

How Cisco IT is Building a Unified Access Network: Wired and Wireless

Catalyst 3850 Switches support BYOD, increase application visibility, and lower operational overhead.

EXECUTIVE SUMMARY	
CHALLENGE	• Prepare for current and future enterprise challenges • Support bring-your-own-device (BYOD) adoption by improving wireless experience • Reduce total cost of ownership by minimizing network support requirements
SOLUTION	• Unified the access architecture by replacing access layer switches with Cisco Catalyst 3850 Switches • Consolidating to one policy, one management strategy, and one network strategy • Left core and aggregation layers unchanged
RESULTS	• Increased workplace efficiency by making the wireless experience equivalent to the wired experience • Reduced network management burden, and decreased helpdesk call volume • Lowered switch and controller count, reducing capital and operational expense
NEXT STEPS	• Continue implementing Cisco Catalyst 3850 Switches in branch offices as part of normal fleet upgrade cycle • Integrate policy management with unified access using Cisco Identity Services Engine • Take advantage of network programmability to simplify operations, using Cisco Open Networking Environment (ONE) architecture

Challenge

Cisco IT aligns its initiatives with enterprise business strategies such as globalization, employee engagement, innovation, and new business models. An ongoing initiative to support these strategies is to consolidate previously separate networks for wired and wireless traffic to a unified access architecture. The goal is one network, one policy, and one management architecture.

“We had two immediate motivations for unifying the wired and wireless networks,” says Brian Christensen, senior director of Global Infrastructure Services for Cisco IT. “One was to narrow the performance gap between wired and wireless infrastructures to support the growing BYOD [bring-your-own-device] trend. The other was to reduce operational overhead by consolidating to a single access policy and management toolset.”

Cisco employees have already registered more than 55,000 personal smartphones, tablets, and other devices to connect to the Cisco network. Although Cisco IT continually improves its wireless networks and has adopted the 802.11n standard, the wired and wireless experiences remain noticeably different. Users especially noticed the performance gap when using smartphones or tablets to access rich-media applications, such as video. “Making the wireless experience closely comparable to the wired experience would enable

employees to work productively from anywhere and encourage collaboration,” says Jawahar Sivasankaran, distinguished engineer with the Cisco IT Customer Strategy and Success team.

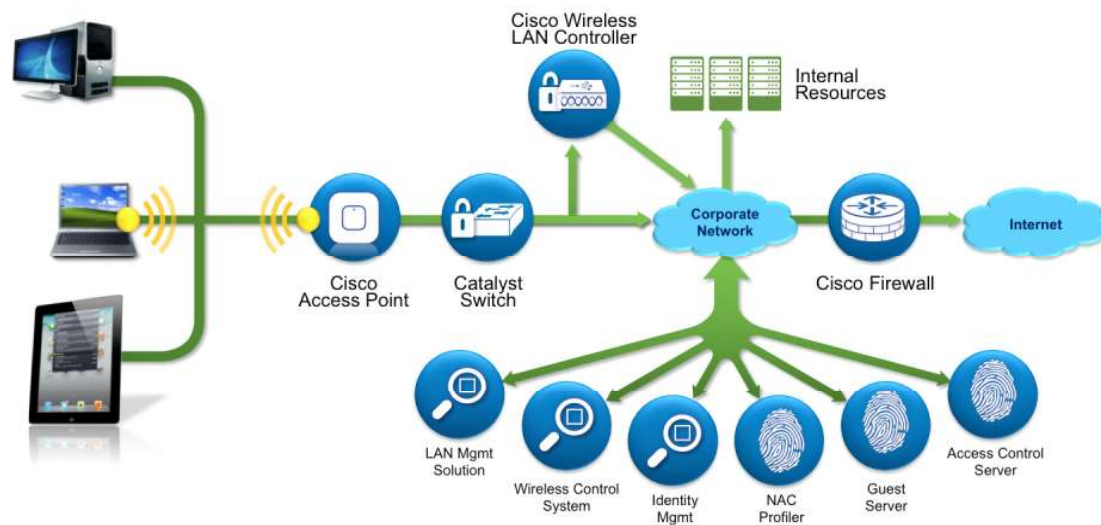
“We had two immediate motivations for unifying the wired and wireless networks. One was to narrow the performance gap between wired and wireless infrastructures to support the growing BYOD trend. The other was to reduce operational overhead by consolidating from two to one access policies and management toolsets.”

Brian Christensen, Senior Director of Global Infrastructure Services , Cisco IT

The main reason for the difference in performance is that most Cisco locations receive wireless services through a centralized controller in another building (Figure 1). The traffic is encapsulated from the edge to the controller, resulting in separate logical and physical connectivity steps. This design also makes it difficult to apply services that improve the user experience, such as WAN optimization, quality of service (QoS), and access control lists (ACLs).

Another reason for the performance gap is that wireless is a shared media, meaning that total available bandwidth is divided among all concurrent connections. “We knew we could provide better support for BYOD if the wired and wireless networks didn’t treat traffic differently,” says Leigh Jewell, member of the technical staff with Cisco IT.

Figure 1. Cisco Offices Previously Had Separate Wired and Wireless Network Infrastructure



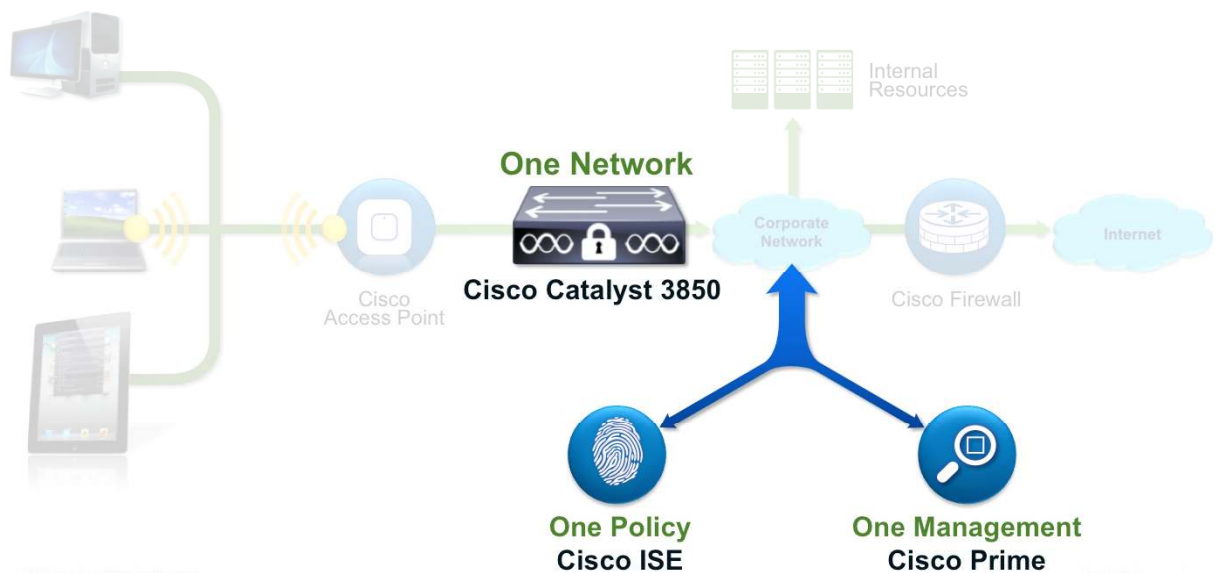
Building a unified access network would also simplify IT operations and management. As it was, the Cisco IT team needed different tools and processes to manage and enforce policy for the wired and wireless networks, increasing costs.

Solution

Cisco IT has implemented its first unified access network, serving three buildings in the San Jose, California campus and another building in Sydney, Australia. The network is currently used in global production by approximately 1000 users. The next step is to roll out the unified access network across the entire Cisco enterprise, beginning with global branch offices.

The foundation of the unified access network is the Cisco Catalyst 3850 Switch, a next-generation stackable switch with an embedded wireless controller that provides fully converged wired and wireless traffic at the access layer. The switch integrates the physical and logical layers of the wired and wireless networks, treating wired and wireless traffic in exactly the same way (Figure 2).

Figure 2. Unified Access Network: Wireless and Wired Experience is Comparable Because Traffic is Treated the Same Way



Unified Policy Management

To enforce a unified policy across wired, wireless, and remote access environments, Cisco IT is implementing Cisco Identity Services Engine (ISE). The goal is to increase security for the BYOD program by providing profiling, registration, and posture enforcement for personal devices. "Our users now have the same experience whether they connect through wired, wireless, or remote access, an important factor in the BYOD experience," Sivasankaran says. A single point of policy enforcement for wired and wireless networks also simplifies IT operations.

“Our users now have the same experience whether they connect through wired, wireless, or remote access, an important factor in BYOD experience.”

—Jawahar Sivasankaran, Distinguished Engineer, Cisco IT Customer Strategy and Success team

The first phase of the deployment focuses on profiling devices. This enables Cisco IT to identify the type of devices connecting to the enterprise environment. Cisco IT is enforcing a BYOD onboarding program in which BYOD devices go through a registration process when connecting to the corporate network. The posture management and enforcement steps enable Cisco IT to secure and manage BYOD devices. This solution also integrates with the existing Mobile Device Management platform that IT has deployed for deeper policy management.

Deployment Process

The transition to One Network involved replacing existing access layer switches with Cisco Catalyst 3850 Switches, leaving the aggregation and core layers intact. Like any other organization, Cisco IT has a strong change management program. The change management in this case involved combining the wired and wireless implementations. “We didn’t encounter any problems during the transition,” says Travis Norling, Cisco IT engineer. “The process took no more than a few minutes for each cable rack, and we completed the transition for an entire building overnight during a short maintenance window.”

The Cisco IT team applied the following best practices during deployment:

- Used color-coded cable labels to distinguish runs from wired jacks and wireless access points.
- Carefully planned mobility zoning and grouping.
- Implemented an efficient design for L2 and L3 roaming and the mobility controller. This gives Cisco IT the flexibility to transition to a L3-edge access design in the future.
- Reused command sets when transitioning software configurations to the new platform, reducing any additional training requirements.

Results

Increased Workforce Efficiency

The unified access platform has positioned Cisco IT to more easily support a mobile workforce, BYOD, and growing use of internal and external cloud services. Users participating in this ongoing deployment see that the throughput and application response has improved, especially for video and rich media traffic. “The unified access network improves the voice and video experience as we can mark QoS earlier in the process and enforce a single set of QoS policies that are common across wired and wireless,” says Michael Anderson, senior network IT design manager for Cisco. “Now that the wireless voice and video experience is similar, employees are more likely to collaborate from wherever they are, with any device, rather than taking the time to walk back to their offices. This increases productivity.”

Operational Efficiency for IT Team

Implementing Cisco Catalyst 3850 Switches at the access layer is freeing up time for IT innovation by reducing support requirements:

- Unified access eliminates the need to manage separate wired and wireless VLANs. Unifying the VLANs assigned for wireless and wired networks simplified the implementation and operations strategy and enabled more efficient IP address space allocation. “A unified access network needs up to 25 percent fewer addresses, depending on the topology,” says Dipesh Patel, IT architect. “We’ll simplify operations even more when we consolidate the address space for wired and wireless networks in hundreds of branch offices.” This design is integrated with Cisco IT’s ongoing IPv6 program, which is progressing towards a dual-stack environment for all of the company’s 500 office sites.
- Helpdesk calls related to wireless connectivity decreased by approximately 10 percent after Cisco IT implemented the Cisco Catalyst 3850 Switch. A few years ago, Cisco IT elevated the wireless network support priority to the same level as wired network support. “This One Network strategy truly aligns the performance capabilities and user expectations with the SLA offered by Cisco IT,” says Sivasankaran.
- Visibility across wired and wireless networks accelerates troubleshooting. When wireless users reported issues with performance, while at the same time wired users were happy with the performance—for example, when accessing a high-definition video stream—Cisco IT had to use different tools and tests to isolate and resolve the problem. “Before we deployed the Catalyst 3850 for unified access, identifying bottlenecks in multicast-sourced video was very cumbersome because the wireless path deviated significantly from the wired path,” Norling says. Cisco IT can look into the same network path and use the same tools for deep-packet inspection and application analysis on wired and wireless traffic.
- Configuring one instead of two devices for BYOD simplifies program management: “Configuring the backend infrastructure for BYOD took quite a bit of time when we had to do it in two places,” says Kumar Ramachandra-Rao, Cisco IT manager. “Our ongoing implementation of Cisco Prime Unified Management in conjunction with unified access is simplifying global operations.” Consolidating to one management platform also helps to avoid mistakes implementing policies and ACLs for the wireless network.
- Simplifying Cisco Catalyst 3850 Switch configuration: Simplified configuration on the wireless infrastructure enables Cisco IT to configure the switches by applying templates. This reduces operational costs and increases availability by reducing configuration errors.
- Lowering capital, energy, and cable costs: So far, Cisco IT has retired over a dozen existing switches at the access layer, and also a pair of wireless LAN controllers. Reducing the device count decreases space, power, and cooling costs; lowers the number of cable drops needed in new facilities; and reduces operational costs.

Next Steps

Next steps for Cisco IT’s unified access strategy include:

- Implementing the Cisco Catalyst 3850 in branch offices following the normal fleet upgrade cycle.
- Extending the unified access architecture to campus sites.
- Closely integrating security and policy management with unified access.
- Taking advantage of Cisco automation tools, such as Auto Smart Ports. With this capability, Cisco IT will be able to ship Cisco Catalyst 3850 Switches to branch offices anywhere in the world. After a local

employee connects the switch to the network, it will configure itself based on a predefined configuration template.

- Simplifying operations and reduce TCO with software-defined networking (SDN) and related programmable network strategies. Using the Cisco Open Networking Environment (ONE) architecture, Cisco IT can support network programmability using internal or third-party applications.

For More Information

To learn more about Cisco Unified Access, visit: www.cisco.com/go/unifiedaccess.

To read an IT insight paper on Cisco's BYOD program, visit:

www.cisco.com/web/about/ciscolatwork/borderless_networks/docs/Cisco_IT_Insights_BYOD_Updated.pdf

To read additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit.

Note

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.



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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)