



AH≡AD

The Enterprise Network Refresh Playbook

Why Do a Network Refresh Now?

With the shift to cloud, IT modernization investments have focused on the data center. The focus on the heavy undertaking that is cloud migration has put networking investments on the backburner. And for a while, that was fine. Workloads might not have remained on-premises, but most workers did -- performing their jobs within the safety and confines of a traditional office network.

But the way we work has evolved, and emerging technologies have with it. This is bad news for enterprises that have kicked the network modernization can down the road. Edge infrastructure, including operational technology (OT), has remained largely neglected, despite the growing momentum around smart devices and AI. The outdated hub-&-spoke network and security model poses major risks in a world of exponentially increasing endpoints.

Spending millions of dollars on modernizing your core data center doesn't mean much for productivity if your network is underperforming for your distributed workforce.

Everything is changing, and to remain competitive, now is the time to upgrade network connectivity and security in unison. An enterprise network and OT refresh is time consuming and challenging from both an engineering and logistical standpoint, but it can be done at both speed and scale. This playbook is designed to help you start building your roadmap to a modern network that lets every device – and every employee – perform at the speed needed for innovation to happen.

Getting Started and Building a Roadmap

An undertaking like a network refresh first requires developing a high-level Strategic Vision. This stage is all about capturing business and technology requirements for an ideal network. Strategic alignment between IT Investments and Business Strategy is critical to building a roadmap that maximizes value, minimizes risk, and leverages existing networking capabilities while expanding on new ones.

The business goals of a successful network refresh might include:

- Eliminating technical debt
- Leveraging an asset-light approach to campus infrastructure
- Providing a modern, reliable, and resilient technology infrastructure that eliminates business impact due to non-standard legacy technology
- Reducing operational overhead while providing a foundation for future business needs and IT capabilities
- Standardizing, consolidating, and enhancing networking technologies across facilities

With those goals in mind, you should now start cataloging a holistic view of your technology stack. When AHEAD performs this type of analysis, we look at:

Storage, HCI, and Compute

- Infrastructure Inventory and Survey
- Architecture alignment and compatibility
- vSphere and AHV Prism central data
- MiTrends, Live Optics, vRO, RVTools, AHEAD Proprietary Scripts

Data Protection

- DPA Reports for configuration
- DPS Health check results
- Performance Assessments
- Unit age reports
- Backup Retention Policies assessment
- Backup Data classification

Network

- Site IDF closet discovery & surveys
- Network Asset Discovery & Inventory
- Wireless Assessment
- Prior network performance assessments

Power, Cooling and Cabling

- Assess type of backbone cabling
- Assess type of horizontal structured cabling
- PDU Statistics from Centralized Monitoring System
- BBU Load Analysis
- Sufficient cooling – Current/Future

Identifying the gaps in your current technology stack allows you to define your ideal target-state conceptual architecture without creating additional technology silos in your organization. The “how” of filling in these gaps becomes the north star in the solution rationalization process. Considering solution alternatives, comparing proofs of concept, and analyzing ease of ecosystem integration are all key to choosing new networking solutions and deciding whether you’ll require solutions from multiple vendors.

From here, you can begin to create your Roadmap – a prioritized list of facilities, projects and tasks that help you achieve the Strategic Vision.

Security from the Start

AHEAD subscribes to a Zero Trust Architecture (ZTA) based closely on the CISA security model. True Zero Trust is based not on individual security products, but on security processes, visibility, automation and analytics across 5 main security pillars – Identity, Device, Data, Applications, and Network. When designing a Zero Trust Network, it's important to keep in mind that an effective ZTA relies on breaking down silos between each pillar and making sure all teams are aware of the security dependencies throughout the organization.

But for now, let's take a look at how to integrate zero trust into the design of your network.

For peak performance in a modern, multicloud network, there are several security goals to keep in mind:

INTER-CLOUD PEERING

Building and securing performant connectivity between your clouds

INTERNET EDGE

Maintaining predictable and resilient paths of egress and controlled ingress to web exposed services

CLOUD CONNECTIVITY

Creating optimal connection for any user, on any device, anywhere, to any cloud service

WORKLOAD SECURITY

Creating advanced protection for apps and services across any cloud

These goals are all accomplished through several main elements of Zero Trust Networking, such as:

- Software Defined Networking – Decoupling networking software and hardware creates a more secure network by creating greater threat visibility across the network and enabling operators to immediately quarantine compromised devices.
- Network Segmentation – Proper segmentation reduces the chance of a successful attack and the threat of movement through the network while also improving performance.
- Zero Trust Network Access (ZTNA) – The key to enabling secure remote work, ZTNA clearly defines access control policies for all your organization's applications, data, and services.
- Secure Access Service Edge (SASE) – Combining all the above elements with other cloud-native services, organizations will work towards this cloud architecture that combines network and security-as-a-service functions.

When embarking on a network refresh, keeping all these security elements in mind can save huge headaches down the road, so long they are implemented correctly. As a partner, AHEAD can design your ZTNA strategy and roadmap, implement consistent policy enforcement across your network, and create a Business Impact Analysis to keep your business resilient and running in the event of a network attack.

Lifecycle Management

Lifecycle management is tedious, but perhaps the most important piece of the network refresh puzzle. Without proper networking assessments and full supply chain transparency, replacing equipment at hundreds or thousands of campuses at speed and top quality can quickly turn into a disaster. But disaster can be prevented.

It starts with assessing each of your locations physically and logically. Each location needs a custom design, equipment procurement, staging, configuration, deployment, and – because not all networks are built on a single vendor’s products -- collaboration with each technology partner to run cables and hang access points.

Facility Prioritization

Through workshops across IT and business departments, settle on a networking vision that aligns goals and reduces risk through a prioritized list of facilities to tackle first.

Facility Surveys

Create a full picture of the assets and facilities at a site to inform procurement and implementation.

Design & Procurement

Designing standard configurations for each location and leveraging vendor programs can drive the cost of a refresh down. From there, AHEAD's Hatch product can synthesize all of your tracking and invoice information so you have full shipping visibility through delivery to any location. We can keep track of all components, where they were shipped, and where they are in the installation process in case a return is needed.

Staging

We employ a methodical approach to unboxing, asset tagging, burn in, and initial configuration of assets to reduce issues during deployment. Our Forge product allows us to stage, configure, and test everything at our Chicago distribution center and ship entire racks to your locations for true plug-and-play.

Asset Disposition

When it comes time to replace equipment, close management of maintenance and warranty contracts is vital. ServiceNow Integration with Hatch allows you to see automated data management for contracts – so you can stop keeping all your contract information in spreadsheets.

Technology Implementation

Wide-scale installation of your procured equipment happens at this stage. Our delivery teams – as many as you need – can install the equipment as soon as it is procured.

Operational Support

Once your network is installed, utilizing managed support services can ease the burden on your operations teams.

Network Automation

A next-generation network relies on automation to both relieve IT staff of mundane work and to keep the network secure. We're offering this set of guiding principles to help you climb the steep curve to network automation maturity.

First, automating a network that's overly complex and fragile is a recipe for outages. Keeping the network simple and as uniform as possible will allow you to automate much more quickly.

Effectively automating networks requires a gradual shift to a different way of thinking and operating as a team. DevOps principles like continuous integration are important to understanding why and how automation can be much safer than manual changes.

There are more tools out there that claim to automate your network than anyone can keep track of. And beware of those that claim to be "the only tool you need." In reality, certain tools work well in certain hands but not so much in others. Maintain a healthy amount of skepticism.

Not everyone has to deal with large demand spikes and declines, so the need to automate for provisioning speed isn't as widespread as it can sometimes seem. Network automation's biggest benefit is the increased reliability you achieve through consistent testing and validation.

Of course, automating networks requires reliable and accurate data about your devices, IP addresses, and so on. Without reliable information, there can be no reliable automation.

A consistent framework can help pull together all of these guidelines.

Why AHEAD for a Network Refresh?

AHEAD is focused on modernizing, automating, and securing our clients' network architecture — in the data center, across the enterprise, and in the cloud. Our networks are built to support the scalability, speed, and efficiency demanded by the digital enterprise, while maintaining security as a foundational element.

AHEAD is uniquely suited to assist clients with their cloud, data center and enterprise networking and network security requirements simply because of our rich experience and deep skillsets. AHEAD's Network Practice holds several industry certifications, with emphasis on cloud and progressive networking solutions like SD-WAN, SDN, and automation. We pride ourselves on bridging traditional networking to the newest platforms and methods available.

- 30+ Cisco Certified Internetwork Experts (CCIEs)
- Over 50 Architects and Engineers
- Cisco Gold Partner
- Fortinet Expert Partner
- VMware Premier Partner
- AWS Premier Consulting Partner & AWS Network Specialty
- Microsoft Azure Gold Cloud Platform Competency
- Palo Alto Networks Diamond Partner
- Extensive experience with Ansible, Terraform, and Python
- Aviatrix Partner

Why Cisco and AHEAD for Networking?

AHEAD is a Cisco Gold Partner with over 45 Cisco Certified Internetworking Experts (CCIEs) on staff and multiple awards and certifications, including:

- Cisco Partner Advisory Board Member
- Cisco Data Center Technical Advisory Board Member
- Multiple Regional Cisco Partner of the Year Awards
- Cisco CCNP/CCDP x90
- Cisco CCNA x125
- 5 Advanced Specializations in DC, ENT, SEC, COLLAB, CX

With cross-functional experts in cloud and data center, AHEAD network teams can leverage the entire Cisco platform to transform your network operations. The AHEAD Foundry and Hatch platform allow us to easily handle large-scale Cisco deployments with asset deployment, logistics, and managed services.





AHEAD builds and manages digital platforms that power the most successful organizations in the world. Our consultative approach, unmatched engineering, and innovative solutions combine to accelerate the impact of technology in every client we serve.

The material in this document is the proprietary property of AHEAD, Inc., also referred to in this document as "AHEAD." This information is sensitive and is to be shared at management discretion only within AHEAD and the company to whom AHEAD submits this document.

All products, trademarks, and copyrights herein are the property of their respective owners.

©2023 AHEAD, Inc. All rights reserved