INSTITUTE FOR DEFENSE ANALYSES

# In-Use and Emerging Disruptive Technology Trends


Laura A. Odell, *Project Leader*

Brendan T. Farrar-Foley
J. Corbin Fauntleroy
Ryan R. Wagner



31 March 2015

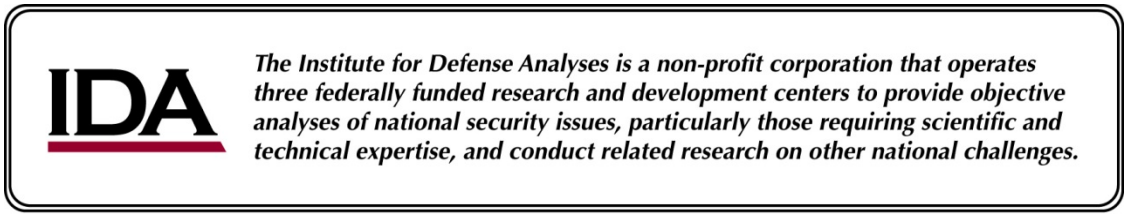




IDA Non-Standard
D-5457
Log: H 15-000243
Copy



INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882




About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract DASW01-04-C-0003, Task BK-5-3754, "Web as a Service (WaaS), Future Office, COOP," and Task BK-5-3448, "Next-Generation Networks," for the Office of the Secretary of Defense, Chief Information Officer Director, Enterprise Information Technology Services Directorate. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments

Thomas H. Barth, Cameron E. DePuy

# IDA Executive Summary

The Department of Defense (DoD) is facing rapid advancements in technology that will significantly change the way its information technology (IT) infrastructure is implemented and managed. Technologies are being developed and used in the commercial world that increase the efficiency of network resources, improve security across the network, and improve mobile access and collaboration. Many companies are implementing anytime, anywhere connectivity across their workforces to improve productivity, reduce costs, and increase mobility and collaboration in their workplaces. Expectations in a digital world, on a daily basis include instant communication, collaboration, and enhanced technologies that facilitate a mobile workforce in and outside the traditional workplace. DoD must adapt to the workforce's use of technology to attract and retain the best and the brightest. There is an implicit expectation that the technology in the workplace should be as good as or better than that at home.

The Office of the Secretary of Defense (OSD) Chief Information Officer (CIO) asked IDA to research and assess emerging low-risk, high-impact technologies that would prepare DoD for a more mobile, agile, and efficient workforce. OSD CIO is the leader in IT and information management for networking, computing, information assurance, enterprise services, and applications for the Pentagon Reservation. The motivation for this work was the OSD CIO's need to better understand the potential of emerging and in-use technologies to meet their strategic vision of dependable, reliable, and secure IT services with easy access to network resources using up-to-date technology.

The IDA team worked closely with the OSD CIO to identify nine potential solution sets that could potentially improve the effectiveness and efficiency of the DoD IT infrastructure. The team examined current research, vendor information on cutting-edge and mature commercial products, technology standards, and related federal government programs to develop an understanding of technologies directly applicable to the Pentagon environment. A series of concise analysis summaries was developed to inform decision makers in a "quick-look" format. Each summary describes a specific technology, how it works, its constraints and limitations within the current DoD environment, and the potential leverage points available within the current Pentagon information technology infrastructure. An industry snapshot in-use example is included in each summary as well. This document is a compilation of the nine summaries, which are described below.

### Containers: Moving Beyond Virtual Machines

The development of virtual machines (VM) launched a major advancement in information technology. VMs mimic the hardware of a dedicated machine and make it possi-

ble to run the equivalent of many physical machines on just one physical machine. However, VMs must replicate the entire operating system (OS). As a result, it takes time to instantiate a new VM because the machine must be booted up, adding to duplicative overhead that utilizes processing and storage, thereby reducing the number of VM instances that can run on a given physical host. To address this, some major IT service providers have turned to containers for running their services. Containers differ from VMs in that they provide a lightweight layer of abstraction of the OS rather than an entire dedicated OS. In a VM environment, multiple VMs are running, each with an instantiation of a full OS that is created and managed by the hypervisor. A container has only one OS, and each instance of the container shares the single OS kernel. This significantly reduces an application's resource needs, but each container can support only one application at a time. Additionally, containers provide less isolation than VMs, causing additional security considerations. While VMs are separated by the hypervisor, containers are separated by kernel-level functionality such as Linux kernel containment.

A container approach is useful for applications that run in a cloud environment which otherwise might comprise numerous VMs running in parallel. Containers greatly increase efficiency. Writing applications to work within a container environment would allow better resource utilization on physical hosts and provide easier deployment of applications in a consistent environment. When utilizing third-party hosting solutions (on dedicated hosts for security), containers provide a common framework for moving applications between cloud providers, which is critical in avoiding vendor lock-in and could be used for continuity of operations. However, the barrier between containers is thinner than that between VMs, so policy on containers must be implemented accordingly.

**Software-Defined Networking: A New Network Architecture**

Mobile devices and content; cloud services; and end point, application, and server virtualization are putting significant stress on today's hardware-centric network designs. Changes in a virtual environment can require reconfiguration of routers and switches within a network. Network providers are moving away from static network configurations to a more flexible, agile approach, called software-defined networking, that will allow administrators to dynamically reconfigure the network through software and application programmatic interfaces (API). Software-defined networks (SDN) decouple the control and data planes (i.e., the software and hardware), allowing the network to be treated as a virtual entity. The software-defined networking environment uses open APIs to support all services and applications running over the network. This allows the network administrator to manage services and applications without having to touch individual switchers or routers. SDNs can be reconfigured on the fly, providing more robust networks that better tolerate failure and route around congestion.

SDN is an emerging architecture that industry is only beginning to use, and much of the work at this time has been focused on gaining data center efficiencies, not enterprise services. Since all information goes through the controller, scalability is a concern. Security is also a concern. An SDN can provide and enforce a security strategy for the network, but this strategy is dependent on how well the SDN itself is protected. The benefits that are derived from network programmability and centralized control also provide new threat vectors that could compromise the network if security is not designed properly from the start.

**De-Perimeterization: Removing the Network Perimeter**

The concept of a network perimeter has been dead for years, but many have not noticed. The primary factors for this failure are: (1) a mobile workforce (via laptops, tablets, and phones) and (2) outsourcing services (e.g., travel, expense reporting, health care, and payroll) to third-party providers. The effect of these factors on the network environment is referred to as de-perimeterization.

The Jericho Forum describes de-perimeterization as "the erosion of the traditional 'secure' perimeters, or 'network boundaries,' as mediators of trust and security." De-perimeterization diffuses the strict boundaries between the internal and external network, requiring organizations to authenticate and encrypt all IT services, which are made available on a least privilege basis (i.e., being inside the network perimeter does not itself allow unfettered access to network resources and data).

In a de-perimeterized network, security controls are shifted from the network to the endpoints, data centers, information repositories, and applications. De-perimeterization assumes that everyone is untrustworthy, and so the concepts of identification, authentication, and authorization become very important. These concepts are applied at all levels, from user devices to application services to critical information assets. Security becomes a guiding principle for the network and is built into the architecture rather than layered onto it. As a result, a de-perimeterized network is more secure because users and devices are authenticated and access to services and data is controlled.

**Zero Trust: An Alternative Network Security Model**

Traditional network security is based on the concept of a network perimeter that has limited access points into the network and that allows in only trusted users. Once inside, users can gain access to any number of resources on the network. This perimeter-based model of security relies on the assumption that everyone and everything inside the perimeter can be trusted. The network perimeter has not adapted to meet the security challenges presented from remote employees, mobile users, or cloud computing, where the boundary between internal and external networks is blurred. As a way to adapt to this blurring of the network perimeter, Forester Research proposes an alternative network se-

curity model, referred to as Zero Trust. This model takes into account both external and internal threats, ensuring that malicious insiders cannot access information they are not authorized to access, thus reducing the exposure of vulnerable systems and preventing the lateral movement of threats throughout the network. Instead of trusting users and their devices to do the right thing, the security model *verifies* that they are doing the right thing. This means that no entity on the network is trusted based solely on network location, including users, devices, transactions, applications, and packets.

One of the major benefits of using a Zero Trust security model is the improved management and fine-grained control of the security of the network. Zero Trust makes it easier to enforce security compliance across all users, devices, and applications and easier to identify all traffic by user, device, and application, allowing full visibility and control of network resources. Current security architecture designs overlay controls on the network; Zero Trust is a departure from that approach in that it embeds security into the heart of the network.

**Mobile Thin Client End Points**

The rise of the personal computer moved computing to the end user, with applications and data residing on the end point. With ubiquitous high-speed networks, virtualization, web-delivered applications, cloud-based storage, mobile apps, and increasing security challenges, applications and data are moving back to the data center, with the user connecting via mobile devices (mobile thin client end points). The traditional thin client typically stores configuration files and the OS on flash memory—no other data is stored locally—and connects to resources hosted in a data center. However, the mobile thin client takes the paradigm further by using a reduced, hardened OS and relying on web interfaces, application streaming to the browser, and virtual desktop interfaces to access resources. Mobile thin clients are easy to administer and deploy. Updates can be done securely and automatically. Security and usability are enhanced due to data and applications residing in the data center. Applications are web-based or streamed from a data center, and users are always up to date when opening applications, thus reducing expensive and ineffective patching operations.

End points are the most compromised part of the network; more than 90 percent of vulnerabilities are through Java and Flash plugins on the end point. Mobile thin clients protect against these types of vulnerabilities. Since the data remains on the server, there is little opportunity for compromise due to loss of equipment (e.g., having a laptop stolen). They are also a good way to improve the management of end points, their applications, patches, and data. Updates only occur on the server, not on the device; data is always up to date on the server.

## New Trends in Mobile Broadband

Each year cellular, or mobile broadband, providers see an increasing number of mobile devices being used. It is estimated that by 2019 there will be over 9.2 billion mobile subscribers in the world, and over 80 percent of those will be for mobile broadband.[1] This high usage is the leading driver for technology changes that will increase capacity and reduce the cost of mobile broadband networks. Mobile broadband allows users to connect to the Internet from any location where cellular services are available for mobile Internet connectivity. Currently using licensed 225 MHz to 3700 MHz radio frequency bands, mobile broadband maintains Internet connectivity as the user moves from place to place.

With the proliferation of smartphones, tablets, and other mobile devices, it is often assumed that mobile broadband will eventually replace Wi-Fi as the network of choice. The reality is much different. The biggest issue facing mobile broadband is capacity. Network congestion in peak use times is not uncommon and data rates across the network slow significantly. To combat the problem, providers are beginning to offload data to carrier-operated Wi-Fi networks spread across metropolitan areas; these hotspots have more capacity and higher data rates. Major cellular providers are beginning to offer Wi-Fi as a complement to their services and are partnering with cable communications companies to gain access to their Wi-Fi hotspots.

## Emerging Wireless Technologies: Faster Speed–More Data

Wireless networks are ubiquitous, and the desire for anytime, anywhere access with ever-increasing speed and bandwidth has driven development of new technologies and ways of doing business. Recent advancements in V-Band, or millimeter wave (MMW), communications, have led to the development of networks with data transfer rates many times faster than those of today's wireless technology. New short-range wireless communication devices using the unlicensed 60 GHz band (millimeter wave band) can provide data transfer rates of up to 7 Gbps. The 60 GHz band (57–64 GHz) has more spectrum available—up to 7 GHz—than today's 2.4 GHz and 5 GHz wireless solutions containing up to 150 MHz.

Wireless is also advancing into the visible light spectrum to create networks where data rides on light waves, referred to as visible light communications or Li-Fi. Light has a higher frequency than radio frequencies. Li-Fi is essentially an array of flickering light emitting diodes (LED) creating a binary (on=1, off=0) data flow, which can occur at higher rates than the human eye can detect, and a light sensor to detect the data flow; the more LEDs, the more data can be transferred over the network. By using Li-Fi-equipped

[1] GSMA. "Will Wi-Fi relieve congestion on cellular networks?" May 5, 2014. GSMA.com. www.gsma.com/spectrum/wp-content/uploads/2014/05/Wi-Fi-Offload-Paper.pdf

light bulbs, the wireless network can be extended throughout the workplace and used to augment existing networks.

While product development for these emerging wireless technologies is only just beginning, these technologies are changing the future of mobile computing and future wireless networks.

### Find Me, Follow Me: Leveraging Micro-location

Widespread use of mobile devices, such as cell phones and tablets, that routinely use GPS and Bluetooth to provide continuous location information, allows users to be tracked anywhere—both in and outdoors. Many applications pull information about objects, services, and people surrounding the device and at the same time push similar information to other nearby devices. Mobile devices containing these types of applications are becoming the standard, making the concept of Find Me, Follow Me (FM/FM) possible in the workplace.

The FM/FM concept comes from the phone industry—a result of individuals having multiple phones (e.g., office phone, cellphone) and not being tied to a specific location. It has expanded beyond the realm of telephony to end-user devices on the network. Micro-location sensors use a range of signals to triangulate and obtain a user's position, including Global Positioning Systems (GPS), cellular, Bluetooth, Wi-Fi, and near field communication. Used in conjunction with geofencing, which provides a virtual fence around a space or building so that information going into and out of the space can be limited or controlled, indoor micro-location allows routing of phone calls to the nearest phone or office, sharing of documents with some but not others, and automated check-in for a space or meeting. Identity verification technologies are also an important part of FM/FM. Location is determined by device, and identity verification ensures that the correct user is associated with the device. By deploying FM/FM technologies, such as indoor micro-location and identity verification, organizations may be able to be decrease labor costs, increase public safety, reduce insider threat, provide indoor navigation aids, and allow meeting check-in, document sharing, and resource allocation optimization.

### Building Mobility into the Classified Environment

Today's demand for wireless and cellular access in the Pentagon is overwhelming. Advances in wireless and mobile broadband technology now make it possible to provide seamless mobile access to information using commodity hardware and software. Deploying an architecture that supports secure wireless communications is a key factor in enabling mobility in a classified environment. An "all in one" wireless network architecture currently gaining traction uses the same physical infrastructure (including Wi-Fi radio equipment) for both classified and unclassified data. But deployment of wireless networks is only half the battle in enabling mobility; devices accessing the network must

securely support the network architecture and meet security constraints. Care must be taken to select devices that can use Wi-Fi in a sensitive compartmented information facility (SCIF) environment without emitting signals that could be remotely read by nearby devices. Advancements in wearable medical devices present new challenges for classified wireless networks. Between collecting personally identifiable information, meeting Americans with Disabilities Act (ADA) requirements, and accommodating returning American veterans with wireless prosthetics and devices, planning for wearable devices must occur.

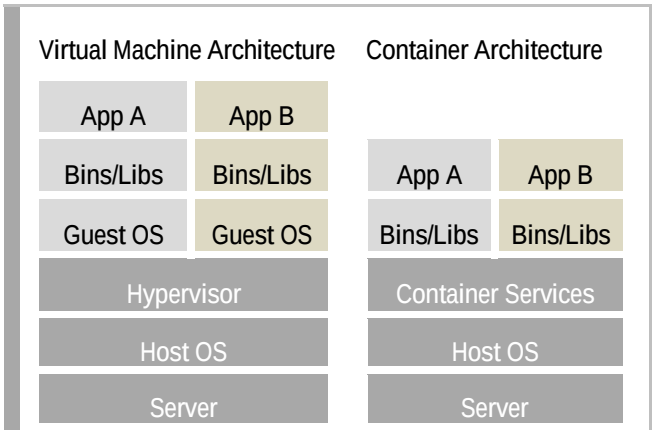
It is inevitable that wireless networks and mobile broadband become part of the infrastructure that supports DoD in the Pentagon. Programs, such as NSA's Commercial Solutions for Classified (CSfC) and DISA's DoD Mobility Classified Capabilities (DMCC) are leading the way toward integrating classified and unclassified work. Government agencies should join forces to leverage DoD programs and NSA research to build a wireless network that has the ability to adapt to emerging technology and can reliably support tenants at both the unclassified and classified levels.

# Contents

# IDA Containers: Moving Beyond Virtual Machines

The development of virtual machines (VM) launched a major advancement in information technology. VMs mimic the hardware of a dedicated machine and make it possible to run the equivalent of many physical machines on just one physical machine. This approach offers a number of benefits. First, VMs improve security by adding another layer of separation between applications running on a particular host. Second, because dedicated machines are often idle, using a combination of VMs can make better use of processing resources; for example, one VM can peak its utilization of the processor while other VMs on the same physical equipment are idle. Third, VMs make it possible to quickly duplicate machines and move services from one physical host to another. Along with accommodating spikes in usage and improving continuity of operations, VMs allow third parties to provide the basic physical infrastructure (e.g., space, electricity, environmental control, connectivity, and physical hardware) for a fee. The latter concept is often referred to as Infrastructure as a Service.

The problem with VMs is that they replicate the entire operating system (OS). Replicating the entire OS increases the time it takes to instantiate a new VM, because the machine must be booted up, adding duplicative overhead that utilizes processing and storage, which reduces the number of VM instances that can run on a given physical host. To address this, some major IT service providers have turned to *containers* for running their services.



*Adapted from: http://www.zdnet.com/what-is-docker-and-why-is-it-so-darn-popular-7000032269/*

***What are containers?*** Containers differ from VMs in that they provide an abstraction of the OS rather than an entire dedicated OS. In a VM environment, multiple VMs are running, each with an instantiation of a full OS that is created and managed by the hypervisor (a virtual machine monitor). Each instance of a VM is heavily isolated from the others. A container has only one OS, and each instance of the container shares the single OS kernel. This significantly reduces an application's resource needs.

***Why use containers?*** Because of their "lightweight" nature, containers can be started faster, require fewer resources, and allow more applications to run on a physical host. A container can be started much faster than a VM because no additional OS needs to boot

up; the time savings can be significant because a VM needs additional configuration when booted for the first time. A recent PricewaterhouseCoopers analysis notes that, while a traditional VM takes over 30 seconds to boot, a container can start in a tenth of a second. (Morrison & Riznik 2014) However, the savings are less meaningful in cases in which new instances are rarely needed.

In comparing the KVM (Kernel-based Virtual Machine) tool for Linux to LXC (Linux Containers), IBM researchers found that VMs are only half as fast at random memory input and output as containers running applications on the native OS. (Felter et al. 2014) The researchers also found that random memory read latency increased by two to three times, while containers maintained the same performance as a native application. Finally, a physical host can run four to six times as many containers as a VM when tuned appropriately. (Vaughan-Nichols 2014)

In addition to scale, containers make it easier to deploy applications. Applications are written specifically to run within the container. By doing this, a standard interface may be used to communicate with multiple resources outside the container, such as a database. A developer simply writes an application to function within a container, as opposed to developing the application to also communicate directly with various outside resources, leading to a simpler and cleaner development process. Additionally, if the development, test, and production environments all run the same container, then updates to applications can be done seamlessly. Containers could also lead to easier movement of applications between disparate clouds.

In a way, developing an application for a container environment is much like loading a shipping container: one entity packs the container without having to worry about things like shipment method (e.g., ship, truck, train), and the transport provider moves the container from one location to another without needing to understand what is inside the container. Containers are an advancement in virtualization that furthers the innovations provided by VMs.

| Features of Virtual Machines and Containers | | |
|---|---|---|
| Feature | Virtual Machine | Container |
| Time taken to start up | Substantially longer: Boot of OS plus app loading | Substantially shorter: Only apps need to start because OS kernel is already running |
| Memory on disk required | Complete OS plus apps | App only |
| Process Isolation | More or less complete | If root is obtained, container host could be compromised |
| Container Automation | Varies widely depending on OS and apps | Docker image gallery; others |

*Source: Microsoft (azure.microsoft.com/en-us/documentation/articles/virtual-machines-docker-vm-extension/)*

***What are the limitations?*** Containers have limitations. Each container can support only one application at a time. Additionally, containers provide less isolation than VMs, causing additional security considerations. While VMs are separated by the hypervisor, containers are separated by kernel-level functionality such as Linux kernel containment. (LCX 2014) Sharing physical hosts with non-Department of Defense (DoD) tenants is not advisable at this time. Because containers do not provide a complete OS, they rely on the underlying OS to provide specific functionality. Currently, the most widely used container software runs only within a Linux environment, which means that only applications that run in a Linux environment can run in a container. However, this is changing. Microsoft is developing additional container support for Windows Server and the Azure cloud service. (Zander 2014) Although this currently limits the utility of this particular program, it does not limit the utility of the container approach in general.

***Docker 1.0***

*Container support is growing rapidly across the industry. For example, Google uses containers for its own infrastructure, running everything in a container, with over two billion containers started each week. With the release of Docker 1.0, a new open-source container technology, more companies are moving toward the use of containers in their data centers and cloud environments. From financial institutions to software companies, Docker is bringing standardization to container technology in the market place. Major companies supporting Docker include Microsoft (Azure), Google (Compute Engine), Red Hat (OpenShift), and Amazon (Web Services). Even virtualization provider VMware has plans to integrate containers into its services. (Vaughan-Nichols 2014)*

***What does this mean for DoD?*** A container approach is useful for applications that run in a cloud environment that otherwise might comprise numerous VMs running in parallel. It greatly increases efficiency. Writing applications to work within a container environment would allow better resource utilization on physical hosts and provide easier deployment of applications in a consistent environment. When utilizing third-party hosting solutions (on dedicated hosts for security), containers provide a common framework for moving applications between cloud providers, which is critical in avoiding vendor lock-in and could be used for continuity of operations. However, the barrier between containers is thinner than that between VMs, so policy on containers must be implemented accordingly.

***What are the policy implications?*** Because containers are a relatively new technology, little policy guidance is available to guide those wishing to use this technology to manage the risk or employ it in a way that is interoperable across DoD. On the cloud service provider side, the DoD Chief Information Officer (CIO) should request that the Defense Information Systems Agency (DISA) assess the feasibility of offering a container-

compatible service. The service would involve the ability to run containers in the DISA or third-party cloud environment and the capability to orchestrate the instantiation and shutdown of container instances. Because some DISA-provided services might be run more efficiently in containers than VMs, DISA should report on the feasibility of converting some services to run in containers within the next five years. DoD CIO, DISA, and interested Combatant Commands/Services/Agencies should create a policy for a standard implementation of containers that is conducive to use across the DoD. Based on enabling the consumer-driven needs for containers, DISA should develop guidance for the secure development, configuration, and administration of container-based applications.

**References**


Felter, Wes, Alexandre Ferreira, Ram Rajamony, and Juan Rubio. "An Updated Performance Comparison of Virtual Machines and Linux Containers." *technology* 28 (2014): 32.

LCX, "Linux Containers." LinusContainers.org. www.linuxcontainers.org (accessed December 14, 2014)

Morrison, Alan and Pini Riznik. "Containers are Redefining Application-Infrastructure Integration." Technology Forecast: Rethinking Integration, Iss. 1. PWC.com. 2014. www.pwc.com/technologyforecast (accessed December 2014)

Vaughan-Nichols, Steven J. "What is Docker and why is it so darn popular?" zdNet.com. August 4, 2014. www.zdnet.com/what-is-docker-and-why-is-it-so-darn-popular-7000032269/ (accessed December 14, 2015)

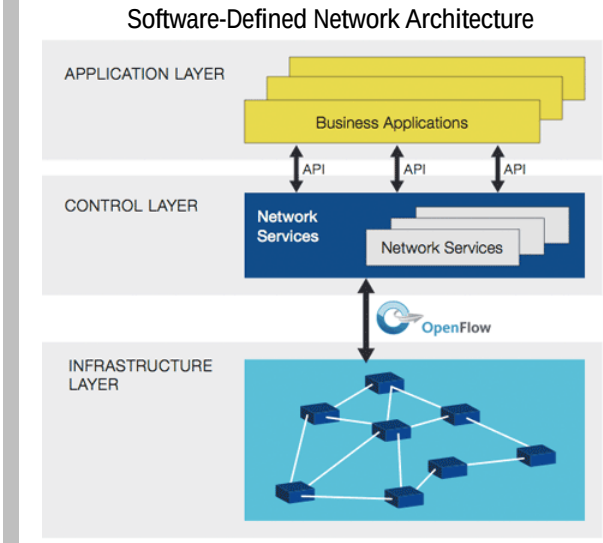
Zander, Jason. "New Windows Server containers and Azure support for Docker." October 15, 2014. azure.microsoft.com/blog/2014/10/15/new-windows-server-containers-and-azure-support-for-docker/ (accessed December 2014)

# Software-Defined Networking: A New Network Architecture

Mobile devices and content; cloud services; and end point, application, and server virtualization are putting significant stress on today's hardware-centric network designs. Changes in a virtual environment can require reconfiguration of routers and switches within a network. Network providers are moving away from static network configurations to a more flexible and agile approach that will allow administrators to dynamically reconfigure the network through software and application programmatic interfaces (API). This approach, called *software-defined networking*, has the potential to change how networks are architected, deployed, and operated.

***What is software-defined networking?*** Software-defined networking decouples the control and data planes (i.e., the software and hardware), allowing the network to be treated as a virtual entity. The software-defined network (SDN) environment uses open APIs to support all services and applications running over the network. This allows the network administrator to manage services and applications without having to touch individual switchers or routers. (SDX Central 2014)

***How does an SDN work?*** The core building blocks for an SDN are the controllers, switches, and network overlays. The SDN controller shifts network programming from a distributed model (device to device) to a centralized model (controller to device). It discovers the topology of the network switches and acts as the middleware between the applications and the switches, programming the forwarding tables of the hardware and software switches. The overlays are used "to create network containers that are logically isolated from one another while sharing the same physical network." (Banks 2013)




*Source: Open Networking Foundation. https://www.opennetworking.org/sdn-resources/sdn-definition*

The breakthrough in software-defined networking came in 2008 with the development of an open standard for a network protocol called OpenFlow. OpenFlow facilitates communication between the controller and the switches, separating the heavy lifting of networking from the simple table lookup portion. Because it does not need to do com-

plex processing, which comes at a high expense, an OpenFlow switch can be an inexpensive commodity device. Each set of packets from one specific IP address port is sent, or "flows," to another IP address. Devices that implement the OpenFlow protocol have a lookup table in which flows are associated with specific actions like forward or drop. The OpenFlow device references its table to determine where a packet should be sent based on a particular stream and then performs that action. Logging is about the only additional overhead needed. In certain circumstances (e.g., when an OpenFlow device encounters a packet for which it has no associated flow instructions), the OpenFlow device will connect to a network controller to ask what action to take. The network controller acts as the brain of the network.

***Why use software-defined networks?*** A protocol as simple as OpenFlow makes possible a number of new capabilities. As mentioned previously, because most of the complex processing is removed from the OpenFlow switches, they can be very inexpensive commodity devices.

A software-defined network can also be reconfigured on the fly. This means more robust networks that better tolerate failure and route around congestion. Applications can dynamically architect the network in real time. This can be done to create the appearance of a virtual network running on top of a physical network. This strategy can be used to isolate one application's network traffic from another's and to allow applications—and their associated networks—to be moved from one data center to another. This latter technique was used after the Fukushima disaster to keep applications running despite rolling blackouts. (ESG Global 2014) SND also allows for rapid deployment of new applications, services, and infrastructure because network configuration can be handled through the controller.

Software-defined networking has the potential to greatly increase utilization of existing network resources. A recent Google white paper describes Google's successful deployment of an SDN in its back-end corporate network, which supports its data centers. The paper documents network performance gains from an average of 30 percent network utilization to an almost 90 percent sustained network utilization after deploying the software-defined network. (LCX 2014)

***What are the limitations of software-defined networking?*** There are a few things to consider with respect to SDNs. First, this is an emerging architecture that industry is only beginning to use, and much of the work at this time has been focused on gaining data center efficiencies, not enterprise services. Since all information goes through the controller, scalability has been identified as a concern, but companies such as Google have been able to implement it on a large scale. There are security impacts with regard to SDNs. An SDN can provide and enforce a security strategy for the network, but this strategy is dependent on how well the SDN itself is protected. The benefits that are derived from network programmability and centralized control also provide new threat vec-

tors that could compromise the network if security is not designed properly from the start. (Kreutz et al. 2013)

***What are the implications for the Department of Defense (DoD)?*** Implementing SDNs will require DoD to consider feasibility, standards, and security. The Defense Information Systems Agency (DISA) should examine the feasibility of using an SDN for their data centers in order to improve management of the networks and utilization of resources. This has been done on a similar scale in the private sector (see sidebar). This examination should consider how software-defined networking would be implemented, given the current state of the architecture, and using various alternative vendors to ensure that vendor lock-in does not occur, and it should examine the costs of implementation.

DoD should encourage DISA and NSA to work with the National Institute of Standards and Technology (NIST) and the standards organizations to continue to flesh out and push for standards to ensure a competitive marketplace. This is particularly important for DoD to achieve cost savings. New technology presents an ever-changing environment in which protocols must adapt and respond. Controllers with proprietary protocols will face challenges in keeping current with those changes, resulting in additional costs. While OpenFlow is the current standard, vendors are already exploring proprietary features that can be used only with their own equipment. Finally, DoD should task NSA to examine the security risks of software-defined networking. As mentioned previously, using an SDN will result in new threat vectors, and it is important to identify these vectors before implementation in order for the SDN to be secure.

***Google: Building an SDN***

*Over the past four years, Google has been using a software-defined wide area network (WAN) to connect multiple data centers across the world. The decision to move to an SDN was based on the inability of the traditional WAN architecture "to achieve the scale, fault tolerance, cost efficiency and control required for [the] network." This is one of the largest software-defined networks deployed to date. (Jain et al. 2013)*

*At the time the project started, none of the network devices on the market had OpenFlow support or could meet the scale requirements. As a result, Google built its own network switches to use in the WAN. Due to the relative newness of OpenFlow, it was not clear what functionality needed to reside in the controller and what needed to reside in the network device. Google found that for a large-scale network, programming individual flows can take a long time and bottlenecks occurred when moving packets from the control plane to the data plane. (Google 2014)*

*Google's SDN WAN demonstrates an effective approach for gradually introducing SDN infrastructure into an existing network. Google has realized many of the efficiencies it sought to achieve with its SDN. The WAN has enabled cost savings in the WAN bandwidth, running many links with almost 100 percent utilization. (Jain et al. 2013)*

**References**


Banks, Ethan. “SDN: The Core Building Blocks.” NetworkWorld.com. June 28, 2013. www.networkworld.com/article/2167704/lan-wan/sdn--the-core-building-blocks.html (accessed November 2014)

ESG Global. “VMware Acquires Nicira to Bolster Software-Defined Data Center.” ESG-Global.com. www.esg-global.com/blogs/vmware-acquires-nicira-to-bolster-software-defined-data-center/ (accessed December 2, 2014)

Google. “Inter-Data Center WAN with centralized TE using SDN and OpenFlow.” OpenNetworking.org. www.opennetworking.org/images/stories/downloads/sdn-resources/customer-case-studies/cs-googlesdn.pdf (accessed November 12, 2014)

Jain, Sushant, Alok Kumar, Subhasree Mandal, Joon Ong, Leon Poutievski, Arjun Singh, Subbaiah Venkata et al. “B4: Experience with a globally-deployed software defined WAN.” In *Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM*, pp. 3–14. ACM, 2013.

Kreutz, Diego, Fernando Ramos, and Paulo Verissimo. “Towards secure and dependable software-defined networks.” In *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking*, pp. 55–60. ACM, 2013.

SDX Central. “What is Software Defined Networking (SDN)?” SDXCentral.com. www.sdxcentral.com/resources/sdn/what-the-definition-of-software-defined-networking-sdn/ (accessed November 12, 2014)

# De-Perimeterization: Removing the Network Perimeter

The concept of a network perimeter has been dead for years, but many have not noticed. In addition to the failure of the perimeter model to provide adequate security, two factors have contributed to killing the corporate perimeter as we know it: (1) a mobile workforce (via laptops, tablets, and phones) and (2) outsourcing services (e.g., travel, expense reporting, health care, and payroll) to third-party providers. Laptops frequently cross from inside the enterprise perimeter to outside the perimeter and back again, increasing the risk of malware contamination. Mobile devices (e.g., smart phones or tablets) generally stay outside the enterprise perimeter and access enterprise services through limited interfaces like an encrypted web service. Finally, to reduce costs, companies are increasingly using third-party providers to handle services that are not part of their core functions. These factors have resulted in changes to network perimeters that have affected security for the entire network. The effect of these factors on the network environment is referred to as de-perimeterization.

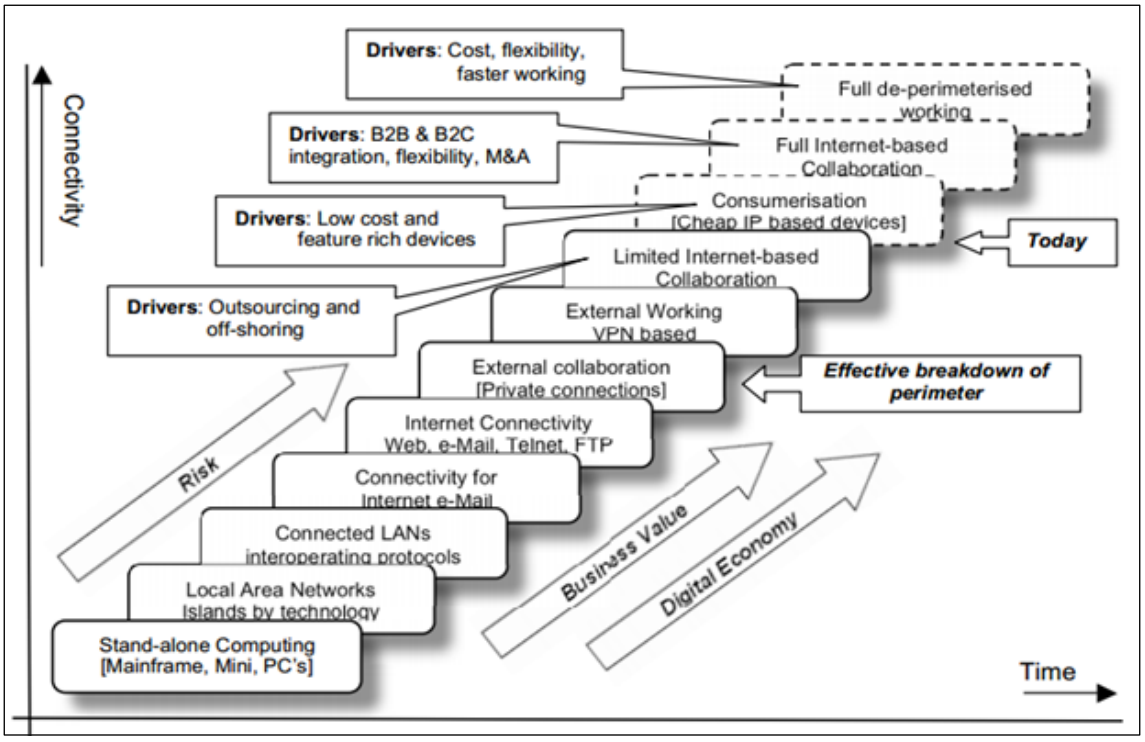
***What is de-perimeterization?*** De-perimeterization is a term coined by the Jericho Forum to "describe the erosion of the traditional 'secure' perimeters, or 'network boundaries,' as mediators of trust and security." (The Jericho Forum 2006) It represents the diffusion of the strict boundaries between the internal and external network. It leverages access controls, encryption, and newer types of information technology (IT) services to ensure that devices (and their users) have the exact same experience regardless of whether they are inside or outside an enterprise network while protecting IT assets from unauthorized users. De-perimeterization does not require the removal of firewalls and intrusion prevention systems, but it acknowledges that a perimeter security-based model of "crunchy-exterior-with-a-chewy-interior" networks is outdated.

De-perimeterization requires organizations to authenticate and encrypt all IT services, which are made available on a least privilege basis (i.e., being inside the network perimeter does not itself allow one unfettered access to organizational crown jewels). Some services that are available only within the network perimeter or via virtual private network (VPN), like a network storage drive, must be changed out for alternative services that operate in the same way regardless of network location (e.g., cloud-based storage with local drive synchronization).

***Why de-perimeterize?*** Much of the currently deployed technology is aimed at securing organizational borders through perimeterized networks. But more modern technology is being driven by the demand for connectivity outside of the network. Operating models are changing to reflect a distributed workforce at different locations, data exchange both

within and across organizations, and many, complex, and often conflicting, compliance mandates. Correspondingly, IT risks are changing due to several factors, including the ability to access data in real time, no matter where the user is located, and the move of applications and data to the cloud. (McCumber 2008)

Most networks with a hardened perimeter model continue to layer on solutions for problems that arise with the implementation of new technologies. As a result, the perimeter "eventually becomes hardened to the point that it negatively impacts the ability of the business to react effectively to new opportunities or to conduct business," according to Ido Dubrawsky, Security Advisor at Microsoft. At the same time, industry is beginning to realize that "traditional firewalls and perimeter defenses are increasingly unable to defend against malicious software that uses the Web or email as a transport medium." The de-perimeterization approach alleviates issues with the current hardened perimeter model while simultaneously enabling new technologies.




*Source: Jericho Forum*

De-perimeterization enables new ways of working and collaborating without the perimeter impeding business. It allows direct business-to-business integration, partners and contractors to directly access the data they need (and have the authorization to access) as if they were physically connected, direct electronic interaction with customers, and local connectivity in offices without the network infrastructure that is expensive and hinders performance. But this collaboration comes with a requirement for increased security, which involves implementing access controls and encryption that make lateral movement within a network much more difficult. (The Jericho Forum 2007)

***How does it affect security network?*** In a de-perimeterized network, security controls are shifted from the network to the end-points, data centers, information repositories, and applications. An implication of de-perimeterization is the movement of data and services from end-user devices to data centers, where they can be contained and monitored more easily. De-perimeterization assumes that everyone is untrustworthy, and so the concepts of identification, authentication, and authorization become very important. These concepts are applied at all levels, from user devices to application services to critical information assets. Security becomes a guiding principle for the network and is built into the architecture rather than layered onto it. As a result, a de-perimeterized network is more secure, since users and devices are authenticated and access to services and data is controlled.

***What does this mean for the Department of Defense (DoD)?*** De-perimeterization is already occurring across DoD. Most organizations provide the ability to link laptops to the network through the Internet; third-party providers are providing key services to DoD and need to be able to pass data through the firewall to their own network; and smartphones are routinely used for sending and retrieving email. DoD needs to acknowledge the metamorphosis to de-perimeterization. But moving to a de-perimeterized network does not happen quickly. A likely first step is to begin to introduce device authentication, which requires an inventory of DoD IT assets.

***What are the policy implications?*** DoD policy should de-emphasize the relative importance of perimeter security and secure enclaves. Instead, host-based mechanisms for ensuring security should begin to take up the slack. Simultaneously, policy should enable user mobility via migration of services (e.g., network storage) from desktops to data centers. Access to services should be individually authenticated and encrypted and provided in a manner that does not require a VPN. Methods of device authentication should be implemented to augment user authentication.

***Eliminating the Corporate Perimeter***

*Google has implemented a new security model in their "Beyond Corp" technology project. The mission of the Beyond Corp project is to "re-architect corporate services to remove any privileges associated with having a corporate network address." This model moves security away from the perimeter down to the packet, or transaction, level. It allows users to access the corporate network anywhere. The notion of a corporate perimeter no longer applies.*

*Google utilizes both user and device authentication—authenticating and authorizing users only after their devices have been verified as belonging to the Google inventory and as being in a secure state. The requirement for device authentication has a couple of desirable side effects. First, it ensures that only approved devices can access sensitive resources. Second, it dovetails with the need for a current inventory of approved devices. (Gannes 2013)*

**References**


Dubrawsky, Ido. “The ‘De-perimeterization’ of Networks.” TechNet, Microsoft, Inc. September 12, 2007. technet.microsoft.com/en-us/library/cc512604.aspx (accessed November 2014)

Gannes, Liz. “Google CIO Ben Fried on How Google Works.” Allthingsd.com. October 10, 2013. AllThingsD.com/20131010/google-cio-ben-fried-on-how-google-works/ (accessed January 2015)

The Jericho Forum. *Architecture for De-perimeterisation*. April 2006. collaboration.opengroup.org/jericho/Architecture_v1.0.pdf (accessed November 2014)

The Jericho Forum. *Business Rationale for De-perimeterisation*. January 2007. www.jerichoforum.org (accessed November 2014)

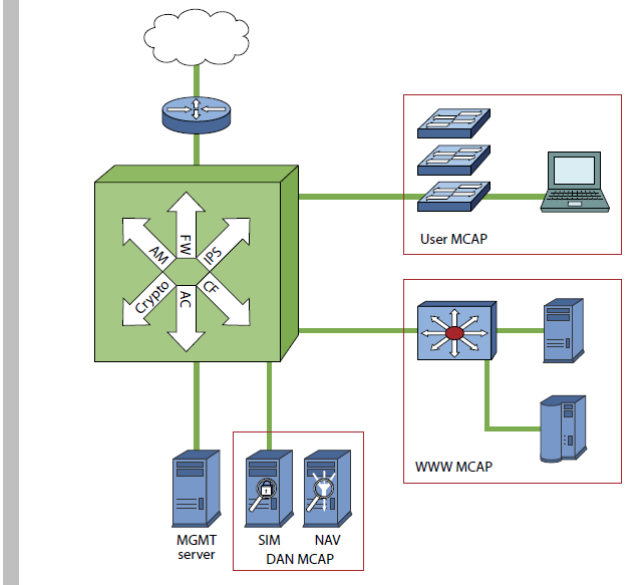
Kindervag, John. “No More Chewy Centers: Introducing the Zero Trust Model of Information Security.” Forrester Research, Inc. November 15, 2012.

McCumber, John. “De-Perimeterization: Protecting and Managing Endpoints and Mobile Data.” Symantec Government Symposium. July 31, 2008.

# Zero Trust:
# An Alternative Network Security Model

Traditional network security is based on the concept of a network perimeter with limited access points into the network that only allows trusted users in. Once inside, users can gain access to any number of resources on the network. This perimeter-based model of security relies on the assumption that everyone and everything inside the perimeter can be trusted. It is not adapted for remote employees, mobile users, or cloud computing, where the boundary between internal and external networks is blurred. Modern network security must also address increased use of wireless technologies, increased data sharing with partner organizations through the network, and the need to support guest users. Most concerning of all is the rise of insider threats, whether intentionally malicious or just careless. (Palo Alto Networks 2014) As a way to combat the eroding network perimeter, an alternative network security model, referred to as Zero Trust, has been proposed.

***What is Zero Trust?*** Developed by Forrester Research in 2010, around the same time the idea of network de-perimeterization was gaining interest, the Zero Trust model takes into account both external and internal threats, ensuring that malicious insiders cannot access information they are not authorized to access, thus reducing the exposure of vulnerable systems and preventing the lateral movement of threats throughout the network. Zero Trust is built around three key concepts: (1) ensure that all resources are accessed securely regardless of location; (2) adopt a least privilege strategy and strictly enforce access control; and (3) inspect and log all traffic. (Forrester Research 2014) In the Zero Trust model all network traffic is treated as untrusted. Instead of trusting users and their devices to do the right thing, the security model verifies that they are doing the right thing. (Kindervag 2010a) This means that no entity on the network is trusted based solely on network location, including users, devices, transactions, applications, and packets.



*Source: Forrester Research, 2010*

A proposed Zero Trust network architecture is built around a segmentation gateway (SG), which is used to define trust boundaries. It takes all

the functionality found in individual, standalone security products (e.g., intrusion prevention systems, web application firewalls, network access control, virtual private network (VPN) gateways) and embeds them into the SG along with a packet-forwarding engine. This moves security from a unified thread management (UTM) design, which is a perimeter control, to an embedded security design. (Kindervag 2010b)

The SG defines global policy and links to trust zones, referred to as the micro core and perimeter (MCAP) by Forrester, which are "distinct pockets of infrastructure where member resources operate at the same level of trust and share functionality" (e.g., user, database, and application MCAPs). (Palo Alto Networks 2014) A centralized management infrastructure handles administration and monitoring of the network. Since an essential concept of Zero Trust is that all traffic on the network is logged and inspected, the SG is supported by a data acquisition network (DAN) that supports the monitoring and analysis of network traffic. The DAN "facilitates the extraction of network data…to a single place" where it can be inspected and analyzed in near real time. (Kindervag 2010b)

***What are the benefits?*** One of the major benefits of using a Zero Trust security model is the improved management and fine-grained control of the security of the network. With centralized security via the SG, it becomes easier to enforce security compliance across all users, devices, and applications and easier to identify all traffic by user, device, and application, allowing full visibility and control of network resources. It is possible to augment an existing hierarchical network with a Zero Trust subnetwork, which can be extended over time to gradually replace the existing network. (Kindervag 2010b)

Zero Trust principles apply from the network layer up through the application layer and can be used not only for validating network devices and resources but also for authenticating transactions.

Zero Trust is intended to provide a secure foundation for the extended enterprise (e.g., users, devices, cloud services, other service providers, partners, and supply chain). If every user, device, and access point can be inspected and logged, policies and controls can be created to discover and mitigate misuse and abuse of consumer technologies (e.g., smartphones, tables, social media). (Tanzi 2014) Rather than removing perimeters, the Zero Trust model adds inspection of data in transit everywhere within the enterprise. (Palo Alto Networks 2014)

***What are the limitations?*** Current security architecture designs overlay controls on the network; Zero Trust is a departure from that approach in that it embeds security into the heart of the network. As a result, shifting from a perimeter-based security model to a Zero Trust model will not be easy. Zero Trust networks must be built from the inside out, and not all components of Zero Trust architecture are available today, although there are vendors who support least privilege access control, inspection of all network traffic, and advanced threat technologies components.

With the addition of SGs and MCAPs, implementation would require a significant scale-up in the form of network complexity, security monitoring, logging, and security information and event management (SIEM) capabilities. To keep costs down, an organization should consider first applying the Zero Trust Model to end-user and peripheral-device networks and to the highest security portions of a network. This will achieve higher impact at lower cost in a shorter time than trying to apply Zero Trust principles across the enterprise.

Finally, the market place for Zero Trust technology is evolving, and not all features of the SG as proposed by Forester are available. (Kindervag 2013) To date, most companies focus on the end-user environment. Not much work has been done on the backend environment.

***What does this mean for DoD?*** DoD should consider Zero Trust as a possible security model, given the sensitive nature of the data it processes. However, two critical factors must be addressed before implementing Zero Trust. The first is the requirement for multifactor authentication and trusted identity; the second is a device inventory, which is critical to ensuring that devices can properly authenticate.

***Zero-Trust in Practice***

*With recent data breaches, such as those at Target and Home Depot, Zero Trust security concepts are becoming more popular with organizations that store or process credit card infomration, health information, and other sensitive data. Netflix is one of the companies moving toward a Zero Trust network architecture for its campus network services. Netflix's goal is to provide employees with the same IT experience, whether at Netflix headquarters, a local coffee shop, or home. This mobile culture extends to upper management—the VP of IT Operations does not have an office and works wherever he needs to be, using his phone, tablet, or laptop. Such mobility requires a security model that ensures that the personal data from almost 2 million subscribers cannot be accessed by unauthorized users. Netflix is implementing certificate-based authentication, logging all network activity, and creating dashboards to monitor network activities. (Amplify Partners 2014)*

Also, the way information technology (IT) services are delivered will need to be rethought. As an example, consider the typical network drive. The drive can only be mounted/accessed when the device is logically (e.g., on a VPN) on the internal network. However, the Zero Trust model requires that access be the same regardless of where the device is on the Internet. This can be addressed by using a different type of file service, one in which the file service is available anywhere and all transactions are authenticated and encrypted. This would look much like Dropbox, Box, Google Drive, or Microsoft OneDrive.

To implement Zero Trust, DoD will need to change the way it thinks about trust and create a dialogue among the Defense Information Systems Agency, the National Security

Agency, and other major IT stakeholders about Zero Trust and how its core concepts can be built into the network. Zero Trust pairs well with other technologies such as network de-perimeterization and cloud-based applications. DoD should begin to integrate Zero Trust concepts into future planning for its IT services and infrastructure.

DoD should implement a pilot, building a small Zero Trust enclave in a space where it can be expanded to include additional nodes quickly, once it is satisfied with testing.

**References**


Amplify Partners. "Netflix VP of IT on the Future of Infrastructure." March 12, 2014. www.amplifypartners.com/interviews/netflix-vp-of-it-on-the-future-of-infrastructure/ (accessed November 5, 2014)

Forrester Research. *Developing a Framework to Improve Critical Infrastructure Cybersecurity*. National Institute of Science and Technology, April 8, 2014.

Kindervag, John. *No More Chewy Centers: Introducing the Zero Trust Model of Information Security*. Forrester Research. November 15, 2010.

Kindervag, John. *Build Security into Your Network's DNA: The Zero Trust Network Architecture*. Forrester Research. November 11, 2010.

Kindervag, John. *Market Overview: Network Segmentation Gateways, Q4 2013*. Forrester Research. December 12, 2013.

Palo Alto Networks. *Getting Started with a Zero Trust Approach to Network Security*. Retrieved November 5, 2014. PaloAltoNetworks.com. www.paloaltonetworks.com/resources/whitepapers/zero-trust-network-security.html (accessed January 2015)

Tanzi, Tony. "Establishing a Zero-Trust Infrastructure," CommSolutions.com. www.commsolutions.com/blog/establishing-zero-trust-infrastructure/ (accessed November 7, 2014)

# IDA Mobile Thin Client End Points

In the early days of computing, the user sat in front of a terminal connected to a central server, which controlled the data and applications. The rise of the personal computer (PC) moved computing to the end user, with applications and data residing on the end point. With ubiquitous high-speed networks, virtualization, web-delivered applications, cloud-based storage, mobile apps, and increasing security challenges, applications and data are moving back to a central server or data center that the user connects to via mobile devices, web-based applications, or virtual desktop interfaces (VDI) to access their resources.

***What are mobile thin clients?*** A thin client is an end-point computer whose "main or sole function is to process keyboard input and screen output and which accesses most or all application programs and data from a central server via a network." (LIP 2014) Thin clients typically store configuration files and the operating system on flash memory—no other data is stored locally—and they connect to resources hosted in a data center. However, the mobile thin client takes the paradigm further by using a reduced (smaller with limited functionality), hardened operating system (OS) and relying on web interfaces, application streaming to the browser and VDIs to access resources. Mobile thin clients need a network connection for application and data access under most circumstances; however, advancements in offline web-delivered applications are evolving rapidly and becoming viable for applications such as email, word processing, and spreadsheets.

***What are the benefits of mobile thin clients?*** Mobile thin clients are easy to administer and deploy. Updates can be done securely and automatically. Security and usability are enhanced due to data and applications residing in the data center. A hardened, reduced OS at the client means reduced vulnerability to malware. (ITRG 2013) Applications are web-based or streamed from a data center, so users are always up to date when opening applications, thus reducing expensive and ineffective patching operations. Users are able to easily log into any mobile thin client at their desks, in a conference room, or at home. Since only cached local data exists, users pick up where they left off when they sign in. An added benefit is that power usage can be as low as 1/50 of thick client requirements, with potentially large cost savings over a large organization. For example, HP features a Chromebook powered by a USB plug like those used with smartphones.

***What does it cost to implement mobile thin clients?*** The end point cost of a mobile thin client is significantly less expensive than that of a traditional laptop; running around $200 to $400 versus a traditional enterprise laptop at $1,800+. Because mobile thin clients run web or streamed applications and not intensive local applications, their useful shelf life is longer—potentially 5 to 7 years instead of 3 to 5 for a laptop. Costs are low enough that it makes sense to stock extra devices versus buying expensive warranties and service

agreements. Because data is not stored locally, there is no need for "keep my hard drive" programs that add costs to laptop purchases.

| Comparison of Client Types | | |
|---|---|---|
| Mobile Thin Client | Thin Client | Thick Client |
| Easy deployment, configuration from central management console. | Easy to deploy requiring no extra or specialized software installation. | More expensive and time-consuming for IT to deploy; configuration at client required. |
| Offline capabilities allow some applications to continue to operate without a network connection. Local encrypted data storage allows for caching of application data. | Client needs constant communication with the server. | Only requires intermittent communication with server. End point provides robust technology and provides better uptime. |
| Local storage is completely encrypted and very difficult to extract data from. Tabs are sandboxed from accessing other data. | No local data storage available. Data cannot be exfiltrated from end point. | End point contains full copies of large quantities of data. Risk of data loss when device is stolen or compromised is high. |
| Applications delivered via the web use few server resources; VDI or application streaming requires more. | Require fewer resources on end point but more on servers. Server resources used at high utilization. | Requires more resources on individual end points but fewer on servers. These resources are normally idle when not running intensive applications. |
| Extremely portable because most applications are delivered via the web. | More portable in that applications are all on the server and so can be accessed from any client. | Not portable in that most resources are stored on an individual end point. Reinstallation to another end point requires time and reconfiguration. |
| Reduced security threats due to use of trusted platform module (TPM) and reduced attack surface. | Reduced security threats due to no local data storage and applications on server. | Increased security threat due to large complex operating system and applications. |

*Adapted from http://www.viewsonic.com/us/news/technology-trends/thin-client/, Mobile thin client content via IDA.*

While costs are greatly reduced at the end point, they are increased in the data center. Additional servers are required to run applications rather than on the end point, and many choose to simultaneously enhance security in the data center since all applications and data are now stored there. But, proper realignment of applications can mitigate the need for increased resources. Cost efficiencies are usually seen in large-scale implementations. (Stonecypher 2013)

Management and deployment costs are also greatly reduced. To deploy a mobile thin client, the user can be given a new one that is ready to be used; no additional configuration is required—the user only has to log in. A robust management console allows for configuration, application installation, and patching, with no end-user interaction—as opposed to deploying a PC with Windows that requires desktop images, patching, testing, and log-in from the user to continue configuration. Gartner estimates the annual support cost for a PC laptop to be $3,400 to $5,900, depending on the quality of management and configuration. (Gartner 2014) The cost to maintain a mobile thin client is an order of magnitude below that.

***What are the limitations of mobile thin clients?*** Mobile thin clients are not always the best choice in certain situations. Resource-hungry applications, such as video and graphic applications, can considerably slow down the performance of the client due to the large amount of network traffic they generate. (ITRG 2013, Stonecypher 2013) However, recent advances suggest this might be a short-term problem. Adobe recently released a cloud version of Photoshop, proving that heavy graphics applications are viable for delivery via the web.

Latency in the network or lag issues can also affect performance. The network needs to have a stable network connection, both internal and to the Internet, and with guaranteed up-time. (ITRG 2013, Stonecypher 2013) Network resources need to be properly balanced with redundant failovers; otherwise, the network can become a single point of failure, with every thin client connected to it becoming less useful should the network or critical resources on it become unavailable.

***Chromebook – A Mobile Thin Client Solution***

*Google's Chromebook is the most prominent example of a deployed mobile thin client concept. The devices are being used extensively in education as a way to reduce IT equipment costs and the level of effort required to maintain equipment and the network in schools. Similar to DoD, school districts deploy a large number of computers distributed across numerous facilities. Maintaining security on equipment that is physically distributed is difficult; the device makes it easy for IT managers to ensure that software and patches are up to date. Sharing computers is common in this environment, and the device allows users to log in and retrieve documents easily without having to spend time reconfiguring PCs to user preferences. Applications can be used only when connected to the network, and the enhanced security means that the device can used in school, at home, or anywhere a Wi-Fi connection can be found.*

***What technologies enable mobile thin clients?*** Because mobile thin clients have only minimal software that resides locally, and they are dependent upon server resources and applications, other technologies are required to make them functional. Services are delivered to the end user through a web browser; therefore, web-delivered applications or interfaces must be used. In some cases, these can be full web interfaces; in others, technologies like Citrix Receiver can be used to encapsulate desktop programs (i.e., MS Office) so they can be accessed from a client with a minimal OS. Application streaming, similar to web applications but with non-web protocols, is another means of delivering the interface of an application to the end user. However, this may require additional proprietary licensing and software on the client side. VDIs provide the user a complete desktop with applications and data, just as if they had a PC sitting in front of them. While some advantages are gained (e.g., data and app persistence and improved security), the overall advantages are diminished by the higher performance requirements of both servers and end points.

***What are the implications for DoD?*** End points are the most compromised part of the network; over 90 percent of vulnerabilities are through Java and Flash plugins on the end point. Mobile thin clients protect against these types of vulnerabilities. Since the data remains on the server, there is little opportunity for compromise due to loss of equipment (e.g., having a laptop stolen). They are also a good way to improve the management of end points, their applications, patches, and data. Updates only occur on the server, not on the device; data is always up to date on the server. In addition, it may be possible to reduce not only the costs of endpoints, but reduce facility power requirements and cost.

**References**


Gartner. "Effective Management Can Cut TCO of Desktops by 42 Percent." Gartner.com. www.gartner.com/newsroom/id/636308 (accessed January 2015)

Info-Tech Research Group (ITRG). "Thin vs. Fat: The Debate Rages On…." February 11, 2013. InfoTech.com. (accessed November 2014)

The Linux Information Project (LIP). "Thin Client Definition." Linfo.org. www.linfo.org/thin_client.html (accessed November 11, 2014)

Stonecypher, Lamar. "Reviewing the Pros and Cons of Thin Client Computing." Brighthub.com. April 3, 2013. www.brighthub.com/environment/green-computing/articles/66417.aspx (accessed November 12, 2014)

# New Trends in Mobile Broadband

Each year cellular, or mobile broadband, providers see an increasing number of mobile devices being used. It is estimated that by 2019 there will be over 9.2 billion mobile subscribers in the world, and over 80 percent of those will be for mobile broadband. (GSMA 2014) This high usage is the leading driver for technology changes that will increase capacity and reduce the cost of mobile broadband networks. Today's users require reliable, efficient, and low-cost access to mobile services.

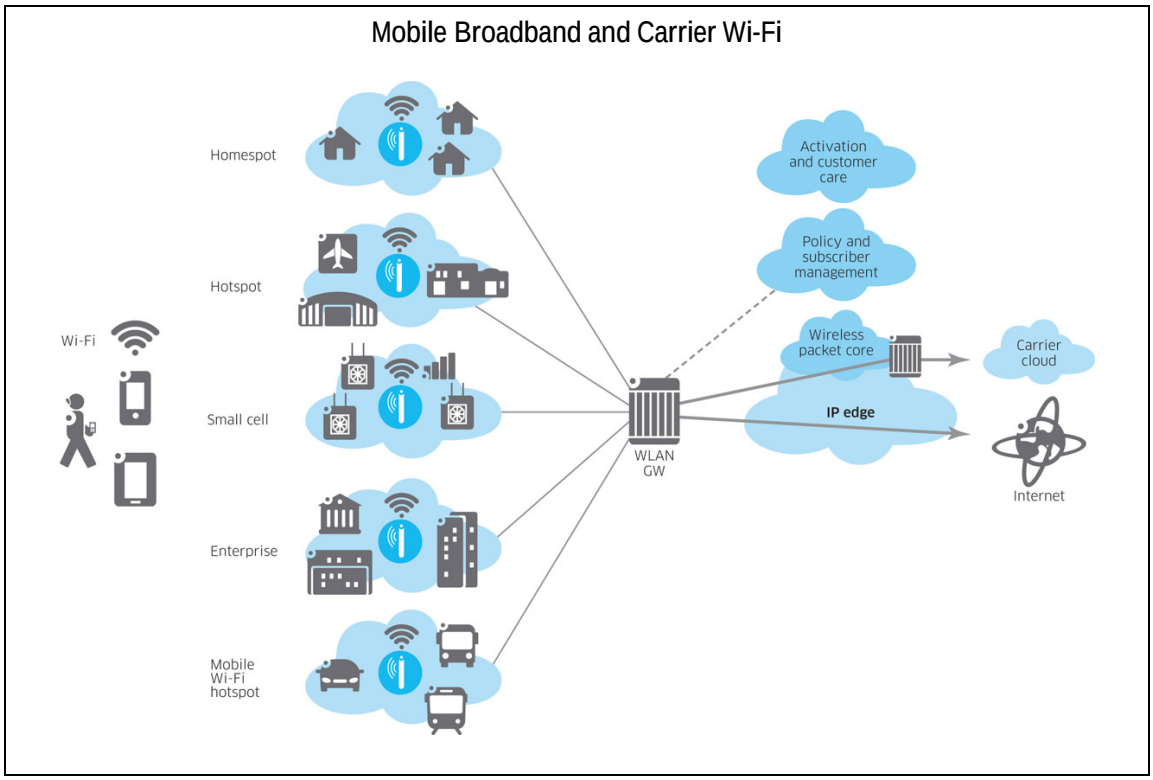
***What is mobile broadband?*** Mobile broadband technology, also called wireless wide area network (WWAN) technology, provides wireless high-speed Internet access through portable devices. Mobile broadband allows users to connect to the Internet from any location where cellular services based on technologies like Global System for Mobiles (GSM) or Code Division Multiple Access (CDMA)—or their successors—are available for mobile Internet connectivity. Currently using licensed 225 MHz to 3700 MHz radio frequency bands, mobile broadband maintains Internet connectivity as the user moves from place to place. (Microsoft 2015, Weiss 2015)

Cellular phone service has gone through many iterations over the past 25 years. The first wireless Internet access became available in 1991 as part of the second generation (2G) of mobile phone technology. Through each generational evolution, mobile broadband achieved higher data transfer rates, improved the user experience, and made mobile technology a "must have" for many. (GSMA 2014) Today's fourth generation (4G) technologies using the long-term evolution (LTE) process for high-speed data for phones and other mobile devices are able to provide internet protocol (IP)-based voice, messaging, and data (i.e., anything other than phone calls and simple text messages) at speeds of up to 75 Mbps for upload and up to 300 Mbps for download. This speed means that devices no longer have to be tethered to a wired connection to download data. (3GPP 2015) Mobile-broadband networks will likely evolve into the fifth generation (5G) starting around 2020. (Norell et al. 2015)

| Evolution of Mobile Technology | | |
|---|---|---|
| Generation | Primary Services | Key Differentiator |
| 1G | Analogue Phone Calls | Mobility |
| 2G | Digital phone calls and messaging | Secure, mass adoption |
| 3G | Phone calls, messaging, data | Better Internet experience |
| 3.5G | Phone calls, messaging, broadband data | Broadband Internet applications |
| 4G | All-IP services (including voice, messaging) | Faster broadband Internet, lower latency |

*Source: GSMA Intelligence*

***What is Voice over LTE (VoLTE)?*** LTE was originally seen as a completely IP mobile broadband system to be used just for carrying data, and the mobile network operators (MNO) would carry voice either by reverting to circuit-switched 2G/3G systems or by using a form of Voice over IP (VoIP). The packet-switched Voice over LTE (VoLTE) scheme was created as a way to standardize IP-based voice traffic in a way that maintains call quality. VoLTE enables providers to transmit voice services using a single data network in the same manner they transmit data—it "chops up voice calls into packets, just as emails, Facebook messages, and all other communications over the Internet are 'packetized.'" By turning voice into IP packets, MNOs are able to offer higher-quality voice calls. (Reardon 2014) It has been suggested that VoLTE will likely serve as the foundation for telecom-grade voice and video calling services in future 5G networks that are currently under development. (Norell et al. 2015)




*Source: Alcatel-Lucent*

***What is Wi-Fi Calling?*** Wi-Fi calling allows cellular phones to operate a VoIP client to communicate with telephony switching equipment, thus allowing wireless cellular infrastructure—and its associated tolls—to be bypassed. When Wi-Fi calling is configured to work seamlessly with VoLTE calling, a Wi-Fi-equipped mobile device can automatically switch between conventional cellular and Wi-Fi VoIP modes, even during the course of a conversation, without dropping the call. If a building has Wi-Fi access, the call is handed off from the conventional mobile broadband network to the Wi-Fi LAN, taking ad-

vantage of VoIP technology to maintain the call without drop-out. (Hillier & Hillier 2011) Major MNOs are beginning to build out Wi-Fi-enabled services to their customers.

***What is carrier Wi-Fi?*** The biggest issue facing MNOs is capacity. The licensed cellular frequency band is smaller than the unlicensed Wi-Fi frequency band. As a consequence, network congestion in peak use times is not uncommon and data rates across the network slow significantly. To combat the problem, cellular providers are beginning to offload data to carrier-operated Wi-Fi networks spread across metropolitan areas; these hotspots have more capacity and higher data rates. Often, the hotspots consist of carrier-configured Wi-Fi networks running on home consumers' Wi-Fi routers. Mobile devices can be configured to automatically join these carrier Wi-Fi networks when in range. It has been estimated that by 2016 more than half of all traffic from mobile devices will be offloaded to a fixed network by means of Wi-Fi devices and cellular femtocells (very low-range, low-power base stations used inside a building to improve cellular reception). (Cisco 2015, Reeves 2013)

Carrier Wi-Fi is about more than offloading data. With the emergence of IP services over mobile broadband, cellular providers are having to rethink the way they deliver voice and messaging services. (Huet & Evans 2013) MNOs are developing their own Wi-Fi hotspots that can be used to reduce their customers' costs (e.g., data transmitted over Wi-Fi will not count towards the customer's data allocation) and, at the same time, control the quality and speed of service. Major cellular providers are beginning to offer Wi-Fi as a complement to their services and are partnering with cable communications companies to gain access to their Wi-Fi hotspots.

***Are there alternatives to mobile broadband?*** Cable communications companies are using their network infrastructure to break into the mobile broadband market. For example, Cablevision recently began providing a Wi-Fi only phone service, called FreeWheel, in the New York City area; it enables customers to bypass traditional 3G and 4G LTE cellular wireless networks for a monthly fee ($9.95 per month when bundled with other Cablevision services) that is less than those of the major cellular providers. (Weiss 2015)

In some especially remote areas, cellular towers and wired backhaul may not be practical. Companies are working to address this. In one particularly high-profile example, Google's Project Loon is experimenting with LTE service delivered from high-altitude balloons. (Google 2015) While carrier Wi-Fi brings Wi-Fi speeds to high-density areas, Project Loon brings LTE access to areas with no wireless access at all.

Broadband communication signals travel over the air via radio frequencies, often referred to as spectrum. There is no shortage of ideas for sharing spectrum. One approach is dynamic frequency selection (DFS), which allows low-powered devices to share spectrum

***Ultra-Narrowband Wireless Network***

*Sigfox, a global Internet service provider that specializes in the internet of things, is building an ultra-narrowband wireless data network in the San Francisco area. Using the 900 MHz band used by cellular phones and baby monitors to transmit a small amount of information at a mere 100 bits per second, it can support millions of connections, as compared to a cellular network, which can support faster speeds but far fewer connections. This network is designed to link anything to the network, from smoke detectors to dog collars to bicycle locks. (Churchill 2014, Fitchard 2014)*

*The cost of traditional cellular connectivity and equipment is high, so Sigfox is building an alternate network specifically optimized and priced for low-bandwidth communication, such as a utility meter or a traffic sensor that only needs to transmit intermittently and only a few of packets of data. Sigfox is talking with utilities about connected meters, with municipal governments about smart applications, and even with consumer-facing device makers about linking internet-of-things gadgets directly to its network. (Qualcomm 2015) Sigfox technology already covers all of France, most of the Netherlands, and parts of Russia and Spain. (Churchill 2014)*

with high-priority, high-power devices like radar systems. When a low-priority device detects a high-priority device using the same band, it selects a different band. (LII 2015)

As an alternative to DFS, databases of licensed radio frequency usage can be compiled. These databases might contain information such as frequency, time of day, location, and power of the radio frequency (RF) usage. In areas and at times when licensed RF spectrum is not in use by the licensee, other applications can use this "white space." One such database is already available from Google. (Google 2015) The Federal Communications Commission (FCC) is experimenting with the expanded use of white space. (FCC 2015)

It is also possible to use LTE on unlicensed spectrum, such as the 5 GHz band. This is called LTE-U. The technology allows for small-cell deployments that could ease the pressure on traditional cellular infrastructure. (Qualcomm 2015) However, LTE currently does not have the same "politeness protocol" (to not stomp on neighboring transmitters) that Wi-Fi has, so deployments of LTE-U in its current form could cause problems with existing Wi-Fi hotspots. (Reedy 2015)

***Will mobile broadband replace Wi-Fi or the other way around?*** With the proliferation of smartphones, tablets, and other mobile devices, it is often assumed that mobile broadband will eventually replace Wi-Fi as the network of choice. The reality is much different. MNOs regularly offload data to nearby Wi-Fi LANs as a way to improve their services. And with the advent of carrier Wi-Fi, it is clear that Wi-Fi complements mobile broadband—it does not replace it.

However, a more appropriate question might be: will Wi-Fi replace mobile broadband? Some believe that mobile broadband could actually go away as consumers turn toward Wi-Fi as a better mobile networking solution. In Europe, many cell phone owners are replacing mobile broadband with Wi-Fi for voice, messaging, and data. The same is not likely to occur in the United States because mobile broadband is reliable and convenient to use over long distances and in rural areas, while Wi-Fi availability, cost, and quality of service are variable depending upon location and provider. (CNN 2014)

***What does this mean for DoD?*** It is inevitable that more smartphones and mobile devices will be used within the Pentagon. A building-wide cellular infrastructure is not the answer to retrieving and sending data—even cellular service providers have recognized that cellular networks need to be integrated with local Wi-Fi networks to provide capacity, speed, and low cost to users with respect to the massive amounts of data going over the network. Seamless handoffs between mobile broadband and Wi-Fi are important, and technologies such as VoLTE will allow people to move their devices from office to office without being disconnected. Wi-Fi allows for additional network management using existing tools in the DoD enterprise, whereas a cellular deployment could either limit network management options or require additional infrastructure.

On a larger scale, DoD must be prepared to utilize an array of wireless networking technologies. A wise strategy would incorporate a mix of long-range—and probably more expensive and of lower bandwidth—wireless technologies with shorter-range wireless technologies to dynamically route application data over the proper network based on the specific application's requirements for range, bandwidth, cost control, and the physical environment in which the application is operating.

**References**


3GPP. "LTE Overview." 3GPP.org. www.3gpp.org/technologies/keywords-acronyms/98-lte (accessed March 2, 2015)

Cisco. "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2014–2019." February 3, 2015. Cisco.com. www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf (accessed March 3, 2015)

CNN. "You might not need a mobile carrier by 2020." CNN.com. November 11, 2014. money.cnn.com/2014/11/07/technology/mobile/wifi-mobile-carrier/ (accessed March 2015)

Churchill, Sam. "Sigfox Building 900 MHz M2M Silicon Valley Network." DailyWireless.org. December 15, 2014. www.dailywireless.org/2014/12/15/sigfox-building-900-mhz-m2m-silicon-valley-network/ (accessed March 2015)

Federal Communications Commission. *White Space Database Administration*. FCC.gov. www.fcc.gov/encyclopedia/white-space-database-administration (accessed March 2, 2015)

Fitchard, Kevin. “Sigfox brings its internet of things network to San Francisco.” Gigaom.com. May 20, 2014. https://gigaom.com/2014/05/20/sigfox-brings-its-internet-of-things-network-to-san-francisco/

Google. *Project Loon*. Google.com. www.google.com/loon/ (accessed March 2, 2015)

Google. *Spectrum Database*. Google.com. www.google.com/get/spectrumdatabase/ (accessed March 2, 2015)

GSMA. “Will Wi-Fi relieve congestion on cellular networks?” May 5, 2014. GSMA.com. www.gsma.com/spectrum/wp-content/uploads/2014/05/Wi-Fi-Offload-Paper.pdf (accessed February 2, 2015)

Hillier, Peter Matthew, and Katayoun Hillier. “Call processing telecommunication system and methods thereof in a WIFI network.” U.S. Patent Application 12/930,450, filed January 7, 2011.

Huet, Fredric and Sam Evans. “The Value of Reach in an IP World.” Greenwich Consulting. February 2013.

Legal Information Institute (LII), Cornell University Law School. “47 CFR 15.403 - Definitions.” Law.Cornell.edu. www.law.cornell.edu/cfr/text/47/15.403 (accessed March 2015)

Microsoft. “What is Mobile Broadband?” WindowsMicrosoft.com. windows.microsoft.com/en-us/windows7/what-is-mobile-broadband (accessed February 4, 2015)

Norell, Lennart, Anders Lundstrom, Hakan Osterlund, Henrik Johansson, and Daniel Nilsson. “Wi-Fi calling – extending the reach of VoLTE to Wi-Fi.” Ericsson Review, Vol 2015 No. 1. January 30, 2015.

Qualcomm. “Extending benefits of LTE Advanced to unlicensed spectrum.” QualComm.com. www.qualcomm.com/invention/technologies/lte/unlicensed (accessed March 2, 2015)

Reardon, Marguerite. “6 reasons why you'll eventually want voice over LTE.” CNet.com. August 30, 2014. www.cnet.com/news/6-reasons-why-youll-eventually-want-voice-over-lte/ (accessed March 2, 2015).

Reedy, Sarah. “Why Some Operators Think LTE-U is Rude.” LightReading.com. www.lightreading.com/mobile/4g-lte/why-some-operators-think-lte-u-is-rude/a/d-id/708912 (accessed March 2, 2015)

Reeves, Scott. “Pros and cons of using femtocells.” TechRepublic.com. November 11, 2013. www.techrepublic.com/blog/data-center/pros-and-cons-of-using-femtocells/ (accessed March 2, 2015)

Weiss, Todd R. “Cablevision Unveils Freewheel WiFi-Only Phone Service.” Eweek.com. January 27, 2015. www.eweek.com/mobile/cablevision-unveils-a-wifi-only-phone-service-called-freewheel.html#sthash.F0WAIS8y.dpuf (accessed February 2015)

# IDA Emerging Wireless Technologies: Faster Speed – More Data

Wireless networks are ubiquitous in our daily lives, and the desire for anytime, anywhere access with ever increasing speed and bandwidth has driven development of new technologies and ways of doing business. Recent advancements in *V-Band, or millimeter wave (MMW), communications*, have led to the development of networks with data transfer rates many times faster than those of today's wireless technology. Wireless is also advancing into the visible light spectrum to create networks where data rides on light waves, referred to as *visible light communications or Li-Fi*. While product development behind these emerging wireless technologies is only just beginning, these technologies are changing the future of mobile computing, as well as considerations for implementations of wireless networks more than a few years into the future.

***What is MMW communications?*** New short-range wireless communication devices are being developed using the unlicensed 60 GHz band (millimeter wave band). These devices can provide data transfer rates of up to 7 Gbps as compared to current Wi-Fi rates of 54 to 600 Mbps. The 60 GHz band (57 to 64 GHz) has more spectrum available—up to 7 GHz—than today's 2.4 GHz and 5 GHz wireless solutions containing up to 150 MHz. This allows wider channels with broader spectrum, enabling MMW devices to support extremely fast communications with lower power consumption. (Wi-Fi Alliance 2013) MMW frequencies have a much shorter wave length than do the RF frequencies of current wireless systems. The shorter wave length provides the potential for higher directivity of the signal which also requires highly directional antennas. (Baykas et al. 2011) Higher frequencies generally increase drop-off of signal strength, making them harder to pick up from a distance. These frequencies tend not to penetrate through walls in the same way that lower frequencies do, which affects the shielding requirements for rooms using these technologies, especially for classified networks.

There are two IEEE standards for MMW communications: IEEE 802.15.3c for wireless personal area networks and IEEE 802.11.ad (WiGig) for wireless networks designed to maintain backward compatibility with 2.4 and 5 GHz wireless communications. Both standards are very similar, although research indicates the latter is probably a better choice in many circumstances since it is backward compatible with prior versions of Wi-Fi operating on the 2.4 and 5 GHz bands. (Bhusal & Moh 2011) A third related standard is IEEE 802.11.ac, an extension of the IEEE 802.11n standard for 2.4/5 GHz Wi-Fi. This extension increases the speed of the wireless by using multi-user, multiple-input, multiple-output (MU-MIMO) technology, which takes advantage of beamforming to transmit multiple frames to different clients, all at the same time and over the same

frequency spectrum. (Cisco 2014a, Gast 2013) Depending on the number of antennas, MU-MIMO can increase the theoretical maximum wireless speeds from 3.47 Gbps to 6.93 Gbps, thereby attaining the speed of a 60 GHz network in a 2.4 and 5 GHz network. MU-MIMO allows an access point to deliver data to its clients faster than a single antenna could. (Cisco 2014a)

| Comparison of Wireless Standards | | | |
|---|---|---|---|
| Characteristics | Wi-Fi | WiGig/60GHZ | VLC/Li-Fi |
| Standard | IEEE 802.11n/ag | IEEE 802.11ad/802.15.3c | IEEE 802.15.7 |
| Operating Frequency Range | 2.4 to 5 GHz | 60GHz ISM band | 400 and 800 THz |
| Maximum Data Rate | 54 to 600 Mbps | Up to 7 Gbps* | Up to 10 Gbps* |
| Typical distance | 100 meters | 1 to 12 meters | > 10 meters |
| Antenna technology | Directional/Omni-directional | Beamforcing | LED (Optical) |
| Modulation formats | Various: Binary phase-shift keying (BPSK), Quadrature phase-shift keying (QPSK), and Quadrature amplitude modulation (QAM) | Various: single carrier and OFDM | Various: On-Off Keying (OOK), Variable pulse position modulation (VPPM), Color shift keying (CSK) |

*Source: Wi-Fi – http://www.ijert.org/view.php?id=5532&title=li-fi-technology-in-wireless-communication; WiGig – www.radio-electronics.com; VLC – http://visiblelightcomm.com/an-ieee-standard-for-visible-light-communications/*
*Rates achieved in laboratory conditions.

***What are the benefits of MMW communications?*** The greatest benefit of WiGig is the higher data transfer rates it provides. In addition, higher frequencies mean smaller components, including the antenna. Due to the smaller size, 60 GHz chipsets for MMW communications incorporate antennas directly into the chip or the package. (Daniels et al. 2010) In addition, MMW communications are considered less likely to be intercepted due to the short transmission distances and the narrow antenna beam width. (Stevens & Grafton 2011)

***What are the challenges of MMW communications?*** First and foremost, due to the need for multiple antennas and operation on a different frequency band, deployment of MMW communications will require hardware upgrades to the wireless access point and client infrastructure. However, backward compatibility of WiGig allows for a piecemeal upgrade approach. Also, MMW communications are difficult to use in non-line-of-sight environments. MMW communications suffer from faster attenuation (i.e., gradual path loss) due to the high frequency of MMW, which makes it sensitive to shadowing, or signal fading, caused by obstacles in the wave path (e.g., walls or buildings). (Guo 2007) Multipath effects can also be caused by refractions or scatterings from the ground, buildings, ceilings, or walls. These objects create two or more signal paths between the transmitter and receiver and require intense computation to separate the signal from the noise, something that only the latest signal processors have been able to do efficiently enough for commercial application. The solution to this issue is adaptive beamforming using “direc-

tional antennas to reduce interference and focus a signal between two devices into a concentrated 'beam'." (Wi-Fi Alliance 2013) The beam can be reflected off walls to maintain communication if there is an obstacle in the path of the wave, such as someone walking between two MMW devices.

***What is dynamic frequency selection (DFS)?*** Wireless devices look for the least congested channel to use, but the increase in the number of wireless devices is resulting in an ever increasing demand on available channels. As a result, the Federal Communications Commission (FCC) and vendors have turned to DFS as solution for resolving the interference with others using the same frequencies. DFS "is a mechanism that dynamically detects signals from other systems and avoids co-channel operation with these systems, notably radar systems." (LII 2015) DFS instructs the transmitter on a device to switch to another channel whenever the presence of a radar signal is detected. The transmitter continuously monitors the available operating spectrum, listening for radar signals. It will either leave the channel associated with the signal or flag it as unavailable for use. (Cisco 2015b) DFS is required for systems operating in the 5 GHz band in order to avoid radio transmissions from primary-use or mission critical systems (i.e., first responders, airports, weather stations, and military installations). (Jabbusch 2013) Since portions of the 5 GHz band are allocated to radar systems, DFS allows wireless local area networks (WLAN) to avoid interference with radar systems in situations where they are co-located. (Cisco 2015b)

***Classified Wi-Fi Networks***

*The National Security Agency (NSA) is piloting an unclassified/classified wireless network. A goal of the network architecture is to connect the networks so users from different groups within NSA can each reach back to their home network when they are collaborating in another group's space. Unclassified and classified communications share the same Wi-Fi frequencies and the same wireless and wired infrastructure until they reach the switches, which split communication traffic into the traditional unclassified or classified networks. All communications have two independent layers of encryption while broadcasting over RF and transiting through shared infrastructure.*

***What is visible light communications (VLC)?*** Li-Fi provides a multi-Gigabit short-range optical network as an alternative to the WiGig Gigabit radio frequency (RF) solution. (Li-Fi Consortium 2014) Instead of using RF, visible light is used to carry information. Light has a higher frequency than RF. (WTA 2014) It is essentially an array of flickering light emitting diodes (LED) creating a binary (on=1, off=0) data flow, which can occur at higher rates than the human eye can detect, and a light sensor to detect the data flow; the more LEDs, the more data can be transferred over the network. By using Li-Fi-equipped light bulbs, the wireless network can be extended throughout the workplace and used to augment existing networks. Since it is limited by line of sight (LOS), it will not be able to

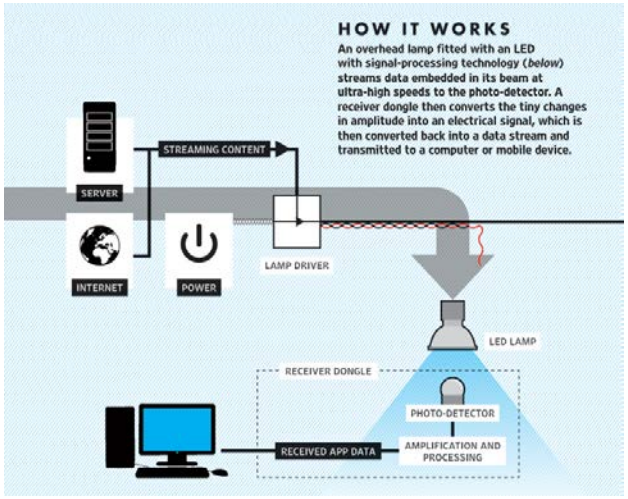
totally replace Wi-Fi. (Li-Fi Consortium 2014) A Li-Fi wireless network requires additional features to provide the same quality of service as does an RF-based wireless network. Since light cannot go through walls, rooms need to be connected with each other through a Li-Fi connector that sends the data from one side of the wall to the other through an optical fiber cable; more than one may be needed depending on the size of the room. (Li-Fi Consortium 2014)

***What are the benefits of visible light communications?*** Li-Fi has much faster data transfer rates than Wi-Fi. Currently, Li-Fi prototypes have achieved almost 10 Gbps; much higher than today's Wi-Fi or even WiGig. Even higher data transfer rates are anticipated as the technology matures. By using LEDs, which are natural beamformers, it is easy to separate uplink and downlink channels. Users must be able to see the light to access the network, thereby reducing the ability for someone outside the room or building to intercept communications. (Sawers 2014) This may be especially useful against attacks attempting to access large amounts of data.

Since light does not strongly interact with radio frequency signals, neighboring RF networks will have no impact on the network. Li-Fi can be used in situations where radio waves are banned due to interference with electronics (e.g., aircraft and hospitals). (Elgala et al. 2007)

***What are the challenges of visible light communications?*** The data receiver must be in sight of the transmitter bulb in order for Li-Fi to operate. Since light cannot go around or through walls, it is limited to LOS, although it will work through windows and with indirect or reflected light. Li-Fi cannot be used to completely replace a Wi-Fi network due to these limitations, but it can be a complementary component. (Erewise 2014) At this time, Li-Fi is still very much in the early stages of development, and it may takes years before commercial products are readily available.

Visual Light Communications (VLC)




Source: http://purelifi.com/what_is_li-fi/how-does-vlc-work/

***What are the implications for DoD?*** DoD is looking for ways to increase and expand its use of wireless communications because current wireless frequencies are growing more crowded. Warfighters have been using MMW for secure satellite and point-to-point communications for some time, and there is interest in moving these technologies into broader non-military applications. WiGig and Li-Fi are promising technologies for satis-

fying user demand for communications in Sensitive Compartmented Information Facilities (SCIF) and other closed spaces due to the decreased ability of the frequencies to penetrate walls; however, the greater capacity, agility, and flexibility provided by WiGig and Li-Fi at the endpoints may require reengineering of the network upstream to prevent bottlenecks caused by the smaller bandwidth and data transfer rates of legacy equipment. But implementing any of these technologies will require a Defense Intelligence Agency review of their security vulnerabilities.

**References**


Wi-Fi Alliance. "WiGig® and the future of seamless connectivity." September 2013.

Baykas, Tuncer, Chin-Sean Sum, Zhou Lan, Junyi Wang, M. Azizur Rahman, Hiroshi Harada, and Shuzo Kato. "IEEE 802.15.3c: The First IEEE Wireless Standard for Data Rates over 1Gb/s." IEEE Communications Magazine. July 2011.

Bhusal, Rabin and Sangman Moh. "Qualitative and Quantitative Comparison of IEEE 802.15.3c and IEEE 802.11ad for Milti-Gbps Local Communications." Wireless Personal Communications 75: 2135–2149. 2014.

Cisco. *802.11ac: The Fifth Generation of Wi-Fi*. Cisco.com. March 2014. www.cisco.com/c/en/us/products/collateral/wireless/aironet-3600-series/white_paper_c11-713103.pdf (accessed January 1, 2015)

Cisco. "FCC Regulations Update." Cisco.com. www.cisco.com/c/en/us/products/collateral/wireless/aironet-1300-series/prod_white_paper0900aecd801c4a88.pdf (accessed February 26, 2015)

Daniels, Robert C., James N. Murdock, Theodore S. Rappaport, and Robert W. Heath. "60GHz Wireless: Up Close and Personal." IEEE Microwave Magazine. December 2010.

Elgala, Hany, Raed Mesleh, Harald Haas, and Bogdan Pricope. "OFDM visible light wireless communication based on white LEDs." In *Vehicular Technology Conference, 2007. VTC2007-Spring. IEEE 65th*: 2185–2189. IEEE, 2007.

Erewise. "Li Fi Technology: Light Fidelity." Erewise.com. www.erewise.com/current-affairs/li-fi-technology-light-fidelity_art53046b047a994.html#.VIcY1mN7sjw (accessed December 8, 2014)

Gast, Mathew. *802.11ac: A Survival Guide*. O'Reilly Media. August 12, 2013.

Guo, Nan, Robert C. Qiu, Shaomin S. Mo, and Kazuaki Takahashi. "60-GHz millimeter-wave radio: Principle, technology, and new results." EURASIP Journal on Wireless Communications and Networking 2007, no. 1 (2007): 48–48.

Legal Information Institute (LII), Cornell Law School. "47 CFR 15.403 – Definitions." Law.Cornell.edu. www.law.cornell.edu/cfr/text/47/15.403 (accessed February 26, 2015)

Li-Fi Consortium. "Li-Fi Network." LiFiConsortium.org. www.lificonsortium.org/tech6.html (accessed December 8, 2014)

Jabbusch, Jennifer. “Dynamic Frequency Selection: Why It’s Critical in 802.11ac.” NetworkComputing.com. October 13, 2013. http://www.networkcomputing.com/wireless-infrastructure/dynamic-frequency-selection-why-its-critical-in-80211ac/a/d-id/1234480? (accessed February 2015)

Sawers, Paul. “Let there be Li-Fi: Meet the man who’s bringing connectivity to the world through LED.” TheNextWeb.com. http://thenextweb.com/insider/2014/08/21/purelifi-li-fi-vlc-led/ (accessed December 8, 2014)

Stevens, Mark and Grant Grafton. “The Benefits of 60 GHz Unlicensed Wireless Communications.” Sub10Systems.com. March 2011. www.sub10systems.com/wp-content/uploads/2011/03/White-Paper-Benefits-of-60GHz.pdf (accessed December 5, 2014)

Wireless Technology Advisor (WTA). “Wireless Technology Trends: Understand Them and Get Ahead of the Crowd.” Wireless-Technology-Advisor.com. www.wireless-technology-advisor.com/wireless-technology-trends.html (accessed December 5, 2014)

# Find Me, Follow Me: Leveraging Micro-Location

Widespread use of mobile devices, such as cell phones and tablets, that routinely use GPS and Bluetooth to provide continuous location information allows users to be tracked anywhere—both in and outdoors. Many applications pull information about objects, services, and people surrounding the device and at the same time push similar information to other nearby devices. Mobile devices containing these types of applications are becoming the standard, making the concept of *Find Me, Follow Me* ubiquitous in the workplace.

***What is Find Me, Follow Me (FM/FM)?*** The FM/FM concept comes from the phone industry—a result of individuals having multiple phones (e.g., office phone, cellphone) and not being tied to a specific location. FM/FM allows a caller to dial a single number and have the call routed to whichever phone the recipient might be able to answer. The Find Me service forwards calls for a user to any one of a set of phone numbers; the Follow Me service forwards calls based on a schedule. (PC Magazine 2015) When using the Find Me service, dialing a phone number may result in several phones ringing simultaneously or ringing in a sequence (e.g., office phone, cell phone, then home phone, followed by voicemail). The Follow Me service routes calls according to the calling schedule provided by the recipient (e.g., Monday through Thursday, call the office and then route to cellphone; Friday call home office). FM/FM enables finding a person without specifically knowing where that person might be—letting "the phone system" make the best attempt to find the person.

FM/FM has expanded beyond the realm of telephony to end-user devices on the network. Smartphones have pushed the concept further with applications such as Apple's Find My Friends or FourSquare, which can locate friends through their cell phones or provide information about friends who are nearby and entertainment options. By adding additional sensor and recognition technologies, the FM/FM concept can become a powerful way to increase enterprise efficiency while also using information technology (IT) resources in ideal and convenient ways. By deploying FM/FM technologies, such as indoor micro-location and identity verification, organizations may be able to decrease labor costs, increase public safety, reduce insider threat, provide indoor navigation aids, and allow meeting check-in, document sharing, and resource allocation optimization.

***What are the technologies for FM/FM?*** Indoor micro-location is the process of locating a person or object with high accuracy with respect to an indoor space. (Zafari 2015) Used in conjunction with geofencing, which provides a virtual fence around a space or building so that information going into and out of the space can be limited or controlled, indoor micro-location allows routing of phone calls to the nearest phone or office, sharing

of documents with meeting participants but not others, and checking into a space or meeting. The use of indoor micro-location began in stores and malls, but it is spreading to the health industry for patient tracking, as a navigation aid in hospitals, and as a classroom aid in education.

Micro-location sensors use a range of signals to triangulate and obtain a user's position, including Global Positioning Systems (GPS), cellular, Bluetooth, Wi-Fi, and near field communication. GPS is ill-equipped to handle micro-location indoors due to the 10-meter accuracy and need for direct-to-sky sightlines; however, newer technologies can use mobile phones and Wi-Fi access points or low energy Bluetooth to achieve very accurate locations indoors. (LocalZ 2014) Micro-location technology is already on the market. Apple's iBeacon, using Bluetooth low-energy (BLE) wireless technology, is the leading vendor for micro-location technology. The beacons are small, cheap Bluetooth transmitters. Applications installed on a cellphone use the signals transmitted by these beacons and respond accordingly when the phone comes into range. (Ranger 2015) Other innovative companies, such as Omnitrail, are finding ways to do micro-location with extremely small battery drain and high precision (<1.5m accuracy) via already active Wi-Fi traffic, using cellphones as the beacon. (Ullah 2014)

Indoor Micro-location Technology Comparison

| Technology | High Accuracy | Low Power | Ease/Cost of Deployment | User Effort | No New Infrastructure |
|---|---|---|---|---|---|
| Cell ID | ○ | ● | ● | ● | ● |
| Wi-Fi | ◔ | ◔ | ● | ◑ | ● |
| Bluetooth | ◑ | ◑ | ◑ | ◑ | ◑ |
| RFID | ● | ● | ◔ | ◑ | ○ |
| Ultrasound | ● | ◑ | ◔ | ◑ | ○ |
| Ultra-wideband | ● | ● | ◔ | ◑ | ○ |
| OmniTrail | ● | ● | ● | ● | ● |

*Source: Omnitrail*

*Meets criteria: ● Doesn't meet criteria: ○*

Identity verification technologies are an important part of FM/FM. Location is determined by device, and identity verification ensures that the correct user is associated with the device. Users in secure locations such as the Pentagon are already restricted to certain areas within the building through badge technology. Badge scanning is used to provide entry to closed spaces; however, this method depends on a human verifier within an office space. Automated entry requires stronger methods to verify that the user is who the badge indicates. Identity verification can take many forms, including facial recognition, iris scanning (available up to 3 meters away), or other biometrics. Companies such as Morphotrust are pioneering multimodal biometrics technologies (e.g., iris, finger, and

face capture capability) that are widely used at U.S. and foreign borders and ports of entry. Accuracy is now extremely high, and verification nearly instant. (Albers 2014)

***How can FM/FM technologies be used?*** Being able to identify the micro-location of an individual along with another identification factor (biometrics or badge) allows many applications.

*Automated office space entry*—Adding individuals to calendar invites for a specific office could automatically provide access to closed areas for those individuals at specified times. Entry into the closed areas using identity verification could automatically sign in an individual, resulting in the potential for removing or reassigning front desk personnel at each office space. This technology could also be used to alleviate the recurring problem of badging infrequent Pentagon visitors. When added to a meeting, the badge system could automatically reactivate a person's badge to allow access into the building, and reduce access to individuals not needing to enter at other times. The move to the use of the Common Access Card (CAC) for entry into the Pentagon would make this possible.

*Automatically share documents and resources for a meeting with participants*—Based on micro-location to within a single room, micro-location applications could identify who is present and provide access to files, printers, projectors, and contact lists.

*Automatic routing of telephone calls*—Knowing a user's micro-location could support automatic routing of phone calls to the nearest phone or, if outside the office, to the user's cellphone. Callers would no longer need multiple numbers or require access to a recipient's schedule in order to contact that person.

*Indoor navigation*—Inside large buildings such as the Pentagon, personnel often spend considerable time finding meeting locations and the appropriate entry point of a closed space. Micro-location technologies can alleviate this problem by providing maps of the building and directions to office spaces.

*Guest computers*—Similar to the roaming profiles used in previous years, FM/FM technology could allow an individual to sign into any workstation and have immediate access to his or her applications and documents.

*Insider threat reduction*—One government agency is already using micro-location tracking technology to determine whether someone in a restricted area of the building should not be there. Identity verification along with micro-location can be used to identify who is in a space and whether that person has been given access to the area. If someone attempts to enter a space she or he does not have access to, security would be alerted.

***What are the limitations of FM/FM?*** Currently, many vendors provide indoor micro-location technology, but compatibility between beacons and devices is still an issue. Most solutions are proprietary and require users to install an application or require the vendor to place software in the operating system. Many vendors merely provide "proximity to

***Facilitating Customer Service***

*OmniTrail is piloting solutions with a large EU-based retail company interested in passive presence micro-location solutions for work force and asset tracking. Leveraging the retail location's existing Wi-Fi infrastructure reduced the obstacles to implementation. This solution is enabling optimization of staff deployment, scheduling, and clock-in, bolstering internal messaging apps to facilitate more efficient customer service and provide navigation and product guides. The solution is also being evaluated for insight into in-store customer behavior.*

*The U.S. Transportation Security Administration (TSA) is working with MorphoTrust, USA to provide passport and driver's license scanners in airports as a first step toward eliminating boarding passes. TSA agents who now visually verify the authenticity of identity cards and passports will place them on a scanner that will do the verification for them. The machine would ensure that the ID card or passport is authentic and identify those that have been altered or tampered with. It will also confirm that the holder of the document is booked on a flight at the terminal, eliminating the need for a boarding pass. (Magnuson 2014)*

sensor" solutions. Few solutions provide "passive presence" capabilities that do not require the user to open an application or turn on a radio to provide their location information.

Another potential limitation with FM/FM technologies is what happens when the system doesn't work as expected. For instance, if a group is using FM/FM technologies to provide automated access and sign into restricted office spaces but a person requesting entry is not properly recognized or not added to an invitation, that person may be unable to quickly correct the situation. The former (improper recognition) is a technology issue. The latter (no invite to the meeting) is a cultural issue and may be more difficult to solve.

Privacy concerns would also need to be addressed. Micro-location technology would enable monitoring of all personnel activity. While this is useful for identifying criminal activity or locating someone within a building, location data should be treated as personally identifiable information (PII). Tracking the physical location of personnel in real time could present a personal safety issue in some cases (e.g., harassment) if location data is not properly secured. (Edquist 2014)

***What does this mean for DoD?*** With the introduction of Wi-Fi to the Pentagon, DoD should ensure that any equipment being installed has the ability to be upgraded for indoor micro-location. The potential for capability enhancement, including collaboration, access control, and customer service, is high.

Identity verification technology could improve access to the Pentagon—adding verification of known personnel (matched to badge) and flagging unknown or known undesirable persons to keep them from entering. FM/FM technology will make it easy to locate anyone within the building and track their movements throughout the building. Currently the

Pentagon has records of everyone entering and leaving the building, but security staff may not know who is in a particular space, how many individuals are in a space, or whether someone has entered a space to which they should not have access. FM/FM technologies would be useful to first responders and security personnel during a dangerous event, allowing them to identify who needs to be evacuated or whether everyone has been evacuated. DoD should begin evaluating these technologies to determine the impact they might have on operations, security, and safety.

**References**


Jim Albers (Senior Vice President, MorphoTrust), in discussion with the authors, October, 2014.

Edquist, Grace. "Micro-Location: The Next Digital Frontier?" *Madison Magazine*. April 2014.

LocalZ. "What's the best micro-location technology?" LocaZ.co. January 21, 2014. http://localz.co/blog/whats-best-micro-location-technology/ (accessed February 2, 2015)

Magnuson, Stew. "TSA System May Make Boarding Passes Obsolete." NationDefenseMagazine.com. October 2014. www.nationaldefensemagazine.org/archive/2014/October/Pages/TSASystemMayMakeBoardingPassesObsolete.aspx (accessed February 2, 2015)

PC Magazine. *Encyclopedia*. PCMag.com. www.pcmag.com/encyclopedia/term/56685/find-me-follow-me (accessed January 29, 2015)

Ranger, Steve. "What is Apple iBeacon? Here's what you need to know." ZDNet.com. www.zdnet.com/article/what-is-apple-ibeacon-heres-what-you-need-to-know/ (accessed January 29, 2015)

Shah Ullah (Chief Executive Officer, Omnitrail), in discussions with the authors, November 2014.

Zafari, Faheem, Ioannis Papapanagiotou, and Konstantinos Christidis. "Micro-location for Internet of Things equipped Smart Buildings." arXiv preprint arXiv:1501.01539 (2015). arxiv.org/pdf/1501.01539.pdf (accessed January 29, 2015)

# Building Mobility into the Classified Environment

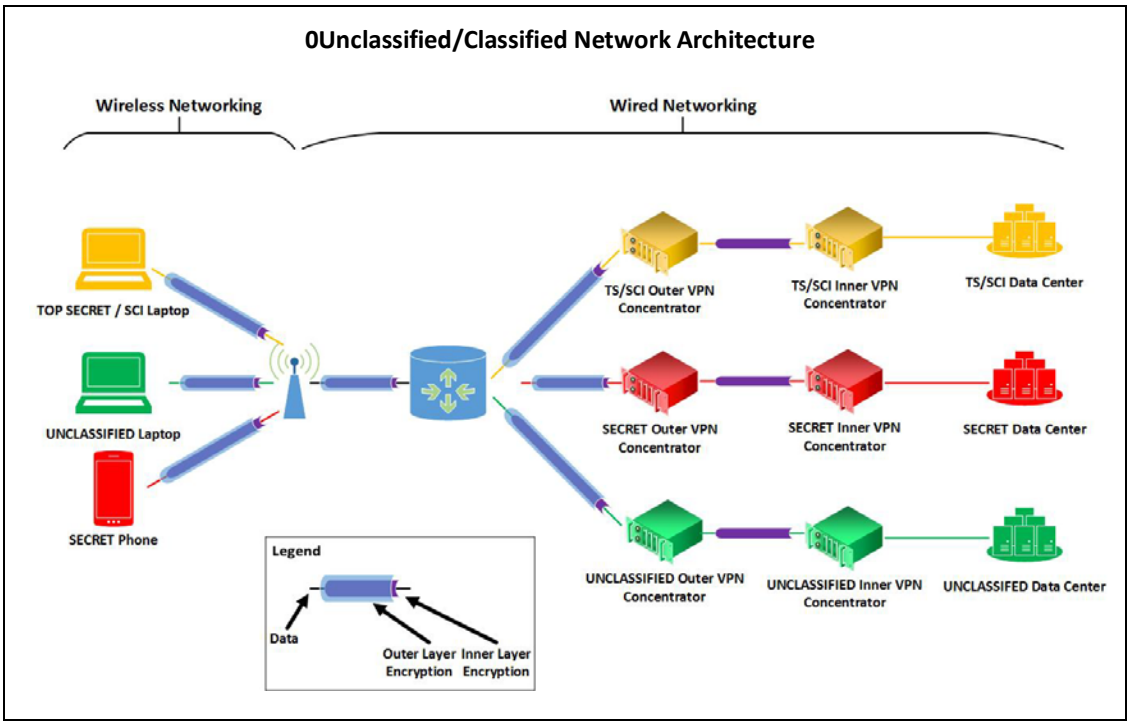
Today's demand for wireless and cellular access in the Pentagon is overwhelming. Advances in wireless and mobile broadband technology now make it possible to provide seamless mobile access to information-using commodity hardware and software. By leveraging programs within the Department of Defense (DoD), such as Commercial Solutions for Classified (network architecture) and DoD Mobility Classified Capabilities (mobile broadband), the Pentagon can be a world-class facility, providing ubiquitous wireless service anywhere, anytime, and supporting mobile wireless devices that connect all levels of classification.

***What are the relevant architecture considerations?*** Deploying an architecture that supports secure wireless communications is a key factor in enabling mobility in a classified environment. An "all-in-one" wireless network architecture currently gaining traction uses the same physical infrastructure (including Wi-Fi radio equipment) for both classified and unclassified data for Tier-1 transport. All data in transit, regardless of classification, is encrypted with two approved products from different vendors that form an inner and outer layer of encryption. This is in addition to any wireless encryption using Wi-Fi Protected Access (WPA) types of security protocols. The data at each level of classification is split out and routed to its own set of cryptographic devices (e.g., virtual private network (VPN) concentrators) that remove the outer and then inner layers of encryption. As a result, classified network isolation begins at the points at which the data is separated and routed by classification, rather than by having a physically separate classified network.

Deployment of wireless networks is only half the battle in enabling mobility—devices accessing the network must securely support the network architecture and meet all security constraints. Care must be taken to select devices that can use Wi-Fi in a sensitive compartmented information facility (SCIF) without emitting signals that could be remotely read by nearby devices. Additionally, the inner and outer layers of encryption should be wrapped and unwrapped in an environment that is strongly isolated from the user-exposed operating system. This will require new software architecture deployments on end-user devices like laptops. Additionally, if DoD moves to end-user devices that provide only thin client interfaces, additional modifications to backend architectures may be needed to provide information technology (IT) services in a form that is readily utilized by thin client mechanisms.

***Does enabling mobility make networks harder to manage?*** An architecture that combines unclassified and classified access to a large number of mobile devices requires a

different way of managing devices and content. Mobile device vendors are continually updating their operating systems and adding new features to stay competitive. Therefore, DoD IT staff need the capability to inventory hardware and applications, maintain operating system (OS) configurations, deploy mobile apps (updating, re-moving, and configuring), remotely view and control the device for troubleshooting, and conduct mobile content management. Many Enterprise Mobility Management (EMM) suites on the market




*Source: Institute for Defense Analysis*

provide these capabilities in an integrated manner.

The National Security Agency (NSA) is experimenting with intelligent sensors, advanced data analytics, and visualization techniques to reduce the human-intensive burden of monitoring the network infrastructure, including endpoint devices. NSA is developing a system that monitors the network, alerts the staff to any violations or intrusions, and implements an automated response to mitigate the violation in real time with minimal human involvement. The responses, referred to as automated courses of action (ACOA), are predetermined actions that are designed to match the level of violation to or intrusion into the organization's network. As levels of tolerance are agreed to by an organization and thresholds for action are determined, the ACOAs can be expanded to reflect the appropriate risk profile. This allows decision makers to focus their attention on the more complex problems that require critical thinking or "a human in the loop." Visualizations of network activity can also be used to pinpoint the physical locations of devices of interest, such as where an attempted connection of an unauthorized device to a particular network is occurring.

***How does mobility affect user identification and authentication?*** Classified mobility implementations require a high degree of certainty of the identity of the user. Multi-factor authentication should be used, along with additional factors, to determine that the intended user is using the device and has actively signed in. Factors are typically based on something the user *knows* (username and password), something the user *has* (badge or token), and something the user *is* (fingerprint, facial recognition). Going forward, behavior-based authentication methods can be useful in determining that the user currently using the device is the intended user. Behavior-based authentication captures a fourth type of factor—something the user *does*—for multifactor authentication, and it has the added benefit of continuously evaluating whether the users are themselves. Behavior-based techniques may include key force and speed analysis, heart rate fluctuation measurement (via a wearable device), and machine-learning-based analysis of the user's normal activities. These techniques are valuable since they cannot be reproduced without the user since the actions are unconscious and non-transferable.

Systems using behavior-based authentication can determine the probability of the user conducting normal business versus engaging in inappropriate actions. The system can detect abnormal behaviors based on previously approved thresholds of the organization and require authentication to proceed or trigger additional automated courses of action. For example, if a user logs into a computer but walks away from his or her device and someone else sits down to use it, the system can detect the change in users. Low-risk activities that the user has not done before (e.g., open a file in a folder that the user typically doesn't use) require re-authentication by the user to ensure he or she is aware of the action and that it is abnormal. Potentially higher-risk activities (e.g., multiple file downloads) can be blocked until unlocked by a supervisor or administrator. Note that this sort of behavior tracking would have prevented cases such as WikiLeaks in which an abnormal action (downloading thousands of cables) occurred. Using machine learning techniques, authentication systems can establish the "normal" behaviors for each user instead of relying on an administrator's attempt to identify all potential acceptable behaviors in the system against which the user can be checked.

The Defense Advanced Research Projects Agency's (DARPA) Active Authentication program is researching ways of validating the identity of the person using a device by focusing on the unique aspects of the individual through the use of software-based biometrics. Biometrics are human characterizations that can be used to recognize a person by one or more intrinsic physical or behavioral traits. The program has two phases. The first phase is examining data that can be collected without the use of additional sensors (e.g., mouse or keystroke movements or how the user crafts written language in an email or document). The second phase focuses on development of "a solution that integrates any available biometrics using a new authentication platform suitable for deployment on a standard DoD desktop or laptop." (DARPA 2015)

***How do you protect classified wireless networks?*** One problem with wireless communications is that information is transmitted through radio frequencies—anyone with the right equipment can intercept these transmissions. Several approaches can be used to impede this kind of attack. One common method is to deliberately not broadcast the service set identifiers (SSID) (wireless network names) of the networks. This makes it very difficult for anyone to connect to the network in anything other than a deliberate manner. This prevents non-U.S. Government personnel from accidentally connecting to a government network and having their data monitored. Another method is allowing only devices that identify themselves with approved media access control (MAC) addresses (network hardware serial numbers) to connect, although it is possible for malicious users to spoof a MAC address. Additionally, requiring devices to use protections like the IEEE 802.1x standard to authenticate when connecting to the network simultaneously protects the network from attack and protects personally identifiable information (PII) that can be processed or stored by a wireless network operated by the DoD.

***Can classified devices be restricted to specific areas?*** By definition, mobile devices can go anywhere, but moving a device from one classified area to another requires a way to ensure that data cannot be obtained without the proper access controls. NSA is currently exploring a way to implement a secret sharing protocol to mitigate this problem. In this protocol, one secret share is stored on the user's side and an additional secret share is stored in the classified network. When the device is on the classified network, the two secret shares can be combined and the drive decrypted. As soon as the device is removed from an area where it can connect to the classified network, the network secret share becomes unavailable and the drive data is inaccessible. Reconnecting the device to the classified network restores drive accessibility. This capability would allow personnel to securely and simply transport their classified laptops from one classified location to another. Secret Share keys can alternatively be enforced by very accurate geofencing using Wi-Fi-based micro-location and passive presence technologies. This might enable a device to operate at different classification levels depending on location in the facility, be disabled completely ("turned into a brick"), or be disabled for only personal use when leaving the facility.

Another approach to restricting the mobility of a device to a specific area, which is available today, is to place a radio frequency identification (RFID) scanning system, similar to the shoplifting detection/deterrence systems used in department stores, at the exit of a classified area. Any attempt to remove a tagged device would set off an alarm alerting personnel to the problem. The combination of these approaches creates a robust technical capability to disable devices as they leave an area, along with behavioral cues and reminders.

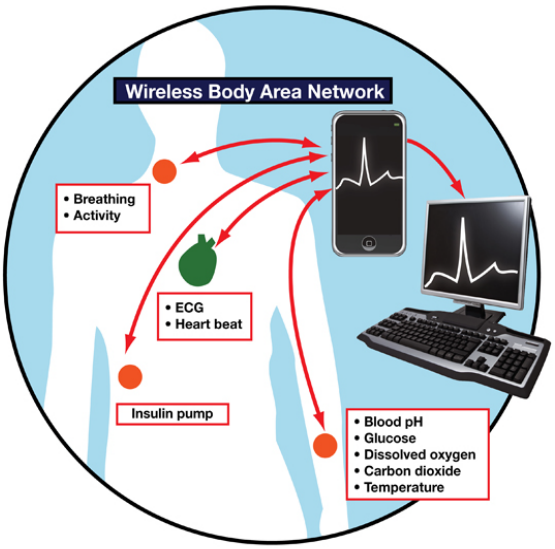
One of the goals of the Pentagon network architecture is to connect departmental, service, and agency networks together in such a way that users from different organizations with-

in the Pentagon can reach their own "home base" networks when they are collaborating outside their assigned spaces. Ubiquitous network access can be achieved using network virtualization and software-defined networking by allowing multiple networks to run concurrently across the same physical network hardware and fiber. This would allow a user to attend a meeting in another space and be able to sign into his home network to check information stored there or share information with meeting participants through email or collaboration software without needing complex manual techniques to gain access.

***How do wireless wearable medical devices impact classified wireless?*** In the very near future, wearable medical devices will be the norm for persons with chronic health conditions such as, cardiac arrhythmias, diabetes, and Parkinson's disease. Advances in healthcare have resulted in wearable and implantable medical devices that can "either transfer data to a remote center, direct the patient to take a specific action, or automatically perform a function based on what the sensors are reading." (EMBS 2015) Many of these devices are leveraging low-power Bluetooth wireless interfaces to link to a smartphone.

These devices present a new challenge to classified wireless networks. Data collected by a device is considered both PII and personal health information (PHI), which must be kept secure and may be subject to other regulations and laws. Wearable medical devices have been shown to be vulnerable to attack, either for stealing sensitive health information or actually changing the parameters of the device itself (such as adjusting insulin dosage). Increasing concerns about such events led to a recent Government Accountability Office (GAO) report recommending that the Federal Drug Administration (FDA) leverage its post-market efforts to identify and investigate information security problems with these devices. (GAO 2012)

There is also the potential for violation of the Americans with Disabilities Act (ADA) if proper planning for wearable devices does not occur. Perhaps even more concerning, a restriction on wireless prosthetics or devices may affect returning American veterans as they reintegrate into the workforce. When restricting medical devices in sensitive areas, considerations must include the expense of the device, impact on the health of the wearer, and impact on the person's



Source: EEtimes.com

ability to do the job. Also, it may be unreasonable to require employees to move to a less effective or less feature-rich device.

NSA has developed a policy for its own classified wireless networks with respect to wearable fitness devices (e.g., Fitbit, Nike Fuel Band, and Apple Watch Sport). NSA allows devices that collect data from passive sensors (e.g., motion sensors and heartrate monitors). However, wearable devices that contain cellular radio, Wi-Fi capabilities, camera or video, and microphone or audio transmission capable are prohibited. Devices with Bluetooth capability can be used as long as the device meets the rest of the criteria in the policy instruction. This is particularly important since many wearable medical devices use low-power Bluetooth to transmit to a handheld device. Wearable fitness devices are not permitted in any NSA/Central Security Service (CSS) SCIF. (NSA 2015a) NSA has made a good start in terms of policy for *fitness devices* in classified areas, but as wearable devices evolve, further work is needed on policy for *medical devices* that transmit data via mobile broadband or Wi-Fi for analysis, either to a handheld device or over the Internet to a medical facility for review.

***What policy and guidelines apply to classified wireless networks and mobile broadband?*** Several DoD directives and instructions are applicable to wireless networks and communications. Additionally, the National Institute of Standards and Technology (NIST) provides federal guidelines for securing wireless networks and the Defense Information Systems Agency (DISA) and NSA provide guides for implementing secure wireless networks and mobile communications devices. The instructions and guidelines are intended to provide information assurance and security across the DoD network infrastructure.

*DoD Directive 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG)* establishes policy for the use of commercial wireless devices, service, and technologies with the DoD GIG. This directive applies to all commercial wireless devices, services, and technologies (e.g., wireless networks; personal electronics devices, including laptops; and personal communication devices, including cellular phones, audio/video recording devices, and other commercial wireless devices capable of storing, processing, or transmitting information). (ASD(NII) 2007)

*DoDI 8420.01, Commercial Wireless Local Area Network (WLAN) Devices, Systems, and Technologies* establishes policy for commercial wireless local area network (WLAN) devices, systems, and technologies. It provides procedures for implementing standards compliance, security certification and validation, intrusion detection, and spectrum supportability for unclassified and classified WLANs. (DoD CIO 2009)

*DoD Instruction (DoDI) 8500.01, Cybersecurity* establishes policy on information assurance for all DoD information systems that receive, process, store, display, and transmit

DoD information, including all mobile computing devices such as laptops, handhelds, and personal digital assistants that operate in wireless mode. (DoD CIO 2014)

*NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs)* provides guidelines for improving the security configuration and monitoring of IEEE 802.11 wireless local area networks within unclassified environments. (NIST 2012)

*DISA Security Technical Implementation Guides (STIGs)* and *NSA Security Configuration Guides* provide configuration standards for DoD information assurance (IA) and IA-enabled devices/systems. The STIGs contain technical guidance to "lock down" information systems and software that might otherwise be vulnerable to a malicious computer attack. (DISA 2009, NSA 2015b)

***What is the Commercial Solutions for Classified (CSfC) program?*** The DoD is increasingly turning to the commercial market to provide technology solutions to meet mission requirements. NSA/CSS's Information Assurance Directorate (IAD) is developing new ways to leverage emerging technologies to deliver more timely information assurance solutions. The CSfC program was established to enable commercial products to be used in layered solutions to protect classified data. NSA/CSS developed a series of capability packages that provide a technical architecture that will allow DoD customers to independently implement secure solutions using layered commercial-off-the-shelf (COTS) products. The packages provide high-level security and configuration guidance that will allow customers within the DoD to successfully implement their own solutions. (NSA 2015b)

***What classified mobile device services are available?*** DISA is enabling mobile classified communications through the DoD Mobility Classified Capabilities (DMCC), developed in partnership with industry, the military services, and NSA. DISA began a pilot phase in

***Wearable Medical Devices***

*With rising healthcare costs and reductions in the length of hospital stays, doctors are beginning to rely on wearable medical and implantable devices that provide continuous monitoring of chronic health conditions and perform an automatic action, request the patient to take action, or transmit data to a remote site for review by medical personnel.[2] For example, patients with diabetes may have an insulin pump that monitors blood glucose and can suspend insulin delivery if blood glucose levels are too low.*

*Advancements in technology have resulted in miniaturized sensors that make portable monitoring technology easier to wear and use. Cardiac outpatients experiencing arrhythmias traditionally were given bulky heart monitors that could be worn for only 24 to 48 hours. CardioNet's Mobile Cardiac Outpatient Telemetry™ (MCOT™) unit (available through GSA) can be worn for up to 21 days. The MCOT device records continuously, automatically transmitting data to the CardioNet Center wirelessly via mobile broadband at physician-designated thresholds for monitoring. (Cardio Net 2015)*

early 2014 and is slowly transitioning DMCC to its customer base; full operational capability is expected by 2017. Classified mobile devices are intended to support command and control, with an estimated need of approximately 25,000 devices. (DoD CIO 2013) The initial DMCC Secret-level offering included testing and approval of classified mobility devices, Public Key Infrastructure (PKI) solutions/capabilities, a mobile device management solution, email capability, and limited international roaming capability via a virtual private network. DISA provides all DMCC devices access to enterprise email via Outlook Web Access. (DISA 2015) The challenges for DISA's mobility program (both unclassified and classified) include supporting mobility from the cloud, network access control through derived credentials, and development of secure mobile applications. (Youst 2014)

***What does this mean for DoD?*** Smartphones and mobile devices are a necessary tool for conducting business within DoD. It is inevitable that wireless networks and mobile broadband are going to become part of the infrastructure that supports DoD in the Pentagon. Programs such as CSfC and DMCC are leading the way toward integrating classified and unclassified work. Research being conducting at NSA is allowing more mobility of the workforce within the building and devices to be freely moved from unclassified to classified areas. Government agencies should join forces to leverage DoD programs and NSA research to build a wireless network that has the ability to adapt to emerging technology and can reliably support tenants at both the unclassified and classified levels.

**References**


Assistant Secretary of Defense for Networks and Information Integration. *Department of Defense Directive 8100.02 – Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG)*. Issued April 23, 2007.

Cardio Net. "Cardio Net MCOT™" CardioNet.com. CardioNet.com. www.cardionet.com/government_03.htm (accessed March 18, 2015)

Defense Information Systems Agency. "DoD Mobile Classified Capabilities." DISA.mil. www.disa.mil/Enterprise-Services/Mobility/Classified-Capabilities (accessed March 19, 2015)

Department of Defense Chief Information Officer. *Department of Defense Instruction 8500.01 – Cybersecurity*. Issued March 14, 2014.

Department of Defense Chief Information Officer. *Department of Defense Commercial Mobile Device Implementation Plan*. February 15, 2013.

Department of Defense Chief Information Officer/Assistant Secretary of Defense for Networks and Information Integration. *Department of Defense Instruction 8420.01 – Commercial Wireless Local Area Network (WLAN) Devices, Systems, and Technologies*. Issued November 3, 2009.

Engineering in Medical and Biological Society, Institute of Electrical and Electronics Engineers. "Wearable & Implantable Technologies." EMBS.org.

www.embs.org/about-biomedical-engineering/our-areas-of-research/wearable-a-implantable-technologies (accessed March 18, 2015)

Information Assurance Support Environment, Defense Information Systems Agency. *Security Technical Implementation Guides (STIGs)*. IASE.DISA.mil. iase.disa.mil/stigs/Pages/index.aspx (accessed March 11, 2015)

Information Innovation Office, Defense Advanced Research Projects Agency. "Active Authentication." DARPA.mil. www.darpa.mil/our_work/i2o/programs/active_authentication.aspx (accessed March 19, 2015)

National Institute for Standards and Technology. *Special Publication 800-153 – Guidelines for Securing Wireless Local Area Networks (WLANs)*. February 2012.

National Security Agency. *NSA/CSS Policy Instruction 6-0006 – Personal Use of Wearable Fitness Devices*. Issued March 3, 2015.

National Security Agency. *Security Configuration Guides*. NSA.gov. www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/ (accessed March 18, 2015)

National Security Agency. *Commercial Solutions for Classified Program*. NSA.gov. www.nsa.gov/ia/programs/csfc_program/ (accessed March 12, 2015)

U.S. Government Accountability Office. *Medical Devices: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices*. Report to Congressional Requesters. August 2012.

Youst, Greg. "DoD's Strategic Mobility Vision: Needs & Challenges." Presentation at National Institute of Standards and Technology Information Security and Privacy Advisory Board (ISPAB). October 22, 2014 Meeting.

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE (DD-MM-YY) | 2. REPORT TYPE | 3. DATES COVERED (From – To) |
|---|---|---|
| 31-03-15 | Non-Standard Final | |

**4. TITLE AND SUBTITLE**

In-Use and Emerging Disruptive Technology Trends

**5a. CONTRACT NUMBER**

DASW01-04-C-0003

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBERS**

**6. AUTHOR(S)**

Brendan T. Farrar-Foley, J. Corbin Fauntleroy, Laura A. Odell, Ryan R. Wagner,

**5d. PROJECT NUMBER**

**5e. TASK NUMBER**

BK-5-3754/3448

**5f. WORK UNIT NUMBER**

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES**

Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311-1882

**8. PERFORMING ORGANIZATION REPORT NUMBER**

NS D-5457
H 15-000243

**9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

Lytwaive L. Hutchinson
Office of the Secretary of Defense, Chief Information Officer
Director, Enterprise Information Technology Services Directorate
The Pentagon, Rm. 2B913A

**10. SPONSOR'S / MONITOR'S ACRONYM**

OSD CIO

**11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)**

**12. DISTRIBUTION / AVAILABILITY STATEMENT**

Approved for public release; distribution is unlimited.

**13. SUPPLEMENTARY NOTES**

Project Leader: Laura A. Odell

**14. ABSTRACT**

This document contains quick look analysis summaries of in-use and emerging capabilities that are important to Office of the Secretary of Defense (OSD) performance and efficiencies objectives. Each summary describes a specific technology and implementation challenges and limitations. Options available to the Department of Defense to leverage the capability in its current information technology infrastructure and an industry snapshot in-use example are included in the analysis as well.

**15. SUBJECT TERMS**

Emerging Technology, Disruptive Technology, Containers, De-perimeterization, Wi-Fi, Mobile Broadband, Cellular, Zero-Trust, Mobile Thin Client, Software Defined Networking, Face Recognition Software, Find Me Follow Me

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | Lytwaive L. Hutchinson |
| Unclassified | Unclassified | Unclassified | Unlimited | 60 | 19b. TELEPHONE NUMBER (Include Area Code) (703) 695-2865 |