The Key to Transitioning to a Secure, Adaptable Multicloud Network Environment

How evolvable networks — and GSA's next-generation EIS contract — can ease the transition off of aging TDM networks, improve security and lower total IT costs.

By FedScoop Staff

Time is running out for federal agencies to transition away from MaBell-era copper wire circuits and TDM-switching technology. The impetus to replace these time-division multiplexing (TDM) networks with more efficient, all-Internet Protocol (IP) packet delivery platforms is coming from all directions.

It's not just the White House that is pushing agencies to upgrade and modernize aging government IT systems, with the administration's Federal IT Modernization Report, its Cloud Smart strategy and other initiatives.

"What's also driving this transition is the dependence on equipment that's not only end-of-life, but end-of-service," says networking expert Quinten Johnson, a former AT&T executive who now heads up federal sales for Juniper Networks. It's no longer unusual to find federal IT engineers scouring eBay to locate replacement parts for their networks, he says. It's also getting harder to find people who understand legacy equipment. That's driving up maintenance costs and putting agency networks at greater risk.

> **What's also driving this transition from TDM to IP is the dependence on equipment that's not only end-of-life, but end-of-service.**
>
> — QUINTEN JOHNSON, JUNIPER NETWORKS.

As importantly, these older circuit-based systems lack the features, functionality and scalability that IP-based systems offer, and that organizations increasingly need to keep up with today's fast-changing IT demands and the global shift to cloud computing.

U.S. telecom giants Verizon and AT&T recognized that fact nearly a decade ago in announcing plans to sunset their TDM networks, and transition to IP-based fiber and wireless systems. TDM's method of dividing, transmitting and receiving independent signals over a common channel using synchronized switches was simply no match for the greater capacity and flexibility of IP packet methods. Their transition gained momentum when FCC decided in 2013 to issue new policy orders, designed to "expedite" the transition of the nation's telecommunications infrastructure to IP to support future growth.

The pressure for agencies to move off TDM systems, however, took on greater urgency when the U.S. General Services Administration (GSA) released its next-generation Enterprise Infrastructure Solutions (EIS) acquisition vehicle in 2017. GSA made it clear in a 2018 transition document that it intended to decommission all GSA-managed TDM-based private branch exchanges (PBX) by May 31, 2020, saying, "Agencies are strongly encouraged to replace TDM-based voice solutions with transformative solutions including voice-over-IP or wireless."

Silver lining for agencies

The good news for government agencies: The technology that has been helping organizations move from circuit-to-packet platforms has evolved in significant ways. Today's modern network offerings not only pave the way for moving from TDM to IP; they also simplify network operations, improve security and lower total operating costs.

According to research gathered by Nemertes, a global advisory firm, organizations that moved from TDM to IP networking reduced their annual equipment maintenance costs by 34 percent and saw overall operational costs drop an average of 8 percent per year — and as much as 26 percent at larger enterprises.

As importantly, these newer solutions — especially those which capitalize on open standards-based, software-defined networking platforms — can help agencies more readily adapt to the evolution of multicloud services, Johnson says.

Among the many upsides of GSA's EIS contract, agencies can expect greater flexibility, fewer obstacles and as much as 21 percent lower costs in acquiring these newer technology solutions compared to previous acquisition contracts EIS was designed to replace, according to GSA and an ACT-IAC industry working group.

That's not to say replacing aging circuit-based infrastructure with more modern IP networks will be easy or straightforward. Agency leaders face a series of pivotal decisions on what combination of hardware and software platforms to invest in — and whether to stick with incumbent suppliers, or partner with more forward-leaning and agile platform or service providers.

But agencies have an unparalleled opportunity to streamline and modernize their infrastructure and introduce a measure of simplicity into IT operations by adopting an open and evolvable networking platform, say Johnson and others.

Organizations that moved from TDM to IP networking reported

34%

reduction in annual equipment maintenance costs and up to

26%

reduction in overall IT operational costs

Source: Nemertes research

Agencies using GSA's EIS contract can expect

21%

lower IT acquisition costs for new technology solutions compared to prior contract vehicles

Source: ACT-IAC and GSA

The way forward

"One of the challenges agency CIOs face is prioritizing what they're modernizing: They have a mixture of TDM networks, various ATM, SDH, DWDM and other switching protocols, and a plethora of connectivity devices," says Greg Fletcher, who leads Juniper Network's U.S. civilian agencies business development.

"Perhaps the biggest concern we hear from our customers is figuring out the most cost-effective or efficient way to modernize. No site is the same. There's no one-size-fits-all approach," he says. "In some cases, it makes sense to work natively within the system to change the output into an IP protocol. In other cases, commercially available products, like Juniper's CTP (Circuit to Packet) platform makes better sense."

"CTP provides a way to reliably encapsulate and transport voice and serial data, including TDM and circuit-based applications over an IP network — taking advantage of the scale and cost savings that come with IP — and then pushes them back out at the other end of the network in their original protocol," he explains. Juniper's CTP series platforms meet a variety of federal requirements, including Department of Defense joint interoperability certification standards, according to Fletcher.

The larger opportunity for agencies, however, lies in laying a centrally managed networking foundation that can take full advantage of IP operating environments — and that supports a cohesive multicloud strategy, not simply multiple cloud and on-premises silos.

Fletcher's advice for engineering networks for an evolving IT ecosystem: Build on top of an open and evolvable software-defined networking platform that can operate across private, hybrid and public cloud environments.

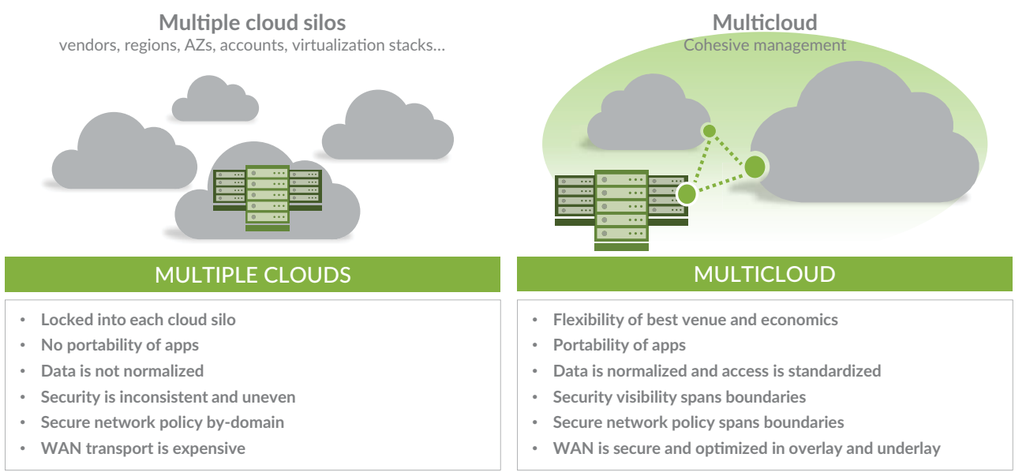
He also recommends selecting networking solutions that are capable of:

- Deploying software-defined wide area networks to the edge.
- Controlling core, end-to-end networking services and security centrally.
- Orchestrating networking policies across multiple environments and that can span across network layers from top to bottom.
- Fostering "reliability-first" automated operation.
- Ensuring multi-vendor freedom.

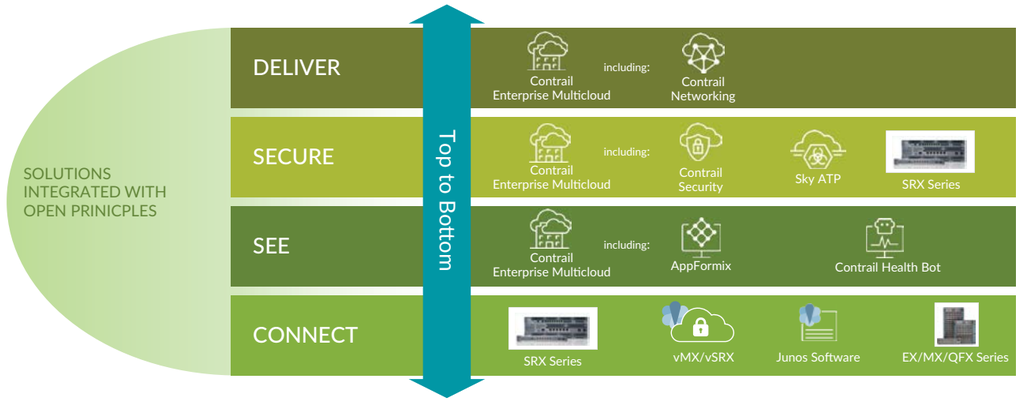
Security and simplicity across networks

Collectively, SDN network capabilities give agency CIOs and their IT teams greater total control over their entire IT enterprise by leveraging the ability to make software services accessible through an IP address. That simplifies common operational tasks, and allows greater flexibility for agency program teams to provide more agile and responsive service to their stakeholders.

But perhaps the ultimate dividend for investing in open, evolvable, software-defined networks is the opportunity to achieve pervasive security by leveraging intent-based security policies that follow workloads across environments.



Source: Juniper Networks



Source: Juniper Networks

"Agencies are dealing with a daisy chain of security devices," says Fletcher. "Networks have many endpoints and many solutions; each box has to be managed and secured separately. In the world of SDN, it's virtual software — essentially just one box. So, it's easier to secure and manage your networks centrally."

> **Agencies are dealing with a daisy chain of security devices. In the world of SDN, it's essentially just one box.**
>
> — GREG FLETCHER, JUNIPER NETWORKS

For IT administrators, that simplifies the ability to quickly identify and block a laptop infected with malware from gaining extended access to an agency's networks. And for DevOps teams, SDN also makes it easier to "shift left" — giving them greater ability to focus on preventing software problems instead of detecting them after the fact.

From SD-WAN to AI-driven enterprise

Open, evolvable software-defined wide area networks (SD-WAN) are already providing a host of other benefits, including:

- Faster branch and virtual private cloud rollouts.
- Overcoming a shortage of branch IT expertise.
- Virtual private network segmentation.
- Better on-ramps to multicloud.
- Greater app and user policy controls.
- More enforceable service level agreements.
- More bandwidth on demand.

As agencies begin to modernize their networks from end to end, and from WAN to campus to branch, they can expect another benefit: Greater ability to leverage artificial intelligence in real time to support faster decision making across the enterprise.

All of those benefits will depend on using established SDN solutions and architectures that have a proven record in government.

"We've been dedicated to the federal space for 20 years," Fletcher says, adding that Juniper has evolved organically — rather than through a collection of acquisitions — to help agencies, including DOD and the White House, move from TDM to IP and now to the cloud.

"What differentiates us is our open source approach, which allows agencies to acquire best of breed solutions and avoid vendor lock-in — and brings in a broader community of developers and best practices for government to rely on."

Find out more how Juniper Network's open, evolvable software-defined networking solutions can help your agency take full advantage of IP and multicloud networking.

---

fedscoop

JUNIPER NETWORKS