Top 3 Networking Challenges for Federal Government

1. IT staff has limited time and resources to manage complex network demands.
   - 43% of IT time is spent troubleshooting; the #1 consumer of time (Cisco DNA Customer Survey)

2. Defending the network is hard. Attacks continue to increase.
   - 80% of security breaches occur within the perimeter (ZK Research)

3. As the demands on the network become more complex, controlling more wireless and IoT devices is becoming increasingly difficult.
   - 46% of network devices will be machine-to-machine by 2020 (Cisco VNI)

The Solution: Cisco DNA Center

DNA Center is the network manager, orchestrator and command center for Cisco DNA, an open, software-driven platform.

The Benefits

- End-to-end troubleshooting
- Automated provisioning of access switches
- Easily click and create virtual networks within the software defined network (SDN)
- Macro- and microsegmentation
- Stops attacks from spreading
- No VLANs or ACLs to configure
- Zero touch/rapid remote deployments
- Segment and control wireless and IoT devices
- Seamless, flexible environment for wired and wireless

Upgrade to Catalyst 9000 SDA-capable switches

DNA Assurance & Analytics

- FIPS Approved
- Encrypted Traffic Analysis

Shift IT time from maintaining the infrastructure to new projects

Analysis and testing with customers using SD-Access revealed that:
- Saved time on network provisioning: 67%
- Improved issue resolution: 80%
- Reduced operating expense: 81%

To learn more about DNA for government, visit cisco.com/go/FederalDNA