ACME Corporation

The Master Plan

Joel Gomez David Phan Nick Willhite

June 9, 2017

Contents

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	postfix
Active Directory (AD)	openldap
Domain Name Server (DNS)	(-$30,000)
Dynamic Host Configuration Protocol (DHCP)	dhcpd

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

Server Zone	
Addresses	**Service**
10.1.160.1	DHCP
10.1.160.2	DNS
10.1.160.3	Active Directory
10.1.160.4	Database
10.1.160.5	NFS
10.1.160.6	Backups

DMZ Zone	
Addresses	**Service**
10.1.170.1	Web
10.1.170.2	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 that they are physically connected to as their gateway to ensure that they connect to the network only via the preassigned switch port.

1.3.2 Network Topology Map

The upgraded Acme Corp. network is expanded from an all layer 2 network to a combination of layer 2 and layer 3 – allowing for a more robust and "smart" network. The new network accounts for future expansion in the form of available ports on the four main routers that can host additional switches when the time comes to expand the network. IP address availability is assured by the spacing between VLAN subnets once the 254 useable addresses on a particular VLAN have been exhausted.

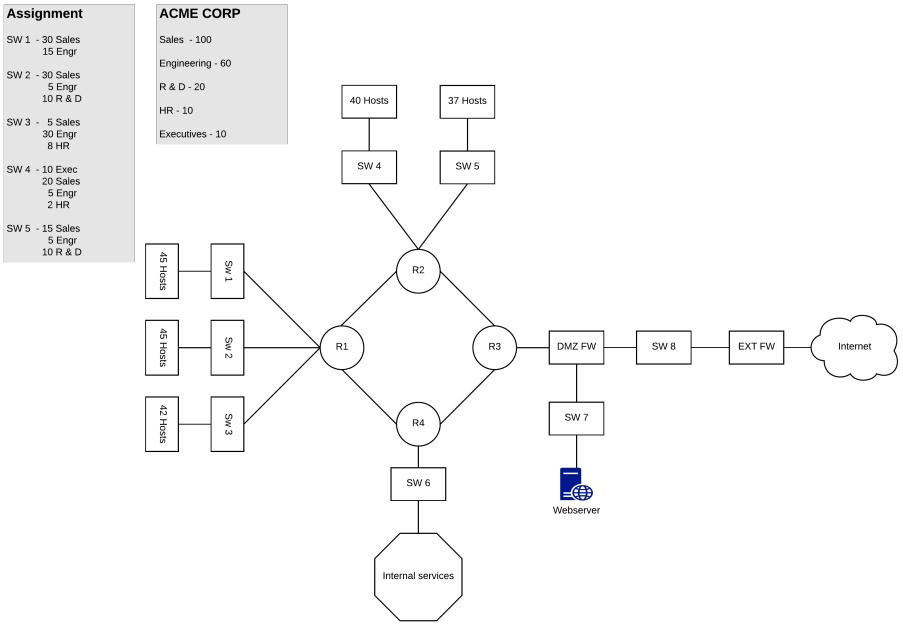

Figure 1: Topology Map for Acme Corp

2 Implementation

2.1 Network Access

2.2 Network File System

The Network File System (NFS) service for Acme Corp. relies on the in-built support for NFS baked into the Linux kernel.
Assumption!: The upgraded network requirements did not specify if Acme Corp. user directories are hosted from the NFS server. It is assumed that business operations require departments to share files in the specific department shared directory and that users will only store personal files in their own home directories. With this assumption in mind, only department-specific shares are configured on the NFS server.

2.2.1 Network/Interface Information

Network Gateway
The NFS server itself connects to the network through Fa0/5 of Switch 6 and is a

member of the Acme Corp. "Server Zone". The default gateway for the NFS server is the static IP for Fa0/5 on the **10.1.10.0/24** subnet, TBD.

IP Address
The NFS server is a member of the Internal Services ("Server Zone"), and is likewise configured on subnet **10.1.160.x**, with a static IP address of **10.1.160.5**.

2.2.2 Server Setup/Configuration

To enable the NFS functionality of the Linux kernel, the nfs−kernel−server package must be installed on the server.

```
# apt install nfs-kernel-server
```

Additionally, some config files must be modified from the defaults.

/etc/idmapd.conf

The only necessary change to this file is assigning the Acme Corp. domain.

```
Domain = acme.com
```

/etc/exports

The exports file defines which directories will be exported and to which user groups. Per the upgraded network requirements, the NFS shares are assigned only to the respective subnets for which they are "allowed visibility".

```
# mounts Executive share to IPs on the Executive VLAN
/home/exec 10.1.110.0/24(rw)

# mounts HR share to IPs on the Executive, and HR VLANs
/home/hr 10.1.110.0/24(rw) 10.1.120.0/24(rw)

# mounts R&D share to IPs on the Executive, HR,
# R&D, and Engineering VLANs
/home/rnd 10.1.110.0/24(rw) 10.1.120.0/24(rw) \
    10.1.130.0/24(rw) 10.1.140.0/24(rw)

# mounts Engineering share to IPs on the Executive,
# HR, R&D, and Engineering VLANs
/home/engr 10.1.110.0/24(rw) 10.1.120.0/24(rw) \
    10.1.130.0/24(rw) 10.1.140.0/24(rw)
```

```
# mounts Sales share to IPs on the Executive, HR,
# and Sales VLANs
/home/sales 10.1.110.0/24(rw) 10.1.120.0/24(rw) \
    10.1.150.0/24(rw)
```

2.2.3 Client Setup/Configuration

To enable the NFS functionality on each client workstation, the nfs−client package must be installed on each respective workstation.

```
# apt install nfs-client
```

Additionally, some config files must be modified from the defaults.

```
/etc/idmapd.conf
```

The only necessary change to this file is assigning NFS server domain (as configured by the DNS).

```
Domain = nfs.acme.com
```

Each client must be configured to mount the share on system boot. This can be done by editing the following file on the client:

```
/etc/fstab
```

```
# [share] is a place holder for the appropriate
# department share folder
nfs.acme.com:/home/[share]  /home/[share]  nfs defaults 0 0
```

* Some clients may require a line for each share that must be mounted. For example, an Executive client must mount all network shares so the client configuration might look like:

```
nfs.acme.com:/home/exec     /home/exec    nfs defaults 0 0
nfs.acme.com:/home/hr       /home/hr      nfs defaults 0 0
nfs.acme.com:/home/rnd      /home/rnd     nfs defaults 0 0
nfs.acme.com:/home/engr     /home/engr    nfs defaults 0 0
nfs.acme.com:/home/sales    /home/sales   nfs defaults 0 0
```

Additionally, each client must be configured with the autofs package.

```
# apt install autofs
```

And the following files must be edited, respectively:

```
/etc/auto.master
```

```
/-  /etc/auto.mount
```

```
/etc/auto.mount
```

```
/home/[share] -fstype=nfs,rw nfs.acme.com:/home/[share]
```

* [share] is a place holder for *each* share that must be mounted, as before. An entry must be created for each share to be mounted.

Finally, a directory should be created on each respective client for each NFS share that will be mounted.

2.3 Web server

The Acme Corp. web server must host a website that is accessible to Sales, and a back-end database that is accessible to HR.

Assumption!: The network upgrade requirements do not state what Sales will be using the website for (i.e. Retrieving information only or also creating/updating information). At the time of the upgrade, it is assumed that the website is solely a tool that Sales uses to show-off Acme Corp's products to potential clients. If the requirements of the network change in the future and Sales requires CRUD functionality, it is trivial to create a new database and setup appropriate accounts and permissions to allow such functionality.

2.3.1 Network/Interface Information

Network Gateway
The web server connects to the network through Fa0/1 of Switch 7 and is a member of the Acme Corp. "Demilitarized Zone". The default gateway for the web server is the static IP for Fa0/1 on the **10.1.10.0/24** subnet, TBD.

IP Address
The web server is a member of the External Services (DMZ), and is likewise configured on the subnet 10.1.170.x, with a static IP address of **10.1.160.1**.

2.3.2 Server Setup/Configuration

The Acme Corp. web server will run a LAMP stack using Apache and PHP. The following will install the necessary packages on the web server (the database is installed on a separate server, so it is not a required package on the web server).

```
# apt install apache2 php7.0 libapache2-mod-php7.0 \
      php7.0-mcrypt php7.0-mysql
```

Additionally, a few default files should be edited as demonstrated below.

```
/etc/apache2/sites-enabled/000-default.conf
```

ServerAdmin directive should be changed to "systems@acme.com".

```
/etc/apache2/apache2.conf
```

Remove FollowSymLinks from the <Directory /var/www/> scope.

Additionally, the following should be appended to the end of the file:

```
ServerName 'web.acme.com'
```

2.4 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.

2.5 Email

For our email setup, we are configuring a Postfix server to send email through our external SMTP provider, SendGrid.

2.5.1 Installing Postfix

1. Install Postfix with the following command:

   ```
   $ sudo apt-get install postfix
   ```

2. During installation, a prompt will appear asking for your **General type of mail configuration.** Select **Internet Site.**
3. Enter the fully qualified name of your domain,**fqdn.acmecorp.com**
4. Once the installation is finished, edit the **main.cf** file with your favorite text editor.

   ```
   $ sudo vim /etc/postfix/main.cf
   ```

5. Set **myhostname** parameter to be configured with your server's FQDN:

   ```
   myhostname = fqdn.acmecorp.com
   ```

2.5.2 How to configure SMTP Usernames and Passwords

1. Open or create the **/etc/postfix/sasl_passwd** file, using your favorite text editor:

   ```
   $ sudo vim /etc/postfix/sasl_passwd
   ```

2. Add your destination (SMTP Host), username, and password in the following format:

   ```
   [smtp.sendgrid.net]:587 username:password
   ```

3. Create the hash db file for Postfix by running the command:

   ```
   $ sudo postmap /etc/postfix/sasl_passwd
   ```

   If successful, there should be a new file generated, **sasl_passwd.db** in the **/etc/postfix/** directory.

2.5.3 How to secure your Password and Hash Database Files

1. We change the permissions of **/etc/postfix/sasl_passwd** and **/etc/postfix/sasl.passwd.db** so that only the root user can read or write to the file. Run the commands:

   ```
   $ sudo chown root:root /etc/postfix/sasl_passwd
   $ sudo chown root:root /etc/postfix/sasl_passwd.db
   $ sudo chmod 0600 /etc/postfix/sasl_passwd
   $ sudo chmod 0600 /etc/postfix/sasl_passwd.db
   ```

2.5.4 How to configure the Relay Server

1. Open the **/etc/postfix/main.cf** file with your favorite text editor:

   ```
   $ sudo vim /etc/postfix/main.cf
   ```

2. Update the **relayhost** parameter to show your external SMTP relay host.

   ```
   relayhost = [smtp.sendgrid.net]:587
   ```

3. At the end of the file, add the following parameters to enable authentication:

   ```
   # enable SASL authentication
   smtp_sasl_auth_enable = yes
   # disallow methods that allow anonymous authentication.
   smtp_sasl_security_options = noanonymous
   # where to find sasl_passwd
   smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
   # enable STARTTLS encryption
   ```

```
smtp_use_tls = yes
# where to find CA certificates
smtp_tls_CAfile = /etc/ssl/certs/ca-certificates.crt
```

Save your changes.

4. Restart Postfix, by running the command:

```
$ sudo service postfix restart
```

2.5.5 Design Justifications

We connected our server to a mailing service, SendGrid because it helps AcmeCorp avoid pitfalls like having our server IP getting blacklisted by anti-spam services. We chose port 587 (mail submission agent) for our email client to email server communication, because the MSA accepts email after authentication. It helps stop outgoing spam when netmasters of DUL ranges can block outgoing connections to the SMTP port (port 25).

2.6 Firewall & Security

2.6.1 ACLs

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
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 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

2.6.2 Honey Pot

2.6.3 Design Justifications

The upgraded Acme Corp. network is configured to DENY all ports by default, and selectively open ports for known applications and services that have been pre-approved or specified in the new network requirements. It is possible that this policy may need to be revisited as necessary since blocking of ALL ports may likely cause unexpected behavior for applications and services that were not explicitly noted in the upgrade requirements, (i.e. ports for printing, ping, et al. are blocked in the current configuration). The upgraded network architects realize that this is a trade-off as a result of extreme security measures.

2.7 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';
```

Lastely 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.

2.8 DNS

2.9 DHCP

2.10 Configuration Management

2.11 Backups

2.12 VPN