Summer 2015

Enhanced Child’s Play LAN Design

Nicholas B. Bordo
The University Of Akron, nbb5@zips.uakron.edu

Please take a moment to share how this work helps you through this survey. Your feedback will be important as we plan further development of our repository.

Follow this and additional works at: http://ideaexchange.uakron.edu/honors_research_projects

Part of the OS and Networks Commons

Recommended Citation

This Honors Research Project is brought to you for free and open access by The Dr. Gary B. and Pamela S. Williams Honors College at IdeaExchange@UAkron, the institutional repository of The University of Akron in Akron, Ohio, USA. It has been accepted for inclusion in Honors Research Projects by an authorized administrator of IdeaExchange@UAkron. For more information, please contact mjon@uakron.edu, uapress@uakron.edu.
Enhanced Child’s Play LAN Design

Nicholas Bordo
# Table of Contents

Table of Contents

- Project Plan ............................................ 2
- Project Analysis ........................................ 6
- Presentation .............................................. 8
- Project Description .................................... 13
  - IP Address Scheme ................................ 15
  - Logical Network Topology ....................... 18
  - Detailed Network Topology ..................... 19
- Network Device Configuration ..................... 20
  - Cisco 1841 Configuration ....................... 21
  - Cisco 2851 Configuration ....................... 27
  - Cisco 2960 Configuration ....................... 33
  - Cisco 3560 Configuration ....................... 38
  - Cisco Code Updates ................................ 43
- 1 VM Server Setup ..................................... 45
  - Changing Windows Server 2012 R2 Name ...... 46
  - Installing Hyper-V ................................ 48
  - Configuring IP address and DNS on Windows Server 2012 R2 ............................. 54
  - Configuring Windows Server 2012 R2 to use NTP ........................................ 57
- 2 Basic Linux Server Configurations ............. 59
  - Installing Ubuntu Server 14.04 ................ 60
  - Changing an Ubuntu Server 14.04 Hostname ........ 75
  - Configuring Ubuntu server 14.04 Ethernet interfaces ..................................... 76
  - Configuring Login Banner Messages on Ubuntu Server 14.04 ......................... 78
  - Configuring Ubuntu server 14.04 as a Syslog Client ..................................... 80
  - Configuring Ubuntu server 14.04 As a SNMP Agent ...................................... 81
- 3 DNS Server Setup .................................... 82
- 4 DHCP Server Setup ................................... 92
- 5 NTP Server Setup .................................... 97
- 6 FTP Server Setup ................................... 102
- 7 OpenNMS Setup ...................................... 122
  - Configuring OpenNMS SNMP Server Setup .......................... 123
  - Configuring SNMP for Windows Server 2012 R2 ......................... 140
- 8 Syslog Server Setup .................................. 148
- 9 Installing and configuring FileZilla Client ........ 150
  - Security Policy ..................................... 157
- Testing Documentation ................................ 158
- Weekly Journals ........................................ 165
- Research References ................................. 176
Project Plan
Nicholas Bordo

Project Name:
Enhanced Child’s Play LAN Design

Project Description:
Child’s Play is a charity event hosted by the student chapter of the Association for Computing Machinery at the University of Akron. This event allows people to compete in various video game tournaments while simultaneously raising money for charity. In order to make this possible, a network is crucial. However, in previous years, the performance has been poor. The goal of this project is to implement a new network design which will offer more functionality and reliability than in previous years. This network will be able to operate completely inside of an existing network on a temporary basis. This design offers potential use in environments other than on the campus of the University of Akron.

Existing Equipment:
- 2 Desktop PCs to be used as servers
- 2 Laptop PCs to simulate users
- Cisco 1841 Router
- Cisco 2851 Router
- Cisco 2960 Switch
- Cisco 3560 Switch

Detailed Objectives:
1. Research
   a. Open source SNMP server and Syslog server
      i. Configuration examples
      ii. Best practices for network monitoring
   b. Linux NTP Server
      i. How to run a isolated NTP server
   c. Linux FTP server
      i. Setup process of a Linux FTP server
      ii. How to configure RAID array on FTP server
      iii. How to create a folder for storage of device configuration files with restricted access
      iv. How to create a Folder for users to download game files
   d. Linux DHCP Server
      i. How to configure DHCP for Several different subnets of users.
      ii. Storing static IP addresses
   e. Linux DNS Server
      i. How to forward DNS requests onto a external server outside of the LAN
ii. How to create local domain names for LAN servers

2. Design
   a. Create network device topology
      i. Determine IP address scheme for servers, network devices, and user PCs
      ii. VLAN numbering and naming
      iii. Assign connecting interfaces of devices
      iv. Create network diagram
      v. Assign domain names to all devices in the network including virtual machines
   b. Servers
      i. Determine which servers to use for each network service
      ii. Decide which services to host as virtual machines
      iii. Determine required hardware in servers
   c. Purchasing
      i. Determine what equipment, if any, needs to be purchased
   d. Security
      i. Create authentication credentials which will be used to authenticate between network device services
      ii. Create a standard network administrator management account information
      iii. Create standard banner message for devices warning of unauthorized access to the network being restricted
      iv. Determine which hosts will be able to remotely manage network devices and who will not

3. Implementation
   a. Purchase any necessary hardware outlined in the design phase
   b. Network devices
      i. Rack devices
      ii. Update devices to most recent IOS version
      iii. Cable network connections according to the topology diagram
      iv. Connect servers to the network
      v. Assign IP addresses to device in the network according to the IP address scheme
      vi. Complete configuration of network devices
   c. Servers
      i. Install remaining hardware into servers
      ii. Remove any unnecessary hardware from servers
      iii. Install virtual machine software
      iv. Install services on servers and VMs
   d. User test PCs
      i. Install Windows 7 on one laptop
      ii. Install Linux on second laptop
      iii. Install FTP client application on both laptops

4. Testing
   a. Confirm LAN connectivity between all devices
i. Ping devices on the network using both IP addresses and domain names of devices
b. Confirm internet connectivity of all devices
   i. Ping test domain names such as Google.com to confirm internet connectivity and proper domain name resolution
c. Confirm operation of network services as seen by users.
   i. DHCP
      1. User test machines are receiving an IP address
   ii. DNS
      1. Users are able to use domain names for local and internet IP address lookups
   iii. FTP
      1. Users are able to access FTP server and are able to login and download software
d. Confirm operation of network services as seen by network devices and servers
   i. DNS
      1. Devices can be looked up using their domain names
   ii. FTP
      1. Network devices are able to backup their configuration to FTP server in a versioned format
      2. Normal users are not able to access this folder unless they are able to authenticate with the proper credentials
   iii. SNMP
      1. SNMP server is receiving traps from devices
   iv. Syslog
      1. Syslog server is receiving log messages from devices
   v. NTP
      1. Servers and network devices all have a synchronized time

5. Documentation:
   a. Project plan
   b. Project Description
      i. Description
      ii. Network Diagram
c. Network devices
      i. Performing IOS upgrade
      ii. Racking and cabling of network devices.
      iii. Router Configuration commands
      iv. Switch configuration commands
      v. Interface IP address assignment
d. Windows Virtualization Server
      i. Installation of hyper-V
      ii. Table of servers are virtualized on device
      iii. Installation of Virtual machines
e. Linux Server
      i. Installation of operating system
f. NTP Server Setup
   i. Installation of NTP server
   ii. Configuration of NTP server

g. SNMP and Syslog Server
   i. Installation of SNMP and Syslog server on Windows Virtualization server
   ii. Configuration of SNMP and Syslog server

h. FTP Server Setup
   i. Installation of RAID array in server
   ii. Configuration RAID array for storage on FTP server
   iii. Installations and configuration of FTP server
   iv. Installation of FTP client on user test laptops.

i. DHCP Server
   i. Installation and configuration DHCP server
   ii. Assignment of subnets to DHCP pools.

j. DNS Server
   i. Installation and configuration DNS server
   ii. Adding network device names to DNS.

Estimated Times:

<table>
<thead>
<tr>
<th>Planning</th>
<th>Research</th>
<th>Installation</th>
<th>Configuration</th>
<th>Testing</th>
<th>Documentation</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>20</td>
<td>10</td>
<td>40</td>
<td>20</td>
<td>30</td>
<td>130</td>
</tr>
</tbody>
</table>

Actual:

<table>
<thead>
<tr>
<th>Planning</th>
<th>Research</th>
<th>Installation</th>
<th>Configuration</th>
<th>Testing</th>
<th>Documentation</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>25</td>
<td>16</td>
<td>48</td>
<td>23</td>
<td>65</td>
<td>185</td>
</tr>
</tbody>
</table>
The Enhanced Child’s Play LAN Redesign was a successful project. All of the objectives that were placed in the project proposal were met. There were a few issues that needed to be sorted out along the way, but all issues have since been resolved. The first issue encountered was with the configuration of the DHCP server.

Configuring the isc-dhcp-server involves making many changes to the dhcpd.conf file. The syntax that is required for this file to work properly is somewhat complicated. The isc-dhcp-server service indicated that it started when rebooted, however still remained offline. This issue was resolved after creating a new version of the configuration file with the proper syntax.

After the DHCP server was functional, the next problem involved networks routing. The symptoms of this issue were that about 50% of all traffic was lost. Every other ping to google.com would time out. After some research, it was discovered that when using a Cisco device with an interface obtaining its IP via DHCP, a default route is automatically injected into the routing table of the router. This is actually the desired operation for the router, however the conflict was caused by the static route which was manually configured on the device. The router was attempting to load balance between the two static routes, but was incorrectly routing the information. Once the manually configured static route was removed, the issue was resolved.

There were also a few issues with the DNS server. The first of these problems was another syntax issue, involving the complexities of a reverse lookup. After a large amount of research, this problem was resolved. Another issue with the DNS server was slow lookup times. When this occurred, DNS requests would often time out the first time they were sent. This was caused by the internal DNS server using the routers as a primary DNS server. In turn, the routers were using the internal DNS server as their primary name servers causing a DNS request loop. Once the routers were removed as DNS servers, the issue was resolved.
The final issue was with the configuration of GLBP. The initial intention of using GLBP was to dynamically assign traffic to go to one device more often than another. The Cisco 1841 router only has a FastEthernet interface with very limited bandwidth. The Cisco 2851 has a GigabitEthernet interface, which has a much higher bandwidth cap. The idea was to have more traffic sent to the Cisco 2851 router, however the operation of the weighted load balancing method used by GLBP was misunderstood. This method operates more like interface tracking in HSPR and VRRP rather than sending more traffic to one device than another. GLBP is still configured, but this initial operational method has to be abandoned.
ENHANCED CHILD’S PLAY LAN DESIGN

Nicholas Bordo

PROJECT EXPLANATION

- Charity Event
  - Hosted by the UA ACM Student Chapter
- Poor Network performance
  - Two network crashes during event
- Internet bandwidth constraints
  - Limited internet connectivity
Original Network Design

SERVICES RUN ON ROUTER

- 1841 Router performed
  - DNS
  - DHCP
  - NAT
  - Routing(Internet)
NEW SERVICE DISTRIBUTION

- 2 Routers
  - NAT
  - Routing
    - Internet
    - GLBP
- Virtual Server (Hyper-V)
  - DHCP
  - DNS
  - NTP
  - Syslog
  - SNMP(OpenNMS)
- Physical Server
  - FTP
PROBLEMS SOLVED

- Increased internet bandwidth
- Bandwidth conservation with FTP server
- Router redundancy
- Dedicated servers for DNS and DHCP
- Logging of events in network
- Monitoring of network health.

VIDEO OF SETUP
PROBLEMS

- Routing
  - Overlapping subnets
  - 50% Packet Loss
- DHCP Configuration
- DNS
  - Reverse Lookup
  - Request timeouts
- NTP
  - Takes a long time to converge
  - Log messages using incorrect time.

Questions or Comments?
Project Description
Enhanced Child’s Play LAN Design
Nicholas Bordo

The Enhanced Child’s Play LAN Design is intended for use at the University of Akron’s ACM Student Chapter Child’s Play Charity event, which is a daylong event. Many PC and Console game tournaments are held for prizes. Traditionally, this event is held the Saturday before Thanksgiving and has an attendance of over 100 people. Tournaments are held for all different genres of games from both the PC and console worlds. For the last two years a very basic LAN design was used PC gaming room. It involved a home router connected to two switches. This kind of equipment is not truly meant for such a demanding task and hiccups ensued. The purpose of this project was to address and resolve this issue.

A basic outline of the previous setup was a Cisco 1841 router which was connected to the University’s internal network. This provided the internet connection. The router was then connected to two switches, one 2960 and one 3560. These switches were port channeled together and one of them was connected to the 1841 router. On two separate occasions the router overloaded and crashed due to the amount of users using the network. A reboot of the router fixed this issue, however there was considerable impact to the network while the router was rebooted. There was only one person capable of managing this network and it took some time for the problem to be resolved. This project was focused on addressing these issues to maximizing efficiency.

This new design utilizes all of the devices in the original setup with the addition of some new ones. An additional router was added to provide redundancy in the event that one router fails. Some of the services the router was providing have been delegated to a dedicated server. Services such as DNS and DHCP are now performed by dedicated servers. In addition to offloading these two services there will also be monitoring and diagnostic software running to more quickly resolve network issues. There will be servers for NTP to keep accurate time in the network, a Syslog server to log any problems that occur in the network, and a SNMP server to monitor the
health of the network. In order to conserve internet bandwidth an FTP server was added. This will hold a large repository of game files which can be transferred to user’s computers using the internal switched network rather than using internet bandwidth. The combination of these new elements should result in little to no network downtime at the Child's Play Charity event in coming years.
# IP Address Scheme

## Summary:

<table>
<thead>
<tr>
<th>Networks</th>
<th>172.20.32.0/19</th>
<th>172.24.64.0/20</th>
<th>192.168.128.0/22</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices</td>
<td>User VLAN 37</td>
<td>Server Addresses VLAN 10</td>
<td>Networking Devices/Management VLAN 5</td>
</tr>
<tr>
<td></td>
<td>First 20 reserved for network devices</td>
<td>First 20 reserved for network devices</td>
<td>First 20 reserved for network devices</td>
</tr>
<tr>
<td>Beginning</td>
<td>172.20.32.0</td>
<td>172.24.64.0</td>
<td>192.168.128.0</td>
</tr>
</tbody>
</table>

### VLAN 5 Management:

<table>
<thead>
<tr>
<th>Network Devices</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Interface</th>
<th>Connected Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GLBP-Gateway</td>
<td>192.168.128.1</td>
<td>255.255.252.0</td>
<td>GLBP Virtual</td>
<td>GLBP Virtual</td>
<td>VLAN 5 Gateway address of GLBP instance.</td>
</tr>
<tr>
<td>ACM-RTR-2851-gig-0-1-5</td>
<td>192.168.128.2</td>
<td>255.255.252.0</td>
<td>Fa0/1.5</td>
<td>ACM-SW-3560-fa-0-1</td>
<td></td>
</tr>
<tr>
<td>ACM-RTR-1841-fa-0-1-5</td>
<td>192.168.128.3</td>
<td>255.255.252.0</td>
<td>gig0/1.5</td>
<td>ACM-SW-2960-gig-0-1</td>
<td></td>
</tr>
<tr>
<td>ACM-SW-3560</td>
<td>192.168.128.11</td>
<td>255.255.252.0</td>
<td>VLAN 5</td>
<td>VLAN interface</td>
<td>Management ip address</td>
</tr>
<tr>
<td>ACM-SW-2960</td>
<td>192.168.128.12</td>
<td>255.255.252.0</td>
<td>VLAN 5</td>
<td>VLAN interface</td>
<td>Management ip address</td>
</tr>
<tr>
<td>ACM-RTR-2851</td>
<td>192.168.132.2</td>
<td>255.255.255.255</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACM-RTR-1841</td>
<td>192.168.132.3</td>
<td>255.255.255.255</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP Pool</td>
<td>192.168.131.250-254</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**ACM** - RTR - 2851

**ACM** - RTR - 1841
### VLAN 10 Server:

<table>
<thead>
<tr>
<th>VLAN 10 Servers</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Interface</th>
<th>Connected Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GLBP-Gateway</td>
<td>172.24.64.1</td>
<td>255.255.240.0</td>
<td>GLBP Virtual</td>
<td>GLBP Virtual</td>
<td>VLAN 10 Gateway address of GLBP instance.</td>
</tr>
<tr>
<td>ACM-RTR-2851-gig-0-1-10</td>
<td>172.24.64.2</td>
<td>255.255.240.0</td>
<td>Fa0/1.10</td>
<td>ACM-SW-3560 fa 0/1</td>
<td></td>
</tr>
<tr>
<td>ACM-RTR-1841-fa-0-1-10</td>
<td>172.24.64.3</td>
<td>255.255.240.0</td>
<td>Gig0/1.10</td>
<td>ACM-SW-2960 gig 0/1</td>
<td></td>
</tr>
<tr>
<td>ACM-VM-HOST-1</td>
<td>172.24.64.21</td>
<td>255.255.240.0</td>
<td>ACM-SW-3560 fa0/48</td>
<td>ip address of Microsoft Server hosting VM's</td>
<td></td>
</tr>
<tr>
<td>ACM-DNS-1</td>
<td>172.24.64.22</td>
<td>255.255.240.0</td>
<td>ACM-SW-3560 fa0/48</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACM-DHCP-1</td>
<td>172.24.64.23</td>
<td>255.255.240.0</td>
<td>ACM-SW-3560 fa0/48</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACM-NTP-1</td>
<td>172.24.64.24</td>
<td>255.255.240.0</td>
<td>ACM-SW-3560 fa0/48</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACM-SNMP-1</td>
<td>172.24.64.25</td>
<td>255.255.240.0</td>
<td>ACM-SW-3560 fa0/48</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACM-SYSLOG-1</td>
<td>172.24.64.26</td>
<td>255.255.240.0</td>
<td>ACM-SW-3560 fa0/48</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACM-FTP-1</td>
<td>172.24.64.27</td>
<td>255.255.240.0</td>
<td>ACM-SW-2960 Gig0/2</td>
<td>On gig port to maximize bandwidth available to LAN for FTP Transfers</td>
<td></td>
</tr>
<tr>
<td>DHCP Pool</td>
<td>172.24.79.0-255</td>
<td>255.255.240.0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Range: 172.24.64.0 - 172.24.79.255

First 20 reserved for network devices
VLAN 37 User:

<table>
<thead>
<tr>
<th>Network Devices</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Interface</th>
<th>Connected Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GLBP-Gateway</td>
<td>172.20.32.1</td>
<td>255.255.224.0</td>
<td>GLBP Virtual</td>
<td>GLBP Virtual</td>
<td>VLAN 10 Gateway address of GLBP instance.</td>
</tr>
<tr>
<td>ACM-RTR-2851-gig-0-1-10</td>
<td>172.20.32.2</td>
<td>255.255.224.0</td>
<td>Fa0/1.10</td>
<td>ACM-SW-3560 fa 0/1</td>
<td></td>
</tr>
<tr>
<td>ACM-RTR-1841-fa-0-1-10</td>
<td>172.20.32.3</td>
<td>255.255.224.0</td>
<td>Gig0/1.10</td>
<td>ACM-SW-2960 gig 0/1</td>
<td></td>
</tr>
<tr>
<td>User-pool</td>
<td>172.20.32.21-172.20.63.255</td>
<td>255.255.224.0</td>
<td></td>
<td>IP addresses that will be used for users connecting to the network.</td>
<td></td>
</tr>
</tbody>
</table>
Logical Network Topology
<table>
<thead>
<tr>
<th>Network Device Configuration</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 1841 Configuration</td>
<td>21</td>
</tr>
<tr>
<td>Cisco 2851 Configuration</td>
<td>27</td>
</tr>
<tr>
<td>Cisco 2960 Configuration</td>
<td>33</td>
</tr>
<tr>
<td>Cisco 3560 Configuration</td>
<td>38</td>
</tr>
<tr>
<td>Cisco Code Updates</td>
<td>43</td>
</tr>
</tbody>
</table>
Cisco 1841 Configuration
Configuration Explanation for ACM Cisco 1841

For the purposes of these instructions, anything after “#” is a comment for the benefit of the reader to better explain the function of a command.

Hostname:
hostname acm-rtr-1841
    #Changes the hostname

Security Configuration:
service password-encryption
    #Enables encryption of passwords in running configuration
enable secret 5 $1$.OWX$iTBgfa8tMnw0rLh4i9bE7.
    #Sets enable password. Password is shown encrypted refer to security documentation for further information.

username acm1an privilege 15 secret 5 $1$bO/.$zUNnFZpnR9WuoHHnamRPr.
    #Creates the admin user account. Password is shown encrypted refer to security documentation for further information.

key chain cisco
    #Used for authentication between protocols.
key 8512
    key-string 7 032752180500701E1D48
        #Key is shown encrypted refer to security documentation for further information.

no ip http server
    #Disables web interface configuration
no ip http secure-server
    #Disables secure web interface configuration

Clock:
clock timezone US/EST -5
    #Sets time zone to Eastern Standard Time.
clock summer-time US/EST recurring
    #Allows for time adjustment during Daylight savings
ntp update-calendar
    #This updates the router’s hardware clock
ntp server 172.24.64.24 prefer
    #This sets the NTP server to sync with internal NTP server

Logging:
logging buffered 4096
logging source-interface Loopback0
    #Logs will originate from the IP address of the loopback 0 interface
logging 172.24.64.26

**DNS Information:**
ip domain name tydrous.tv
  # Specifies the domain name the device belongs to.
ip name-server 172.24.64.22
  # Specifies the name server to use.

**DNS Server:**
# Disable if internal DNS server is functioning.

ip dns server
  # Allows the server to act as a forwarding DNS Server
ip dns spoofing
  # Spoofs the DNS requests and forwards to a DNS Server. Disable if internal DNS server is functioning.

**Automatic Backup of device configurations:**
archive
  path ftp://172.24.64.27/archive/$h/$h-$t
    # Sets the location of FTP server and name of file.
    # $h dynamically inserts the hostname of the device.
    # $t is the current time when the file was sent to the FTP server.

write-memory
  # Whenever a write memory is done the configuration is backup to the ftp server.

# FTP Username and password for configuration backup
ip ftp username acm1an
ip ftp password 703281A18055F16435C0210
  # Password is shown encrypted. Refer to security documentation for further information.

kron occurrence archive-conf in 2:0 recurring
  # Performs the following policy every 2 hours
  policy-list acm-archive

kron policy-list acm-archive
  # Does the following command when the policy is called.
  cli write

**SNMP:**
snmp-server community AKacmRe@d0Nly RO
  # Sets the read only community string
snmp-server community wR1t3RD@kacMmgnt RW
  # Sets the read write community string
snmp-server trap-source Loopback0
    #Traps for this device will originate from the address of the Loopback0 interface.

#SNMP device details
snmp-server location ACM Akron Childs Play Rack B Right side of PC Gaming room
snmp-server contact Nicholas Bordo @ 330-703-9601

#Various traps device will send
snmp-server trap link ietf
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps eigrp
snmp-server enable traps envmon
snmp-server enable traps flash insertion removal
snmp-server enable traps cpu threshold
snmp-server enable traps syslog

snmp-server host 172.24.64.25 AKacmRe@d0Nly udp-port 161
    #Address, community string, and port number

Banner Message:
banner login ^C
============================================================================
Access Restricted!
============================================================================

These devices are the property of the University of Akron Student
Chapter of the ACM. Access to network resources is restricted to
authorized personnel only. Please disconnect immediately if you are
not an authorized user. All activity on these devices is logged.
============================================================================

^C
Configuration access:
line con 0
    exec-timeout 15 0
        #Session will time out after 15 minutes.
logging synchronous
login local
    #Uses local user database for authentication
line aux 0
line vty 0 4
    exec-timeout 15 0
logging synchronous
login local
transport input ssh
    #Allows SSH access to devices
transport output all
line vty 5 15
exec-timeout 15 0
logging synchronous
login local
transport input ssh
transport output all

**Interface configuration:**
interface Loopback0
ip address 192.168.132.3 255.255.255.255
  #Sets IP address of loopback interface

interface FastEthernet0/0
description UPLINK TO OUTSIDE NETWORK
ip address dhcp
  #Gets IP address via host network. Also automatically sets default static route
ip nat outside
  #NAT internet facing interface

interface FastEthernet0/1
description UPLINK TO acm-sw-3560
no ip address
ip nat inside

#Management VLAN sub interface
interface FastEthernet0/1.5
description UPLINK TO acm-sw-3560
encapsulation dot1Q 5
  #Sets encapsulation type between router interface and switch
ip address 192.168.128.3 255.255.252.0
  #Sets IP address
ip nat inside
  #Configures this interface as a LAN facing interface.

#Server VLAN sub interface
interface FastEthernet0/1.10
description UPLINK TO acm-sw-3560
encapsulation dot1Q 10
ip address 172.24.64.3 255.255.240.0
ip nat inside

interface FastEthernet0/1.37
description UPLINK TO acm-sw-3560
encapsulation dot1Q 37
ip address 172.20.32.3 255.255.224.0
ip helper-address 172.24.64.23
ip nat inside
**GLBP Configuration:**

```
track 1 interface FastEthernet0/0 line-protocol
    #Used for GLBP fail over if internet interface goes down down.
```

```
#Management VLAN sub interface GLBP Configuration
interface FastEthernet0/1.5
glp 5 ip 192.168.128.1
    #Sets the Virtual IP address of the default gateway

glp 5 priority 130
    #This router will be the AVG for this VLAN
glp 5 preempt
    #Allows a device with a higher priority to take over as AVG at any time.
glp 5 weighting 130 lower 80 upper 90
    #Sets weight values
glp 5 load-balancing weighted
    #Changes load-balancing type from round robin to weighted

glp 5 authentication md5 key-chain cisco
    #Uses the cisco key to validate GLBP neighbors
glp 5 weighting track 1 decrement 60
    #Decreases weight of the tracked interface if the internet interface goes down. Operates very similarly to interface tracking for HSRP and VRRP.
```

```
#Server VLAN sub interface GLBP Configuration
interface FastEthernet0/1.10
glp 10 ip 172.24.64.1

glp 10 priority 110 #This router will be the AVF for this VLAN
glp 10 preempt
glp 10 weighting 110 lower 80 upper 90
glp 10 load-balancing weighted

glp 10 authentication md5 key-chain cisco
glp 10 weighting track 1 decrement 40
```

```
#User VLAN sub interface GLBP Configuration
interface FastEthernet0/1.37

glp 37 ip 172.20.32.1

glp 37 priority 110 #This router will be the AVF for this VLAN
glp 37 preempt
glp 37 weighting 110 lower 80 upper 90
glp 37 load-balancing weighted

glp 37 authentication md5 key-chain cisco
glp 37 weighting track 1 decrement 40
```

**EIGRP:**

```
router eigrp 373
    #Autonomous system number
passive-interface FastEthernet0/0
    #Does not send routing updates out these interfaces
```
passive-interface FastEthernet0/1.10
    #Does not send routing updates out these interfaces
passive-interface FastEthernet0/1.37
    #Does not send routing updates out these interfaces
network 172.20.32.0 0.0.31.255
    #User VLAN Network
network 172.24.64.0 0.0.15.255
    #Server VLAN Network
network 192.168.128.0 0.0.3.255
    #Management VLAN Network
network 192.168.132.3 0.0.0.0
    #Loopback interface
no auto-summary
    #Does not summarize on classful boundaries.

NAT:
ip nat inside source list 101 interface FastEthernet0/0 overload
    #Sets up Port Address translation on internet facing interface for LAN uses.

#ACL To define the inside networks to be translated
access-list 101 permit ip 172.20.32.0 0.0.31.255 any
access-list 101 permit ip 172.24.64.0 0.0.15.255 any
access-list 101 permit ip 192.168.128.0 0.0.3.255 any
access-list 101 permit ip host 192.168.132.3 any
Cisco 2851 Configuration
Configuration Explanation for ACM Cisco 2851

For the purposes of these instructions, anything after "#" is a comment for the benefit of the reader to better explain the function of a command.

Hostname:
hostname acm-rtr-2851
#Changes the hostname

Security Configuration:
service password-encryption
#Enables encryption of passwords in running configuration
enable secret 5 $1$.OWX$iTBgf8tMrw0rLh4i9bE7.
#Sets enable password. Password is shown encrypted refer to security documentation for further information.

username acm1an privilege 15 secret 5 $1$bO/.$zUNnFZpnR9WuoHHnamRPr.
#Creates the admin user account. Password is shown encrypted refer to security documentation for further information.

key chain cisco
#Used for authentication between protocols.
key 8512
key-string 7 032752180500701E1D48
#Key is shown encrypted refer to security documentation for further information.

no ip http server
#Disables web interface configuration
no ip http secure-server
#Disables secure web interface configuration

Clock:
clock timezone US/EST -5
#Sets time zone to Eastern Standard Time.
clock summer-time US/EST recurring
#Allows for time adjustment during Daylight savings
ntp update-calendar
#This updates the router's hardware clock
ntp server 172.24.64.24 prefer
#This sets the NTP server to sync with internal NTP server

Logging:
logging buffered 4096
logging source-interface Loopback0
#Logs will originate from the IP address of the loopback 0 interface

logging 172.24.64.26

**DNS Information:**

ip domain name tydrous.tv
  #Specifies the domain name the device belongs to.

ip name-server 172.24.64.22
  #Specifies the name server to use.

**DNS Server:**

  #Disable if internal DNS server is functioning.

ip dns server
  #Allows the server to act as a forwarding DNS Server

ip dns spoofing
  #Spoofs the DNS requests and forwards to a DNS Server. Disable if internal DNS server is functioning.

**Automatic Backup of device configurations:**

archive
  path ftp://172.24.64.27/archive/$h/$h-$t
    #Sets the location of FTP server and name of file.
    # $h dynamically inserts the hostname of the device.
    # $t is the current time when the file was sent to the FTP server.

write-memory
  #Whenever a write memory is done the configuration is backup to the ftp server.

#FTP Username and password for configuration backup
ip ftp username acm1an
ip ftp password 703281A18055F16435C0210
  #Password is shown encrypted. Refer to security documentation for further information.

kron occurrence archive-conf in 2:0 recurring #Performs the following policy every 2 hours
  policy-list acm-archive

kron policy-list acm-archive #Does the following command when the policy is called.
  cli write

**SNMP:**

snmp-server community AKacmRe@d0Nly RO
  #Sets the read only community string

snmp-server community wR1t3RD@kacMmgnt RW
  #Sets the read write community string

snmp-server trap-source Loopback0
#Traps for this device will originate from the address of the Loopback0 interface.

#SNMP device details
snmp-server location ACM Akron Childs Play Rack A Left side of PC Gaming room
snmp-server contact Nicholas Bordo @ 330-703-9601

#Various traps device will send
snmp-server trap link ietf
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps eigrp
snmp-server enable traps envmon
snmp-server enable traps flash insertion removal
snmp-server enable traps cpu threshold
snmp-server enable traps syslog

snmp-server host 172.24.64.25 AKacmRe@d0N!y udp-port 161
    #Address, community string, and port number

Banner Message:
banner login ^C
===================================================================
Access Restricted!

These devices are the property of the University of Akron Student Chapter of the ACM. Access to network resources is restricted to authorized personnel only. Please disconnect immediately if you are not an authorized user. All activity on these devices is logged.
===================================================================

^C

Configuration access:
line con 0
    exec-timeout 15 0
        #Session will time out after 15 minutes.
    logging synchronous
    login local
        #Uses local user database for authentication
line aux 0
line vty 0 4
    exec-timeout 15 0
    logging synchronous
    login local
    transport input ssh
        #Allows SSH access to devices
transport output all
line vty 5 15
exec-timeout 15 0
logging synchronous
login local
transport input ssh
transport output all

**Interface configuration:**

interface Loopback0
ip address 192.168.132.2 255.255.255.255
    #Sets IP address of loopback interface

interface GigabitEthernet0/0
description UPLINK TO OUTSIDE NETWORK
ip address dhcp
    #Gets IP address via host network. Also automatically sets default static route
ip nat outside
    #NAT internet facing interface

interface GigabitEthernet0/1
description UPLINK TO acm-sw-2960
no ip address
ip nat inside
    #Configures this interface as a LAN facing interface.

#Management VLAN sub interface
interface GigabitEthernet0/1.5
description UPLINK TO acm-sw-2960
encapsulation dot1Q 5
    #Sets encapsulation type between router interface and switch
ip address 192.168.128.2 255.255.252.0
    #Sets IP address
ip helper-address 172.24.64.23
    #Directs DHCP Requests to the DHCP Server
ip nat inside
    #Configures this interface as a LAN facing interface.

#Server VLAN sub interface
interface GigabitEthernet0/1.10
description UPLINK TO acm-sw-2960
encapsulation dot1Q 10
ip address 172.24.64.2 255.255.252.0
ip helper-address 172.24.64.23
ip nat inside

interface GigabitEthernet0/1.37
description UPLINK TO acm-sw-2960
encapsulation dot1Q 37
ip address 172.20.32.2 255.255.224.0
ip helper-address 172.24.64.23
ip nat inside

**GLBP Configuration:**

track 1 interface FastEthernet0/0 line-protocol
    #Used for GLBP fail over if internet interface goes down down down.

#Management VLAN sub interface GLBP Configuration
interface FastEthernet0/1.5
glbp 5 ip 192.168.128.1
    #Sets the Virtual IP address of the default gateway

glbp 5 priority 110
    #This router will be the AVG for this VLAN
glbp 5 preempt
    #Allows a device with a higher priority to take over as AVG at any time.
glbp 5 weighting 110 lower 80 upper 90
    #Sets weight values
glbp 5 load-balancing weighted
    #Changes load-balancing type from round robin to weighted
glbp 5 authentication md5 key-chain cisco
    #Uses the cisco key to validate GLBP neighbors
glbp 5 weighting track 1 decrement 40
    #Decreases weight of the tracked interface if the internet interface goes down. Operates very similarly to interface tracking for HSRP and VRRP.

#Server VLAN sub interface GLBP Configuration
interface FastEthernet0/1.10
glbp 10 ip 172.24.64.1
glbp 10 priority 130 #This router will be the AVG for this VLAN
glbp 10 preempt
glbp 10 weighting 130 lower 80 upper 90
glbp 10 load-balancing weighted
glbp 10 load-balancing weighted
glbp 10 authentication md5 key-chain cisco
glbp 10 weighting track 1 decrement 60

#User VLAN sub interface GLBP Configuration
interface FastEthernet0/1.37
glbp 37 ip 172.20.32.1
glbp 37 priority 130 #This router will be the AVG for this VLAN
glbp 37 preempt
glbp 37 weighting 130 lower 80 upper 90
glbp 37 load-balancing weighted
glbp 37 load-balancing weighted
glbp 37 authentication md5 key-chain cisco
glbp 37 weighting track 1 decrement 60
**EIGRP:**

router eigrp 373

  #Autonomous system number
  passive-interface GigabitEthernet0/0
    #Does not send routing updates out these interfaces
  passive-interface GigabitEthernet0/1.10
    #Does not send routing updates out these interfaces
  passive-interface GigabitEthernet0/1.37
    #Does not send routing updates out these interfaces

  network 172.20.32.0 0.0.31.255
    #User VLAN Network
  network 172.24.64.0 0.0.15.255
    #Server VLAN Network
  network 192.168.128.0 0.0.3.255
    #Management VLAN Network
  network 192.168.132.2 0.0.0.0
    #Loopback interface

  no auto-summary
    #Does not summarize on classful boundaries.

**NAT:**

ip nat inside source list 101 interface GigabitEthernet0/0 overload

  #Sets up Port Address translation on internet facing interface for LAN uses.

  #ACL To define the inside networks to be translated
  access-list 101 permit ip 172.20.32.0 0.0.31.255 any
  access-list 101 permit ip 172.24.64.0 0.0.15.255 any
  access-list 101 permit ip 192.168.128.0 0.0.3.255 any
  access-list 101 permit ip host 192.168.132.3 any
For the purposes of these instructions, anything after “#” is a comment for the benefit of the reader to better explain the function of a command.

**Hostname:**
hostname acm-sw-2960
#Changes the hostname

**Security Configuration:**
service password-encryption
#Enables encryption of passwords in running configuration
enable secret 5 $1$.OWX$iTBgfa8tMnw0rLh4i9bE7.
#Sets enable password. Password is shown encrypted refer to security documentation for further information.

username acm1an privilege 15 secret 5 $1$bO/.$zUNnFZpnR9WuoHHnamRPr.
#Creates the admin user account. Password is shown encrypted refer to security documentation for further information.

key chain cisco
#Used for authentication between protocols.
key 8512
key-string 7 032752180500701E1D48
#Key is shown encrypted refer to security documentation for further information.

no ip http server
#Disables web interface configuration
no ip http secure-server
#Disables secure web interface configuration

**Clock:**
clock timezone US/EST -5
#Sets time zone to Eastern Standard Time.
clock summer-time US/EST recurring
#Allows for time adjustment during Daylight savings
service timestamps log datetime localtime
#This updates the switch's hardware clock
ntp server 172.24.64.24 prefer
#This sets the NTP server to sync with internal NTP server

**Logging:**
logging buffered 4096
logging source-interface Vlan5
# Logs will originate from the IP address of the Vlan 5 interface

logging 172.24.64.26

**DNS Information:**
ip domain name tydrous.tv
  # Specifies the domain name the device belongs to.
ip name-server 172.24.64.22
  # Specifies the name server to use.

**DNS Server:**
# Disable if internal DNS server is functioning.

ip dns server
  # Allows the server to act as a forwarding DNS Server
ip dns spoofing
  # Spoofs the dns requests and forwards to a DNS Server. Disable if internal DNS server is functioning.

**Automatic Backup of device configurations:**
archive
path ftp://172.24.64.27/archive/$h/$h-$t
  # Sets the location of FTP server and name of file.
  # $h dynamically inserts the hostname of the device.
  # $t is the current time when the file was sent to the FTP server.

write-memory
  # Whenever a write memory is done the configuration is backup to the ftp server.

# FTP Username and password for configuration backup
ip ftp username acm1an
ip ftp password 703281A18055F16435C0210
  # Password is shown encrypted. Refer to security documentation for further information.

kron occurrence archive-conf in 2:0 recurring # Performs the following policy every 2 hours
policy-list acm-archive

kron policy-list acm-archive # Does the following command when the policy is called.
cli write

**SNMP:**
snmp-server community AKacmRe@d0Nly RO
  # Sets the read only community string
snmp-server community wR1t3RD@kacMmgnt RW
  # Sets the read write community string
snmp-server trap-source Vlan5
#Traps for this device will originate from the address of the Vlan5 interface.

#SNMP device details
snmp-server location ACM Akron Childs Play Rack A Left side of PC Gaming room
snmp-server contact Nicholas Bordo @ 123-456-7890

#Various traps device will send
snmp-server trap link ietf
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps eigrp
snmp-server enable traps envmon
snmp-server enable traps flash insertion removal
snmp-server enable traps cpu threshold
snmp-server enable traps syslog
snmp-server host 172.24.64.25 AKacmRe@d0N!y udp-port 161
   #Address, community string, and port number

**Banner Message:**

banner login ^C
====================================================================
Access Restricted!
These devices are the property of the University of Akron Student
Chapter of the ACM. Access to network resources is restricted to
authorized personnel only. Please disconnect immediately if you are
not an authorized user. All activity on these devices is logged.
====================================================================
^C

**Configuration access:**

line con 0
   exec-timeout 15 0
      #Session will time out after 15 minutes.
logging synchronous
login local
      #Uses local user database for authentication
line aux 0
line vty 0 4
   exec-timeout 15 0
logging synchronous
login local
transport input ssh
      #Allows SSH access to devices
transport output all
line vty 5 15
   exec-timeout 15 0
logging synchronous
login local
transport input ssh
transport output all

**VTP:**
vtp domain ACM-VTP
   #Sets VTP domain to arbitrary value. Not used.
vtp mode transparent
   #Will add VLANs to its database from VTP but will not send out VLAN information.

**Spanning Tree:**
spanning-tree mode pvst
   #Sets spanning tree type to per VLAN spanning tree

**VLAN Database:**
vlan 5
   name MANAGEMENT

vlan 10
   name SERVERS

vlan 37
   name USERS

**Port Channels:**
interface Port-channel2
   description PORT-CHANNEL to acm-sw-3560
   switchport mode trunk
      #Sets switchport to trunking for port channel between two switches.

**Interface configuration:**
interface range FastEthernet0/1-42
   #Applies configuration changes to interfaces FA0/1-FA0/42 at the same time.
description USER INTERFACE TO LAN
   switchport access vlan 37
      #Sets the access VLAN to User vlan
   switchport mode access
      #Changes the mode of the interface to access
   spanning-tree portfast
      #Forces the port to go into forwarding state much faster
   spanning-tree bpduguard enable
      #Disables port if a switch is detected trying to participate in spanning tree.

interface range FastEthernet0/43-46
   #Applies configuration changes to interfaces FA0/1-FA0/42 at the same time.
description PORT-CHANNEL to acm-sw-3560
   switchport mode trunk
      #Changes the mode of the interface to trunking between the two switches
channel-group 2 mode desirable
# Forces the creation of a port channel on these interfaces and those on the neighboring switch.

interface FastEthernet0/47
description MANAGEMENT INTERFACE
switchport access vlan 5
# Sets the access VLAN to the Management VLAN
switchport mode access
# Changes the mode of the interface to access

interface FastEthernet0/48
description MANAGEMENT INTERFACE
switchport access vlan 5
switchport mode access

interface GigabitEthernet0/1
description UPLINK TO acm-rtr-2851
switchport mode trunk

interface GigabitEthernet0/2
description TO acm-ftp-1
switchport access vlan 10
# Sets the access VLAN to the Server VLAN
switchport mode access
# Changes the mode of the interface to access
switchport port-security mac-address sticky
# Allows a device to be connected to an interface, but no others can be connected. Port will shut down if another mac address is seen on the interface.
spanning-tree portfast
# Forces the port to go into forwarding state much faster
spanning-tree bpduguard enable
# Disables port if a switch is detected trying to participate in spanning tree.

interface Vlan1
no ip address
no ip route-cache
shutdown
# Disables the default management VLAN

interface Vlan5
description MANAGEMENT INTERFACE
ip address 192.168.128.12 255.255.252.0
# This sets the IP address of the management interface. Used to access the device.

Routing:
ip default-gateway 192.168.128.1
# Sets a default gateway for the switch
Cisco 3560 Configuration
Configuration Explanation for ACM Cisco 3560

For the purposes of these instructions, anything after "#" is a comment for the benefit of the reader to better explain the function of a command.

Hostname:
hostname acm-sw-3560
    #Changes the hostname

Security Configuration:
service password-encryption
    #Enables encryption of passwords in running configuration
enable secret 5 $1$.OWX$iTBgfa8tMnw0rLh4i9bE7.
    #Sets enable password. Password is shown encrypted refer to security documentation for further information.

username acm1an privilege 15 secret 5 $1$bO/.$zUNnFZpnR9WuoHHnamRPr.
    #Creates the admin user account. Password is shown encrypted refer to security documentation for further information.

key chain cisco
    #Used for authentication between protocols.
key 8512
    key-string 7 032752180500701E1D48
        #Key is shown encrypted refer to security documentation for further information.

no ip http server
    #Disables web interface configuration
no ip http secure-server
    #Disables secure web interface configuration

Clock:
clock timezone US/EST -5
    #Sets time zone to Eastern Standard Time.
clock summer-time US/EST recurring
    #Allows for time adjustment during Daylight savings
service timestamps log datetime localtime
    #This updates the switch’s hardware clock
ntp server 172.24.64.24 prefer
    #This sets the NTP server to sync with internal NTP server

Logging:
logging buffered 4096
logging source-interface Vlan5
    #Logs will originate from the IP address of the Vlan 5 interface
logging 172.24.64.26

**DNS Information:**
ip domain name tydrous.tv    
    #Specifies the domain name the device belongs to.
ip name-server 172.24.64.22  
    #Specifies the name server to use.

**DNS Server:**  
#Disable if internal DNS server is functioning.

ip dns server  
    #Allows the server to act as a forwarding DNS Server
ip dns spoofing  
    #Spoofs the dns requests and forwards to a DNS Server. Disable if internal DNS server is functioning.

**Automatic Backup of device configurations:**
archive  
path ftp://172.24.64.27/archive/$h/$h-$t  
    #Sets the location of FTP server and name of file.  
    # $h dynamically inserts the hostname of the device.  
    # $t is the current time when the file was sent to the FTP server.
write-memory  
    #Whenever a write memory is done the configuration is backup to the ftp server.

#FTP Username and password for configuration backup  
ip ftp username acm1an  
ip ftp password 703281A18055F16435C0210  
    #Password is shown encrypted. Refer to security documentation for further information.

kron occurrence archive-conf in 2:0 recurring  
    #Perform the following policy every 2 hours
policy-list acm-archive  

kron policy-list acm-archive  
    #Does the following command when the policy is called.
cli write

**SNMP:**
snmp-server community AKacmRe@d0Nly RO  
    #Sets the read only community string
snmp-server community wR1t3RD@kacMmgnt RW  
    #Sets the read write community string
snmp-server trap-source Vlan5
    #Traps for this device will originate from the address of the Vlan5 interface.

#SNMP device details
snmp-server location ACM Akron Childs Play Rack A Left side of PC Gaming room
snmp-server contact Nicholas Bordo @ 123-456-7890

#Various traps device will send
snmp-server trap link ietf
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps eigrp
snmp-server enable traps envmon
snmp-server enable traps flash insertion removal
snmp-server enable traps cpu threshold
snmp-server enable traps syslog
snmp-server host 172.24.64.25 AKacmRe@d0N!y udp-port 161
    #Address, community string, and port number

Banner Message:
banner login ^C
====================================================================
Access Restricted!

These devices are the property of the University of Akron Student
Chapter of the ACM. Access to network resources is restricted to
authorized personnel only. Please disconnect immediately if you are
not an authorized user. All activity on these devices is logged.
====================================================================
^C

Configuration access:
line con 0
    exec-timeout 15 0
        #Session will time out after 15 minutes.
logging synchronous
login local
    #Uses local user database for authentication
line aux 0
line vty 0 4
    exec-timeout 15 0
logging synchronous
login local
    transport input ssh
        #Allows SSH access to devices
transport output all
line vty 5 15
    exec-timeout 15 0
logging synchronous
login local
transport input ssh
transport output all

VTP:
vtp domain ACM-VTP
   #Sets VTP domain to arbitrary value. Not used.
vtp mode transparent
   #Will add VLANs to its database from VTP but will not send out VLAN information.

Spanning Tree:
spanning-tree mode pvst
   #Sets spanning tree type to per VLAN spanning tree

VLAN Database:
vlan 5
   name MANAGEMENT

vlan 10
   name SERVERS

vlan 37
   name USERS

Port Channels:
interface Port-channel2
   description PORT-CHANNEL to acm-sw-3560
   switchport mode trunk
      #Sets switchport to trunking for port channel between two switches.

Interface configuration:
interface range FastEthernet0/1-42
   #Applies configuration changes to interfaces FA0/1-FA0/42 at the same time.
description USER INTERFACE TO LAN
switchport access vlan 37
   #Sets the access VLAN to User vlan
switchport mode access
   #Changes the mode of the interface to access
spanning-tree portfast
   #Forces the port to go into forwarding state much faster
spanning-tree bpduguard enable
   #Disables port if a switch is detected trying to participate in spanning tree.

interface range FastEthernet0/43-46
   #Applies configuration changes to interfaces FA0/1-FA0/42 at the same time.
description PORT-CHANNEL to acm-sw-2960
switchport mode trunk
    #Changes the mode of the interface to trunking between the two switches
channel-group 2 mode desirable
    #Forces the creation of a port channel between these interfaces and those on the neighboring switch.

interface FastEthernet0/47
description MANAGEMENT INTERFACE
switchport access vlan 5
    #Sets the access VLAN to the Management VLAN
switchport mode access
    #Changes the mode of the interface to access

interface FastEthernet0/47
description UPLINK TO acm-rtr-1841
switchport trunk encapsulation dot1q
switchport mode trunk

interface FastEthernet0/48
description VM SERVER
switchport access vlan 10
    #Sets the access VLAN to the Server VLAN
switchport mode access
    #Changes the mode of the interface to access
switchport port-security mac-address sticky
    #Allows a device to be connected to an interface, but no others can be connected. Port will shut down if another mac address is seen on the interface.
spanning-tree portfast
    #Forces the port to go into forwarding state much faster
spanning-tree bpduguard enable
    #Disables port if a switch is detected trying to participate in spanning tree.

interface Vlan1
no ip address
no ip route-cache
shutdown
    #Disables the default management VLAN

interface Vlan5
description MANAGEMENT INTERFACE
ip address 192.168.128.11 255.255.255.252.0
    #This sets the IP address of the management interface. Used to access the device.

**Routing:**
ip default-gateway 192.168.128.1
    #Sets a default gateway for the switch
Cisco Code Upgrades

For the purposes of these instructions, anything after "#" is a comment for the benefit of the reader to better explain the function of a command.

Transferring the new code to the device:

In order to complete a code upgrade, the new code must first be placed onto the device. This can be done by transferring the code from an FTP server or a USB flash drive, if the device is capable. This example will use a FTP server. Here is the command to begin the transfer:

```
acm-sw-3560# copy ftp://172.24.64.27/archive/acm-sw-3560/code/c3560-ipservicesk9-mz.122-55.SE10.bin flash:
```

172.24.64.27 is the IP address of the FTP server
/archive/acm-sw-3560/code/c3560-ipservicesk9-mz.122-55.SE10.bin is the path and filename.
flash: is the local destination of the file.

When the transfer is complete, the cli should look similar to this:

```
12749374 bytes copied in 260.997 secs (47996 bytes/sec)
acm-sw-3560
```

Now that the new code file has been transferred to the switch, the device must be told to boot to that code.

Enter configuration terminal and use the boot command to specify the location of the code file to boot from.

```
acm-sw-3560(config)#boot system flash:c3560-ipservicesk9-mz.122-55.SE10.bin
```

Use the show boot command to verify that the new code will be used on boot.

show boot

```
ACM-SW-3560#show boot
BOOT path-list : flash:c3560-ipservicesk9-mz.122-55.SE10.bin
Config file : flash:/config.text
Private Config file : flash:/private-config.text
Enable Break : no
Manual Boot : no
TFTP path-list : 
Auto upgrade : yes
Auto upgrade path : 
NVRAM/Config file buffer size : 524288
Timeout for Config Download : 0 seconds
Config Download via TFTP: disabled (next boot: disabled)
```
The system is ready to reload and begin using the new code.

   acm-sw-3560#reload

After the device has reloaded check the version of code the device is running.

   show version

Device has been successfully upgraded to a new code.
VM Server Setup

Changing Windows Server 2012 R2 Name 46
Installing Hyper-V 48
Configuring IP address and DNS on Windows Server 2012 R2 54
Configuring Windows Server 2012 R2 to use NTP 57
Changing Windows Server 2012 R2 Name

For the purposes of these instructions, anything after “#” is a comment for the benefit of the reader to better explain the function of a command.

Changing server name:

In the Server Manager, click on the current name of the server.

In this window, select the “Change…” button to configure the new name of the server.
In the dialog that appears, enter the desired name of the server and click “OK”.

For this name change to take effect, the server must be rebooted.

After reboot the name change is complete.
Installing Hyper-V
These instructions are for installing Hyper-V on Windows Server 2012 R2

For the purposes of these instructions, anything after “#” is a comment for the benefit of the reader to better explain the function of a command.

Start with a clean installation of Windows Server 2012 R2

Adding the Hyper-V Role:
In order to add the Hyper-V, access the Server manager and click on the “Manage” drop down. Then, select the “Add Roles and Features” option.

This will bring up the Add Roles and Features Wizard. “Role based or feature-based installation” is the option that is appropriate for adding Hyper-V. Click Next.
In this window select, the server to add the Hyper-V Role. Click “Next” when the server has been selected.

In this list is where the Hyper-V option is located. Check the box for Hyper-V. Click Next.
A dialog box will appear with a list of dependent features, which must be installed along with Hyper-V. These are required for the operation of Hyper-V. Click “Add Features” and click Next again to continue.

This window is where features would be added, however, no additional features need to be installed at this time to complete the Hyper-V installation. Click Next.
Here is where the configuration of the various Hyper-V specific options begins. Click Next.

First, a virtual switch must be created for the Virtual machines Hyper-V. These VMs will use this switch to communicate with the rest of the network while only being physically connected to one Ethernet cable. Check the box next to the Ethernet adapter to use for the virtual switch and click “Next”.

![Create Virtual Switches](image-url)
This tutorial will not be utilizing the Migration feature. Click “Next” to skip.

Here is where the default storage locations of the VMs will be. The defaults can be used or custom folders can be created. Click “Next”.

---

Hyper-V can be configured to send and receive live migrations of virtual machines on this server. Configuring Hyper-V now enables any available network on this server to be used for live migrations. If you want to dedicate specific networks for live migration, use Hyper-V settings after you install the role.

- **Allow this server to send and receive live migrations of virtual machines**

  - **Authentication protocol**
    - Select the protocol you want to use to authenticate live migrations.
    - **Use Credential Security Support Provider (CredSSP)**: This protocol is less secure than Kerberos, but does not require you to set up constrained delegation. To perform a live migration, you must be logged in to the source server.
    - **Use Kerberos**: This protocol is more secure but requires you to set up constrained delegation in your environment to perform tasks such as live migration when managing this server remotely.

If this server will be part of a cluster, do not enable migration now. Instead, you will configure the server for live migration, including specifying networks, when you create the cluster.

---

Hyper-V uses default locations to store virtual hard disk files and virtual machine configuration files, unless you specify different locations when you create the files. You can change these default locations now, or you can change them later by modifying Hyper-V settings.

- **Default location for virtual hard disk files**: C:VMs\VHD
- **Default location for virtual machine configuration files**: C:VMs\Configuration Files
Configuration of Hyper-V is now complete and the install process can begin. Click “Install” to begin the installation of the new role onto the server. A restart will be required before these changes can take effect.

Once the install is finished, click “Close” and restart the server.

Installation of Hyper-V is complete.
Configuring IP address and DNS on Windows Server 2012 R2
These instructions are for setting a static IP and DNS on Windows Server 2012 R2

For the purposes of these instructions, anything after “#” is a comment for the benefit of the reader to better explain the function of a command.

This tutorial will be using the domain name tydrous.tv. This procedure will work for any other domain name simply replace tydrous.tv with the different domain.

**Start with a clean installation of Windows Server 2012 R2**

**Setting a Static IP address and DNS server:**
Right click on the network icon in the taskbar and select the “Open Network and Sharing Center”.

In the Network sharing Center select the “Change adapter settings” option in the top left corner of the window.

Select the adapter that is connected to the network. In this case, it will be the virtual switch adapter used by Hyper-V. Right click on the adapter and select “Properties”.

```
Troubleshoot problems
Open Network and Sharing Center
```

```
Control Panel Home
Change adapter settings
Change advanced sharing settings
```

```
Network Connections
```

```
Organize ▼ Disable this network device Diagnose this connection Rename this connection ▼
```

```
Ethernet
Enabled
Intel(R) Ethernet Connection 1217-V
```

```
vEthernet [Intel(R) Ethernet Connection 1217-V - Virtual Switch)
```

```
Unidentified network
```
Scroll down to the bottom and select the “Internet Protocol Version 4 (TCP/IPv4) and select “Properties”.

Select “Use the following IP address” and enter the IP address information of the device and the default gateway information. Then select “Use the following DNS server addresses” and enter the desired DNS server.
Now hit the “Advanced…” button to open the advanced IP configurations dialog. Then, select the DNS tab.

Here, select the “Add…” button under the DNS suffix option.

In the dialog that appears, enter the domain name suffix of the network. In this case, enter “tydrous.tv”.

Configuration of static IP address and DNS server is complete.
Configuring Windows Server 2012 R2 to use NTP

For the purposes of these instructions, anything after "#" is a comment for the benefit of the reader to better explain the function of a command.

This tutorial will be using the domain name tydrous.tv. This procedure will work for any other domain name simply replace tydrous.tv with the different domain.

**Configuring NTP Clock**

To configure Windows server 2012 to use NTP click on the clock in the bottom right of the screen. This will bring up the calendar window.

Once the Calendar is open click on the button “Change date and time settings”. This will bring up the windows to edit the Internet time.

Click on “Internet Time”.

![Calendar window showing the change date and time settings button](image-url)
Click on “Change settings…”

This will bring up the dialog box where the time server can be selected. Type in the name of the NTP server to use in the server box and click “Update now”. Then click “OK”.

**Configuration of Windows server 2012 R2 for NTP is complete.**
Basic Linux Server Configurations

Installing Ubuntu Server 14.04 60
Changing an Ubuntu Server 14.04 Hostname 75
Configuring Ubuntu server 14.04 Ethernet interfaces 76
Configuring Login Banner Messages on Ubuntu Server 14.04 78
Configuring Ubuntu server 14.04 as a Syslog Client 80
Configuring Ubuntu server 14.04 As a SNMP Agent 81
Installing Ubuntu server 14.04

For the purposes of these instructions, anything after “#” is a comment for the benefit of the reader to better explain the function of a command.

**Downloading the ISO file:**
Navigate to [www.ubuntu.com/download/server](http://www.ubuntu.com/download/server) and click on the “Download” button. The download should start automatically once the next page loads.

![Download Ubuntu Server](image)

**Download Complete**

**Creating a Virtual Machine:**
If a virtual machine has already been created, it may be easier to simply import the already created template virtual machine rather than complete the remainder of the installation process.

Once the ISO file has been downloaded, the Ubuntu Server to be installed.

Start by opening the Hyper-V Manager. Once this is open select the “Action” drop down to “New” and the “Virtual Machine...”.
This will open, a new window where the name of the Virtual Machine can be specified. There is also an option to save the virtual machine in a location other than the default. Once finished, click the “Next” button.

The next window offers a choice between two options: Generation 1 and Generation 2. For the purposes of this tutorial, Generation 1 is acceptable. Click “Next” when finished.
The next screen allows for the allocation of system memory to the VM. 2 Gigabytes of memory, or 2048 MB, should be sufficient for the basic Ubuntu server installation. This amount can be altered later. Check the “Use Dynamic Memory” option to allow Hyper-V to dynamically assign memory to the virtual machine as needed during operation. Click “Next” when finished.
Next, the Ethernet interface needs to be assigned to the VM. When using multiple VMs, it is necessary for a virtual switch to be used. Select from the drop down. A new virtual switch may need to be created. Click “Next” when finished.

Next the virtual hard disk needs to be created. This is where the operation system will be installed. Do not forget to change the value of the virtual hard disk. This could create a virtual hard disk that is larger than necessary. A 30GB hard drive should be more than enough.
Next is where the ISO downloaded previously will come into play. Select the “Install an Operating system from a bootable CD/DVD-ROM” Option and then “Image file(.iso):” Now browse to the location of the ISO downloaded previously and click “Next” to continue.

A summary of all the parameters configured in the process are displayed. Click “Finish” to complete the VM creation.

Creation of Virtual Machine Complete.
Installation of Ubuntu 14.04:

Now that the virtual machine is created, the Ubuntu Operating system needs to be installed. Go to the Hyper-V Manager and right click on the Virtual machine that was just created. Select the “Start” option and then the “Connect” option. This will begin the startup process of the new virtual machine and the VM will automatically boot to the ISO that was previously specified.

From this point on, the installation process is the same as a dedicated server. The only difference is that when booting for a normal server, a flash drive or CD/DVD would be used as the boot media instead of an ISO file.

Once the server has finished booting, the installation process can begin. Select a language to continue.
Once the Language is selected, the installation screen will be shown. Select “Install Ubuntu Server.

This will begin the installation process where again a language will need to be selected.
Set the location of the server. This will be used for time purposes.

The keyboard layout will need to be determined. Select “No” for the detect configuration of the keyboard layout.
Select the appropriate keyboard layout.

Ubuntu will begin the process of loading all of the necessary files for the installation process. After this process is complete, the server will automatically detect an IP address using DHCP. Once this auto detection is complete, a hostname will need to be set for the installation of Ubuntu. Hit Tab and Enter to continue.
Now a basic user will need to be created. A generic username and password will be used in this tutorial, but any username and password can be used here. Hit Tab and Enter to continue.

Enter a username. Hit Tab and Enter to continue.

Enter a password. Hit Tab and Enter to continue.
Verify the password previously entered. Hit Tab and Enter to continue.

The Ubuntu Server gives the option of encrypting the home directory of this user.

Now Ubuntu will attempt to set up the clock. Verify the information presented.

Begin partitioning the hard drive of the server. Select the option “Guided - use entire disk and set up LVM.”
There may be a list of options if several hard drives are connected to the server. Select the desired to be the boot hard drive.

More advanced partition options are available, however this tutorial will not cover them. Select “Yes” to continue hard drive partitioning.

The default value is the full size of the disk. Hit Tab and Enter to continue.
To complete the partitioning of the disk, hit “Yes”.

At this point, the installation process will begin working on writing information to the hard disk, which was just partitioned. This can take quite a while depending on the system.

After this process has finished, a dialog box will appear asking about any proxy settings. This can be left blank. Hit Tab and Enter to continue.

After this Ubuntu will begin configuring apt which is used to update and install packages in Ubuntu. After that is complete, the server will begin to install packages. Once this is finished, the server will ask what time of update management should be used. Automatic updates can be used, but for this tutorial no automatic updates will be selected.
Here are some other optional packages that can be installed. Only the OpenSSH server will be selected in this tutorial. Installation of other protocols will be covered in other tutorials done post operating system installation. Use the arrow keys to move up and down and spacebar to select the packages to install. Hit Tab and Enter to continue.

This package will now be downloaded and installed. This will take a while.

Finally, once the installation is finished the server will ask if GRUB should be installed to the master boot record. Since this is the only operating system being installed on this server, select “Yes”.

After this dialog, the installation is finished. Hit continue to reboot the server. If doing a VM installation, Hyper-V will automatically remove the ISO from the boot options. If installing on a physical server, remove the boot media before rebooting.
After reboot, a screen similar the screen picture below should appear and the server is now ready for further configuration.

Installation of Ubuntu Server 14.04 is Complete.
Changing an Ubuntu Server 14.04 Hostname

For the purposes of these instructions, anything after "#" is a comment for the benefit of the reader to better explain the function of a command.

This tutorial will be using the domain name tydrous.tv. This procedure will work for any other domain name simply replace tydrous.tv with the different domain.

**Editing the Hosts file:**
In order to change the hostname of an Ubuntu device, there are two files that need to be edited.

```
sudo vim /etc/hosts
```

The default configuration of this file will look similar to this.

```
127.0.0.1 localhost
default-tvd
127.0.1.1 basic-install.tydrous.tv basic-install
# The following lines are desirable for IPv6 capable hosts:
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Here is what renaming an Ubuntu server host looks like when the name is changed to renamed-install. Save and exit the file when finished.

```
127.0.0.1 localhost
default-tvd
127.0.1.1 renamed-install.tydrous.tv renamed-install
172.24.79.1 renamed-install.tydrous.tv
# The following lines are desirable for IPv6 capable hosts:
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

The second file that needs to be edited is the hostname file:

```
sudo vim /etc/hostname
```

This file will only contain one line, which can be replaced with the new name of the server. Save and exit the file when finished.

After that file has been edited, the server needs to reboot for the change to take effect.

```
sudo reboot
```

**Ubuntu Server name change complete.**
Configuring Ubuntu server 14.04 Ethernet interfaces

For the purposes of these instructions, anything after "#" is a comment for the benefit of the reader to better explain the function of a command.

This tutorial will be using the domain name tydrous.tv. This procedure will work for any other domain name simply replace tydrous.tv with the different domain.

**Editing the interfaces file:**

```
sudo vim /etc/network/interfaces
```

#This file holds the interface IP address information loaded on boot.
#Opens the file using vim for editing with write privileges
#Hit the “i” key to enter insert mode in vim

The file will look similar to this:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet dhcp
```

This configuration of the primary network interface is using DHCP to obtain an IP address. This is not the ideal setup for a server. To set a static IP address, comment out both of the statements for the primary network interface and add the following:

```
auto eth0
iface eth0 inet static
    address 172.24.64.27 #IP address of the server or host
    gateway 172.24.64.1 #Default gateway of the subnet
    netmask 255.255.240.0 #Subnet mask
    network 172.24.64.0 #Network address of the subnet
    broadcast 172.24.79.255 #Broadcast address of the subnet
    dns-nameserver 172.24.64.22 #IP of the DNS server.
```

If the DNS server is not yet configured on the network, use one of the gateway devices as the DNS server temporarily. 172.24.64.2 or 172.24.64.3

The final file should look similar to this:

```
# The loopback network interface
```
auto lo
iface lo inet loopback
# The primary network interface

#UNCOMMENT TO RE-ENABLE DHCP
#auto eth0
#iface eth0 inet dhcp

#STATIC IP CONFIG
auto eth0
iface eth0 inet static
address 172.24.64.22
gateway 172.24.64.1
netmask 255.255.240.0
network 172.24.64.0
broadcast 172.24.79.255
dns-nameservers 172.24.64.22
dns-domain tydrous.tv

#Once this information has been added, save and exit the file.
#In vim, hit the “Esc” key, type “:wq”, and hit “Enter”

Now, either restart the networking daemon or reboot the server
sudo service networking restart

or

sudo reboot

Configuration of Ethernet Interface is complete.
Configuring Login Banner Messages on Ubuntu Server 14.04

For the purposes of these instructions, anything after "#" is a comment for the benefit of the reader to better explain the function of a command.

Creating the banner message file:
By default, the banner message file that is used is the issue.net file

```
sudo vim /etc/issue.net
```

Any information that is currently in the file can be deleted and replaced with a custom banner message. Here is an example banner message:

```
==================================================================
Access Restricted!
These devices are the property of the University of Akron Student
Chapter of the ACM. Access to network resources is restricted to
authorized personnel only. Please disconnect immediately if you are
not an authorized user. All activity on these devices is logged.
==================================================================
```

Save and exit the file when the custom message has been entered.

Banner message creation complete.

Editing the SSH config file to show the Banner message:
By default, SSH does not enable this feature. Open the sshd_config file and scroll close to the bottom of the file.

```
sudo vim /etc/ssh/sshd_config
```

Uncomment the line "Banner /etc/issue.net". This is the default file and path used for this feature, but this can be changed to be anything if desired.

```
PrintLastLog yes
TCPKeepAlive yes
#UseLogin no

#MaxStartups 10:30:60
Banner /etc/issue.net

# Allow client to pass locale environment variables
AcceptEnv LANG LC_-

Subsystem sftp /usr/lib/openssh/sftp-server
```

Configuration of the SSH config file is complete.
Restart the SSH Process:

Now that the files have been configured, the SSH process has to be restarted for these changes to take effect.

```
sudo service ssh restart
```

SSH Process has been restarted.

Verifying the operation of the SSH Banner Message:

At this point, the device should be ready for testing SSH to the device using form of terminal emulator or another Linux machine. If the configuration was completed successfully, the message should display after a username has been entered.

```
login as: cisco
Access Restricted!
These devices are the property of the University of Akron Student Chapter of the ACM. Access to network resources is restricted to authorized personnel only. Please disconnect immediately if you are not an authorized user. All activity on these devices is logged.
cisco@acm-dns-1's password: *
```

SSH banner message on Ubuntu Server 14.04 is complete.
Configuring Ubuntu server 14.04 as a Syslog Client

These instructions are for configuring rsyslog as a client on Ubuntu Server 14.04

For the purposes of these instructions, anything after "#" is a comment for the benefit of the reader to better explain the function of a command.

**Alterations to Client Configuration file:**

In order for devices to make use of this new server, an addition needs to be made to the rsyslog file. The following statement needs to be added to any participating Ubuntu servers. This IP address is the IP of the syslog server:

```
.*@172.24.64.26
```

Save and exit the file.

**Alterations to Client Configuration file are complete.**

**Restarting the client rsyslog Process:**

Now that the file has been configured to use an external syslog server, the rsyslog process needs to be restarted.

```
sudo service rsyslog restart
```

Now that the client is finished setting up the rsyslog service, the logs should be visible in the directory specified in the previous step.

```
ls /var/log/remote-logs
```

Configuration of rsyslog is complete.
Configuring Ubuntu server 14.04 as a SNMP Agent

For the purposes of these instructions, anything after “#” is a comment for the benefit of the reader to better explain the function of a command.

**Installing the SNMPD Package:**

```
sudo apt-get update  #Updates the apt list of packages
sudo apt-get install snmpd  #Installs the snmpd package
```

Type “y” for yes to verify installation of this package if prompted.

**Editing the interfaces file:**

Save a backup of the original configuration file
```
sudo mv /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.back
```

Create and edit the snmpd.conf file. Alter information for specific device:
```
sudo vim /etc/snmp/snmpd.conf
```

```
rocommunity AKacmRe@d0N!y
syslocation "ACM Akron Childs Play Rack B Right side of PC Gaming room"
syscontact Nicholas Bordo @ 123-456-7890
```

rocommunity = the read only community string
syslocation = Text description of location of device
syscontact = Contact information for technician responsible for device.

```
rocommunity AKacmRe@d0N!y
syslocation "ACM Akron Childs Play Rack B Right side of PC Gaming room"
syscontact Nicholas Bordo @ 123-456-7890
```

Edit the snmpd file to use the file previously configured. Comment out the existing line and add in the line as follows.

```
sudo vim /etc/default/snmpd
```

```
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -l smux,muxtrigger,muxTriggerConf -p /var/run/snmpd.pid -c /etc/snmp/snmpd.conf'
```

Save and exit the file.

Restart the snmpd process
```
sudo service snmpd restart
```

**SNMP Agent Configuration Complete**
DNS Server Setup
These instructions are for installing Bind9 on Ubuntu Server 14.04

For the purposes of these instructions, anything after “#” is a comment for the benefit of the reader to better explain the function of a command.

This tutorial will be using the domain name tydrous.tv. This procedure will work for any other domain name simply replace tydrous.tv with the different domain.

**Start with a clean installation of Ubuntu 14.04**
Refer to the instructions on how to install Ubuntu Server 14.04 for a clean installation.

**Set the interface information for the server:**
Refer to the instructions for configuring Ubuntu Server 14.04 Ethernet interfaces.

NOTE:
In this setup, use the default gateway address as the DNS name server. Since the DNS server is not yet working, this server will need to use the DNS function of the gateway in order to download the Bind9 package later in these instructions. Use the example in the Configuring Ubuntu Server 14.04 Ethernet interfaces instructions.

**Set hostname of server:**
Refer to the instructions for changing an Ubuntu Server 14.04 hostname.

**Installing the DNS Server Package Bind9:**
```
sudo apt-get update          #Updates the apt list of packages
sudo apt-get install bind9   #Installs the Bind9 package
```

Type “y” for yes to verify installation of this package if prompted.

**Beginning Bind9 Configuration:**

**First file to edit is “/etc/bind/named.conf.options**
Before editing, create a backup of the named.conf.options
```
sudo cp /etc/bind/named.conf.options /etc/bind/named.conf.options.back
```

```
sudo vim /etc/bind/named.conf.options
```
The file will look similar to this. Comments have been removed for clarity.

```
options {
    directory "/var/cache/bind";
    dnssec-validation auto;
    auth-nxdomain no;  # conform to RFC1035
    listen-on-v6 { any; };
};
```
To allow only internal users to be able to query this DNS server, configure an Access Control List (ACL) to for internal user IP addresses only. Add the following lines at the top of the file above options.

```
acf "goodusers" {
    192.168.128.0/22;
    192.168.132.0/24;
    172.24.64.0/20;
    172.20.32.0/19;
    localhost;
    localnets;
};
```

To use this ACL to restrict query access add the following:

```
recursion yes;
allow-query { goodusers; };
```

Configure the IP address the DNS server will listen on for DNS requests.

```
listen-on { 172.24.64.22; };
```

Disable zone transfers between DNS servers:

```
allow-transfer { none; };
```

Configure the servers this internal server will send DNS queries to if the internal DNS does not have any results for the query.

```
forwarders {
    #Unknown DNS requests will be sent to the servers in the following list.
    8.8.8.8;       #Google public DNS server
    8.8.4.4;      #Google public DNS server
    #If available include the DNS server of the ISP
};
```
The complete file should look similar to this:

```plaintext
acl "goodusers" {
  192.168.128.0/22;
  192.168.132.0/24;
  172.24.64.0/20;
  172.20.32.0/19;
  localhost;
  localnets;
};

options {
  directory "/var/cache/bind";

  recursion yes;
  allow-query { goodusers; };
  listen-on { 172.24.64.22; };
  allow-transfer { none; };
  forwarders {
    8.8.8.8;
    8.8.4.4;
  };

  //forward only:

  //--------------
  // If BIND logs error messages about the root key being expired,
  // you will need to update your keys. See https://www.isc.org/bind-keys
  //--------------
  dnssec-enable yes;
  dnssec-validation yes;

  auth-nxdomain no;  // conform to RFC1035
  listen-on-v6 { any; };
};
```

Once this information has been added, save and exit the file. In vim, hit the “Esc” key, type “:wq”, hit “Enter”.

**named.conf.options configuration complete.**

**Second file to edit /etc/bind/named.conf.local**

```plaintext
sudo vim /etc/bind/named.conf.local
```

This file should be mostly empty, and will look similar to this.

```plaintext
// Do any local configuration here

//

// Consider adding the 1918 zones here, if they are not used in your
// organization
#include "/etc/bind/zones.rfc1918";
```

Add the following lines to the bottom of the file.
//FORWARD LOOKUP ZONES holds A records, maps hostnames to IPs

zone "tydrous.tv"
{
    type master;
    file "/etc/bind/zones/db.tydrous.tv";
};

//REVERSE LOOKUP ZONES Holds PTR records, maps IP address to a hostname

//User Subnet
zone "20.172.in-addr.arpa" IN {
    type master;
    file "/etc/bind/zones/db.20.172";
    allow-update { none; };
};

//Server Subnet
zone "24.172.in-addr.arpa" IN {
    type master;
    file "/etc/bind/zones/db.24.172";
    allow-update { none; };
};

//Network device subnet
zone "168.192.in-addr.arpa" IN {
    type master;
    file "/etc/bind/zones/db.168.192";
    allow-update { none; };
};

Once this information has been added, save and exit the file.
In vim, hit the “Esc” key, type “:wq”, hit “Enter”

Explanation:
Since this is the first DNS server to be configured for this domain, the type must be master.

At this point, this directory and file does not exist and will be created in a later step. File names can be anything, the db included at the beginning is just by convention. This must match the name of the file created in the later step. The same applies to the reverse lookup zone, however, naming of the file is important.

The zone name for the reverse lookup table must be the inverse of the IP address of the DNS server, excluding the first octet of the IP address. For example a DNS server with the IP address of 192.168.1.50 would have a reverse lookup zone name of 1.168.192.in-addr.arpa.

**Verification of named.conf files:**
To verify that the two named.conf files, named.conf.local and named.conf.options have been properly configured use the following command:

```
sudo named-checkconf
```

If no text has been output, then no errors were found in the named.conf files.

**Creating zone files:**

**First create the zones directory:**
```
sudo mkdir /etc/bind/zones
```

#This will be where the database files are put which were pointed to in the named.conf.local file previously.

**Create the forward lookup zone file:**
There are some template files that are provided in the Bind directory. Copy the /etc/bind/db.local file to the zones directory with the name given in the named.conf.local file for the forward lookup zone. In this case, db.tydrous.tv was used.
```
sudo cp /etc/bind/named.conf.local /etc/bind/zones/db.tydrous.tv
```

After being copied will look similar to this:
```
; BIND data file for local loopback interface
;
@ IN NS localhost.
@ IN A 127.0.0.1
@ IN AAAA ::1
;
@ IN SOA localhost. root.localhost. ( 2 2 604800 864000 604800 ) ; Negative Cache TTL
@ IN 604800 2 86400 2419200 604800 ; Serial Refresh Retry Expire
```
This file is what Bind uses to look up hostnames and map them to IP addresses when queried. All of the devices on the network will be given a name and a corresponding IP address, which will also be listed here. Here is a sample configuration file:

```
$TTL 604800
@ IN SOA acm-dns-1.tydrous.tv. root.tydrous.tv. ( 2 ; Serial
604800 ; Refresh
86400 ; Retry
2419200 ; Expire
604800 ) ; Negative Cache TTL

@ IN NS acm-dns-1.

; LOOPBACK INTERFACES
acm-rtr-2851 IN A 192.168.132.2
acm-rtr-1841 IN A 192.168.132.3

; MANAGEMENT VLAN IP ADDRESSES
mgmt-gw IN A 192.168.128.1
acm-rtr-2851-mgmt IN A 192.168.128.2
acm-rtr-1841-mgmt IN A 192.168.128.3
acm-sw-3560 IN A 192.168.128.11
acm-sw-2960 IN A 192.168.128.12

; SERVER VLAN IP ADDRESSES
srvr-gw IN A 172.24.64.1
acm-rtr-2851-srvr IN A 172.24.64.2
acm-rtr-1841 IN A 172.24.64.3
acm-vm-host-1 IN A 172.24.64.21
acm-dns-1 IN A 172.24.64.22
acm-dhcp-1 IN A 172.24.64.23
acm-ntp-1 IN A 172.24.64.24
acm-snmp-1 IN A 172.24.64.25
acm-syslog-1 IN A 172.24.64.26
acm-ftp-1 IN A 172.24.64.27

; USER VLAN IP ADDRESSES
usr-gw IN A 172.20.32.1
acm-rtr-2851-usr IN A 172.20.32.2
acm-rtr-1841-usr IN A 172.20.32.3
```

# Once this information has been added, save and exit the file.
# In vim, hit the “Esc” key, type “:wq”, and hit “Enter”

Explanation:

All of the default values in the top portion of the file can be left the way they are, with the exception of the localhost information. This needs to be changed to reflect the information of the DNS server for the domain along with the domain information.

The home address information 127.0.0.1 and the IPv6 address can be removed.
Creation of the forward lookup zone file is complete.

**Forward Lookup zone file verification:**
Bind9 comes with a tool that can be used to check the configuration files for syntax errors. The first parameter is the domain name being used, and the second is the full path of the file being verified.

```
named-checkzone tydrous.tv /etc/bind/zones/db.tydrous.tv
```

If the command outputs something similar to the following image with the OK status, then the file contains no Syntax errors. If there is an error, the tool will supply and line number where the error can be found and corrected.

```
cisco@acm-dns-1:/etc/bind/zones$ named-checkzone tydrous.tv /etc/bind/zones/db.tydrous.tv
zone tydrous.tv/IN: loaded serial 2
OK
cisco@acm-dns-1:/etc/bind/zones$
```

Forward Lookup zone file verification complete.

**Create the reverse lookup zone file:**
Since there are several subnets being used in this network, there will need to be three different reverse lookup files. These files will be used to take IP addresses and map them to names. The reverse lookup files can be very tricky, so make sure to follow the configuration examples below. There is also a tool available to generate large reverse lookup tables here:

http://www.zytrax.com/books/dns/ch3/#ipv4-calculator

For each of these reverse lookup files, only the last 2 octets need to be included, however, in reverse order and followed by the type of file and the name. **A period is required at the end of each name.**

```
sudo vim /etc/bind/zones/db.20.172
```

db.20.172 file contents:

```
$TTL 172800 ; default TTL = two days
$ORIGIN 20.172.in-addr.arpa.
@ 3600 SOA acm-dns-1.tydrous.tv. hostmaster.tydrous.tv. 1 172800 900 1209600
  NS acm-dns-1.tydrous.tv. ;Subnet device addresses
  1.32  PTR usr-gw.tydrous.tv.
  2.32  PTR acm-rtr-2851-gig0-1-37.tydrous.tv.
  3.32  PTR acm-rtr-1841-fa-0-1-37.tydrous.tv.
```

```
sudo vim /etc/bind/zones/db.24.172
```

```
db.24.172 file contents:

$TTL 172800 ; default TTL = two days
$ORIGIN 24.172.in-addr.arpa.
@   SOA acm-dns-1.tydrous.tv. hostmaster.tydrous.tv. 1 172800 900 1209600
    3600
    NS acm-dns-1.tydrous.tv.
1.64  PTR srvr-gw.tydrous.tv.
2.64  PTR acm-rtr-2851-gig0-1-10.tydrous.tv.
3.64  PTR acm-rtr-1841-gig0-1-10.tydrous.tv.
21.64 PTR acm-vm-host-1.tydrous.tv.
22.64 PTR acm-dns-1.tydrous.tv.
23.64 PTR acm-dhcp-1.tydrous.tv.
24.64 PTR acm-ntp-1.tydrous.tv.
25.64 PTR acm-snmp-1.tydrous.tv.
26.64 PTR acm-syslog-1.tydrous.tv.
27.64 PTR acm-ftp-1.tydrous.tv.

sudo vim /etc/bind/zones/db.168.192

db.168.192 file contents:

$TTL 172800 ; default TTL = two days
$ORIGIN 168.192.in-addr.arpa.
@   SOA acm-dns-1.tydrous.tv. hostmaster.tydrous.tv. 1 172800 900 1209600
    3600
    NS acm-dns-1.tydrous.tv.
1.128  PTR mgmt-gw.tydrous.tv.
2.128  PTR acm-rtr-2851-gig0-1-5.tydrous.tv.
3.128  PTR acm-rtr-1841-fa-0-1-5.tydrous.tv.
11.128 PTR acm-sw-3560.tydrous.tv.
12.128 PTR acm-sw-2960.tydrous.tv.
2.132  PTR acm-rtr-2851.tydrous.tv.
3.132  PTR acm-rtr-1841.tydrous.tv.

#Once this information has been added, save and exit the file.
#In vim, hit the “Esc” key, type “:wq”, and hit “Enter”

Explanation:

Similar to the information changed in the top half of the db.tydrous.tv file, the localhost information must be switched out with the name of the DNS server and its domain. All other default values can be retained.

The number that is in the @ column represents the IP address on the subnet
**Starting Bind9:**

Now Bind9 is ready to be started.

```
sudo service bind9 restart
```

* Stopping domain name service... bind9
  waiting for pid 2710 to die

* Starting domain name service... bind9

Check the syslog file for error messages if the bind9 did not start properly.

```
tail -f /var/log/syslog
```

For information on how to configure devices to use this DNS server, refer to the following:

- Configuring Ubuntu server 14.04 Ethernet interfaces
- Configuring IP address and DNS Server for Windows Server 2012 R2

**Bind startup is now complete.**

**Verification of Bind9:**

Use the `nslookup` command to verify the operation of Bind9.

To verify internal forward lookup, use `nslookup` to query for the IP address of a device by its hostname.

```
cisco@acm-dns-1:~$ nslookup acm-ftp-1
Server:    172.24.64.22
Address:   172.24.64.22#53
Name:      acm-ftp-1.tydrous.tv
Address:    172.24.64.27
```

To verify internal reverse lookup, use `nslookup` to query for the hostname of a device by its IP address.

```
cisco@acm-dns-1:~$ nslookup 172.24.64.27
Server:      172.24.64.22
Address:     172.24.64.22#53

27.64.24.172.in-addr.arpa  name = acm-ftp-1.tydrous.tv.
```

To verify external forward lookup, use `nslookup` to query for the IP address of a domain name such as google.com
To verify external reverse lookup, use nslookup to query for the domain name of an IP address such as Google’s public DNS servers 8.8.8.8.

Do this verification again using a Windows device on the USER VLAN, using the command prompt to run the same checks using the nslookup command. If all checks come back with the proper results, the configuration of Bind9 is Complete.

**Configuration of Bind9 is Complete.**
DHCP Server Setup
These instructions are for installing isc-dhcp-server on Ubuntu Server 14.04

For the purposes of these instructions, anything after "#" is a comment for the benefit of the reader to better explain the function of a command.

This tutorial will be using the domain name tydrous.tv. This procedure will work for any other domain name simply replace tydrous.tv with the different domain.

**Start with a clean installation of Ubuntu 14.04**
Refer to the instructions on how to install Ubuntu Server 14.04 for a clean installation.

**Set the interface information for the server:**
Refer to the instructions for configuring Ubuntu Server 14.04 Ethernet interfaces.

**Set hostname of server:**
Refer to the instructions for changing an Ubuntu Server 14.04 hostname.

**Installing the DHCP Server Package isc-dhcp-server:**
sudo apt-get update  #Updates the apt list of packages
sudo apt-get install isc-dhcp-server  #Installs the dhcpcd package

Type “y” for yes to verify installation of this package if prompted.

Disregard the “fail” message that may displayed during the installation process. Since the dhcp server is not yet installed it fails to start.

**Beginning DHCP Configuration:**

**First file to edit is “/etc/dhcp/dhcpd.conf”**

```bash
sudo vim /etc/dhcp/dhcpd.conf
#Opens the file using vim for editing with write privileges
#Hit the “i” key to enter insert mode in vim
#Once this file is open, there will be several lines which start with the “#” symbol. These are commented templates for setting up network subnets that the server will use to hand out IP addresses.

Uncomment the section for the “internal subnet”. This section should look something like the following:

```bash
subnet 10.5.5.0 network 255.255.255.224 {
    range 10.5.5.26 10.5.5.30;
    option domain-name-server ns1.internal.example.org;
    option domain-name “internal.example.org”;
    option routers 10.5.5.1;
```
option broadcast-address 10.5.5.31;
default-lease-time 600;
max-lease-time 7200;
}

This information will be replaced with the information for the USER VLAN network.
subnet 172.20.32.0 netmask 255.255.224.0 {
   range 172.20.32.21 172.20.63.254;

   option routers 172.20.32.1;
   option domain-name-servers 172.24.64.22;
   option domain-name "tydrous.tv";
   option broadcast-address 172.20.63.255;
   option subnet-mask 255.255.224.0;

   default-lease-time 600;
   max-lease-time 7200;
}

Explanation:
   option domain-name-server specifies the DNS server which will be provided to the DHCP clients.

   option domain-name sets the domain of DHCP clients

   option router sets the default gateway provided to the DHCP clients

   option broadcast-address is simple the broadcast address of the subnet

   default-lease-time is the length of time a client will be reserved a specific IP address

If the server will be on a different subnet than the DHCP clients an additional subnet statement will be needed for the DHCP servers subnet, but left empty.

This would look similar to this:
subnet 172.24.64.0 network 255.255.240.0 {
}

Or if a portion of the server subnet is going to be used for DHCP for new server installation use the following:

subnet 172.24.64.0 netmask 255.255.240.0 {
   range 172.24.79.1 172.24.79.254;
option domain-name-servers 172.24.64.22;
option domain-name "tydrous.tv";
option routers 172.24.64.1;
option broadcast-address 172.24.79.255;

default-lease-time 600;
max-lease-time 7200;
}

The final result of the dhcpd.conf file will look similar to this:

```
subnet 172.20.32.0 netmask 255.255.255.240 {
  range 172.20.32.21 172.20.63.254;
  option routers 172.20.32.1;
  option domain-name-servers 172.24.64.22;
  option domain-name "tydrous.tv";
  option broadcast-address 172.20.63.255;
  option subnet-mask 255.255.255.0;
  default-lease-time 600;
  max-lease-time 7200;
}
```

```
subnet 172.24.64.0 netmask 255.255.255.240 {
  range 172.24.79.1 172.24.79.254;
  option domain-name-servers 172.24.64.22;
  option domain-name "tydrous.tv";
  option routers 172.24.64.1;
  option broadcast-address 172.24.79.255;
  default-lease-time 600;
  max-lease-time 7200;
}
```

Configuration of dhcpd.conf file Complete.

**Starting the DHCP Server:**
Now that the dhcpd.conf file has been configured, the DHCP server needs to be started.

```
sudo service isc-dhcp-server restart
```

DHCP Server started.
Connecting clients to the network:
At this point, the server should be able to provide IP addresses to clients on the network. Connect a host to one of the USER VLAN ports on either of the switches and test to see if the host receives an IP address. A release renew may be necessary if the host was previously connected to a different LAN.

To release and renew a DHCP client IP address, use the following commands:

Windows:
If a Windows client is configured to use DHCP, the following commands can be used to renew the IP address:

```
ipconfig /release
ipconfig /renew
```

If the device correctly obtained an IP address from the DHCP server, the results of the ipconfig /all command should look similar to this:

```
Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix .  tydrous.tv
  Description . . . . . . . . . . . . : Realtek PCIe GBE Family Controller
  Physical Address . . . . . . . . . : 08-2E-5F-81-25-33
  DHCP Enabled . . . . . . . . . . . : Yes
  Autoconfiguration Enabled . . . . . : Yes
  Link-local IPv6 Address . . . . . : fe80::3028:12cd:5759:4ebd%13(Preferred)
  IPv4 Address . . . . . . . . . . . : 172.20.32.21(Preferred)
  Subnet Mask . . . . . . . . . . . : 255.255.224.0
  Lease Obtained . . . . . . . . . . : Wednesday, March 25, 2015 3:13:57 PM
  Lease Expires . . . . . . . . . . : Wednesday, March 25, 2015 3:23:56 PM
  Default Gateway . . . . . . . . . : 172.20.32.1
  DHCP Server . . . . . . . . . . . : 172.24.64.23
  DHCPv6 IAID . . . . . . . . . . . : 285748831
  DHCPv6 Client DUID . . . . . . . : 00-01-00-01-1A-D4-E9-8F-08-2E-5F-81-25-33
  DNS Servers . . . . . . . . . . . : 172.24.64.22
  NetBIOS over Tcpip . . . . . . . : Enabled
```

Ubuntu Linux:
If a Linux client is configured to use DHCP, the following commands can be used to renew the ip address:

```
sudo dhclient -r
dsud dhclient
```

Connection of clients to network complete.

Verify DHCP Server is giving out IP addresses:
To view the leases that the DHCP server has issued to DHCP clients, use the following command to view the leases file:

```
sudo cat /var/lib/dhcp/dhcpd.leases
```
DHCP Server configuration complete.
NTP Server Setup
These instructions are for installing NTP on Ubuntu Server 14.04

For the purposes of these instructions, anything after "#" is a comment for the benefit of the reader to better explain the function of a command.

This tutorial will be using the domain name tydrous.tv. This procedure will work for any other domain name simply replace tydrous.tv with the different domain.

**Start with a clean installation of Ubuntu 14.04**
Refer to the instructions on how to install Ubuntu Server 14.04 for a clean installation.

**Set the interface information for the server:**
Refer to the instructions for Configuring Ubuntu Server 14.04 Ethernet interfaces.

**Set hostname of server:**
Refer to the instructions for changing an Ubuntu Server 14.04 hostname.

**Installing the NTP Server Package:**
```
sudo apt-get update  #Updates the apt list of packages
sudo apt-get install ntp  #Installs the NTP package
```
Type "y" for yes to verify installation of this package if prompted.

**Beginning NTP Configuration:**

**First file to edit is ntp.conf**
```
sudo vim /etc/ntp.conf
#Opens the file using vim for editing with write privileges
#Hit the "i" key to enter insert mode in vim
```

The file will look similar to this. Comments have been removed for clarity:

```plaintext

driftfile /var/lib/ntp/ntp.drift
statistics loopstats peerstats clockstats
driftfile loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable
server 0.pool.ntp.org
server 1.pool.ntp.org
server 2.pool.ntp.org
server 3.pool.ntp.org
server ntp.ubuntu.com
restrict -4 default kod notrap noaccess
restrict -6 default kod notrap noaccess
restrict 127.0.0.1
restrict ::1
```
Here, the other NTP servers used for synchronization will be specified. The more servers, the more accurate the NTP time will be for the network. If possible, use NTP servers that are geographically close to the location of the server.

Here is a list of US NTP servers:
- server 0.us.pool.ntp.org
- server 1.us.pool.ntp.org
- server 2.us.pool.ntp.org
- server 3.us.pool.ntp.org

Additional Servers can be found on this site:

This information will need to be placed into the ntp.conf

Next, to prevent other internet time servers from using this internal NTP server as a time source, restrict the capabilities of each of the time servers added in the previous step. To restrict this access, enter the following for each of the NTP peer servers:

```
restrict 0.us.pool.ntp.org mask 255.255.255.255 nomodify notrap noquery
restrict 1.us.pool.ntp.org mask 255.255.255.255 nomodify notrap noquery
restrict 2.us.pool.ntp.org mask 255.255.255.255 nomodify notrap noquery
restrict 3.us.pool.ntp.org mask 255.255.255.255 nomodify notrap noquery
```

In order for the device on our network to be able to use this server to set time, some different restrictions are necessary. Use the following for all of the different subnets on the network that should be allowed to use the NTP server:

```
restrict 192.168.128.0 mask 255.255.252.0 nomodify notrap
restrict 192.168.132.0 mask 255.255.255.0 nomodify notrap
restrict 172.24.64.0 mask 255.255.240.0 nomodify notrap
restrict 172.20.32.0 mask 255.255.224.0 nomodify notrap
```

Once that information has been added, save and exit the file.

The finished configuration file should look similar to this. Some comments have been removed for clarity:
Configuration of ntp.conf file is complete.

**Restarting the NTP service:**

Now that the configuration is complete, the NTP service can be restarted.

```
sudo service ntp restart
cisco@acm-ntp-1:~$ sudo service ntp restart
  * Stopping NTP server ntpd
  * Starting NTP server ntpd
```

After the NTP service has successfully restarted, the status of the peering process can be checked.
```
sudo ntpq -np
```

Most likely, the server will not yet be synced with the external time sources. This usually takes between 5 to 10 minutes or longer to be fully synced with the internet time sources. Continue to run this command periodically. This is what the ntpq command will output when the server is not finished syncing.
Here is what the table should look like when the NTP server is finished syncing. Until this state is reached, other devices will not properly sync their times with the internal NTP server since it is not yet considered a valid time source.

### Configuration of NTP server is complete.

**Client configuration:**

Now that the NTP server is up and running, the clients need to be configured to use this new time source.

In order to accomplish this, two packages need to be installed:

```
sudo aptitude install ntp ntpdate
```

Once those packages have been installed, it is time to begin editing the NTP configuration file.

```
sudo vim /etc/ntp.conf
```

Since this file is only going to be using the internal time clock for its time the statements specifying additional time servers can be deleted. Now the internal time server must be set and have similar restrictions placed on it.
server acm-ntp-1.tydrous.tv

restrict default notrust nomodify nopeer

restrict acm-ntp-1.tydrous.tv

The final client configuration file should look similar to following:

```
# Specify one or more NTP servers.
server acm-ntp-1.tydrous.tv

# By default, exchange time with everybody, but don't allow configuration.
restrict default notrust nomodify nopeer
restrict -4 default kcd notrap nomodify nopeer noquery
restrict -6 default kcd notrap nomodify nopeer noquery

# Local users may interrogate the ntp server more closely.
restrict acm-ntp-1.tydrous.tv
restrict 127.0.0.1
restrict ::1
```

Once those have been added, save and exit the file.

**Configuration of the client ntp.conf file is complete.**

**Restart the NTP service on the client device.**

Once the configuration file is finished, restart the NTP service.

```
sudo service ntp restart
```

**Client configuration for NTP is complete.**

To configure Windows devices to use the internal NTP server, refer to the Configuring Windows Server 2012 R2 to use NTP.
FTP Server Setup
These instructions are for installing vsftpd on Ubuntu Server 14.04

For the purposes of these instructions, anything after "#" is a comment for the benefit of the reader to better explain the function of a command.

This tutorial will be using the domain name tydrous.tv. This procedure will work for any other domain name simply replace tydrous.tv with the different domain.

Set the interface information for the server:
Refer to the instructions for Configuring Ubuntu Server 14.04 Ethernet interfaces.

Installation of Ubuntu 14.04 and Creating RAID Array:
Refer to the instructions on how to install Ubuntu Server 14.04 for a clean installation. Once the server has finished booting the installation process can begin. Select a language to continue.

Once the Language is selected, the installation screen will be shown. Select “Install Ubuntu Server”.
This will begin the installation process, where a language will need to be selected again.
Set the location of the server. This will be used for time purposes.

The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.

This is a shortlist of locations based on the language you selected. Choose “other” if your location is not listed.

Country, territory or area:

Antigua and Barbuda
Australia
Botswana
Canada
Hong Kong
India
Ireland
New Zealand
Nigeria
Philippines
Singapore
South Africa
United Kingdom
United States
Zambia
Zimbabwe
other

The keyboard layout will need to be determined. Select “No” for the detect configuration of the keyboard layout.

You can try to have your keyboard layout detected by pressing a series of keys. If you do not want to do this, you will be able to select your keyboard layout from a list.
Select the appropriate keyboard layout.

Ubuntu will begin the process of loading all of the necessary files for the installation process. After this process is complete, the server will automatically detect an IP address using DHCP. Once this auto detection is complete, a hostname will need to be set for the installation of Ubuntu. Hit Tab and Enter to continue.
A basic user will need to be created. A generic username and password will be used in this tutorial, but any username and password can be used here. Hit Tab and Enter to continue.

Enter a username. Hit Tab and Enter to continue.

Enter a password. Hit Tab and Enter to continue.
Verify the password previously entered. Hit Tab and Enter to continue.

Ubuntu Server gives the option of encrypting the home directory of this user.

Ubuntu will attempt to set up the clock. Verify the information presented.
Begin partitioning the hard drive of the server. Select the “Manual” option.

**[Partition disks]**

The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.

Partitioning method:

- Guided - use entire disk
- Guided - use entire disk and set up LVM
- Guided - use entire disk and set up encrypted LVM
- Manual

Here, there are 3 10 GB hard drives. The following process will have to be completed individually for all three. Select the hard drive that will be configured as part of the RAID Array and hit Enter to create the new partition table on the disk.

**[Partition disks]**

This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.

- Guided partitioning
- Configure iSCSI volumes

  - SCSI0 (0,0,0) (sda) - 31.5 GB Msft Virtual Disk
  - SCSI0 (0,0,0) (sda) - 10.7 GB Msft Virtual Disk
  - SCSI4 (0,0,2) (sdc) - 10.7 GB Msft Virtual Disk
  - SCSI4 (0,0,3) (sdd) - 10.7 GB Msft Virtual Disk

  Undo changes to partitions
  Finish partitioning and write changes to disk

Creating a new partition on the disk will erase all data. Hit “Yes” to continue creating this new partition.

**[Partition disks]**

You have selected an entire device to partition. If you proceed with creating a new partition table on the device, then all current partitions will be removed.

Note that you will be able to undo this operation later if you wish.

Create new empty partition table on this device?

<Go Back>  <Yes>  <No>
Drive space will need to be allocated to this partition. Select the “FREE SPACE” option and hit Enter to continue.

```
[!!! Partition disks]

This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.

- Guided partitioning
- Configure software RAID
- Configure the Logical Volume Manager
- Configure encrypted volumes
- Configure iSCSI volumes

SCSI3 (0,0,0) (sda) - 21.5 GB Msf Virtual Disk
SCSI4 (0,0,1) (sdb) - 10.7 GB Msf Virtual Disk
part/lor - 10.7 GB FREE SPACE
SCSI4 (0,0,2) (sdc) - 10.7 GB Msf Virtual Disk
SCSI4 (0,0,3) (sdd) - 10.7 GB Msf Virtual Disk

Undo changes to partitions
Finish partitioning and write changes to disk
```

Select “Automatically partition the free space” and hit enter to continue. This will assign the free space on the disk to this newly created partition.

```
[!!! Partition disks]

How to use this free space:

Create a new partition
Automatically partition the free space
Show Cylinder/Header/Sector information
```

The new partition will be created. Complete this task for the remaining 2 hard drives. The finished result should look similar to this:
Create the software RAID. Select “Configure software RAID”.

Until this point, all of the partition changes have not been put into use. Select “Yes” to complete the process and continue with the RAID setup.

Select “Create MD device”.

This is the software RAID (or MD, "multiple device") configuration menu. Please select one of the proposed actions to configure software RAID.

Software RAID configuration actions:
- Create MD device
- Delete MD device
- Finish

<Go Back>
This tutorial will be setting up a RAID 5 configuration with 3 hard drives, which is the minimum required for this type of RAID. Drive requirements for other types of RAID are as follows: 2 hard drives are required for RAIDs 0 and 1, 3 for RAID 5, and RAIDs 6 and 10 both require 4 hard drives.

Here is a website to calculate the amount of storage space will be available for any type of raid configuration:  
https://www.icc-usa.com/raid-calculator/

This RAID 5 configuration will result in 17.2GB of storage space.

Enter the number of drives participating in the RAID Array, in this case 3. Hit Tab and Enter to continue.

Enter the number of spare drives in this array, which is 0 in this case. Hit Tab and Enter to continue.
Here is where the drives that will participate in the RAID Array will be selected. Use the arrow keys to move up and down and spacebar to select the drive. In this case, the drives /dev/sdb1, /dev/sdc1, and /dev/sdd1 are the drives configured to participate in this array. The 5 version of these drives is the swap space for that drive. Hit Tab and Enter to continue.

Again, a prompt will appear to confirm the partition changes to be written to this disk. Hit Yes to continue.

Hit “Finish” if this is the only RAID array to be created.

Now that the configuration of the RAID Array is finished, the operating system boot disk will need to be partitioned. This can be done manually or select the “Guided partitioning” option.
Select the “Guided - use entire disk” option.

If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.

Partitioning method:

- Guided - resize SCSI3 (0,0,0), partition #1 (sda) and use freed space
- Guided - resize SCSI4 (0,0,3), partition #1 (sdc) and use freed space
- Guided - use entire disk
- Guided - use entire disk and set up LVM
- Guided - use entire disk and set up encrypted LVM
- Manual

<Go Back>

Select the drive that is not participating in the RAID array.

Note that all data on the disk you select will be erased, but not before you have confirmed that you really want to make the changes.

Select disk to partition:

- RAID device #0 - 17.2 GB Software RAID device
- SCSI (0,0,0) (sda) - 21.5 GB Msft Virtual Disk
- SCSI4 (0,0,1) (sdb) - 10.7 GB Msft Virtual Disk
- SCSI4 (0,0,2) (sdc) - 10.7 GB Msft Virtual Disk
- SCSI4 (0,0,3) (sdd) - 10.7 GB Msft Virtual Disk

<Go Back>

Finish by writing the changes to the disk. Hit “Yes” to continue.

Before the Logical Volume Manager can be configured, the current partitioning scheme has to be written to disk. These changes cannot be undone.

After the Logical Volume Manager is configured, no additional changes to the partitioning scheme of disks containing physical volumes are allowed during the installation. Please decide if you are satisfied with the current partitioning scheme before continuing.

The partition tables of the following devices are changed:
- SCSI3 (0,0,0) (sda)

Write the changes to disks and configure LVM?

Yes

<No>
This is where the size of the partition is set. The default value is the max variable size of the drive.

A summary of the drives will appear. Select “Finish partitioning and write changes to disk” option.
Verify the changes to the partition table.

If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.

The partition tables of the following devices are changed:
SSIS (0,0,0) (sda)

The following partitions are going to be formatted:
partition #1 of SSIS (0,0,0) (sda) as ext4
partition #5 of SSIS (0,0,0) (sda) as swap

Write the changes to disks?
(Yes) (No)

After this process has finished, a dialog box will appear asking about any proxy settings. This can be left blank. Hit Tab and Enter to continue.

If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank.

The proxy information should be given in the standard form of 'http://[user][pass]@[host]:[port]/'.

HTTP proxy information (blank for none):

After this Ubuntu will begin configuring apt, which is used to update and install packages in Ubuntu. After that is complete, the server will begin to install packages. Once this is finished, the server will ask what type of update management should be used. Automatic updates can be used, but for this tutorial, no automatic updates will be selected.

Applying updates on a frequent basis is an important part of keeping your system secure.

By default, updates need to be applied manually using package management tools. Alternatively, you can choose to have this system automatically download and install security updates, or you can choose to manage this system over the web as part of a group of systems using Canonical's Landscape service.

How do you want to manage upgrades on this system?
- automatic updates
- Install security updates automatically
- Manage system with Landscape

Here are some other optional packages that can be installed. Only the OpenSSH server will be selected in this tutorial. Installation of other protocols will be covered in other tutorials done post operating system installation. Use the arrow keys to move up and down and spacebar to select the packages to install. Hit Tab and Enter to continue.
This package will now be downloaded and installed. This will take a while.

Finally, once that installation is finished, the server will ask if GRUB should be installed to the master boot record. Since this is the only operating system being installed on this server, select “Yes”.

After this dialog, the installation is finished. Hit continue to reboot the server. If doing a VM installation, Hyper-V will automatically remove the ISO from the boot options. If installing on a physical server, remove the boot media before rebooting.

After reboot, a screen similar the screen picture below should appear and the server is now ready for further configuration.
Configure the RAID Array:
Determine the designation of the RAID array

```
sudo fdisk -l
```

```
Disk /dev/md0: 17.2 GB, 17168334848 bytes
2 heads, 4 sectors/track, 4191488 cylinders, total 33531904 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 524288 bytes / 1048576 bytes
Disk identifier: 0x00000000
```

Enter the fdisk config
```
sudo fdisk /dev/md0
```

```
/dev/md0 is the designation of the RAID array
```

1. Type n to create a new partition
2. Type p to create a primary partition
3. Hit enter to use the default partition number(1)
4. Hit enter again twice to use the default first and last sector of the drive to partition the entire array.
5. Type w to the write those changes to the disk

```
cisco@raid-test:~$ sudo fdisk /dev/md0
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF disklabel
Building a new DOS disklabel with disk identifier 0x00000000.

Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.

Warning: Invalid flag 0x0000 of partition table 4 will be corrected by w(rite)

The device presents a logical sector size that is smaller than the physical sector size. Aligning to a physical sector (or optimal I/O) size boundary is recommended, or performance may be impacted.

Command (m for help): n
Partition type: 
  p  primary (0 primary, 0 extended, 4 free)
  e  extended
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-33531903, default 2048): 1
Using default value 2048
Last sector, +size(K,M,G) (2048-33531903, default 33531903): 1
Using default value 33531903
Command (m for help): w
The partition table has been altered!
Calling ioctl() to re-read partition table.
Syncing disks.
cisco@raid-test:~$
```

Format the array:
Check to see what the name of the partition created is.
```
sudo fdisk -l
```
/dev/md0p1 is the name of the partition and this formats that partition with the ext3 file system.

```
sudo mkfs -t ext3 /dev/md0p1
```

Format of RAID Array Partition is complete.

**Mount the Array:**
Create the mount point the array will be mounted to.

```
sudo mkdir /media/array
```

Configure the array to be auto mounted on boot by editing the fstab file located in /etc/ directory.

```
sudo vim /etc/fstab
```
Add the line:

```
/dev/md0p1  /media/array  ext3  defaults  0  2
```

#/dev/md0p1 is the partition of the array
#/media/array is the mounting point.

Save and exit the file.

Either restart or mount the drive manually

```
sudo mount -a
```
Check if the array mounted correctly

```
cat /proc/mounts | grep /dev/md0p1
```
If you receive the result of the array, then it has been properly mounted. It should look similar to this:

```
cisco@raid-test:~$ cat /proc/mounts | grep /dev/md0pl
/dev/md0pl /medie/array ext3 rw,relatime,stripe=256,data=ordered 0 0
```

**Install the FTP Daemon and other packages:**

```
sudo apt-get update
sudo apt-get install libpam-pwdfile vsftpd vim apache2 apache2-utils
```

libpam-pwdfile is used to create the username and password database
vsftpd is the FTP Daemon
vim is a CLI text editor - may already be installed
apache2 is used used for password encryption
apache2-utils are used for password encryption

**Configuration of vsftpd:**

Backup the original vsftpd.conf file.
```
sudo mv /etc/vsftpd.conf /etc/vsftpd.conf.backup
```

Create the vsftpd.conf file
```
sudo vim /etc/vsftpd.conf
```
Add the following lines to the file
```
listen=YES
anonymous_enable=NO
local_enable=YES
write_enable=YES
local_umask=022
nopriv_user=vsftpd
virtual_use_local_privs=YES
guest_enable=YES
user_sub_token=$USER
local_root=/media/array/ftp/$USER
chroot_local_user=YES
hide_ids=YES
guest_username=vsftpd
```
Save and exit the file.

**vsftpd configuration is complete.**

**Creating the users database:**

Make a directory to place the Virtual user database in
```
sudo mkdir /etc/vsftpd
```

Create the database file and add the first user to it.
```
sudo htpasswd -cd /etc/vsftpd/vsftpdb.passwd acmpublic
```

```
cisco@raid-test:/etc$ sudo htpasswd -cd /etc/vsftpd/vsftpdb.passwd acmpublic
New password: 
Re-type new password: 
Adding password for user acmpublic
```
This creates the file with the -c option using the MD5 algorithm and adds the user acmpublic to the database. It then prompts for a password and asks to confirm it.

**User database has been created.**

**Configuring the PAM File:**
This file tells the FTP server where to find the usernames and passwords to authenticate against at login

Back up the original file vsftpd

```bash
sudo mv /etc/pam.d/vsftpd /etc/pam.d/vsftpd.backup
```

Create a new vsftpd file

```bash
sudo vim /etc/pam.d/vsftpd
```

Add the following 2 lines to the file:

```bash
auth required pam_pwdfile.so /etc/vsftpd/vsftpdb.passwd
account required pam_permit.so
```

Save and exit the file.

Create a user with the permissions you would like all virtual users to have.

```bash
sudo useradd --home /home/vsftpd --gid nogroup -m --shell /bin/false vsftpd
```

Restart the FTP service for the changes to take effect

```bash
sudo service vsftpd restart --system
```

If the service is stopped, then check the vsftpd.conf file for errors. This will prevent the service from starting back up properly.

**Configuration of PAM file is complete.**

**Creating directories for users:**
Create the directories specified in the vsftpd.conf file for the users.

These directories must exist otherwise the user will not be able to login to the ftp server.

Make the directories and alter the permissions and owner of the files.

```bash
sudo mkdir /media/array
sudo mkdir /media/array/ftp/acmpublic
sudo chmod -w /media/array/ftp/acmpublic
sudo mkdir /media/array/ftp/acmpublic/Public
sudo chmod -R 755 /media/array/ftp/acmpublic/Public
sudo chown -R vsftpd:nogroup /media/array/ftp/acmpublic
```
Adding additional users:

```bash
sudo htpasswd -d /etc/vsftpd/vsftpdb.passwd cisco
*next two lines ask for password to be set*
  sudo mkdir /media/array/ftp/cisco
  sudo chmod -w /media/array/ftp/cisco
  sudo mkdir /media/array/ftp/cisco/public
  sudo chmod -R 755 /media/array/ftp/cisco/public
  sudo chown -R vsftpd:nogroup /media/array/ftp/cisco
```
Configuring OpenNMS SNMP Server Setup
These instructions are for installing OpenNMS 1.12.1 on Ubuntu Server 14.04

For the purposes of these instructions, anything after “#” is a comment for the benefit of the reader to better explain the function of a command.

This tutorial will be using the domain name tydrous.tv. This procedure will work for any other domain name simply replace tydrous.tv with the different domain.

**Start with a clean installation of Ubuntu 14.04**
Refer to the instructions on how to install Ubuntu Server 14.04 for a clean installation.

**Set the interface information for the server:**
Refer to the instructions for configuring Ubuntu Server 14.04 Ethernet interfaces.

**Set hostname of server:**
Refer to the instructions for changing an Ubuntu Server 14.04 hostname.

**Beginning OpenNMS installation Configuration:**

**Installing the Oracle 7 Java Package:**
As of the creation of this guide, Java 7 is the most recent version supported by OpenNMS 1.12.1.

First, additions need to be made to the apt package lists so that the apt-get command will be able to find the packages that need to be installed. This file likely does not exist and will need to be created.

```
sudo vim /etc/apt/sources.list.d/webupd8team-java.list
```

Add the following lines to the file created in the previous step.

```
deb http://ppa.launchpad.net/webupd8team/java/ubuntu precise main

deb-src http://ppa.launchpad.net/webupd8team/java/ubuntu precise main
```

Save and exit the file by typing “esc” then “shift” + “:” and “wq”

An apt key must be retrieved to allow access to this apt download server.

```
sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys EEA14886
```

Output should look similar to the following:
Now that the key has been successfully added, update the apt package list and begin the installation of Java 7.

```
sudo apt-get update
sudo apt-get install oracle-java7-installer
```

Type “y” and then Enter to continue.

Java will require their terms and conditions to be accepted during the installation process. Select “OK” to continue with the installation.

Hit “OK” to Continue.
After the installation of Java 7, initialize the java environment variables.

```
sudo apt-get install oracle-java7-set-default
```

Installation of Java 7 complete.

**Adding OpenNMS to apt package list:**

Similar to the process followed for addition of Java 7 to the apt package list, navigate to the `/etc/apt/sources.list.d/` directory. Create a file named `opennms.list`:

```
sudo vim /etc/apt/sources.list.d/opennms.list
```

Add the following lines to the `opennms.list` file:

```
deb http://debian.opennms.org stable main
deb-src http://debian.opennms.org stable main
deb http://debian.opennms.org stable main
deb-src http://debian.opennms.org stable main
```

Add an apt key for access to the OpenNMS download server:

```
sudo wget -O http://debian.opennms.org/OPENNMS-GPG-KEY | sudo apt-key add -
sudo apt-get update
```

Update the apt package list:

```
sudo apt-get update
```
Verify that the OpenNMS package has been added to the list, but do NOT install it. Additional setup is required before OpenNMS is ready to be installed.

```
apt-cache search opennms
```

The results will look similar to this:

```
Addition of OpenNMS to the package list is complete.
```

**PostgreSQL Installation:**

Update package list and begin the install of the PostgreSQL package.

```
sudo apt-get update
dsudo apt-get install postgresql
```

```
cisco@asm-mp:~# sudo apt-get install postgresql
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libpq5 postgresql-9.3 postgresql-9.3-client postgresql-9.3-client-common postgresql-9.3-common
Suggested packages:
  oldstdb ident-server locales-all postgresql-doc postgresql-blacklist
The following NEW packages will be installed:
  libpq5 postgresql postgresql-9.3 postgresql-9.3-client postgresql-9.3-client-common postgresql-9.3-common
0 upgraded, 7 newly installed, 0 to remove and 125 not upgraded.
Need to get 3,005 kB of additional disk space.
Do you want to continue? [y/n] y
```

Type “y” and then Enter to continue.

After installation is complete, check what version of PostgreSQL was installed.

```
pg_lscusters -h
```

Make note of this version number. In this case, the version is 9.3.
Locate the pg_hba.conf file.

    sudo vim /etc/postgresql/$VERSION/main/pg_hba.conf

$VERSION represents whatever version number was determined in the previous step.

Three lines need to be altered in this file and should be located near the bottom of the file. Change the method for local, IPv4, and IPv6 to trusted.

```
# "local" is for Unix domain socket connections only
local  all              all    trust  #peer
# IPv4 local connections:
host  all              all    127.0.0.1/32 trust  #md5
# IPv6 local connections:
host  all              all    ::1/128 trust  #md5
# Allow replication connections from localhost, by a user with the
# replication privilege.
local  replication      postgres  peer
host  replication      postgres  127.0.0.1/32  md5
host  replication      postgres  ::1/128  md5
```

Save and exit the file by typing “esc” then “shift + :” and “wq”

To apply these changes, the PostgreSQL service must be restarted.

    sudo service postgresql restart

**Installation of PostgreSQL complete.**

**Java Development Kit install:**

Install corresponding jdk for the Java 7 installed earlier.

    sudo apt-get update
    sudo apt-get install openjdk-7-jre

Type “y” and then Enter to continue.

**Java Development Kit install complete**

**Installing a Mail Transfer agent**

Regardless of whether or not the automatic email feature is used, a Mail Transfer Agent (MTA) still needs to be installed for OpenNMS to install properly.

    sudo apt-get install default-mta
Accept all of the default responses when prompted during the install process. The default MTA for Ubuntu should be Exim.

Hit Enter to continue.

**Default MTA Installation complete**

**Installing OpenNMS:**

Now that all of the preparations are complete install OpenNMS:

- `sudo apt-get update`
- `sudo apt-get install opennms`
Type “y” and hit Enter to continue.

Once OpenNMS has finished downloading, a message will appear.

During the unpacking process a window will appear stating “IPLIKE installation failed”. This will be addressed in a later step.

After the installation of OpenNMS is complete, it may be desirable to delete the apt-get file created previously to prevent auto updates to OpenNMS. This step is optional.

OpenNMS Package install complete
Configuring Java:
To configure Java for the use with OpenNMS, run the following scripts:

```
sudo /usr/share/opennms/bin/runjava -s
```

```
sudo /usr/share/opennms/bin/runjava -S /usr/bin/java
```

Java Configuration complete

Creating the OpenNMS Database:

```
sudo /usr/share/opennms/bin/install -dis
```

Installing IPLIKE:

```
sudo /usr/sbin/install_iplike.sh
```

This command will only have one line of output

```
cisco@acm-snp-1:~$ sudo /usr/sbin/install_iplike.sh
CREATE_FUNCTION
```

If the command ran successfully, this is the expected output.

Verify Connection to Post GRE SQL:
To verify that the Post GRE SQL database is functioning properly, enter the following command:

```
psql -U postgres --host=localhost opennms
```
If the prompt is similar to the one shown above, the connection was successful. Type “\q” to exit this promote.

**Starting OpenNMS:**
If all steps were completed with no issues, OpenNMS is now ready to be started.

```
sudo service opennms start
```

This process will take some time since there are several sub processes that OpenNMS is also starting.

Check the status:

```
sudo service opennms status
```

If all services are running, OpenNMS is now ready to be accessed via a web browser.

**Accessing OpenNMS:**
Navigate to the address [http://172.24.64.25:8980/opennms/](http://172.24.64.25:8980/opennms/) using a web browser of any kind on a computer which can connect to the SNMP server.
The default login information is
Username: admin
Password: admin

**Changing default Admin password:**
Mouse over “admin” in the top right and select the “Change Password” option in the drop down menu.

This will bring up an additional page with only one option. Select “Change Password”.

Fill out the information in the Password Change form and click “Submit”:

**Scanning for Devices:**
At this point, in the tutorial devices configured for SNMP will be required on the network. If devices have not yet been configured perform that step now. Refer to the following for instructions on SNMP Agent configuration.
Configuring Ubuntu server 14.04 as a SNMP Agent or Configuring Cisco device
Configuring SNMP for Windows Server 2012 R2
If there is at least one device configured continue the Scanning for devices step.

To begin, access the admin configuration page and select the “Configure Discovery” button:

Configuring an IP range for discovery:
Enter the IP address range: Begin IP and End IP:

Add Include Range to Discovery
Add a range of IP addresses to include in discovery. Begin and End IP addresses are required.
You can set the number of Retries and Timeout. If these parameters are not set, default values will be used.

Begin IP Address:
192.168.132.0

End IP Address:
192.168.132.255

Retries:
1

Timeout (ms):
2000

Add Cancel

Continue this process for all of the networking device subnet ranges:

<table>
<thead>
<tr>
<th>Include Ranges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Begin Address</td>
</tr>
<tr>
<td>192.168.132.0</td>
</tr>
<tr>
<td>192.168.128.0</td>
</tr>
<tr>
<td>172.24.64.0</td>
</tr>
</tbody>
</table>

Then click “Save and Restart Discovery”.

**Altering the Community String for SNMP discovery:**
If the network devices have been configured to use a different read and write community string, this can be changed on the “Configure SNMP Community Names by IP” page.
Fill in the information for the First and Last IP addresses along with the desired “Read Community String” and “Write Community String”. All other values can be left blank or default. Then, click “Save Config”.

On this same page, it is also possible to look up the community string a particular IP address is configured to use. Type in the IP address to look up in the text box and click “Look up”. The information configured for the IP address will be displayed in the fields below and can be altered and saved as desired.

Viewing Nodes:
At this point, OpenNMS should be either finished or in the process of discovering SNMP devices for the network address ranges specified. To view the devices it has discovered, access the nodes page.
All of the discovered devices, or “Nodes”, are listed here. Additional information about each node can be viewed by clicking on the desired Node.

Installation and Basic Configuration of OpenNMS is now complete.

**Accessing Resource Graphs:**

OpenNMS offers many statistics and graphs for devices it manages. To access this information, click on the “Resource Graphs” button in the node page.

Select the information from the device to be viewed by checking the box to the left of the desired items. Then click on the “Graph Selection” button at the bottom center of the window.
Example output:

```
```

137
What occurs during an outage:

The main purpose of OpenNMS or any SNMP server is to monitor the health of the network. Here is a quick look at what will happen in the event of a device losing connection to the network. When a network issue is detected by OpenNMS, alarms are generated and displayed on the home screen. The following is an example of the connection loss of one of the two head end routers in this network.

When OpenNMS detects the loss of connection with one of the devices it monitors, alarms are generated for that device. Outages are noted in the summary of network performance and alarms are listed to the left. Detailed information can be viewed about the alarms by clicking on the “alarms” button on the left in the Nodes with Pending Problems section.

Details about the individual node can also be viewed by clicking on the name of the node in the list of alarms. The .1 addresses are still accessible since those are not located directly on the device and are virtual interfaces for gateway redundancy using GLBP. Only one of the routers was lost in this scenario.
Action can then be taken to resolve the issue by contacting the person responsible for the failed device. When the issue is resolved OpenNMS automatically clears the alarms for the downed node. It may take some time for the alarms to clear, but after 5 to 10 minutes, OpenNMS should see no pending problems on the network. Outage information is noted in the summary section as well as in the individual device page.
Configuring SNMP for Windows Server 2012 R2

For the purposes of these instructions, anything after "#" is a comment for the benefit of the reader to better explain the function of a command.

This tutorial will be using the domain name tydrous.tv. This procedure will work for any other domain name simply replace tydrous.tv with the different domain.

**Configuring Windows Server SNMP:**
Open the Server manager and select the “Add Roles and Features” option from the “Manage” drop down menu.

Make sure the “Role-based or feature based installation” is selected and click “Next”.

![Add Roles and Features Wizard](image-url)
Select the server to add the feature to and click “Next”.

Skip the Server Roles window without selecting any roles to add and move to the Features window by clicking “Next”.
Select the “SNMP Service” option by checking the box to the left. Then, click "Next".

If presented with a dialog box, click “Add Feature” and click “Next” again at the Features window.
Click “Install” to begin adding the feature. The install process will complete in the background.

Once the installation is complete click on the “Close” button and return to the Server Manager window. Click on “Tools” and select the “Services” option.
Scroll down to “SNMP Service” and right click on it and select the “Properties” option.

Select the “Agent” tab and enter in the contact information and location of the server.

Click on the “Security” tab and then click on the first “Add…” button to configure the community string.
Enter in the read only community string in the “Community Name” text box. Make sure the community string is configured as “READ ONLY” and then click “Add”.

Configure the host IP address that the server will send its SNMP traps to. Click the second “Add…” button.
Enter the IP address of the SNMP server. In this case, enter “172.24.64.25” and click “Add”.

Complete the SNMP configuration by Clicking “OK”.

Configuration of SNMP for Windows Server 2012 R2 is complete.

Adding the server to OpenNMS:
If the device is not automatically discovered by OpenNMS, a static configuration might be necessary. Navigate to the configure OpenNMS page and click on “Add Interface for Scanning” button.
Type in the IP address of the device to add and click the “Add” button.

Verify that the new device has been added by going to the Nodes page.

Adding the Windows server to OpenNMS is complete.
Syslog Server Setup
These instructions are for rsyslog on Ubuntu Server 14.04

For the purposes of these instructions, anything after "#" is a comment for the benefit of the reader to better explain the function of a command.

**Start with a clean installation of Ubuntu 14.04**
Refer to the instructions on how to install Ubuntu Server 14.04 for a clean installation.

**Set the interface information for the server:**
Refer to the instructions for configuring Ubuntu Server 14.04 Ethernet interfaces.
NOTE:
In this setup use the default gateway address as the dns-nameserver. Since the DNS server is not yet working this server will need to use the DNS function of the gateway in order to download the Bind9 package later in these instructions. Using the example in the Configuring Ubuntu Server 14.04 Ethernet interfaces instructions.

**Set hostname of server:**
Refer to the instructions for changing an Ubuntu Server 14.04 hostname.

**Beginning Syslog server Configuration:**
There are no additional packages that need to be installed in order to set up a syslog server. The default installation of Ubuntu Server 14.04 uses rsyslog for local logging. This tutorial will convert that local logging service into one that will aggregate log files from many devices into one place.

**Editing the rsyslog.conf file:**
The configuration file for the rsyslog process can be found at the following location.
sudo vim /etc/rsyslog.conf

The file will be full of many options, and there are two that need to be uncommented. An additional statement will need to be added to the end. The 2 lines surrounded by the red box are the two that need to be uncommented.

```
$ModLoad imuxsock  # provides support for local system logging
$ModLoad imklog    # provides kernel logging support
$ModLoad immark    # provides --MARK-- message capability
# provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514
# provides TCP syslog reception
$ModLoad intcp
$InputTCPServerRun 514
```
In addition, there is a statement that needs to be added to the bottom of the file. This statement is what will allow the syslog server to dynamically create new log files for different devices it receives log messages from:

```bash
$template DynaFile,"/var/log/remote-logs/%HOSTNAME%.log"
.*.*?.DynaFile
```

**Configuration of the rsyslog file is complete**

**Giving rsyslog ownership of the log directory:**
Since the rsyslog process needs to be able to make alterations to the log folder, it needs ownership of that folder. Change directories to the /var directory and alter the owner of the file.

```bash
cd /var
sudo chown syslog:syslog log
```

To verify that the files owner has changed, use the following command:

```bash
ls -l /var
```

```
cisco@acm-syslog-1:~$ ls -l /var
total 40
drwxr-xr-x 2 root  root  4096 Apr 10 2014 backups
drwxr-xr-x 8 root  root  4096 Feb  8 23:38 cache
drwxrwxrwt 1 root  root  4096 Feb  8 23:41 crash
drwxr-xr-x 38 root  root  4096 Feb  8 23:43 lib
drwxrwxr-x  2 root  staff  4096 Apr 10 2014 local
lrwxrwxrwx 1 root  root   9 Feb  8 23:29 lock  -> /run/lock
-rwxrwxr-x 10 syslog  syslog  4096 Mar 25 19:49 log
drwxr-xr-x 2 root  mail  4096 Jul 22 2014 mail
drwxr-xr-x 2 root  root  4096 Jul 22 2014 opt
lrwxrwxrwx 1 root  root   4 Feb  8 23:29 run  -> /run
-rwxr-xr-x  5 root  root  4096 Feb  8 23:29 spool
drwxrwxrwt 2 root  root  4096 Feb  8 23:43 tmp
```

Ownership change of log directory is complete.

**Restarting the rsyslog process:**
Now that all the preparations are finished, it is time to apply these new changes and restart the rsyslog process:

```bash
sudo service rsyslog restart
```

```
cisco@acm-syslog-1:~$ sudo service rsyslog restart
rsyslog stop/waiting
rsyslog start/running, process 1963
```

Restart compete

For instructions on configuring a client to send Syslog messages to this server, refer to the “Configuring Ubuntu server 14.04 as a Syslog Client”.

**Configuration of rsyslog is complete.**
Installing and configuring FileZilla Client

For the purposes of these instructions, anything after "#" is a comment for the benefit of the reader to better explain the function of a command.

**Downloading FileZilla Installer:**

Go to filezilla-project.org.

Click on “Download” on the left side of the screen **not** the “Quick Download Link”. The quick download option contains possible bloatware that could be installed.

Click on the "Show additional download options" button
This will bring up different options other than the quick download option. Click on the .exe version of FileZilla.

The download should start automatically after 5 seconds when the page loads. If not, click the “direct link” button.

Run the installer after it finishes downloading.

Blindly agree to the terms and conditions by hitting the “I Agree” button.
This can be a single user install or for all users on the machine.

The default options are fine for this application of FileZilla. Click “Next” to continue.

Here is where the installation path can be set. The default option is fine. Click “Next” to continue.
This is the final step before installation. A shortcut can be placed in the start menu under the specified folder. Click “Install” when finished.

Click “Finished” to complete installation and launch FileZilla.

Installation of FileZilla is complete.

Using FileZilla:

When FileZilla is first opened, it will look similar to this:
To connect to the internal FTP server, go to the file drop down menu and select “Site Manager...” and click on “New Site”.

Give the site a name and enter the information as follows:
Host: acm-ftp-1
Logon Type: Normal
User: acmpublic
Password: ACMcp123

Select “Connect”.

Game files are located in the Public folder:
To download a file, drag a folder on the server into the destination folder on the local machine and the transfer will start.
Security Policy

Remote Access Policy:

Devices on the USER VLAN will not be permitted to remote to any of the servers or network devices. This includes telnet, SSH, and remote desktop of server and network devices on the SERVER VLAN and MANAGEMENT VLAN.

Passwords:

Network devices:
   acm1an
   L!sc0Worki

   username acm1an priv 15 secret L!sc0Worki

   Network device FTP account info
   acm1an
   Lisc0ftpARCH
   L!sc0Worki

Servers:
   Windows Server
   acms3rv
   W1sc0vr3S

   Linux Servers
   L!sc0vr3S

FTP Account information:
   Public FTP User
   acmpublic
   ACMcp123

   Network device FTP account info
   acm1an
   Lisc0ftpARCH
   L!sc0Worki

SNMP Community Strings:
   SNMP Community String Read Only
   AKacmRe@d0Nly
   SNMP Community String Read Write
   wR1t3RD@kacMmgnt
Testing Documentation
Nicholas Bordo

Confirming full LAN Connectivity:
Test will be between acm-ftp-1 (172.24.64.27) and a test PC connected to the USER VLAN on the 2960 switch.

```
Pinging acm-ftp-1.tyndrus.bu [172.24.64.27] with 32 bytes of data:
  Reply from 172.24.64.27: bytes=32 time<1ms TTL=63
  Reply from 172.24.64.27: bytes=32 time<1ms TTL=63
  Reply from 172.24.64.27: bytes=32 time<1ms TTL=63
  Reply from 172.24.64.27: bytes=32 time<1ms TTL=63

Ping statistics for 172.24.64.27:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Test Client was able to ping FTP server with hostname and IP address.

Test successful.

Confirming Internet Connectivity:
This test will verify that users have connection to the internet by performing a ping to Google.com from a Windows 7 Computer on the USER VLAN.

```
Pinging 172.24.64.27 with 32 bytes of data:
  Reply from 172.24.64.27: bytes=32 time<1ms TTL=63
  Reply from 172.24.64.27: bytes=32 time<1ms TTL=63
  Reply from 172.24.64.27: bytes=32 time<1ms TTL=63
  Reply from 172.24.64.27: bytes=32 time<1ms TTL=63

Ping statistics for 172.24.64.27:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Client was able to resolve a domain name into an IP address on the internet and ping that web server.
Test successful.

Proper Operation of DHCP Server:
Tests to verify that clients are able to successfully obtain an IP address from the DHCP server automatically.
Output of the command:

```bash
sudo cat /var/lib/dhcp/dhcpd leases
```

```
lease 172.20.32.21 {
  starts 6 2015/03/28 22:20:01;
  ends 6 2015/03/28 22:30:01;
  cltt 6 2015/03/28 22:20:01;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet 00:2E:5F:01:25:33;
  uid "\001\010.\_\20132";
  client-hostname "Wadleigh";
}
```

Server recognizes that a host has requested an IP address and the server has assigned an address.

Test client received an IP address, and all other relevant information such as default gateway and DNS server from the DHCP Server.

Test successful.
Proper operation of FTP Server:
Test will include verification that users are able to transfer files to and from the FTP server and that the Cisco network devices are able to back up their configuration files to the FTP server.

File was successfully downloaded from FTP server.

File was successfully uploaded to FTP server.
Every time the configuration is saved, the device backs up its configuration to the FTP server. The exclamation point at the end of the “Writing” line signifies a successful FTP backup.

**Test successful.**

**SNMP Trap Verification:**
Verify that the SNMP Server is receiving SNMP Traps from devices on the network.

SNMP server is receiving events from devices on the network successfully.

**Test successful.**

**Verification that Syslog Server is receiving log files from devices:**
Check that syslog server is receiving log messages from the devices on the network.

Output of the following command:

```bash
tail /var/log/remote-logs/acm-sw-2960.tydrous.tv.log
```

Syslog server is successfully receiving log messages from acm-sw-2960 and is storing them.

**Test Successful.**

**NTP Clock Accuracy:**
This test is to verify that the devices in the network are properly synchronizing with the internal NTP server.

The Cisco switch has associated with the NTP server which is located at 172.24.64.24.
The switch is also using the same time as the acm-ntp-1 server.

This is the list of associations that the NTP server has made with internet time sources.

<table>
<thead>
<tr>
<th>Remote</th>
<th>Refid</th>
<th>At T When Poll Reach</th>
<th>Delay</th>
<th>Offset</th>
<th>Jitter</th>
</tr>
</thead>
<tbody>
<tr>
<td>69.167.160.102</td>
<td>129.6.15.29</td>
<td>2 u 623 1024 377</td>
<td>41.786</td>
<td>4.009</td>
<td>0.611</td>
</tr>
<tr>
<td>108.166.189.70</td>
<td>173.203.211.73</td>
<td>3 u 631 1024 377</td>
<td>55.949</td>
<td>-1.412</td>
<td>0.474</td>
</tr>
<tr>
<td>173.200.193.178</td>
<td>193.190.230.65</td>
<td>2 u 651 1024 377</td>
<td>85.650</td>
<td>1.382</td>
<td>0.502</td>
</tr>
<tr>
<td>170.214.2.264</td>
<td>187.254.163.42</td>
<td>2 u 656 1024 377</td>
<td>85.835</td>
<td>0.726</td>
<td>0.596</td>
</tr>
<tr>
<td>67.212.115.147</td>
<td>192.168.101.60</td>
<td>2 u 36 1024 377</td>
<td>46.988</td>
<td>1.053</td>
<td>0.414</td>
</tr>
<tr>
<td>173.251.230.140</td>
<td>200.08.196.212</td>
<td>2 u 784 1024 377</td>
<td>56.787</td>
<td>1.547</td>
<td>0.515</td>
</tr>
<tr>
<td>66.175.216.101</td>
<td>173.294.66.27</td>
<td>2 u 678 1024 377</td>
<td>83.044</td>
<td>1.041</td>
<td>0.450</td>
</tr>
<tr>
<td>204.2.134.163</td>
<td>187.203.163.32</td>
<td>2 u 351 1024 377</td>
<td>89.636</td>
<td>0.668</td>
<td>0.193</td>
</tr>
<tr>
<td>95.189.94.4</td>
<td>192.90.2.20</td>
<td>2 u 508 1024 377</td>
<td>117.914</td>
<td>0.946</td>
<td>0.167</td>
</tr>
</tbody>
</table>

Test Successful.

Verification of network Services:

Routing tables:

All subnets are reachable from both routers. There is also a static route in each routing table directing traffic to the internet.

Routing is working as intended.
GLBP:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Grp</th>
<th>Fwd Pri</th>
<th>State</th>
<th>Address</th>
<th>Active router</th>
<th>Standby router</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/1.5</td>
<td>5</td>
<td>-</td>
<td>Active</td>
<td>192.168.128.1</td>
<td>local</td>
<td>192.168.128.2</td>
</tr>
<tr>
<td>Fa0/1.5</td>
<td>5</td>
<td>1</td>
<td>Listen</td>
<td>007.b400.0501</td>
<td>192.168.128.2</td>
<td>-</td>
</tr>
<tr>
<td>Fa0/1.5</td>
<td>5</td>
<td>2</td>
<td>Active</td>
<td>007.b400.0502</td>
<td>local</td>
<td>-</td>
</tr>
<tr>
<td>Fa0/1.10</td>
<td>10</td>
<td>-</td>
<td>Standby</td>
<td>172.24.64.1</td>
<td>172.24.64.2</td>
<td>local</td>
</tr>
<tr>
<td>Fa0/1.10</td>
<td>10</td>
<td>1</td>
<td>Active</td>
<td>007.b400.0a01</td>
<td>local</td>
<td>-</td>
</tr>
<tr>
<td>Fa0/1.10</td>
<td>10</td>
<td>2</td>
<td>Listen</td>
<td>007.b400.0a02</td>
<td>172.24.64.2</td>
<td>-</td>
</tr>
<tr>
<td>Fa0/1.37</td>
<td>37</td>
<td>-</td>
<td>Standby</td>
<td>172.20.32.1</td>
<td>172.20.32.2</td>
<td>local</td>
</tr>
<tr>
<td>Fa0/1.37</td>
<td>37</td>
<td>1</td>
<td>Active</td>
<td>007.b400.2501</td>
<td>local</td>
<td>-</td>
</tr>
<tr>
<td>Fa0/1.37</td>
<td>37</td>
<td>2</td>
<td>Active</td>
<td>007.b400.2502</td>
<td>172.20.32.2</td>
<td>-</td>
</tr>
</tbody>
</table>

Both routers can see one another as participating in GLBP. The Cisco 1841 router is the active router for only the MANAGEMENT VLAN. The Cisco 2851 is the active router for both the Server and USER VLAN.

GLBP is operating as intended.

EIGRP:

<table>
<thead>
<tr>
<th>IP-EIGRP neighbors for process 373</th>
</tr>
</thead>
<tbody>
<tr>
<td>H Address</td>
</tr>
<tr>
<td>-----------</td>
</tr>
<tr>
<td>0  192.168.128.2</td>
</tr>
<tr>
<td>0  192.168.128.3</td>
</tr>
</tbody>
</table>

Both routers have each other an EIGRP neighbors.
Both routers are receiving all the routes for the internal subnets.
Project Weekly Journals
Nicholas Bordo

Name(s): Nicholas Bordo

Summary – Week ending:

<table>
<thead>
<tr>
<th>Date</th>
<th>Start Time</th>
<th>End Time</th>
<th>Description</th>
<th>Total Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/26/2015</td>
<td>13:30</td>
<td>16:30</td>
<td>Connection and installation of networking devices.</td>
<td>3</td>
</tr>
<tr>
<td>1/28/2015</td>
<td>14:00</td>
<td>15:00</td>
<td>Configuration of network devices</td>
<td>1</td>
</tr>
<tr>
<td>1/30/2015</td>
<td>14:00</td>
<td>16:00</td>
<td>Research on FTP Server</td>
<td>2</td>
</tr>
</tbody>
</table>

Total Hours This Week 6

Total Hours to Date 6

Journal Details (sample)

1/26/2015
- Made a network diagram and IP address scheme for the network with all currently known devices.
- Created a corresponding network diagram for all of the connections between devices.
- Racked network devices and connected them according to the network diagram created.
- Did basic configuration of devices
  - IP address assignment
  - VLAN creation
  - Point to point links
  - Port channel configuration
  - Basic Security measures
    - Secured console and VTY lines
    - Added basic username and password for local authentication

1/28/2015
- Continued to work on network configuration
  - Added loopback interfaces to routers
  - Configured EIGRP routing between routers
  - Basic GLBP configuration for two routers

1/30/2015
- Researched how to install Ubuntu server using a USB flash drive.
  - Did a test installation using this method
- Researched installing the FTP service on Ubuntu and tested this method.
Name(s): Nicholas Bordo

Summary – Week ending:

<table>
<thead>
<tr>
<th>Date</th>
<th>Start Time</th>
<th>End Time</th>
<th>Description</th>
<th>Total Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/2/2015</td>
<td>12:30</td>
<td>17:30</td>
<td>Continued configuring network devices/Networking Research</td>
<td>5</td>
</tr>
<tr>
<td>2/3/2015</td>
<td>19:00</td>
<td>22:00</td>
<td>FTP Server Research/configuration testing</td>
<td>3</td>
</tr>
<tr>
<td>2/4/2015</td>
<td>14:00</td>
<td>18:00</td>
<td>Research on FTP Server/configuration testing</td>
<td>4</td>
</tr>
<tr>
<td>2/5/2015</td>
<td>19:00</td>
<td>23:00</td>
<td>Configuration Testing for ftp server</td>
<td>4</td>
</tr>
<tr>
<td>2/6/2015</td>
<td>12:00</td>
<td>18:00</td>
<td>IP address redesign/FTP server OS install and Config</td>
<td>6</td>
</tr>
<tr>
<td>2/7/2015</td>
<td>12:00</td>
<td>16:00</td>
<td>Windows Server 2012 R2 install</td>
<td>4</td>
</tr>
</tbody>
</table>

Total Hours This Week: 26
Total Hours to Date: 26

Journal Details (sample)

2/2/2015
- Continued configuration of network devices and connected them to external network (residential internet connection)
  - Ran into issue where devices were getting DHCP address that overlapped with one of the subnets
  - Did research and troubleshooting on how to keep this issues from happening

2/3/2015
- Did additional research on how to configure vsftpd for virtual users
- Began testing configurations found during research on virtual machine installations of Ubuntu Server 14.04
  - Kept a clean VM instance to make iteration of methods quicker
- Ran through several options and test configurations

2/4/2015
- Continued testing and research of vsftp configurations with VM’s
- Created documentation for installing Ubuntu Server 14.04 using Virtual box
  - Took screen shots of installation process for document creation

2/5/2015
- Successfully configured vsftpd with the desired features
- Documented setups for configuration of vsftpd
- Consulted with Professor Kropff regarding issue discovered on 2/2/2015 regarding subnet overlap
  - Resulting conclusion:
    - Due to the basic operation of Cisco routing absolutely mitigating this problem may not be possible with current hardware inventory
    - Redesign network subnet with uncommonly used subnets to best avoid subnet overlap with host network

2/6/2015
- Redesigned all IP subnets with new less commonly used IP address ranges
  - Reconfigured network devices with new network ip addresses
- Installed Ubuntu Server 14.04 on dedicated server
● Used documentation created on 2/5/2015 to install and configure vsftpd
● Configured network connectivity
  o Verified end to end connectivity from test host to ftp server

● Used test host to connect to FTP server
  o Successfully connected, but permissions configured on FTP server need to be modified

2/7/2015
● Installed Windows Server 2012 R2 using Dreamspark download
  o Installed on second dedicated server
  o Ran into issues where network adapter was not detected by the driver installation software
● Researched solutions to network adapter problem
  o Found solution and applied the fix and installed the driver
  o Documented steps used to install driver on machine
● Installed Hyper-V Role
  o Installed the Hyper-V role on machine
  o Documented steps taken to install Hyper-V
● Changed name of server to name designated in IP address documentation
Name(s): Nicholas Bordo

Summary – Week ending:

<table>
<thead>
<tr>
<th>Date</th>
<th>Start Time</th>
<th>End Time</th>
<th>Description</th>
<th>Total Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/9/2015</td>
<td>12:30</td>
<td>18:30</td>
<td>Completed FTP Server setup/Device configuration for Archive</td>
<td>6</td>
</tr>
<tr>
<td>2/10/2015</td>
<td>19:00</td>
<td>22:00</td>
<td>DHCP Server research and configuration</td>
<td>3</td>
</tr>
<tr>
<td>2/11/2015</td>
<td>14:00</td>
<td>18:00</td>
<td>Configuration/Testing of DHCP Server</td>
<td>4</td>
</tr>
<tr>
<td>2/12/2015</td>
<td>19:00</td>
<td>22:00</td>
<td>Research on SNMP Server</td>
<td>3</td>
</tr>
<tr>
<td>2/13/2015</td>
<td>12:00</td>
<td>15:00</td>
<td>Installation of SNMP Server on Virtual Machine</td>
<td>3</td>
</tr>
<tr>
<td>2/15/2015</td>
<td>12:00</td>
<td>16:00</td>
<td>Configuration and research of network device SNMP config</td>
<td>4</td>
</tr>
</tbody>
</table>

Total Hours This Week: 23
Total Hours to Date: 23

Journal Details (sample)

2/9/2015
- Completed the configuration of the FTP server.
  - Permissions issues were resolved and files are now able to be transferred in both directions.
  - Created user account for network devices to use for configuration backup.
  - Did test transfer of files.
- Setup configuration Archive on network device
  - Used the archive feature combined with Kron to schedule regular configuration backups to FTP server.
  - Tested this backup method on all devices to verify operation.

2/10/2015
- Began research on DHCP server configuration
  - Research the configuration files for dhcp3-server and isc-dhcp-server
  - Used isc-dhcp-server for DHCP server
  - Began testing configurations.

2/11/2015
- Continued to test DHCP server configurations
  - Successfully configured DHCP configuration
  - Tested DHCP server by connecting test PC to network
  - Successfully obtained IP address from server.

2/12/2015
- Researched SNMP Server configuration.
  - Looked through documentation of OpenNMS for installation.

2/13/2015
- Test installation
  - Tested installation process on a virtual machine
  - Did a clean installation on Hyper-v Virtual machine
• Will be used to test out configuration of monitoring process with network devices.

2/15/2015

• Network device SNMP Configuration
  - Tested methods for adding devices for network monitoring
• Continued research for adding network devices and servers to monitoring software.
Name(s): Nicholas Bordo

Summary – Week ending:

<table>
<thead>
<tr>
<th>Date</th>
<th>Start Time</th>
<th>End Time</th>
<th>Description</th>
<th>Total Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/16/2015</td>
<td>12:30</td>
<td>17:30</td>
<td>Research/test of DNS server and Research for SNMP</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>config</td>
<td></td>
</tr>
<tr>
<td>2/17/2015</td>
<td>19:00</td>
<td>22:00</td>
<td>SNMP server setup research</td>
<td>3</td>
</tr>
<tr>
<td>2/22/2015</td>
<td>12:00</td>
<td>16:00</td>
<td>Configuration of SNMP server GUI</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Total Hours This Week</th>
<th>Total Hours to Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>12</td>
</tr>
</tbody>
</table>

Journal Details (sample)

2/16/2015

- Researched DNS Server setup
  - Tested various configurations on test VMs
- Researched proper configuration of SNMP on network devices and servers
  - Looked for examples of cisco SNMP config
  - Looked for examples of Linux server SNMP config

2/17/2015

- Researched setup of OpenNMS server GUI for SNMP capable devices.
  - How to added SNMP functionality to monitored devices in addition to ICMP and SSH monitoring.

2/22/2015

- Applied and tested some configurations of SNMP devices on server
  - Applied test SNMP configurations to network devices.
  - Verified test configuration was sending data to SNMP server.
  - Tested various functions of SNMP monitored devices
  - Explored other functionality of OpenNMS
Name(s): Nicholas Bordo

Summary – Week ending:

<table>
<thead>
<tr>
<th>Date</th>
<th>Start Time</th>
<th>End Time</th>
<th>Description</th>
<th>Total Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/23/2015</td>
<td>12:30</td>
<td>15:30</td>
<td>Worked on documentation of project</td>
<td>3</td>
</tr>
<tr>
<td>2/28/2015</td>
<td>12:00</td>
<td>21:00</td>
<td>Networking to internet, DNS Server setup and testing</td>
<td>9</td>
</tr>
<tr>
<td>3/1/2015</td>
<td>12:00</td>
<td>19:00</td>
<td>DNS Server continued, NTP Server setup and testing</td>
<td>7</td>
</tr>
</tbody>
</table>

**Total Hours This Week** 19

**Total Hours to Date** 19

Journal Details (sample)

2/23/2015

- Worked on getting information for project more organized.
  - Complied some screen shots of server installations.
  - Created some documents for server setup.

2/28/2015

- Worked on getting network connected to the internet.
  - Hooked up one of the routers to an internet connection.
    - Ran into some issues being able to ping out of the network to the internet
      - Troubleshooted that issue and partially resolved it. Still having some latency issues.
      - Will have to revisit this.
  - Began work on DNS server.
    - Installed Bind9 and did an initial test configuration
    - Got service running and resolving internal IPs to hostnames
    - Also able to forward queries to internet DNS servers and return the proper results.

3/1/2015

- Continued work on DNS server
  - Configured clients, servers, and network devices to properly use the internal DNS server.
  - Finished adding additional hostnames to the DNS reverse lookup database
- Began work on NTP server
  - Researched setup process for NTP
  - Did test installation
  - Successfully peer NTP server with internet NTP time sources
  - Configured clients, servers, and network devices to use internal NTP server.
- Documented steps for DNS and NTP server setup
  - Took screen shots and made notes of problems during the installation process.
### Name(s): Nicholas Bordo

### Summary – Week ending:

<table>
<thead>
<tr>
<th>Date</th>
<th>Start Time</th>
<th>End Time</th>
<th>Description</th>
<th>Total Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/2/2015</td>
<td>13:00</td>
<td>20:00</td>
<td>Troubleshooting Network issues &amp; documentation of project</td>
<td>7</td>
</tr>
<tr>
<td>3/4/2015</td>
<td>17:00</td>
<td>19:00</td>
<td>Worked on documentation</td>
<td>2</td>
</tr>
</tbody>
</table>

**Total Hours This Week**

| Total Hours to Date | 9 |

### Journal Details (sample)

#### 3/2/2015

- Trouble shot networking issue
  - Was unable to receive any kind of consistent connection to the internet. Every other ping timed out while one would successfully reach its destination.
    - Root cause of the issue was a problem with the routing in the network configuration.
      - Cisco devices that receive an IP address via DHCP apparently also place the DHCP default gateway information in their routing table making that route the default of all traffic much like most home routers do.
      - Since this operation was the overall goal of the project this behavior is not an issue, however when creating the network configuration this knowledge was unknown to me. When I place a static default route on the routers this information was being confused with the DHCP default route causing every other packet to be lost because of equal cost load balancing.
    - Solution was to remove statically configured default gateway
      - Once the static default route was removed all connection issues were resolved.
  - Worked on documentation for DNS server configuration
    - Created some of the documentation on how to configure Bind9
    - Took screen shots on the DNS server VM.

#### 3/4/2015

- Continued work on DNS server documentation and started on the NTP server documentation
### Name(s): Nicholas Bordo

#### Summary – Week ending:

<table>
<thead>
<tr>
<th>Date</th>
<th>Start Time</th>
<th>End Time</th>
<th>Description</th>
<th>Total Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/10/2015</td>
<td>19:00</td>
<td>4:00</td>
<td>Troubleshooting slow DNS query response</td>
<td>9</td>
</tr>
<tr>
<td>3/12/2015</td>
<td>19:00</td>
<td>2:00</td>
<td>Troubleshooting DNS reverse lookup</td>
<td>7</td>
</tr>
<tr>
<td>3/13/2015</td>
<td>16:00</td>
<td>20:00</td>
<td>Worked on DNS cleanup and documentation</td>
<td>4</td>
</tr>
<tr>
<td>3/14/2015</td>
<td>20:00</td>
<td>23:00</td>
<td>Testing</td>
<td>2</td>
</tr>
<tr>
<td>3/15/2015</td>
<td>12:00</td>
<td>18:00</td>
<td>Testing and documentation</td>
<td>6</td>
</tr>
</tbody>
</table>

**Total Hours This Week**: 28

**Total Hours to Date**: 28

#### Journal Details

**3/10/2015**
- Trouble shot DNS issue
  - Had a problem with DNS queries taking much longer than they should. So long so that web pages would timeout when first trying to load them.
    - Issue was caused by a miss configuration of the DNS spoofing feature on the Cisco routers. Internal DNS server pointed to those routers as their first DNS server and those servers were then pointing back to the internal DNS server. This caused a loop until the request timed out and another DNS server was utilized.
    - Solution: Removed the DNS spoofing feature from the routers and the statement pointing the internal DNS server to the routers as DNS servers. This Spoofing feature was needed up until the point when the internal DNS server was configured.

**3/12/2015**
- Trouble shot reverse lookup issue.
  - Was having issue where reverse lookup would return no results and say that IP address could not be found.
    - Was able to find the solution to my problems on the internet after a large amount of searching and testing. It was caused by a formatting issue in the reverse lookup zone file.

**3/13/2015**
- DNS Clean up
  - Got the Remaining of the subnets functional in DNS for both forward and reverse lookup.
- Continued to work on the documentation for the DNS server

**3/14/2015**
- Tested internet connection redundancy
  - Made some alterations to the GLBP configuration and tested its resilience to losing one devices internet connection and the loss of a device completely.

**3/15/2015**
- Worked on documentation for network configuration and server configurations.
**Name(s): Nicholas Bordo**

**Summary – Week ending:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Start Time</th>
<th>End Time</th>
<th>Description</th>
<th>Total Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/16/2015</td>
<td>19:00</td>
<td>22:00</td>
<td>Worked on documentation and testing</td>
<td>3</td>
</tr>
</tbody>
</table>

**Total Hours This Week**

| Total Hours to Date | 3           |

**Journal Details (sample)**

*3/16/2015*

- Worked on documentation for binder.
  - Took screenshots of configuration files
  - Wrote outline of binder.
- Did testing of network.
  - Tested DNS for proper operation.
  - Tested network configuration
    - Reviewed configurations of network devices
### Name(s): Nicholas Bordo

### Summary – Week ending:

<table>
<thead>
<tr>
<th>Date</th>
<th>Start Time</th>
<th>End Time</th>
<th>Description</th>
<th>Total Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/23/2015</td>
<td>12:00</td>
<td>20:00</td>
<td>Worked on documentation and binder</td>
<td>8</td>
</tr>
<tr>
<td>3/24/2015</td>
<td>17:00</td>
<td>23:00</td>
<td>Worked on documentation and binder</td>
<td>6</td>
</tr>
<tr>
<td>3/25/2015</td>
<td>12:00</td>
<td>22:00</td>
<td>Worked on documentation and binder</td>
<td>10</td>
</tr>
<tr>
<td>3/26/2015</td>
<td>15:00</td>
<td>22:00</td>
<td>Worked on documentation and binder</td>
<td>7</td>
</tr>
<tr>
<td>3/27/2015</td>
<td>10:00</td>
<td>20:00</td>
<td>Worked on documentation and binder</td>
<td>10</td>
</tr>
<tr>
<td>3/28/2015</td>
<td>11:00</td>
<td>20:00</td>
<td>Worked on documentation and binder</td>
<td>9</td>
</tr>
<tr>
<td>3/29/2015</td>
<td>12:00</td>
<td>21:00</td>
<td>Worked on documentation and binder</td>
<td>9</td>
</tr>
</tbody>
</table>

**Total Hours This Week**

**Total Hours to Date**

59
Research References
Nicholas Bordo


