OPEN ACCESS Freely available online

Journal of Information Technology & Software Engineering

Short Communication

Enterprise Network Hardware Refresh

Anshuman Awasthi*

Department of Engineering, Restoration Hardware, USA

ABSTRACT

It is essential to keep the Network Hardware up and running in good condition to support enterprise applications connectivity. Network performance plays a critical role in providing adequate bandwidth to the collaboration tools for an organization.

The average life of the some of the network equipment ranges between 3-5 years, however some may last more than 5 years based on the type of hardware and technology used. The older technology may add performance barriers in the enterprise network.

Performing a Network hardware refresh can be a tedious and complicated task depending on the amount of devices and the architecture. Let us try to understand how to perform a hardware refresh for your Network that function in an enterprise and the types of devices that function in different layers in an OSI model.

Keywords: Network engineering; OSI model; Types of network; Infrastructure network

INTRODUCTION

This article explains how to perform a network hardware refresh and what kind of different devices are involved.

METHODS

Network Engineering using OSI model. It is essential to keep the network hardware current to ensure it provides sufficient bandwidth and is up to date on the required security patches [1]. The network hardware provider usually provides the security and software patches only during the hardware life cycle, and an organization needs to plan a refresh to keep the network running in a healthy state [2].

DESIGN AND INFORMATION GATHERING APPROACH

Document the existing network with all technical details. Create a Wide Area Network (WAN) and supporting Local Area Network (LAN) diagram with minute details like VLAN information, network port requirements, existing network circuit details, and service providers involved.

- Gather details about the environment like no of users, type of devices, maintenance windows [3].
- Prepare a network design based on the collected data and specified customer requirements [4].

Discuss the proposed design with organization's management to seek approval.

Implementation approach

It can be a tedious task to refresh network hardware for any enterprise, as it may come with a lot of known and few unknown challenges [5]. In many cases, an organization already has a working network infrastructure with some issues and has to perform a network hardware refresh [6]. The best approach will be to install a new network environment in parallel to the existing infrastructure and implement a gradual cutover [7]. This may need more budgeting, however mitigates the risk of critical failures.

We can plan a completely different Class C subnet as compared to the existing one so that we do not create any issues with the current local area network, and we can easily differentiate between the two during the implementation process [8]. This approach will also help us to minimize the downtime required during the cutover process, as we understand an organization will be operational during its business hours [9]. To begin with, we should first order a new internet connection from a different internet service provider as connection delivery takes its own time.

We can divide the whole project for a medium-size enterprise in below steps:

- Install and configure new core switches
- Connect new core with the existing network so that it becomes a part of it, but old switches continue to function as is.
- Install and configure all IDF (Intermediate Distribution Frame). POE switches and connect them to new core switches.

***Correspondence to:** Anshuman Awasthi, Director – Department of Engineering, Restoration Hardware, USA, Tel: 8187514274; E-mail: anshumanawasti@gmail.com

Received: February 11, 2020; **Accepted:** March 20, 2020; **Published:** March 27, 2020

Citation: Awasthi A (2020) Enterprise Network Hardware Refresh. J Inform Tech Softw Eng 10:262. doi: 10.24105/2165-7866.9.262.

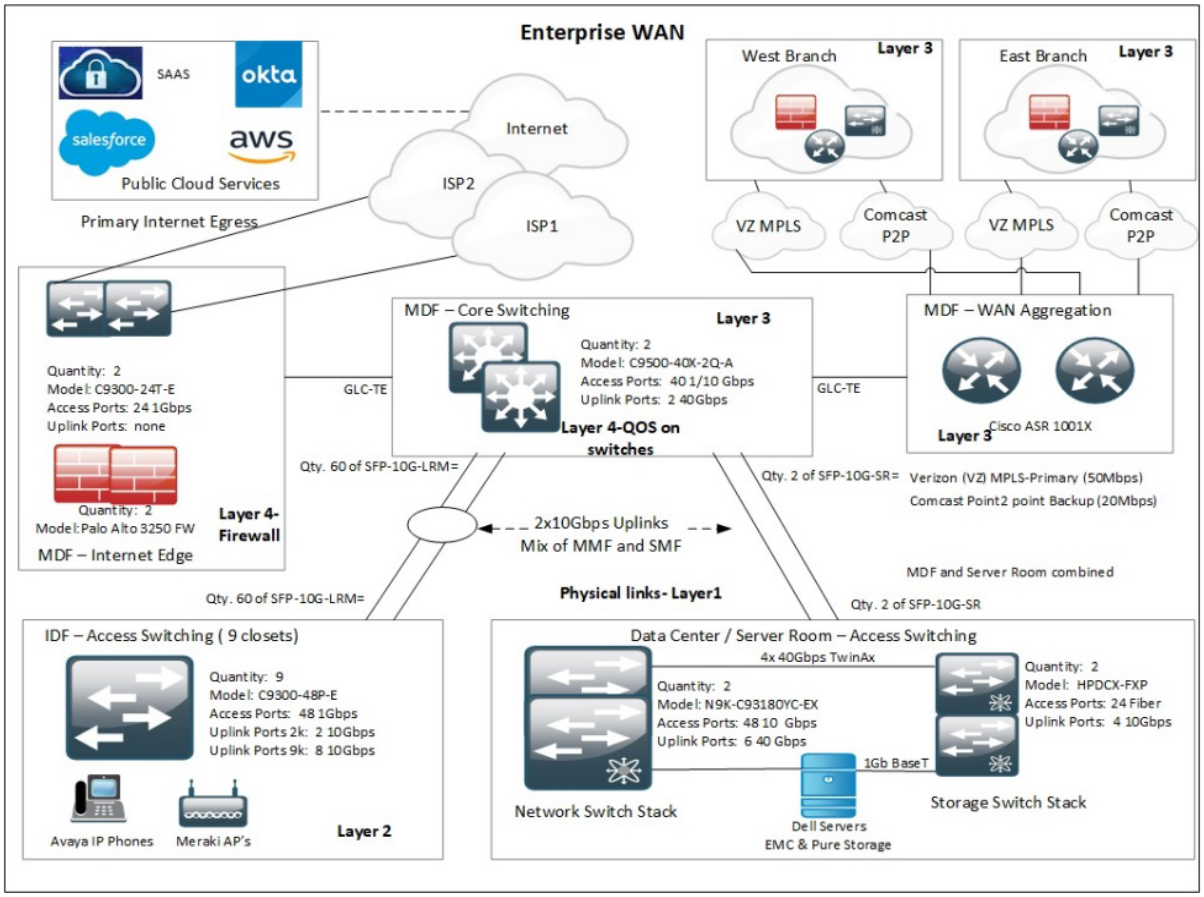

Figure 1: A typical high level Wide Area Network (WAN) is shown below.

- Install and configure all wireless access points and connect all of them to new IDF switches using POE enabled ports.
- Install and configure new internet edge switches and firewall separately.
- Start moving physical connections likes data ports for laptop, printers from old switches to new ones. Once all the links are moved to disable the uplinks for the old switches.

This should complete Layer 2 migration

Take a full maintenance window and perform Layer 3 migration to the new environment by connecting the old and new internet connection to new edge switches.

- All internet traffic should traverse through the internet firewall, as it will act as a virtual gateway.
- In another maintenance window, replace existing routers with a new model like Cisco ASRs

We should only move on to the next step after the successful validation of network connectivity after any changes [10].

To verify the network connectivity at the end of the maintenance we need to prepare a sample checklist, like the one shown below (Figure 1):

- There are no active alerts in the monitoring tool related to the location.
- Log on to a wired network resource and ensure connectivity to internet and internal sites.
- Logon to wireless network resource and verify the connectivity.
- Monitor computes resources on the new network hardware to ensure they are under threshold.
- Establish new SLA (Service Level) monitoring for critical network links and ensure there are no alarms.
- Logon to a different network site resource and ensure connectivity to the site where the maintenance was performed.

CONCLUSION

To design a network for an enterprise different kind of devices are involved in various stages. It is essential to understand the features and capabilities of each device so that they can provide optimal performance and security.

The layer 3 devices are routers and layer 2 devices are network switches. Routers can also be used as gateways to communicate between two different networks. Wireless security needs to be planned as per the organization's info security policy and latest industry standards.

REFERENCES

1. Awasthi A. Network Classification for an Enterprise. Int J Sci Res. 2020; 9(2):635-637.
2. Awasthi A. Disaster Recovery - Foundation Pillars. Int Sci Res. 2020;9(1):1360-1362.
3. Blog - Windows Monitoring Tools.
4. Blog - Windows Monitoring Tools and Technical Issues.
5. Aston B. Kick off Meeting: The Complete Guide to Starting Project

Right.2016.

6. Article – CMS distribution.
7. Team Clarizen .Who are Project Management Stakeholders.2017.
8. CCNA Routing and Switching guide. ISBN: 978-1-118-74973-9.
9. Report- Planning a network upgrade.
10. Sabyasachi. Best Practices for Preparing a Lessons Learned Document.