

# Capstone Project Documentation

## Table of Contents:

- Hypervisor #1 Pg. 2
- Hypervisor #2 Pg. 9
- Pfsense Firewall Pg. 13
- HP Switch #1 Pg. 18
- HP Switch #2 Pg.18
- Admin RouterPg.19
- Client Router Pg. 20
- Admin Switch Pg.20
- Client Switch Pg.21
- LS4-2 Pg. 22
- LS4-3 Pg. 23

Introduction: The following is a comprehensive overview of the IT-OPS 258 capstone project. The primary purpose of this documentation is to provide the reader with a robust understanding of the infrastructure. Ideally this document should enable a seamless transfer of management responsibilities to another professional and provide them with the knowledge needed for continued administration. Each section is denoted by a bolded title which represents a piece of physical hardware. In each of these sections the services and configurations of said hardware are listed. Accompanying this document are a logical diagram and address table which more clearly illustrate the physical configuration of the architecture.

## **Hypervisor #1(Lab server PS04)**

### General system information:

Operating system: Windows Server 2016  
Gigabit Ethernet IP: 192.168.60.15  
Gigabit Ethernet 2 IP: 192.168.65.15

### Hyper-V Virtual Switch(es):

#### Inside:

External Network: Gigabit Ethernet  
Allow Management OS to share NIC?: Yes  
Connected to: Admin console, Domain Controller, WC#1, and WC#2

### Web Server NIC Binding:

External Network: Gigabit Ethernet 2  
Allow Management OS to share NIC?: No  
Connected to: Web Server

### Hyper-V Virtual Machine(s):

#### Admin Console:

Operating system: Windows 10 Pro  
IP:DHCP.  
Virtual Switch: Inside  
Domain: Stand Alone

User Name: Admin  
Password: Pa\$\$word

#### Service(s):

SSH Via Putty to:

Admin Router

Client Router

Admin Switch

Client Switch

Note: Use Saved Sessions in Putty to access, other methods will not work due to out of date devices

Domain Controller:

IP:192.168.60.1

Network: Inside

Virtual Switch: Inside

Domain: Bowler.com

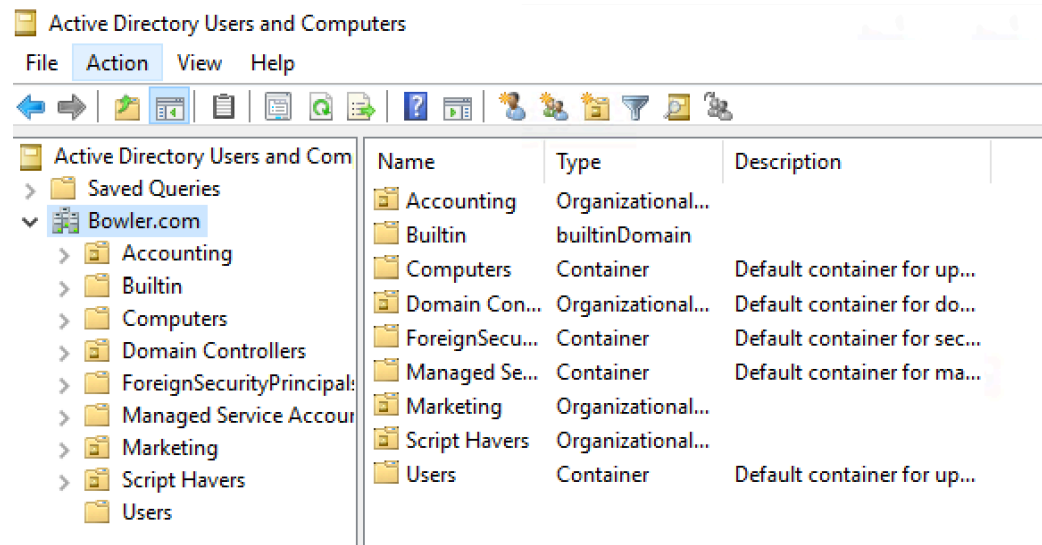
Service(s):

ADDS:

Domain name:

Bowler.com

User(s):



Johnathan Bowler

Username: Sage

Password: Pa\$\$word

Member of:

- Administrators
- Domain Admins
- Domain Users
- Enterprise Admins
- Remote Desktop Users
- Remote Management Users

Chris Cuneo

Username: Cuneo

Password: Enigma123!

Member of:

- Administrators
- Domain Admins
- Domain Users
- Enterprise Admins
- Remote Desktop Users
- Remote Management Users

Marketing Director1

Username:Marketing\_Director\_1

Password:Pa\$\$word

Member of:

- Domain Users
- Remote Desktop Users
- Marketing Directors

Marketing User1

Username:Marketing\_User\_1

Password:Pa\$\$word

Member of:

- Domain Users
- Remote Desktop Users

Accounting Director1

Username:Accounting\_Director\_1

Password:Pa\$\$word

Member of:

Domain Users

Remote Desktop Users

Accounting Directors

Accounting User1

Username:Accounting\_User\_1

Password:Pa\$\$word

Member of:

Domain Users

Remote Desktop Users

Security Group(s):

Marketing Directors

Member(s):

Marketing Director1

Accounting Directors

Member(s):

Accounting Director1

OU(s)

Accounting

Control Delegated to: Accounting Directors

Security Group

Security Group(s):

Accounting Directors

User(s):

Accounting User1  
Accounting Director1

Marketing

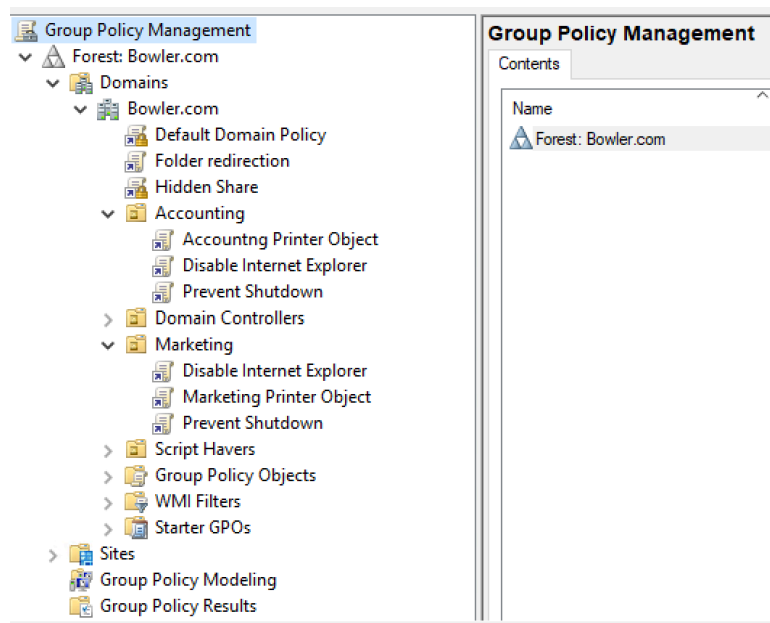
Control Delegated to: Marketing Directors  
Security Group  
Security Group(s):

Marketing Directors

User(s):

Marketing User1  
Marketing Director1

GPO(s)



Disable Internet Explorer:

Linked to: Marketing & Accounting OUs  
Applies to: Members of Marketing and  
Accounting OUs  
Description:  
Disables Internet Explorer for certain

## Users

### Prevent Shutdown:

Linked to: Marketing & Accounting OUs  
Applies to: Members of Marketing and Accounting OUs

Description:  
Makes certain users unable to shutdown the machine

### Folder Redirection:

Linked to: Bowler.com domain  
Applies to: All Users  
Description:  
Redirects "Video" folder to  
"Company Video Share" shared folder

### Hidden Share

Linked to: Bowler.com domain  
folder  
Applies to:

Sage  
Cuneo  
Accounting Directors  
Marketing Directors

Description:  
Deploys a script contained in the  
"Hidden Share" shared folder to  
select users

### Accounting Printer Object:

Linked to: Accounting OU  
Applies to: Members of Accounting  
Description:

Accounting Printer Published in Active Directory

Marketing Printer Object

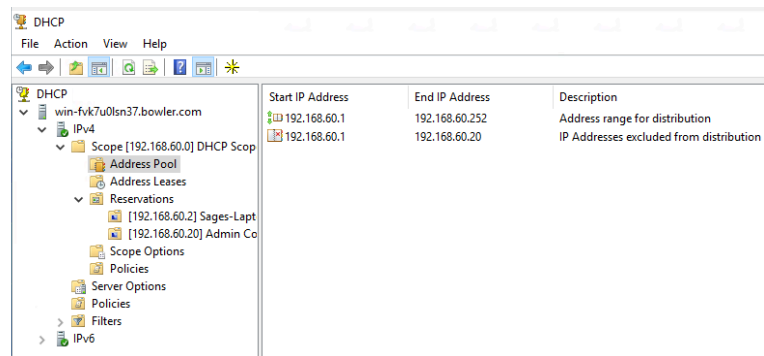
Linked to: Marketing OU

Applies to: Members of Marketing

Description:

Marketing Printer Published in Active Directory.

DHCP:



Start IP Address	End IP Address	Description
192.168.60.1	192.168.60.252	Address range for distribution
192.168.60.1	192.168.60.20	IP Addresses excluded from distribution

Scope: 192.168.60.1-192.168.60.252

Exclusions: 192.168.60.1-192.168.60.20

Reservations: 192.168.60.2

Default Gateway: 192.168.60.8

DNS: 192.168.60.1

DNS:

Forwarders: 8.8.8.8

Forward Lookup Zones:

\_msdcs.Bowler.com

Bowler.com

Conditional Forwarders:

Trust relationship John.com - 192.168.70.1

WC#1:



Operating system: Windows Server 2016  
IP: DHCP  
Virtual Switch: Inside  
Domain: Bowler.com

WC#2:

Operating system: Windows Server 2016  
IP: DHCP  
Virtual Switch: Inside  
Domain: Bowler.com

Web Server:

Operating system: Linux Mint  
IP:192.168.65.5  
Virtual Switch: Web Server NIC Binding  
Domain: Stand Alone  
Service(s):

Apache2 web server

## **Hypervisor #2(Lab Sever PS16)**

General system information:

Operating system: VMWare ESXI  
VMNIC0 IP: 192.168.70.15  
VMNIC1 IP: Assigned to VRouter

Virtual Switch(s):

VirtualSwitch0  
New Switch

ESXI Virtual machine(s):

Domain Controller:

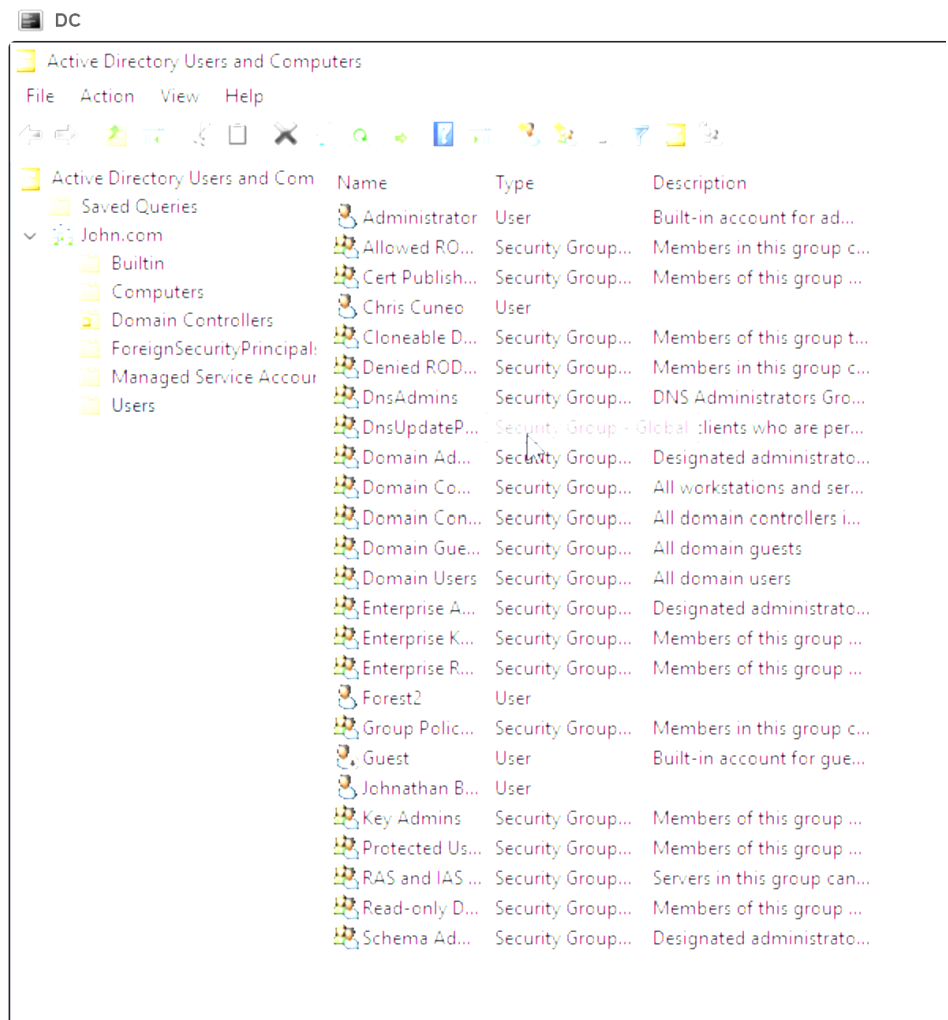
Services:

ADDS:

Domain name:

John.com

User(s):



Johnathan Bowler

Username: Sage

Password: Pa\$\$word

Member of:

Administrators

Domain Admins

Domain Users  
Enterprise Admins  
Remote Desktop Users  
Remote Management Users

Chris Cuneo

Username: Cuneo  
Password: Enigma123!  
Member of:

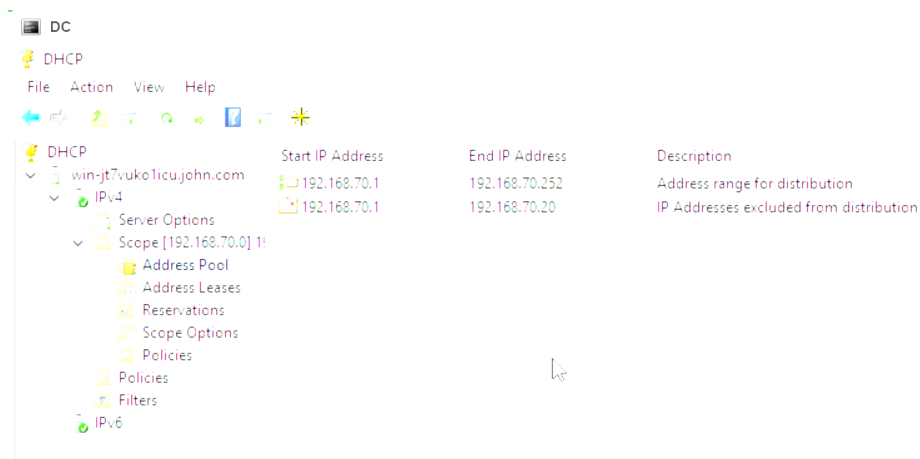
Administrators  
Domain Admins  
Domain Users  
Enterprise Admins  
Remote Desktop Users  
Remote Management Users

Forest2

Username:Forest2  
Password:Pa\$\$word  
Member of:

Domain Users  
Remote Desktop Users

DHCP:



Scope: 192.168.70.1-192.168.70.252  
Exclusions: 192.168.70.1-192.168.70.20  
Reservations: 192.168.60.2  
Default Gateway: 192.168.70.9  
DNS: 192.168.70.1

DNS:

Forward Lookup Zones:

\_msdcs.John.com  
John.com

Conditional Forwarders:

Trust Relationship Bowler.com - 192.168.60.1

LC#1:

Operating system: Ubuntu Linux  
IP: DHCP  
Virtual Switch: Branch  
Domain: John.com

LC#2:

Operating system: Fedora Linux  
IP: DHCP  
Virtual Switch: Branch  
Domain: John.com

VRouter:

<

Operating system: Windows Server

NIC 1 IP: 192.168.60.9/24

NIC 2 IP: 192.168.70.9/24

Virtual Switch(s): VSwitch0(Branch), New Switch(Inside)

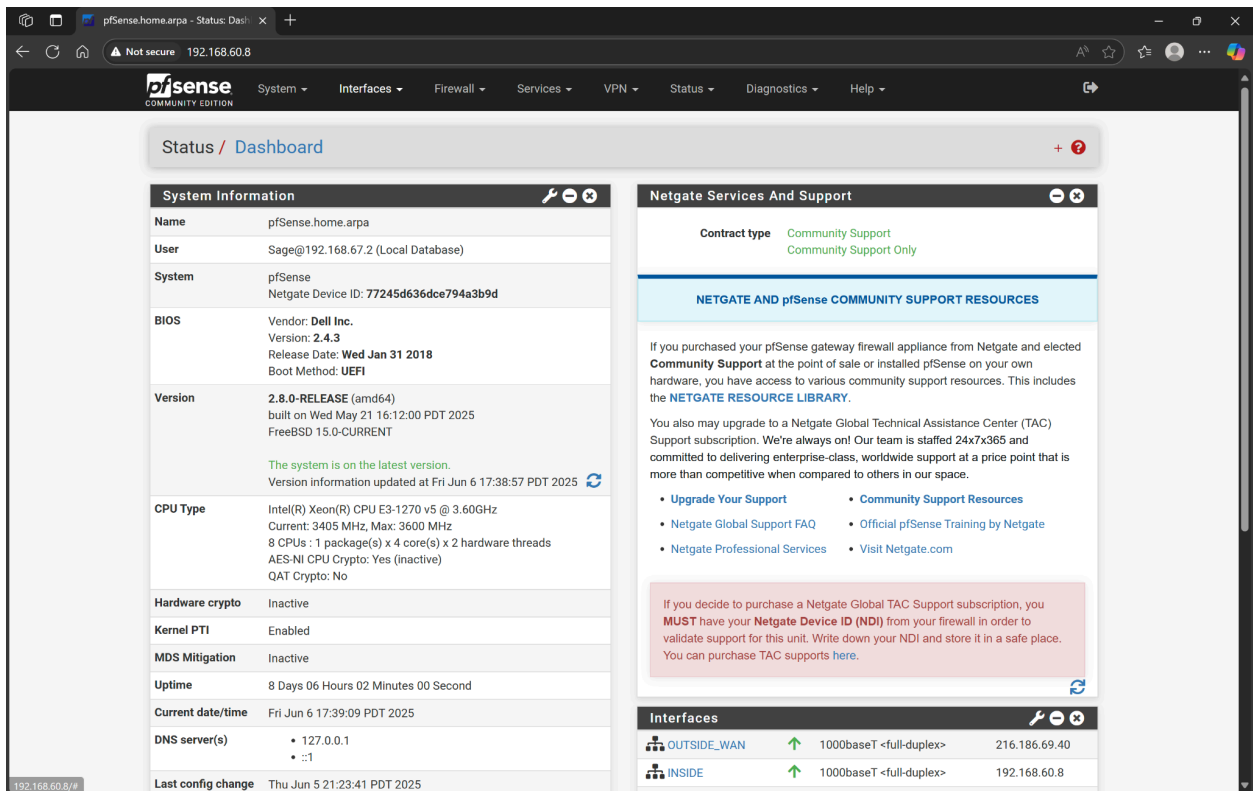
Domain: John.com

Service(s):

RRDS:

Description: Automatic routing between Inside and Branch Networks

## Pfsense Firewall(Lab Server PS22)



User(s)

Chris Cuneo

Username: Cuneo  
Password: Enigma123!

Johnathan Bowler

Username: Sage  
Password:

System Administrator

Username: Admin  
Password:

Routing:

Gateway(s):

WANGW: 216.186.69.100  
VRouter: 192.168.60.9

AdminRouter: 192.168.60.19

Static Route(s):

#1

Network: 192.168.70.0/24

Gateway: 192.168.60.9

#2

Network: 10.0.0.0/12

Gateway: 192.168.60.19

#3

Network: 10.16.0.0

Gateway: 192.168.60.19

Interfaces:

Outside\_WAN(bge0):

IP:216.186.69.40/24

Upstream Gateway: 216.186.69.100/24

Rule(s) For:

#1

Action: Pass

Associated with: NAT Rule #1

Protocol: TCP

Source: Any

Destination IP: 192.168.65.5

Destination Port: HTTP to HTTP

Description: NAT Forward to Web Server

#2

Action: Pass

Associated with: NAT Rule #2

Protocol: ICMP

Source: Any

Destination IP: 192.168.65.5

Description: NAT ICMP to Web Server

#3

Action: Pass  
Protocol: UDP  
Source: Any  
Destination IP: 216.186.69.40  
Destination Port: OpenVPN(1194) to OpenVPN(1194)  
Description: OpenVPN Open-VPN-Remote\_Access wizard

Inside(bge1):

IP:192.168.60.8/24

Rule(s) For:

#1

Description: Anti-Lockout Rule

#2

Action: Pass

Protocol: Any

Source Network: 192.168.70.0/24

Destination: Any

Description: Connectivity For Branch Network

#3

Action: Pass

Protocol: Any

Source Network: 10.0.0.0/12

Destination: Any

Description: Connectivity For Accounting Network

#4

Action: Pass

Protocol: Any

Source Network: 10.16.0.0/12

Destination: Any

Description: Connectivity For HQ Network

#5

Description: Default Allow LAN to any Rule

#6

Description: Default Allow LAN IPv6 to any Rule

#7

Action: Pass



Protocol: TCP  
Source: Any  
Destination: Inside Address  
Destination Port: HTTP to HTTP

DMZ(msk0):

IP:192.168.65.8/24

Rule(s) For:

#1

Action: Pass  
Protocol: TCP  
Source: Any  
Destination: Any  
Destination Port: HTTP to HTTP  
Description: Allow HTTP

#2

Action: Pass  
Protocol: ICMP  
Source: Any  
Destination: Any  
Description: Allow ICMP

Firewall:

NAT Rule(s):

#1

Interface: Outside\_WAN  
Protocol: TCP  
Destination 216.186.69.41/24  
Destination Port: HTTP to HTTP  
Redirect Target IP: 192.168.65.5/24  
Redirect Target Port: HTTP  
Description: Forward to Web Server

#2

Interface: Outside\_WAN

Protocol: ICMP  
Destination IP: 216.186.69.41/24  
Redirect Target IP: 192.168.65.5/24  
Description: ICMP to Web Server

Virtual IP(s):

#1  
Type: IP alias  
Interface: Outside\_WAN  
IP: 216.186.69.41/24  
Description: Web Server IP

OpenVPN:

Interface: Outside\_WAN  
Protocol: UDP4/1194(TUN)  
Tunnel Network: 192.168.67.0/24  
Local Networks: 192.168.60.0/24, 192.168.70.0/24, 10.0.0.0/12, 10.16.0.0/12  
Rules For:

#1  
Action: Pass  
Protocol: Any  
Destination: Any  
Description: OpenVPN Open-VPN-Remote\_Access wizard

## HP Switch #1(#7)

Spanning-tree: enabled

VLAN(s)

Outside

Ports: 1-4

Inside

IP:192.168.60.3  
Ports: 5-8

DMZ

IP:192.168.65.4

Ports: 9-12

Trunk Port(s):

Port 24 trunked to carry inside VLAN to HP Switch #2

## **HP Switch #2(#8)**

Spanning-tree: enabled

VLAN(s)

Inside

IP: 192.168.60.4

Ports: 5-8

Branch

IP: 192.168.70.4

Ports: 13-16

Trunk Port(s):

Port 24 trunked to carry inside VLAN to HP Switch #1

---

## **Custom Project Component**

### **Admin Router(3-13)**

Routing:

OSPF:

Ospf 1

Area: 0

Static Route(s)

IP Route 0.0.0.0 0.0.0.0 192.168.60.8

Description: Route to internet via Pfsense

Interface(s):

Serial 0/1/0

F0/0: Receives trunked traffic from VLANs Inside, HQ, and Account from Admin Switch using 802.1q

FE0.2

IP:192.168.60.19/24

FE0.3

IP:10.0.0.5/12

FE0.4

IP:10.16.0.5/12

VTY Line(s)

0-15

SSH

## **Client Router(3-14)**

Routing:

OSPF:

Ospf 1

Area: 0

Static Route(s)

IP Route 0.0.0.0 0.0.0.0 Serial0/0/1

Description: Route to internet via Admin Router

Interface(s):

Serial 1

F0/0: Receives trunked traffic from VLANs HQ, and Account from Client Switch  
using 802.1q

FE0.3

IP:10.0.0.6

FE0.4

IP: 10.16.0.6

VTY Line(s)

0-15

SSH

## **Admin Switch(2-13)**

Spanning-tree: enabled

Mode: Rapid-pvst

VLAN(s)

Inside

IP: 192.168.60.5/24

Ports: 1-4

Account

IP: 10.0.0.3/12

Ports: 5-8

HQ

IP:10.60.0.3/12

Ports: 9-12

VTY Line(s)

0-3

SSH

4-5

Telnet

ACL 16 permit 10.16.0.0 network traffic only

ACL(s)

ACL 16: Permit traffic from 10.16.0.0 in

Trunk Port(s)

Port 23: Inside, HQ and Account VLANs to router

Port 24: HQ and Account VLANs to Client Switch

## **Client Switch(4-8)**

Spanning-tree: enabled

Mode: Rapid-pvst

VLAN(s)

Account:

IP: 10.0.0.4/12

Ports: 5-8

HQ:

IP:10.60.0.3/12

Ports: 9-12

VTY Line(s)

0-3

SSH

4-5

Telnet  
ACL 16 permit 10.16.0.0 network traffic only.

Trunk Port(s):

Port 23: HQ and Account VLANs to router  
Port 24: HQ and Account VLANs to Admin Switch

ACL(s):

ACL 16 Permit traffic from 10.16.0.0 in

## **Server LS4-2**

**Virtual Machine(s):**

HQ Client:

System Information:

IP: 10.0.0.2/12  
Gateway: 10.0.0.6  
DNS: 192.168.60.1  
Internet Access? Yes

**Account Client:**

System Information:

IP: 10.16.0.2/12  
Gateway: 10.16.0.6  
DNS: 192.168.60.1  
Internet Access? Yes

## **Server LS4-3**

Virtual Machine(s):

HQ Admin:

System Information:

OS: Windows  
IP: 10.0.0.1/12  
Gateway: 10.0.0.5  
DNS: 192.168.60.1  
Internet Access? Yes

Service(s):

TFTP Server  
Description: Stores backup config for Admin Router/Switch and  
Client Router/Switch

Account Admin:

System Information:

OS: Windows  
IP: 10.16.0.1/12  
Gateway: 10.16.0.5  
DNS: 192.168.60.1  
Internet Access? Yes

Service(s):

TFTP Server  
Description: Stores backup config for Admin Router/Switch and  
Client Router/Switch