Distributed Enterprise Multi-Office Networking

A Networking Solution Guide for Distributed Enterprises

ARISTA

CONTENTS

Introduction

Companies across the globe are deferring office leases, location and expansion decisions as they sort through their remote worker and productivity directives. These deferrals are having a ripple effect on distributed enterprise multi-office network upgrades as committing IT funding without quantifiable staffing numbers is challenging.

Cloud computing, IoT devices, cyber-attack sophistication, congested airwaves, and edge-as-a-service deployments are weighing heavily on the need to upgrade multi-office networks. Edge-as-a-service offers a game changer for many, as this places the intelligence at the edge, with more localized traffic autonomy, as cloud computing drives distributed communication architectures. This is different from legacy client/server network designs, where most applications were located in headquarter data centers, and traffic from remote locations was forwarded centrally.

Further as wireless communication has become the de facto medium for all mobile workers, new technologies including Wi-Fi 6, and Wi-Fi 6E are needed to manage signal integrity, higher channel densities, IoT battery preservation, and real time video streaming. And, security remains at the forefront, where access and usage is controlled via nimble firewalls, edge control, and user identity management.

IT departments should not wait for that magic bullet where they have a clear quantitative indication on how many will return to the office. Employee work patterns will continue to evolve; offices are still viewed as fundamental collaboration and productivity workspace whether 3 days a week, or some other number determined by human resources. Newer networking technologies including Wi-Fi 6 and 6E, IoT, adaptable firewall form factors, real time telemetry, and bandwidth optimization (especially at the edge), are necessary for these evolving offices. Many of these technologies will help shape the future of distributed offices, and hybrid workspaces.
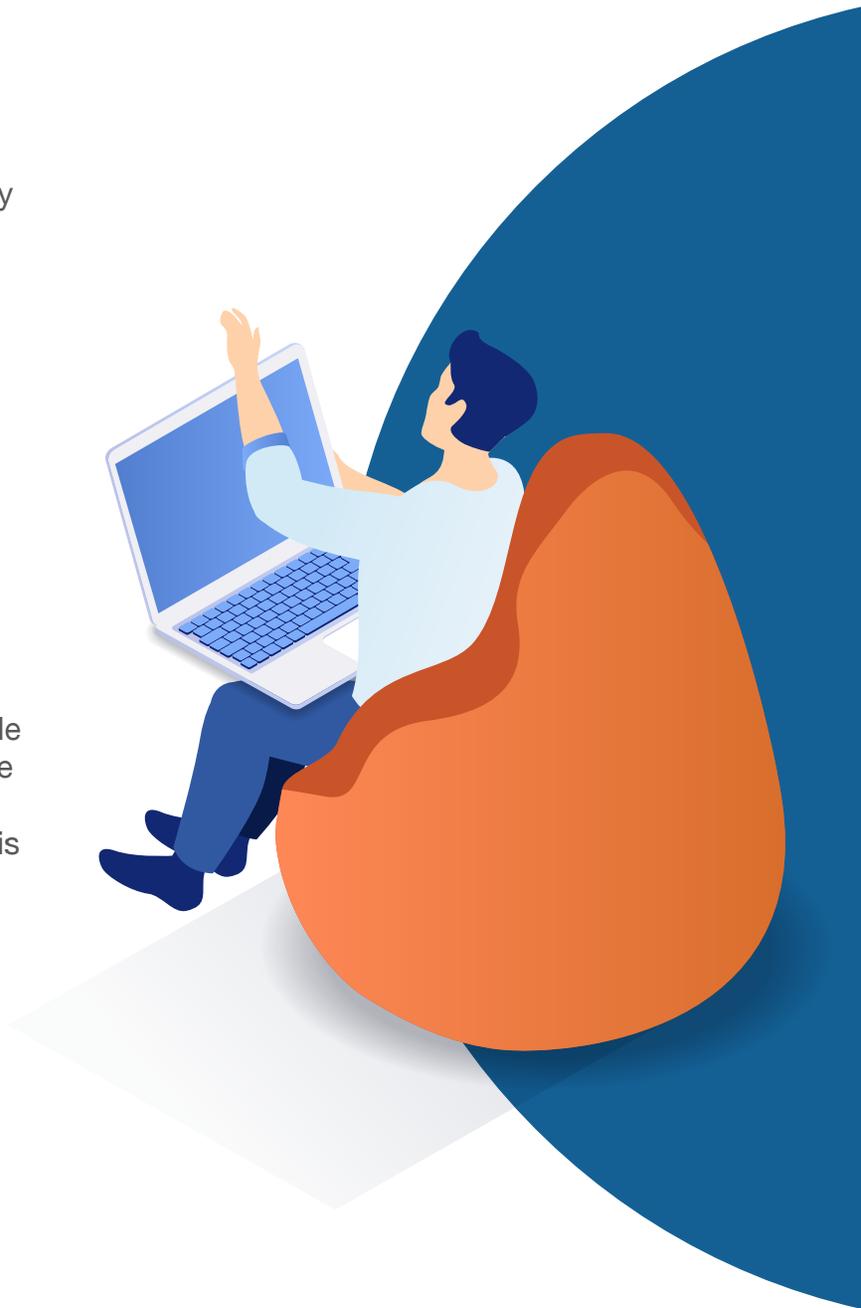
Upgrade Considerations

Distributed enterprise multi-network upgrade considerations should be based on the following:

Size and locations coupled with scale out topologies that are easily expanded as workforces return gradually.

Edge-as-service where there is a focus on endpoint services, including security, reachability, delivery, and high availability.

Wi-Fi 6, Wi-FI 6E Access Point technologies which enhance delivery and security with any endpoint device manufactured post 2020 (IoT, Cellular phones, Laptops, Printer etc,)

Centrally managed, yet distributed forwarding where intelligence resides at the edge.

Multi-gigabit bandwidth inclusive of 1/10/25/50/100Gbps where offices can easily upgrade.

Machine learning with proactive remediation for ensuring uptime, lights out upgrades, and central operations teams that can cover many locations.

Real time telemetry with a central cloud hosted, anonymized data repository. This provides the intelligence for all ML and AI applications.

Sensor technologies within the data stream for non disruptive forensic, cybersecurity and accounting applications.
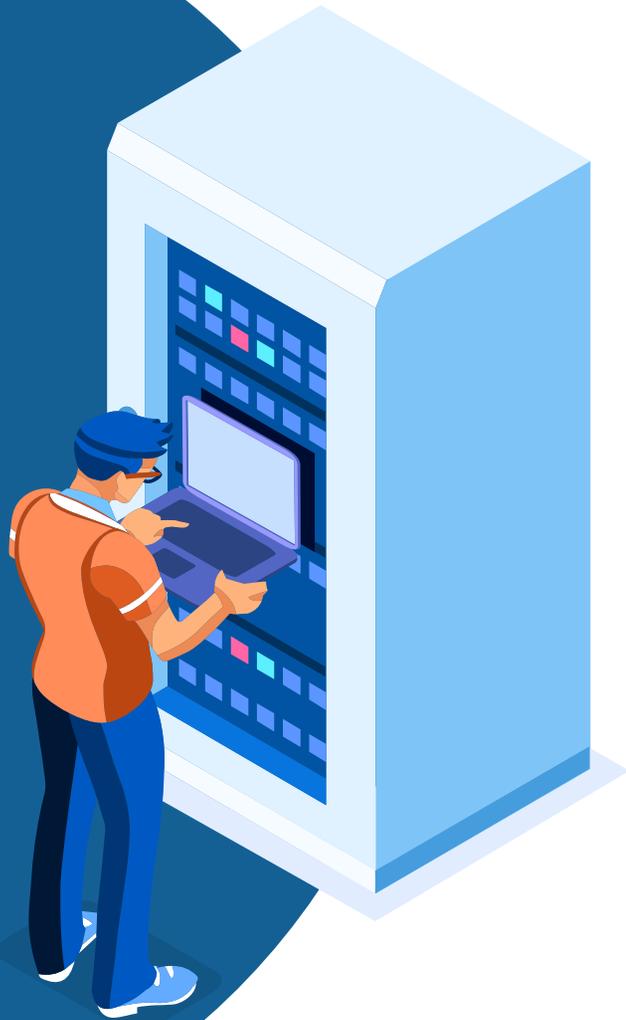
Cloud Centric Vs Headquarters Centric

Cloud computing has been transformative, most notably within the Data Center, as client/server architectures have given way to massively distributed scale out designs, and the outsourcing of compute and storage platforms to cloud hosting providers. This has shifted traffic patterns and driven the need for new, more efficient, less complex leaf/spine networking designs. These shifts in data center and application designs are changing the networking requirements within distributed offices as cloud computing also changes the traffic patterns in these satellite locations.

Where most distributed office networks were designed for primary access to private data centers, located at headquarters (or a few regional sites), the applications employees are accessing today are now highly distributed. Today's applications are no longer file based where a majority of productivity applications are done on someone's laptop, and then sent from a local hard drive to storage repositories. Compute is virtual, storage is distributed, file sharing is cloud centric, and browsers are becoming desktop operating systems. Office networks need to transform in concert with these "cloud" transformations.

Case in point, most containerized applications keep the compute, storage, and data within the cloud. Hardly anything computational or repository based lives locally on someone's desktop. This is driving the need for real time delivery, at a keystroke level on any device, anywhere. Many applications today support mobile phones, with primarily display and input functions only on these devices. And IoT devices are streaming real time telemetry with increased reliance on the cloud infrastructure for their intelligence. Businesses have 100% reliability on their networks, with increased decentralization of their workforces in remote places around the globe.

As cloud computing has changed the networking landscape within data centers over the last 10 years, it is now having the same impact on multi-office communications. Enterprises with many offices must re-architect their networks for these shifts in access, traffic patterns, and the explosion of Wi-Fi devices, leveraging cloud design principles that have been proven within virtualized and containerized data centers.

Evaluating Solutions

When evaluating any distributed enterprise multi-office network solution customer should keep the following in mind:

1. **Flexibility:** Based on unknown occupancy, productivity and collaboration metrics, and the ever changing shift in where the data and applications are located, enterprises need a flexible network that can be re-configured non-disruptively, without any downtime. Edge-as-service where upgrades and changes are done at the edge, is a better architecture than centrally where any control and data plane changes impact hundreds of locations. An architecture where administration is provided centrally within the cloud, yet the forwarding intelligence remains at the edge, accommodating daily changes, with no impact to the user community is the preferred approach.

2. **Industry Standard Platforms:** Different than 30 years ago, where packet based TCP/IP communications was in its infancy, and vendors where innovating a switching chip level, ethernet networking is an industry standard with 1000's of industry defined protocols, and 100's of commonly available communication chips. Customers should be leveraging these standards today when choosing any wired, wireless and/or security platform. Today businesses can choose switches, Wi-Fi Access Points, and Edge Threat Management products based on open standards, with well known communication chips including those from Intel, Broadcom, Qualcomm and several other tier one chip vendors.

3. **Endpoint Services:** Distributed offices are challenged as they lack many of the security controls compared to headquarters; these offices are being bombarded with employee bring-their-own devices, IoT unmanaged building controllers, asset tags, smart kiosks, cameras and other productivity devices. Most offices do not have lobby ambassadors to check devices coming in or out. The network has to safeguard IT assets against anything malicious, intended or unintended. The explosion of managed and unmanaged endpoints is challenging. Businesses should choose offerings based on a zero trust security architecture, where security is enabled across every platform. This includes advanced security sensors within their switches, dedicated radios within their Access Points, hardware based advanced segmentation and encryption, and dedicated firewalls. All of these security capabilities are centrally managed and monitored, yet every service runs locally to insure wire rate throughout and high availability.

4. **Proactive Troubleshooting and Remediation:** Most business level decision makers view networking as a necessary requirement however try to contain their costs. Purchasing decisions are based upon the initial equipment costs (bill of materials) yet 80% of the total cost of ownership is actually the staffing and support costs over 3-5 years. As networking continues to grow in complexity, companies are challenged in containing their staffing costs. They cannot afford to have networking experts in every distributed office. They must be able to manage these offices centrally. A multi-office solution has to have centralized administration and intelligence, via cloud hosting, while delivering edge as a service intelligence. Further branch office networks must stream anonymized real time control and management data to the operations team responsible for uptime (service level agreements) as they need to respond instantaneously to any loss in performance, access, or connectivity across 100's of sites, given the 100% reliance on network driven productivity.

Arista Cognitive Campus (CUE) For Distributed Enterprises

About Arista Cognitive Unified Edge (CUE)

Arista offers right sized enterprise class switches, firewalls, access points, and micro edge connectivity platforms for meeting the needs of both small and large office networks. Customers have many form factors to choose from while leveraging the same features, software infrastructure, and centralized cloud administration capabilities. CUE redefines commercial enterprise networks with enhanced security and connectivity, flexible PoE switching, and Wi-Fi 6/6E offerings that work together seamlessly to ensure connectivity, protection, monitoring, and control across the entire network from headquarters to the network edge.

CloudVision CUE

Centralized Cloud Based Management

- Visibility across globally dispersed networks & endpoints
- Zero touch deployment for hardware appliances
- Advanced alerting & reporting
- Proactive remediation with root cause analytics (one click troubleshooting)

Next Generation Firewall

- Next-gen firewall, with IPS, VPN & more
- Protection, encryption, control & visibility anywhere
- Onboard security for small network appliances & IoT devices
- Full security processing on-premises or in the cloud

WAN Optimization

- Secure, WAN-optimized connectivity for every location
- Seamless scalability with centralized policy management
- Optimal predictive routing technology for first packet, dynamic path selection

Wired Connectivity

- Scalable PoE compact switches with 12 to 48 ports
- Arista's Data Center proven Extensible Operating System (EOS)
- Wire rate encryption/tunneling
- Multi-gigabit uplink speeds from 1 to 100 Gbps
- Centralized management, with optional cloud or appliance based deployment choices

Wi-Fi 6, Wi-Fi 6E Access Points

- Enterprise class Wi-Fi 6 and Wi-Fi 6E technologies
- Optimized performance that scales from 1 to hundreds of users per AP
- Intelligent load balancing and channel optimization across multiple access points
- Multi-gigabit uplink choices based upon bandwidth needs
- Open, published APIs for integration with ITSM and monitoring tools
- Integrated wired/wireless infrastructure management based upon adjacency intelligence
- Integrated BLE technologies

ARISTA

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

arista.com