Borderless Networks Architecture: Connect Anyone, Anywhere, on Any Device

What You Will Learn

The business of government extends beyond physical walls, and so should government networks. IT teams need a new network architecture to securely deliver voice, video, and data services to employees and citizens anywhere, on any device.

This white paper, intended for government network architects, provides a high-level overview of the Cisco® Borderless Networks architecture, focusing on how it supports top government priorities:

- Increasing operational efficiency, to minimize total cost of ownership and increase agility
- Allowing secure access by different government users and citizens while guarding against network damage and unauthorized information disclosure
- Empowering a mobile workforce to access government services from the field, with performance comparable to the experience at headquarters
- Enabling collaboration within and between government agencies and with citizens, from anywhere and with any device
- Supporting virtual desktops that employees can access from anywhere

The Disappearance of Traditional Network Borders

Until recently, very clear borders surrounded government networks. The network extended only as far as the building walls; provided access only to government employees on office PCs or phones; and delivered voice, video, or data, not a combination of services.

Changes in workforce behavior, citizen expectations, and technology have impelled government to break down the traditional borders:

- **The world has become the workplace:** Employees increasingly work in the field, at home, in the car, and in airports.
- **Citizens expect self-service applications:** Citizens want the convenience of online tax filing, business license applications, and eligibility determination. Shifting citizen interactions to online channels when feasible also reduces government costs.
- **People want a choice of devices:** Employees and citizens alike want to access services from a smartphone or laptop, and over Wi-Fi, cellular, and wired networks.
- **New tools are transforming collaboration:** Voice-only conference calls have been supplanted by voice, video, and web collaboration sessions using technologies such as Cisco TelePresence™ systems and Cisco WebEx™ conferencing. Even the process of reaching a coworker has changed. In some governments, employees can view their coworkers' presence information to see if they are available, on the phone, or online, eliminating time spent dialing multiple numbers and leaving voicemail messages.

In summary, the borders that separate people based on location, role, and device are breaking down.

> “Taken together, the Borderless Networks architecture and the Cisco ISR G2 [Integrated Services Router Generation 2] form a sort of central nervous system network that simplifies the delivery of networked business services throughout IT organizations, large and small.”
> **— David Garner, InformationWeek**

Challenges for Network Architects

Delivering network access to anyone, anywhere, anytime, and using any device creates a new set of challenges for government IT teams. For example, a government that wants to adopt voice, video, and web collaboration tools needs a network architecture that can:

- Support converged voice and video
- Enable mobile workers to use government voice, voicemail, instant messaging, and other services when away from their offices
- Protect voice and video traffic from eavesdropping
- Deliver a lifelike voice and video experience that encourages adoption
- Avoid server sprawl, cable sprawl, and high power and cooling costs
- Support government’s move to cloud computing, where shared compute, memory, and storage resources are provided to agencies on demand

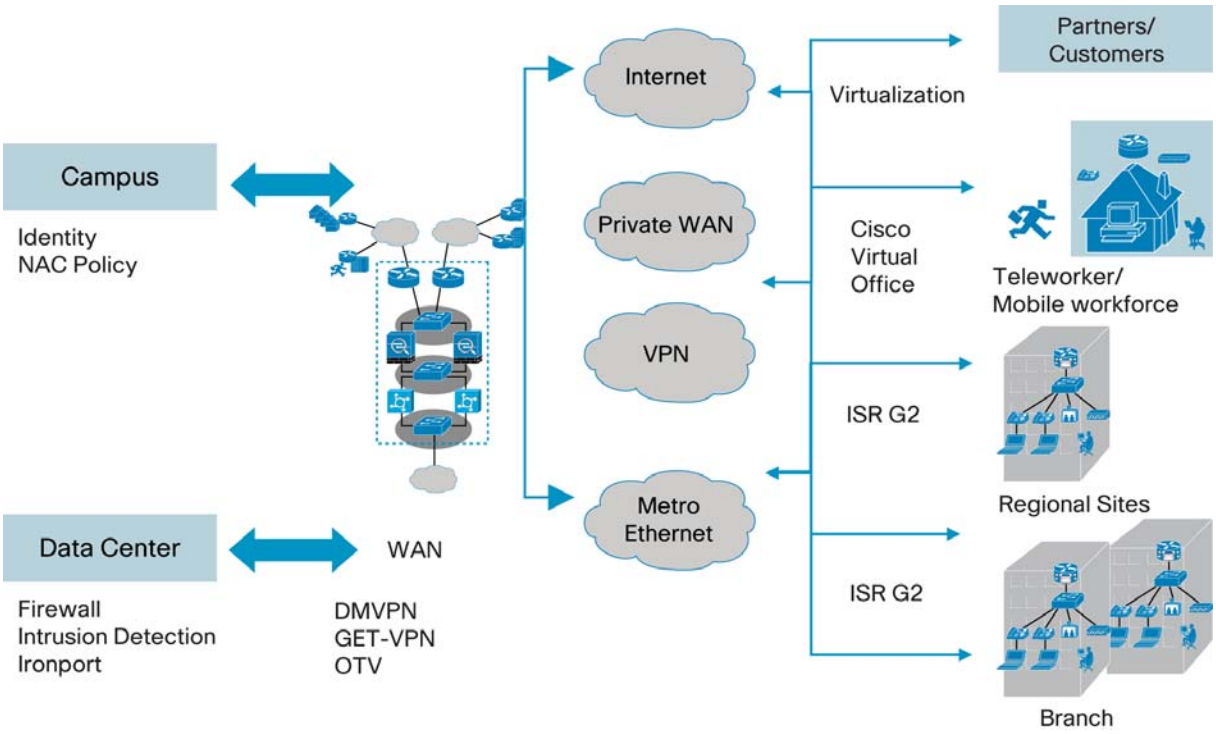
The remainder of the white paper discusses required elements of borderless network architecture: security, mobility, collaboration, virtualization, and operational efficiency.

Security

To confidently extend network access outside existing borders, governments need to protect assets from unauthorized disclosure and networks from unintentional or intentional damage. Implementing separate security solutions for each application is ineffective and costly. Government can improve network security posture and reduce management overhead by integrating security into the network fabric. This approach makes it easier to consistently apply security policies everywhere, including the main campus, data center, remote offices, and home offices, and for citizen access.

The Cisco Borderless Networks architecture authenticates users and devices using the identity-enabled network approach, and enables the government workforce to connect securely from anywhere, using new virtual private network (VPN) technologies. Figure shows how this architecture allows secure access over the Internet, private WAN, VPN, or Metro Ethernet network.

Figure 1. Borderless Security Enables Access From Anywhere



Identity-Enabled Network

Most agencies authenticate the user on the host itself. The drawback is that unauthorized users are already on the network before they are stopped, which increases the chances that intruders can steal private data or harm critical infrastructure. Host-based authentication also drains productivity, because government IT departments need to individually configure every application, and agency users need to take the time to sign in to each application separately.

In the Cisco Borderless Networks architecture, authentication is performed at the point when a user attempts to access the network. When an employee, contractor, or guest attempts to sign on to the agency network, the network confirms that the person and the device are authorized, and then connects the user to the appropriate VLAN. The IT department only needs to set up authentication once, not once for each application. And users only need to sign on once to access all network resources and applications, increasing productivity. Governments can continue using same technology when they move assets from the local network to the cloud.

The security technologies in the Cisco Borderless Networks architecture answer the following questions:

- **Who are you?** The user might be an agency employee, guest, contractor, or consultant. The device might be a PC or laptop, IP phone, video surveillance camera, or temperature or chemical sensor. The U.S. Information Awareness Office (IAO) requires use of 802.1X authentication.
- **Is your device healthy?** When a device attempts to connect to the agency network, it should be scanned to make sure it harbors no infections and has the required antivirus software, operating system patches, and security settings. Government IT departments save time if the security solution can automatically perform remediation on noncompliant devices.
- **Where can you go?** A budget analyst needs access to agency financials while an IT staffer needs access to network management tools. Neither should have access to the other's application.
- **What service level do you receive?** For example, first responders and military personnel need assured service levels for voice, video, and data.

- **What are you doing?** Government needs a record of which users have accessed which resources, and from where.

Secure VPN Connections

Traditional IP Security (IPsec) VPNs are difficult to scale. The Borderless Networks architecture includes advanced VPN technologies to simplify provisioning and maintenance:

- **Dynamic Multipoint VPN (DMVPN):** DMVPN provides secure connectivity between government offices and between offices and the main data center (Figure 2). Unlike traditional VPNs, DMVPNs do not require a permanent VPN connection between two endpoints, avoiding unnecessary bandwidth consumption. Closing the VPN connection when unneeded also reduces processor cycles needed to maintain state for routing protocols. Finally, DMVPNs provide zero-touch deployment, making it more practical to offer VPN access to large groups of users.
- **Group Encrypted Transport (GET) VPN:** GET VPNs do not use tunnels, eliminating the delays caused by IPsec tunnel negotiation (Figure 3). GET VPN complements DMVPN, aiding in delivering voice and video over the VPN.
- **Overlay Transport Virtualization (OTV):** Until recently, the only options for moving application workloads between government data centers for disaster recovery or data center consolidation were dark fiber or Multiprotocol Label Switching (MPLS). OTV, a feature of the Cisco Nexus® switch operating system, requires much less effort from IT departments. OTV allow local Ethernet traffic from a LAN to be tunneled over an IP network to create a “logical data center” spanning several data centers in different locations. Administrators can enable OTV by entering just a few commands for each site, and then easily move virtual machines over the network. Security policies and administrative policies travel with each virtual machine as it moves between servers.

Figure 2. Dynamic Multipoint VPNs Reduce Bandwidth Overhead, Increasing Scalability

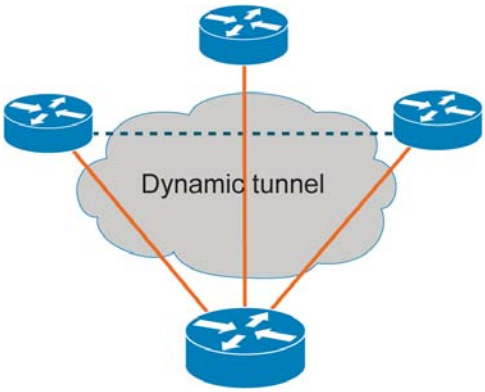
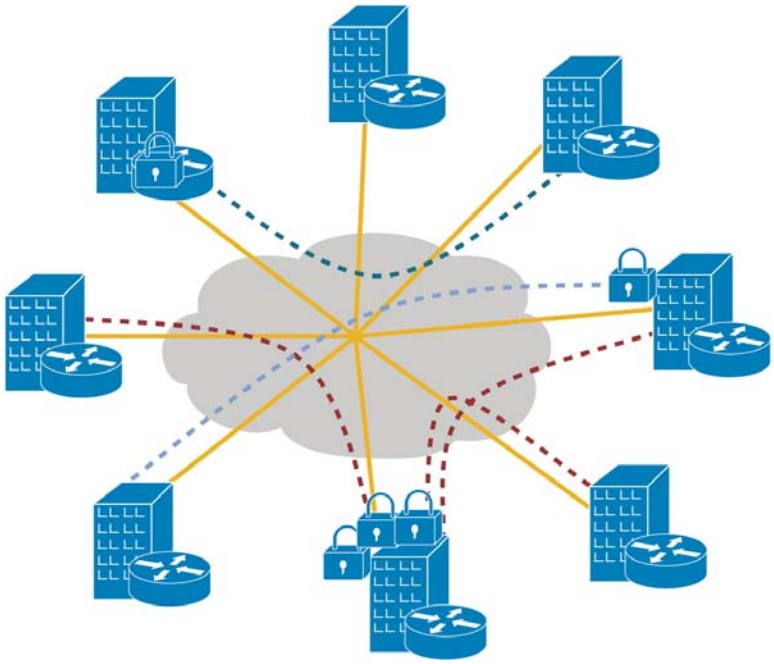


Figure 3. GET VPNs Eliminate the Time Needed to Establish Tunnels



Mobility

A borderless network extends to field workers, teleworkers, and citizens at home, as well as people on the move who connect over Wi-Fi and cellular networks using laptops and smartphones. Mobility solutions cost less to operate when they can be managed in conjunction with the government's wired network and share the same security architecture.

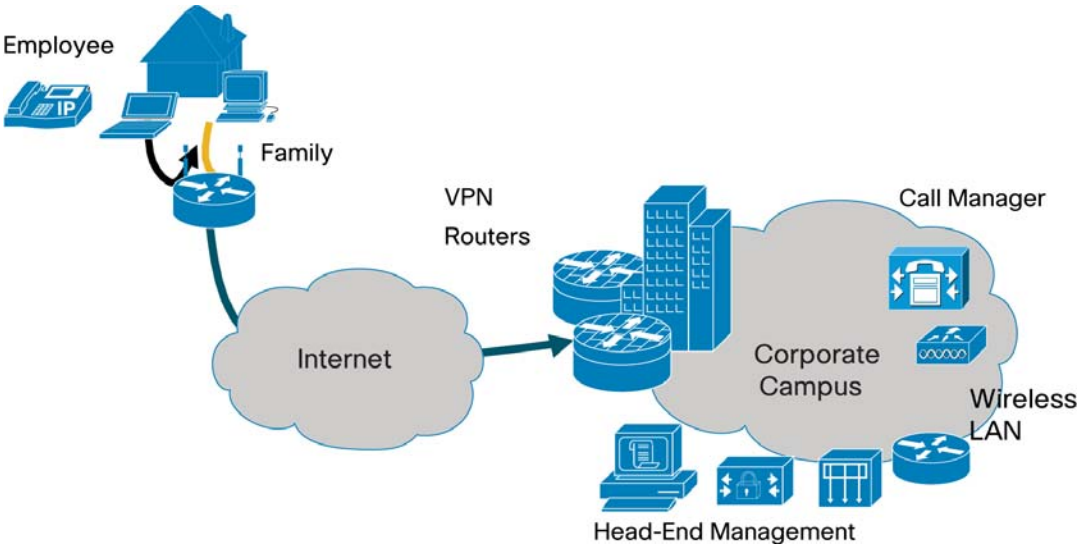
Following are enabling technologies in the Borderless Networks architecture for mobility.

Telework Solutions

As of 2009, the U.S. federal government Office of Personnel Management said that 103,000 teleworkers in 78 agencies worked from home at least once a month. Benefits of telework range from enhanced continuity of operations (COOP) to improved morale and environmental sustainability. Barriers to even more widespread adoption of telework have included somewhat diminished voice and video quality, lack of some of the collaboration tools available in the office, and a complicated sign-on process.

These barriers have been overcome with the Cisco Virtual Office solution. It provides all components required for telework, from the VPN router and management software at headquarters to the IP phone and router with integrated wireless access at the employee's home (Figure 4). Cisco Virtual Office requires almost no provisioning support from government IT groups. Employees simply receive a router and IP phone that they connect at home. When they enter a given URL on their home PC, the website instructs the router to connect back to the agency network to automatically provision itself.

Figure 4. Cisco Virtual Office Configures Itself Over the Network



WAN Optimization and Application Acceleration

Teleworkers typically have a DSL or cable connection at home, which often does not provide adequate bandwidth for video, image-based applications, or even large spreadsheets. Cisco Wide Area Application Services (WAAS) Mobile is software for the PC that operates in conjunction with a Cisco Wide Area Application Engine at the data center to optimize existing WAN bandwidth and accelerate applications. In Denmark, the Lolland municipality implemented Cisco WAAS Mobile so that remote office workers could access data center applications over ADSL connections with 2-Mbps downstream speeds. For the first time, water plant employees could use a centralized mapping application to see where pipes were buried, helping the government find and repair leaks faster. Similarly, financial personnel became more productive because they could access the centralized enterprise resource planning (ERP) application and share spreadsheets. Lolland municipality nurses who visit elderly patients in their homes will soon be able to use Cisco WAAS Mobile to update patient medical records from patients' homes, over the cellular network.

Similarly, the U.S. Peace Corps uses Cisco WAAS so that volunteers in different global offices can share files on a centralized Microsoft SharePoint server in Washington D.C. By avoiding the need for bandwidth upgrades, the Peace Corps saved US$185,315 in the first year alone, and projects savings of $642,610 by the end of 2011, when all 26 sites will have deployed Cisco WAAS.

Location-Based Services

Some government departments need to be aware of the location, condition, and status of mobile assets and people, for example, to:

- Track the location of valuable assets
- Find moveable assets, such as wheelchairs and IV pumps in a healthcare facility
- Locate personnel, such as the closest security officer
- Receive an alert when assets are removed from a defined area
- Detect and pinpoint the location of unauthorized wireless access points that can threaten the security of government networks

The Cisco Unified Wireless Control System can detect the location of all 802.11x devices, including laptops and smartphones, in the wireless coverage area. A government security department, for example, can see the location of officers on a facility map by tracking the location of their Wi-Fi-enabled smartphones. Governments can track the location of non-Wi-Fi-enabled assets by affixing them with active RFID tags. Specialized tags can also transmit environmental or telemetry information, such as temperature, humidity, vibration, fuel levels, and so on. If a tagged item moves outside of a defined area, an alarm can sound.

Combine Wireless and Wired Connectivity in One Device

Traditionally, governments have deployed separate controllers for wired and wireless connectivity, each with its own security system. Separately enforcing security polices on the wired and wireless networks does not make sense in today's borderless networks. Instead, the wireless network should be an extension of the wired network, offering access to the same government services and sharing the same security policies.

The Cisco Unified Wireless Network defined in the Cisco Borderless Networks architecture provides the same level of security, scalability, reliability, ease of deployment, and management available in wired LANs. An important element is the Cisco Catalyst® 6500 Series Wireless Services Module (WiSM), which provides pervasive, campus-wide wireless services. Integrated into the Cisco Catalyst 6500 Series Switch, the WiSM simplifies deployment and management and minimizes the number of devices to manage, power, and cool.

> "Rather than an either-or proposition, many IT managers are finding, after careful consideration of their current network infrastructure as well as their roadmap for future applications, that the best solution is an Aristotelian 'Golden Mean' solution that includes using both wire line technology and wireless technology wherever each is most effective."
>
> **— Stan Schatt, Vice President and Practice Director for Wireless Connectivity, ABIresearch**

Power over Ethernet Plus

Power over Ethernet (PoE) enables mobility on government campuses by eliminating the expense of bringing power lines to remote wireless access points. Instead, a power supply within a Cisco switch or router safely delivers power over the Ethernet cable. Cisco is the first networking vendor to support the IEEE 802.3at PoE standard, sometimes called POE+. The 802.3at standard provides up to 25 watts of power, supporting new 802.11n wireless access points.

Collaboration

Collaboration has supplanted automation as the most promising opportunity to increase government service levels and innovation. Using modern collaboration tools over a borderless network, people can come together from any location with a network connection, including agency headquarters, home, or local government offices near the employee's home or work. By enabling network-based collaboration within and between agencies and with citizens, governments become more agile, reduce costs, and make smarter use of human capital. Used in place of travel, network-based collaboration avoids service delays, lost productivity, expense, and greenhouse gas emissions.

Examples of collaboration tools used today in governments include instant messaging, presence, video telephony, Cisco WebEx and Cisco TelePresence conferencing, and Web 2.0 technologies such as team workspaces.

Employees embrace business video as an alternative to in-person meetings only if the network delivers an excellent user experience. This requires adequate bandwidth as well as quality of service (QoS), which gives priority to latency-sensitive traffic, such as video or voice. QoS is far more noticeable for business video than it is for data applications. If a packet does not arrive for a web-based application, the application can simply resend, and most users will not notice the slight delay in redrawing a web page. In contrast, business video applications do not resend if a packet is dropped. Even a very small percentage of dropped packets is very noticeable because the application might be sending thousands of packets.

To support the increasing use of business video in government, the Cisco Borderless Networks architecture defines a medianet, or media-optimized network. The medianet uses multiple technologies to deliver high-quality voice and video on the same network that carries data and sensor traffic. Some of the technologies include:

- **Media-aware routing:** The network has the intelligence to treat video streams differently depending on whether the employee or citizen is using a PC, smartphone, or other endpoint. Delivering the maximum resolution the device supports improves the user experience; not delivering more resolution than needed reduces bandwidth usage. The Cisco Media Experience Engine (MXE) intelligently senses the device used to view live video streams or video on demand and delivers the video accordingly.
- **Media monitoring:** Embedded smart diagnostics and monitoring tools in Cisco switches and routers help government IT teams quickly troubleshoot and isolate issues.
- **Rich-media network services:** These services, built into Cisco routing and switching infrastructure and voice and video endpoints, enable applications that combine voice, video, and data, such as Cisco WebEx conferencing.
- **APIs:** Government developers can use open APIs to integrate Cisco collaboration tools into business applications. Examples include adding a click-to-call button to internal and citizen-facing websites, or billing usage of Cisco Unified Communications Manager by department.

Virtualization

The Borderless Networks architecture not only untethers government workers from their desks, it also decouples applications from a particular server and data center. Virtualization technology enables an application and operation system, or virtual machine (VM), to move easily between one server and another, and even between data centers. Virtualization improves server utilization to reduce costs; reduces space, power, and cooling costs; and supports COOP.

Organizations often virtualize their services in five phases, shown in Table 1.

Table 1. Phased Approach to Virtualization

Phase	Requirement	Solution
Data center consolidation	Enable LAN-like performance over the WAN	Cisco Wide Area Application Services (WAAS)
	Load balance application workload, as centralized data center receives more traffic	Cisco Application Control Engine (ACE)
	Virtualize storage area network, avoiding the need for separate SANs	Cisco MDS 9000 Series multilayer director switch
Unified fabric	Consolidate separate data and storage networks, reducing costs of cables, server interface cards, and switch ports	Cisco Nexus Family switch with Fibre Channel over Ethernet (FCoE) Support
Unified computing	Unify compute, network, storage, and virtualization in a single management entity	Cisco Unified Computing System
	Apply network, security, and storage policy to individual virtual machines, so that it follows the VM as it moves between servers	Cisco VN-Link
Cloud	Allow multiple organizations to securely share from a common pool of resources for compute, networking, and resources, reducing government costs	The complete suite of Cisco data center virtualization solutions

Cisco VN-Link technology addresses the final barrier to widespread adoption of server virtualization in government:

- Applies network, security, and storage policy at the VM level. The policy moves along with the VM during live migration.
- Provides visibility into individual VMs, not just the server as a whole, to simplify troubleshooting,
- Preserves organizational roles in the IT group by providing role-based access to VM server, storage, and network policy

In VMware vSphere environments, Cisco VN-Link network services are available in the Cisco Nexus 1000V Switch, a software-based switch for the Cisco Unified Computing System. In the future, Cisco VN-Link will also be available through switches that support a new standards-based virtual networking protocol developed by Cisco and VMware and presented to IEEE.

Operational Efficiency

Tools that increase operational efficiency decrease total cost of ownership and provide the agility to adapt to changing citizen needs and technology capabilities. The Cisco Borderless Network architecture includes technologies for network resiliency as well as easy adaptation to changing application requirements and user devices.

Network Resiliency

The Cisco Borderless Network architecture helps to ensure network resiliency with the following capabilities:

- **No service interruption in the event of a switch failure:** With Cisco Virtual Switching System (VSS) technology, two Cisco Catalyst switches operate as a pair. If one switch should fail, the other switch takes over in less than 200 milliseconds.
- **Rapid replacement of failed switches:** With Cisco StackWise® technology, up to nine switches can operate as one 32-Gbps virtual switch. If one switch fails, the IT department can replace it with a new, unconfigured switch. The stack configures the new switch without human intervention, minimizing downtime.
- **Software upgrades without downtime:** IT departments can apply bug fixes and deploy new network features without interrupting existing services, using the Cisco In-Service Software Upgrade (ISSU) feature.
- **Online diagnostics, to accelerate troubleshooting:** Cisco Generic Online Diagnostics (GOLD) provides a common framework to diagnose all network equipment using Cisco IOS® Software. The platform-specific diagnostics take appropriate corrective action in response to diagnostics test results.

Adaptability to Support New Government Services

Simplifying provisioning of new switches and ports helps government accelerate new service introduction while minimizing total cost of ownership. The Cisco Borderless Networks architecture supports government agility with the following features:

- **Zero-touch deployments:** With Cisco Smart Ports, IT departments can centrally administer security patches, bug fixes, enhancements, and new services. Avoiding the need to schedule visits to each office speeds up implementation time and can avoid downtime due to unpatched systems. When the IT team adds new devices to the network, a wizard embedded in Cisco IOS Software automatically detects the type of line connected to the switch port, eliminating time spent manually configuring the port.
- **Rapid upgrade to 10 Gigabit Ethernet:** To support server virtualization and business video, governments are upgrading to 10 Gigabit Ethernet connectivity. IT departments can upgrade Cisco switches to 10 Gigabit Ethernet in 10 seconds. The first step is hot-swapping the TwinGig module with a 10G transceiver, and then provisioning the edge switch with 10 Gigabit Ethernet. Within 10 seconds of auto detect and configuration, the network delivers 10 Gigabit Ethernet from the edge, with no chassis replacement.

- **Remote installation and troubleshooting:** Some government organizations need to staff the network operations center 24 hours a day, simply to have someone available if an error occurs. Using management tools such as Cisco Network Assistant and CiscoWorks, IT personnel can provision and troubleshoot remotely, saving the time to walk or drive to remote offices. Cisco devices with the Smart Call Home feature continually perform proactive diagnostics on their own components to provide real-time alerts and remediation advice when an issue is detected.
- **Automatic QoS configuration:** QoS assigns priority to different types of application traffic traveling over the borderless network. Latency-sensitive applications such as voice and video need higher priority than, say, email. Previously, a network administrator had to manually apply QoS settings to all switches and routers. Now, Cisco AutoQoS automatically configures QoS, applying policies to multiple ports with a single command. This saves time, eliminates need for in-house expertise, and reduces configuration errors.
- **Automated event management:** Ordinarily, network administrators have to manually react to events such as configuring switch interfaces for a new device, or a high error rate on an interface. Cisco IOS Embedded Event Manager automates response. For example, the agency IT team might develop a script that determines the details of a newly connected device and automatically configures the port. Another script might react to a high error rate on a particular interface by notifying network operations personnel and redirecting traffic over a more stable path. Benefits of automated event management are faster reaction, decreased network downtime, and automated response at any time of day.
- **Secure guest access:** A borderless network extends to contractors on the government premises. Rather than building and maintaining a separate network for guest access, government can create a secure VLAN for guest access, using the Virtual Device Context (VDC) feature of the Cisco Nexus 7000 Series Switch.
- **Environmental sustainability:** Green practices are good for government budgets as well as the environment. Cisco EnergyWise provides visibility into power consumption throughout the agency. In addition, PoE reduces the number of power outlets needed in new government buildings, reducing building costs.

Why Cisco

Governments around the world rely on Cisco solutions to increase service efficiency and enhance citizen interactions. Among the first public-sector organizations to adopt the Cisco Borderless Networks architecture is Dexter Community Schools, in Dexter, Michigan. Some of the reasons public sector organizations select Cisco include:

- End-to-end solutions, including the network platform as well as security, collaboration, mobility, and virtualization solutions that operate in collaboration with the network
- A wide variety of integrated tools to reduce total cost of ownership, such as CiscoWorks and Cisco VN-Link
- A world-class Technical Assistance Center (TAC), staffed by more than 200 experts with CCIE® certification
- Smart Business Architecture, which provides best practices for network design for organizations with 100 to 1000 users
- Cisco Validated Designs for specific applications, such as collaboration, to help accelerate deployment
- Cisco SAFE architecture, a large-scale security blueprint
- Customized implementations for different use cases, such as Cyberspace Action for Education (CAFÉ), all tested, validated, and documented to reduce deployment time and cost

Conclusion

Employees and citizens have changed their work habits and expectations. They work outside the office, are just as likely to connect using a smartphone or other mobile device as a desktop PC, and have come to expect real-time video and video on demand. To adapt to these new behavior patterns, government IT organizations need a cost-effective architecture to bring together their previously separate networks for voice, video, data, and mobility.

The Cisco Borderless Networks architecture meets the need, defining a tested approach to extend the government network to connect anyone, anywhere, using any device. Security technologies enable networks to extend beyond building walls. Virtualization and advanced tools for network operations reduce costs and automate processes to support today's 24-hour network operations. And solutions for mobility and collaboration help to increase government service levels, support citizen self-service, and empower an increasingly mobile workforce.

For More Information

To learn more about Cisco Borderless Network technologies, visit http://www.cisco.com/go/borderless.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-602130-00 05/10