

Summer 2015

# Enhanced Child's Play LAN Design

Nicholas B. Bordo

*The University Of Akron*, [nbb5@zips.uakron.edu](mailto: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](http://ideaexchange.uakron.edu/honors_research_projects)



Part of the [OS and Networks Commons](#)

---

## Recommended Citation

Bordo, Nicholas B., "Enhanced Child's Play LAN Design" (2015). *Honors Research Projects*. 181.

[http://ideaexchange.uakron.edu/honors\\_research\\_projects/181](http://ideaexchange.uakron.edu/honors_research_projects/181)

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](mailto:mjon@uakron.edu), [uapress@uakron.edu](mailto:uapress@uakron.edu).

# Enhanced Child's Play LAN Design

Nicholas Bordo

# Table of Contents

Table of Contents	1
Project Plan	2
Project Analysis	6
Presentation	8
Project Description	13
IP Address Scheme	15
Logical Network Topology	18
Detailed Network Topology	19
0 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:

Planning	Research	Installation	Configuration	Testing	Documentation	Total
10	20	10	40	20	30	130

Actual:

Planning	Research	Installation	Configuration	Testing	Documentation	Total
8	25	16	48	23	65	185

# Project Analysis

Nicholas Bordo

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.

# Presentation

Nicholas Bordo

## ENHANCED CHILD'S PLAY LAN DESIGN

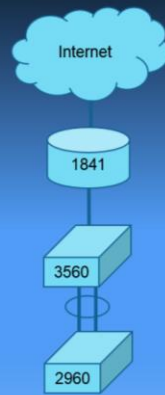
Nicholas Bordo

### 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

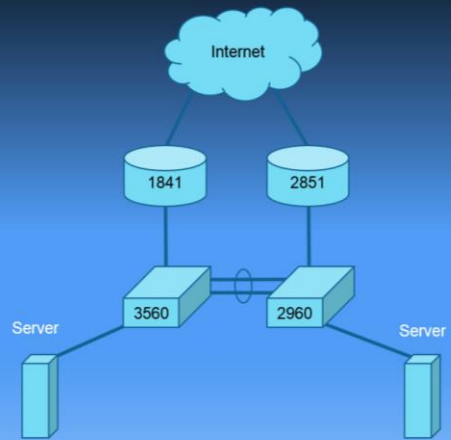


## SERVICES RUN ON ROUTER

- 1841 Router performed
  - DNS
  - DHCP
  - NAT
  - Routing(internet)



## New Network Design



## 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:

Networks	172.20.32.0/19	172.24.64.0/20	192.168.128.0/22
Devices	User VLAN 37	Server Addresses VLAN 10	Networking Devices/ Management VLAN 5
	First 20 reserved for network devices	First 20 reserved for network devices	First 20 reserved for network devices
Beginning	172.20.32.0	172.24.64.0	192.168.128.0
End	172.24.63.255	172.24.79.255	192.168.131.255
ACM-RTR-2851	192.168.132.2	255.255.255.255	loopback0
ACM-RTR-1841	192.168.132.3	255.255.255.255	loopback0

## VLAN 5 Management:

VLAN 5 Management	192.168.128.0/22	Range: 192.168.128.0 - 192.168.31.255		First 20 reserved for network devices	
Network Devices	IP Address	Subnet Mask	Interface	Connected Link	Description
GLBP-Gateway	192.168.128.1	255.255.252.0	GLBP Virtual	GLBP Virtual	VLAN 5 Gateway address of GLBP instance.
ACM-RTR-2851- gig-0-1-5	192.168.128.2	255.255.252.0	Fa0/1.5	ACM-SW-3560- fa-0/1	
ACM-RTR-1841- fa-0-1-5	192.168.128.3	255.255.252.0	gig0/1.5	ACM-SW-2960- gig-0/1	
ACM-SW-3560	192.168.128.11	255.255.252.0	VLAN 5	VLAN interface	Management ip address
ACM-SW-2960	192.168.128.12	255.255.252.0	VLAN 5	VLAN interface	Management ip address
ACM-RTR-2851	192.168.132.2	255.255.255.255			
ACM-RTR-1841	192.168.132.3	255.255.255.255			
DHCP Pool	192.168.131.250-254				

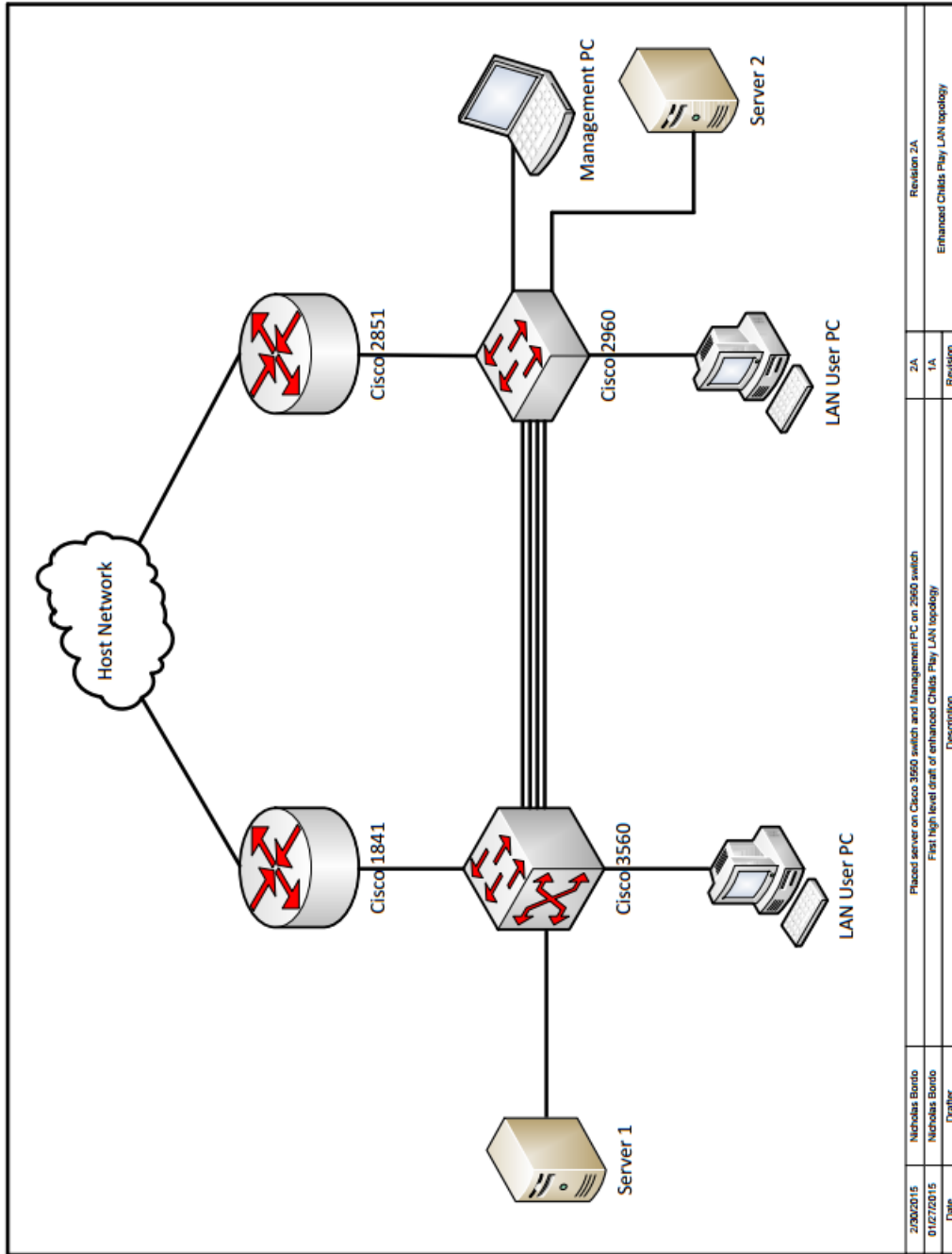
## VLAN 10 Server:

VLAN 10 Servers	172.24.64.0/20	Range: 172.24.64.0 - 172.24.79.255		First 20 reserved for network devices	
Network Devices	IP Address	Subnet Mask	Interface	Connected Link	Description
GLBP-Gateway	172.24.64.1	255.255.240.0	GLBP Virtual	GLBP Virtual	VLAN 10 Gateway address of GLBP instance.
ACM-RTR-2851-gig-0-1-10	172.24.64.2	255.255.240.0	Fa0/1.10	ACM-SW-3560 fa 0/1	
ACM-RTR-1841-fa-0-1-10	172.24.64.3	255.255.240.0	Gig0/1.10	ACM-SW-2960 gig 0/1	
ACM-VM-HOST-1	172.24.64.21	255.255.240.0		ACM-SW-3560 fa0/48	ip address of Microsoft Server hosting VM's
ACM-DNS-1	172.24.64.22	255.255.240.0		ACM-SW-3560 fa0/48	
ACM-DHCP-1	172.24.64.23	255.255.240.0		ACM-SW-3560 fa0/48	
ACM-NTP-1	172.24.64.24	255.255.240.0		ACM-SW-3560 fa0/48	
ACM-SNMP-1	172.24.64.25	255.255.240.0		ACM-SW-3560 fa0/48	
ACM-SYSLOG-1	172.24.64.26	255.255.240.0		ACM-SW-3560 fa0/48	
ACM-FTP-1	172.24.64.27	255.255.240.0		ACM-SW-2960 Gig0/2	On gig port to maximize bandwidth available to LAN for FTP Transfers
DHCP Pool	172.24.79.0 -255	255.255.240.0			

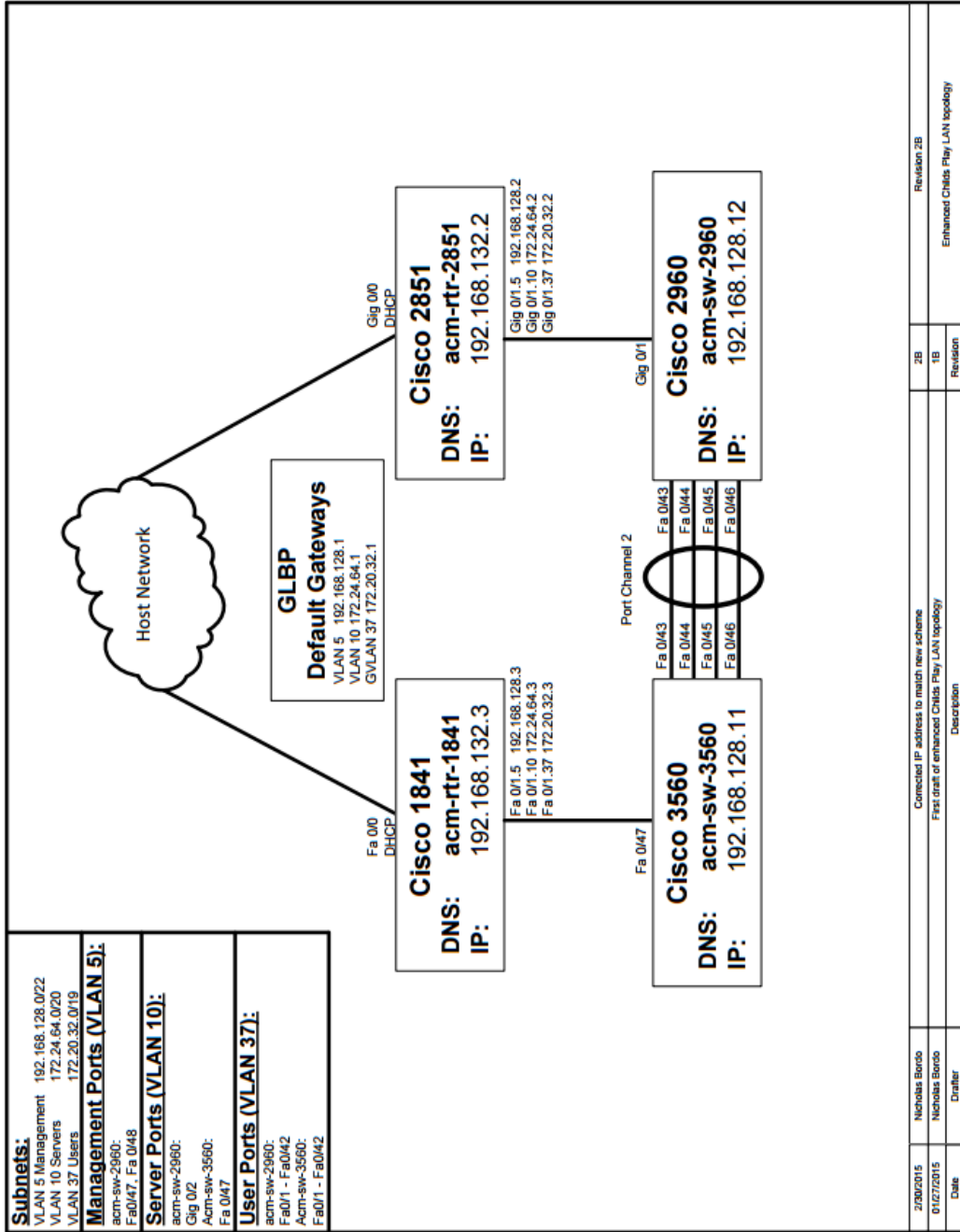
## VLAN 37 User:

VLAN 10 Servers	172.20.32.0/19	Range: 172.20.32.0 - 172.24.63.255		First 20 reserved for network devices	
Network Devices	IP Address	Subnet Mask	Interface	Connected Link	Description
GLBP-Gateway	172.20.32.1	255.255.224.0	GLBP Virtual	GLBP Virtual	VLAN 10 Gateway address of GLBP instance.
ACM-RTR-2851-gig-0-1-10	172.20.32.2	255.255.224.0	Fa0/1.10	ACM-SW-3560 fa 0/1	
ACM-RTR-1841-fa-0-1-10	172.20.32.3	255.255.224.0	Gig0/1.10	ACM-SW-2960 gig 0/1	
User-pool	172.20.32.21- 172.20.63.255	255.255.224.0			IP addresses that will be used for users connecting to the network.

# Logical Network Topology



# Detailed Network Topology



# Network Device Configuration

Cisco 1841 Configuration	21
Cisco 2851 Configuration	27
Cisco 2960 Configuration	33
Cisco 3560 Configuration	38
Cisco Code Updates	43

# 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$iTBgfa8tMrw0rLh4i9bE7.
    #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 7 03281A18055F16435C0210  
    #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@d0N!y 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@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 192.168.132.3 255.255.255.255
    #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
```

```
glbp 5 ip 192.168.128.1
```

```
    #Sets the Virtual IP address of the default gateway
```

```
glbp 5 priority 130
```

```
    #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 130 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 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
```

```
glbp 10 ip 172.24.64.1
```

```
glbp 10 priority 110 #This router will be the AVF for this VLAN
```

```
glbp 10 preempt
```

```
glbp 10 weighting 110 lower 80 upper 90
```

```
glbp 10 load-balancing weighted
```

```
glbp 10 authentication md5 key-chain cisco
```

```
glbp 10 weighting track 1 decrement 40
```

```
#User VLAN sub interface GLBP Configuration
```

```
interface FastEthernet0/1.37
```

```
glbp 37 ip 172.20.32.1
```

```
glbp 37 priority 110 #This router will be the AVF for this VLAN
```

```
glbp 37 preempt
```

```
glbp 37 weighting 110 lower 80 upper 90
```

```
glbp 37 authentication md5 key-chain cisco
```

```
glbp 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$iTBgfa8tMrw0rLh4i9bE7.
    #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 7 03281A18055F16435C0210

#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@d0N!y 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

#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 172.24.64.2 255.255.240.0
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.
```

```
#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 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
```

# Cisco 2960 Configuration

## Configuration Explanation for ACM Cisco 2960

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$iTBgfa8tMrw0rLh4i9bE7.
    #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 7 03281A18055F16435C0210

#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@d0N!y 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$iTBgfa8tMrw0rLh4i9bE7.
    #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 7 03281A18055F16435C0210  
#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@d0N!y 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 192.168.128.11 255.255.252.0
    #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.

```
acm-sw-3560#$/acm-sw-3560/code/c3560-ipservicesk9-mz.122-55.SE10.bin flash:
Destination filename [c3560-ipservicesk9-mz.122-55.SE10.bin]?
Accessing ftp://172.24.64.27/archive/acm-sw-3560/code/c3560-ipservicesk9-mz.122-55.SE10.bin...
Loading archive/acm-sw-3560/code/c3560-ipservicesk9-mz.122-55.SE10.bin !
```

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

```
acm-sw-3560#$/acm-sw-3560/code/c3560-ipservicesk9-mz.122-55.SE10.bin flash:
Destination filename [c3560-ipservicesk9-mz.122-55.SE10.bin]?
Accessing ftp://172.24.64.27/archive/acm-sw-3560/code/c3560-ipservicesk9-mz.122-55.SE10.bin...
Loading archive/acm-sw-3560/code/c3560-ipservicesk9-mz.122-55.SE10.bin !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!
[OK - 12749374/4096 bytes]

12749374 bytes copied in 268.997 secs (47396 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
HELPER path-list   :
Auto upgrade       : yes
Auto upgrade path  :
NVRAM/Config file  :
  buffer size:     524288
Timeout for Config :
  Download:        0 seconds
Config Download    :
  via DHCP:        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
```

```
export@cisco.com.

cisco WS-C3560-48TS (PowerPC405) processor (revision C0) with 131072K bytes of memory.
Processor board ID CAT0923X17F
Last reset from power-on
4 Virtual Ethernet interfaces
48 FastEthernet interfaces
4 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

512K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:14:6A:A6:FD:00
Motherboard assembly number     : 73-9898-05
Power supply part number        : 341-0097-02
Motherboard serial number       : CAT09230FWC
Power supply serial number      : DCA10161HXL
Model revision number           : C0
Motherboard revision number     : A0
Model number                    : WS-C3560-48TS-S
System serial number            : CAT0923X17F
SFP Module assembly part number : 73-7757-03
SFP Module revision Number      : A0
SFP Module serial number        : CAT09221P3U
Top Assembly Part Number        : 800-26162-02
Top Assembly Revision Number    : A0
Version ID                      : V02
CLEI Code Number                : COMMJ00ARB
Hardware Board Revision Number  : 0x01

Switch Ports Model          SW Version  SW Image
-----
*   1 52   WS-C3560-48TS   12.2 (55) SE10   C3560-IPSERVICESK9-M
```

Device has been successfully upgraded to a new code.

# VM Server Setup

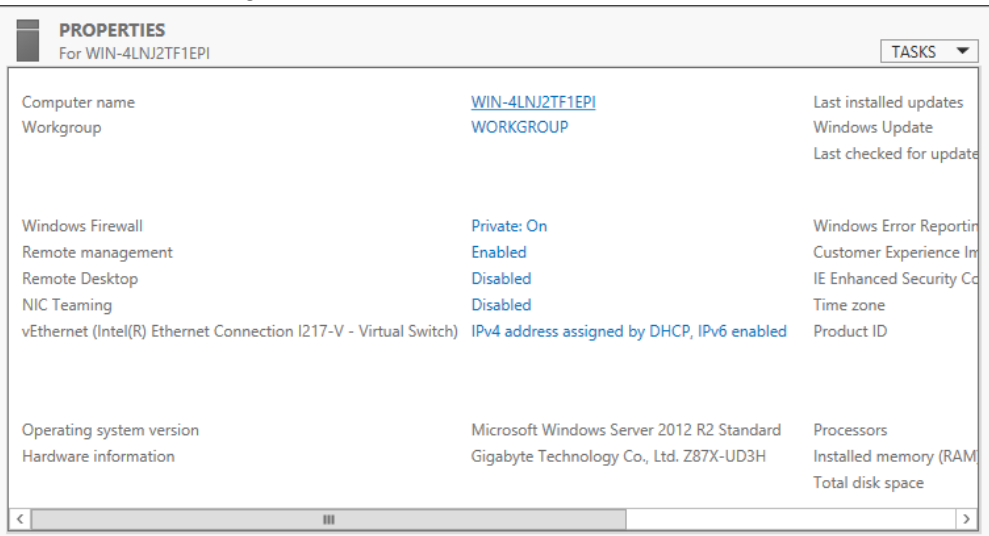
Changing Windows Server 2012 R2 Name	46
Installing Hyper-V	48
Configuring IP address and DNS on Windows Server 2012 R2	54
Configuring Windows Server 2012 R2 to use NTP	57

# Changing Windows Server 2012 R2 Name

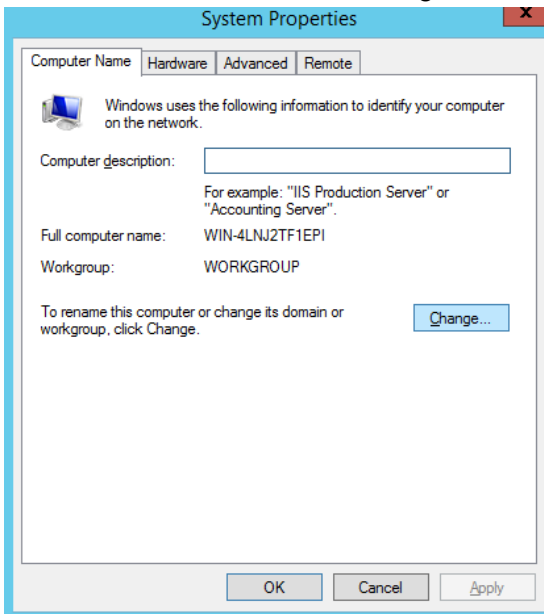
For the purposes of these instructions, anything after “#” is a comment for the benefit of the reader to better explain the function of a command.

## Changing server name:

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

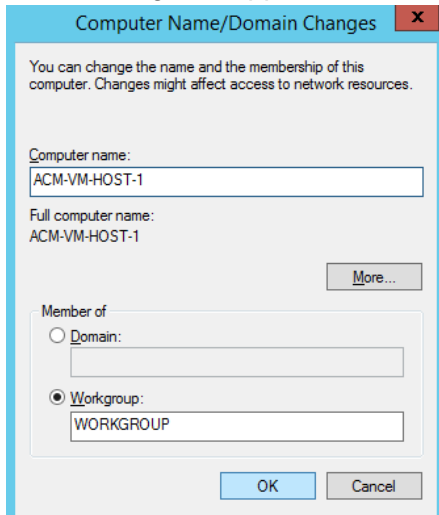


In this window, select the “Change...” button to configure the new name of the server.

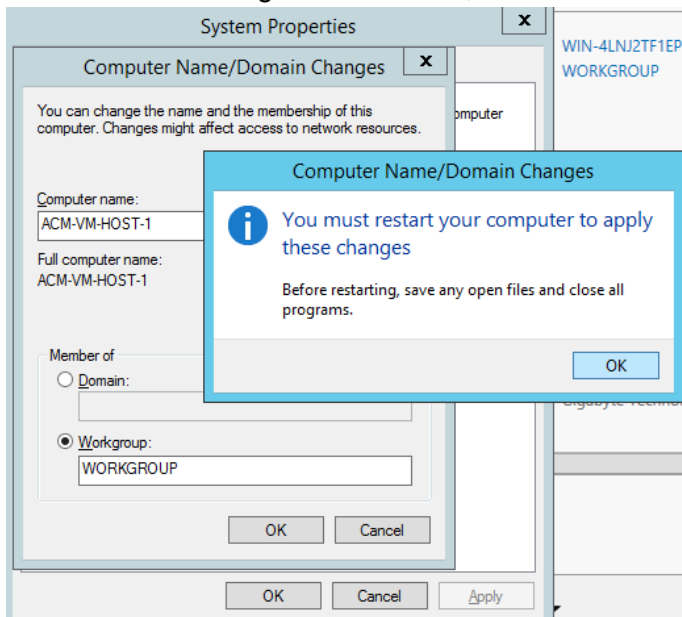




In the dialog that appears, enter the desired name of the server and click “OK”.



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



After reboot the name change is complete.

# Installing Hyper-V

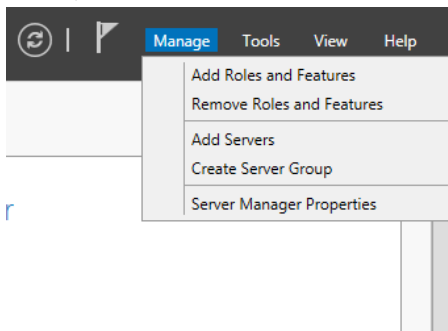
These instructions are for installing Hyper-V on Windows Server 2012 R2

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.

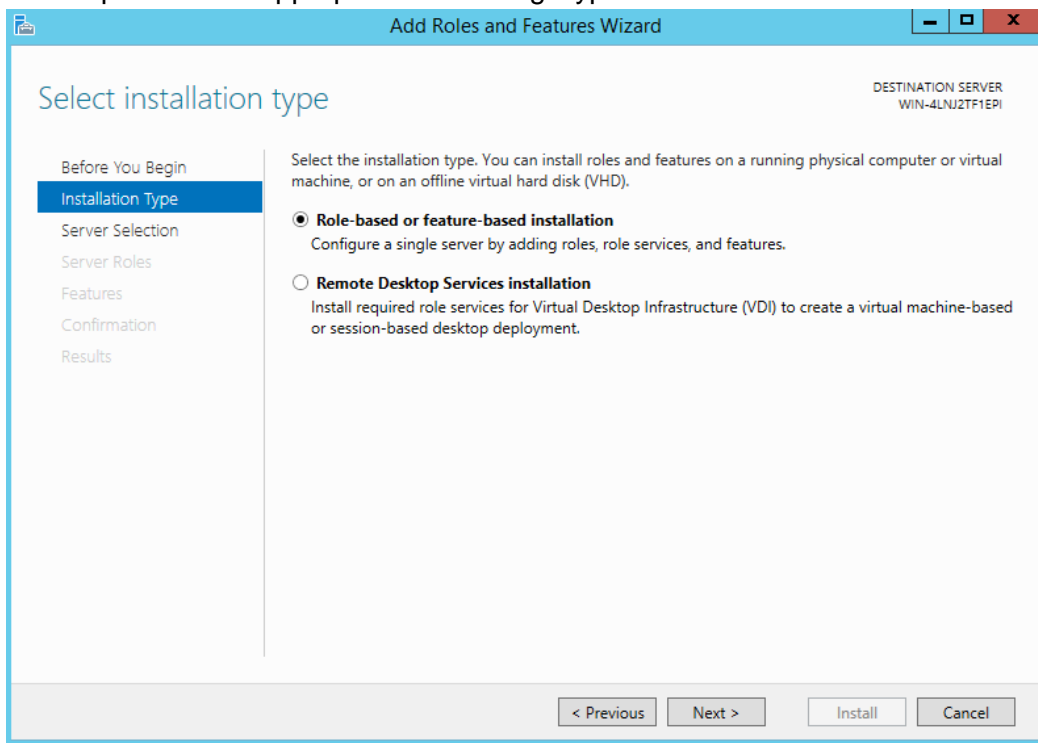
## Start with a clean installation of Windows Server 2012 R2

### Adding the Hyper-V Role:

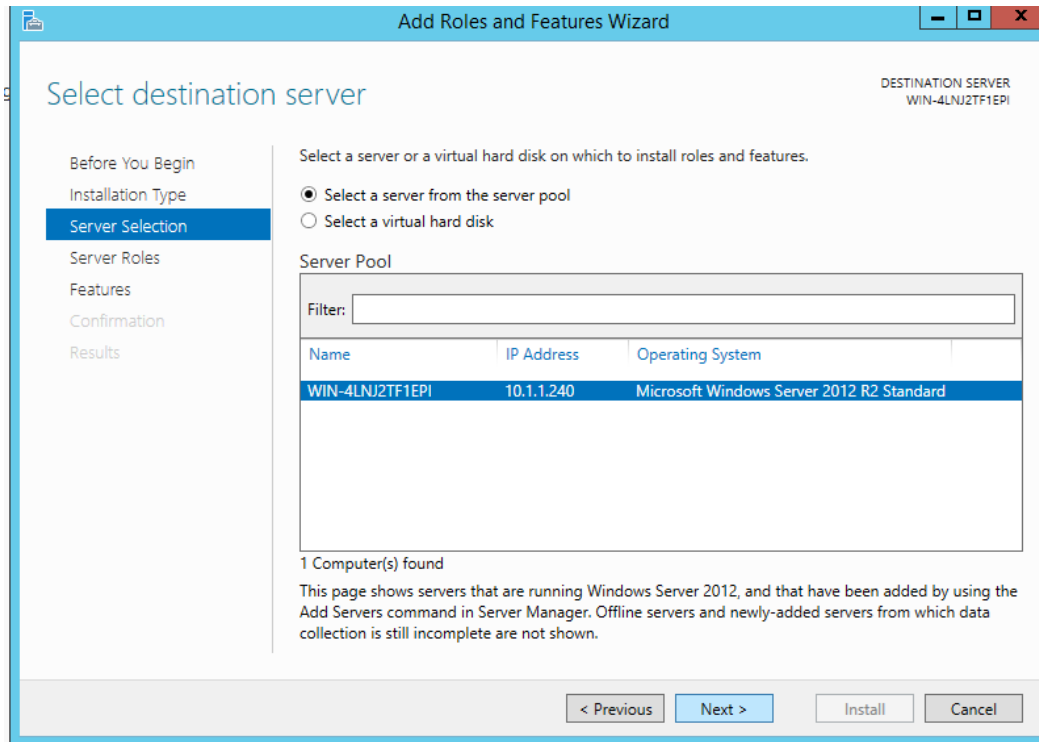
In order to add the Hyper-V, access the Server manager and click on the “Manage” drop down. Then, select the “Add Roles and Features” option.



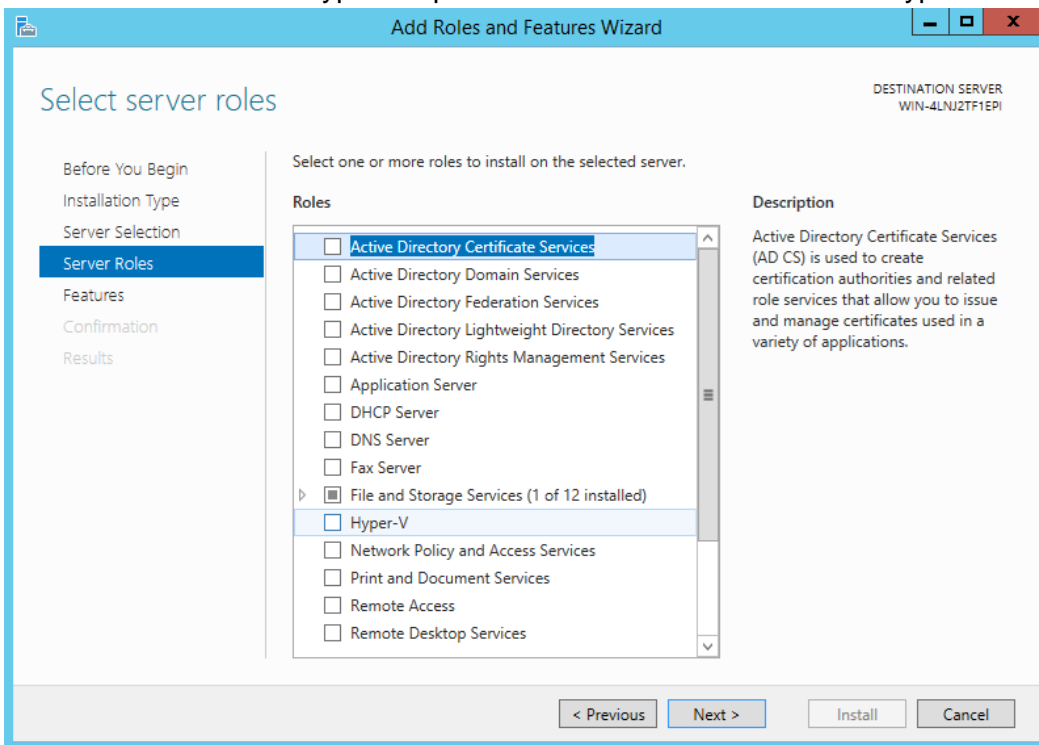
This will bring up the Add Roles and Features Wizard. “Role based or feature-based installation” is the option that is appropriate for adding Hyper-V. Click Next.



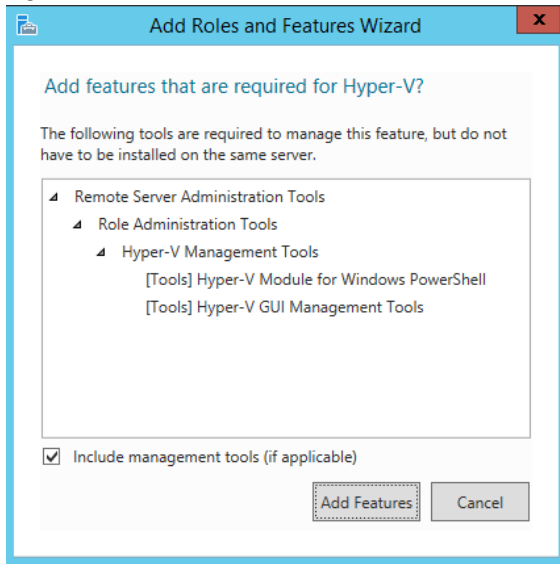
In this window select, the server to add the Hyper-V Role. Click “Next” when the server has been selected.



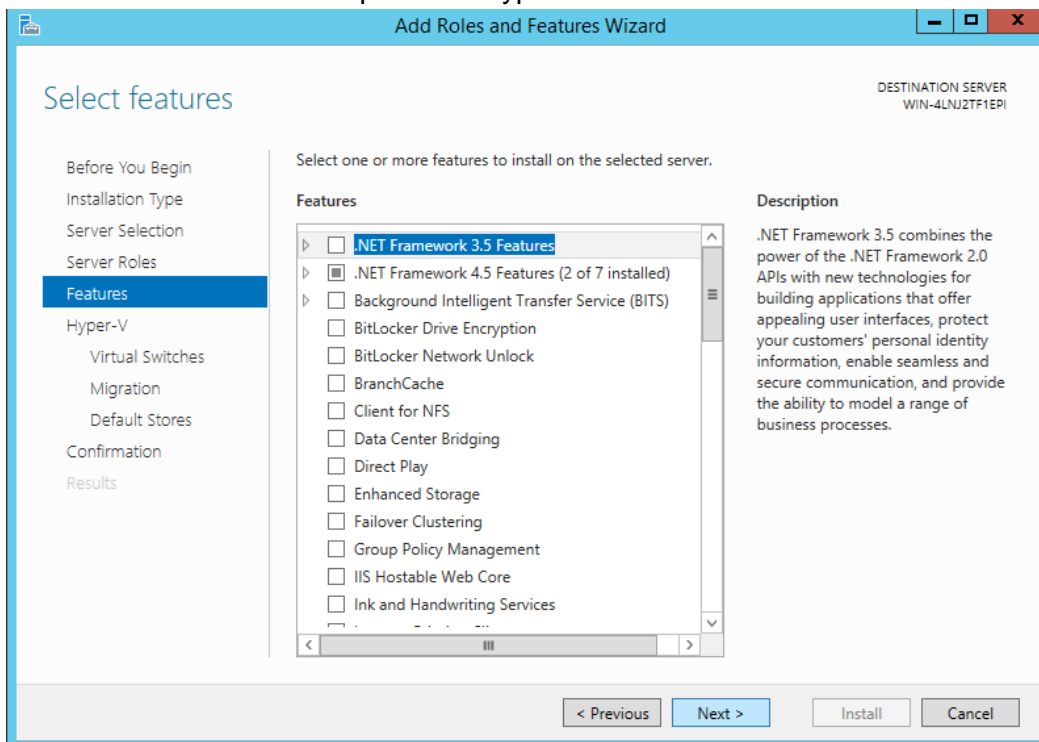
In this list is where the Hyper-V option is located. Check the box for Hyper-V. Click Next.



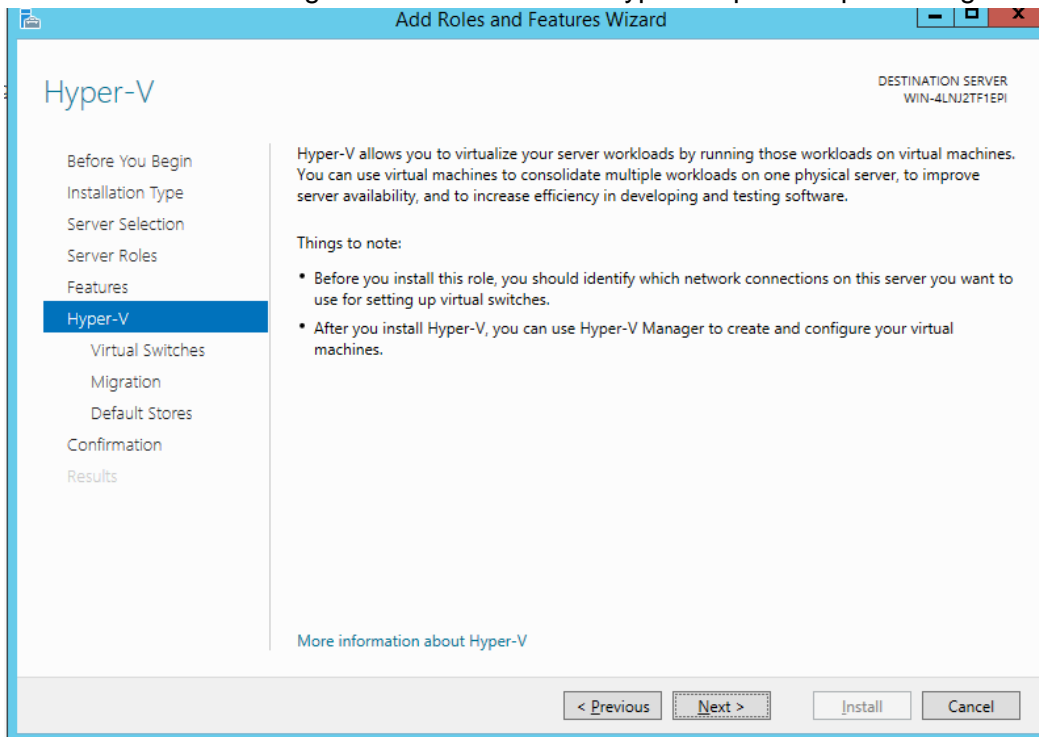
A dialog box will appear with a list of dependent features, which must be installed along with Hyper-V. These are required for the operation of Hyper-V. Click “Add Features” and click Next again to continue.



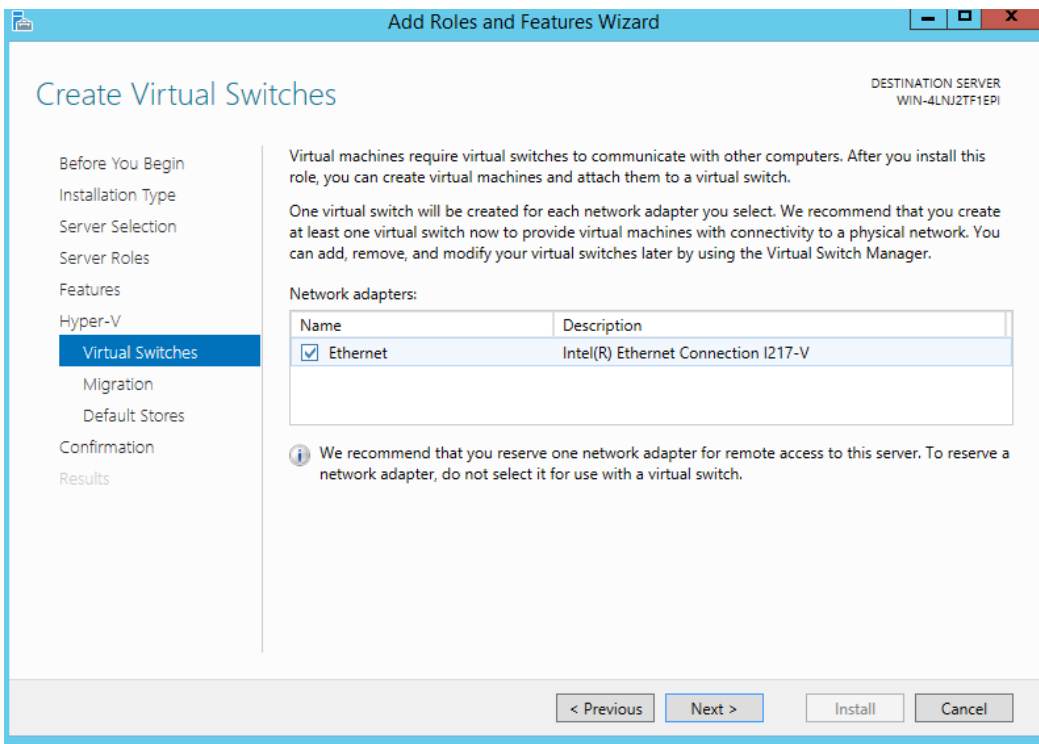
This window is where features would be added, however, no additional features need to be installed at this time to complete the Hyper-V installation. Click Next.



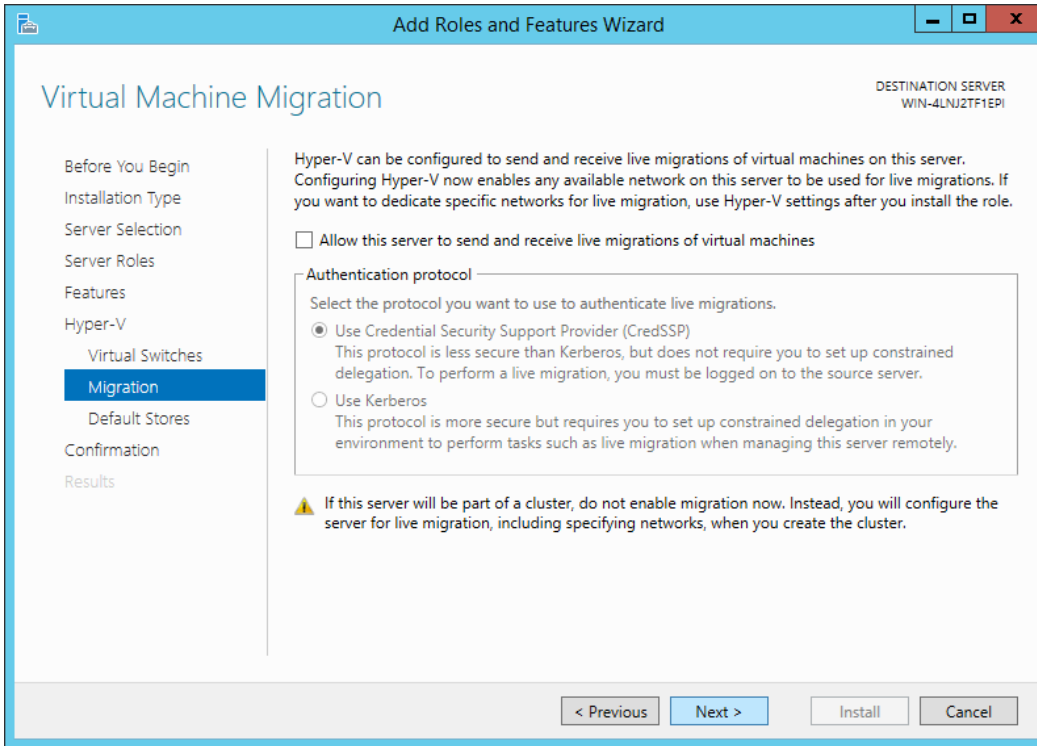
Here is where the configuration of the various Hyper-V specific options begins. Click Next.



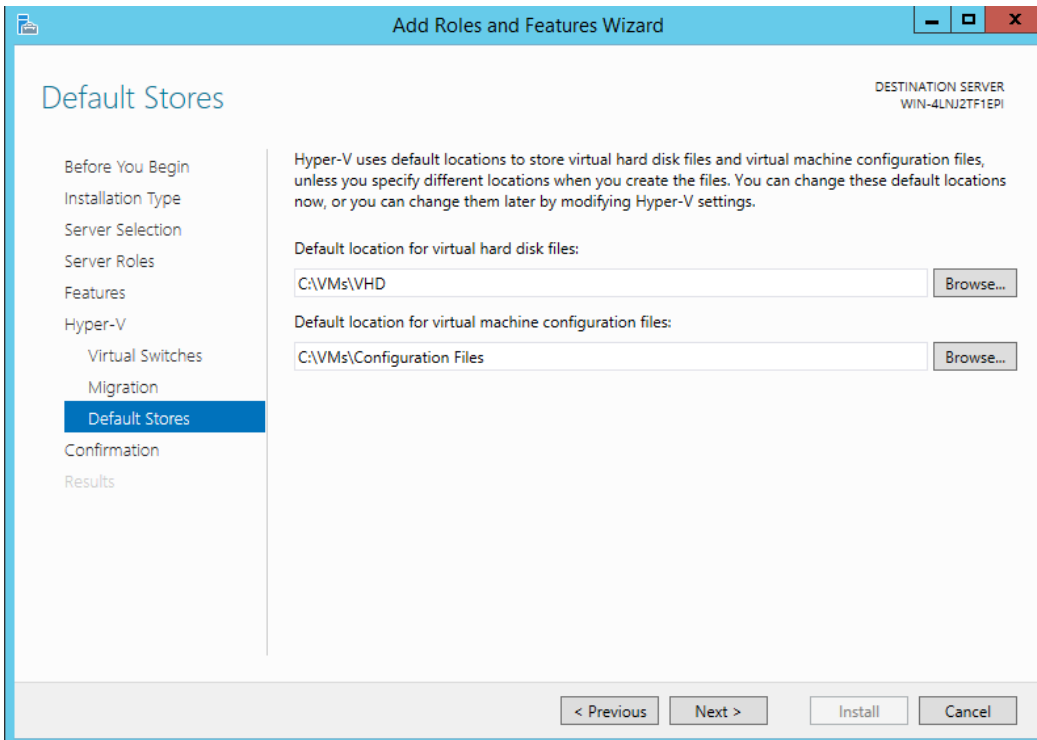
First, a virtual switch must be created for the Virtual machines Hyper-V. These VMs will use this switch to communicate with the rest of the network while only being physically connected to one Ethernet cable. Check the box next to the Ethernet adapter to use for the virtual switch and click "Next".



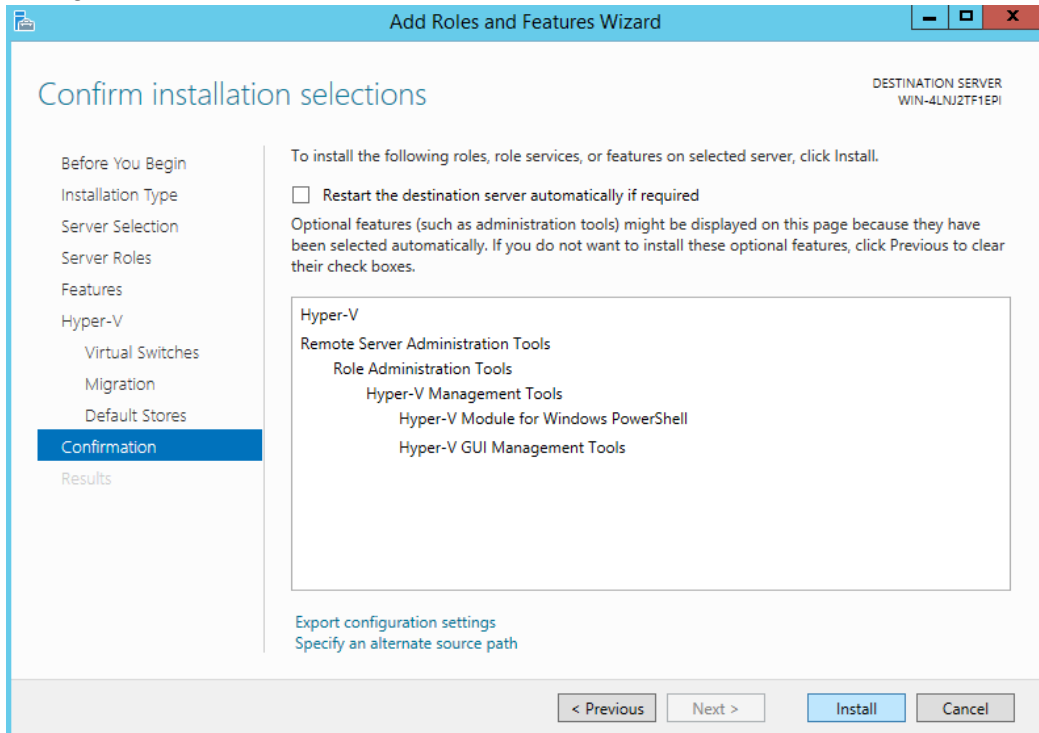
This tutorial will not be utilizing the Migration feature. Click “Next” to skip.



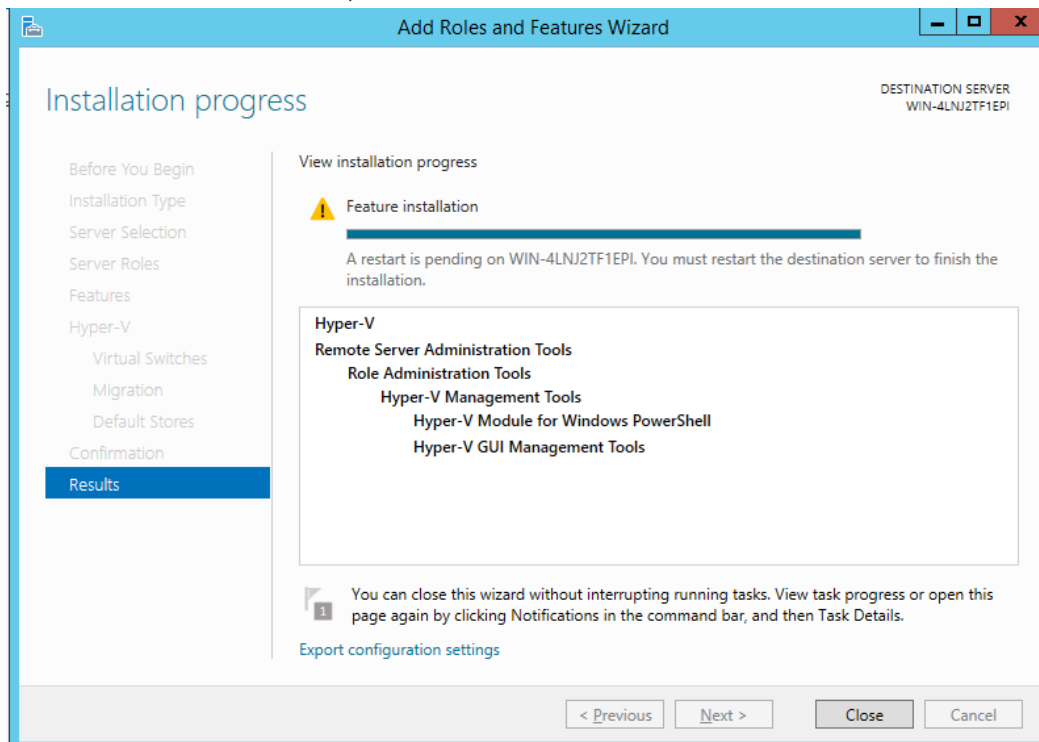
Here is where the default storage locations of the VMs will be. The defaults can be used or custom folders can be created. Click “Next”.



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

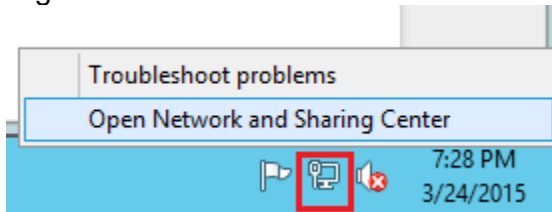
For the purposes of these instructions, anything after “#” is a comment for the benefit of the reader to better explain the function of a command.

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”.



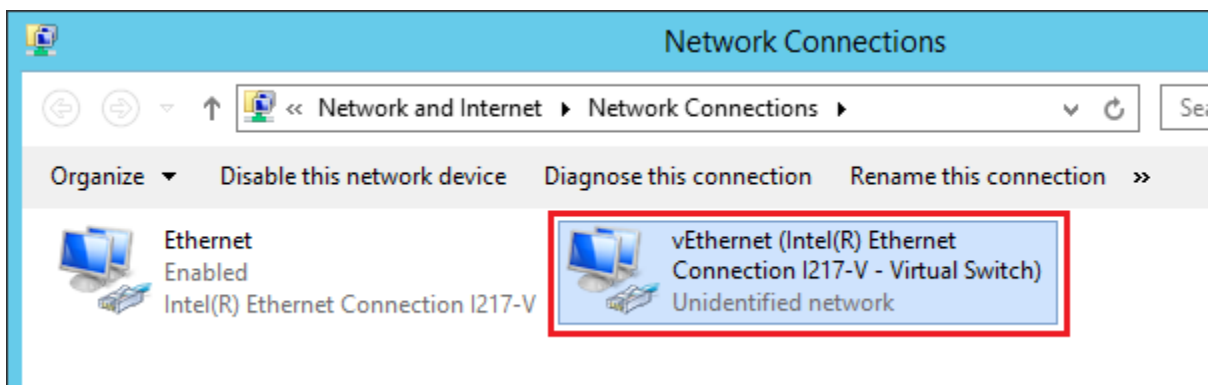
In the Network sharing Center select the “Change adapter settings” option in the top left corner of the window.

Control Panel Home

[Change adapter settings](#)

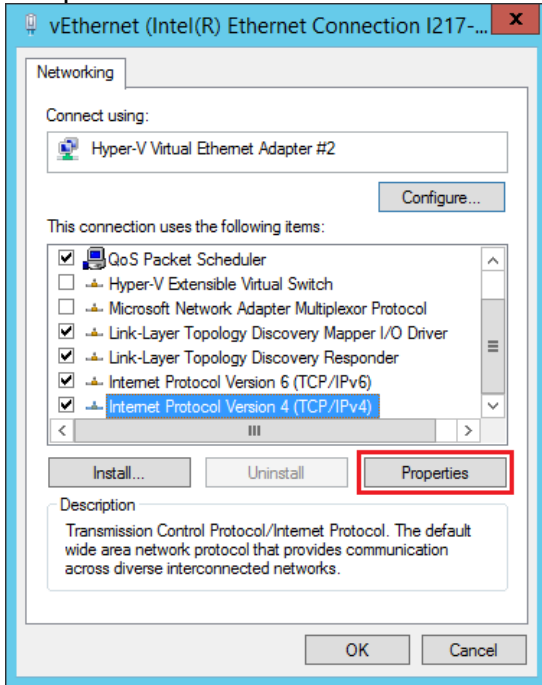
Change advanced sharing settings

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”.

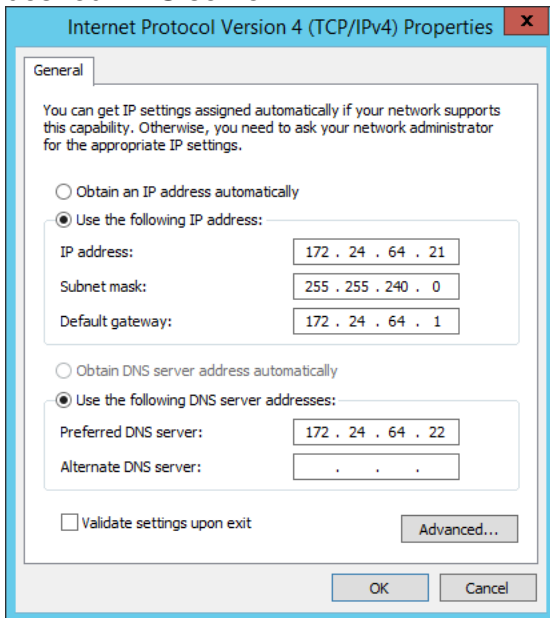




Scroll down to the bottom and select the “Internet Protocol Version 4 (TCP/IPv4) and select “Properties”.

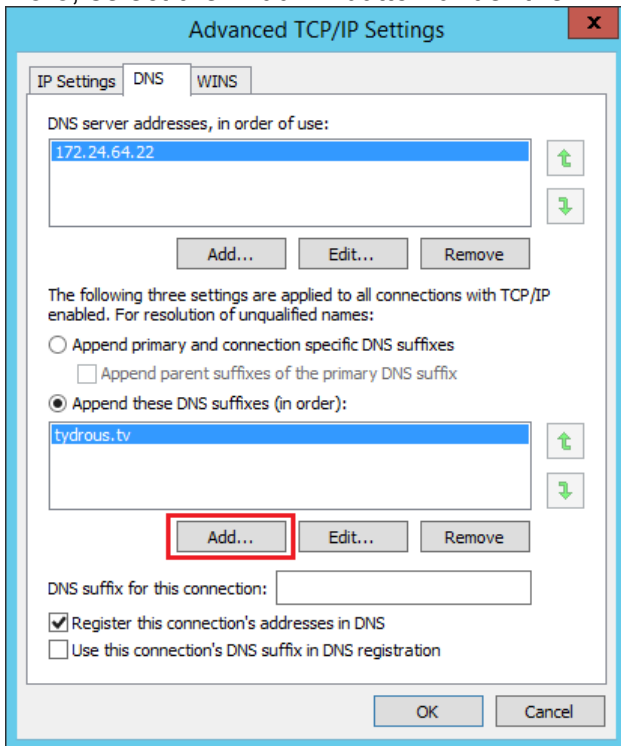


Select “Use the following IP address” and enter the IP address information of the device and the default gateway information. Then select “Use the following DNS server addresses” and enter the desired DNS server.

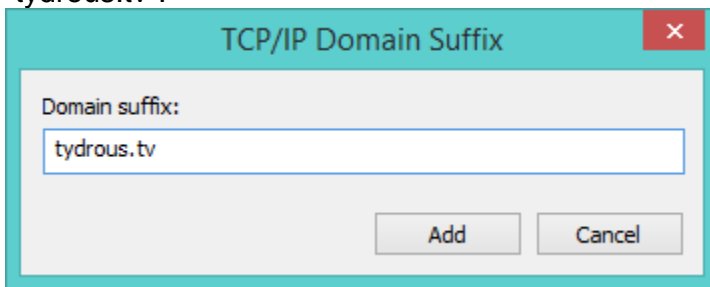


Now hit the “Advanced...” button to open the advanced IP configurations dialog. Then, select the DNS tab.

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.**

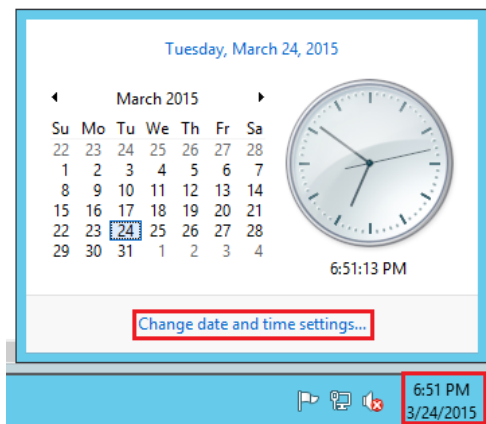
# Configuring Windows Server 2012 R2 to use NTP

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.

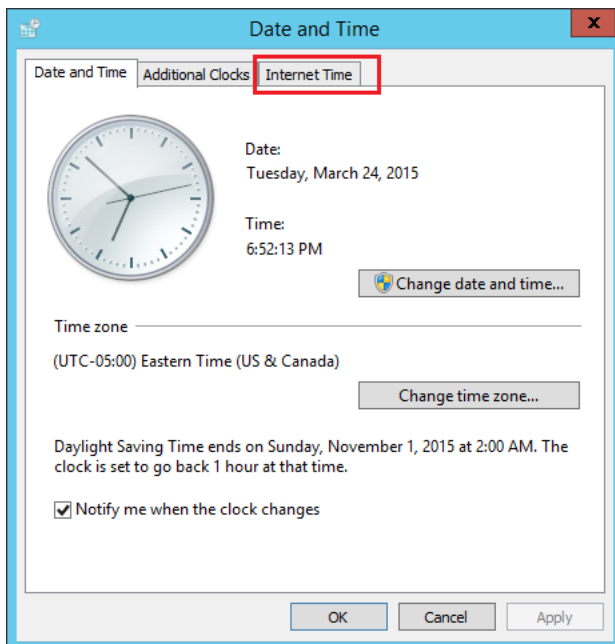
This tutorial will be using the domain name tydrous.tv. This procedure will work for any other domain name simply replace tydrous.tv with the different domain.

## Configuring NTP Clock

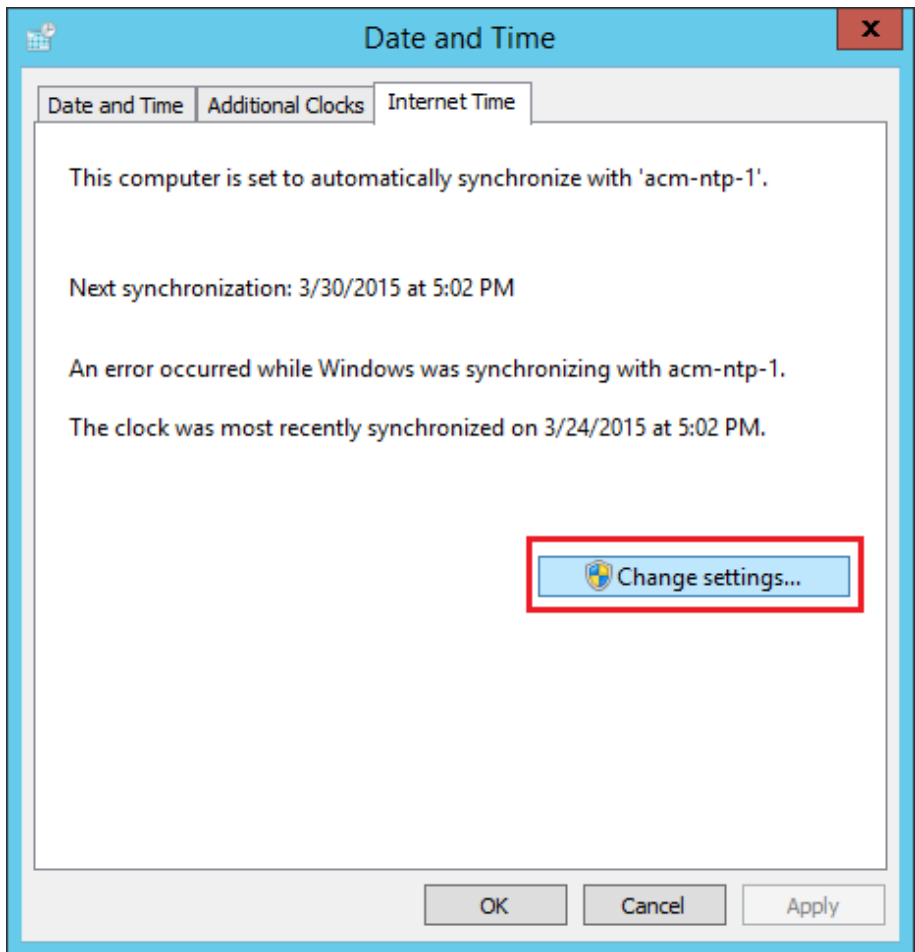
To configure Windows server 2012 to use NTP click on the clock in the bottom right of the screen. This will bring up the calendar window.



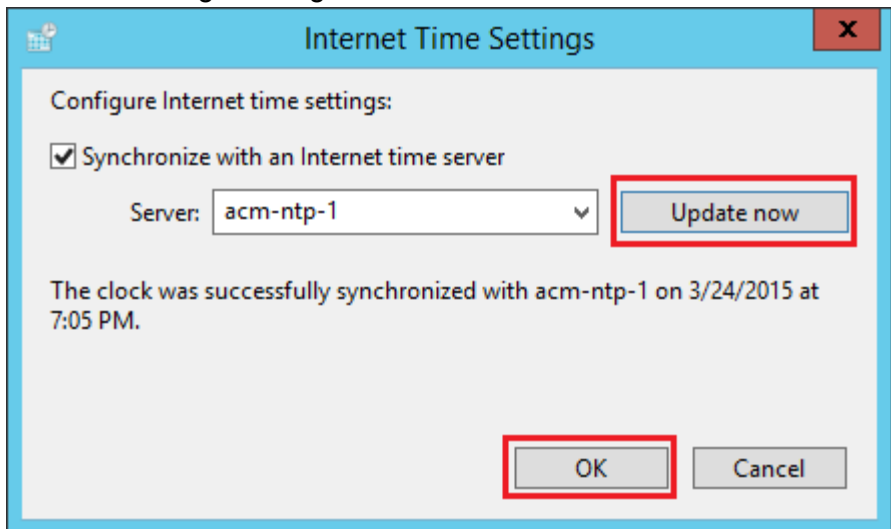
Once the Calendar is open click on the button “Change date and time settings”. This will bring up the windows to edit the Internet time.



Click on “Internet Time”.



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

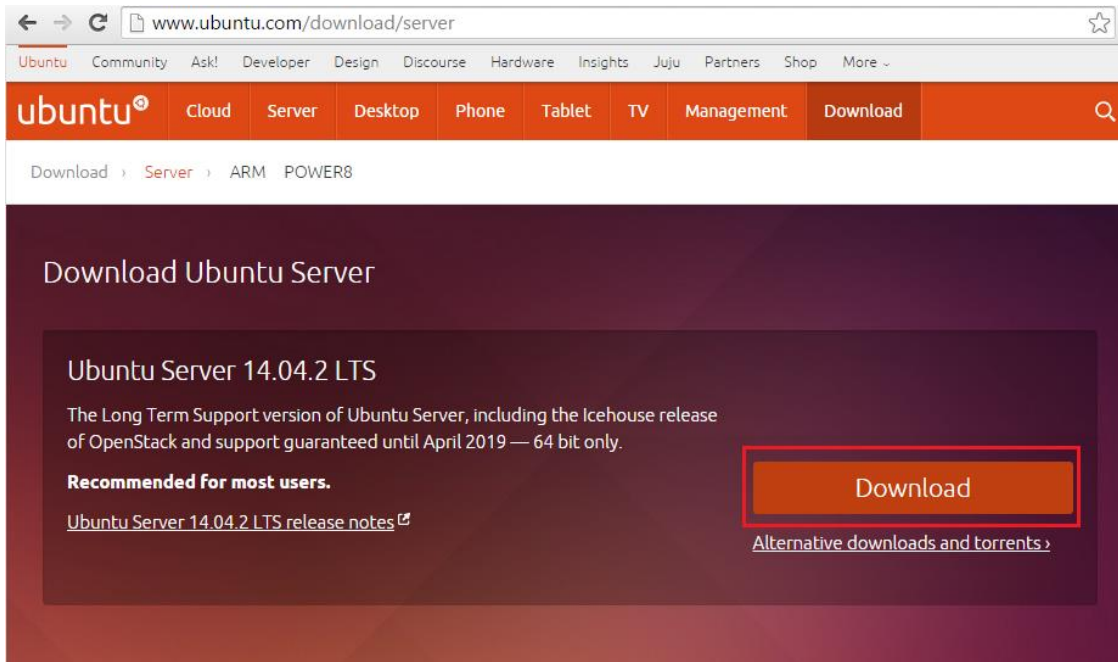
Installing Ubuntu Server 14.04	60
Changing an Ubuntu Server 14.04 Hostname	75
Configuring Ubuntu server 14.04 Ethernet interfaces	76
Configuring Login Banner Messages on Ubuntu Server 14.04	78
Configuring Ubuntu server 14.04 as a Syslog Client	80
Configuring Ubuntu server 14.04 As a SNMP Agent	81

# 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.



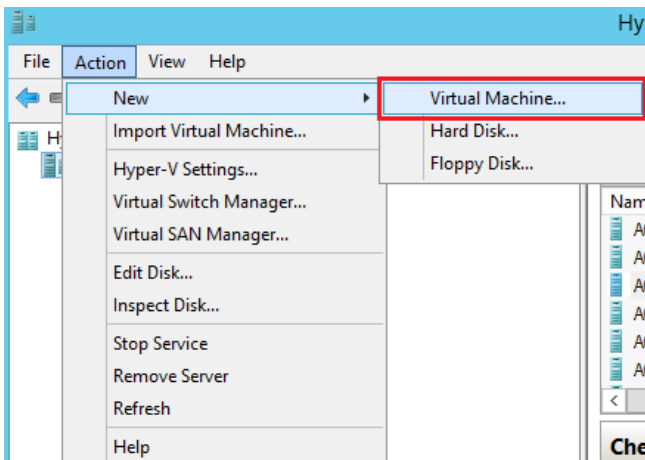
## Download Complete

## Creating a Virtual Machine:

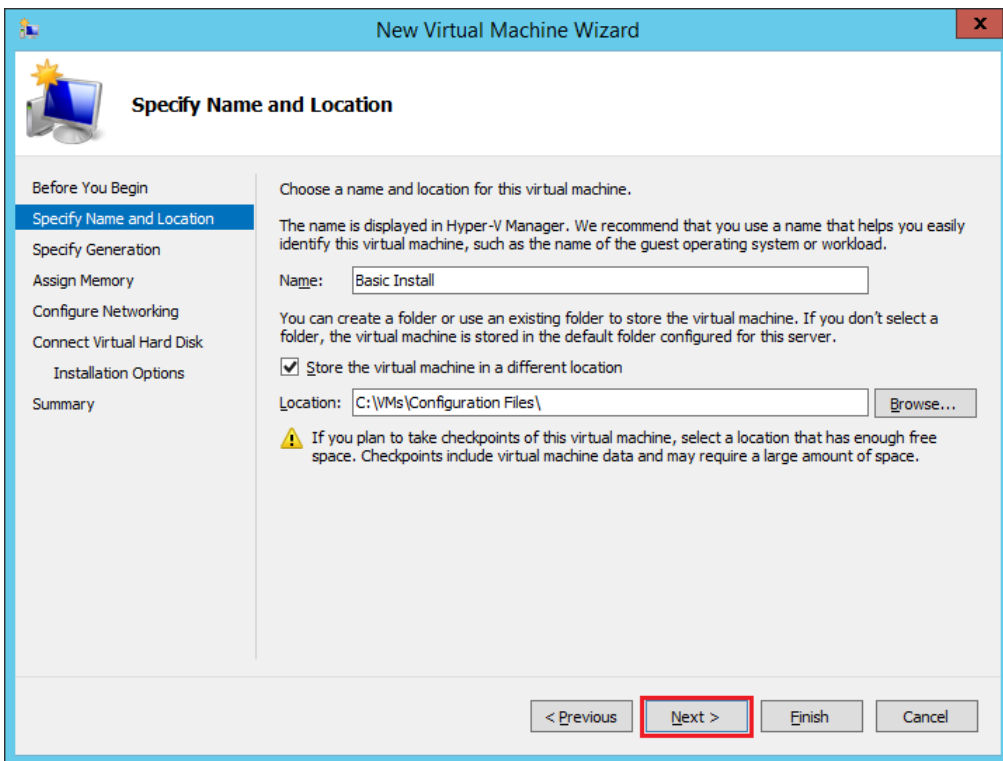
**If a virtual machine has already been created, it may be easier to simply import the already created template virtual machine rather than complete the remainder of the installation process.**

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

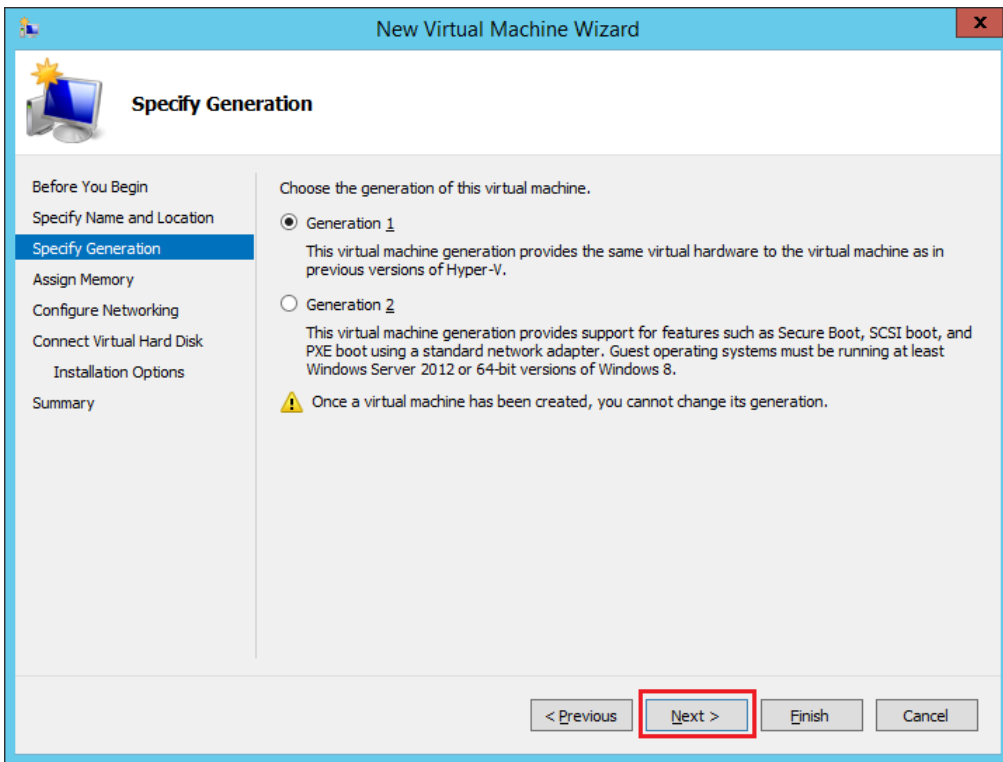
Start by opening the Hyper-V Manager. Once this is open select the “Action” drop down to “New” and the “Virtual Machine...”.



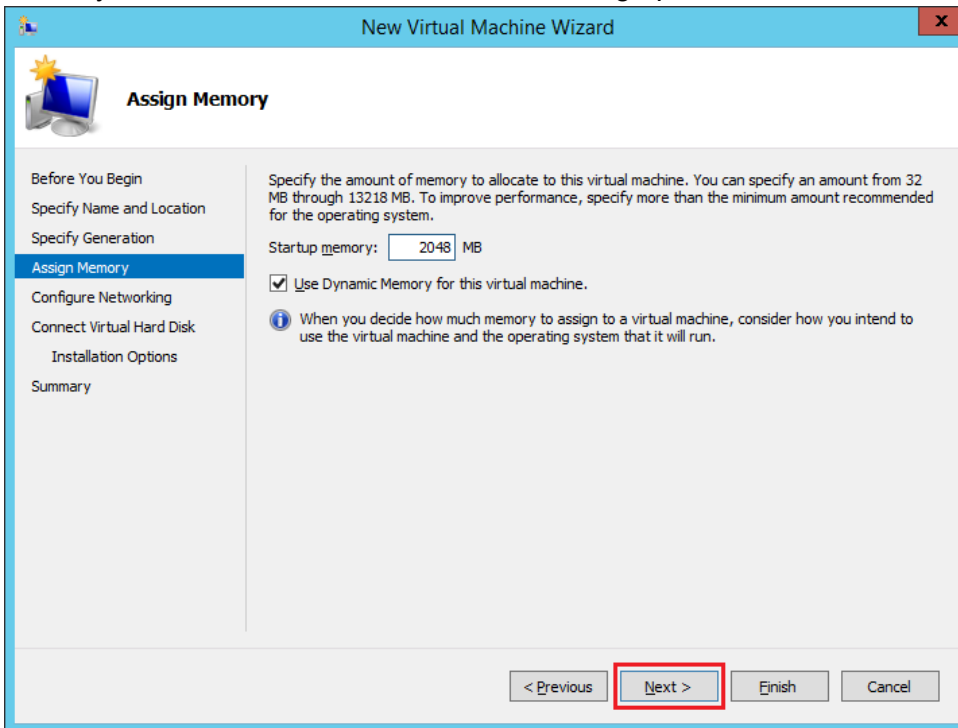
This will open a new window where the name of the Virtual Machine can be specified. There is also an option to save the virtual machine in a location other than the default. Once finished, click the “Next” button.



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.

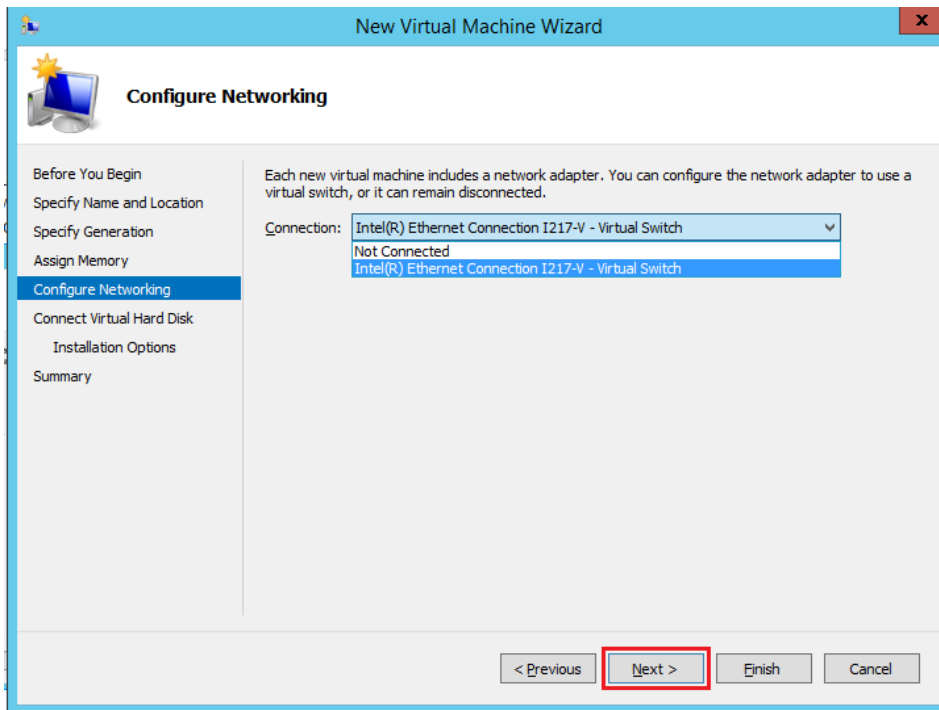


The next screen allows for the allocation of system memory to the VM. 2 Gigabytes of memory, or 2048 MB, should be sufficient for the basic Ubuntu server installation. This amount can be altered later. Check the “Use Dynamic Memory” option to allow Hyper-V to dynamically assign memory to the virtual machine as needed during operation. Click “Next” when finished.

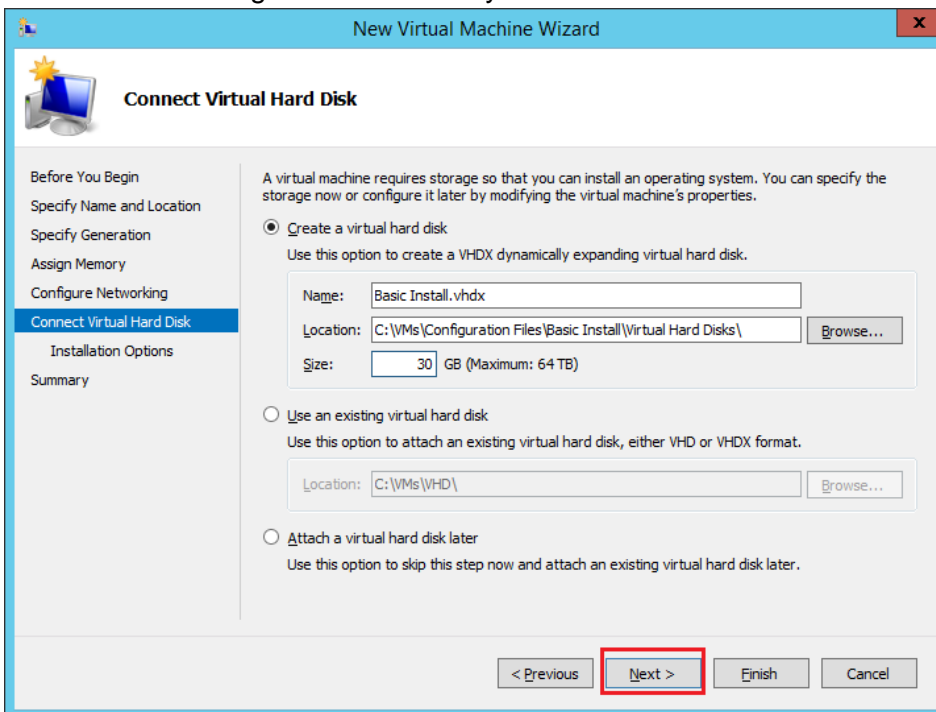




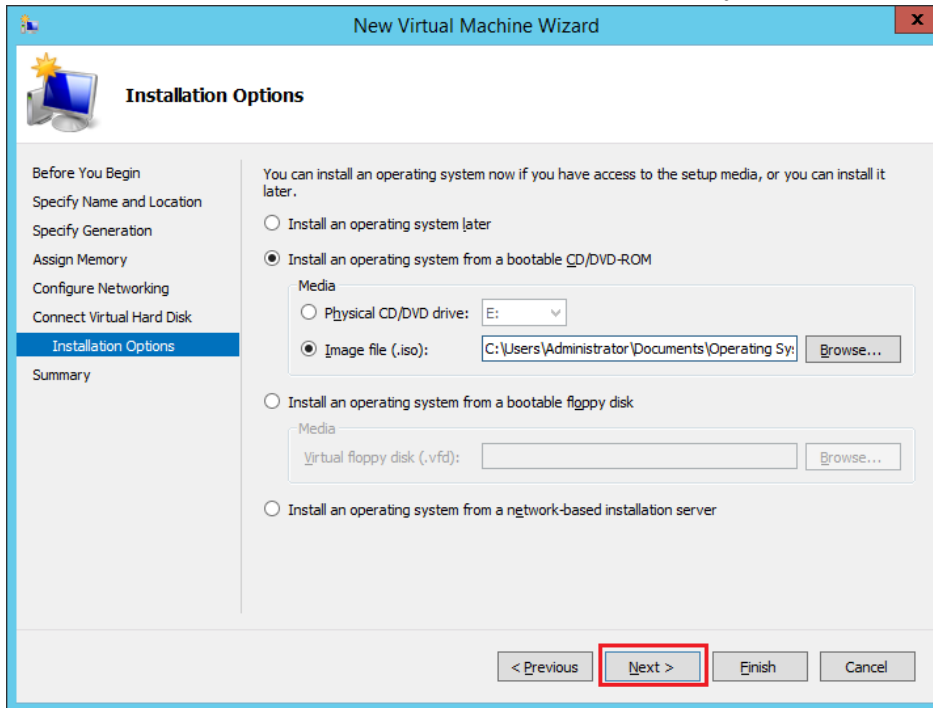
Next, the Ethernet interface needs to be assigned to the VM. When using multiple VMs' it is necessary for a virtual switch to be used. Select from the drop down. A new virtual switch may need to be created. Click "Next" when finished.



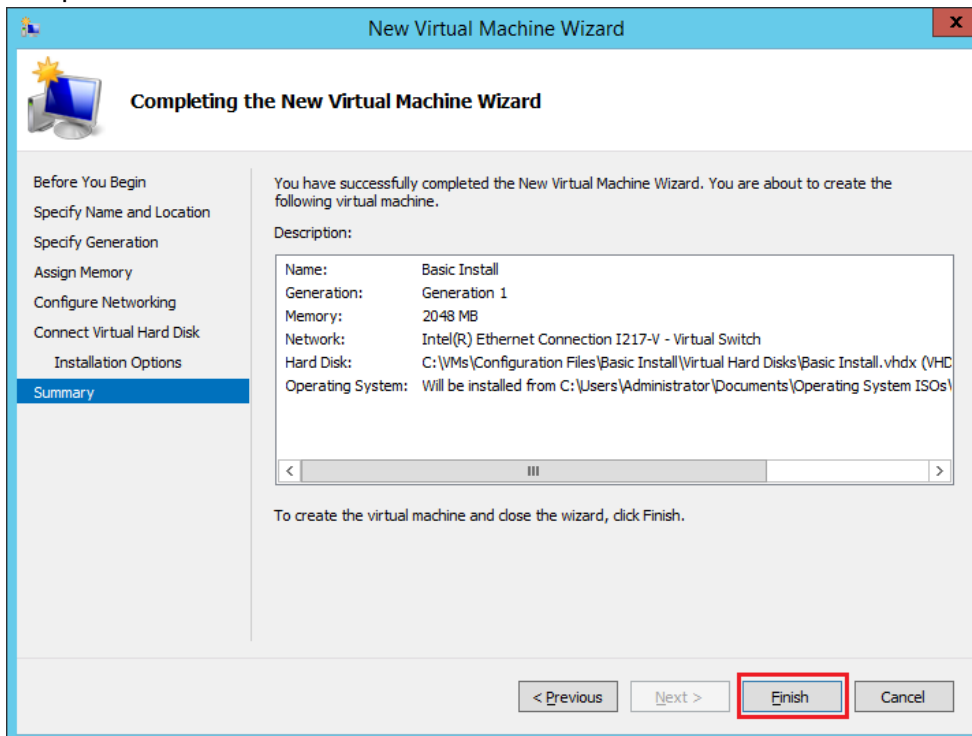
Next the virtual hard disk needs to be created. This is where the operation system will be installed. Do not forget to change the value of the virtual hard disk. This could create a virtual hard disk that is larger than necessary. A 30GB hard drive should be more than enough.



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.



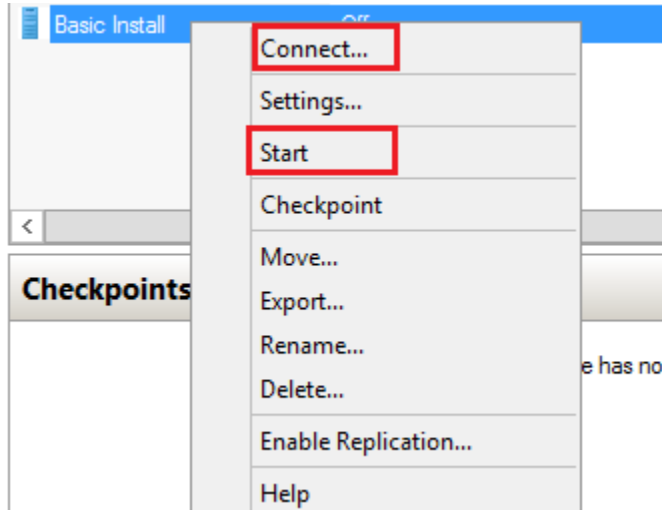
A summary of all the parameters configured in the process are displayed. Click “Finish” to complete the VM creation.



**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.

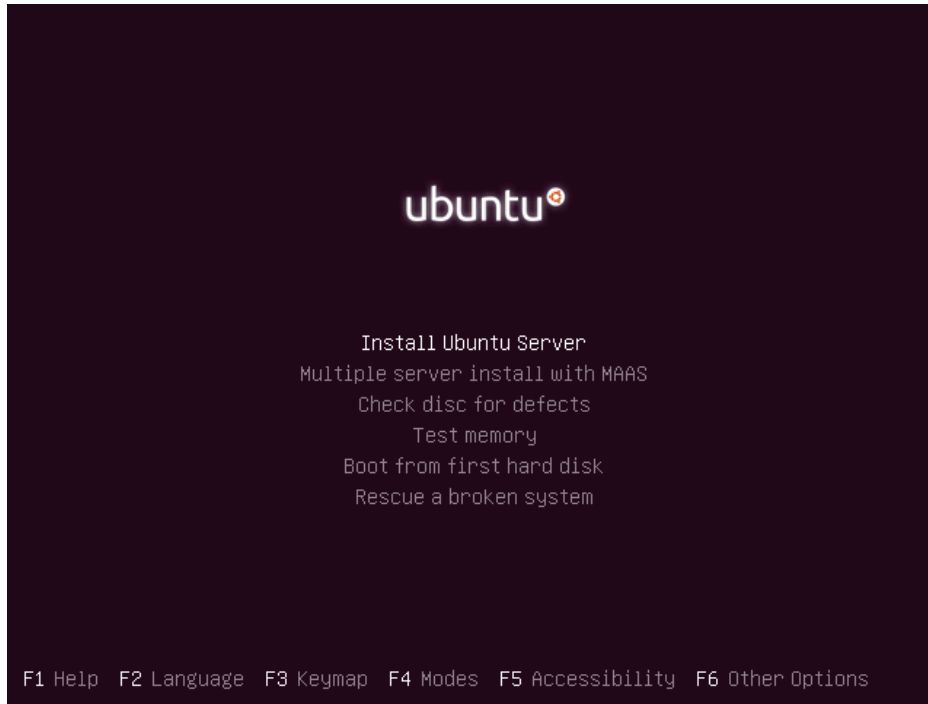


**From this point on, the installation process is the same as a dedicated server. The only difference is that when booting for a normal server, a flash drive or CD/DVD would be used as the boot media instead of an ISO file.**

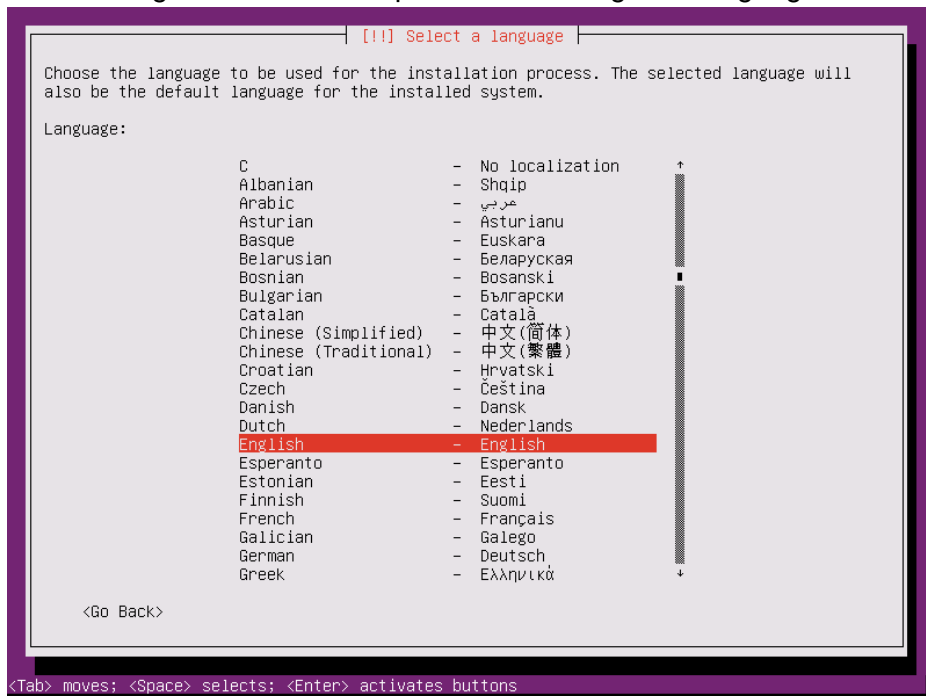
Once the server has finished booting, the installation process can begin. Select a language to continue.



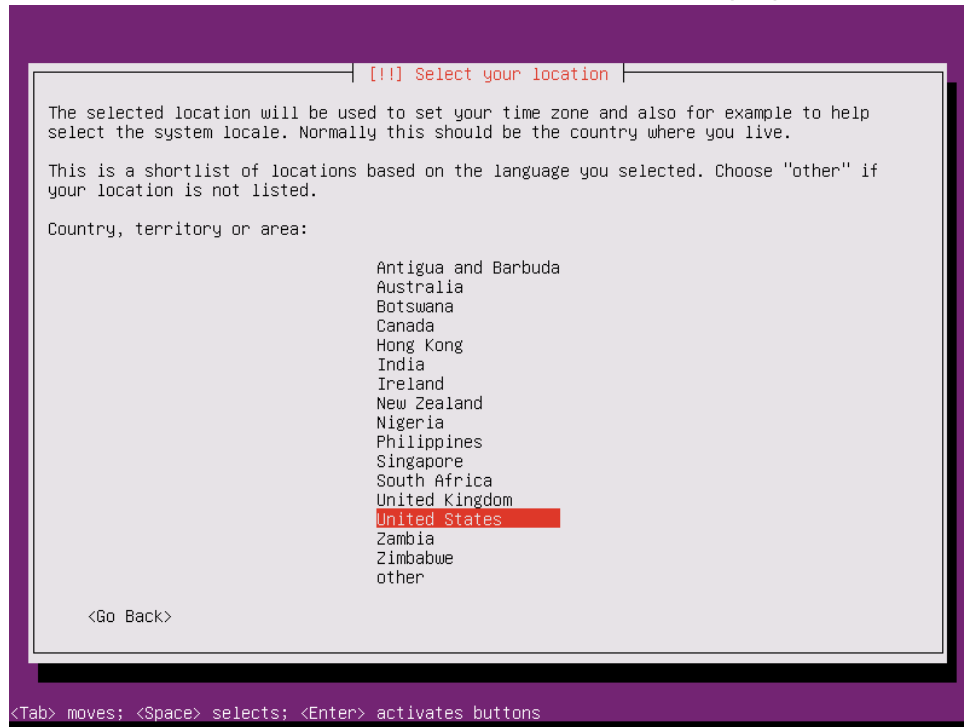
Once the Language is selected, the installation screen will be shown. Select “Install Ubuntu Server.”



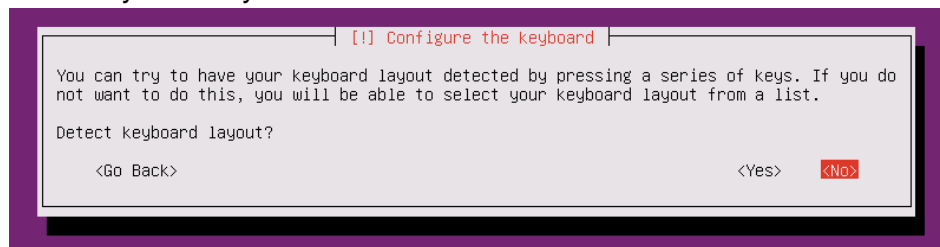
This will begin the installation process where again a language will need to be selected.



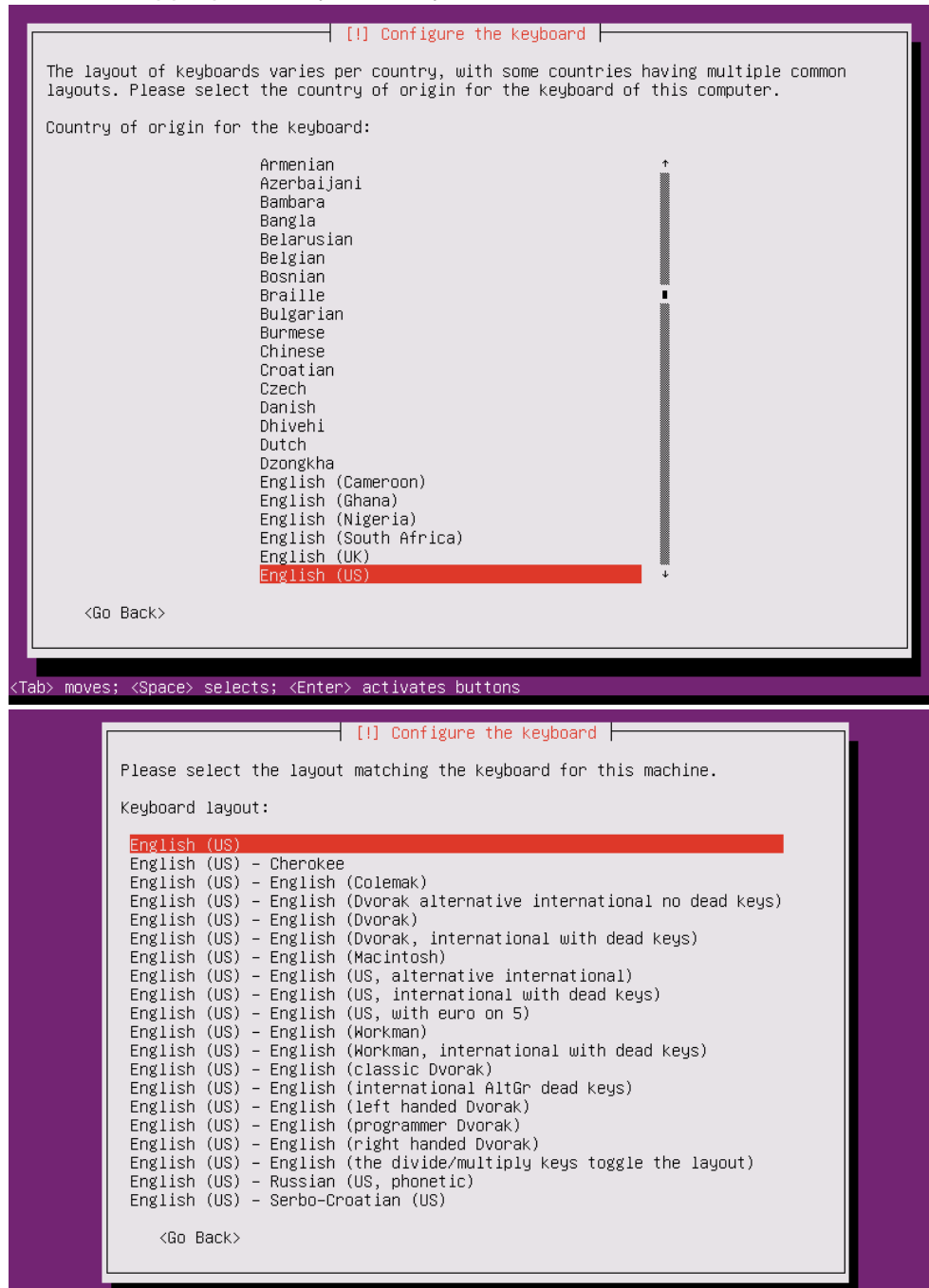
Set the location of the server. This will be used for time purposes.



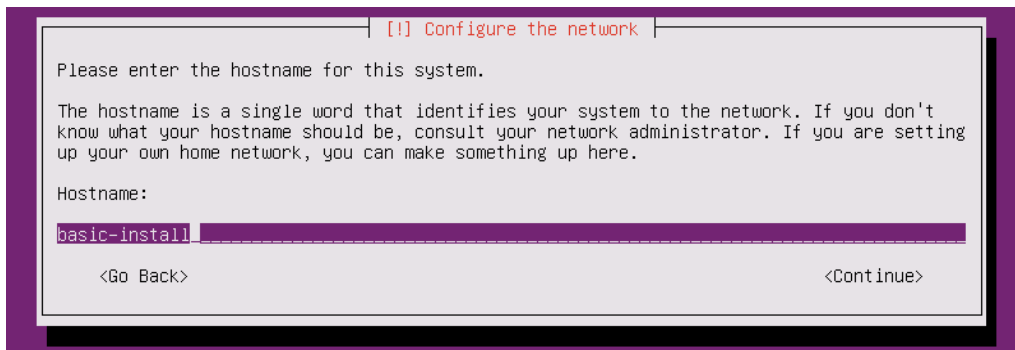
The keyboard layout will need to be determined. Select "No" for the detect configuration of the keyboard layout.



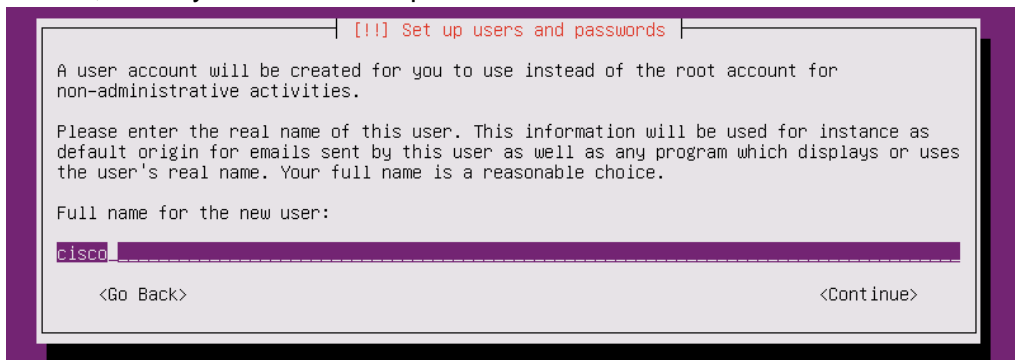
Select the appropriate keyboard layout.



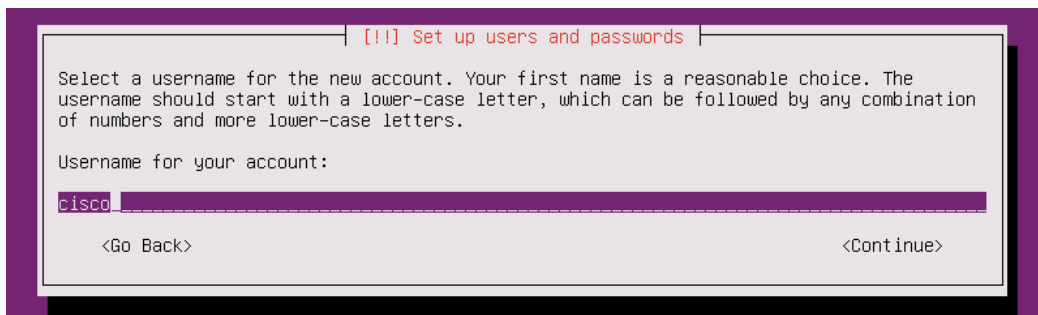
Ubuntu will begin the process of loading all of the necessary files for the installation process. After this process is complete, the server will automatically detect an IP address using DHCP. Once this auto detection is complete, a hostname will need to be set for the installation of Ubuntu. Hit Tab and Enter to continue.



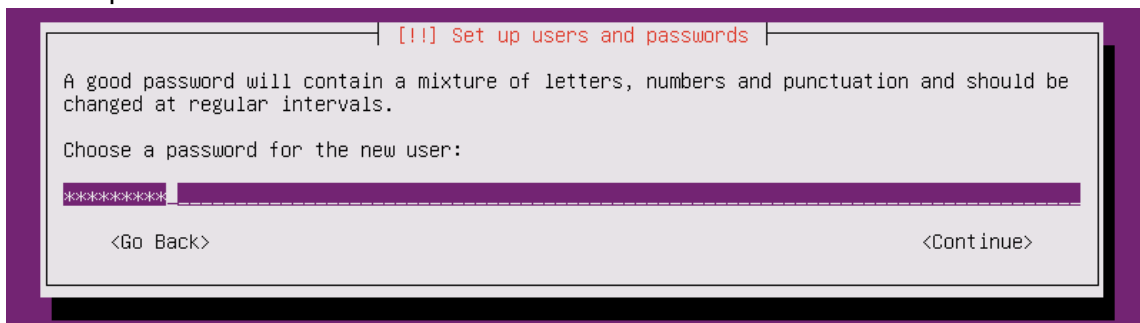
Now a basic user will need to be created. A generic username and password will be used in this tutorial, but any username and password can be used here. Hit Tab and Enter to continue.



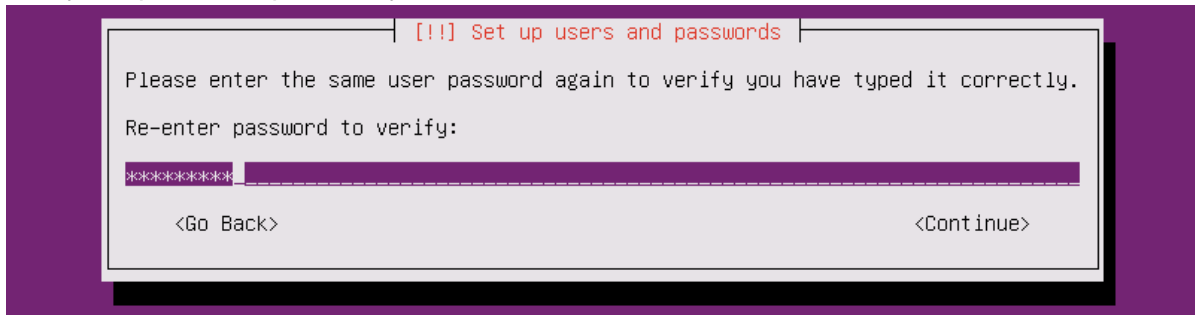
Enter a username. Hit Tab and Enter to continue.



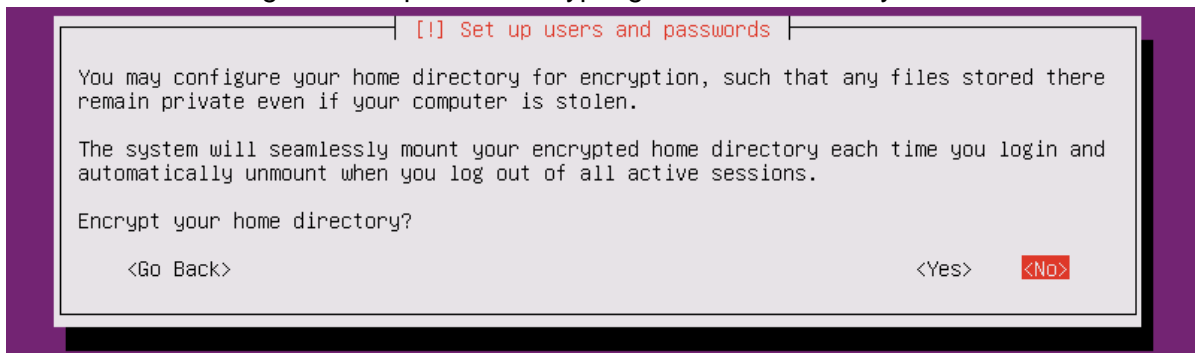
Enter a password. Hit Tab and Enter to continue.



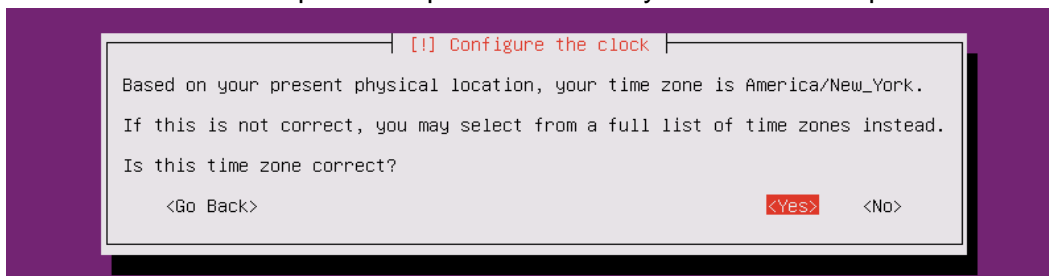
Verify the password previously entered. Hit Tab and Enter to continue.



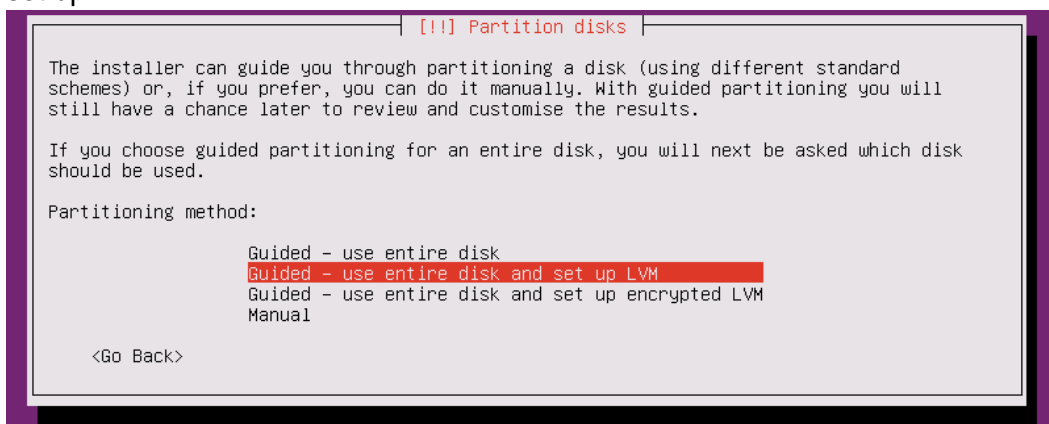
The Ubuntu Server gives the option of encrypting the home directory of this user.



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

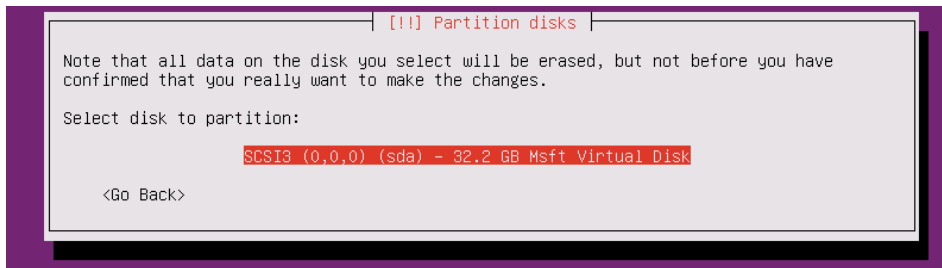


Begin partitioning the hard drive of the server. Select the option "Guided - use entire disk and set up LVM."

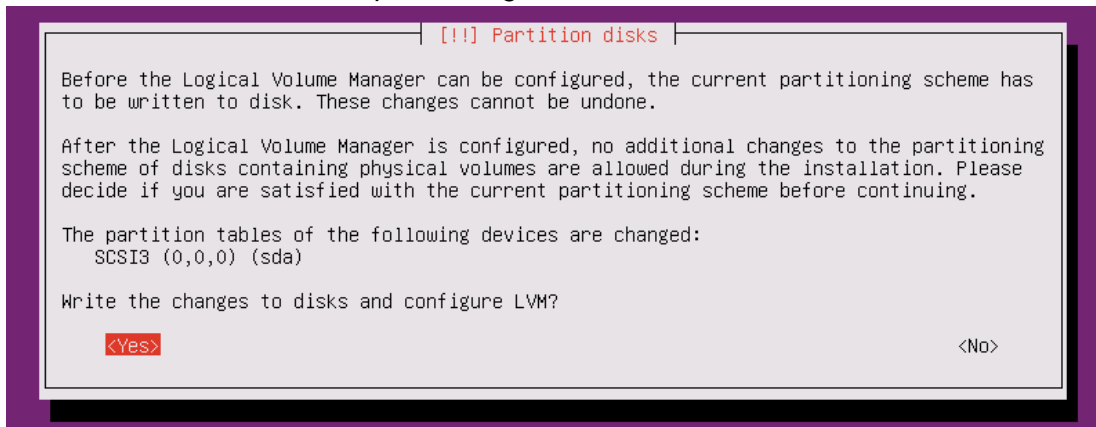




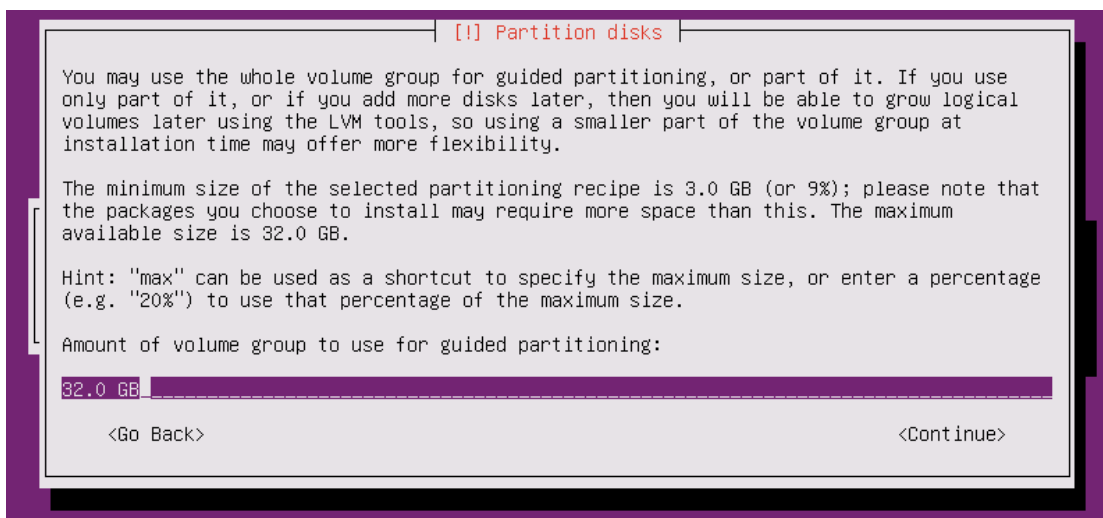
There may be a list of options if several hard drives are connected to the server. Select the desired to be the boot hard drive.



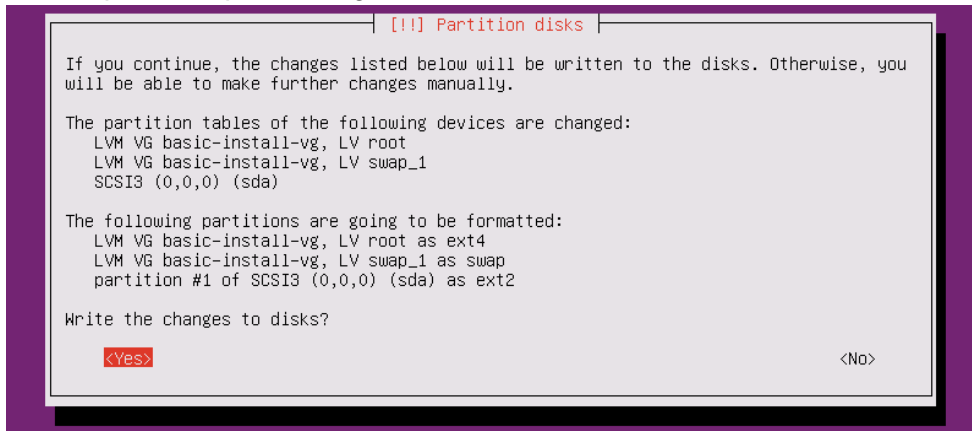
More advanced partition options are available, however this tutorial will not cover them. Select "Yes" to continue hard drive partitioning.



The default value is the full size of the disk. Hit Tab and Enter to continue.

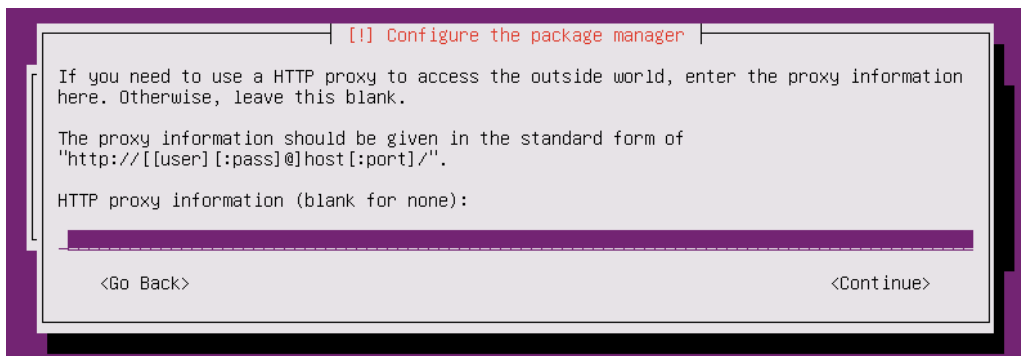


To complete the partitioning of the disk, hit “Yes”.

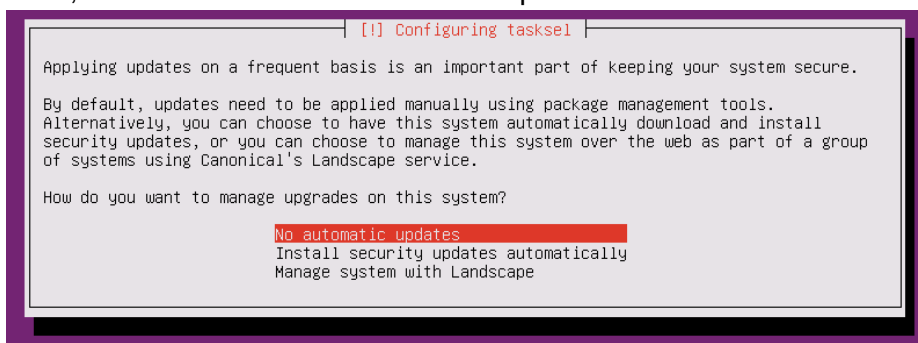


At this point, the installation process will begin working on writing information to the hard disk, which was just partitioned. This can take quite a while depending on the system.

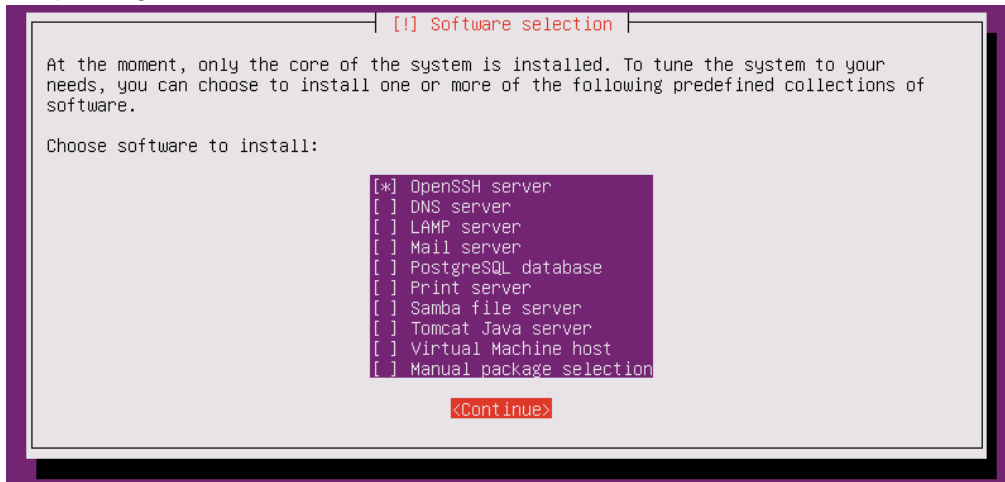
After this process has finished, a dialog box will appear asking about any proxy settings. This can be left blank. Hit Tab and Enter to continue.



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.

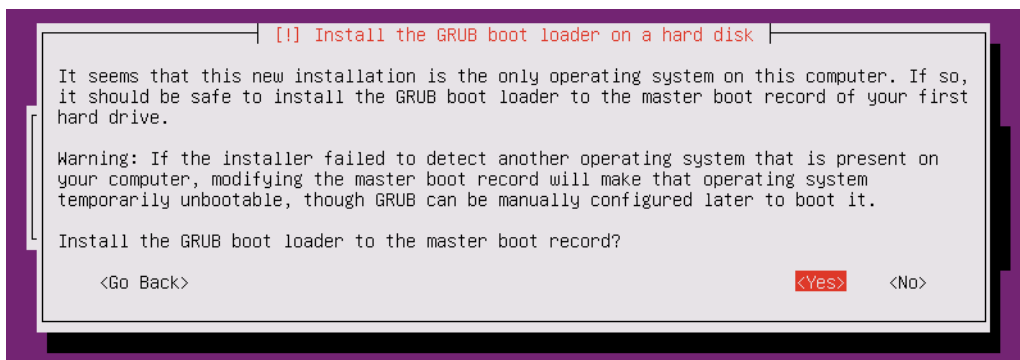


Here are some other optional packages that can be installed. Only the OpenSSH server will be selected in this tutorial. Installation of other protocols will be covered in other tutorials done post operating system installation. Use the arrow keys to move up and down and spacebar to select the packages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

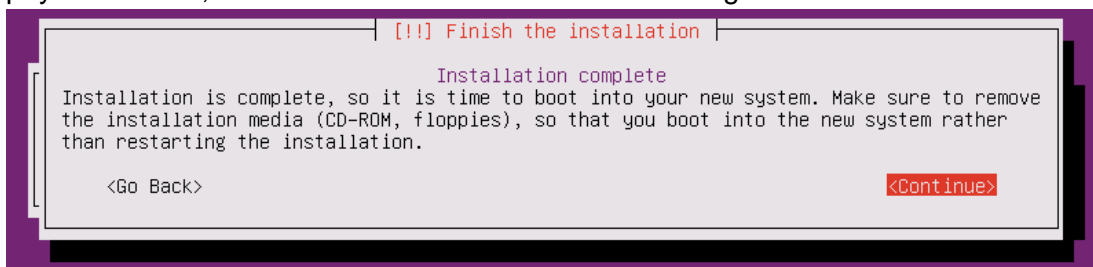


This package will now be downloaded and installed. This will take a while.

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.

```
Ubuntu 14.04.1 LTS basic-install tty1
basic-install login: _
```

**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
```

```
cisco@basic-install:~$ sudo vim /etc/hosts_
```

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

```
127.0.0.1    localhost
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
127.0.1.1    renamed-install.tydrous.tv_
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/networking/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
```

```
cisco@acm-dns-1:~$ sudo service ssh restart
ssh stop/waiting
ssh start/running, process 3772
```

**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
```

```
#####  
#### MODULES ####  
#####  
#External Syslog Server  
*.*@172.24.64.26  
  
$ModLoad imuxsock # provides support for local system logging  
$ModLoad imklog # provides kernel logging support  
#$ModLoad immark # provides --MARK-- message capability
```

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
```

```
cisco@acm-dns-1:~$ sudo service rsyslog restart  
rsyslog stop/waiting  
rsyslog start/running, process 4502
```

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
```

```
cisco@acm-syslog-1:~$ ls /var/log/remote-logs  
acm-dhcp-1.log          acm-rtr-2851.tydrous.tv.log  
acm-dns-1.log          acm-snmp-1.log  
acm-ftp-1.log          acm-sw-2960.tydrous.tv.log  
acm-ntp-1.log          acm-sw-3560.tydrous.tv.log  
acm-rtr-1841.tydrous.tv.log acm-syslog-1.log
```

**Configuration of rsyslog is complete.**

# Configuring Ubuntu server 14.04 as a SNMP Agent

These instructions are for installing SNMPD 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.

## 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
```

```
# snmpd options (use syslog, close stdin/out/err).
#SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -g snmp -I -smux,mteTrigger,mteTriggerConf -p /var/run/snmpd.pid'
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid -c /etc/snmp/snmpd.conf'
```

```
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -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.

```
acl "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:

```
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**

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

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

```
// 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; };  
};
```

```
//FORWARD LOOKUP ZONES  
zone "tydrous.tv"  
{  
    type master;  
    file "/etc/bind/zones/db.tydrous.tv";  
};  
  
//REVERSE LOOKUP ZONES  
//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
;
$TTL      604800
@         IN      SOA     localhost. root.localhost. (
                        2          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        604800 )   ; Negative Cache TTL
;
@         IN      NS     localhost.
@         IN      A      127.0.0.1
@         IN      AAAA   ::1
```



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.
@      SOA acm-dns-1.tydrous.tv. hostmaster.tydrous.tv. 1 172800 900 1209600
3600
      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
```

```
cisco@acm-dns-1:~$ 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

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

Non-authoritative answer:
Name:   google.com
Address: 74.125.141.113
Name:   google.com
Address: 74.125.141.102
Name:   google.com
Address: 74.125.141.101
Name:   google.com
Address: 74.125.141.100
Name:   google.com
Address: 74.125.141.138
Name:   google.com
Address: 74.125.141.139
```

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 dhcpd 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”**

```
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:**

```
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 255.255.224.0 {
    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;
}

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;
}
```

**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
cisco@ACM-DHCP-1:~$ sudo service isc-dhcp-server restart
isc-dhcp-server stop/waiting
isc-dhcp-server start/running, process 34739
```

**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 Tcpi. . . . . : 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  
sudo 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
```

The output should look similar to this:

```
cisco@ACM-DHCP-1:~$ cat /var/lib/dhcp/dhcpd.leases
# The format of this file is documented in the dhcpd.leases(5) manual page.
# This lease file was written by isc-dhcp-4.2.4

lease 172.20.32.21 {
  starts 3 2015/03/25 19:07:54;
  ends 3 2015/03/25 19:17:54;
  tstp 3 2015/03/25 19:17:54;
  cltt 3 2015/03/25 19:07:54;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet 08:2e:5f:81:25:33;
  uid "\001\010._\201%3";
  client-hostname "Nadleeh";
}
server-duid "\000\001\000\001\034m\260a\000\025j\001\360\000";
```

**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:

```
driftfile /var/lib/ntp/ntp.drift

statistics loopstats peerstats clockstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable

server 0.ubuntu.pool.ntp.org
server 1.ubuntu.pool.ntp.org
server 2.ubuntu.pool.ntp.org
server 3.ubuntu.pool.ntp.org

server ntp.ubuntu.com

restrict -4 default kod notrap nomodify nopeer noquery
restrict -6 default kod notrap nomodify nopeer noquery

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:

<http://www.pool.ntp.org/en/>

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:

```

driftfile /var/lib/ntp/ntp.drift

statistics loopstats peerstats clockstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable

server 0.us.pool.ntp.org
server 1.us.pool.ntp.org
server 2.us.pool.ntp.org
server 3.us.pool.ntp.org
server ntp.ubuntu.com

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

# Local users may interrogate the ntp server more closely.
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
restrict 127.0.0.1
restrict ::1

```

**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.

```
cisco@acm-ntp-1:~$ sudo ntpq -np
=====
remote                refid                st t when poll reach  delay  offset jitter
=====
70.35.113.43          216.228.192.69      2 u  51  64   1  77.023  -9.420  0.004
166.70.136.35         166.70.136.41       2 u  50  64   1  55.036  -4.386  0.004
129.250.35.250        207.250.21.22       2 u  50  64   1  29.979  -9.039  0.004
108.61.73.243         55.112.240.44       2 u  49  64   1  30.917   1.057  0.004
97.107.128.58         209.51.161.238      2 u  48  64   1  29.904   2.696  0.004
96.44.142.5           164.244.221.197     2 u  46  64   1  48.735  -6.296  0.004
208.53.158.34         204.2.134.163       3 u  46  64   1  17.860  -0.167  0.004
91.189.89.199         192.93.2.20         2 u  44  64   1 121.895   0.512  0.004
=====
```

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.

```
cisco@acm-ntp-1:~$ sudo ntpq -np
=====
remote                refid                st t when poll reach  delay  offset jitter
=====
+64.251.10.152        209.51.161.238      2 u  19  64  177  49.762  -1.443  6.206
+204.235.61.9         128.174.38.133      2 u  27  64  177  29.592   2.084  6.641
+108.61.194.85        132.163.4.101       2 u  22  64  177  67.870  -0.002  6.147
*97.107.131.6         209.51.161.238      2 u  23  64  177  33.935   4.504  7.663
+108.61.73.244        55.112.240.44       2 u  20  64  177  32.504   4.159  5.176
+66.79.136.240        216.218.254.202     2 u  22  64  177  72.858  -3.408  4.916
+69.41.163.31         139.78.135.14       2 u  17  64  177  49.908   6.046 11.125
-54.236.224.171      199.102.46.72       2 u  14  64  177  32.341   8.860  6.988
+91.189.94.4          131.188.3.220       2 u  17  64  177 105.948   0.818  7.751
=====
```

**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
```

```
cisco@acm-syslog-1:~$ sudo aptitude install ntp ntpdate
The following NEW packages will be installed:
  libopts25(a) ntp
The following packages will be upgraded:
  ntpdate
1 packages upgraded, 2 newly installed, 0 to remove and 100 not upgraded.
Need to get 528 kB of archives. After unpacking 1,676 kB will be used.
Do you want to continue? [Y/n/?] y
```

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.

# Use Ubuntu's ntp server as a fallback.
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 kod notrap nomodify nopeer noquery
restrict -6 default kod 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
```

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

**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:

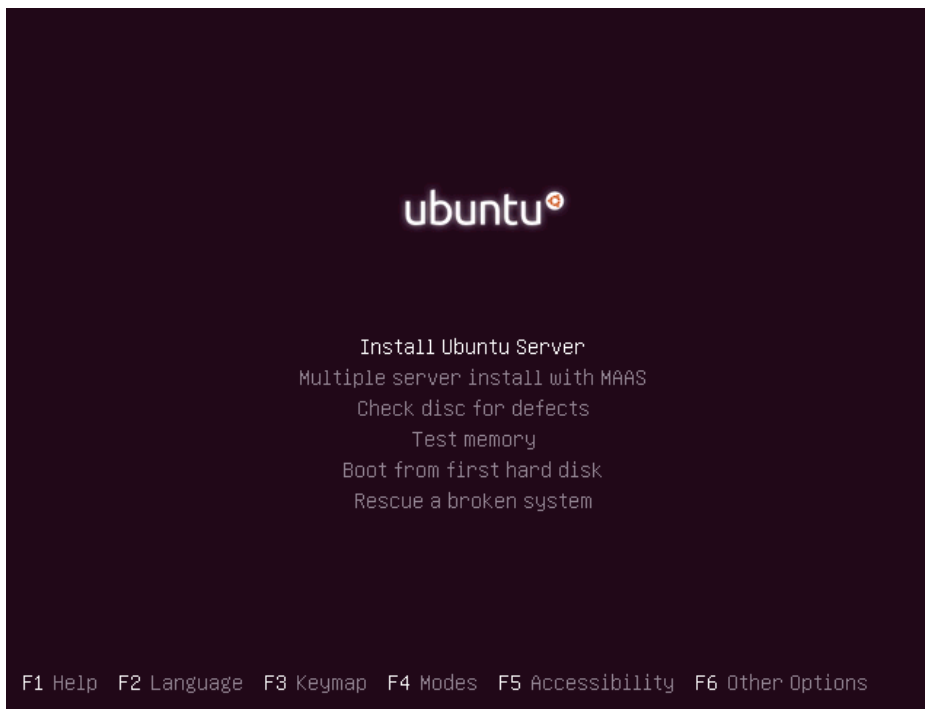
Refer to the instructions on how to install Ubuntu Server 14.04 for a clean installation.

Once the server has finished booting the installation process can begin. Select a language to continue.

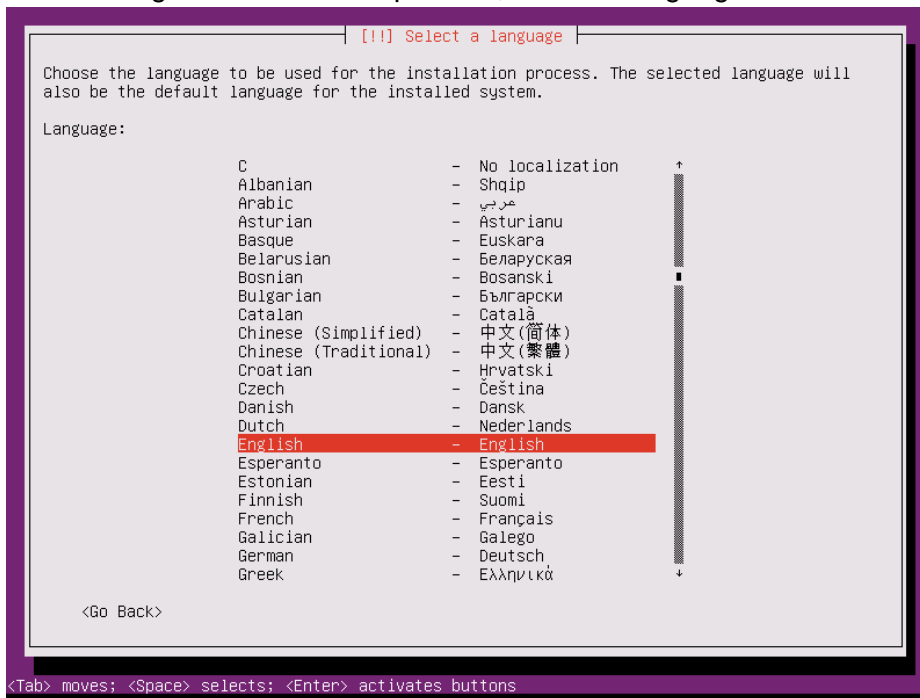


Once the Language is selected, the installation screen will be shown. Select “Install Ubuntu Server”.

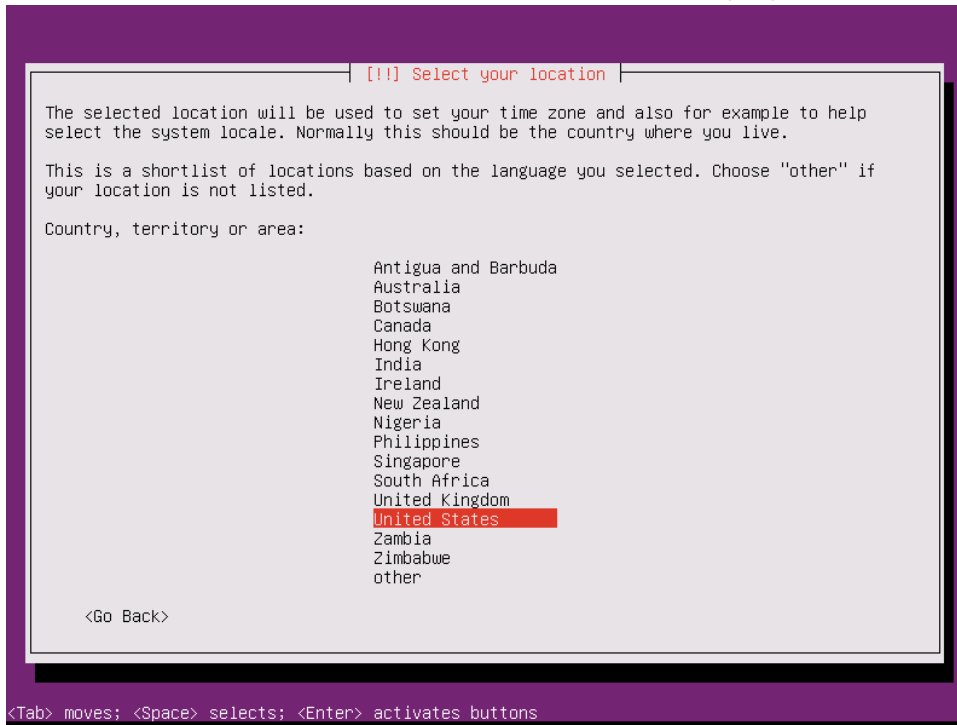




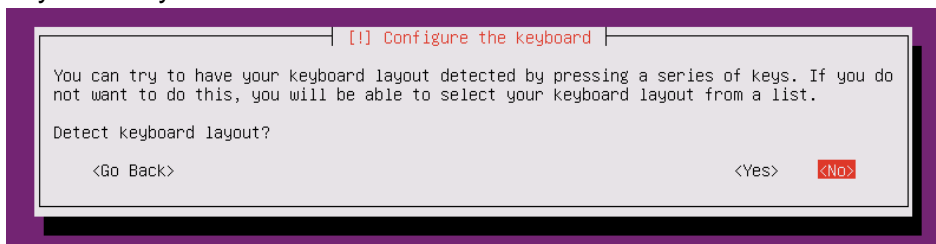
This will begin the installation process, where a language will need to be selected again.



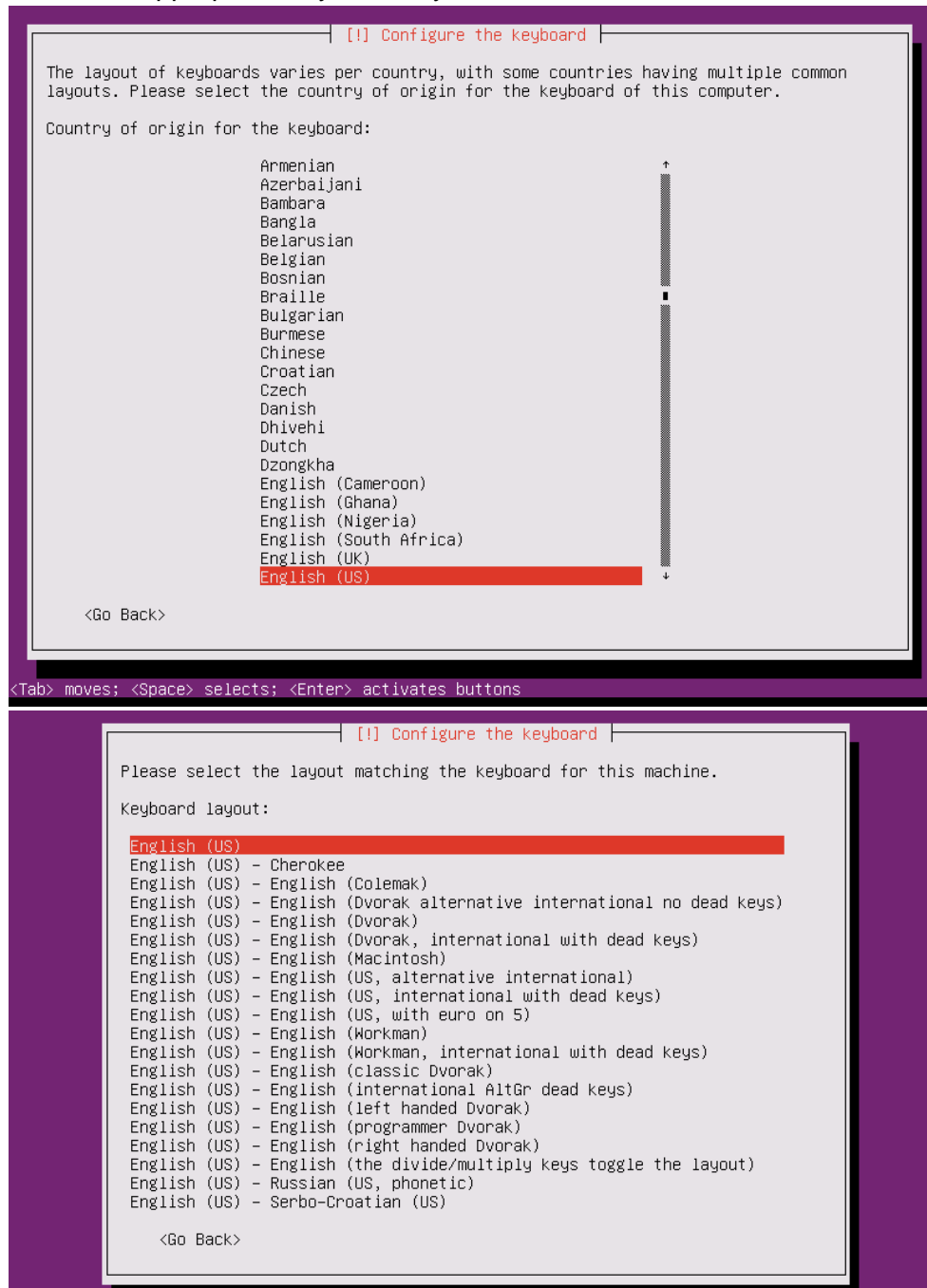
Set the location of the server. This will be used for time purposes.



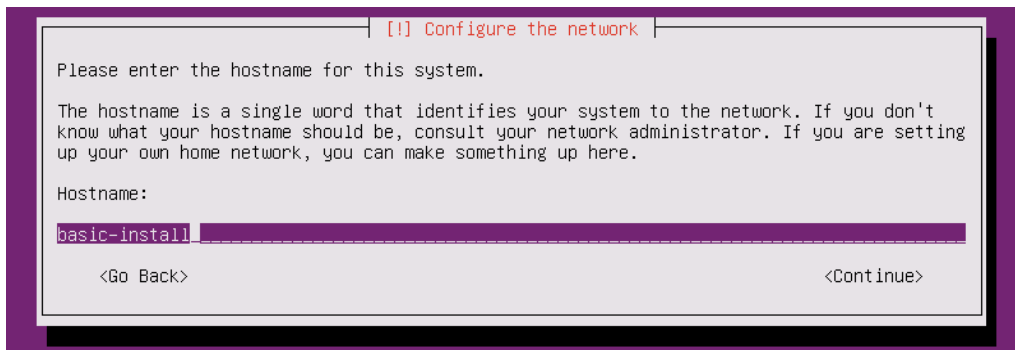
The keyboard layout will need to be determined. Select "No" for the detect configuration of the keyboard layout.



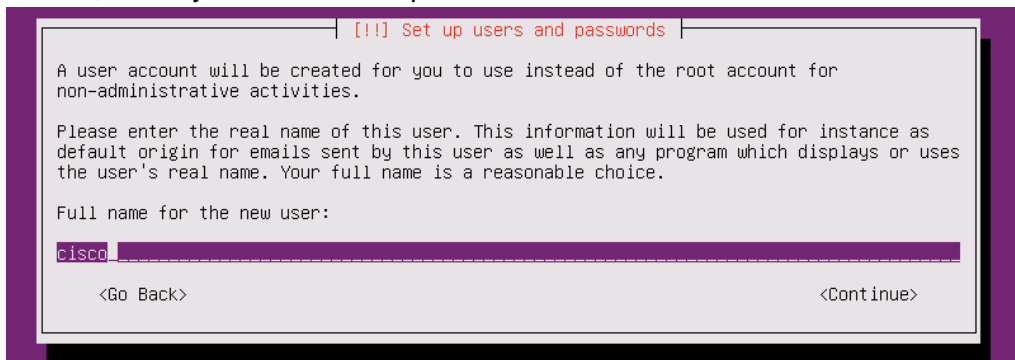
Select the appropriate keyboard layout.



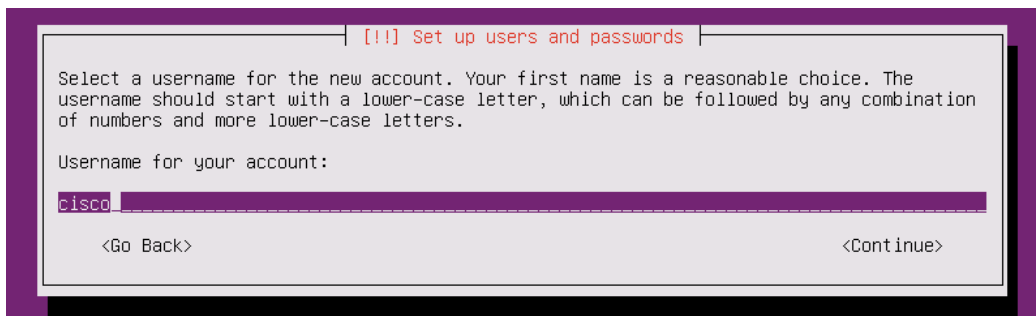
Ubuntu will begin the process of loading all of the necessary files for the installation process. After this process is complete, the server will automatically detect an IP address using DHCP. Once this auto detection is complete, a hostname will need to be set for the installation of Ubuntu. Hit Tab and Enter to continue.



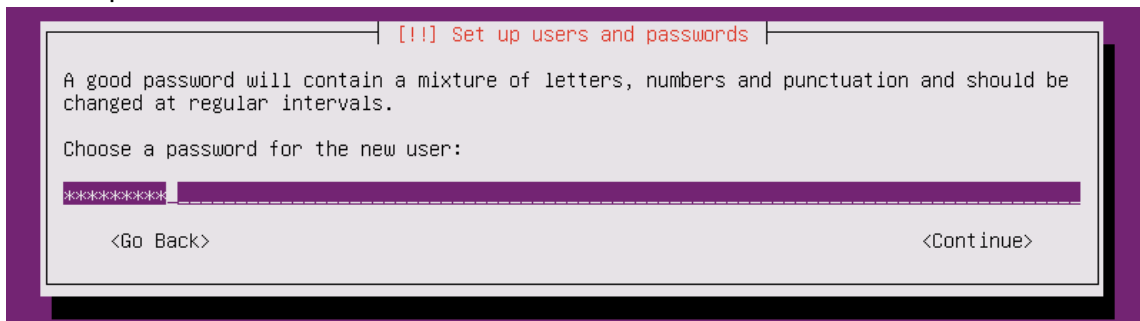
A basic user will need to be created. A generic username and password will be used in this tutorial, but any username and password can be used here. Hit Tab and Enter to continue.



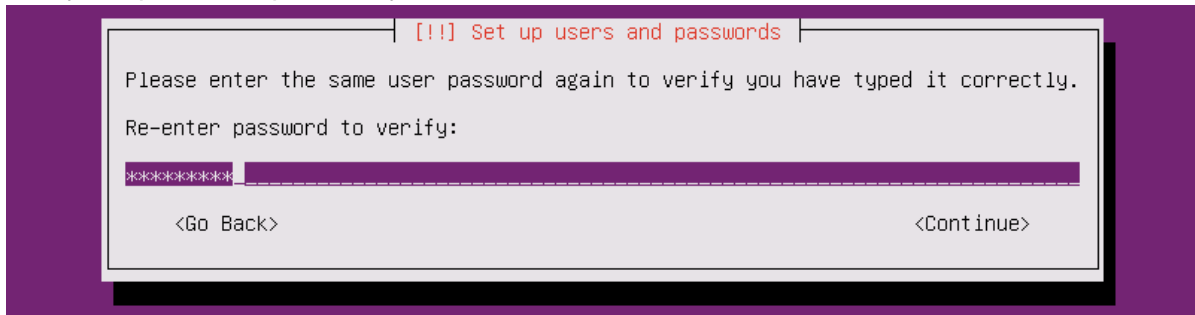
Enter a username. Hit Tab and Enter to continue.



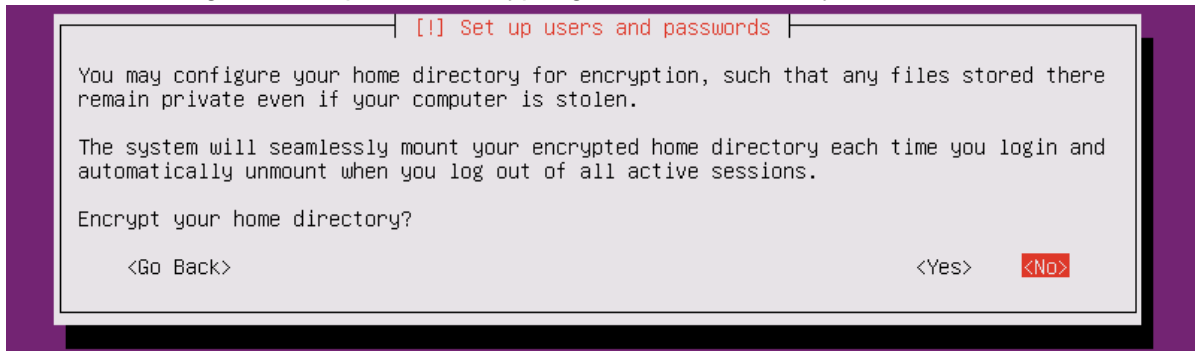
Enter a password. Hit Tab and Enter to continue.



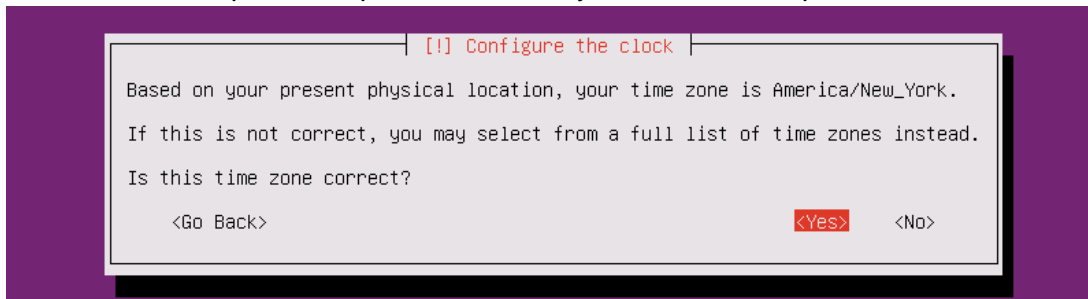
Verify the password previously entered. Hit Tab and Enter to continue.



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

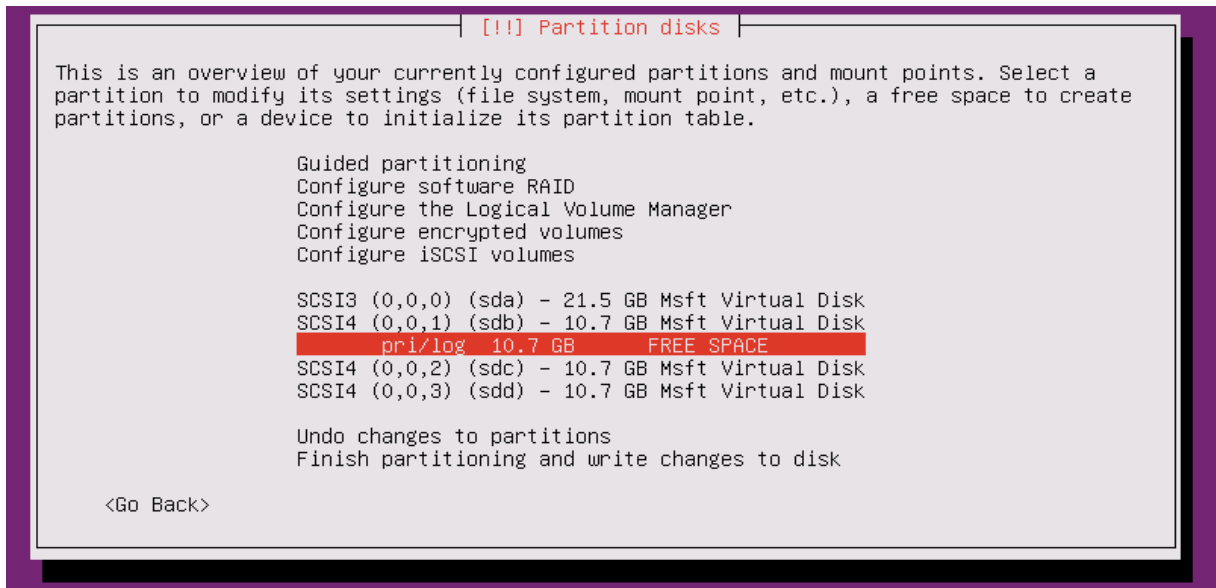


Ubuntu will attempt to set up the clock. Verify the information presented.

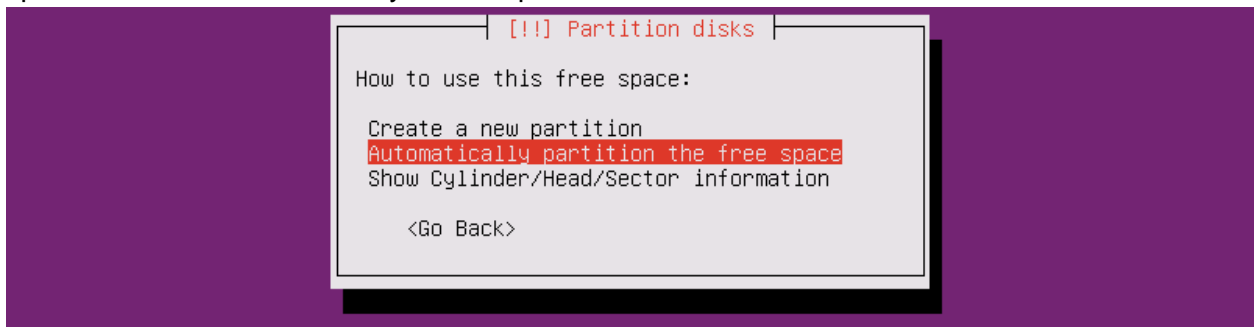




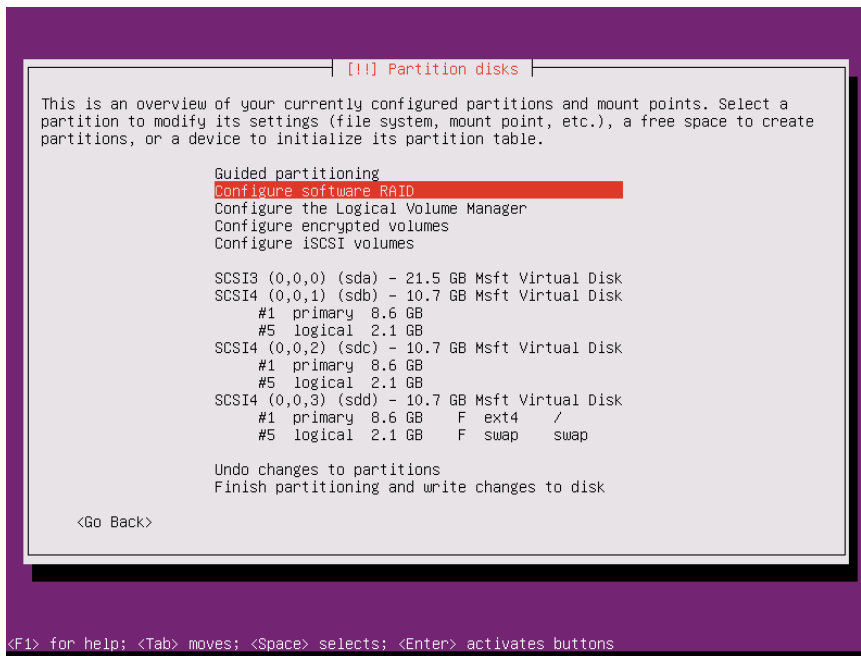
Drive space will need to be allocated to this partition. Select the “FREE SPACE” option and hit Enter to continue.



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.

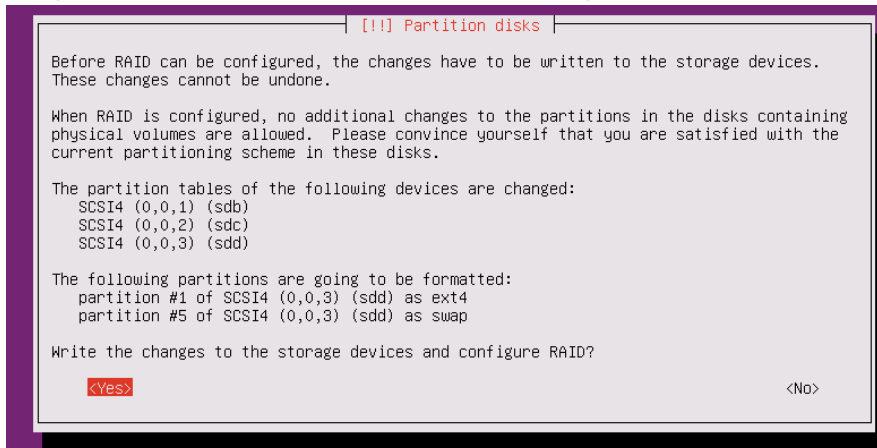


The new partition will be created. Complete this task for the remaining 2 hard drives. The finished result should look similar to this:

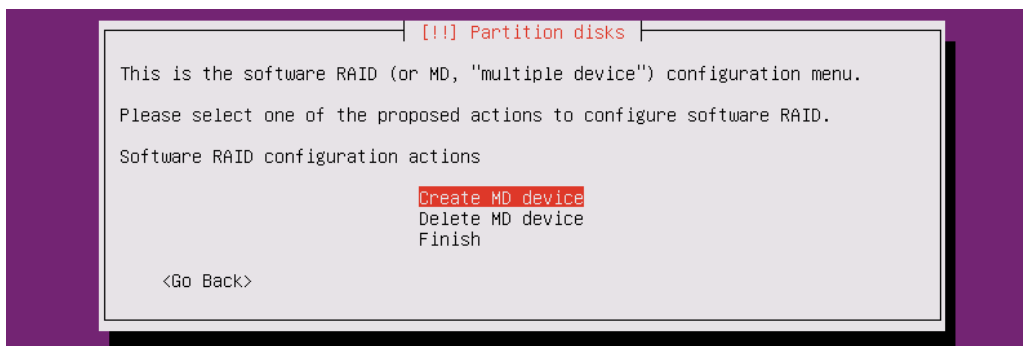


Create the software RAID. Select “Configure software RAID”.

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”.



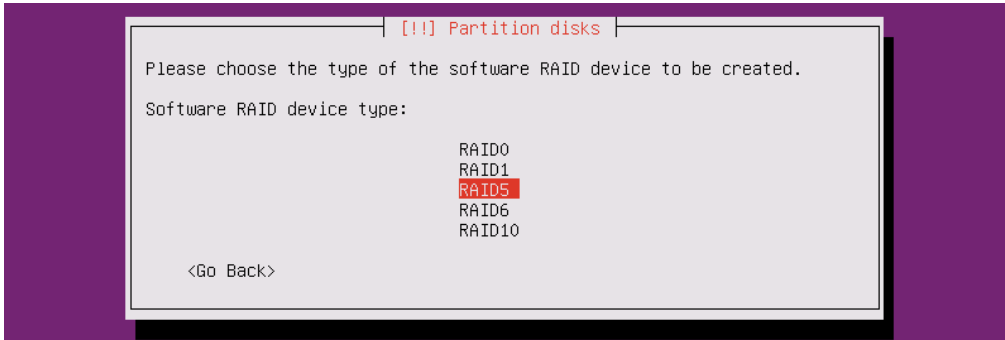


This tutorial will be setting up a RAID 5 configuration with 3 hard drives, which is the minimum required for this type of RAID. Drive requirements for other types of RAID are as follows: 2 hard drives are required for RAID 0 and 1, 3 for RAID 5, and RAID 6 and 10 both require 4 hard drives.

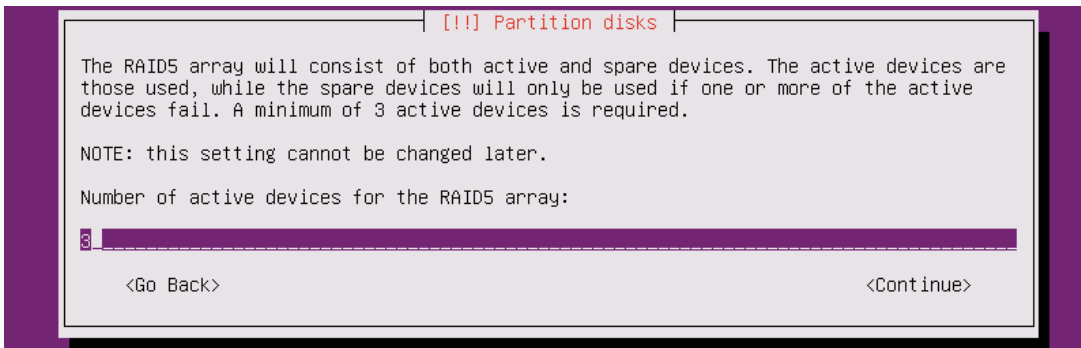
Here is a website to calculate the amount of storage space will be available for any type of raid configuration:

<https://www.icc-usa.com/raid-calculator/>

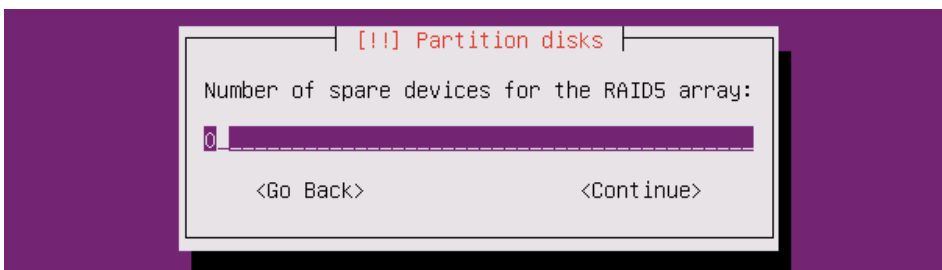
This RAID 5 configuration will result in 17.2GB of storage space.



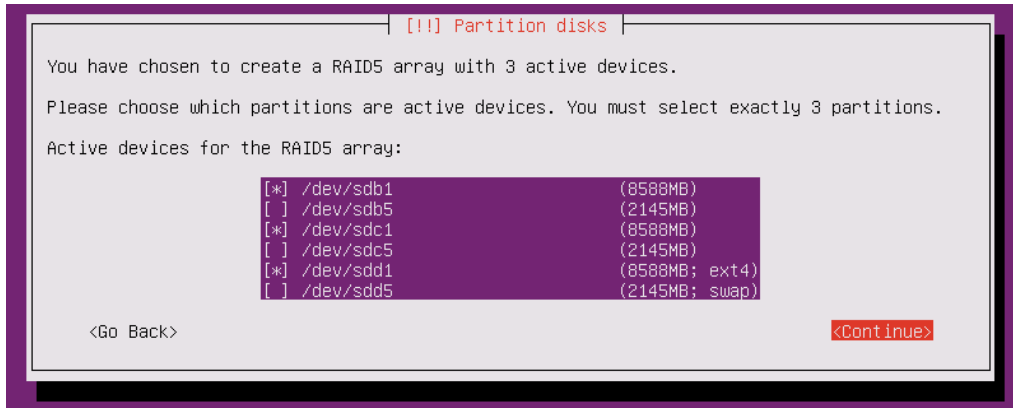
Enter the number of drives participating in the RAID Array, in this case 3. Hit Tab and Enter to continue.



Enter the number of spare drives in this array, which is 0 in this case. Hit Tab and Enter to continue.

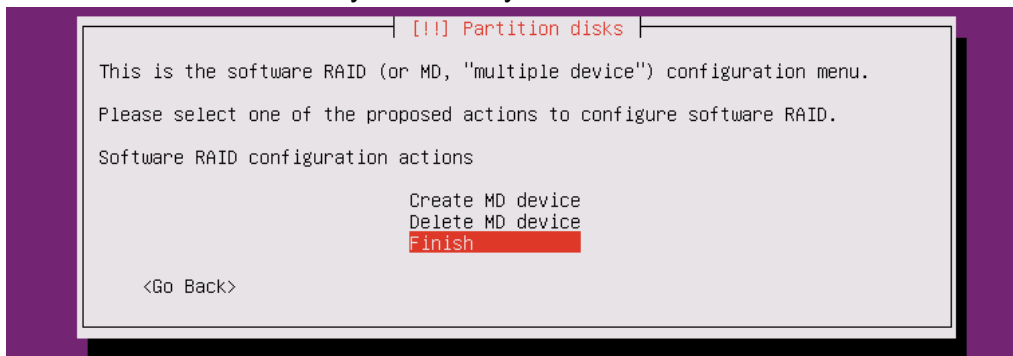


Here is where the drives that will participate in the RAID Array will be selected. Use the arrow keys to move up and down and spacebar to select the drive. In this case, the drives /dev/sdb1, /dev/sdc1, and /dev/sdd1 are the drives configured to participate in this array. The 5 version of these drives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

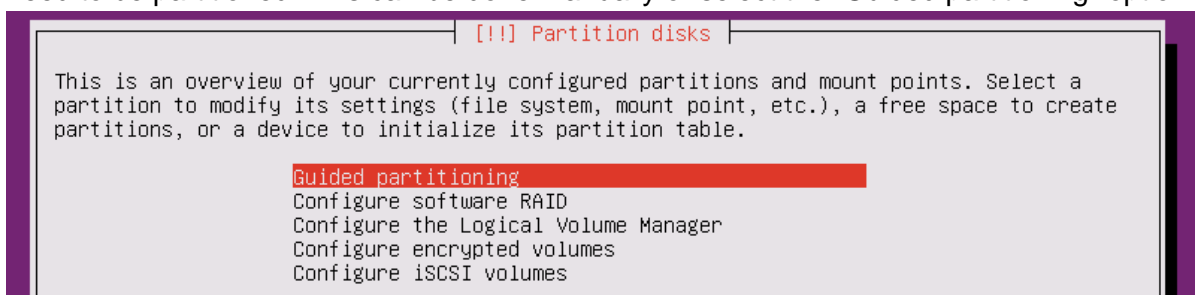


Again, a prompt will appear to confirm the partition changes to be written to this disk. Hit Yes to continue.

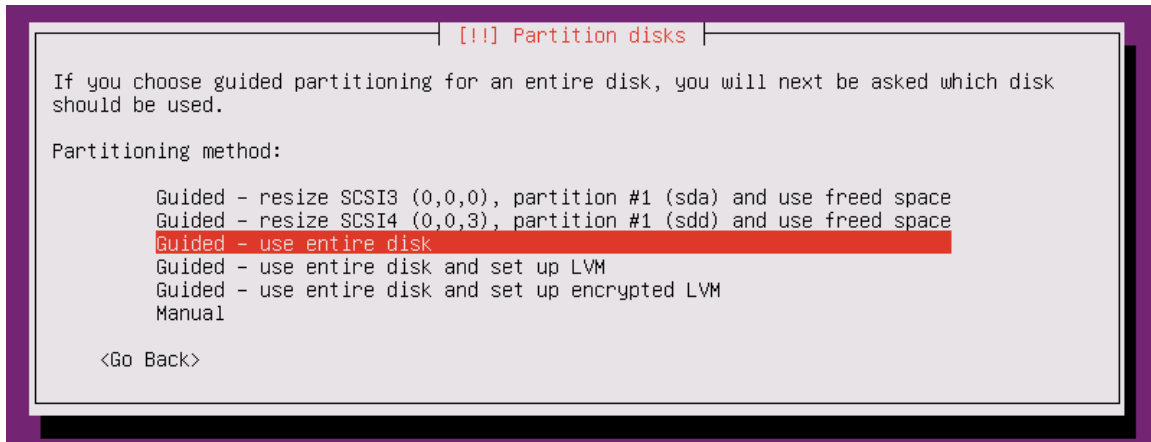
Hit "Finish" if this is the only RAID array to be created.



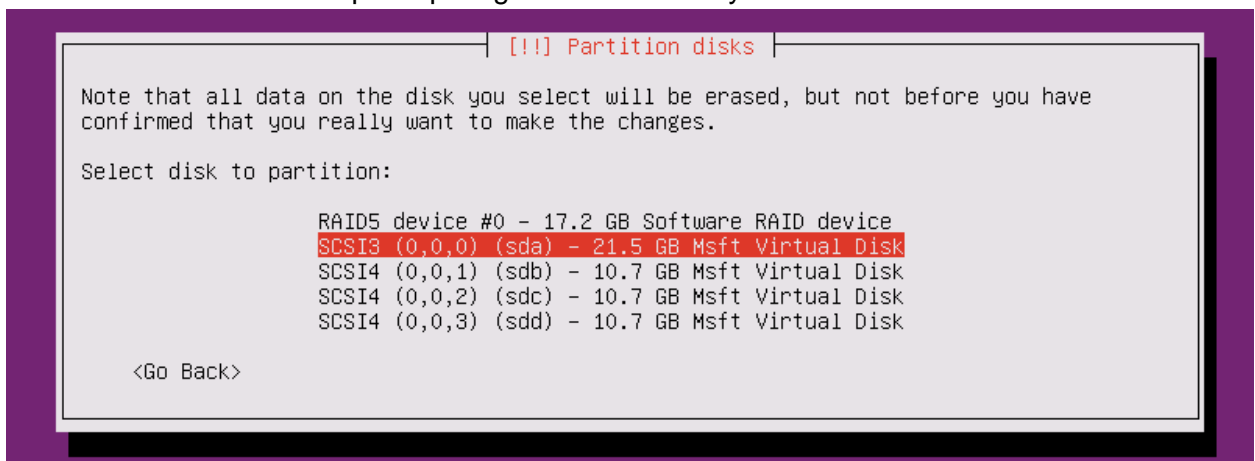
Now that the configuration of the RAID Array is finished, the operating system boot disk will need to be partitioned. This can be done manually or select the "Guided partitioning" option.



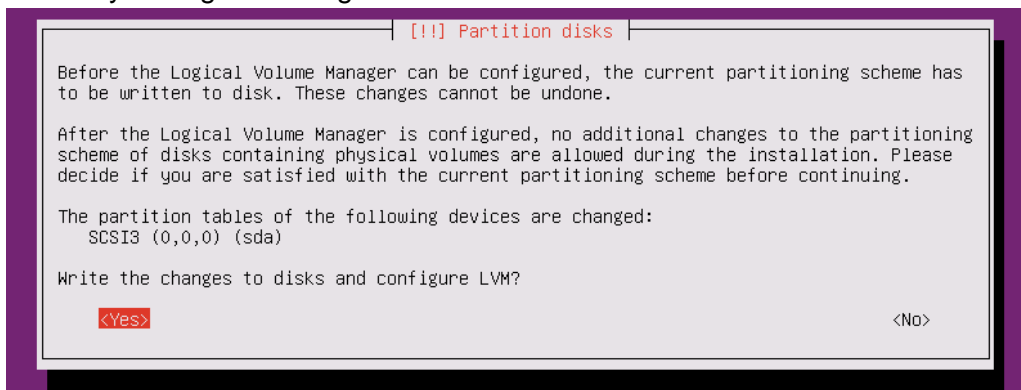
Select the "Guided - use entire disk" option.



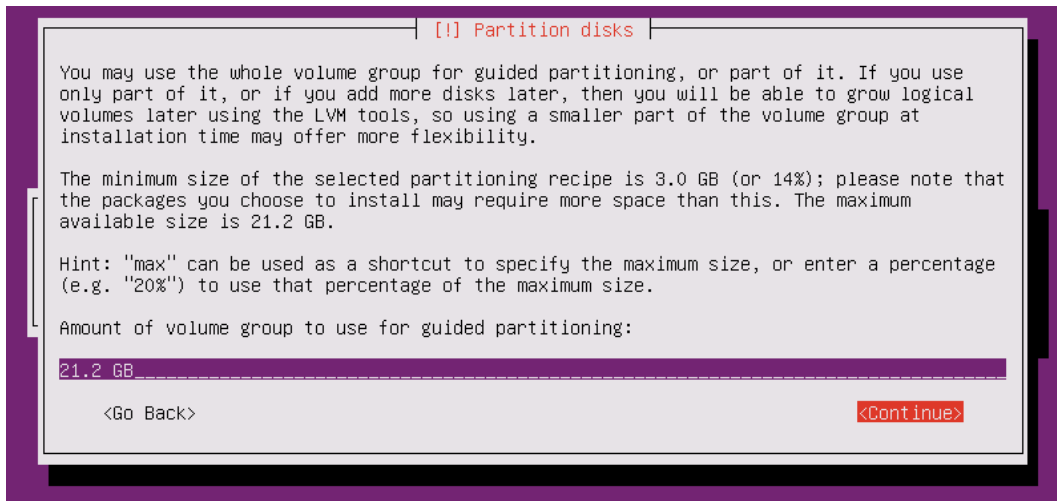
Select the drive that is not participating in the RAID array.



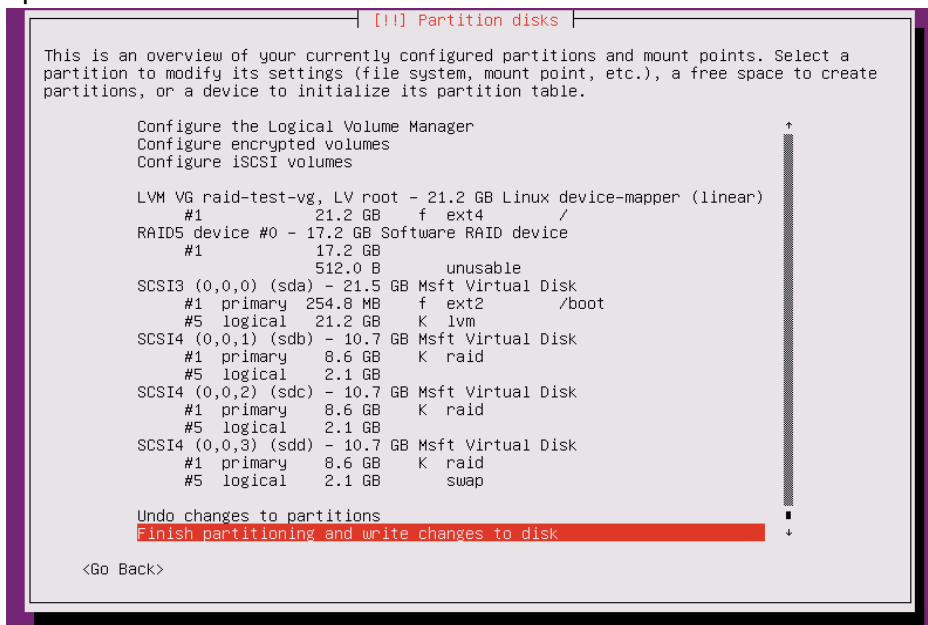
Finish by writing the changes to the disk. Hit "Yes" to continue.



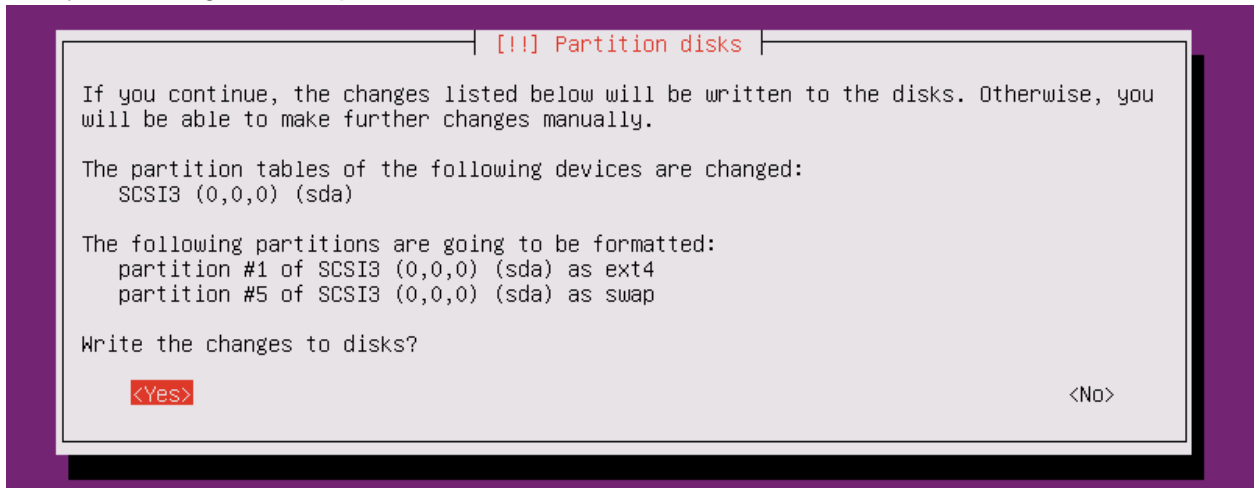
This is where the size of the partition is set. The default value is the max variable size of the drive.



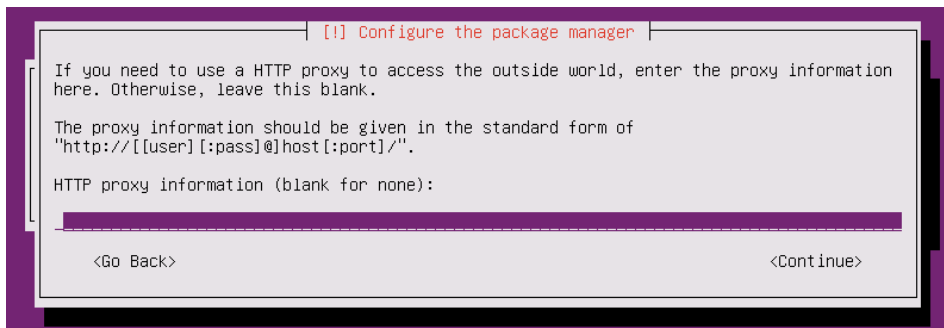
A summary of the drives will appear. Select "Finish partitioning and write changes to disk" option.



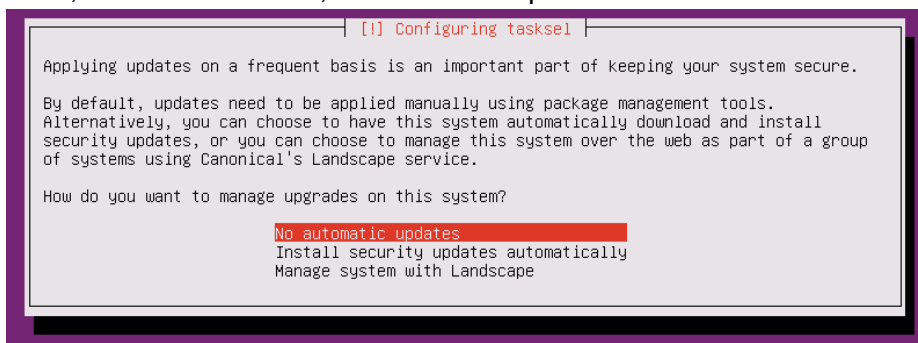
Verify the changes to the partition table.



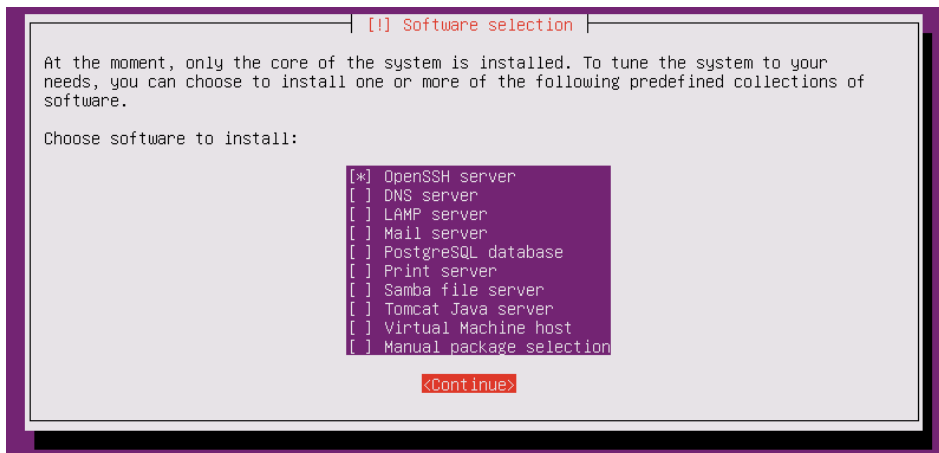
After this process has finished, a dialog box will appear asking about any proxy settings. This can be left blank. Hit Tab and Enter to continue.



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 type of update management should be used. Automatic updates can be used, but for this tutorial, no automatic updates will be selected.

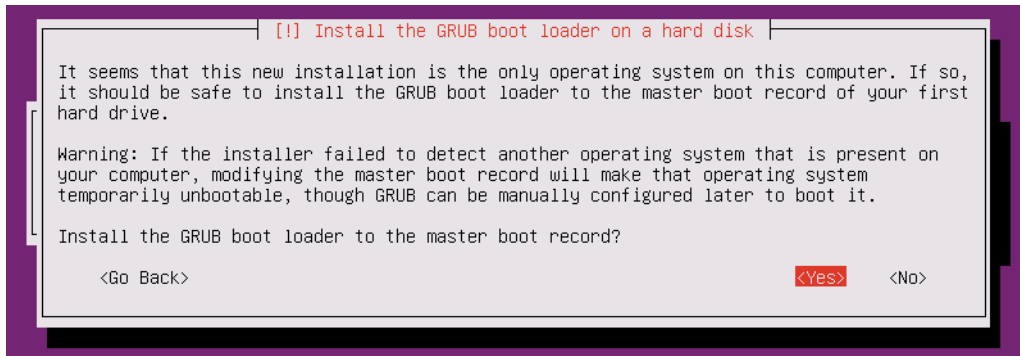


Here are some other optional packages that can be installed. Only the OpenSSH server will be selected in this tutorial. Installation of other protocols will be covered in other tutorials done post operating system installation. Use the arrow keys to move up and down and spacebar to select the packages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

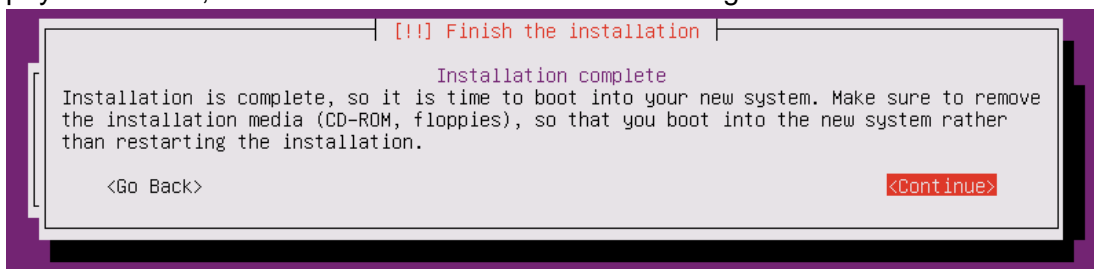


This package will now be downloaded and installed. This will take a while.

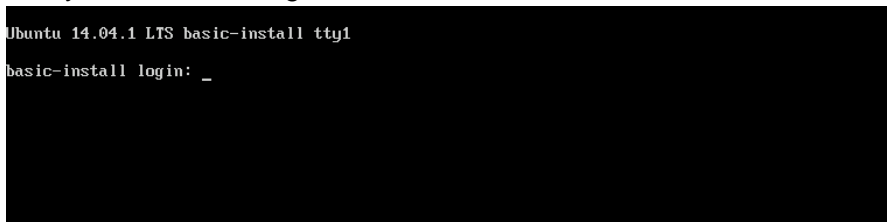
Finally, once that installation is finished, the server will ask if GRUB should be installed to the master boot record. Since this is the only operating system being installed on this server, select “Yes”.



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 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 0x10e4cf39.
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):
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-33531903, default 33531903):
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
```

```

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: 0x10e4cf39

   Device Boot      Start         End      Blocks   Id  System
/dev/md0p1                2048     33531903     16764928   83   Linux

```

/dev/md0p1 is the name of the partition and this formats that partition with the ext3 file system.

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

```

cisco@raid-test:~$ sudo mkfs -t ext3 /dev/md0p1
mke2fs 1.42.9 (4-Feb-2014)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=128 blocks, Stripe width=256 blocks
1048576 inodes, 4191232 blocks
209561 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=4294967296
128 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

```

**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/md0p1
/dev/md0p1 /media/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-pwdfil vsftpd vim apache2 apache2-utils
```

libpam-pwdfil 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

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

Create a new vsftpd file

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

Add the following 2 lines to the file:

```
auth required pam_pwdfile.so /etc/vsftpd/vsftpdb.passwd
```

```
account required pam_permit.so
```

```
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.

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

Restart the FTP service for the changes to take effect

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

```
cisco@raid-test:/etc$ sudo service vsftpd restart --system
vsftpd stop/waiting
vsftpd start/running, process 3085
```

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.

```
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:**

```
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
```

# OpenNMS Setup

Configuring OpenNMS SNMP Server Setup	123
Configuring SNMP for Windows Server 2012 R2	140

# 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
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:

```
cisco@acm-sntp-1:~$ sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys EEA14886
Executing: gpg --ignore-time-conflict --no-options --no-default-keyring --homedir /tmp/tmp.2B73cahHks --no-au
ck-trustdb --trust-model always --keyring /etc/apt/trusted.gpg --primary-keyring /etc/apt/trusted.gpg --keyse
kp://keyserver.ubuntu.com:80 --recv-keys EEA14886
gpg: requesting key EEA14886 from hkp server keyserver.ubuntu.com
gpg: key EEA14886: public key "Launchpad VLC" imported
gpg: Total number processed: 1
gpg:         imported: 1 (RSA: 1)
cisco@acm-sntp-1:~$
```

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
```

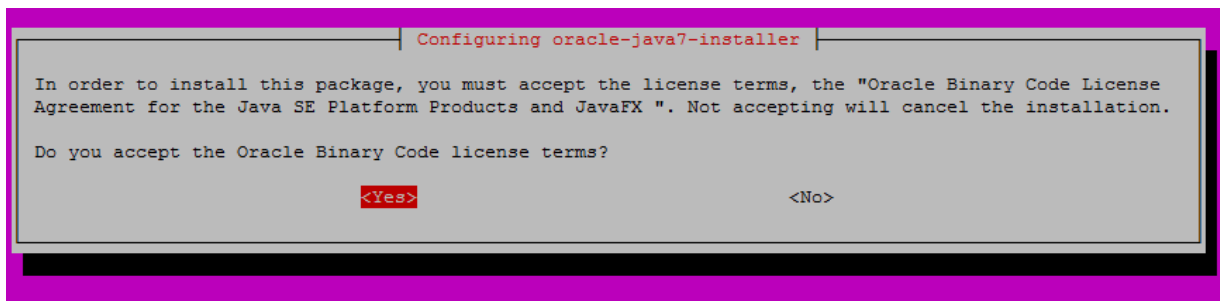
```
cisco@acm-sntp-1:~$ sudo apt-get install oracle-java7-installer
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  binutils gsfonst gsfonst-x11 java-common libfontenc1 libxfont1 x11-common
  xfontst-encodings xfontst-utils
Suggested packages:
  binutilst-doc default-jre equiva binfmt-support visualvm ttf-baekmuk
  ttf-unfontst ttf-unfontst-core ttf-kochi-gothic ttf-sazanami-gothic
  ttf-kochi-mincho ttf-sazanami-mincho ttf-arphic-uming firefox firefox-2
  iceweasel mozilla-firefox iceape-browser mozilla-browser epiphany-gecko
  epiphany-webkit epiphany-browser galeon midbrowser moblin-web-browser
  xulrunner xulrunner-1.9 konqueror chromium-browser midori google-chrome
The following NEW packagest will be installed:
  binutilst gsfonst gsfonst-x11 java-common libfontenc1 libxfont1
  oracle-java7-installer x11-common xfontst-encodings xfontst-utils
0 upgraded, 10 newly installed, 0 to remove and 125 not upgraded.
Need to get 6,429 kB of archivest.
After this operation, 19.2 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

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
```

```
cisco@acm-snm-1:~$ sudo apt-get install oracle-java7-set-default
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  oracle-java7-set-default
0 upgraded, 1 newly installed, 0 to remove and 125 not upgraded.
Need to get 4,686 B of archives.
After this operation, 57.3 kB of additional disk space will be used.
Get:1 http://ppa.launchpad.net/webupd8team/java/ubuntu/ precise/main oracle-java7-set-default all 7u76+7u60arm-0~webupd8~0 [4,686 B]
Fetched 4,686 B in 0s (16.8 kB/s)
Selecting previously unselected package oracle-java7-set-default.
(Reading database ... 56339 files and directories currently installed.)
Preparing to unpack .../oracle-java7-set-default_7u76+7u60arm-0~webupd8~0_all.deb ...
Unpacking oracle-java7-set-default (7u76+7u60arm-0~webupd8~0) ...
Setting up oracle-java7-set-default (7u76+7u60arm-0~webupd8~0) ...
cisco@acm-snm-1:~$
```

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 -
```

```
cisco@acm-snm-1:~$ sudo wget -O - http://debian.opennms.org/OPENNMS-GPG-KEY | sudo apt-key add -
--2015-03-23 17:43:57-- http://debian.opennms.org/OPENNMS-GPG-KEY
Resolving debian.opennms.org (debian.opennms.org)... 64.146.64.214
Connecting to debian.opennms.org (debian.opennms.org)|64.146.64.214|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1760 (1.7K)
Saving to: 'STDOUT'

100%[=====] 1,760 --.-K/s in 0s

2015-03-23 17:43:57 (94.8 MB/s) - written to stdout [1760/1760]
OK
```

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:

```
cisco@acm-snmpp-1:~$ apt-cache search opennms
libopennmsdeps-java - Enterprise-grade Open-source Network Management Platform (Required Libraries)
opennms-plugin-protocol-cifs - Enterprise-grade Open-source Network Management Platform (CIFS Protocol Support)
opennms-ncs - Enterprise-grade Open-source Network Management Platform (NCS)
mib2events - Create OpenNMS configuration from MIB files
opennms-plugin-provisioning-dns - Enterprise-grade Open-source Network Management Platform (DNS Provisioning Adapter)
opennms-plugin-ticketer-otrs - Enterprise-grade Open-source Network Management Platform (OTRS Ticketer Support)
opennms-remote-poller - Enterprise-grade Open-source Network Management Platform (Remote Poller)
opennms - Enterprise-grade Open-source Network Management Platform (Full Install)
opennms-plugin-provisioning-rancid - Enterprise-grade Open-source Network Management Platform (RANCID Provisioning Adapter)
opennms-server - Enterprise-grade Open-source Network Management Platform (Daemon)
opennms-plugin-collector-vtdxml-handler - Enterprise-grade Open-source Network Management Platform (VTD XML Handler)
libopennms-java - Enterprise-grade Open-source Network Management Platform (OpenNMS Libraries)
opennms-plugin-protocol-nsclient - Enterprise-grade Open-source Network Management Platform (NSClient Protocol Support)
opennms-webapp-jetty - Enterprise-grade Open-source Network Management Platform (Jetty Web UI)
opennms-plugin-protocol-dhcp - Enterprise-grade Open-source Network Management Platform (DHCP Protocol Support)
opennms-contrib - Enterprise-grade Open-source Network Management Platform (Contrib)
opennms-plugins - Enterprise-grade Open-source Network Management Platform (All Plugins)
opennms-plugin-protocol-xml - Enterprise-grade Open-source Network Management Platform (XML Collection Support)
opennms-plugin-provisioning-link - Enterprise-grade Open-source Network Management Platform (Link Provisioning Adapter)
opennms-db - Enterprise-grade Open-source Network Management Platform (Database)
opennms-plugin-provisioning-smmp-hardware-inventory - Enterprise-grade Open-source Network Management Platform (SNMP Hardware Inventory Provisioning Adapter)
opennms-plugin-collector-juniper-tca - Enterprise-grade Open-source Network Management Platform (Juniper TCA Collection Support)
opennms-plugin-provisioning-map - Enterprise-grade Open-source Network Management Platform (Map Provisioning Adapter)
libopennms-release-perl - Manage OpenNMS packaging/release repositories.
opennms-plugin-ticketer-rt - Enterprise-grade Open-source Network Management Platform (RT Ticketer Support)
librrd2-jni - java native interface library for rrdtool
opennms-doc - Enterprise-grade Open-source Network Management Platform (Documentation)
opennms-jmx-config-generator - Enterprise-grade Open-source Network Management Platform (JMX Config Generator)
mib2opennms - Create OpenNMS configuration from MIB files
opennms-plugin-ticketer-jira - Enterprise-grade Open-source Network Management Platform (JIRA Ticketer Support)
opennms-common - Enterprise-grade Open-source Network Management Platform (Common Files)
opennms-plugin-protocol-radius - Enterprise-grade Open-source Network Management Platform (RADIUS Protocol Support)
opennms-webapp - open network monitoring and management application, (web interface)
opennms-plugin-provisioning-smmp-asset - Enterprise-grade Open-source Network Management Platform (SNMP Asset Provisioning Adapter)
opennms-plugin-protocol-xmp - Enterprise-grade Open-source Network Management Platform (XMP Protocol Support)
```

**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
sudo apt-get install postgresql
```

```
cisco@acm-snmpp-1:~$ 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-client-9.3 postgresql-client-common
  postgresql-common ssl-cert
Suggested packages:
  oidentd ident-server locales-all postgresql-doc-9.3 openssl-blacklist
The following NEW packages will be installed:
  libpq5 postgresql postgresql-9.3 postgresql-client-9.3
  postgresql-client-common postgresql-common ssl-cert
0 upgraded, 7 newly installed, 0 to remove and 125 not upgraded.
Need to get 3,695 kB of archives.
After this operation, 15.7 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Type “y” and then Enter to continue.

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

```
pg_lsclusters -h
```

Make note of this version number. In this case, the version is 9.3.

```
cisco@acm-snmpp-1:~$ pg_lsclusters -h
9.3,main 5432 online postgres /var/lib/postgresql/9.3/main /var/log/postgresql/postgresql-9.3-main.log
```



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
```

```
libgnomevfs2-0 libgnomevfs2-common libgphoto2-6 libgphoto2-l10n
libgphoto2-port10 libgraphite2-3 libgtk-3-0 libgtk-3-bin libgtk-3-common
libgtk2.0-0 libgtk2.0-bin libgtk2.0-common libgudev-1.0-0 libgusb2
libharfbuzz0b libice6 libicu52 libidl-common libidl0 libieee1284-3 libisl10
libjasper1 libjbig0 libjpeg-turbo8 libjpeg8 liblcms2-2 libl1vm3.4 libltdl7
libmpc3 libmpfr4 libnspr4 libnss3 libnss3-nsdb libogg0 liborbit-2-0
liborbit2 libpango-1.0-0 libpangocairo-1.0-0 libpangoft2-1.0-0 libpciaccess0
libpixman-1-0 libpulse0 libsane libsane-common libsecret-1-0
libsecret-common libsm6 libsendfile1 libtdb1 libthai-data libthai0 libtiff5
libx86-dxtn-s2tc0 libudisks2-0 libv4l-0 libv4lconvert0 libvorbis9a
libvorbisenc2 libvorbisfile3 libvpx1 libwayland-client0 libwayland-cursor0
libx11-xcb1 libxaw7 libxcb-dri2-0 libxcb-dri3-0 libxcb-glx0 libxcb-present0
libxcb-render0 libxcb-shape0 libxcb-shm0 libxcb-sync1 libxcomposite1
libxcursor1 libxdamage1 libxfixes3 libxft2 libxi6 libxinerama1 libxkbcommon0
libxmu6 libxpm4 libxrandr2 libxrender1 libxshmfence1 libxt6 libxtst6 libxv1
libxxf86dga1 libxxf86vml openjdk-7-jre openjdk-7-jre-headless
policykit-1-gnome sound-theme-freedesktop tzdata-java udisks2 x11-utils
The following packages will be upgraded:
  tzdata
1 upgraded, 165 newly installed, 0 to remove and 124 not upgraded.
Need to get 83.7 MB of archives.
After this operation, 256 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

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.

```
Postfix Configuration
Please select the mail server configuration type that best meets your needs.

No configuration:
  Should be chosen to leave the current configuration unchanged.
Internet site:
  Mail is sent and received directly using SMTP.
Internet with smarthost:
  Mail is received directly using SMTP or by running a utility such
  as fetchmail. Outgoing mail is sent using a smarthost.
Satellite system:
  All mail is sent to another machine, called a 'smarthost', for delivery.
Local only:
  The only delivered mail is the mail for local users. There is no network.

General type of mail configuration:

    No configuration
    Internet Site
    Internet with smarthost
    Satellite system
    Local only

    <Ok>                <Cancel>
```

Hit Enter to continue.

```
Postfix Configuration
The "mail name" is the domain name used to "qualify" _ALL_ mail addresses without a domain name. This
includes mail to and from <root>: please do not make your machine send out mail from root@example.org
unless root@example.org has told you to.

This name will also be used by other programs. It should be the single, fully qualified domain name (FQDN).

Thus, if a mail address on the local host is foo@example.org, the correct value for this option would be
example.org.

System mail name:
acm-snmp-1.tydrous.tv

    <Ok>                <Cancel>
```

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
```

```

cisco@acm-snmp-1:~$ sudo apt-get install opennms
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  heirloom-mailx iplike-pgsq193 jicmp jicmp6 libauthen-sasl-perl
  libdbd-pg-perl libdbi-perl libencode-locale-perl libfile-listing-perl
  libfont-afm-perl libgetopt-mixed-perl libhtml-form-perl libhtml-format-perl
  libhtml-parser-perl libhtml-tagset-perl libhtml-tree-perl
  libhttp-cookies-perl libhttp-daemon-perl libhttp-date-perl
  libhttp-message-perl libhttp-negotiate-perl libio-html-perl
  libio-socket-inet6-perl libio-socket-ssl-perl liblwp-mediatypes-perl
  liblwp-protocol-https-perl libmailtools-perl libnet-http-perl
  libnet-smtp-ssl-perl libnet-snmp-perl libnet-ssleay-perl libopennms-java
  libopennmsdeps-java libsocket6-perl libtie-ixhash-perl liburi-perl
  libwww-perl libwww-robotrules-perl libxml-parser-perl libxml-twig-perl
  libxml-xpathengine-perl libxml2-utils opennms-common opennms-db
  opennms-server opennms-webapp-jetty
Suggested packages:
  libdigest-hmac-perl libgsapi-perl libclone-perl libmldbm-perl
  libnet-daemon-perl libplrpc-perl libsql-statement-perl libdata-dump-perl
  libcrypt-ssleay-perl libcrypt-dss-perl libauthen-ntlm-perl
  libunicode-map8-perl libunicode-string-perl xml-twig-tools opennms-doc jrd
  rrdtool
The following NEW packages will be installed:
  heirloom-mailx iplike-pgsq193 jicmp jicmp6 libauthen-sasl-perl
  libdbd-pg-perl libdbi-perl libencode-locale-perl libfile-listing-perl
  libfont-afm-perl libgetopt-mixed-perl libhtml-form-perl libhtml-format-perl
  libhtml-parser-perl libhtml-tagset-perl libhtml-tree-perl
  libhttp-cookies-perl libhttp-daemon-perl libhttp-date-perl
  libhttp-message-perl libhttp-negotiate-perl libio-html-perl
  libio-socket-inet6-perl libio-socket-ssl-perl liblwp-mediatypes-perl
  liblwp-protocol-https-perl libmailtools-perl libnet-http-perl
  libnet-smtp-ssl-perl libnet-snmp-perl libnet-ssleay-perl libopennms-java
  libopennmsdeps-java libsocket6-perl libtie-ixhash-perl liburi-perl
  libwww-perl libwww-robotrules-perl libxml-parser-perl libxml-twig-perl
  libxml-xpathengine-perl libxml2-utils opennms opennms-common opennms-db
  opennms-server opennms-webapp-jetty
0 upgraded, 47 newly installed, 0 to remove and 124 not upgraded.
Need to get 506 MB of archives.
After this operation, 649 MB of additional disk space will be used.
Do you want to continue? [Y/n]

```

Type “y” and hit Enter to continue.

Once OpenNMS has finished downloading, a message will appear.

```

Configuring opennms-db

The OpenNMS installer must now be run manually

Previous versions of this package would invoke the installer to handle
initial setup, or upgrade an existing database. This is no longer the
case. You must manually run /usr/share/opennms/bin/install to complete
this install/upgrade. Full install documentation can be found in the
opennms-doc package or viewed online at the OpenNMS wiki,
(http://www.opennms.org/index.php/Official\_Documentation).

<Ok>

```

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

```

Configuring iplike-pgsq193

IPLIKE installation failed

Failed to install iplike into the templatel or opennms databases. See /tmp/install_iplike.log for details.
To skip this step and install manually, set the environment variable SKIP_IPLIKE_INSTALL before installing
this package. To install iplike into your database, use the /usr/sbin/install_iplike.sh script. See
`install_iplike.sh -h` for more details.

<Ok>

```

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
```

```
cisco@acm-snmp-1:~$ sudo /usr/share/opennms/bin/runjava -s
runjava: Looking for an appropriate JRE...
runjava: Checking for an appropriate JRE in JAVA_HOME...
runjava: skipping... JAVA_HOME not set
runjava: Checking JRE in user's path: "/usr/bin/java"...
runjava: found an appropriate JRE in user's path: "/usr/bin/java"
runjava: value of "/usr/bin/java" stored in configuration file
cisco@acm-snmp-1:~$
```

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

```
cisco@acm-snmp-1:~$ sudo /usr/share/opennms/bin/runjava -S /usr/bin/java
runjava: checking specified JRE: "/usr/bin/java"...
runjava: specified JRE is good.
runjava: value of "/usr/bin/java" stored in configuration file
```

Java Configuration complete

## Creating the OpenNMS Database:

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

```
Processing ServiceConfigMigratorOffline: Fixes service-configuration.xml if necessary when upgrading from 1.12: NMS
-6970
- Running pre-execution phase
  Backing up /usr/share/opennms/etc/service-configuration.xml
  Zipping /usr/share/opennms/etc/service-configuration.xml
- Running execution phase
  Disabling service OpenNMS:Name=Dhcpd because it is not on the default list of enabled services
  Disabling service OpenNMS:Name=Capsd because it is not on the default list of enabled services
  Disabling service OpenNMS:Name=SmpPoller because it is not on the default list of enabled services
  Fixing logging prefix for service OpenNMS:Name=Provisiond
  Fixing logging prefix for service OpenNMS:Name=Reporrd
  Fixing logging prefix for service OpenNMS:Name=Alarmd
  Fixing logging prefix for service OpenNMS:Name=Askd
  Disabling service OpenNMS:Name=Linkd because it is not on the default list of enabled services
  Disabling Linkd (to promote EnhancedLinkd)
  Disabling service OpenNMS:Name=Correlator because it is not on the default list of enabled services
  Disabling service OpenNMS:Name=TlId because it is not on the default list of enabled services
  Disabling service OpenNMS:Name=Syslogd because it is not on the default list of enabled services
  Disabling service OpenNMS:Name=Xmlrpc because it is not on the default list of enabled services
  Disabling service OpenNMS:Name=XmlrpcProvisioner because it is not on the default list of enabled services
  Disabling service OpenNMS:Name=AsteriskGateway because it is not on the default list of enabled services
  Disabling service OpenNMS:Name=AccessPointMonitor because it is not on the default list of enabled services
- Saving the execution state
- Running post-execution phase
  Removing backup /usr/share/opennms/etc/service-configuration.xml.zip
Finished in 0 seconds
Upgrade completed successfully!
```

## Installing IPLIKE:

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

This command will only have one line of output

```
cisco@acm-snmp-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
```

```

cisco@acm-snmp-1:~$ psql -U postgres --host=localhost opennms
psql (9.3.6)
SSL connection (cipher: DHE-RSA-AES256-SHA, bits: 256)
Type "help" for help.

opennms=# \q
cisco@acm-snmp-1:~$ █

```

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
```

```

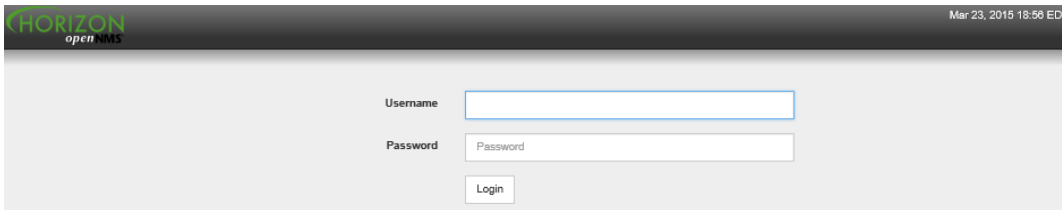
cisco@acm-snmp-1:~$ sudo service opennms status
OpenNMS.Eventd      : running
OpenNMS.Trapd       : running
OpenNMS.Queued      : running
OpenNMS.Actiond     : running
OpenNMS.Notifd      : running
OpenNMS.Scriptd     : running
OpenNMS.Rtcd        : running
OpenNMS.Pollerd     : running
OpenNMS.PollerBackEnd : running
OpenNMS.EnhancedLinkd : running
OpenNMS.Ticketer    : running
OpenNMS.Collectd     : running
OpenNMS.Discovery   : running
OpenNMS.Vacuumd     : running
OpenNMS.EventTranslator: running
OpenNMS.PassiveStatusd : running
OpenNMS.Statsd      : running
OpenNMS.Provisiond  : running
OpenNMS.Reportd     : running
OpenNMS.Alarmd      : running
OpenNMS.Ackd        : running
OpenNMS.JettyServer : running
opennms is running

```

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

### **Accessing OpenNMS:**

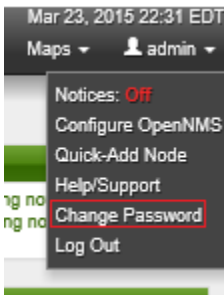
Navigate to the address <http://172.24.64.25:8980/opennms/> using a web browser of any kind on a computer which can connect to the SNMP server.



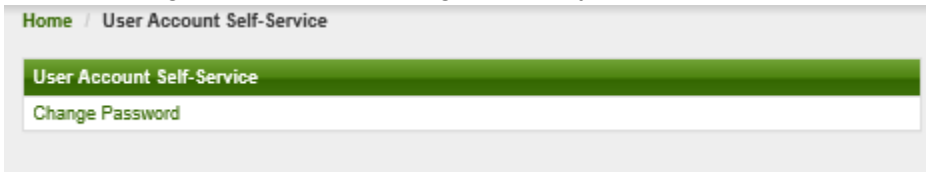
The default login information is  
Username: admin  
Password: admin

**Changing default Admin password:**

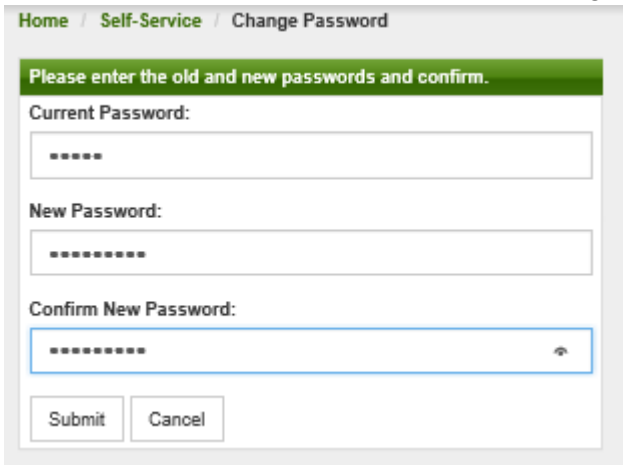
Mouse over “admin” in the top right and select the “Change Password” option in the drop down menu.



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:

The screenshot shows the OpenNMS Admin interface. The top navigation bar includes 'Search', 'Info', 'Status', 'Reports', 'Dashboards', 'Maps', and 'admin'. The main content area is divided into two columns. The left column contains a sidebar menu with sections: 'OpenNMS System' (Configure Users, Groups and On-Call Roles, System Information, Instrumentation Log Reader), 'Operations' (Configure Discovery, Configure SNMP Community Names by IP, Configure SNMP Data Collection per Interface, Manage and Unmanage Interfaces and Services, Manage Thresholds, Send Event, Configure Notifications, Scheduled Outages, Manage Events Configuration, Manage SNMP Collections and Data Collection Groups), and a 'Notification Status' section with radio buttons for 'On' and 'Off' (the 'Off' button is selected) and an 'Update' button. The right column contains a 'Descriptions' section with detailed text about system settings and configuration options. A dropdown menu is open in the top right corner, showing options: 'Notices: Off', 'Configure OpenNMS' (highlighted with a red box), 'Quick-Add Node', 'Help/Support', 'Change Password', and 'Log Out'.

Configuring an IP range for discovery:

The screenshot shows the OpenNMS Admin interface for the 'Discovery' configuration page. The top navigation bar includes 'Search', 'Info', 'Status', 'Reports', 'Dashboards', 'Maps', and 'admin'. The main content area is titled 'Home / Admin / Discovery / Modify Configuration'. It features a 'Save and Restart Discovery' button at the top. Below this is a 'General Settings' section with several input fields: 'Initial sleep time (sec.):' (30), 'Restart sleep time (hours):' (24), 'Threads:' (1), 'Retries:' (1), and 'Timeout (ms.):' (2000). Below the general settings are four sections: 'Specifics' (No specifics found, Add New), 'Include URLs' (No include URLs found, Add New), 'Include Ranges' (No include ranges found, Add New), and 'Exclude Ranges' (No exclude ranges found, Add New). The 'Add New' button in the 'Include Ranges' section is highlighted with a red box.

Enter the IP address range: Begin IP and End IP:

**Home**

**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:**

**End IP Address:**

**Retries:**

**Timeout (ms):**

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

Include Ranges				
Begin Address	End Address	Timeout (ms.)	Retries	Action
192.168.132.0	192.168.132.255	2000	1	<input type="button" value="Delete"/>
192.168.128.0	192.168.131.255	2000	1	<input type="button" value="Delete"/>
172.24.64.0	172.24.79.255	2000	1	<input type="button" value="Delete"/>

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.

**Operations**

- Configure Discovery
- Configure SNMP Community Names by IP
- Configure SNMP Data Collection per Interface
- Manage and Unmanage Interfaces and Services
- Manage Thresholds
- Send Event
- Configure Notifications
- Scheduled Outages
- Manage Events Configuration
- Manage SNMP Collections and Data Collection Groups



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”.

Updating SNMP Configuration

General Parameters

Version: v2c  
Default: v2c

First IP Address: 192.168.132.0

Last IP Address: 192.168.132.255

Timeout: 1800  
Default: 3000 ms

Retries: 1  
Default: 1

Port: 161  
Default: 161

Proxy Host:

Max Request Size: 65535  
Default: 65535

Max Vars Per Pdu: 10  
Default: 10

Max Repetitions: 2  
Default: 2

v1/v2c specific parameters

Read Community String: public  
Default: public

Write Community String: private  
Default: private

Save Options

Send Event  Default: enabled

Send Locally  Default: disabled

Save Config Cancel

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.

Home / Admin / Configure SNMP by IP

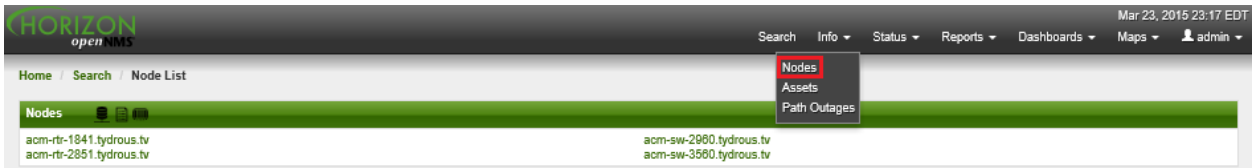
SNMP Config Lookup

IP Address

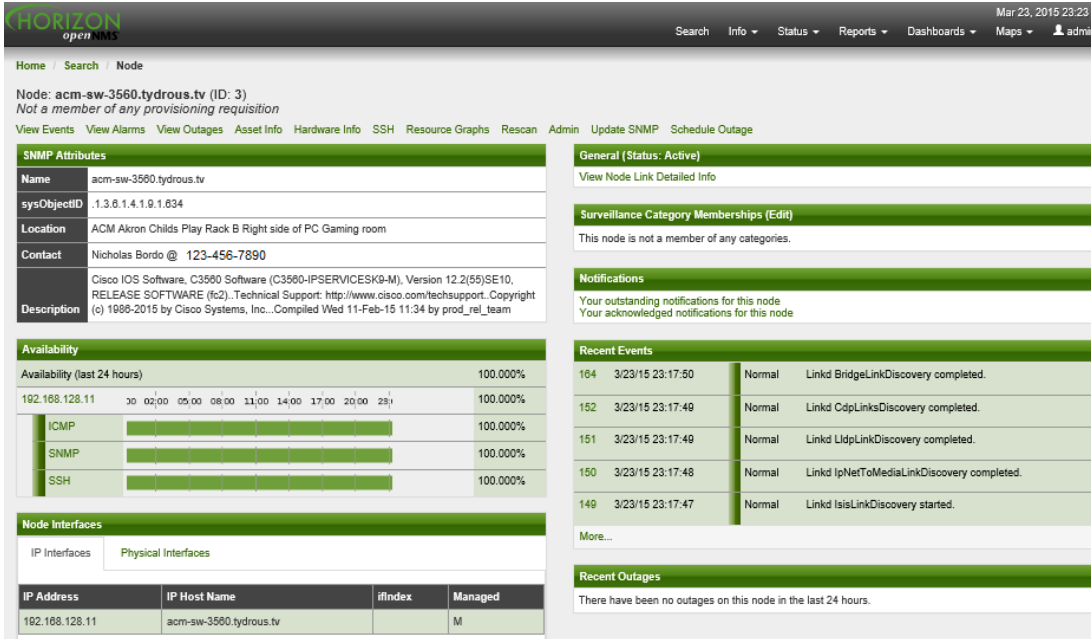
Look up

### **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.



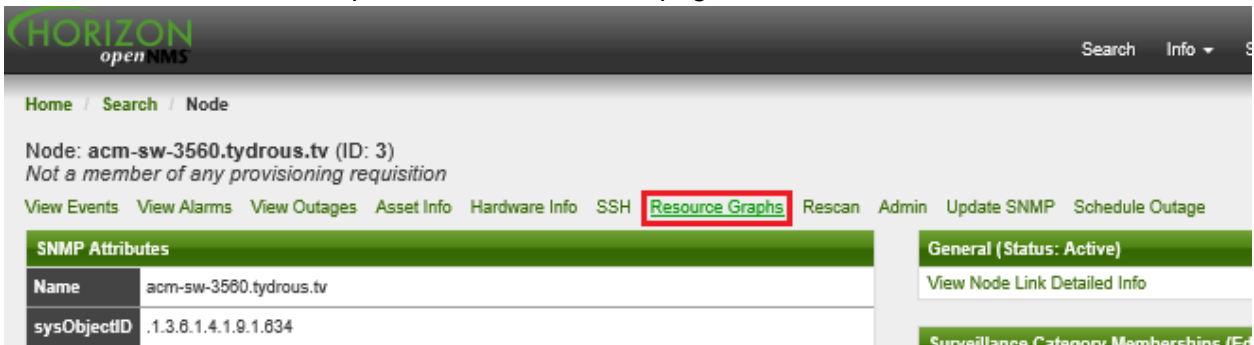
All of the discovered devices, or “Nodes”, are listed here. Additional information about each node can be viewed by clicking on the desired Node.



**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.

**HORIZON**  
openNMS

Mar 24, 2015 15:15 EDT

Search Info Status Reports Dashboards Maps admin

Home / Reports / Resource Graphs / Choose

Node: acm-sw-3560.tydrus.tv

**Node Resources**

- ▼ SNMP Node Data (1)
  - Node-level Performance Data
- ▼ SNMP Interface Data (1)
  - VI6 (MANAGEMENT VLAN INTERFACE, 1 Gbps)
- ▼ Response Time (1)
  - 192.168.128.11

Clear Selection    Select All    **Graph Selection**    Search    Graph All

Example output:

**HORIZON**  
openNMS

Mar 24, 2015 15:19 E

Search Info Status Reports Dashboards Maps admin

Home / Reports / Resource Graphs / Results

Time period Last Day ▾  
From Mon Mar 23 15:19:00 EDT 2015  
To Tue Mar 24 15:19:00 EDT 2015

Node: acm-sw-3560.tydrus.tv  
SNMP Interface Data: VI6 (MANAGEMENT VLAN INTERFACE, 1 Gbps)

SNMP Interface Data

**Bits In/Out (High Speed)**

In	Avg : 1.75 k	Min : 1.54 k	Max : 2.72 k
Out	Avg : 1.19 k	Min : 867.4B	Max : 1.85 k
Tot In : 160.17 M		Tot Out : 68.01 M    Tot : 168.18 M	

**Cisco Packets In/Out**

Out	Avg : 849.76	Min : 0.00	Max : 3.00
In	Avg : 86.74	Min : 0.00	Max : 1.00

## 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.

The screenshot shows the OpenNMS home dashboard. The top navigation bar includes 'Search', 'Info', 'Status', 'Reports', 'Dashboards', 'Maps', and 'admin'. The main content area is divided into several sections:

- Nodes with Pending Problems:** A box indicating that 'acm-rtr-1841.tydrous.tv' has 5 alarms (3 minutes).
- Nodes with Outages:** A box indicating that 'acm-rtr-1841.tydrous.tv' has 2 minutes of outage.
- Availability Over the Past 24 Hours:** A table showing network performance metrics.
- Notifications:** A box stating 'You have no outstanding notices'.
- Resource Graphs:** A search box for resource graphs.
- KSC Reports:** A box stating 'No KSC reports defined'.

Categories	Outages	Availability
Network Interfaces	6 of 39	99.994%
Web Servers	0 of 1	100.000%
Email Servers	0 of 1	100.000%
DNS and DHCP Servers	4 of 17	99.994%
Database Servers	0 of 0	100.000%
JMX Servers	0 of 0	100.000%
Other Servers	4 of 24	99.994%
<b>Total</b>	<b>Outages</b>	<b>Availability</b>
Overall Service Availability	14 of 82	99.994%

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.

The screenshot shows the 'Alarms List' page in OpenNMS. The top navigation bar includes 'Search', 'Info', 'Status', 'Reports', 'Dashboards', 'Maps', and 'admin'. The main content area includes a search bar and a list of alarms.

Home / Alarms / List

View all alarms | Advanced Search | Long Listing | Severity Legend | Acknowledge entire search

Alarm(s) outstanding | node=acm-rtr-1841.tydrous | Acknowledge all alarms that match the current search constraints, even those not shown on the screen

Results 1-5 of 5

Ack	Severity	Node	Count	Last Event Time	Log Msg
<input type="checkbox"/>	9	acm-rtr-1841.tydrous.tv	1	Mar 25, 2015 1:43:24 PM	Interface 172.20.32.3 is down.
<input type="checkbox"/>	8	acm-rtr-1841.tydrous.tv	1	Mar 25, 2015 1:43:24 PM	Interface 192.168.132.3 is down.
<input type="checkbox"/>	7	acm-rtr-1841.tydrous.tv	1	Mar 25, 2015 1:43:24 PM	Interface 172.24.64.3 is down.
<input type="checkbox"/>	6	acm-rtr-1841.tydrous.tv	1	Mar 25, 2015 1:43:24 PM	Interface 192.168.128.3 is down.
<input type="checkbox"/>	5	acm-rtr-1841.tydrous.tv	1	Mar 25, 2015 1:41:45 PM	SNMP data collection on interface 192.168.132.3 failed with 'Timeout retrieving SnmpCollectors for 192.168.132.3 for /192.168.132.3: SnmpCollectors for 192.168.132.3: snmpTimeoutError for: /192.168.132.3'.

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.

Node: **acm-itr-1841.tydrous.tv** (ID: 2)  
 Not a member of any provisioning requisition

View Events View Alarms View Outages Asset Info Hardware Info SSH Resource Graphs Rescan Admin Update SNMP Schedule Outage

SNMP Attributes	
Name	acm-itr-1841.tydrous.tv
sysObjectID	1.3.6.1.4.1.9.1.620
Location	ACM Akron Chills Play Rack B Right side of PC Gaming room
Contact	Nicholas Bordo @ 330-703-9601
Description	Cisco IOS Software, 1841 Software (C1841-IPBASEK9-M), Version 12.4(24)T8, RELEASE SOFTWARE (fc1), Technical Support: http://www.cisco.com/techsupport. Copyright (c) 1986-2012 by Cisco Systems, Inc. Compiled Sun 09-Sep-12 03:09 by prod_rel_team

General (Status: Active)  
View Node Link Detailed Info

Surveillance Category Memberships (Edit)  
This node is not a member of any categories.

Notifications  
Your outstanding notifications for this node  
Your acknowledged notifications for this node

Recent Events

647	3/25/15 13:43:24	Minor	Interface 172.20.32.3 is down.
648	3/25/15 13:43:24	Minor	Interface 192.168.132.3 is down.
645	3/25/15 13:43:24	Minor	Interface 172.24.64.3 is down.
644	3/25/15 13:43:24	Minor	Interface 192.168.128.3 is down.
643	3/25/15 13:41:45	Minor	SNMP data collection on interface 192.168.132.3 failed with 'Timeout retrieving SnmpCollectors for 192.168.132.3 for /192.168.132.3: SnmpCollectors for 192.168.132.3: snmpTimeoutError for /192.168.132.3'.

More...

Recent Outages

Interface	Service	Lost	Regained	Outage ID
172.20.32.3	DNS	3/25/15 13:43:24		14
172.20.32.3	ICMP	3/25/15 13:43:24	DOWN	13
172.20.32.3	SSH	3/25/15 13:43:24	DOWN	12
192.168.132.3	DNS	3/25/15 13:43:24	DOWN	11
192.168.132.3	SNMP	3/25/15 13:43:24	DOWN	10
192.168.132.3	ICMP	3/25/15 13:43:24	DOWN	9
192.168.132.3	SSH	3/25/15 13:43:24	DOWN	8
172.24.64.3	DNS	3/25/15 13:43:24	DOWN	7
172.24.64.3	ICMP	3/25/15 13:43:24	DOWN	6
172.24.64.3	SSH	3/25/15 13:43:24	DOWN	5
192.168.128.3	DNS	3/25/15 13:43:24	DOWN	4
192.168.128.3	ICMP	3/25/15 13:43:24	DOWN	3
192.168.128.3	SNMP	3/25/15 13:43:24	DOWN	2
192.168.128.3	SSH	3/25/15 13:43:24	DOWN	1

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.

Horizon open NMS Mar 25, 2015 14:08 EDT

Search Info Status Reports Dashboards Maps admin

Home

**Nodes with Pending Problems**

There are no pending problems.

**Nodes with Outages**

There are no current outages

**Availability Over the Past 24 Hours**

Categories	Outages	Availability
Network Interfaces	0 of 39	99.692%
Web Servers	0 of 1	100.000%
Email Servers	0 of 1	100.000%
DNS and DHCP Servers	0 of 17	99.655%
Database Servers	0 of 0	100.000%
JMX Servers	0 of 0	100.000%
Other Servers	0 of 24	99.676%
<b>Total</b>	<b>Outages</b>	<b>Availability</b>
Overall Service Availability	0 of 82	99.679%

**Notifications**

You have no outstanding notices  
There are no outstanding notices  
On-Call Schedule

**Resource Graphs**

Search

**KSC Reports**

No KSC reports defined

Search

**Quick Search**

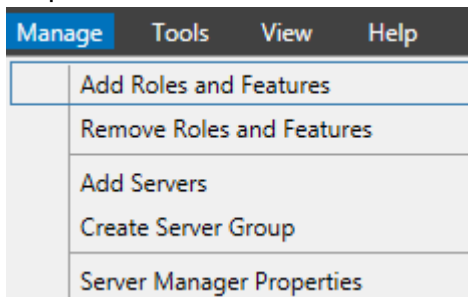
# Configuring SNMP for Windows Server 2012 R2

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.

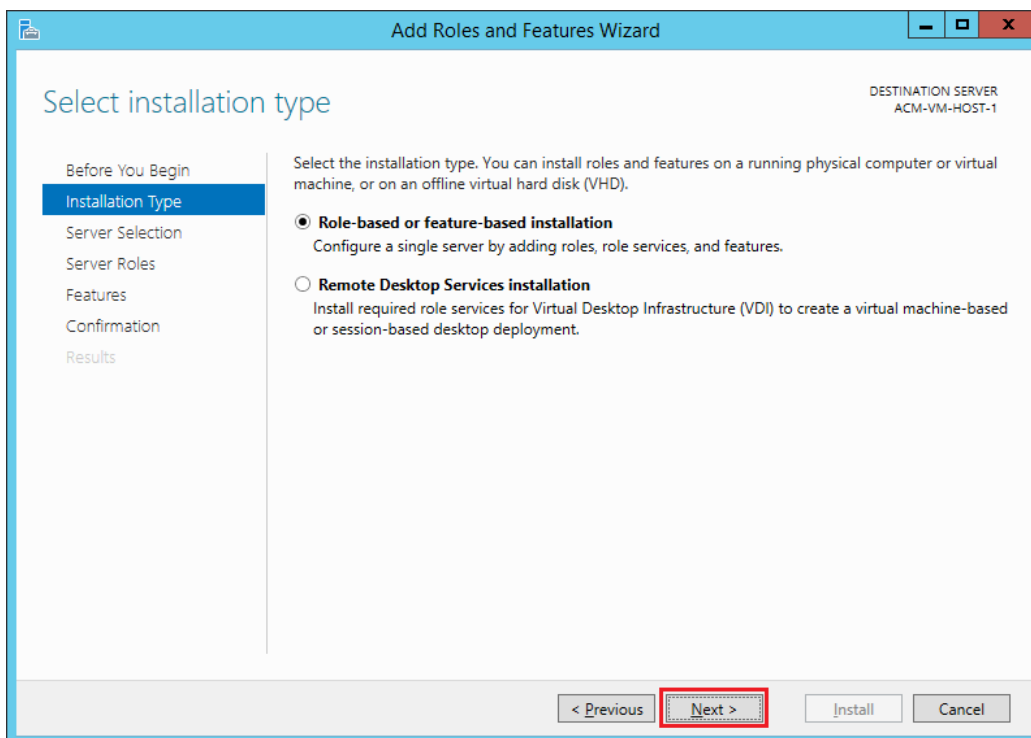
This tutorial will be using the domain name tydrous.tv. This procedure will work for any other domain name simply replace tydrous.tv with the different domain.

## Configuring Windows Server SNMP:

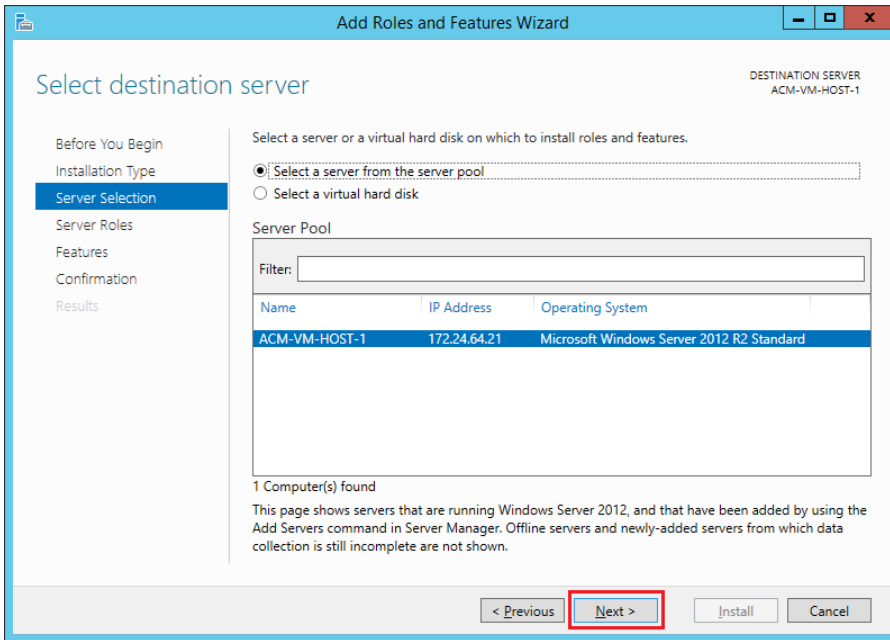
Open the Server manager and select the “Add Roles and Features” option from the “Manage” drop down menu.



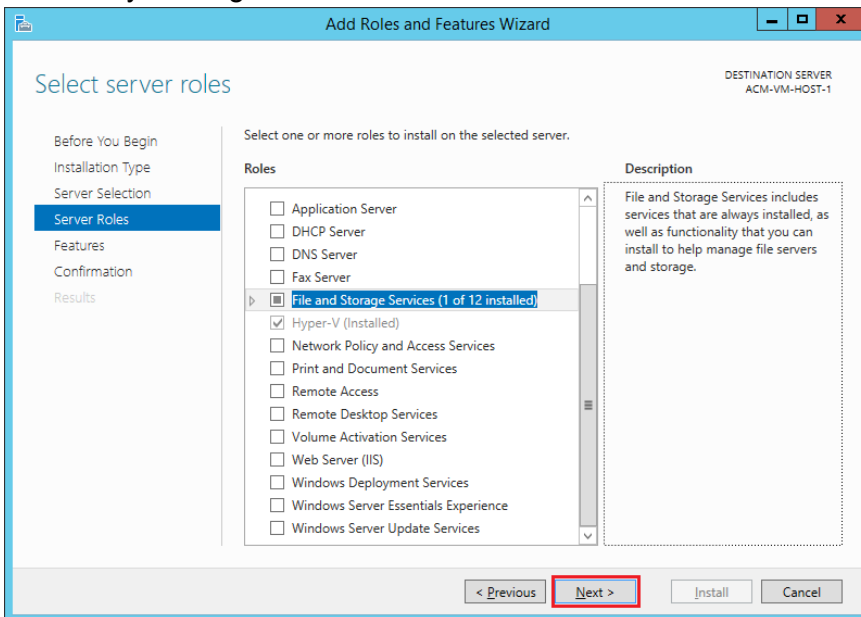
Make sure the “Role-based or feature based installation” is selected and click “Next”.



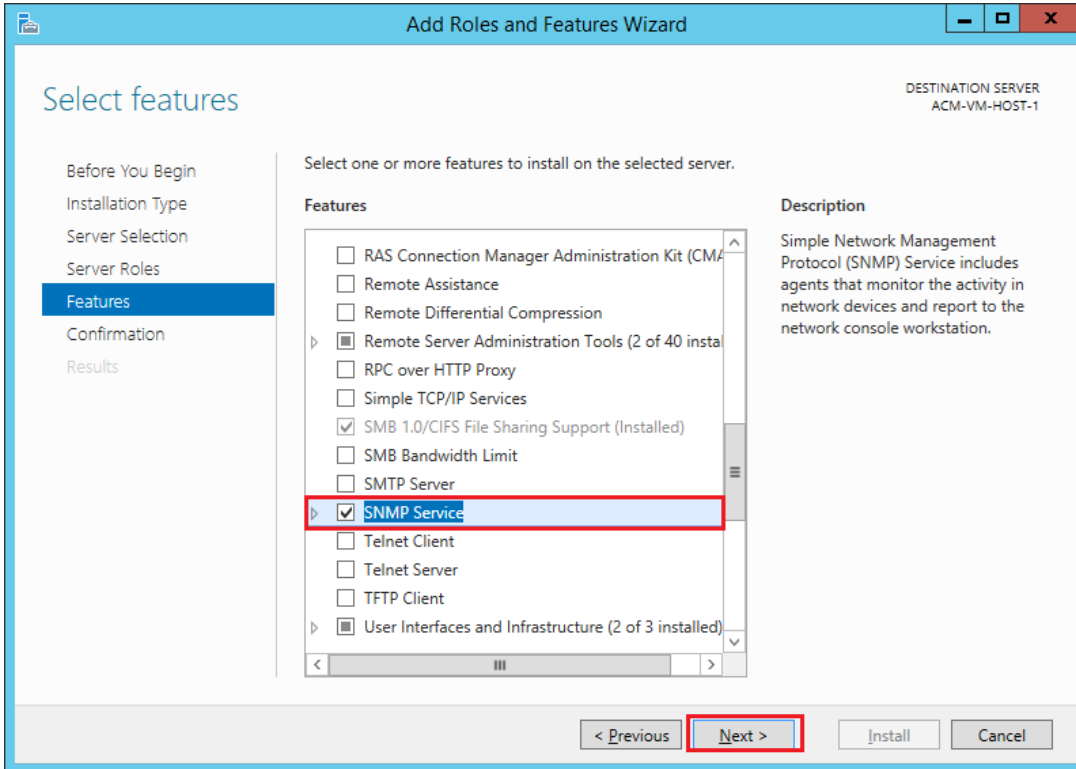
Select the server to add the feature to and click “Next”.



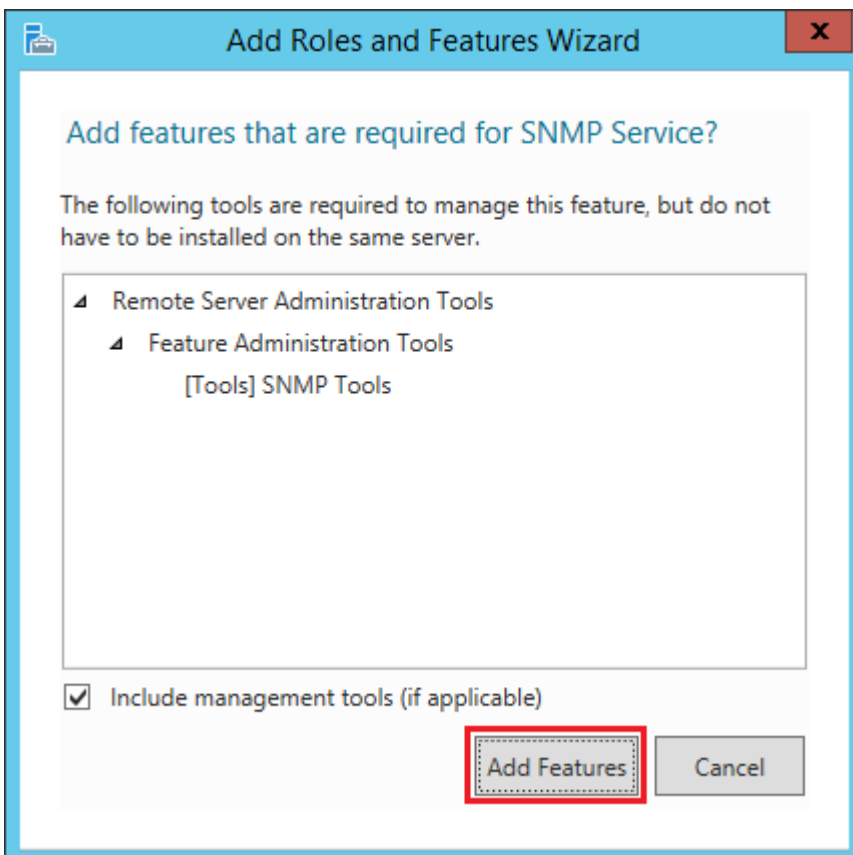
Skip the Server Roles window without selecting any roles to add and move to the Features window by clicking “Next”.



Select the "SNMP Service" option by checking the box to the left. Then, click "Next".

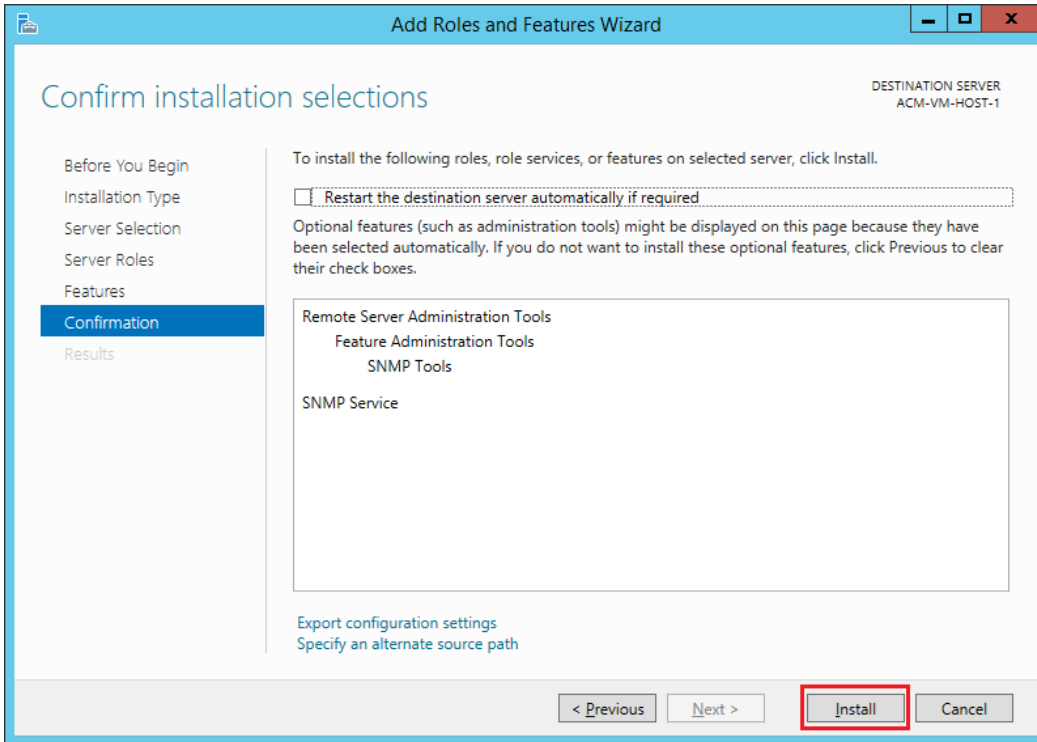


If presented with a dialog box, click "Add Feature" and click "Next" again at the Features window.

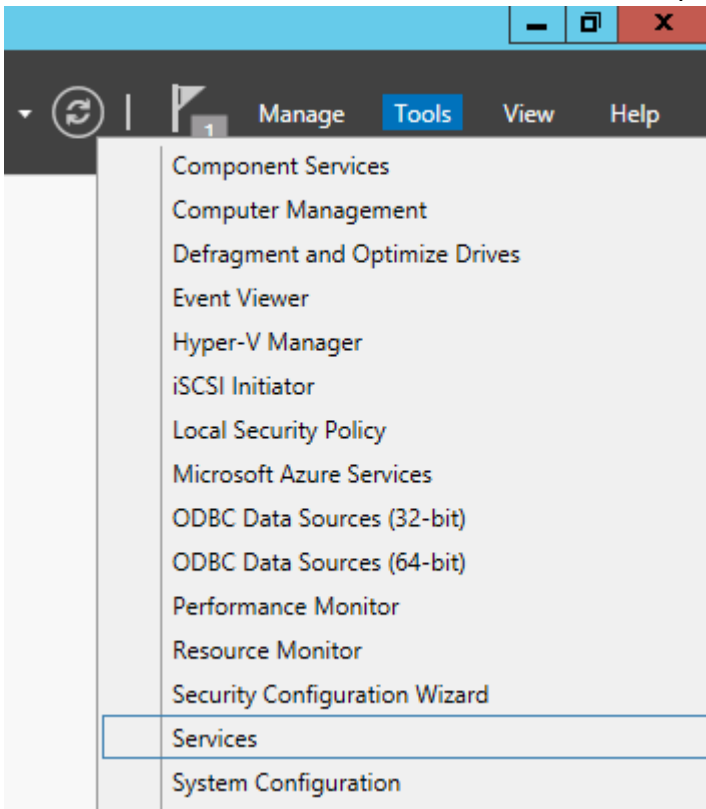




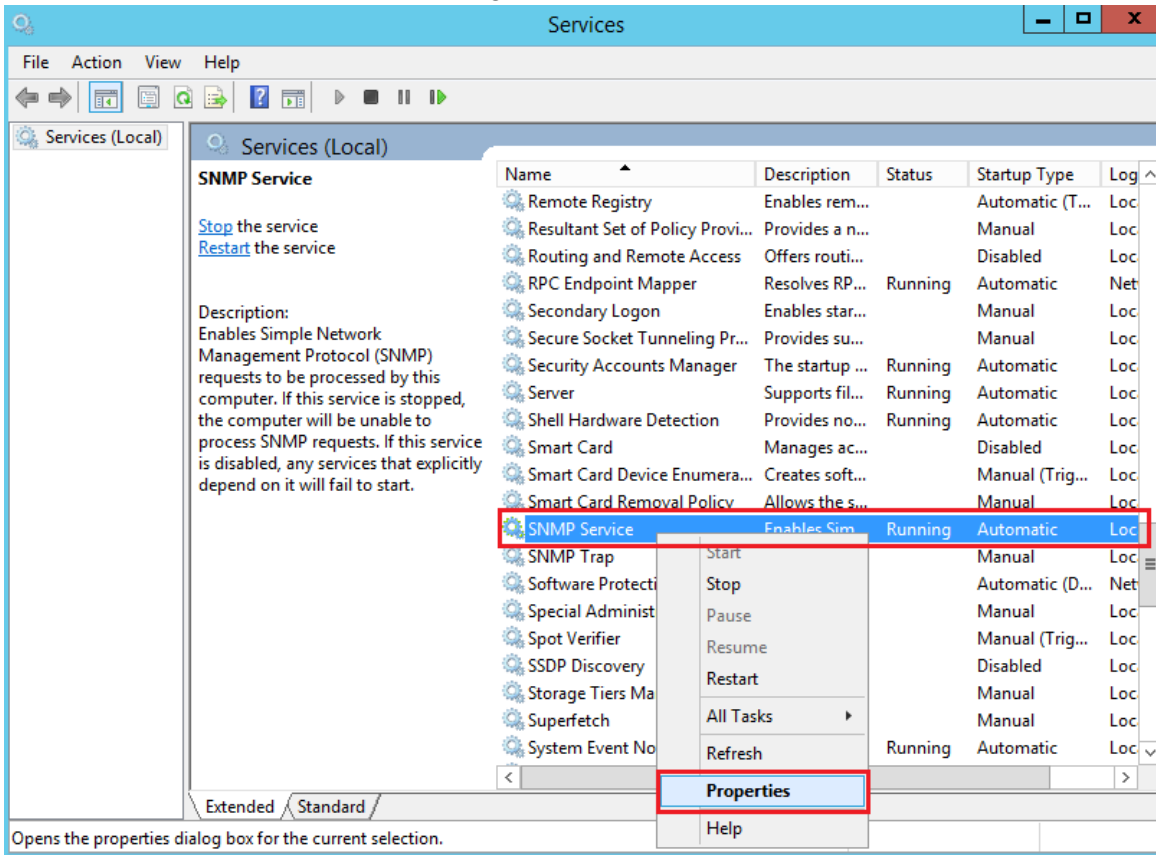
Click “Install” to begin adding the feature. The install process will complete in the background.



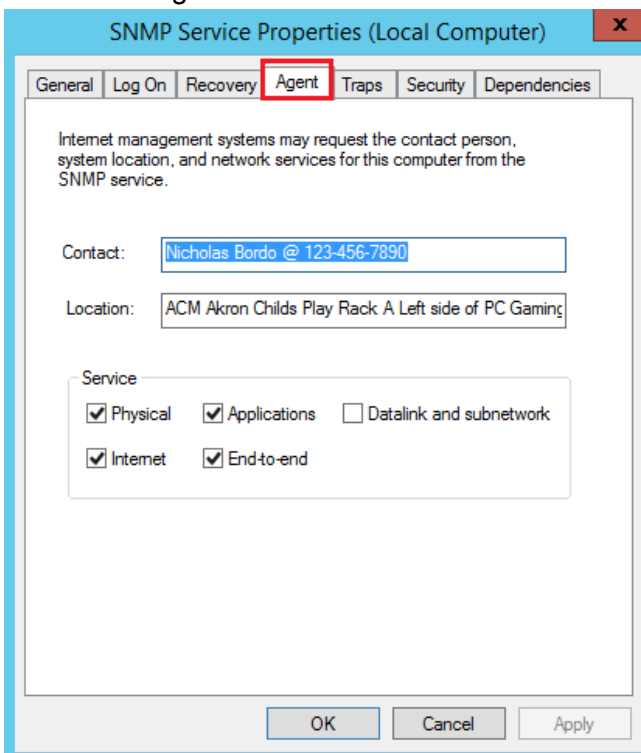
Once the installation is complete click on the “Close” button and return to the Server Manager window. Click on “Tools” and select the “Services” option.



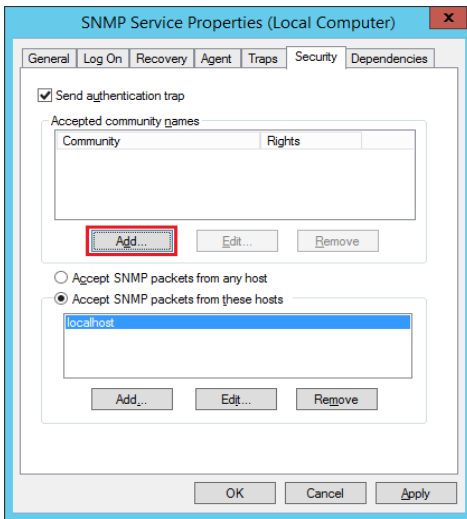
Scroll down to “SNMP Service” and right click on it and select the “Properties” option.



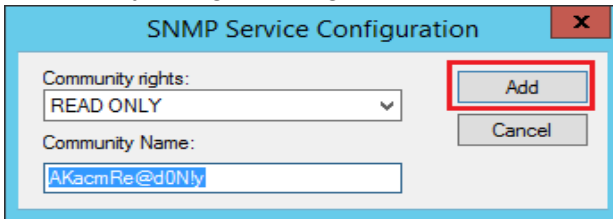
Select the “Agent” tab and enter in the contact information and location of the server.



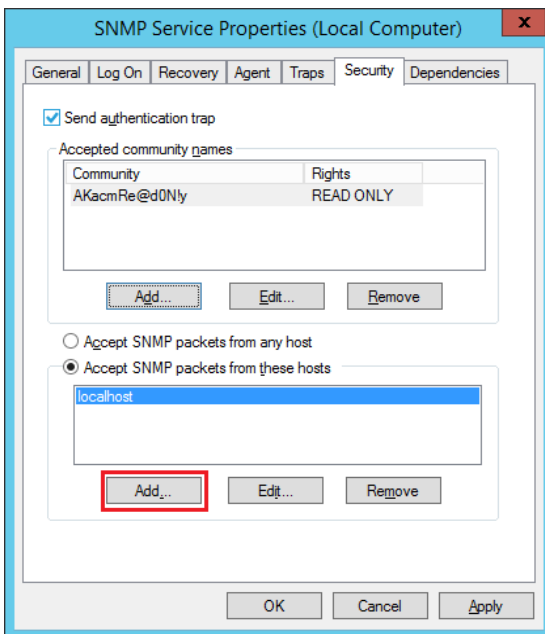
Click on the “Security” tab and then click on the first “Add...” button to configure the community string.



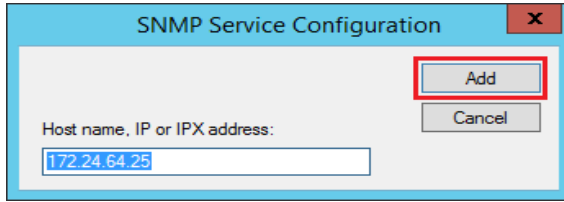
Enter in the read only community string in the “Community Name” text box. Make sure the community string is configured as “READ ONLY” and then click “Add”.



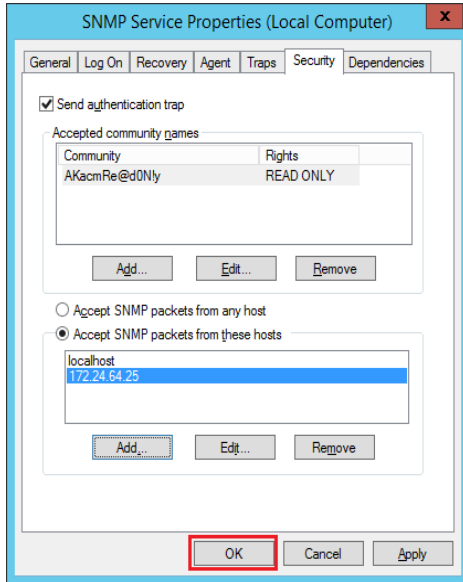
Configure the host IP address that the server will send its SNMP traps to. Click the second “Add...” button.



Enter the IP address of the SNMP server. In this case, enter “172.24.64.25” and click “Add”.



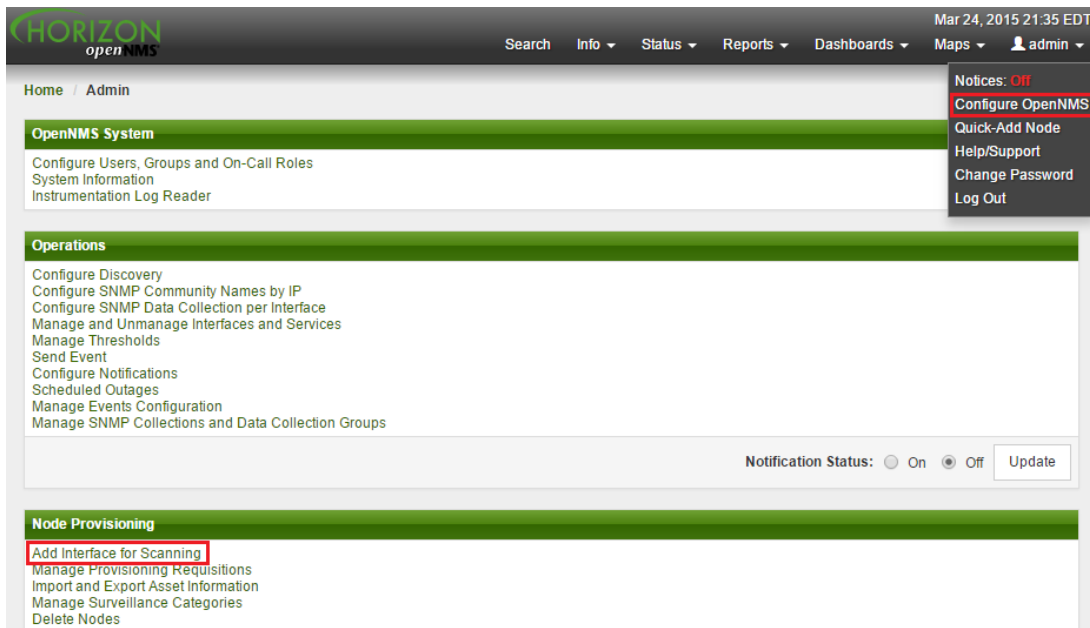
Complete the SNMP configuration by Clicking “OK”.



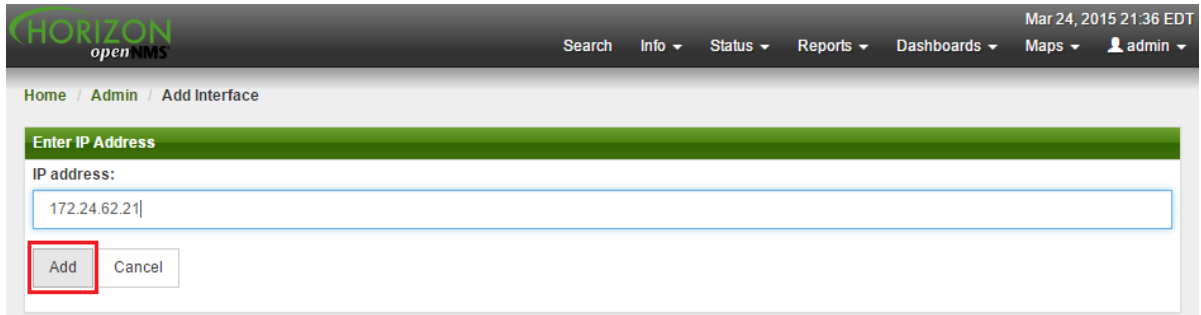
Configuration of SNMP for Windows Server 2012 R2 is complete.

### **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.

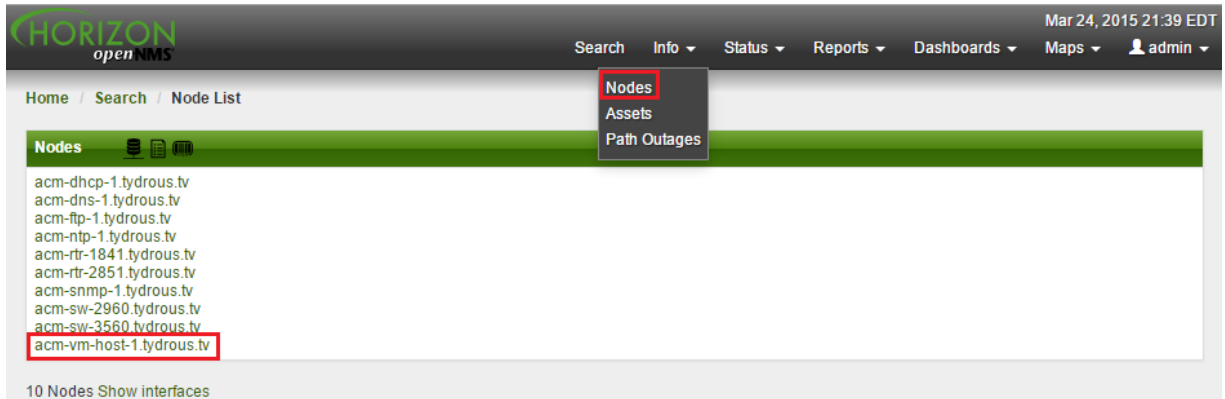


Type in the IP address of the device to add and click the “Add” button.



The screenshot shows the 'Add Interface' page in the OpenNMS web interface. The page title is 'Enter IP Address'. Below the title, there is a text input field labeled 'IP address:' containing the value '172.24.62.21'. Below the input field, there are two buttons: 'Add' and 'Cancel'. The 'Add' button is highlighted with a red rectangular box.

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



The screenshot shows the 'Node List' page in the OpenNMS web interface. The page title is 'Node List'. Below the title, there is a list of nodes. The 'Nodes' menu item in the top navigation bar is highlighted with a red rectangular box. The list of nodes includes:

- acm-dhcp-1.tydrous.tv
- acm-dns-1.tydrous.tv
- acm-fip-1.tydrous.tv
- acm-ntp-1.tydrous.tv
- acm-rtr-1841.tydrous.tv
- acm-rtr-2851.tydrous.tv
- acm-snmp-1.tydrous.tv
- acm-sw-2960.tydrous.tv
- acm-sw-3560.tydrous.tv
- acm-vm-host-1.tydrous.tv

The 'acm-vm-host-1.tydrous.tv' entry is highlighted with a red rectangular box. At the bottom of the page, it says '10 Nodes Show interfaces'.

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.

```
#####  
### MODULES ###  
#####  
  
$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  
#$ModLoad imtcp  
#$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:

```
$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.

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

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

```
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  2 root  root  4096 Feb  8 23:41 crash  
drwxr-xr-x 38 root  root  4096 Feb  8 23:43 lib  
drwxrwsr-x  2 root  staff 4096 Apr 10  2014 local  
lrwxrwxrwx  1 root  root   9 Feb  8 23:29 lock -> /run/lock  
drwxrwxr-x 10 syslog syslog 4096 Mar 25 19:49 log  
drwxrwsr-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  
drwxr-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:

```
sudo service rsyslog restart
```

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

Restart complete

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

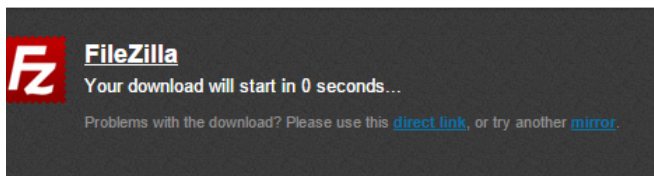




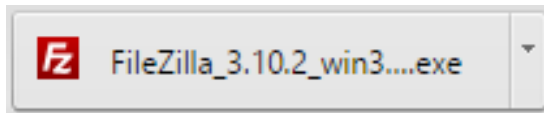
This will bring up different options other than the quick download option. Click on the .exe version of FileZilla.



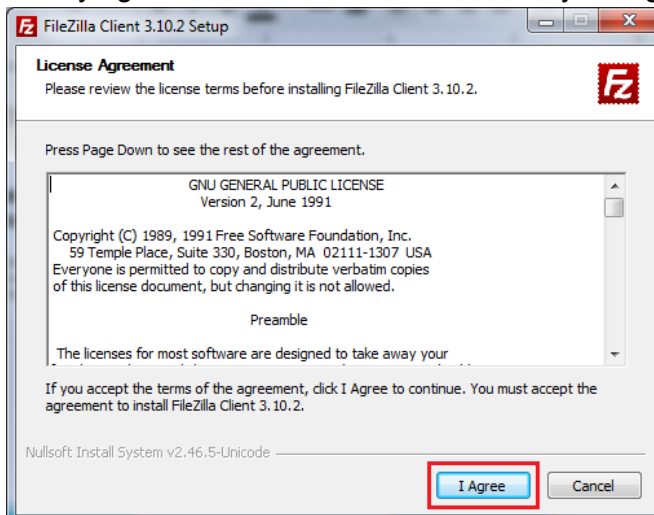
The download should start automatically after 5 seconds when the page loads. If not, click the “direct link” button.



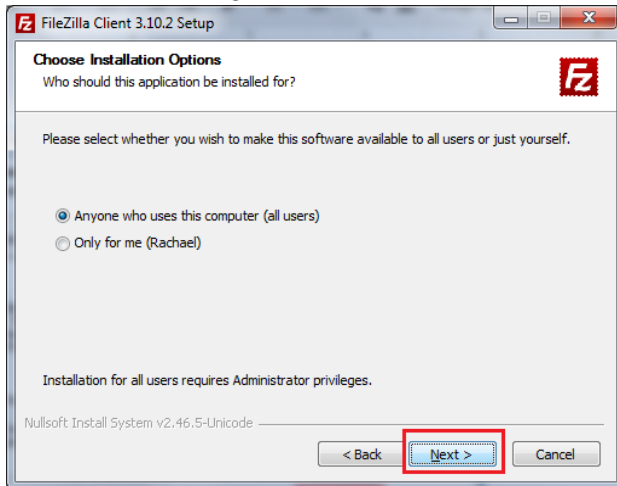
Run the installer after it finishes downloading.



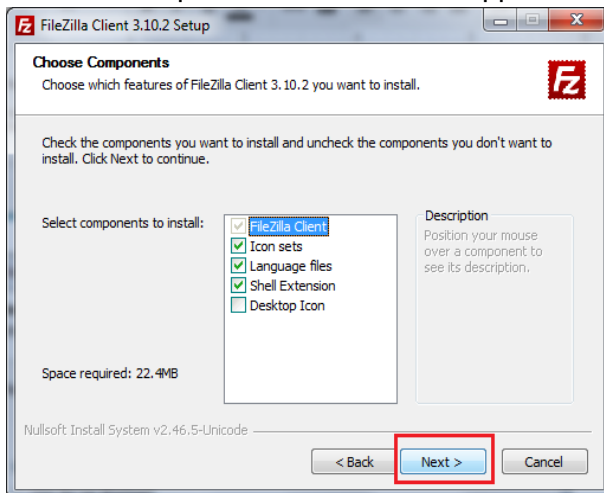
Blindly agree to the terms and conditions by hitting the “I Agree” button.



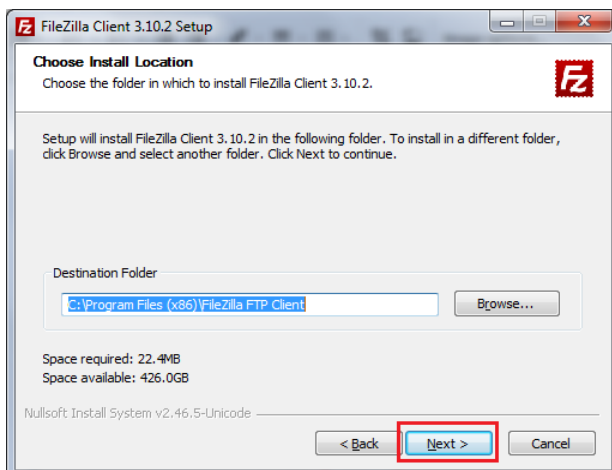
This can be a single user install or for all users on the machine.



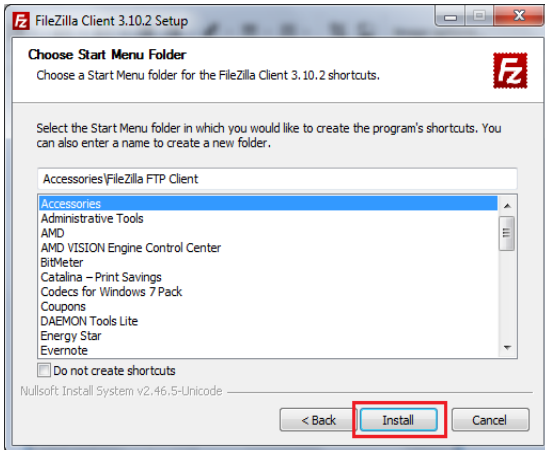
The default options are fine for this application of FileZilla. Click "Next" to continue.



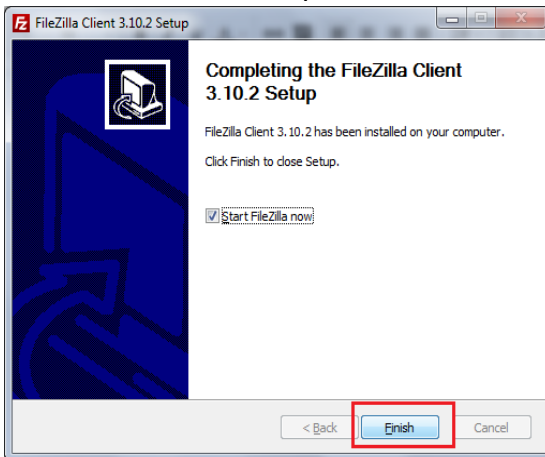
Here is where the installation path can be set. The default option is fine. Click "Next" to continue.



This is the final step before installation. A shortcut can be placed in the start menu under the specified folder. Click “Install” when finished.



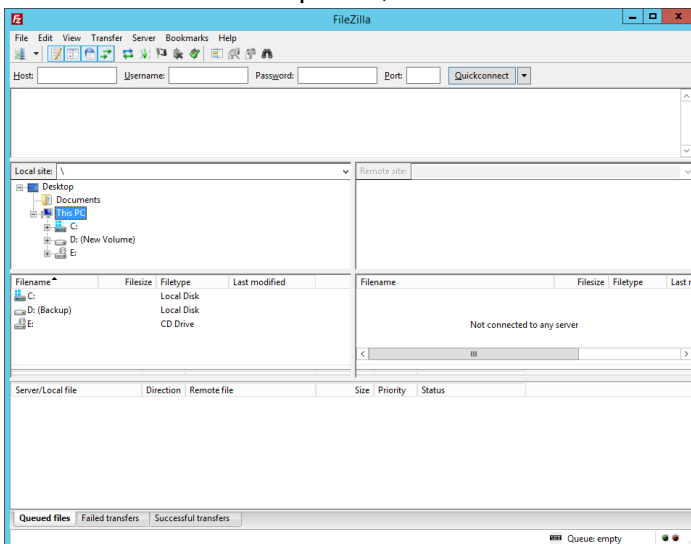
Click “Finished” to complete installation and launch FileZilla.



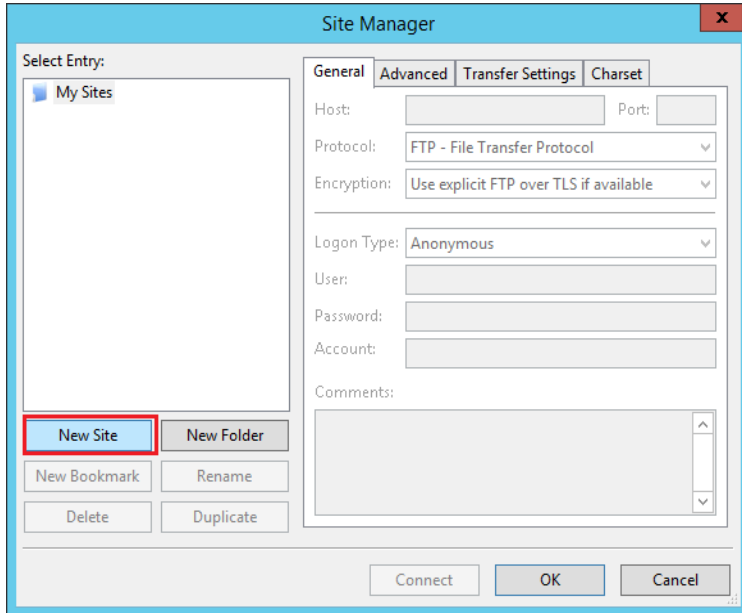
**Installation of FileZilla is complete.**

### **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:

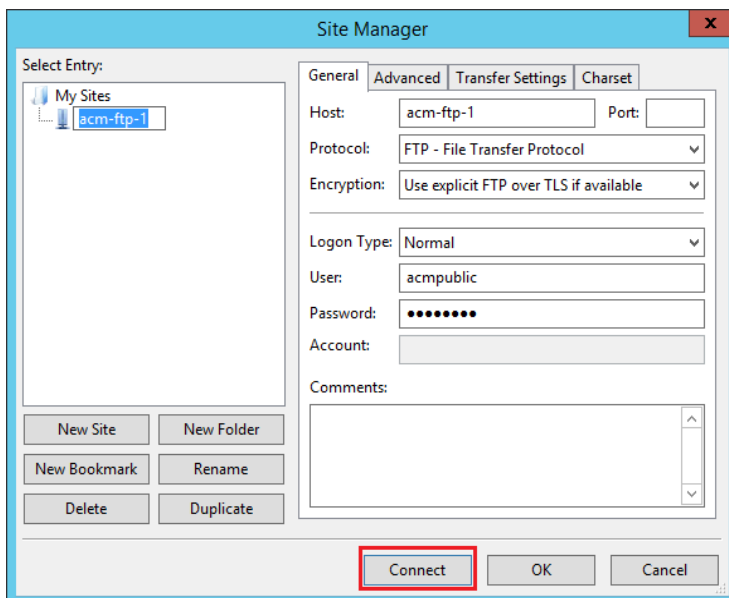
Host: acm-ftp-1

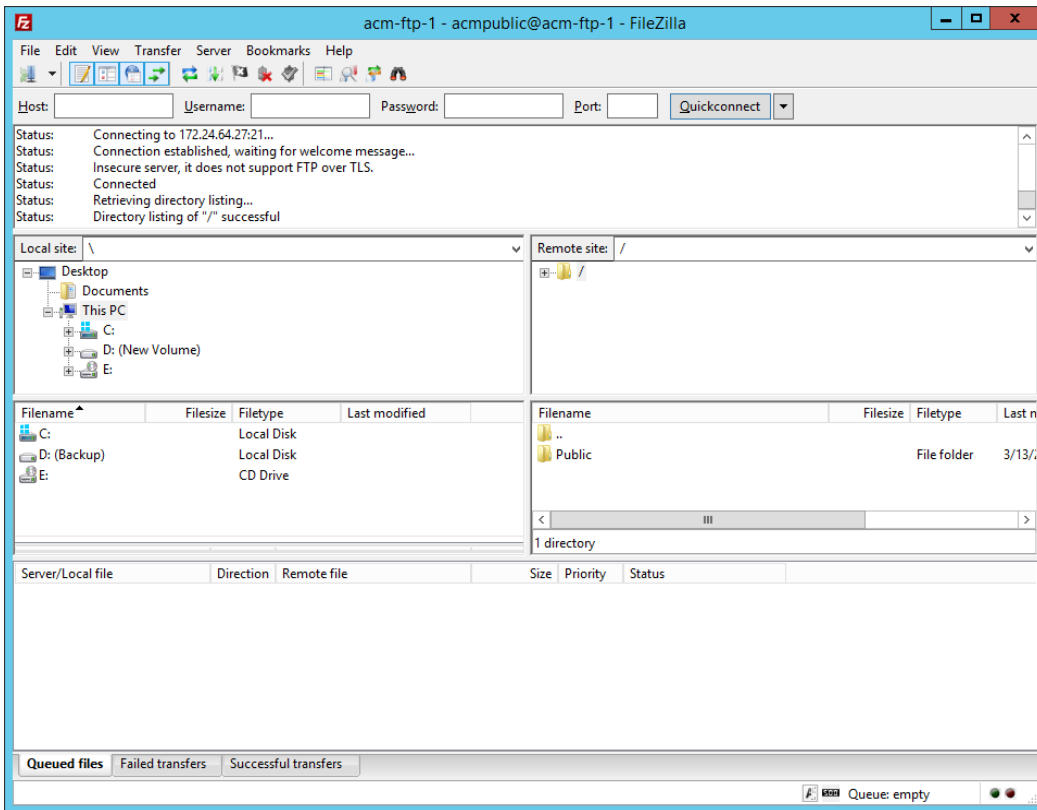
Logon Type: Normal

User: acmpublic

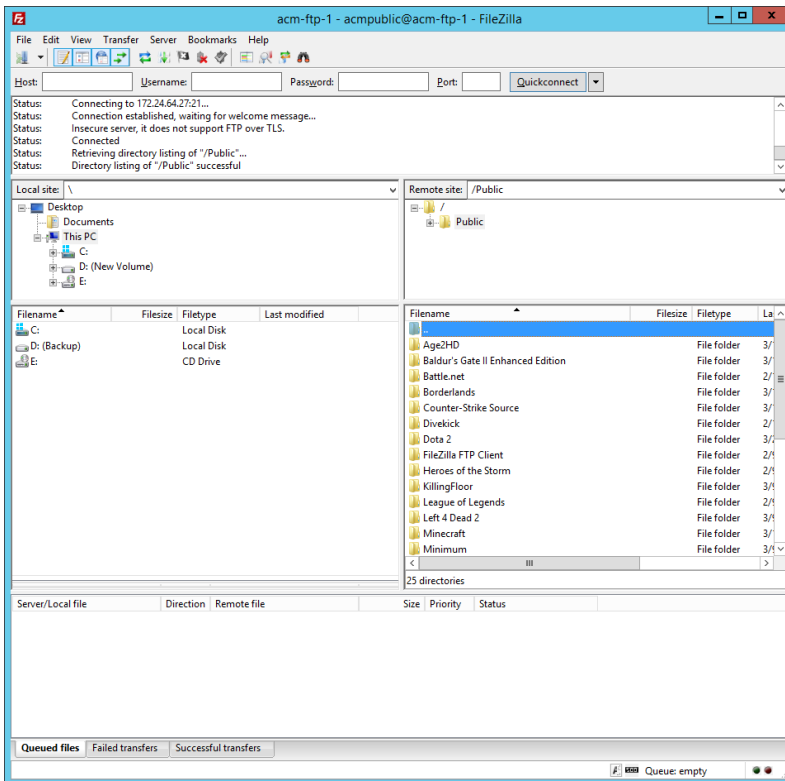
Password: ACMcp123

Select “Connect”.

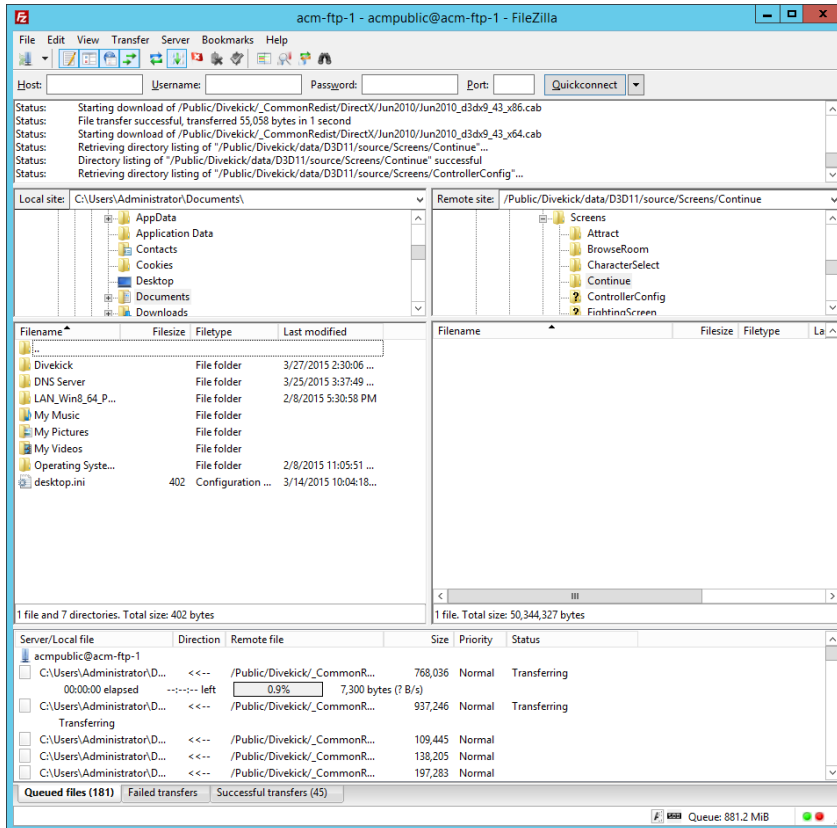




Game files are located in the Public folder:



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@d0N!y

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.tydrous.tv [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
```

```
C:\Users\Nick>ping 172.24.64.27
```

```
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
```

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.

```
C:\Users\Nick>ping google.com
```

```
Pinging google.com [216.58.216.206] with 32 bytes of data:
Reply from 216.58.216.206: bytes=32 time=33ms TTL=53
Reply from 216.58.216.206: bytes=32 time=34ms TTL=53
Reply from 216.58.216.206: bytes=32 time=32ms TTL=53
Reply from 216.58.216.206: bytes=32 time=33ms TTL=53
```

```
Ping statistics for 216.58.216.206:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 32ms, Maximum = 34ms, Average = 33ms
```

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:

```
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 08:2e:5f:81:25:33;
  uid "\001\010.\_ \201%3";
  client-hostname "Nadleeh";
}
```

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

```
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

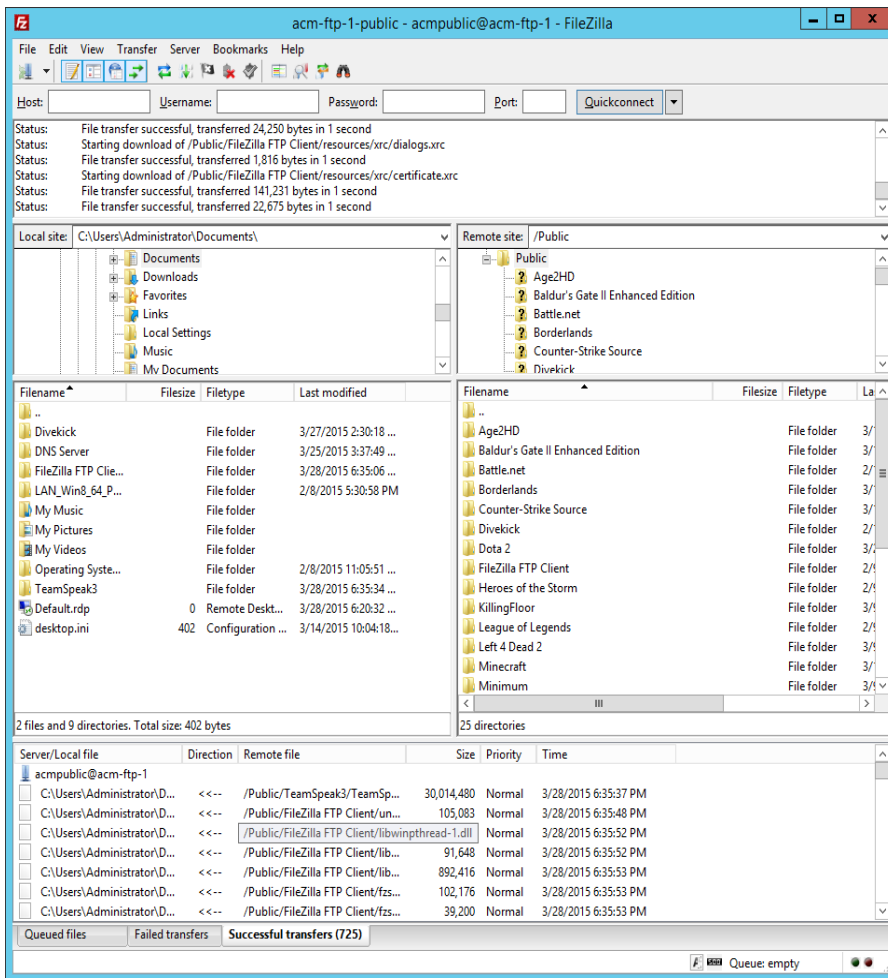
DNS Servers . . . . . : 172.24.64.22
NetBIOS over Tcpi. . . . . : Enabled
```

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

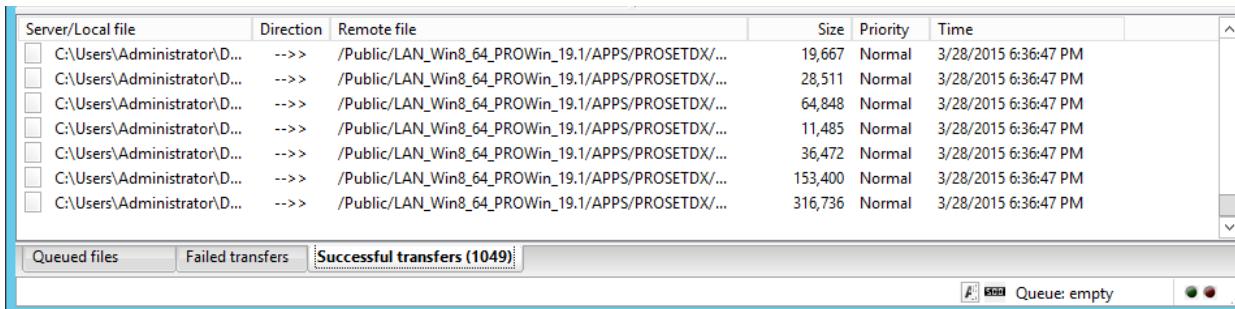
**Test successful.**

## 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.

```
acm-rtr-2851#wr
Building configuration...
[OK]
Writing archive/acm-rtr-2851/acm-rtr-2851-Mar-28-18:32:05-5 !
acm-rtr-2851#
```

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.

Event ID	Severity	Time	Source	Destination	Message
1582	Normal	Mar 28, 2015 6:45:24 PM	acm-rtr-2851.tydrous.tv	192.168.132.2	Linkd IpNetToMediaLinkDiscovery completed.
1581	Normal	Mar 28, 2015 6:45:21 PM	acm-rtr-2851.tydrous.tv	192.168.132.2	Linkd CdpLinksDiscovery completed.
1580	Normal	Mar 28, 2015 6:45:19 PM	acm-rtr-2851.tydrous.tv	192.168.132.2	Linkd BridgeLinkDiscovery completed.
1579	Normal	Mar 28, 2015 6:45:19 PM	acm-rtr-2851.tydrous.tv	192.168.132.2	Linkd IsisLinkDiscovery completed.
1578	Normal	Mar 28, 2015 6:45:19 PM	acm-rtr-2851.tydrous.tv	192.168.132.2	Linkd OspfLinkDiscovery completed.

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:

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

```
cisco@acm-syslog-1:~$ tail /var/log/remote-logs/acm-sw-2960.tydrous.tv.log
Mar 28 14:56:19 acm-sw-2960.tydrous.tv 78: Mar 28 15:57:08: %LINK-3-UPDOWN: Interface FastEthernet0/48, changed state to up
Mar 28 14:56:19 acm-sw-2960.tydrous.tv 79: Mar 28 15:57:09: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/48, changed state to up
Mar 28 15:08:11 acm-sw-2960.tydrous.tv 80: Mar 28 16:09:00: %LINK-3-UPDOWN: Interface FastEthernet0/48, changed state to down
Mar 28 15:08:12 acm-sw-2960.tydrous.tv 81: Mar 28 16:09:01: %LINK-3-UPDOWN: Interface FastEthernet0/48, changed state to down
Mar 28 15:45:58 acm-sw-2960.tydrous.tv 82: Mar 28 16:46:47: %LINK-3-UPDOWN: Interface FastEthernet0/48, changed state to up
Mar 28 15:45:58 acm-sw-2960.tydrous.tv 83: Mar 28 16:46:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/48, changed state to up
Mar 28 16:59:24 acm-sw-2960.tydrous.tv 84: Mar 28 18:00:14: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/48, changed state to down
Mar 28 16:59:25 acm-sw-2960.tydrous.tv 85: Mar 28 18:00:15: %LINK-3-UPDOWN: Interface FastEthernet0/48, changed state to down
Mar 28 16:59:29 acm-sw-2960.tydrous.tv 86: Mar 28 18:00:18: %LINK-3-UPDOWN: Interface FastEthernet0/28, changed state to up
Mar 28 16:59:29 acm-sw-2960.tydrous.tv 87: Mar 28 18:00:19: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/28, changed state to up
cisco@acm-syslog-1:~$
```

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.

```
acm-sw-2960#show ntp associations

address      ref clock      st  when  poll reach  delay  offset  disp
*~172.24.64.24  67.212.115.147  3   63   128  377   1.9   -0.01  0.1
* master (syncd), # master (unsyncd), + selected, - candidate, ~ configured
```

The Cisco switch has associated with the NTP server which is located at 172.24.64.24.

```
acm-sw-2960#show clock
19:47:12.187 US/EST Sat Mar 28 2015
```

The switch is also using the same time as the acm-ntp-1 server.

```
cisco@acm-ntp-1:~$ date
Sat Mar 28 19:47:12 EDT 2015
```

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

```
cisco@acm-ntp-1:~$ ntpq -np
=====
remote          refid           st t when poll reach  delay  offset  jitter
=====
-69.167.160.102 129.6.15.29    2 u 625 1024 377  41.786  4.009  0.611
-108.166.189.70 173.203.211.73 3 u 831 1024 377  55.949 -1.412  0.474
+173.230.144.178 193.190.230.65 2 u 651 1024 377  88.550  1.382  0.502
+204.2.134.164   187.253.153.32 2 u 656 1024 377  89.135  0.726  0.395
*67.212.115.147 192.168.101.60 2 u 36 1024 377  45.988  1.053  0.414
-173.255.230.140 200.98.196.212 2 u 784 1024 177  56.787  1.547  0.515
+66.175.216.101 173.234.66.27  2 u 678 1024 377  88.044  1.041  0.450
+204.2.134.163  187.253.153.32 2 u 934 1024 377  89.636  0.068  0.483
-91.189.94.4     192.93.2.20    2 u 808 1024 377  117.314 4.046  0.369
=====
```

**Test Successful.**

### Verification of network Services:

Routing tables:

```
acm-rtr-2851#show ip ro
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.1.254 to network 0.0.0.0

   192.168.132.0/32 is subnetted, 2 subnets
C       192.168.132.2 is directly connected, Loopback0
D       192.168.132.3
         [90/130816] via 192.168.128.3, 06:52:39, GigabitEthernet0/1.5
   172.20.0.0/19 is subnetted, 1 subnets
C       172.20.32.0 is directly connected, GigabitEthernet0/1.37
   172.24.0.0/20 is subnetted, 1 subnets
C       172.24.64.0 is directly connected, GigabitEthernet0/1.10
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
S*     0.0.0.0/0 [254/0] via 192.168.1.254
C       192.168.128.0/22 is directly connected, GigabitEthernet0/1.5
```

```
acm-rtr-1841#show ip ro
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.1.254 to network 0.0.0.0

   192.168.132.0/32 is subnetted, 2 subnets
D       192.168.132.2
         [90/156160] via 192.168.128.2, 06:53:35, FastEthernet0/1.5
C       192.168.132.3 is directly connected, Loopback0
   172.20.0.0/19 is subnetted, 1 subnets
C       172.20.32.0 is directly connected, FastEthernet0/1.37
   172.24.0.0/20 is subnetted, 1 subnets
C       172.24.64.0 is directly connected, FastEthernet0/1.10
C       192.168.1.0/24 is directly connected, FastEthernet0/0
S*     0.0.0.0/0 [254/0] via 192.168.1.254
C       192.168.128.0/22 is directly connected, FastEthernet0/1.5
```

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:

```
acm-rtr-1841#show glbp brief
Interface  Grp  Fwd Pri State      Address          Active router    Standby router
Fa0/1.5    5    -   130 Active    192.168.128.1   local            192.168.128.2
Fa0/1.5    5    1   -   Listen   0007.b400.0501  192.168.128.2   -
Fa0/1.5    5    2   -   Active   0007.b400.0502  local            -
Fa0/1.10   10   -   110 Standby   172.24.64.1     172.24.64.2     local
Fa0/1.10   10   1   -   Active   0007.b400.0a01  local            -
Fa0/1.10   10   2   -   Listen   0007.b400.0a02  172.24.64.2     -
Fa0/1.37   37   -   110 Standby   172.20.32.1     172.20.32.2     local
Fa0/1.37   37   1   -   Active   0007.b400.2501  local            -
Fa0/1.37   37   2   -   Listen   0007.b400.2502  172.20.32.2     -
```

```
acm-rtr-2851#show glbp brief
Interface  Grp  Fwd Pri State      Address          Active router    Standby route
Gi0/1.5    5    -   110 Standby   192.168.128.1   192.168.128.3   local
Gi0/1.5    5    1   7   Active   0007.b400.0501  local            -
Gi0/1.5    5    2   7   Listen   0007.b400.0502  192.168.128.3   -
Gi0/1.10   10   -   130 Active   172.24.64.1     local            172.24.64.3
Gi0/1.10   10   1   7   Listen   0007.b400.0a01  172.24.64.3     -
Gi0/1.10   10   2   7   Active   0007.b400.0a02  local            -
Gi0/1.37   37   -   130 Active   172.20.32.1     local            172.20.32.3
Gi0/1.37   37   1   7   Listen   0007.b400.2501  172.20.32.3     -
Gi0/1.37   37   2   7   Active   0007.b400.2502  local            -
```

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:

```
acm-rtr-1841#show ip eigrp ne
IP-EIGRP neighbors for process 373
H   Address          Interface          Hold Uptime      SRTT   RTO  Q  Seq
                               (sec)            (ms)          Cnt  Num
0   192.168.128.2     Fa0/1.5           12 06:59:14      6     200  0  15
acm-rtr-1841#

acm-rtr-2851#show ip eigrp ne
IP-EIGRP neighbors for process 373
H   Address          Interface          Hold Uptime      SRTT   RTO  Q  Seq
                               (sec)            (ms)          Cnt  Num
0   192.168.128.3     Gi0/1.5           14 06:59:00      3     300  0  16
acm-rtr-2851#
```

Both routers have each other as EIGRP neighbors.

```
acm-rtr-1841#show ip eigrp top
IP-EIGRP Topology Table for AS(373)/ID(192.168.132.3)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 172.20.32.0/19, 1 successors, FD is 28160
   via Connected, FastEthernet0/1.37
   via 192.168.128.2 (28416/2816), FastEthernet0/1.5
P 192.168.128.0/22, 1 successors, FD is 28160
   via Connected, FastEthernet0/1.5
P 192.168.132.2/32, 1 successors, FD is 156160
   via 192.168.128.2 (156160/128256), FastEthernet0/1.5
P 192.168.132.3/32, 1 successors, FD is 128256
   via Connected, Loopback0
P 172.24.64.0/20, 1 successors, FD is 28160
   via Connected, FastEthernet0/1.10
   via 192.168.128.2 (28416/2816), FastEthernet0/1.5
acm-rtr-1841#
```

```
acm-rtr-2851#show ip eigrp topology
IP-EIGRP Topology Table for AS(373)/ID(192.168.132.2)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 172.20.32.0/19, 1 successors, FD is 2816
   via Connected, GigabitEthernet0/1.37
P 192.168.128.0/22, 1 successors, FD is 2816
   via Connected, GigabitEthernet0/1.5
P 192.168.132.2/32, 1 successors, FD is 128256
   via Connected, Loopback0
P 192.168.132.3/32, 1 successors, FD is 130816
   via 192.168.128.3 (130816/128256), GigabitEthernet0/1.5
P 172.24.64.0/20, 1 successors, FD is 2816
   via Connected, GigabitEthernet0/1.10
acm-rtr-2851#
```

Both routers are receiving all the routes for the internal subnets.

# Project Weekly Journals

Nicholas Bordo

**Name(s): Nicholas Bordo**

**Summary – Week ending:**

Date	Start Time	End Time	Description	Total Hours
1/26/2015	13:30	16:30	Connection and installation of networking devices.	3
1/28/2015	14:00	15:00	Configuration of network devices	1
1/30/2015	14:00	16:00	Research on FTP Server	2
			<b>Total Hours This Week</b>	<b>6</b>
			<b>Total Hours to Date</b>	

## **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:**

Date	Start Time	End Time	Description	Total Hours
2/2/2015	12:30	17:30	Continued configuring network devices/Networking Research	5
2/3/2015	19:00	22:00	FTP Server Research/configuration testing	3
2/4/2015	14:00	18:00	Research on FTP Server/configuration testing	4
2/5/2015	19:00	23:00	Configuration Testing for ftp server	4
2/6/2015	12:00	18:00	IP address redesign/FTP server OS install and Config	6
2/7/2015	12:00	16:00	Windows Server 2012 R2 install	4
			<b>Total Hours This Week</b>	<b>26</b>
			<b>Total Hours to Date</b>	

**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
  - Verified end to end connectivity from test host to ftp server
- Used test host to connect to FTP server
  - Successfully connected, but permissions configured on FTP server need to be modified

#### 2/7/2015

- Installed Windows Server 2012 R2 using Dreamspark download
  - Installed on second dedicated server
  - Ran into issues where network adapter was not detected by the driver installation software
- Researched solutions to network adapter problem
  - Found solution and applied the fix and installed the driver
  - Documented steps used to install driver on machine
- Installed Hyper-V Role
  - Installed the Hyper-V role on machine
  - 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:**

Date	Start Time	End Time	Description	Total Hours
2/9/2015	12:30	18:30	Completed FTP Server setup/Device configuration for Archive	6
2/10/2015	19:00	22:00	DHCP Server research and configuration	3
2/11/2015	14:00	18:00	Configuration/Testing of DHCP Server	4
2/12/2015	19:00	22:00	Research on SNMP Server	3
2/13/2015	12:00	15:00	Installation of SNMP Server on Virtual Machine	3
2/15/2015	12:00	16:00	Configuration and research of network device SNMP config	4
			<b>Total Hours This Week</b>	<b>23</b>
			<b>Total Hours to Date</b>	

**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:**

Date	Start Time	End Time	Description	Total Hours
2/16/2015	12:30	17:30	Research/test of DNS server and Research for SNMP config	5
2/17/2015	19:00	22:00	SNMP server setup research	3
2/22/2015	12:00	16:00	Configuration of SNMP server GUI	4
			<b>Total Hours This Week</b>	<b>12</b>
			<b>Total Hours to Date</b>	

**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:**

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

**Journal Details (sample)**

2/23/2015

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

2/28/2015

- o 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
      - o Trouble shot that issue and partially resolved it. Still having some latency issues.
      - o 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

- o 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
- o Began work on NTP server
  - Researched setup process for NTP
  - Did test installation
  - Successfully peered NTP server with internet NTP time sources
  - Configured clients, servers, and network devices to use internal NTP server.
- o 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:**

Date	Start Time	End Time	Description	Total Hours
3/2/2015	13:00	20:00	Troubleshooting Network issues & documentation of project	7
3/4/2015	17:00	19:00	Worked on documentation	2
			<b>Total Hours This Week</b>	<b>9</b>
			<b>Total Hours to Date</b>	

**Journal Details (sample)**

3/2/2015

- o 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.
      - o 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.
      - o 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
      - o Once the static default route was removed all connection issues were resolved.
- o 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:**

Date	Start Time	End Time	Description	Total Hours
3/10/2015	19:00	4:00	Troubleshooting slow DNS query response	9
3/12/2015	19:00	2:00	Troubleshooting DNS reverse lookup	7
3/13/2015	16:00	20:00	Worked on DNS cleanup and documentation	4
3/14/2015	20:00	23:00	Testing	2
3/15/2015	12:00	18:00	Testing and documentation	6
			<b>Total Hours This Week</b>	<b>28</b>
			<b>Total Hours to Date</b>	

**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:**

Date	Start Time	End Time	Description	Total Hours
3/16/2015	19:00	22:00	Worked on documentation and testing	3
			<b>Total Hours This Week</b>	<b>3</b>
			<b>Total Hours to Date</b>	

**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:**

<b>Date</b>	<b>Start Time</b>	<b>End Time</b>	<b>Description</b>	<b>Total Hours</b>
3/23/2015	12:00	20:00	Worked on documentation and binder	8
3/24/2015	17:00	23:00	Worked on documentation and binder	6
3/25/2015	12:00	22:00	Worked on documentation and binder	10
3/26/2015	15:00	22:00	Worked on documentation and binder	7
3/27/2015	10:00	20:00	Worked on documentation and binder	10
3/28/2015	11:00	20:00	Worked on documentation and binder	9
3/29/2015	12:00	21:00	Worked on documentation and binder	9
			<b>Total Hours This Week</b>	<b>59</b>
			<b>Total Hours to Date</b>	

# Research References

Nicholas Bordo

Admin. "Rsyslog." Rsyslog. N.p., 1 June 2010. Web. 27 Mar. 2015.

<<http://www.rsyslog.com/article60/>>

Anicas, Mitchell. "How To Configure BIND as a Private Network DNS Server on Ubuntu 14.04 | DigitalOcean." How To Configure BIND as a Private Network DNS Server on Ubuntu 14.04 | DigitalOcean. N.p., 12 Aug. 2014. Web. 27 Mar. 2015.

<<https://www.digitalocean.com/community/tutorials/how-to-configure-bind-as-a-private-network-dns-server-on-ubuntu-14-04>>

Bainbridge, Chris. "Installation/SoftwareRAID." Ubuntu Documentation. N.p., 27 Mar. 2015.

Web. 27 Mar. 2015. <<https://help.ubuntu.com/community/Installation/SoftwareRAID>>.

Bourdeau, Julian. "Setup VSFTPD with Custom Multiple Directories and (virtual) Users Accounts on Ubuntu (no Database Required)." Sigerr. N.p., 3 June 2013. Web. 27 Mar. 2015.

<<http://www.sigerr.org/linux/setup-vsftpd-custom-multiple-directories-users-accounts-ubuntu-step-by-step/>>.

Braiam. "How Do I Do a Complete BIND9 DNS Server Configuration with a Hostname?"

Askubuntu.com. N.p., 31 Jan. 2014. Web. 27 Mar. 2015.

<<http://askubuntu.com/questions/330148/how-do-i-do-a-complete-bind9-dns-server-configuration-with-a-hostname>>

"Catalyst 2960-X Switch Network Management Command Reference, Cisco IOS Release 15.0(2)EX - Network Management Commands [Cisco Catalyst 2960-X Series Switches]." Cisco. Cisco, n.d. Web. 28 Mar. 2015.

<[http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0\\_2\\_EX/network\\_management/command\\_reference/b\\_nm\\_15ex\\_2960-x\\_cr/b\\_nm\\_15ex\\_2960-x\\_cr\\_chapter\\_010.html](http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/network_management/command_reference/b_nm_15ex_2960-x_cr/b_nm_15ex_2960-x_cr_chapter_010.html)>.

"Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 - SNMP

Commands [Cisco IOS Software Release 12.2]." Cisco. Cisco, 27 June 2007. Web. 28 Mar. 2015.

<[http://www.cisco.com/c/en/us/td/docs/ios/12\\_2/configfun/command/reference/ffun\\_r/frf014.html#wp1134024](http://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/command/reference/ffun_r/frf014.html#wp1134024)>.

Danscourses. "Install and Configure a DHCP Server in Ubuntu 11.10." YouTube. YouTube, 16

Apr. 2012. Web. 27 Mar. 2015.

<<https://www.youtube.com/watch?v=9Vc6-0smd64>>

"DNS Reverse Mapping." Zytrax. Zytrax, 1 Oct. 2014. Web. 27 Mar. 2015.

<<http://www.zytrax.com/books/dns/ch3/>>

Dsmythies. "BIND9ServerHowto." *Ubuntu.com*. N.p., 22 Feb. 2013. Web. 27 Mar. 2015  
<<https://help.ubuntu.com/community/BIND9ServerHowto>>

Feleol, Alex. "SNMP No Windows Server 2012 R2." YouTube. YouTube, 3 Apr. 2014. Web. 27 Mar. 2015. <<https://www.youtube.com/watch?v=4M8kXS-BgyE>>.

"GLBP - Gateway Load Balancing Protocol." Cisco. Cisco, n.d. Web. 28 Mar. 2015.  
<[http://www.cisco.com/en/US/docs/ios/12\\_2t/12\\_2t15/feature/guide/ft\\_glbp.html](http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_glbp.html)>.

Hillcoat, Robert. "Cisco IOS Archive." Web log post. *Allthingsnetworking*. N.p., 29 May 2013. Web. 28 Mar. 2015. <<https://allthingsnetworking.wordpress.com/2013/05/29/cisco-ios-archive/>>.

Indigo. "OpenNMS in 8 Minutes ..." Vimeo. Vimeo, 2009. Web. 27 Mar. 2015.  
<<https://vimeo.com/3745873>>.

"InstallingANewHardDrive." Ubuntu Documentation. N.p., 14 Dec. 2013. Web. 27 Mar. 2015.  
<<https://help.ubuntu.com/community/InstallingANewHardDrive>>.

Malhoit, Lauren. "How to Create an FTP Server on an Ubuntu 12.04 Virtual Machine." TechRepublic. N.p., 14 Aug. 2012. Web. 27 Mar. 2015.  
<<http://www.techrepublic.com/blog/smb-technologist/how-to-create-an-ftp-server-on-an-ubuntu-1204-virtual-machine/>>

NIXCRAFT. "Linux Force DHCP Client (dhclient) to Renew IP Address." Linux Unix Tutorial for Beginners and Advanced Users NixCraft RSS. N.p., 15 Nov. 2007. Web. 27 Mar. 2015.  
<<http://www.cyberciti.biz/faq/howto-linux-renew-dhcp-client-ip-address/>>

Pakpahan, Andrew. "How to Enable SNMP Monitoring on Ubuntu Server 12.04.2." Web log post. : How to Enable SNMP Monitoring on Ubuntu Server 12.04.2. N.p., 22 Sept. 2012. Web. 27 Mar. 2015. <<http://andrewpakpahan.blogspot.com/2012/09/how-to-enable-snmp-monitoring-on-ubuntu.html>>

Pepelnjak, Ivan. "DHCP Response Sets the Default Route « IpSpace.net." Web log post. *IpSpace*. N.p., 5 June 2005. Web. 28 Mar. 2015. <<http://blog.ipSPACE.net/2007/06/dhcp-response-sets-default-route.html>>

"Quick HOWTO : Ch08 : Configuring the DHCP Server." Linux Home Networking. N.p., 22 July 2012. Web. 27 Mar. 2015.  
<[http://www.linuxhomenetworking.com/wiki/index.php/Quick\\_HOWTO:\\_Ch08:\\_Configuring\\_the\\_DHCP\\_Server#.VP3BH\\_nF-Sp](http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO:_Ch08:_Configuring_the_DHCP_Server#.VP3BH_nF-Sp)>

Ruchi. "Network Time Protocol (NTP) Server and Clients Setup in Ubuntu." Ubuntu Geek. N.p., 5 Aug. 2008. Web. 27 Mar. 2015.

<<http://www.ubuntugeek.com/network-time-protocol-ntp-server-and-clients-setup-in-ubuntu.html>>

SAIVE, RAVI. "Protect SSH Logins with SSH & MOTD Banner Messages." Tecmint Linux Howtos Tutorials Guides. N.p., 20 Nov. 2012. Web. 27 Mar. 2015.

<<http://www.tecmint.com/protect-ssh-logins-with-ssh-motd-banner-messages/>>

TCC\_2. "Cisco Support Community." *Router Log Timestamp Entries Are Different from the System Clock When the NTP Is Configure*. Cisco, 28 Oct. 2014. Web. 28 Mar. 2015.

<<https://supportforums.cisco.com/document/24156/router-log-timestamp-entries-are-different-system-clock-when-ntp-configure>>.

"Tutorial Introduction." - OpenNMS. N.p., 4 Mar. 2012. Web. 27 Mar. 2015.

<[http://www.opennms.org/wiki/Tutorial\\_Introduction](http://www.opennms.org/wiki/Tutorial_Introduction)>.

VDevices. "DigitalOcean-User-Projects/Articles-and-Tutorials." GitHub. N.p., 12 Nov. 2013. Web. 27 Mar. 2015.

<[https://github.com/DigitalOcean-User-Projects/Articles-and-Tutorials/blob/master/set\\_hostname\\_fqdn\\_on\\_ubuntu\\_centos.md](https://github.com/DigitalOcean-User-Projects/Articles-and-Tutorials/blob/master/set_hostname_fqdn_on_ubuntu_centos.md)>

Will224. "Configure Ubuntu Server 12.04 LTS as a Syslog Server." *Spiceworks Community Global*. N.p., 23 Jan. 2014. Web. 27 Mar. 2015.

<[http://community.spiceworks.com/how\\_to/65683-configure-ubuntu-server-12-04-lts-as-a-syslog-server](http://community.spiceworks.com/how_to/65683-configure-ubuntu-server-12-04-lts-as-a-syslog-server)>.