BROCADE

Executive Overview: The Necessity of Network Modernization

Today, connecting to data from anywhere at any time is not a nice-to-have option—it is mandatory. The age of the Internet of Things (IoT) is upon us. And as the demand for devices and subsequent data grows, this increased traffic will travel on an outdated network infrastructure. Will government agency networks be able to meet the new IoT demands?

Not without change. Agencies are realizing that keeping old, closed, legacy networks up and running is costing them more than just budget—it is stifling innovation and hampering mission success.

A New Direction Needed

Legacy IP relies on costly equipment that needs constant re-investment to remain functional. But organizations are searching for ways to cut back their IT spending, and the legacy approach no longer works. What does work is agility.

The New IP represents the modernization of networking. It entails transitioning traditional networks from a "plumbing"-like approach based on proprietary hardware, manual configuration, limited flexibility, and high cost to an intelligent network that is built on Ethernet fabrics and embraces a software-centric, highly virtualized environment based on open standards. The New IP offers dramatically better scalability, flexibility, automation, adaptability, security, and control, and is responsive to the applications and data that it serves. Moreover, the New IP is an optimized, innovative network that will allow the Federal government to deliver data to citizens and warfighters alike, while saving $7 billion over five years.

To learn how a modern network will cut costs and improve agency mission outcomes, download the full version of "The Necessity of Network Modernization" white paper at www.brocade.com/federal.

Drivers for the New IP—By the Numbers

Organizations do not make IT decisions blindly. These numbers make the case for the New IP:

- **Scale for growth:** The ability to scale is important, but legacy IT already is buckling under the weight of the global increase in IT use. Gartner predicts that the number of connected "things" will increase from 4.9 billion in 2015 to 25 billion by 2020.[1] Legacy networks cannot meet the new demands of the IoT.
- **Spend wisely:** In 2015, of the overall $79 billion budgeted for Federal IT, agencies planned to spend about $58 billion on the operation and maintenance of legacy systems[2]—or nearly 73 cents of every dollar—according to the U.S. Government Accountability Office's High-Risk List. That is not sustainable, and the New IP helps agencies reduce costs dramatically.
- **Be open:** Leveraging open standards and multivendor networks could save Federal agencies $7.03 billion over the next five years, according to Gartner's Total Cost of Infrastructure and Operations methodology.
- **Promote competition:** Introducing a second vendor to promote competition helps cash-conscious agencies control costs, and 94 percent of agencies claim that the introduction of a second vendor can reduce capital costs by 30 to 40 percent.[3]

1 Gartner. "Gartner Says 4.9 Billion Connected 'Things' Will Be in Use in 2015." November 11, 2014. http://www.gartner.com/newsroom/id/2905717.

2 GAO. "GAO High-Risk Series: An Update. Improving the Management of IT Acquisitions and Operations." GAO 15-290. February 11, 2015. http://www.gao.gov/products/GAO-15-290.

3 MeriTalk. "Infrastructure Independence, Set My IT Free." March 2013. http://www.meritalk.com/infrastructureindependence.

- **Simplify:** Intelligent Ethernet fabrics can help agencies deploy network capacity five times faster and increase network utilization by 200 percent.
- **Save with SDN:** The New IP allows agencies to leverage Software-Defined Networking (SDN). Consulting firm Deloitte says SDN alone can reduce networking costs by as much as 50 percent and reduce IT budgets by 7.5 percent.[4]
- **Secure your network:** In 2014, the average number of days that attacks were present on a victim's network before being discovered was 229 (more than seven months).[5] The need for a robust infrastructure and a comprehensive security strategy—utilizing Ethernet fabrics, data encryption, and SDN—is more critical than ever. Using SDN to abstract and centrally manage security services provides a new paradigm for IT professionals. It enables provisioning of new security models by dynamically leveraging both physical and virtual assets, and adjusting end-to-end security deployments based on a particular mission.

Is Your Network Ready for the New IP?

Your agency does extensive market research when developing requirements.	Yes	No
Your agency requirements are linked to mission outcomes and defined in terms of desired features, functions, capabilities, and service levels to meet those outcomes.	Yes	No
Your agency networks are vendor-independent, using open, industry-standard protocols and restricting the use of proprietary protocols.	Yes	No
Your agency networks are agile and flexible, allowing you to quickly scale in or out and rapidly deploy new applications.	Yes	No
Your agency networks adequately protect and secure critical information, ensure data privacy today, and are prepared for the cyber threats of tomorrow.	Yes	No
Your agency networks are intelligent, automated, and simple to manage and administer.	Yes	No
Your agency networks are prepared for the explosive growth in mobility and the Internet of Things, in which everything is connected.	Yes	No
Your agency networks can be acquired as your needs warrant—whether they include a capital purchase, lease, Infrastructure as a Service, cloud, or any combination.	Yes	No

Next Steps

If you answered no to one or more of the survey questions, download the white paper "The Necessity of Network Modernization—A Roadmap to Mission Readiness" to learn what steps your agency can take to get on the path to the New IP.

Visit www.brocade.com/federal.

4 "Network Effect." *The Economist.* December 15, 2012. http://www.economist.com/news/business/21568435-software-defined-networking-inspiring-hope-and-hype-network-effect.

5 IT Governance. "Cyber Security Breaches Can Go Undetected, IT Governance's Cyber Watch Boardroom Survey Finds." July 2014. http://www.itgovernance.co.uk/media/press-releases/cyber-security-breaches-can-go-undetected.aspx?ut.

Corporate Headquarters
San Jose, CA USA
T: +1-408-333-8000
info@brocade.com

European Headquarters
Geneva, Switzerland
T: +41-22-799-56-40
emea-info@brocade.com

Asia Pacific Headquarters
Singapore
T: +65-6538-4700
apac-info@brocade.com

BROCADE