levels of device trust map to the "trusted," "selective," and "untrusted" security zones of Intel's security architecture, discussed in "Rethinking Information Security to Improve Business Agility."

With the new Wi-Fi connectivity model, exposed services would be accessible to partially trusted devices using an Internet connection, application firewalls, and access lists that would prevent the security level from being compromised. Along the new model, we would increase the number of exposed services, and employees would have access to other exposed services beyond those available today, such as applications for reserving conference rooms and setting up teleconference bridges.

IMPLEMENTATION

We implemented the new smart phone connectivity model, shown in Figure 3, by creating two new virtual Wi-Fi networks on our existing Wi-Fi infrastructure, each of which uses a different security mechanism:

- **A secured enterprise network for fully trusted devices.** Uses enterprise-class authentication such as Extensible Authentication Protocol - Transport Layer Security (EAP-TLS) or Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling (EAP-FAST) and enterprise-class encryption such as Wi-Fi Protected Access II (WPA2). In addition, access lists on the routers allow only desired traffic to be delivered to the smart phone.
- **An Internet connection-based network for partially trusted and non-trusted devices.** Uses consumer-class authentication and encryption. In addition, the connection requires employees to enter additional authentication information on a splash page. The Internet connection network is closed, and users outside of Intel cannot access it accidentally.

Phase 1: Evaluation and Analysis

We are currently in the final stages of the evaluation and analysis phase; we have completed one PoC for the secured enterprise network and one PoC for the Internet connection-based network. We have also analyzed the potential impact of smart phone network traffic on our Wi-Fi network.

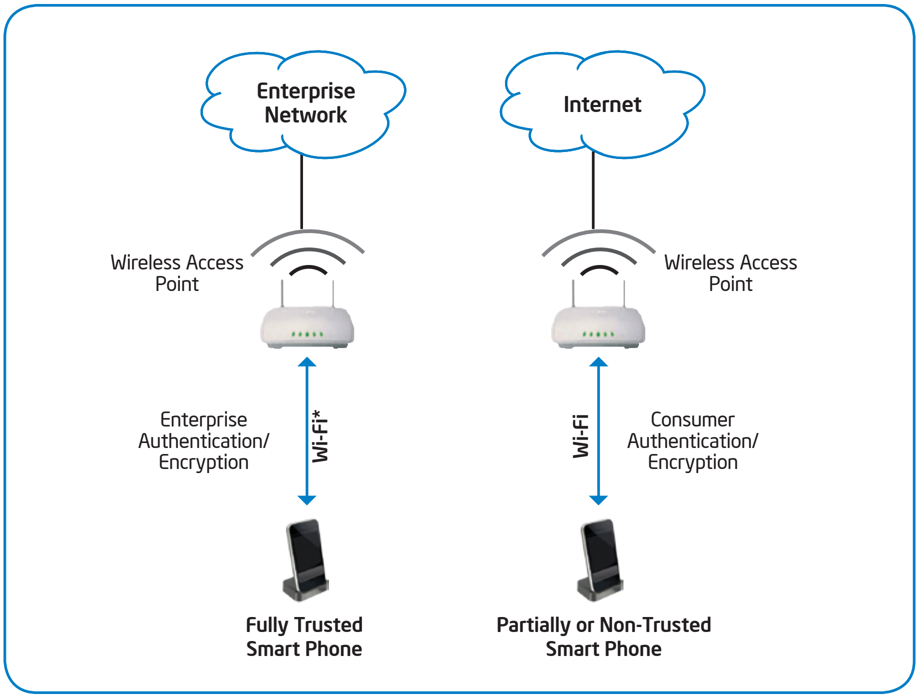
Enterprise Network
Internet
Wireless Access Point
Wireless Access Point
Enterprise Authentication/ Encryption
Wi-Fi*
Wi-Fi
Consumer Authentication/ Encryption
Fully Trusted Smart Phone
Partially or Non-Trusted Smart Phone

Figure 3. Our new smart phone connectivity model creates two virtual Wi-Fi* networks on our existing Wi-Fi infrastructure, using two different security mechanisms.

VOICE OVER IP

To test the secured enterprise network, we completed a PoC with 50 employees using Voice over IP (VoIP) on their smart phones over the Wi-Fi network. For this project, employees accessed only VoIP services over Wi-Fi, not the entire suite of services offered on Intel's network.

We configured each smart phone to connect to the enterprise wireless LAN (WLAN) and then to register with the enterprise VoIP private branch exchange (PBX). This placed users' office extensions on their phones while they were in the office and covered by the enterprise WLAN. As shown in Figure 4, when users were on campus, incoming and outgoing calls were VoIP over WLAN by default. When participants were off campus and the WLAN was not available, the default call type was cellular.

Offloading cellular calls to VoIP has three main advantages:

- Avoidance of costly cellular fees.
- Ability to use a smart phone as an office extension; employees have a single phone number and can receive calls anytime, anywhere, using that number.
- Increased mobility and productivity.

We collected user feedback after this PoC, which was very positive. The majority of users reported good voice quality and asked to keep using this new service.

CONNECTING PERSONAL DEVICES TO THE INTERNET

To test the Internet connection-based network, we completed a PoC that used Wi-Fi to connect personal and corporate devices the Internet. The PoC included 50 employees who used the Wi-Fi network mainly for e-mail—both personal and business-related—as well as for browsing the Web, watching video, and using voice applications.

Such a service offers several advantages:

- **Employee productivity.** Employees can use Intel's fast, reliable Wi-Fi connectivity on campus to access the Internet from personal devices. This is especially useful for companion devices that do not have cellular connectivity, such as netbooks.

- **Potential cost avoidance.** Offloading cellular voice and data traffic to the Intel Wi-Fi network enables Intel or the employee—depending on who pays for the service plan—to avoid costly cellular usage fees.
- **Preparation for the future.** As the consumerization of IT continues and employees increasingly want to bring their own devices into the enterprise, we can use this connectivity model for next-generation devices.
- **Employee satisfaction.** Employees appreciate the connectivity model's "reasonable personal use" policy, whereby they can access the Internet using their personal devices while on campus.

We received positive feedback from the PoC users. The majority reported good performance. We are planning to conduct a full pilot later this year and then to offer this service in our production environment.

WI-FI NETWORK IMPACT ANALYSIS

We analyzed the potential impact of smart phones on the Wi-Fi network based on current smart phone use cases such as accessing e-mail, browsing the Web, and instant messaging. We collected cellular network traffic statistics over the course of two weeks and extrapolated this data to help us determine if our current Wi-Fi infrastructure, such as the number of APs located in office environments, is sufficient to accommodate the anticipated increase in network traffic that smart phones will generate.

Our assessment of 860 employee- and corporate-owned smart phones showed the following results:

- The average smart phone user transfers 2.1 megabits (Mbits) of data per day.
- 95 percent of smart phone users transfer less than 4 Mbits of data per day; only 1 percent of smart phone users at Intel transfer more than 9.2 Mbits per day.
- A single smart phone user transfers an average hourly maximum of about 160 kilobits (Kbits), as shown in Figure 5.

Performing a statistical analysis of these results, in which we assume these 160 Kbits were transferred over a 10-second period of time, we determined that a single smart phone would generate a traffic peak—calculated by dividing the number of Kbits by the number of seconds—of only about 16 kilobits per second (Kb/s). This figure represents a negligible percent of the theoretical maximum throughput—150 megabits per second (Mb/s)—of Intel's 802.11n Wi-Fi network.

When we posit that multiple smart phones may be using the same AP simultaneously, the network impact would still be quite minimal. Our WLAN site survey guidelines mandate that a single AP be capable of covering an area of 20 open-space offices and of simultaneously serving the 20 employees located in that area.

We can safely say that, based on current smart phone usage at Intel, Intel's enterprise Wi-Fi network is capable of handling the aggregate effect of 20 smart phones, each with occasional peaks of 16 Kb/s.

Phase 2: Pilot Projects

We will expand both the secured enterprise network VoIP PoC and the Internet connection-based network PoC later in 2011. This will enable us to test the connectivity model with a greater number

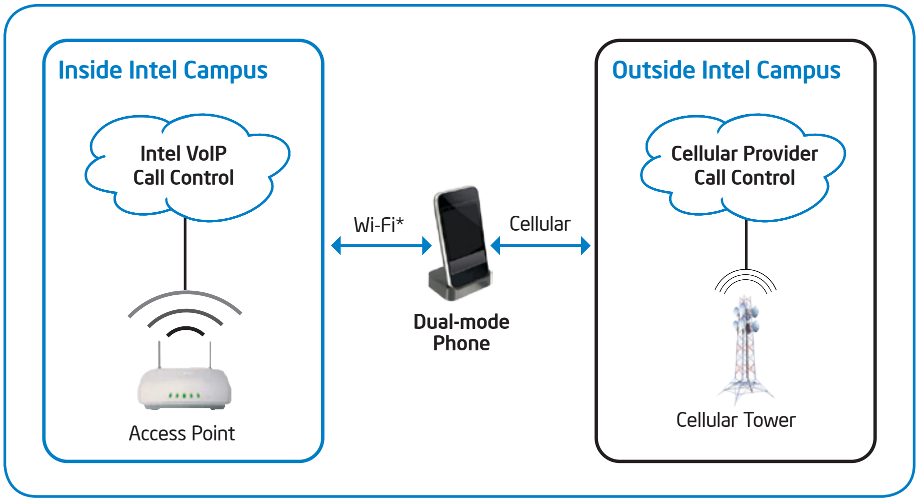

Figure 4. Using Voice over IP (VoIP) on the enterprise Wi-Fi* network enables Intel employees to use their smart phones as their office phones—anywhere, at any time, with a single telephone number.

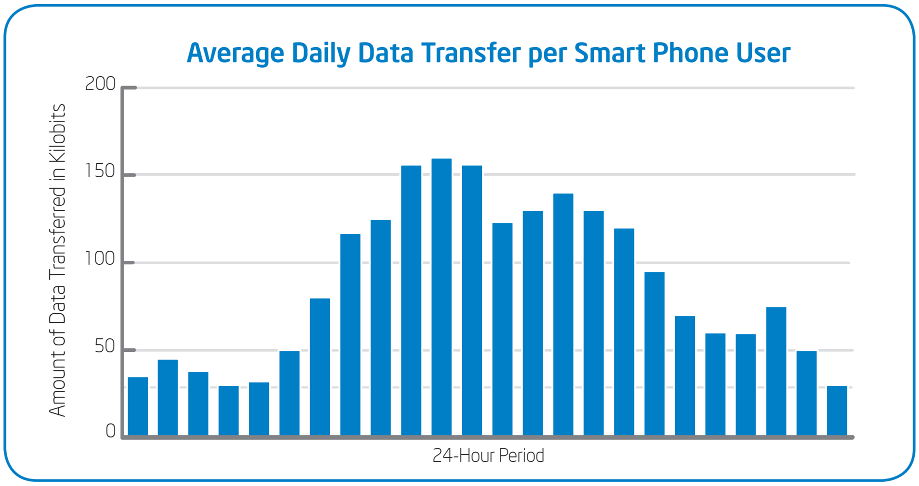

Figure 5. On average, a smart phone at Intel transfers no more than 160 kilobits (Kbits) of data during any given hour of the day.

Intel IT and Intel Product Groups Collaborate to Improve Product Design

As we developed a new Wi-Fi* connectivity model for smart phones, we encountered two critical challenges:

- Establishing a reliable, secure method of authenticating devices to the network. For devices that store and access both corporate and personal data, we need to implement distinct authentication protocols for each partition.
- Managing the device to reduce risk to the network.

Currently, few smart phone models support these requirements. We are therefore working with Intel Ultra Mobile Group to improve product design by providing a set of enterprise features and requirements for smart phones. These include:

- Better ability to authenticate to a network
- Fast, secure encryption
- Support for anti-virus protection
- Support for remote device lock and wipe
- Ability to create secure corporate and personal data partitions

We anticipate that, in the future, devices based on Intel® Atom™ processors will include many of these enhancements and will become part of our smart phone Wi-Fi connectivity plan—thereby meeting Intel IT's long-term goal of using Intel® architecture-based systems whenever they meet our enterprise needs.

of smart phones on multiple campuses and will also provide an opportunity to evaluate a support model tailored for this technology.

Phase 3: Expanded Deployment

Once we complete Phases 1 and 2, we plan to expand deployment of Wi-Fi smart phone connectivity at Intel. We have Phase 3 activities planned in several areas.

SUPPORT ADDITIONAL APPLICATIONS

In addition to the VoIP application we are already investigating, we anticipate making other applications available to fully trusted devices—those that have access to the secured enterprise Wi-Fi network. For example, we hope to make collaboration tools, such as video and online meeting applications, available to users of smart phones and possibly other companion devices as well.

We also plan to explore context-aware applications—which combine physical location with user preferences—to provide services such as directions to conference rooms or printers.

INCREASE THE NUMBER OF EXPOSED SERVICES

We plan to add to the list of exposed services available to partially trusted devices through the Internet connection-based Wi-Fi network. We also hope to be able to make a select few exposed services available even to non-trusted devices by tailoring the applications to work with a firewall in a secure manner.

IMPROVE WI-FI COVERAGE THROUGHOUT THE ENTERPRISE

Although current levels of smart phone use will have minimal effect on the Wi-Fi network in terms of bandwidth and the number of wireless APs, we will continue to invest in the WLAN infrastructure to anticipate future needs. Our project with VoIP and smart phones indicated that we need to add APs in areas such as stairwells, elevators, bathrooms, smoking areas, multi-level parking buildings, and even along sidewalks between buildings to achieve true mobility in the office environment. These additional APs will help provide continuous Wi-Fi coverage, allowing seamless voice calls across campuses.

From June 2010 to March 2011—40 weeks—total AP count at Intel has increased by 22.4 percent, from 6,765 to 8,274. In addition, the number of connections has increased by 58 percent.

As network traffic increases, especially due to bandwidth-intensive applications such as video, we may also need to perform additional network analysis site surveys to determine if our environment has enough APs and the network bandwidth to support them.

CONTINUE TO COLLABORATE WITH PRODUCT GROUPS

We will continue to work with Intel Ultra Mobile Group and industry to define requirements for enterprise-level security and manageability for smart phones. For example, we will explore in more depth the concept of business and personal partitions on smart phones. In order to use the same radio interface for both the personal and corporate partitions at the same time, we expect future smart phones to support sharing of both Wi-Fi and cellular interfaces. One method of supporting this usage is a virtual network interface card (NIC).

CONCLUSION

To protect Intel's data and intellectual property, smart phone users at Intel are currently limited to using cellular networks for voice calls and to access corporate data. Because we anticipate that smart phones will become increasingly important companion devices for Intel employees, we are developing a secure Wi-Fi connectivity model for smart phones that accommodates both corporate and personal use cases.

The Wi-Fi connectivity model will enable us to meet the need for smart phone Wi-Fi connectivity and to avoid costly cellular usage fees, without compromising information security. In addition, Wi-Fi connectivity offers employees more reliable voice reception and coverage, which supports enhanced mobility and productivity, as well as faster and more reliable data transmission. As an added benefit, we can use this connectivity model for other devices across the Compute Continuum in the future, such as for tablets and laptop PCs.

We are introducing smart phone Wi-Fi connectivity in phases, starting with evaluation and analysis, followed by several PoCs and pilot projects. Based on the results of our network impact analysis, Intel's Wi-Fi enterprise network can support the introduction of smart phones without negatively affecting network traffic, given the current usage models of e-mail, contact and calendar information, and Web browsing. The introduction of additional smart phone applications, such as context-aware applications, VoIP, and collaboration tools, may increase network utilization and would require Intel IT to perform wireless site surveys to determine if we have enough APs and network capacity to handle additional network traffec.

Over time, we plan to deploy smart phone Wi-Fi connectivity throughout the enterprise. Full deployment of our new smart phone connectivity model is contingent on the maturation of smart phone security and manageability features, such as faster, better encryption and the ability to securely partition corporate and personal data on the device.

FOR MORE INFORMATION

Visit www.intel.com/IT to find white papers on related topics:

- "Maintaining Information Security while Allowing Personal Hand-Held Devices in the Enterprise"

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

CONTRIBUTORS

Selim Aissi
Lead Strategic Planner,
Intel Ultra Mobile Group

ACRONYMS

AP	access point
DMZ	demilitarized zone
EAP-TLS	Extensible Authentication Protocol - Transport Layer Security
EAP-FAST	Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling
Kbit	kilobit
Kb/s	kilobits per second
Mbit	megabit
Mb/s	megabits per second
NIC	network interface card
PBX	private branch exchange
PoC	proof of concept
VoIP	Voice over IP
WLAN	wireless LAN
WPA2	Wi-Fi Protected Access II

This paper is for informational purposes only. THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Intel disclaims all liability, including liability for infringement of any patent, copyright, or other intellectual property rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Printed in USA
0611/JLG/KC/PDF

♻ Please Recycle
324596-001US