FCW

Network Modernization: A Stepping-Stone to the Future

In the federal government, oversight agencies have long urged agencies to modernize their networks. Modernization is moving along, as most agencies have initiatives underway, but some aren't as far along as they could be.

While there has been progress—especially in switching from the Networx telecommunications contracting vehicle to the more modern Enterprise Infrastructure Solutions (EIS) contract, agencies are at different levels in implementing modern technologies, replacing legacy infrastructure and shoring up security. Without significant progress, it's difficult to increase efficiency; enable protection of sensitive data, networks and critical infrastructure; and move forward with broader IT modernization plans. Legacy networking technology also can inhibit agencies' use of emerging technologies like artificial intelligence and machine learning, the Internet of Things (IoT) and edge computing, all of which require bandwidth, network speed and flexibility.

gremlin / iStock

SPONSORED BY: COMCAST BUSINESS

In the federal government, oversight agencies have long urged agencies to modernize their networks. Modernization is moving along, as most agencies have initiatives underway, but some aren't as far along as they could be.

While there has been progress—especially in switching from the Networx telecommunications contracting vehicle to the more modern Enterprise Infrastructure Solutions (EIS) contract, agencies are at different levels in implementing modern technologies, replacing legacy infrastructure and shoring up security. Without significant progress, it's difficult to increase efficiency; enable protection of sensitive data, networks and critical infrastructure; and move forward with broader IT modernization plans. Legacy networking technology also can inhibit agencies' use of emerging technologies like artificial intelligence and machine learning, the Internet of Things (IoT) and edge computing, all of which require bandwidth, network speed and flexibility.

Current networking infrastructure were put to the test during the past few years when so many agency employees began working remotely, putting a major strain on network infrastructure demand. Comcast, which provides fiber-rich infrastructure, saw an increase of about one-third in network traffic, slightly more in mobile data usage and a 285% increase in voice and video calls.

Supporting that kind of effort is a big job that takes money, time and planning, but it's critical work. By breaking it down into manageable pieces and repurposing existing technology when feasible, agencies can create a transition path that will get them where they need to go.

ESTABLISH A BASELINE

The first step is setting a baseline network architecture that will work today but positions the agency for the future. The baseline network should be able to handle many different types of traffic and support a wide array of network characteristics. The goal is to create a network that provides as much flexibility as possible to embrace newer technologies over time.

Developing the right baseline requires understanding where you want to end up—ideally, with a flexible, expandable, future-ready network infrastructure. A more technology-agnostic, universal approach to modernization can provide more flexibility and jumpstart the journey. This approach also helps give agencies the flexibility to add features and more modern applications to their networks over time.

Colin Gosnell, head of solution engineering at Comcast Government Services, used an agency procurement for 4G wireless networking services he came across a few years ago as an example of the benefits of this approach.

BartekSzewczyk / iStock

"The agency needed a way to access a database sitting at an agency data center somewhere, so it wrote RFP [request for proposals] based on the 4G wireless networking standard at the time," he explained. Two years later, the agency now favors the cloud instead of standard data centers and 5G has become the standard. The RFP, however, was so specific that the agency will likely have to revamp its entire network.

"If they had said early on that they wanted to establish an Ethernet network for all of their data, wherever it is located, that would have been a better baseline architecture," he explained. "It would have given them much greater flexibility and wouldn't have required an overhaul."

CHOOSE THE RIGHT COMBINATION OF CONNECTIVITY OPTIONS

Older agency networks can have legacy technologies, such as Time-Division Multiplexing (TDM) and first-generation Virtual Private Networks (VPNs), which can present challenges.

Given the age of TDM, it can be difficult to find replacement parts and engineers who can troubleshoot the technology.

"When TDM was popular, networking revolved around connecting buildings and sending and receiving packets of data," Gosnell explained. "Today, networks are defined by the applications that run across it. It makes sense to develop a plan and transition today, even if it's still technically working."

For most agencies, the logical replacement for TDM are Ethernet private lines, which provide point-to-point connectivity between locations across a data network. The baseline architecture can handle many different technologies that flow across it. Another related option is an Ethernet Virtual Private Line, which enables agencies to create virtual environments that connect multiple segments with each other. Both types of Ethernet private line technology enable all sites within a specified group talk to each other and can prevent others from participating. This increases both network flexibility and security.

Federal agencies have some options in moving towards more efficient communications. For instance, agencies can use technology to convert TDM signals into Ethernet or IP signals that can travel over an Ethernet solution. This approach, while temporary, enables agencies to use TDM signals to emulate circuits over a modern network architecture to continue delivering TDM service.

> **"Establishing a baseline and choosing the right technologies can take time, and complexities are bound to crop up."**

Another example is that during the pandemic, some agencies relied on VPNs. On the plus side, VPNs enabled remote workers to remain productive by providing access to both cloud and on premise applications while enforcing policy. Many agencies took the opportunity to ramp up use of VPNs for that purpose. When implemented correctly, VPNs can provide effective encryption at the data level--from remote devices to servers in agency environments. They also can give agency IT personnel the ability to monitor data traffic flowing in and out of the network. Bridging that gap requires technology that can help provide network security. Comcast's WorkRemote solution establishes a dedicated connection in the remote user's environment and creates an extension from that environment to the agency environment. Essentially, this process adds an extra layer of transport security, eliminating the uncontrollable environment of the public Internet while still providing required flexibility.

Another important modern network technology is Software Defined Networking (SDN), a software-based method of controlling the network that relies on virtualized network functions. Federal oversight agencies are bullish on SDN, finding that its flexible architecture is well-suited to large networks and global network infrastructure. By adding SDN to a baseline Ethernet architecture, agencies can improve network performance, resilience and security and the way services are delivered. The most important functions for a comprehensive SDN solution include intelligent routing, application visibility, centralized management, policy enforcement, and strong security features like network segmentation.

While all of these modern network technologies can make a difference in productivity, efficiency and security, an important technology to help improve mobile communications is 5G, the latest generation of wireless technology for mobile networks. Consultancy ESG expects 5G to take its place as a legitimate business tool very soon, and government must be ready. 5G has much lower latency than 4G, resulting in much faster download and upload speeds. It can also be important for edge computing environments, which depend on fast access to data.

5G is well on its way to changing the way individual devices access agency networks, but that's just the beginning. Next up is private 5G networks, which are already beginning to make its way into agencies' Requests for Information (RFI). The idea, Gosnell explained, is to provide agency employees with mobile devices that can connect only to the agency's network. Users would plug their devices into private hotspots that connect on a 5G network like a dedicated path, choosing a 5G signal to connect back to the network.

Viktoriia Hnatiuk / iStock

ACCELERATING YOUR NETWORK TRANSFORMATION

Establishing a baseline and choosing the right technologies can take time, and complexities are bound to crop up. One way to hit the ground running is by taking advantage of the EIS contract. Agencies can pick and choose the technologies they need without having to vet them individually. As new technologies are established, EIS is already in place, making it easier to bring those new technologies on board. SD-WAN technology, for example, wasn't in the original scope of EIS but was added as demand rose.

PeopleImages / iStock

Many agencies are also taking advantage of the funds available through the Technology Modernization Fund (TMF), which provides loans to agencies for IT modernization projects that demonstrate a strong return on investment. The TMF, created in 2017, sets aside hundreds of millions of dollars to support IT modernization projects from the proposal development process, initial concept development, to final contract award.

Agencies can also take gradual modernization steps instead of aiming at a complete overhaul. Another way to ease the transition is by repurposing existing network equipment when it doesn't impact the overall project. For example, agency router networks today may still be using MPLS technologies, and some of that is reusable, at least temporarily.

This gradual approach also makes sense for other reasons. By replacing just part of the network initially, an agency can see how it performs, or see that some of its legacy systems may not be compatible with the new network technology.

SECURITY IS NON-NEGOTIABLE

Federal agencies today know that network security is critical. It's part of every mandate and regulation, from the Federal Zero Trust Strategy to the Executive Order on Improving the Nation's Cybersecurity. And for good reason; cybercrime is at an all-time high. In the first half of 2021, public sector agencies experienced 44.6 million attacks of some type. While some were minor, others were large, impactful attacks sponsored by nation-states. When these attacks steal information and disrupt or deny access to resources, costs mount and services can come to a halt.

Helping to ensure that an agency's networks and Internet-connected devices are protected is more important than ever. Modern networks are more likely to employ tools and processes to help keep them safe, including Zero Trust, Zero Trust Network Access (ZTNA) for secure application access, SD-WANs and Secure Access Service Edge (SASE), which combines cloud-hosted security, ZTNA and advanced networking, enabling remote users to connect securely to resources from any location.

Agencies that need more security features also might consider an add-on solution like Comcast Business SecurityEdge™, which helps Comcast Business Internet customers block threats like malware, ransomware, phishing, and botnet attacks across all connected devices. In addition, it helps prevent users from accessing compromised websites and infected links while on the network.

CONCLUSION

Modernizing agency networks to the point where they can take advantage of cutting-edge technologies and processes takes time, but the benefits are clear. Modern networks can foster productivity by providing employees with reliable connectivity to data, applications and platforms from wherever they work. At the same time, modern networks can better handle rapid innovation, help improve security for both inbound and outbound connections, and position agencies to embrace future trends, technologies and processes. ■