CIT241 Network Communication
consulting

Network Design and Installation Proposal

Overview

CIT 241Networking Communications, Inc. was provided a Request for Proposal (RFP) by Dunder Mifflin Paper Company, Inc., a paper sales company based in New York and have other offices throughout the US, to propose a design and installation of a network for 100 users with additional devices such as printers and laptops. This proposal will also include organizing VLANs for different groups of the company, future scalability, a single ISP connection and secure wireless connectivity.

December 10, 2018

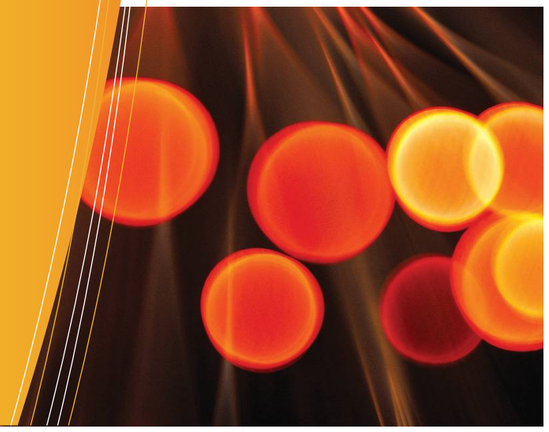
Network Engineer: Hiram Todd

Dunder Mifflin, Inc.

Paper Company

consulting
sales
staffing
support

TABLE OF CONTENTS



Customer Requirements

This network design proposal is Dunder Mifflin's requirements for the new tenant improvement for the Scranton branch in Pennsylvania. This plan is the design and installation of a new data network system that will include a wide range of flexibility. What will consist in this network design proposal per RFP (Request of Proposal) of Dunder Mifflin is a network support for a three-story office building with 100 users. The first floor will include 25 users in the marketing department, 5 users IT department, 5 users in the accounting department, and 5 users in the server room. The second floor will only consist of 50 users in the sales department and the third floor for 5 executive offices and 5 for the human resources department. Each floor will share 2 printers and each executive office will have a dedicated printer. Each department will have their own VLAN (Virtual Local Area Network) and subnet.

The Server Room needs to support many application servers on different VLANs. One server will be dedicated to the Accounting Department and should only be accessible from the Accounting Department VLAN.

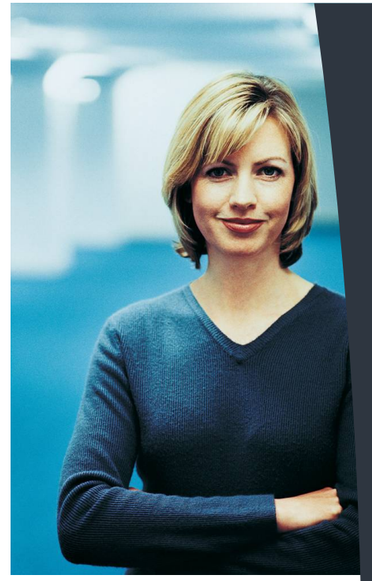
The network design proposal will include only Cisco equipment and the Cisco 3 Layer Hierarchical model layers: core, distribution and access layer. For the core layer, two Cisco routers will be used to connect to Dunder Mifflin's departments and their ISP (Internet Service Provider).

No matter if external or internal of the network, LAN (Local Area Network) and WAN (Wide Area Network) will pass through the core layer routers which purpose is to forward incoming and outgoing packets quickly and secured through the ACL (Access Control List) settings for general LAN security. The distribution and access layer will handle the ACLs for intranetworking policies and security. Three Cisco switches will serve the distribution layer as the communication point between the access and the core layers, and four Cisco switches in the access layer to communicate between the department computers and distribution layer. In order to provide fault tolerance, seven switches will be beneficial in case a switch goes down and having three also offers scalability in case of company growth.

This proposal also includes the flexibility of not only scalability, but redundancy, and very importantly, security.

The network requirement also involves a server room that is independent from the rest of the main building and includes its own humidity control with a design criteria of 72□F and 45% RH as measured at the return air of the AC unit. Under-floor air distribution system is preferred but ducted systems are acceptable. The room's specifications include sound-isolating walls, ceiling, and doors, no windows for security and sound, a nine-foot ceiling, anti-static floor finishing for raised floor tiles or sheet vinyl, and 42 to 48-inch-wide doors with heights of 8 feet. The room will also require at least one phone, seismic braced computer racks, grounding, and maximum electrical intensity of computing equipment of 300 watts per square foot.

DUNDER MIFFLIN, INC.
PAPER COMPANY



NETWORK EQUIPMENT

WEB SOLUTIONS

EBUSINESS SOLUTIONS

TABLE OF CONTENTS

Terms and Definitions

• **Cisco 3-Layer Hierarchical Model**

- This model consists of three-layers that helps to design, implement, and maintain scalable, reliable, and cost-effective network infrastructure. Each layer; Core Layer, Distribution Layer, and Access Layer, have their own feature and functionality, and these help in reducing network complication.

- **Core Layer:** also known as the network backbone, is responsible in transporting a great deal of traffic quickly. The layer provides connectivity between high speed devices in the distribution layer, such as high-end routers and switches with redundant links.

- **Distribution Layer:** this is the communication point between the Core and the Access Layers. This layer's main function is to provide routing, filtering, and WAN access. It also determines the how packets access the core and the fastest way that network service is accessed.

- **Access Layer:** On the network, this layer controls the user and workgroup access to resources. Usually, this is the layer where Layer 2 switches and access are incorporated and provide connectivity between the various computers and servers. Here is where you can implement security to ports, manage access control and policy, and create separate collision domains.

• **VLAN (Virtual Local Area Network)** are used to group broadcast traffic and multiple domains and each VLAN is in own broadcast domain.

- **VLANs** with the help of subnets help to separate out groups of users and network traffic. Through this method, departments will acquire their own subnet and VLAN.

- **Subnet** is the division of an IP network which is a set of communications protocols used in the internet and other similar networks.

• **ISP** (Internet Service Provider) is the organization that will be providing the internet service to the business and its employees. ISP should be pre-selected before work on network can begin.

• **DHCP** (Dynamic Host Configuration Protocol) is a client/server protocol that automatically provides an IP (Internet Protocol) host with an IP address along with subnet mask and a default gateway.

• **DNS** (Domain Name System) is a protocol within the set of standards for how computers exchange data on the internet and on many private networks which are known as TCP/IP protocol suite.

• **NAT** (Network Address Translation) generally operates on router or firewall, and helps improve security by reusing IP addresses. NAT is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide internet access to the local hosts.

NETWORK EQUIPMENT

WEB SOLUTIONS

EBUSINESS SOLUTIONS

TABLE OF CONTENTS

Terms and Definitions (cont.)

• **IGRP** (Internal Gateway Routing Protocol) is a proprietary network protocol designed to send all or a portion of its routing table in s routing message update at regular intervals to each of its neighboring routers in order to choose the best path between a source and a destination.

• **BGP** (Border Gateway Protocol) is a routing protocol used to transfer data and information between different host gateways, the internet or autonomous systems.

• **eBGP** (External Border Gateway Protocol) is an extension of BGP that is used for communication between distinct autonomous systems and enables network connections between those systems implemented with BGP.

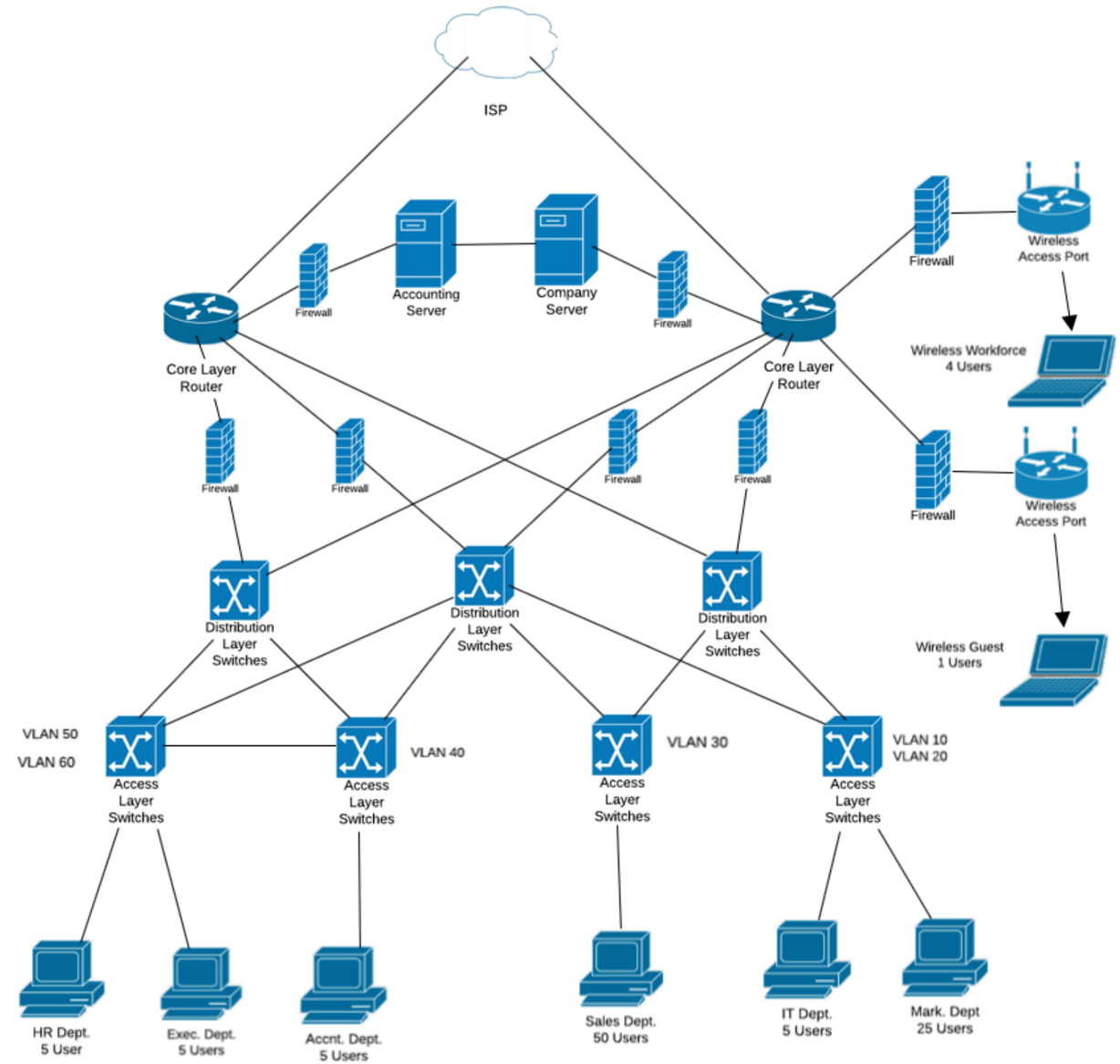
NETWORK EQUIPMENT

WEB SOLUTIONS

EBUSINESS SOLUTIONS

Physical Newtork Design Diagram

TABLE OF CONTENTS



NETWORK EQUIPMENT

WEB SOLUTIONS

EBUSINESS SOLUTIONS

Logical Networking Design Addressing

Department	VLAN	Begin IP Address	End IP Address	IP Access Switch	Mask
IT Dept.	VLAN 10	192.168.10.1	192.168.10.124	192.168.10.125/25	255.255.255.128
Mark. Dept.	VLAN 20	192.168.20.129	192.168.20.190	192.168.20.128/26	255.255.255.192
Sales Dept.	VLAN 30	192.168.30.193	192.168.30.222	192.168.30.192/27	255.255.255.224
Accnt. Dept.	VLAN 40	192.168.40.225	192.168.40.254	192.168.40.224/27	255.255.255.224
Exec. Dept.	VLAN 50	192.168.50.241	192.168.50.254	192.168.50.240/28	255.255.255.240
HR Dept.	VLAN 60	192.168.60.245	192.168.60.249	192.168.60.248/29	255.255.255.248

TABLE OF CONTENTS

Equipment Cost List

Switch

Device	Quantity	Cost Per Unit	Total Cost
Cisco Catalyst 3850 Series model 48	2	$5,998	$11,996
	- 48 Multigigabit ports - 48 UPOE ports - Ethernet management port: RJ-45 connectors, 4-pair Cat-5 UTP cabling - Management console port: RJ-45-to-DB9 cable for PC connections		
Cisco Catalyst 3850 Series model 24	2	$11,630	$23,260
	- 24 multigigabit ports - 24 UPOE ports - Ethernet management port: RJ-45 connectors, 4-pair Cat-5 UTP cabling - Management console port: RJ-45-to-DB9 cable for PC connections		
Cisco Catalyst 9300 Series 24	3	$12,140	$36,420
	- 24 Multigigabit Cisco UPOE (100 Mbps or1, 2.5, 5 or 10 Gbps) - Ethernet management port: RJ-45 connectors, 4-pair Cat-5 UTP cabling - Management console port: RJ-45-to-DB9 cable for PC connections		

NETWORK EQUIPMENT

WEB SOLUTIONS

EBUSINESS SOLUTIONS

TABLE OF CONTENTS

Equipment Cost List (Cont.)

Routers

Device	Quantity	Cost Per Unit	Total Cost
Cisco ASR 1009-X Model	2	$7,607.25	$15,214.50
	- Ethernet management port: RJ-45 connectors, 4-pair Cat-5 UTP cabling - Management console port: RJ-45-to-DB9 cable for PC connections - These routers will be secure with Firewall and Data Encryption for protection between the new branch and Tech Inc. main office.		
Cisco AIR-WLC2125-K9	1	$3,306.00	$3,306.00
	- Management console port: RS-232 (DB-9 males/RJ-45 connector included) - Network: Eight 10/100 Mbps Ethernet (RJ-45) including two 802.3af or Cisco PoE ports rated for use with Cisco Aironet lightweight access points - LED indicators: Link activity (each 10/100 port), Power Status, Alarm, Access Point Joined - Designed for use with Cisco Wireless Control System - Command-line interface: Telnet, SSH, serial port - WEP and Temporal Key Integrity Protocol-Message Integrity Check (TKIP-MIC): RC4 40, 104 and 128 bits (both static and shared keys) - Secure Sockets Layer (SSL) and Transport Layer Security (TLS): RC4 128-bit and RSA 1024- and 2048-bit - Advanced Encryption Standard (AES): CCM, Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)		

Equipment Total Cost:

$90,196.50

NETWORK EQUIPMENT

WEB SOLUTIONS

EBUSINESS SOLUTIONS

TABLE OF CONTENTS

Install Cost Breakdown

Installations	Total
Wiring	$4,560.00
Cabinets & Cables	$12,385.00
Network Setup	$20,682.00
Total	$37,627

Labor and Network Configuration

Items	Hourly Rate
Labor & Networking Setup	$185
Total	$7,400

Total Cost of Network
$135,223.50

Project Timeline
3 Week Install

Network Objectives

Scalability

This network design proposal allows the network capability to grow and add more computers, workstations, and other devices without the need to revise the network design. This system also offers the ability to transition from IPv4 to IPv6. The design allows all of the departments included in this proposal to increase two times their size with plenty of IP addresses.

Also, server room is designed to allow four racks for future servers, routers, and switches when growth is needed.

Security

For security, critical alarms will be applied to the functioning of the AC system and physical data of the room mapped into the Facilities Management System. Also, there will be monitoring and alarms that are provided by the department for their notification of critical operating criteria of the computing systems, separate from the Facilities Management System. All entrances to the server room will be properly secured, and with alarms. Access should only be limited to the company's IT specialists. At the core layer, in order to provide extra security for private networks, the Network Address Translation (NAT) will also be configured.

NETWORK EQUIPMENT

WEB SOLUTIONS

EBUSINESS SOLUTIONS

TABLE OF CONTENTS

Appendix

I. What network design pattern did you use for your proposal? Why did you choose this pattern? Have you explained in your proposal the benefit of the design you are recommending?

The network design pattern proposed is the Cisco 3 Layer Hierarchical model layers: core, distribution and access layer for supporting scalability, which is explained in this proposal.

II. Are you recommending the use of NAT? Why?

For additional security, NAT will be configured in order to allow private networks to connect to the internet and exclude the need to obtain registered addresses for every host.

III. What internal routing protocol(s) are you recommending? Why did you select the protocol(s) you did?

The chosen routing protocol for this network design is IGRP for proper management of routing flow within the connected routers of the host network.

IV. What protocol(s) are you using to connect with the ISP? Why did you select the protocol(s) you did?

The protocol chosen for this design proposal is eBGP for proper enabling network connections when it comes to autonomous systems. This will help to advertise the block of public IP addresses to ISP service of internet.

V. How are you addressing the security requirements?

At the core layer, the Network Address Translation (NAT) will be configured along with critical alarms for the functioning of the AC system and physical data of the room mapped into the Facilities Management System. Also, there will be monitoring and alarms that are provided by the department for their notification of critical operating criteria of the computing systems, separate from the Facilities Management System. All entrances to the server room will be properly secured, and with alarms. Access should only be limited to the company's IT specialists.

VI. How are you addressing the potential need for future expansion?

This network design proposal allows the network capability to grow and add more computers, workstations, and other devices without the need to revise the network design. This system also offers the ability to transition from IPv4 to IPv6. The design allows all of the departments included in this proposal to increase two times their size with plenty of IP addresses.

Also, server room is designed to allow four racks for future servers, routers, and switches when growth is needed.

VII. Are you confident in the resiliency of your proposed network design? What design elements will provide the resiliency?

The design for this proposed network is recommended as it provides both the internal and external protocols needed to allow the various departments their needed data with the needed security.

NETWORK EQUIPMENT

WEB SOLUTIONS

EBUSINESS SOLUTIONS