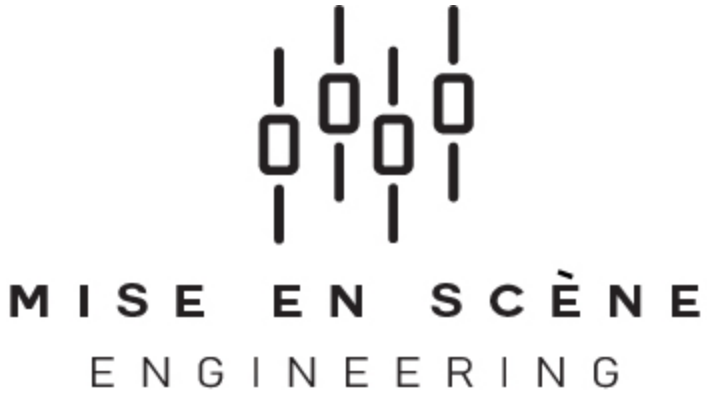
Date: June 15th 2018

Mise En Scene Engineering



Student Project Final Report

Group 5-B2

Group Members:

Gabriel Kwan (Leader + Hardware)

David Lee (MS + Hardware)

Vanessa Luu (Networking)

Arjay Emata (Linux)

Noel Lee (Linux)

Aaron Yang (MS + Hardware)

Johnny Le (Networking)

Table of Contents

Mise En Scene Engineering

Mission Statement

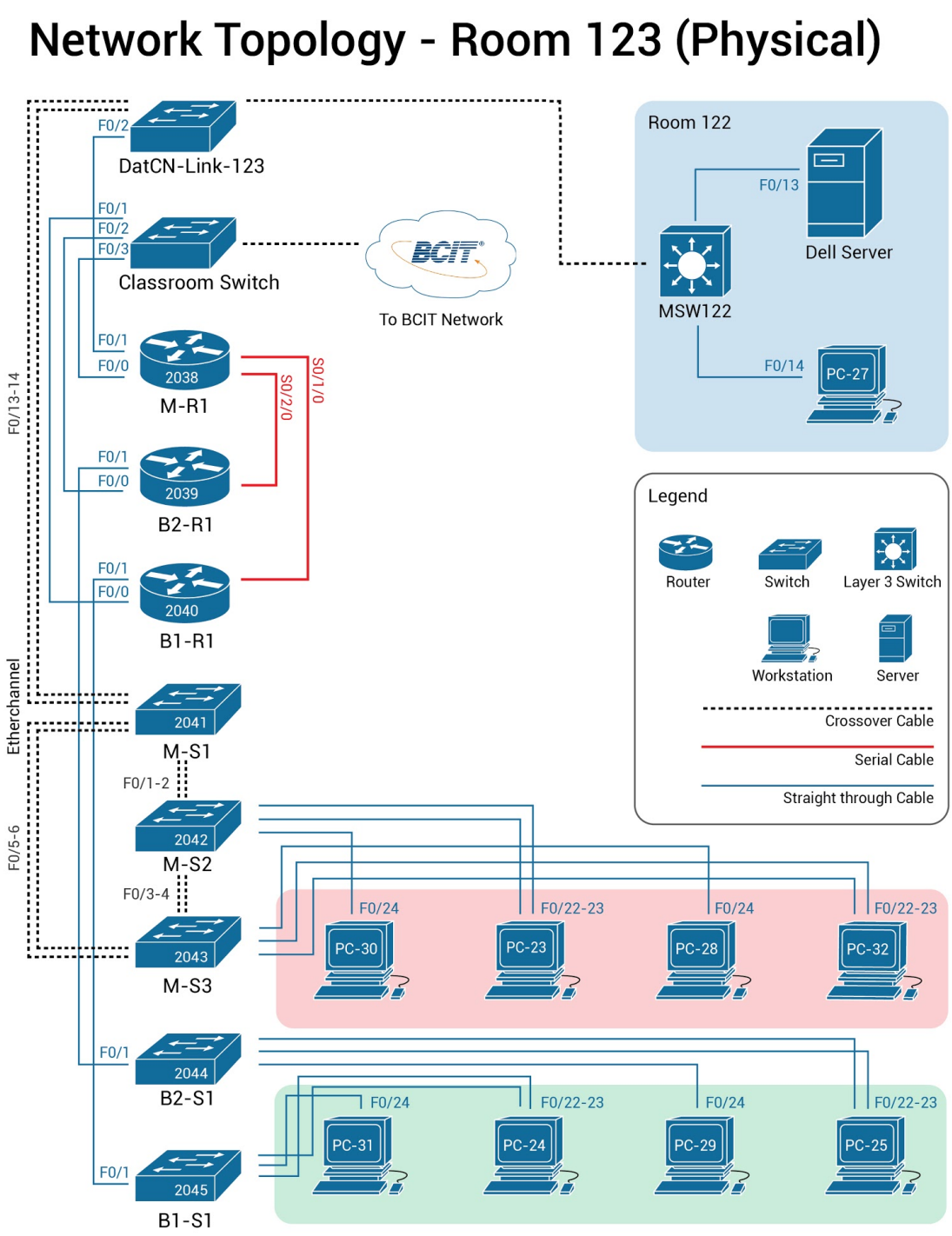
In an increasingly connected world, our engineers require infrastructure keep pace. This plan will enable them to do so with peace of mind and allow them to make the world a better place, one job at a time.

Mise En Scene Engineering believes in providing our clients with technical solutions along with innovative designs that are not only practical, but sustainable as well. Our company is committed to meeting the needs of our clients by finding quality alternatives that are cost-effective and long-lasting. We aim to push boundaries by challenging ourselves to become leaders in innovation and technology.

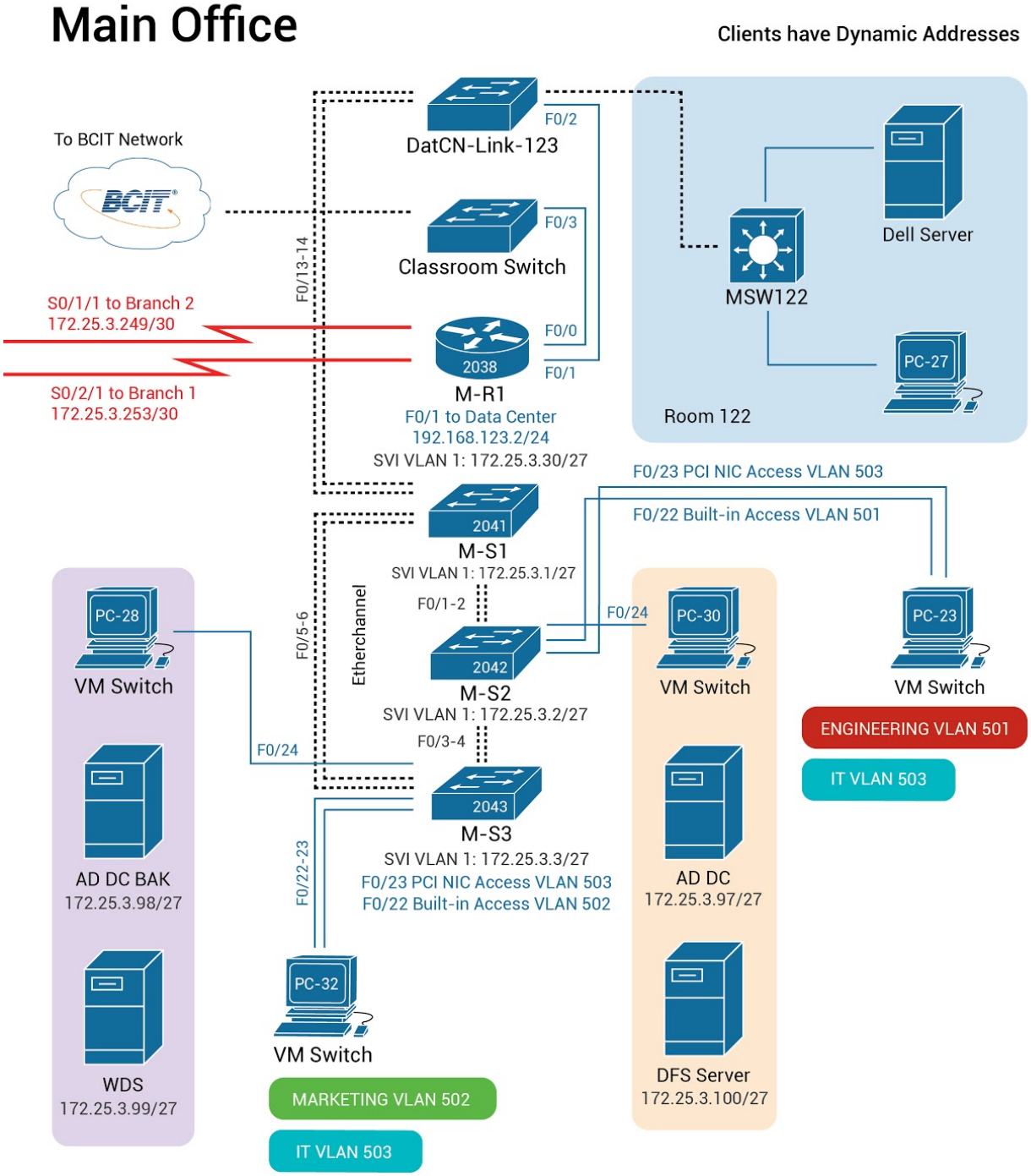
Introduction

The purpose of this document is to help provide a general description of the components and operation of Mise En Scene Inc's network. It includes an overview of the network infrastructure, features that have been implemented, and why those features have been chosen. The appendix included expands on the features and configurations of the network.

Topology

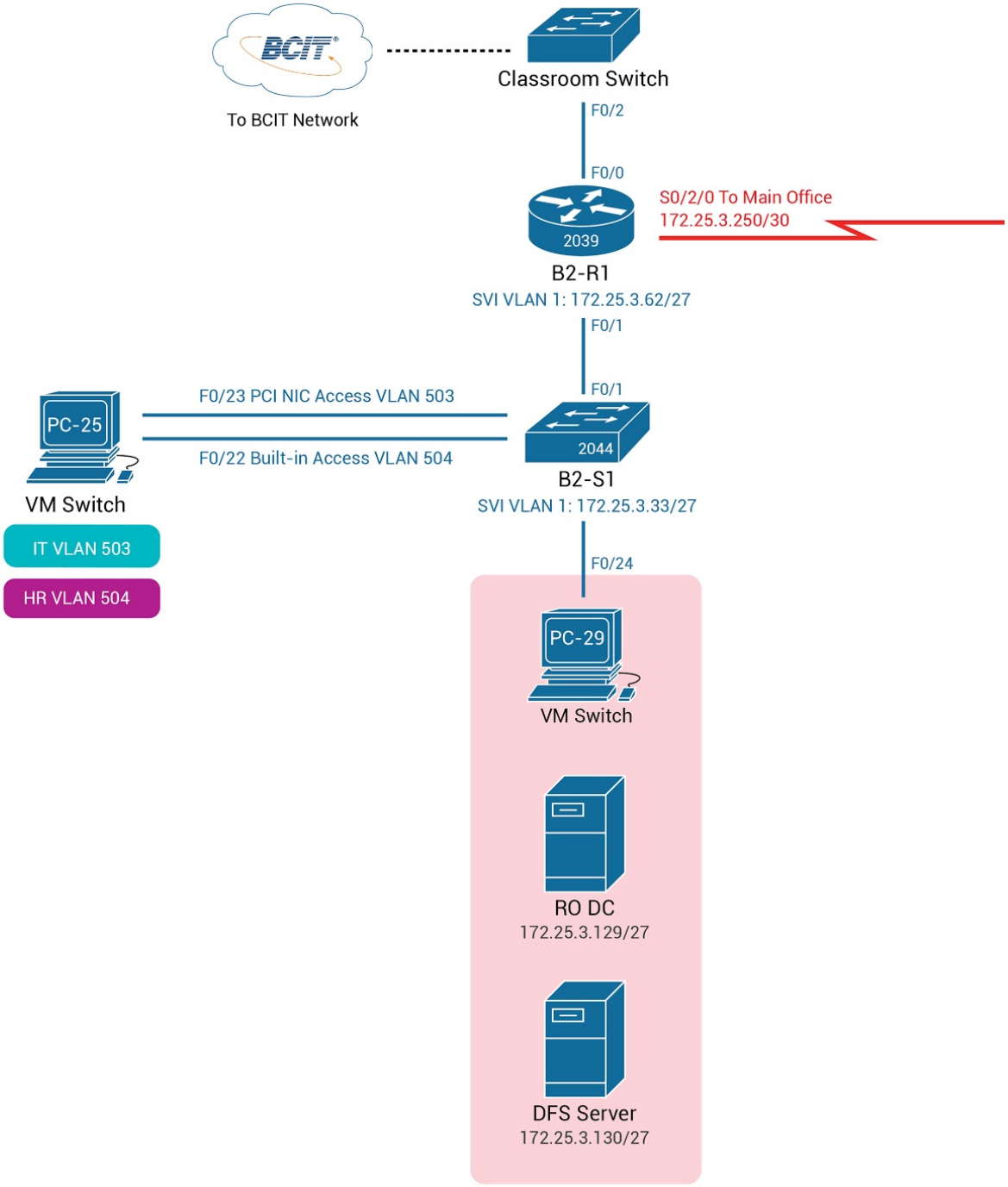

Network Topology - Room 123 (Physical)
F0/2
DatCN-Link-123
F0/1
F0/2
F0/3
Classroom Switch
BCIT
To BCIT Network
Room 122
F0/13
Dell Server
MSW122
F0/14
PC-27
F0/1
F0/0
2038
M-R1
S0/2/0
S0/1/0
F0/1
F0/0
2039
B2-R1
F0/1
F0/0
2040
B1-R1
F0/13-14
Etherchannel
F0/5-6
Legend
Router
Switch
Layer 3 Switch
Workstation
Server
Crossover Cable
Serial Cable
Straight through Cable
2041
M-S1
F0/1-2
2042
M-S2
F0/3-4
2043
M-S3
F0/24
F0/22-23
F0/24
F0/22-23
PC-30
PC-23
PC-28
PC-32
F0/1
2044
B2-S1
F0/1
2045
B1-S1
F0/24
F0/22-23
F0/24
F0/22-23
PC-31
PC-24
PC-29
PC-25

Main Office


Clients have Dynamic Addresses
To BCIT Network
BCIT
DatCN-Link-123
F0/2
Classroom Switch
F0/3
F0/13-14
S0/1/1 to Branch 2
172.25.3.249/30
S0/2/1 to Branch 1
172.25.3.253/30
2038
M-R1
F0/0
F0/1
F0/1 to Data Center
192.168.123.2/24
SVI VLAN 1: 172.25.3.30/27
MSW122
Dell Server
PC-27
Room 122
F0/23 PCI NIC Access VLAN 503
F0/22 Built-in Access VLAN 501
2041
M-S1
SVI VLAN 1: 172.25.3.1/27
F0/1-2
Etherchannel
F0/5-6
2042
M-S2
SVI VLAN 1: 172.25.3.2/27
F0/3-4
F0/24
2043
M-S3
SVI VLAN 1: 172.25.3.3/27
F0/23 PCI NIC Access VLAN 503
F0/22 Built-in Access VLAN 502
F0/22-23
PC-28
VM Switch
AD DC BAK
172.25.3.98/27
WDS
172.25.3.99/27
PC-32
VM Switch
MARKETING VLAN 502
IT VLAN 503
PC-30
VM Switch
AD DC
172.25.3.97/27
DFS Server
172.25.3.100/27
PC-23
VM Switch
ENGINEERING VLAN 501
IT VLAN 503

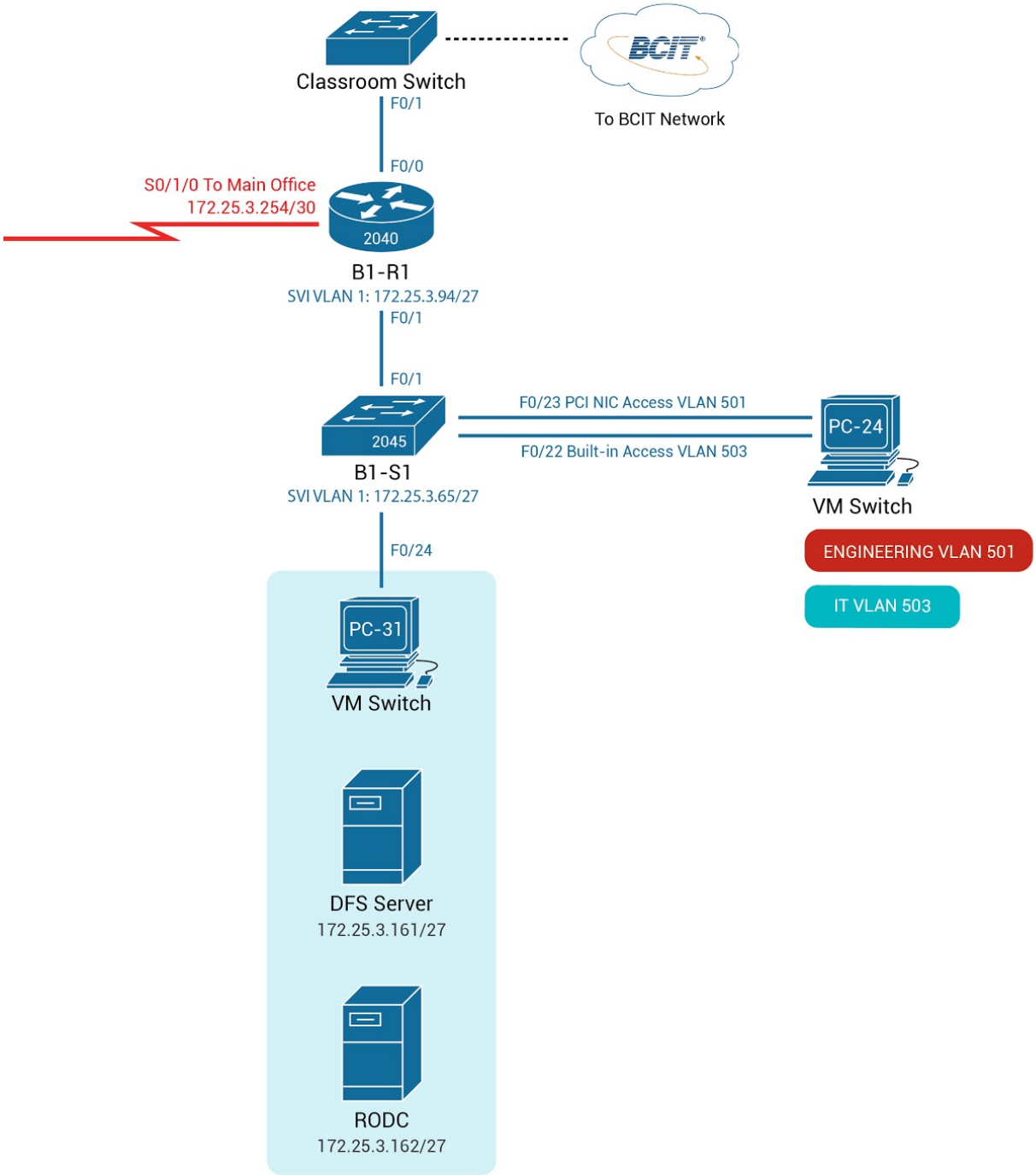
Branch 2 Office

Clients have Dynamic Addresses



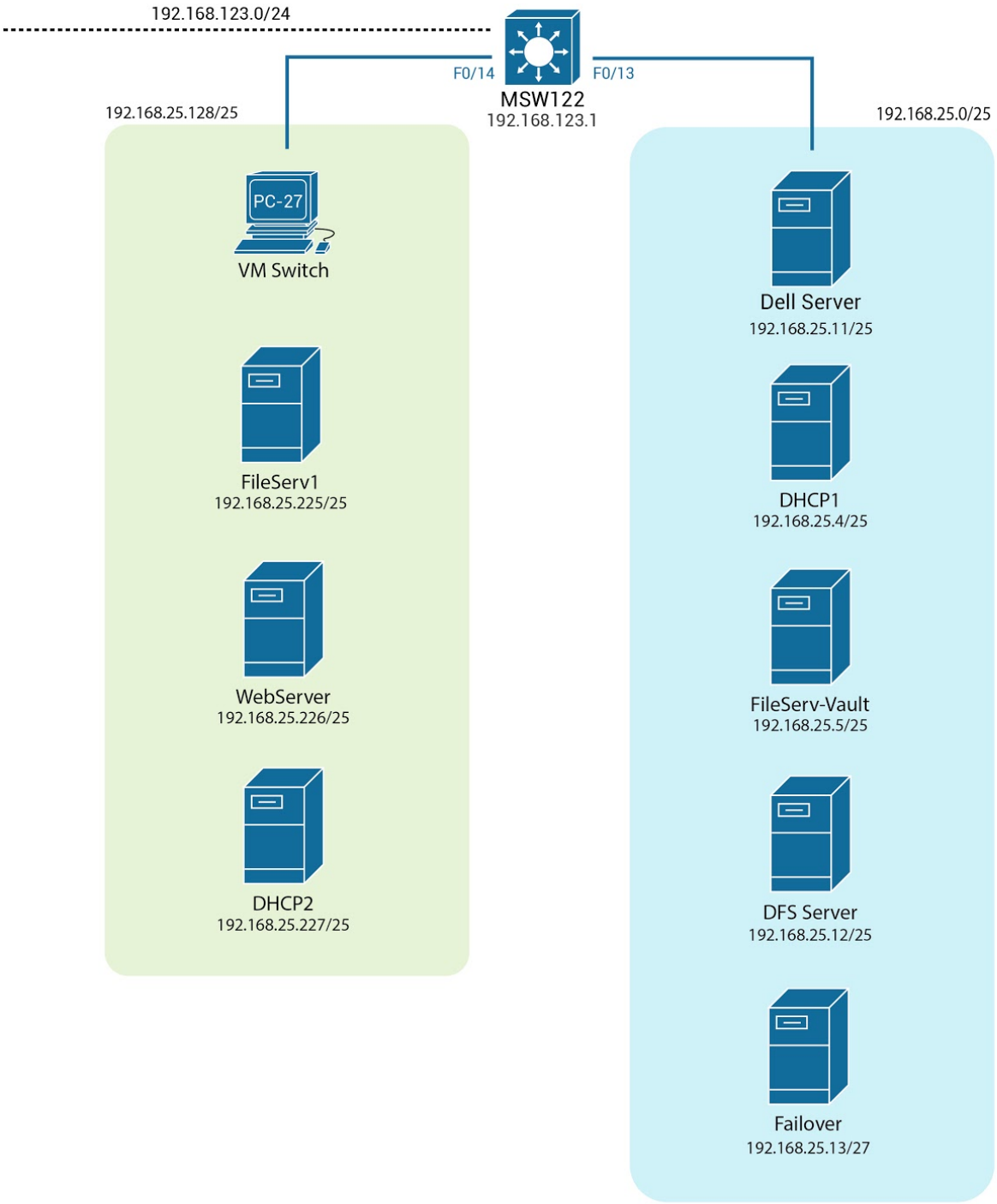
Branch 1 Office

Clients have Dynamic Addresses



Data Center (Room 122)

Clients have Dynamic Addresses



Hardware Setup

General Workflow

1. Raid 1E for fault tolerance provides server with physical fault tolerance, the server will be used for the primary dfs server
2. Drives in the PC and workstation server were picked based on their age
3. CISCO routers and switches were chosen based on cost, availability and team's familiarity
4. Backuping of machines via periodically transfering VM's from hot storage to cold storage

Networking Devices

Primary reasons for choosing Cisco network devices was availability and cost. Forwarding rate is not a concern due to the limited amount of hosts available. Furthermore, the team is most familiar with IOS and its operations.

In terms of cost, used managed 24 port cisco 2950 switches employed in our topology cost roughly $30 on ebay.[1] This is in contrast to listed price of CA$5,449.36 for 2960s[2] with the same number of ports. Even at discount, 2960s cost $1,005.03 per switch. For comparison, each port on the 2950s cost $1.25 whereas each port on the 2960 cost $41.87. As such, the low cost of these used switches makes scaling the number of hosts more cost effective. Brand new 2960s are prohibitively expensive for the initial setup. Replacing these devices will also be very costly.

Routers we plan to deploy are 2801s. While our particular routers are EOL, they are quite cheap. Refurbished 2801s cost roughly as $150.[3] Similar ISR Cisco routers cost $1,038.98. Replacing 2801s, if there are failures, will be cheap. Conversely, because they are EOL, they will be increasingly rare. Nonetheless, the 2801s will start us off at a low cost and shifting to the 4000 series should not be too difficult should the need arises.

---

[1] https://www.ebay.com/sch/Computer-Networking-Switches-/51268/i.html?_nkw=cisco+2950&_udlo=20&_udhi=30

[2] http://www.router-switch.com/ws-c2960s-24td-l-p-1511.html

[3] https://www.ebay.com/p/Cisco-2801-2-Port-10-100-Wired-Router-CISCO2801-V-K9/108865008

Because we are using managed cisco switches with CLI configurations, changing to newer or more powerful Cisco switches would not be difficult. Established configurations can be easily ported to newer cisco switches and routers with minor modifications to comply with newer versions of IOS. Some downsides would be that because we are using only cisco devices, we can potentially find ourselves locked into the ecosystem. However, this should not pose a problem provided cisco maintains its quality into the future.

In terms of familiarity, most of the current IT department have been trained to use cisco hardware. Changing to different products may introduce unnecessary administrative overhead. If the primary goal is to establish a working network as soon as possible, we should stick to cisco for the time being.

Exact setup will be described in the networking portion of this document.

Drives

Current implementation

Where we employ the 3.5 inch Drives were based mostly on size and date of manufacture. Because we are using used drives it was important for use to use newer drives for more important devices such as servers. As such, most of the smaller drives have been relegated for regular clients use. Current usage of drives can be found in the Hardware section of the appendix.

Scaling for the future

Costs of drives have gone down significantly which makes drive expansion quite affordable. Additional 3.5 inch hard drives can be purchased for as low as 50 dollars from Best Buy at larger capacities like 1TB.[4] From amazon, sas drives can be found as low as 80 dollars for 1TB drives on amazon.[5] If necessary, scaling additional drives on the ESXI Dell Server should not be an issue. However, speed is an issue.

The other options would be ssds. While they use less power, and much faster, they cannot compete with 3.5 inch drives in terms of GB per dollar. [6]

---

[4] https://www.amazon.ca/s/ref=nb_sb_noss_2?url=search-alias%3Daps&field-keywords=hdd

[5] https://www.amazon.com/9W5WV-ENTERPRISE-ST91000640SS-Compatible-PowerVault/dp/B011MAMVEE/ref=pd_lpo_vtph_147_bs_t_1?_encoding=UTF8&psc=1&refRID=8PXBQ41ZVZRZNJFF0WS9

[6] http://www.storagereview.com/ssd_vs_hdd

In terms of power, according to building computers.net, 2.5 inch SSDs typically use between 0.6 to 2.8Ws of power.[7] This can translate to long term cost savings. Based on BC Hydro small general commercial rates[8], at $0.1173 per kWh and assuming the maximum power usage of an ssd, continuous use for a year equates to $3 per year. In comparison, 3.5inch HDD typically use 6.5 to 9W. Even if we were to use the lowest probable power use of HDD, it would cost $6.96 per year at the same rate. This is double the cost of SSD.

In terms of speed, typical sequential reads and writes of HDD's hover around 100mb/s[9]. This is in contrast to typical sequential read and writes speeds of 500mb/s on SSDs. Therefore SSD's speed is much higher. However the cost of GB per dollar is heavily in favor of HDD. As previously mentioned, 1TB drives cost as low as 49.99. SSD's that match this capacity cost roughly 300 dollars. [10] This is 6 times the initial cost. Even factoring the power consumption, SSD do not recover from an economic perspective.

Ideally, the servers will continue to use conventional drives for maximum capacity, but the workstations could have smaller capacity drives. User's should be directed archive finished projects to the DFS namespace after they are done with them in order to preserve space.

Computers

Current implementation

The Workstations are Dell Precision Tower 3000 workstations equipped with Xeon E3, 16GB DDR3 RAM and equipped with a variety of drives via hard drive toaster, which costs $1299 with the current configuration.[11] This does not include the hard drives or OS. The planned 14 clients require individual licenses. Currently we have a maximum of 9 3.5 hard drives and 4 SAS 33.3GB hard drives were available for testing purposes. As such all demonstration clients and servers will be running in VMs. More drives can be acquired as the company grows.

We also have a Dell Server with a Xeon processor and 8GB of ram. While much slower than our Xeon workstation, it has the capacity for up to 9 SAS drives and built in raid capabilities. Only 4 drives were used in a RAID 1E configuration for a total of 67GB.

---

[7] http://www.buildcomputers.net/power-consumption-of-pc-components.html
[8] https://app.bchydro.com/accounts-billing/rates-energy-use/electricity-rates/business-rates.html
[9] https://photographylife.com/nvme-vs-ssd-vs-hdd-performance
[10] https://www.amazon.ca/Crucial-MX500-NAND-SATA-Internal/dp/B077SF8KMG/ref=sr_1_16?ie=UTF8&qid=1529027736&sr=8-16&keywords=1TB
[11] Price based on dell configuration website for Dell precision T3362 with equivalent specs. Volume pricing may differ.

Management of servers will be done remotely via Server Manager on Clients for Microsoft NOS or via vmware workstation for linux. Windows Servers could also be managed via vmware if GUI is required.

For the purposes of this demo, each of the vms will be using one of the two NICS. Each NIC will be connected to a port of a switch that is assigned to a particular VLAN and will be assigned an IP based on the addressing table found here.

Scaling for the future

Non-Engineering or IT roles may not require require xeon processors. We could use cheaper office machines such as Dell Inspiron desktops. Base configurations cost $499 to $699. A middle ground configuration at $599 has a pentium silver processor with 8GB of ram with a 3.5 1TB drive. [12] These should be sufficient for basic documents and are roughly half the cost of the Xeon workstations/servers.

Engineering PC's may also require additional GPU power for more complex tasks as CAD. Using Nvidia Quadro K1200 which retail at $299 should be a keep prices low while providing low level acceleration for more demanding tasks.

Used dell servers can be purchased for a low cost as well. For example, a used R710 with 2 E5540 QC Xeons @ 2.53 GHZ, 72 GB of RAM and 4x145 GB drives with additional slots for 4 more drives cost $580 after shipping.[13] If additional storage or more powerful servers are in need, this could be a more affordable alternative. Newer R730s start from $3,539.[14] While these offer significantly more scalability, they do cost more. If the goal is short term expandability, than the used R710 would be a better route. Long term, the R730s will provide better performance and drive space.

Data Recovery Plan

Because most of our important server machines are running on virtual machines, backup, migration and even upgrading these machines should not be difficult. While we have yet to

[12] https://www.dell.com/en-ca/shop/desktops/inspiron-small-desktop/spd/inspiron-3472-desktop

[13] https://www.ebay.ca/itm/16-Logical-Cores-DELL-R710-Server-2x-E5540-QC-Xeon-2-53GHz-72GB-RAM-4x146Gb/322931286218?hash=item4b303460ca:g:vHsAAOSwnTdaK~R0

[14] https://www.dell.com/en-ca/work/shop/povw/poweredge-r730

implement this due to hardware limitations, we will transfer important VMs such as the AD controllers, and DFS to offline storage once it becomes available. Virtual machine snapshots will also be made before significant changes, updates and on a weekly basis manually. If things do break, simply reverting back to a previous snapshot will resolve the issue.

For backing up configurations our networking devices, they will be backed via vstftp via linux web server into the samba share in the IT folder. Documents in the namespace will be replicated periodically based on the schedule. It will also be moved to cold storage solution at a later date.

Issues

Network Devices

One issue that we ran into when installing the routers was that they did not fit the rack. This was because the rack was mounted too close to the wall. As such we could not secure them properly without putting undue pressure on the power cables.

Another issue was that some of the ethernet jacks were not legible, likely due to continuous use. Simply noting which port went where resolved the issue. See topology and or appendix for exact ports that were employed.

ESXI

Another Issue we ran into was a driver issue for ESXI 6.0 and external hard drive enclosures. Because of the limited number of SAS drives for the Dell Server and the need for RAID 1, we opted to install ESXI on the a dell workstation. With RAID 1E and 33GB drives, we had a maximum drive size of roughly 67GB. For reference, vmware's recommendation for the virtual drive size for Windows Server 2016 is 40GB.

However, large file transfers between a client and the ESXI server ultimately failed. Attempts to install VMS remotely also resulted in failures. Upon refreshing the management page resulted in drive pool shown empty. While we could not determine the exact issue, it is likely an issue with a external hard drive enclosures driver included in our particular version of ESXI. We eventually just installed ESXI on the Dell server to avoid the issues all together. However, this requires us to ration the limited capacity more carefully.

VMs on the dell workstations are run in vmware workstation for interoperability with the ESXI server. Migration and movement of vhds should not be an issue.

Microsoft

General Workflow

1. 2 domain controllers in Main Office, one for backup
2. Created two RODC's in Branch 1 and Branch 2, linked servers to domain in their own respective sites
3. Basic GPO's for passwords, default application installation, and automatically mapped drives
4. The mapped drive will use DFS replication for increased uptime
5. Configured WDS with Windows 10 Enterprise to push out Operating system to Clients
6. Assign and configure each vm's nic to point to their associated VLAN

Client Operating System: Windows 10 Enterprise

All clients are installed with Windows 10 Enterprise. This version of windows has most of the important features and allows more flexibility than other versions of Windows 10.

Network Operating System: Windows Server 2016

We will be deploying Windows Server 2016 as our primary network operating system. While most of the team members are more familiar with 2012R2, 2012R2 has started extended maintenance and will be EOL by 2023. Most of the currently planned roles and features we are implementing currently is still available in 2016. Using 2016 also allows us to use any new features microsoft may choose to add to 2016. Conversely, future updates may break features of Windows Servers we are currently implementing. However, we believe the potential for new powerful features outweighs the impending EOL of 2012R2. Migration might also prove increasingly difficult as the 2016 diverges further from 2012R2 original feature set. This is especially so since windows server 2019 is around the corner.[15]

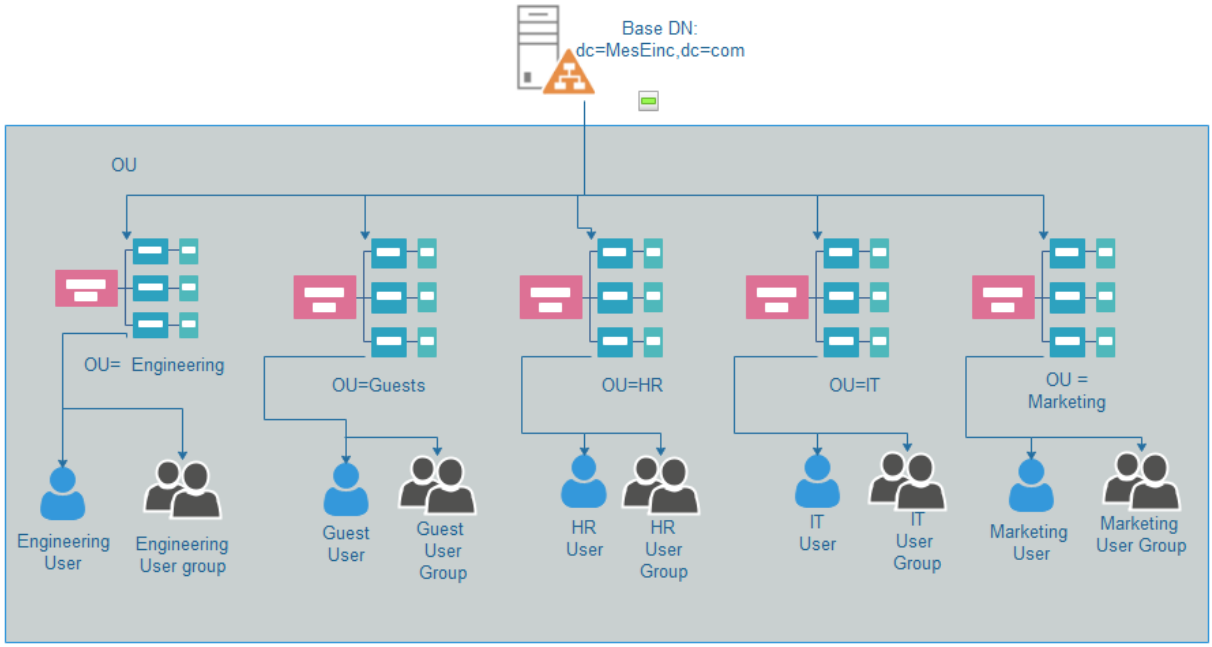
Testing and demo will be using 2016 data center. If implemented permanently we will use standard for cost savings. 2016 Data Center costs $6000~ USD versus $882 for standard[16].The only notable feature is Storage Replica which does synchronization block level. While this feature allows for syncing of open files, the DFS meets our needs currently for backups.

---

[15] https://cloudblogs.microsoft.com/windowsserver/2018/03/20/introducing-windows-server-2019-now-available-in-preview/

[16] https://www.microsoft.com/en-ca/cloud-platform/windows-server-pricing

OU Structure

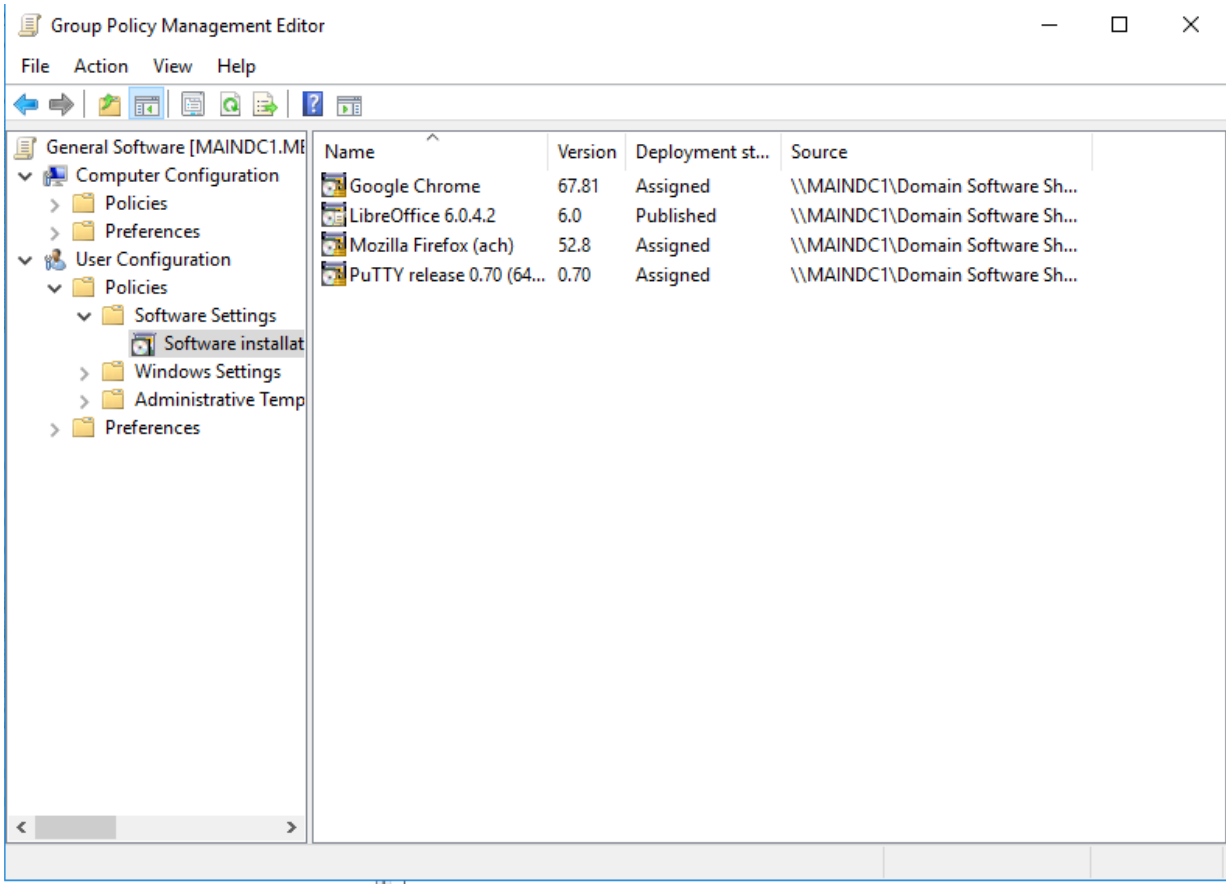


Group Policy Objects

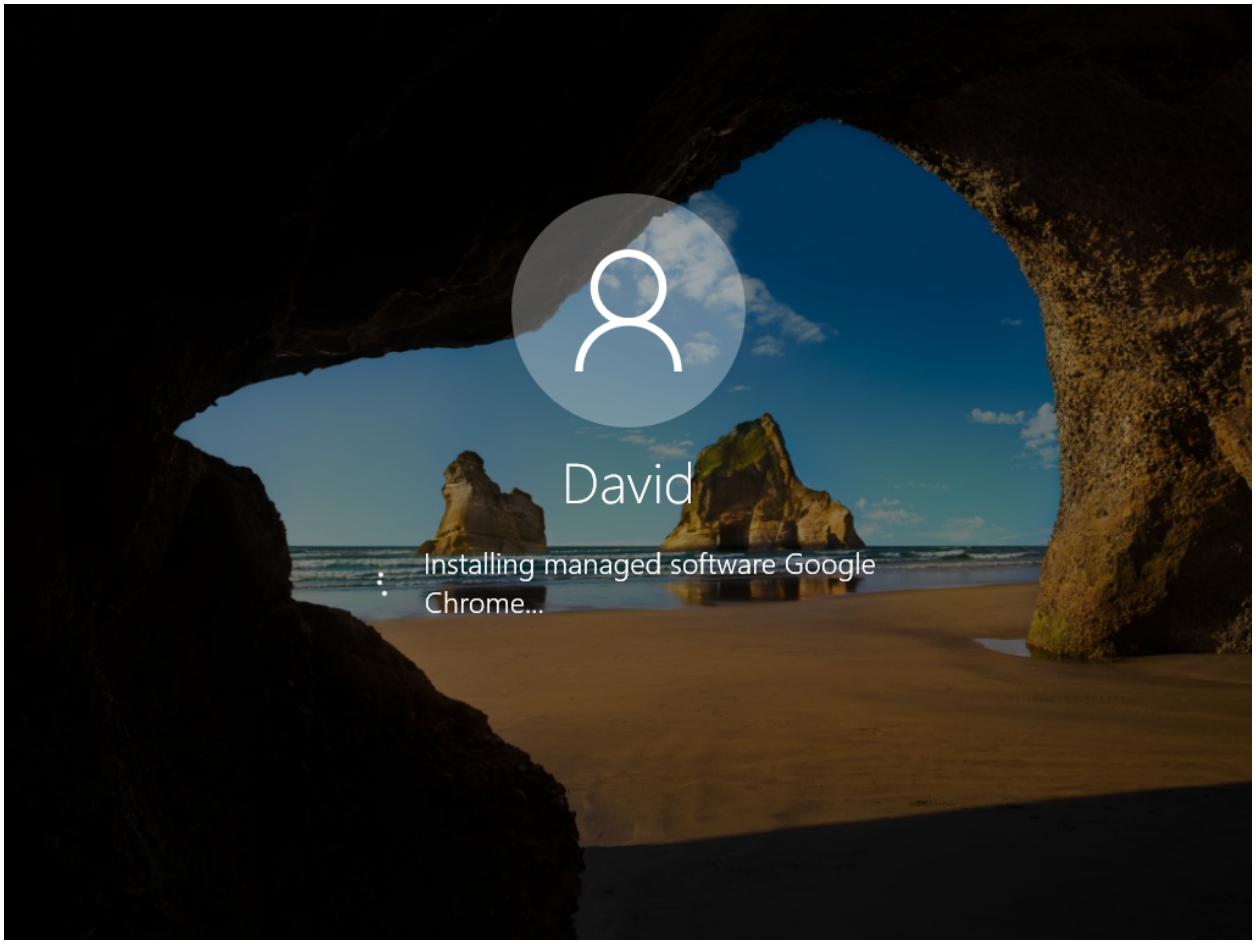
General

Software Installation GPO

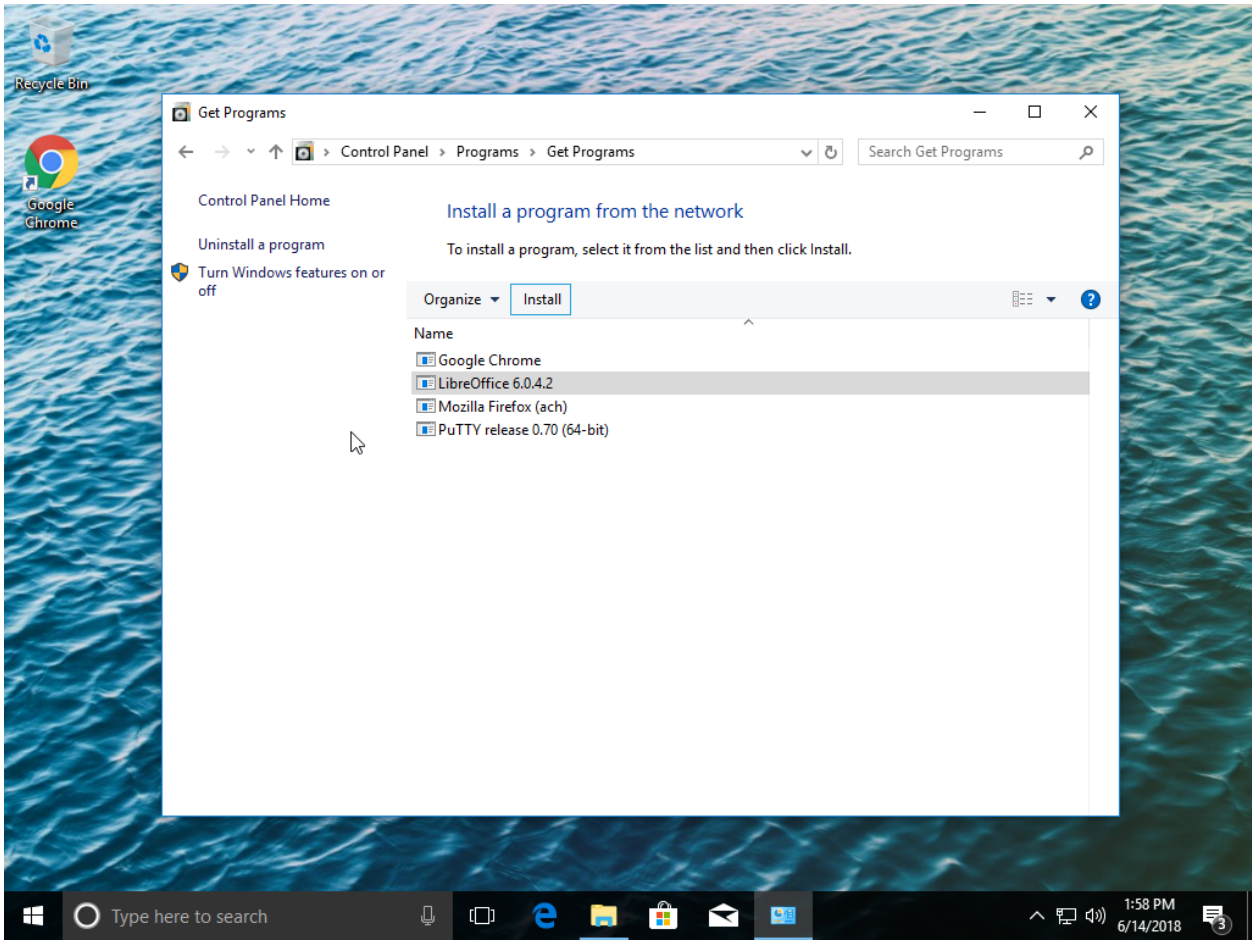
We set this GPO to automatically install Software to client Workstation to decrease unnecessary administrative overhead. Applications that are being pushed to the users should reflect the needs of the user. For example, the IT group will have PuTTY pushed out automatically. The engineering team will have sketchup pushed out automatically. More general applications such as chrome browser and Libreoffice will be published in a more general software installation GPO.



Software currently being deployed.



Google Chrome being installed when user logs in



LibreOffice must be installed from control panel

Libreoffice Issues

We were unable to find an msi installer for MS Office 2016. We resorted to libre office which does have a msi installer. MSI installer is required for application publishing to work. While Libreoffice would allow easy publishing/assignment of the application, there are some issues The most glaring issue with libreoffice is compatibility with MS formatted documents. While simple documents tend to translate well, complicated documents with special formatting created in MS Office tend not to render properly in Libreoffice. This could also be avoided entirely if we used G-SUITE but that means placing a huge amount of trust in Google to keep our information private. Cost benefit-analysis may be necessary.

While we wanted to have seamless installations for libreoffice by publishing via computer configuration, we had to deploy it via the user instead. This requires the user to install it via the control panel.

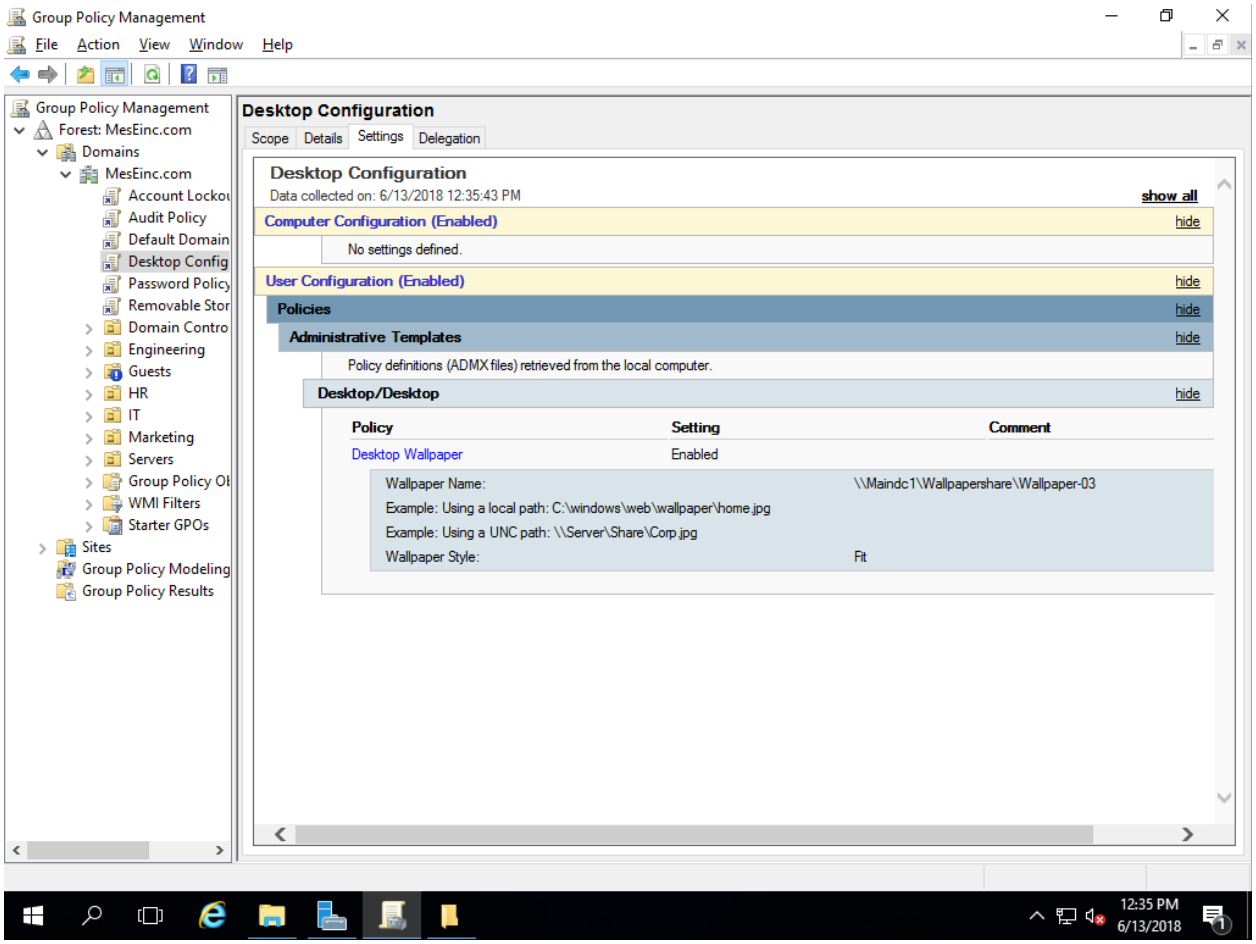
Another issue with the libreoffice install was that the package contained too many languages which prevented us from adding the file to the GPO. We then had to remove those languages from the package. Using an application called SuperOrca, we will remove those languages with the exception of English. The detailed process can be found in the appendix here.

Google Chrome ADM GPO

Added to the Chrome for increase security and easier administration this GPO sets defined options for our current Web browser this lets us control what can be done reducing the risk of problems for Workstations. As of June 14th, 2018, has not been implemented.

Desktop Wallpaper + Logoff Script GPO

We added a GPO to automatically push out a set wallpaper for all of our company's workstations, To do this we had to share the intended picture and add in the share path to the GPO.



Wallpaper Configuration.

Issues

One of the issues for this GPO is that when using Windows 10 it caches the last known wallpaper in to its own hard drive thus making it impossible to automatically update whenever the administrator wanted to change the wallpaper. What we had to do was add a logoff script GPO

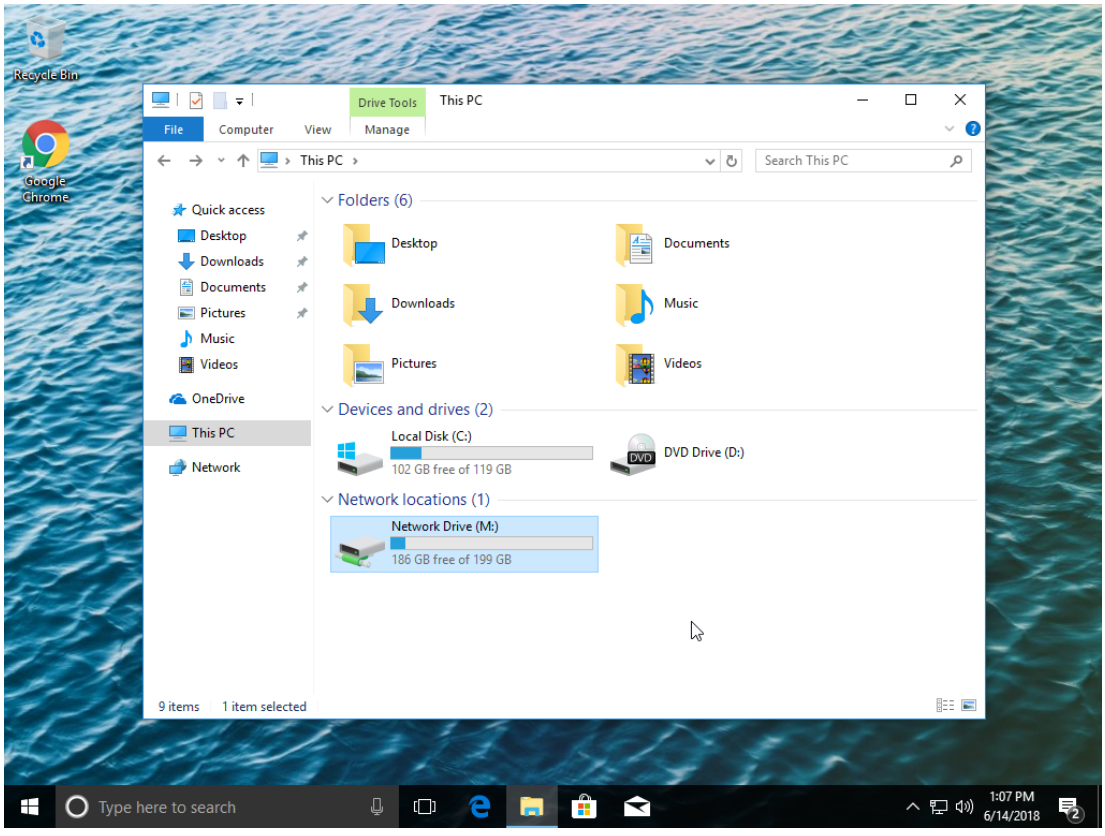
In order to resolve this, we added an additional GPO to automate the process of constantly deleting the cached image to allow the Desktop wallpaper to stay updated every time.

The script is as follows:

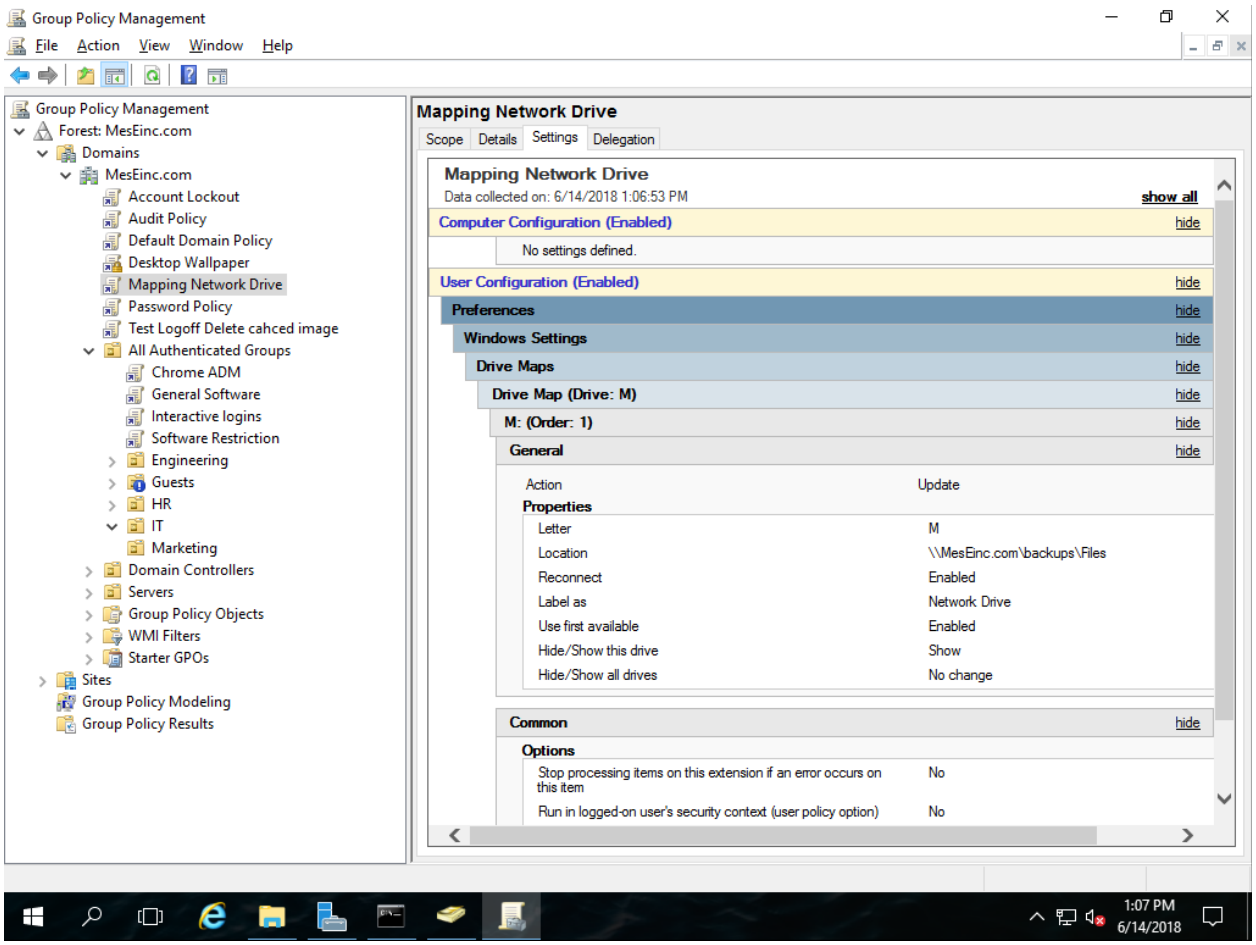
del %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Themes\

Drive Mapping GPO

This GPO was set to allow all domain joined user and computers to use one single domain based drive, we added several different folders inside based on each group and assigned the needed permissions to only allow the assigned group to access and edit. Thus creating a singular and organized organization work space.



Mapped drive via GPO.



GPO settings for mapped drive deployment

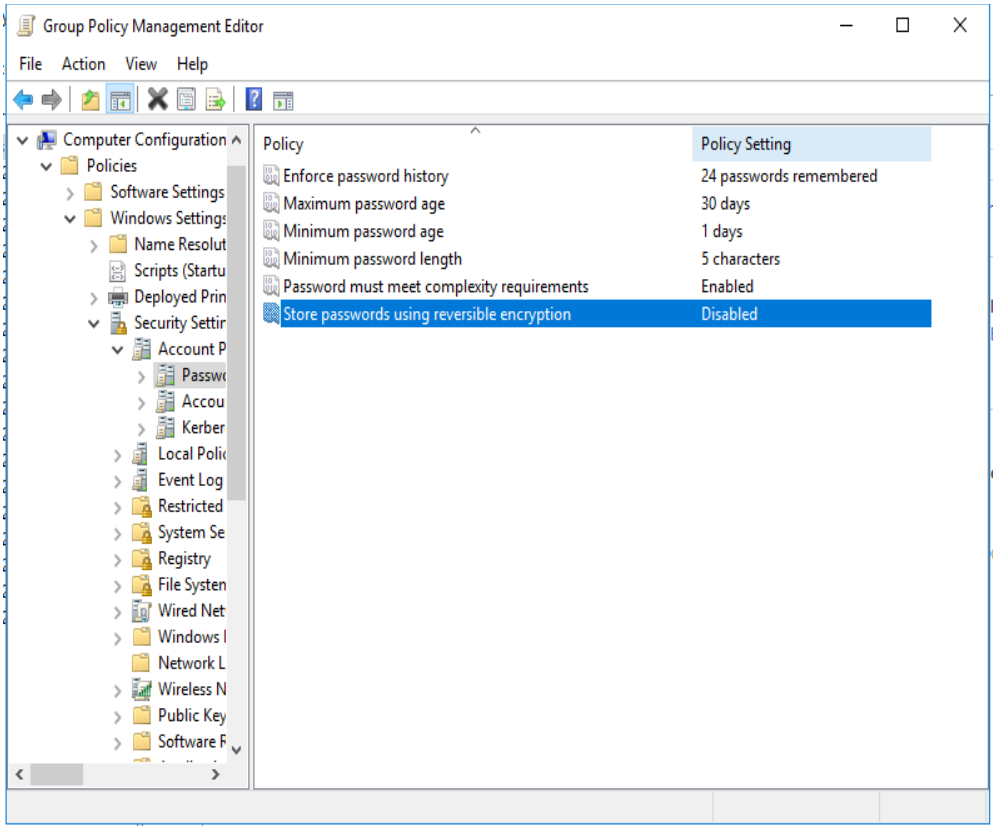
Security

Password Policy GPO

We are using this GPO to enforce set specifications for passwords to increase account security at this moment we have several policies enabled such as -

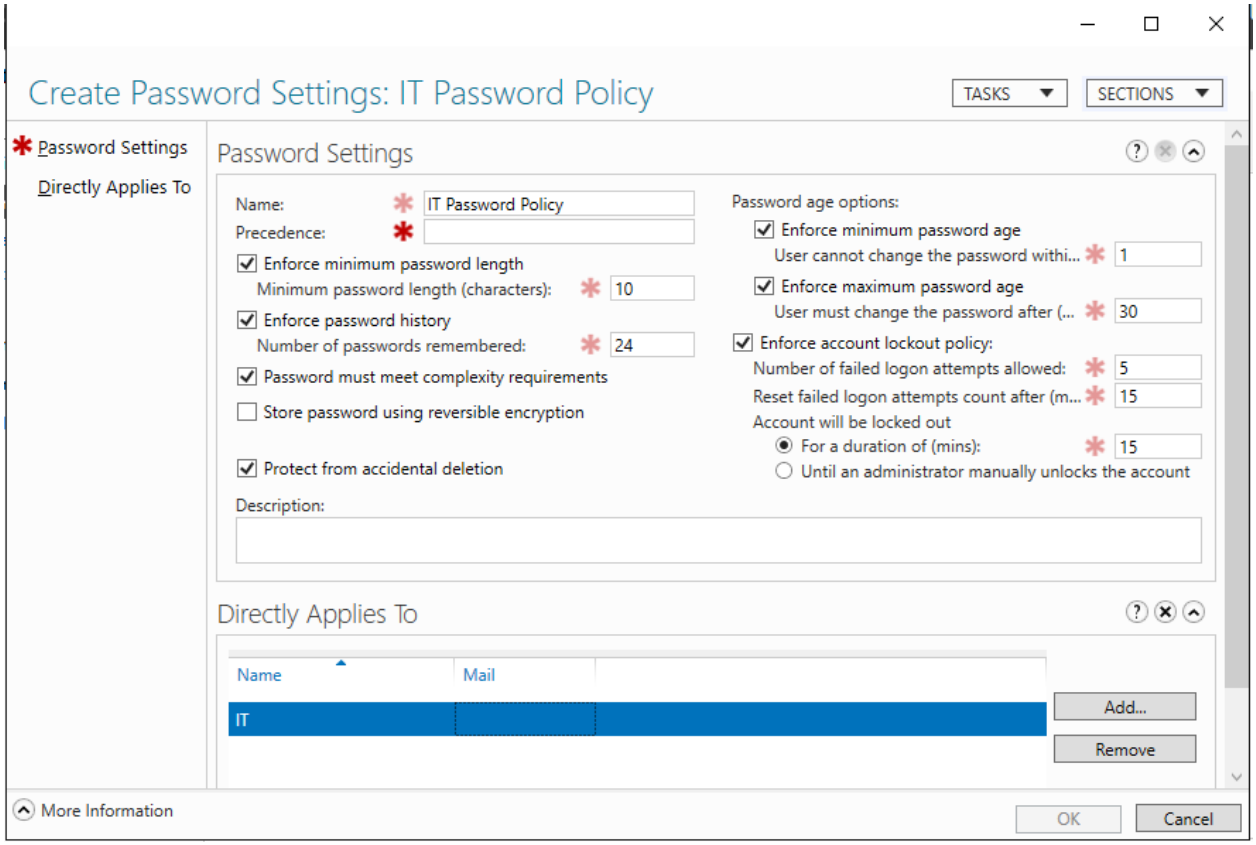
- Enforce Password History - 24 (So you must use at least 24 different passwords)
- Maximum Password Age - 30 (Max amount of days before you have to change your password)
- Minimum Password Age - 1 (Minimum amount of days before your allowed to change your password)
- Minimum Password Length - 5 (Passwords must have a minimum of 5 characters)
- Password Complexity - Enabled (Passwords must meet the specifications before being set)

- Store passwords using reversible encryption - Disabled (Do not allow passwords to be decrypted)



Computer Password Policy GPO (Group Policy Object)

Because the IT department has a significant amount of control over the computer systems, their password policies will be more stringent. Password lengths will be increased to 10 which will make it considerably harder to crack. Their specific password policy will be applied via fine-grained password policy.



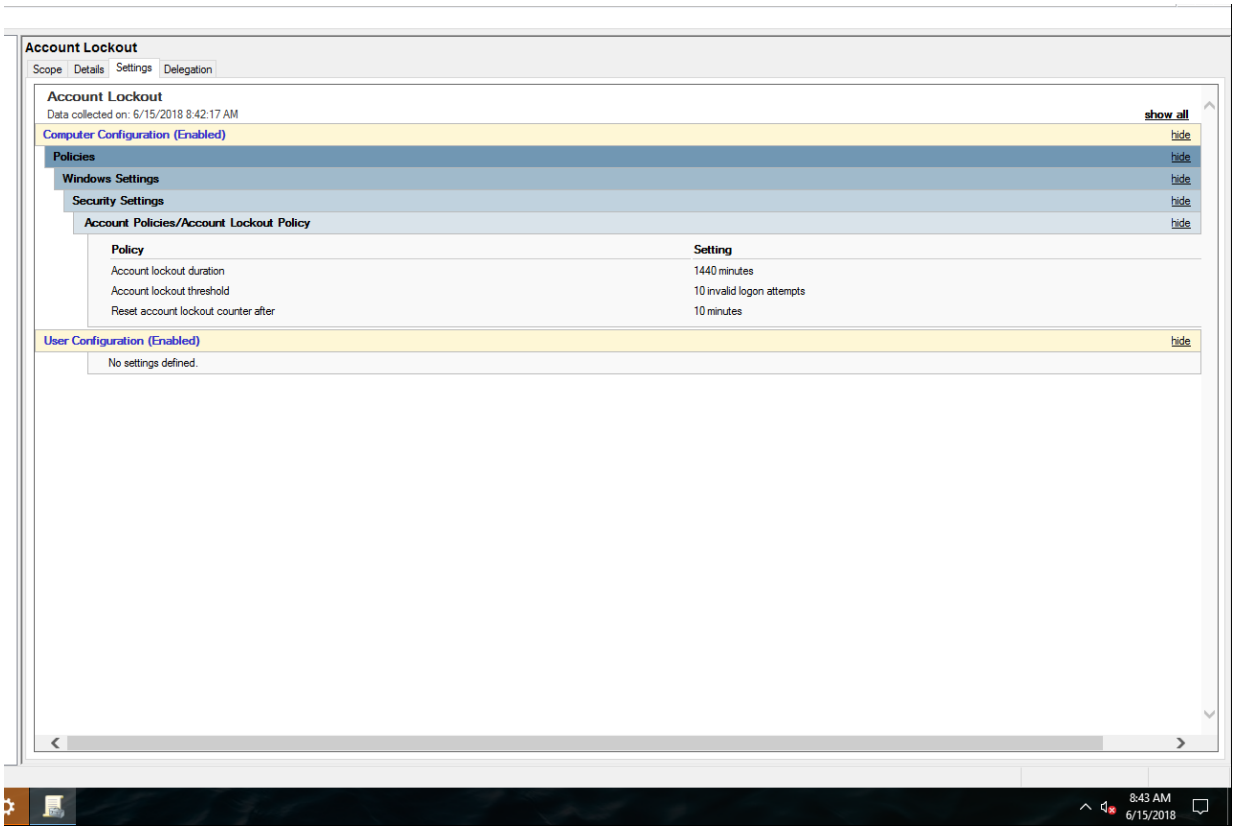
Fine Grained Policies for IT department.

Account Lockout Policy Security

According to Randy Smith's blog post[17], best practice for lockout policy would be the following:

- Account lockout duration: 1440 minutes
- Account lockout threshold: 10 invalid logon attempts
- Reset account lockout after: 0 minutes

[17] https://www.ultimatewindowssecurity.com/wiki/page.aspx?spid=AccountLockout



GPO for lockout policy

Effectively within 24 hours, 10 failed attempts lock a user out until manually unlocked by administrator.

Removable Storage and DVDs

Removable storage use will be restricted to IT. All work should be conducted within the offices until further notice. IT may require external devices to move software or install software until WDS/Application Publishing has been fully implemented. This has not been fully implemented.

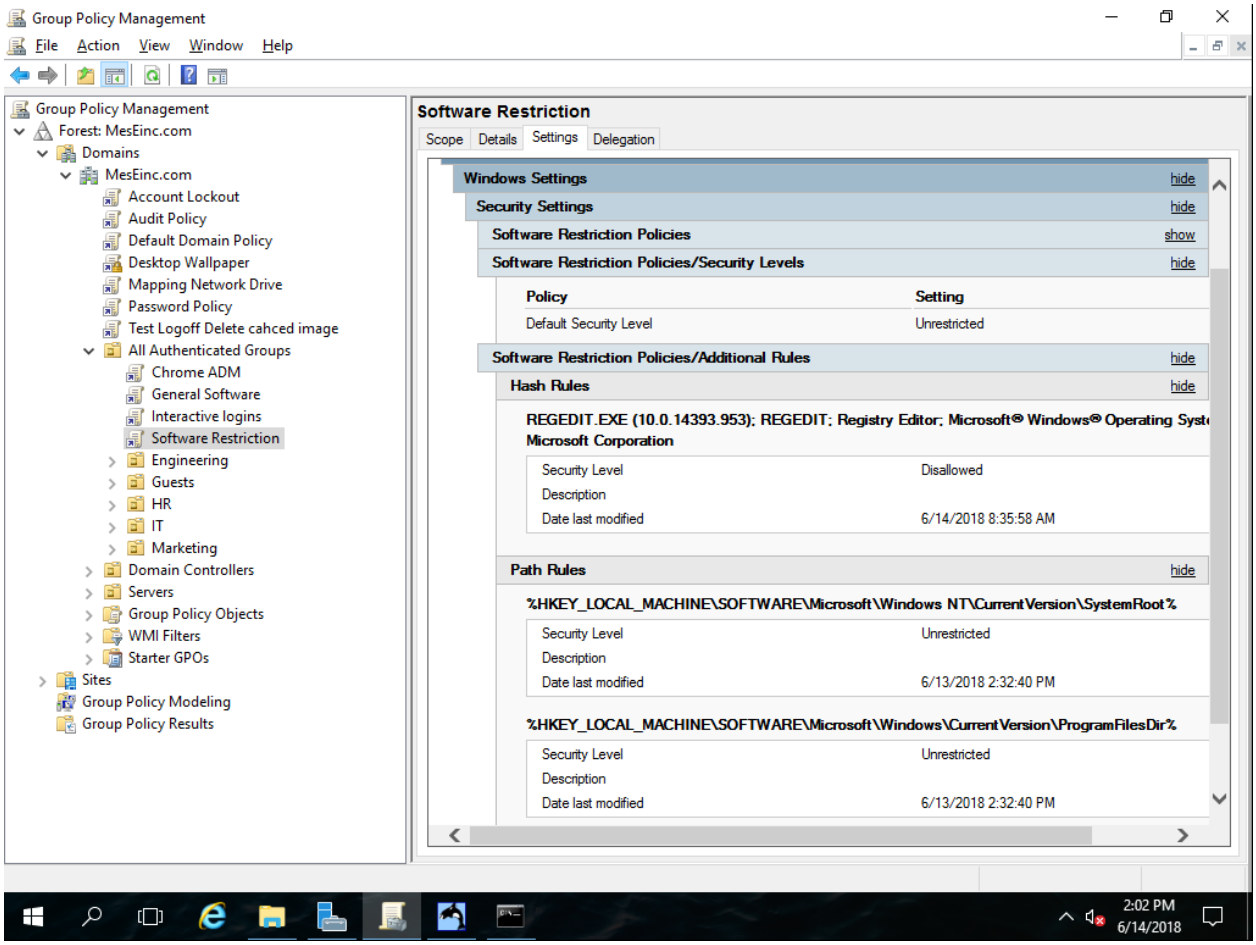
- CD and DVD: Deny read access: Enabled
- CD and DVD: Deny write access: Enabled
- Removable Disks: Deny read access: Enabled
- Removable Disks: Deny write access: Enabled
- (Added IT to the Delegation and **deny** *Apply group Policy*)

Recycle Bin

Objects recycle bin will be enabled just in case something is deleted by accident.

Software Restrictions

Software restrictions are enabled to prevent users from accessing applications, such as regedit, when they should not. Regedit is a very powerful tool but it can also be devastating in the wrong hands.

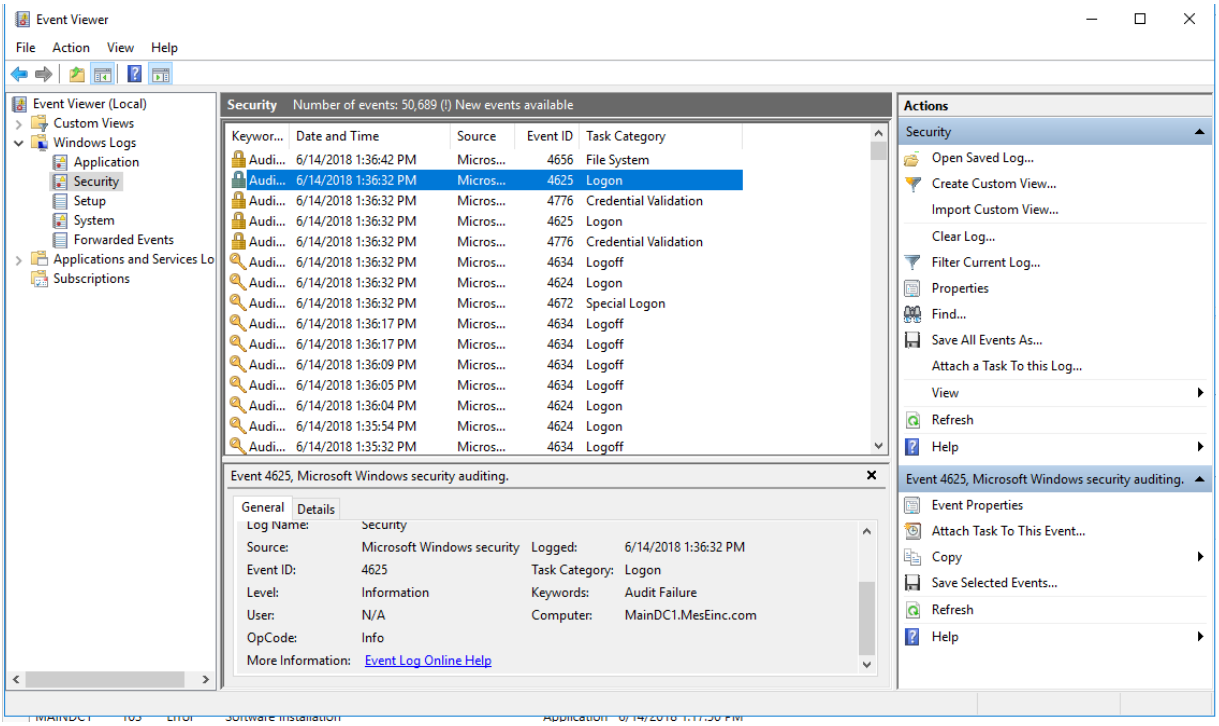


Software restrictions policies

Auditing

The following will be audited.

- Audit account logon events: Failure
- Audit object access: Failure



Viewing Audits in event viewer.

WDS

WDS will be used to for two reasons. First, it enables quick and easy deployment of clients and even servers. It also provides a means of customizing the time of images you are deploying. For example, we could include certain applications, drivers for certain groups of computers. We currently do not have any plans for customizing images. This is currently not implemented.

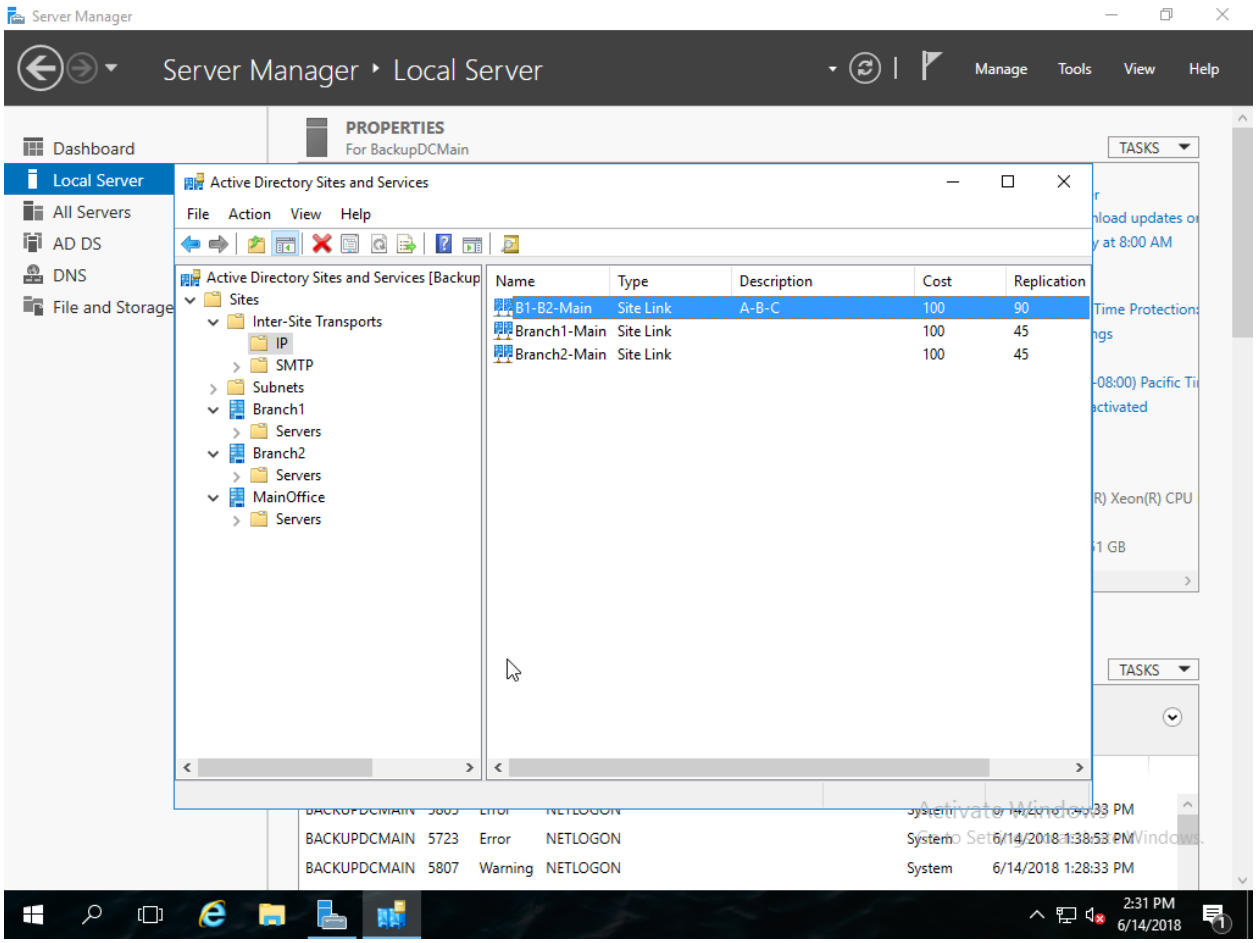
Issues

Due to some issues with DHCP, WDS is currently not working. Specifically, while the PXE boot was able to find acquire a DHCP addresses from the server, they were not able to find the image to boot. Some research yielded additional configuration that we could place into the dhcpd.conf of our DHCP servers. While likely to work, we were unable to figure out how the WDS shares its boot images. Other's mention that no additional configuration is necessary. This proves to be untrue as the lack of configuration resulted in PXE informing us that there was no image to boot.

Active Directory

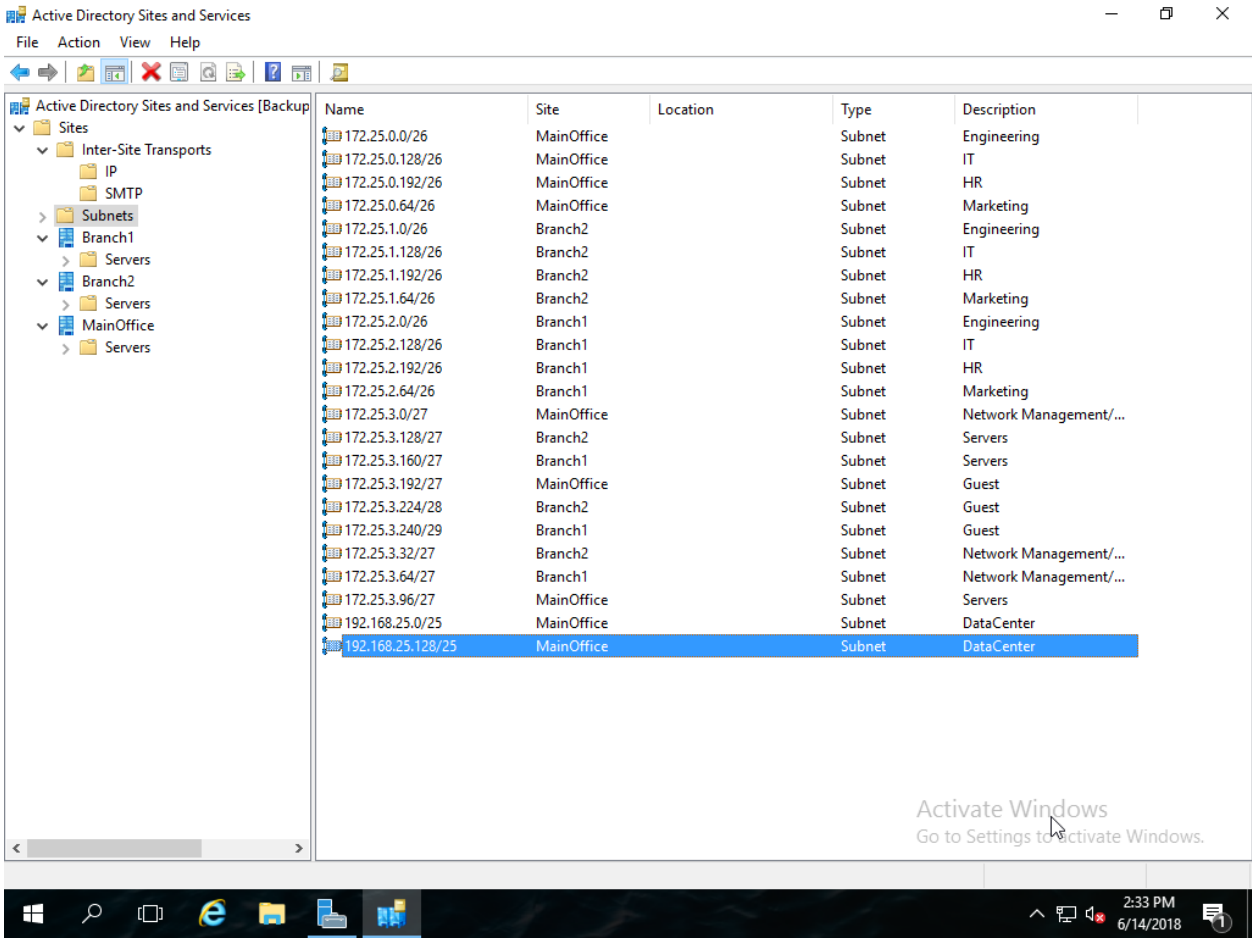
Sites

Site Connections



Site and their connections

There will be three sites. Main branch, branch 1 and branch 2. Each of the sites will have a distinct direct connection established to the main branch. These connections will be replicated at 45 minutes. All the sites will also be directly connected together with an additional connection. Each branch will contain and RODC. This connection will be replicated every 90 minutes. We feel that replication every 45 minutes will allow for timely replication without taking up too much bandwidth. The Main branch will contain two DCs. One will server as the primary DC and the second one will serve as the secondary DCs. Roles will be distributed amongst the two evenly. All DC will have a catalog and passwords will be cached on the sites.



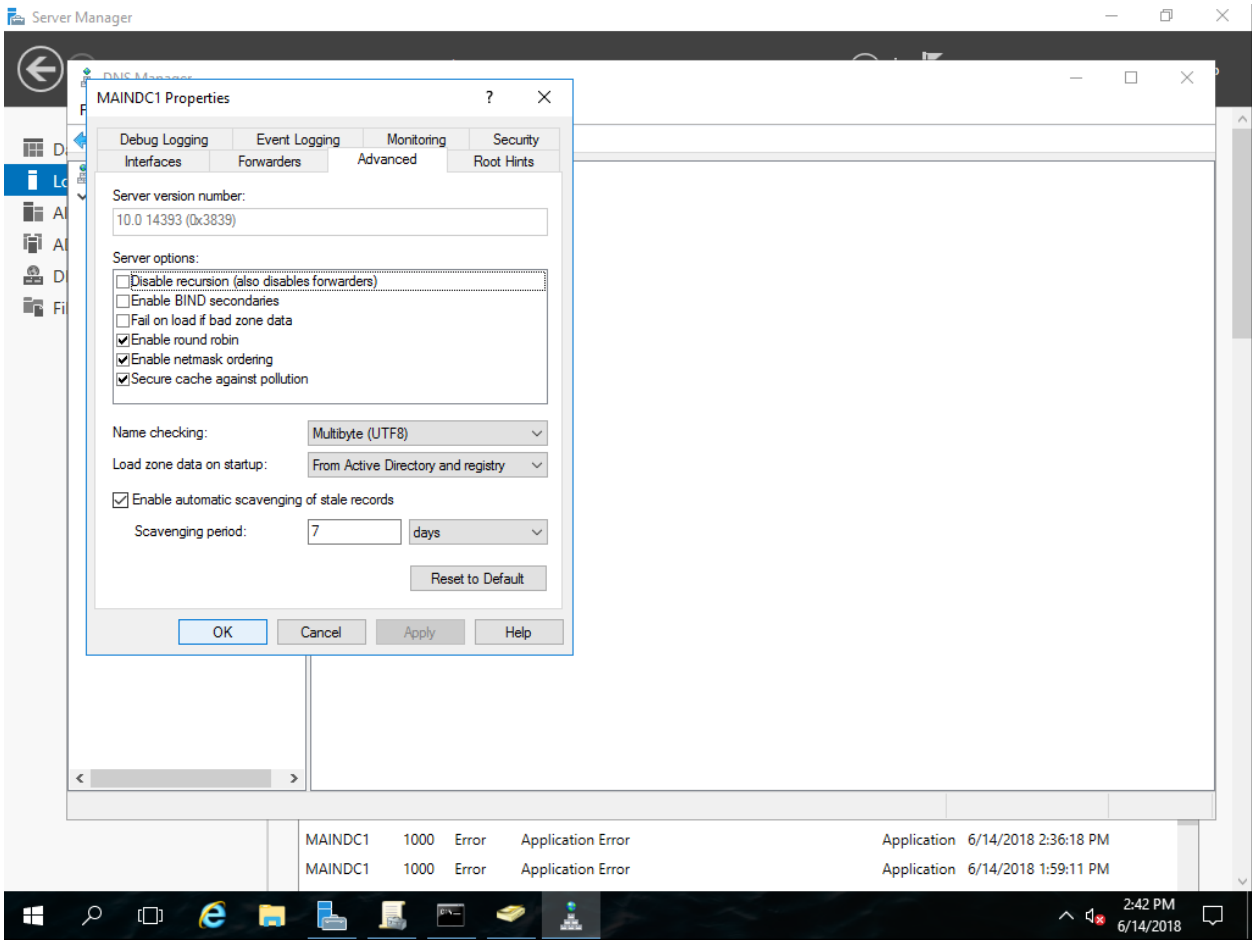
Subnets in sites

Subnets

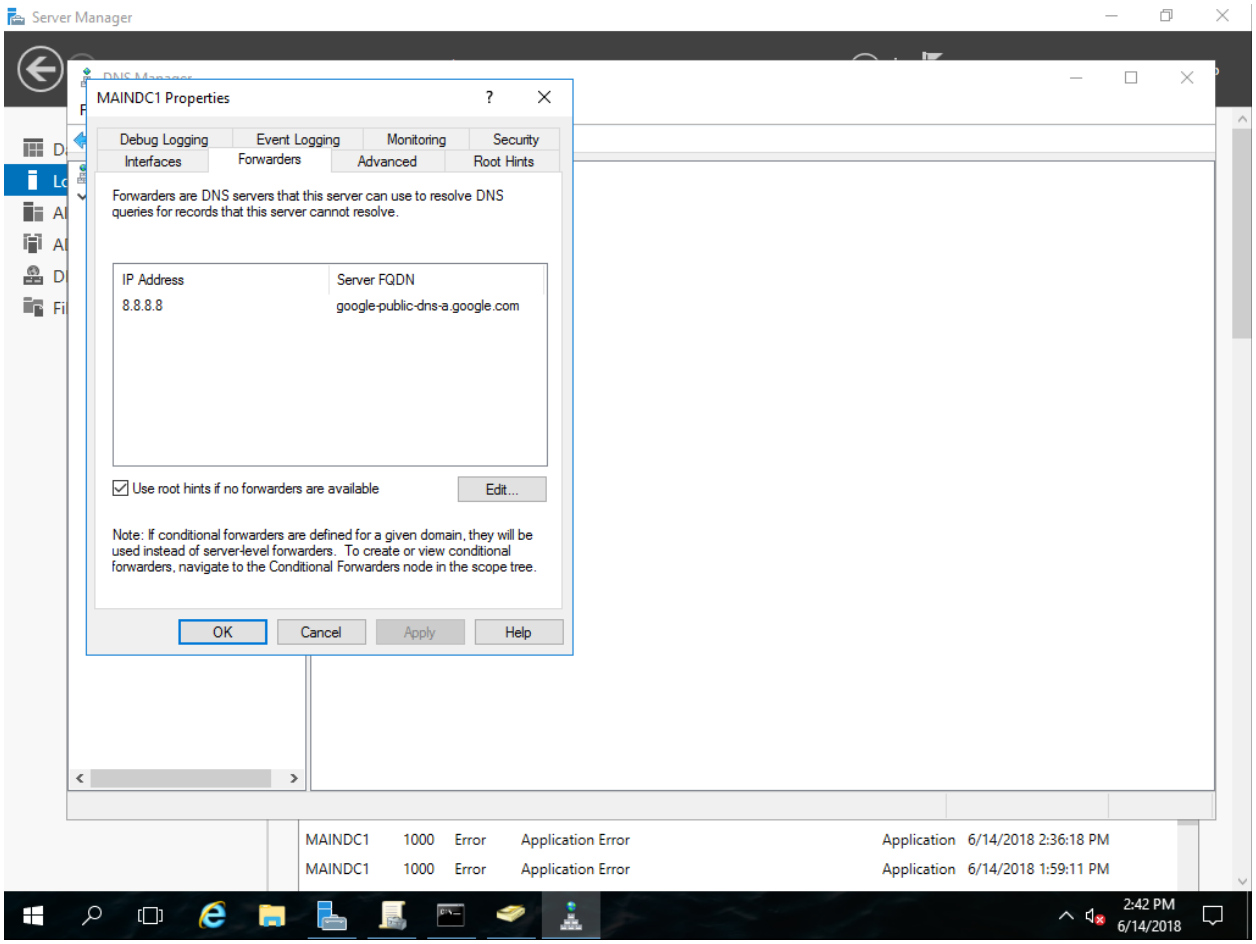
Subnets based on our addressing list and are assigned based to their appropriate sites.

DNS

The DNS role will be installed and synced on all domain controllers. Each of the sites will have a local DNS server. A failover will be assigned to them via DHCP server. Failover for the sites will be the primary domain controller. Main branch failover will be the backup domain controller. Linux servers will currently be manually inputted until SAMBA can be configured for them to join the domain. DNS forwarding is currently set to Google DNS. Additional DNS servers should be added in case Google's DNS goes down such as cloudflare.



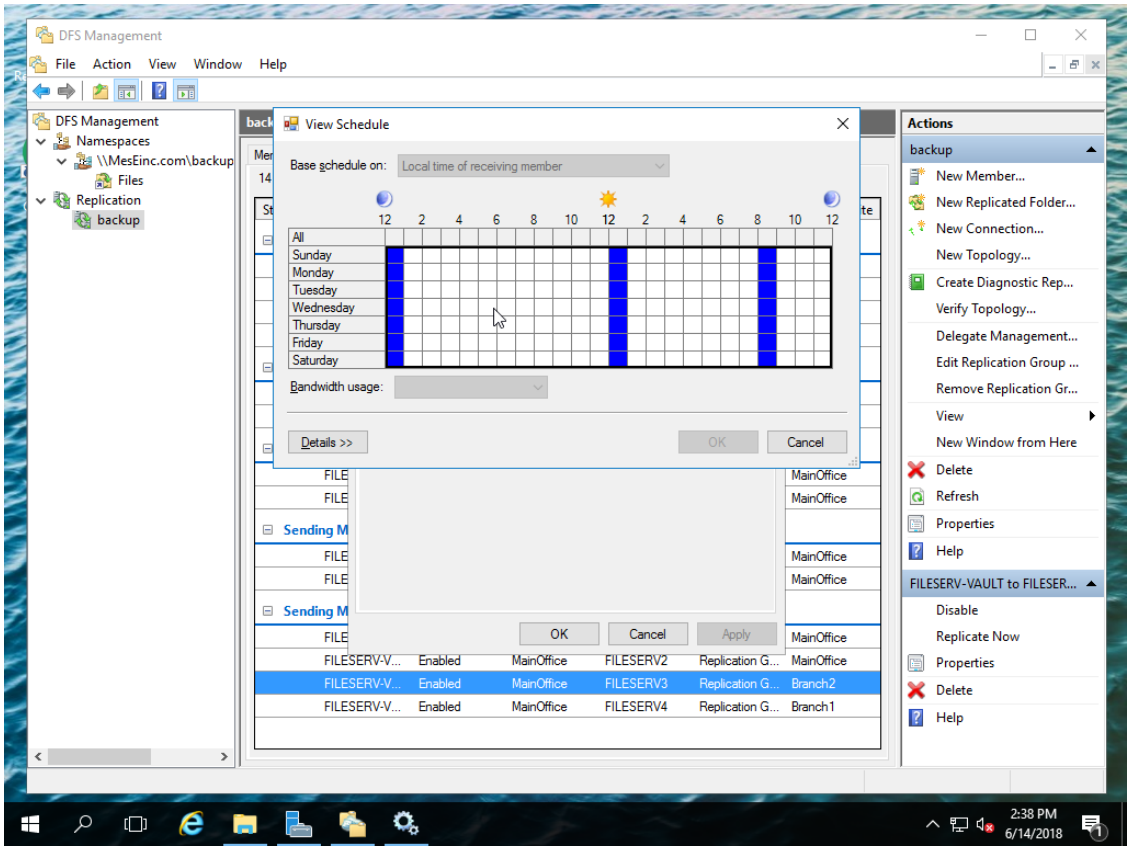
DNS scavenging enabled globally on the server



DNS forwarding enabled with 8.8.8.8. More will be added at a later date. This includes google's secondary DNS(8.8.4.4) and cloudflare (1.1.1.1)

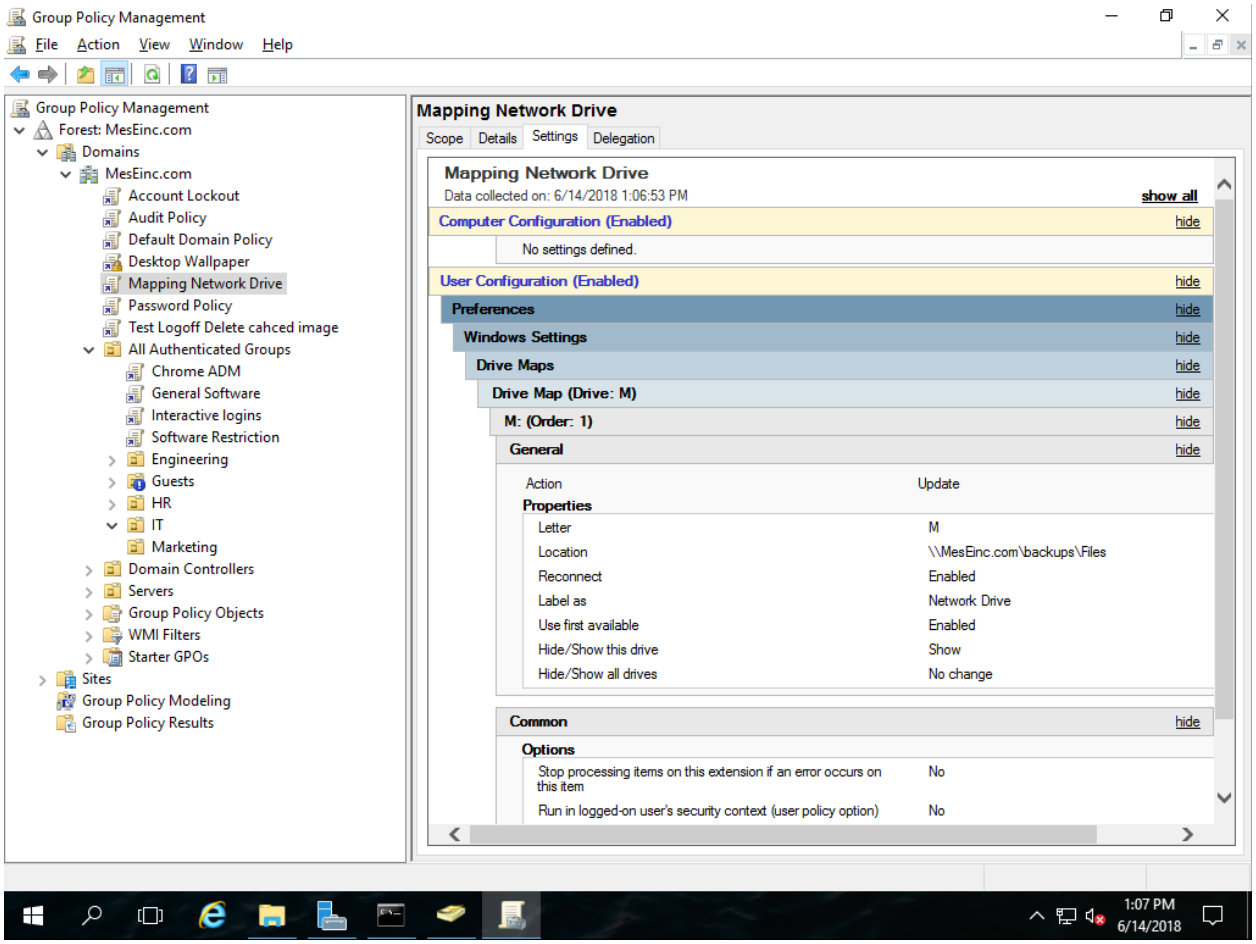
DFS and Mapped drives

With DFS replication and namespace, every site's DF server will have a copy of files that will be synchronization during off hours.

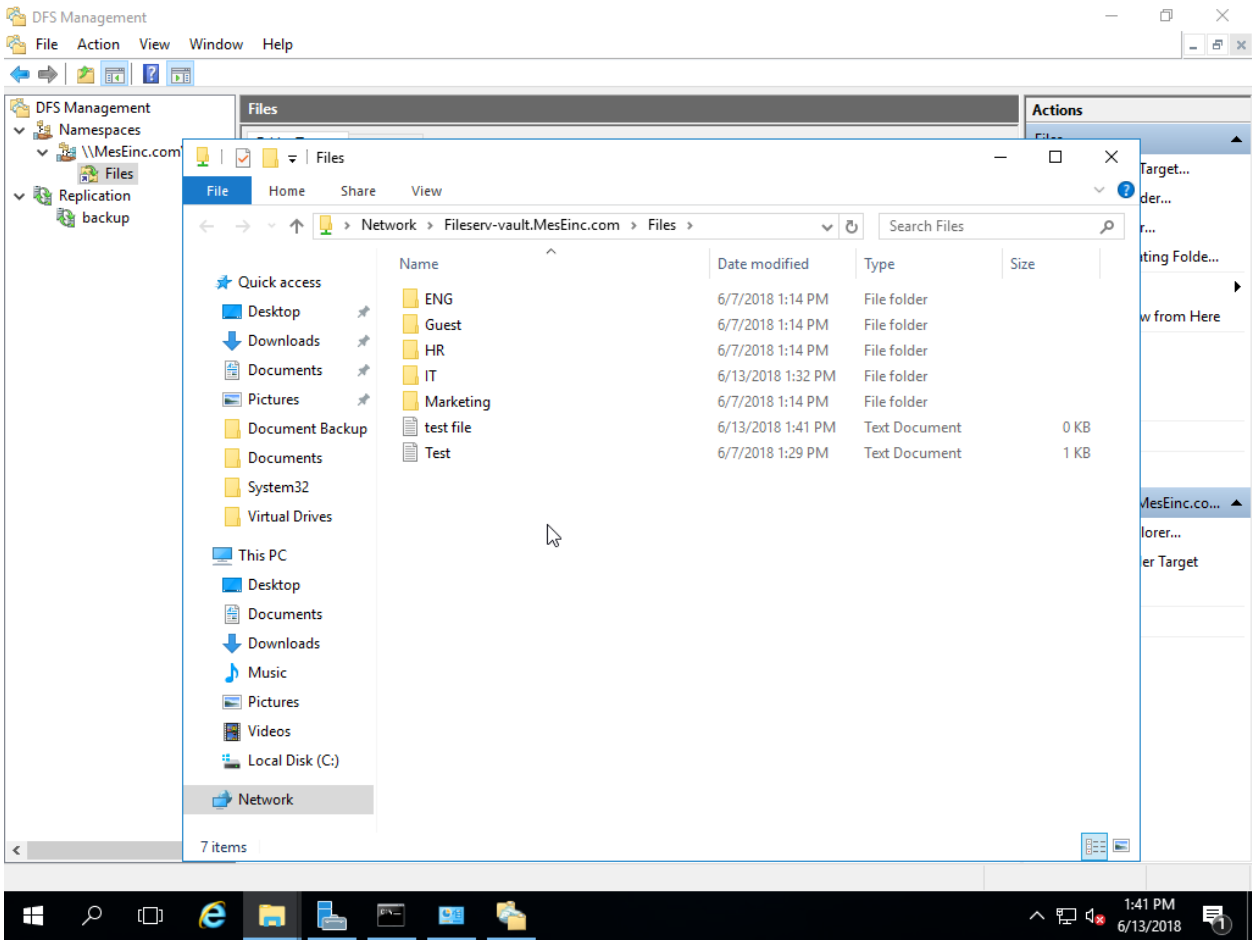


Schedule for automatic replication.

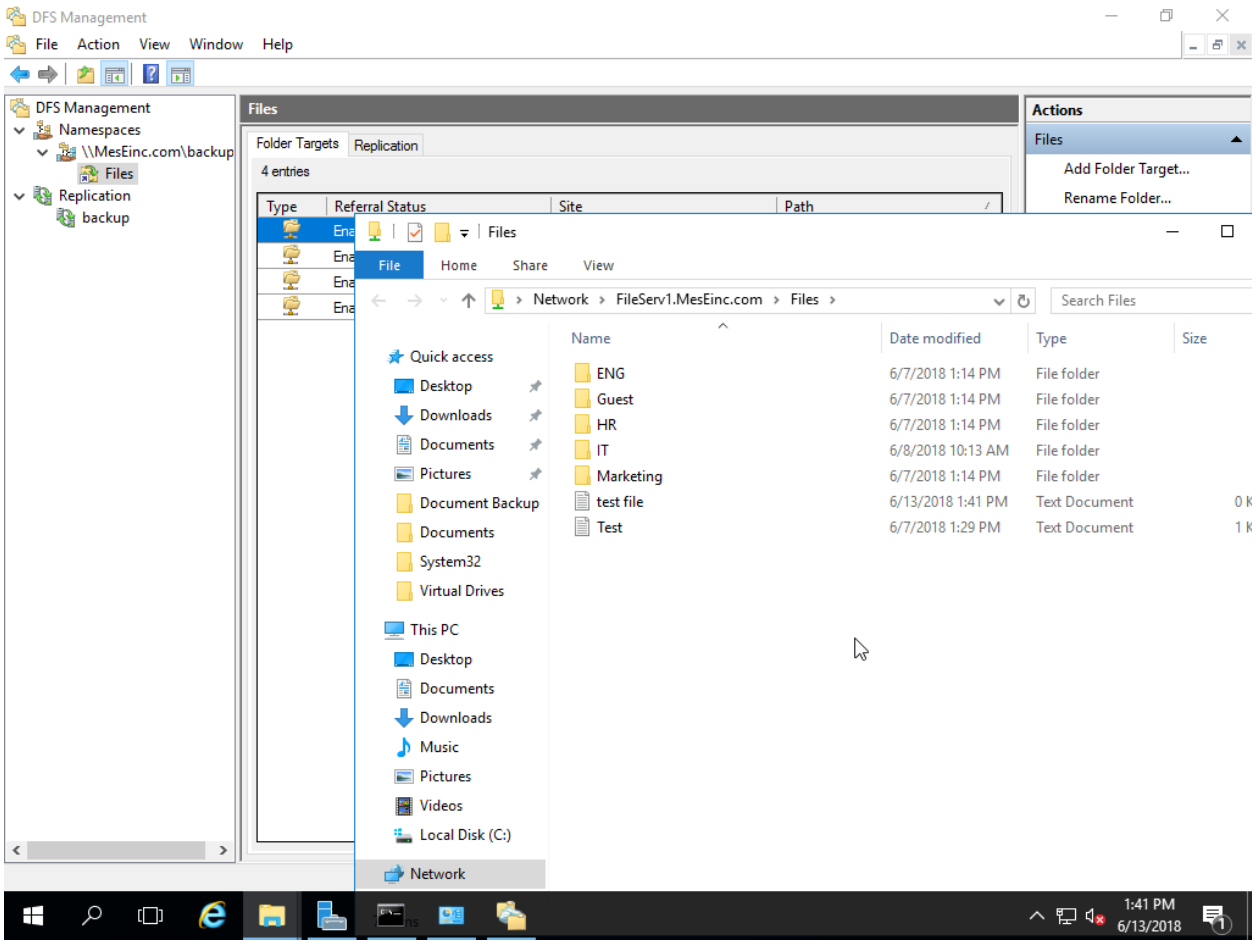
In case any of these server goes down, the clients will be able to access information stored on the any of the alternative DF servers. The primary DF will be located in the server room. Drives will be automatically mapped to clients via GPO. The namespace will contain folders with the appropriate ntfs permissions for their respective OUs/groups. Steps to do so can be found in the appendix. These shares can be accessed by linux clients via SAMBA. General steps for setting up DFS found here.



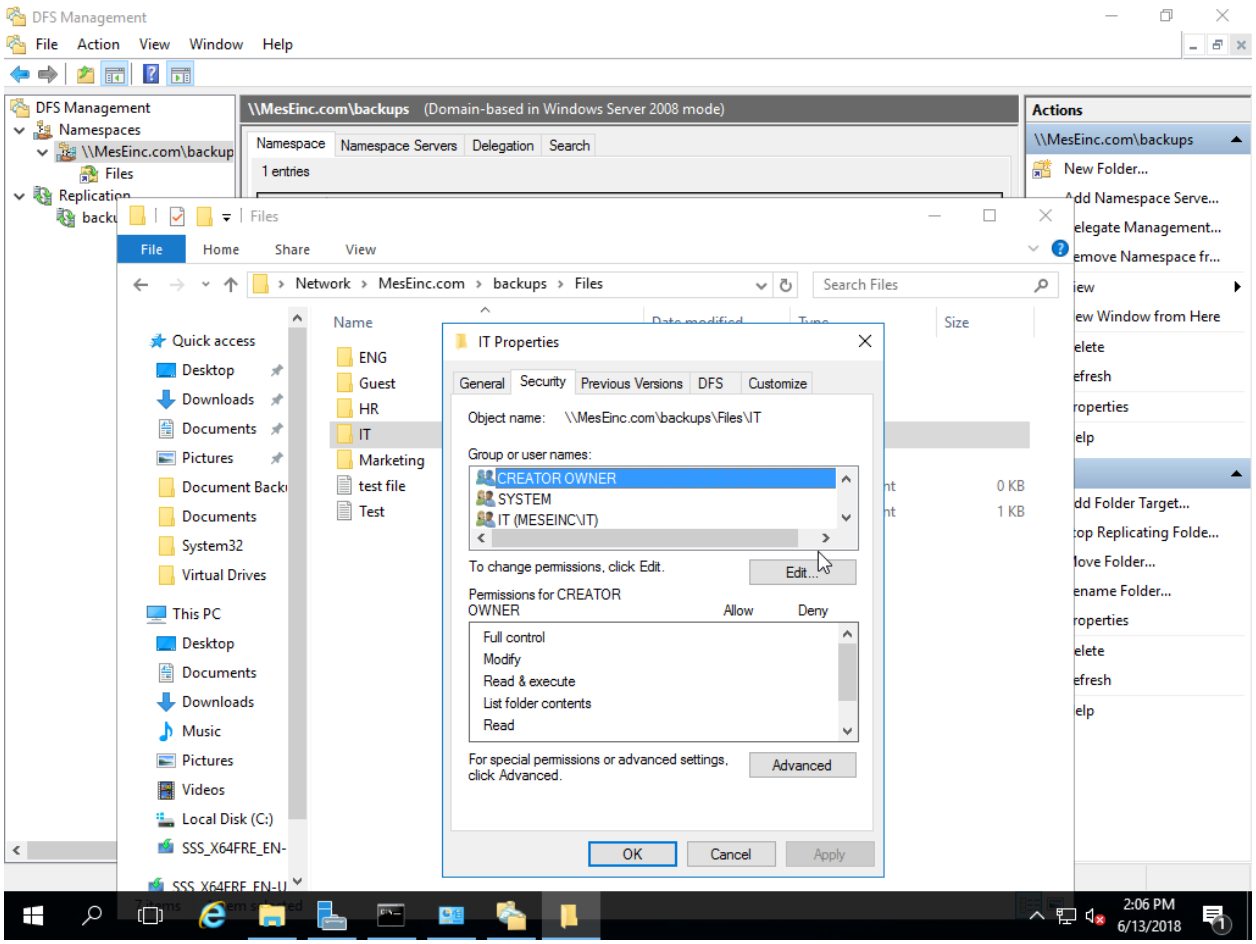
GPO for mounting namespace automatically.



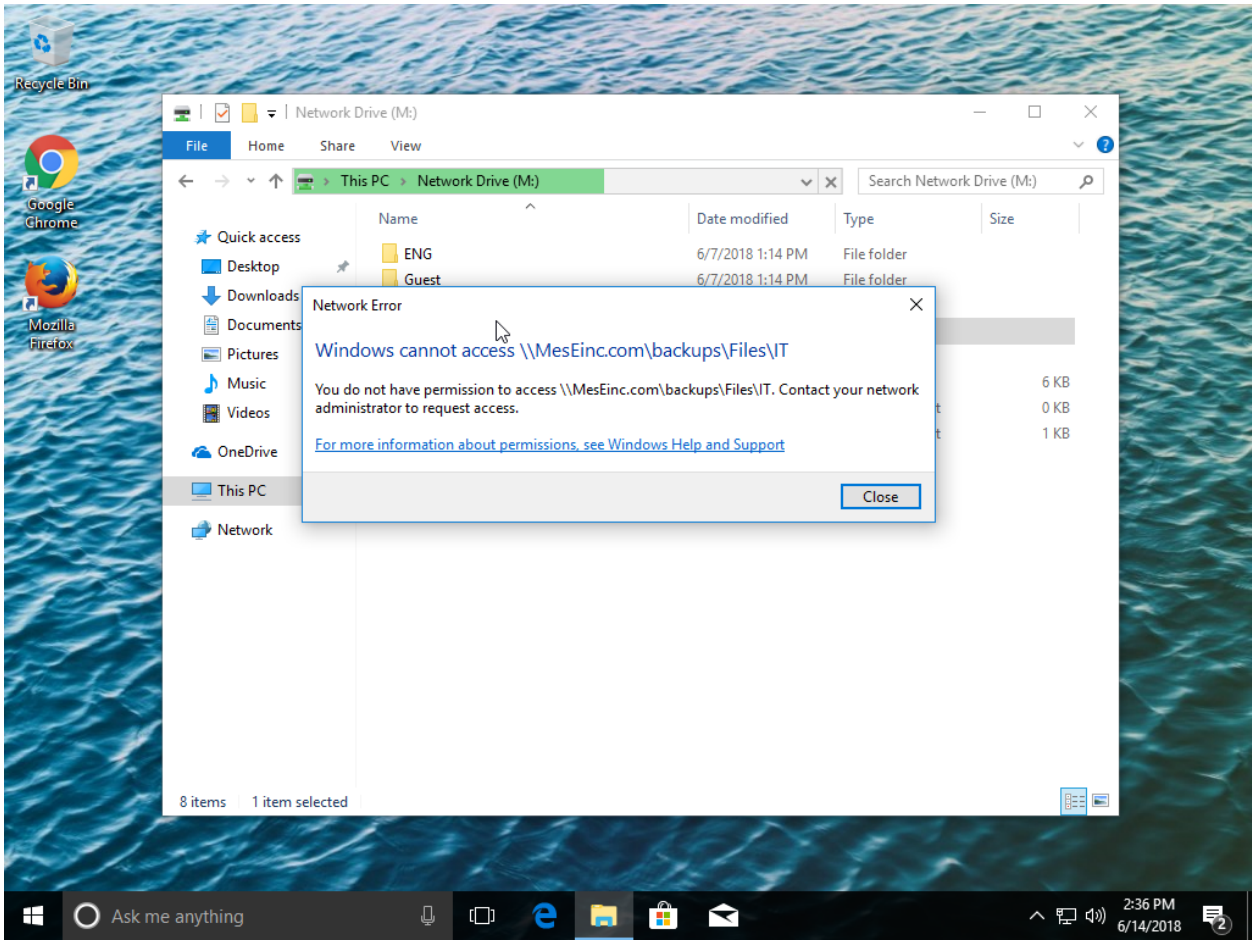
Files are replicated amongst Fileserv-vault



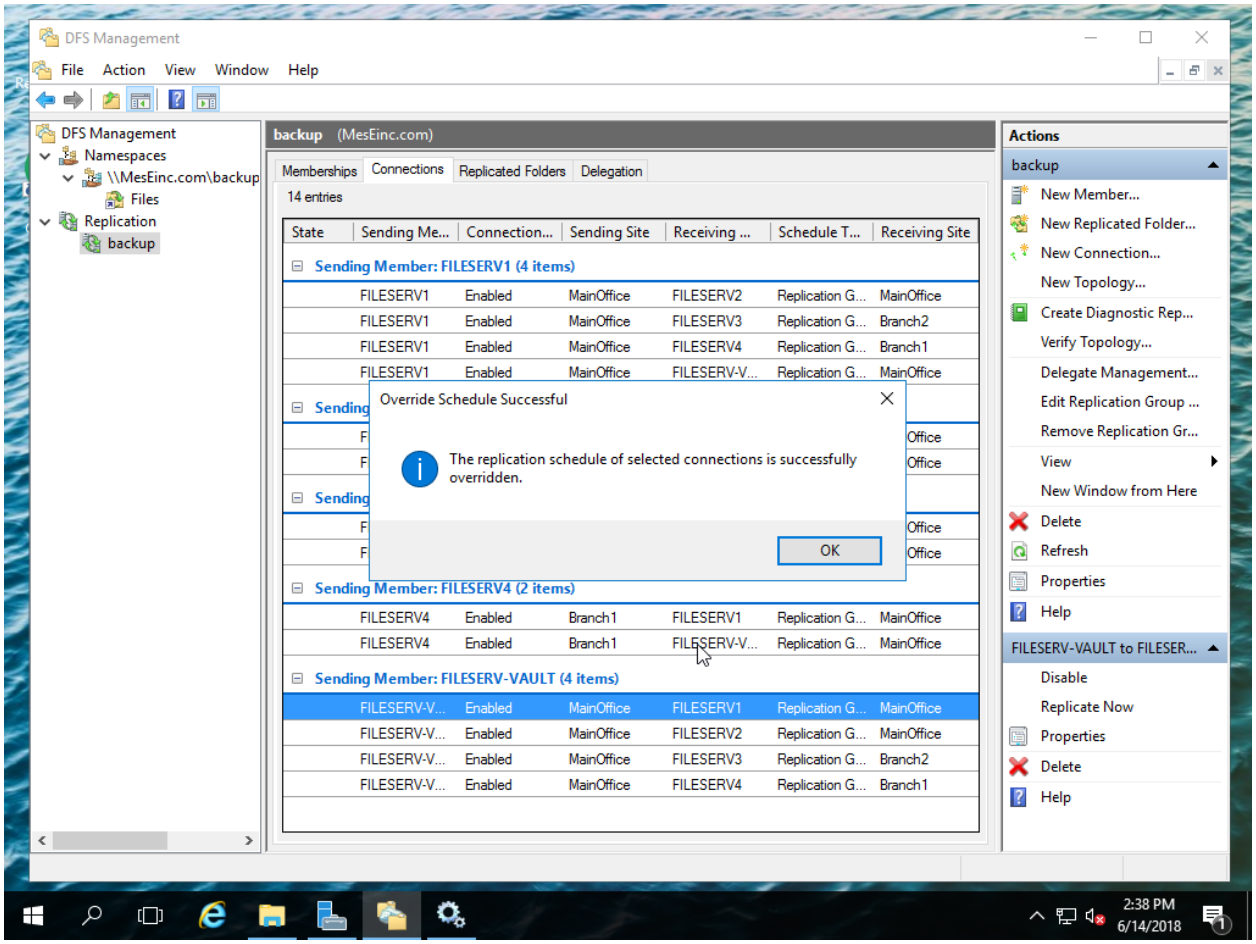
Replicated files on fileserv1



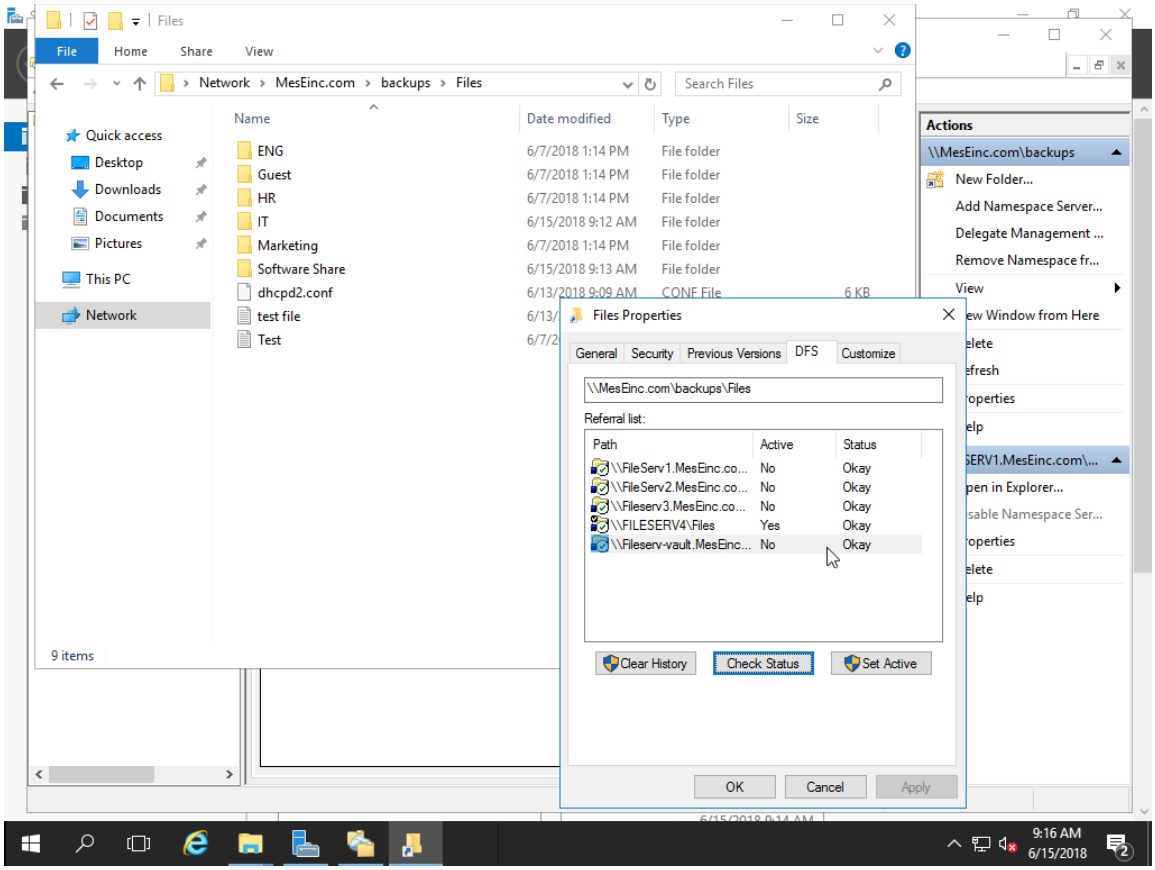
Replicated folders on the namespace. NTFS replication is transferred over.



When using marketing1 account, they do not have access to IT mapped drive.



Manual replication is possible in DFS management. Select the Sending member and the receiving member, and select replicate now on the Actions pane on the right hand side.


Files
File
Home
Share
View
Network › MesEinc.com › backups › Files
Search Files
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Name
Date modified
Type
Size
ENG
Guest
HR
IT
Marketing
Software Share
dhcpd2.conf
test file
Test
9 items
Actions
\\MesEinc.com\backups
New Folder...
Add Namespace Server...
Delegate Management ...
Remove Namespace fr...
View
Files Properties
General
Security
Previous Versions
DFS
Customize
\\MesEinc.com\backups\Files
Referral list:
Path
Active
Status
\\FileServ1.MesEinc.co...
\\FileServ2.MesEinc.co...
\\Fileserv3.MesEinc.co...
\\FILESERV4\Files
\\Fileserv-vault.MesEinc...
No
Yes
Okay
Clear History
Check Status
Set Active
OK
Cancel
Apply
9:16 AM
6/15/2018

DFS status

LINUX

Hardware/Software

- IBM Server 2x at Data Center
    - ESxi 6.0.0
    - Vm1 Centos 7
        - Samba
        - DHCP
- Dell workstation at Data Center
    - Failover for DHCP

General Workflow

1. Centos will be the samba client accessing file server that will will contain html configuration and files (implemented)
2. Centos server will periodically pull data from file share and place them in the appropriate location in linux server to push out to web client (not yet implemented)
3. Dell workstation will be a failover for DHCP (not implemented)
4. Web server will contain frontpage containing company information for potential clients

Centos 7

We choose centos 7 because it is free and is essentially downstream Redhat without branding. Because of the nature of the Centos project, there is plenty of documentation that is applicable. This includes documentation for openSuse, Redhat Linux, Fedora and any other RPM based distribution.

While fedora does offer a server release, we opted against it because it is comparatively unstable and it's frequent updates may cause unnecessary breakage. Fedora has a approximate 13 month release cycle with EOL for every two new versions released. [18] Centos 7 EOL is 2024.[19]

[18] https://fedoraproject.org/wiki/Fedora_Release_Life_Cycle
[19] https://linuxlifecycle.com/

Issues

Centos SELinux has given us a lot of trouble. This includes interfering with dhcp failover which required putting SELinux into permissive mode. It also blocks certain outputs from journalctl that are necessary for troubleshooting.

Samba

Samba is employed as a means of accessing the DFS file shares from Linux to import html data as well as any configurations the IT team may wish to edit using Microsoft tools. See appendix for detailed commands.

Issues

The current method of Samba connection is not secure; passwords are sent in clear text. Further configuration in samba.conf is required.

Currently, mounting of SAMBA share requires manual mounting. We could create a bash script or alias to simplify the command. We could further have this bash script run on startup. Further research is required on this front.

Copying files from the DFS shares when using SAMBA result in links. We have currently not figured out how to do direct copies, we have found an alternative by using the cat command. For example, if we need to copy file “test.txt” to the linux machine, we would use the following:

$ cat test.txt >> /path/to/folder/test.txt

This effectively concatenate text in file “test.txt” to /path/to/folder/test.txt.
For example, if we created a dhcpd.conf file on a windows machine we could transfer this file to the network share to the /etc/dhcp/ by via the following process:

1. From workstation move file to network share
2. Mount samba share on linux using mount.cifs
3. Change the name of existing dhcpd.conf to dhcpd.bak for backup
4. On linux, use cat //samba/share/dhcpd.conf >> /etc/dhcp/dhcpd.conf
5. Restart dhcpd

DHCP

We decided to do DHCP on Linux because we believed it to have a lesser payload while being used and transmitted over our network connection. Also another main reason we choose

Linux/Centos 7 for DHCP server is because of security. Todays in IT environments, the usage of linux is increasing tremendously and it leads to one of the top level worldwide market share. Linux system is outstanding on security. When vulnerability is found in linux, patches are updated quickly, and it is able to receive security sources. On the server side view, we think it is a huge advantage for running a server. In our network we will also configure deny and allow rules which will make it easy for admins to make subnets for developer's virtual hosts in VMWare with the same prefix. This is for the purposes of testing.

The default lease time is set to 24 hours. The maximum lease time is 48 hours. We feel that these are ideal times to ensure that there is not too much address turnover while ensuring addresses are kept even if DHCP servers are down.

Web-Server

We choose to run the webserver on the linux because we are more familiar with apache web server. Running this will result in less administrative overhead due the need to learn the alternatives such as windows IIS or NGINX.

VSFTPD

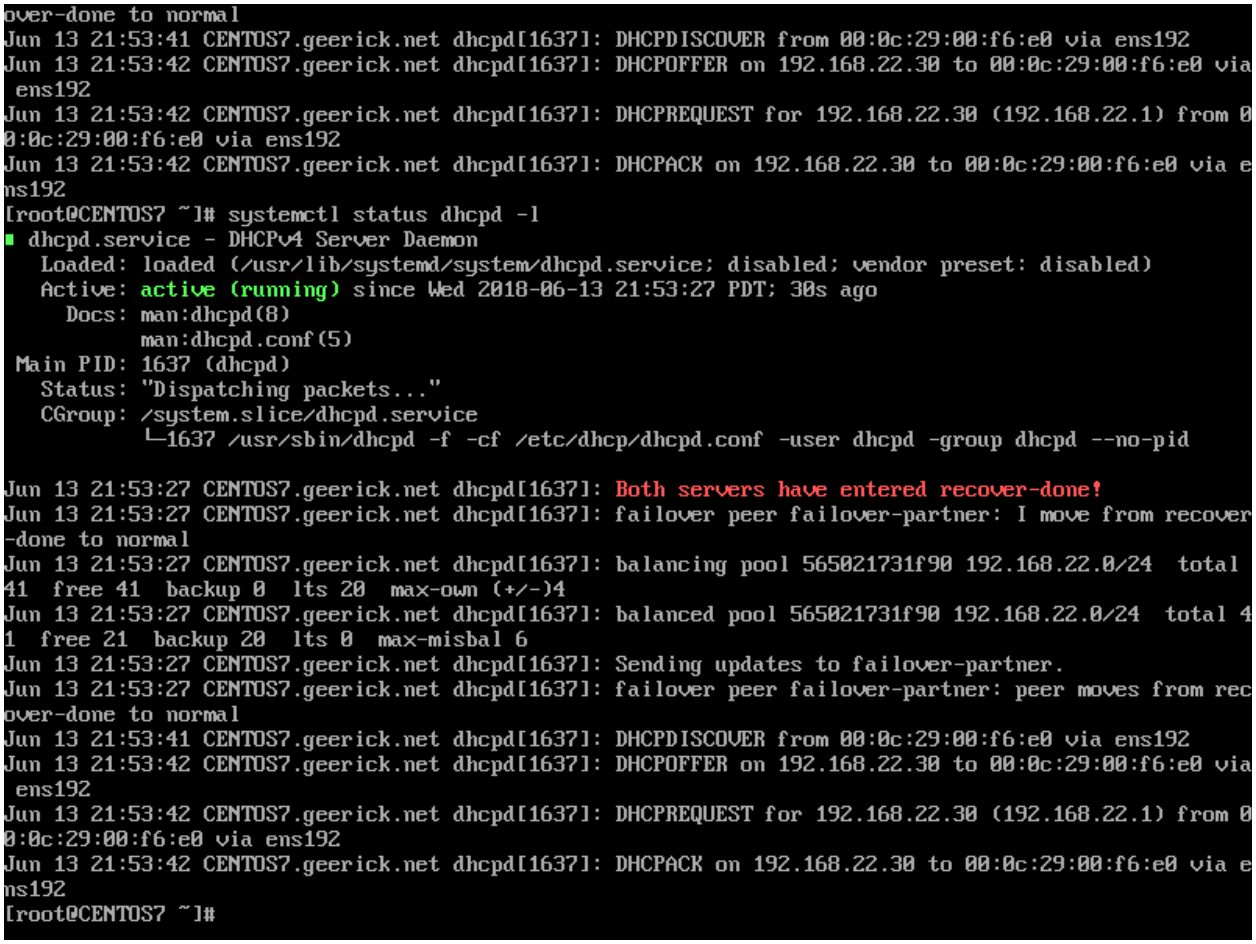
We chose to use VSFTPD (Very Secure file transfer protocol daemon) because it is more stable and secure (hence the very secure part), it also decreases the chances of an attacker gaining access to our server through FTP vulnerabilities.

DHCP Failover

Our team decided to configure DHCP failover so that both servers will be managing the same pool of addresses so that they will be able to share the load of leases for that pool. It also provides as a backup for one another in case of failure of one server due to network outages. (Not working as of June 14, 2018)

Issues

The DHCP servers was not able to communicate with each other. The primary server was always stuck in recovery mode and the secondary server assumes that the primary server holds all the leases. While test runs worked, we were unable to get it working in practice.



This is a screenshot in a test environment. If the failover works, the “both servers have entered recover-done!” message should be sent. We could not get this working in the live environment.

Syslog

System log contains many different type of errors and messages of the system. The errors and messages are very important for understanding system errors or troubleshooting the problem. The log information will save to /var/log as the file by the syslog daemon. Because log history is very important information, we need to save logs to a separate server. Therefore, we decided to set up our cisco device’s syslog on our web-server. When the device system gets hacked or has a problem, we will be able to check the system of the device by analyzing the logs on web-server.

Cisco/Network Infrastructure

Routers

In this network there are three routers: M-R1, B1-R1 and B2-R1. The router for the main office which is found in site A is M-R1. B1-R1 belongs to site B and B2-R1 belongs to site C. These routers are connected via serial links and are responsible for routing between the datacenter, the main office and the branch offices.

As the primary router for the main office, M-R1 is responsible for route redistribution between two dynamic routing protocols: EIGRP and OSPF. It is also in charge of filtering the routing table entries.

The B1-R1 and B2-R1 routers are routers for the branch offices. They route the traffic of their respective offices and are equipped with features that protect information from security threats.

Switches

There are five layer-2 switches in the network: M-S1, M-S2, M-S3, B1-S1 and B2-S1. These switches provide network access to the clients. They also provide access to the server machines by establishing a connection to the datacenter switch.

Switches M-S1, M-S2, and M-S3 are located in site A. These switches are linked together by EtherChannel bundles which are configured with the Port Aggregation Control protocol (PAgP) in an active negotiating state. The M-S1 switch has also established an EtherChannel link to the DatCN-Link-123 switch.

B1-S1 is found in site B and is connected to the Branch1 router. The B2-S1 switch is found in site C and is connected to the Branch2 router. The switches are configured with a default gateway in order to be reached and all the unused ports are shut down.

Features

Router-on-a-Stick

Currently each router is being used to perform routing for our VLANs in each branch office and to the main office. F0/1’s subinterfaces are being used for each VLAN, this saves on costs as

we can configure as many subinterfaces as needed per VLAN without needing individual physical ports.

OSPF/EIGRP

Route Redistribution

In order to have multiple routing protocols running at the same time, we needed to redistribute OSPF routes into EIGRP and EIGRP routes into OSPF. This allows OSPF and EIGRP to be advertised through M-R1.

After OSPF and EIGRP fully converged, there were too many routes in the routing table for us to see our own networks. In order for us to limit the routing table entries, we needed to filter out the other routes by applying an ACL.

```
Gateway of last resort is 142.232.194.254 to network 0.0.0.0

C    192.168.123.0/24 is directly connected, FastEthernet0/1.24
     192.168.25.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.25.0/25
          [90/30720] via 192.168.123.1, 23:57:17, FastEthernet0/1.24
S       192.168.25.0/24 [120/0] via 172.25.3.211, Tunnel500
                        [120/0] via 172.25.3.210, Tunnel500
D       192.168.25.128/25
          [90/30720] via 192.168.123.1, 00:30:52, FastEthernet0/1.24
     142.232.0.0/24 is subnetted, 1 subnets
C       142.232.194.0 is directly connected, FastEthernet0/0
     172.25.0.0/16 is variably subnetted, 27 subnets, 7 masks
O       172.25.3.160/27 [110/65] via 172.25.3.254, 00:09:40, Serial0/1/1
O       172.25.1.128/26 [110/782] via 172.25.3.250, 00:08:47, Serial0/2/1
C       172.25.0.128/26 is directly connected, FastEthernet0/1.503
O       172.25.3.128/27 [110/782] via 172.25.3.250, 00:08:50, Serial0/2/1
O       172.25.2.128/26 [110/65] via 172.25.3.254, 00:09:42, Serial0/1/1
O       172.25.3.240/29 [110/65] via 172.25.3.254, 00:09:42, Serial0/1/1
C       172.25.3.254/32 is directly connected, Serial0/1/1
C       172.25.3.252/30 is directly connected, Serial0/1/1
C       172.25.3.250/32 is directly connected, Serial0/2/1
C       172.25.3.248/30 is directly connected, Serial0/2/1
O       172.25.3.224/28 [110/782] via 172.25.3.250, 00:08:50, Serial0/2/1
C       172.25.3.208/28 is directly connected, Tunnel500
O       172.25.1.192/26 [110/782] via 172.25.3.250, 00:08:50, Serial0/2/1
C       172.25.0.192/26 is directly connected, FastEthernet0/1.504
C       172.25.3.192/28 is directly connected, FastEthernet0/1.506
O       172.25.2.192/26 [110/65] via 172.25.3.254, 00:09:42, Serial0/1/1
O       172.25.3.32/27 [110/782] via 172.25.3.250, 00:08:50, Serial0/2/1
O       172.25.1.0/26 [110/782] via 172.25.3.250, 00:08:50, Serial0/2/1
C       172.25.0.0/26 is directly connected, FastEthernet0/1.501
S       172.25.0.0/22 [120/0] via 172.25.3.211, Tunnel500
                      [120/0] via 172.25.3.210, Tunnel500
C       172.25.3.0/27 is directly connected, FastEthernet0/1.1
O       172.25.2.0/26 [110/65] via 172.25.3.254, 00:09:42, Serial0/1/1
C       172.25.3.96/27 is directly connected, FastEthernet0/1.505
O       172.25.1.64/26 [110/782] via 172.25.3.250, 00:08:50, Serial0/2/1
C       172.25.0.64/26 is directly connected, FastEthernet0/1.502
O       172.25.3.64/27 [110/65] via 172.25.3.254, 00:09:45, Serial0/1/1
O       172.25.2.64/26 [110/65] via 172.25.3.254, 00:09:45, Serial0/1/1
S*   0.0.0.0/0 [1/0] via 142.232.194.254, FastEthernet0/0
```

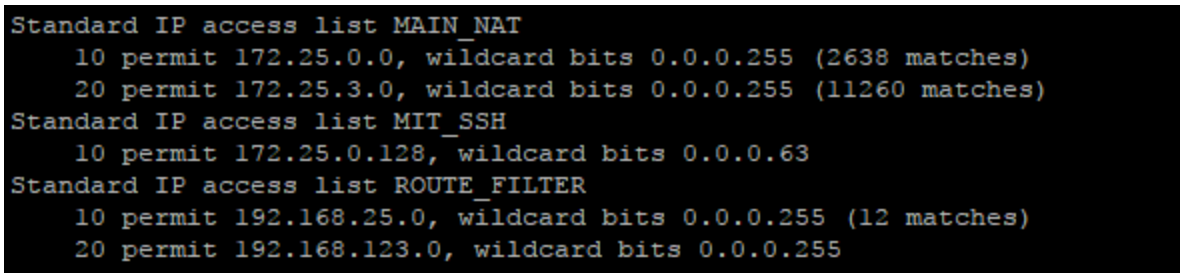
Figure above shows the output of the **show ip route** command on Main router after the ACL filter has been applied.

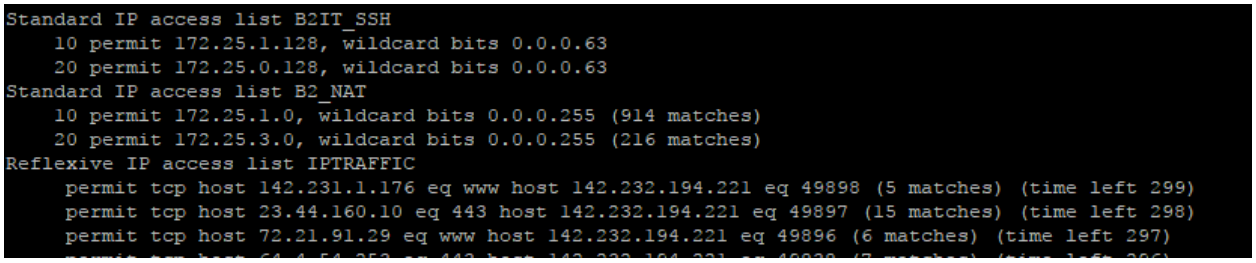
Global Authentication

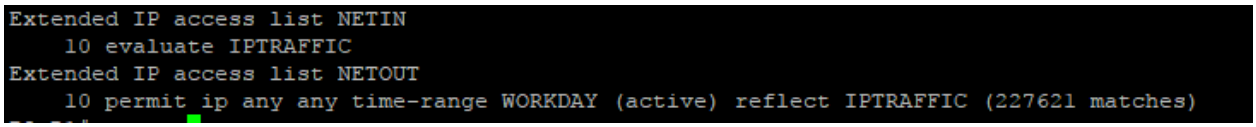
OSPF is configured with MD5 authentication globally to enable routers to update and exchange routing information securely. We chose to use MD5 authentication for OSPF because it is considered the most secure mode, it does not send plain text passwords over the network.

ACLs

Currently one of the ACLs applied is being used to filter out routing table entries by limiting the traffic allowing only the 192.168.25.0 network through M-R1. Another ACL that we have applied is for remote management of network devices. This is to allow only the IT department in the main office and each branch access to network devices for security purposes. One of the advanced ACLs that we have applied is a time-based ACL, it allows access to the outside network/internet only during working hours 8:00am to 5:00pm. This is to ensure that no access and usage of network resources are used during off hours.







Figures above show output of the **show access-list** command

Etherchannel

Etherchannel is primarily used on the Main office switches to provide fault tolerance and high speed connections. It also allows for scalability in the future because it uses existing wires and ports that do not need to be upgraded to provide higher bandwidth. All Etherchannel links are configured as trunk links, this ensures that we can send and receive data between VLANs.

```
Number of channel-groups in use: 3
Number of aggregators:           3

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         PAgP      Fa0/1(Pd)   Fa0/2(P)
2      Po2(SU)         PAgP      Fa0/13(P)   Fa0/14(Pd)
4      Po4(SU)         PAgP      Fa0/5(P)    Fa0/6(Pd)
```

Figure above shows output of the **show etherchannel summary** command

Point-to-Point Protocol (PPP)

The serial links are implemented with PPP encapsulation method as it has numerous advantages over HDLC. Our priority is to send data through the serial link connections in a secure manner. That is why we chose the Challenge Authentication Protocol (CHAP) considering it uses three-way handshakes to establish bidirectional authentication.

Port Security

To secure our ports we limited the number of addresses that send out traffic within the network by applying the switchport security feature. This feature is administered on our access ports to mitigate any potential Layer-2 attacks such as MAC flooding or MAC spoofing. The Mac-Address Sticky command will record the number of MAC addresses that associated with the port which prevents any third-party from accessing the network.

```
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
---------------------------------------------------------------------------
     Fa0/22            10           6                 0         Restrict
     Fa0/23            10           1                 0         Restrict
     Fa0/24            10           3                 0         Restrict
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 7
Max Addresses limit in System (excluding one mac per port) : 1024
```

Figures above show output of the **show port-security** command

SSH Authentication

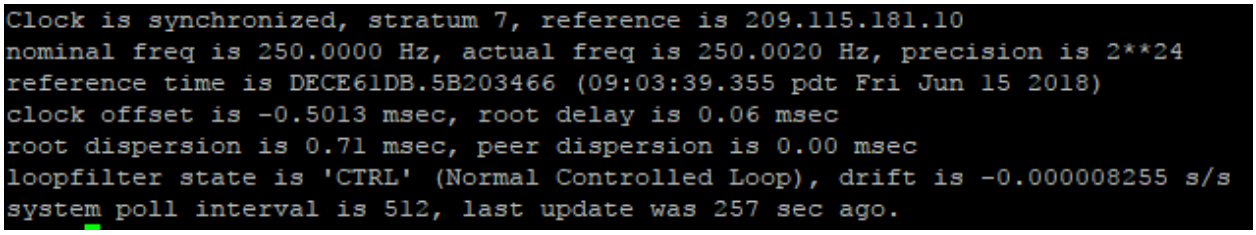
Version 2 of SSH is enabled on our devices for the reason being that this version implements encryption algorithms that are more advanced than Telnet's plaintext. In order to prevent non-SSH connections, the VTY lines on our devices are configured so that it is limited to only SSH traffic.

NAT

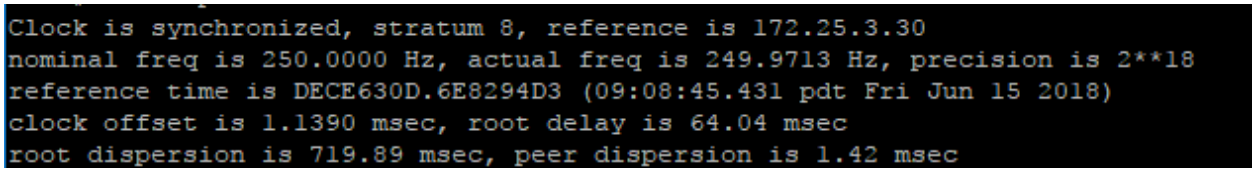
NAT is being used to allow the PCs connectivity to the internet by translating our assigned private addresses to public addresses. Each router is configured with PAT, to allow for each private address accessibility to the outside network.

NTP

We are using a public time server as our NTP server, ca.pool.ntp.org. The Main router is configured with the public time server and will act as the server for all other devices in our network. All other devices are connected as peers to the Main router. We set up NTP to allow for our network devices to have their clocks synchronized, this is important as we have an ACL that is time-based and blocks access to the outside network during off hours.



Above figure shows the **show ntp status** command on the Main router configured as the NTP server for our network devices.



The figure above shows the **show ntp status** command on one of the main office switches connected as a peer to our Main router.

Spanning Tree

We implemented the Rapid PVST variant of the Spanning Tree protocol in order to maintain the quality of the network as well as the integrity of the data that is received. This network protocol is used alongside PortFast to bypass the listening and learning states. Portfast BDPUGuard was also configured as it helps prevent switching loops from occuring.

Syslog

Our routers and switches forward log messages that have a severity level of 6 or lower to the Syslog server. The information generated from our network devices are delivered through the local2 facility. Using the local2 facility allows us to closely monitor our network devices and fixate on any issues that require attention.

```
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes, 0 overruns)
    Console logging: level debugging, 54 messages logged
    Monitor logging: level debugging, 0 messages logged
    Buffer logging: level debugging, 56 messages logged
    Exception Logging: size (4096 bytes)
    File logging: disabled
    Trap logging: level debugging, 55 message lines logged
        Logging to 172.25.3.1, 9 message lines logged
        Logging to 192.168.25.226, 2 message lines logged
```

Figures above show output of the **show logging** command

DMVPN using GRE

Using DMVPN allows scalability of IPSec VPNs by combining the use of GRE tunnels, IPSec encryption, and Next Hop Resolution Protocol (NHRP). We've chosen this feature to allow our branch sites to connect to the main branch securely with IPSec encryption on both ends of the tunnel while also being able to implement it in a larger network in the future.

```
Main#show crypto ip sa

interface: Tunnel500
    Crypto map tag: Tunnel500-head-0, local addr 142.232.194.220

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (142.232.194.220/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (142.232.194.221/255.255.255.255/47/0)
   current_peer 142.232.194.221 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 605, #pkts encrypt: 605, #pkts digest: 605
    #pkts decaps: 664, #pkts decrypt: 664, #pkts verify: 664
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 142.232.194.220, remote crypto endpt.: 142.232.194.221
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x6C89146D(1820922989)
     PFS (Y/N): N, DH group: none
```

Figure above shows output of the **show crypto ipsec sa** command

Appendix

Linux

Basic Installation of Centos 7

Installing Centos.7 - Basic configuration

1.1 Change Software Selection ‘Minimal Install’ to ‘Development and Creative Workstation’

1.2 Enable Network & Hostname

1.3 In ‘Installation destination’, Configure partitioning for standard and swap (Enable ‘I will configure partitioning’ option)

1.4 Setup root password, create user.

1.5 Accept license policy

1.6 Disable kdump

Web Server Configuration

1. Basic Installation for APM (Apache + php + Mysql)

1.1 Check the which service we have right now.

- **rpm -qa httpd php mariadb-server**

httpd-2.4.6-17.el7.centos.1.x86_64
(only web-server file should be shown)

1.2 Install mariadb & php services

- **yum install mariadb-server mariadb php php-mysqlnd**

(If installation is fail, reboot the linux)

1.3 Confirm download (3 services should be shown)

- **rpm -qa httpd php mariadb-server**

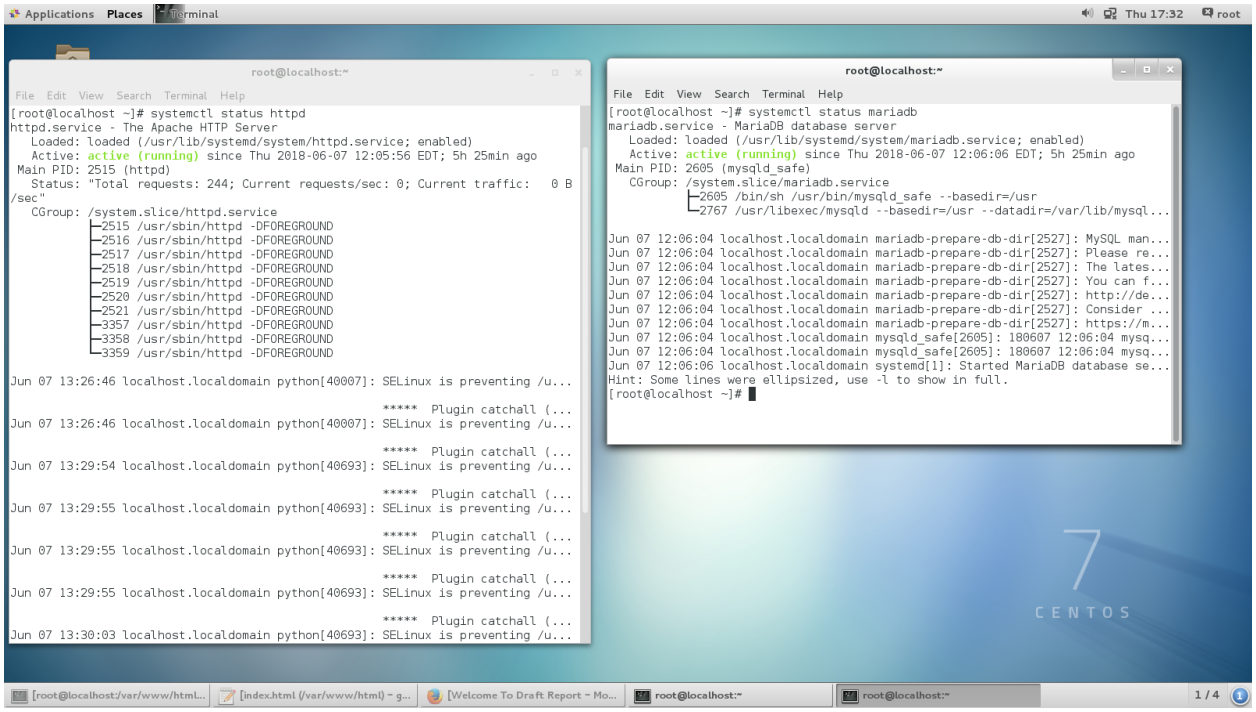
php-5.4.16-45.el7.x86_64
httpd-2.4.6-17.el7.centos.1.x86_64
mariadb-server-5.5.56-2.el7.x86_64

1.4 Start the service that i just downloaded
(php is one of function on apache, no command needs for php)

- **systemctl restart httpd**
- **systemctl restart mariadb**

1.5 make the service always running

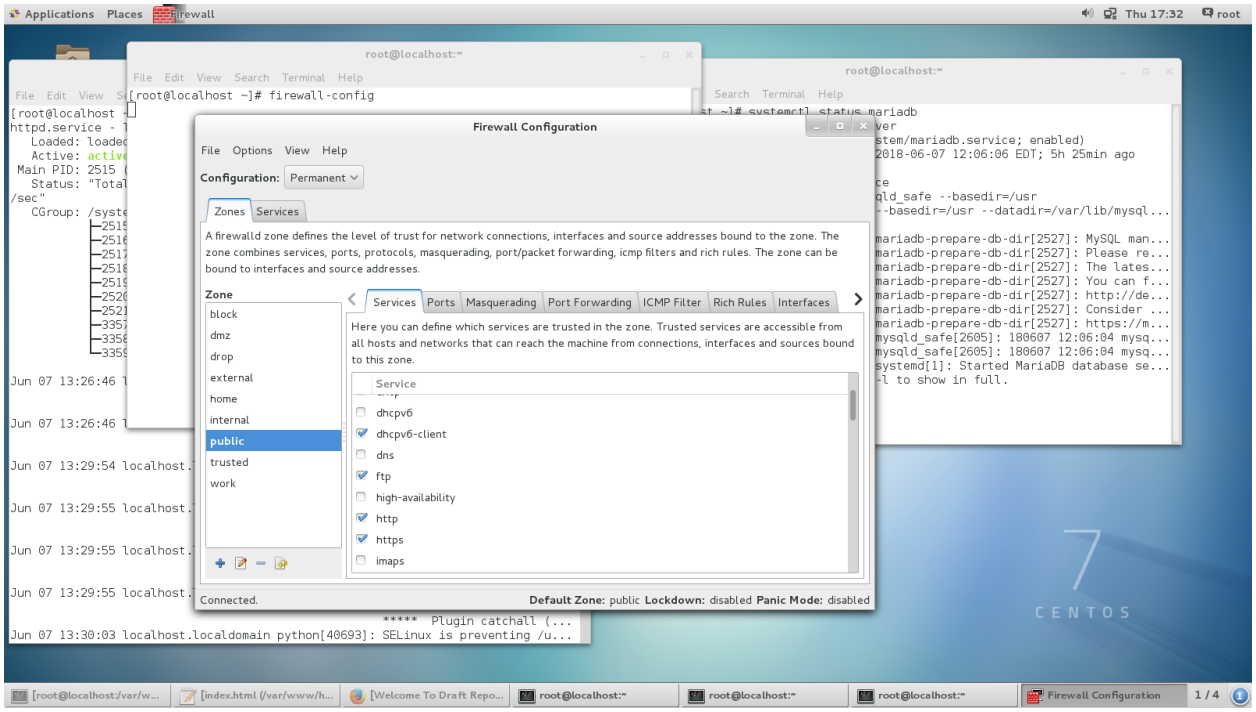
- **systemctl enable httpd**
- **systemctl enable mariadb**



1.6 make firewall to accept the http service

- **firewall-config**

In firewall box, change configuration 'Runtime' to 'permanent'
and select http, https to enable.
lastly, in option menu, 'click Reload Firewall'



1.7 To check apache running correctly,
open Firefox, in address bar, enter 'localhost'

1.8 To check php running correctly,
change directory to html, and see what contents html directory contain.

- **cd /var/www/html/**
- **pwd**

/var/www/html

- **ls** (should be empty first)

1.9 create & configure php file for testing.

- **touch phpinfo.php**
- **gedit phpinfo.php**

1.10 In php file, add line for testing

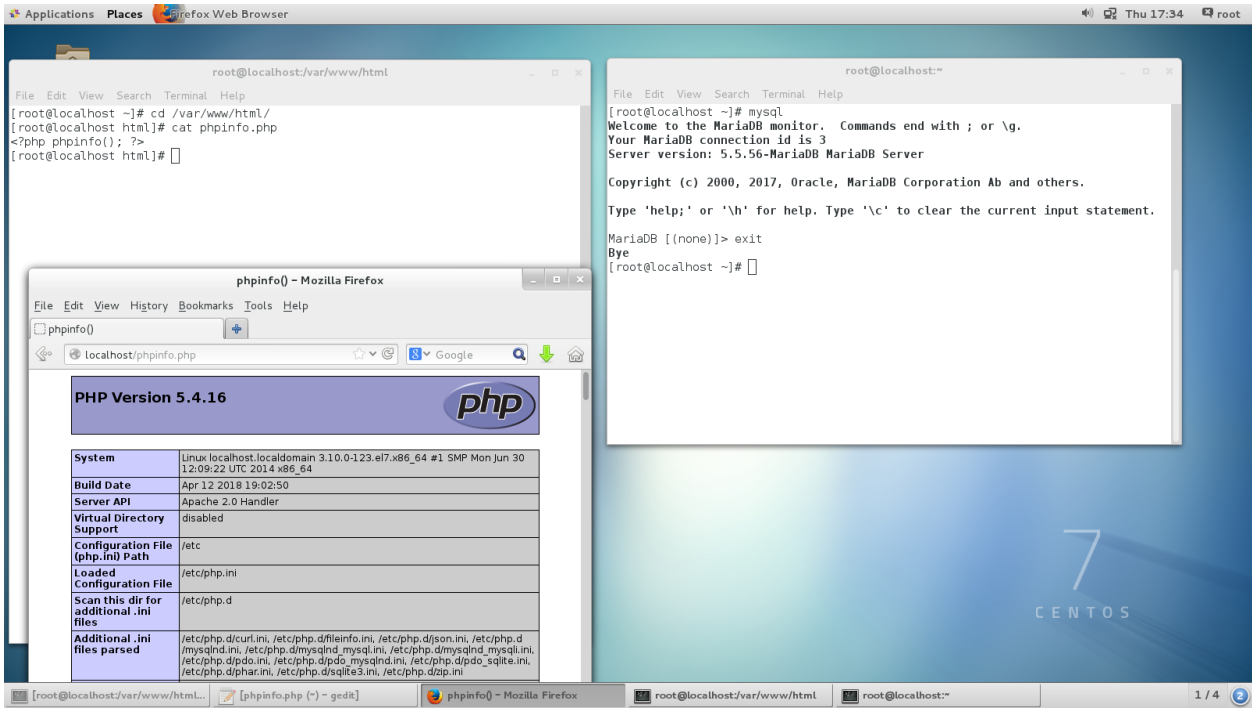
```
<?php   phpinfo();      ?>
```

1.11 Turn on firefox again, and see php is working, In firefox address bar, type 'localhost/phpinfo.php'

1.12 To check mysql(mariadb) running correctly, On command line,

- **mysql**

- **quit** (to exit)



2. Configuring Main web page

Configuring html & index file.

For designing Our company web-page, We need to create index.html file inside of /var/www/html/ and add coding to the file.

This is our coding for index.html

```
<!doctype html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <title>Welcome To MISE EN SCENE</title>

<style type="text/css">
body {
background-color: #efefef;
background-image:
url("http://postfiles13.naver.net/MjAxODA2MDhfOTIg/MDAxNTI4NDAyOTE2NzQz.982FzJk4B0
```

```
YGtxHflXF3AD8tAIme8DK4mJMQDob02CIg.7VHd5ubGOUCQpokHPv9wpFLRa2yM8hlIn0BXX
6TMx60g.JPEG.sasuke231/background.jpg?type=w2");
background-repeat: repeat;
}
.main{position:fixed; left:150px; top:30px;}
.main2{position:fixed; left:150px; top:150px;}
.group{position:fixed; left:1000px; top:150px;}
</style>

</head>
 <body>
<div class="main">
 <font size ="8" color="08088A">
 <p> MISE EN SCENE </p>

<div class="main2">
 <font size ="5" color="0B0B61">
  <p> 2018 Student Project Final Report</p>
  <img
src="https://postfiles.pstatic.net/MjAxODA2MTRfMjcz/MDAxNTI4OTA2MzMwNDE4.j3BrYZFV_5
jMYsPPdWqAvc2OSFjzC1SvWIpZdfrZiyQg.tKCDW1REZnyKo29EjASeZY_xvxVglZvX3o2Rzc8
FFIUg.JPEG.sasuke231/MES_Logo.jpg?type=w2" alt="missing image" width="317"
height="172">

<div class="group">
<font size ="4" color="0A0A2A">
 <p>Group Members</p>
 <font size ="2" color="0A0A2A">
 <p>Gabriel Kwan</p>
 <p>David Lee</p>
 <p>Vanessa Luu</p>
 <p>Arjay Emata</p>
 <p>Noel Lee</p>
 <p>Aaron Yang</p>
 <p>Johnny Le</p>

<div class="link1">
<h2>Links</h2>
<p>Link to Company Report: <a href="/CompanyReports" target="_blank"> Link</a>
 </body>
</html>
```

Steps.

1.1 Use <title> tag for declaring what the page's title is.

1.2 Design logo and background image, uploaded to our blog, and get the copy of image’s address (image source).

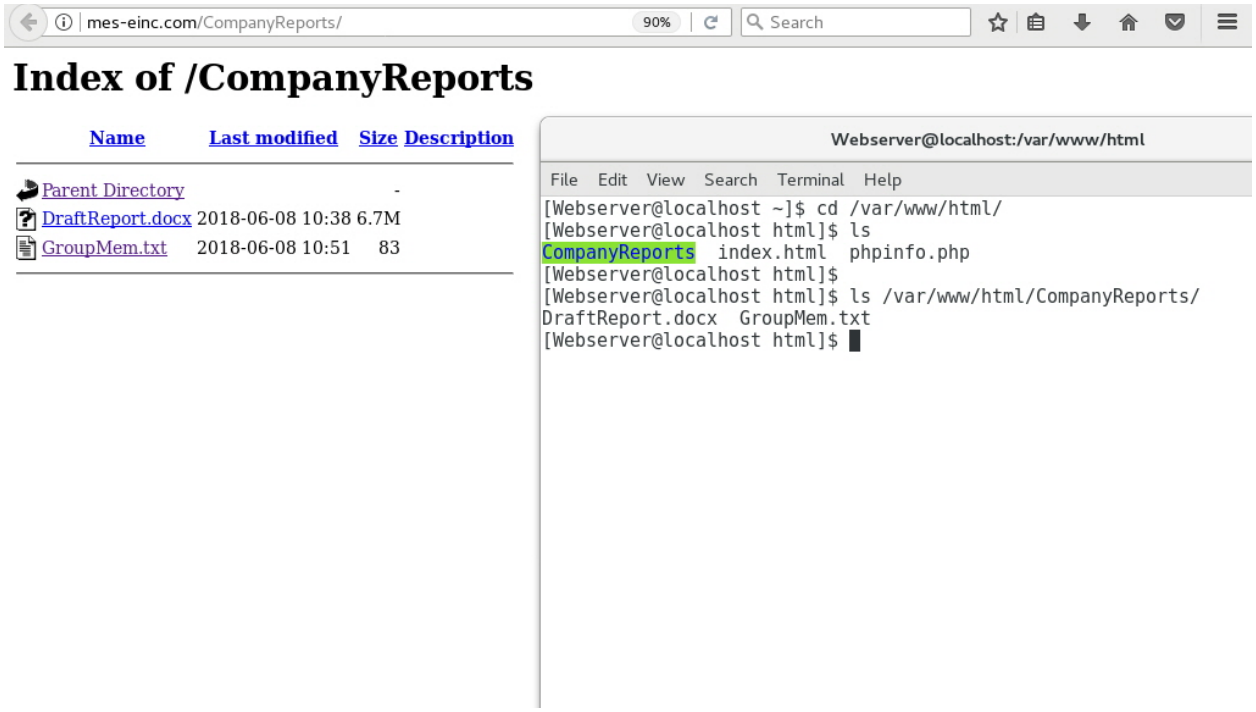
1.3 Setup background color, pattern and background image.
For the background image, we brought the image address from previous step.

1.4 Use tag to defines a division or a section in an HTML document.
Create 4 tag for title text, subtitle text, members name and link.
Set up the position of each contents by using tag

1.5 Set up color and size for each content.

1.6 For second which is our logo, brought the image address from blog, just like we did in background image.

1.7 For the fourth ,
Create the folder name ‘CompanyReports’ inside of html folder and make a link to enabling access to this folder from the web page.
Later, we'll put our draft report to ‘CompanyReports’ folder, so we can see the draft report from our web page.

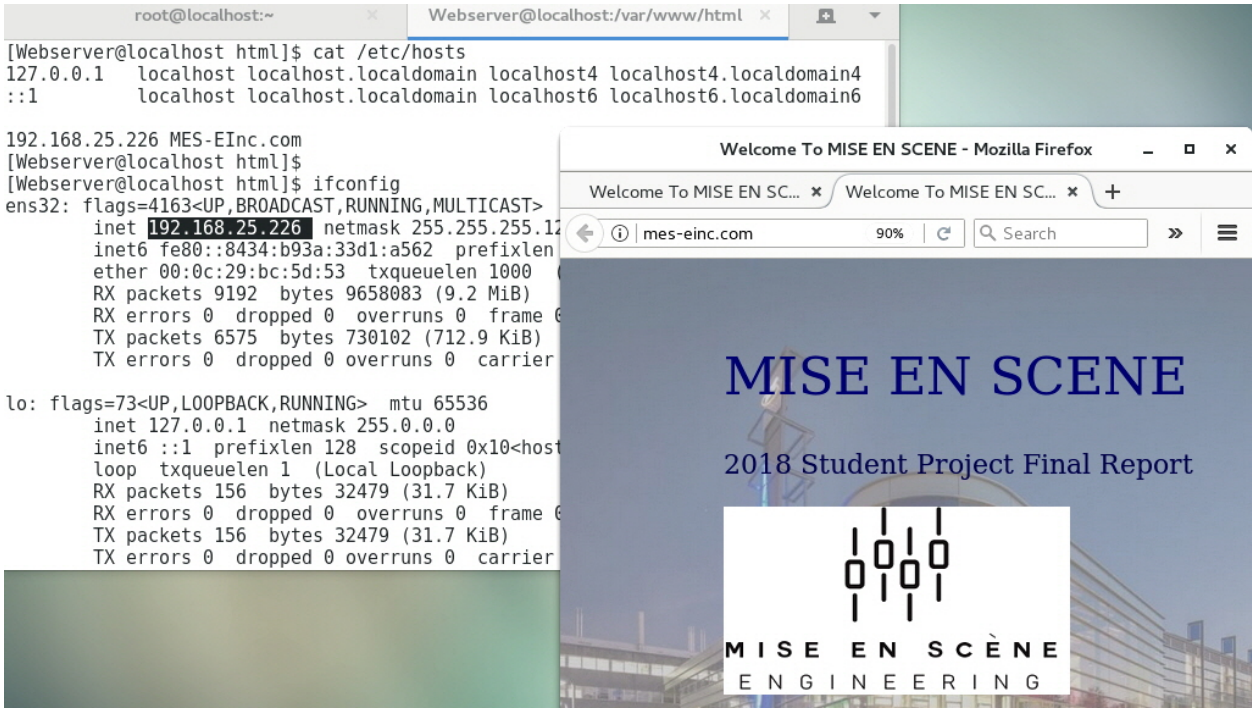


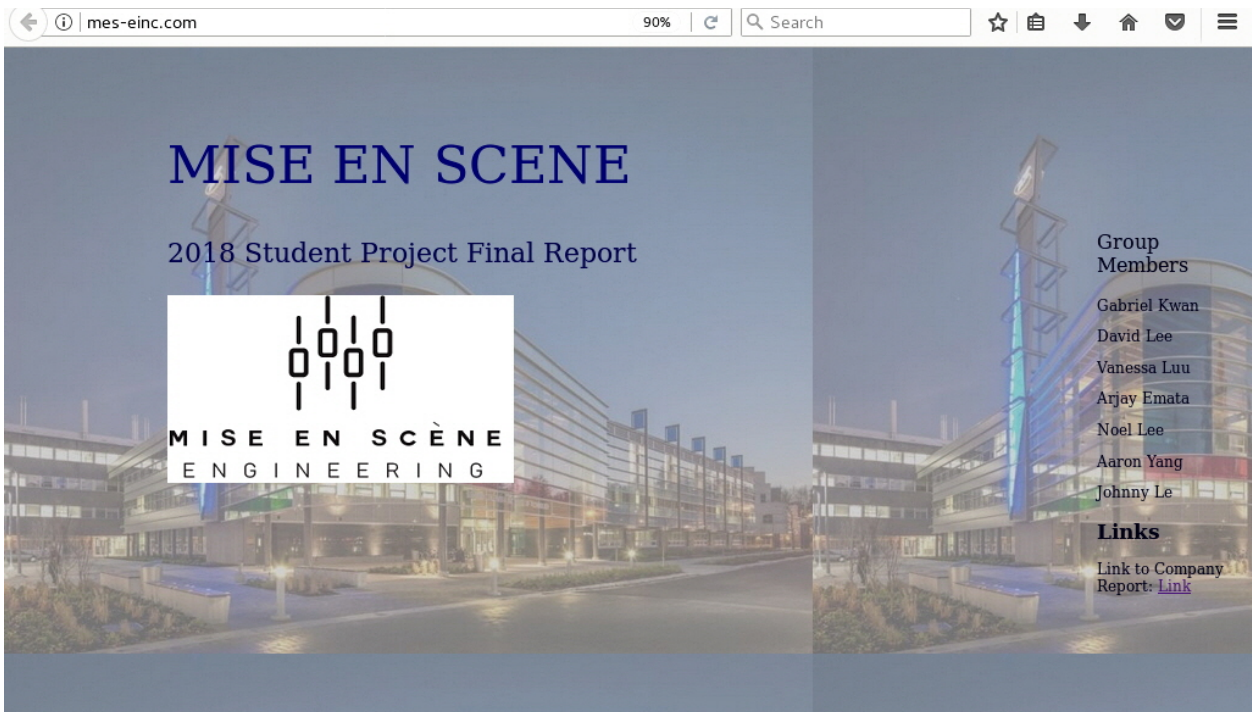
1.8 Configure host file to redirect the address

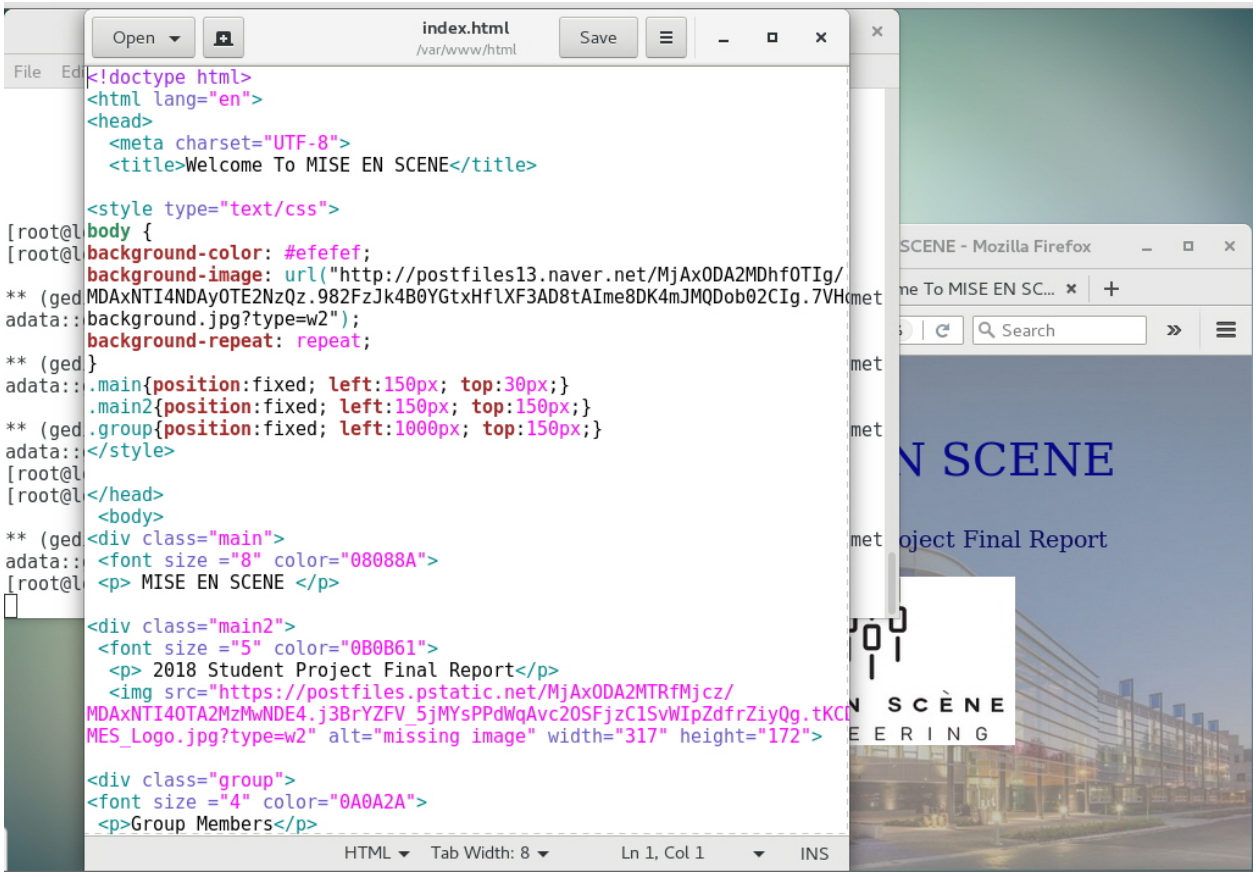
Check the local ip address first, by entering ‘ifconfig’ command, and add extra line in /etc/hosts.

gedit /etc/hosts, add one line that contains,

current local ip address and the address that wants to redirect.


root@localhost:~
Webserver@localhost:/var/www/html
[Webserver@localhost html]$ cat /etc/hosts
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.25.226 MES-EInc.com
[Webserver@localhost html]$
[Webserver@localhost html]$ ifconfig
ens32: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>
inet 192.168.25.226 netmask 255.255.255.12
inet6 fe80::8434:b93a:33d1:a562 prefixlen
ether 00:0c:29:bc:5d:53 txqueuelen 1000
RX packets 9192 bytes 9658083 (9.2 MiB)
RX errors 0 dropped 0 overruns 0 frame
TX packets 6575 bytes 730102 (712.9 KiB)
TX errors 0 dropped 0 overruns 0 carrier
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host
loop txqueuelen 1 (Local Loopback)
RX packets 156 bytes 32479 (31.7 KiB)
RX errors 0 dropped 0 overruns 0 frame
TX packets 156 bytes 32479 (31.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier
Welcome To MISE EN SCENE - Mozilla Firefox
Welcome To MISE EN SC...
Welcome To MISE EN SC...
mes-einc.com
90%
Search
MISE EN SCENE
2018 Student Project Final Report
MISE EN SCÈNE
ENGINEERING

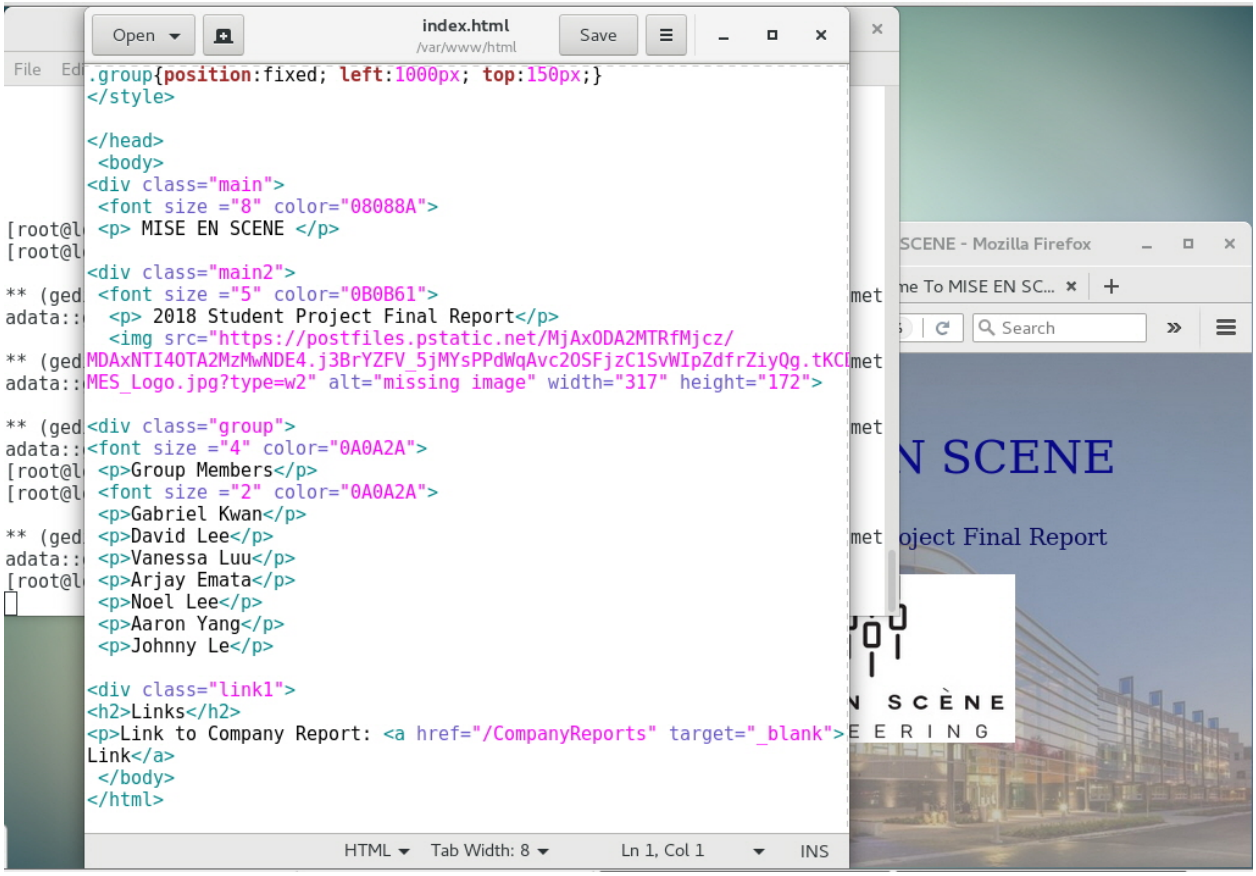

mes-einc.com
90%
Search
MISE EN SCENE
2018 Student Project Final Report
MISE EN SCÈNE
ENGINEERING
Group Members
Gabriel Kwan
David Lee
Vanessa Luu
Arjay Emata
Noel Lee
Aaron Yang
Johnny Le
Links
Link to Company Report: Link


Open
index.html
/var/www/html
Save
<!doctype html>
<html lang="en">
<head>
<meta charset="UTF-8">
<title>Welcome To MISE EN SCENE</title>
<style type="text/css">
body {
background-color: #efefef;
background-image: url("http://postfiles13.naver.net/MjAxODA2MDhfOTIg/
MDAxNTI4NDAyOTE2NzQz.982FzJk4B0YGtxHflXF3AD8tAIme8DK4mJMQDob02CIg.7VH
background.jpg?type=w2");
background-repeat: repeat;
}
.main{position:fixed; left:150px; top:30px;}
.main2{position:fixed; left:150px; top:150px;}
.group{position:fixed; left:1000px; top:150px;}
</style>
</head>
<body>

<font size ="8" color="08088A">
 MISE EN SCENE

<font size ="5" color="0B0B61">
 2018 Student Project Final Report
<img src="https://postfiles.pstatic.net/MjAxODA2MTRfMjcz/
MDAxNTI4OTA2MzMwNDE4.j3BrYZFV_5jMYsPPdWqAvc2OSFjzC1SvWIpZdfrZiyQg.tKC
MES_Logo.jpg?type=w2" alt="missing image" width="317" height="172">

<font size ="4" color="0A0A2A">
Group Members
HTML
Tab Width: 8
Ln 1, Col 1
INS
SCENE - Mozilla Firefox
Search
N SCENE
oject Final Report
N SCÈNE
E E R I N G


Open
index.html
/var/www/html
Save
.group{position:fixed; left:1000px; top:150px;}
</style>
</head>
<body>

<font size ="8" color="08088A">
 MISE EN SCENE

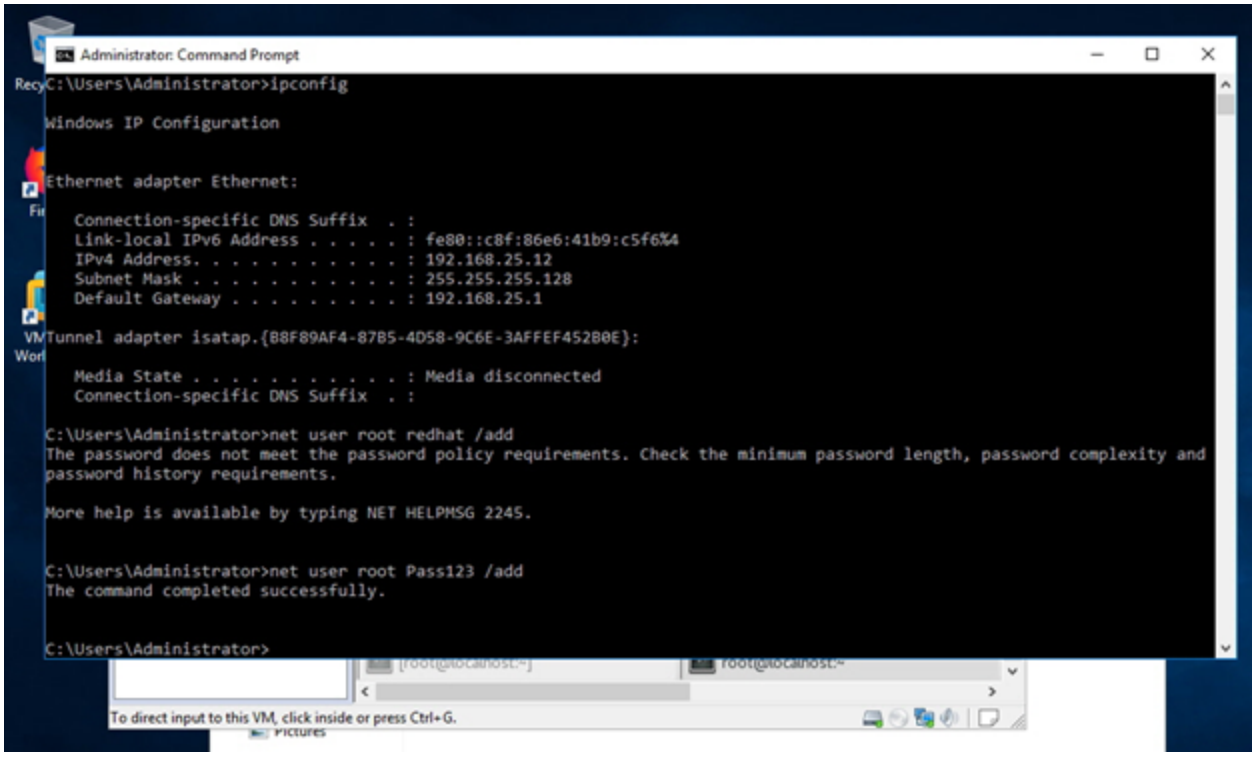
<font size ="5" color="0B0B61">
 2018 Student Project Final Report
<img src="https://postfiles.pstatic.net/MjAxODA2MTRfMjcz/
MDAxNTI4OTA2MzMwNDE4.j3BrYZFV_5jMYsPPdWqAvc2OSFjzC1SvWIpZdfrZiyQg.tKCI
MES_Logo.jpg?type=w2" alt="missing image" width="317" height="172">

<font size ="4" color="0A0A2A">
Group Members
<font size ="2" color="0A0A2A">
Gabriel Kwan
David Lee
Vanessa Luu
Arjay Emata
Noel Lee
Aaron Yang
Johnny Le

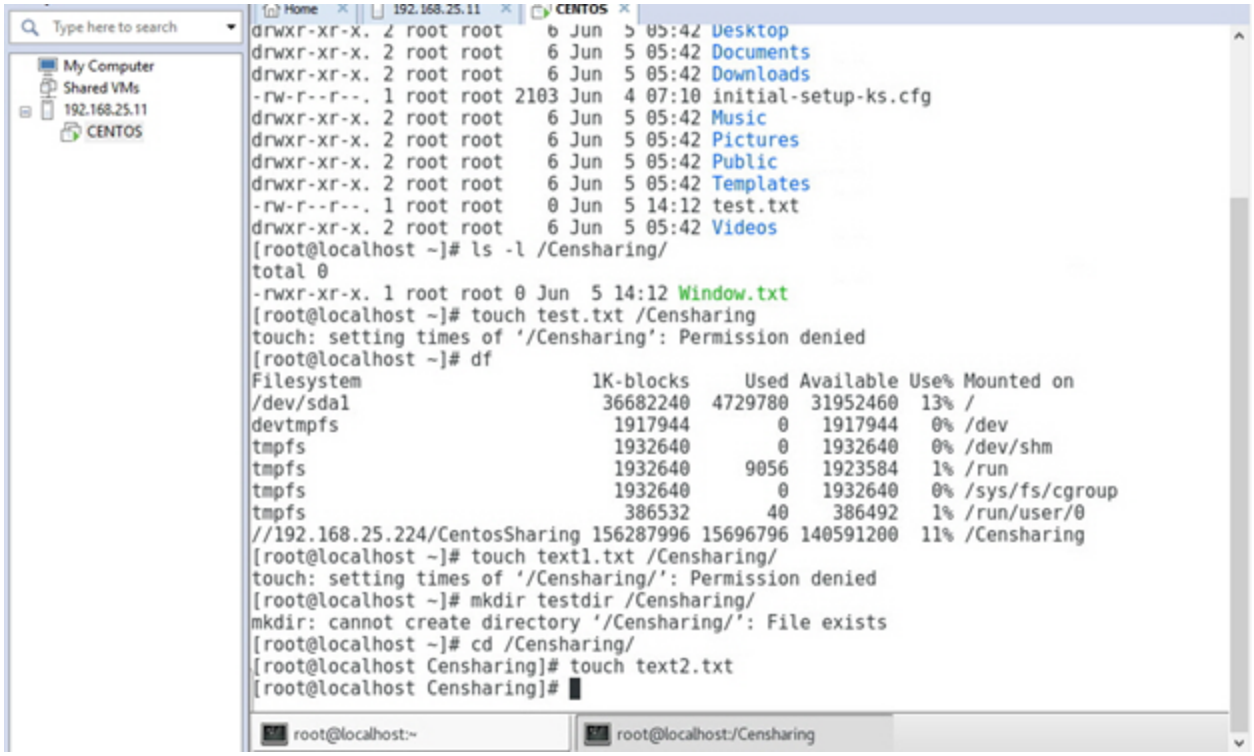
<h2>Links</h2>
Link to Company Report:
Link
</body>
</html>
HTML
Tab Width: 8
Ln 1, Col 1
INS
SCENE - Mozilla Firefox
Search
N SCENE
oject Final Report

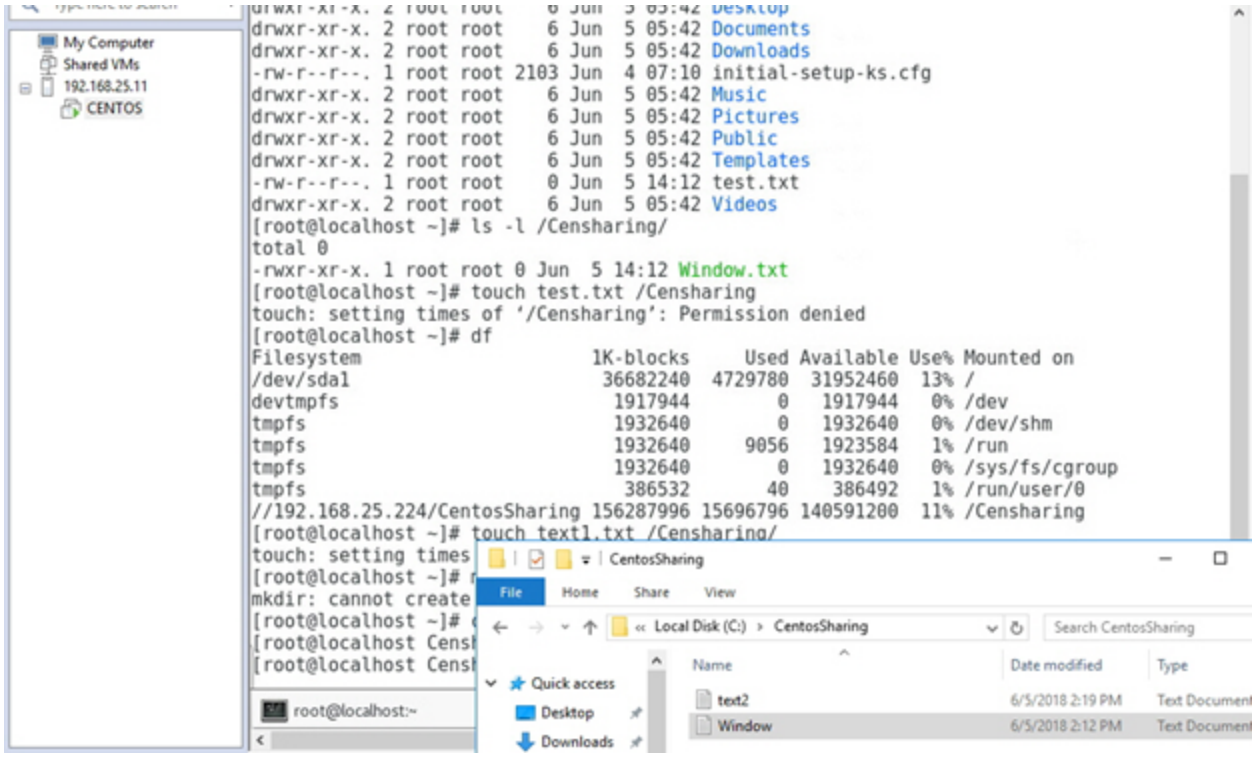
SAMBA Configuration

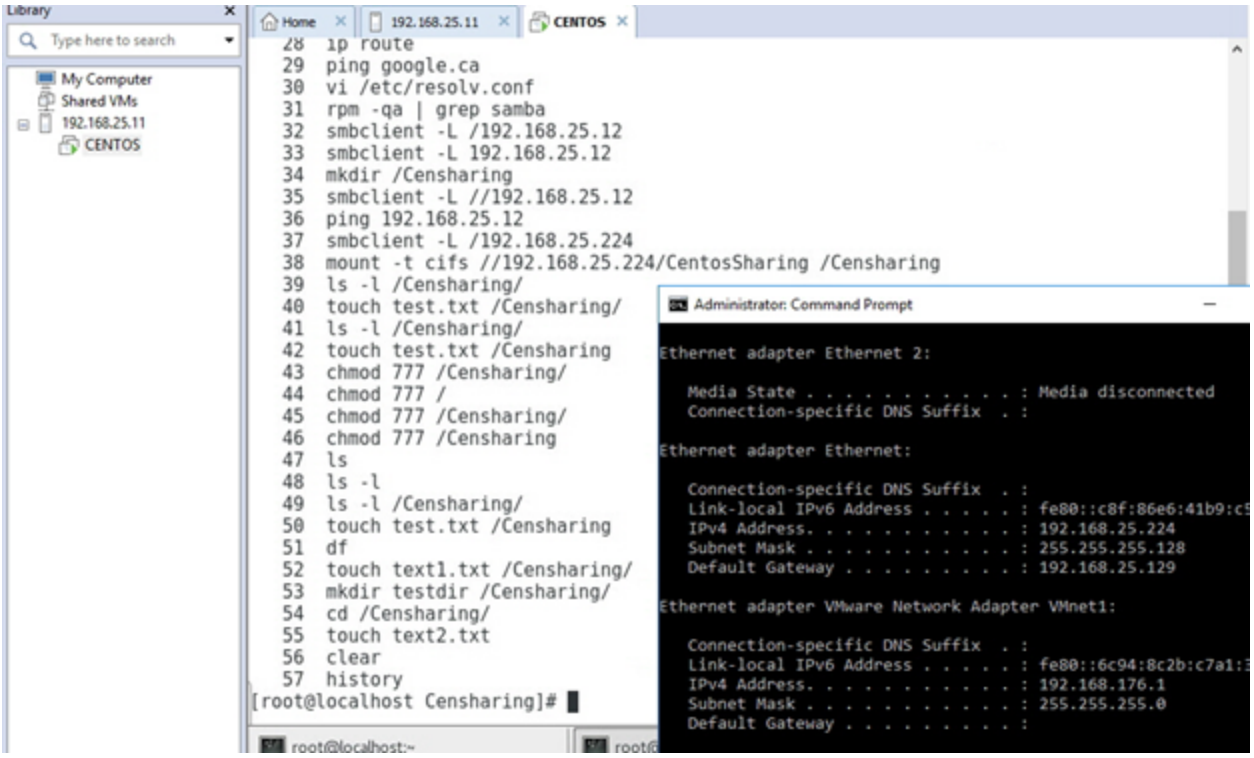
- 1 SAMBA server (Linux to windows)
    1 Create folder in windows for sharing
    2 Gives right permission to the folder
    3 In windows admin cmd, type **'net user root [password] /add'** to add linux user to domain
    4 Check ethernet ip address by typing **'ipconfig'**



5 **'rpm -qa | grep samba'** check samba server
6 **'smbclient -L [local address]'** to connect windows
7 In Linux, **'mkdir [/mountpoint]'** to create mounting folder for sharing
8 Mount the folder by typing **'mount -t cifs [//local address][/window folder] [/mountpoint]'**
(alternative command for specific user)
mount.cifs -o username=[username] //[local address]/location /[mount point]
    - **May require install cifs-utils**
9 **'ls -l [/mountpoint]'** to see the connection


Type here to search
My Computer
Shared VMs
192.168.25.11
CENTOS
Home
192.168.25.11
CENTOS
drwxr-xr-x. 2 root root 6 Jun 5 05:42 Desktop
drwxr-xr-x. 2 root root 6 Jun 5 05:42 Documents
drwxr-xr-x. 2 root root 6 Jun 5 05:42 Downloads
-rw-r--r--. 1 root root 2103 Jun 4 07:10 initial-setup-ks.cfg
drwxr-xr-x. 2 root root 6 Jun 5 05:42 Music
drwxr-xr-x. 2 root root 6 Jun 5 05:42 Pictures
drwxr-xr-x. 2 root root 6 Jun 5 05:42 Public
drwxr-xr-x. 2 root root 6 Jun 5 05:42 Templates
-rw-r--r--. 1 root root 0 Jun 5 14:12 test.txt
drwxr-xr-x. 2 root root 6 Jun 5 05:42 Videos
[root@localhost ~]# ls -l /Censharing/
total 0
-rwxr-xr-x. 1 root root 0 Jun 5 14:12 Window.txt
[root@localhost ~]# touch test.txt /Censharing
touch: setting times of '/Censharing': Permission denied
[root@localhost ~]# df
Filesystem 1K-blocks Used Available Use% Mounted on
/dev/sda1 36682240 4729780 31952460 13% /
devtmpfs 1917944 0 1917944 0% /dev
tmpfs 1932640 0 1932640 0% /dev/shm
tmpfs 1932640 9056 1923584 1% /run
tmpfs 1932640 0 1932640 0% /sys/fs/cgroup
tmpfs 386532 40 386492 1% /run/user/0
//192.168.25.224/CentosSharing 156287996 15696796 140591200 11% /Censharing
[root@localhost ~]# touch text1.txt /Censharing/
touch: setting times of '/Censharing/': Permission denied
[root@localhost ~]# mkdir testdir /Censharing/
mkdir: cannot create directory '/Censharing/': File exists
[root@localhost ~]# cd /Censharing/
[root@localhost Censharing]# touch text2.txt
[root@localhost Censharing]#
root@localhost:~
root@localhost:/Censharing


My Computer
Shared VMs
192.168.25.11
CENTOS
drwxr-xr-x. 2 root root 6 Jun 5 05:42 Documents
drwxr-xr-x. 2 root root 6 Jun 5 05:42 Downloads
-rw-r--r--. 1 root root 2103 Jun 4 07:10 initial-setup-ks.cfg
drwxr-xr-x. 2 root root 6 Jun 5 05:42 Music
drwxr-xr-x. 2 root root 6 Jun 5 05:42 Pictures
drwxr-xr-x. 2 root root 6 Jun 5 05:42 Public
drwxr-xr-x. 2 root root 6 Jun 5 05:42 Templates
-rw-r--r--. 1 root root 0 Jun 5 14:12 test.txt
drwxr-xr-x. 2 root root 6 Jun 5 05:42 Videos
[root@localhost ~]# ls -l /Censharing/
total 0
-rwxr-xr-x. 1 root root 0 Jun 5 14:12 Window.txt
[root@localhost ~]# touch test.txt /Censharing
touch: setting times of '/Censharing': Permission denied
[root@localhost ~]# df
Filesystem 1K-blocks Used Available Use% Mounted on
/dev/sda1 36682240 4729780 31952460 13% /
devtmpfs 1917944 0 1917944 0% /dev
tmpfs 1932640 0 1932640 0% /dev/shm
tmpfs 1932640 9056 1923584 1% /run
tmpfs 1932640 0 1932640 0% /sys/fs/cgroup
tmpfs 386532 40 386492 1% /run/user/0
//192.168.25.224/CentosSharing 156287996 15696796 140591200 11% /Censharing
[root@localhost ~]# touch text1.txt /Censharing/
touch: setting times
[root@localhost ~]#
mkdir: cannot create
[root@localhost ~]#
[root@localhost Censh
[root@localhost Censh
root@localhost:~
CentosSharing
File
Home
Share
View
Local Disk (C:) › CentosSharing
Search CentosSharing
Quick access
Desktop
Downloads
Name
Date modified
Type
text2
6/5/2018 2:19 PM
Text Document
Window
6/5/2018 2:12 PM
Text Document


Library
Type here to search
My Computer
Shared VMs
192.168.25.11
CENTOS
Home
192.168.25.11
CENTOS
28 ip route
29 ping google.ca
30 vi /etc/resolv.conf
31 rpm -qa | grep samba
32 smbclient -L /192.168.25.12
33 smbclient -L 192.168.25.12
34 mkdir /Censharing
35 smbclient -L //192.168.25.12
36 ping 192.168.25.12
37 smbclient -L /192.168.25.224
38 mount -t cifs //192.168.25.224/CentosSharing /Censharing
39 ls -l /Censharing/
40 touch test.txt /Censharing/
41 ls -l /Censharing/
42 touch test.txt /Censharing
43 chmod 777 /Censharing/
44 chmod 777 /
45 chmod 777 /Censharing/
46 chmod 777 /Censharing
47 ls
48 ls -l
49 ls -l /Censharing/
50 touch test.txt /Censharing
51 df
52 touch text1.txt /Censharing/
53 mkdir testdir /Censharing/
54 cd /Censharing/
55 touch text2.txt
56 clear
57 history
[root@localhost Censharing]#
Administrator: Command Prompt
Ethernet adapter Ethernet 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::c8f:86e6:41b9:c
IPv4 Address. . . . . : 192.168.25.224
Subnet Mask . . . . . : 255.255.255.128
Default Gateway . . . . . : 192.168.25.129
Ethernet adapter VMware Network Adapter VMnet1:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::6c94:8c2b:c7a1:
IPv4 Address. . . . . : 192.168.176.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

DHCP Server

1. Installing DHCP service.

- **yum install dhcp**

2. Disable dnsmasq for preventing collision between dnsmasq and DHCP service.

- **ps -ef | grep dnsmasq**

nobody 1909 1 0 12:05 ? 00:00:00 /sbin/dnsmasq --conf-file=/var/lib/libvirt/dnsmasq/default.conf

root 2627 2503 0 12:12 pts/0 00:00:00 grep --color=auto dnsmasq

- **kill -9 1909**

- **systemctl disable dnsmasq**

3. Once installation is complete configure static ip

4. Configure dhcpd.conf file and make them to lease ip address for clients.

In the configuration file, we add one section per one network. For each section, we set-up network address with the subnet mask. we used option router as clients default-gateway, range is for the setting up range pool to lease, default-lease-time & max-lease-time for the leasing time. Also for the main section of each department, we set-up option domain-name, option domain-name-servers for DNS.

- **gedit /etc/dhcp/dhcpd.conf** (command for configure dhcp config file)

---------- here is our dhcpd.conf file for the primary DHCP Server

```
# DHCP Server Configuration file.
#Incoming from ISP


subnet 192.168.25.0 netmask 255.255.255.128 {
        option routers 192.168.25.126;
        range 192.168.25.1 192.168.25.125;
        default-lease-time 86400;
        max-lease-time 172800;
```

```
}

#Engineering
subnet 172.25.0.0 netmask 255.255.255.192 {
        option routers 172.25.0.62;
        default-lease-time 86400;
        max-lease-time 172800;
        option domain-name "MesEInc.com";
        option domain-name-servers 172.25.3.97, 172.25.3.98;
        range 172.25.0.1 172.25.0.61;
}

subnet 172.25.1.0 netmask 255.255.255.192 {
        option routers 172.25.1.62;
        default-lease-time 86400;
        max-lease-time 172800;
        option domain-name "MesEInc.com";
        option domain-name-servers 172.25.3.130, 172.25.3.97;
        range 172.25.1.1 172.25.1.61;
}

subnet 172.25.2.0 netmask 255.255.255.192 {
        option routers 172.25.2.62;
        default-lease-time 86400;
        max-lease-time 172800;
        option domain-name "MesEInc.com";
        option domain-name-servers 172.25.3.161, 172.25.3.97;
        range 172.25.2.1 172.25.2.61;

}

#Marketing
subnet 172.25.0.64 netmask 255.255.255.192 {
        option routers 172.25.0.126;
        default-lease-time 86400;
        max-lease-time 172800;
        option domain-name "MesEInc.com";
        option domain-name-servers 172.25.3.97, 172.25.3.98;
        range 172.25.0.65 172.25.0.125;
}

subnet 172.25.1.64 netmask 255.255.255.192 {
```

```
        option routers 172.25.1.126;
        default-lease-time 86400;
        max-lease-time 172800;
        option domain-name "MesEInc.com";
        option domain-name-servers 172.25.3.130;
        failover peer “failover-partner”;
        range 172.25.1.65 172.25.1.125;
}

subnet 172.25.2.64 netmask 255.255.255.192 {
        option routers 172.25.2.126;
        default-lease-time 86400;
        max-lease-time 172800;
        option domain-name "MesEInc.com";
        option domain-name-servers 172.25.3.161, 172.25.3.97;
        failover peer “failover-partner”;
        range 172.25.2.65 172.25.2.125;
}

#IT
subnet 172.25.0.128 netmask 255.255.255.192 {
        option routers 172.25.0.190;
        default-lease-time 86400;
        max-lease-time 172800;
        option domain-name "MesEInc.com";
        option domain-name-servers 172.25.3.97, 172.25.3.98;
        range 172.25.0.129 172.25.0.189;
}

subnet 172.25.1.128 netmask 255.255.255.192 {
        option routers 172.25.1.190;
        default-lease-time 86400;
        max-lease-time 172800;
        option domain-name "MesEInc.com";
        option domain-name-servers 172.25.3.130;
        range 172.25.1.129 172.25.1.189;
}

subnet 172.25.2.128 netmask 255.255.255.192 {
        option routers 172.25.2.190;
        range 172.25.2.129 172.25.2.189;
        default-lease-time 86400;
```

```
        max-lease-time 172800;
        option domain-name "MesEInc.com";
        option domain-name-servers 172.25.3.161, 172.25.3.97;
        range 172.25.2.129 172.25.2.189;
}

#HR
subnet 172.25.0.192 netmask 255.255.255.192 {
         option routers 172.25.0.254;
        default-lease-time 86400;
         max-lease-time 172800;
        option domain-name "MesEInc.com";
        option domain-name-servers 172.25.3.97, 172.25.3.97;
        range 172.25.0.193 172.25.0.253;
}

subnet 172.25.1.192 netmask 255.255.255.192 {
        option routers 172.25.1.254;
        default-lease-time 86400;
        max-lease-time 172800;
        option domain-name "MesEInc.com";
        option domain-name-servers 172.25.3.130, 172.25.3.97;
        failover peer “failover-partner”;
        range 172.25.1.193 172.25.1.253;

}

subnet 172.25.2.192 netmask 255.255.255.192 {
        option routers 172.25.2.254;
        default-lease-time 86400;
        max-lease-time 172800;
        option domain-name "MesEInc.com";
        option domain-name-servers 172.25.3.161, 172.25.3.97;
        range 172.25.2.193 172.25.2.253;

}

#Guest
subnet 172.25.3.192 netmask 255.255.255.224 {
        option routers 172.25.0.222;
        default-lease-time 86400;
        max-lease-time 172800;
```

```
        option domain-name "MesEInc.com";
        option domain-name-servers 172.25.3.97, 172.25.3.97;
        range 172.25.3.193 172.25.3.221;

}

subnet 172.25.3.224 netmask 255.255.255.240 {
        option routers 172.25.0.238;
        range 172.25.3.225 172.25.3.237;
        default-lease-time 86400;
        max-lease-time 172800;
        option domain-name "MesEInc.com";
        option domain-name-servers 172.25.3.130, 172.25.3.97;

}

subnet 172.25.3.240 netmask 255.255.255.248 {
        option routers 172.25.0.246;
        default-lease-time 86400;
        max-lease-time 172800;
        option domain-name-servers 172.25.3.161, 172.25.3.97;
        range 172.25.3.241 172.25.3.245;
}



-----------------------------------------------------------------

----------definition for primary fail-over, goes in top of the config of primary dhcpd.conf
Failover peer failover-partner {
        primary;
        address dhcp1.MesEinc.com;
        peer address dhcp2.MesEinc.com;
        max-response-delay 60;
        mclt 3600;
        split 128;
        max-unacked-updates 10;
        Load balance max seconds 3;

}
```

--------definition for secondary fail-over. Goes on top of the config of primary dhcpd.conf--------

```
 DHCP Server Configuration file.
Incoming from ISP
failover peer failover-partner {
        secondary;
        address dhcp2.meseinc.com;
        peer address dhcp1.meseinc.com;
        max-response-delay 60;
        max-unacked-updates 10;
        load balance max seconds 3;

}
--------- Format for failover subnets-----------------
# The range goes within a pool and failover peer is specified. Use the failover peer
# “failover-partner”
# defined in the above section
#Engineering
subnet 172.25.0.0 netmask 255.255.255.192 {
        option routers 172.25.0.62;
        default-lease-time 86400;
        max-lease-time 172800;
        option domain-name "MesEInc.com";
         option domain-name-servers 172.25.3.97, 172.25.3.98;
   Pool {
        Failover peer “failover-partner”;
        range 172.25.0.1 172.25.0.61;
        }
}
```

-------Authentication for failover, placed at the end of each of the dhcpd.conf----------

```
 Authentication
omapi-port 7911;
omapi-key omapi_key;
Key ompai_key {
        Algorithm hmac-md5;
        Secret test==;
}
```

---

5. Restart dhcp service

- **systemctl restart dhcpd**

6. verify dhcp service is running, and check it runs without any problem (service should now say active)

- **systemctl status dhcpd**

7. Make dhcp service always running.(after boot)

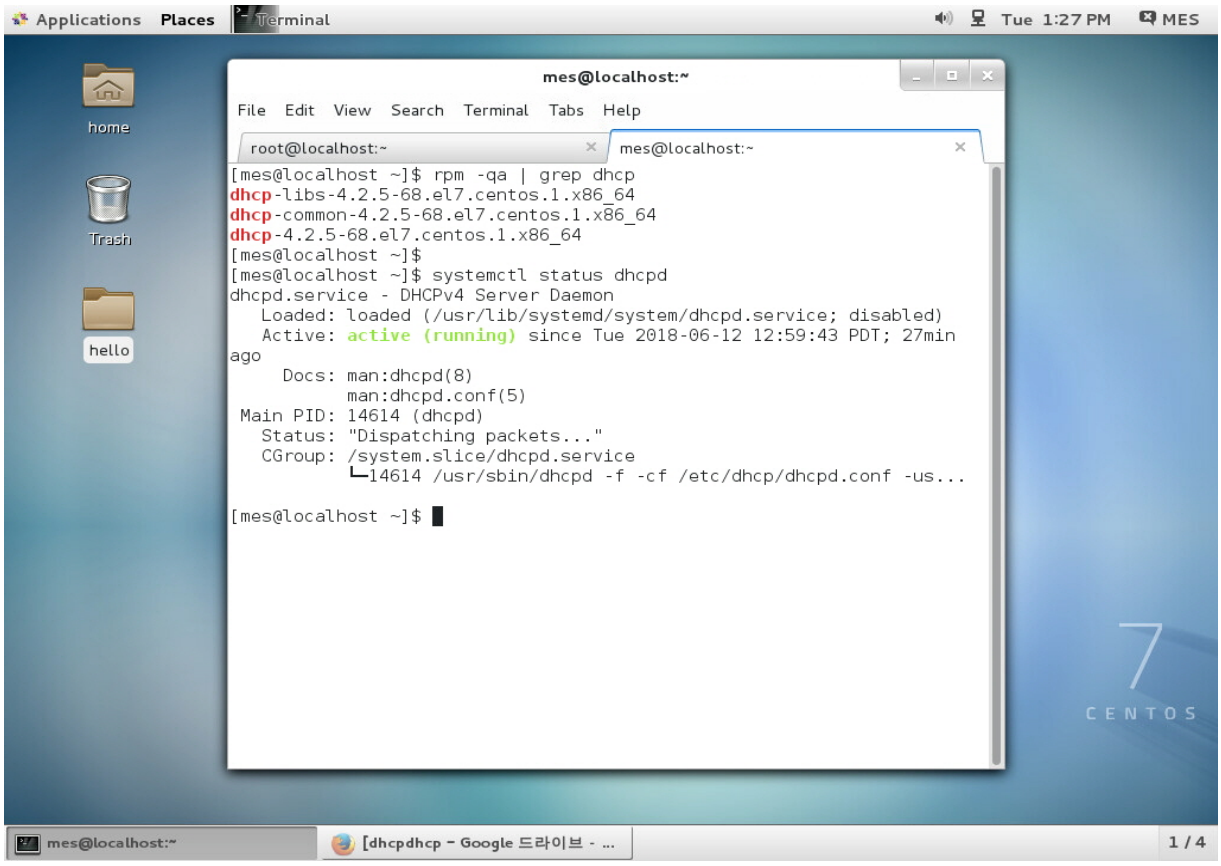
- **systemctl enable dhcpd**

8. Disable firewall for stop blocking lease.

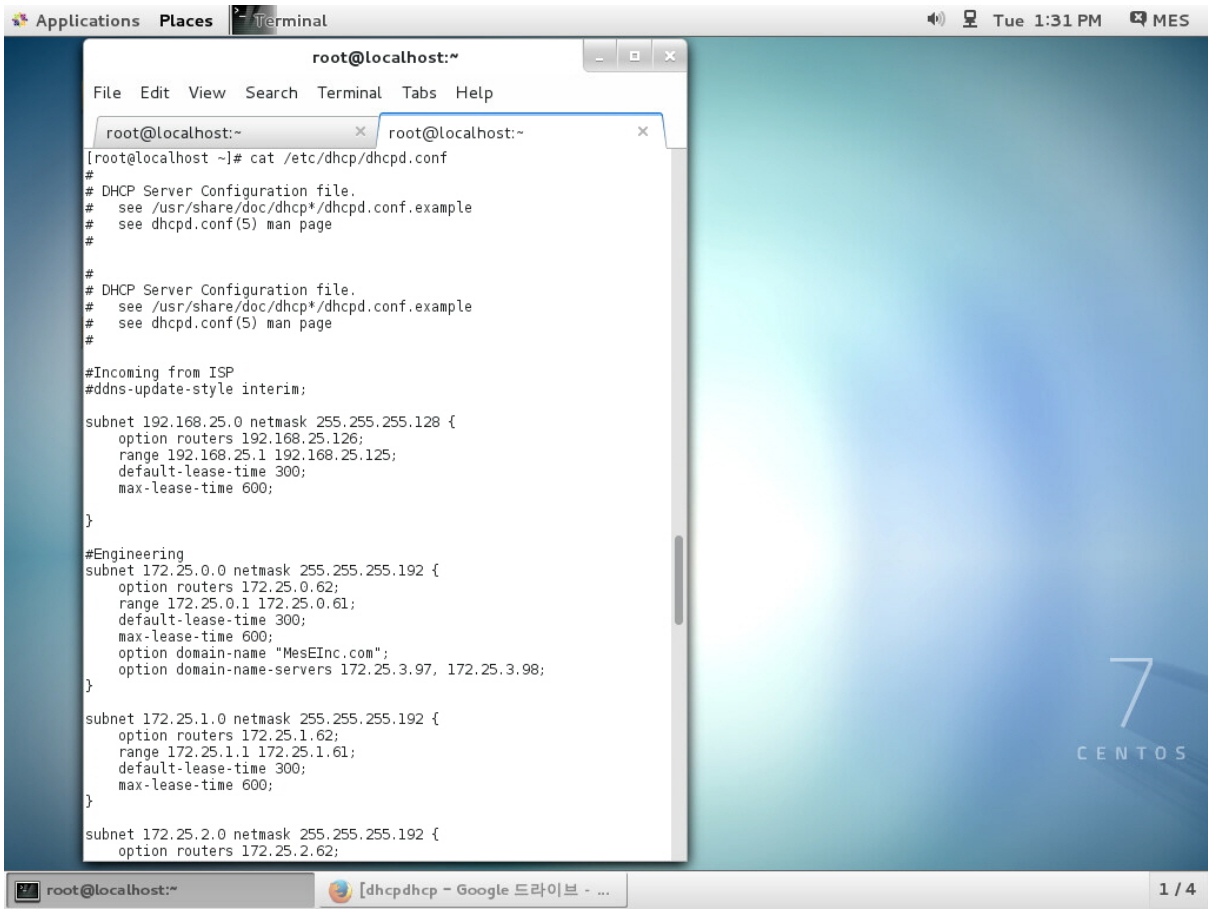
- **systemctl stop firewalld**

9. Verify server lease ip addresses, and client receiving address.

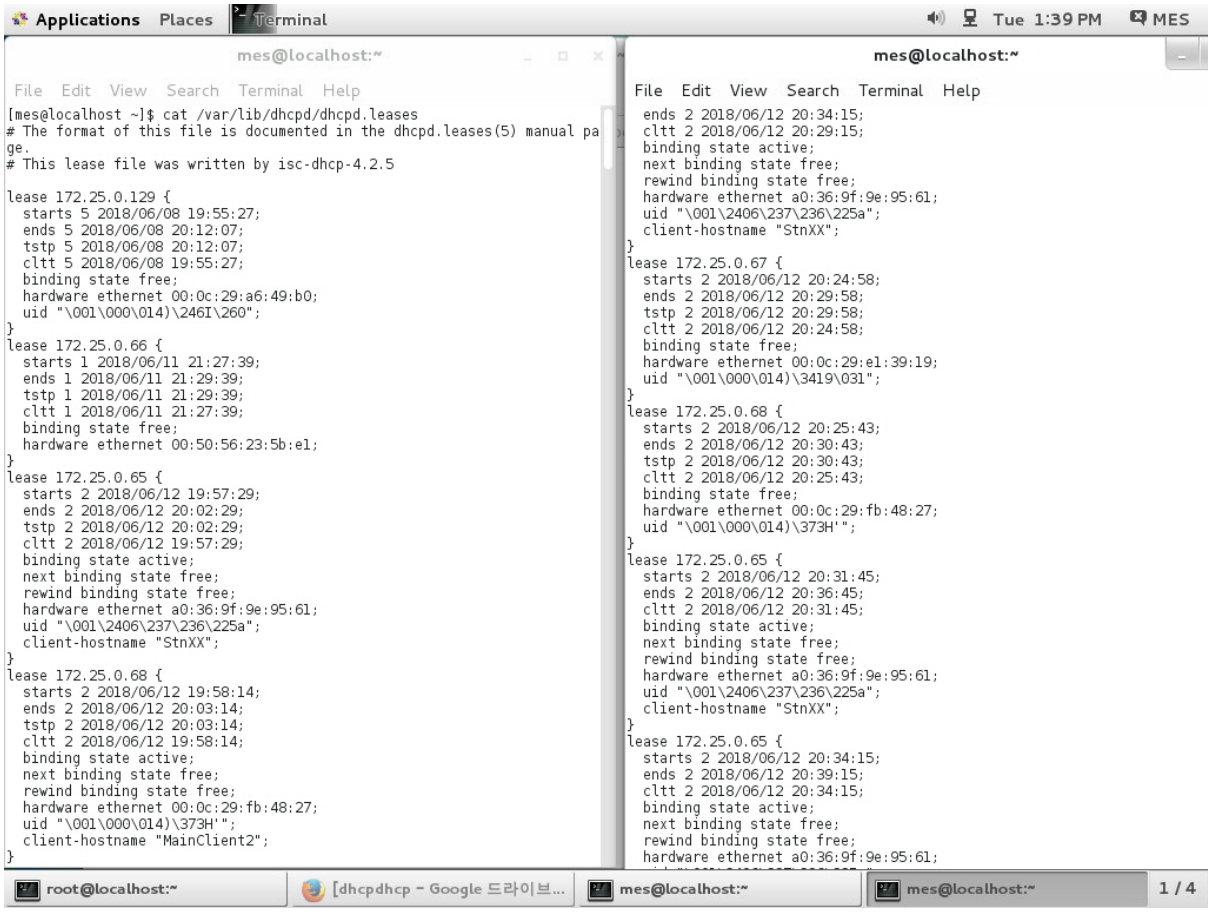
- **cat /var/lib/dhcpd/dhcpd.leases**



Screenshot of checking DHCP service.



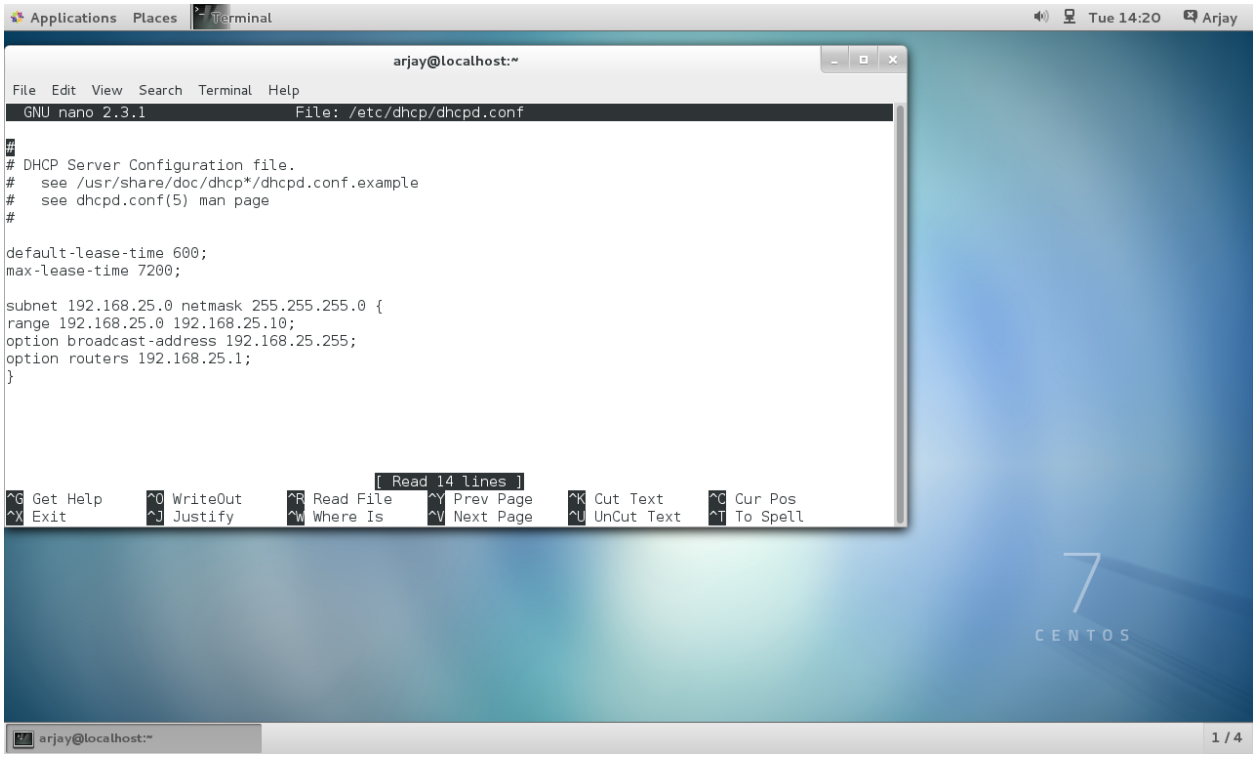
First page of DHCP config file



lease database

2. Configuring DHCP on Client Server

4.1 Once DHCP is running on the main server go to the client server and click the network settings icon and switch the ethernet interfaces to on. The interfaces should now gain an address within the range specified in the DHCP config file.


Applications Places Terminal
Tue 14:20 Arjay
arjay@localhost:~
File Edit View Search Terminal Help
GNU nano 2.3.1 File: /etc/dhcp/dhcpd.conf
#
DHCP Server Configuration file.
see /usr/share/doc/dhcp*/dhcpd.conf.example
see dhcpd.conf(5) man page
#
default-lease-time 600;
max-lease-time 7200;
subnet 192.168.25.0 netmask 255.255.255.0 {
range 192.168.25.0 192.168.25.10;
option broadcast-address 192.168.25.255;
option routers 192.168.25.1;
}
[Read 14 lines]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
7
CENTOS
arjay@localhost:~
1 / 4

VSFTPD Installation and Configuration

1 . Installation of VSFTPD

1.1- Install vsftpd service with **yum install vstpd**

1.2 - Start service manually then enable with **systemctl start vsftpd** and **systemctl enable vsftpd**.

1.3 - To allow access to the FTP services you must open port 21 with following commands:

firewall-cmd --zone=public --permanent --add-port=21/tcp
firewall-cmd --zone=public --permanent --add-service=ftp
firewall-cmd --reload

1.4 - Configure /etc/vsftpd/vsftpd.conf file to change anonymous_enable=NO

1.5 - Configure /etc/vsftpd.userlist file with following:

userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
userlist_deny=NO
chroot_local_user=YES
allow_writeable_chroot=YES

1.6 - Allow SELinux boolean to allow FTP to read files in a user's home directory with command:

semanage boolean -m ftpd_full_access --on

1.7 - Restart service with **systemctl restart vsftpd**

2. Testing FTP Server

2.1 - Add FTP user with command & change password:

Useradd -m -c "Gabriel Kwan, CEO" -s /bin/bash Gabriel
Passwd Gabriel

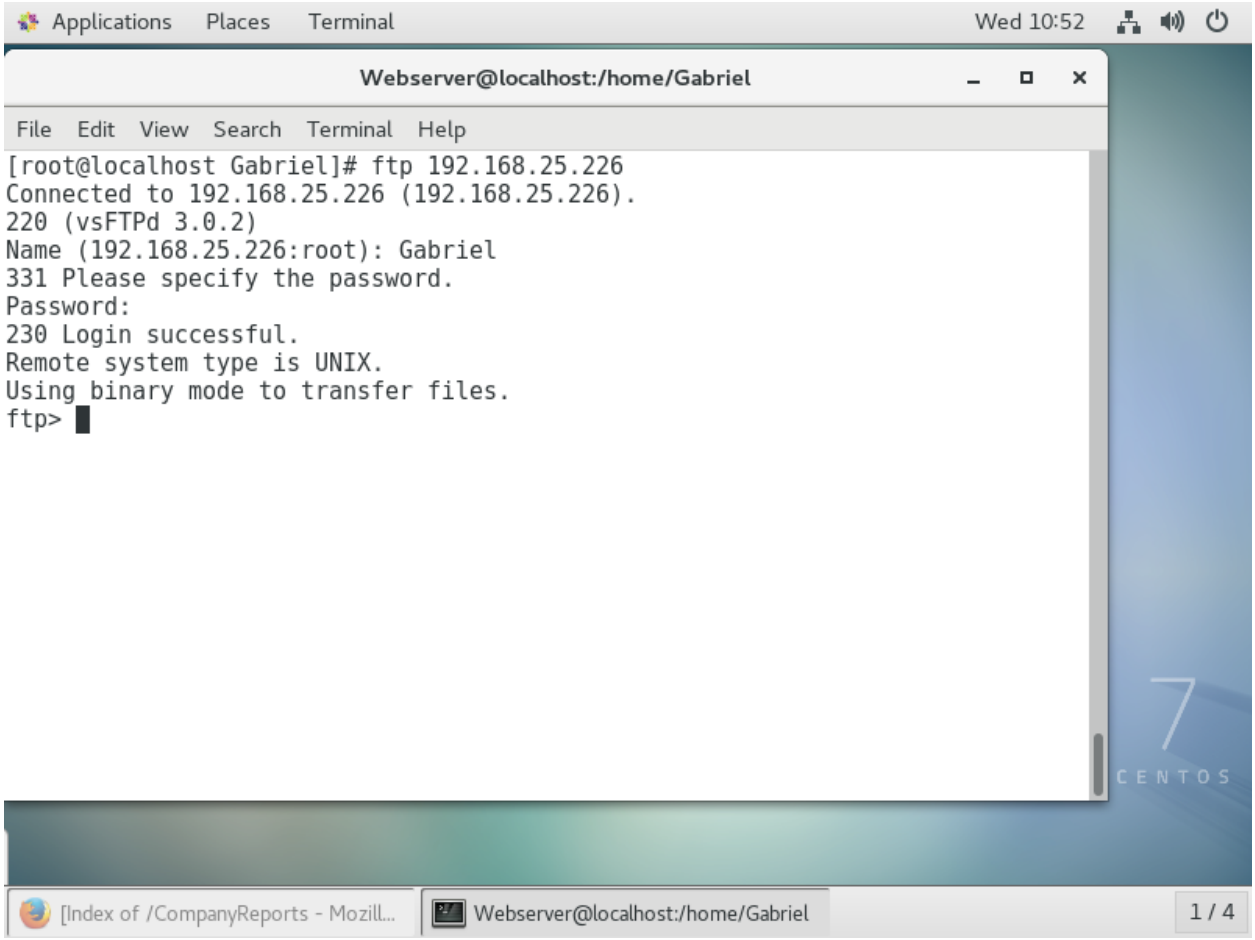
2.2 - Add user to /etc/vsftpd.userlist file:

Echo "Gabriel" | tee -a /etc/vsftpd.userlist

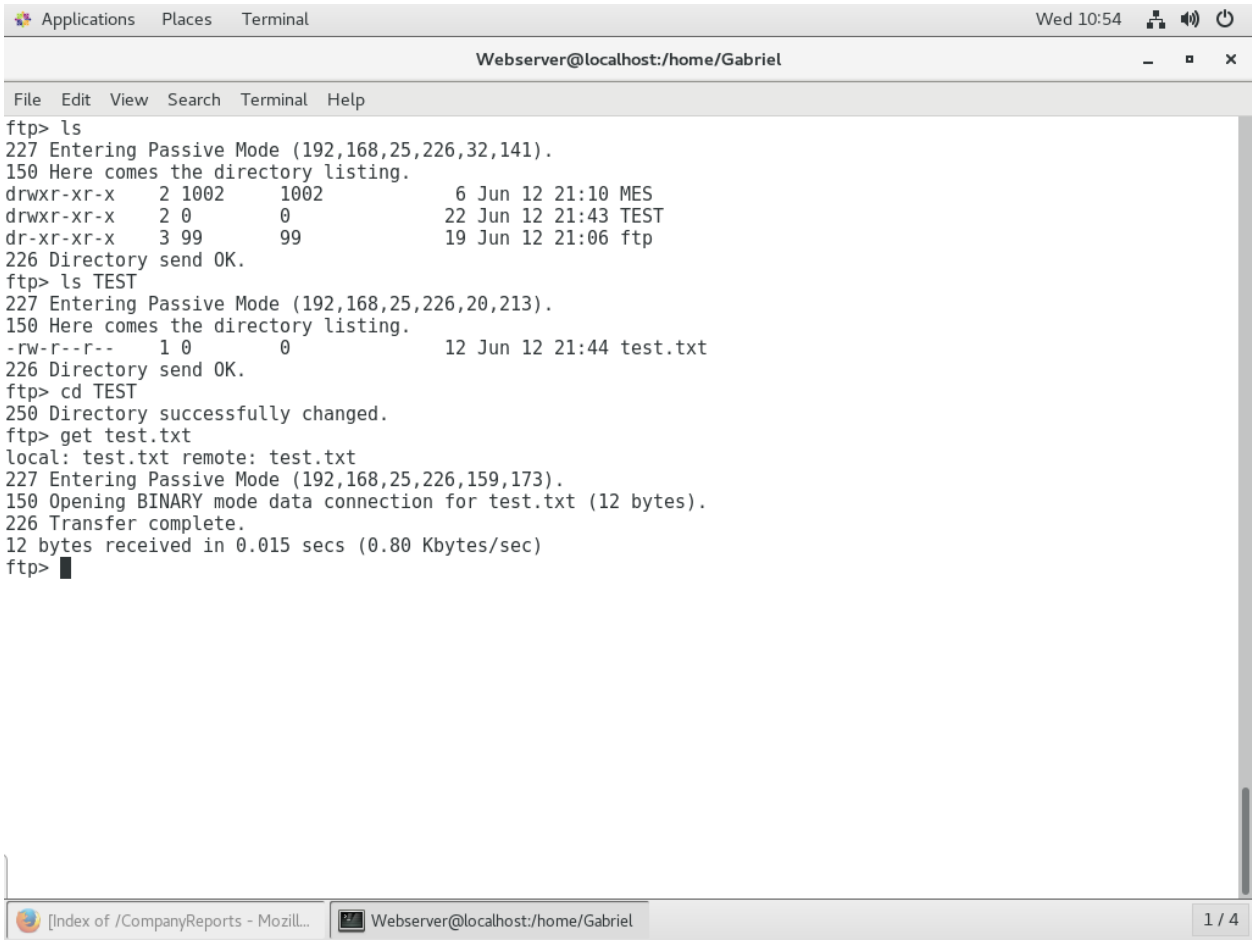
3. Connect to FTP server

3.1 ftp [ip address]

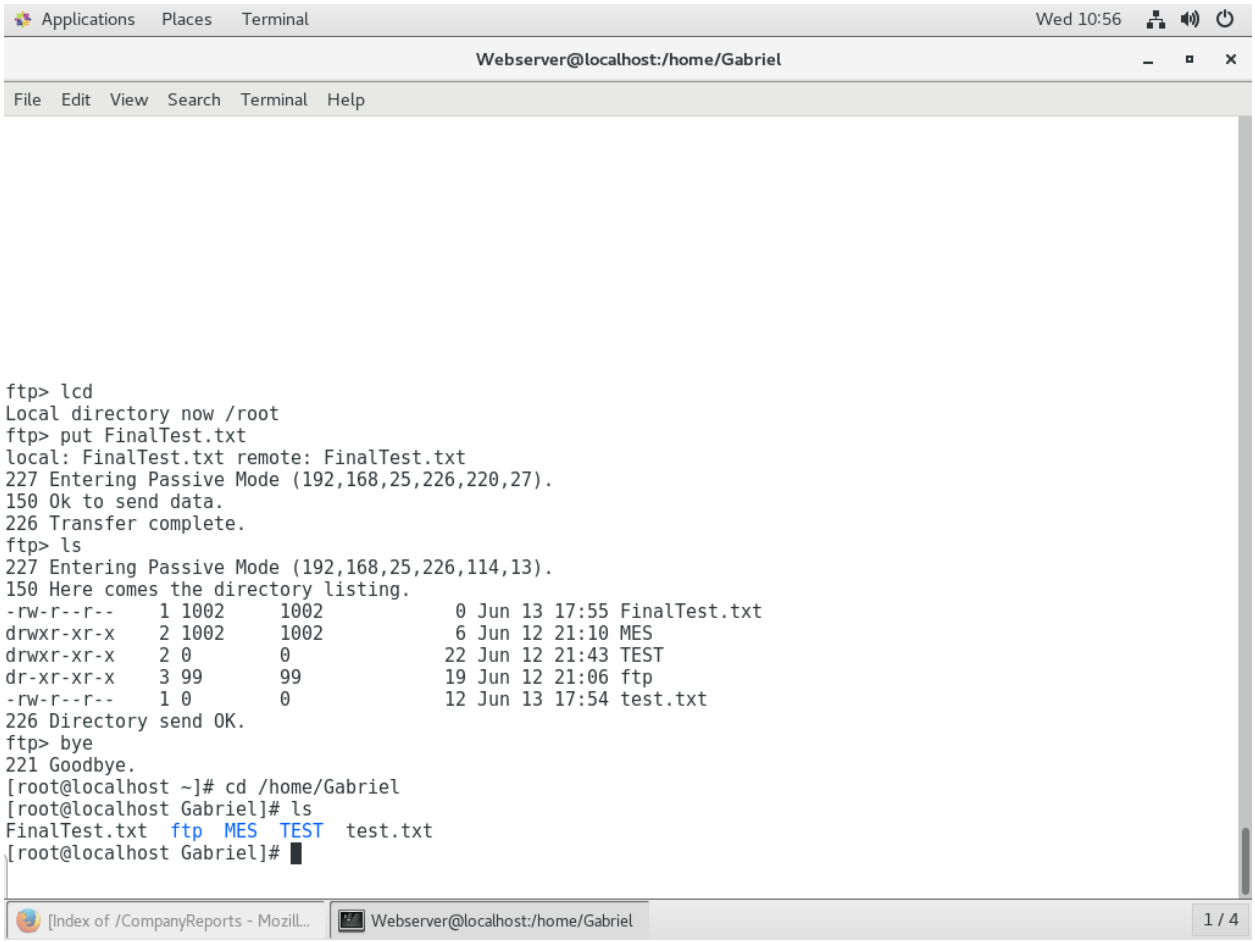
If correctly set up should look like the following:



4. Transfer files to and from Local & Remote Servers.
    4.1 - Use get command once in ftp server to transfer a file from the remote system to the local system's current directory.



4.2 - use put command to transfer a file from the local system to a directory on the remote system.


Applications Places Terminal
Wed 10:56
Webserver@localhost:/home/Gabriel
File Edit View Search Terminal Help
ftp> lcd
Local directory now /root
ftp> put FinalTest.txt
local: FinalTest.txt remote: FinalTest.txt
227 Entering Passive Mode (192,168,25,226,220,27).
150 Ok to send data.
226 Transfer complete.
ftp> ls
227 Entering Passive Mode (192,168,25,226,114,13).
150 Here comes the directory listing.
-rw-r--r-- 1 1002 1002 0 Jun 13 17:55 FinalTest.txt
drwxr-xr-x 2 1002 1002 6 Jun 12 21:10 MES
drwxr-xr-x 2 0 0 22 Jun 12 21:43 TEST
dr-xr-xr-x 3 99 99 19 Jun 12 21:06 ftp
-rw-r--r-- 1 0 0 12 Jun 13 17:54 test.txt
226 Directory send OK.
ftp> bye
221 Goodbye.
[root@localhost ~]# cd /home/Gabriel
[root@localhost Gabriel]# ls
FinalTest.txt ftp MES TEST test.txt
[root@localhost Gabriel]#
[Index of /CompanyReports - Mozill...
Webserver@localhost:/home/Gabriel
1 / 4

Syslog Configuration

Steps:
1. Create directory and file to save the logs
- **cd /var/log/**
- **mkdir ciscolog**
- **cd /var/log/ciscolog**
- **touch logs**

2. Configure main config file of syslog
- **gedit /etc/rsyslog.conf**

----------on the rsyslog.conf file
remove #s in UDP,TCP syslog reception

##RULES## part, add line

local.* /var/log/ciscolog/log

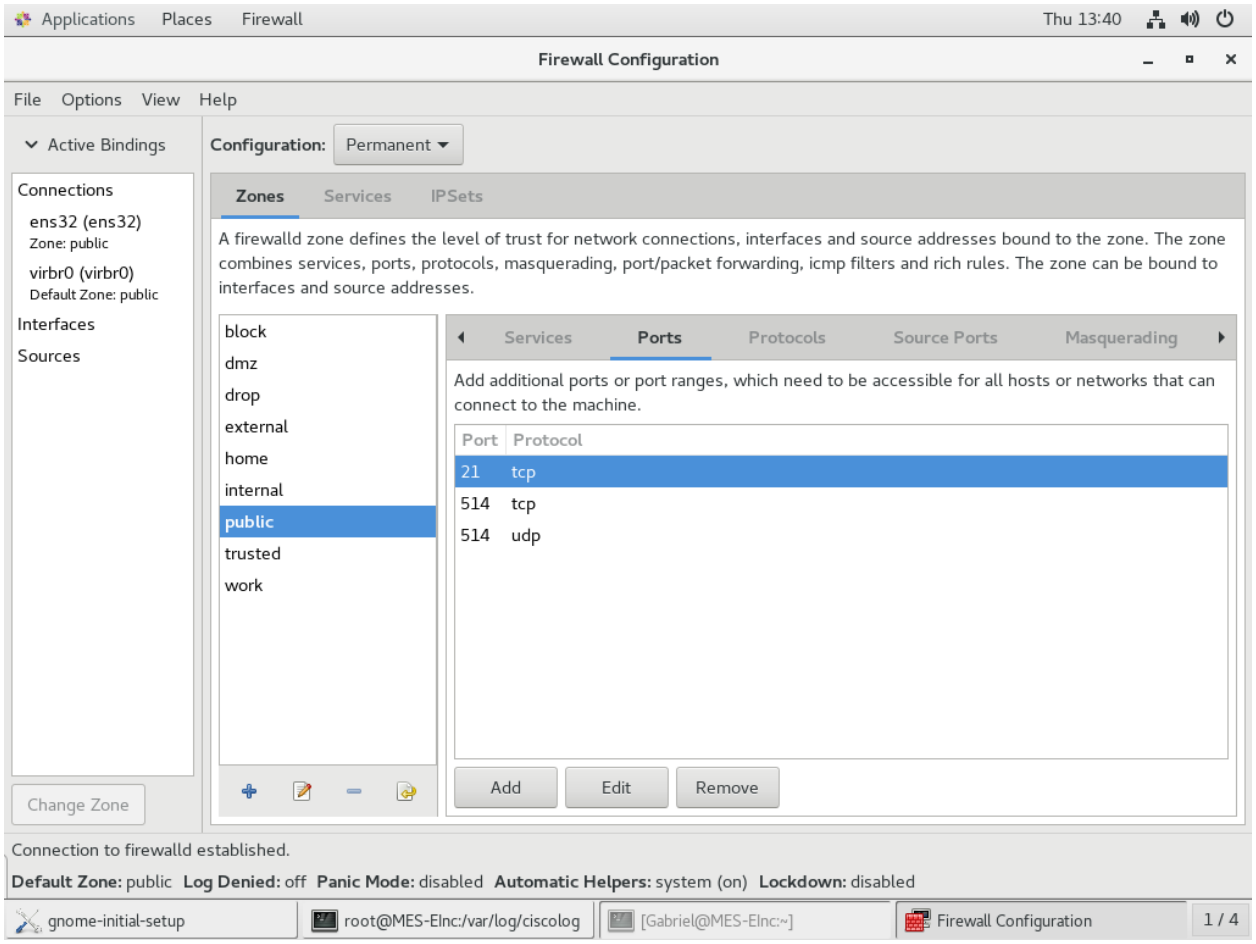
begin forwarding rule##
under the #*.* @@remote-host:514, add the address of device which wants to save the log, and write default port number after address.

. @@ 172.23.3.1:514
----------save the configuration

3. Configure firewall to stop blocking the ports

- **firewall-config**

Change configuration Runtime to Permanent.
In the port tab, add tcp & udp default ports.(514)



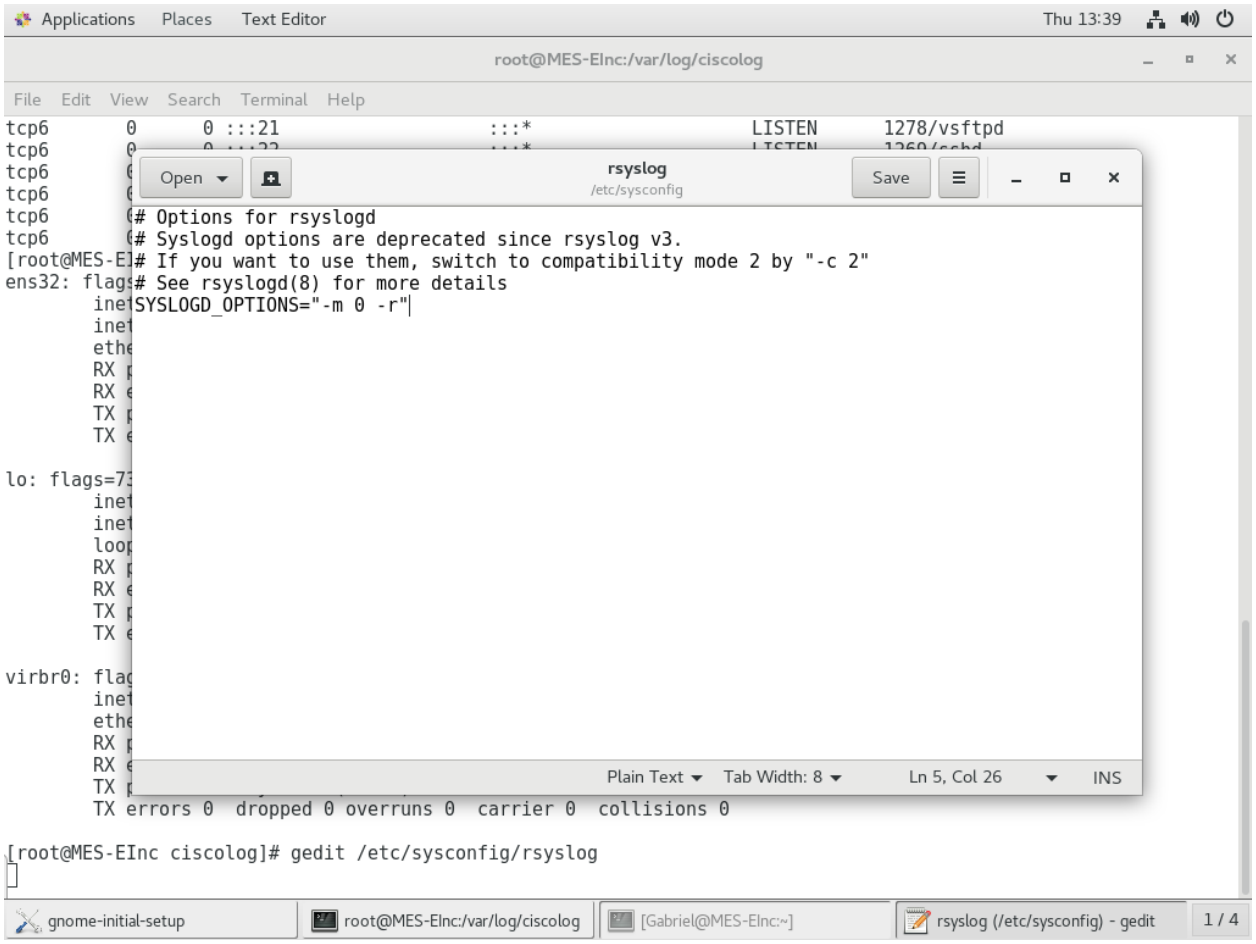
4. configure remote syslog

- **gedit /etc/sysconfig/rsyslog**

----------on the rsyslog file

#Add line to make remote accessible.

SYSLOGD_OPTIONS="-m 0 -r"



5. restart syslog service

- **systemctl restart rsyslog**

6. On the cisco device, type command to check the logs.

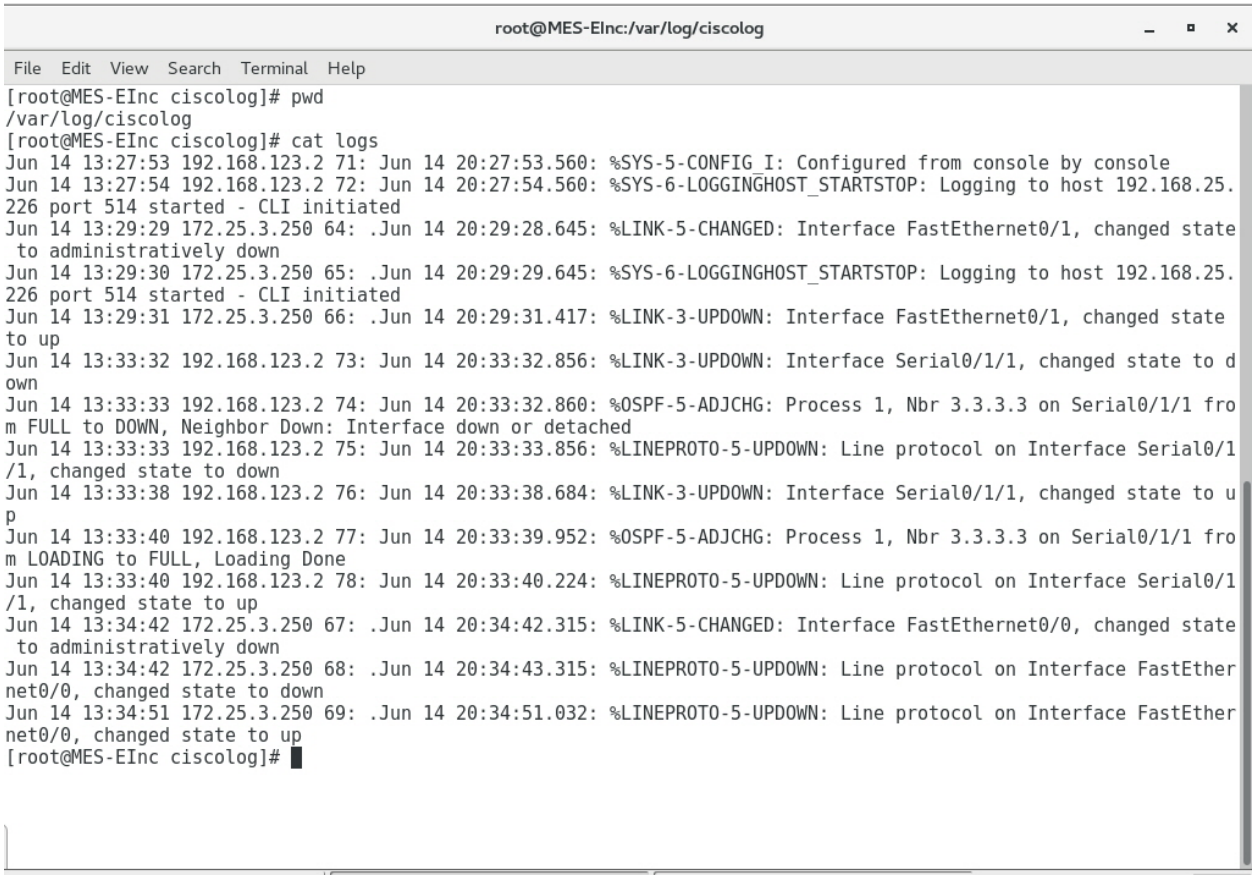
- (config)# **logging on**
- (config)# **logging 192.168.25.226** (web-server address)
- (config)# **logging facility local2**
- (config)# **logging trap debugging**
- (config)# **logging trap informational**

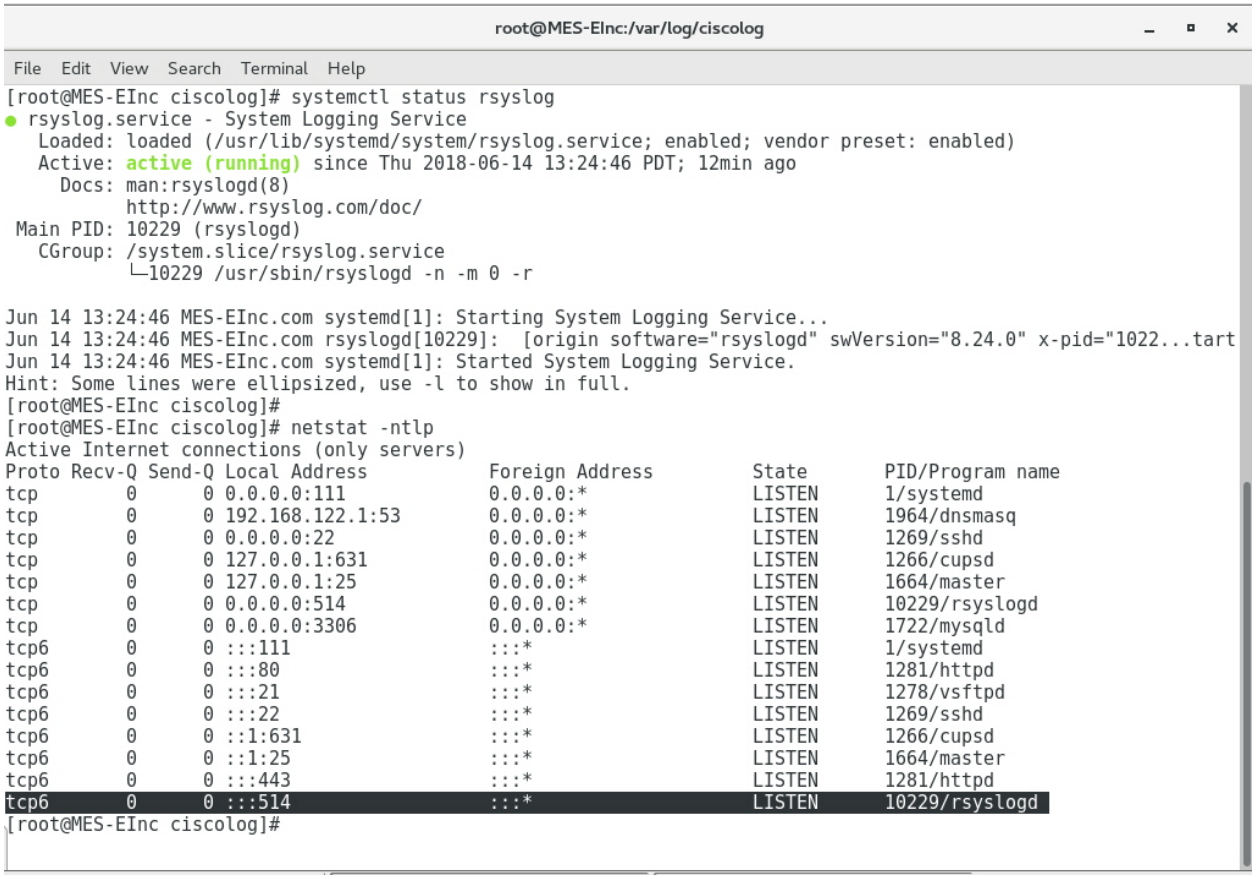
7. Turn off the port on the cisco device (turn on after off)

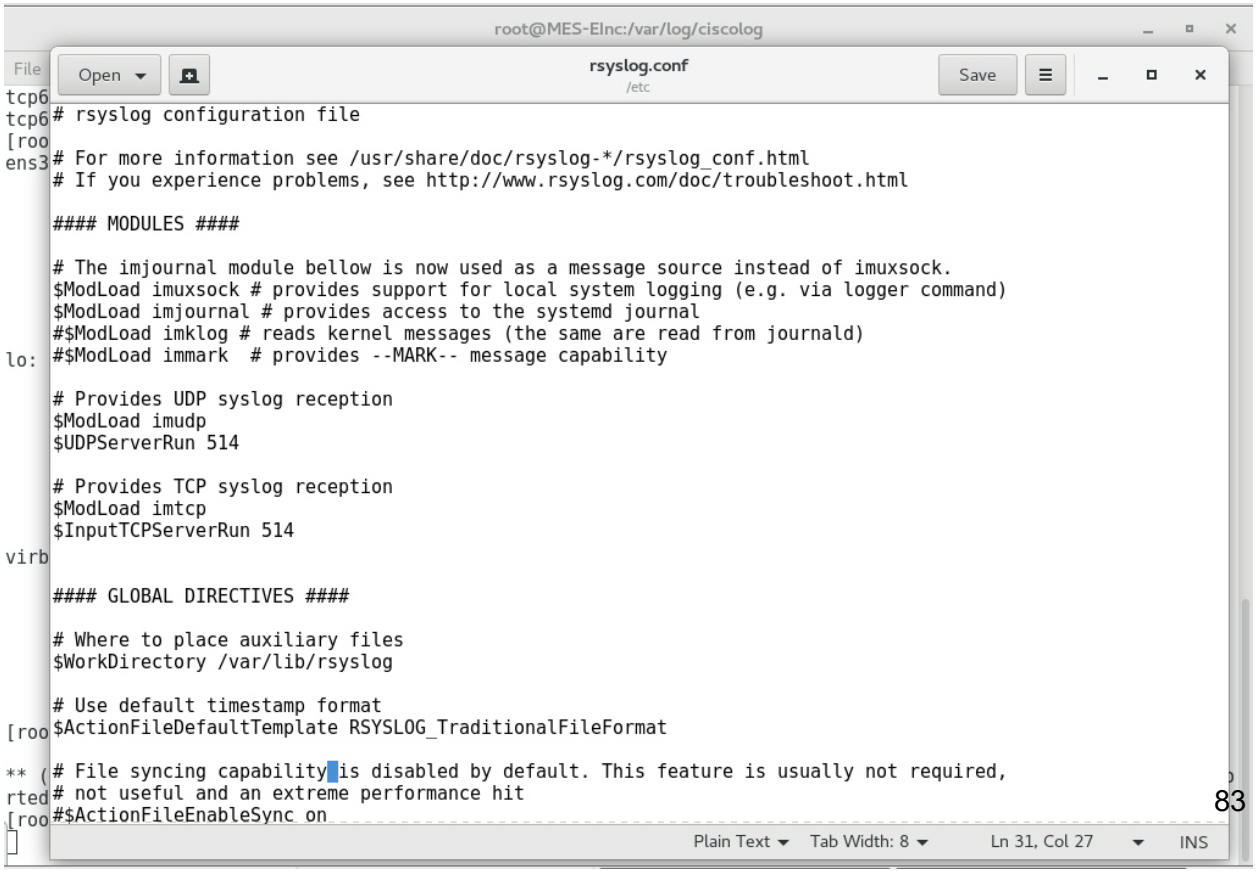
- (config)# **int f0/1**
- (config)# **shut**
- (config)# **no shut**

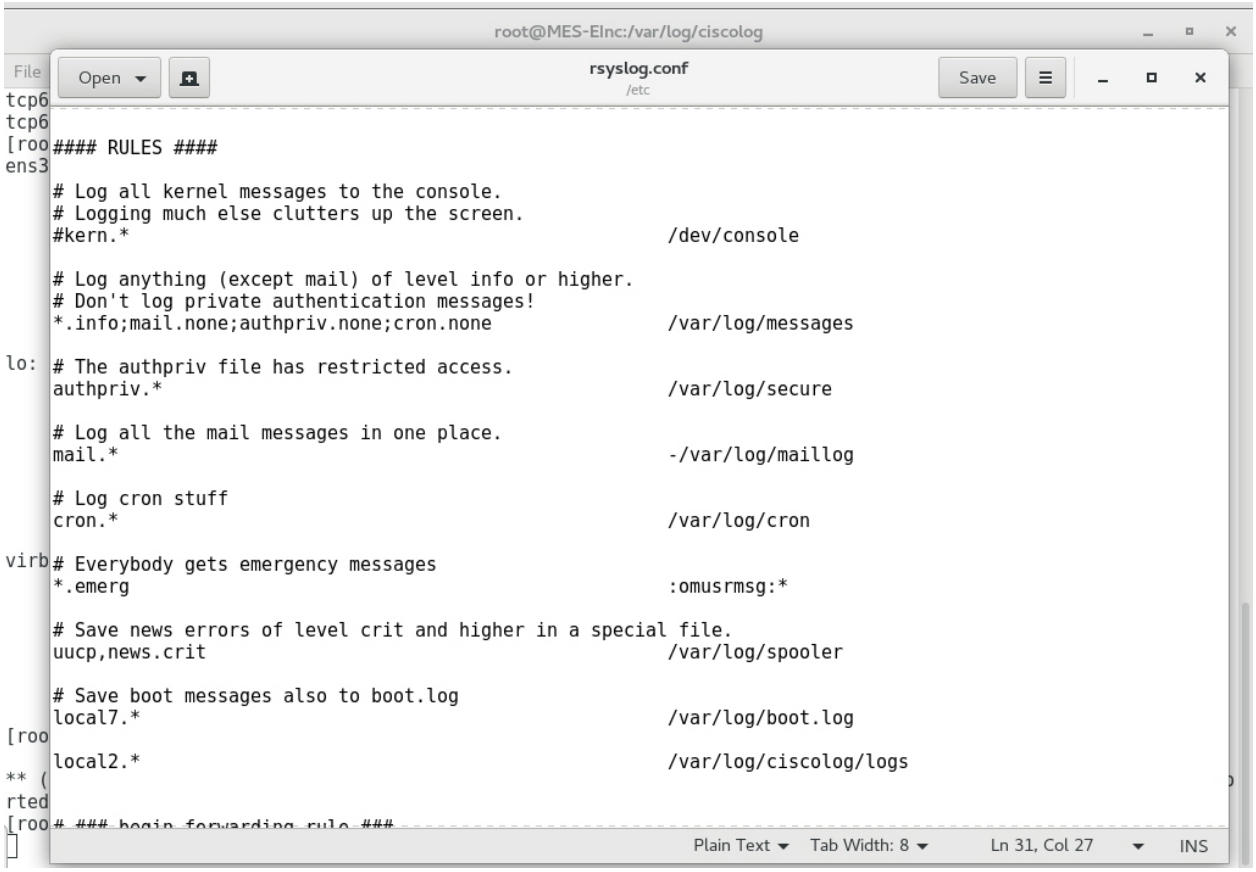
8. check the syslog directory to see the device's logs are saved.

- **cat /var/log/ciscolog/logs**




root@MES-EInc:/var/log/ciscolog
File Edit View Search Terminal Help
[root@MES-EInc ciscolog]# systemctl status rsyslog
● rsyslog.service - System Logging Service
Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
Active: active (running) since Thu 2018-06-14 13:24:46 PDT; 12min ago
Docs: man:rsyslogd(8)
http://www.rsyslog.com/doc/
Main PID: 10229 (rsyslogd)
CGroup: /system.slice/rsyslog.service
└─10229 /usr/sbin/rsyslogd -n -m 0 -r
Jun 14 13:24:46 MES-EInc.com systemd[1]: Starting System Logging Service...
Jun 14 13:24:46 MES-EInc.com rsyslogd[10229]: [origin software="rsyslogd" swVersion="8.24.0" x-pid="1022...tart
Jun 14 13:24:46 MES-EInc.com systemd[1]: Started System Logging Service.
Hint: Some lines were ellipsized, use -l to show in full.
[root@MES-EInc ciscolog]#
[root@MES-EInc ciscolog]# netstat -ntlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp 0 0 0.0.0.0:111 0.0.0.0:* LISTEN 1/systemd
tcp 0 0 192.168.122.1:53 0.0.0.0:* LISTEN 1964/dnsmasq
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 1269/sshd
tcp 0 0 127.0.0.1:631 0.0.0.0:* LISTEN 1266/cupsd
tcp 0 0 127.0.0.1:25 0.0.0.0:* LISTEN 1664/master
tcp 0 0 0.0.0.0:514 0.0.0.0:* LISTEN 10229/rsyslogd
tcp 0 0 0.0.0.0:3306 0.0.0.0:* LISTEN 1722/mysqld
tcp6 0 0 :::111 :::* LISTEN 1/systemd
tcp6 0 0 :::80 :::* LISTEN 1281/httpd
tcp6 0 0 :::21 :::* LISTEN 1278/vsftpd
tcp6 0 0 :::22 :::* LISTEN 1269/sshd
tcp6 0 0 ::1:631 :::* LISTEN 1266/cupsd
tcp6 0 0 ::1:25 :::* LISTEN 1664/master
tcp6 0 0 :::443 :::* LISTEN 1281/httpd
tcp6 0 0 :::514 :::* LISTEN 10229/rsyslogd
[root@MES-EInc ciscolog]#


root@MES-EInc:/var/log/ciscolog
Open
rsyslog.conf
/etc
Save
rsyslog configuration file
For more information see /usr/share/doc/rsyslog-*/rsyslog_conf.html
If you experience problems, see http://www.rsyslog.com/doc/troubleshoot.html
MODULES
The imjournal module bellow is now used as a message source instead of imuxsock.
$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)
$ModLoad imjournal # provides access to the systemd journal
#$ModLoad imklog # reads kernel messages (the same are read from journald)
#$ModLoad immark # provides --MARK-- message capability
Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514
Provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514
GLOBAL DIRECTIVES
Where to place auxiliary files
$WorkDirectory /var/lib/rsyslog
Use default timestamp format
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat
File syncing capability is disabled by default. This feature is usually not required,
not useful and an extreme performance hit
#$ActionFileEnableSync on
Plain Text
Tab Width: 8
Ln 31, Col 27
INS


root@MES-EInc:/var/log/ciscolog
File
Open
rsyslog.conf
/etc
Save
RULES
Log all kernel messages to the console.
Logging much else clutters up the screen.
#kern.* /dev/console
Log anything (except mail) of level info or higher.
Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none /var/log/messages
The authpriv file has restricted access.
authpriv.* /var/log/secure
Log all the mail messages in one place.
mail.* -/var/log/maillog
Log cron stuff
cron.* /var/log/cron
Everybody gets emergency messages
.emerg :omusrmsg:
Save news errors of level crit and higher in a special file.
uucp,news.crit /var/log/spooler
Save boot messages also to boot.log
local7.* /var/log/boot.log
local2.* /var/log/ciscolog/logs
Plain Text
Tab Width: 8
Ln 31, Col 27
INS

Hardware

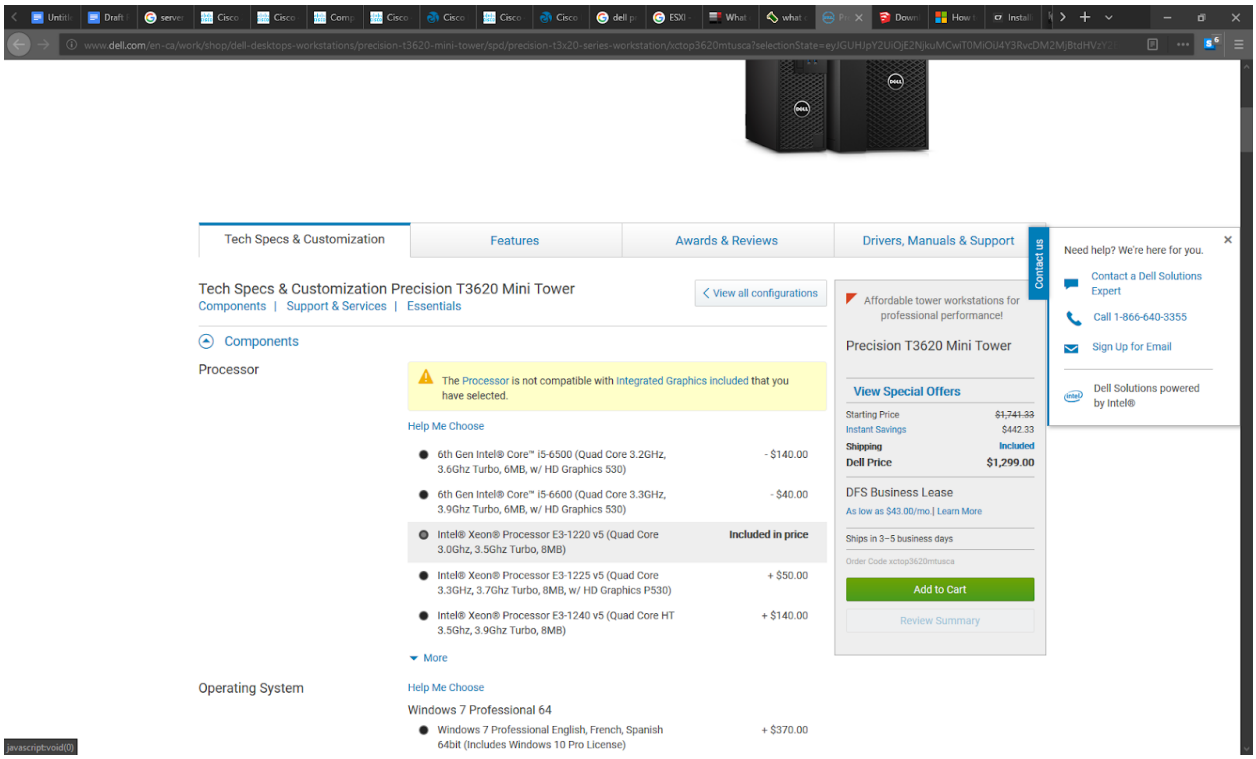
* drive assignments subject to change.

DEVICE	Drive/Config Store	ASSOC. ROLES	Site	ROOM	NOTES
C28	B19	VM (WDS, ADDC2)	M	123	Password:Pa$$w0rd, b19=250GB, 2007
C29	B15	RODC	1	123	Password:Pa$$w0rd, B15=160, 2008
Server 1	SAS1	VM (DFS/DHCP)	M	122	
Server 1	SAS2	VM (DFS/ DHCP)	M	122	
Server 1	SAS3	VM (DFS/ DHCP)	M	122	
Server 1	SAS4	VM (DFS/ DHCP)	M	122	
Link Switch	n/a		M	122	
M-SW 1	n/a		M	123	
M-SW 2	n/a		M	123	
M-SW 3	n/a		M	123	
M-R1	n/a		M	123	
C31	B17	RODC	1	123	B17/14=80, 2005
C30	B18	VM(ADDC1, DFS)	M	123	B18=500GB, unsure probably newest
B2-SW1	n/a		2	123	
B2-R1	n/a		2	123	
C25	B13	VM(clients)	1	123	B13/12=160, 2008
C24	B16	VM(clients)	2	123	B16=160GB, 2008
B1-SW 1	n/a		1	123	
B1-R1	n/a		1	123	
C23	B11	VM(clients)	M	123	B11=80GB, 2005
Computer 9	B20	vm(DFS, DHCP, Web Server)	M	122	b20=160GB, 2008
C32	B12	VM Clients	M		B13/12=160, 2008

Client Hardware/Specifications

- Operating System - Windows 10 Enterprise and Windows Server 2016 Datacenter
- Processor - Intel(R) Xeon(R) CPU E3-1240 v5 @ 3.50GHz
- Memory - 16384MB RAM
- Manufacturer - Dell Inc

Cost:



Microsoft

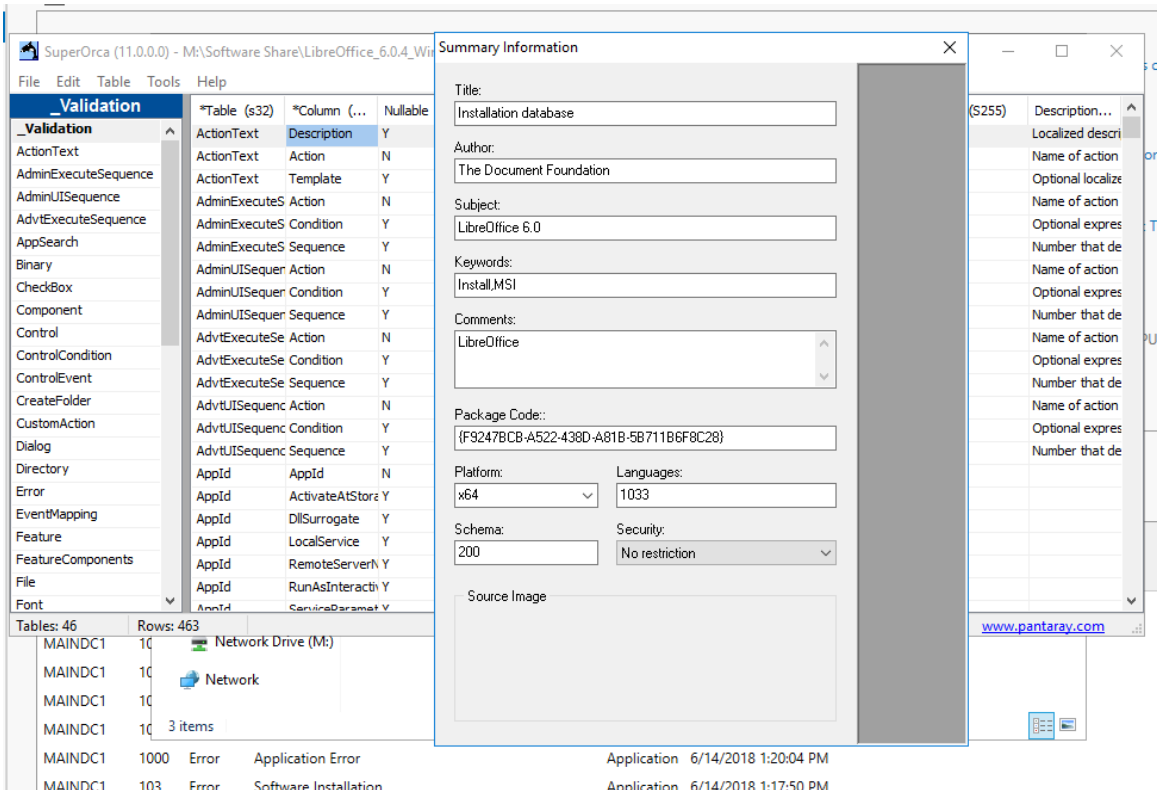
DFS Namespace Wizard Setup and Replication set up

1. Using server manager, Install dfs on server 5 servers.
2. Create replication group containing said servers
3. Topology should be hub and spoke, with datacenter servers as hub members
    a. Those would be fileserv1 and fileserv-vault
4. Fileserv-vault should be the optional hub member
5. Specify folder to be shared on each of the file servers
6. Replication should occur during off hours.
7. Fileserv-1 should be primary member
8. Publish the replication, and create a new namespace using fileserv1 as the namespace server, provide a name
9. Ensure that it is a domain-based namespace
10. Create directory for each of the main OUs allowing only members to access their respective folders.

Libreoffice Language fix

Acquired from: https://helgesverre.com/blog/libreoffice-msi-gpo-error/
Step by Step

1. Download LibreOffice installer from site
2. Download SuperOrca and install
3. Open SuperOrca
4. File > Open > Select the LibreOffice MSI you downloaded previously.
5. Click on Tools > Summary Information
6. With the exception of 1033 (english), remove all other values in the language textbox
7. Now, click on Apply.
8. Save to file share



SuperOrca configuration: prior to changes, the languages textbox has multiple language codes. Removing all of them except 1033 which is english will allow assigning the installer to a GPO.

Networking

Addressing Table

	Branch	Vlan	Network	First	Last	Subnet Mask
Engineering	Main Office	501	172.25.0.0/26	172.25.0.1	172.25.0.62	255.255.255.192
	2nd	501	172.25.1.0/26	172.25.1.1	172.25.1.62	255.255.255.192
	1st	501	172.25.2.0/26	172.25.2.1	172.25.2.62	255.255.255.192
Marketing	Main Office	502	172.25.0.64/26	172.25.0.65	172.25.0.126	255.255.255.192
	2nd	502	172.25.1.64/26	172.25.1.65	172.25.1.126	255.255.255.192
	1st	502	172.25.2.64/26	172.25.2.65	172.25.2.126	255.255.255.192
IT	Main Office	503	172.25.0.128/26	172.25.0.129	172.25.0.190	255.255.255.192
	2nd	503	172.25.1.128/26	172.25.1.129	172.25.1.190	255.255.255.192
	1st	503	172.25.2.128/26	172.25.2.129	172.25.2.190	255.255.255.192
HR	Main Office	504	172.25.0.192/26	172.25.0.193	172.25.0.254	255.255.255.192
	2nd	504	172.25.1.192/26	172.25.1.193	172.25.1.254	255.255.255.192
	1st	504	172.25.2.192/26	172.25.2.193	172.25.2.254	255.255.255.192
Servers	Main Office	505	172.25.3.96/27	172.25.3.97	172.25.3.126	255.255.255.224
	2nd	505	172.25.3.128/27	172.25.3.129	172.25.3.158	255.255.255.224
	1st	506	172.25.3.160/27	172.25.3.161	172.25.3.190	255.255.255.224
Guest	Main Office	506	172.25.3.192/28	172.25.3.193	172.25.3.206	255.255.255.240
	2nd	506	172.25.3.224/28	172.25.3.225	172.25.3.238	255.255.255.240
	1st	506	172.25.3.240/29	172.25.3.241	172.25.3.246	255.255.255.248
Network Management/ Native	Main Office	1	172.25.3.0/27	172.25.3.1	172.25.3.30	255.255.255.224
	2nd	1	172.25.3.32/27	172.25.3.33	172.25.3.62	255.255.255.224
	1st	1	172.25.3.64/27	172.25.3.65	172.25.3.94	255.255.255.224
GRE Tunnel			172.25.3.208/28	172.25.3.209	172.25.3.222	255.255.255.240

Device IP Addressing Table

Device Name	Interface	IP Address	Subnet Mask
Main	F0/0	142.232.194.220	255.255.255.0
	F0/1.1	172.25.3.30	255.255.255.224
	F0/1.24	192.168.123.2	255.255.255.0
	F0/1.501	172.25.0.62	255.255.255.192
	F0/1.502	172.25.0.126	255.255.255.192
	F0/1.503	172.25.0.190	255.255.255.192
	F0/1.504	172.25.0.254	255.255.255.192
	F0/1.505	172.25.3.126	255.255.255.224
	F0/1.506	172.25.3.206	255.255.255.240
	S0/2/1	172.25.3.249	255.255.255.252
	S0/1/1	172.25.3.253	255.255.255.252
	Tunnel500	172.25.3.209	255.255.255.240
M-S1	VLAN1	172.25.3.1	255.255.255.224
M-S2	VLAN1	172.25.3.2	255.255.255.224
M-S3	VLAN1	172.25.3.3	255.255.255.224

Device Name	Interface	IP Address	Subnet Mask
B2-R1	F0/0	142.232.194.221	255.255.255.0
	F0/1.1	172.25.3.62	255.255.255.224
	F0/1.501	172.25.1.62	255.255.255.192
	F0/1.502	172.25.1.126	255.255.255.192
	F0/1.503	172.25.1.190	255.255.255.192
	F0/1.504	172.25.1.254	255.255.255.192
	F0/1.505	172.25.3.158	255.255.255.224
	F0/1.506	172.25.3.238	255.255.255.240
	S0/2/1	172.25.3.250	255.255.255.252
	Tunnel500	172.25.3.210	255.255.255.240

B2-S1	VLAN1	172.25.3.33	255.255.255.224

Device Name	Interface	IP Address	Subnet Mask
B1-R1	F0/0	142.232.194.222	255.255.255.0
	F0/1.1	172.25.3.94	255.255.255.224
	F0/1.501	172.25.2.62	255.255.255.192
	F0/1.502	172.25.2.126	255.255.255.192
	F0/1.503	172.25.2.190	255.255.255.192
	F0/1.504	172.25.2.254	255.255.255.192
	F0/1.505	172.25.3.190	255.255.255.224
	F0/1.506	172.25.3.246	255.255.255.248
	S0/1/1	172.25.3.254	255.255.255.252
	Tunnel500	172.25.3.211	255.255.255.240
B1-S1	VLAN1	172.25.3.65	255.255.255.224

MAC Address Table

Device Name	MAC Address
DHCP1	00:0c:29:a8:4a:62
DHCP2	00:0c:29:09:b5:4a
WebServer	00:0c:29:bc:5d:53
Fileserv-Vault	00-0C-29-c2-d1-5c
fileserv1	00-0c-029-c5-20-05
Main-Client1	00:0C:29:87:CB:5D
Main-Client2	00:0C:29:82:E9:0C
Main-Client3	00:0C:29:99:67:13
Main-Client4 (IT)	00:0C:29:4D:01:53

Main-Client5 (Marketing)	00:0C:29:7D:AD:57
Main-DC	00:0C:29:9D:21:87
Main-DFS	00:0C:29:FA:71:99
Branch1-RODC	00:0C:29:4D:62:F1
Branch1-DFS	00:0C:29:15:BA:1C
Branch1-Client1	00:0C:29:69:BF:4B
Branch1-Client2	00:0C:29:58:CC:EF
Branch1-Client3	00:0C:29:C0:D2:83
Branch1-Client4	00:0C:29:C7:31:F4
Branch2-RODC	00:0C:29:49:6C:08
Branch2-DFS	00:0C:29:9C:FA:3E
ADDC	00:0C:29:4D:02:A0
WDS	00:0C:29:AB:49:D7
Branch2-Client1	00:0C:29:5F:22:9D
Branch2-Client2	00:0C:29:2E:A1:A1
Branch2-Client3	00:0C:29:EF:C5:A9
Branch2-Client4	00:0C:29:F2:15:FC

Configuration

TermServ:142.232.194.1

############################## Main [**2038**]

en

conf t

hostname Main

ip domain-lookup

service password-encryption

enable secret mesinc

line con 0

logg syn

```
password mesinc
exit
username Mes secret password
ip name-server 172.25.3.97
ip name-server 172.25.3.98


!---VLAN Routing
f0/0
no shut
int f0/1
no shut
int f0/1.1
encapsulation dot1q 1 native
description NetworkManagement&Native
ip add 172.25.3.30 255.255.255.224
!
int f0/1.501
encap dot1q 501
description Engineering
ip add 172.25.0.62 255.255.255.192
!
int f0/1.502
encap dot1q 502
Description Marketing
ip add 172.25.0.126 255.255.255.192
!
int f0/1.503
encap dot1q 503
description IT
ip add 172.25.0.190 255.255.255.192
!
int f0/1.504
encap dot1q 504
description HR
ip add 172.25.0.254 255.255.255.192
!
int f0/1.505
encap dot1q 505
description Servers
ip add 172.25.3.126 255.255.255.224
!
```

```
int f0/1.506
encap dot1q 506
description Guests
ip add 172.25.3.206 255.255.255.240
!
int f0/1.24
encap dot1q 24
description DataCN-Link
ip add 192.168.123.2 255.255.255.0
!
int s0/2/1
ip add 172.25.3.249 255.255.255.252
no shut
encapsulation ppp
ppp authentication chap
exit
username B2-R1 password cisco
!
int s0/1/1
ip address 172.25.3.253 255.255.255.252
no shut
encapsulation ppp
ppp authentication chap
exit
username B1-R1 password cisco

!---- SSH config
ip domain-name MesEinc.com
crypto key generate rsa
1024
line vty 0 4
transport input ssh
login local
exec-timeout 5
exit
ip ssh version 2
ip ssh time-out 120
ip ssh authentication-retries 2

!
!---OSPF
router ospf 1
```

```
router-id 1.1.1.1
passive-interface default
no passive-interface s0/2/1
no passive-interface s0/1/1
no passive-interface f0/1.24
network 172.25.0.0 0.0.0.63 area 0
network 172.25.0.64 0.0.0.63 area 0
network 172.25.0.128 0.0.0.63 area 0
network 172.25.0.192 0.0.0.63 area 0
network 172.25.3.96 0.0.0.31 area 0
network 172.25.3.192 0.0.0.31 area 0
network 172.25.3.0 0.0.0.31 area 0
network 172.25.3.248 0.0.0.3 area 0
network 172.25.3.252 0.0.0.3 area 0
exit
!
!---Global Authentication
int s0/2/1
ip ospf message-digest-key 1 md5 cisco
int s0/1/1
ip ospf message-digest-key 1 md5 cisco
router ospf 1
area 0 authentication message-digest
exit

!---Redistribution OSPF/EIGRP
router ospf 1
redistribute eigrp 4700 subnets
!
router eigrp 4700
redistribute ospf 1 metric 100000 100 255 1 1500
network 192.168.123.0
no auto-summary
passive-interface default
no passive-interface s0/2/1
no passive-interface s0/1/1
no passive-interface f0/1.24
!
!---NAT
ip access-list standard MAIN_NAT
permit 172.25.0.0 0.0.0.255
permit 172.25.3.0 0.0.0.255
```

```
remark ALLOW MAIN OFFICE PORT ADDRESS TRANSLATION
exit
ip nat inside source list MAIN_NAT interface f0/0 overload
int f0/1
ip nat inside
int f0/1.1
ip nat inside
Int f0/1.24
Ip nat inside
int f0/1.501
ip nat inside
int f0/1.502
ip nat inside
int f0/1.503
ip nat inside
int f0/1.504
ip nat inside
int f0/1.505
ip nat inside
int f0/1.506
ip nat inside
int f0/0
Ip address 142.232.194.220 255.255.255.0
ip nat outside
exit
ip route 0.0.0.0 0.0.0.0 f0/0 142.232.194.254
!
!---DHCP
int f0/1.501
ip helper-address 192.168.25.4
Ip helper-address 192.168.25.227
int f0/1.502
ip helper-address 192.168.25.4
Ip helper-address 192.168.25.227
int f0/1.503
ip helper-address 192.168.25.4
Ip helper-address 192.168.25.227
int f0/1.504
ip helper-address 192.168.25.4
Ip helper-address 192.168.25.227
int f0/1.505
ip helper-address 192.168.25.4
```

```
Ip helper-address 192.168.25.227
int f0/1.506
ip helper-address 192.168.25.4
Ip helper-address 192.168.25.227

!
!----- syslog
logging on
logging 192.168.25.226
logging facility local2
Logging trap info
Logging trap debug
!
!----- ntp
ntp server ca.pool.ntp.org
ntp peer 172.25.3.62
ntp peer 172.25.3.94
ntp peer 172.25.3.33
ntp peer 172.25.3.65
ntp peer 172.25.3.1
ntp peer 172.25.3.2
ntp peer 172.25.3.3

!---Route filtering
ip access-list standard ROUTE_FILTER
permit 192.168.25.0 0.0.0.255
permit 192.168.123.0 0.0.0.255
remark BLOCK EIGRP ROUTES FROM OTHER GROUPS
router eigrp 4700
distribute-list ROUTE_FILTER in

!---ACLs
ip access-list standard MIT_SSH
permit 172.25.0.128 0.0.0.63
remark SSH FOR MAIN BRANCH IT DEPARTMENT ONLY
Line vty 0 4
access-class MIT_SSH in

!---Time-based ACL
int f0/0
description ACCESS TO THE INTERNET
ip access-group NETOUT out
```

```
ex
!
ip reflexive-list timeout 120
!
time-range WORKDAY
periodic weekdays 8:00 to 17:00
!
ip access-list extended NETOUT
remark ALLOW ACCESS TO INTERNET DURING WORK HOURS
permit ip any any time-range WORKDAY reflect IPTRAFFIC
ex
!
ip access-list extended NETIN
evaluate IPTRAFFIC
ex
!

############################### M-S1 [2041]
en
conf t
hostname M-S1
ip domain-lookup
enable secret mesinc
service password-encryption
line con 0
logg syn
password mesinc
login
exit
username Mes secret password
exit
ip name-server 172.25.3.97
ip name-server 172.25.3.98
!

int range f0/3 - 4, f0/7 - 12, f0/15 - 24
shut
exit

!---VTP
vtp mode server
vtp domain MesEinc.com
```

```
vtp password cisco

vlan 501
name Engineering
vlan 502
name Marketing
vlan 503
name IT
vlan 504
name HR
Vlan 505
Name Servers
Vlan 506
Name Guests
Vlan 1
Name NetworkManagement&Native
vlan 24
name DataCenter

!---Port-Channel
int range f0/1 - 2
channel-group 1 mode desirable
int port-channel 1
sw mo trunk
sw tr native vlan 1
sw trunk allowed vlan 1,500-599
no shut
!
int range f0/5 - 6
channel-group 4 mode desirable
int port-channel 4
sw mo trunk
sw trunk native vlan 1
sw trunk allowed vlan 1,500-599
no shut
!
int range f0/13 - 14
channel-group 2 mode desirable
int port-channel 2
sw mo trunk
sw trunk native vlan 1
sw trunk allowed vlan 1,500-599
```

```
no shut
!

Ip domain-name MesEinc.com
Ip default-gateway 172.25.3.30
Int vlan 1
Ip add 172.25.3.1 255.255.255.224
exi

!---- SSH config
crypto key generate rsa
1024
line vty 0 15
transport input ssh
login local
exec-timeout 5
exit
ip ssh version 2
ip ssh time-out 120
ip ssh authentication-retries 2

!---ACLs
ip access-list standard MIT_SSH
permit 172.25.0.128 0.0.0.63
remark SSH FOR MAIN BRANCH IT DEPARTMENT ONLY
line vty 0 15
access-class MIT_SSH in

|---- spanning tree
Spanning-tree mode rapid-pvst
spanning-tree portfast
spanning-tree portfast bpduguard
spanning-tree extend system-id

!---NTP
ntp server 172.25.3.30
clock timezone pdt -7

!----- syslog
loggng on
logging 192.168.25.226
logging facility local2
```

```
Logging trap info
Logging trap debug

############################## M-S2 [2042]
en
conf t
hostname M-S2
ip domain-lookup
enable secret mesinc
service password-encryption
line con 0
logg syn
password mesinc
login
exit
username Mes secret password
Ip name-server 172.25.3.97
Ip name-server 172.25.3.98

int range f0/5 - 21
shut
Int range g0/1 - 2
Shut

!---Port-Channel
int range f0/1 - 2
channel-group 1 mode desirable
int port-channel 1
sw mo trunk
sw trunk native vlan 1
no shut

int range f0/3 - 4
channel-group 3 mode desirable
int port-channel 3
sw mo trunk
sw trunk native vlan 1
no shut

Int f0/22
No shut
Sw mo acc
```

```
Sw acc vlan 502
switchport port-security
switchport port-security maximum 10
switchport port-security mac-address sticky
switchport port-security violation restrict
!
Int f0/23
Sw m acc
Sw acc vlan 503
switchport port-security
switchport port-security maximum 10
switchport port-security mac-address sticky
switchport port-security violation restrict
!
Int f0/24
Sw m acc
Sw acc vlan 505
switchport port-security
switchport port-security maximum 10
switchport port-security mac-address sticky
switchport port-security violation restrict

!---VTP
vtp mode client
vtp domain MesEinc.com
vtp password cisco

Ip domain-name MesEinc.com
Ip default-gateway 172.25.3.30
Int vlan 1
Ip add 172.25.3.2 255.255.255.224

!---- SSH config
crypto key generate rsa
1024
line vty 0 15
transport input ssh
login local
exec-timeout 5
exit
ip ssh version 2
ip ssh time-out 120
```

ip ssh authentication-retries 2

!---ACLs
ip access-list standard MIT_SSH
permit 172.25.0.128 0.0.0.63
remark SSH FOR MAIN BRANCH IT DEPARTMENT ONLY
Line vty 0 15
access-class MIT_SSH in

|---- spanning tree
Spanning-tree mode rapid-pvst
Spanning-tree portfast
Spanning-tree portfast bpduguard
Spanning-tree extend system-id

!----- syslog
loggng on
logging 192.168.25.226
logging facility local2
Logging trap info
Logging trap debug

################################ M-S3 [2043]
en
conf t
hostname M-S3
ip domain-lookup
enable secret mesinc
service password-encryption
line con 0
logg syn
password mesinc
login
exit
username Mes secret password
Ip name-server 172.25.3.97
Ip name-server 172.25.3.98
exit
!

int range f0/1 - 2, f0/7 - 22

```
shut
Int range g0/1 - 2
shut

!---Port-Channel
int range f0/3 - 4
channel-group 3 mode desirable
int port-channel 3
sw mo trunk
sw trunk native vlan 1
no shut

int range f0/5 - 6
channel-group 2 mode desirable
int port-channel 2
sw mode trunk
sw trunk native vlan 1
no shut

!---VTP
vtp mode client
vtp domain MesEinc.com
vtp password cisco

Ip domain-name MesEinc.com
Ip default-gateway 172.25.3.30
Int vlan 1
Ip add 172.25.3.3 255.255.255.224

Int f0/22
No shut
Sw m acc
Sw acc vlan 501

Int f0/23
Sw m acc
Sw acc vlan 503

Int f0/24
Sw m acc
Sw acc vlan 505
```

```
int range f0/22 - 24
switchport port-security
switchport port-security maximum 10
switchport port-security mac-address sticky
switchport port-security violation restrict

!---- SSH config
crypto key generate rsa
1024
line vty 0 15
transport input ssh
login local
exec-timeout 5
exit
ip ssh version 2
ip ssh time-out 120
ip ssh authentication-retries 2

!---ACLs
ip access-list standard MIT_SSH
permit 172.25.0.128 0.0.0.63
remark SSH FOR MAIN BRANCH IT DEPARTMENT ONLY
Line vty 0 15
Access-class MIT_SSH in

|---- spanning tree
Spanning-tree mode rapid-pvst
Spanning-tree portfast
Spanning-tree portfast bpduguard
Spanning-tree extend system-id

!--NTP
Ntp server 172.25.3.30
Clock timezone pdt -7

!----- syslog
loggng on
logging 192.168.25.226
logging facility local2
Logging trap info
Logging trap debug
```

############################## Branch2 [**2039**]

```
ena
conf t
hostname B2-R1
ip domain-lookup
service password-encryption
line con 0
logg syn
password mesinc
login
exit
username Mes secret password
ip name-server 172.25.3.97
ip name-server 172.25.3.98
!
int f0/1
no shut
!
int f0/1.1
encapsulation dot1q 1 native
Description NetworkManagement&Native
ip add 172.25.3.62 255.255.255.224
Ip virtual-reassembly
|
int f0/1.501
encapsulation dot1q 501
description Engineering
ip add 172.25.1.62 255.255.255.192
!
int f0/1.502
encapsulation dot1q 502
Description Marketing
ip add 172.25.1.126 255.255.255.192
!
int f0/1.503
encapsulation dot1q 503
Description IT
ip add 172.25.1.190 255.255.255.192
!
int f0/1.504
encapsulation dot1q 504
```

```
Description HR
ip add 172.25.1.254 255.255.255.192
!
int f0/1.505
encapsulation dot1q 505
Description Servers
ip add 172.25.3.158 255.255.255.224
!
int f0/1.506
encapsulation dot1q 506
Description G
uests
ip add 172.25.3.238 255.255.255.240
!
!
int s0/2/1
ip add 172.25.3.250 255.255.255.252
no shut
encapsulation ppp
ppp authentication chap
ex
username Main password cisco

router ospf 1
router-id 2.2.2.2
passive-interface default
no passive-interface s0/2/1
network 172.25.1.0 0.0.0.63 area 0
network 172.25.1.64 0.0.0.63 area 0
network 172.25.1.128 0.0.0.63 area 0
network 172.25.1.192 0.0.0.63 area 0
network 172.25.3.128 0.0.0.31 area 0
network 172.25.3.224 0.0.0.15 area 0
network 172.25.3.32 0.0.0.31 area 0
network 172.25.3.248 0.0.0.3 area 0

!---SSH config
ip domain-name MesEinc.com
crypto key generate rsa
1024
line vty 0 4
exec-timeout 5
```

```
transport input ssh
login local
exit
ip ssh version 2
ip ssh time-out 120
ip ssh authentication-retries 2

!---Global Authentication
int s0/2/1
ip ospf message-digest-key 1 md5 cisco
ex
router ospf 1
area 0 authentication message-digest
ex

!---NAT
ip access-list standard B2_NAT
permit 172.25.1.0 0.0.0.255
permit 172.25.3.0 0.0.0.255
remark ALLOW BRANCH 2 PORT ADDRESS TRANSLATION
ex
ip nat inside source list B2_NAT interface f0/0 overload
int f0/1
ip nat inside
int f0/1.1
ip nat inside
int f0/1.501
ip nat inside
int f0/1.502
ip nat inside
int f0/1.503
ip nat inside
int f0/1.504
ip nat inside
int f0/1.505
ip nat inside
int f0/1.506
ip nat inside
int f0/1.507
ip nat inside
int f0/0
Ip address 142.232.194.221 255.255.255.0
```

```
ip nat outside
ex
ip route 0.0.0.0 0.0.0.0 f0/0 142.232.194.254

!---ACLs
ip access-list standard B2IT_SSH
permit 172.25.1.128 0.0.0.63
permit 172.25.0.128 0.0.0.63
remark SSH FOR BRANCH 2 IT DEPARTMENT AND MAIN OFFICE IT
line vty 0 4
access-class B2IT_SSH in

int f0/0
description ACCESS TO THE INTERNET
ip access-group NETOUT out
ex
!
ip reflexive-list timeout 120
!
time-range WORKDAY
periodic weekdays 8:00 to 17:00
!
ip access-list extended NETOUT
remark ALLOW ACCESS TO INTERNET DURING WORK HOURS
permit ip any any time-range WORKDAY reflect IPTRAFFIC
ex
!
ip access-list extended NETIN
evaluate IPTRAFFIC
ex
!

!---NTP
ntp server 172.25.3.30

!----- syslog
loggng on
logging 192.168.25.226
logging facility local2
Logging trap info
Logging trap debug
```

```
############################### B2-S1 [2044]
en
conf t
hostname B2-S1
ip domain-lookup
enable secret mesinc
service password-encryption
line con 0
logg syn
password mesinc
login
exit
username Mes secret password
ip name-server 172.25.3.97
ip name-server 172.25.3.98
exit

!
int range f0/2 - 22
shutdown
int range g0/1 - 2
Shutdown
!
Banner motd ^ ####### WARNING AUTHORIZED ACCESS ONLY!! ####### ^

|---- VTP
vtp version 2
vtp mode server
vtp domain MesEinc.com
vtp password cisco

|---- VLAN
vlan 501
name Engineering
vlan 502
name Marketing
vlan 503
name IT
vlan 504
name HR
Vlan 505
```

```
Name Servers
Vlan 506
Name Guests
Vlan 1
Name NetworkManagement&Native
vlan 24
name DataCenter

Int f0/1
No shut
Sw mo trunk
!
Int f0/22
No shut
Sw m ac
Sw acc vlan 504
!
Int f0/23
Sw m acc
Sw acc vlan 503
!
Int f0/24
Sw m acc
Sw acc vlan 505
ex
!
ip default-gateway 172.25.3.62
int vlan 1
ip add 172.25.3.33 255.255.255.224
ex

!---- SSH config
ip domain-name MesEinc.com
crypto key generate rsa
1024
line vty 0 15
transport input ssh
login local
exec-timeout 5
exit
ip ssh version 2
ip ssh time-out 120
```

```
ip ssh authentication-retries 2

!
!---Port-Security
int range f0/22 - 24
switchport port-security
switchport port-security maximum 10
switchport port-security mac-address sticky
switchport port-security violation restrict

!---ACLs
ip access-list standard B2IT_SSH
permit 172.25.1.128 0.0.0.63
permit 172.25.0.128 0.0.0.63
remark SSH FOR BRANCH 2 IT DEPARTMENT AND MAIN OFFICE IT
line vty 0 15
access-class B2IT_SSH in
!

|---- spanning tree
Spanning-tree mode rapid-pvst
Spanning-tree portfast default
Spanning-tree portfast bpduguard default
Spanning-tree extend system-id

!---NTP
Ntp server 172.25.3.30 prefer
Clock timezone pdt -7

!----- syslog
loggng on
logging 192.168.25.226
logging facility local2
Logging trap info
Logging trap debug

############################## Branch1 [2040]
en
conf t
hostname B1-R1
ip domain-lookup
enable secret mesinc
```

```
Service password-encryption
line con 0
logg sync
password mesinc
username Mes secret password
ip name-server 172.25.3.97
ip name-server 172.25.3.98
exit
!
int s0/1/1
Ip add 172.25.3.254 255.255.255.252
no shut
encapsulation ppp
ppp authentication chap
ex
username Main password cisco

!---VLAN Routing
int f0/1
no shut
int f0/1.1
encap dot1q 1 native
Description NetworkManagement&Native
ip add 172.25.3.94 255.255.255.224
int f0/1.501
encap dot1q 501
Description Engineering
ip add 172.25.2.62 255.255.255.192
int f0/1.502
encap dot1q 502
Description Marketing
ip add 172.25.2.126 255.255.255.192
int f0/1.503
encap dot1q 503
ip add 172.25.2.190 255.255.255.192
Description IT
int f0/1.504
encap dot1q 504
Description HR
ip add 172.25.2.254 255.255.255.192
int f0/1.505
encap dot1q 505
```

```
Description Servers
ip add 172.25.3.190 255.255.255.224
int f0/1.506
encap dot1q 506
Description Guests
ip add 172.25.3.246 255.255.255.248

!---- SSH config
ip domain-name MesEinc.com
crypto key generate rsa
1024
line vty 0 4
transport input ssh
login local
exec-timeout 5
exit
ip ssh version 2
ip ssh time-out 120
ip ssh authentication-retries 2


!---OSPF
router ospf 1
router-id 3.3.3.3
passive-interface default
no passive-interface s0/1/1
network 172.25.2.0 0.0.0.63 area 0
network 172.25.2.64 0.0.0.63 area 0
network 172.25.2.128 0.0.0.63 area 0
network 172.25.2.192 0.0.0.63 area 0
network 172.25.3.160 0.0.0.31 area 0
network 172.25.3.240 0.0.0.7 area 0
network 172.25.3.64 0.0.0.31 area 0
network 172.25.3.252 0.0.0.3 area 0
exit

!---Global Authentication
int s0/1/1
ip ospf message-digest-key 1 md5 cisco
exi
router ospf 1
area 0 authentication message-digest
```

```
exi

!---NAT
ip access-list standard B1_NAT
permit 172.25.2.0 0.0.0.255
permit 172.25.3.0 0.0.0.255
remark ALLOW BRANCH 1 PORT ADDRESS TRANSLATION
ex
ip nat inside source list B1_NAT interface f0/0 overload
int f0/1
ip nat inside
int f0/1.1
ip nat inside
int f0/1.501
ip nat inside
int f0/1.502
ip nat inside
int f0/1.503
ip nat inside
int f0/1.504
ip nat inside
int f0/1.505
ip nat inside
int f0/1.506
ip nat inside
int f0/1.507
ip nat inside
int f0/0
ip address 142.232.194.222 255.255.255.0
ip nat outside
ex
ip route 0.0.0.0 0.0.0.0 f0/0 142.232.194.254

!---ACLs
ip access-list standard B1IT_SSH
permit 172.25.2.128 0.0.0.63
permit 172.25.0.128 0.0.0.63
remark SSH FOR BRANCH 1 IT DEPARTMENT AND MAIN OFFICE IT
line vty 0 4
access-class B1IT_SSH in
!
!---Time-based ACL
```

```
int f0/0
description ACCESS TO THE INTERNET
ip access-group NETOUT out
ex
!
ip reflexive-list timeout 120
!
time-range WORKDAY
periodic weekdays 8:00 to 17:00
!
ip access-list extended NETOUT
remark ALLOW ACCESS TO INTERNET DURING WORK HOURS
permit ip any any time-range WORKDAY reflect IPTRAFFIC
ex
!
ip access-list extended NETIN
evaluate IPTRAFFIC
ex
!
!---NTP
ntp server 172.25.3.30

!----- syslog
loggng on
logging 192.168.25.226
logging facility local2
Logging trap info
Logging trap debug

################################ B1-S1[2045]
en
conf t
hostname B1-S1
ip domain-lookup
enable secret mesinc
Service password-encryption
line con 0
logg syn
password mesinc
login
exit
username Mes secret password
```

Ip name-server 172.25.3.97
Ip name-server 172.25.3.98

int range f0/2 - 22
shutdown
int range g0/1 - 2
Shutdown

Banner motd ^ ####### WARNING AUTHORIZED ACCESS ONLY!! ####### ^

|---- VTP
vtp mode server
vtp domain MesEinc.com
vtp password cisco

|---- VLAN

vlan 501
name Engineering
vlan 502
name Marketing
vlan 503
name IT
vlan 504
name HR
Vlan 505
Name Servers
Vlan 506
Name Guests
Vlan 1
Name NetworkManagement&Native
vlan 24
name DataCenter

!---Port-Security
Int f0/22
No shut
sw mo access
sw access vlan 501

Int f0/23
No shut

```
Sw m acc
Sw acc vlan 503

Int f0/24
Sw m acc
Sw acc vlan 505

Int range f0/22 - 24
switchport port-security
switchport port-security maximum 10
switchport port-security mac-address sticky
switchport port-security violation restrict

Ip default-gateway 172.25.3.94
Int vlan 1
Ip add 172.25.3.65 255.255.255.224

!---- SSH config
ip domain-name MesEinc.com
crypto key generate rsa
1024
line vty 0 15
transport input ssh
login local
exec-timeout 5
exit
ip ssh version 2
ip ssh time-out 120
ip ssh authentication-retries 2

!---ACLs
ip access-list standard B1IT_SSH
permit 172.25.2.128 0.0.0.63
permit 172.25.0.128 0.0.0.63
remark SSH FOR BRANCH 1 IT DEPARTMENT AND MAIN OFFICE IT
line vty 0 4
access-class B1IT_SSH in

|---- spanning tree
Spanning-tree mode rapid-pvst
Spanning-tree portfast default
Spanning-tree portfast bpduguard default
```

Spanning-tree extend system-id

|----NTP
Ntp server 172.25.3.30 prefer
Clock timezone pdt -7

!----- syslog
loggng on
logging 192.168.25.226
logging facility local2
Logging trap info
Logging trap debug