Enterprise Network Design & Implementation

Abstract/Introduction

As is the case with any enterprise, there are a variety of components that make up a network locally (LAN) or over a wide area network (WAN). Oftentimes, as engineers and administrators shuffle into an enterprise as years pass by, configurations can be layered or dated, and hardware can go without reloads or upgrades for extended periods of time causing major security risks and financial hardships in the event of a catastrophic failure. Years will pass without significant infrastructure overhauls due to budgetary reasons, or for a variety of other reasons.

An engineer or administrator's main responsibility in governing an enterprise is ensuring the integrity, stability, security of all hardware and systems, and the fluid continuity of operations while preemptively mitigating failures through redundancy and active/passive maintenance methods. In doing so, it's critical to evaluate the overall health of a network. This is where a holistic, thorough network assessment approach comes into play. With the this type of network assessment, everything, from the cabling infrastructure in a distant, forgotten closet to the primary data center and perimeter data flow, is reviewed and remediation techniques are put in place to pave a way forward towards optimizing the entire enterprise.

The key to any robust network assessment and or redesign is to identify the customer's pain points, assess areas of risk, and provide a fully redundant, scalable solution that includes remediation techniques and industry best practices that fit the customer's vision of their own enterprise for the future with the help of a consultant.

ABOUT THE AUTHOR

Michael Keller is a solutions-driven network architect, engineering professional and consultation expert. For more than two decades, he has supported a wide array of enterprise clients that have expressed the need to upgrade their existing wireless architecture from both a hardware and software perspective. He has validated and overseen countless architectural optimization efforts through surveys, calibrations, configuration, and installations. His experience includes developing, monitoring, and managing enterprise networking equipment for commercial companies and the United States Military.

Problem Statement

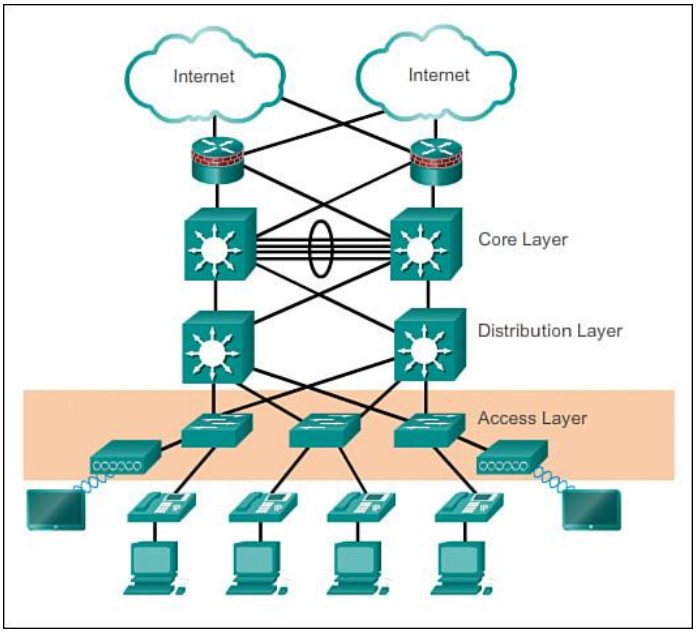
Putting out fires all day can be a trying task for any administrator or engineer, and time is precious. Oftentimes, an assessment is needed when there are active concerns within the enterprise, ranging from simple port configuration difficulties and network access concerns to intricate design and/or routing functionality.

Putting this into perspective is part of the assessor's responsibility, and it is imperative to understand how a network should function optimally without creating an overly complex solution that only adds headaches to an already overworked administrator or team of engineers.

Background

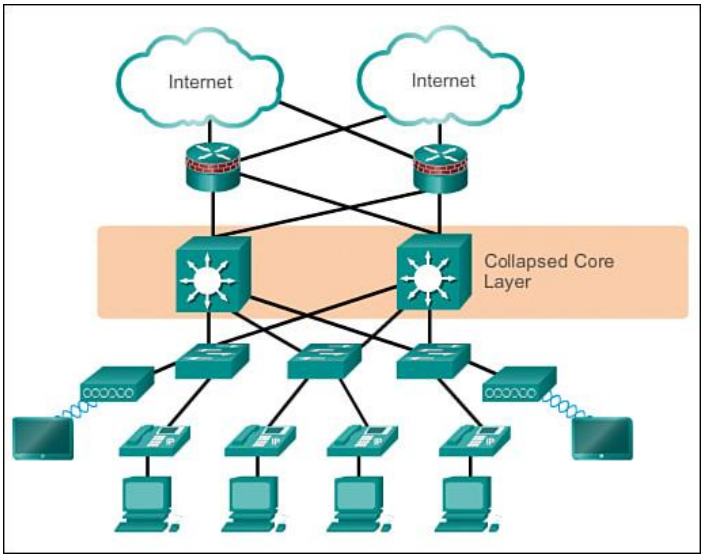
For years, the Cisco Hierarchical Network Design (CHND) has provided stability and resiliency for customers looking to optimize the architectural foundation of their enterprise. Comprising of multiple layers of functionality, the CHND provides a robust, redundant solution where symmetry exists from the access layer all the way to the provider, wherever possible.

Below is an example of the classic three-tier hierarchical design, comprised of three layers: the access, distribution, and core:



Please note that, while the three-tier design has been an industry standard for years, there are other design options one could consider, including the Collapsed Core design – which effectively eliminates the distribution layer (where fiber tends to aggregate between the access and core layers) and

compacts the enterprise into a series of single or redundant uplinks straight from the access layer switches directly into a single or pair of core switches, as shown below:



When assessing a customer's network, under most circumstances, one would hope to start by focusing on how the architecture reflects against industry best practices and designing a path forward.

Solution

After all the mechanics – both physically and logically – of a network are reviewed, a comprehensive solution is put in place by the remote or visiting engineer. This oftentimes includes a design showing areas of improvement, including full redundancy at the core (i.e. Catalyst 9600s) and perimeter (i.e. firewalls and or edge routers), all the way to the access layer, optimizing copper and fiber infrastructure (i.e. OM4 laser-optimized, high bandwidth multimode fiber dual-homed back to a pair of core switches).

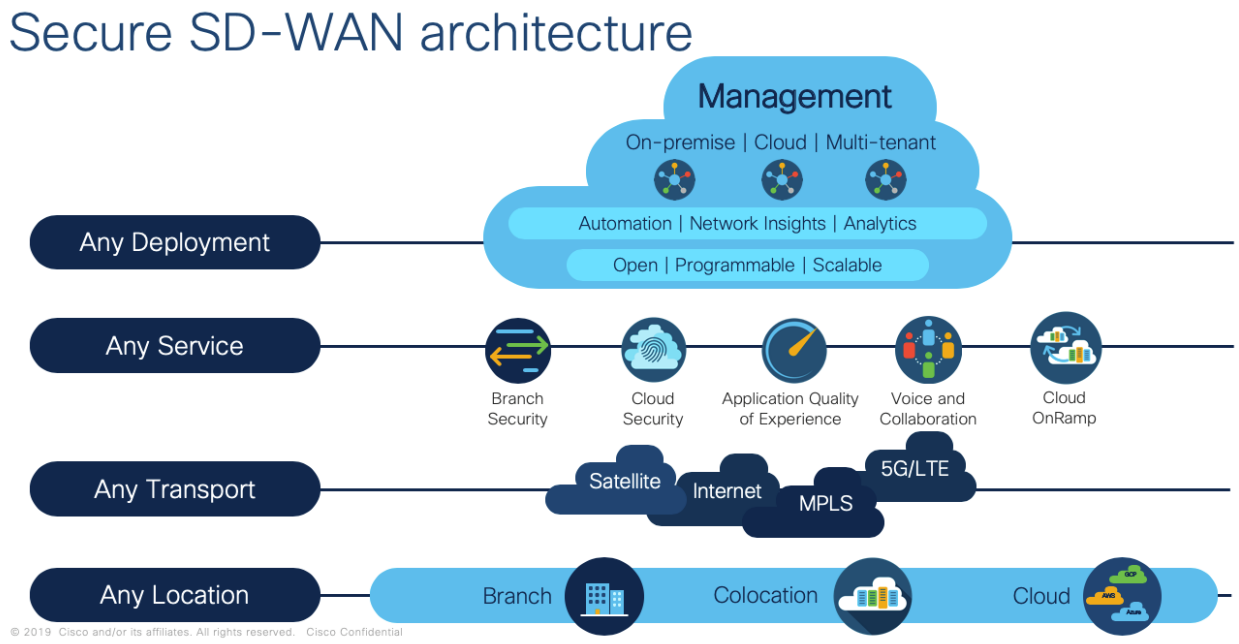
Additional solutions that the assessing engineer/consultant may provide would be in areas where configuration may be optimized, such as utilizing dynamic routing protocols (i.e. BGP, EIGRP, OSPF, etc.), leveraging port-channels for redundancy, and network access (i.e. ACLs, RADIUS, TACACS+, etc.). Industry best practices typically dictate remediation efforts presented to a customer and to work mutually towards a solution that not only reflects best practices, but also identifies areas where improvement can be made.

Below are a just a few items one could highlight during the course of a visual inspection of the customer's infrastructure, as well as configuration items:

- What are the environmental conditions within the intermediate distribution frames (IDFs) or main distribution frames (MDFs)?

- How are the closets cabled from the switches and routers between devices from the internet service provider (ISP) all the way to the hosts?
- Is there power redundancy either within the hardware or in the rack or data center?
- What does the existing port density consist of? Is there any room for additional connections?
- Is there adequate Power-over-Ethernet (PoE) on the switches to support a modern voice or wireless infrastructure?
- How is spanning tree configured? Is it configured correctly?
- If dynamic routing is being used (such as BGP), what are the routers at the perimeter peering with and are routes being potentially summarized? Is iBGP being used?
- Are the switched virtual interfaces (SVIs) configured correctly on the core switches (or firewalls, in some instances), and is there any redundancy such as hot standby routing protocol (HSRP) being used between the cores to ensure failover?
- Are there access control lists (ACLs) configured on the VTY lines for remote access restriction (i.e. SSHv2)?

Again, this is just a small sampling of what one could look for when analyzing physical and logical components of an assessment. Remember: a leak in the data center ceiling can be just as important as a glaring, serious Layer 3 issue. Antiquated architecture or hardware is only one component of the overall picture.



As an aside, it's also important to consider introducing Meraki and/or SD-WAN technology into the equation as a path forward, which can simplify WAN management and operation while also reducing costs. As such, creativity and ingenuity are major players in an effort for the engineer to provide a solution that works best for a customer – such as SD-WAN. A solution sometimes requires thinking

outside the box (which can be predicated on the customer's existing architecture and a willingness, for budgetary or other reasons, to stay with the existing layout either physically or logically).

These are just some of the challenges faced when forging a path towards LAN/WAN optimization. Ultimately, though, working with a consultant to evaluate a customer's enterprise objectively and professionally will pay dividends in risk mitigation and optimization efforts for the enterprise going forward.

References

https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4
https://en.wikipedia.org/wiki/SD-WAN
https://blogs.cisco.com/networking/evolution-cisco-sd-wan-revolution-for-enterprises-with-cloud-first-strategy

References

https://networklessons.com/cisco/ccie-routing-switching/introduction-to-dmvpn

https://en.wikipedia.org/wiki/Dynamic_Multipoint_Virtual_Private_Network

https://www.cisco.com/c/dam/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/prod_presentation0900aecd80313c9d.pdf

https://www.fieldengineer.com/blogs/dynamic-multipoint-vpn

https://hainc.com/dmvpn-what-is-it-when-should-i-use-it/

https://learningnetwork.cisco.com/s/article/dmvpn-concepts-amp-configuration

https://learningnetwork.cisco.com/s/question/0D53i00000Z7vDRCAZ/disabling-splithorizon-for-eigrp-using-dmvpn-ii

About Aspire Technology Partners

Aspire is a professional technology services firm specializing in the delivery of digital infrastructure solutions and managed services designed specifically to achieve our clients' business goals. We believe technology sits at the heart of every enterprise strategy. Our team takes time to understand your business initiatives and align technology solutions to drive the organization forward. Aspire's outcome-driven approach accelerates your journey by combining secure digital infrastructure, world-class design and implementation expertise, and managed services – all centered around transforming today's multi-cloud architectures into enablers of business value. Headquartered in Eatontown, New Jersey, Aspire is focused on serving the tri-state and mid-Atlantic regions with local operations in Mount Laurel, NJ; Albany and White Plains, NY. For more information, visit www.aspiretransforms.com.