

ACME Corporation

The Master Plan

Joel Gomez

David Phan

Nick Willhite

June 4, 2017

Contents

1	Overview	3
1.1	Purpose	3
1.2	Services	3
1.2.1	Existing Services	3
1.2.2	Database	3
1.2.3	Active Directory	4
1.2.4	New Services	6
1.3	Architecture	6
1.3.1	Design Overview	6
1.3.2	Network Topology Map	7
2	Network Access	8
3	NFS	8
4	Webserver	8
5	Email	8
6	Firewall & Security	8
7	Active Directory	10
8	DNS / DHCP	10
9	Configuration Management	10

1 Overview

1.1 Purpose

This document contains pertinent information for the architecture and implementation of Acme Corporation's network upgrade, including details over topology, services, and high-level configuration descriptions where applicable.

1.2 Services

All existing services must be upgraded to accommodate the network upgrade. The scope of each service upgrade will vary based on the need, but each service will be reimplemented to better fit within the post-upgrade network architecture.

1.2.1 Existing Services

The following existing services are upgraded (in no particular order):

Service Description	Preferred Package/Application
Network File System (NFS)	nfs-kernel-server, nfs-client
Webserver	apache2
Database	mariadb
Email	???
Active Directory (AD)	openldap
Domain Name Server (DNS)	-\$30,000
Dynamic Host Configuration Protocol (DHCP)	dhcpcd

1.2.2 Database

We are going with a MariaDB database for ACME as it widely used, easily maintainable, and secure. In order to set up the MariaDB database we would need to install it both the client and server packages.

- `sudo apt-get install mariadb-server`

After running the installation of MariaDB we then would need to set up our admin user so we are then able to populate the database with data that ACME CORP needs to be stored.

By running:

- `sudo mysql_secure_installation`

We are able to do all of the following:

- set root password

- disable remote root login
- remove test database
- remove anonymous users and
- reload privileges

After adding the data that needs to be stored we would then set up the user accounts and privileges for the HR department as they are the only department needing access to the database.

- MariaDB > CREATE USER frankHR@'localhost' IDENTIFIED BY 'password';
- MariaDB > GRANT ALL PRIVILEGES on employees.* to frankHR@'%';
- MariaDB > FLUSH PRIVILEGES;

By the above commands we created a user account from Frank from HR and then have given Frank privileges to access the database 'employees'. Following this same style we would be able to add new tables and users and also give and take away privileges based on needs.

1.2.3 Active Directory

We chose to use OpenLDAP as our active directory protocol.

- sudo apt-get install slapd ldap-utils

This will prompt you administrator password for the administrator LDAP account. After changing some recommended setting we then enter:

- dpkg-reconfigure slapd

The above command reconfigures with the updated information we entered. After running this command we are then asked for numerous pieces of information

- DNS domain name
- Organization name (ACME)
- LDAP admin password which we created earlier
- Selection of backend database.

After the steps above we then test the OpenLDAP by running:

- ldapsearch -x

If the 'Success' message outputs, then Congratulations! Our LDAP Server is working!!

Now to install the LDAP Server Administration portion. Since we will have a team of users that might not be great with computers, we will go with the GUI tool. Which will help the manage and configure the LDAP server. We install it with the following command:

- `sudo apt-get install phpldapadmin`

We then have to set symbolic link for the phpldapadmin directory:

- `ln -s /usr/share/phpldapadmin/ /var/www/html/phpldapadmin`

We then need to edit the config.php file for setting correct time zone:

- `vim /etc/phpldapadmin/config.php`

We will look for a line:

- `$config->custom->appearance['timezone'] = ;`

Change it to ACME Pennsylvania:

- `$$config->custom->appearance['timezone'] = 'US/Pennsylvania';`

Lastly we need to find and replace the domain names with our own. Find "Define LDAP Servers" section with in config file and change the following lines:

```
// Set your LDAP server name //
$servers->setValue('server','name','Unixmen LDAP Server');

// Set your LDAP server IP address //
$servers->setValue('server','host','192.168.1.103');

// Set Server domain name //
$servers->setValue('server','base',array('dc=unixmen,dc=local'));

// Set Server domain name again//
$servers->setValue('login','bind_id','cn=admin,dc=unixmen,dc=local');
```

We need to restart the apache service using:

- `systemctl restart apache2`

Now make sure port "80" and port "389" are open in the firewall/router config and we are finished.

1.2.4 New Services

The following new services are implemented on the new network (in no particular order):

Service Description	Preferred Package/Application
Virtual Local Area Network (VLAN)	vlan
Configuration Management	puppet
Monitoring	nagios
Virtual Private Network (VPN)	openvpn

1.3 Architecture

1.3.1 Design Overview

VLANs

The upgraded network ensures that departments and specific services are isolated (per the new network requirements) by distributing them across separate VLANs. This configuration allows for any combination of hosts assigned to different departments to be physically attached to the same switch (in the event that physical separation is not feasible), while maintaining separation.

The VLANs are assigned as follows:

Addresses	VLAN	Department/Service
10.1.110.0/24	10	Executives
10.1.120.0/24	20	Human Resources
10.1.130.0/24	30	Research & Development
10.1.140.0/24	40	Engineering
10.1.150.0/24	50	Sales
10.1.160.0/24	60	Internal Services
10.1.170.0/24	70	DMZ

Inter-Router/Switch Interfaces

Interfaces between router-router and switch-router (and vice versa) are assigned addresses with a CIDR of /30. The address space 10.1.2.0/24 is reserved specifically for these interfaces.

Switch Ports

Switch ports are statically assigned, as needed, within the address space of 10.1.10.0/24.

Static Hosts

Special hosts (specific services, such as DHCP, etc.) are assigned IP addresses statically within the address space of 10.1.160.0/24 for internal services,

Server Zone	
Addresses	Service
10.1.160.1/24	DHCP
10.1.160.2/24	DNS
10.1.160.3/24	Active Directory
10.1.160.4/24	Database
10.1.160.5/24	NFS

and within the address space of 10.1.170.0/24 for DMZ services.

DMZ Zone	
Addresses	Service
10.1.170.1/24	Web
10.1.170.2/24	SMTP

Workstation Hosts

Workstation IP addresses are dynamically assigned by the DHCP server. Workstations are configured to use the IP of the switch port that they are physically connected to as their gateway to ensure that they connect to the network only via the preassigned switch port.

Through our topology we have upgraded from an all layer 2 network to a combination of layer 2 and layer 3. Thus allowing for a more robust and "smart" network. With the implementation of layer 3 we have added routers to control the broadcast signals that were not controlled within the previous network. We have added redundancy to the network allowing multiple connection points. To control the restrictions we have upgraded the network with VLANs. Thus ensuring isolated departments and services by dividing them into separate VLANs.

1.3.2 Network Topology Map

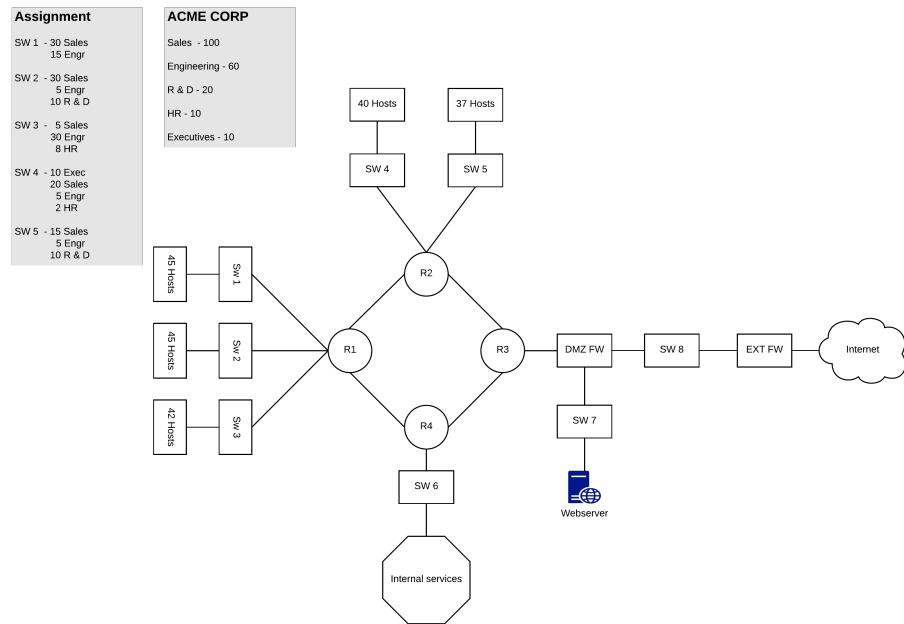


Figure 1: Topology Map for Acme Corp

2 Network Access

3 NFS

4 Webserver

5 Email

6 Firewall & Security

Router 1							
From Zone	To Zone	SRC ADDR	DST ADDR	SRC Port	DST Port	App	Deny / Allow
Trusted	Trusted	10.1.110.0/24	Any	Any	Any	Any	Allow
Trusted	Trusted	10.1.150.0/24	Any	Any	Any	Any	Deny
Trusted	Trusted	10.1.130.0/24	10.1.140.0/24	Any	Any	Any	Allow
Trusted	Trusted	10.1.140.0/24	10.1.130.0/24	Any	Any	Any	Allow
Trusted	Trusted	10.1.120.0/24	Any	Any	Any	Any	Allow
Trusted	Trusted	10.1.120.0/24	10.1.110.0/24	Any	Any	Any	Deny
Trusted	Server	Any	10.1.160.0/24	Any	53, 389, 994	Any	Allow
Server	Trusted	10.1.160.0/24	Any	Any	53, 389, 994	Any	Allow
Trusted	Server	10.1.120.0/24	10.1.160.0/24	Any	3306	Any	Allow

Router 2							
From Zone	To Zone	SRC ADDR	DST ADDR	SRC Port	DST Port	App	Deny / Allow
Trusted	Trusted	10.1.110.0/24	Any	Any	Any	Any	Allow
Trusted	Trusted	10.1.150.0/24	Any	Any	Any	Any	Deny
Trusted	Trusted	10.1.130.0/24	10.1.140.0/24	Any	Any	Any	Allow
Trusted	Trusted	10.1.140.0/24	10.1.130.0/24	Any	Any	Any	Allow
Trusted	Trusted	10.1.120.0/24	Any	Any	Any	Any	Allow
Trusted	Trusted	10.1.120.0/24	10.1.110.0/24	Any	Any	Any	Deny
Trusted	Server	Any	10.1.160.0/24	Any	53, 389, 994	Any	Allow
Server	Trusted	10.1.160.0/24	Any	Any	53, 389, 994	Any	Allow
Trusted	Server	10.1.120.0/24	10.1.160.0/24	Any	3306	Any	Allow
Server	Trusted	10.1.160.0/24	10.1.120.0/24	Any	3306	Any	Allow
Trusted	DMZ	Any	10.1.170.0/24	Any	25, 993, 80, 443	Any	Allow
DMZ	Trusted	10.1.170.0/24	Any	Any	25, 993, 80, 443	Any	Allow
Any	Any	Any	Any	Any	Any	Any	Deny

Router 3							
From Zone	To Zone	SRC ADDR	DST ADDR	SRC Port	DST Port	App	Deny / Allow
Trusted	DMZ	10.1.0.0/24	10.1.170.0/24	Any	25 ,993 , 80, 443	Any	Allow
DMZ	Trusted	10.1.170.0/24	10.1.0.0/24	Any	25, 993, 80, 443	Any	Allow
Server	DMZ	10.1.160.0/24	10.1.170.0/24	Any	3306	Any	Allow
DMZ	Server	10.1.170.0/24	10.1.160.0/24	Any	3306	Any	Allow
Any	Any	Any	Any	Any	Any	Any	Deny

Router 4							
From Zone	To Zone	SRC ADDR	DST ADDR	SRC Port	DST Port	App	Deny / Allow
Server	Server	Any	Any	Any	Any	Any	Allow
Trusted	Server	10.1.0.0/24	Any	Any	53, 389, 994	Any	Allow
Server	Trusted	10.1.160.0/24	10.1.0.0/24	Any	53, 389, 994	Any	Allow
DMZ	Trusted	10.1.170.0/24	10.1.0.0/24	Any	25, 993, 80, 443	Any	Allow
Trusted	Server	10.1.120.0/24	10.1.160.0/24	Any	3306	Any	Allow
Server	Trusted	10.1.160.0/24	10.1.120.0/24	Any	3306	Any	Allow
Server	DMZ	10.1.160.0/24	10.1.170.0/24	Any	3306	Any	Allow
DMZ	Server	10.1.170.0/24	Any	Any	3306	Any	Allow
Any	Any	Any	Any	Any	Any	Any	Deny

Firewall							
From Zone	To Zone	SRC ADDR	DST ADDR	SRC Port	DST Port	App	Deny / Allow
Trusted	DMZ	10.1.0.0/24	10.1.170.0/24	Any	80, 443	Meme.com	Deny
DMZ	Trusted	10.1.170.0/24	10.1.0.0/24	Any	25, 993, 80, 443	Any	Allow
Server	DMZ	10.1.160.0/24	10.1.170.0/24	Any	3306	Any	Allow
DMZ	Server	10.1.170.0/24	10.1.160.0/24	Any	3306	Any	Allow
Any	Any	Any	Any	Any	Any	Any	Deny

7 Active Directory

8 DNS / DHCP

9 Configuration Management