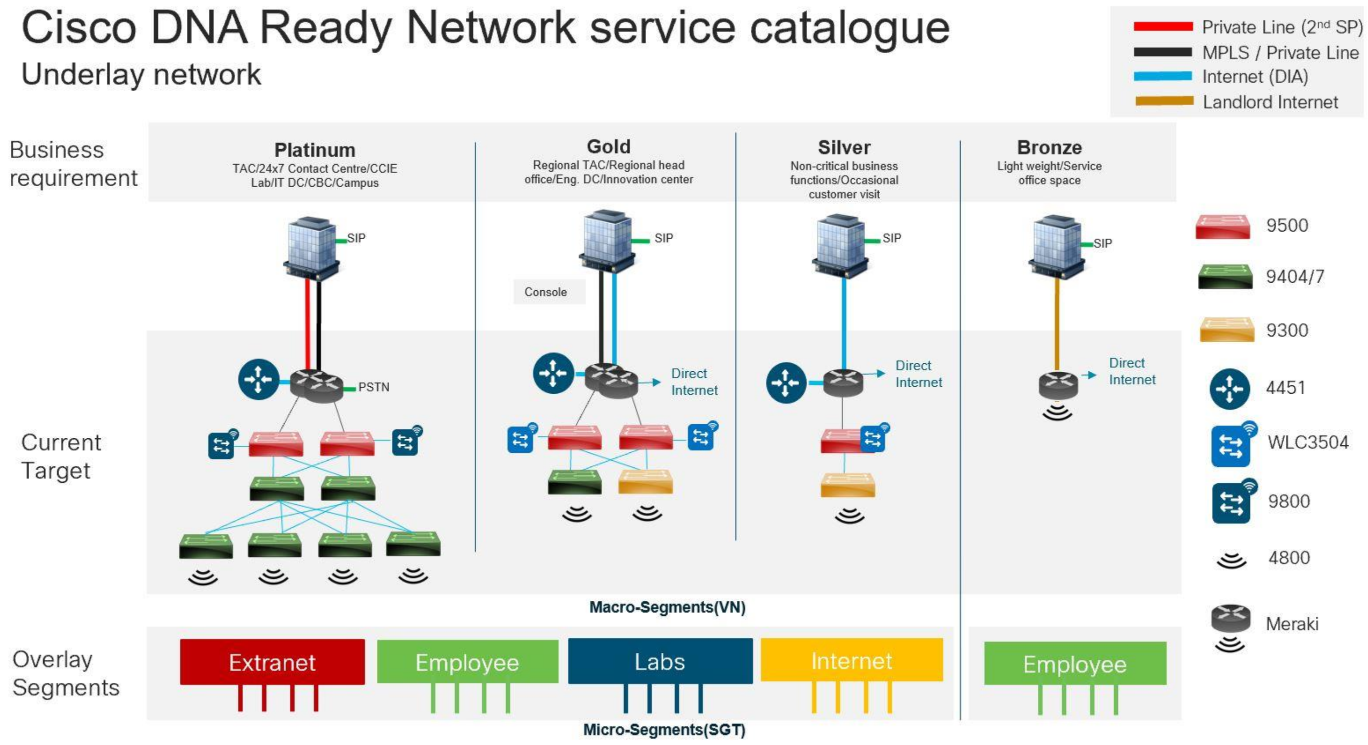
Cisco IT Case Study

Location doesn’t matter, with Catalyst 9000s and software-defined access

Cisco IT manages thousands of switches in more than 400 global offices. We’re always looking for ways to strengthen compliance with security policy, improve the user experience, and simplify our jobs to make more time for innovation. As “customer zero” for new Catalyst 9000 switch features, we try out different use cases, develop deployment guidelines, and influence new feature development. “We were excited about using Catalyst 9000 switches to add capacity to our wireless infrastructure without having to rewire horizontal cable runs,” says Leigh Jewell, Cisco IT architect. “I was also very interested to trial software-defined access (SD-Access) to see how it could extend and complement our existing TrustSec deployment.”

Our new network design, shown in this figure, uses Catalyst 9000s of different sizes to match device count and traffic volume.



A parallel Catalyst 9000 network for testing

Trying out new features in a production network is risky, so we built a parallel network in our North Sydney, Australia office to experiment with the new Catalyst 9000. The existing network (Catalyst 3850 and 4500 switches) continued to operate during our early trials. The new network combines our wired and wireless LANs into a single fabric. It consists of 22 Catalyst 9300 switches on three floors—two stacks on each floor. We plan to run this parallel network for some time, trying out new switch features as soon as they’re available so we can share our experiences with customers. Lessons learned are guiding our global migration to Catalyst 9000 switches in our other branch offices.

Software-defined access

The 9300 network in Sydney is Cisco's first SD-Access network. Just as we do in our global production network, we use Identity Services Engine (ISE) to set policy for individual users—for example, limiting their access to specific applications. Enforcing security policies based on identity rather than location saves time for IT and gives people more flexibility to choose where they work. "In the past we assigned users to a specific VLAN depending on their job role at a specific site," Jewell says. "But whenever someone moved to a different floor, we had to move their configuration with them. Now ISE applies the appropriate security policy no matter where users connect from because they authenticate via 802.1X."

Faster certification of new configurations

To simplify management, we previously used just two sizes of switches (the stackable Catalyst 3850 and 4500) despite the wide range of office sizes across Cisco. But management still wasn't as simple as we'd like because each switch runs a different version of IOS software. That meant we had to certify any new code or code update twice. For example, if we wanted to change the quality of service (QoS) configuration for phones, we had to write a different test plan each switch platform, with different commands and a different target test result.

Certifying new code and configurations is twice as fast on Catalyst 9000s because every switch in the family uses the same software: IOS XE. And the fact that all switches in the 9000 family have the same features simplifies operations.

Centrally defined configuration, pushed out from Cisco DNA Center

We don't configure the 9000 switches in Sydney. When we connect a switch to the network, Cisco DNA Center pushes out a configuration that our central engineering team has extensively tested. (Cisco DNA Center looks at the model and serial number to select the right configuration.) The minor fine-tuning we did took less than 15 minutes in total for all 22 switches.

Better security compliance—with one consistent policy stored in high-speed memory

Our previous switch platforms don't implement security policy in the same way because of memory constraints. That means administrators have to follow different procedures, leading to delays and possible mistakes. Now our security policy is uniform and consistent because all Catalyst 9000 models implement policy the same way.

20% more capacity for our wireless access points

Our Sydney office is designed as a Cisco Connected Workplace, meaning that instead of working at an assigned desk we move around throughout the day to the best space for the task at hand: conference room, casual seating area, audio privacy room, etc. (Read the Connected Workplace case study here.) Keeping up with growing demand for wireless requires either more access points or a way to support more connections on existing access points.

"The Catalyst 9300s deliver five times more Ethernet capacity to our wireless access points, providing wired-like performance," Jewell says. The reason: the 9300s can deliver 2.5 or 5Gbps over the existing copper cabling to access points that support Multigigabit Technology. We currently use Aironet 4800s running 802.11ac Wave 2, which take full advantage of the Catalyst 9000's Multigigabit Technology to eliminate bottlenecks in the Ethernet connection. "We can scale bandwidth without changing the cable plant by installing newer access points," Jewell says. "We're saving $250-$1000 per access point—and we have tens of thousands of access points."

> "The Catalyst 9300s deliver five times more Ethernet capacity to our wireless access points, providing wired-like performance."
>
> **—Leigh Jewell, IT Architect**

Faster troubleshooting and remediation

Soon after the new network went live, an executive reported problems connecting to wireless. “Looking at the Cisco DNA Center dashboard, we very quickly saw that the wireless controller had been configured to use ISE in the wrong region, causing a delay,” Jewell says. The administrator swapped to the correct authentication servers with the click of a button.

Overcoming early challenges

As customer zero we encountered a few bugs that we reported to the engineering team. The engineering team promptly fixed them, giving customers the benefit our testing.

We also had to adjust our culture. Having the switches connect to Cisco DNA Center for a centrally defined configuration saves us a lot of time; the tradeoff is that we have a little less autonomy.

Next steps

As customer zero for new Catalyst 9000 features, we continue to share ideas with the business unit to make the platform even better. For example, currently we completely wipe the previous configuration before re-configuring. That’s fine for the current deployment but could cause unacceptable delays when we’re using the switches in hundreds of offices. Therefore, we’ve asked the business unit to support incremental updates—just the parts of the configuration that have changed.

Our testing has expanded to include other Catalyst 9000 models that will soon be part of our production environment: Catalyst 9400s for larger branch office sites, Catalyst 9500s for our largest branch offices, and potentially Catalyst 9600s for some of our large campus sites.

Other plans:

- Continue using Cisco DNA Center for zero-touch deployment, saving significant time as we upgrade more than 6000 switches in more than 400 sites.
- Continue gathering network baseline data with our Cisco DNA Assurance analytics tools and gain more experience with the network and wireless assurance monitoring and troubleshooting features.
- Extend segmentation across our full intuitive network by integrating Cisco SD-Access, SD-WAN, and Application-Centric Infrastructure (ACI). This work has begun. When traffic moves across segments, the firewall will enforce policy. “The added bonus of segments is that the SD-WAN can make intelligent traffic engineering decisions based on the network that the device is connected to,” Jewell says. “For example, lab traffic can be directed to a low-cost backup link.”
- Use the dual-stack support (IPv4 and IPv6) in Cisco DNA Center 1.3, which gives users the same experience with servers or applications using either protocol.
- Centrally manage the Catalyst 9000 switches on multiple sites

For more information

Cisco Catalyst 9000 Switches
Cisco DNA Center
Cisco SD-Access