Network Magic

#123 West State, Chicago 60616

Network Design Proposal

Delivered :April 04,2020

Prepared by: Sonita Bose, Network Manager

Prepared for : Networking Magic

Table of Contents

Executive Summary

The company has been operating on the Information technology platform catering to 200+ employees for quite a long time. It is said that a building premises is a physical asset with the longest life in a business. The physical asset that comes in next is the networking. The networking in the premises which catered earlier to all means of communication like Desk Phones, Fax Machines have served a long period of time and have faced the brunt of obsolescence with suitable upgradation over time.

After the onset of Information Technology, companies are more dependent on the networking assets. The objective is to upgrade the networking backbone of the company as the token-ring network has completed its end-of-life decades ago. Current design is living on borrowed time. Latest networking capabilities are designed to have longer life and a lower total cost of ownership. The obsolete networking is proving to be a closed door to new technologies like video conferencing and Virtual Private Networking which will enable us to work in a secure environment from anywhere.

I would like to replace the Token-Ring backbone with IEEE 802.3 (Ethernet) for the Wired Networking and IEEE 802.11 (Wi Fi) for the Wireless Networking. We will place a Security Appliance after the ISP Drop to secure our network from the internet. The new backbone layer 3 switch will enable IEEE 802.1p standards so that we can use VoIP phones in our office. We will see better printing efficiency as they will get a better connection to the network.

Please find the network diagram and floor plan to facilitate this change in the document below. An excel sheet showing the Bill of Materials is attached to give you an estimate of costs of materials alone. We would need to hire a new ISP to provide us with access to the Internet.

Problem Statement

The Token-Ring Network that is currently being operated in the premises are facing the following problems.

- Latest devices do not have hardware interfaces or software drivers for Token Ring Network
- Printers have to be run on HP JetDirect 500X Token Ring Print servers. Direct Network Printers cannot be used as no new Printer supports Token Ring Interfaces.
- Wireless Access Ports cannot be used in a Token Ring Network
- VOIP Phones cannot be supported.

Proposed Solution

The entire network backbone needs to be removed to accommodate Ethernet based Layer 1 Hardware. This will enable us to comply with the latest IEEE 802.3 standards and open our path to new technologies that have come up and will be coming up in the future.

The New Backbone will provide us with the following basic services.

- Workgroup Networking for 150 Desktop Users with ability to expand
- Secure and reliable connection to the Email server and File Servers.
- Use of Network Printers based on Windows Active Directory ownership.
- Secure connection with the Internet
- Provision for 120 VOIP Phones for employees to talk to one another.
- Provision for 50 BYOD users to work in a wireless securely accessed environment
- Use of latest printers without Print Servers.

The Backbone consists of the following

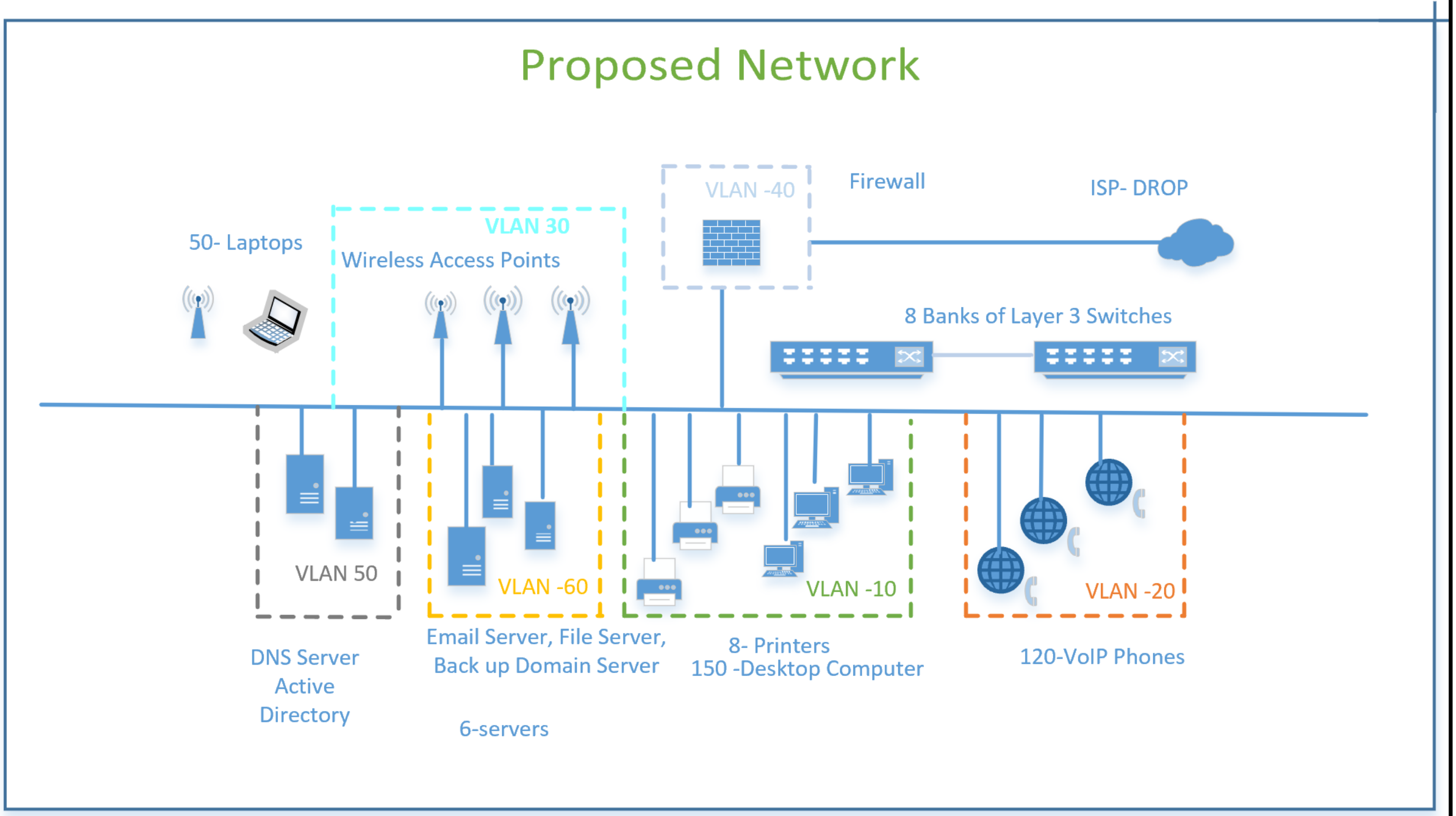
- 8 x Layer 3 Switches which support Virtual Trunking Protocol. The layer 3 switch will provide the following functions.
    1. Act as a DHCP Servers so that the devices in each Virtual LAN can get an IPv4 IP Address on lease on booting up from a pool of ip addresses reserved for the class of devices. They will be assigned subnet masks, gateway addresses and DNS addresses by the DHCP Servers.
    2. Act as a static router between the VLANs.
    3. Enable VoIP Telephony
    4. Enable Wireless Access for Laptops with Domain Server Authentication
- Fresh Cat 6 Cabling
- Replaced Ethernet Network Interface Cards on Desktops which has Token Ring Cards.

VLAN Groups and DHCP Pools

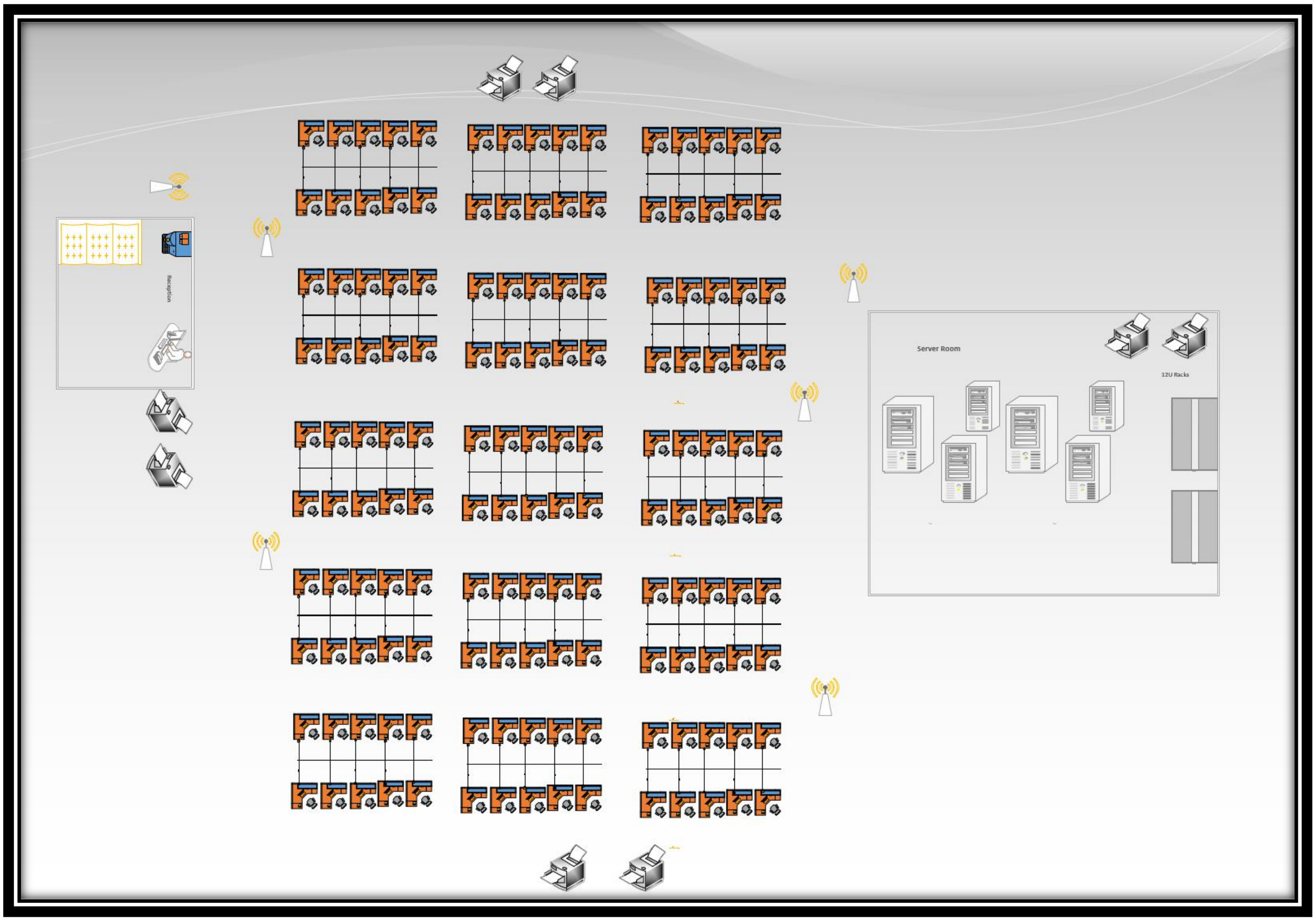
VLAN ID	Network Address	No of Hosts	DHCP Pools	Device Group
VLAN 10	192.168.010.0/24	255	192.168.010.010 – 020 Static IP	Printers Backup Domain Server
		255	192.168.010.100 – 250	Desktops
VLAN 20	192.168.020.0/24	255	192.168.020.100 – 250	VOIP Endpoints
VLAN 30	192.168.030.0/24	255	192.168.030.010 – 016 Static IP to MAC Address Mapping	Wireless Access Points
		255	192.168.030.100 – 200	WAP Stations
VLAN 40	192.168.040.0/24	255	192.168.040.010 Static IP – Gateway to the Internet	Security Device
VLAN 50	192.168.050.0/24	255	192.168.050.010 - 20 Static IP	DNS Server Active Directory
VLAN 60	192.168.060.0/24	255	192.168.060.010 - 20	Email Server File Server

Table 1

Network Diagram



Floor Plan



- The floor plan consist of 30 workstations of 5 rows.
- There are 2 printers at each East, West, North and South.
- The server room is on the right with two 12U racks.
- There is an illustration of the reception on the left with a coffee machine and sofa.
- There are 6 WAPs situated at different positions of the floor.

Criterion for Selection of Hardware

Internet Service Provider

The Internet Service Provider suggested is AT&T's Business Internet at 1 GBps.

The ISP Drop gets plugged in to the Security Appliance mentioned below.

Security Appliance

Cisco Meraki MX84 Cloud Managed Security Appliance and Enterprise License and Support

- The Security Appliance will be connected to one of the Ports of the stack of Layer three switches mentioned below. This port is a port on VLAN 40 and will have an internal ip address of 192.168.040.1 which will be the internet gateway for all VLANs.
- The Security Appliance has a backplane with a capacity of 500 Mbps.
- It can cater to 200 clients.
- You can have identity based policy besides general policies
- It can detect Malware and provide Intrusion prevention.
- The device can identify and manage Application Layer content and manage it e.g. prioritize Skype, throttle Torrents or block TikTok
- CIPA-compliant content filtering can implement, safe-search enforcement, and YouTube for Schools

- It can be used to allow VPN connectivity so that users can work securely from home or while travelling.
- It has provision to insert SIM cards to access mobile internet services as a failover automatically.
- The device has 8 ports with 1g/10g/SFP+ options to connect to the LAN backbones.
- Connection to WAN can be established through 2 x GbE RJ45 plus 1 x USB (cellular failover)
- Rack Mountable - occupies 1U

Stack of 8 x Layer 3 Switches with 48 ports each

Cisco SF300-48PP 48-port 10/100 PoE+ Managed Switch with Gig Uplinks

- 8 Switches provide 384 high speed ports connected to the patch panel. This can accommodate all the devices required plus plenty more for expansion.
- Each switch has a capacity to switch at 17.6 GBps
- Total Ports 48 Fast Ethernet + 4 Gigabit Ethernet (2 Combo Ports)

- This Layer 3 switch supports VLAN Trunking Protocol which enables a stack of Switches connected with Inter Switch Links to share VLAN configurations over the stack. as per IEEE 802.1Q specifications.
- We plan to divide the ports into 6 static port VLANs as described in Table 1 of the proposed solution section.
- The ability to provide Static routing / Layer 3 switching between VLANs allows us to segment the network into separate workgroups and communicate across VLANs without degrading network performance.
- The VLAN 20 that supports VOIP Phones get the benefit of QoS (IEEE 802.11e) and POE+ (IEEE 802.3at). The automated voice VLAN capabilities let you plug any IP phone (including third-party phones) into your IP telephony network and receive an immediate dial tone. The switch automatically configures the device with the right VLAN and QoS parameters to prioritize voice traffic.
- The Layer 3 of this Switch functions as an IPv4 DHCP Server leasing IP addresses for multiple DHCP pools depending on the VLANs set up.
- Dynamic VLAN assignment via Radius server along with 802.1x client authentication enables employees with BYOD to login securely and work in a secure environment due to the capability to relay Dynamic Host Configuration Protocol (DHCP) Protocol packets at Layer 2
- A great safety feature is the time based ACLs and Port Operation to restrict access to the network during predesignated times, such as business hours.

- It offers advanced defense mechanisms, including Dynamic ARP Inspection (DAI), IP Source Guard, and Dynamic Host Configuration Protocol (DHCP) snooping, detect and block deliberate network attacks. Combinations of these protocols are also referred to as IPMB (IP-MAC-port binding).
- It includes embedded QoS intelligence to prioritize delay-sensitive services such as voice and video and help ensure consistent network performance for all services.
- This switch supports Smart Auto detect. It disables intrusion by ensuring posts meant for Wireless Access Points or VoIP Phones cannot be used to plug in a laptop. It has the ability to detect the following connection events.
    - CISCO_PHONE_EVENT to detect that a phone device is connected to an interface.
    - CISCO_SWITCH_EVENT to detect that a switch is connected to an interface.
    - CISCO_ROUTER_EVENT to detect that a router is connected to an interface.
    - CISCO_WIRELESS_AP_EVENT to detect that a wireless application is connected to an interface.
    - CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT to detect that a wireless lightweight application is connected to an interface.

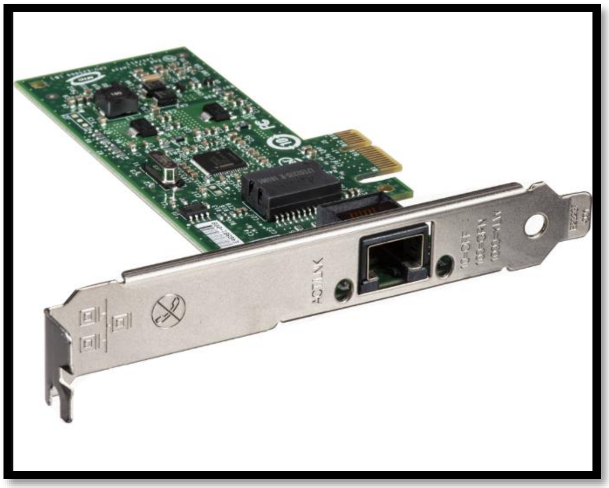
Ethernet Network Interface Cards

Intel i350-T4 1GB Quad Port Ethernet Card for Servers

- This is a Quad Port Gigabit Ethernet Adapters (1GbE)
- We will use this to replace the NIC on every Server to be able to connect to the new Ethernet backbone.

Intel Gigabit CT PCI-E Network Adapter EXPI9301CTBLK for Desktops

- This is a Gigabit Ethernet Adapters (1GbE)
- We will use this to replace the NIC on every Desktop to be able to connect to the new Ethernet backbone.



Wired Network

- Each workstation is equipped with two RJ45 interfaces on a single face plate. One for data connection, the other is for the VoIP Phones. Auto Smart Ports can detect VoIP Phones and connect them to the VoIP VLAN. Since we have POE+ ports on the switch we do not need power bricks to power the VoIP Phones.
- Patch Cords on the Patch Panels ensure which VLANs they get connected to. This takes care of the Desktops and Printers.
- Servers in the server room are connected to RJ45 face plates wired through the patch panel to respective ports on the switch belonging to the VLAN they belong to.
- There are 6 Wireless access points in the building. We need to run Cat 5 cables to convenient points on the ceiling where Wireless Access Point below can be plugged in. Again since we have POE+ ports we do not need power to run the WAPs.
- We will be using IPv4 Addressing to identify the devices in the network as we have a very small number of nodes and the possibility of growing to more than 500 nodes is not there.

Wireless Network

Wireless Access Point

Cisco WAP351 Wireless-N Dual Radio Access Point with Single Point Setup

- This Wireless Access Point supports **802.11n** connectivity
- It also has port that allows access point to be powered by backbone switch
- The WAP itself is a DHCP client
- It has robust security, including WPA2, **802.1X with RADIUS** secure authentication, and rogue-access-point detection, helps protect sensitive business information. 802.1x is a network authentication protocol that opens ports for network access when an organization authenticates a user's identity and authorizes them for access to the network. The user's identity is determined based on their credentials or certificate, which is confirmed by the RADIUS server.
- Using a bridge mode Clients can access the main DHCP server of the Layer 3 switch to get a lease from DHCP Pools assigned to the WAP pool after Radius authentication from the Active Directory.

Pricing and Billing

Item Type	Item Description	Qty	Rate	Total Amount
Security Appliance	Cisco Meraki MX84 Enterprise License and License	1	$1,377.00	$1,377.00
Layer 3 Switch	Cisco SF300-48PP 48-port 10/100 PoE+ Managed Switch with Gig Uplinks	8	$1,356.00	$10,848.00
Wireless Access Point	Cisco WAP351 Wireless-N Dual Radio Access Point with 5-Port Switch	6	$320.00	$1,920.00
Intel NICs for Servers	Intel i350-T4 1gb Quad Port PCI-E FH Network Card THGMP	8	$64.00	$512.00
Intel NICs for Desktops	Intel Gigabit CT PCI-E Network Adapter EXPI9301CTBLK	150	$55.00	$8,250.00
10 Outlet PDU	CyberPower CPS1215RM Basic PDU, 120V/15A, 10 Outlets, 15ft Power Cord	2	$42.00	$84.00
12 U Rack	Tripp Lite SRW12USG SmartRack 12U Wall-Mount Rack Enclosure	2	$374.00	$748.00
24 Port Patch Panel	TRIPP LITE Cat6 PoE+ Compliant Patch Panel 24-Port	16	$75.00	$1,200.00
Face Plates	Cat6 Wall Plate and Keystone, Fly Tiger,Rj45 Jack Ethernet Connector	200	$10.00	$2,000.00
Patch Cords	Amazon Basics RJ45 Cat-6 Ethernet Patch Internet Cable - 10 Feet	200	$7.00	$1,400.00
Patch Cords	iMBA Price (10 Pack) (1ft) Molded UTP Cat6 Ethernet Patch Cable RJ45 M/M	400	$15.00	$6,000.00
Cat 6 Cables	Cat6 Ethernet Solid Bulk Cable (23 AWG, UTP) - 1000-Foot, Red	10	$120.00	$1,200.00
	Total			$35,539.00
	Illinois State Tax @ 6.26%			$2,221.19
	Net			$37,760.19

Total Cost to the Company

Hardware	$37,760.19
Installation and Commissioning	$5,330.85
Net	$ 43,091.04

Internet Connection charges per month	$ 500

Extra Credit

Implementation of VoIP phones without power brick implementation

The Layer 3 switch **Cisco SF300-48PP 48-port 10/100 PoE+ Managed Switch** supports IEEE 802.3at (POE+) standards which enables the VoIP Telephones to draw power from the Switch ports through RJ45 connections we do not need use power bricks to run VOIP Phones

Network Management and Security Best Practices

- Once the network is set up we will take a benchmark of the performance of the network in all VLANs.
- We will be monitoring the performance so that we can identify weaknesses in the design and implementation of the network.
- The IT Department should follow Configuration Management by having a Change Request system where any changes to the network, configuration, policies, routing rules etc are raised in the changes go through a workflow of approval, implementation and validation. The workflow needs to be documented and preserved so that the reasons for changes are visible to the network managers and engineers when considering further amendments or enhancements. Absence of such information makes it very difficult to maintain the network.
- The network security needs to be audited by a 3rd Party.
- Regular audit to be done periodically.
- Network Management Services include provisions for logging events. These logs need to be examined t pre-defined intervals to evaluate security and performance of the network.
- The Managed devices like Switches, Routers, Security Appliances all have facilities for dumping configuration as a text file. All versions need to be saved in repository like GitHub.

- The configuration versions should start with the baseline configuration that will be implemented after commissioning of the network. Documentation should include full design consideration and methodologies.
- Good network management includes well documented and tested procedures to switch over to back-up resources in case of failures. A Standard Operating Manual needs to be prepared and preserved for use during failures.
- The network design presented in the proposal has many security features like VoIP Ports can only be used for VoIP Phones, or Wireless Access Ports are leased IP addresses mapped to MAC Addresses. However we still need physical security of the network. All network hardware being in the server room, the room has to have secure systems so that unauthorized persons cannot enter the room. This can be achieved by using password operated keys or whatever means suitable.

Conclusion

We have provided a state of art, Industry standard network design to bring your Information Technology Networking Backbone at par with the latest and appropriate technology in the market.

Care has been taken to ensure that you will be able to keep at pace with further developments in Information Technology without any financial burden on the networking assets.

I hope that you realize the benefits provided and approve the project plan.

It would be my pleasure to provide you with any further guidance or clarifications needed for this project. Feel free to call me on +1 2345 9620 .