IT@Intel White Paper

Intel IT
Employee Hotspot
March 2014

Evolving the Mobile Employee Hotspot for IT Consumerization

The Employee Hotspot Wi-Fi network, which began as a benefit for employees, has provided significant value to the business, increasing employee productivity and decreasing costs.

Sanjay Rungta
Senior Principal Engineer, Intel IT

Manish Dave
Staff Engineer, Intel IT

Roy Beiser
Network Specialist, Intel IT

Executive Overview

IT consumerization and the business need for broader network access present Intel IT with a continuously evolving challenge. The growing adoption of bring your own device (BYOD) poses additional challenges as consumer choices expand and employee expectations for network support grows.

In 2005, Intel IT implemented a Guest Internet Access Wi-Fi* network, giving contractors and visitors on Intel's campuses the ability to access the Internet using their own devices for business reasons. In late 2007 the mobile industry was transformed with the first touch smartphones, and by 2009 smartphones were common for employees, but they were not able to connect to the enterprise Wi-Fi network. In 2010, Intel IT enabled a mobile Employee Hotspot service to accommodate personal devices accessing the Internet. But what began as a benefit for employees has provided significant value to the business, increasing employee productivity.

We anticipate multiple devices per employee in the future and advances in device technology that will require more bandwidth and connectivity options. To stay ahead of demand, we re-architected the overall Employee Hotspot service using an overlay network, making it easier to deploy with lower cost. This new overlay network uses virtual routing and forwarding technology, which can use our existing network infrastructure without additional hardware. The benefits of this approach include the following:

- **Improved security and scalability.** Adding capabilities such as application layer gateways, cloud-based proxies, and mobile security allow us to detect and respond more quickly to threats while increasing scalability for high-demand usage.
- **Improved usability.** Implementing a new hotspot account management system enables employees to add and remove devices easily and update passwords quickly.
- **Improved productivity.** Adding new network security capabilities allows us to provide access to business applications such as collaboration tools.
- **Reduced costs.** Reusing our existing network infrastructure with the new overlay network eliminates the need for dedicated routers.

As our strategy evolves to keep pace with the realities of IT consumerization, we plan to explore whether other services on the corporate network and Employee Hotspot can be migrated to a converged overlay network to further reduce infrastructure costs. We will also look for opportunities that will provide more access to business applications and data, increasing employees' productivity as well as opportunities to improve overall security and usability.

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

IT consumerization and the business need for broader network access present Intel IT with a continuously evolving challenge. In the past we managed the demand with Guest Internet Access (GIA), providing contractors and visitors with access while they were onsite. We added an Employee Hotspot Wi-Fi* network to allow employees to connect to the Internet with personally owned mobile devices. The growing adoption of bring your own device (BYOD) presents additional challenges as consumer choices expand and employee expectations for network support grow.

What started as a benefit for employees—enabling user choice when accessing data and services—has since become a significant benefit to the business through cost savings and increased employee productivity.

Guest Internet Access

The launch of the Intel® Centrino® processor technology in 2003 made possible mobility with ubiquitous network access. It also raised expectations for consistent connectivity on personal devices used for business activities. Intel has had over 30,000 contractors who over time have required network and Internet access to conduct business activities. To improve productivity we found it necessary to grant secure access to online resources.

In response to this critical business need, we designed GIA in 2005. At that time, the network security architecture, which protects the network from malicious activity, did not include granting access to unknown, unregistered devices. Some of the ways we addressed this restriction included the following:

- **Legal liability.** All visitors are required to accept the Terms of Use and Acceptable Use Policy before gaining access.
- **Authentication and account provisioning.** A new central service allows sponsors to create temporary self-expiring accounts for visitors.
- **Access controls.** Visitors are allowed network access to the Internet and VPN access to their home sites but not the Intel intranet. Compliance to policies such as specific antivirus DAT files and patch levels are also assessed prior to granting access.

During the first 24 months after deployment, GIA was enabled primarily for contractors supporting factory build-out. During this process, several contractors' field sales engineers (FSEs) travel to a single Intel facility to be in constant communication with engineering teams working to acquire factory tool certification. Prior to GIA's deployment, FSEs often returned to hotels or public Internet access sites to access their corporate office intranet services, which resulted in a loss of productivity. After deployment, 98 percent of FSEs reported time savings by having access to their intranet site from the clean room.

Intel Sales and Marketing employees also used GIA to illustrate the Wi-Fi capabilities of the new Intel Centrino processor technology–based laptops, which were available at the Sales and Marketing offices.

Employee Hotspot Wi-Fi Network 1.0

After deploying GIA, we began to see an emerging demand to support Internet connectivity for personally owned mobile devices. From 2009 to 2010 we experienced a 94-percent increase in the number of handheld devices accessing corporate services. In response to this growing business need, we deployed the Employee Hotspot.

Unlike GIA, which focuses on campus visitors and is used for temporary access, we intended the Employee Hotspot to coincide with Intel's "Great Place to Work" philosophy, providing employees with the benefit of personal

Internet access on mobile devices. But what started out as merely a nice-to-have employee benefit has transformed into a solution that enables significant productivity gains and benefits the entire enterprise.

INITIAL EMPLOYEE HOTSPOT IMPLEMENTATION

Our initial implementation comprised the following:

- **Infrastructure.** The initial implementation of the Employee Hotspot used network architecture similar to that used for GIA, which allowed us to do the following:
  - Isolate the hotspot traffic using VLAN technology
  - Enforce security controls
  - Reuse the existing WAN, demilitarized zone (DMZ), and Internet Service Provider (ISP) network infrastructure

  VLANs mapped to specific hotspot Service Set Identifications (SSIDs), which were routed by a dedicated site router to the centralized DMZ using Generic Routing Encapsulation tunnels, as shown in Figure 1.
- **Secure access.** To maintain protection against malware and malicious traffic, we filtered network traffic through a transparent proxy, which acted as a bridge between the DMZ hub router and the external firewall. Using a modular access model, devices connected to the hotspot and performed the required authentication. Application gateways enforced the appropriate access level and control policies–based profiles.
- **Device and user registration.** Similar to GIA user authentication, we required employees to register and provision their network account for their personal devices, a process that required them to accept legal terms and conditions for network access. Once the network accounts were provisioned, employees configured the Wi-Fi profile on their device. Then the device automatically connected to any hotspot whenever it was within the coverage area, allowing employees to connect automatically on any Intel campus worldwide.

These three components were a good start, but evolving use cases and technologies raised some issues.

EMPLOYEE HOTSPOT 1.0 - CHALLENGES

As employees added new mobile devices, the demand for business productivity tools on these devices also increased. Allowing employees to access services can provide cost savings and productivity increases for the enterprise. At the same time, the initial Employee Hotspot design had challenges and limitations, which affected its ability to meet future demand:

- **Security.** The initial implementation focused on providing Internet access and hence was limited in its ability to provide secure access to internal enterprise services, such as social collaboration tools, that could further increase productivity and overall adoption.
- **Usability.** Users were required to authenticate once a day. Because user names often include underscores, logging on to some devices was a frustrating experience.
- **Scalability.** Local dedicated site routers had bandwidth limitations. Because of the static nature of bandwidth management on the legacy infrastructure, which was originally built for GIA and later used for the Employee Hotspot, the initial design was not able to dynamically manage the bandwidth requirements of the anticipated increase in personal device usage.
- **Agility.** Bringing new sites online with the initial model was time consuming because it required installing new network infrastructure dedicated to Internet access at the site.
- **Expense.** The dedicated network equipment across 120 sites was reaching its end of life, requiring new capital investment. We attempt to keep our network projects at zero budget whenever possible.

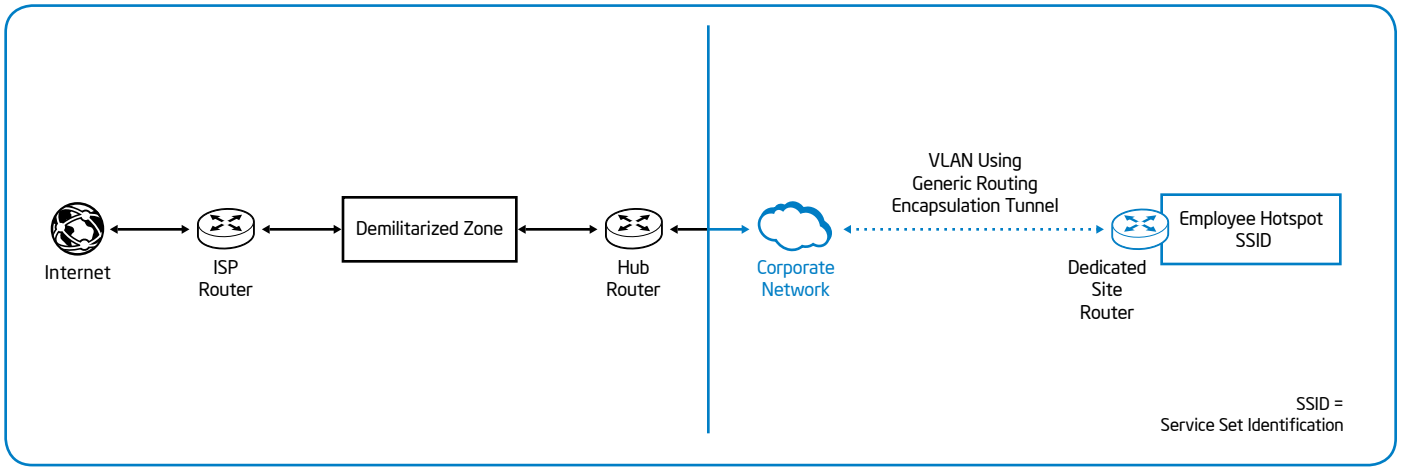

Figure 1. The initial implementation of the Employee Hotspot network isolated hotspot traffic using VLAN technology and dedicated site routers.

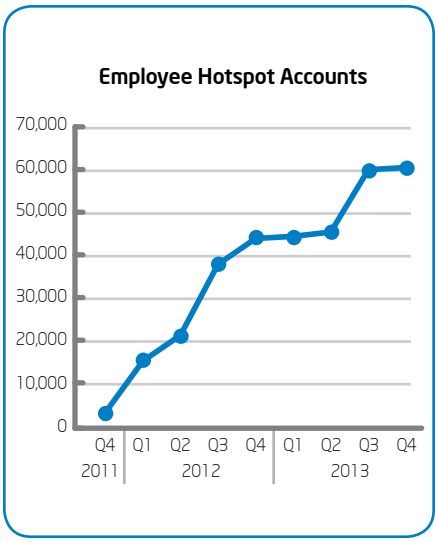

Figure 2. The number of Employee Hotspot accounts grew significantly from 2011 through 2013.

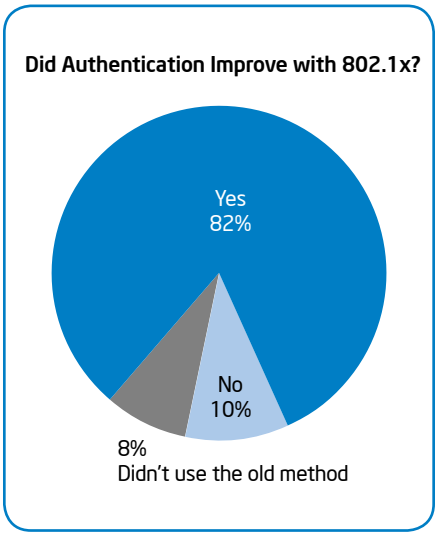

Figure 3. Eighty-two percent of users surveyed in the second survey preferred the improved authentication experience.

We examined each of these areas looking for ways to make improvements. We immediately addressed the security and usability challenges. To overcome the operational challenges of scalability, agility, and expense, we are in the process of re-engineering the solution, creating Employee Hotspot 2.0 (discussed later).

EMPLOYEE HOTSPOT 1.0 - IMPROVEMENTS TO EMPLOYEE EXPERIENCE AND AUTHENTICATION

We sought to improve the usability of the Employee Hotspot service and the overall employee experience, with the goal of increasing adoption rates and productivity. To achieve this goal, we made several changes to mobile device access, including improvements to the password reset process, trimming it from a few hours to minutes. A new hotspot account management system provided employees with a single portal for registering, onboarding, and managing the lifecycle of their mobile devices and the services they subscribe to.

We also changed the authentication to 802.1x, an Institute of Electrical and Electronics Engineers standard for Port-based Network Access Control that provides an authentication mechanism to devices that needed to attach to a LAN or WLAN. Changing the authentication from web-based to 802.1x allowed employees to store credentials in a Wi-Fi profile on each registered device and move throughout the enterprise with automatic connection.

After making these changes, we surveyed the users and received a positive response. We also saw an increase in adoption, as shown in Figure 2. More than 93 percent of survey responders indicated that they would continue to use the service. We also determined that there would be no negative impact to the existing wireless infrastructure and the dedicated network load would be within acceptable limits.

A second survey yielded the following results:

- More than 95 percent of survey responders said they would continue to use the service.
- Eighty-two percent of responders preferred the improved authentication experience, as shown in Figure 3.
- Fewer than 1 percent of devices, which were primarily legacy e-readers, were unsupported.

These promising results indicated that we were on the right track, and employees valued the hotspot service.

Emerging Usage Models

As growth continues in the use of personal 2-in-1 devices and companion tablets to access both corporate and personal data within the enterprise, we anticipate that employees will increasingly adopt the Employee Hotspot service. While designing improvements to address the operational challenges of scalability, agility, and expense defined above, we also identified the following emerging usage models:

- **Multiple devices per employee.** We have seen an increase from an average of 1.1 devices to 1.4 devices per employee since 2010, and we expect this growth trend to continue. Employees want to easily add, replace, and manage devices, and at the same time we must continue to ensure network security. Network capacity must meet the demand with robust account management and authentication.
- **Personal devices used for business.** The use of personal devices to access business data, such as collaboration tools, calendars, voice, and video, directly benefits the enterprise through increased employee productivity. Currently these applications are accessed over the Internet through the DMZ, which is not as efficient as using the Employee Hotspot.

- **Next-generation applications for personal devices.** We expect that next-generation devices such as tablets and 2-in-1 devices will allow full bandwidth connections rather than the current smartphone model of working offline, then syncing data. The Employee Hotspot must be able to scale dynamically to accommodate bursts of bandwidth usage in this scenario without disrupting existing business traffic.

These emerging uages models will lead us to further evolve the architecture.

ALIGNING OUR EMPLOYEE HOTSPOT WI-FI NETWORK WITH BYOD TRENDS

As demand for BYOD networking continues to grow, we must work to evolve our network services. We have developed a new architecture to provide network capabilities that continue to provide business value for employees, help us prepare for the next wave of consumerization, and contain cost.

Based on the emerging usage models, we evaluated our current network infrastructure for opportunities to reuse equipment and resources. As in our previous deployments, using an overlay network was the best approach for containing costs. Our new design, like its predecessor, is built on the existing WAN infrastructure. However, the new design eliminates the need for dedicated routers, giving us the additional benefit of rapidly deploying new sites and field offices.

Employee Hotspot Wi-Fi Network 2.0

We are in the process of implementing a new design that merges both the GIA and Employee Hotspot services with the existing LAN/WAN infrastructure using an overlay network. With new routing and forwarding technology we can use the campus LAN and WAN routers, removing the dedicated site routers that have been serving the GIA and Employee Hotspot 1.0 network. Figure 4 illustrates the overlay technology.

This approach has significant benefits, including the following:

- **Reduces costs.** Leveraging the benefit of our existing multitier, private LAN/WAN eliminates the need for dedicated hardware at each site.
- **Ability to rapidly add new sites.** We can bring new global sites online in significantly less time because no new routers are required.
- **Improves security.** We can improve the security and isolation model with technology that isolates network routing instances. Network and cloud service providers already widely use this technology.
- **Increases resilience.** We use dual paths from each site to two DMZ hubs, which provide failover if one DMZ hub or Internet egress point fails.

The following two sections discuss in more detail the solution architecture and our approach to security.

ARCHITECTURE

The new architecture uses virtual routing and forwarding (VRF) technology to overlay the hotspot network on the corporate LAN and WAN networks, eliminating the need for dedicated routers. VRF is an Internet Protocol (IP) technology that allows multiple instances of a routing table to coexist on the same router at the same time. This approach

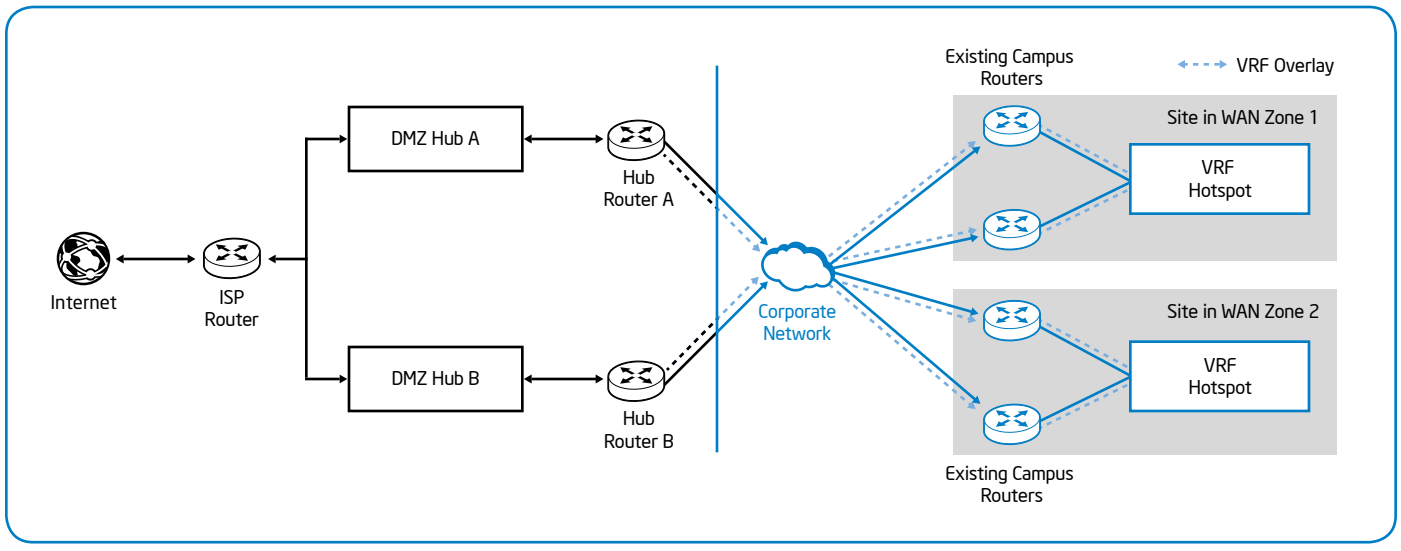

Figure 4. The topology of the virtual routing and forwarding (VRF) overlay network uses dual paths to two demilitarized zones (DMZs), which increases resilience.

provides the added advantage of increasing security by maintaining complete isolation of routing instances, which is analogous to how data center server virtualization allows a single server to support multiple virtual machines. By running multiple instances of VRF on the WAN and LAN routers, we can support both the GIA and Employee Hotspot while maintaining secure isolation between the networks.

Similarly this approach takes advantage of existing infrastructure to support the new network transport service. The new design also includes reusing the campus Dynamic Host Configuration Protocol servers for managing client IP addressing for external and internally hosted services.

SECURITY

The new design adds capabilities to securely allow access to internally hosted services, increasing productivity for employees on their personal devices. A modular, centralized security event management system enables our security operations team to detect and address security incidents more quickly (see Figure 5).

- **Application layer gateways.** Ingress traffic is filtered to exposed services with more granular access control through application-aware gateways, such as web application firewalls, web services security gateways, and web VPN connectivity portals.
- **Cloud-based proxies.** To support more devices and bandwidth-intensive applications, cloud-based proxy filtering can scale services to meet the demand. It also allows implementation of hotspot services at sites that cannot backhaul traffic to the DMZ. Instead, hotspot traffic is forwarded to the cloud proxy service using a local ISP.
- **Mobile security.** Mobile device and application manageability and security capabilities with a granular trust model define a set of increasing restrictions based on the person requesting access, the device being used, the location, and the time.
- **Voice over IP (VoIP) and collaboration.** Our planned enhancements include VoIP enabling and collaboration solutions such as videoconferencing on personal devices.

CONCLUSION

The Employee Hotspot Wi-Fi network, which began as a benefit for employees, has provided significant value to the business, increasing employee productivity and decreasing cost.

From the GIA, which improved productivity for visitors and contractors working on the premises, to the addition of the Employee Hotspot, which gives employees consistent Internet connectivity on mobile devices, We have continuously refined our network architecture to meet the demand.

The new VRF overlay network improves the experience of employees accessing services from personal devices, increases security and scalability, and allows us to offer broader business application services that further increase employee productivity. The use of overlay networks has also allowed us to reuse existing network hardware, keeping costs to a minimum.

The redesign and the pilot are in the final stages, and we will transition the GIA and Employee Hotspot access network to the

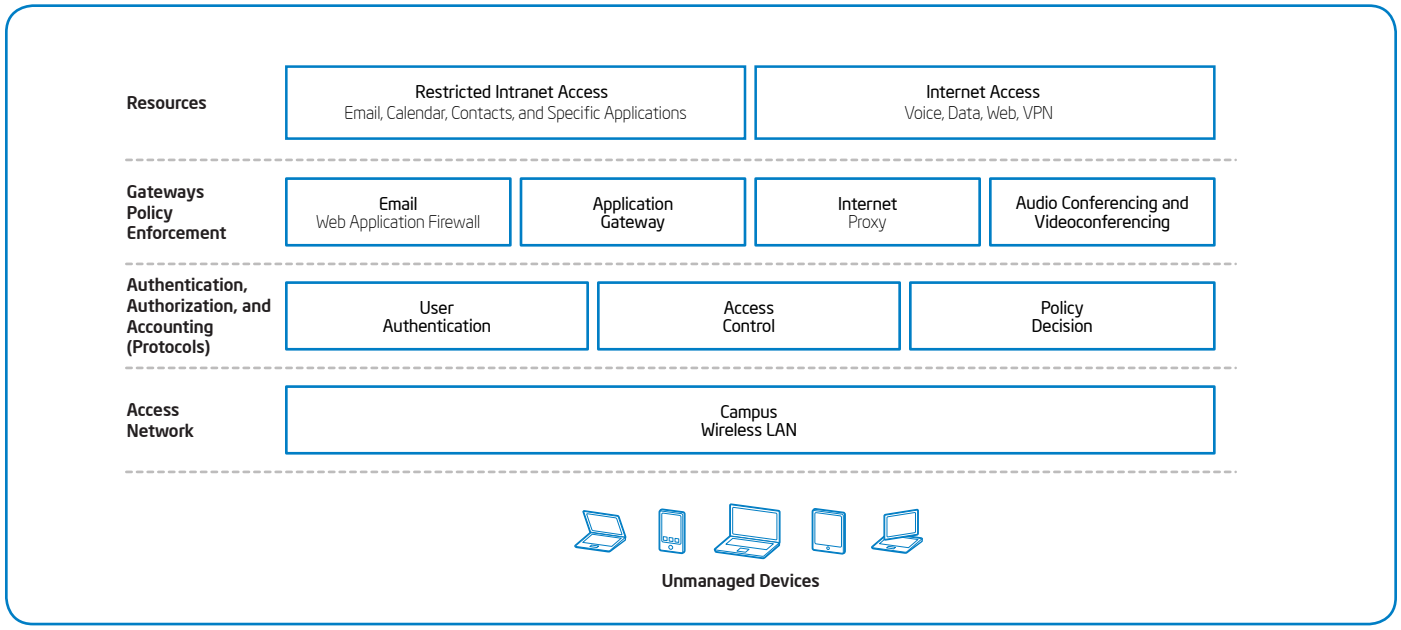

Figure 5. Modular access architecture enables secure access to business data.

overlay network across the enterprise. We anticipate concluding within the year. In the coming months we will deliver voice and video services for collaboration on the new Employee Hotspot and allow employees to use the device of their choice for a wider range of business applications.

As our strategy evolves to keep pace with the realities of IT consumerization, we plan to determine whether other services on the corporate network and Employee Hotspot can be migrated to a converged overlay network to further reduce infrastructure costs. We will continue acting on opportunities to provide more access to business applications and data, increasing employees' productivity, as well as opportunities to improve overall security and usability as we embrace the consumerization transformation.

FOR MORE INFORMATION

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

- "A Roadmap for Connecting Smart Phones to the Intel Wi-Fi* Network"
- "Nine Things You Should Never Do While on a Wi-Fi Hotspot"

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

CONTRIBUTORS

Todd Butler
Product Line Manager

Chandra Chitneni
Staff Network Engineer

Neil Doran
Program Manager

Dick Freeman
Senior Network Engineer

Avigail Garti
Network Engineer

Kevin Heine
Senior Network Engineer

Chris Steenkolk
Network Engineer

ACRONYMS

BYOD	bring your own device
DMZ	demilitarized zone
FSE	field sales engineers
GIA	Guest Internet Access
IP	Internet Protocol
ISP	Internet Service Provider
SSID	Service Set Identification
VoIP	voice over IP
VRF	virtual routing and forwarding

0314/JGLU/KC/PDF 330108-001US

Look Inside.™