2015

DESIGN IN NETWORK

FINAL TERM PROJECT

Submitted To:

Project Manager:

Prof. Fareed-U-Deen

Project supervisor:

Prof. Rehan Ahmad

Project Advisor:

Zain-Ul-Abideen Khan

Submitted By:

Waqar Ahmed

Muhammad Imtiaz

Muhammad Nabeel

Muhammad Faisal

Muhammad Faizan

Dedication

We dedicate our work to

The Sons of Motherland

&

Soldiers of PAK ARMAY,

Who are continuously sacrificing
their today
for the tomorrow of Nation.

****

Acknowledgement

Firstly, thank to Allah with his blessing we have finished our project **Design In Network** The real spirit of achieving a goal is through the way to excellence and discipline. We would have never succeeded in completing task without the cooperation, encouragement and help provided by various personalities. We want to thank IT department of **Superior University Lahore & New Channel** for providing us the necessary environment and other resources to deliver our research and project work. With deep sense of gratefulness we express our sincere thanks to our honored and admirable supervisor, **MR.Zain- Ul- Abideen Khan** for his valuable guidance in carrying out this work under their effective Supervision, support, clarification and cooperation. We are also thankful to all the staff members of our department specially **Prof. Muhammad Azam& Prof.Muhamnmad Rehan** for their full cooperation and help.

We could not forget to thank our beloved parents and sibling for always mentally and financially supporting us whiles this project till the end.

****

Table of Contents

Serial Description page Number

Chapter 5
Domain Name System (DNS)

1. Domain Name System
2. DNS Queries
3. Installation of DNS
4. Zone
5. Zone Types
6. Step to create a Zone

Chapter 6
Window Deployment service (WDS)

1. WDS
2. Installation of WDS
3. Configuration of WDS

Chapter 7
Threat Management Gateway (TMG)

1. TMG
2. Installation of TMG
3. Configuration of TMG
4. Create Users
5. Apply Policies

Chapter 8
File Transfer Protocol (FTP)

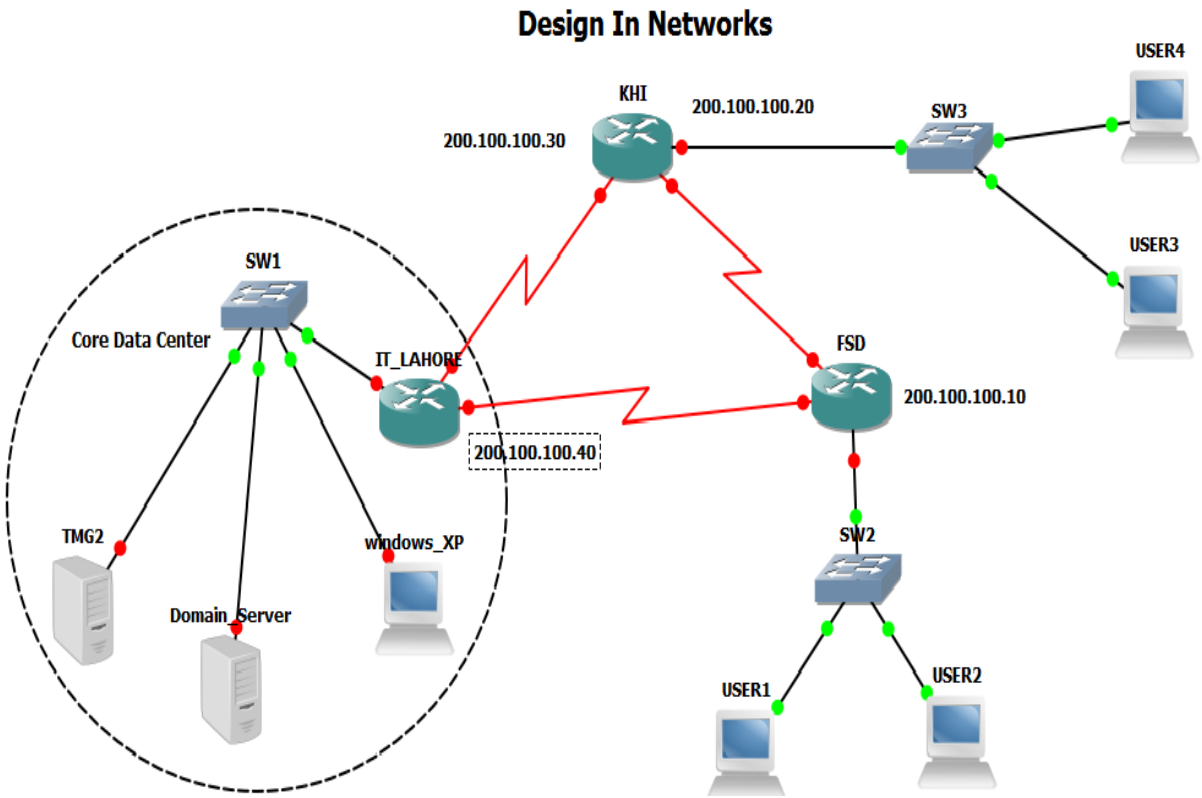
1. FTP
2. Installation
3. Configuration

Chapter no. 1

Design in Networks

Introduction

Design in networks is a core data network which has three departments. These departments are situated at different locations. These locations are Lahore, Karachi & Faisalabad. The department of Lahore is core data center or Domain controller for other departments because these departments controlled from this department. Lahore department is connected with acting as domain and it is using different services like active directory, DHCP, DNS, IIS, WDS, TMG and FTP are running on this core data center. Karachi & Faisalabad are locally connected with internet .If any department Karachi or Faisalabad want to use any of the services of domain controller that are installed on domain controller Lahore .For connectivity with Lahore these two departments use WAN connectivity by dialing the VPN .This WAN connectivity can be accessed through routers by using RIP protocol.



Chapter no. 2

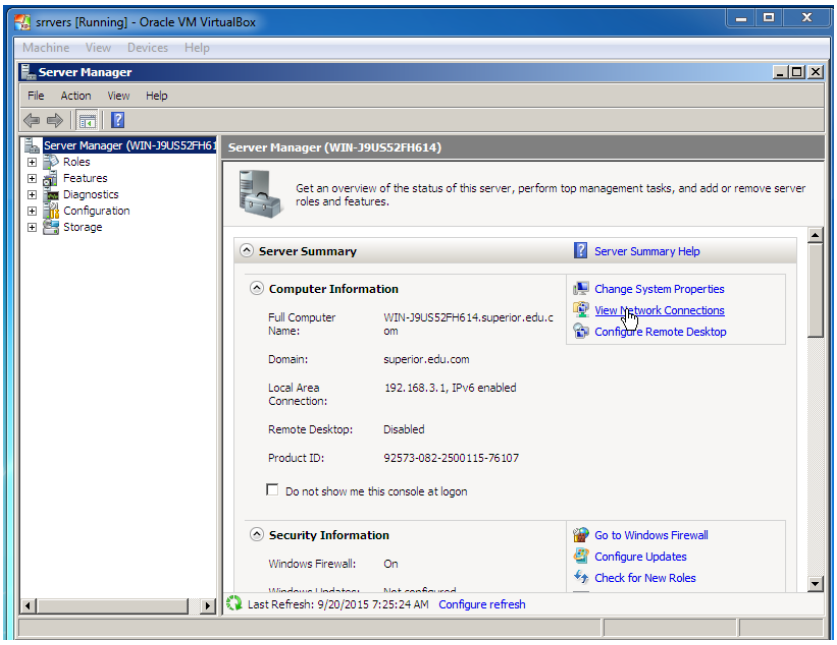
Domain Controller (DC)

Active Directory

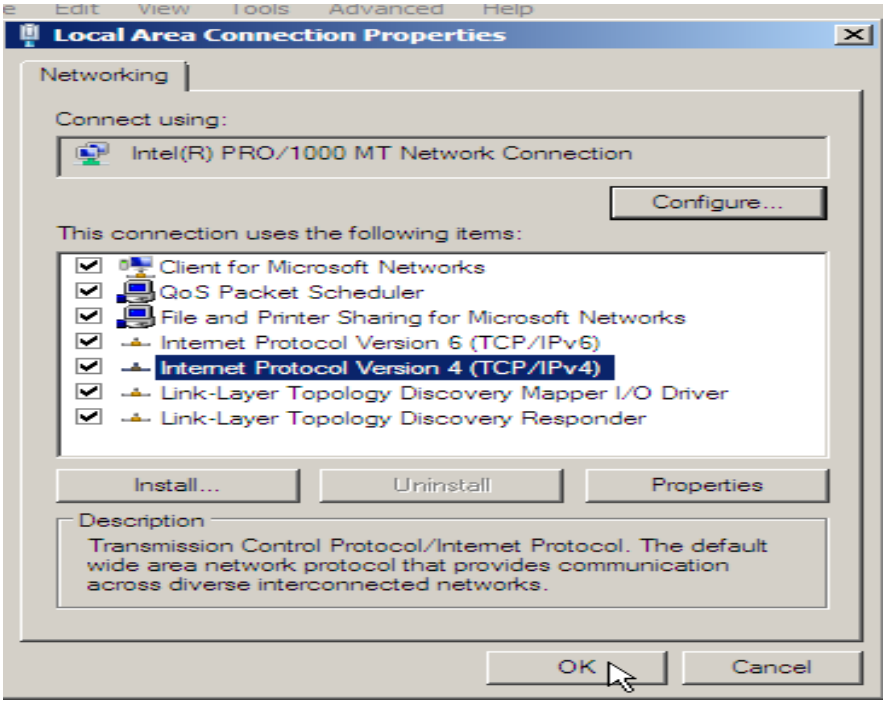
Active Directory (AD) is a directory services created by Microsoft for Windows domain networks. It is included in most Windows Server operating systems.
Active Directory provides the means to manage the identities and relationships that make up your organization's network. Integrated with Windows Server, Active Directory gives you out of the box functionality needs to centrally configure and administer system, user, and application settings. Active Directory provides a central location for network administration and security. Server computer that run Active Directory are called Domain Controller.
The Windows Active Directory provides central authentication and authorization services for Windows based computers. It also enables Network Administrators to assign policies, deploy software, and apply critical updates to an organization. Active Directory was designed to support hundreds of computers simultaneously.
When a users attempts to log on to a Windows computer that is on a Windows Domain, Windows automatically attempts to verify the user's password with the Active Directory (which typically resides on a separate central computer).

How To Configure Active Directory Domain Services

- From the Windows Start menu, open Administrative Tools > Server Manager.
- In the Server Summary section of the Server Manager window, click View Network Connections.



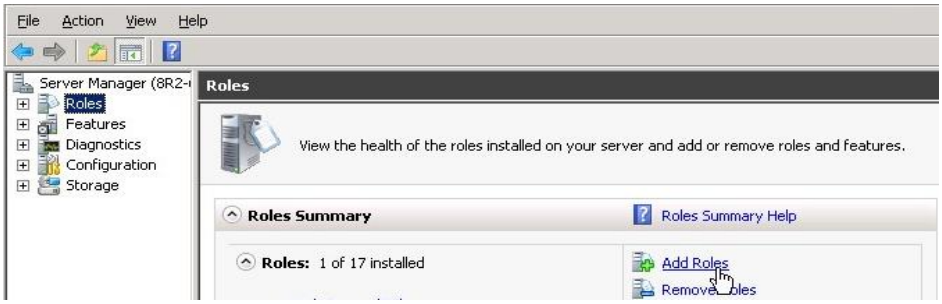
- In the Network Connections window, right-click the private adapter and select Properties and on appearing screen click on TCP/IPV4.



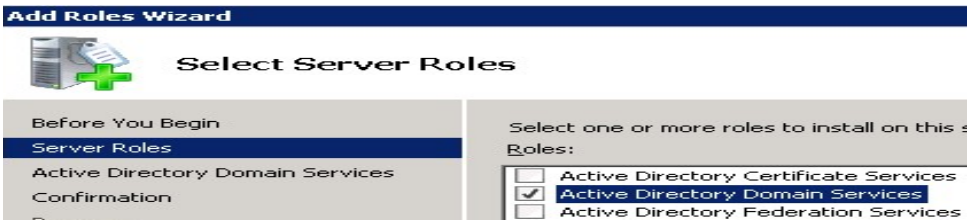
- Copy the IP address that is displayed in the IP address box and paste it into the Preferred DNS and Click ok.

Adding up the Active Directory Domain Services Role:-

- In the Server Manager window, open the Roles directory and in the Roles Summary section, click Add Roles**.**



- On the Select Server Roles page, select the Active Directory Domain Services check box, and then click Next button.



Click next and when Role added successfully click Close.

Active Directory Domain Services

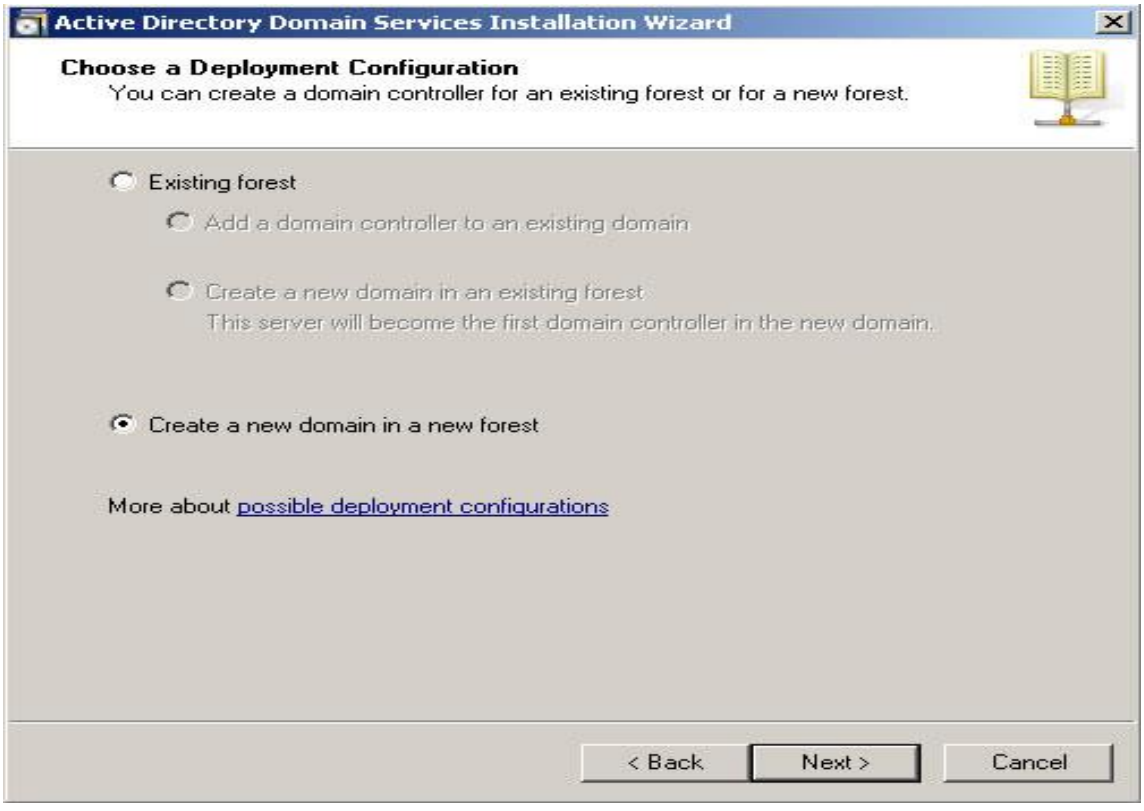
If Remote registry is not enable it can be enable by using the steps below

- open the Server Manager window if it is not already open.
- In the Properties area of the Local Servers page, click Remote Management.
- Select the Enable remote management of this server from other computers check box.

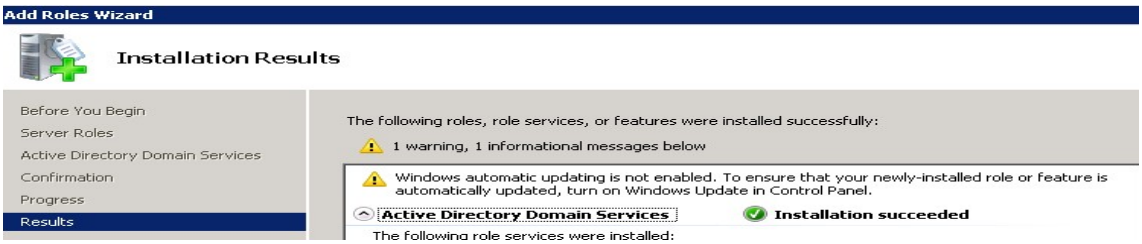
Configuring Active Directory Domain Services

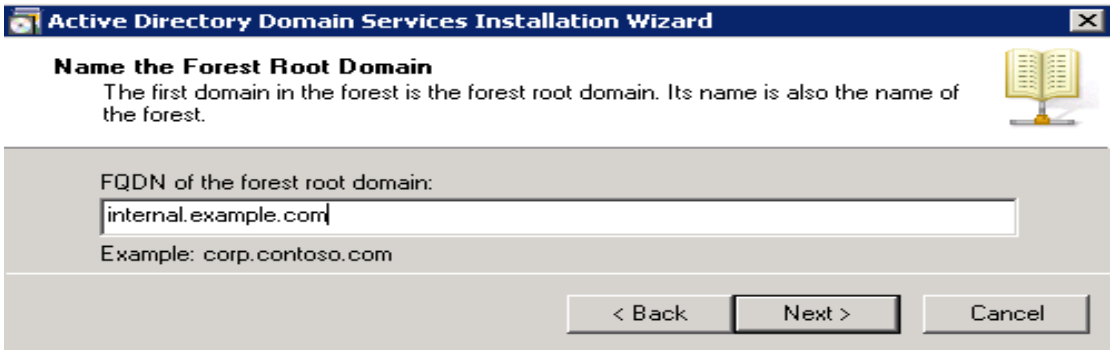
- open the Server Manager window and Select Roles > Active Directory Domain Services. In the Summary section, click Run the Active Directory Domain Services Installation Wizard .

- On the Welcome page of the Active Directory Domain Services Installation Wizard, ensure that the Use advanced mode installation check box is cleared, and then click Next. button
- On the Operating System Capability page, click Next button.
- On the Choose a Deployment Configuration page, select Create a new domain in a new forest and then click Next.

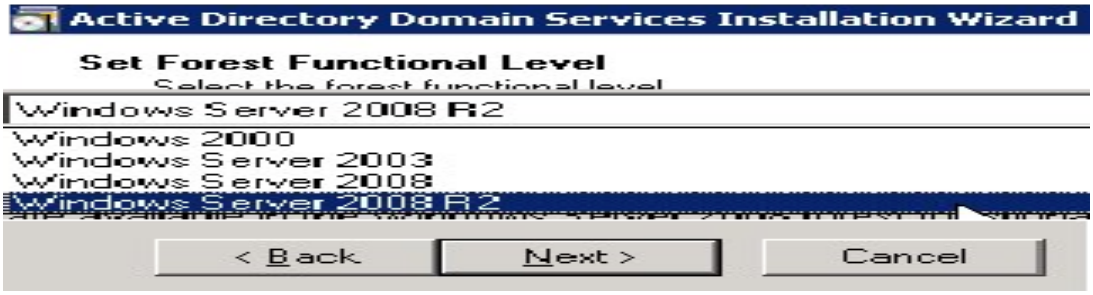


- Now for installing domain services just click onActive Directory Domain Services.
- On the Name the Forest Root Domain page, enter the domain name that you choose during preparation steps. Then, click next

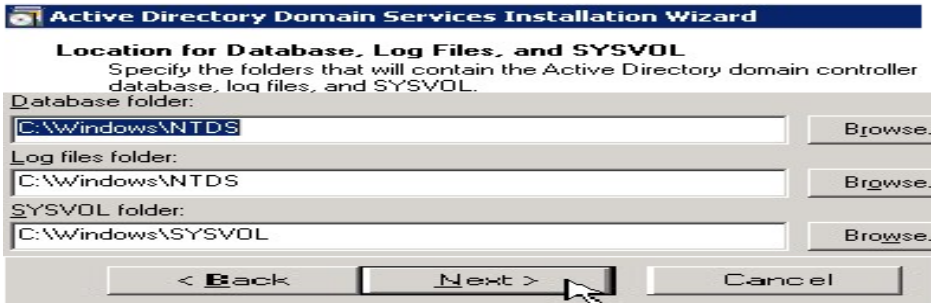




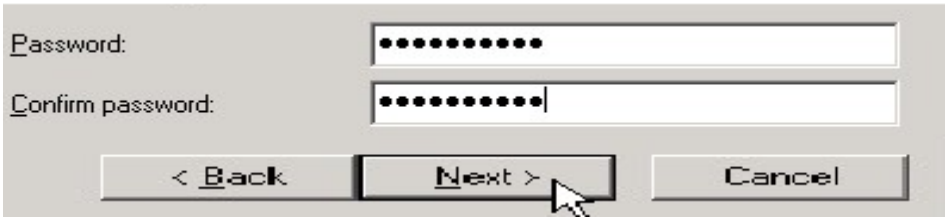
- After the installation verifies the NetBIOS name, on the Set Forest Functional Level page, select Windows Server 2008 R2 in the Forest level list. Then, click Next button.



- On the Additional Domain Controller Options page, ensure that the DNS server check box is selected, and then click next**.**
- When clicks next it should appear a dialogue box you want to continue or not click Next**.**
- On the Location for Database, Log Files, and SYSVOL page, accept the default values and then click Next.



- On the Directory Services Restore Mode Administrator Password page, enter the domain administrator password that you chose during the preparation steps.

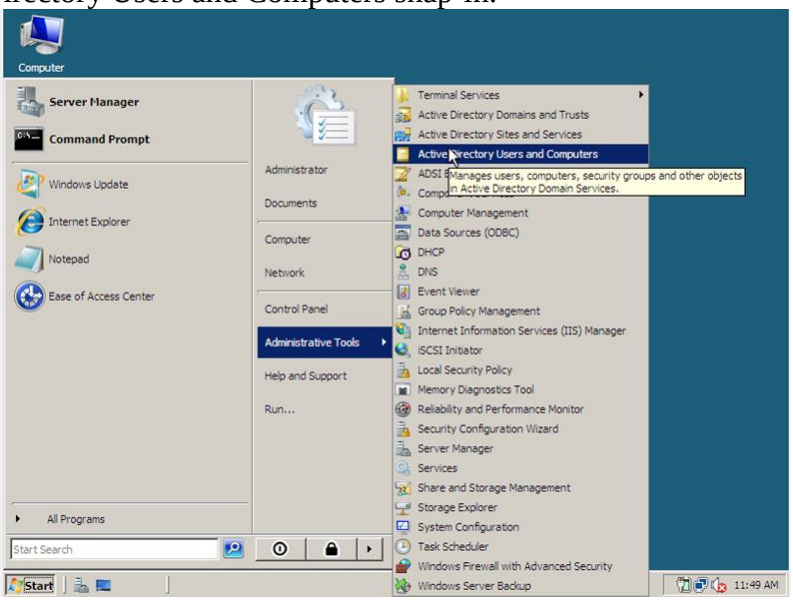


- On the Summary page, review your selections and then click Next**.** To continue installation process.
- Now the wizard appears click the finish button .

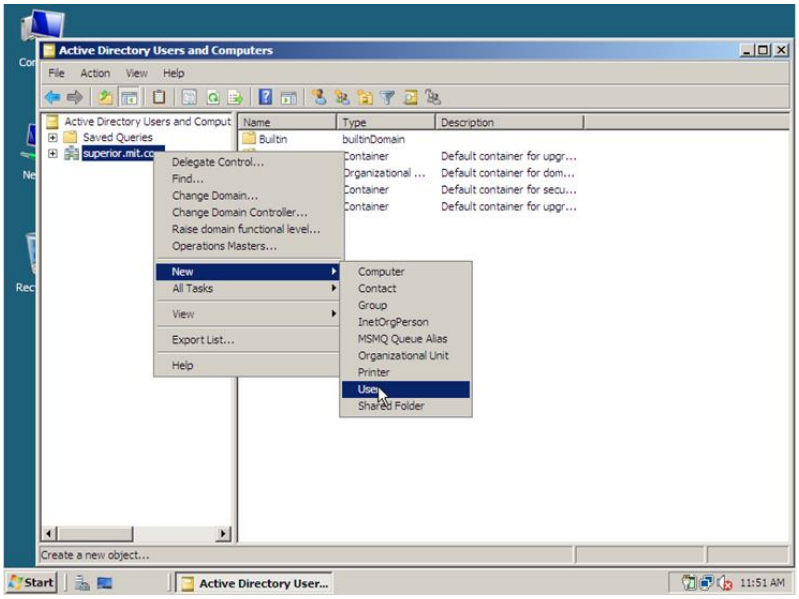
CREATE USER:

One of the first things to do in a new network is to create Users, also called User Objects. As long as you know the information about the user you need to create, the process will take no time at all.

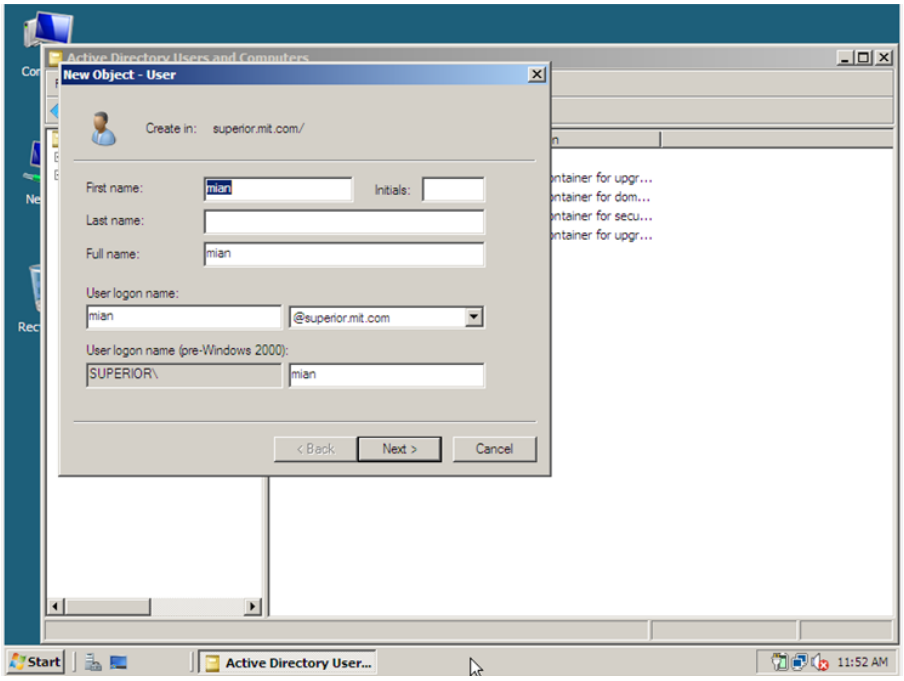
- This is a task we want to do from a Domain Controller, and you should have the Administrative Tools in your Start menu next to the Control Panel link. We'll choose the Active Directory Users and Computers snap-in.



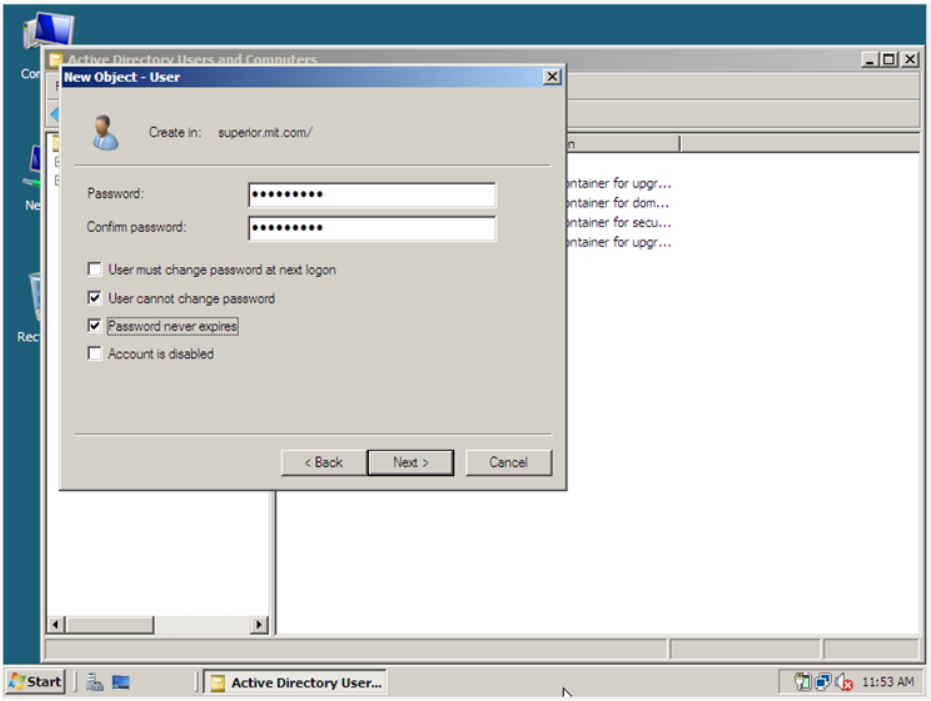
- Once we're inside the Active Directory Users and Computers snap-in, we'll need to expand the domain in which we want to create the user, and right-click on the Users folder. We'll then select New User.



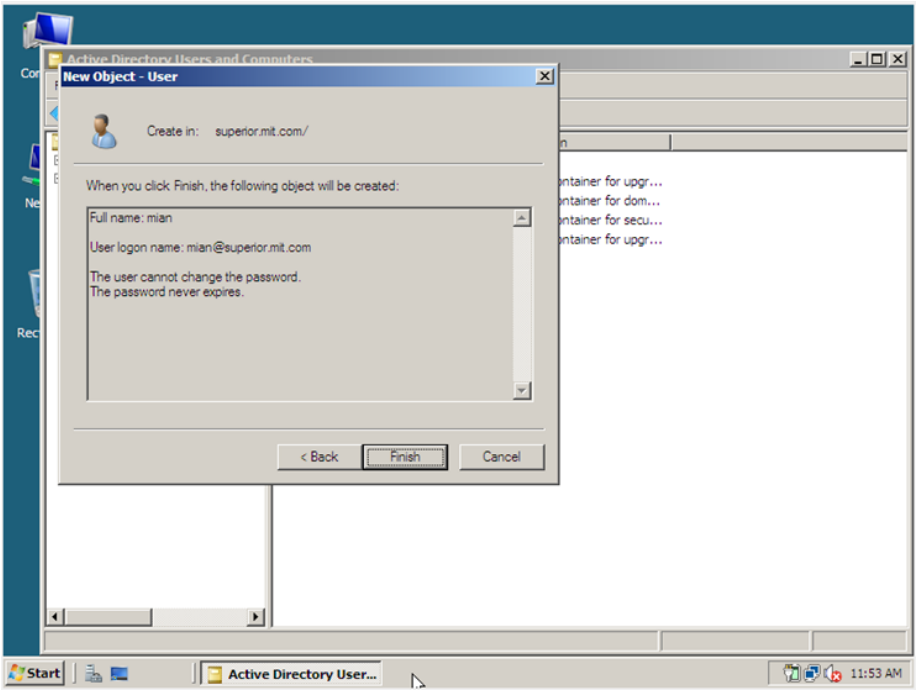
- The New Object – User box will pop up and require you to put in the user's name and create the user logon. You'll need to use a standard method of creating user logon names, as this will cause much less confusion in the future. If you have a small network, you may want to just stick to using the first initial and last name because it's shorter. If you anticipate that your network will grow quite large, the standard advice is to use the full first and last name separated by a period..



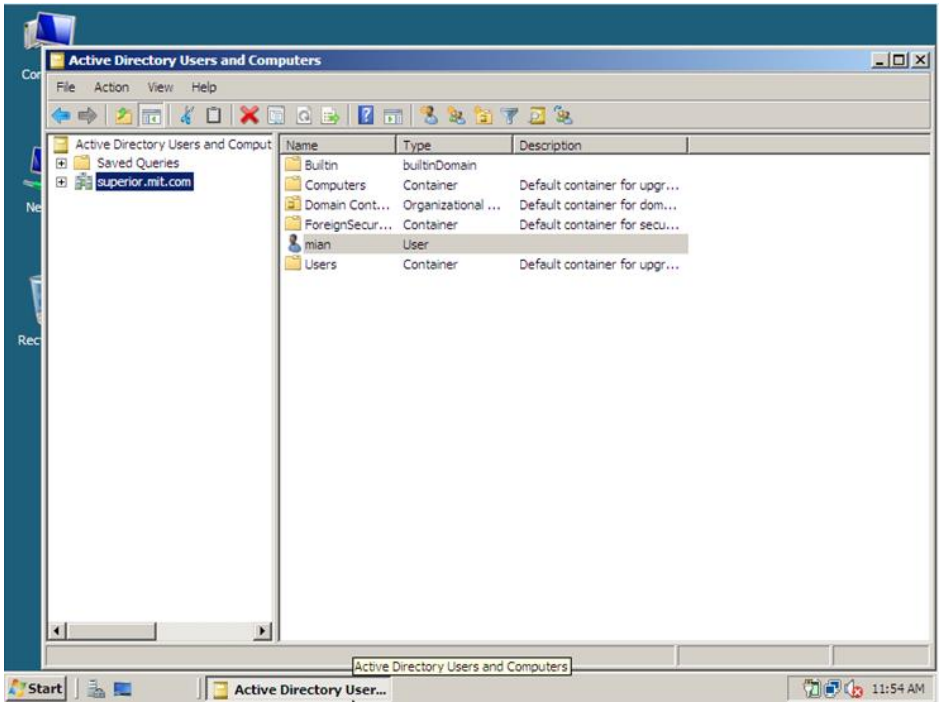
- Next we'll give the user an initial password, and make sure to have them change it as soon as they first logon.



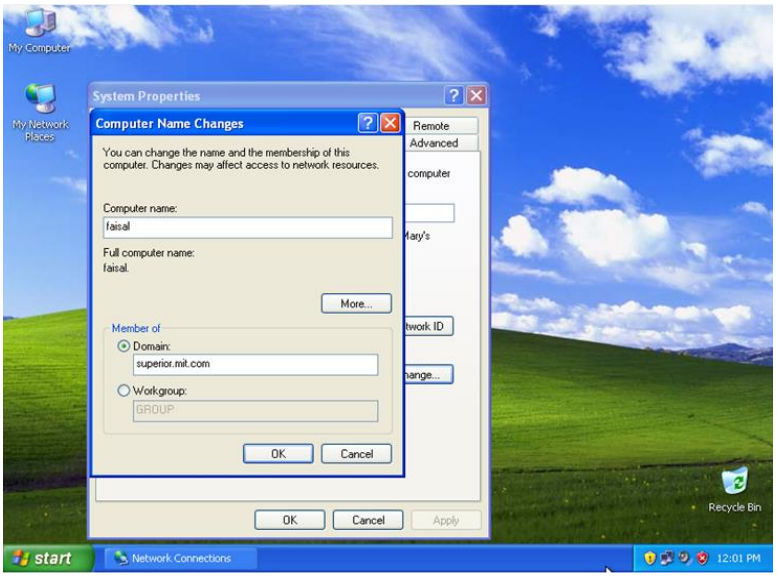
- When we're finished, we'll get a nice summary of our work.



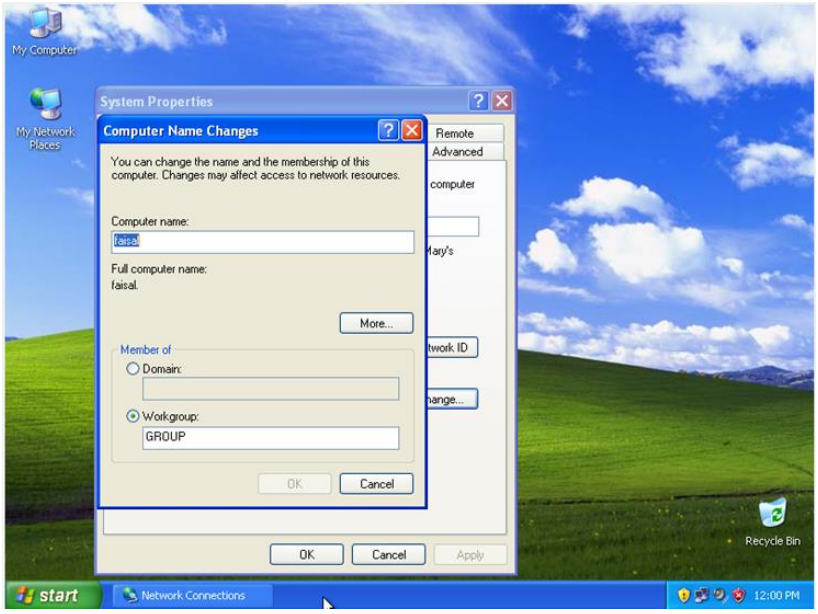
- When we go back to the Users folder in the domain, we can see our newly created user.



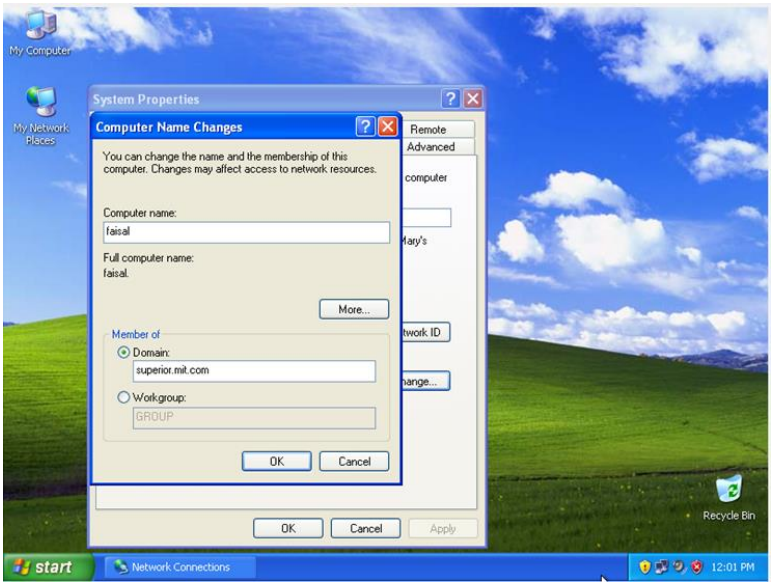
Domain Join



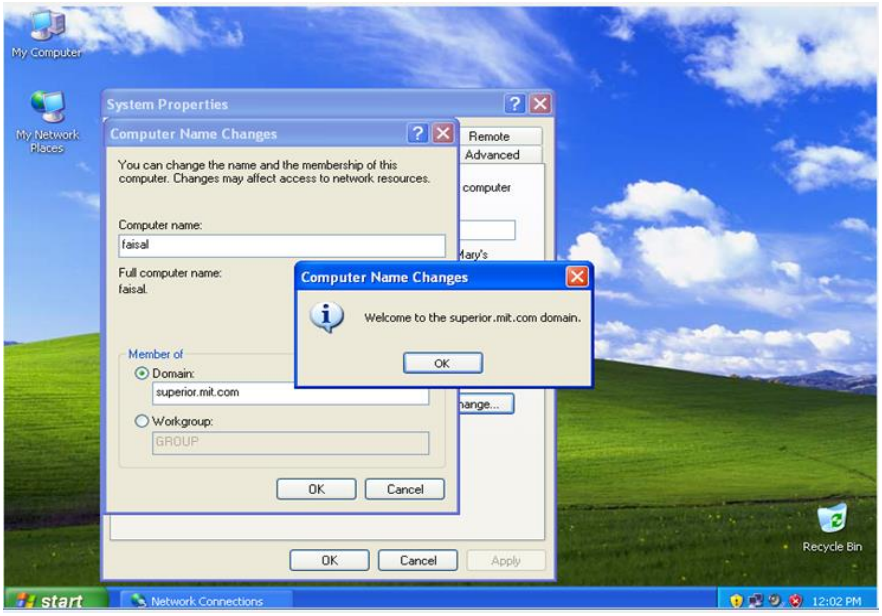
Click on the change button, from here you can change your Computers Name to a more friendly name.



- Now type in the name of your domain, our Domain is superior.mit.com but yours will be whatever you made it when you set up Active Directory.

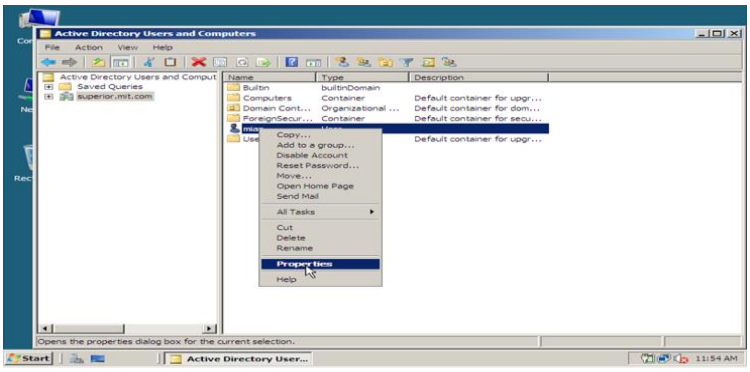


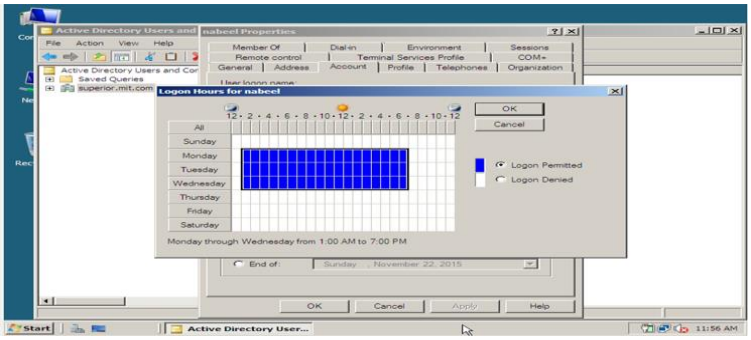
- At the end your domain is joined when you click ok and your client is need to be restarted.



Add Policies:

- If you want to deploy some policies on the user you have created in active directory domain controller. Just right click on the user that is created and go to its properties.





- Now on next wizard screen click on account button and apply the login hour in a week you want to permit for this user.

Dynamic Host Configuration Protocol (DHCP)

IP Assigning:

We can assign IP addresses to the computer by two They are ways

Manual IP Configuration (Static IP)

Automatic IP Configuration (Dynamic IP)

DHCP gives flexibility of administration to the system administrator. In Manual IP configuration we will click on the properties of the network adapter and give IP address manually which is called Static IP address. If you have 5-10 computers then it is easy to manually assign IP addresses to them.

But if you have a large environment having 1000 of computers thenit is quite difficult to assign IP addresses manually. There must be an easy way to perform this task and the easy way is to use DHCP server. In DHCP or Automatic IP Configuration the IP addresses are automatically assigned to the client computers which are called Dynamic IP addresses.

DORA (Discovery, Offer, Request, Acknowledgment

Client Broadcast DHCP Discover Packet

The client broadcasts messages on the network subnet using the destination address 255.255.255.255 or the specific subnet broadcast address. A DHCP client may also request its last-known IP address. If the client remains connected to the same network, the server may grant the request. Otherwise, it depends whether the server is set up as authoritative or not. An authoritative server denies the request, causing the client to issue a new request. A non-authoritative server simply ignores the request, leading to an implementation-dependent timeout for the client to expire the request and ask for a new IP address.

DHCP Server unicast DHCP Offer Packet to the client

When a DHCP server receives a DHCPDISCOVER message from a client, which is an IP address lease request, the server reserves an IP address for the client and makes a lease offer by sending a DHCPOFFER message to the client. This message contains the client's MAC address, the IP address that the server is offering, the subnet mask, the lease duration, and the IP address of the DHCP server making the offer.

The server determines the configuration based on the client's hardware address as specified in the CHADDR (client hardware address) field. Here the server, 192.168.1.1, specifies the client's IP address in the YIADDR (your IP address) field.

DHCP Client send a DHCP request message to the DHCP server

In response to the DHCP offer, the client replies with a DHCP request, broadcast to the server, requesting the offered address. A client can receive DHCP offers from multiple servers, but it will accept only one DHCP offer. Based on required server

identification option in the request and broadcast messaging, servers are informed whose offer the client has accepted. When other DHCP servers receive this message, they withdraw any offers that they might have made to the client and return the offered address to the pool of available addresses.

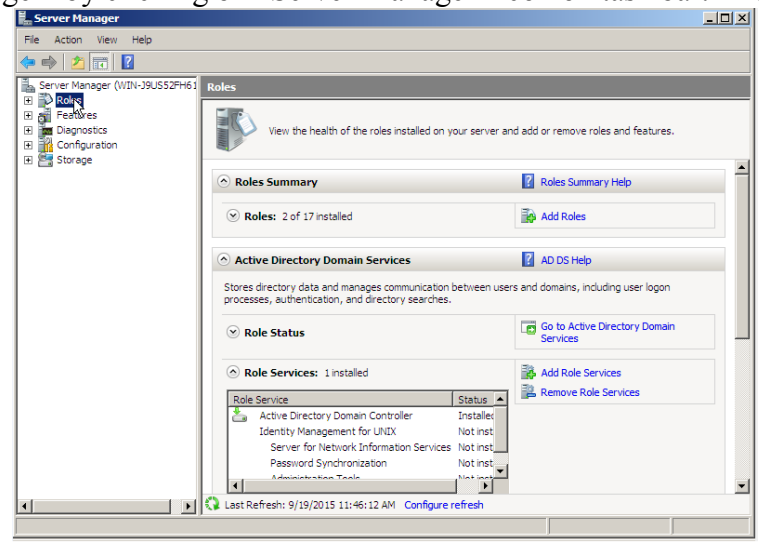
DHCP Server send a DHCP Acknowledge message to the DHCP Client

When the DHCP server receives the DHCP REQUEST message from the client, the configuration process enters its final phase. The acknowledgement phase involves sending a DHCP ACK packet to the client. This packet includes the lease duration and any other configuration information that the client might have requested. At this point, the IP configuration process is completed.

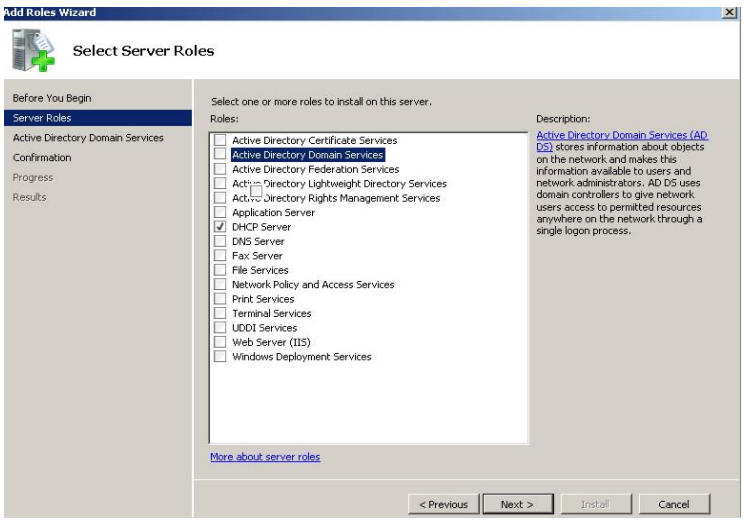
Configuration DHCP Server

Let's see how we can configure DHCP server in a Windows Server Environment. For the demo I will be using Windows 2008 R2 Server.

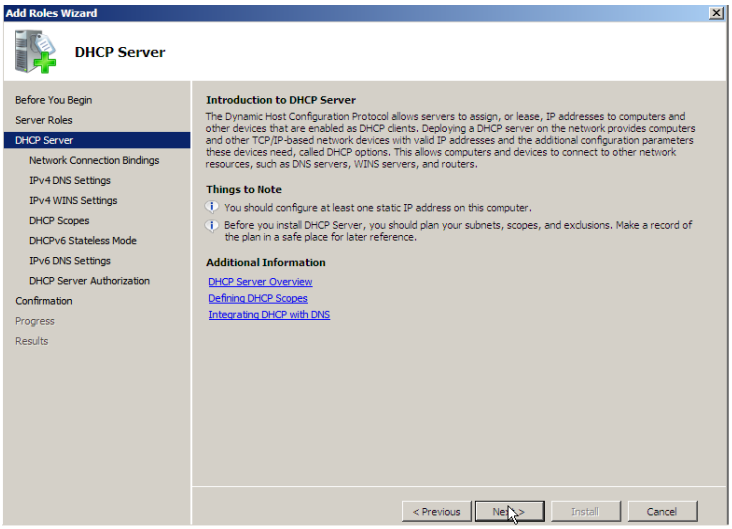
To start first need to log in to the server with administrator privileges. Then start the "server Manager" by clicking on "Server Manager" icon on task bar. Then go to "Roles"



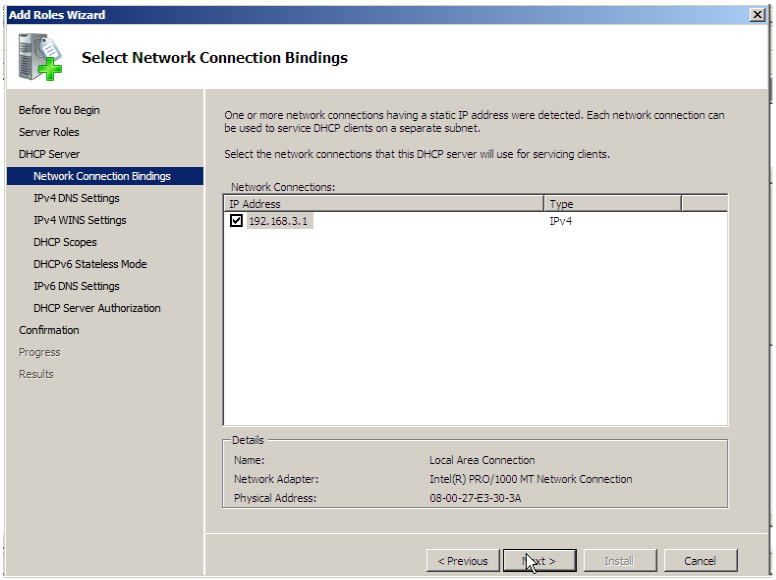
- Then click on "Add Roles" option to open Add roles Wizard.



- Then it will load the Roles Wizard and select the “DHCP Server” From the list and click next to continue
- Then it will give description about the role. Click next to continue.

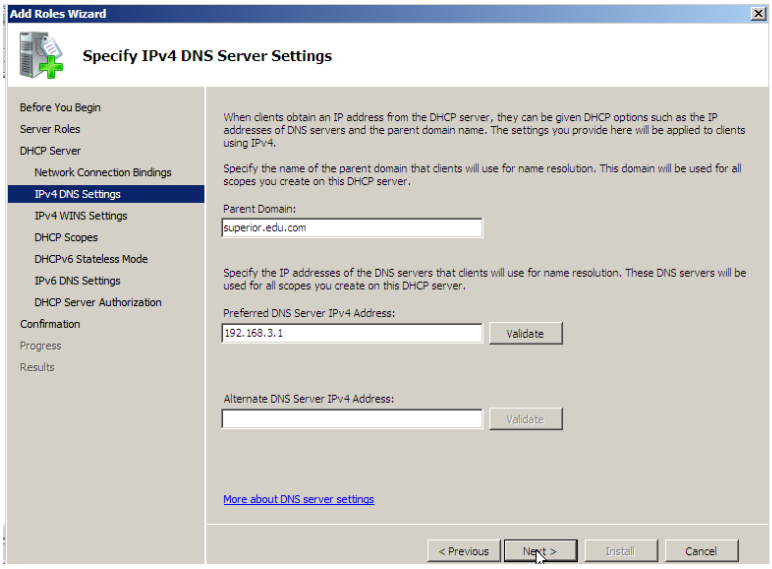


Next window is asking to use which interface to serve DHCP clients. If server has multiple NIC with multiple IP you can add them also to serve DHCP clients.

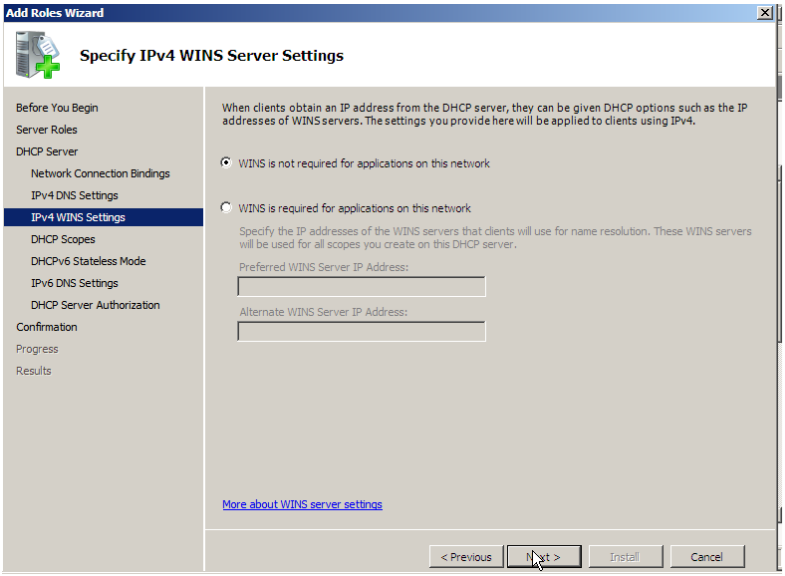


- (In next window it will give opportunity to add DNS settings that should apply for DHCP clients.
- Domain Name System DNS) configuration involves the following configuration tasks for TCP/IP properties on each computer:
- Set a DNS computer or host name for each computer. For example, in the fully qualified domain name wkstn1.widgets.tailspintoys.com. The DNS computer name is the left-most label wkstn1.
- Set a primary DNS suffix for each computer, which is placed after the computer or host name to form the FQDN. Using the previous example, the primary DNS suffix is widgets.tailspintoys.com.

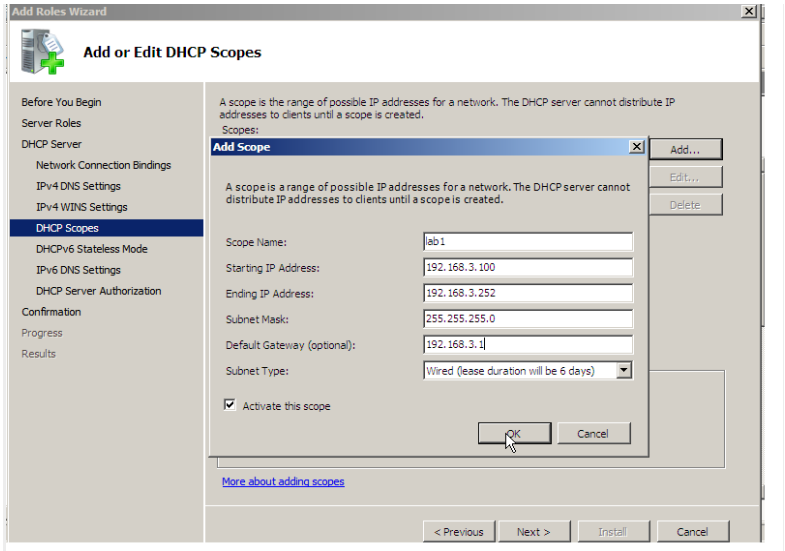
- Set a list of DNS servers for clients to use when resolving DNS names, such as a preferred DNS server, and any alternate DNS servers to use if the preferred server is not available.
- Set the DNS suffix search list or search method to be used by a client when it performs DNS query searches for short, unqualified domain names.



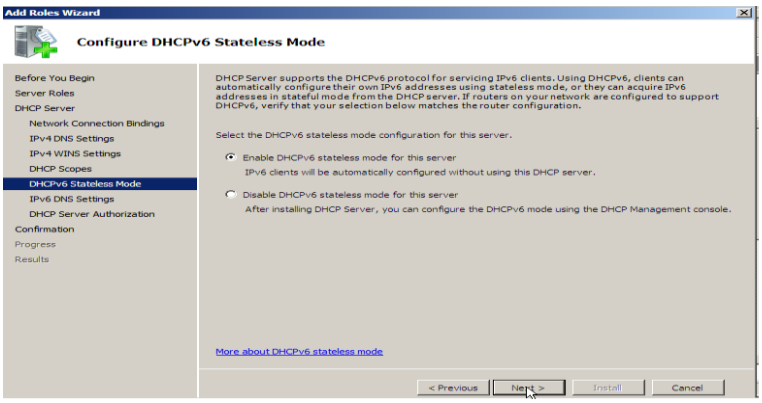
- Next window is to define the WINS server details.
- Windows Internet Name Service (WINS) provides a distributed database for registering and querying dynamic mappings of NetBIOS names for computers and groups used on your network. WINS maps NetBIOS names to IP addresses and was designed to solve the problems arising from NetBIOS name resolution in routed environments. WINS is the best choice for NetBIOS name resolution in routed networks that use NetBIOS over TCP/IP.



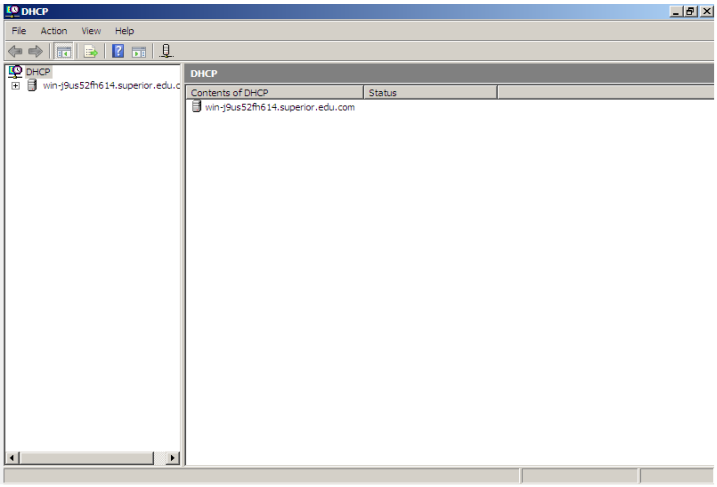
- In next window we can add the scope, the Starting IP, End IP of the DHCP range, subnet mask, default gateway, leased time etc.
- A scope is an administrative grouping of IP addresses for computers on a subnet that use the Dynamic Host Configuration Protocol (DHCP) service. The administrator first creates a scope for each physical subnet and then uses the scope to define the parameters used by clients. A scope has the following properties:
- A range of IP addresses from which to include or exclude addresses used for DHCP service lease offerings.
- A subnet mask, which determines the subnet for a specific IP address.
- A scope name.
- Lease duration values, which are assigned to DHCP clients that receive dynamically allocated IP addresses.
- Any DHCP scope options configured for assignment to DHCP clients, such as Domain Name System (DNS) server, router IP address, and Windows Internet Name Service (WINS) server address.
- Reservations optionally used to ensure that a DHCP client always receives the same IP address.



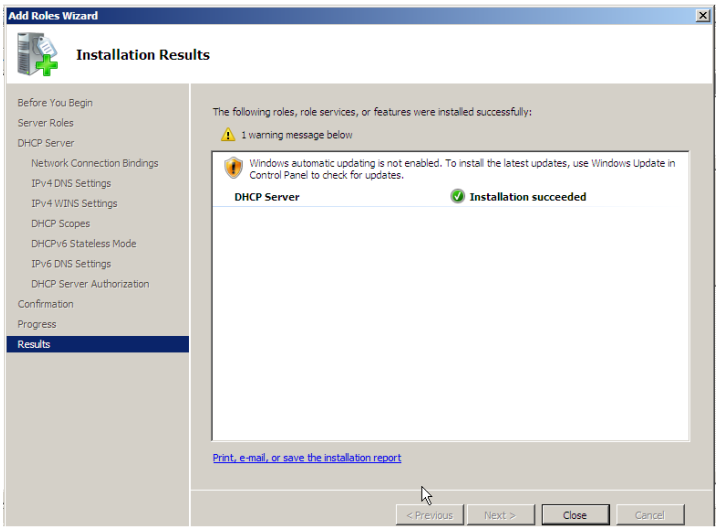
- In next Window it can configure to support IPv6 as well.



- Then it will give the confirmation window before begin the install. Click on “Install”.
- When I first installed a DHCPv6 server on Window Server 2008 R2, my clients (Vista and Windows 7) were unable to receive IP addresses. Thus, I started goggling to find out what went wrong. I found quite a few official and unofficial resources with promising advice. In the end, it turned out that most of those resources were either outdated or simply provided wrong information. In my last post aboutDHCPv6 server installation, I mentioned the wrong advice regarding client settings.
- Once installation finishes DHCP server interface can open from Start > Administrative Tools > DHCP



Using the DHCP it is possible to even configure multiple Scopes configurations to the network. In a network there can be different network segments. It is waste to setup different DHCP servers for each segment. Instead of that it is possible to create different Scopes to issue DHCP for them.



Web Server IIS

IIS (**Internet Information Server**) is a group of Internet servers (including a Web or Hypertext Transfer Protocol server and a File Transfer Protocol server) with additional capabilities for Microsoft's Windows NT and Windows 2000 Server operating systems.

Stands for "Internet Information Services." IIS is a web server software package designed for Windows Server. It is used for hosting websites and other content on the Web.

Microsoft's Internet Information Services provides a graphical user interface (GUI) for managing websites and the associated users. It provides a visual means of creating, configuring, and publishing sites on the web. The IIS Manager tool allows web administrators to modify website options, such as default pages, error pages, logging settings, security settings, and performance optimizations.

IIS can serve both standard HTML web pages and dynamic web pages, such as ASP.NET applications and PHP pages. When a visitor accesses a page on a static website, IIS simply sends the HTML and associated images to the user's browser. When a page on a dynamic is accessed, IIS runs any applications and processes any scripts contained in the page, then sends the resulting data to the user's browser.

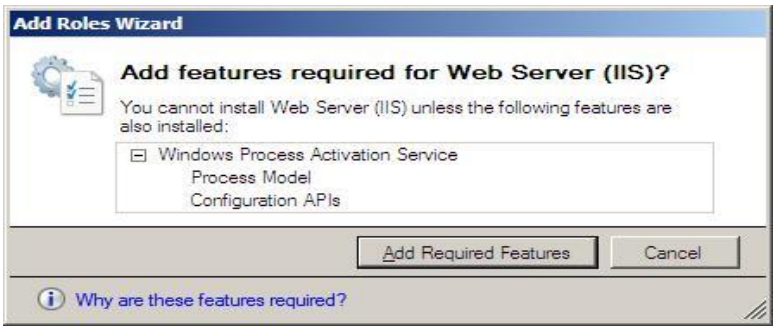
While IIS includes all the features necessary to host a website, it also supports extensions (or "modules") that add extra functionality to the server. For example, the Win Cache Extension enables PHP scripts to run faster by caching PHP processes. The URL Rewrite module allows webmasters to publish pages with friendly URLs that are easier for visitors to type and remember. A streaming extension can be installed to provide streaming media to website visitors.

IIS is a popular option for commercial websites, since it offers many advanced features and is supported by Microsoft. However, it also requires requires a commercial license and the pricing increases depending on the number of users. Therefore, Apache HTTP Server, which is open source and free for unlimited users, remains the most popular web server software.

- Launch the Add Roles Wizard using one of these methods:
  On a new Windows Server 2008 installation click Add Roles from the Initial Configuration Task Window

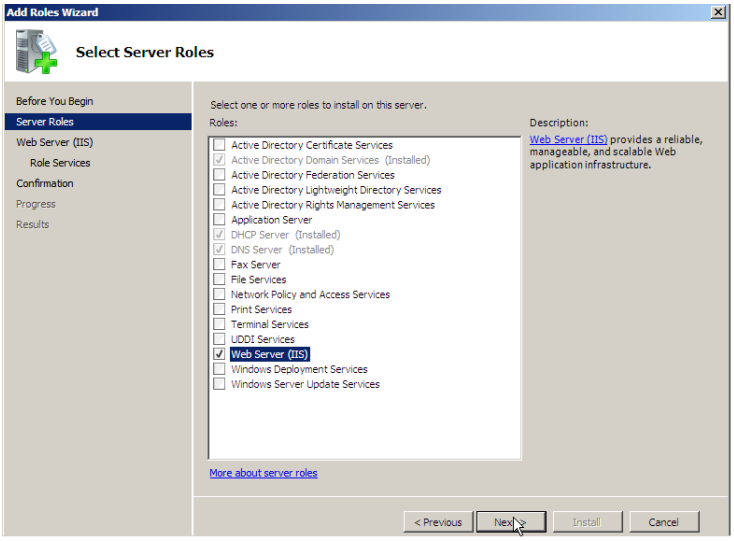
  From the Server Manager click Add Roles from the Roles Summary or Roles Manager
- The Add Roles Wizard will begin with some recommendations for the installation; click the Next button to proceed.

- You may be prompted to add the Windows Process Activation Service feature, in this case click the Add Required Features button.

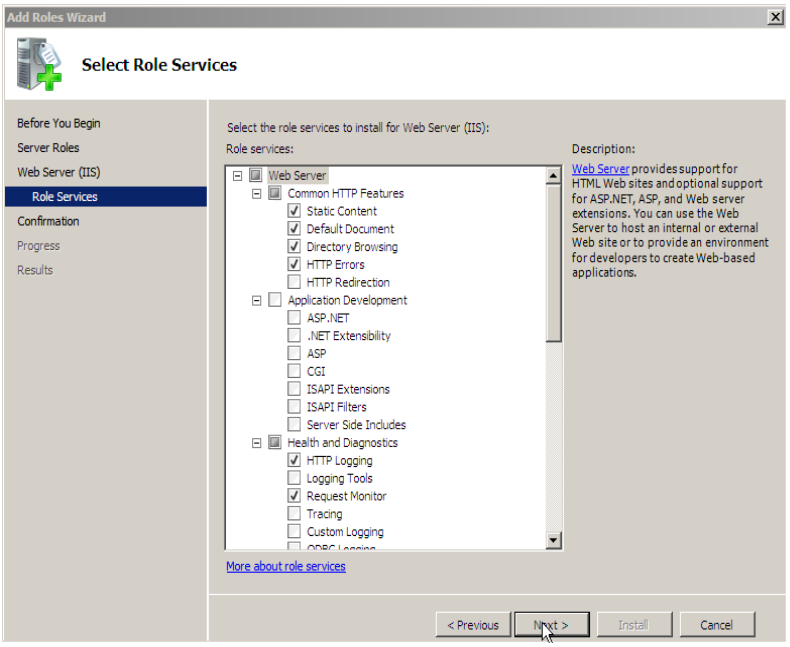


From the Select Server Roles Wizard step check the box labeled Web Server (IIS) and click Next to continue.

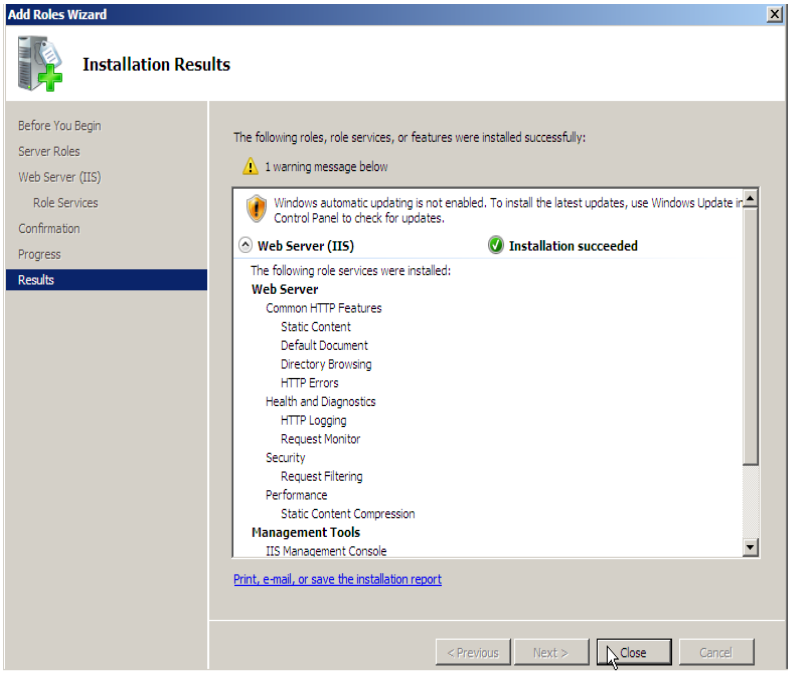
Note: If you use the Add Roles Wizard to install IIS, you get the default installation, which has a minimum set of role services. If you need additional IIS role services, such as Application Development or Health and Diagnostics, make sure to select the check boxes associated with those features in the Select Role Services page of the wizard.



- After reviewing the Web Server Installation introduction, click the Next button to begin selecting the role services to install.
- Server roles describe the main function or functions performed by a server in your organization. For example, a domain controller performs the Domain Controller server role. Server roles must have role-specific services enabled. The Security Configuration Wizard (SCW) enables services that are necessary for the selected server to perform the server roles that you select on this page. Unnecessary services are disabled.

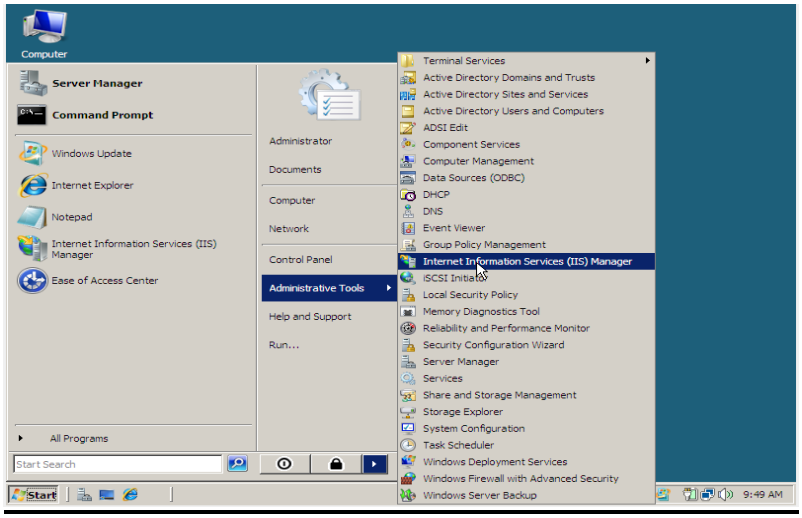


- When the wizard is finished installing the roles, review the installation results and click the Close button to complete the installation.

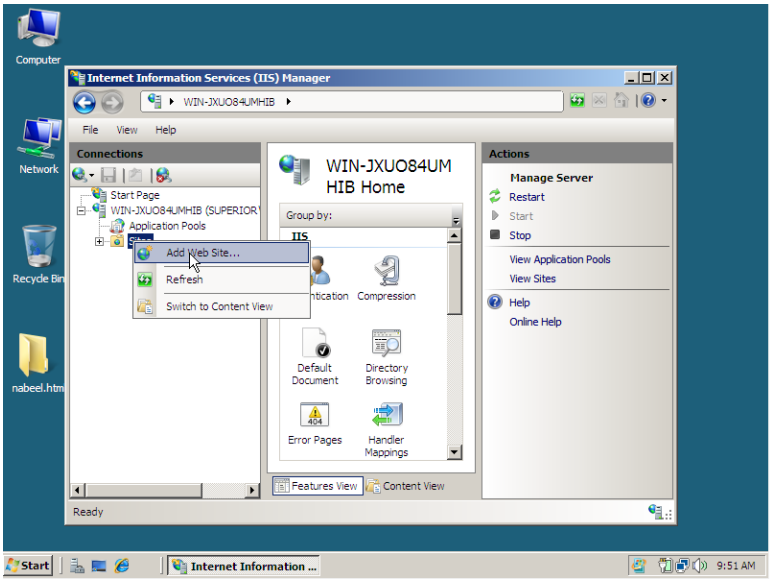


Configuration of Web Server IIS

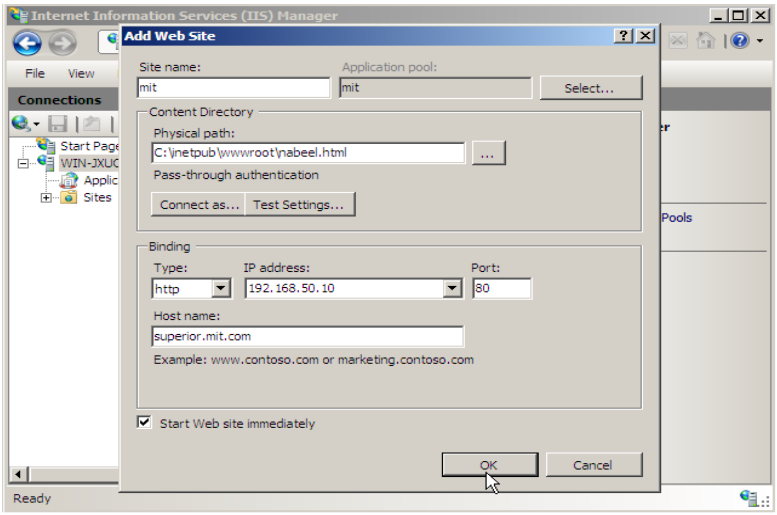
- Let's go ahead and open IIS Manager by going to Start -> Administrative Tools -> Internet Information Services (IIS) Manager



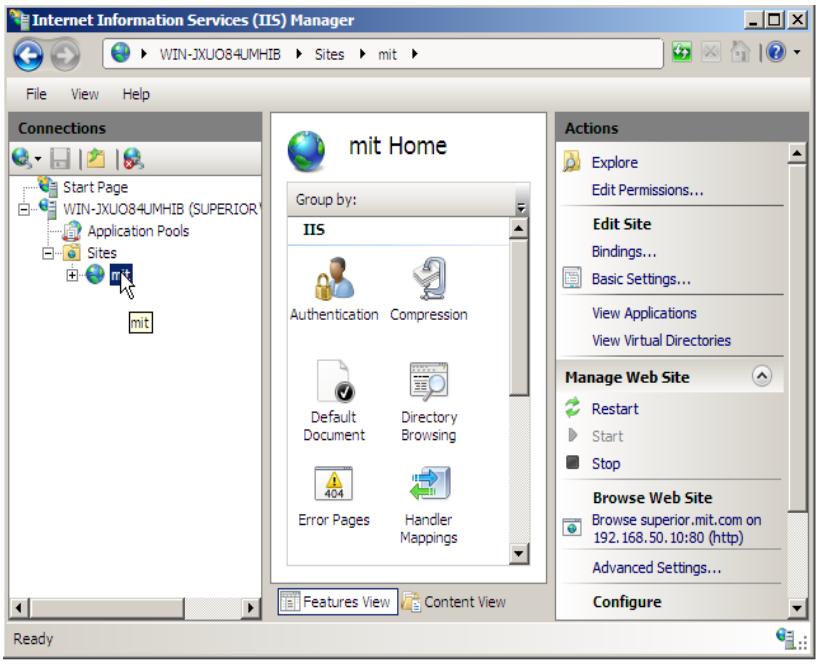
- Once IIS Manager opens, expand out the web server and then expand the Sites folder. Right click on sites and then click on Add Web Site



In the Add Web Site window we have some basic information to fill out for a static site:
Site Name – Name of the site, this will be either domain.com or *.domain.com (Where * would represent a sub domain name such as www or blog for example)
Physical Path – The location on the local server that will hold the files for the website If you did not set this up beforehand you can create a folder through this interface
Type – choose either http or https depending on whether your site will use Secure Socket Layer (SSL) certificate or not
IP Address – From the dropdown you can specify what IP the website should answer on or use the default switch of All Unassigned
Host Name – If you would like this site to respond to other domain names you can put these here.



You have now installed IIS 7 and configured a static website. Just place your html files in the directory you specified when creating the site and you are good to go



Installation of IIS

- Go to server manager click on Roles.
- Click on add roles and click on next.
- Select Web Server (IIS) and click on next.
- Click on next then install and then close.

Steps for making DNS Zone

- Open DNS from administrative tools.
- Select forward look up zone.
- Right click on it and select new zone.
- Select primary zone
- Give name to the zone
- Inside this newly created zone create a host record by right clicking
- Give name www and assigning imp address of your choice.

Steps for making a website

- Open note pad and write some html code
- <html><body>
- This is test website for webhosting.
- <body></html>
- Make a folder with the name in C drive and save this file with index.html.

Steps for Creating site

- Open IIS from administrative tools.
- Right click on site and select add new site
- Give name to the new website
- Give a physical path
- Give host name
- Click ok
- Now click on the default document and remove all documents .
- Add your own documents index.html to the default document .
- Enable it and then click ok.
- Stop the web site then start the web site.
- Now go the internet explorer and type the URL.

Domain Name System (DNS)

A DNS server is a server software program that performs Domain Name Services (DNS). This involves taking a full host name such as 'www.vicomsoft.com' or a domain name such as 'vicomsoft.com' and returning the corresponding Internet Protocol (IP) address such as 195.224.81.4.

DNS Queries

There are two types of queries in DNS

Recursive Query

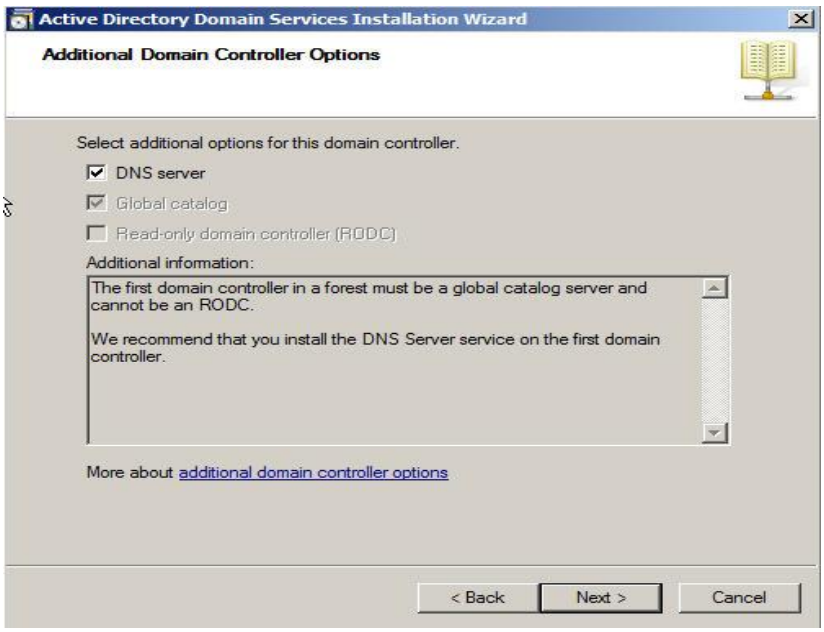
It goes from DNS client to DNS server. Its answer is complete means complete.

Iterative queries

It goes from DNS server to DNS server. Its answer is not complete mean referral. Iterative query is used to reach from one DNS to another DNS reply for 60 minutes in his cache

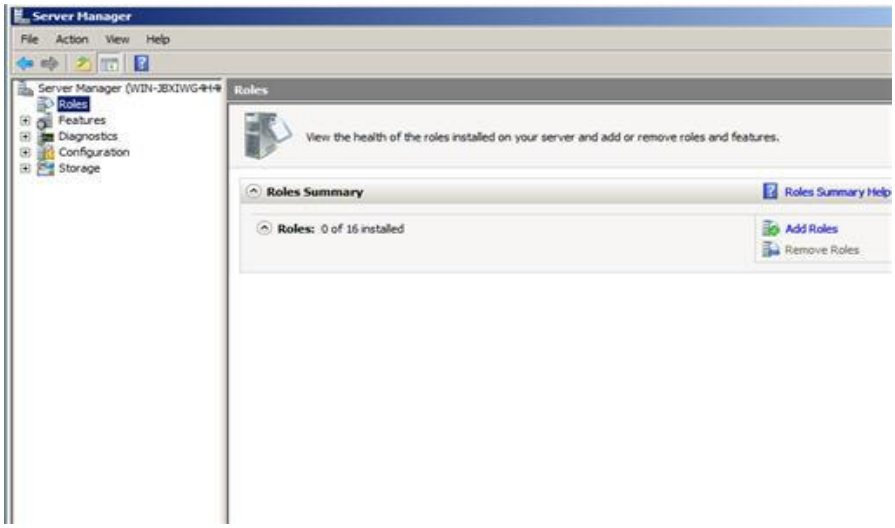
DNS Installation

You can install a DNS server from the Control Panel or when promoting a member server to a domain controller (DC). During the promotion, if a DNS server is not found, you will have the option of installing it.

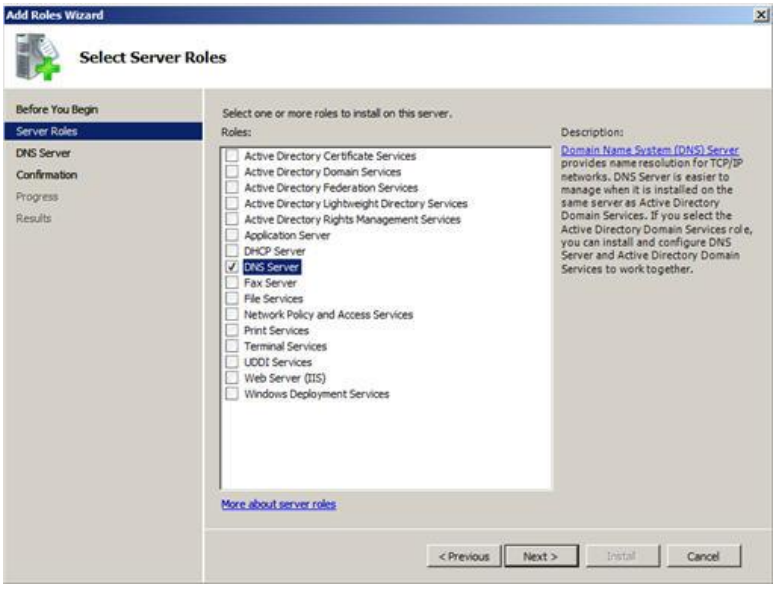


To install a DNS server from the Control Panel, follow these steps:

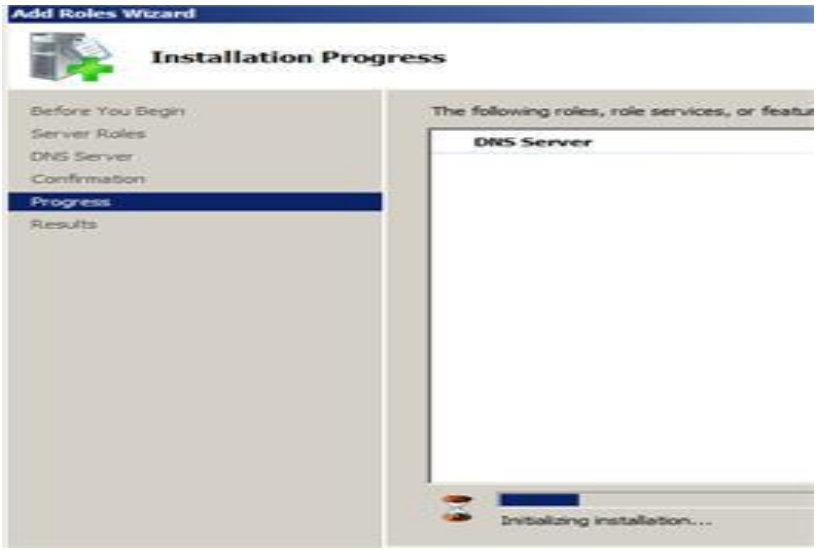
- From the Start menu, select | Control Panel | Administrative Tools | Server Manager.
- Expand and click Roles
- Choose Add Roles and follow the wizard by selecting the DNS role.
- Click Install to install DNS in Windows Server.



- Expand and click Roles



- Select DNS role



- Click finish to end setup wizard

DNS console and configuration

- After installing DNS, you can find the DNS console from Start | All Programs | Administrative Tools | DNS. Windows 2008 provides a wizard to help configure DNS.
- When configuring your DNS server, you must be familiar with the following concepts:
- Forward lookup zone
- Reverse lookup zone
- Zone types
- A forward lookup zone is simply a way to resolve host names to IP addresses. A reverse lookup zone allows a DNS server to discover the DNS name of the host. Basically, it is the exact opposite of a forward lookup zone. A reverse lookup zone is not required, but it is easy to configure and will allow for your Windows Server 2008 Server to have full DNS functionality.
- When selecting a DNS zone type, you have the following options: Active Directory (AD) Integrated, Standard Primary, and Standard Secondary. AD Integrated stores the database information in AD and allows for secure updates to the database file. This option will appear only if AD is configured. If it is configured and you select this option, AD will store and replicate your zone files.
- A Standard Primary zone stores the database in a text file. This text file can be shared with other DNS servers that store their information in a text file. Finally, a Standard Secondary zone simply creates a copy of the existing database from another DNS server. This is primarily used for load balancing.
- To open the DNS server configuration tool:
- Select DNS from the Administrative Tools folder to open the DNS console.
- Highlight your computer name and choose Action | Configure a DNS Server... to launch the Configure DNS Server Wizard.
- Click Next and choose to configure the following: forward lookup zone, forward and reverse lookup zone, root hints only Click Next and then click Yes to create a forward lookup zone
- Select the appropriate radio button to install the desired Zone Type
- Click Next and type the name of the zone you are creating.
- Click Next and then click Yes to create a reverse lookup zone.
- Repeat Step 5.
- Choose whether you want an IPv4 or IPv6 Reverse Lookup Zone

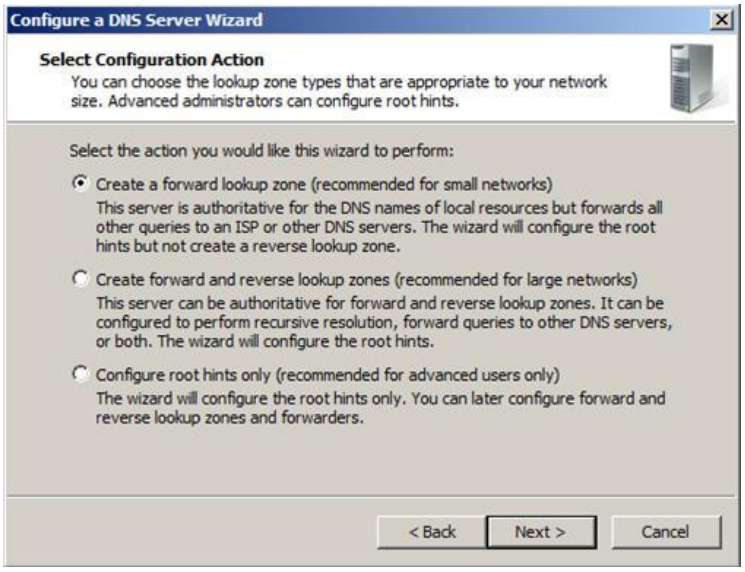
- Click Next and enter the information to identify the reverse lookup zone
- You can choose to create a new file or use an existing DNS file .
- On the Dynamic Update window, specify how DNS accepts secure, nonsecure, or no dynamic updates.
- If you need to apply a DNS forwarder, you can apply it on the Forwarders window.
- Click Finish .

ZONE

Database of DNS is called Zone.Or partition of domain name is called zone.when you click on zone then you will se e two zones one is forward look up zone and second is reverse look up zone.

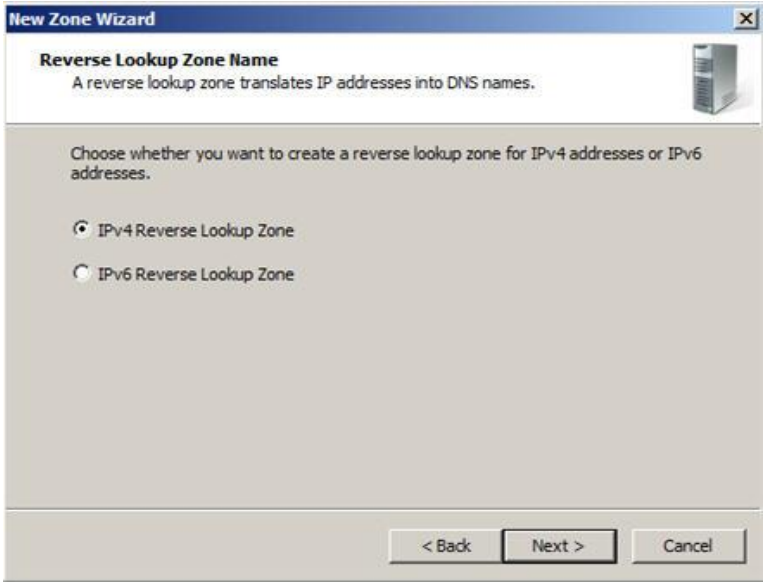
Forward Look up Zone

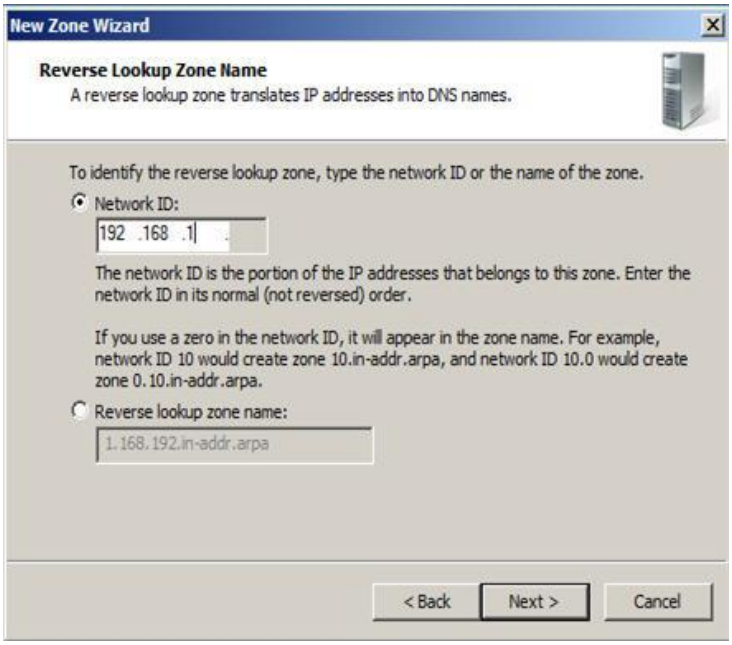
It send name and get ip adress of the computer .



Reverse Look up Zone

It send ip adress and get name of computer.





Steps to create a Zone

Here are process to crate the Zones.

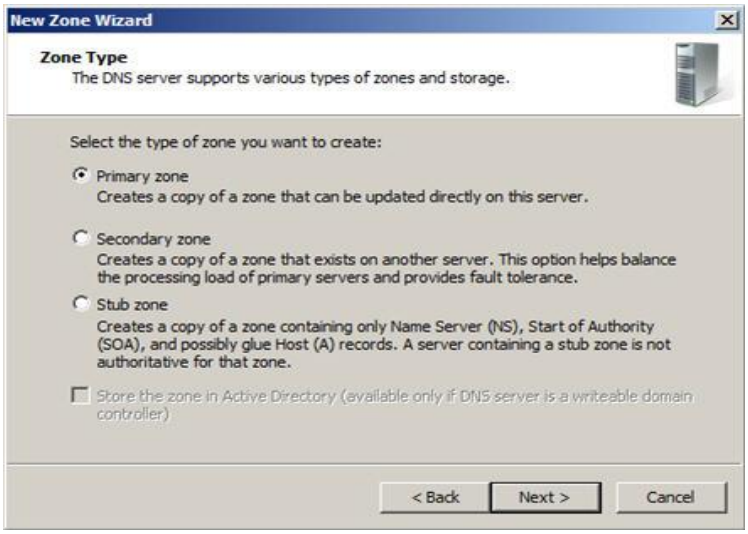
- Select forward look up zone.
- Right click on it and select new zone.
- Give name to the zone.
- Now right click on newly created zone.
- Create new host.
- Give name to the host.
- Give ip adress to the host.

ZONE TYPES

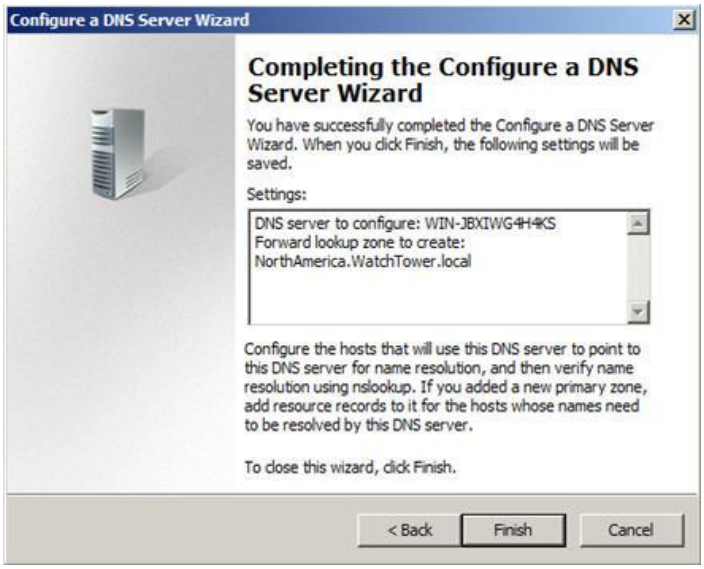
There are four types of zones.

Primery DNS ZONE

It is standard zone which is writeable.



Secondary DNS zone
It is also a standard zone which is read only



- Complete the configure a DNS server Finish

Chapter no.6

Windows Deployment Services (WDS)

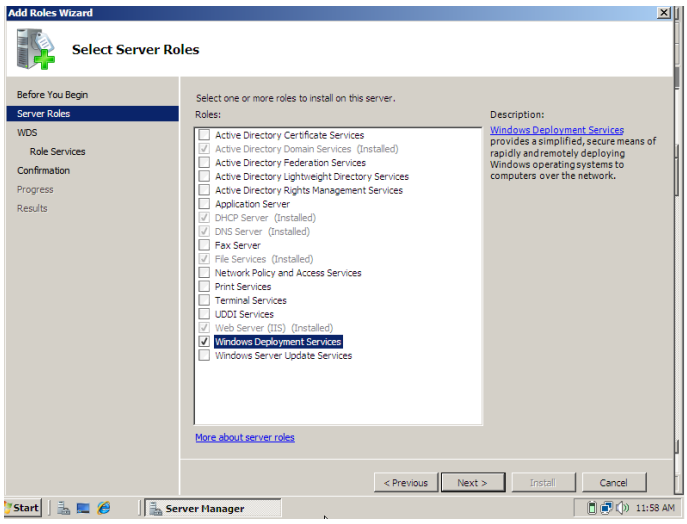
Windows Deployment Services (WDS) ?

Windows Deployment Services is the updated and redesigned version of Remote Installation Services (RIS). Windows Deployment Services enables you to deploy Windows operating systems over the network, which means that you do not have to install each operating system directly from a CD or DVD

Windows Deployment Services is a server technology from Microsoft for network-based installation of Windows operating systems. It is the successor to Remote Installation Services.[1] WDS is intended to be used for remotely deploying Windows Vista, Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012, but also supports other operating systems because unlike its predecessor RIS, which was a method of automating the installation process, WDS uses disk imaging, in particular the Windows Imaging Format (WIM). WDS is included as a Server Role in all 32-bit and 64-bit versions of Windows Server 2008, and is included as an optionally installable component with Windows Server 2003 Service Pack 2

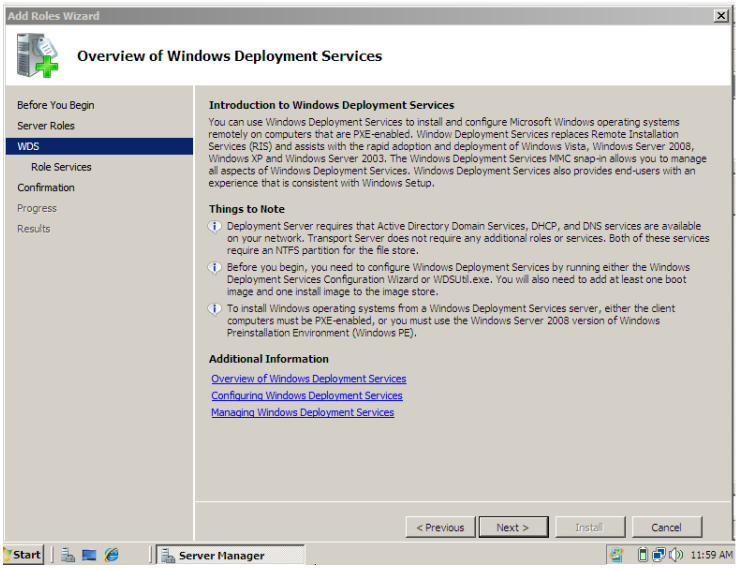
Steps Add the WDS role:-

In Server Manager, Highlight and select Windows Deployment Services and click next.

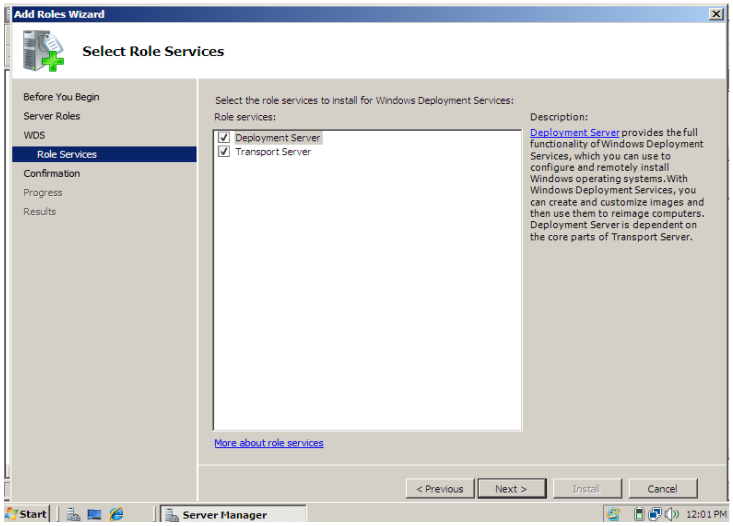


you will get an information screen which has some info including the following:

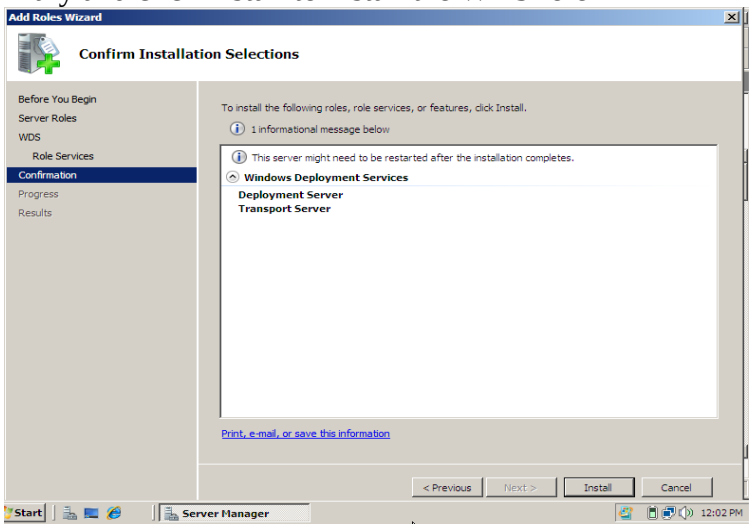
Before you begin, you need to configure Windows Deployment Services by running either the Windows Deployment Services Configuration Wizard or WDSUtil.exe. You will also need to add at least one boot image and one install image in the image store



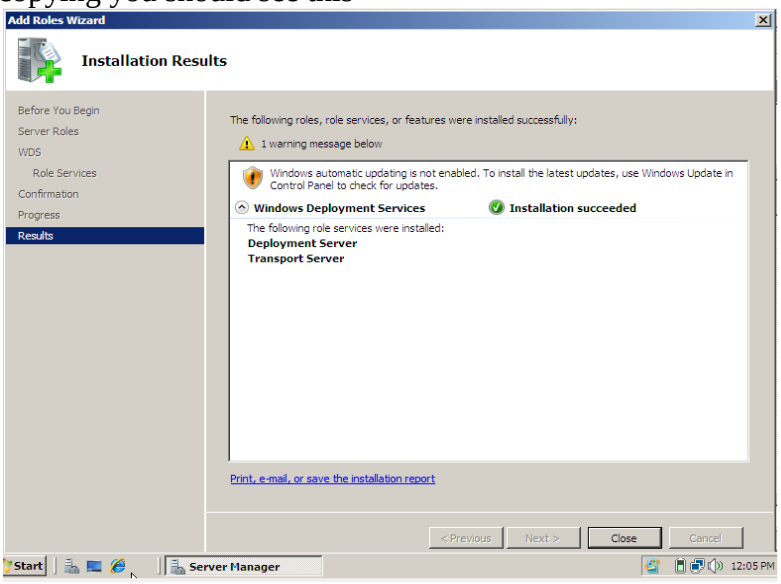
- Click next and notice the two role services listed, Deployment Server and Transport Server, make sure they are both selected and click next to continue.



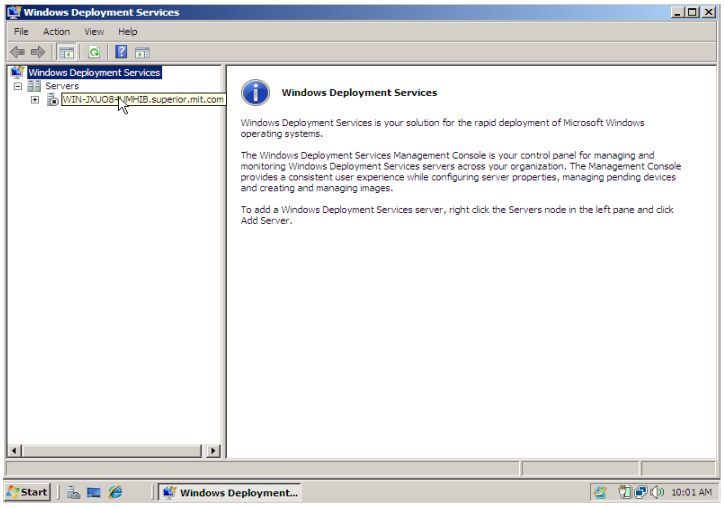
- View the summary and click install to install the WDS role



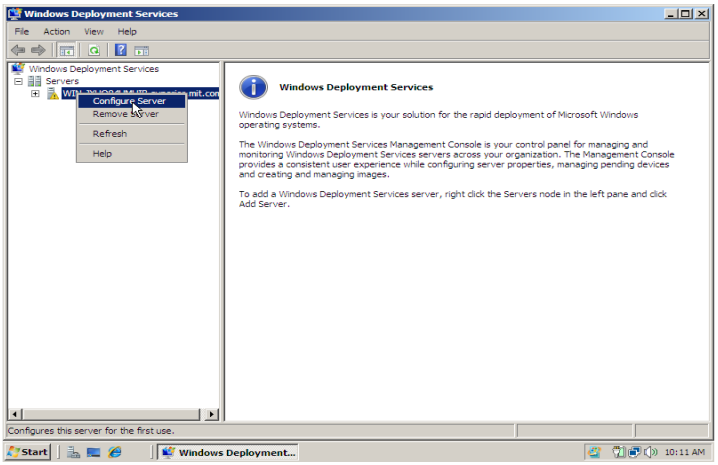
- After some copying you should see this



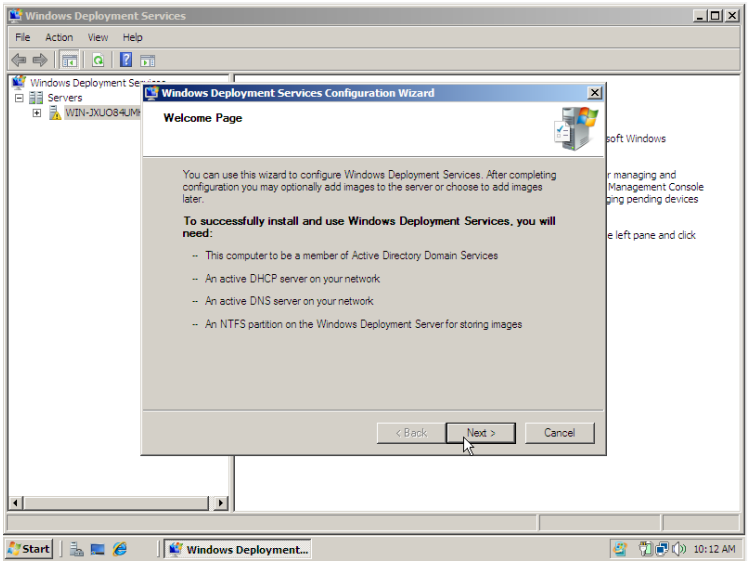
- Configure the Windows Deployment Services gui (mmc snap in)
- Click on Start/All Programs/Administrative tools/Windows Deployment Services.
- At this point we can see that WDS is not configured yet**,** so let's do that now.



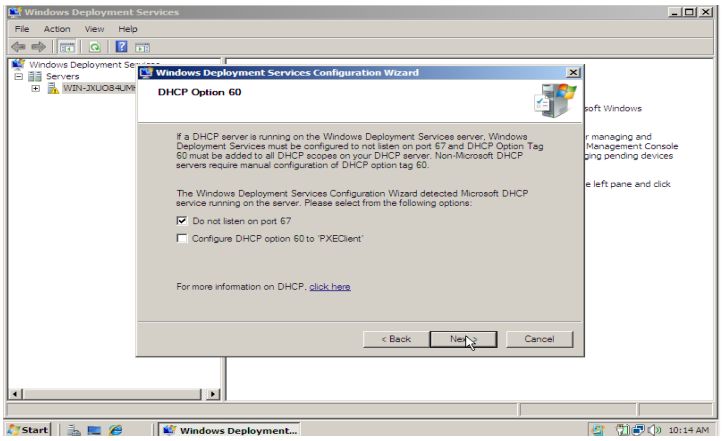
- Right click on the server name in the left pane and choose Configure Server

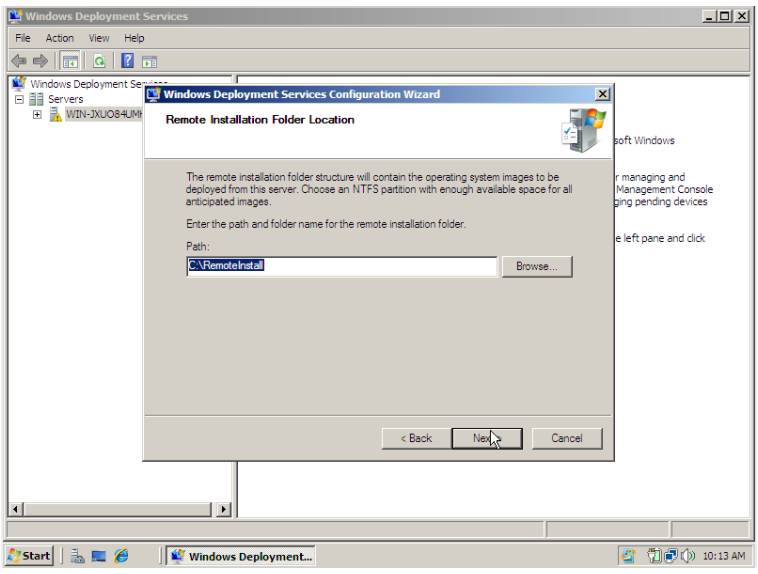


- At the welcome page click next

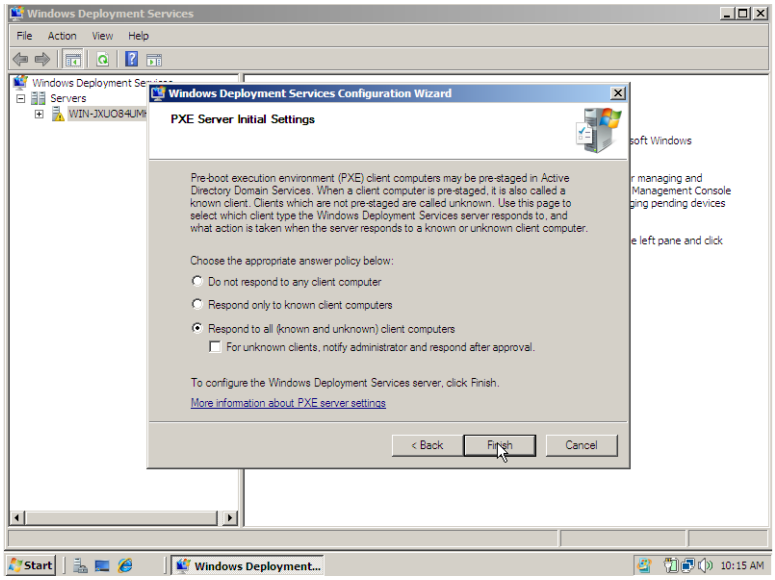


- change the remote install path from the default C:\RemoteInstall to D:\RemoteInstall.

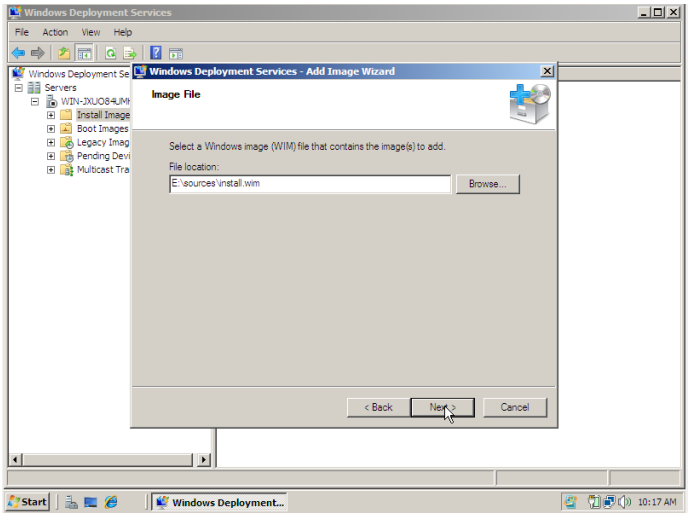




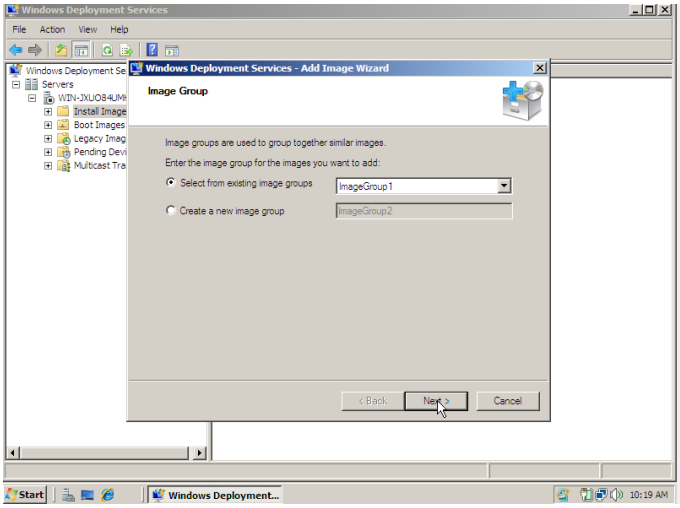
- we put a checkmark in each of the DHCP options then clicked next
- I then chose to respond to all known and unknown computers (by default it's set to Do not respond to any**)**



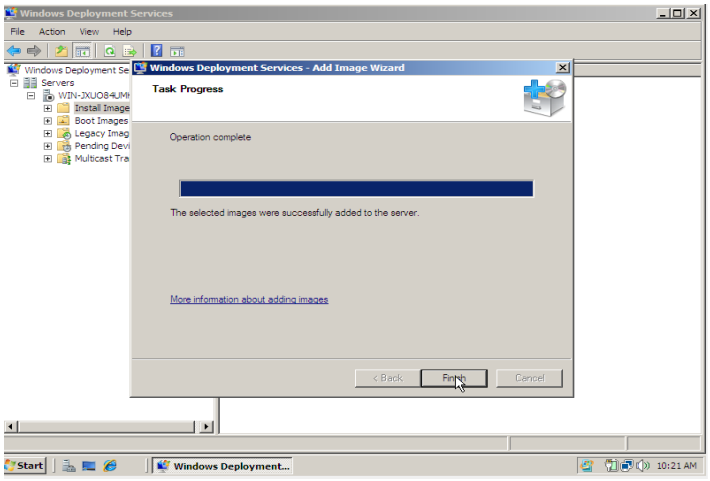
- clicking on Finish applies these settings when done, you'll be told that the configuration is complete and that you can now add images to the WDS server**,**
- click on Finish (again).
- The Windows Deployment Add image wizard will appear, insert your Windows 2008 Server DVD and click Browse, select the sources folder on the Windows 2008 DVD and then click next.



- You'll be prompted to create a new image group, lets call it ImageGroup1 (the default name, you can change it later to Windows Server 2008 or Windows Vista Sp1 or whatever...)

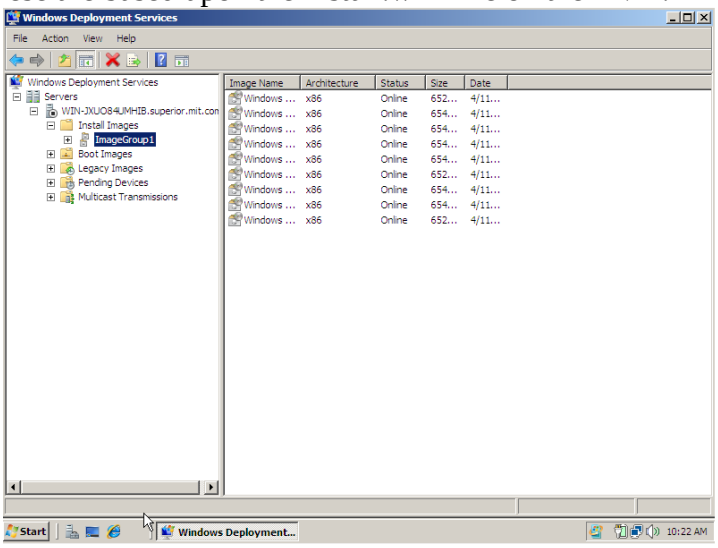


- After a long while, the selected images will be added to the WDS server



- click finish and review the WDS server as it is now

- In the Install Images pane, we can see the six available images from the Windows 2008 Server DVD, these are based upon the install.wim file on the DVD.



- you can now PXE boot your client computers to the Windows 2008 WDS server. troubleshooting note: if you add a new image to WDS and attempt to pxe boot and then install the image but get an error saying something like 'could not display the list of' then make sure you have used BOOT.WIM from a Windows Server 2008 DVD or Windows Vista sp1.

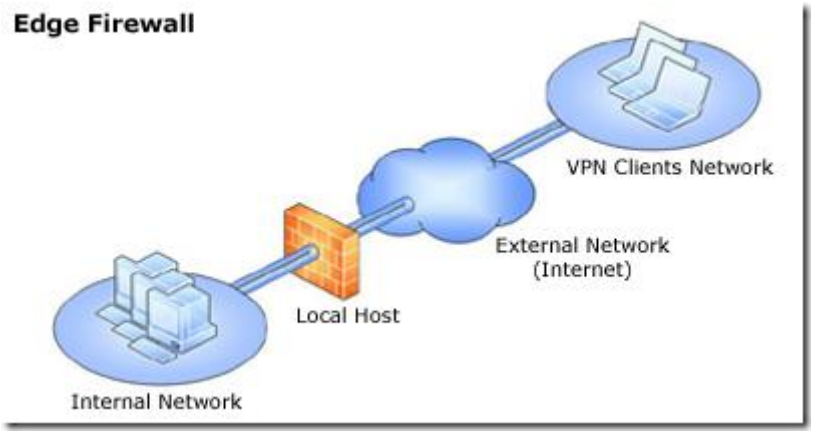
Chapter no. 7

Threat Management Gateway

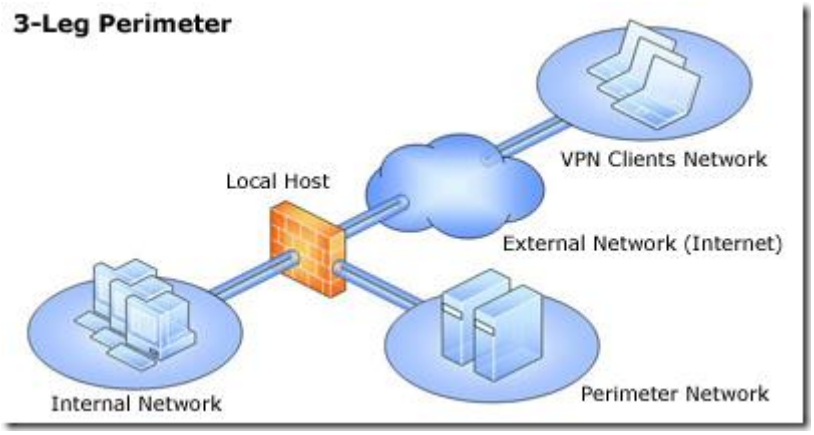
TMG 2010 has been built on top of the core capabilities delivered in Microsoft Internet Security and Acceleration (ISA) Server 2004/2006 in order to deliver a comprehensive, enhanced and integrated network security gateway. TMG provide additional protection capabilities to help secure the corporate network from external/Internet-based threats.TMG 2010 prevent abuse of networks from internal and external entity. Forefront provide more management capabilities in terms security and protection. TMG 2010 is available in Standard Edition and Enterprise Edition. Standard version does not support Array/NLB/CARP support and Enterprise Management. For E-mail Protection both version requires Exchange license.

TMG 2010 provide the following enhanced protection capabilities:

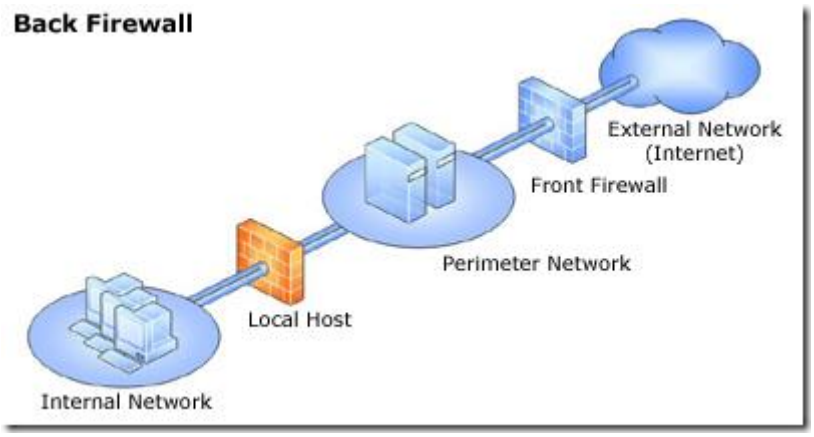
- Malware inspection
- URL filtering
- HTTP filtering
- HTTPS inspection
- E-mail protection
- Network Inspection Systems (NIS)
- Intrusion detection and prevention
- Secure routing and VPN
- Understanding Network Topology
- The following TMG network topologies are available:
- Edge firewall—In this topology, TMG is located at the network edge, where it serves as the organization's edge firewall, and is connected to two networks: the internal network and the external network (usually the Internet).

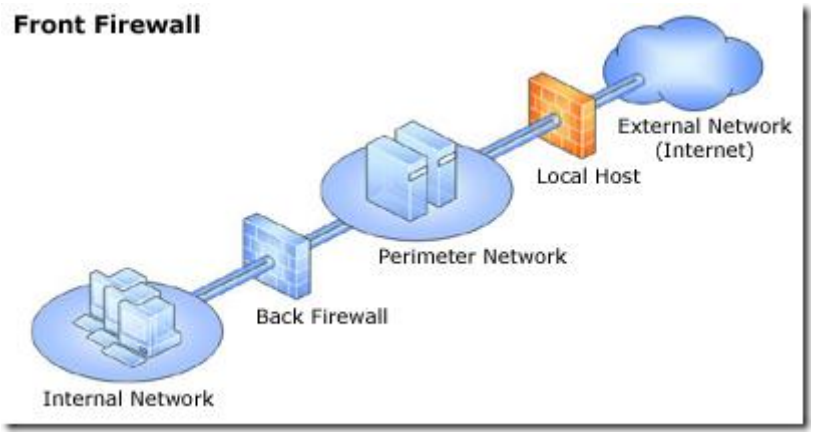


- 3-Leg perimeter—This topology implements a perimeter (DMZ) network.TMG is connected to at least three physical networks: the internal network, one or more perimeter networks and the external network.



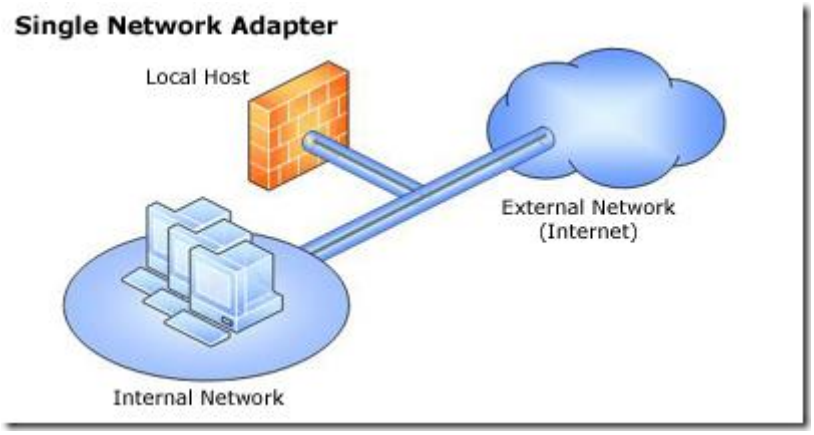
- Back firewall—In this topology, TMG is located at the network's back-end. Use this topology when another network element, such as a perimeter network or an edge security device, is located between TMG and the external network.TMG is connected to the internal network and to the network element in front of it.





- Single network adapter—This topology enables limited TMG functionality. In this topology, TMG is connected to one network only, either the internal network or a perimeter network. Typically, you would use this configuration when TMG is located in the internal corporate network or in a perimeter network, and another firewall is located at the edge, protecting corporate resources from the Internet

.



- Functionality of a single network adapter topology
- The single network adapter topology enables limited TMG functionality, that includes:

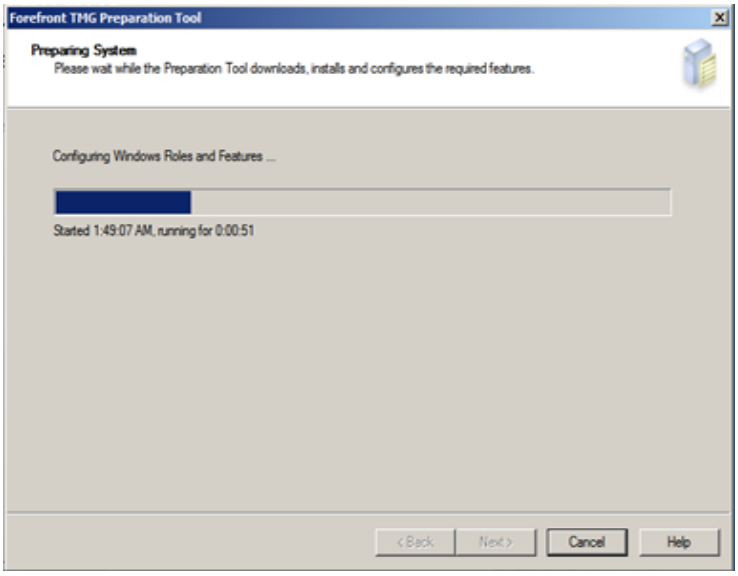
- Forward (CERN) proxy for HTTP, HTTPS, and CERN proxy FTP (download only).
- Web caching for HTTP and CERN proxy FTP.
- Web publishing. HTTP-based communications, such as Microsoft Office SharePoint Server, Exchange Outlook Web Access 2007, ActiveSync®, and remote procedure call (RPC) over HTTP (Outlook Anywhere, Terminal Services Gateway or WSMAN-based traffic).
- Dial-in client virtual private network (VPN) access.
- Limitations of a single network adapter topology
- The following limitations apply when you use the single network adapter topology:

- Server publishing and site-to-site VPN are not supported.
- Secure NAT and TMG Client traffic are not supported.
- Access rules must be configured with source addresses that use only internal IP addresses.
- Firewall policies must not refer to the external network.
- Hardware Requirements
- Systems requirements depends on number of users and deployment scenario. TMG is a vital part in a ICT infrastructure. To achieve best performance, you must add best processing power and memory in TMG server however the following will give you an optimum performance.Processor- Intel Xeon (Dual core/Quad-core/i7) or AMD Option (dual core/quad core). Intel Hyper-Threading Technology enabled in bios if Intel server board.
- RAM-8GB
  Disk Space –50GB systems partitions and 150GB logging +60GB-100GB Web caching in a separate partition. RAID 5 configuration would be highly recommended. NIC- 2 Gigabit NIC with redundant configuration (number of NICs depends on deployment scenario)
- Important! TMG has been built on 64 architecture.
- Operating Systems and features
- Windows Server 2008 SP2 64 bit or Windows Server 2008 R2Microsoft .NET Framework 3.5 SP1Windows Web Services API Network Policy Server. Routing and Remote Access Services. Active Directory Lightweight Directory Services Tools. Network Load Balancing Tools. Windows Power Shell Windows Installer

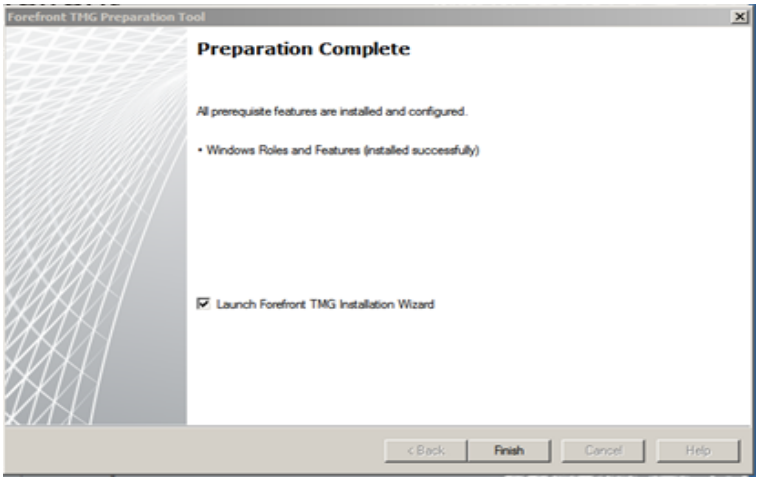
4.5Important! It's not recommended to install any application or programmed in TMG server other then antivirus program. It must be a dedicated server for TMG. Disable unnecessary services after installing operating systems. Install Machine Certificate from Enterprise Root CA Authority before installing TMG. TMG server must be a member of Active Directory Domain.

- Installation of Forefront TMG
- Prepare a 64 bit Windows Server 2008. Insert Forefront TMG DVD into the server. Run preparation tools.

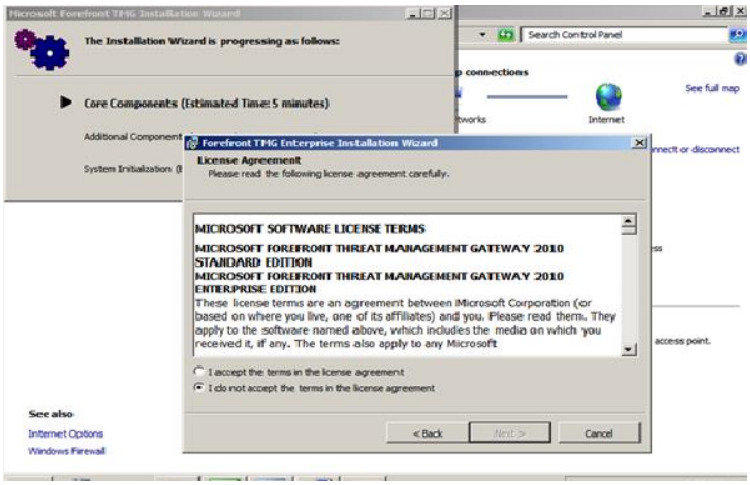
- Wait for the system to install preparation tools



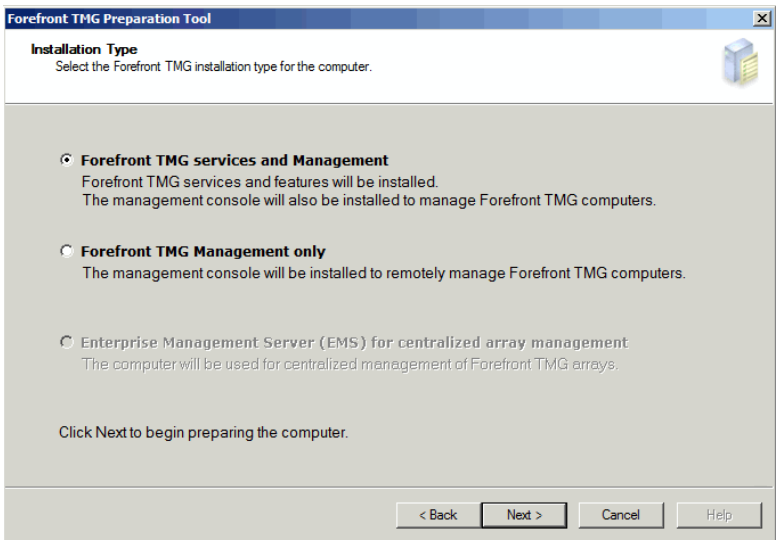
- Now click the finish button to complete the preparations tools wizard.



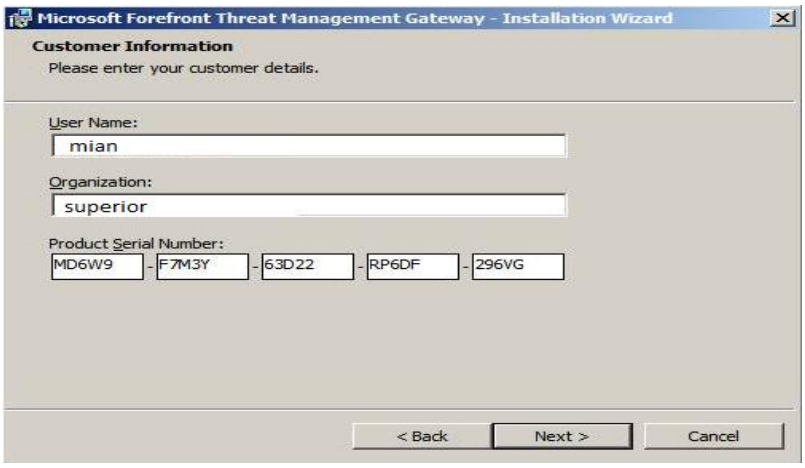
- Skip the welcome screen by clicking Next**.** To be able to continue with the installation you need to accept the EULA, so choose I accept the terms in the license agreement**,** then click Next**.**



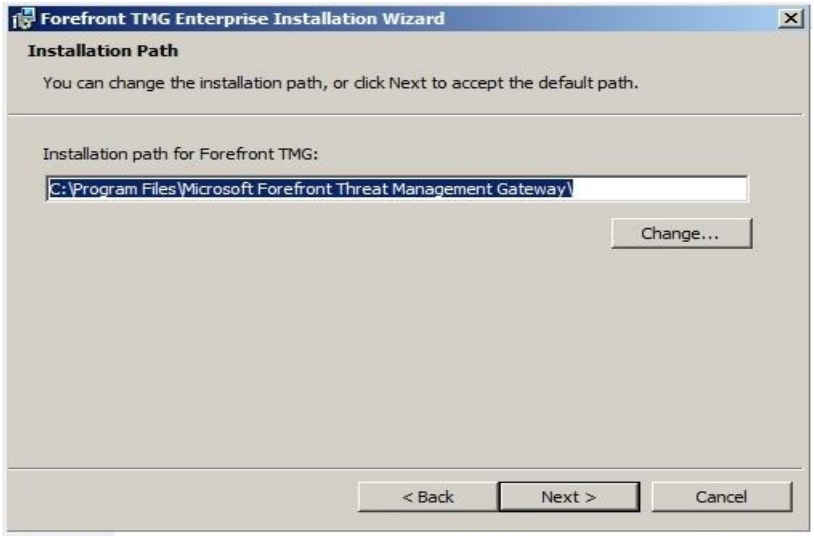
- On the Setup Scenarios page, you have the option to install the Forefront TMG or install only the TMG Management console. we'll select Install Forefront Threat Management Gateway and click Next.



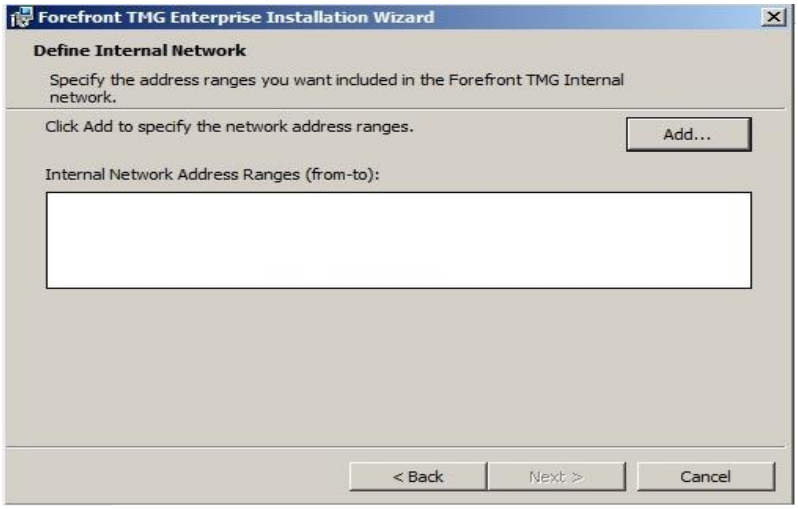
- On the Customer Information page, enter your User Name and Organization. The Product Serial Number will be filled in for you. Click Next.



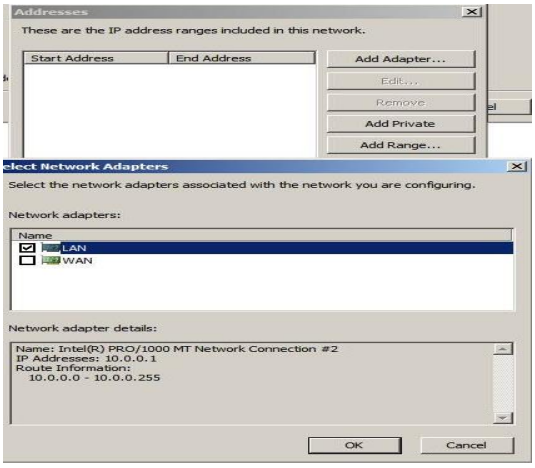
- Leave the default installation path and click Next**.**

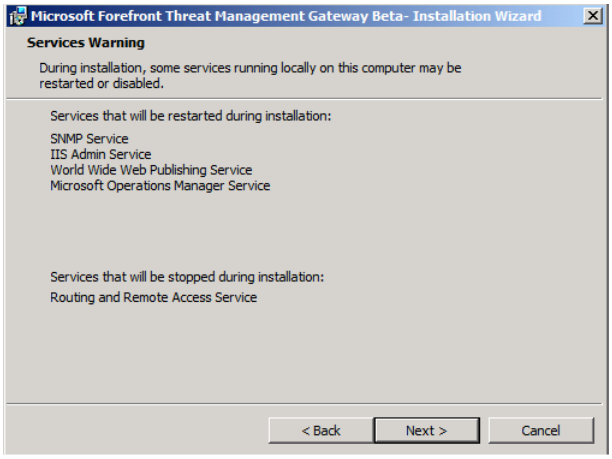


- Click the next button appear appears on forefront TMG.

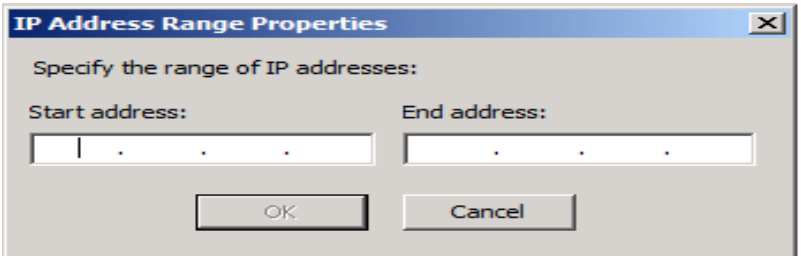


- Firstly click on the add adapter button then add adapters in Wizard.

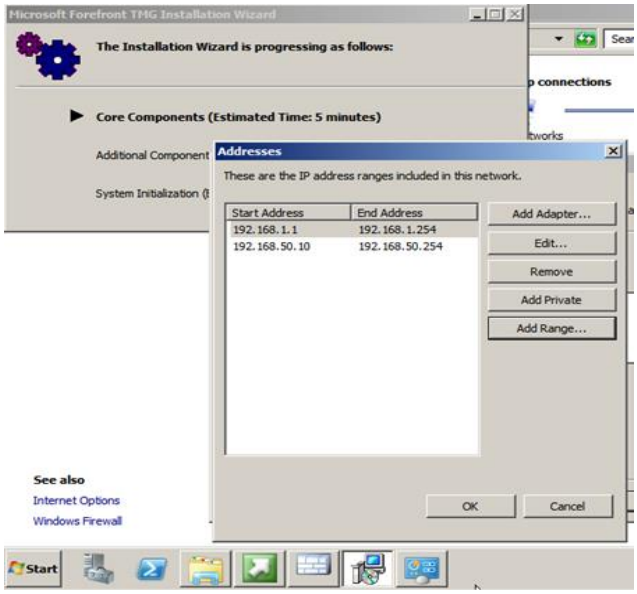




- Now define the ranges of ip addresses in both the adapters with respect to your network.

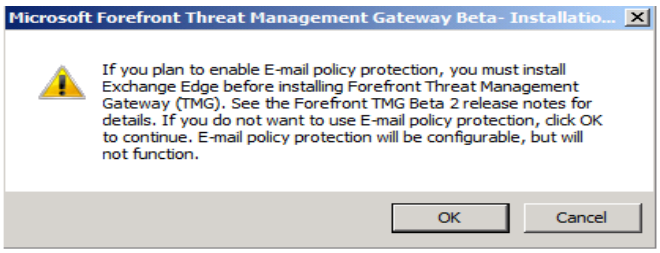


- When you finish defining ip addresses click ok button and this screen appears.

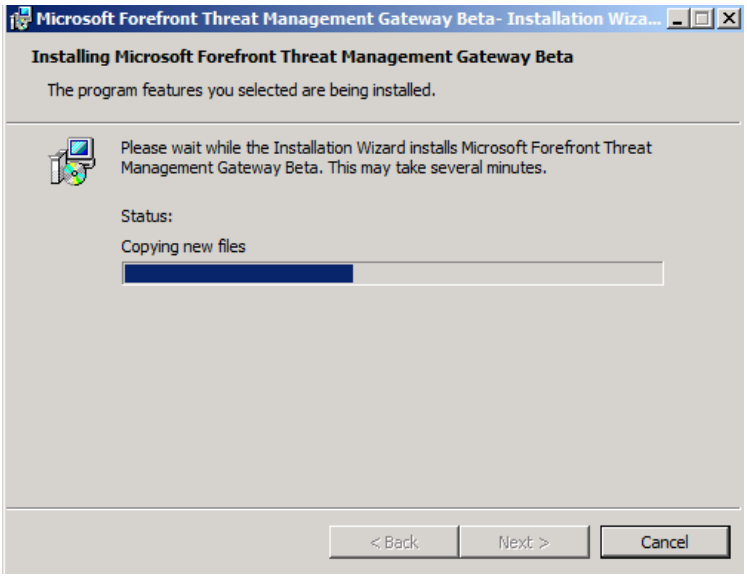


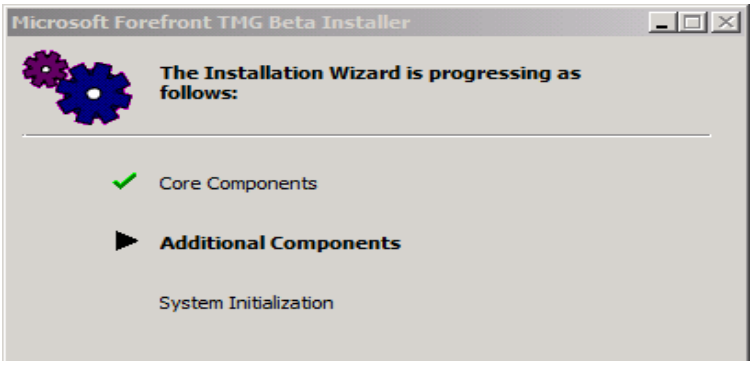
- On the Services Warning page, you will be notified that the following services will be restarted or disabled during installation as seen in the below screen shot,

- Click Next Ok, we are set for the installation, on the Ready to Install page, click Install
- click on the OK button so that installation continues, else if you do plan to use the E-mail policy protection, click on the Cancel button, install Exchange Edge and then run the Forefront installation again.

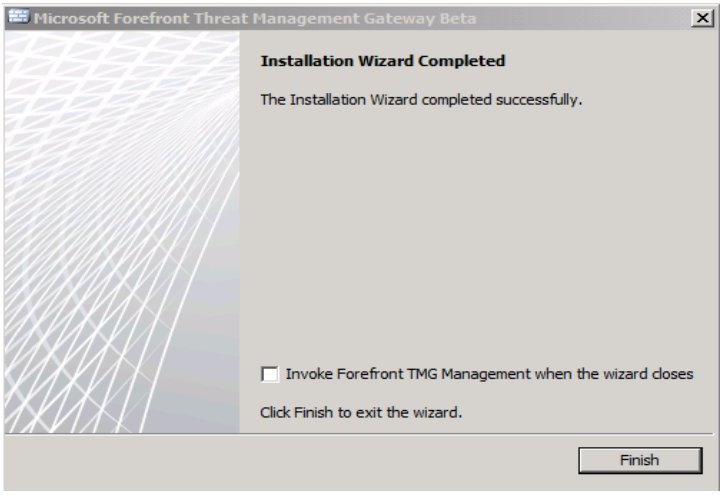


- Installation will proceed and wizard will show the following screens by clicking on next button on wizard.

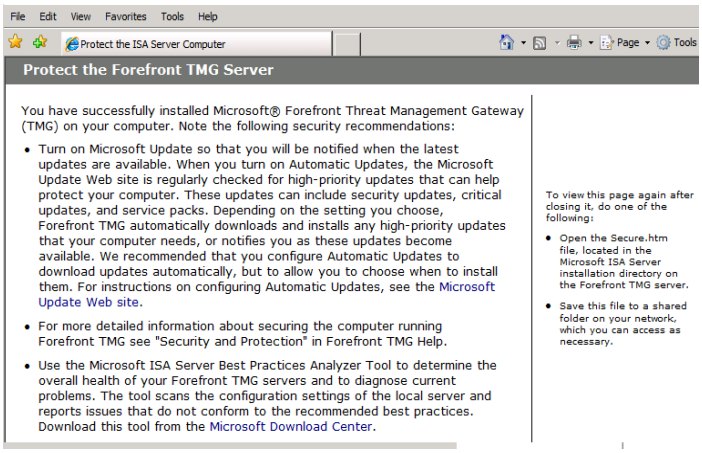




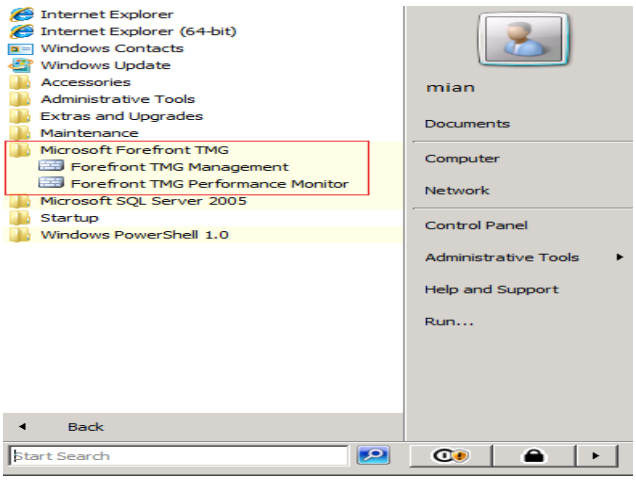
- When installation completes, you can invoke TMG Management when the wizard closes by enabling the checkbox available in the below screenshot. Click on Finis



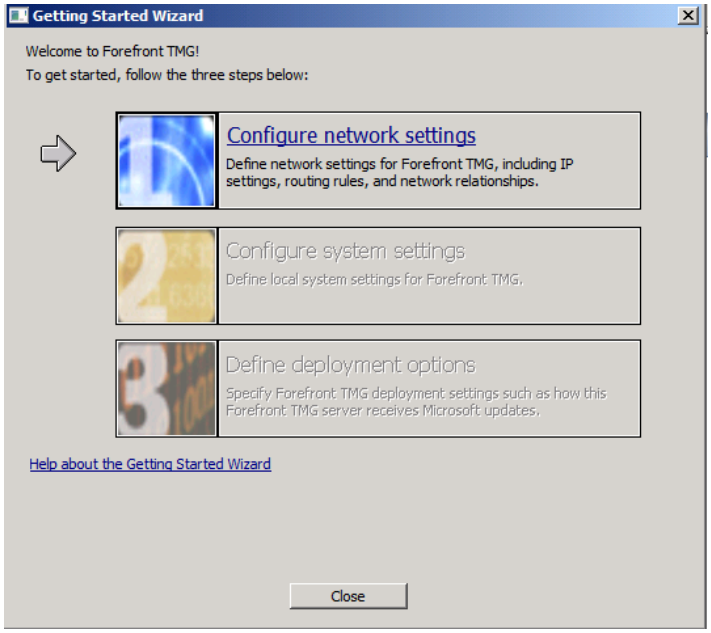
- An html page will pop up after you click the Finish button, listing few recommendations. Take a read them.

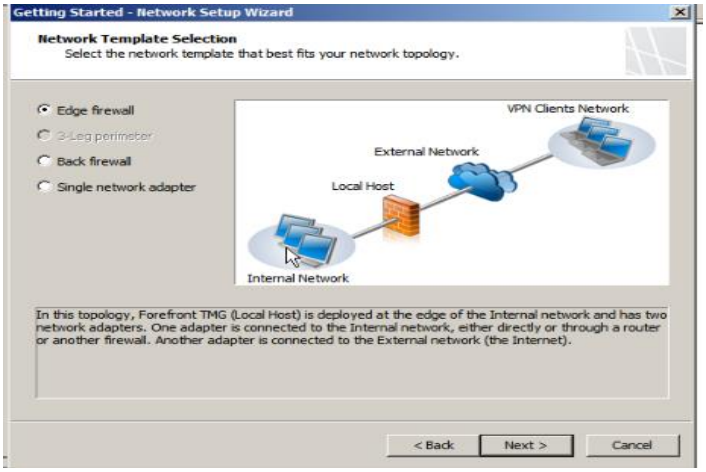


- To open Forefront TMG Management Console, click on Start > All Programs > Microsoft Forefront TMG**,** click on Microsoft Forefront TMG Management.

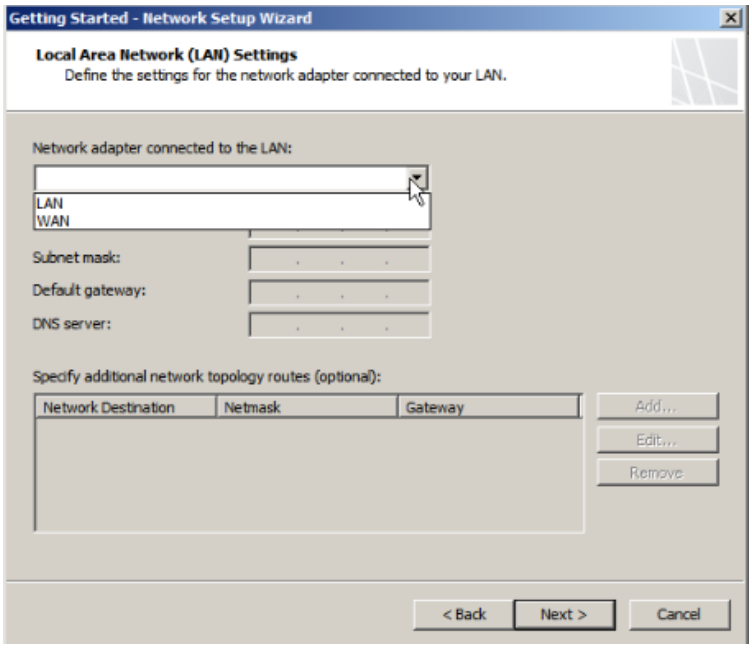


- Forefront TMG management console will open, and we will be greeted with the Getting Started Wizard page opened. This wizard is used to configure or modify basic deployment settings.

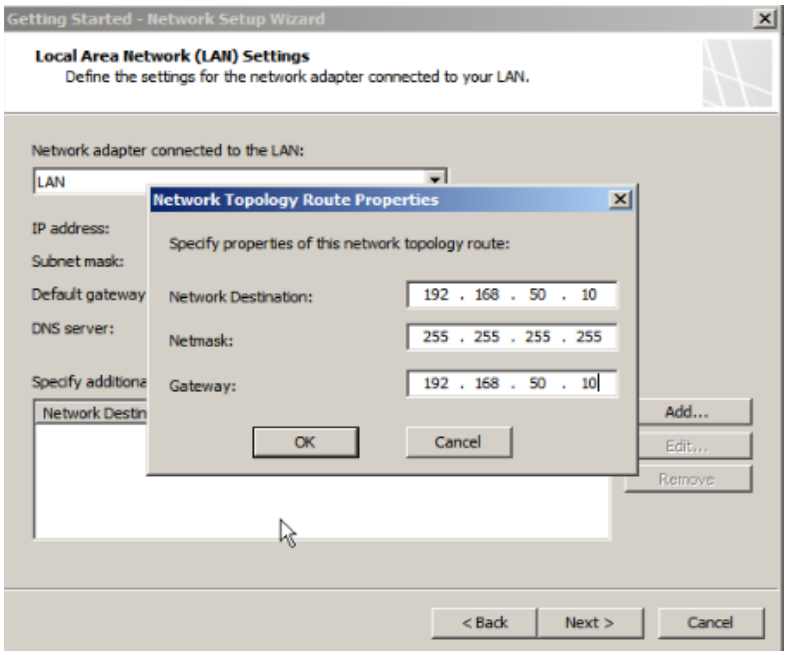




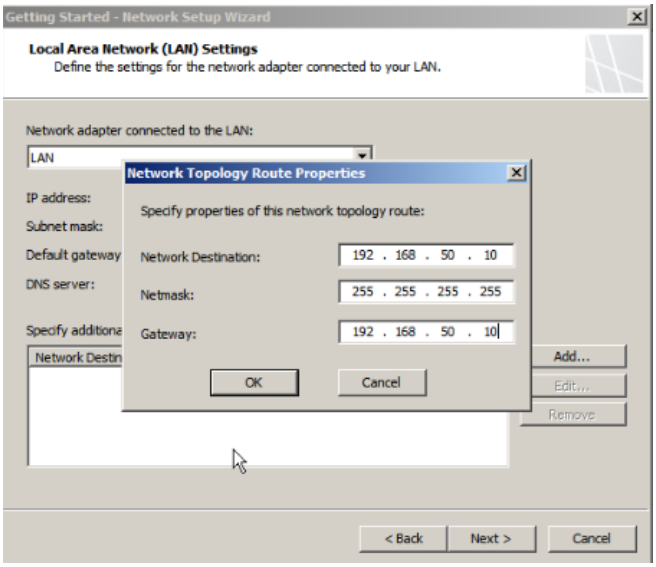
- Now select edge firewall radio button on this diagram and click the next button.



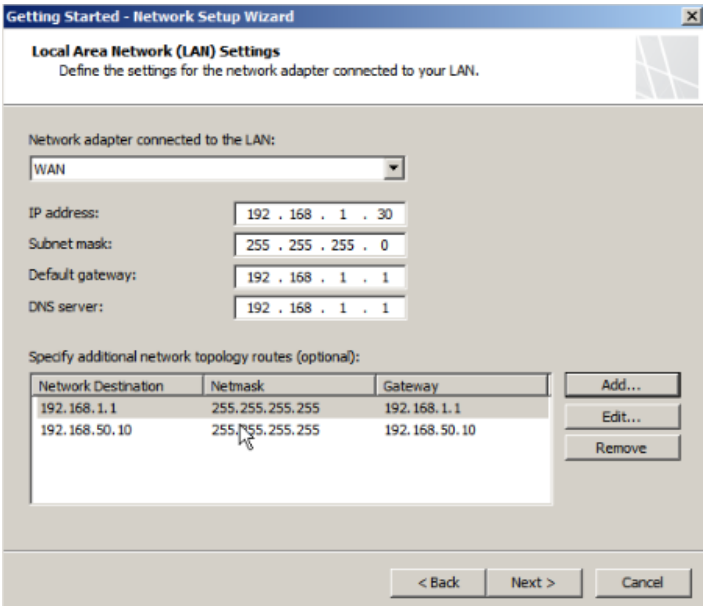
- Now drop down the network adapter connected to network in TMG and select the networks one by one.



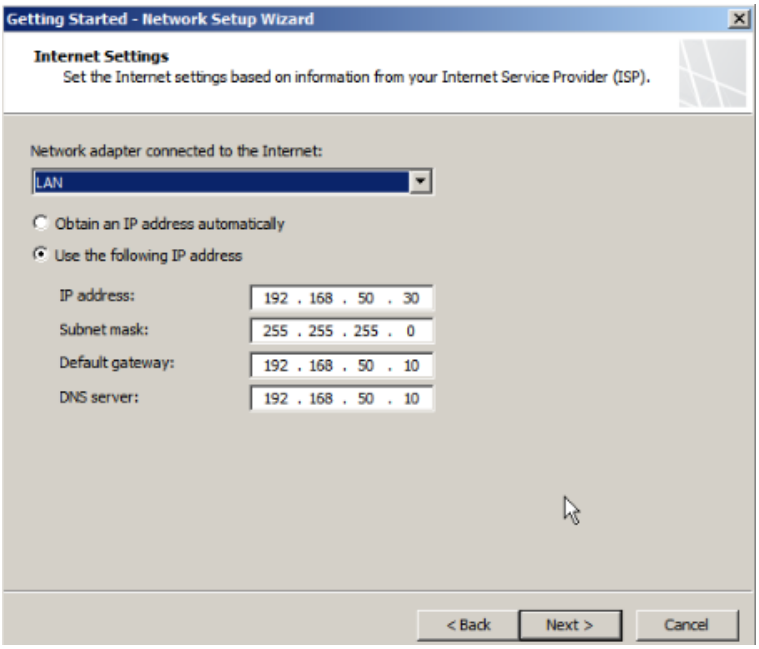
- Now when you have added adapters by click the add button wizard will show network route properties now define the ip addresses for network destination and default gateway for both LAN and WAN.



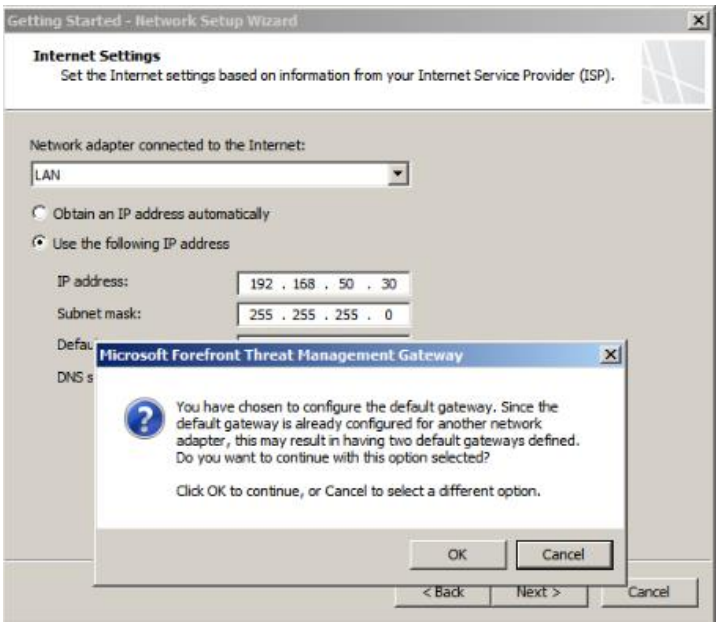
- When you added the ip addresses on both LAN and WAN it would see like that on screen.



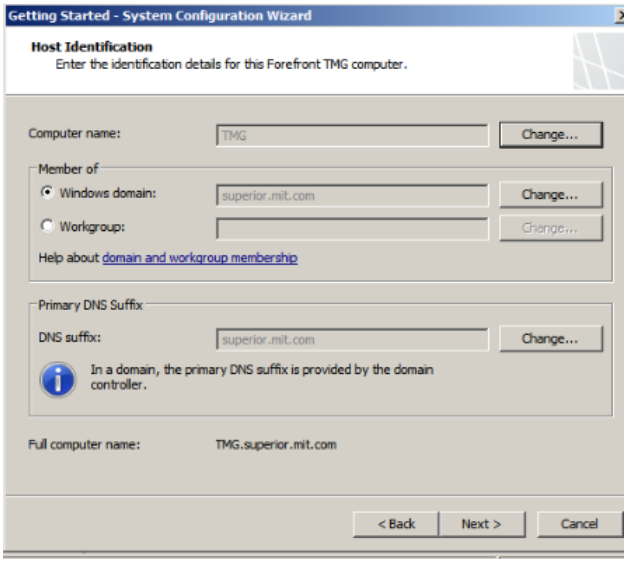
- After clicking ip address of LAN and WAN click next button on wizard.



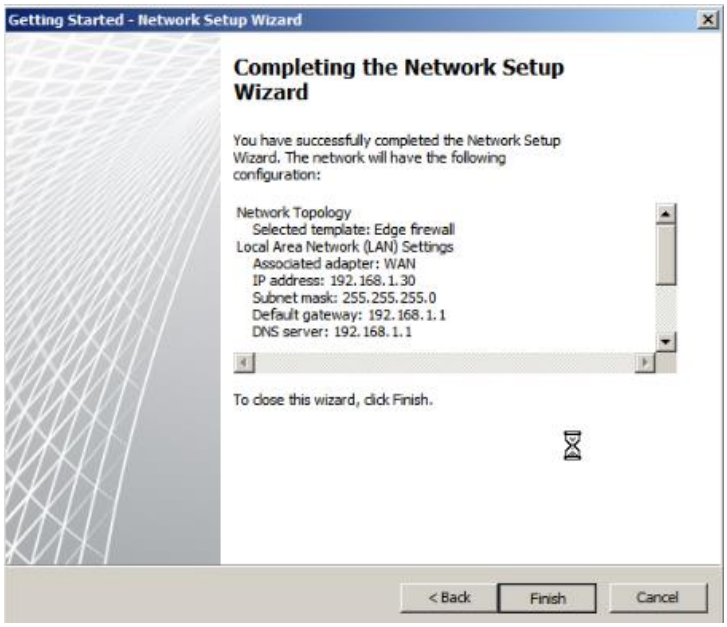
- When you click the next button wizard would show the message you have already configure the default gateway for other network click it ok .



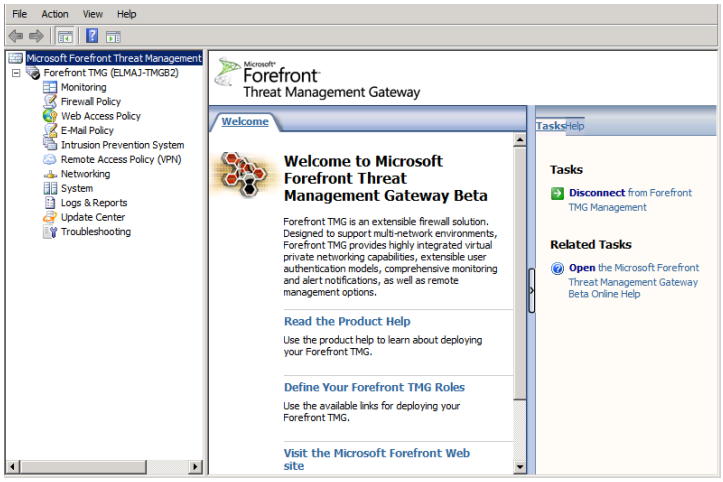
- Now when you click the next button it will by default show the name of system and also show the domain name.



- Finish button to complete the setup wizard.

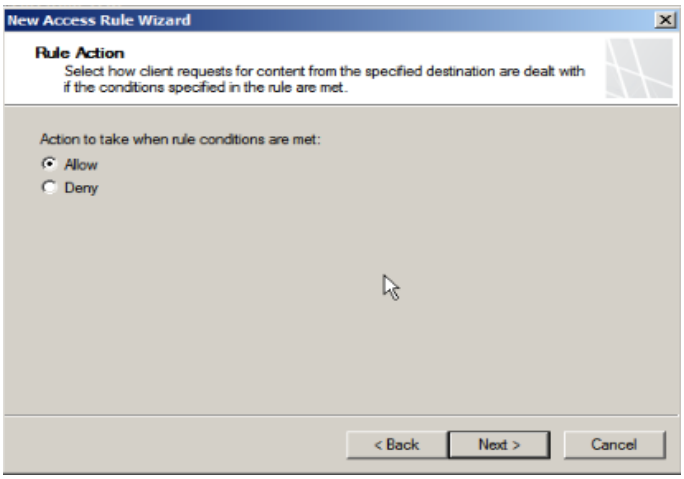


- For the time being you can ignore this wizard and click on Close**.** I did this because I want to show you the left pane multiple new nodes such as Web Access Policy , E-mail Policy, Intrusion Prevention System , Logs & Reports and Update Center.

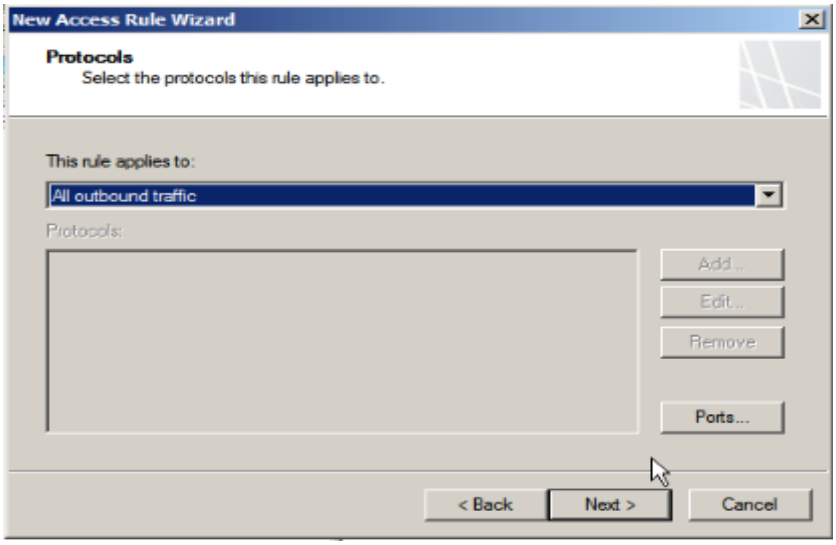


- Now on the left of the screen expand forefront TMG .right click on fire wall policy add access rule

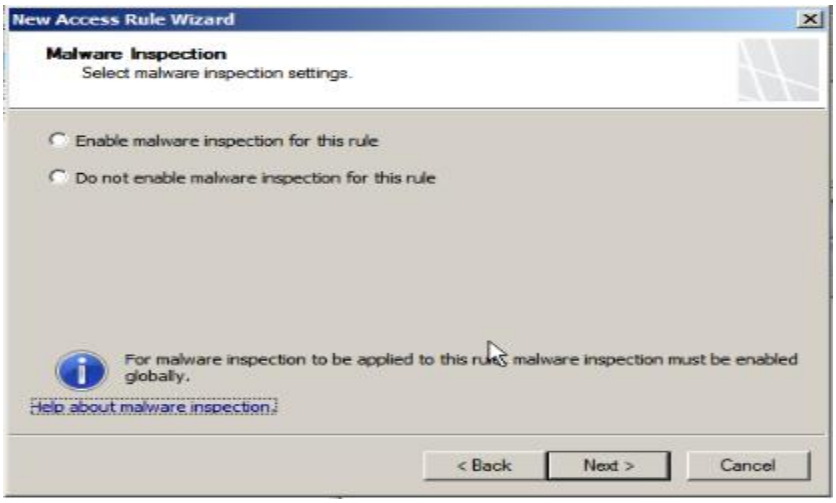
- Click the next button of wizard and check radio button allow on screen.



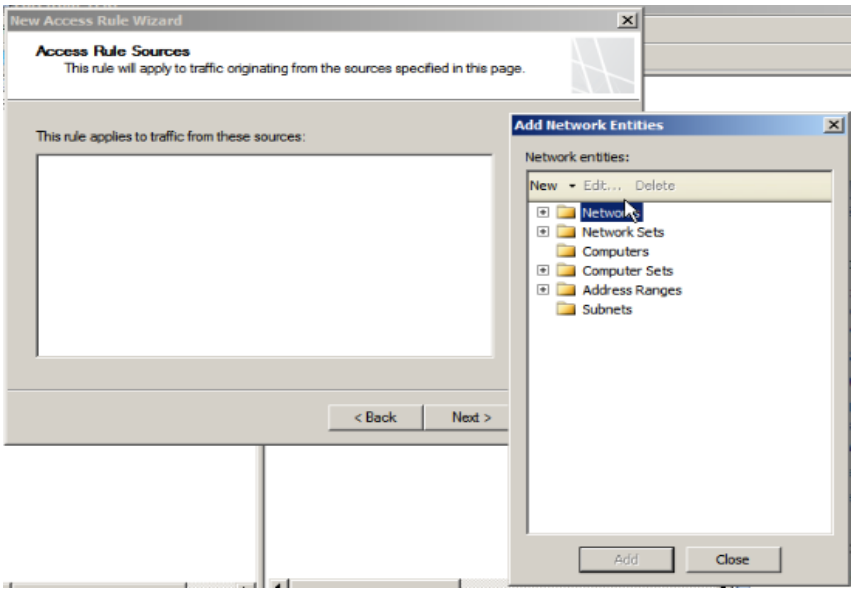
- Click the next button on wizard select all out bounded traffic from drop down list.



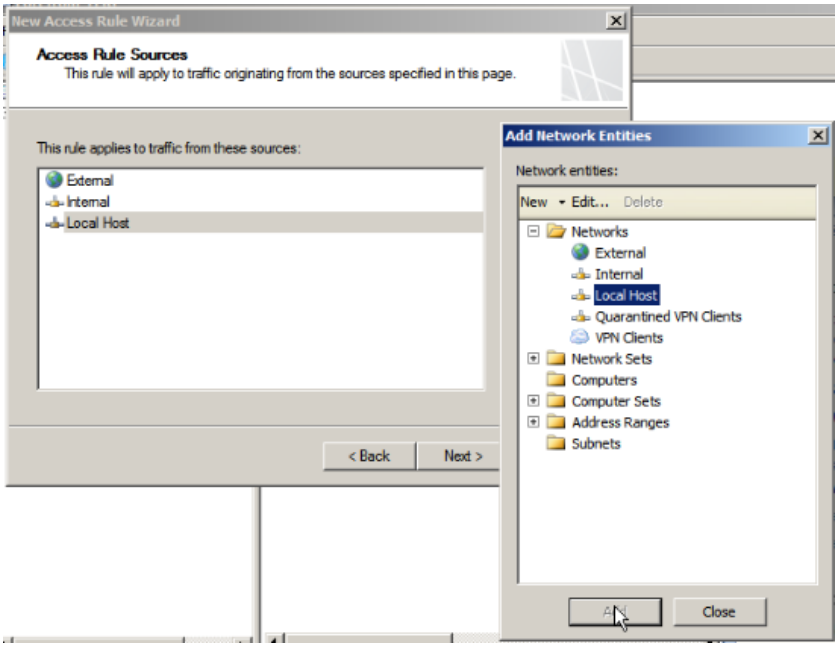
- Click next button and select enable malware selection for this rule.



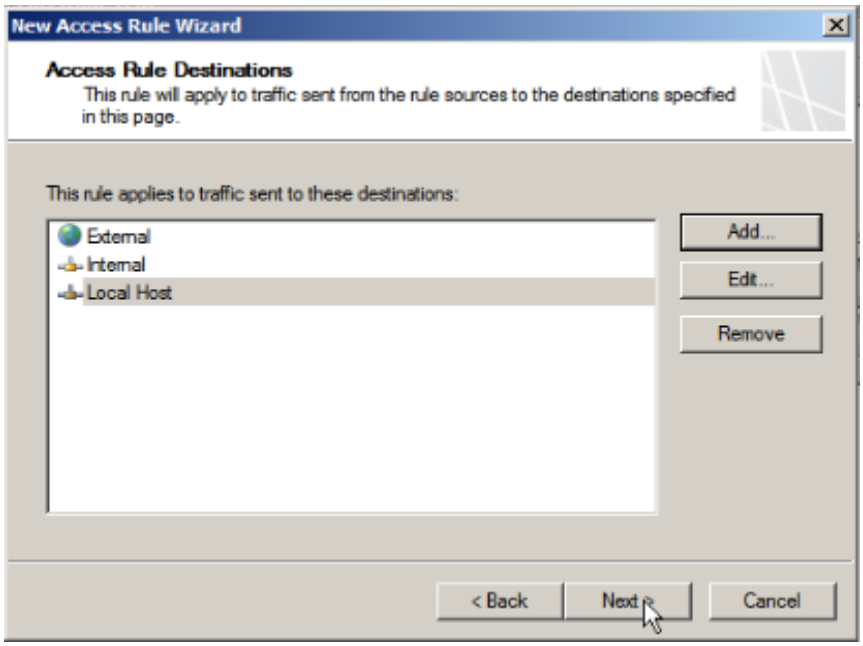
- Now when you click the add button to add internal and external networks.



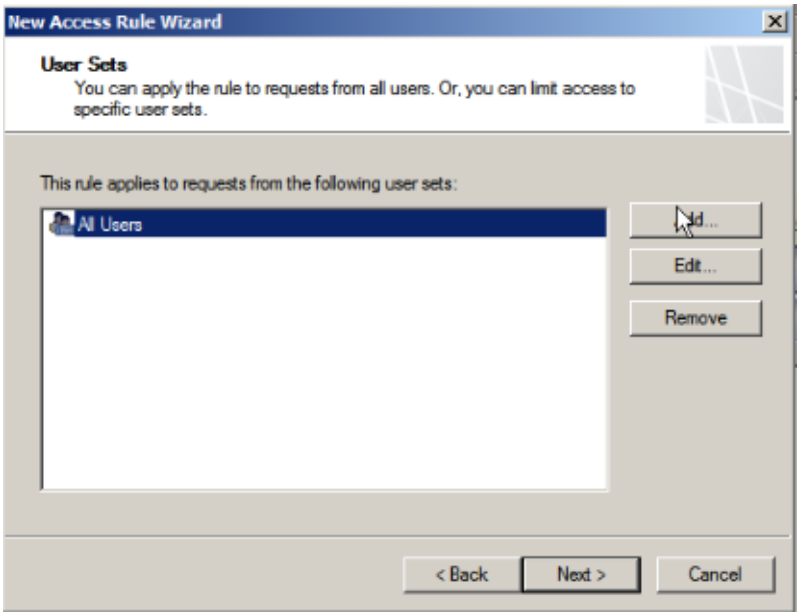
- Now expand network by clicking on networks and add internal and external networks and local host one by one.



- After adding them click the next button to continue wizard of threat management gateway.

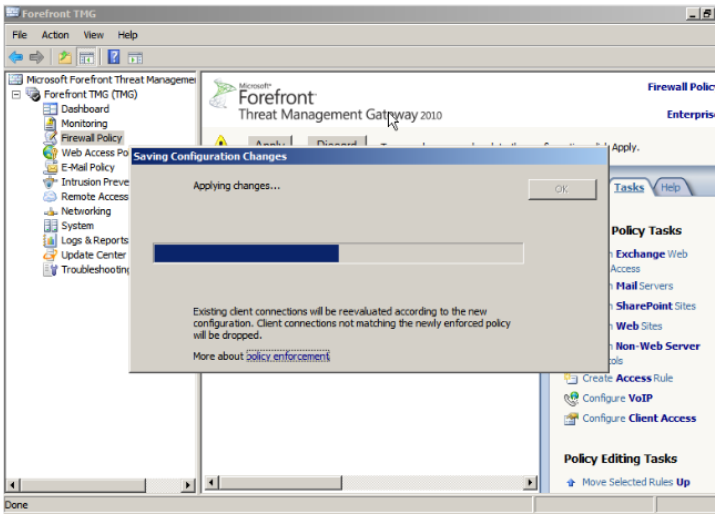


- Now on the next screen wizard click all users to add users and click next button.

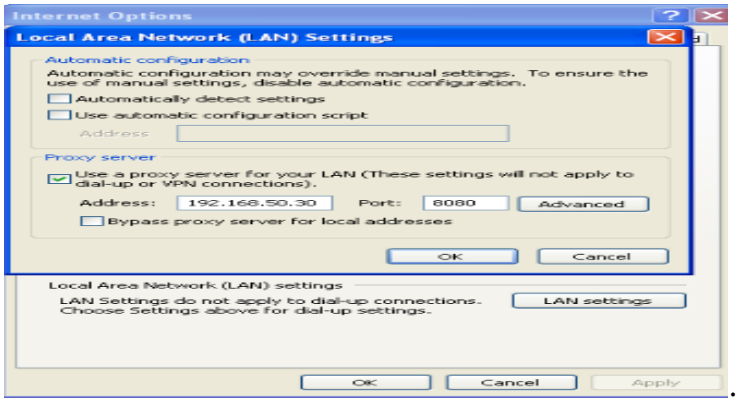


- To complete the setup click finish button to complete button to finish button to complete setup.

- After finishing the button following screen will appear now click apply on the top of screen to save and apply the changes.



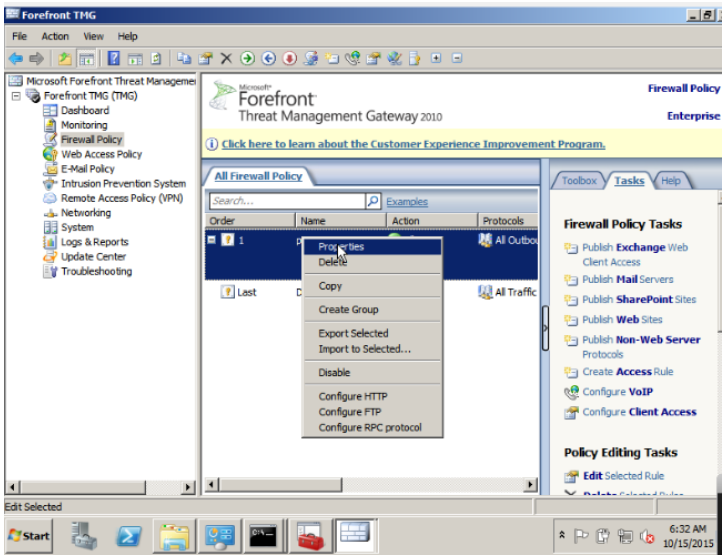
- Now power on the client on the server and open internet explorer go to internet options>connections>LAN settings and assign the ip address of TMG and port 8080 and click ok.



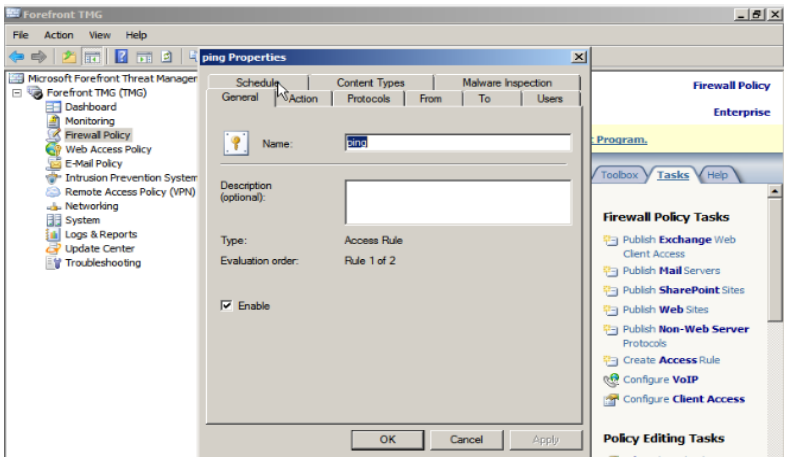
.

- Now when you enter web address it will go to TMG and give the internet access

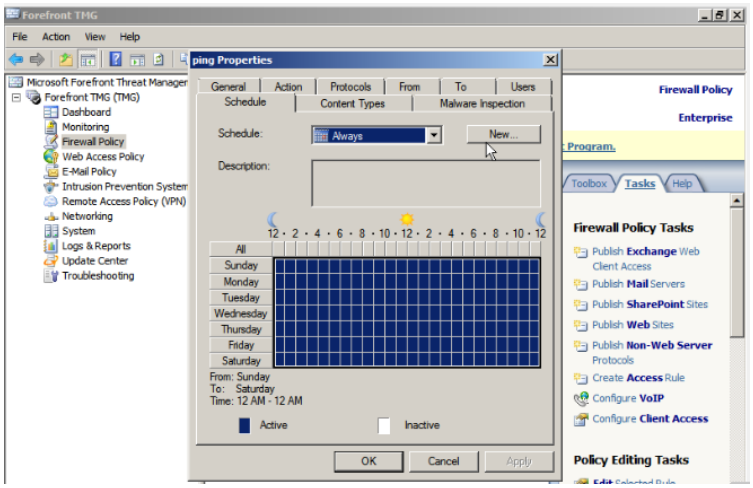
.



- Now for a policy and for new user on TMG right click on ping and go to its properties as shown above.



- Now for the user click on the new button on the right corner of screen.



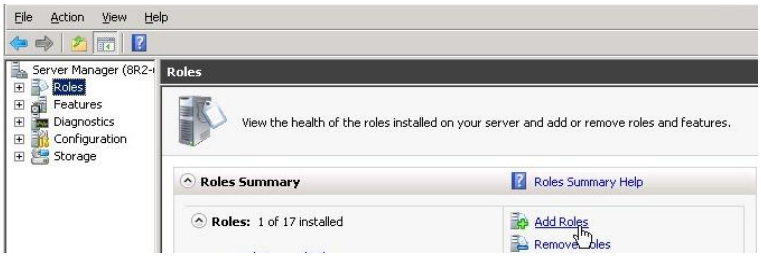
- When you click new it will ask for user enter the user to complete the wizard of user policy in TMG.

Chapter no. 8

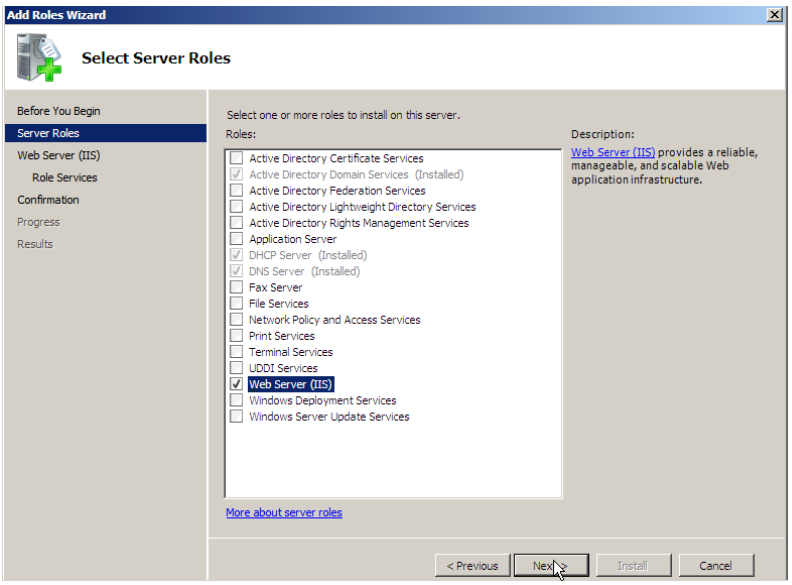
File Transfer Protocol (FTP)

FTP, also known as File Transfer Protocol, is a protocol for the rapid, simple transmission of files across a network supporting the TCP/IP protocol. This network is generally the Internet, or a local network. FTP is a way of accessing files on another computer. FTP uses the Client-Server architecture, meaning that there is a server that holds the files, and does the authentication, and a client, or the end-user, who is accessing the files. The server listens on the network for connection requests from other computers. The client can make a connection to the FTP server by using FTP client software. Once connected and authenticated (via SFTP) the client can do things such as uploading files, to the server, downloading files (taking the server's files and putting them on his own computer) from the server, and renaming, deleting files on the server, changing file permissions, etc.

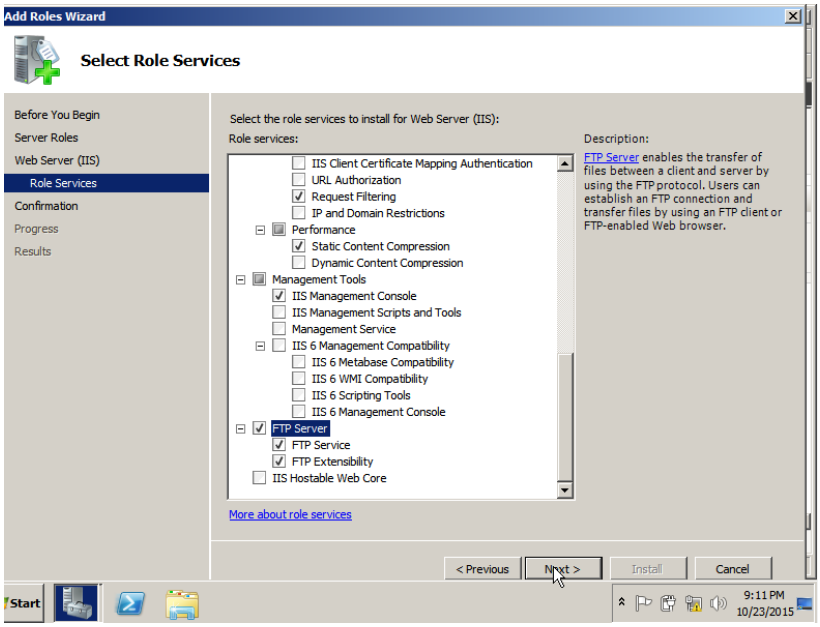
- Open Server Manager, go to Roles and click "Add Roles".



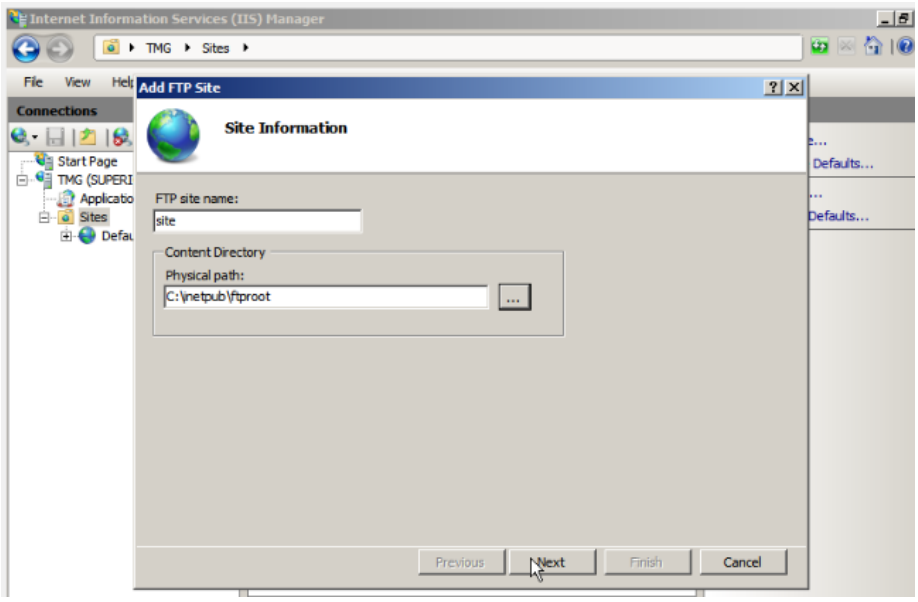
- In the Add Role Wizard, select Web Server (IIS) role to install



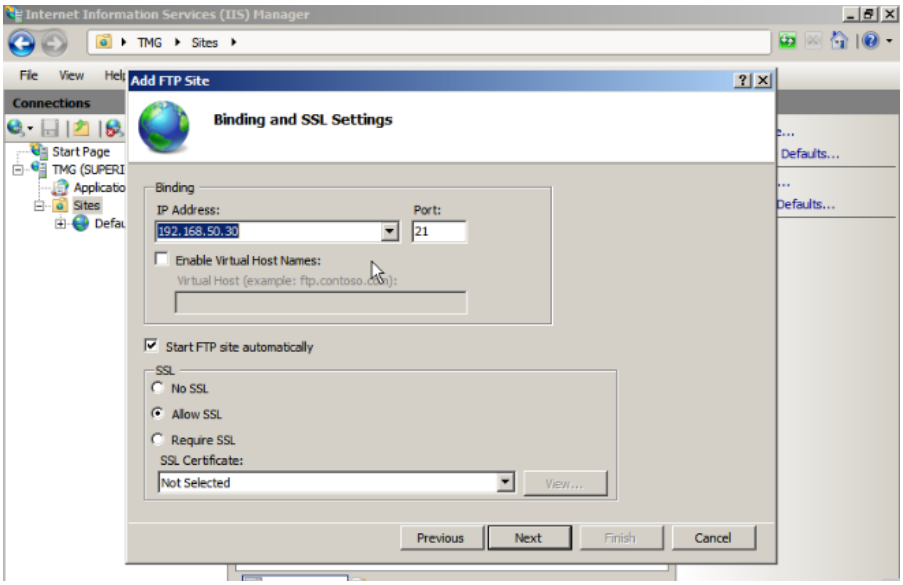
- Click Next until you reach Select Role Services page, leave the default and check FTP Server, FTP Service and FTP Extensibility at the bottom. Click Next, follow the wizard and finish the role installation.



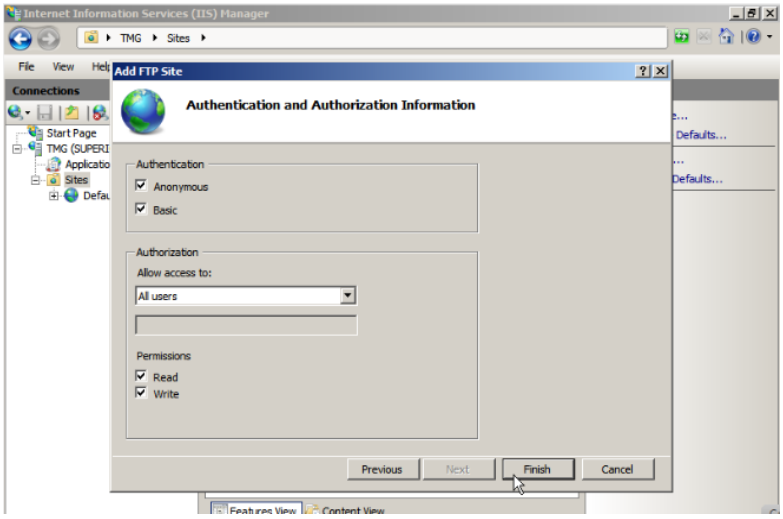
- Now open IIS Manager from Start > Administrative Tools, expand the server, right click Sites, and click Add FTP Site, give it a site name and configure the physical path as needed.



- Configure Binding and SSL. In our case, we'd like to bind to all unassigned IP addresses and do not use SSL.



- Enable Basic Authentication and configure authorization. In our case I'll start with allowing All users both Read and Write permission as long as all users on the server are password protected.



- Click Finish to finish the configuration.