Lab – Preparing Your Network for Active Directory

Overview

In this lab, you will lay out the design for your network, learn the importance of having a good naming convention and how to correctly configure an IP addressing scheme for your network.

Virtual lab design

1. One virtual install of server 2012 full, 2016 full or 2019 full.
2. One virtual installer server 2012 core, 2016 core or 2019 core.
3. One virtual install of Windows 10 capable of joining a domain.
4. Additional machine may be required for some labs

Regardless if your network has three devices or 20 devices, how you design the network will determine how well it performs, how long it will last and how easy it is to troubleshoot.

The first machine up on your network should be your forest root. This is the first domain controller in the forest. As with most small to medium-sized networks, we will be using the single domain model.

A single domain forest model reduces administrative complexity by providing the following advantages:

- Any domain controller can authenticate any user in the forest.
- All domain controllers can be global catalogs, so you do not need to plan for global catalog server placement.

We will be creating a Microsoft domain forest using a single domain controller but before we get to that part, we first need to first design a naming convention and IP scheme for our network.

The one cardinal rule to designing a network is to keep it simple. Be sure to plan for growth and that your network will last somewhere between five and seven years.

Choose the right domain name

You should NOT name your domain based on something that will change or become outdated. Examples include naming your domain after a product line, operating system, or anything else likely to change over time. Stick with something that make will still make sense 5 or even 10 years down the road.

Stick with short names of 15 characters or less, this will allow for the NETBIOS name to easily be the same as the domain name.

Every device on your domain will have two names: a domain name and a NETBIOS name. Some older operating systems and software use NetBIOS names to locate each other on the network.

Think long term as much as possible.

Alternatives to .Local

There's a lot of debate on how to properly name an internal network. If you're creating a testing environment such as we are, then using .local is fine but there is an RFC 2606 that has top-level domains (TLDs) reserved just for testing purposes.

The popular consensus is to avoid using .local for any production network and for your testing lab environment, you can use one the following reserved under RFC 2606.

.test
.example
.invalid
.localhost

As you can see from the names, these were created for testing and not for production and that is a primary consideration when choosing whether to use one of these reserved top-level domain names. Again, these would not be used to name a production network.

For production networks you are strongly advised to reserve your own domain name on the Internet, even if you are not planning on using it soon. This will ensure there will be no conflicts later with another business on the Internet wanting to use the same domain name.

Once you have your registered ICANN domain name, you can add a prefix to it to create a

subdomain that is not registered on the Internet.

You could use your registered external domain name internally, but this creates management issues and requires the use of two different DNS servers.

1. Internal DNS -- contains records for the internal servers mapped to internal addresses
2. External DNS -- mapped to public addresses (Split Horizon DNS)

Not recommended.

The Solution: Using Subdomains

Using your registered external domain name and prefixing it with a subdomain name is considered best practices by Microsoft and the industry.

A subdomain name can be based on location or function though there may be other criteria.

I have registered the domain name of syberoffense.com. Internally, I would create a subdomain based on one of the two is previously mentioned criteria.

If I use location, my internal network could be called, us.syberoffense.com

When using location for your subdomain name, you could use the subdomain of **asia** to represent a global presence, **asia.syberoffense.com** or you could prefix your external domain name using the name of a city or town the organization resides in such as, **tucson.syberoffense.com** if I based the subdomain on function my internal network could be called, **lab.syberoffense.com**

Location and function are the two primary naming conventions we use.

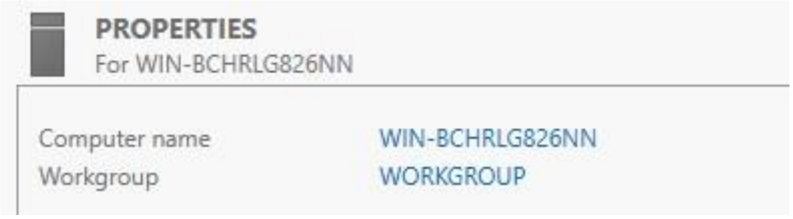
Choose your forest domain name:______________________

Choose a subdomain prefix________________________

The last thing you want to have to do is to rename an existing production domain so make sure you give this ample thought and do it right the first time.

The second part of any naming convention deals with how you will identify devices on your network. By default, Microsoft will give each host on the network a unique name, but this name is not conducive to good network management nor does it ease having to find and troubleshoot problem devices.

Right now, my primary domain controller has a default name given to it during the install.



PROPERTIES
For WIN-BCHRLG826NN

Computer name WIN-BCHRLG826NN
Workgroup WORKGROUP

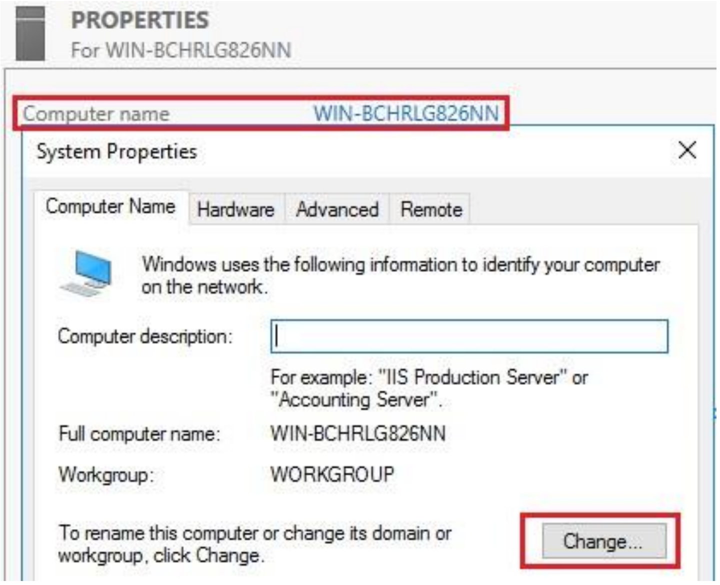
What you must remember is regardless of what I rename this machine, that name will be prefixed to the name given to the domain. This ends up being the fully qualified domain name (FQDN) for the device. The way I identify domain controllers is by prefixing them with the name, DC1, DC2 and so on. I know that when I see the name DC1 this is my forest root. DC2 would be replica or backup of the forest root if I had one.

Video Tutorial for This Lab Begins Here!

I can now rename this server to DC1 to prepare it for promotion as my forest root.

Using Server Manager, renaming a server is as easy as clicking on the current name with your left mouse button to bring up the System Properties dialog box, clicking on the change button and typing in the new name.

Left click on the name of the Server. Click the change button.



PROPERTIES
For WIN-BCHRLG826NN

Computer name WIN-BCHRLG826NN

System Properties

Windows uses the following information to identify your computer on the network.

Computer description:

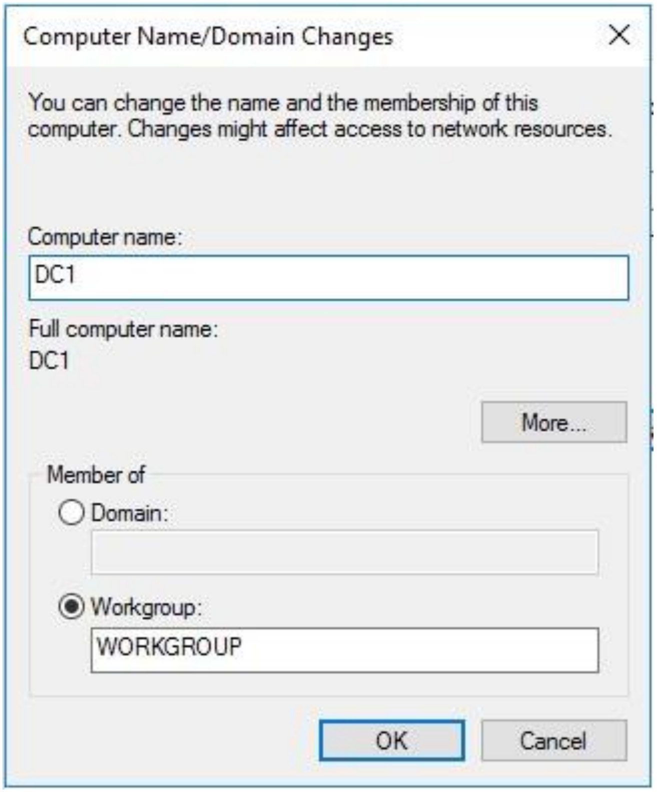
For example: "IIS Production Server" or "Accounting Server".

Full computer name: WIN-BCHRLG826NN

Workgroup: WORKGROUP

To rename this computer or change its domain or workgroup, click Change.

On the next, in the text box marked, Computer Name, type in the new name for the server. Press OK. Restart for the change to take effect.



Computer Name/Domain Changes

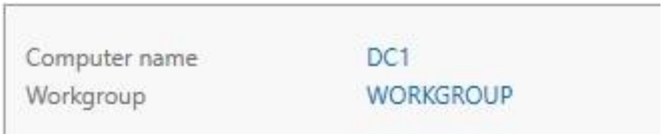
You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name:
DC1

Full computer name:
DC1

Member of
○ Domain:
● Workgroup:
WORKGROUP

Once our server is back up, we can go into server manager and once it has refreshed, from the left window pane if we click on a local server we can see that our name change has taken effect.



Computer name	DC1
Workgroup	WORKGROUP

Designing an IP Addressing Scheme for Your Network

when it comes to networking and working with Microsoft domains and IP addressing, two things we don’t want to have happen, we don’t want to have to rename the domain and secondly, we don’t want to have to redo our IP scheme.

This does happen but there are ways to prevent it. The first is to ensure that you have buy-in from the management and they approve of both your naming convention and your IP addressing scheme.

Having multiple eyes on the target is never a bad thing. You would do well to remember that if you touch it you own it so get it right the first time.

In this example I have a small to medium size network and I have identified all the devices that will need IP addressing.

I have one firewall, one switch, to servers and 25 workstations all running Windows 10 professional.

I have planned and included ample room for growth into this IP scheme. The network should last somewhere between five and seven years as should my IP addressing scheme.

Here’s how I have broken down and allocated my IP addressing scheme for this network:

Network IP Addressing Scheme for us.syberoffense.com

Network IP address:

192.168.145.0 Subnet mask:

255.255.255.0 default gateway:

192.168.145.1

Available hosts: 254 IP

Reservations:

.1-.9 Networking Devices:

.1 – Firewall (Default Gateway) Assigned to the inside or LAN Interface of the device.

.2-9 can be used for switches and the IDS/IPS.

Servers: .10 -.19

Printers: .20 - .29

Hosts: .30 -254

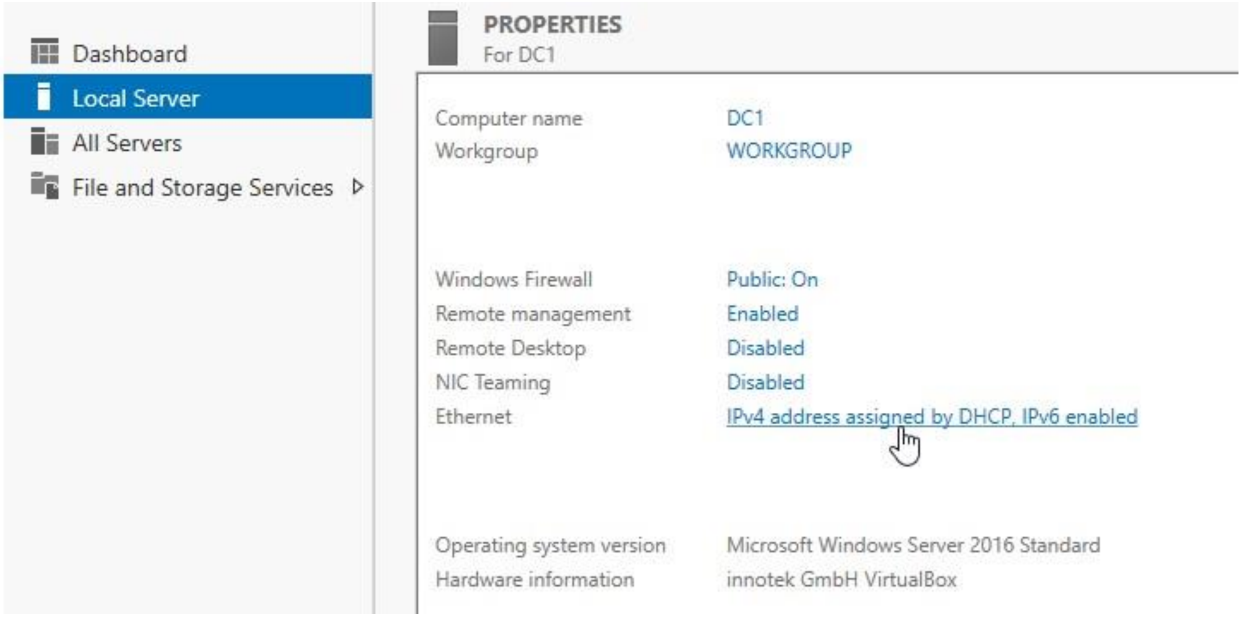
Because I could, I gave myself plenty of room for growth in each of the areas where I reserved a block of IP addresses. You can reserve the blocks from your IP addressing scheme the way you best see fit, this is just an example.

Configuring the Forest Root with A Static IP Address

Since our forest root will need to be found always by all the other devices on the network, we need to configure it with a static IP address so that its IP address never changes. Before you can promote this machine to a domain controller or install DNS it will require the same.

Using server manager, we go to the left window pane and we click on local server. This brings up the properties of DC1.

Inside the center window pane, we scroll down until we come to where it says ethernet.



PROPERTIES
For DC1

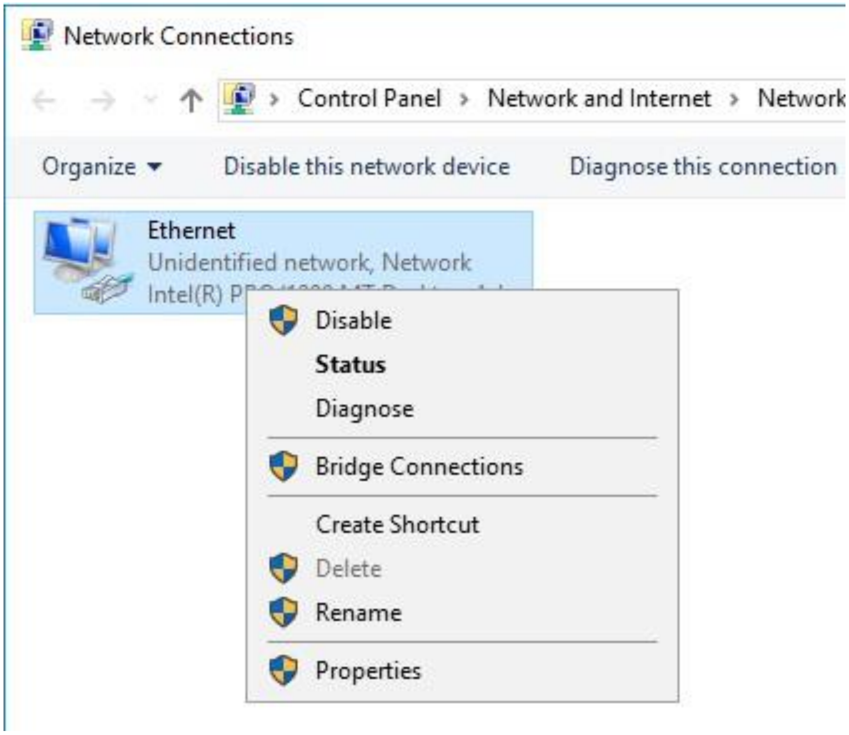
Computer name DC1
Workgroup WORKGROUP

Windows Firewall Public: On
Remote management Enabled
Remote Desktop Disabled
NIC Teaming Disabled
Ethernet IPv4 address assigned by DHCP, IPv6 enabled

Operating system version Microsoft Windows Server 2016 Standard
Hardware information innotek GmbH VirtualBox

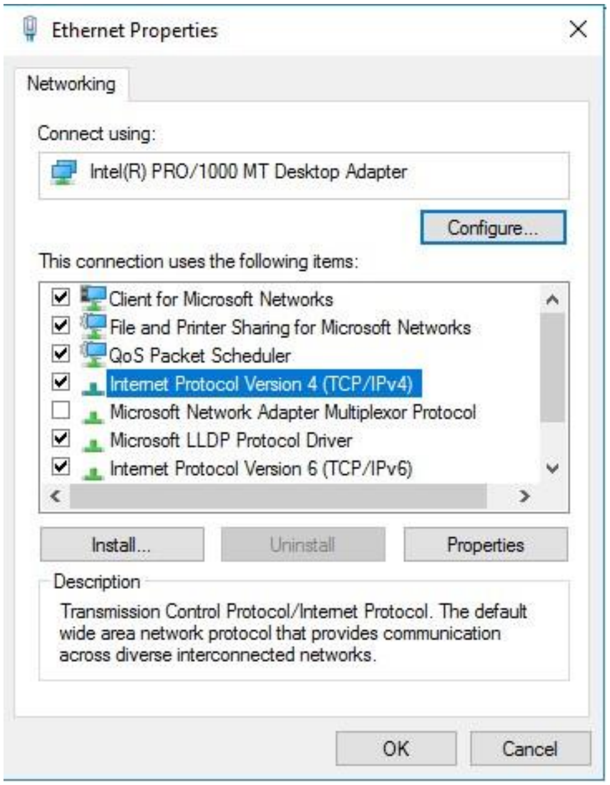
We shipped our mouse over to the second calm and using our left mouse button, we click where it says IPv4 address assigned by DHCP, IPv6 enabled. This brings up our networking connections.

Right-click on your ethernet adapter, and from the context menu select properties.



This brings up the ethernet properties for your networking adapter.

Inside the window pane, select the option for, **Internet Protocol Version 4 (TCP/IPv4)**.



Connect using:

Intel(R) PRO/1000 MT Desktop Adapter

This connection uses the following items:

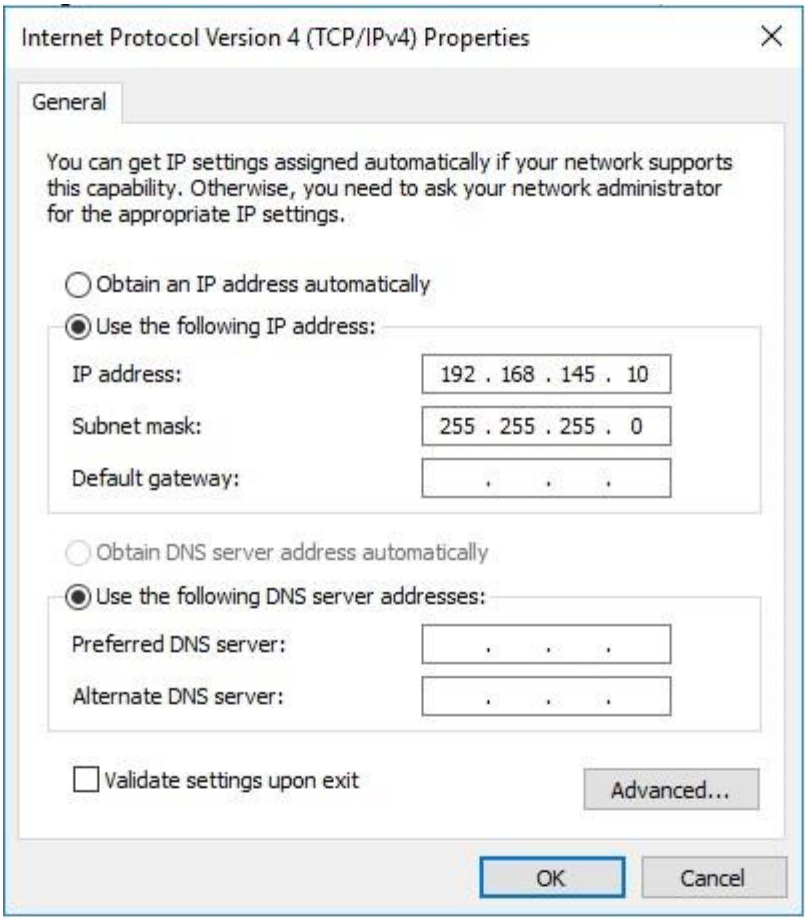
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

This brings up the TCP/IP properties window for IPv4. Click on a radio button next to, use the following IP address:

Each block of the IP address is referred to as an octet. The first three octets of a class C network represent the networking portion of the IP address. The fourth or the last octet, represents the host IP assigned to the device. In this example, I have assigned the first available IP address from the block of IP's I reserved for my servers. Once I've typed in the host IP in the last octet, I can use the tab to the to fill in the information for the subnet mask. We don't need worry about the default gateway or the IP information for the DNS server. Once this machine becomes the DNS server for the domain, it will assign itself a loopback address of 127.0.0.1 for the preferred DNS server.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 145 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

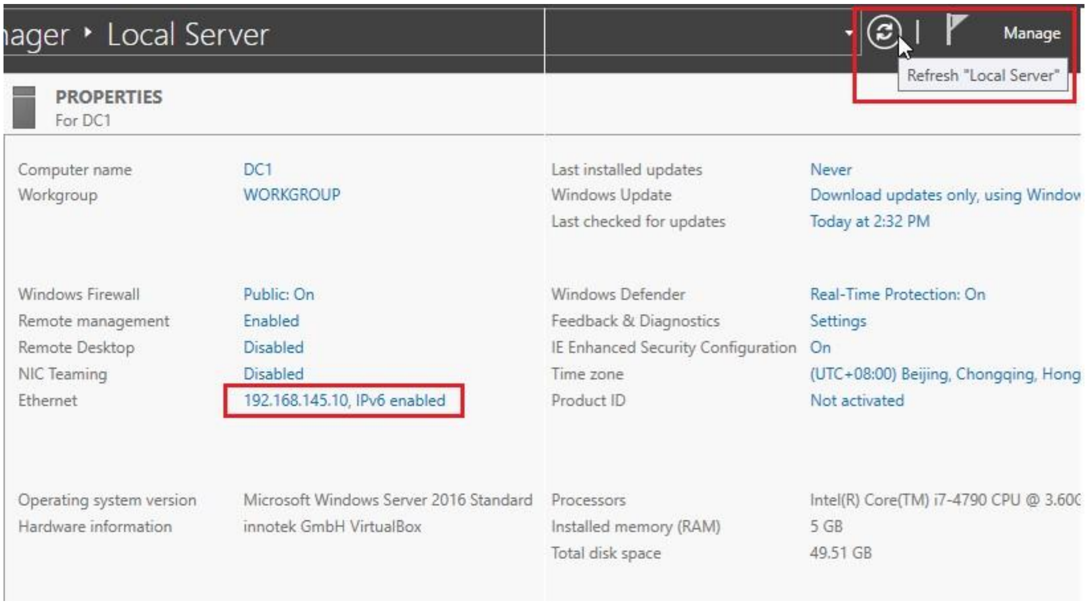
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Click okay and on the next window click okay. Close out the window for your networking connections. Back at server manager, if you click on the refresh button, you will see that the IP addressing for your server changes from dynamic to be in statically configured with the IP address you assigned in the TCP/IP properties.



PROPERTIES
For DC1

Computer name	DC1	Last installed updates	Never
Workgroup	WORKGROUP	Windows Update	Download updates only, using Windov
		Last checked for updates	Today at 2:32 PM
Windows Firewall	Public: On	Windows Defender	Real-Time Protection: On
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC+08:00) Beijing, Chongqing, Hong
Ethernet	192.168.145.10, IPv6 enabled	Product ID	Not activated
Operating system version	Microsoft Windows Server 2016 Standard	Processors	Intel(R) Core(TM) i7-4790 CPU @ 3.60(
Hardware information	innotek GmbH VirtualBox	Installed memory (RAM)	5 GB
		Total disk space	49.51 GB

Summary

In this lab, we looked at the importance of having the right naming convention when designing a new network. We also look at some ways we can prevent issues with our naming convention by first registering our domain name and then assigning a subdomain name as a prefix to our internal network. Finally, we looked at how to go about selecting an IP addressing scheme for network. Any device that needs to be always available on the network needs to be configured with a static IP address. These include firewalls, switches, servers and printers. Once you map to these devices and their IP addresses change, they will no longer be readily available.