Joseph Martinez

Networking I: Network +
CNG – 124

Chapter One Labs

Lab 1.1 Understanding Elements of a Network

Lab 1.2 Building a Simple Peer-to-Peer Network

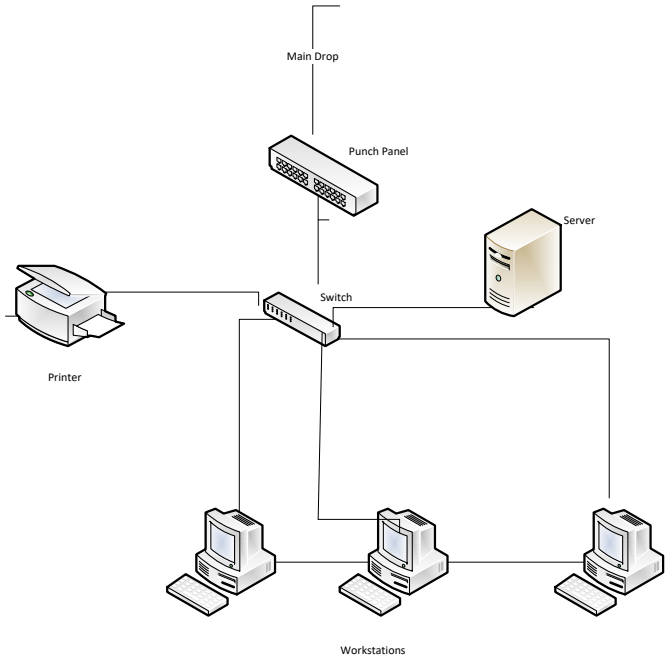
Lab 1.3 Building a Simple Client/Server Network

Lab 1.4 Sharing a Network Computer

Chapter One: An Introduction to Networking

Lab. 1.1 Understanding Elements of a Network

Cherry Creek South Classroom 204 Network Topology:

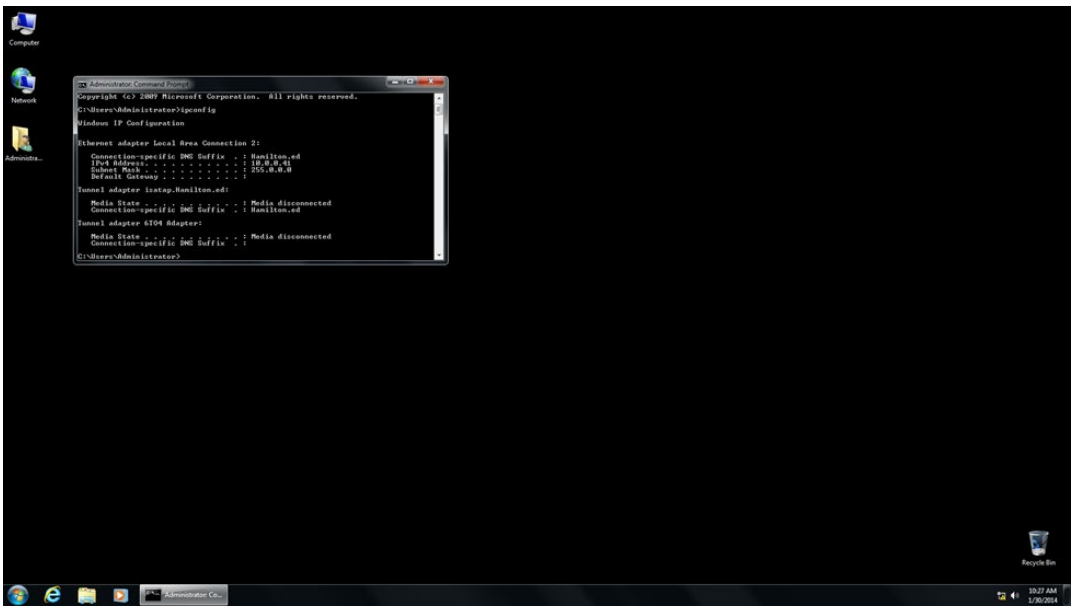


- N.O.S (Network Operating System).: Windows Server 2008
- O.S (Operating System).: Windows 7
- A node is anything in a topology with an IP address.
- "The Internet protocol suite is the networking model and a set of communications protocols used for the Internet and similar networks. It is commonly known as TCP/IP, because it's most important protocols, the Transmission Control Protocol (TCP) and the Internet Protocol (IP), The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used by servers on an IP network to allocate IP addresses to computers." (Wikipedia)

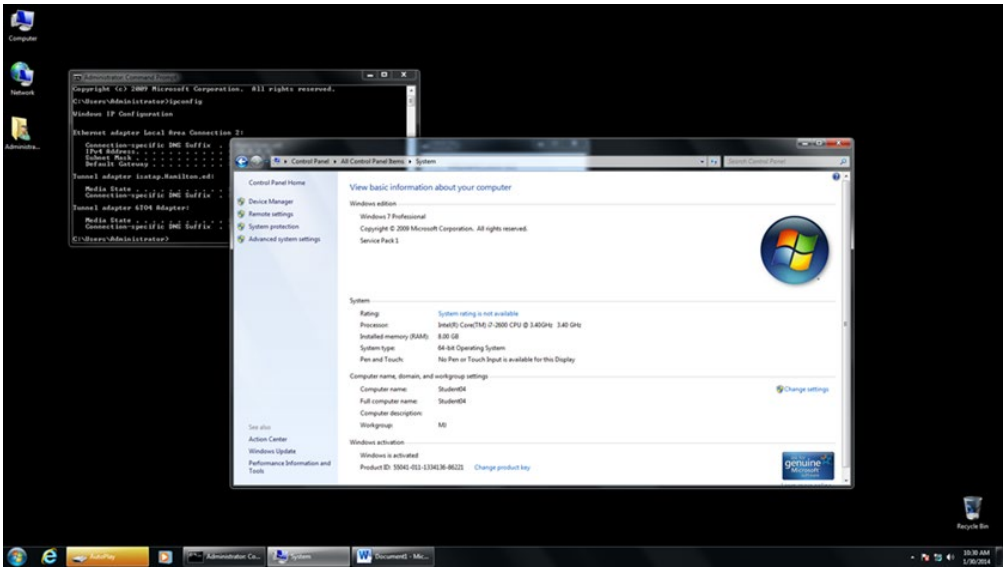
Lab 1.2 Building a Simple Peer-to-Peer Network

To build a simple peer-to-peer network, boot two workstations to the 2nd partition –Unplug the connected RJ-45 cables to the network and plug in the RJ-45 crossover cable.

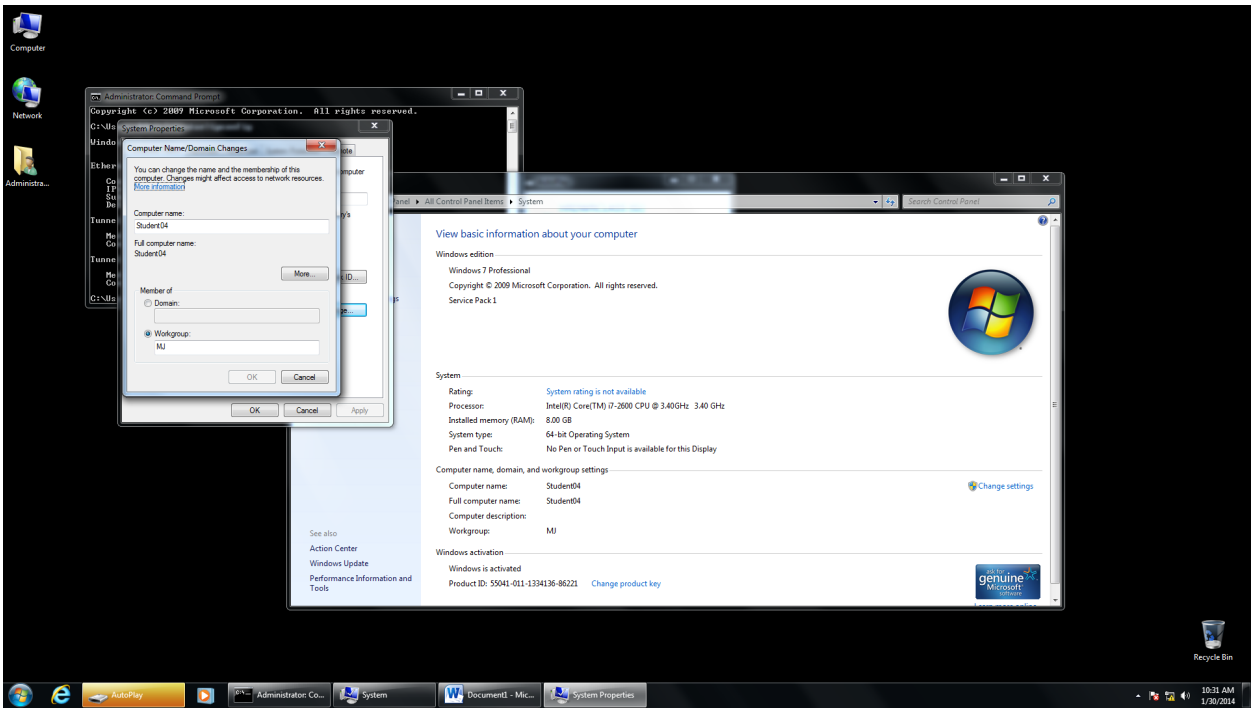
Check the I.P. address and configuration from command prompt.



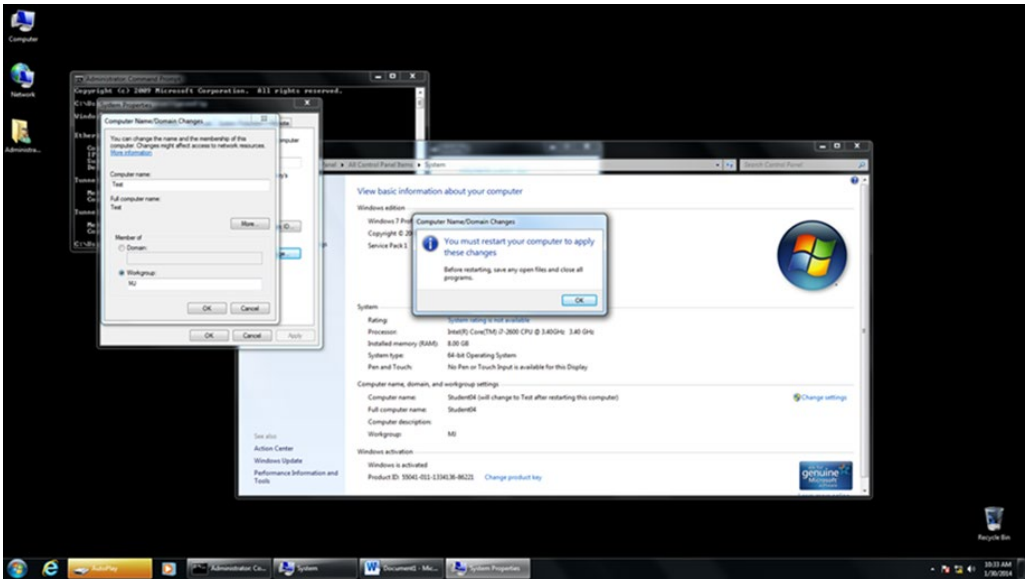
Right click my Computer, Properties:



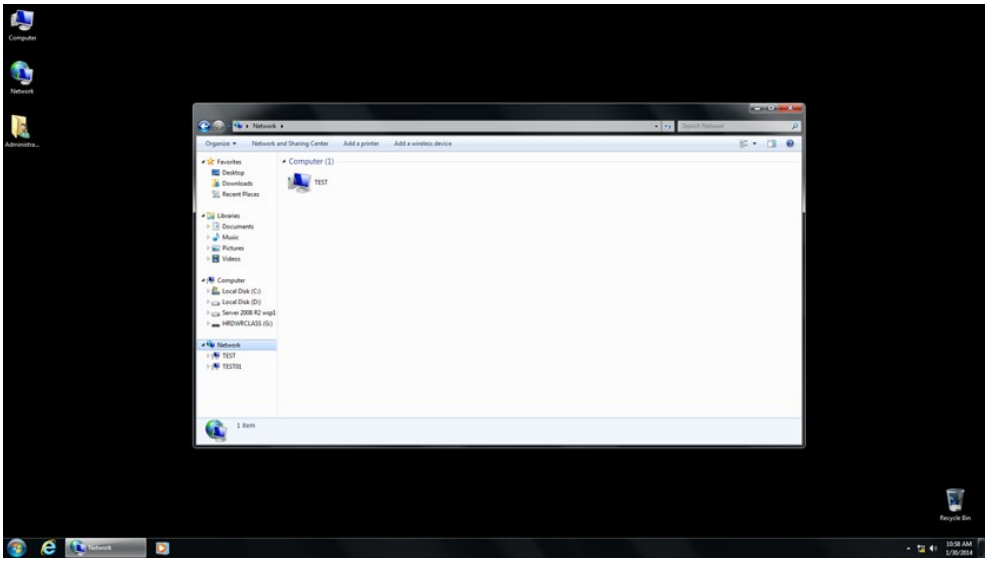
Click change settings – User Account Control dialog box appears – Log in as Administrator – Click Change in System Properties Box – Click Workgroup: Give the workgroup a name (any name) – Click OK.



Computer Name/Domain Changes box appears – click OK – another dialogue box appears welcoming you to the (named) workgroup – You must restart your computer to apply these changes.

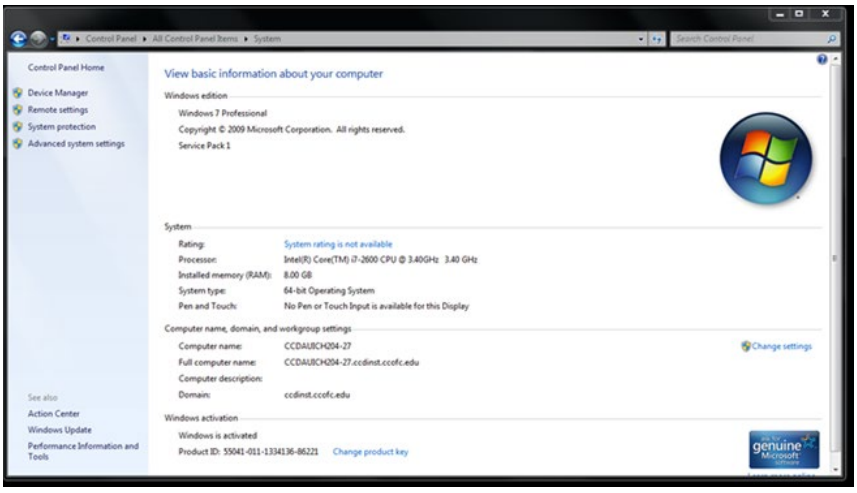


Complete all previous steps on 2nd Computer – Ping IP address to assure that both workstations are communicating – Put flash drive in one of the workstations – Right click flash drive icon – Share with (click Advanced Settings) – Click Share this Folder – Add – New Share - Right click Workstation 1 and observe flash drive files on shared workstation – Remove flash drive and put into workstation 2 – Repeat all steps on this page on 2nd workstation.



Lab 1.3 Building a Simple Client/Server Network

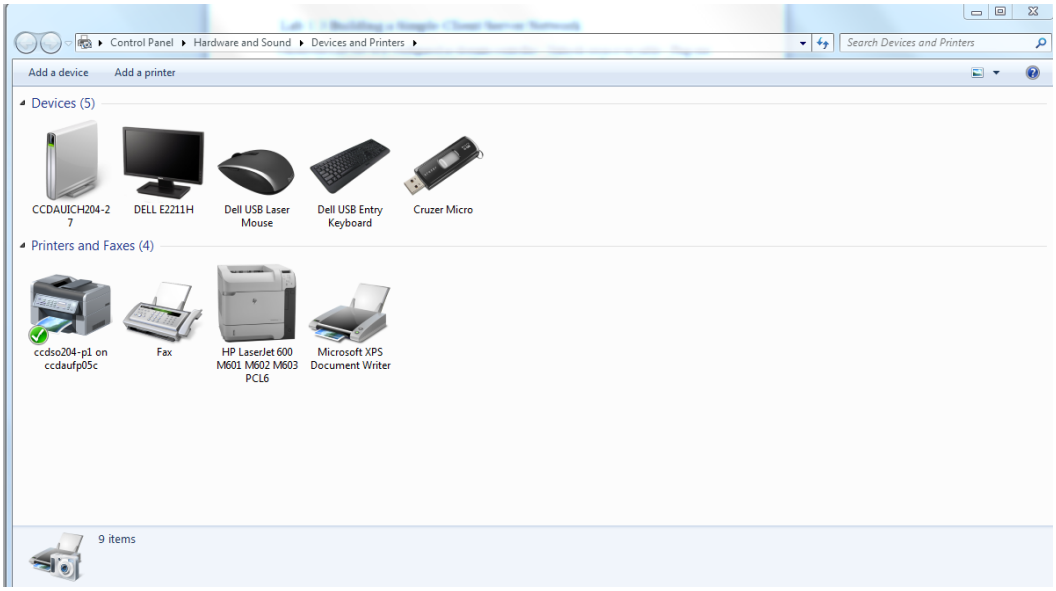
Classroom lab server was configured as client/server controller, though through log in domains though you have already started to configure peer-to- peer network – Unhook cross over cable – Plug one end of a RJ-45 into workstation and the other end into switch plug on floor – Verify that link lights on workstation and switch are blinking – Server is connected to switch - Check if N.I.C. cards are connected - Double click Network – Network Sharing – Change adapter settings



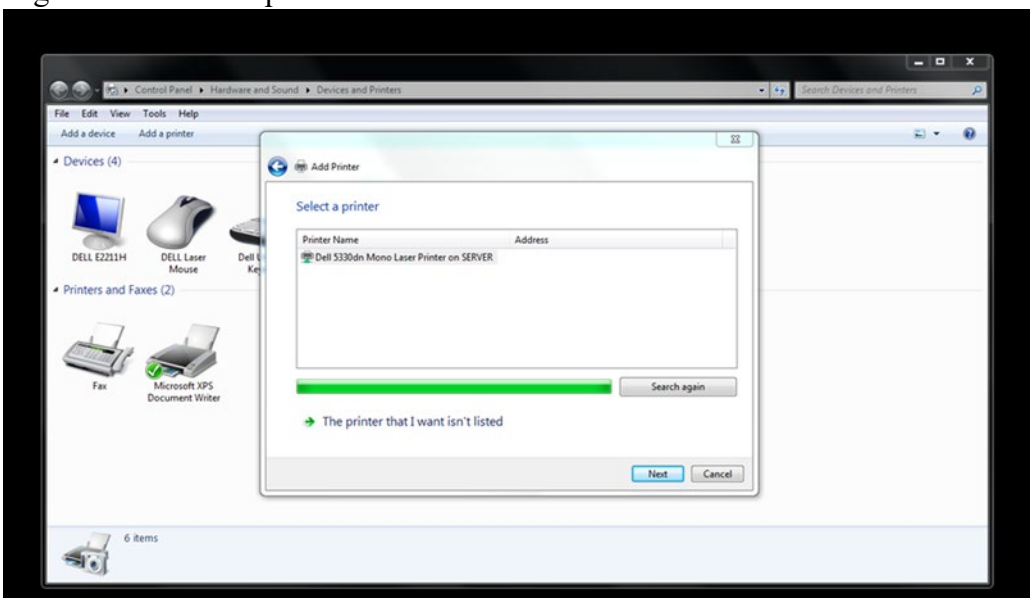
Go to Systems - Change settings to Student26 on one workstation and Student27 on the other – Click domain radio button – join Hamilton domain with username and password – Restart.

Lab 1.4 Sharing a Network Computer

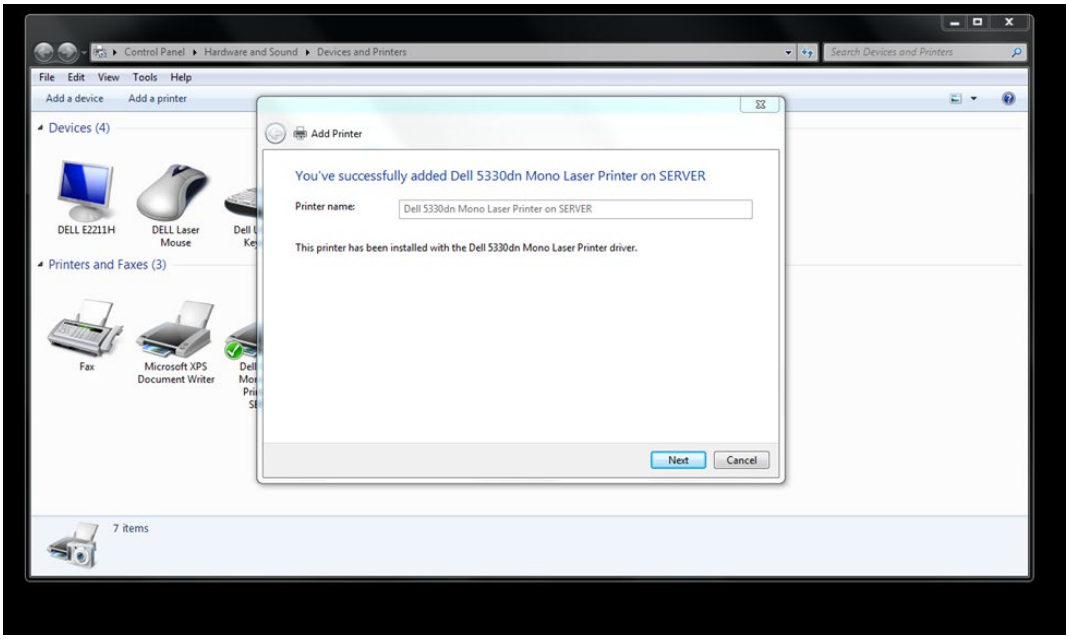
Click Devices and Printers



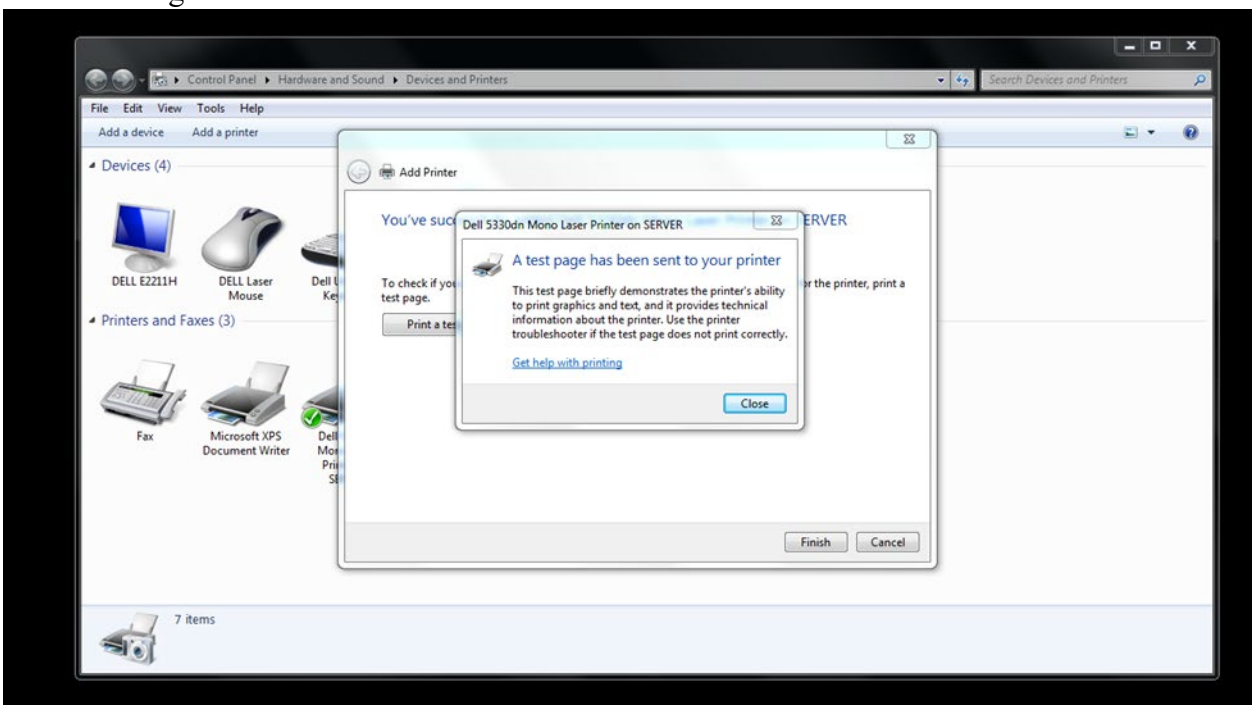
Right click network printer to be uninstalled – Remove device - Click Add Printer



Click Add Network Printer – Click Next



Print Test Page



Configure N.I.C. card and restart

Windows
Printer Test Page

Congratulations!

If you can read this information, you have correctly installed your Dell 5330dn Mono Laser Printer on SERVER.

The information below describes your printer driver and port settings.

Submitted Time: 11:20:15 AM 1/30/2014
Computer name: SERVER
Printer name: \\SERVER\Dell 5330dn Mono Laser Printer
Printer model: Dell 5330dn Mono Laser Printer
Color support: Yes
Port name(s): 10.0.0.15
Data format: RAW
Share name: 5330dn Mono Laser Printer (Dell)
Location:
Comment:
Driver name: sdu1m.dll
Data file: sdu1mpp.dll
Config file: sdu1mdu.dll
Driver version: 4.00
Environment: Windows x64

Additional files used by this driver:
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1mu.dll
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1mu2.dll
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1mo.dll
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1mcm.dll (0, 5, 2, 0)
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1mlf.dll
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1mum.dll (0, 3, 47, 0)
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1mum.xml
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1mcm.ctd
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1mpp.ver
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1mu.ini
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1mud.bmp
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1mue.bmp
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1mul.bmp
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1mu.bmp
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1mu1.bmp
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1mu3.bmp
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1mu4.bmp
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1mu01.bmp
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1mu11.bmp
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1mu31.bmp
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1mu41.bmp
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1muA0.bmp
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1muA1.bmp
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1muB0.bmp
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1muB1.bmp
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1muw1.bmp
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1muw2.bmp
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1muw4.bmp
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1muw6.bmp
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1muwA.bmp
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1muwB.bmp
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1muwC.bmp
C:\Windows\system32\spool\DRIVERS\x64\3\sdu1muwD.bmp

Lab 1.1 Questions

1. Which of the following best describes a networks physical topology? B (The physical layout of a network).
2. Which of the following is the most popular type of modern network architecture for businesses? A (client/server).
3. Which of the following elements is not required for a client to connect to a server on a client/server LAN? C (e-mail address).
4. Which of the following are capable of acting as a network server? B, D (Windows Server 2008, Linux, UNIX).
5. Network protocols are used to do which of the following? A, D (ensure reliability delivery of data, indicate the source and destination addresses for data packets).
6. On a client/server network, clients may have only one protocol installed at any time. False
7. A significant difference between the peer-to-peer and client/server network types is that a peer-to-peer network: C (does not usually provide centralized management for shared resources).
8. Why is it necessary for each client/server network to have a unique address? "To deliver data between two Internet hosts, it is necessary to move data across the network to the correct host, and within that host to the correct user or process. TCP/IP uses three schemes to accomplish these tasks:
   • Addressing: IP addresses deliver data to the correct host.
   • Routing: Gateway delivers data to the correct network.
   • Multiplexing: Protocol and port numbers deliver data to the correct software module within the host." (Wikipedia)

Lab 1.2 Questions

1. What physical topology would you use to create your peer-to-peer network where all the workstations are connected to a single hub or switch? A (bus).
2. Which of the following operating systems allow you to create a peer-to-peer network from a group of workstations? A, B, C, D (MS-DOS, Windows XP Professional, Linux, Windows 7).
3. Which of the following components are not necessary to create a peer-to-peer network from a group of workstations? C, D (network media, Web browser).
4. What is the primary difference between peer-to-peer and client/server architectures? Peer-to-peer: Simple to configure, often less expensive to set up and maintain, not very flexible, as the network grows larger, adding elements of the network may be difficult. Client/server: User log in accounts and passwords for anyone can be assigned in one place. Centrally shared resources, problems can be monitored, diagnosed and fixed from

one location, can handle heavy processing loads, dedicated to handling requests from clients enabling faster response time, faster processing and larger disk storage.

5. On a peer-to-peer network consisting of four XP workstations, each user can individually control which of her local data files she wants to share with others. False

Lab 1.3 Questions

1. Which of the following are or could be shared as resources across a network? B, C (printers, documents).
2. Even in a client/server network, it is possible to share documents between individual users' computers as you can in a peer-to-peer network. True
3. You are the network administrator for a small company. When users take vacations, they would like to allow other users to update the files stored on their computers. In addition, several users have complained that they accidentally deleted important files on their local computer and would like some way to recover them. How would you recommend that they restore their files? B (store the files on the server, which is backed up nightly).
4. A very large organization might have thousands of servers. Do the benefits of client/server still apply to such an organization? D (Yes, because managing thousands of servers is no more difficult than managing a few computers).
5. In this lab, what kind of network service did you configure on your client/server network? A (management service).
6. Which two of the following issues make peer-to-peer networks less scalable than client/server networks? C, D (Adding nodes to peer-to-peer network increases the risk that an intruder can compromise a shared data folder, Adding new resource-sharing locations and ensuring that all authorized uses have access to new resources becomes less manageable as the peer-to-peer network grows.)

Lab 1.4 Questions

1. Many printers come with network cards so that they do not need to be attached to a computer. How would the process of sharing such a printer differ from sharing a printer attached to a computer? B
2. Users may share printers in a peer-to-peer network. What are the potential disadvantages of this? A,B
3. In this lab, what kind of network service did you configure on your client/server network? C
4. Suppose that you configured software on a Windows Server 2008 computer that checked printers on the network to make sure that they were operating correctly. What sort of network service would this software provide? B
5. How can you tell whether a printer is shared or not? D

Joseph Martinez

Networking I: Network +

CNG – 124

Chapter Two Labs

Lab 2.1 IP Address Assignments

Lab 2.2 Configuring TCP/IP for a Windows Computer

Lab 2.3 Finding the MAC Address of another Computer

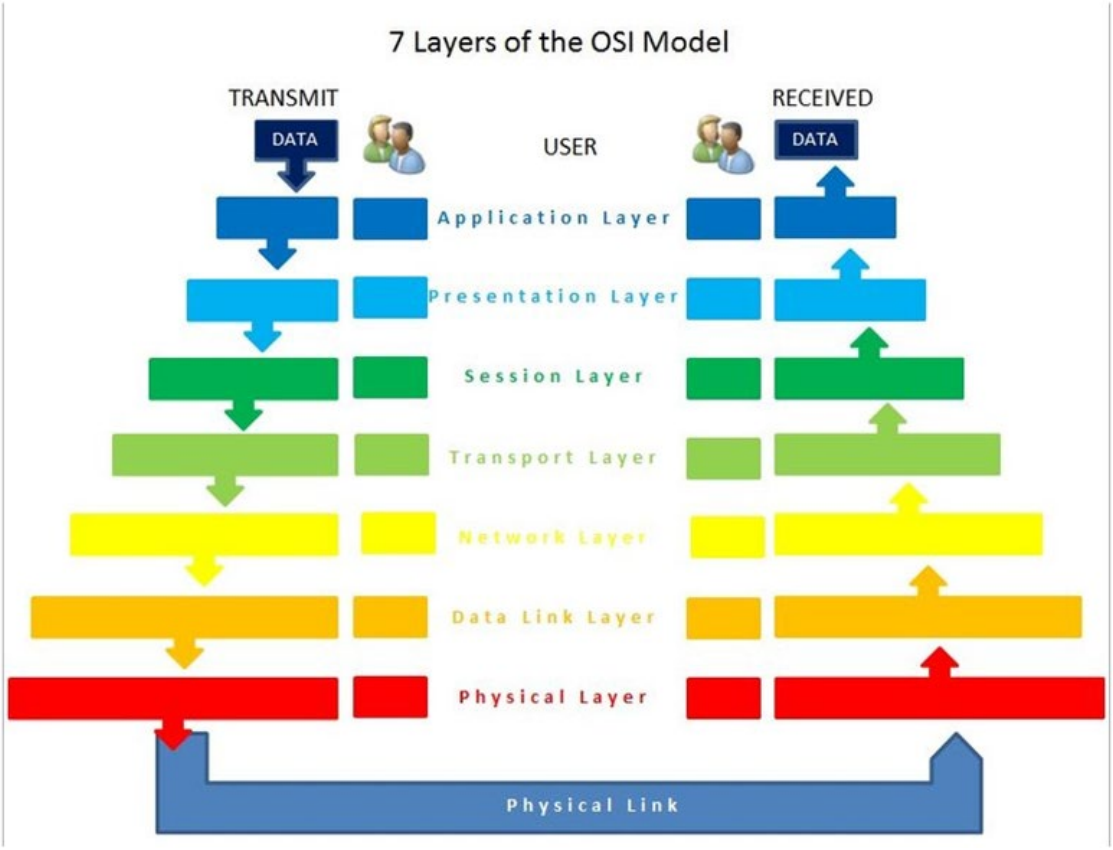
Lab 2.4 Looking at Network Connection on a Windows Computer

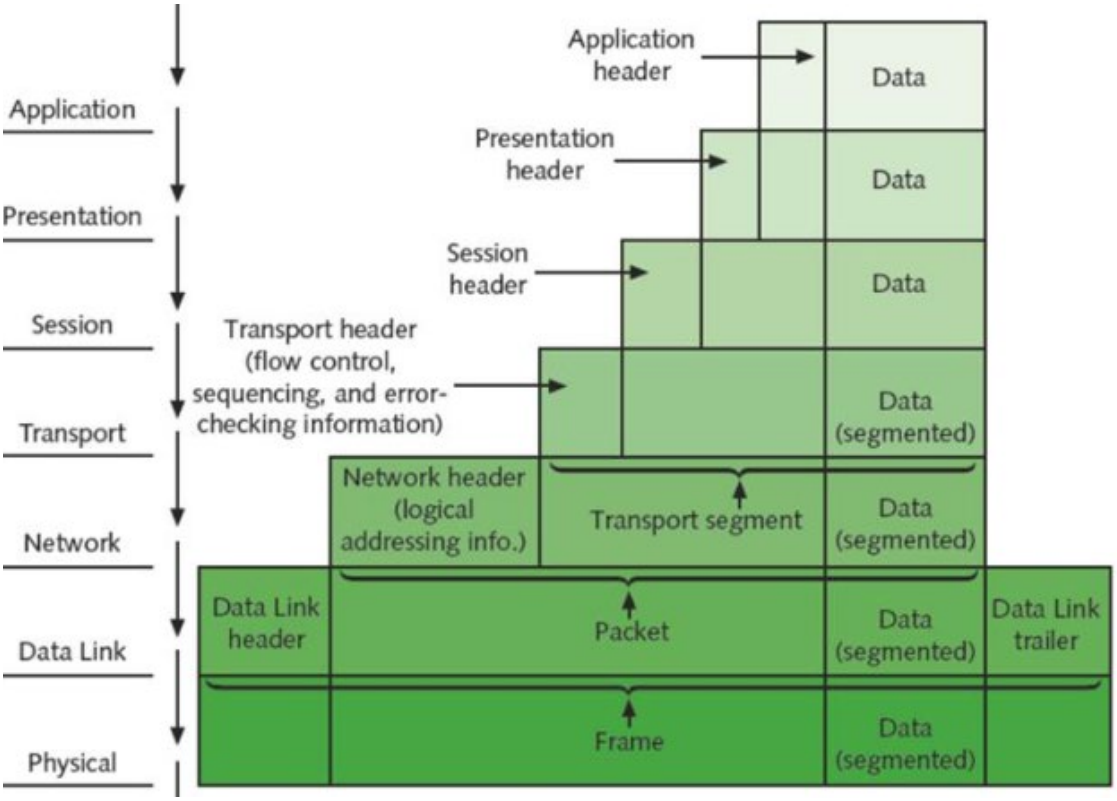
Lab 2.5 Viewing Ethernet Frame

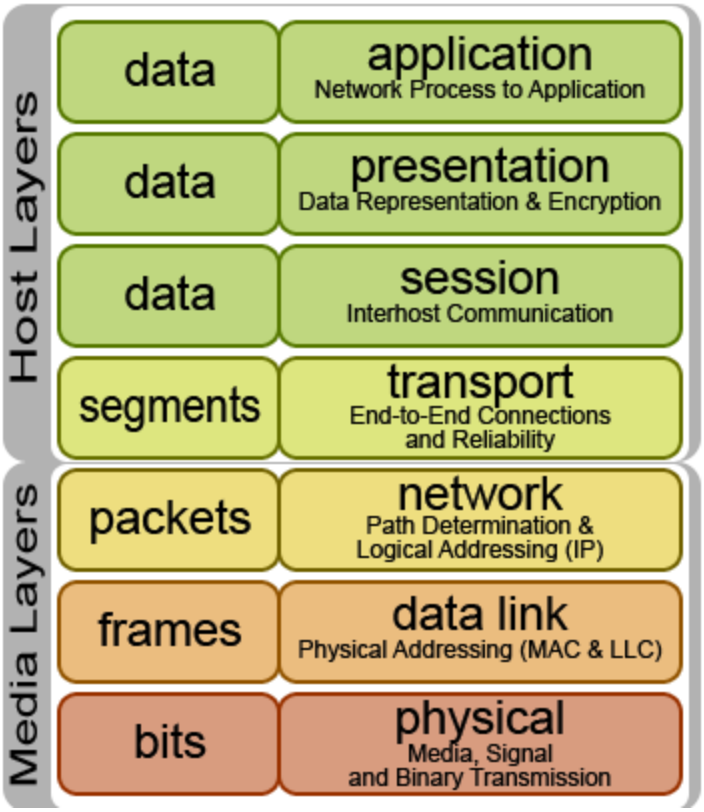
Chapter Two: Networking Standards and the OSI Model

Protocols are the rules by which computers communicate.

"Open Systems Interconnection (OSI) is an effort to standardize computer networking that was started in 1977 by the International Organization for Standardization (ISO), along with the International Telecommunication Union (ITU); it coordinates standards for telecommunications. The Open Systems Interconnection (OSI) model is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers" (Wikipedia). "The OSI model defines a networking framework to implement protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy" (Google).




Application
Presentation
Session
Transport
Network
Data Link
Physical
Application header
Data
Presentation header
Data
Session header
Data
Transport header (flow control, sequencing, and error-checking information)
Data (segmented)
Network header (logical addressing info.)
Transport segment
Data (segmented)
Data Link header
Packet
Data (segmented)
Data Link trailer
Frame
Data (segmented)
data unit
layers


Host Layers
data
application
Network Process to Application
data
presentation
Data Representation & Encryption
data
session
Interhost Communication
segments
transport
End-to-End Connections and Reliability
Media Layers
packets
network
Path Determination & Logical Addressing (IP)
frames
data link
Physical Addressing (MAC & LLC)
bits
physical
Media, Signal and Binary Transmission

Application (Layer 7)

This layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and FTP are applications that exist entirely in the application level. Tiered application architectures are part of this layer.

Presentation (Layer 6)

The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station. Presentation Layer formats and manages data encryption as well as decryption, providing freedom from compatibility problems. It is sometimes called the syntax layer.

Session (Layer 5)

This layer establishes, manages and terminates connections between applications: allows two application processes on different machines to establish, use and terminate a connection, called a session. •Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

Tansport (Layer 4)

The transport layer provides: •Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message. •Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments. •Message traffic control: tells the transmitting station to "back-off" when no message buffers are available. •Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer). Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, prepending a header to each frame. The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries. In addition, if the lower layers do not maintain sequence, the

transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.

Network (Layer 3)

Routing: routes frames among networks. This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing. •. Frame fragmentation: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station. •Logical-physical address mapping: translates logical addresses, or names, into physical addresses. •Subnet usage accounting: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information. IP operates in this layer.

Data Link (Layer 2)

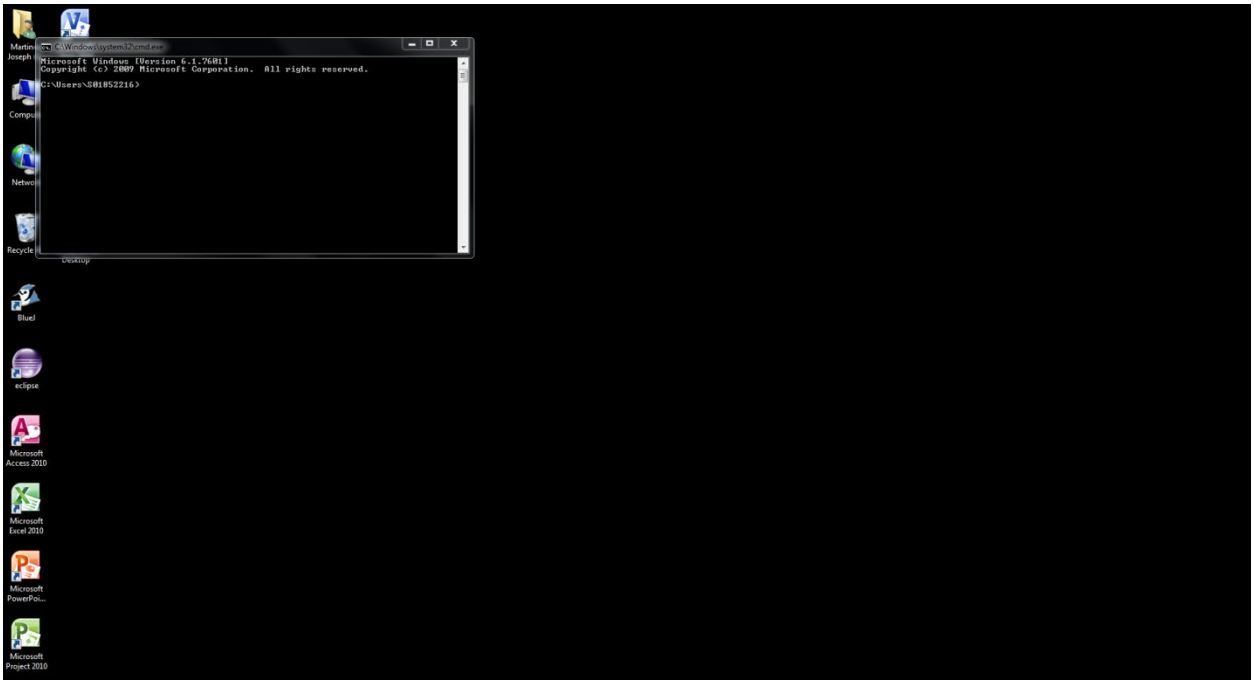
At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization, frame error checking: checks received frames for integrity.The data link layer is divided into two sub layers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sub layer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.

Physical (Layer 1)

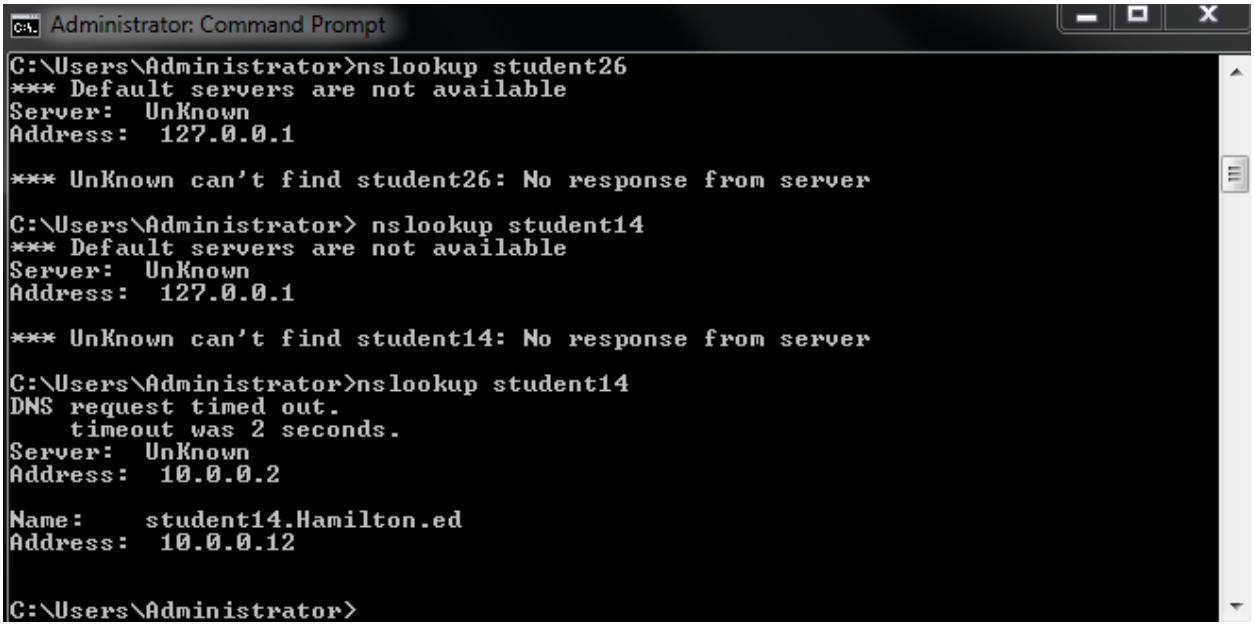
This layer conveys the bit stream , transmits bits as electrical impulse or optical signals, light or radio signal -- through the network at the electrical and mechanical level appropriate for the phsical medium. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components. Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. Transmission technique: determines whether the encoded bits will be transmitted by baseband (digital) or broadband (analog) signaling. (Microsoft Home Page Support & Webopedia.com)

Lab 2.1 IP Address Assignments

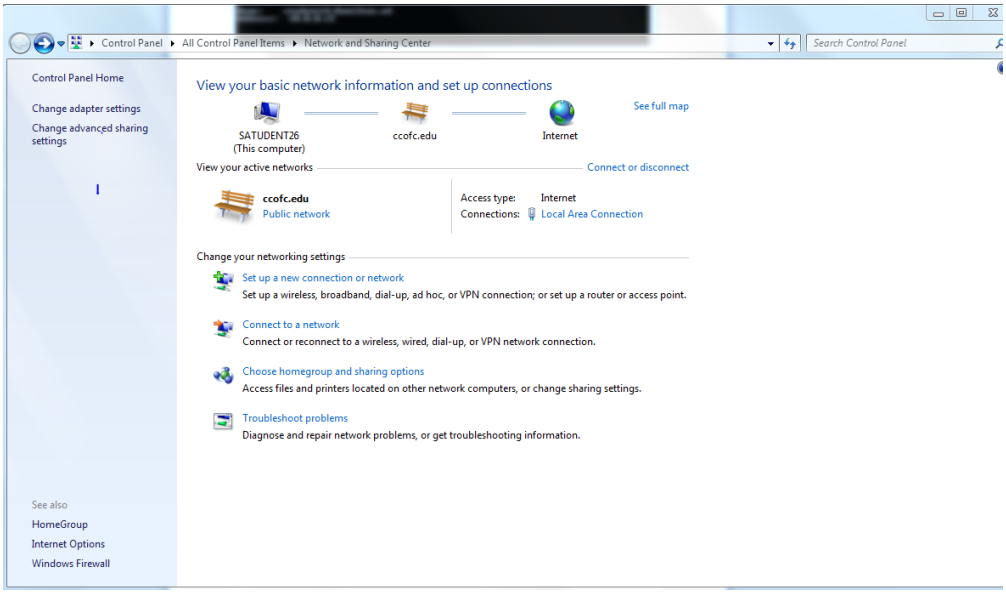
In Windows 7, click Start, type **cmd** in the Search programs and files text box, press **Enter**.

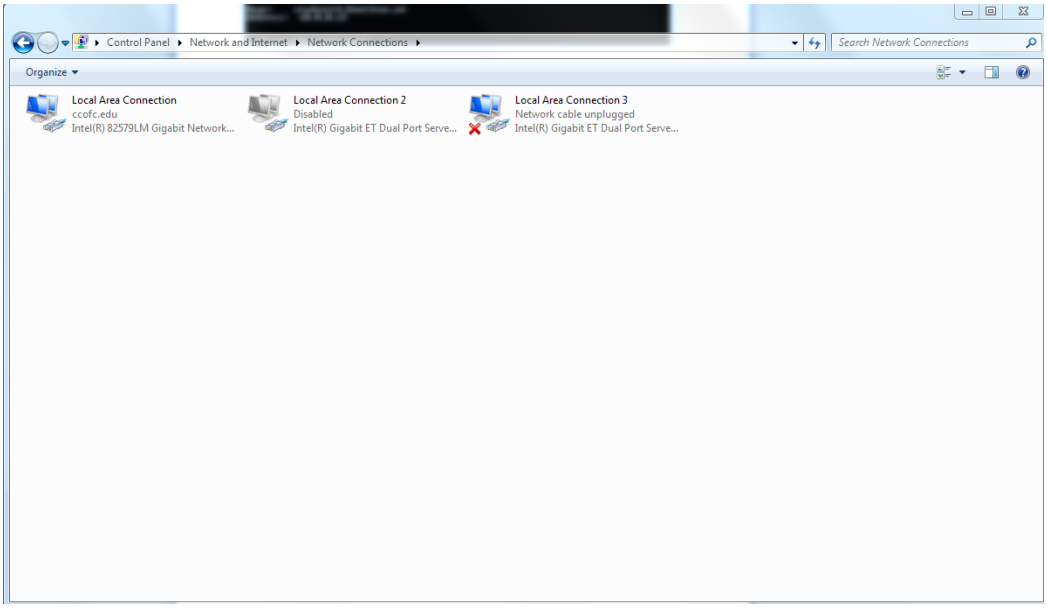


In the command prompt window, type nslookup (space) and (name of any website), Enter.

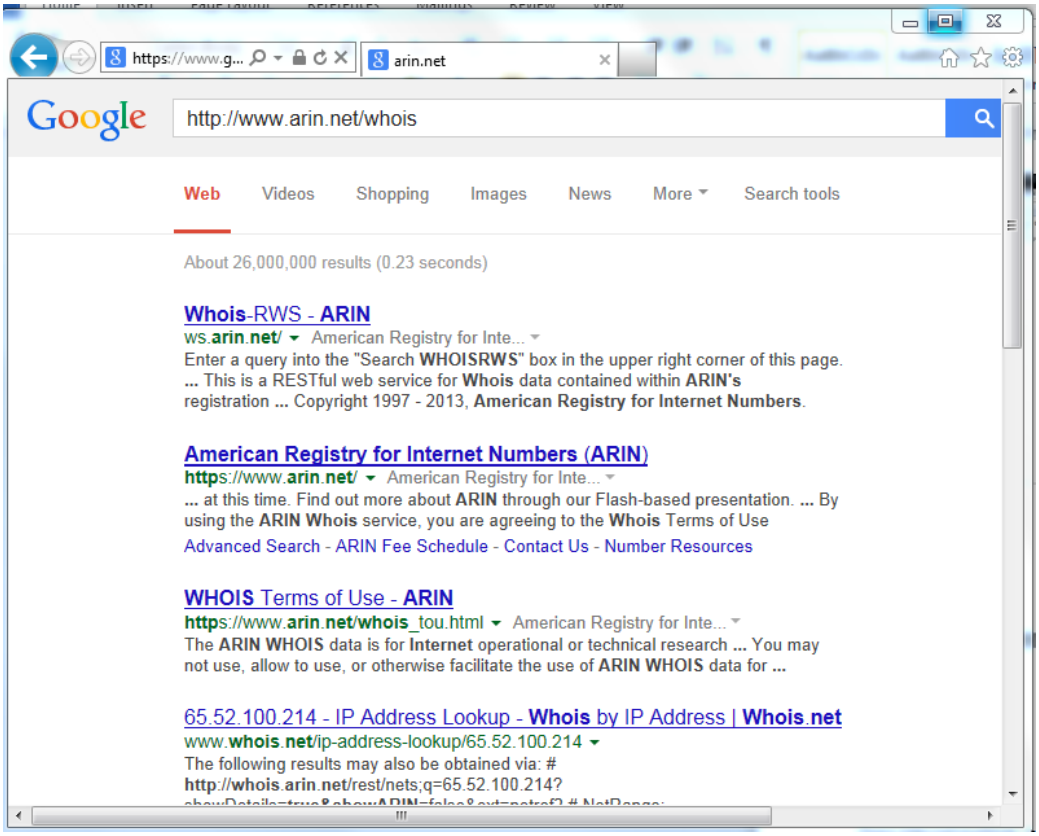


At the time of this lab, the domain server was down at C.C.D. on partition 1, so I went to partition 2 and pinged Student 14 and **nslookup**. I verified that the I.P. address is given for Student 14. To get access to the internet while on partition 2, open network sharing center at task bar bottom right – change adapter settings disable partition 3 and enable partition 2.





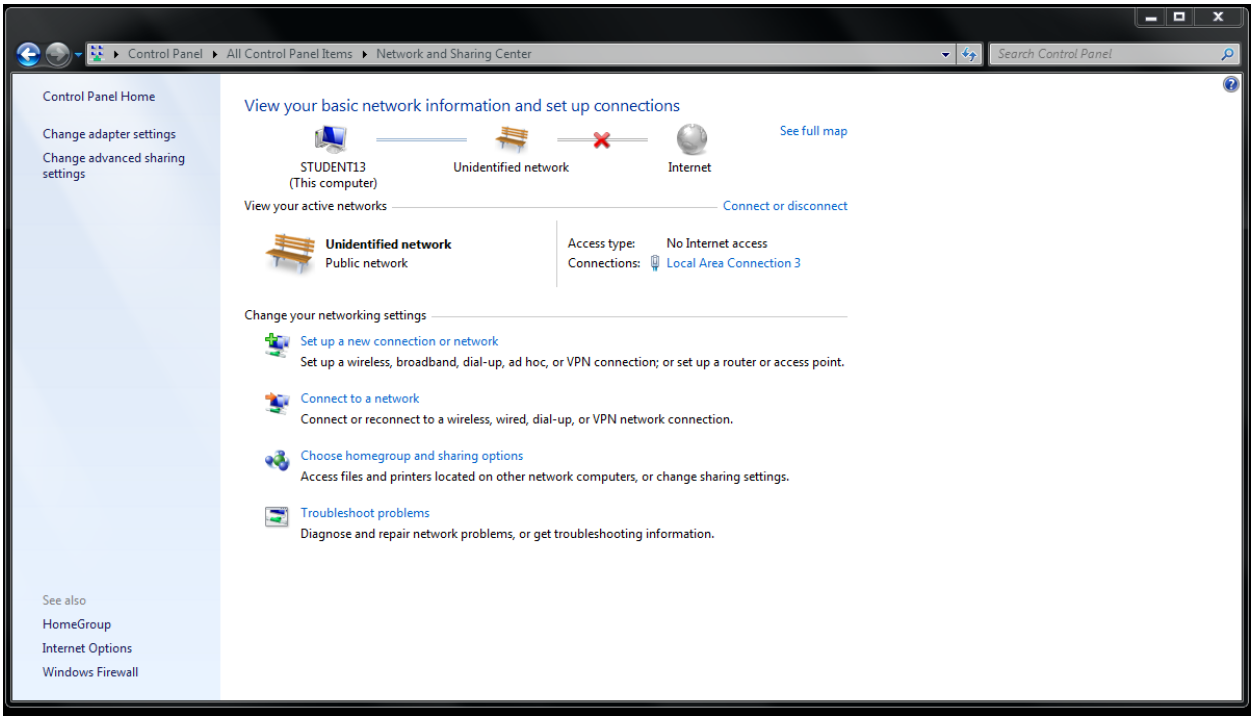
Open Internet explorer, in the address bar http://www.arin.net/whois/



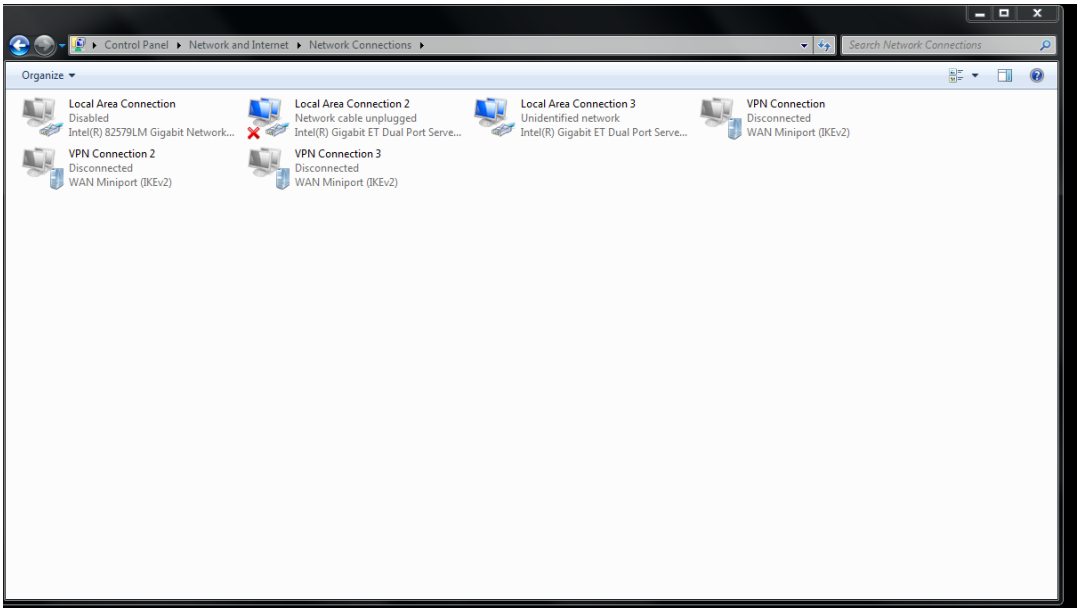
Domain Name: yahoo.com
Registry Domain ID:
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2013-09-06T10:15:13-0700
Creation Date: 2002-12-11T00:00:00-0800
Registrar Registration Expiration Date: 2023-01-18T21:00:00-0800
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: compliance@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientUpdateProhibited
Domain Status: clientTransferProhibited
Domain Status: clientDeleteProhibited
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Yahoo! Inc.
Registrant Street: 701 First Avenue
Registrant City: Sunnyvale
Registrant State/Province: CA
Registrant Postal Code: 94089
Registrant Country: US
Registrant Phone: +1.4083493300
Registrant Phone Ext:
Registrant Fax: +1.4083493301
Registrant Fax Ext:
Registrant Email: domainadmin@yahoo-inc.com
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: Yahoo! Inc.
Admin Street: 701 First Avenue
Admin City: Sunnyvale
Admin State/Province: CA
Admin Postal Code: 94089
Admin Country: US
Admin Phone: +1.4083493300
Admin Phone Ext:
Admin Fax: +1.4083493301
Admin Fax Ext:
Admin Email: domainadmin@yahoo-inc.com
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: Yahoo! Inc.
Tech Street: 701 First Avenue
Tech City: Sunnyvale
Tech State/Province: CA
Tech Postal Code: 94089
Tech Country: US
Tech Phone: +1.4083493300
Tech Phone Ext:
Tech Fax: +1.4083493301
Name Server: ns2.yahoo.com
Name Server: ns4.yahoo.com
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2014-02-04T15:03:14-0800 <<<
The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars.

Lab 2.2 Configuring TCP/IP for a Windows Computer

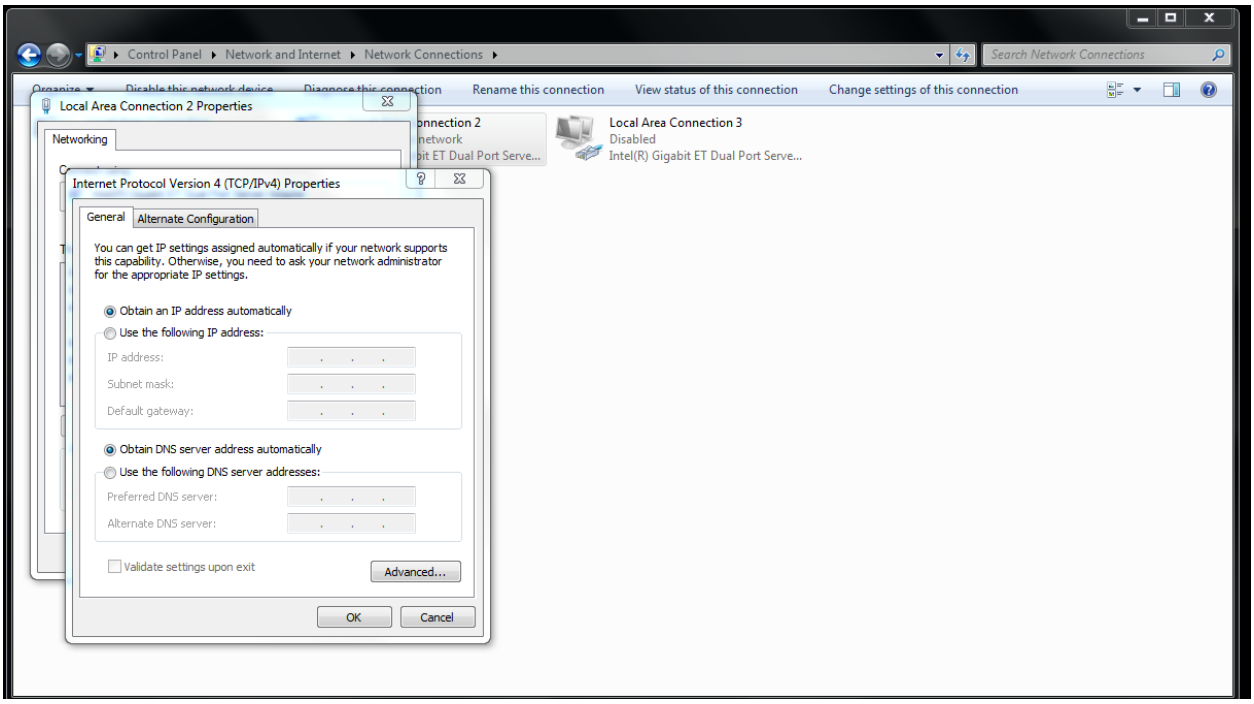
In Windows 7, click Start button - Control panel - Network and Internet - Network and Sharing center



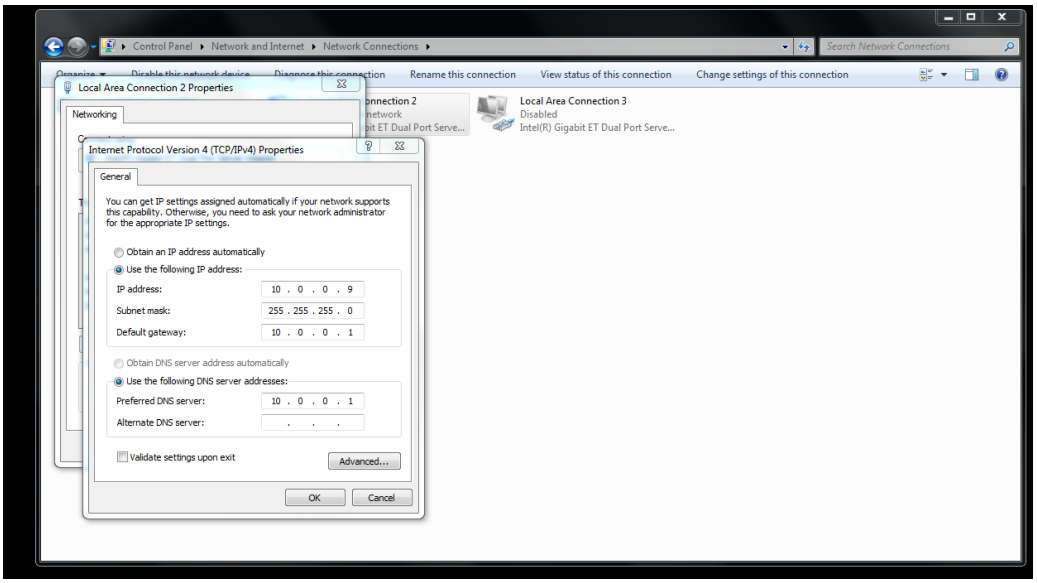
Change adapter settings - right click local area 2



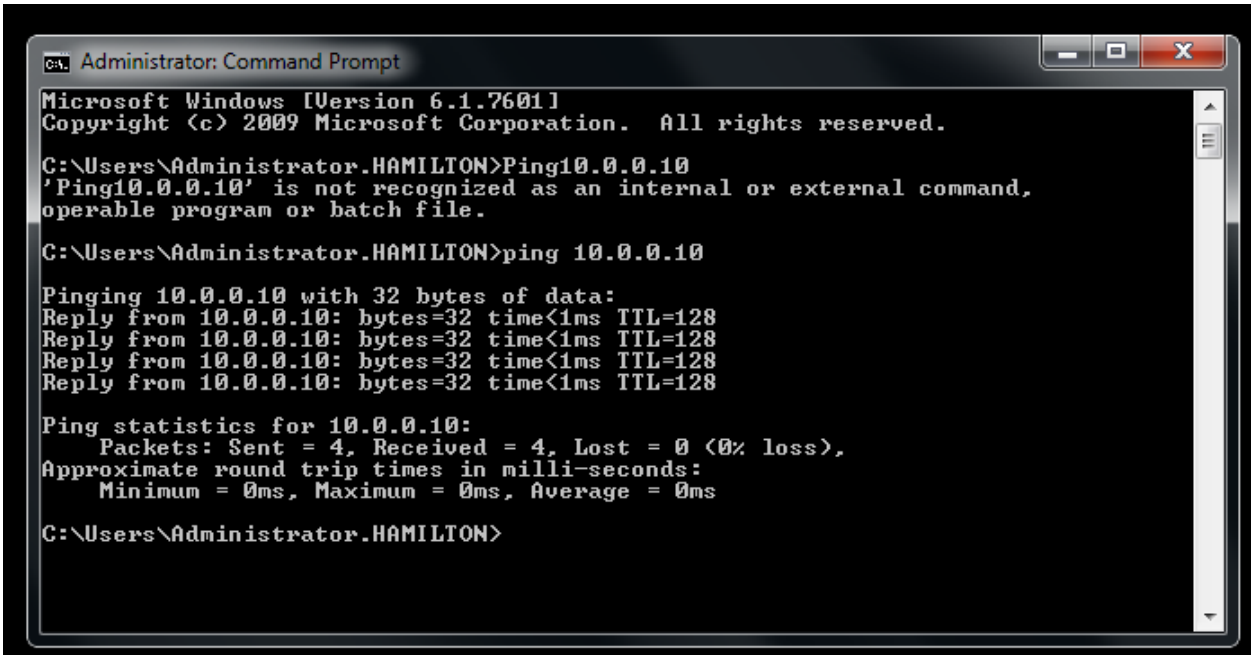
Double click Internet Protocol Version 4



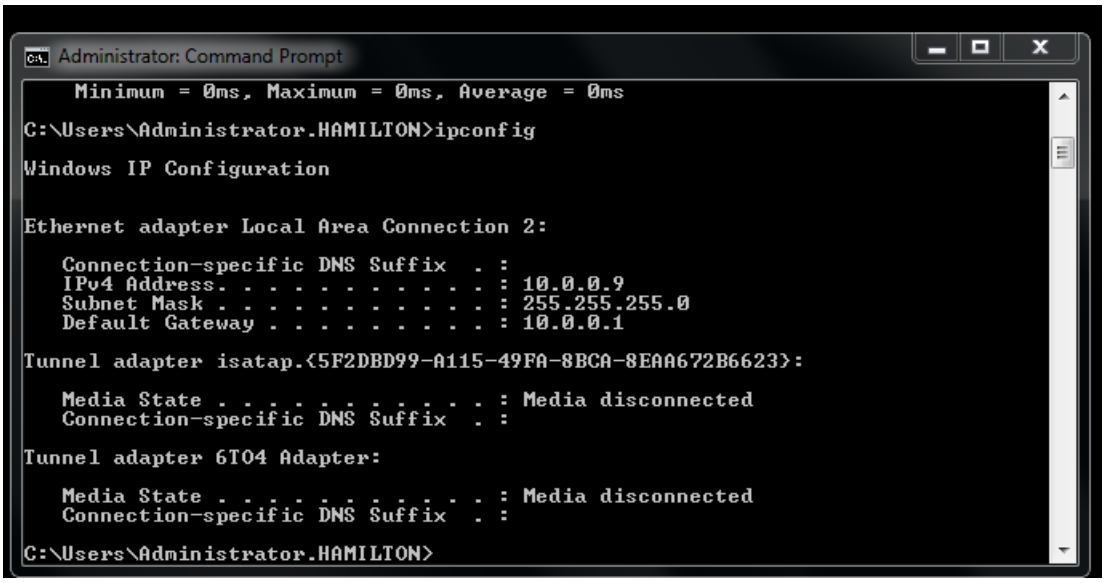
Click Use the following IP address: button – Enter 10.0.0.9 in the address text box. Enter 255.255.255.0 in the Subnet mask text box. Enter 192.0.0.1 in the Default gateway text box. Click the Use the following DNS server address option button. Click OK



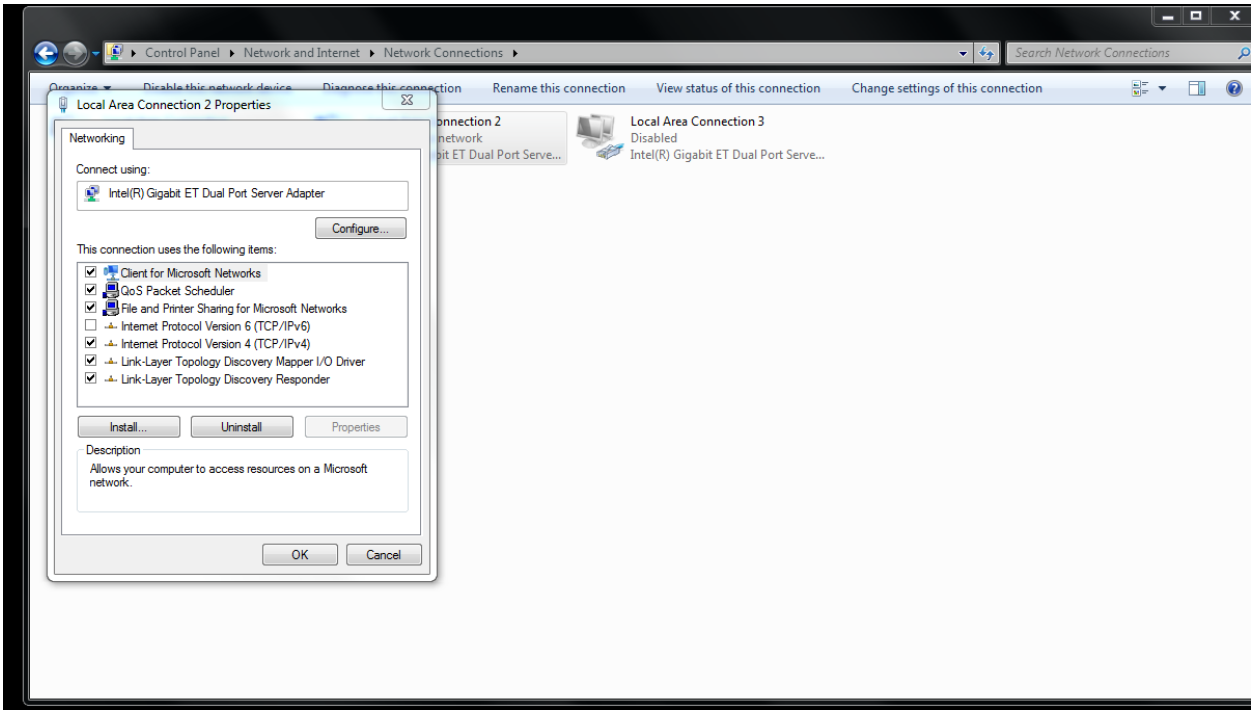
Restart - Type ping 10.0.0.10 and Enter and check that the packets were received



Type ipconfig and press Enter. The computer displays its IP address, subnet mask, and default gateway. Verify that it matches the information that was entered in the Internet Protocol Version 4 (TCP/IPv4).

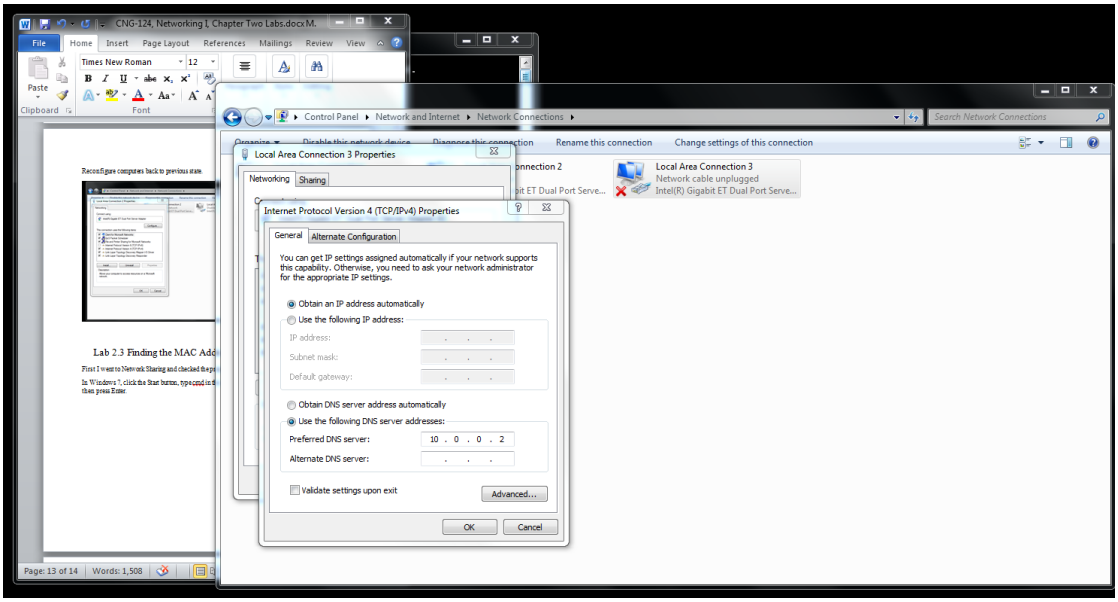


Reconfigure computers back to previous state.

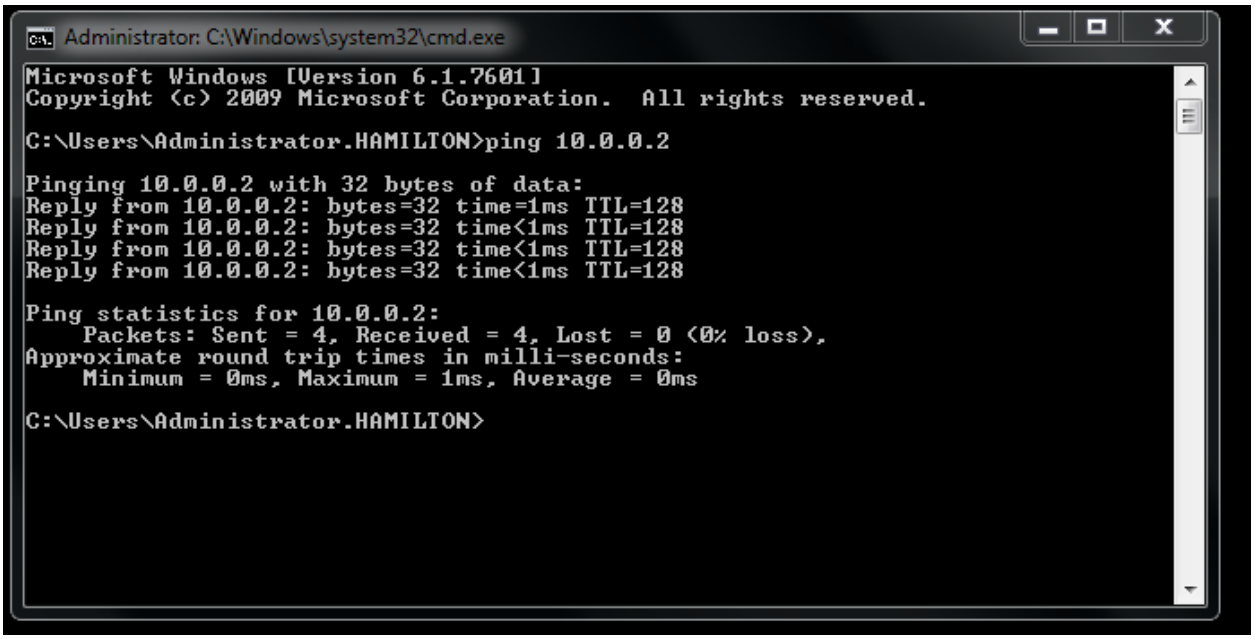


Lab 2.3 Finding the MAC Address of another Computer

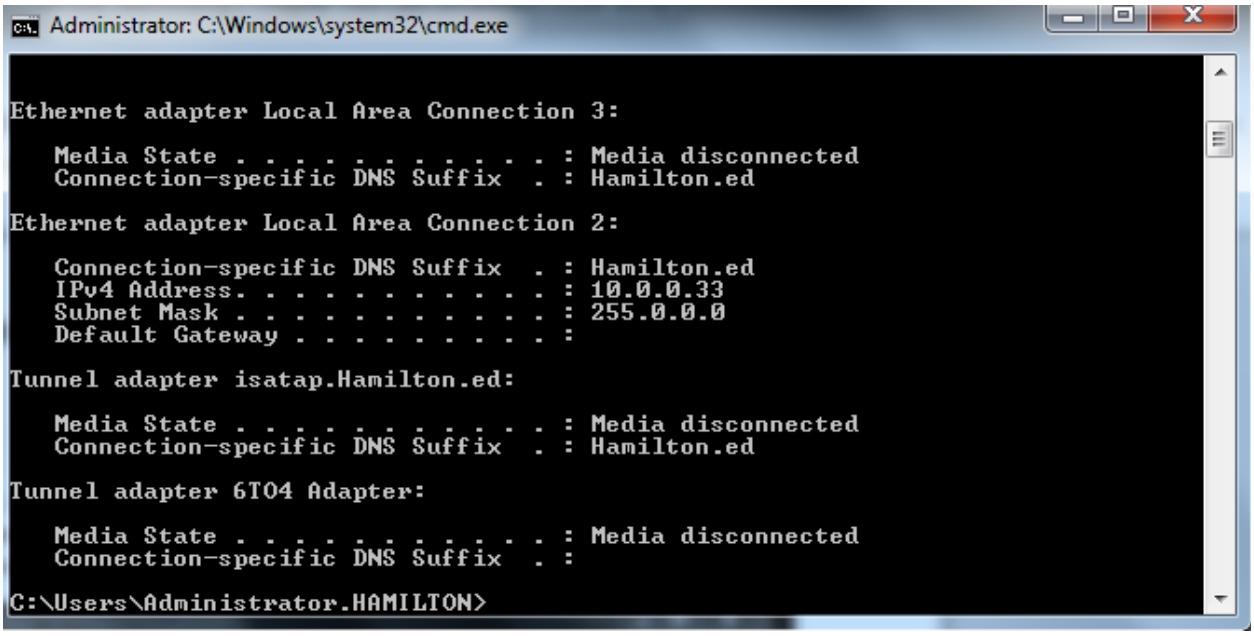
First I went to Network Sharing and checked the properties on partition 2 and partition 3 to make sure that the network adapter (NIC) card is configured properly. Right click partition icon, click properties, click TCP/IPv4, click properties, make sure obtaining an IP address automatically button is turned on and making sure the Use the following DNS Server address button is on and the IP address for Preferred DNS Server is 10.0.0.2



In Windows 7, click the Start button, type **cmd** in the search programs and files text box, and then press Enter. Ping 10.0.0.2 (Server). The computer indicated that it has received four replies from the Server.

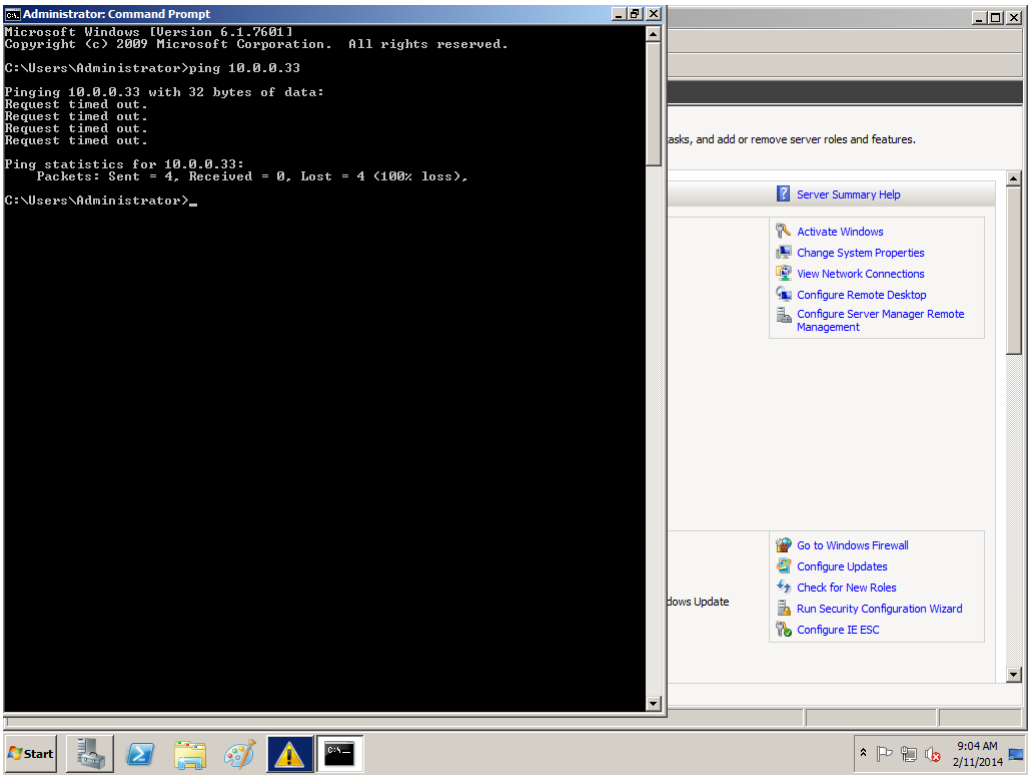


Next, I ipconfig the command prompt to find out my IP address

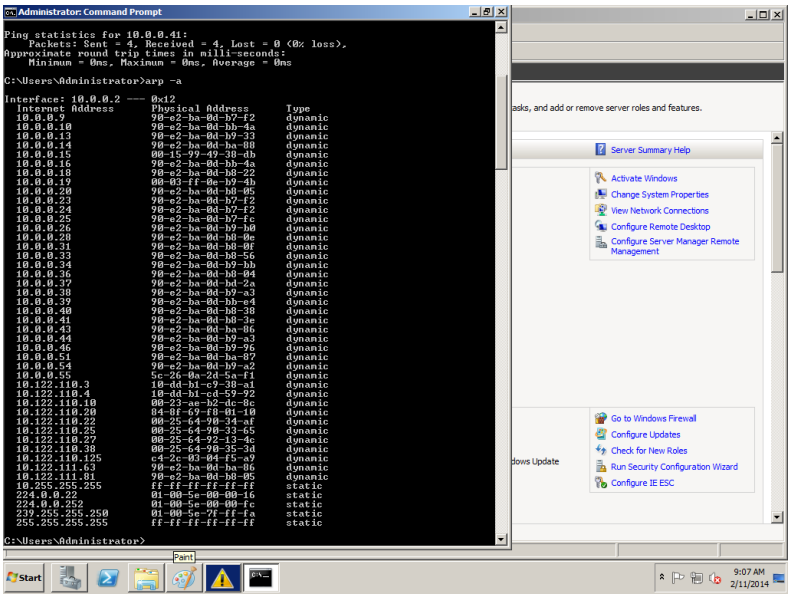


My workstation's IP address is 10.0.0.33

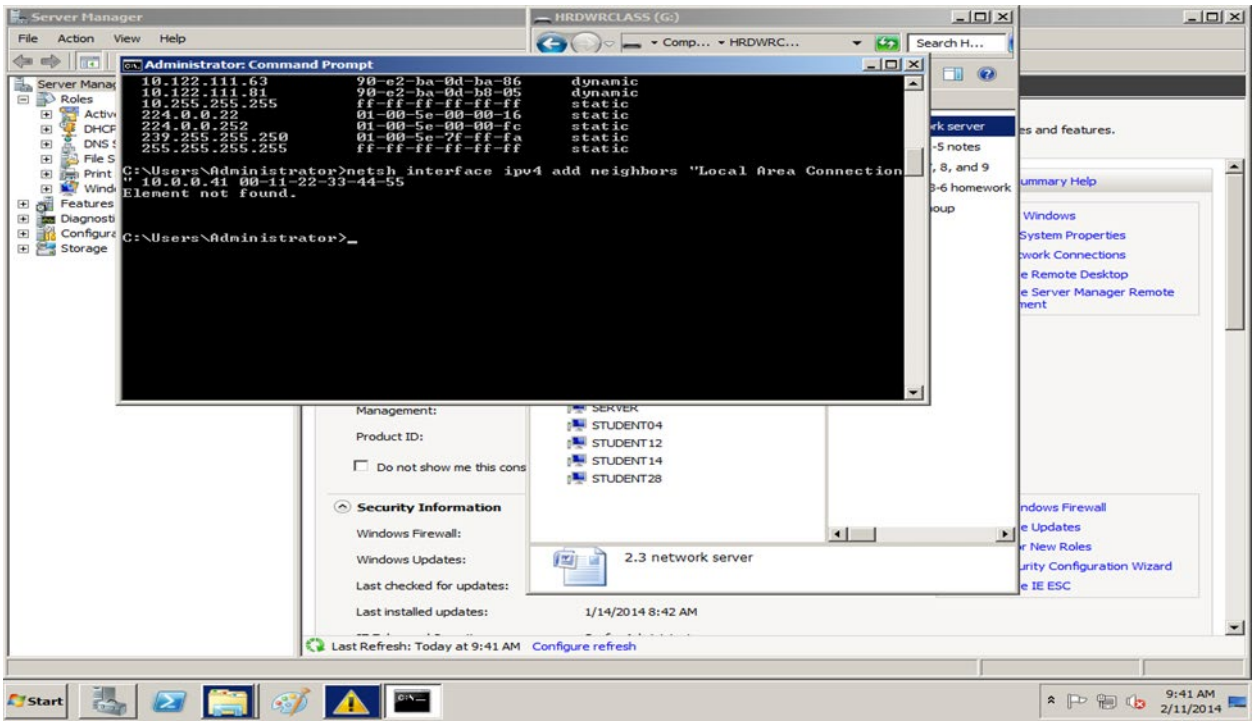
From the server I pinged my workstation address 10.0.0.33 At first it was timed out and then the packets were received.



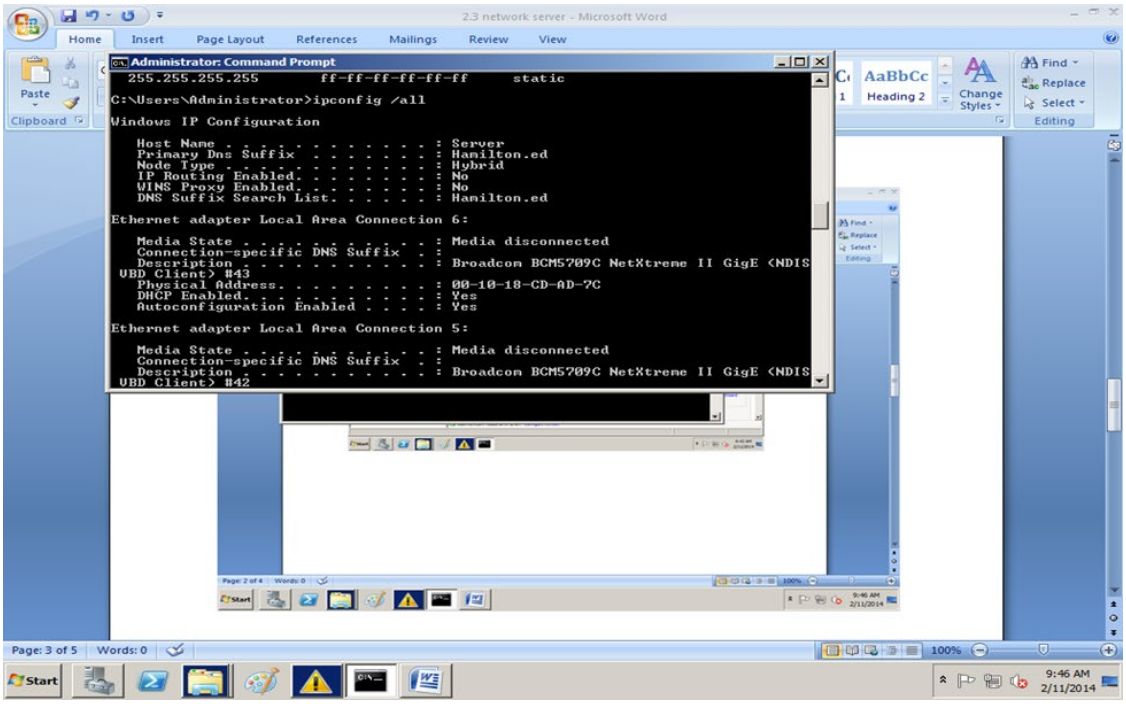
On the Server command prompt, type **arp -a** It lists every node on the switch, the IP address and the Mac address for every node. My Mac address is listed as 41-90-ez-ba-0d-b8-5



Next In the command prompt, I replaced the actual Mac address with the bogus Mac address given in the book, pressed Enter



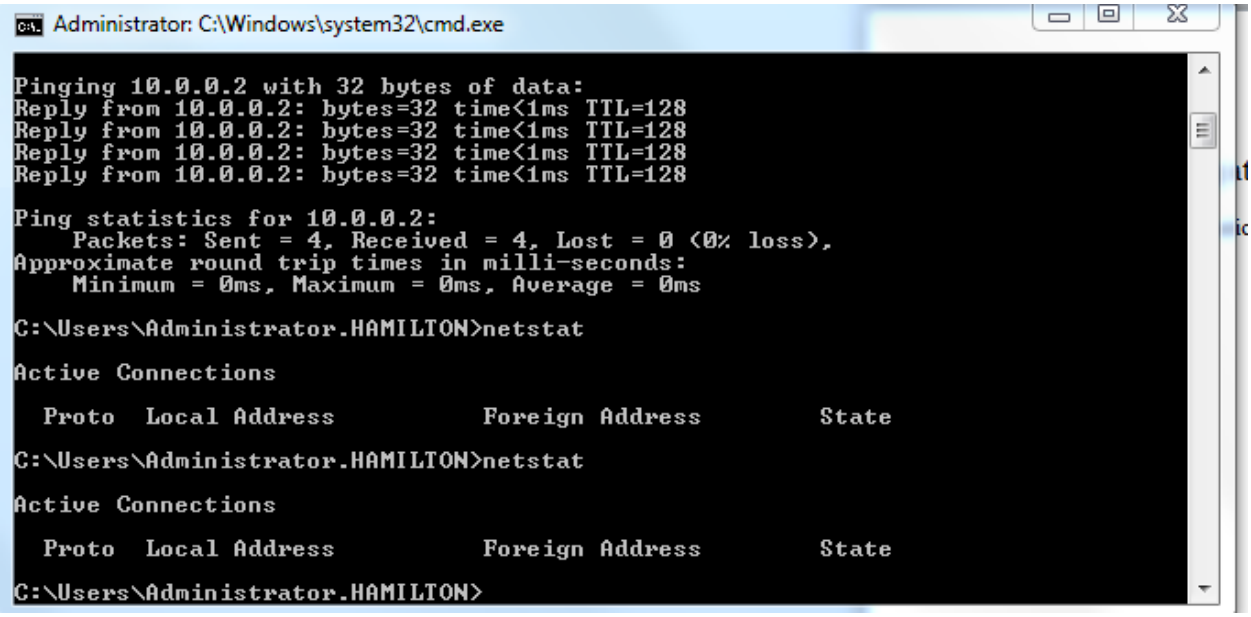
It read **Element not found,** next pinged Server successfully. Then on the Server command prompt **ipconfig /all.** It listed all information for all nodes on Network.



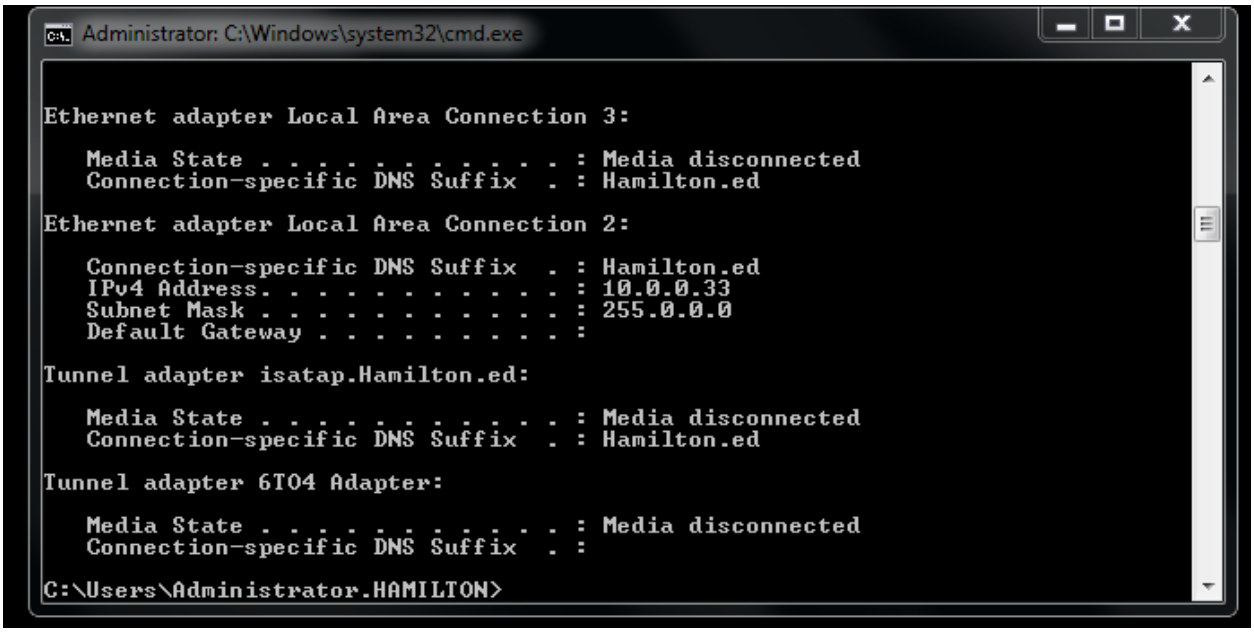
Lab 2.4 Looking at Network Connection on a Windows Computer

In Windows 7 workstation go to command prompt, type **netstat** and Enter

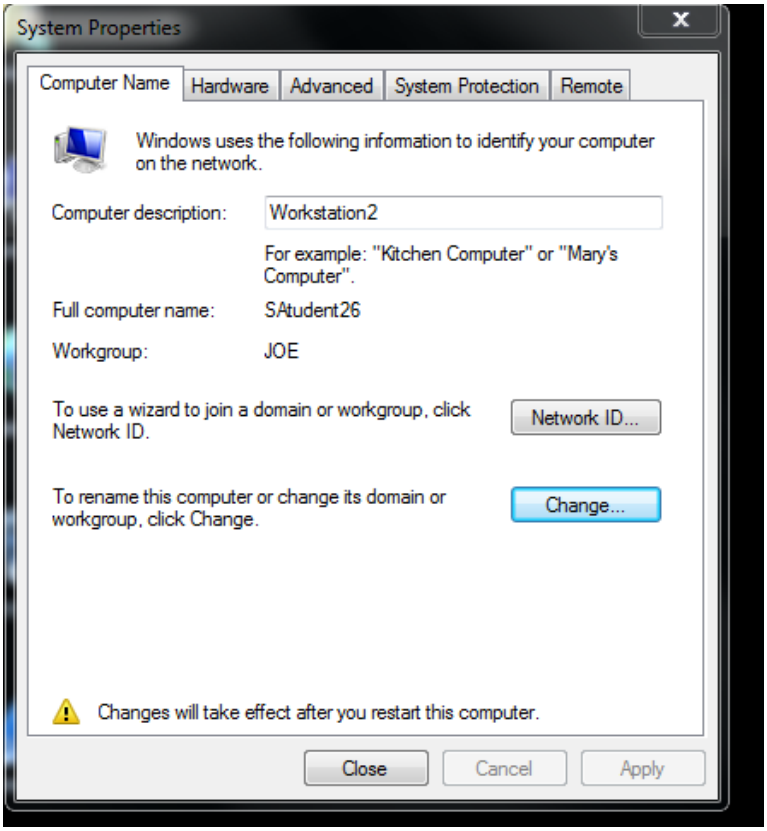
2.4 done with 2 workstations – After next 3 pages Lab 2.4 done with Server and workstations

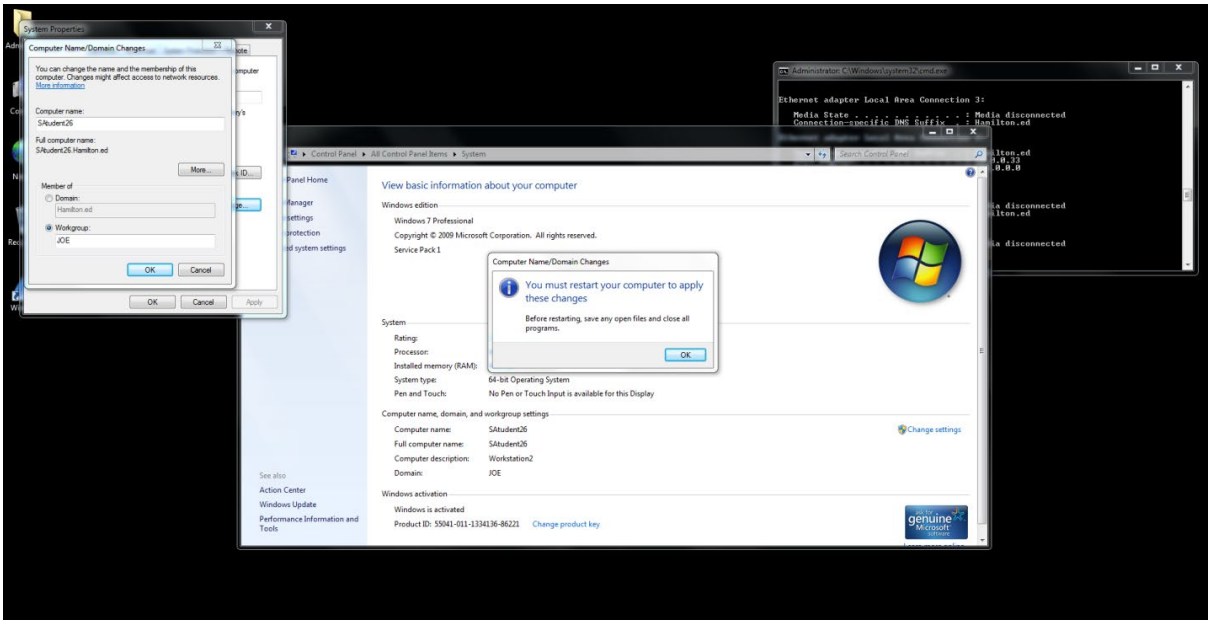


This is netstat on workstation as the only workstation on network

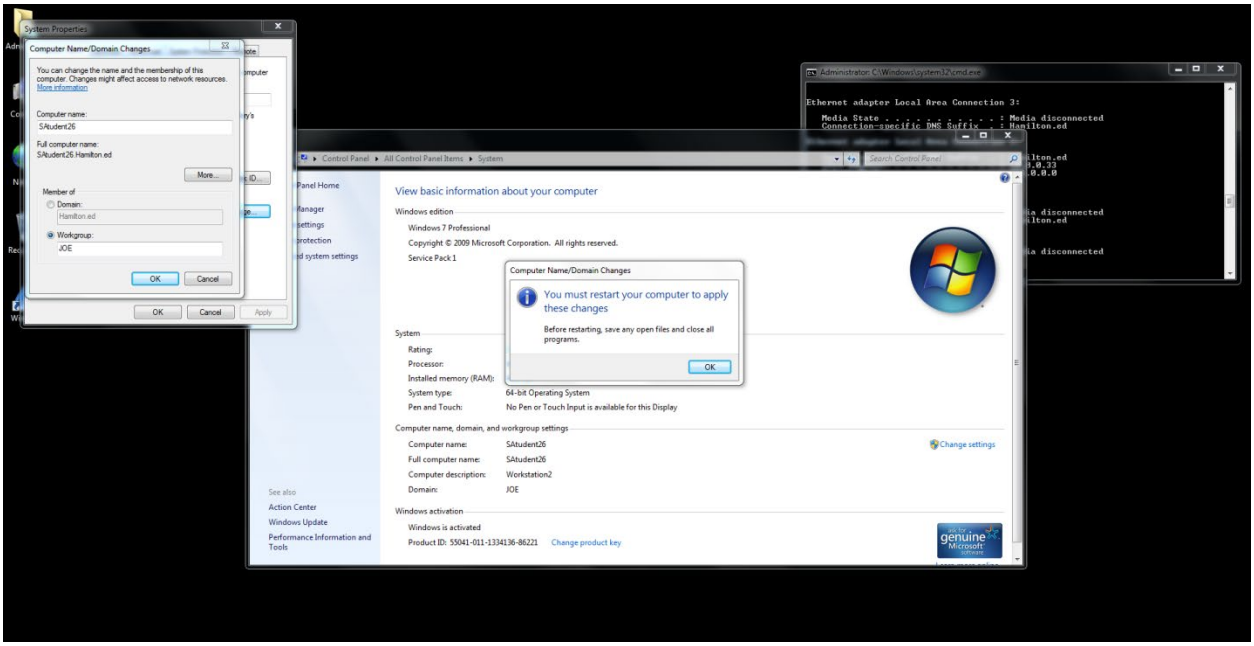


This is netstat with two workstations on network.


System Properties
Computer Name
Hardware
Advanced
System Protection
Remote
Windows uses the following information to identify your computer on the network.
Computer description:
Workstation2
For example: "Kitchen Computer" or "Mary's Computer".
Full computer name:
SAtudent26
Workgroup:
JOE
To use a wizard to join a domain or workgroup, click Network ID.
Network ID...
To rename this computer or change its domain or workgroup, click Change.
Change...
Changes will take effect after you restart this computer.
Close
Cancel
Apply


View basic information about your computer
Computer Name/Domain Changes
You must restart your computer to apply these changes
Before restarting, save any open files and close all programs.
OK

Restart



Lab 2.4 Looking at Network Connection on a Windows Computer

Always check NIC card after booting up Windows 7 Enterprise Server

- Use the following IP address:

IP address: 10.0.0.23

Subnet mask: 255.255.255.0

Default gateway: 10.0.0.1

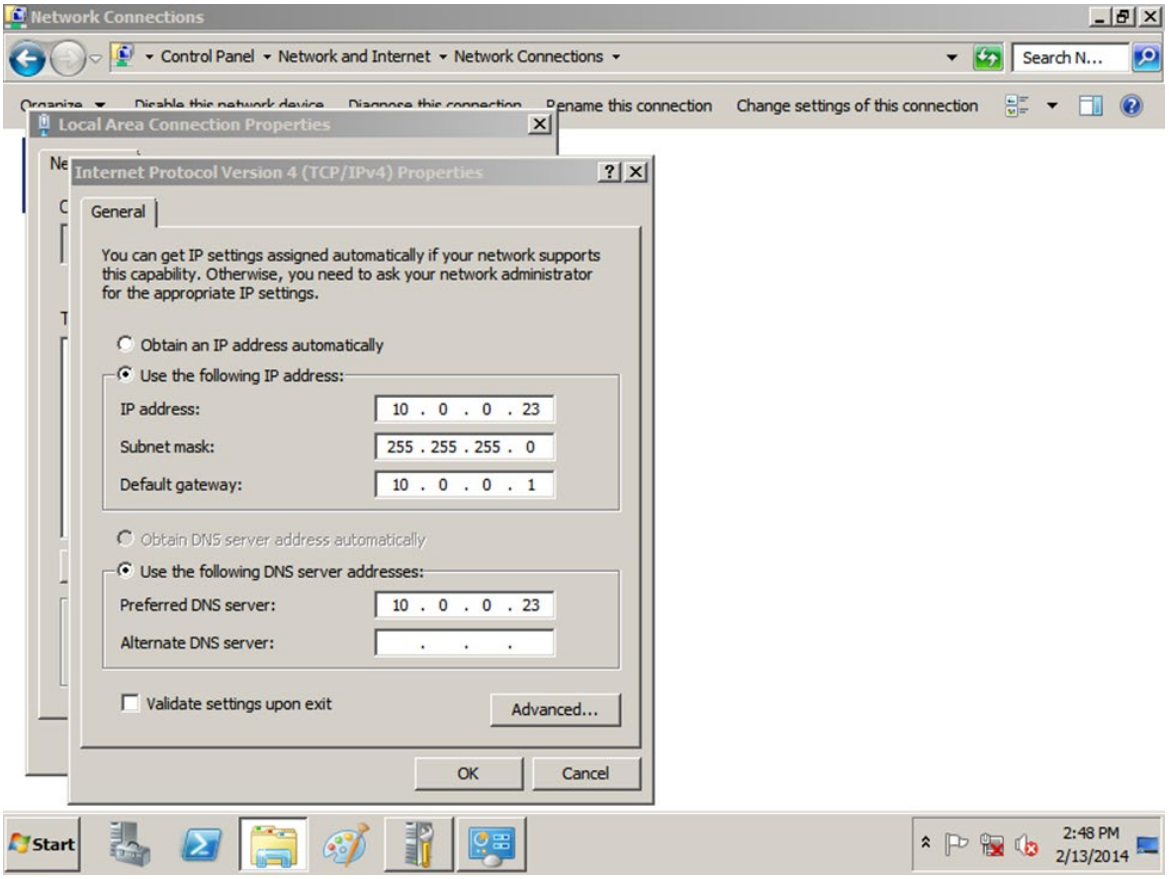
- Use the following DNS Server addresses –

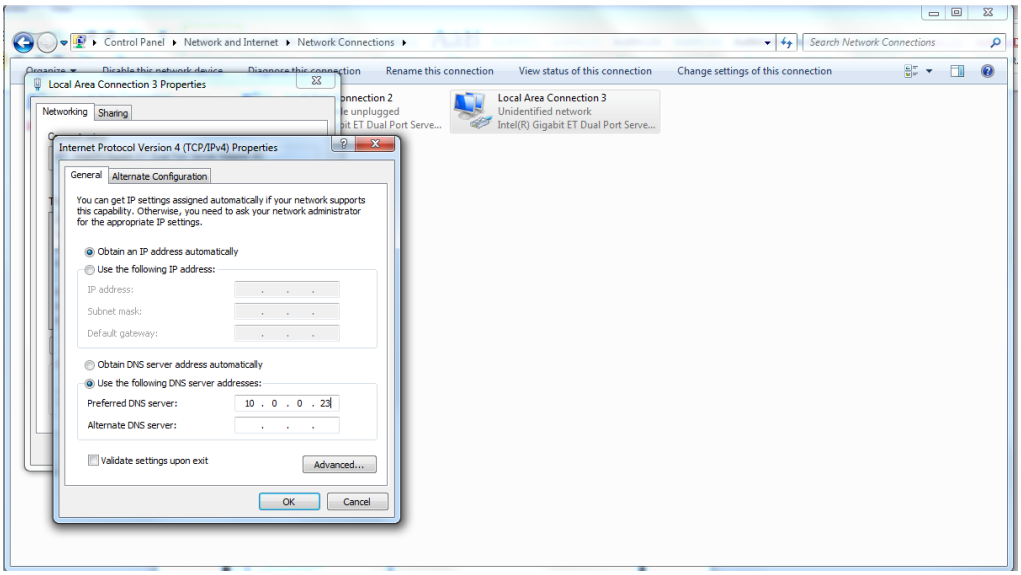
  Preferred DNS server: 10.0.0.23

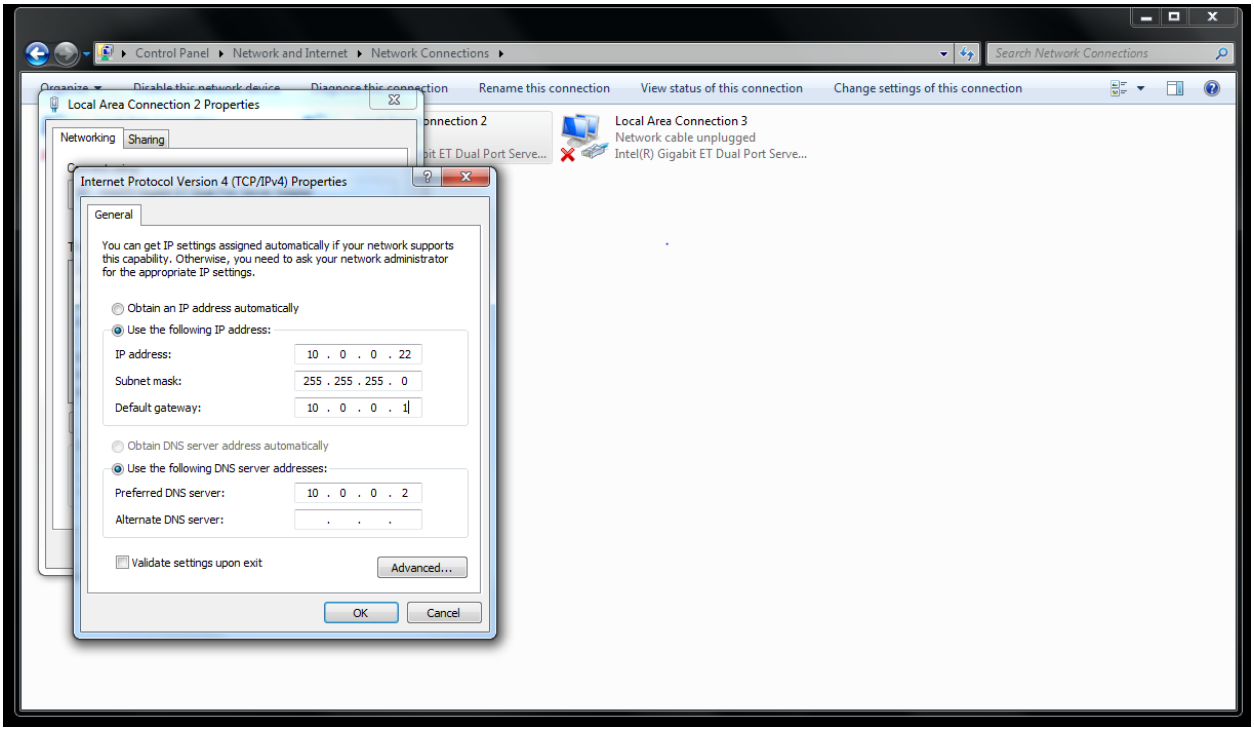
  Alternate DNS server: (Leave blank)

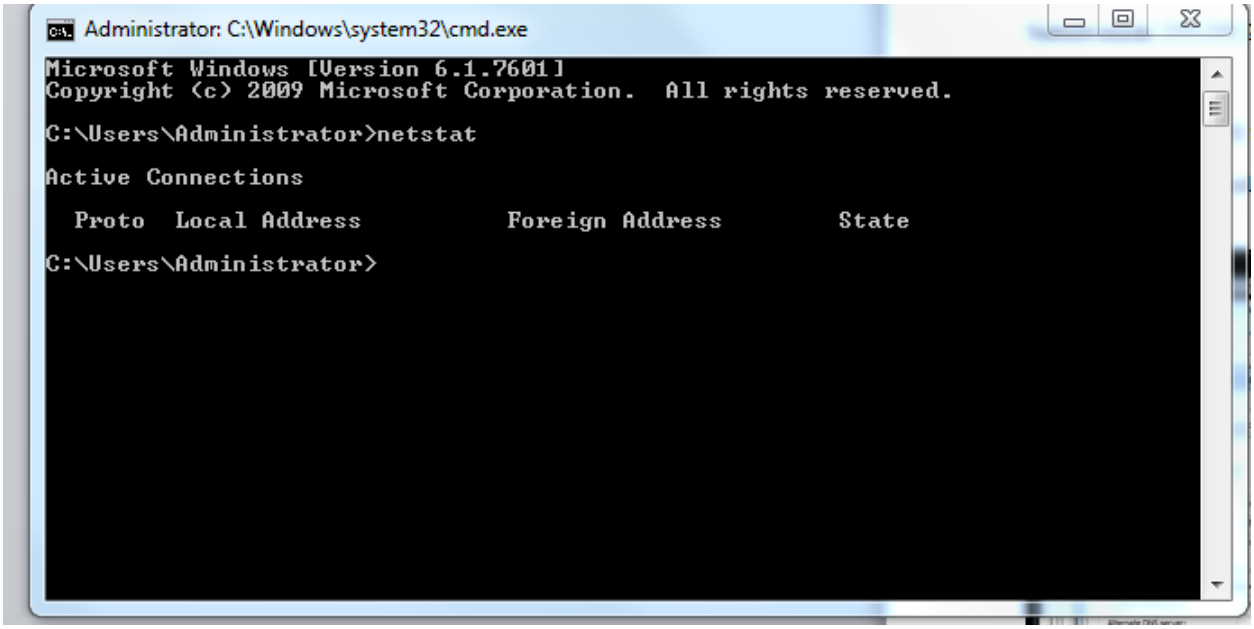
Always check NIC card on workstation –

- Always obtain IP address automatically
- Use the following DNS address 10.0.0.23

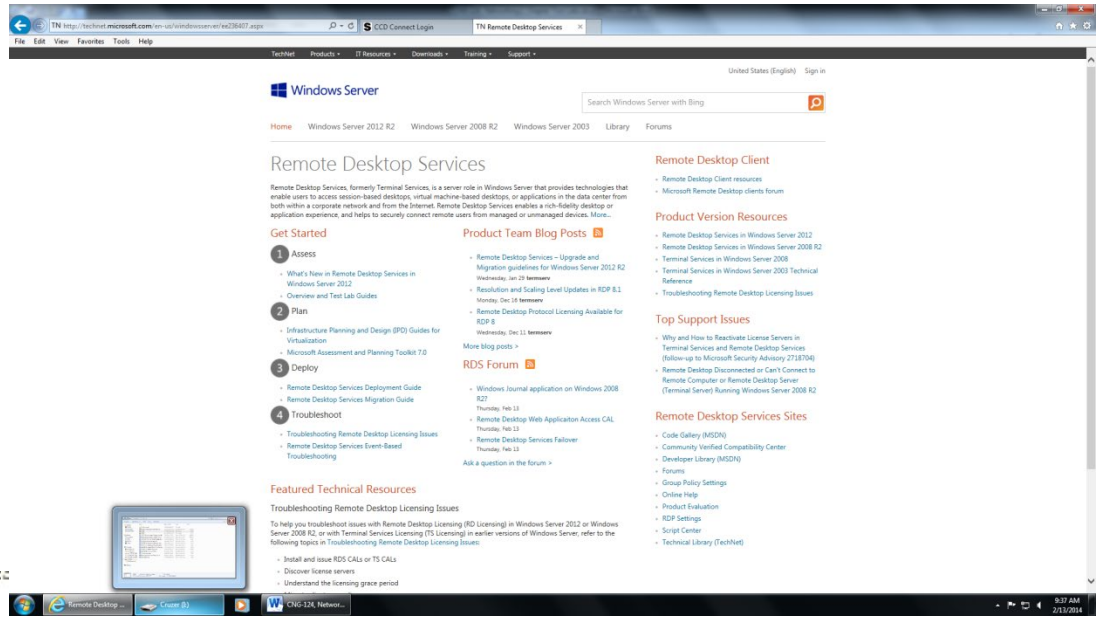

Network Connections
Control Panel ▸ Network and Internet ▸ Network Connections
Search N...
Rename this connection
Change settings of this connection
Local Area Connection Properties
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network 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: 10 . 0 . 0 . 23
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 0 . 0 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 10 . 0 . 0 . 23
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel
Start
2:48 PM
2/13/2014


Control Panel ▸ Network and Internet ▸ Network Connections
Search Network Connections
Rename this connection
View status of this connection
Change settings of this connection
Local Area Connection 3 Properties
Networking
Sharing
Local Area Connection 3
Unidentified network
Intel(R) Gigabit ET Dual Port Serve...
Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
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:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 10 . 0 . 0 . 23
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

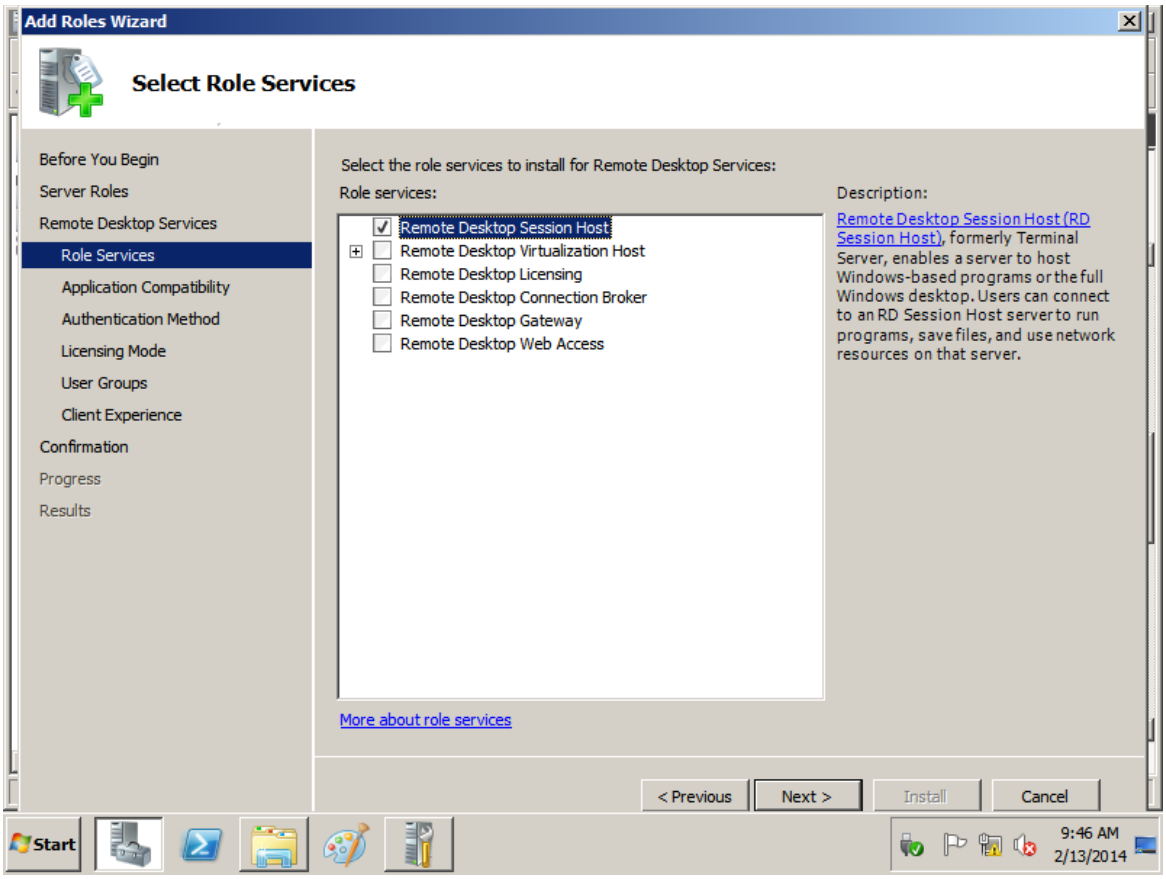

Control Panel ▸ Network and Internet ▸ Network Connections ▸
Search Network Connections
Rename this connection
View status of this connection
Change settings of this connection
Local Area Connection 2 Properties
Networking
Sharing
Local Area Connection 3
Network cable unplugged
Intel(R) Gigabit ET Dual Port Serve...
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: 10 . 0 . 0 . 22
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 0 . 0 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 10 . 0 . 0 . 2
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

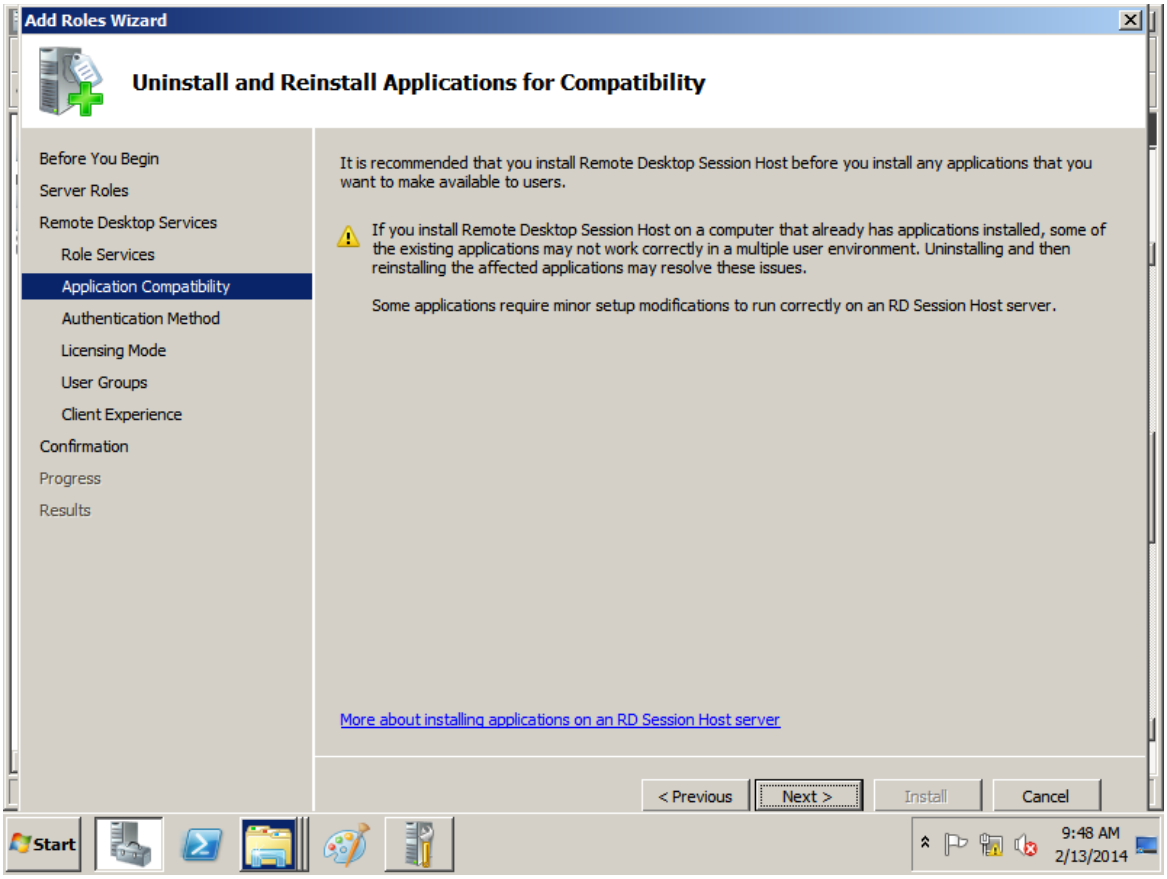

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>netstat
Active Connections
Proto Local Address Foreign Address State
C:\Users\Administrator>

Google: On Server is Remote Desktop Connection is formerly known as Terminal Services



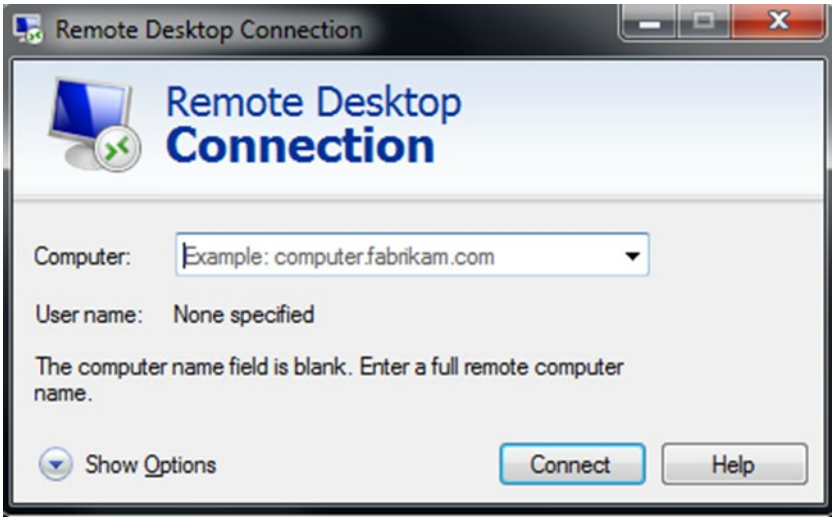
Install Remote Desktop Session Host from role services on Server

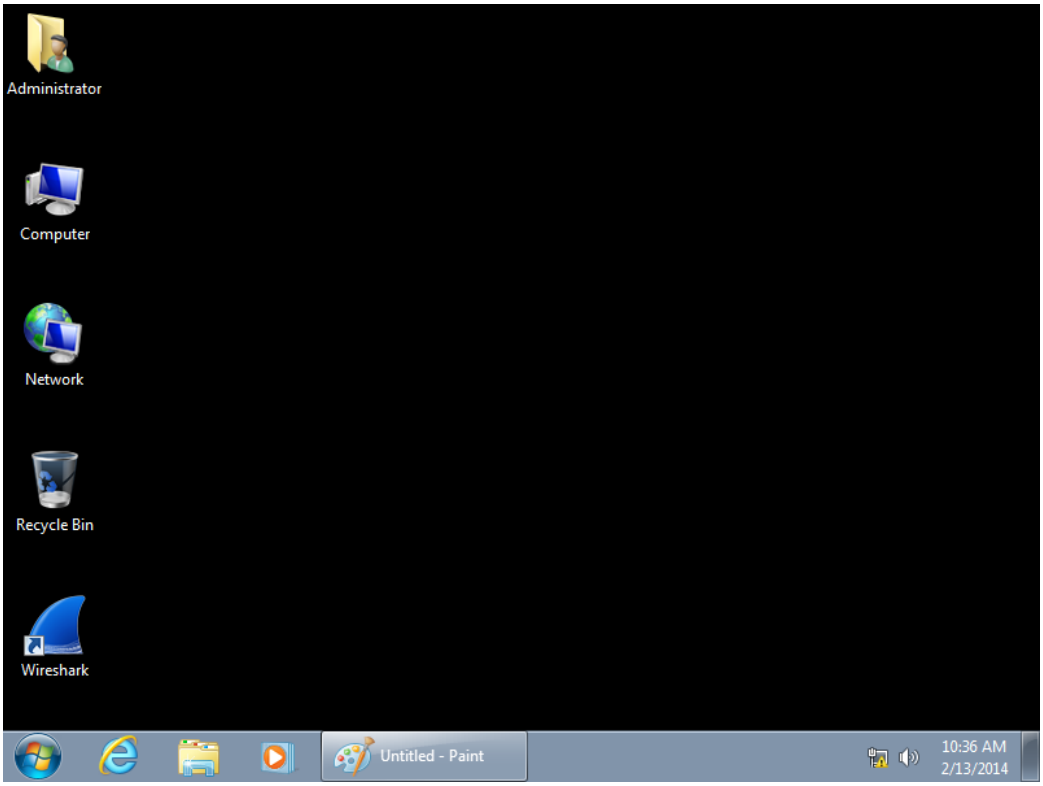




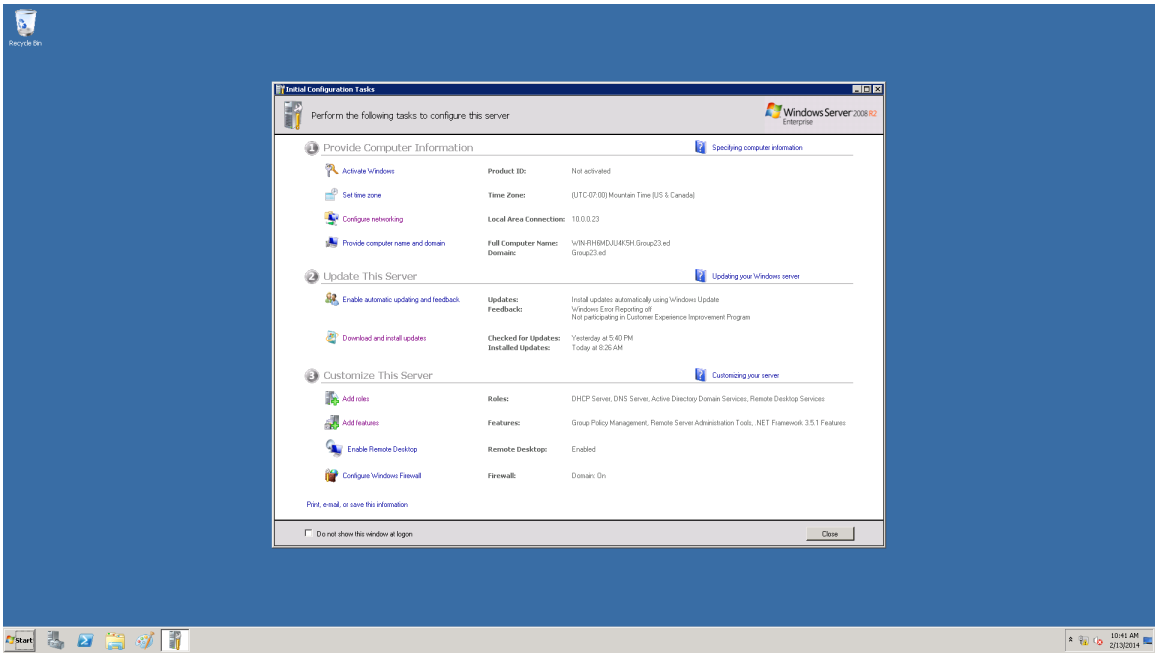
Next you open a new TCP connection by using the Remote Desktop Connection. Start – All Programs – Accessories, click Remote Desktop Connection

With the Server and the workstations open and remote desktop connection open on both, type the IP address of the other into each



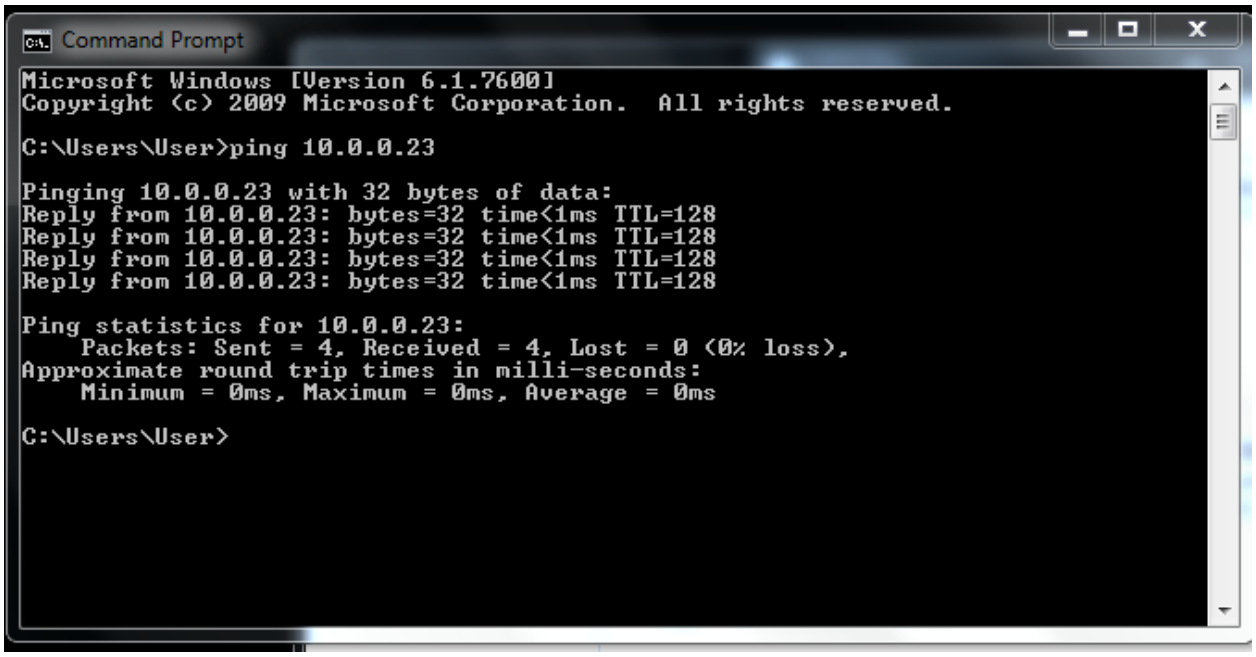


Above is the Workstation Screen on the Server monitor. Below is the server screen on the workstation monitor. Remote Desktop successfully installed and Lab. 2.4 complete.



Lab 2.5 Viewing Ethernet Frame

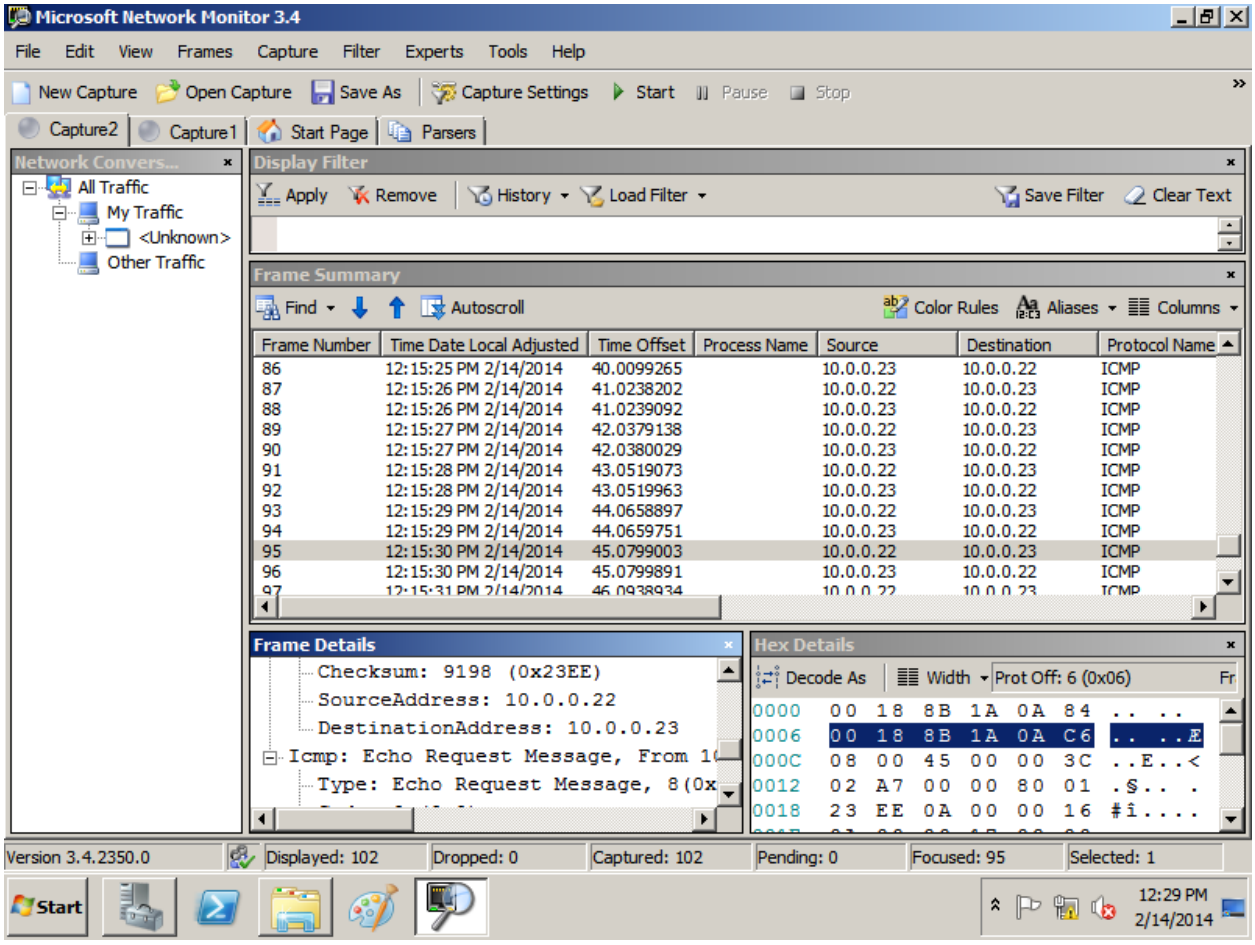
Verify that workstation and Server are communicating - On workstation - Ping Server **-t** 10.0.0.23 and press Enter – (**-t** sets up workstation for Server to read Microsoft Network Monitor 3.4



On Server - Install Microsoft Network Monitor 3.4

On Server – Start button - All Programs – Click Microsoft Network Monitor 3.4 icon – Local Area Connection is checked – Click New Capture – When the number of frames captured is 100, click stop on the toolbar. Locate a frame with "ICMP" in the Protocol field and click that row.

"The Internet Control Message Protocol (ICMP) [RFC792] protocol is classic example of a client server application. The ICMP server executes on all IP end system computers and all IP intermediate systems (i.e routers). The protocol is used to report problems with delivery of IP datagrams within an IP network. It can be sued to show when a particular End System (ES) is not responding, when an IP network is not reachable, when a node is overloaded, when an error occurs in the IP header information, etc. The protocol is also frequently used by Internet managers to verify correct operations of End Systems (ES) and to check that routers are correctly routing packets to the specified destination address." (Support.microsoft.com.)



Click the plus sign next to the Ethernet – click the plus sign next to Ipv4 – Click the plus signs next to Icmp. Lab 4, finished and successful.

IPv4 subnetting reference

“In the IPv4 address space certain address blocks are specially allocated or reserved for special uses such as loopback interfaces, private networks (RFC 1918),[1] and state-less auto configuration (Zeroconf, RFC 3927) of interfaces. Such addresses may be used without registration or allocation from Regional Internet Registries (RIRs). However, these address ranges must not be routed into the public Internet infrastructure. The netmask is a bitmask that can be used to separate the bits of the network identifier from the bits of the host identifier. It is often written in the same notation used to denote IP addresses. Not all sizes of prefix announcement may be routable on the public Internet: see routing, peering. The blocks numerically at the start and end of classes A, B and C were originally reserved for special addressing or future features, i.e., 0.0.0.0/8 and 127.0.0.0/8 are reserved in former class A; 128.0.0.0/16 and 191.255.0.0/16 were reserved in former class B but are now available for assignment; 192.0.0.0/24 and 223.255.255.0/24 are reserved in former class C.

While the 127.0.0.0/8 network is a Class A network, it is designated for loopback and cannot be assigned to a network."

Class	Leading bits	Start	End	Default Subnet Mask in dotted decimal	CIDR notation
A	0	0.0.0.0	127.255.255.255	255.0.0.0	/8
B	10	128.0.0.0	191.255.255.255	255.255.0.0	/16
C	110	192.0.0.0	223.255.255.255	255.255.255.0	/24
D	1110	224.0.0.0	239.255.255.255	not defined	not defined
E	1111	240.0.0.0	255.255.255.255	not defined	not defined

Internet Control Message Protocol

The Internet Control Message Protocol (ICMP) is one of the main protocols of the Internet Protocol Suite. It is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached. ICMP can also be used to relay query messages.[1] It is assigned protocol number 1.[2] ICMP[3] differs from transport protocols such as TCP and UDP in that it is not typically used to exchange data between systems, nor is it regularly employed by end-user network applications (with the exception of some diagnostic tools like ping and traceroute). ICMP for Internet Protocol version 4 (IPv4) is also known as ICMPv4. IPv6 has a similar protocol, ICMPv6." (Wikipedia)

Lab 2.1 Review Questions

1. C 2. A,B 3. D 4. C 5. A,C,D

Lab 2.2

1. B 2. C 3. D 4. A 5. Using DHCP to assign IP addressing can nearly eliminate duplicate addressing problems. 6. D

Lab 2.3

1. B 2. A 3. C 4. B 5. A 6. C 7. C 8. A

Lab 2.4

1. B 2. C 3. D 4. C 5. A 6. C

Lab 2.5

1. Physical Layer 2. Data Link Layer 3. D 4. D

Joseph Martinez

Networking I: Network +

CNG – 124

Chapter Three Labs

Transmission Basics and Networking Media

Lab 3.1 Learning Media Characteristics

Lab 3.2 Creating UTP Crossover Cable to Connect Two Computers

Lab 3.3 Comparing Throughput

Lab 3.4 Understanding How a Category 5 Cable Fails

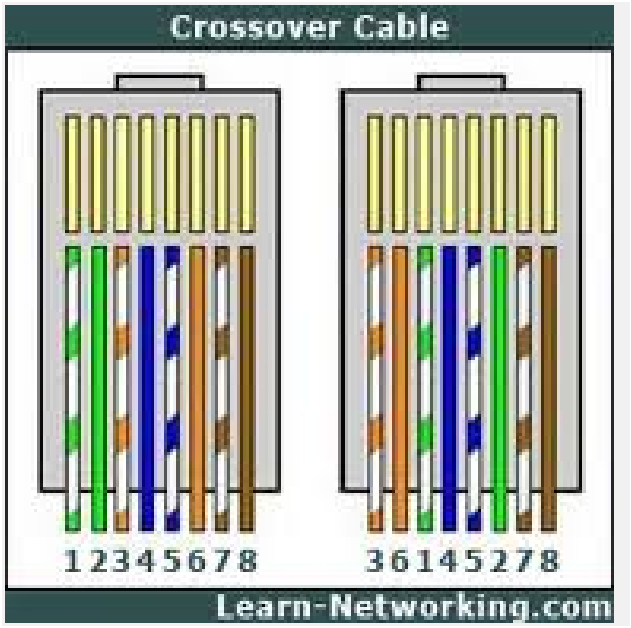
Lab 3.5 Connecting Two Switches with Fiber-Optic Cable

Lab 3.1 Learning Media Characteristics

Store or Web site name:	Circuit City	
Item	**Cost in $ amount**	**Notes**
Category 5 cable	.55	1-300 feet per foot
Highest-quality available	60.	VOX-high quality coiled cable 29.5 Ft.
Low-end, four-port Ethernet hub or switch with RJ-45 connections	50.	Netgear N30E
16-port hub or switch with RJ-45 connections	70.	Netgear
802.11n wireless access point or a home router that includes a wireless access point	35.	Tendra Wireless N300
Desktop Computer	400.	400-244
Laptop Computer	1100.	MD760LL/A Mac Book Air
Ethernet NIC for desktop	132.	N-FX-LC-02F
PCMCIA or USB NIC for a desktop	17.	NT-B20
Wireless network card for a desktop	315.	WIC-1U5U-T1V2RF
Wireless network card for a desktop	315.	CISCCO HWIC-2T
Windows 7 Professional	140.	Microsoft
50 workstations and 20 laptops with operating systems	29,957.	50 Lenovo desktops, HP laptops
Category 5 cable to connect all workstations and 20 laptops	5. per ft.	
Category 5e,6,6e, or 7 cable to connect all 50 workstations and 20 laptops	400.	
Wired and wireless NICs for desktops and laptops	Wired: 20. Wireless: 20.	Tendra TEL9901G,W311Mi
One wireless access point and a sufficient number of hubs or switches to connect all the workstations and laptops to the network	Wireless access@35. Switch @30.	Greenet 880G,8 port
Total cost of the network with Category 5 cable	48,300.	
Total cost of the network with highest-quality cable available	31,000.	

Lab 3.2 Creating UTP Crossover Cable to Connect Two Computers

- Creating a TIA/EIA 568A and TIA/EIA 568B crossover cable

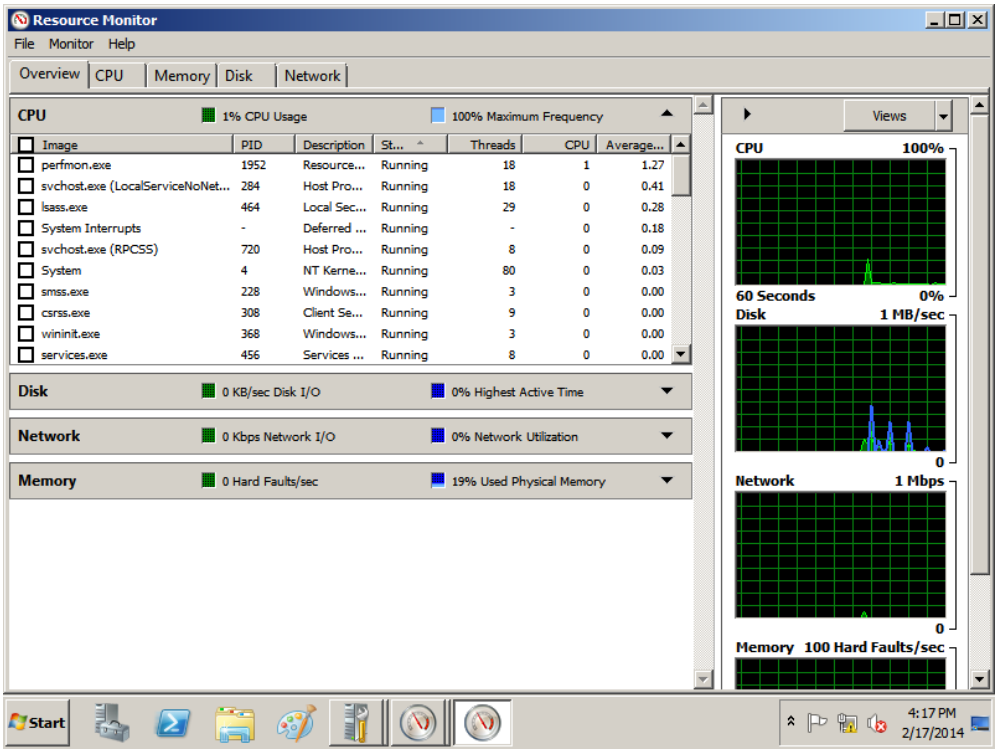


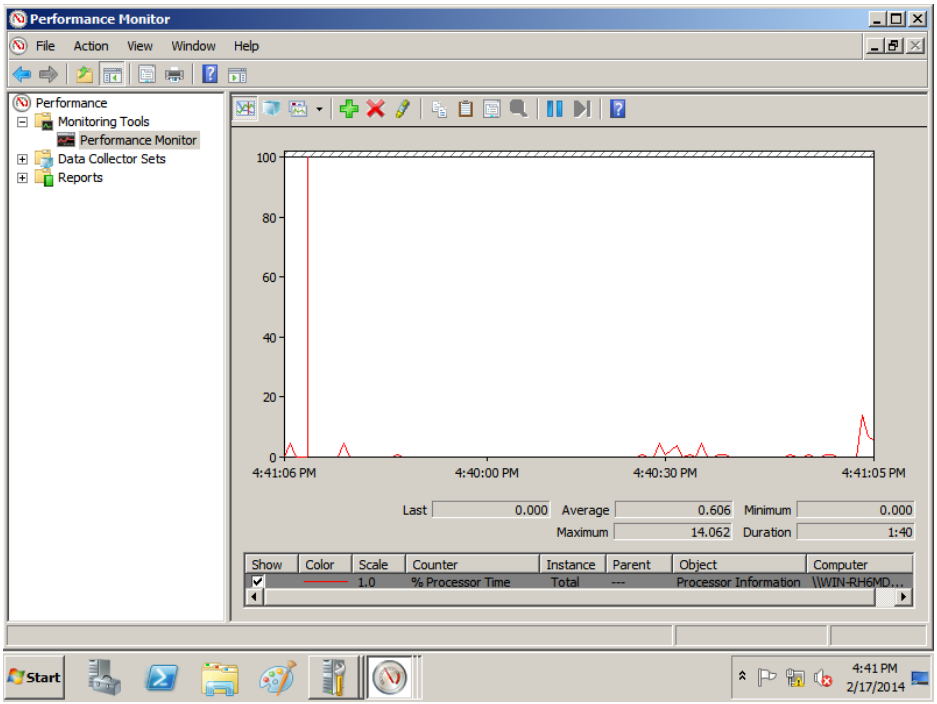
- Follow steps 1 through 7 in lab book
- Test the cable on the tester
- Connect two work stations together – ping both workstations and verify that they are communicating.

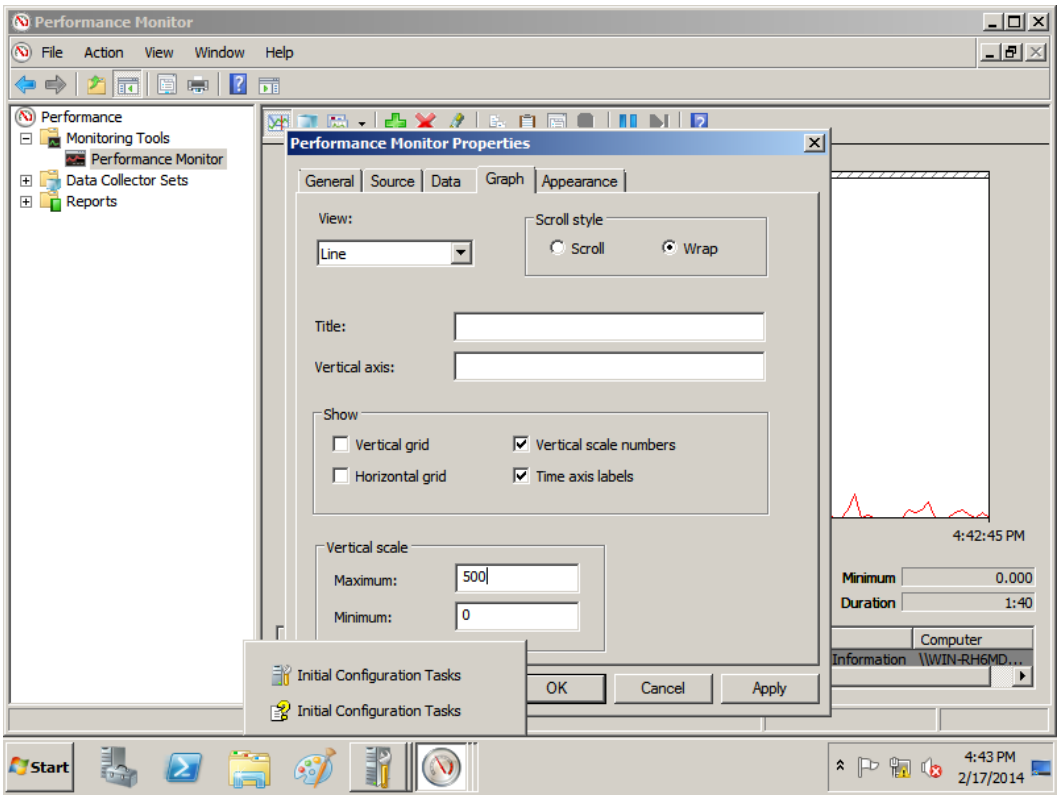
Complete steps 9 through 13

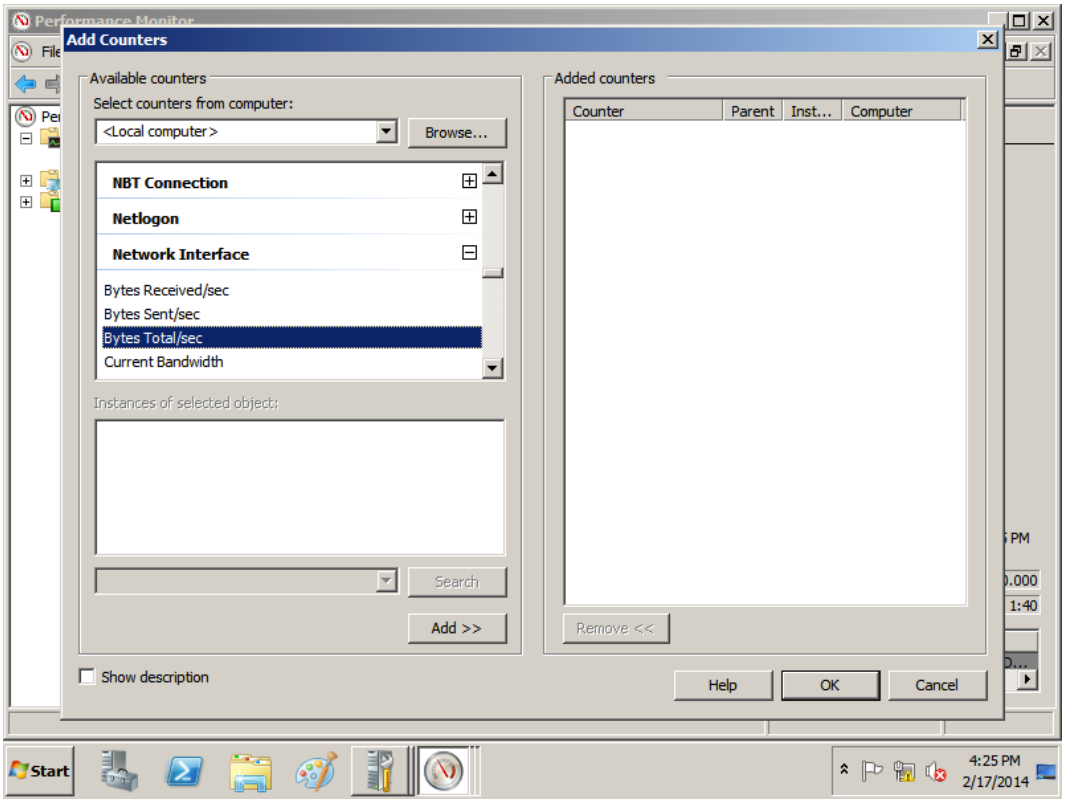
Lab 3.3 Comparing Throughput

Connect Server 1 and workstation to switch – On Server 1 – Start – all programs – administrator tools – performance monitor – Add counters – Network Interface -


Resource Monitor
File Monitor Help
Overview CPU Memory Disk Network
CPU 1% CPU Usage 100% Maximum Frequency
Image PID Description St... Threads CPU Average...
perfmon.exe 1952 Resource... Running 18 1 1.27
svchost.exe (LocalServiceNoNet... 284 Host Pro... Running 18 0 0.41
lsass.exe 464 Local Sec... Running 29 0 0.28
System Interrupts - Deferred ... Running - 0 0.18
svchost.exe (RPCSS) 720 Host Pro... Running 8 0 0.09
System 4 NT Kerne... Running 80 0 0.03
smss.exe 228 Windows... Running 3 0 0.00
csrss.exe 308 Client Se... Running 9 0 0.00
wininit.exe 368 Windows... Running 3 0 0.00
services.exe 456 Services ... Running 8 0 0.00
Disk 0 KB/sec Disk I/O 0% Highest Active Time
Network 0 Kbps Network I/O 0% Network Utilization
Memory 0 Hard Faults/sec 19% Used Physical Memory
Views
CPU 100%
60 Seconds 0%
Disk 1 MB/sec
0
Network 1 Mbps
0
Memory 100 Hard Faults/sec
Start
4:17 PM
2/17/2014

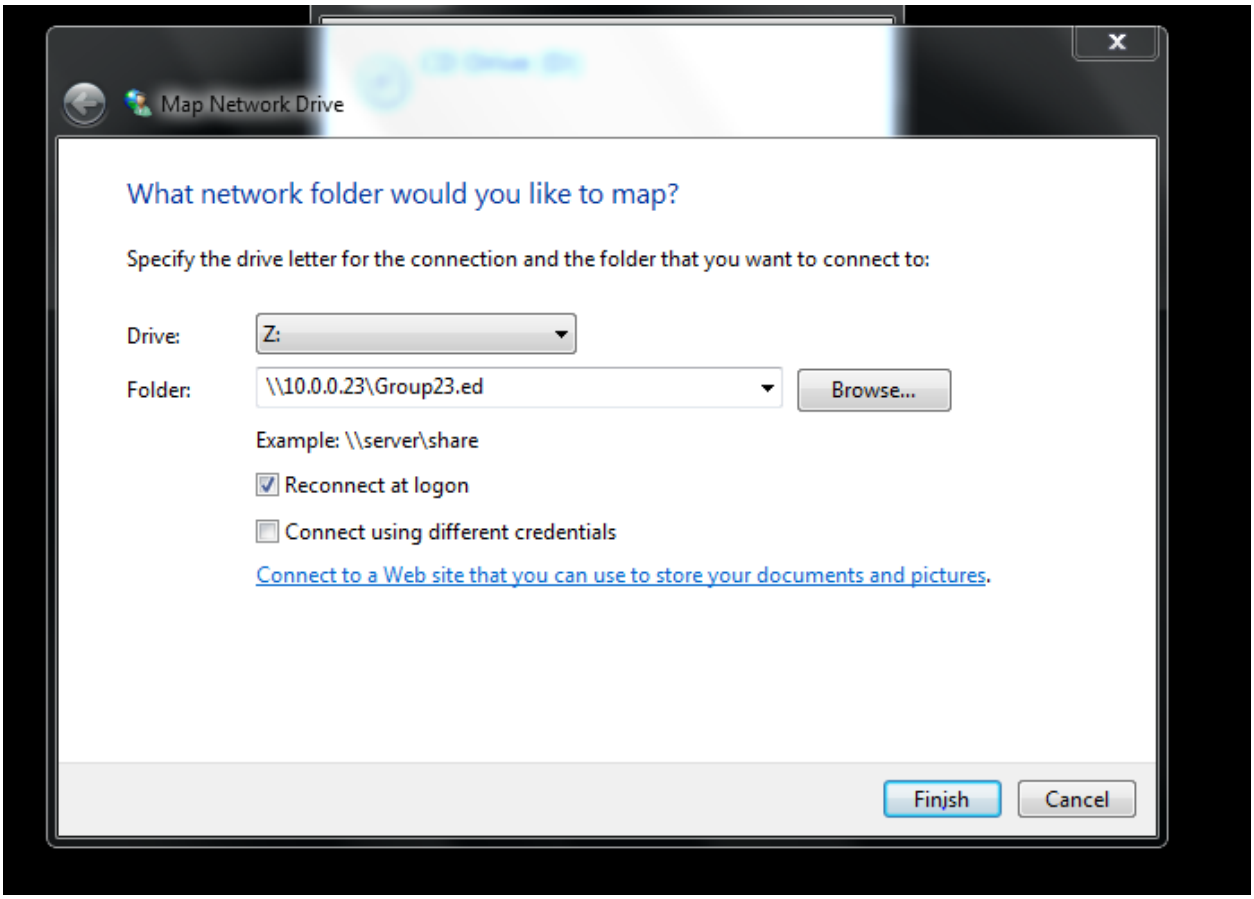

Performance Monitor
File Action View Window Help
Performance
Monitoring Tools
Performance Monitor
Data Collector Sets
Reports
100
80
60
40
20
0
4:41:06 PM
4:40:00 PM
4:40:30 PM
4:41:05 PM
Last 0.000 Average 0.606 Minimum 0.000
Maximum 14.062 Duration 1:40
Show Color Scale Counter Instance Parent Object Computer
1.0 % Processor Time Total --- Processor Information \\WIN-RH6MD...
Start
4:41 PM
2/17/2014


Performance Monitor
File Action View Window Help
Performance
Monitoring Tools
Performance Monitor
Data Collector Sets
Reports
Performance Monitor Properties
General Source Data Graph Appearance
View:
Line
Scroll style
Scroll
Wrap
Title:
Vertical axis:
Show
Vertical grid
Horizontal grid
Vertical scale numbers
Time axis labels
Vertical scale
Maximum:
500
Minimum:
0
OK
Cancel
Apply
4:42:45 PM
Minimum 0.000
Duration 1:40
Computer
Information \\WIN-RH6MD...
Initial Configuration Tasks
Initial Configuration Tasks
Start
4:43 PM
2/17/2014


Add Counters
Available counters
Select counters from computer:
<Local computer>
Browse...
NBT Connection
Netlogon
Network Interface
Bytes Received/sec
Bytes Sent/sec
Bytes Total/sec
Current Bandwidth
Instances of selected object:
Search
Add >>
Added counters
Counter
Parent
Inst...
Computer
Remove <<
Show description
Help
OK
Cancel
Start
4:25 PM
2/17/2014

Expand the Network Interface category, click Bytes Total/sec – Add – OK

Log on to Workstation – Start – Computer – Map network drive – choose z

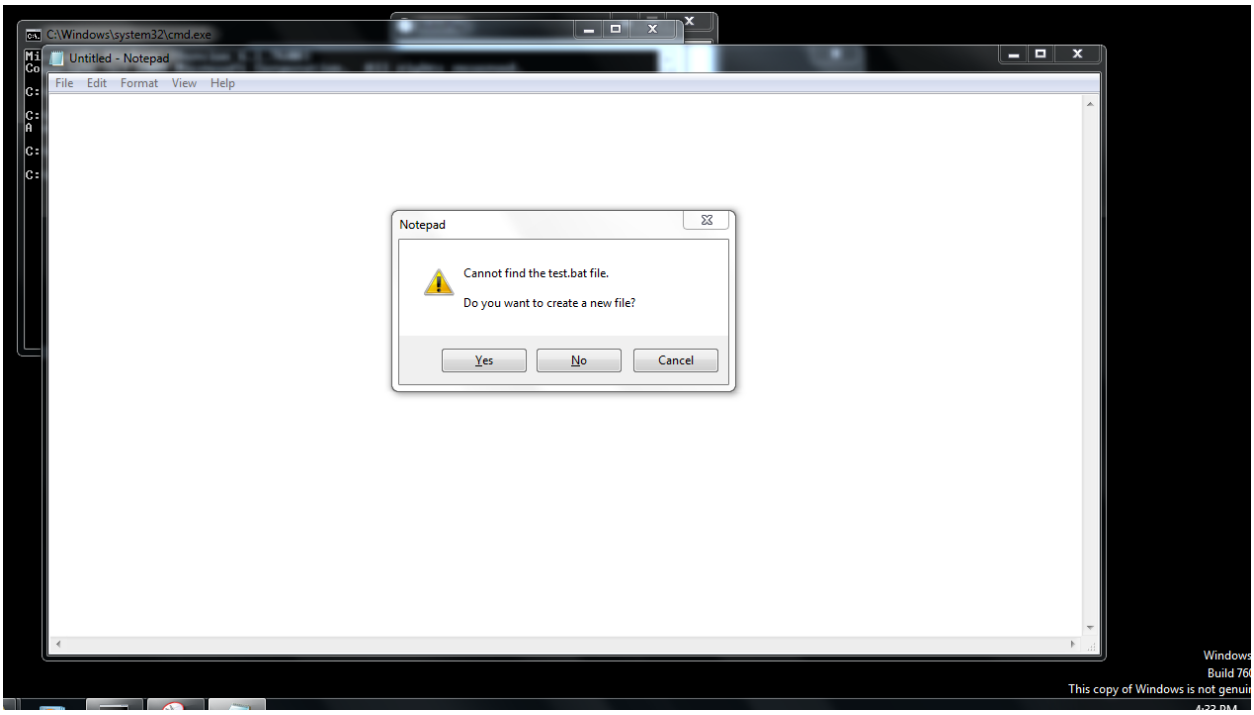


Type I.P. address of the server \\10.0.0.23\netplus - click Finish

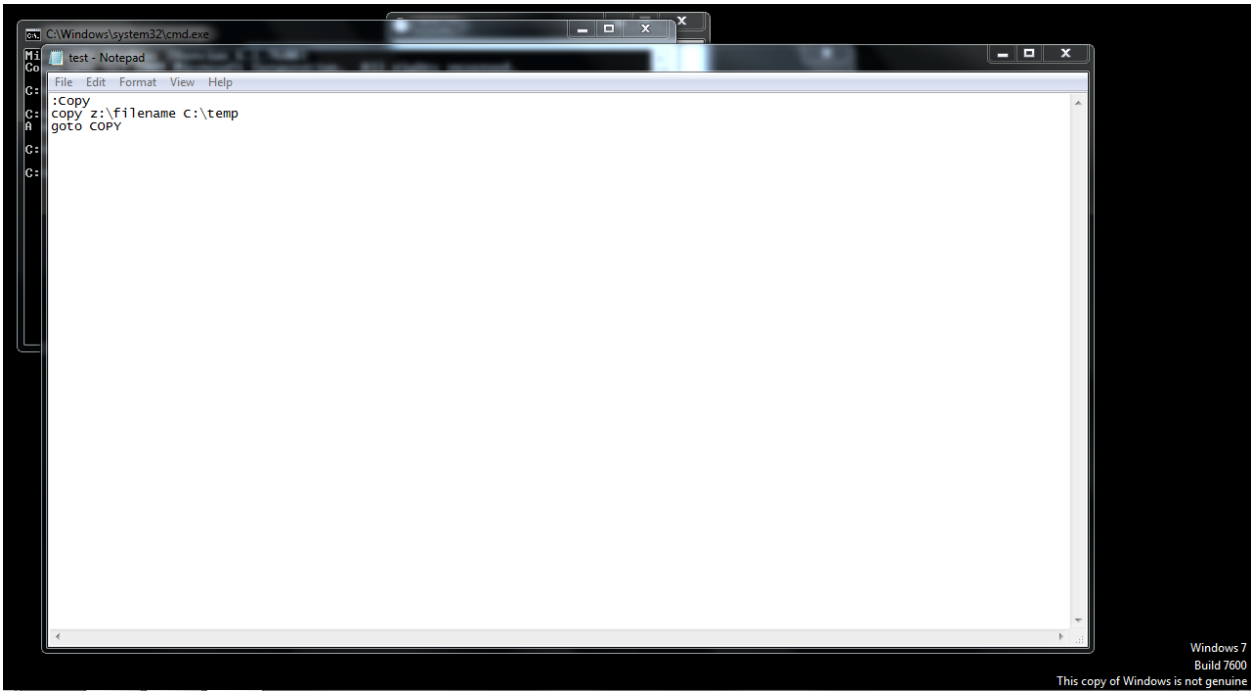
Start - cmd – Enter – Start – All programs –Accessories –command prompt

Type **mkdir C:temp** – Enter

Type notepad test.bat - Yes

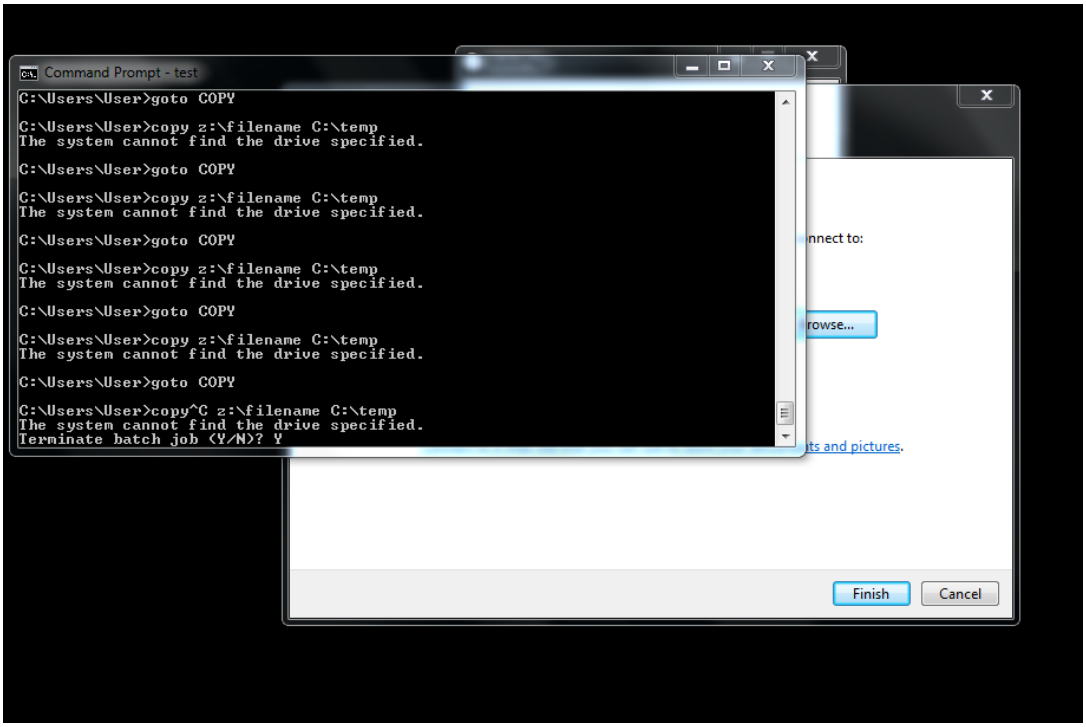


In notepad enter: Copy – copy z:\filename C:\temp – goto COPY

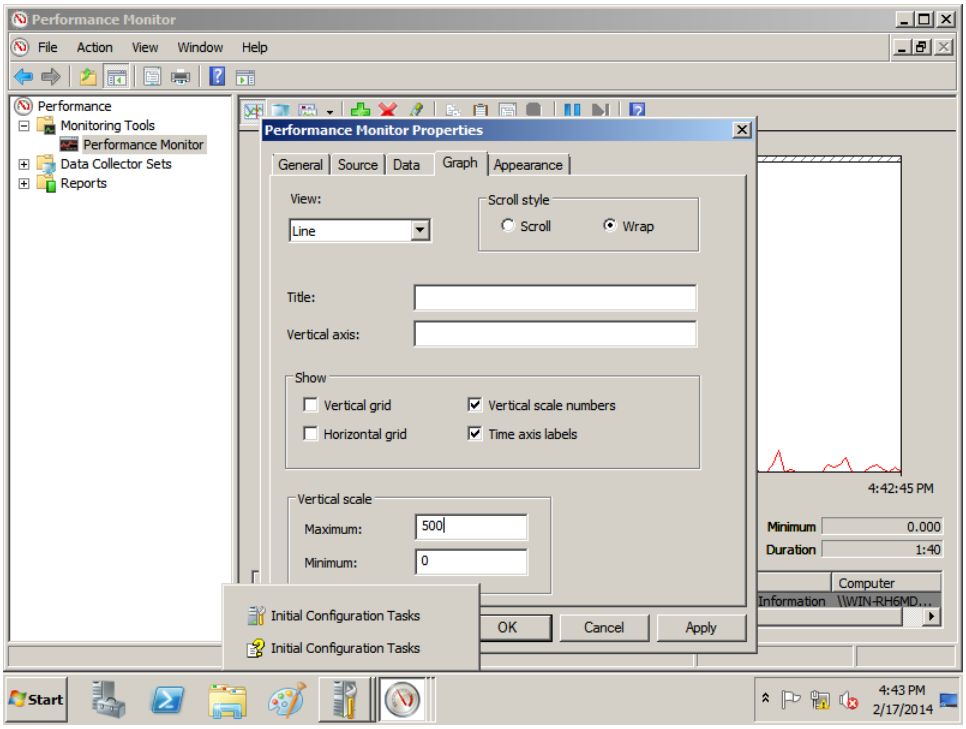


Exit - Save

Command prompt – type test – Enter. The batch file continuously copies the file to the Workstation from the shared folder on Windows Server 2008



On the Server – click Graph – in the maximum text box click 500, 5000, and then 50,000



After a minute, look at the Average box at the bottom of the graph and record the number of bytes received per second. Multiply this number by 8 to find the number bits per second. Record the number bits received per second and compare it with the bandwidth.

0.406 bytes x 8 = 3.248 bits

Steps 25 through 29 successful

At the command prompt on the Workstation, press Ctrl+C to stop the batch file. Type Y - Enter

Review Questions

Lab 3.1

1. A
2. A
3. D
4. A
5. D
6. B

Lab 3.2

1. A,D
2. B
3. A,D
4. B
5. C
6. A
7. A

Lab 3.3

1. A,B
2. C
3. C
4. A
5. D
6. B
7. B

Lab 3.4

1. D\
2. B,C
3. C
4. C
5. B
6. D

Lab 3.5

1. B
2. D
3. D
4. C
5. A

Joseph Martinez

Networking I: Network +

CNG – 124

Chapter Four Labs

Introduction to TCP/IP Protocols

Lab 4.1 Configuring IP Addresses and Subnet Masks

Lab 4.2 Automatically Assigning IP Addresses with DHCP

Lab 4.3 Configuring Domain Name System (DNS) Properties

Lab 4.4 Using FTP

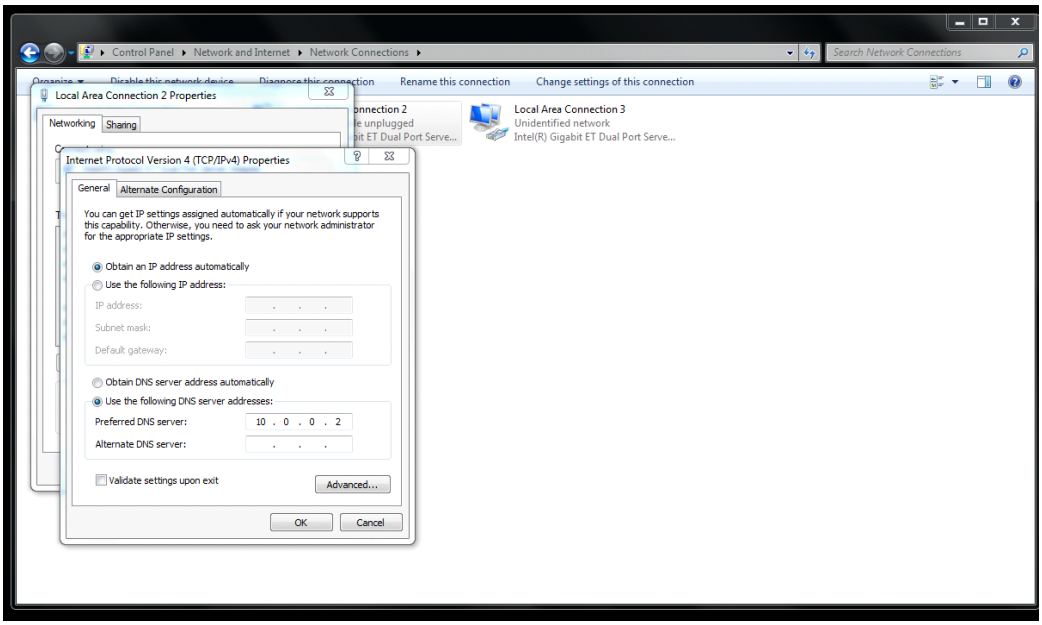
Lab 4.5 Understanding Port Numbers

Lab 4.6 Disabling Unnecessary Protocols

Lab 4.1 Configuring IP Addresses and Subnet Masks

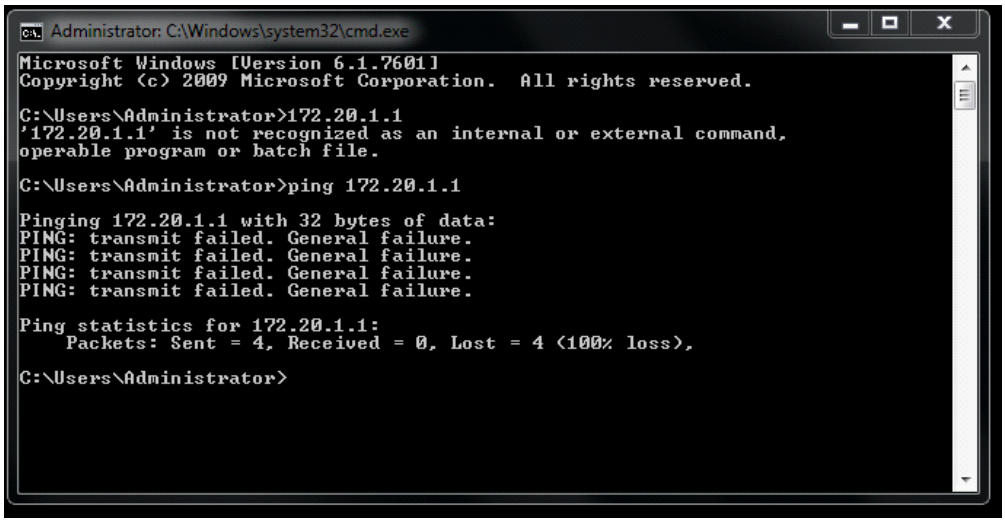
Two workstations: On one workstation click

+ Start – Control Panel – Network and Internet – Network and Sharing Center – Change Adapter Settings. In the Network Connections window, right click Local Area Connection and select Properties.

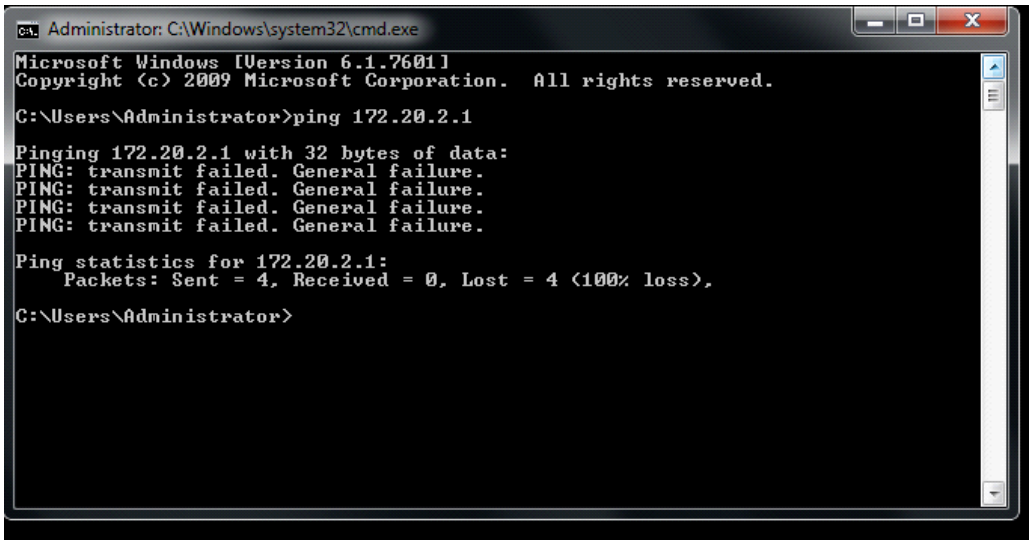


Double click Internet Protocol Version 4 (TCIP/IPv4). Enter 172.20.1.1 in the IP address text box. Enter 255.255.255.0 in the subnet mask text box. Click OK

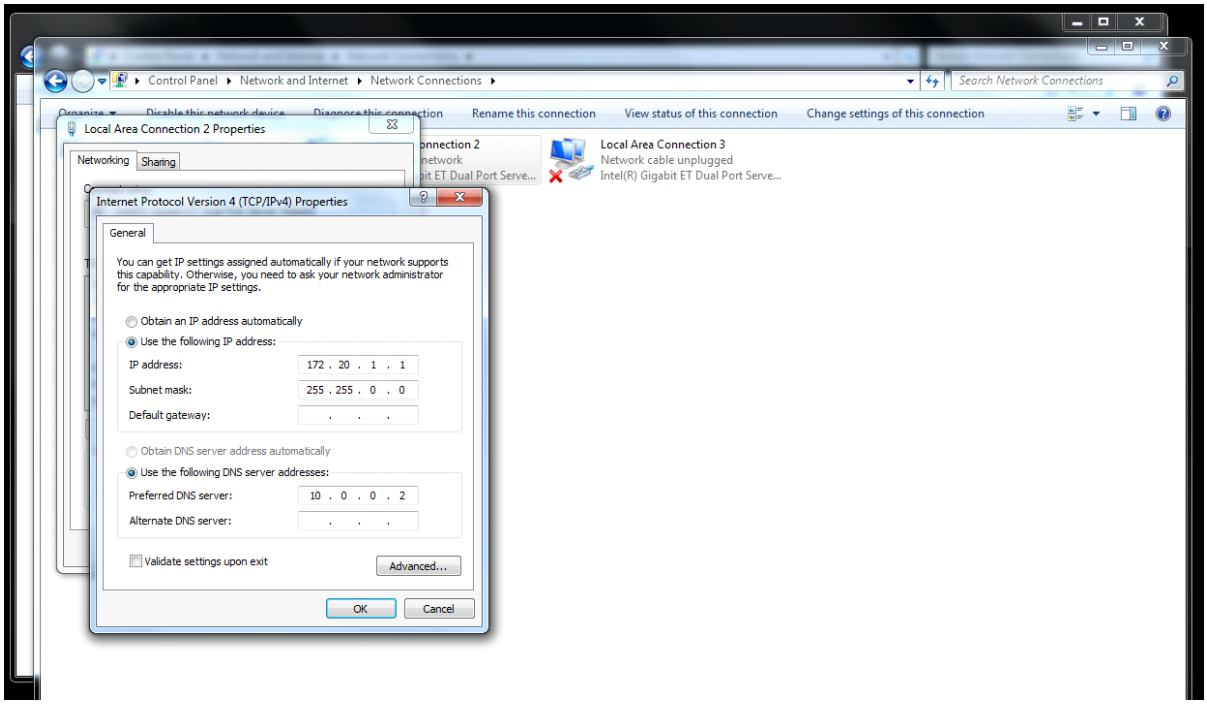
Configure second computer in a different network using 172.20.2.1 as the IP address and 255.255.255.0 as the subnet mask. Second computer - Command Prompt – Ping 172.20.1.1



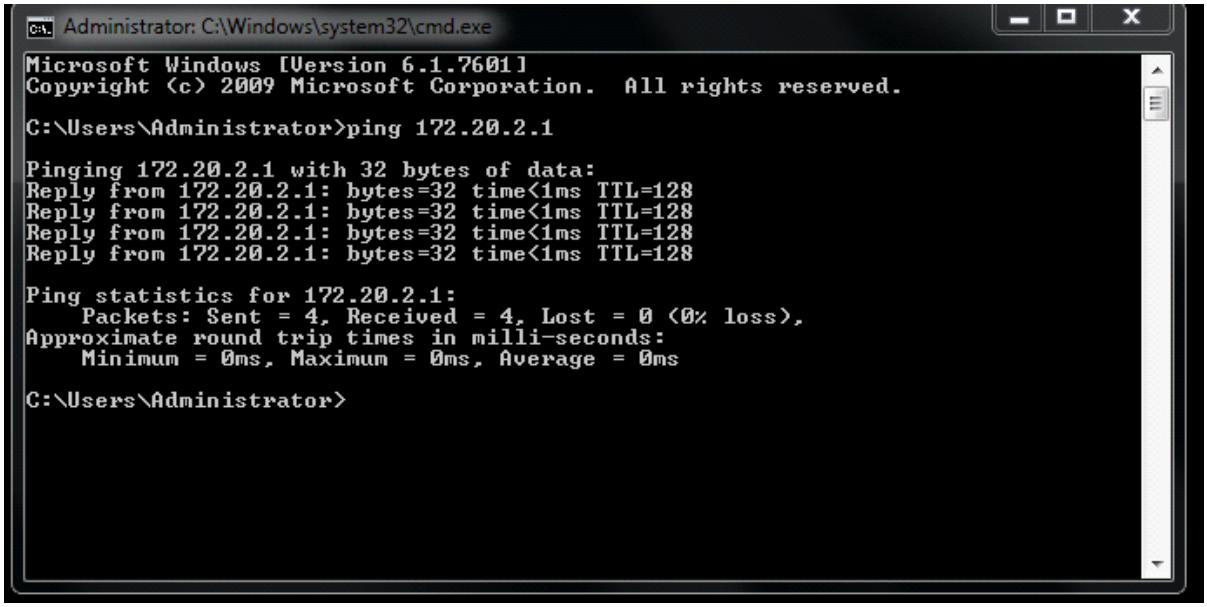
First computer Ping 172.20.1.1



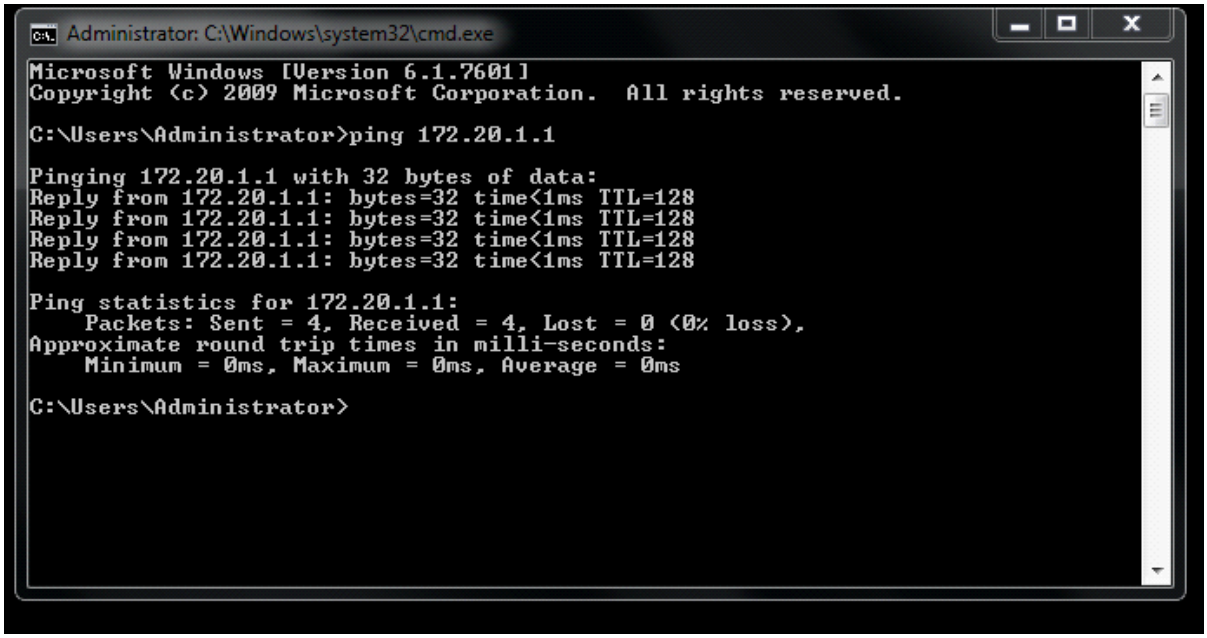
They are both not connecting. Next, change the subnet mask on both computers so that they are on the same network – change to 255.255.0.0



Ping successful from first computer to second.



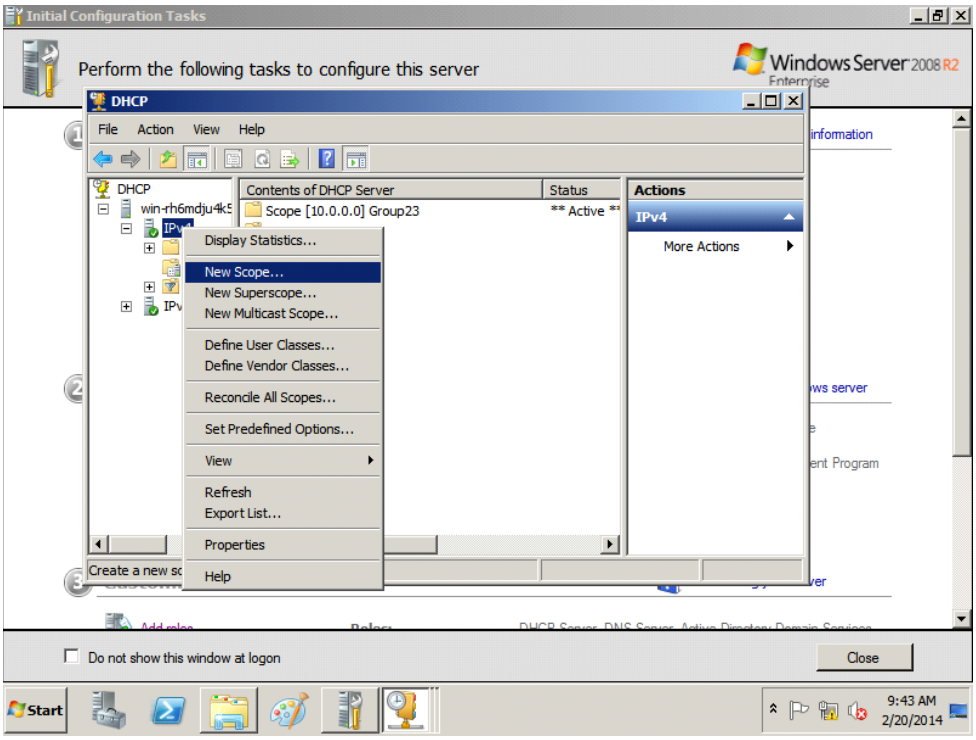
Ping successful from second computer to first.

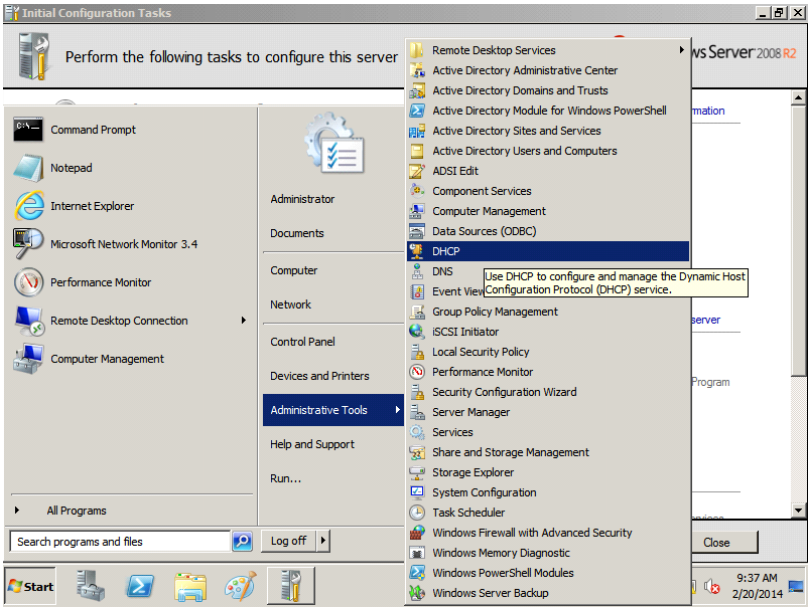


Lab 4.2 Automatically Assigning IP Addresses with DHCP

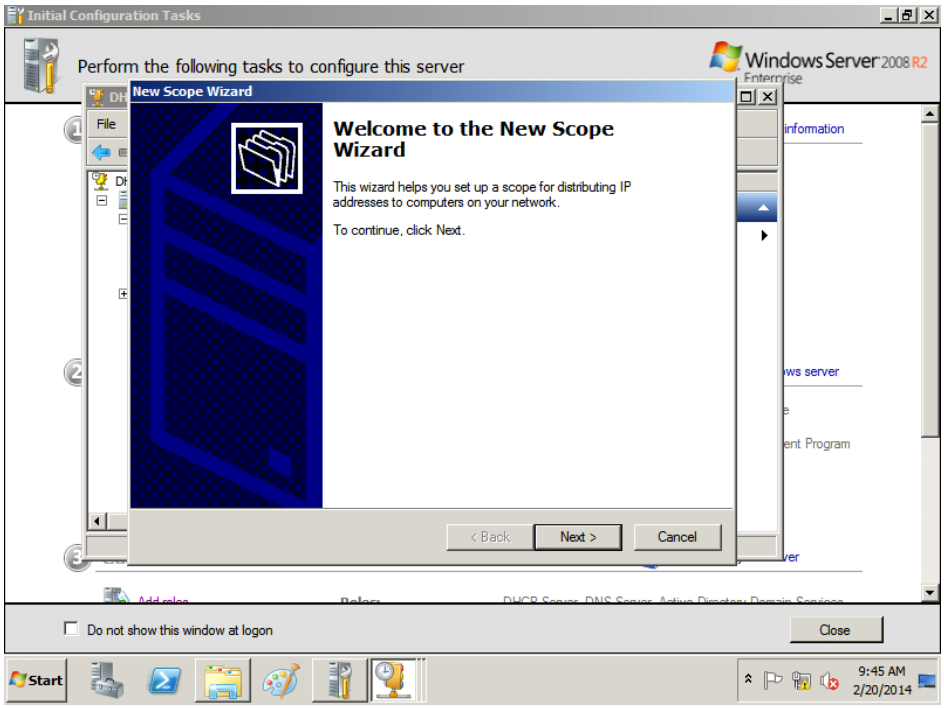
In this lab you assign addresses to client workstations automatically with the Host Dynamic Configuration Protocol (DHCP) server.

Log on to Server, when desktop appears click Start – Administrative Tools – click DHCP – click server1.netpluslab.net in the left pane – right click IPv4 – New Scope

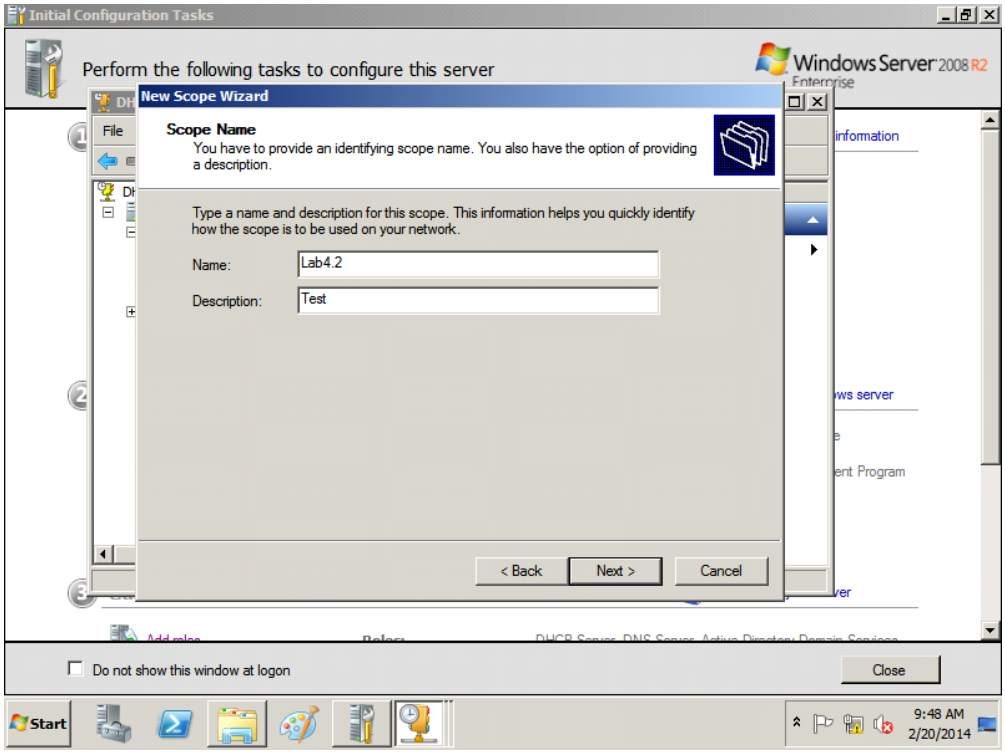




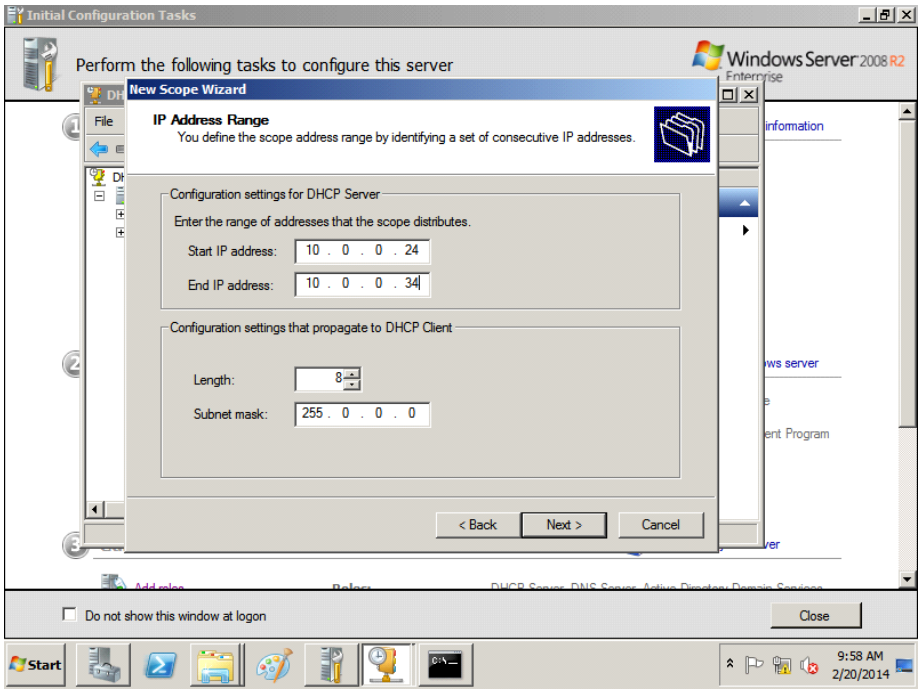
New Scope Wizard opens - Next



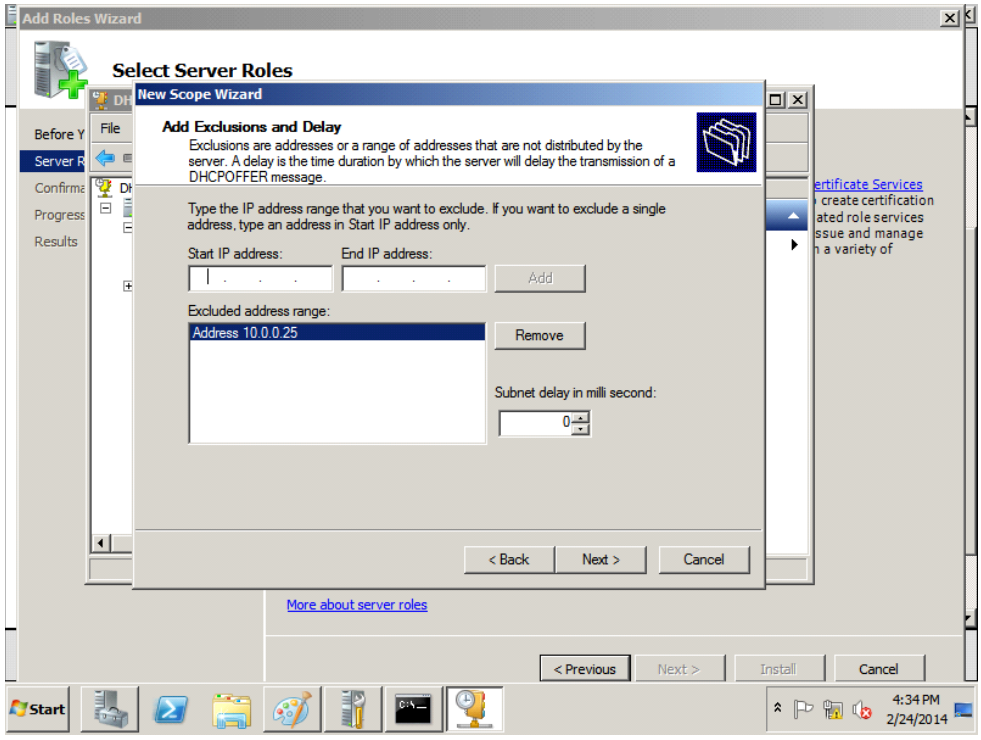
Enter Lab 4.2 in the name box – Enter Test in the Description box



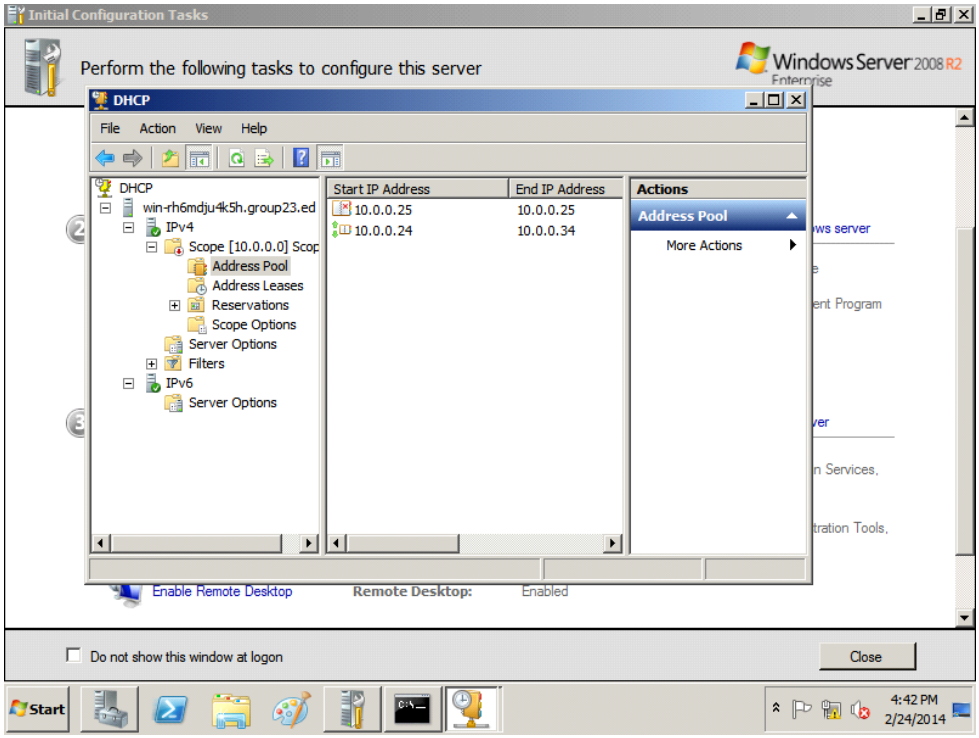
Now I configured the DHCP server to assign IP addresses from 10.0.0.24 to 10.0.0.23.



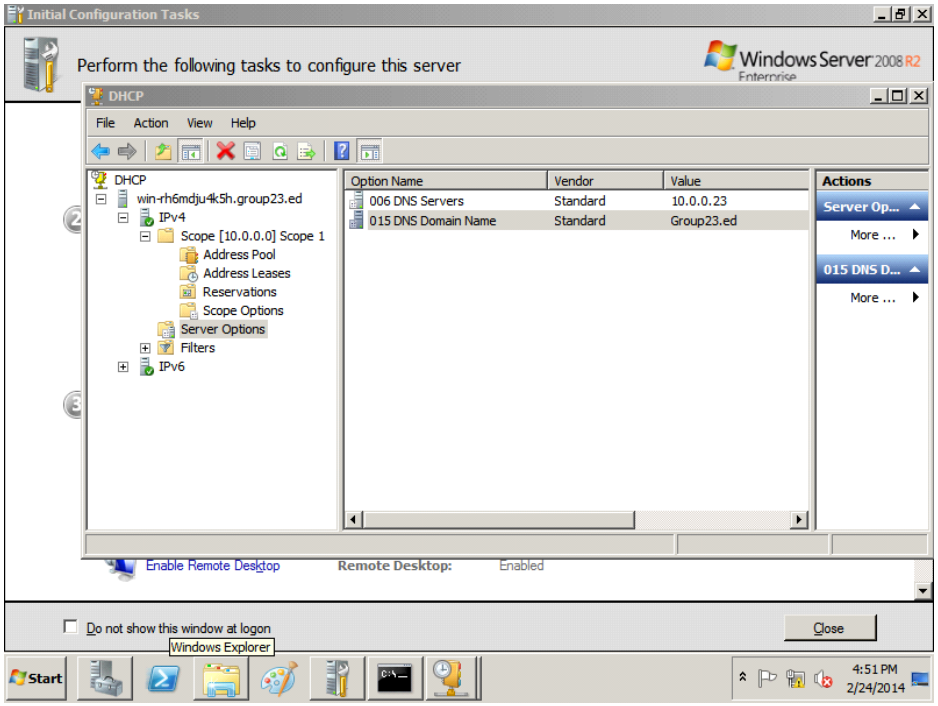
Next on Lab #7, I excluded the IP address 10.0.0.25 from the DHCP Scope. This allows to be able to reserve this static IP address for existing server in the middle of the range of IP addresses to be used for DHCP scope. Click Next.



Complete steps 9 through 14, configuring options – specify the default gateway used by clients – Add



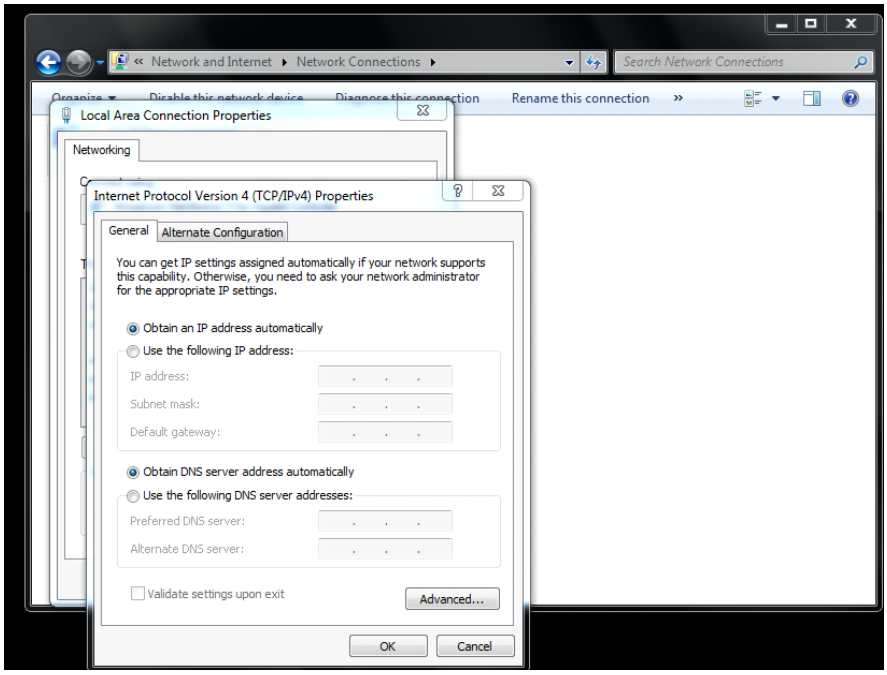
Clients can now use the server as their DNS server. In server1 group23.ed icon is a whit circle with a red arrow in the center, right click IPv4 in the left pane, and select Authorize from the

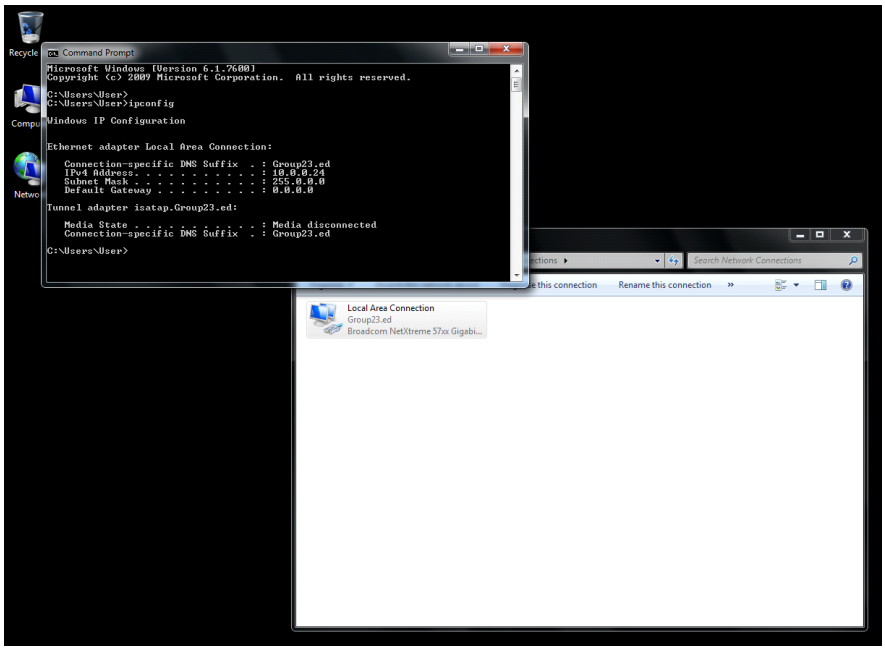


shortcut menu.

Log onto the workstation – Start –Control Panel – Network and Internet – Network Sharing – right click Network – Properties –Change Adapter Settings – Right click Local Area Connection

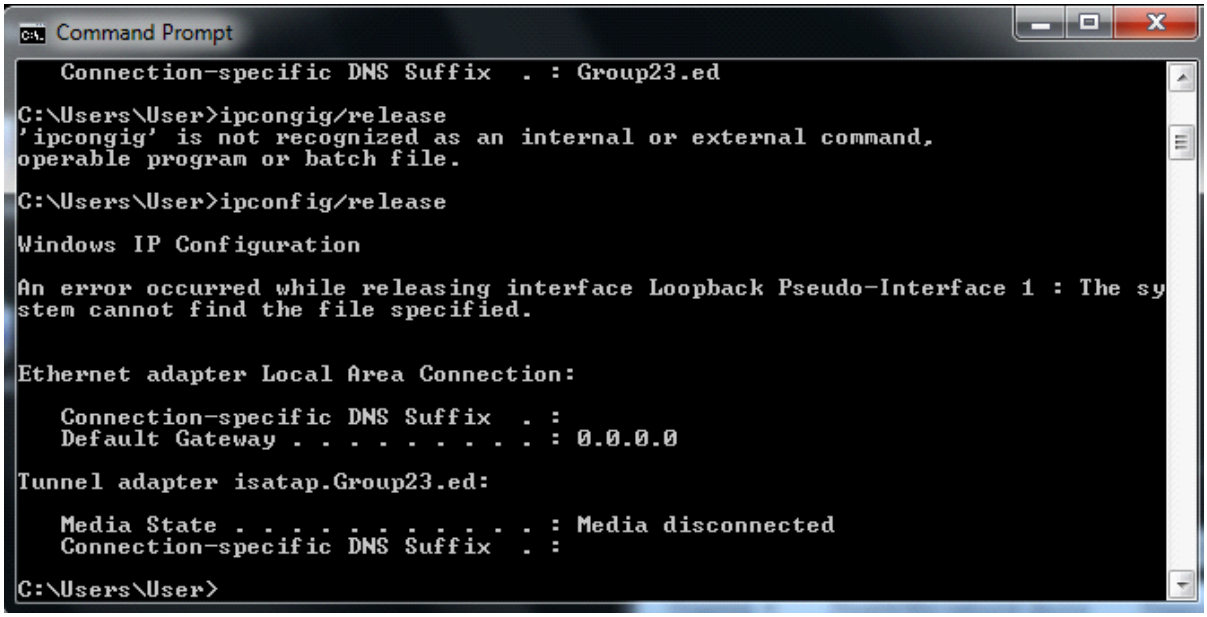
– Properties – Internet Protocol Version 4 – Internet Protocol – Obtain IP address automatically – Obtain DNS server automatically - OK





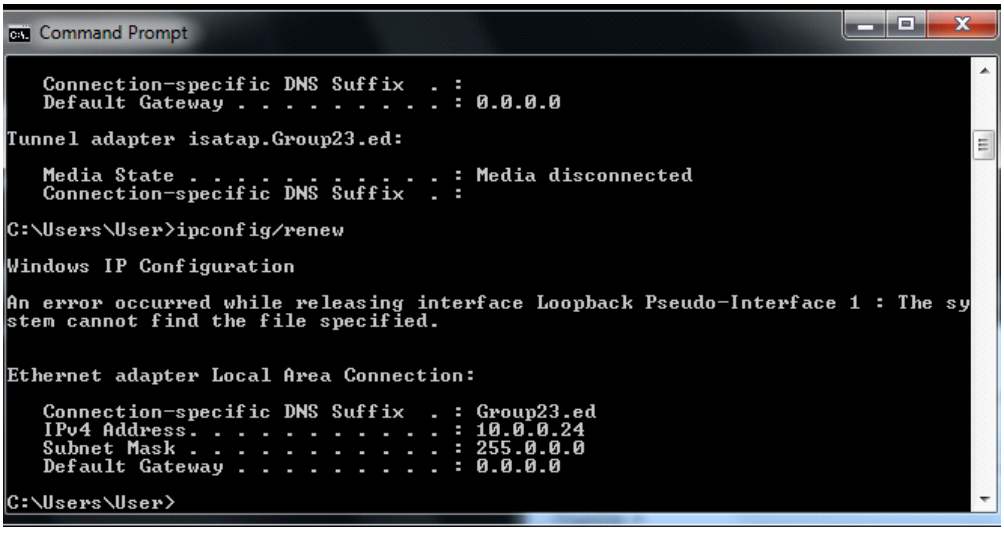
Command Prompt – ipconfig – new IP address is 10.0.0.24 (above)

Type ipconfig/release - Enter



The computer releases any current address assigned by DHCP

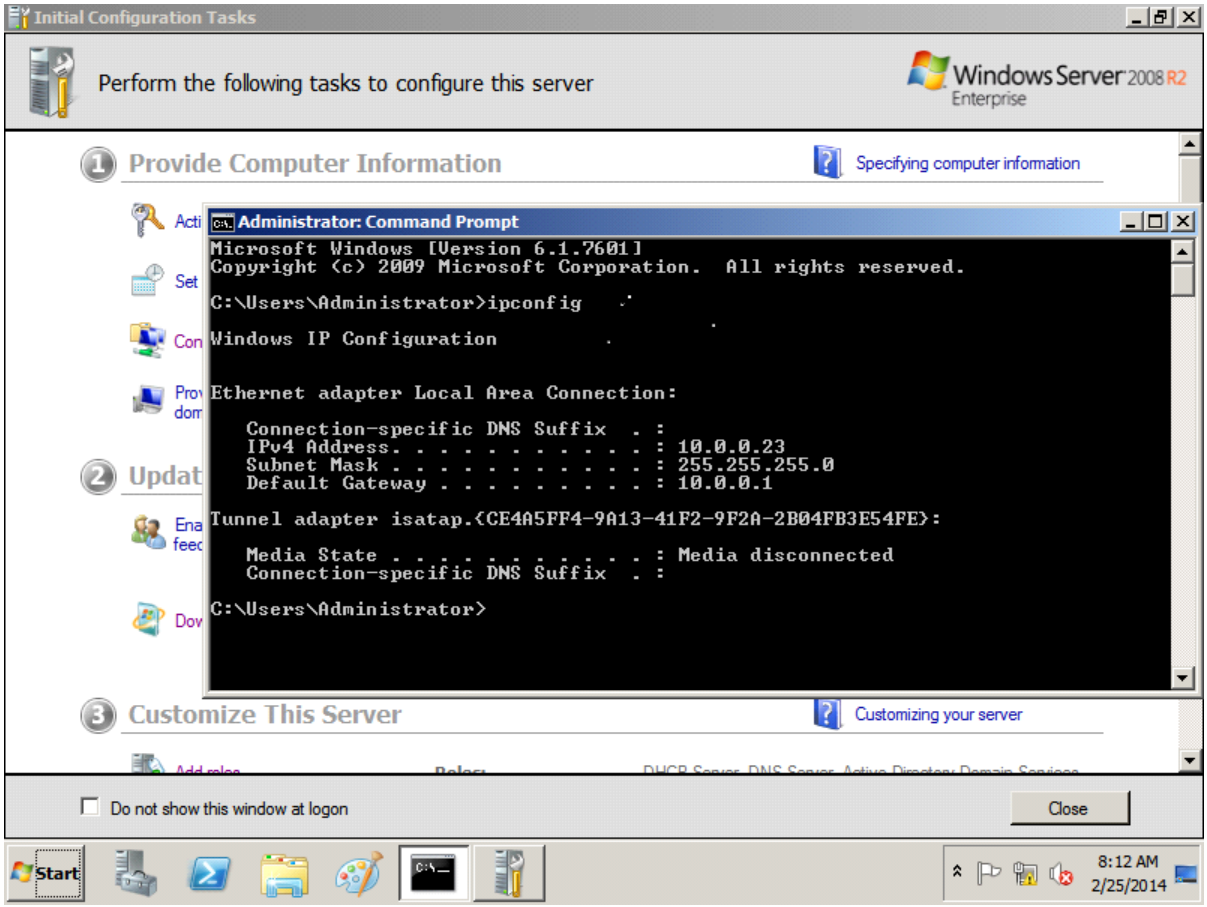
The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used by servers on an IP network to allocate IP addresses to computers. The purpose of DHCP is to automate the IP address configuration of a computer without a network administrator. IP addresses are typically selected from a range of assigned IP addresses stored in a database on the server and issued to a computer which requests a new IP address. An IP address is assigned to a on computer for a set interval, after which, the computer must renew the IP address or acquire a new one



I then typed in ipconfig/renew and my previous IP address was given. (above) 10.0.0.24 – Type ipconfig/all

I then typed ipconfig/all. The computer prints the new IP address and subnet mask for the computer.

Connect Server to switch – type ipconfig in command promp – IP of DHCP is given.



WINS is a naming service used to register and resolve name-to-address mappings for NetBIOS clients on TCP/IP-based networks.Because NetBIOS naming is a required feature for networking that is supported in all previous versions of Windows, install and use WINS if you are operating the Windows 2000 DHCP service in a network environment that includes DHCP clients running under any of the following earlier Microsoft operating systems:

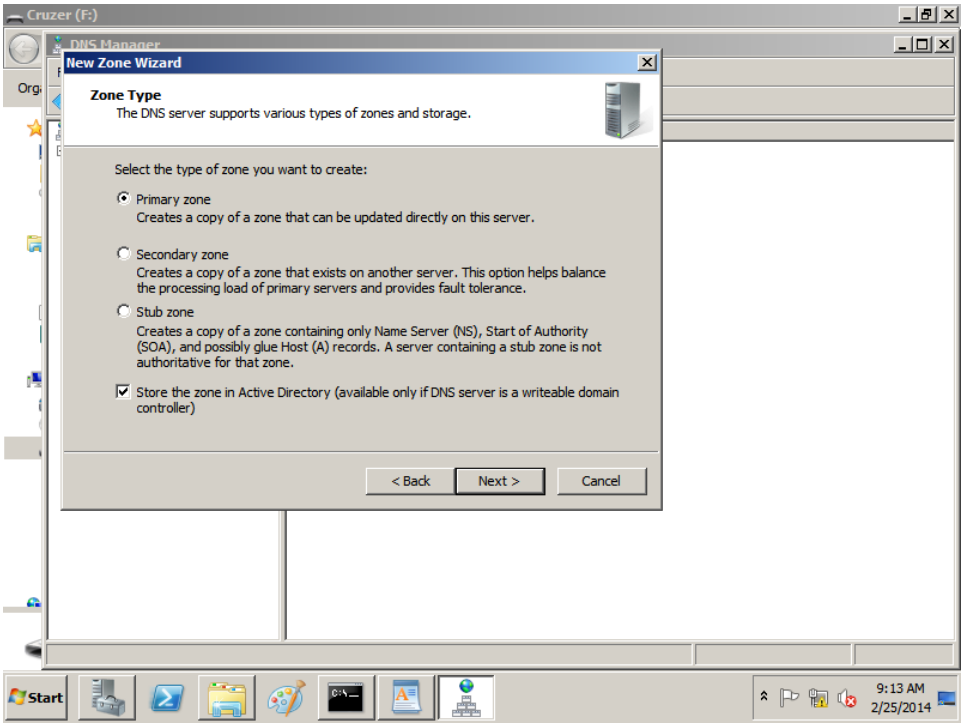
APIPA: A feature of Microsoft Windows, APIPA is a DHCP failover mechanism for local networks. With APIPA, DHCP clients can obtain IP addresses when DHCP servers are non-functional. APIPA exists in all modern versions of Windows except Windows NT.

When a DHCP server fails, APIPA allocates IP addresses in the private range 169.254.0.1 to 169.254.255.254. Clients verify their address is unique on the network using ARP. When the DHCP server is again able to service requests, clients update their addresses automatically.

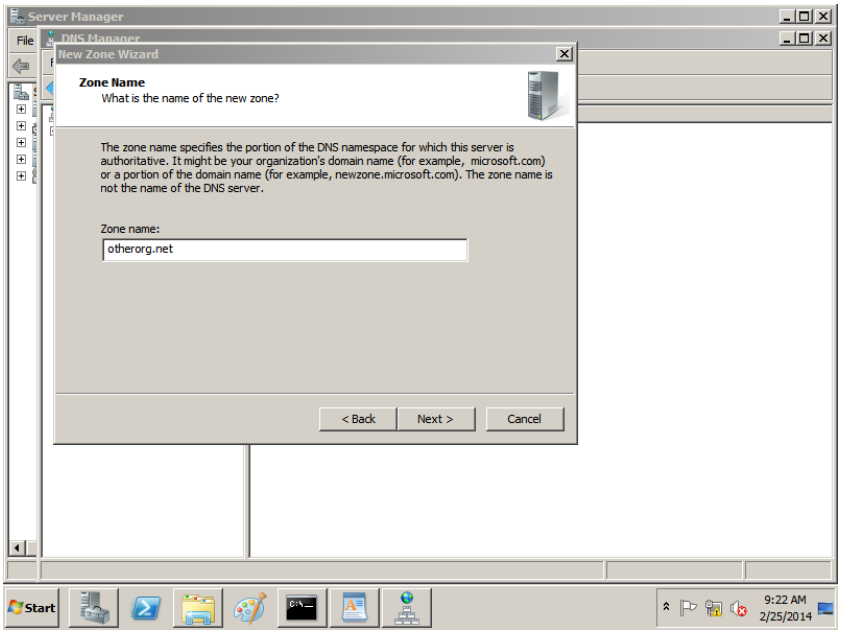
In APIPA, all devices use the default network mask 255.255.0.0 and all reside on the same subnet.

Lab 4.3 Configuring Domain Name System (DNS) Properties

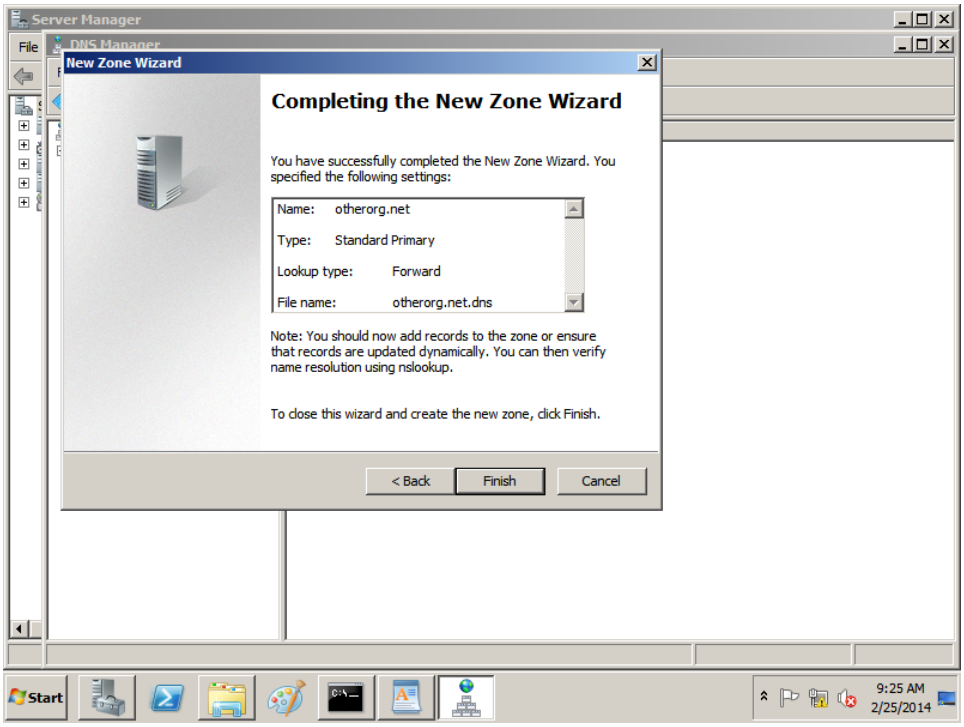
On Server - Start -Administrator Tools, then click DNS. The DNS Manger opens – plus sign (+) right click the name of the server – click New Zone. The New Zone Wizard opens. Next –



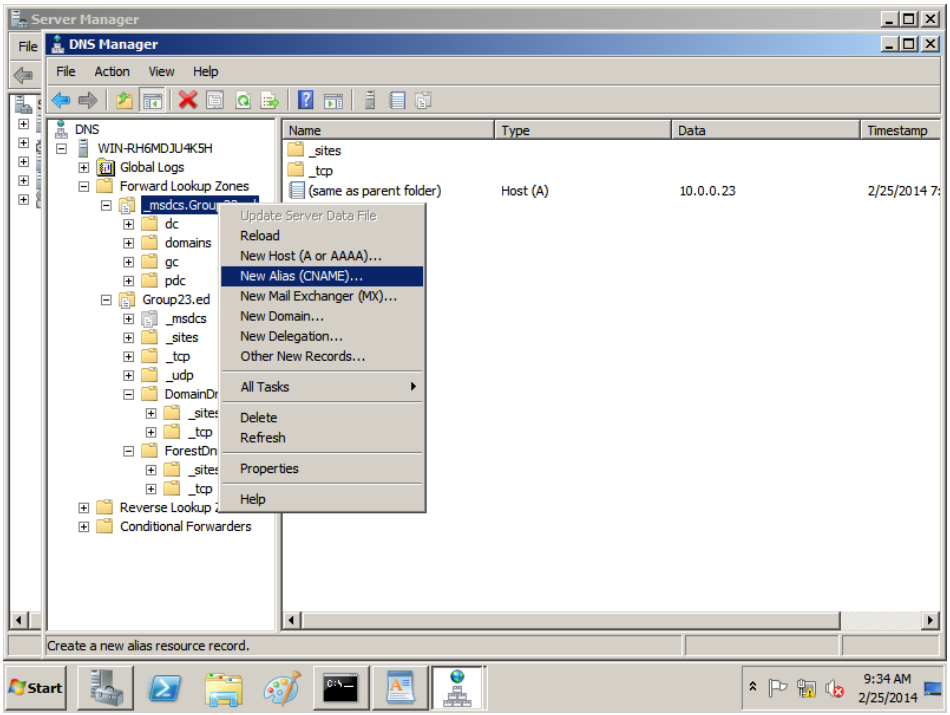
Primary Zone - Next



In the Zone name box type otherorg.net – Next – click Finish

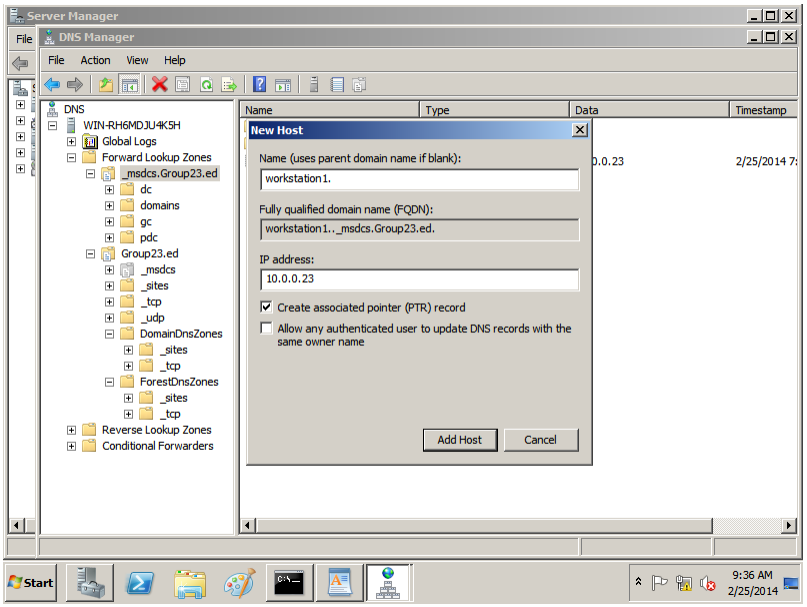


In the left pane of the DNS Manager window click the plus sign (+) next to the Forward Lookup Zones folder. The tree expands, - click the other.net folder to select it. Right click the folder and click New Host (A orAAAA)

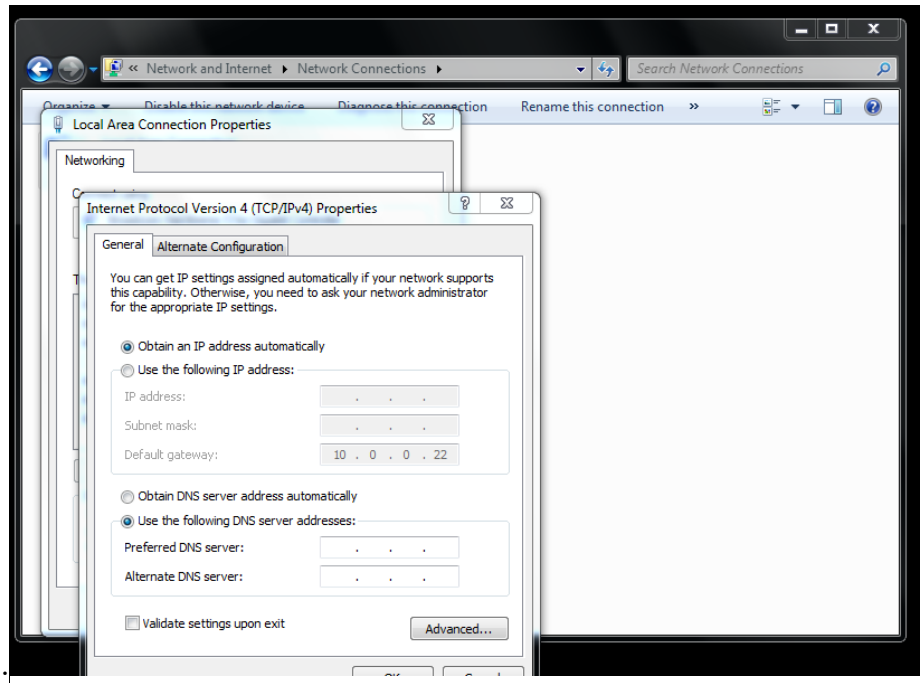


(NewAlias is highlighted, though for the Lab, A or AAAA was chosen).

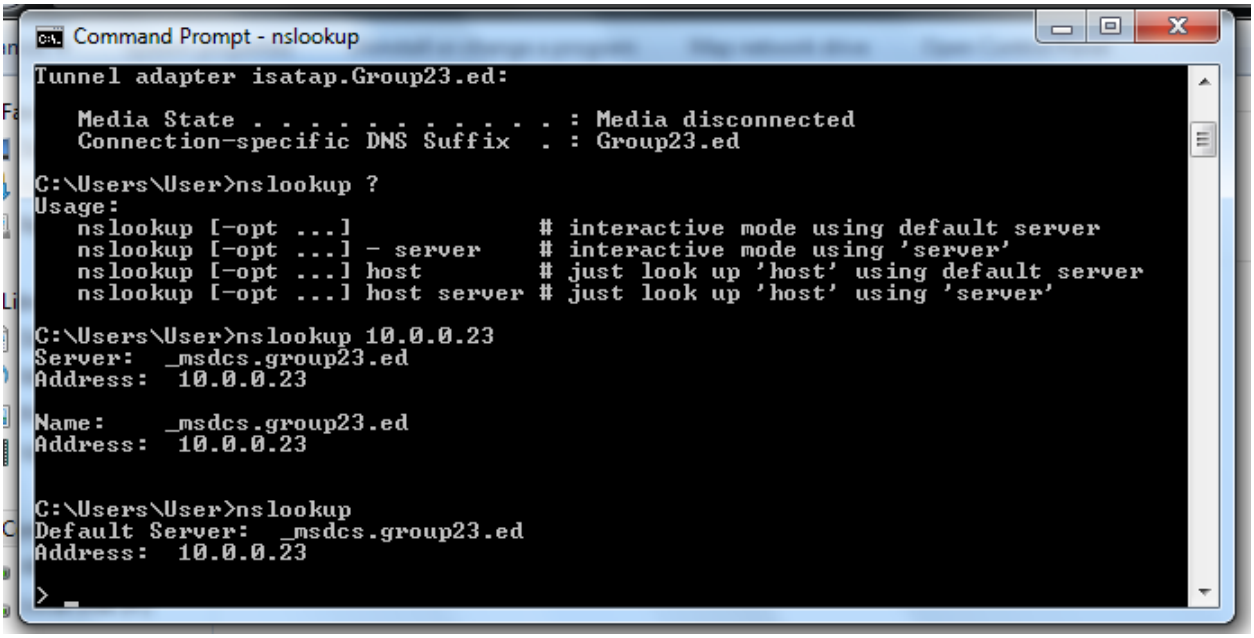
Add name and IP address – Click Add Host – after creation, click OK.



Repeat steps 12 through 15 for workstation 2. – Log onto workstation 1- Start – Control Panel – Network and Internet – Network Sharing Center – Change Adapter Settings – The Network Connections window opens. Right click Local Area Connection – Properties – double click Internet Protocol Version 4 (TCP/IP4) – dialogue box opens – Type DNS IP number 10.0.0.23 – OK – Close.

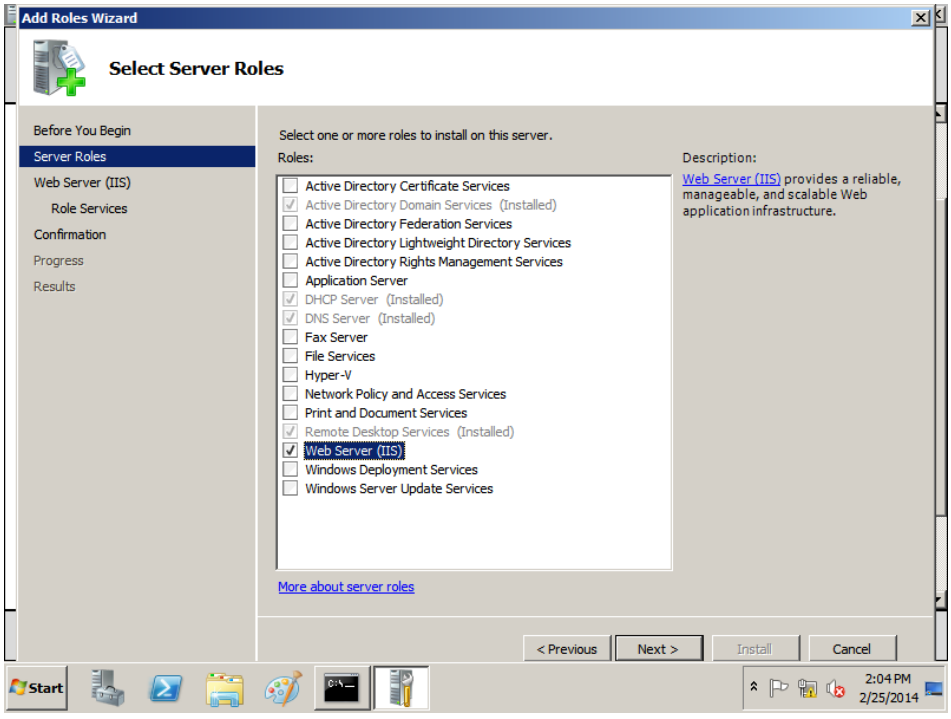


In the Command Prompt type – nslookup msdcs.group23.ed – Enter – The computer displays its IP address as well as the IP address of the Server answering the request. –Ping – Log off.

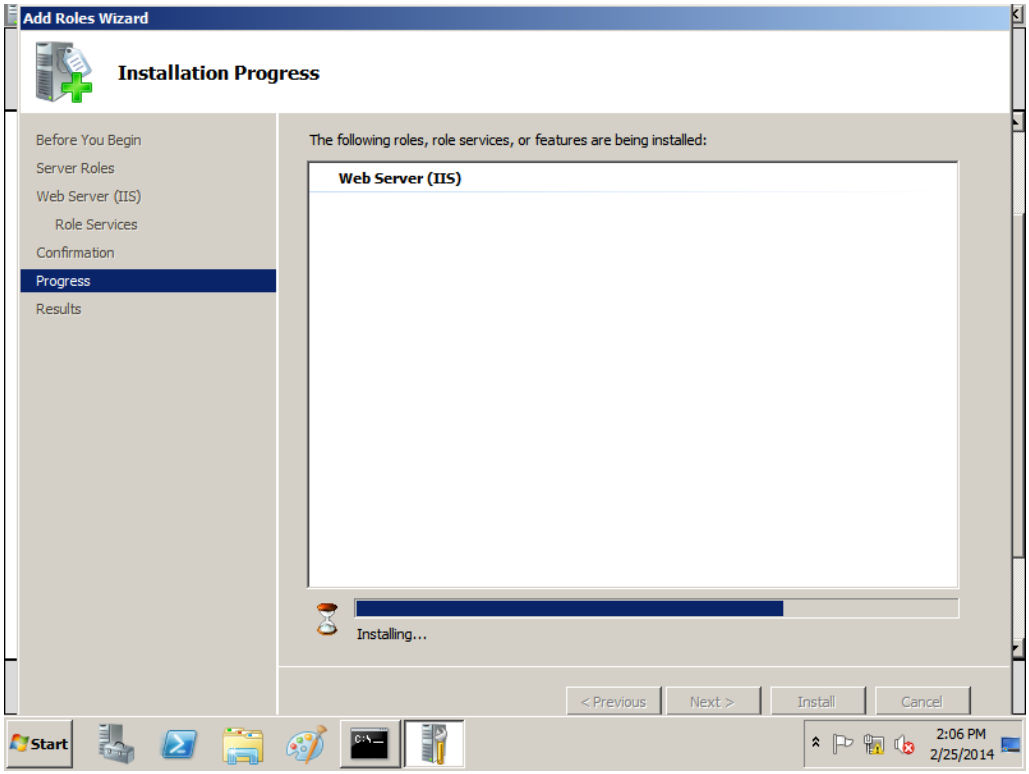


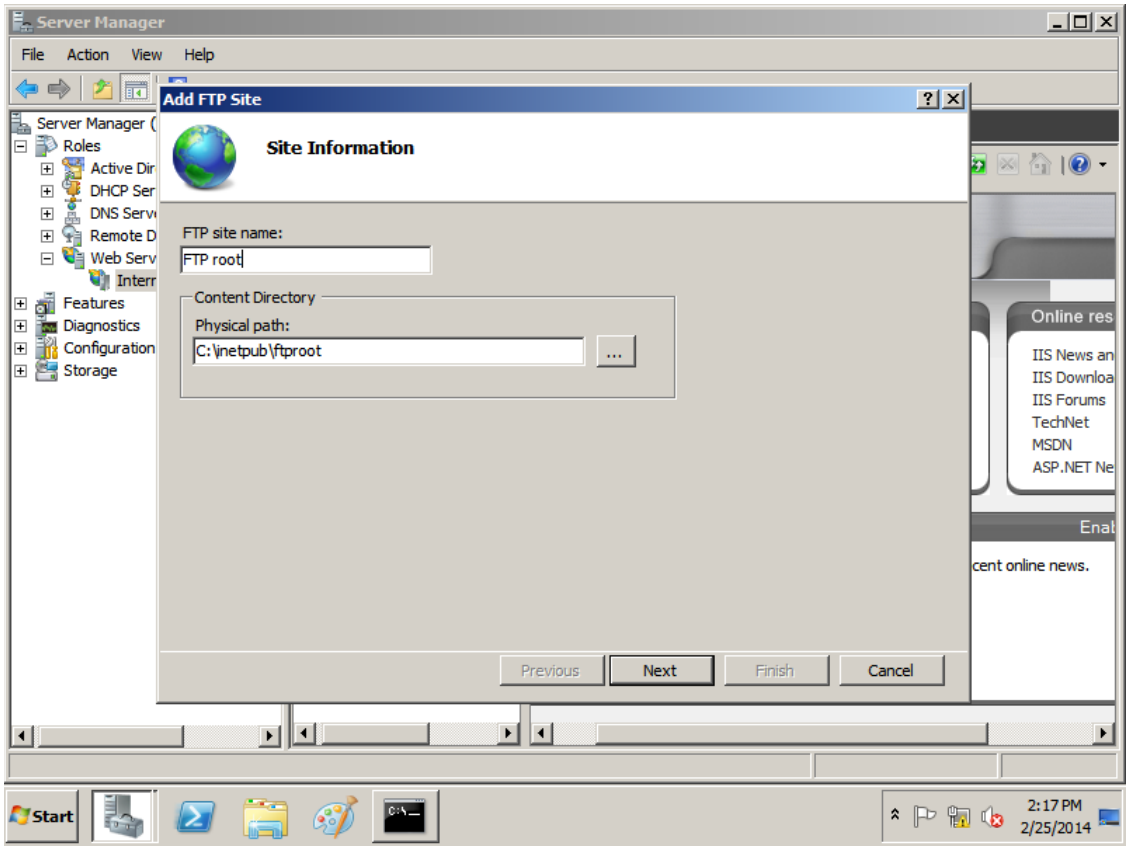
Lab 4.4 Using FTP

Install File Transfer Protocol (FTP) on Server – Add Role Wizard – Select Server Roles – click Web Server (IIS) – Next

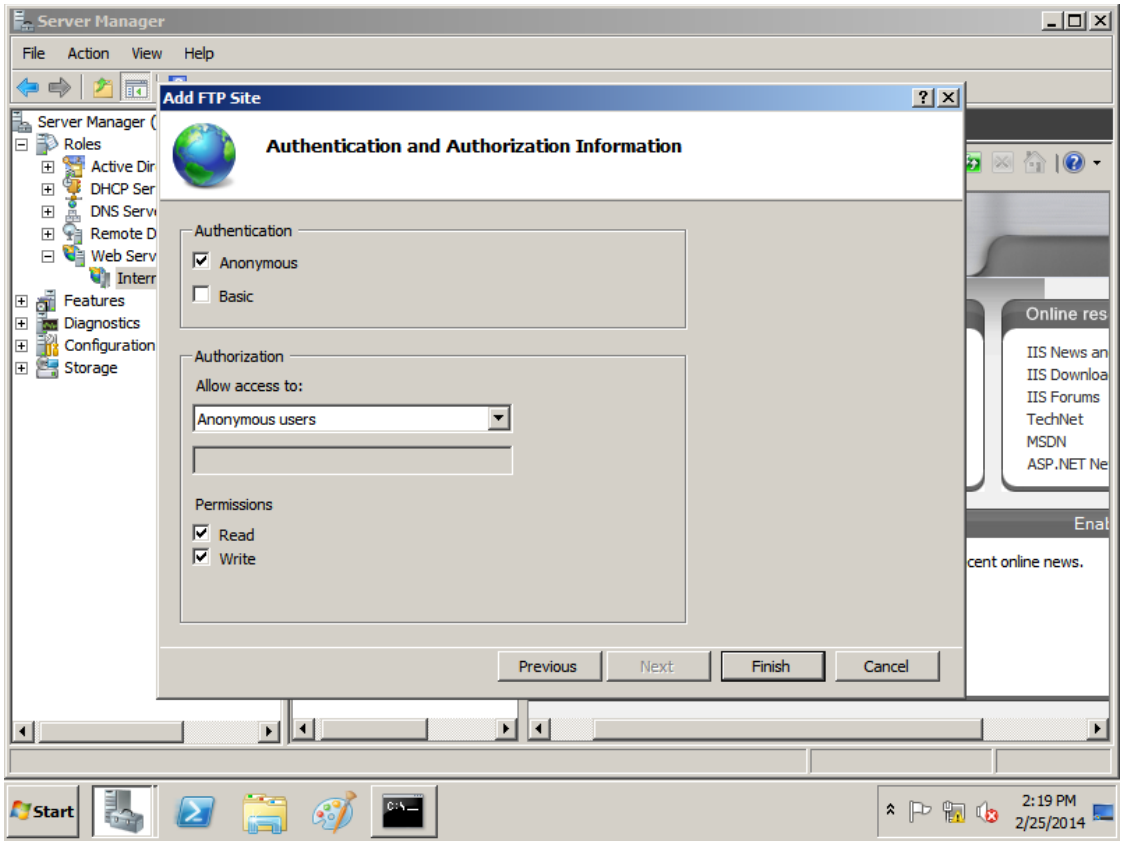


Installing / configuring

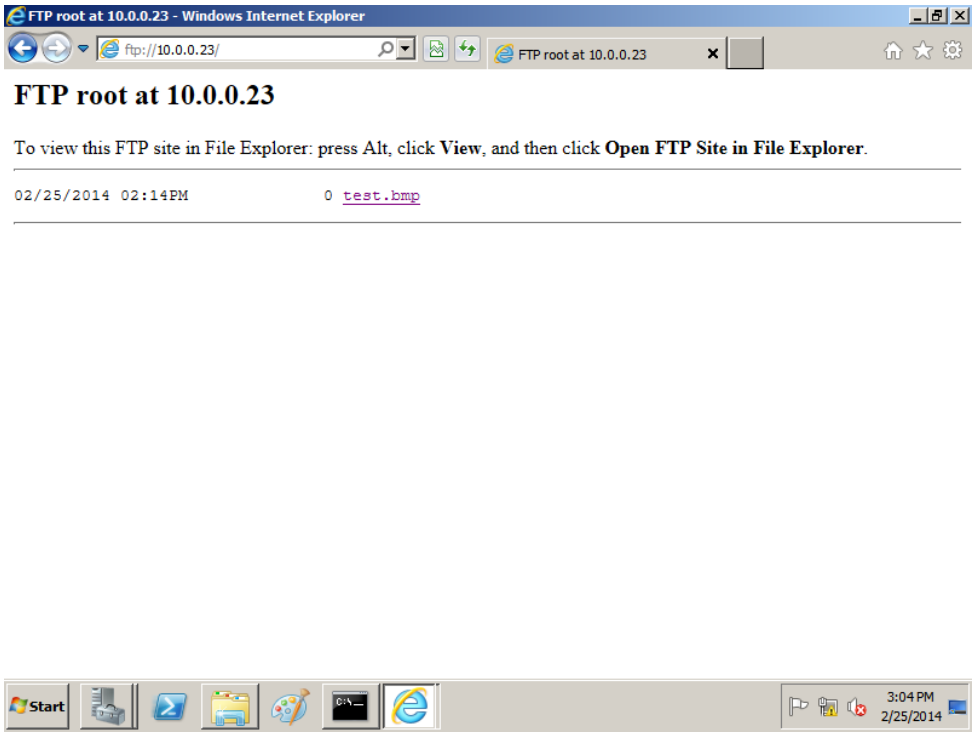




Add FTP Site – FTP site name: FTP root Content Directory – Physical Path: C:\inetpub\ftproot

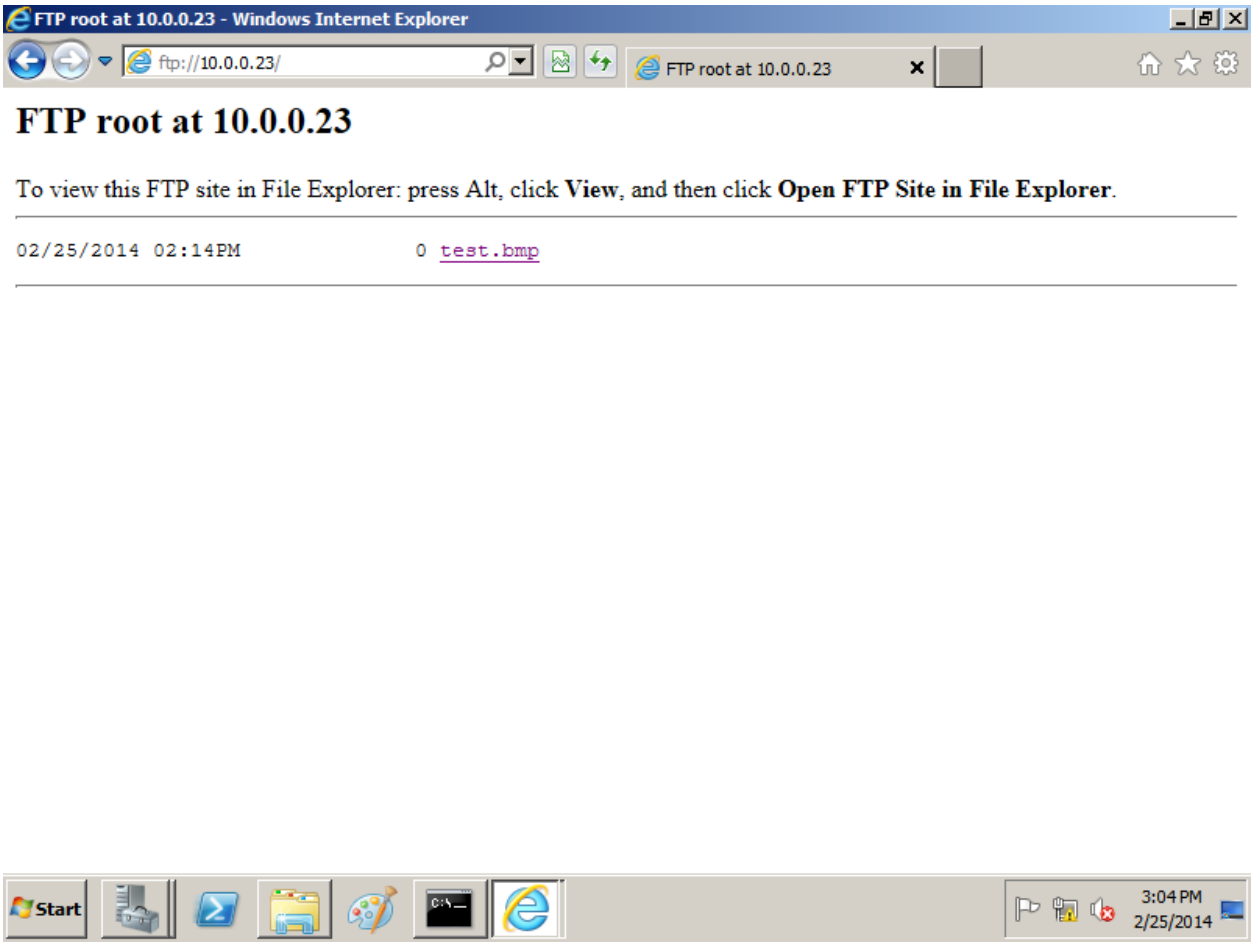


Authentication – Anonymous Allow access to: Anonymous users w/ read / write permissions.



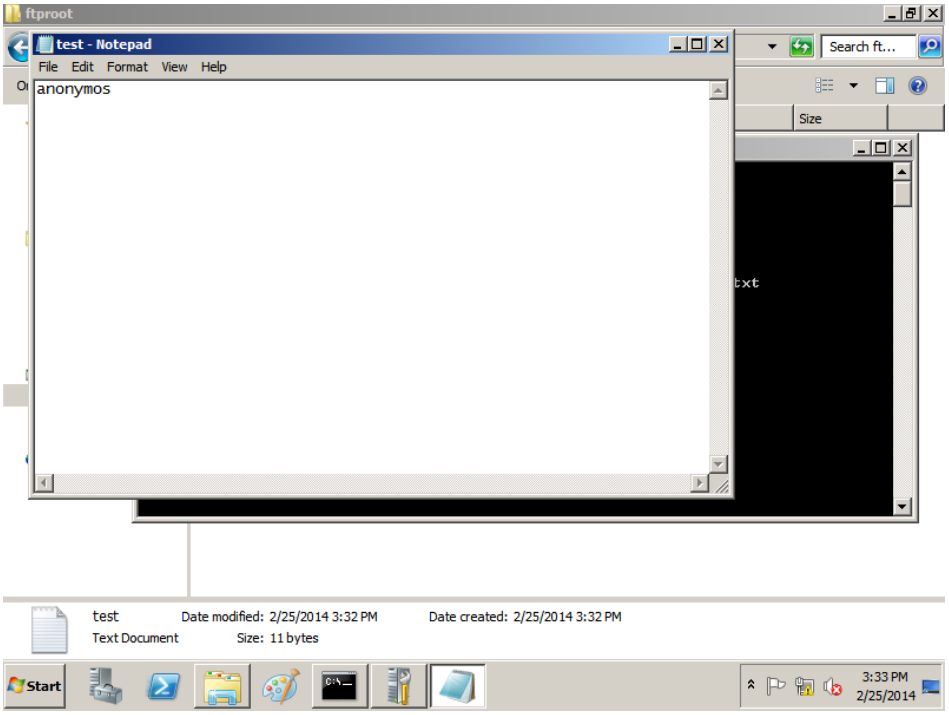
On Server got to Internet Explorer – ftp//10.0.0.23/ - Enter – Opens anonymous file (above)

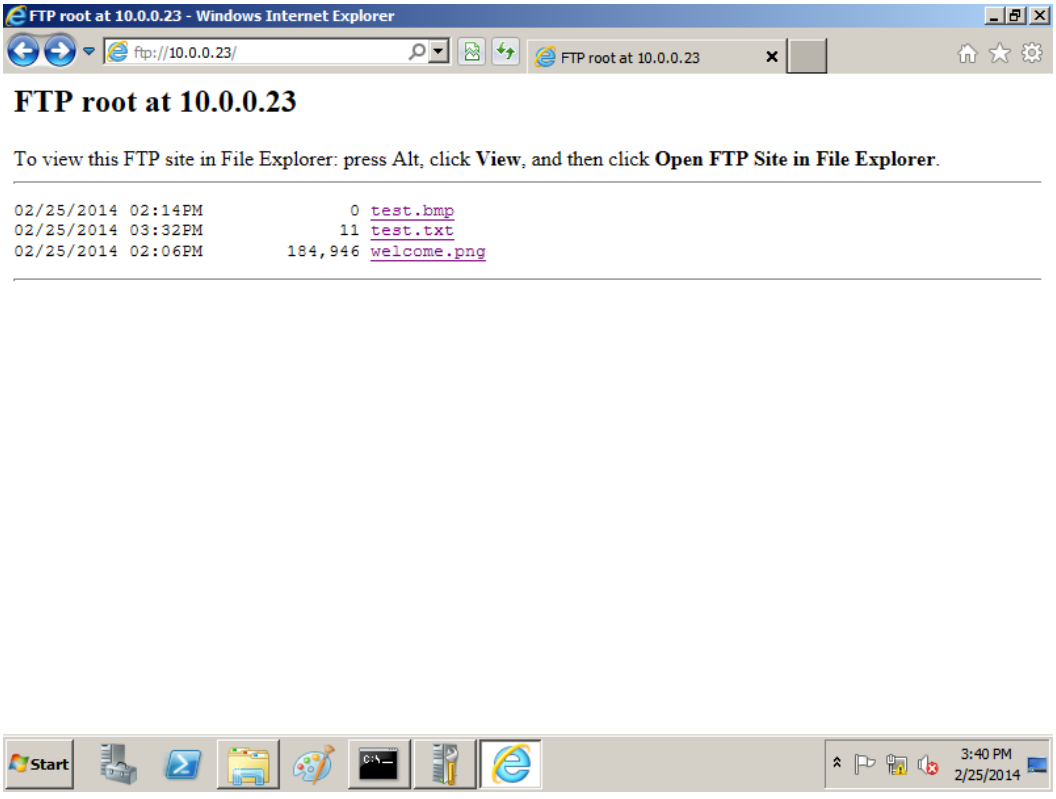
Activity: Log on to Server – Start – Command prompt – **type echo Joe > C:\Inetpub\ftproot\test.txt** – Enter. This creates a file named test in the **C:\Inetpub\ftproot directory.** At the command prompt, type copy **C:\Inetpub\wwwroot\welcome.png C:\Inetpub\ftproot –** Enter. The computer copies the file from one directory to another. The image file is now available on the FTP site configured on the computer.

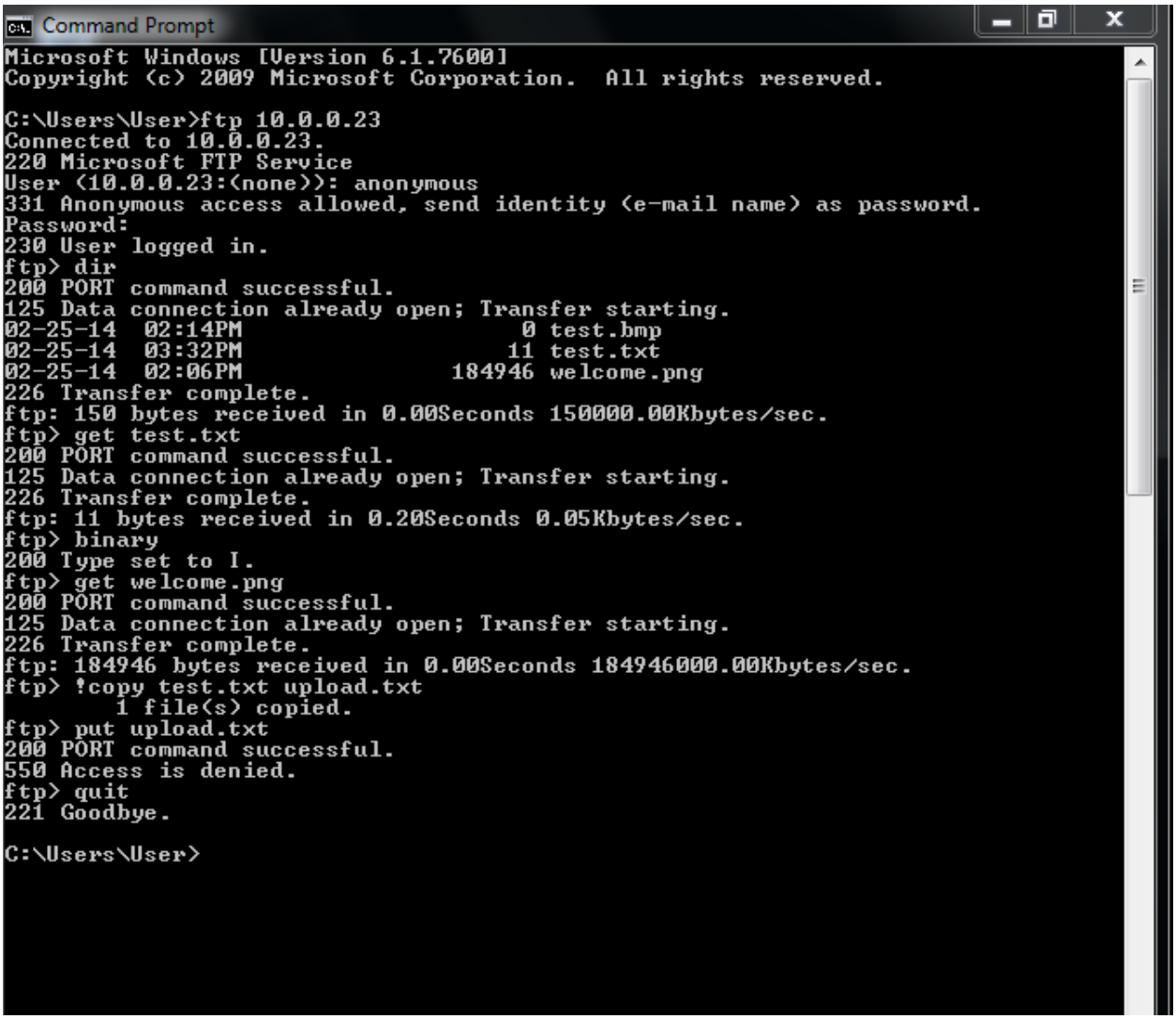


Log onto workstation – Start – cmd – ftp 10.0.0.23 Enter. You have connected and the remote computer is running in the Microsoft FTP service.

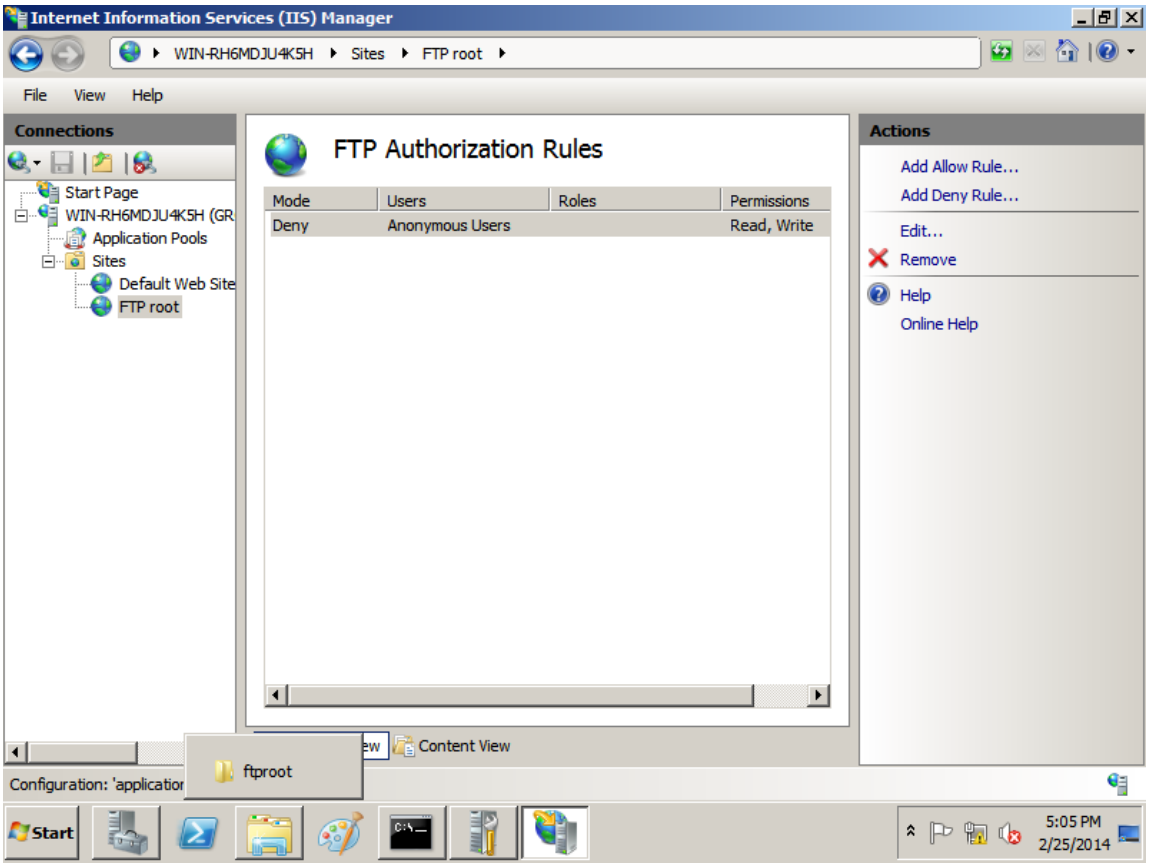
Below is the following steps on Lab: 7, 8, 9, 10, 11, 12, 13, 14, 15, and 16.


ftproot
test - Notepad
File Edit Format View Help
anonymos
Search ft...
Size
test
Date modified: 2/25/2014 3:32 PM
Date created: 2/25/2014 3:32 PM
Text Document
Size: 11 bytes
Start
3:33 PM
2/25/2014

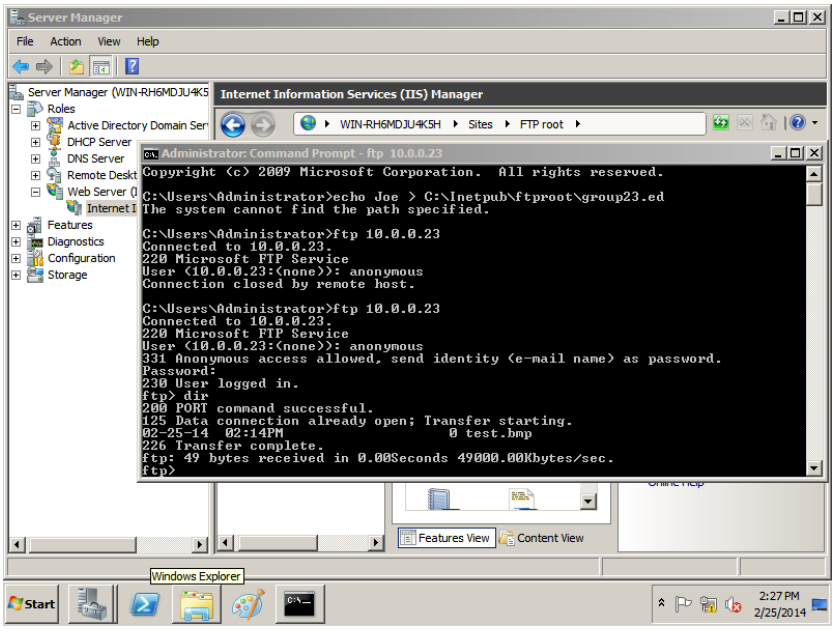

FTP root at 10.0.0.23 - Windows Internet Explorer
ftp://10.0.0.23/
FTP root at 10.0.0.23
FTP root at 10.0.0.23
To view this FTP site in File Explorer: press Alt, click View, and then click Open FTP Site in File Explorer.
02/25/2014 02:14PM 0 test.bmp
02/25/2014 03:32PM 11 test.txt
02/25/2014 02:06PM 184,946 welcome.png
Start
3:40 PM
2/25/2014

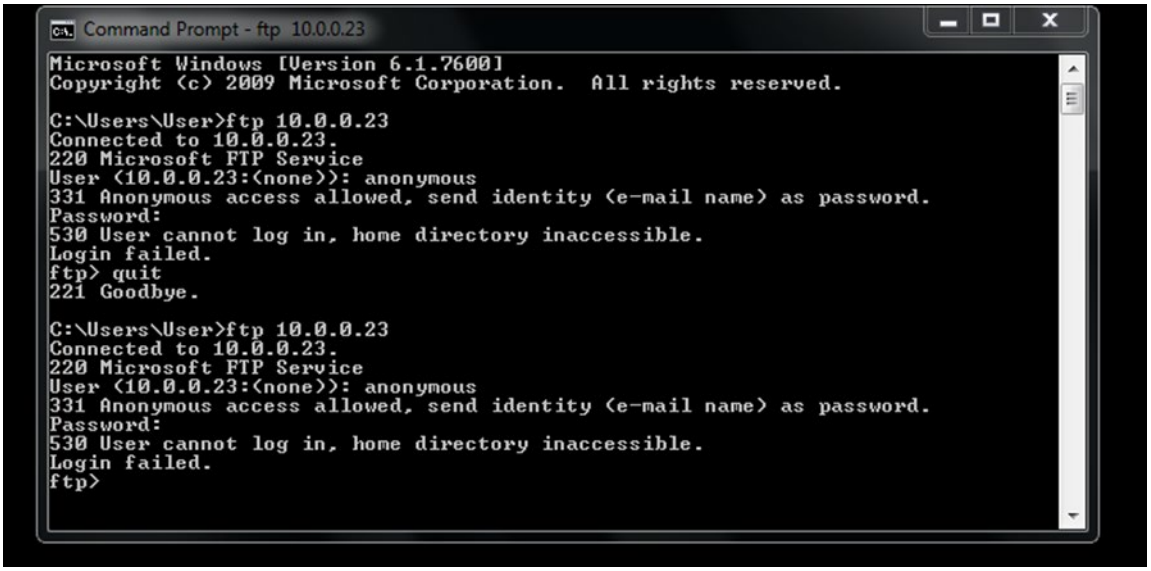


Server 1: Start – Administrative Tools – Internet Information Services (IIS) Manager. The Internet information window opens. Click Local Host icon in the left pane. – double click FTP sites icon in the right pane. An icon for Default FTP sit appears. Right click Default FTP Site and click properties

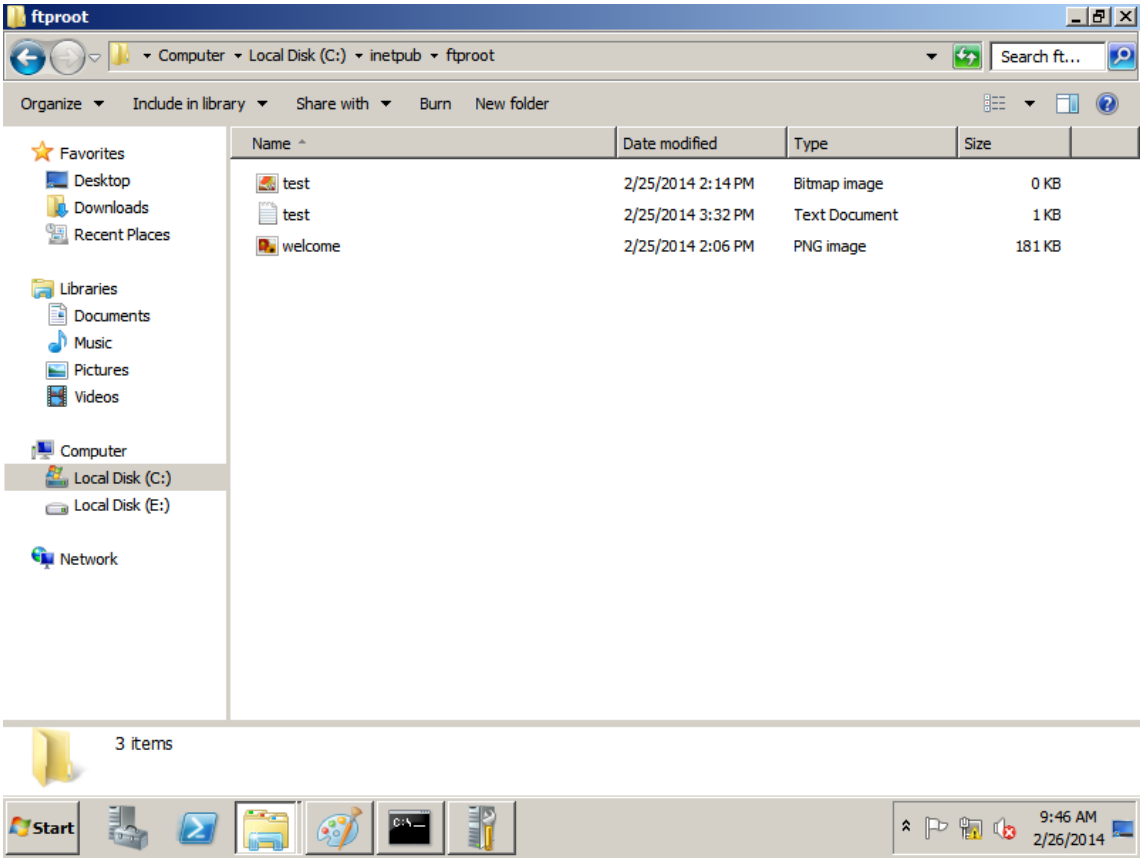


(Above) Click Security Accounts tab. Uncheck the Allow anonymous connections check box. The IIS Manager dialogue box opens. Click Yes – click Home Directory – Select Writ check box. At this point, you are ready to up load files. Click OK. Right click Server in the left pane – All Tabs – Restart IIS





In the cmd Type ftp 10.0.0.23 – Enter. Type anonymous – Enter. Type password – Enter. The ftp> prompt indicates that user anonymous cannot log on and that the logon failed. Type Quit – **Enter. Type put upload.txt – Enter**

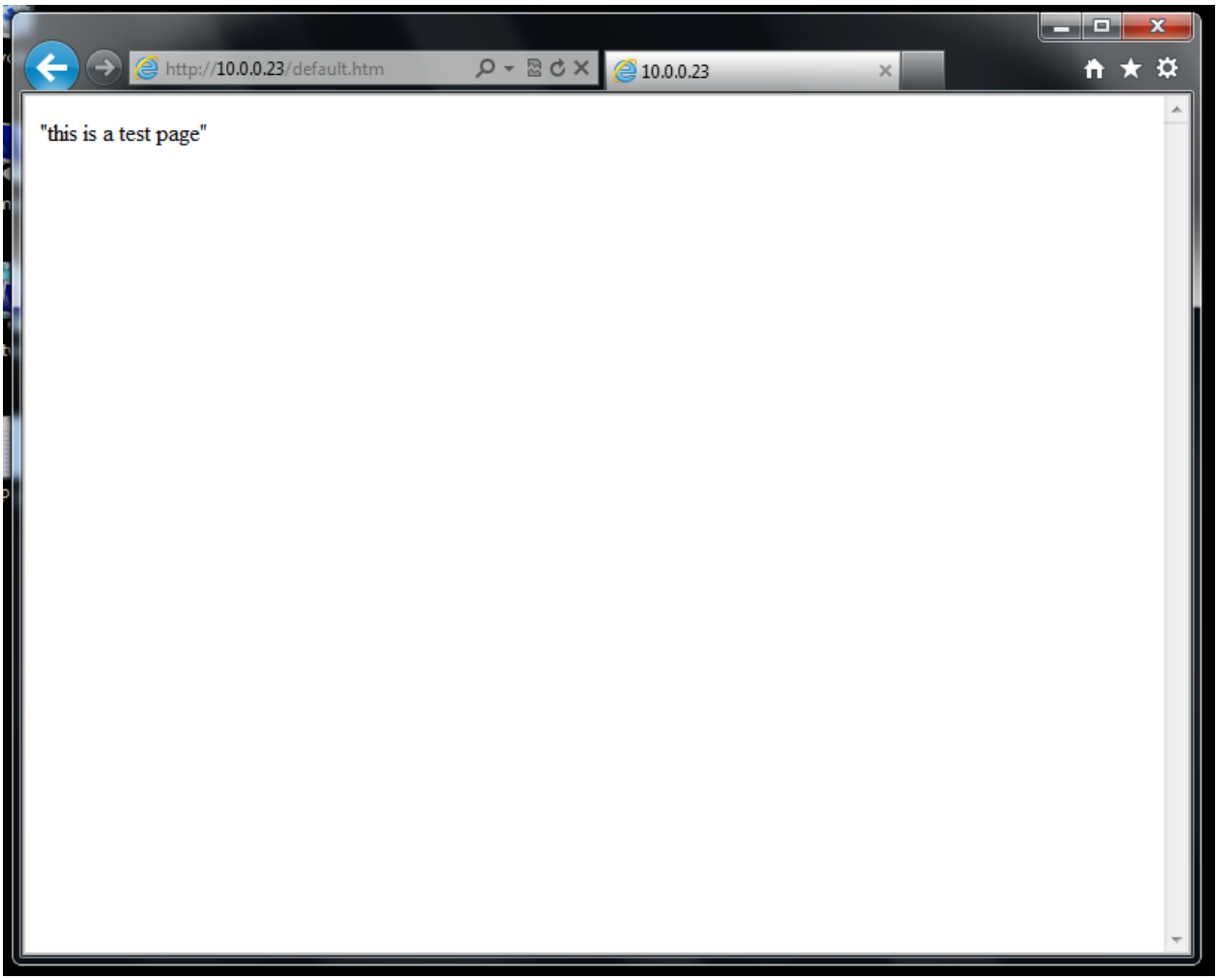


Double – click the Local Disk (C:) – double-click the **Inetpub** folder, double-click **ftproot** folder. Log off

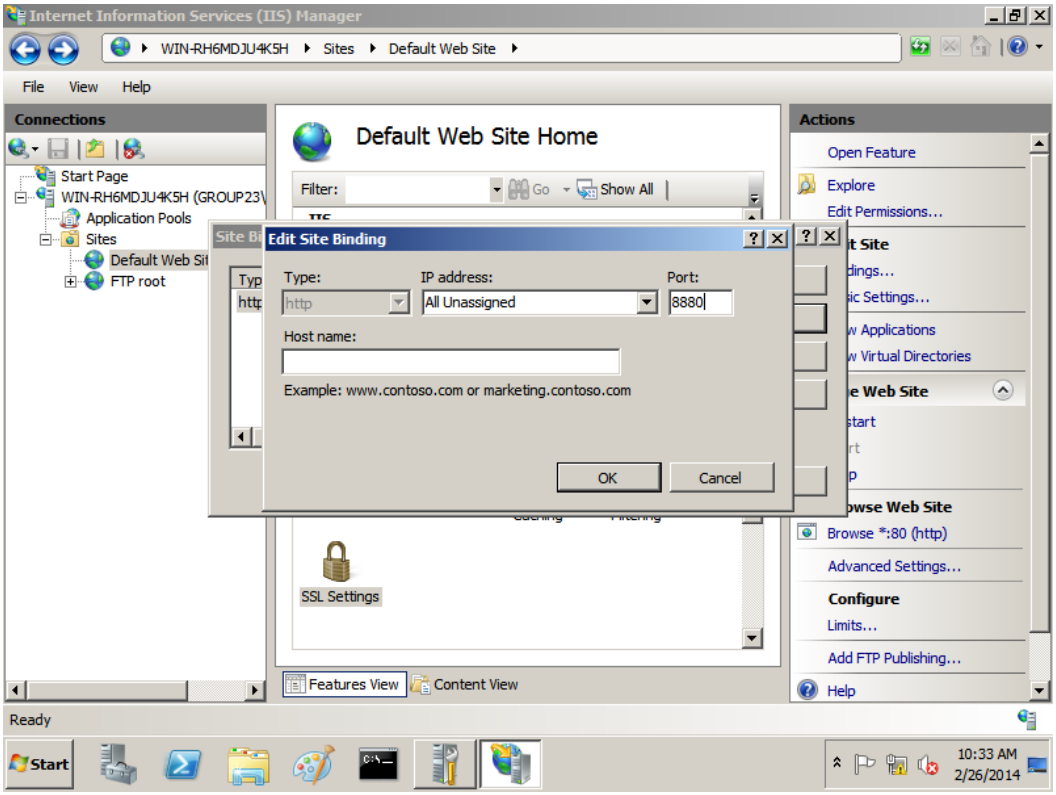
Lab 4.5 Understanding Port Numbers

On the Server create a folder named **default.htm** containing the text “This is test page” in location **C:\Inetpub\wwwroot**

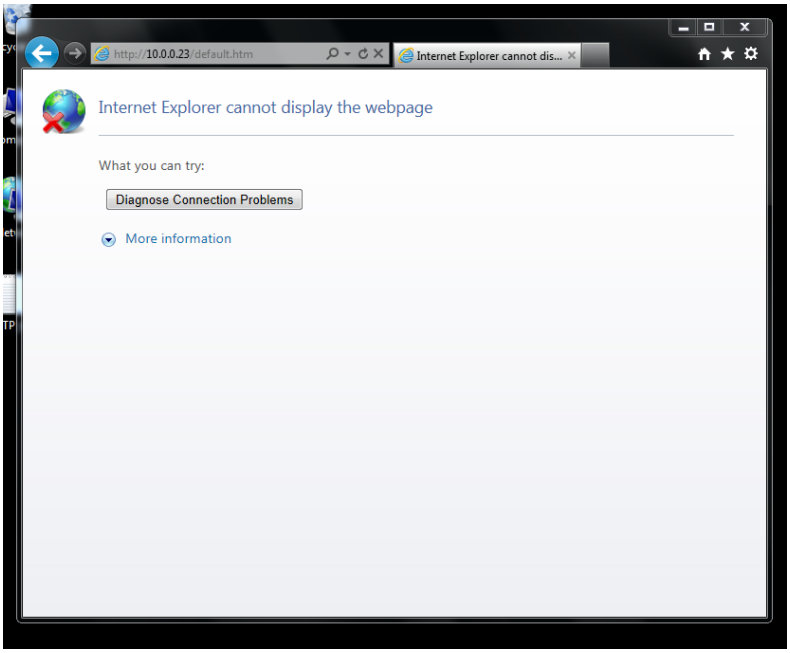
Log on to workstation – open windows explorer – In the address bar type http://10.0.0.23 and press Enter. A web page opens containing the text “This is a test page”.



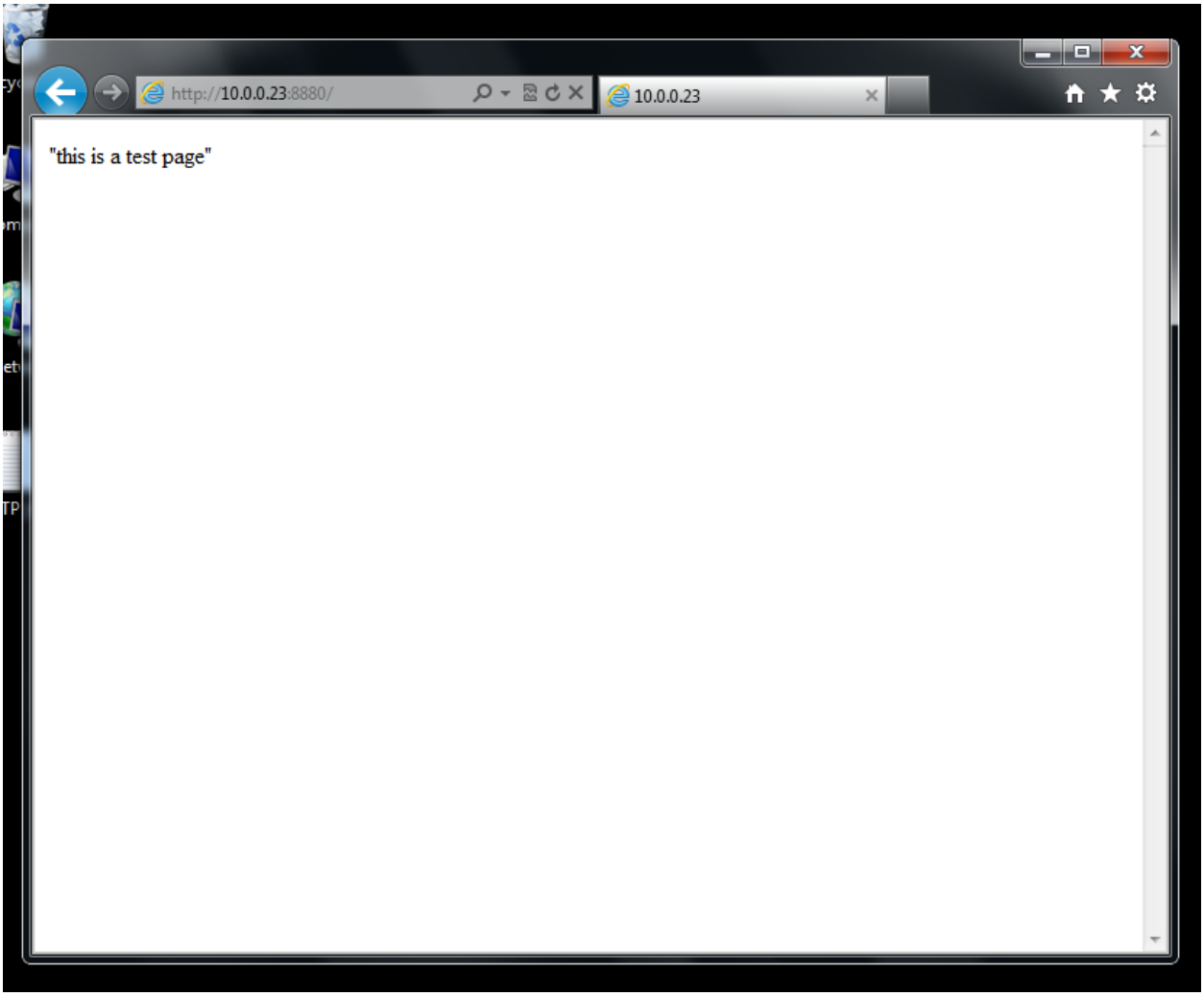
Server, Start – Administrator Tools – Internet Information Services (IIS) The Internet Information services Manager window opens. In the left pane click (Group23\Administrator) icon. Double click default web sites icon. Click Edit Site –Bindings – highlight 80 to 8880 http port -



Click OK. Under Manage Website - click Restart – ExitOn workstation close Internet Explorer, (this ensures the Internet Explorer doesn't use its cache to open the web page that you want to open). Start – All Programs – Internet Explorer – In the address bar type **http:// 10.0.0.23** – Enter, an error message appears indicating that the page cannot be displayed.



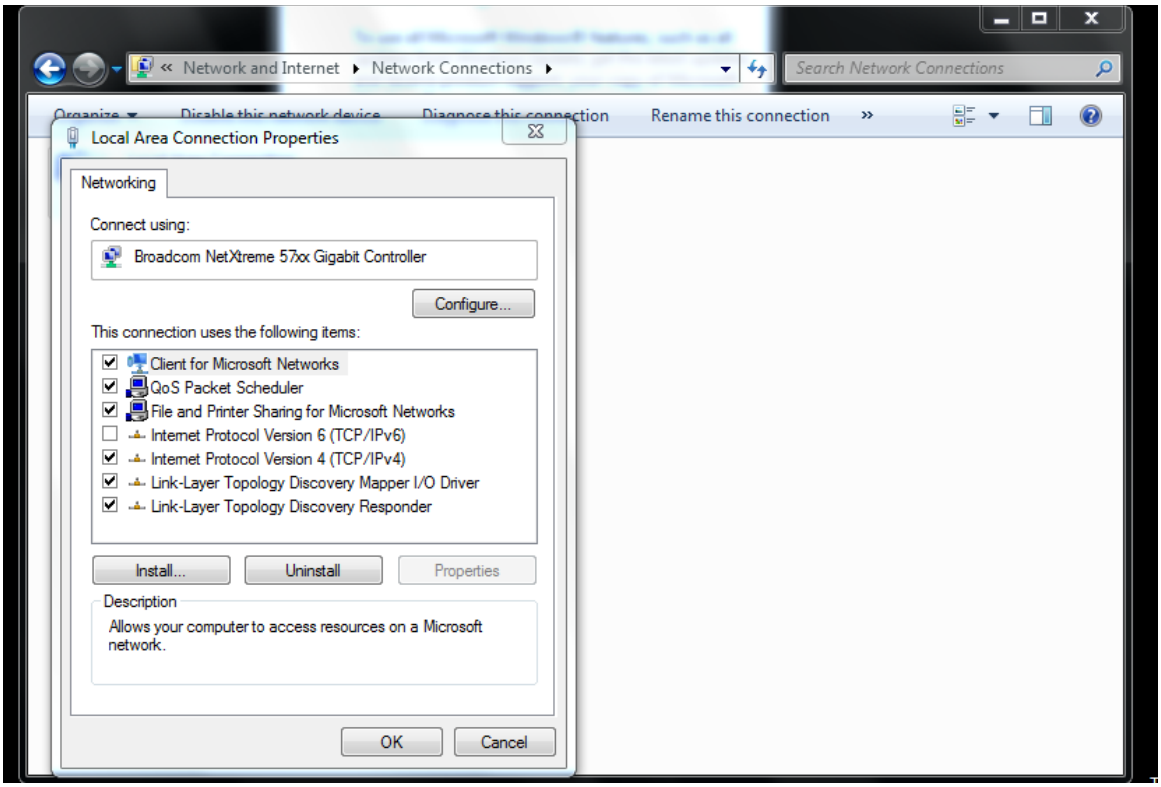
Next: In the address bar type **http:// 10.0.0.23:8880** – Enter. A web page displays the text “This is a test page”.



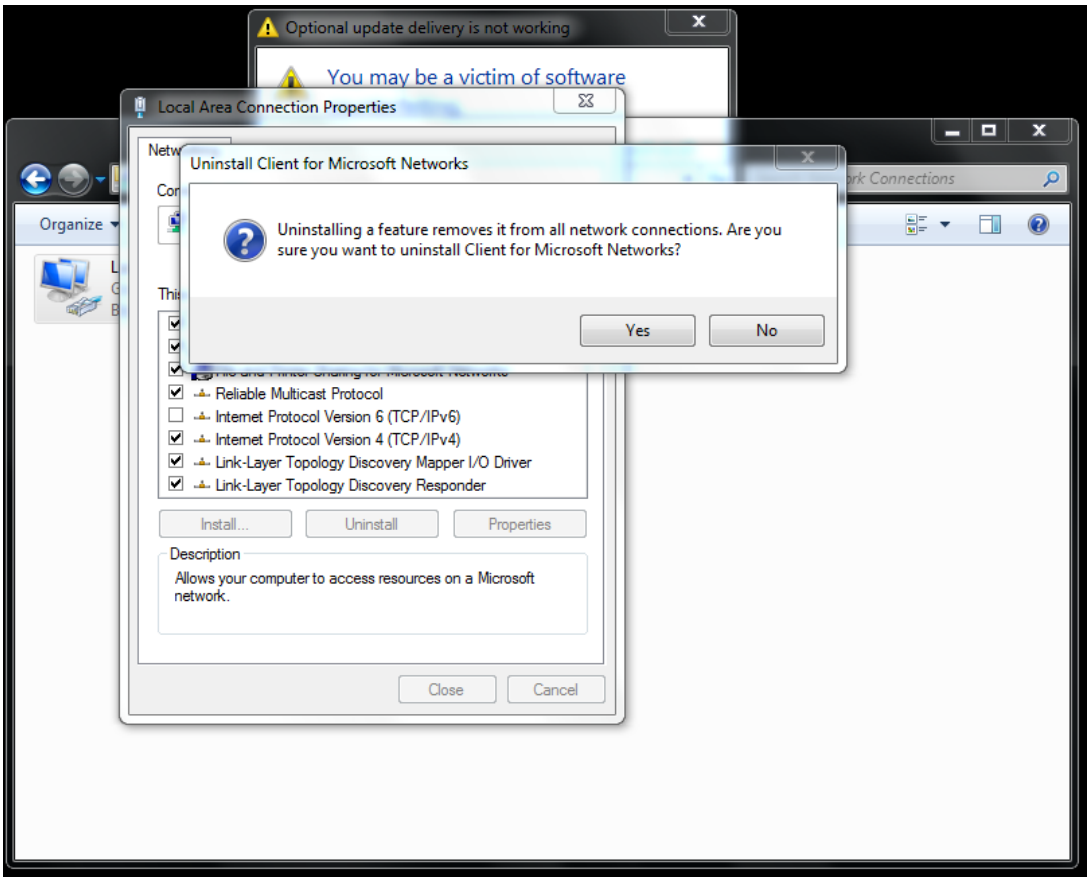
Log off both computers.

Lab 4.6 Disabling Unnecessary Protocols

Log onto the workstation – Start – Control Panel – Network and Internet – Network Sharing Center – Change Adapter Settings. The Network Connections window opens. Right click Local Area Connection – Properties – Install – Protocol – Reliable Multicast Protocol.



After installation – Uninstall – Yes to remove the protocol



Reboot

Log on to Server: Start –Control Panel – Network and Internet – Network Sharing Center – Change Adapter Settings – double click Local Area Connection – Properties – (Repeat steps 4 through 7. You have successfully removed the Reliable Multicast Protocol from Windows Server 2008.

Lab 4.2 Questions

- 10.0.0.24 2. 8 days 3. Manual configuration, DHCP 4. Yes 5. B,C

6. D 7. C,D

Joseph Martinez

Networking I: Network +

CNG – 124

Chapter Five Labs

Topologies and Ethernet Standards

Lab 5.1 The Parallel Backbone

Lab 5.2 Building a Daisy Chain

Lab 5.3 Examining Ethernet Frames

Lab 5.4 Capturing Network Data

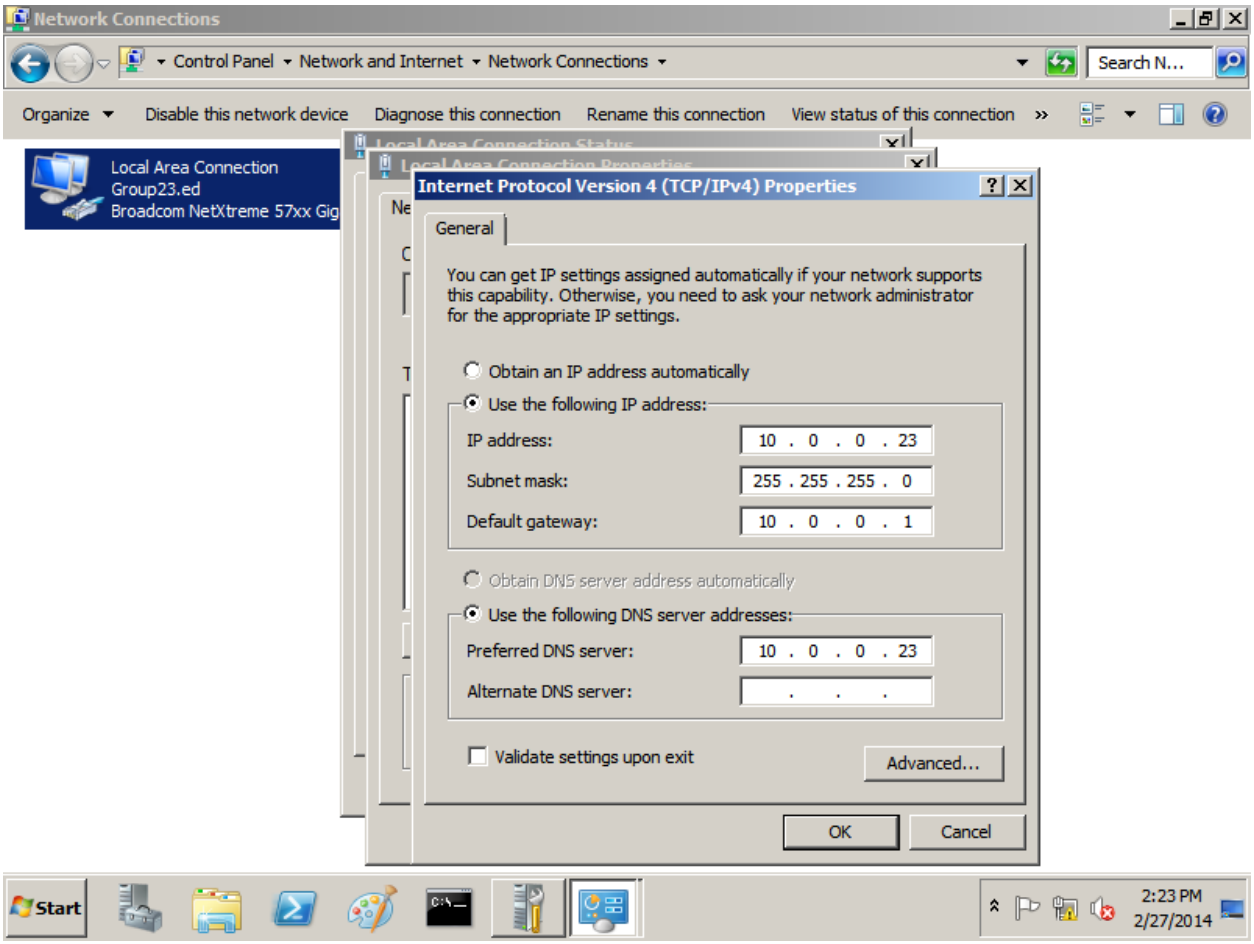
Lab 5.1 The Parallel Backbone:

Materials Required: Two Servers: each with 2 NIC's – Routing and Remote Access Services,

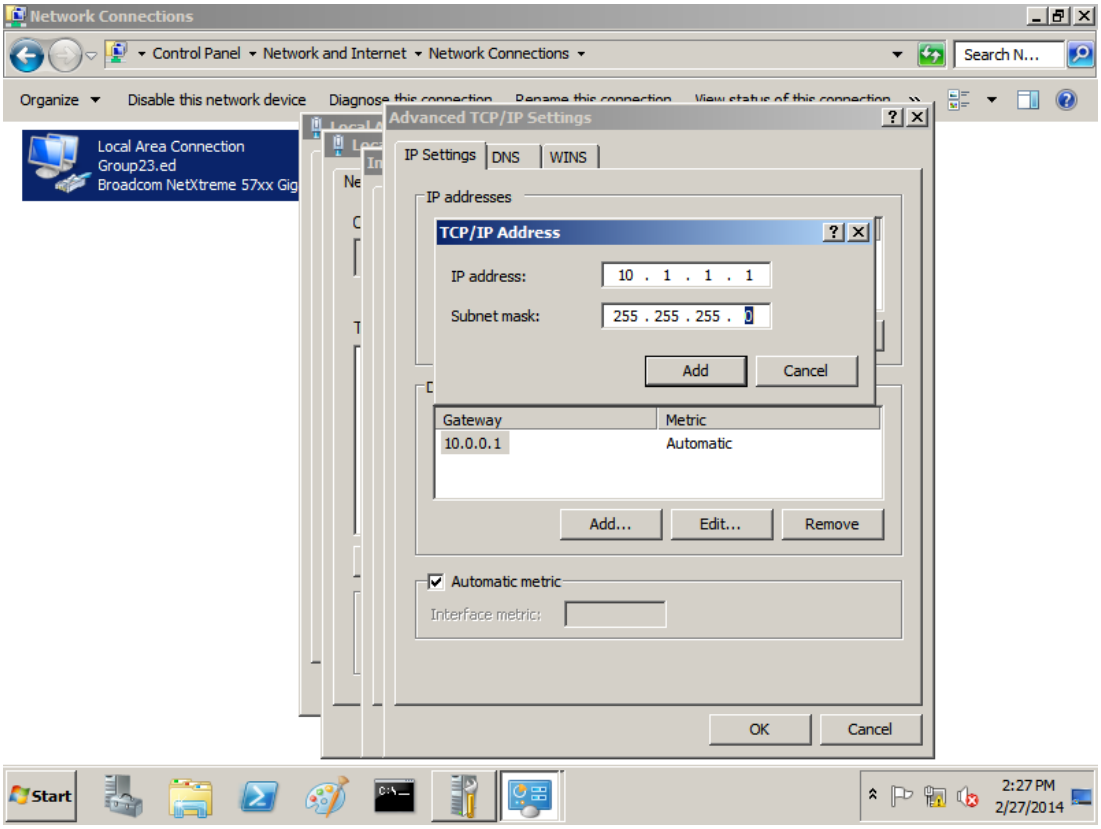
Installed, but not enabled. (RRAS)

Power on the two Servers and two switches – Plug one cable into a NIC in Server 1. Plug the other end of the cable into Switch 1- plug another cable into the second NIC in's Server 1 – plug the other end of the cable into Switch 2. Both NICs on Server 1 are now connected to different Switches. Plug a third cable into a NIC on Server 2. Plug the other end of this cable into one of the Switches. Plug the fourth cable into the second NIC on Server 2. Plug the other end of this cable into the other Switch. Both NIC's on Server 2 are now plugged into different switches, and each other is connected.

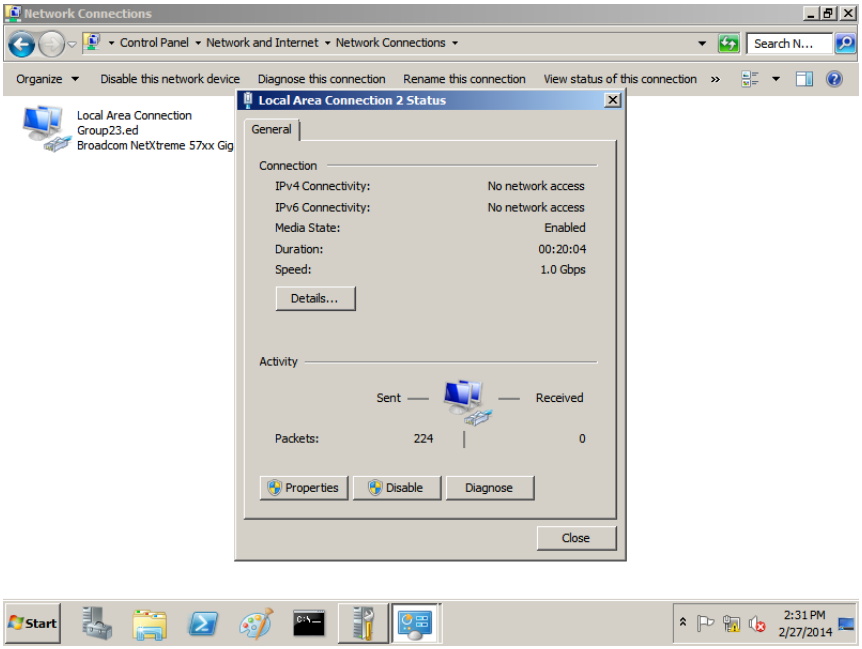
Server 1 –Start – Control Panel – Network and Sharing Center – Manage Network Connections - Local Area Connections – Properties – (ICP/IPv4). 10.0.0.23, default subnet mask -255.255.0.0 – Select Use the Following D.N.S. button and enter 10.0.2. 23 in the Preferred D.N.S. Server Text Box.



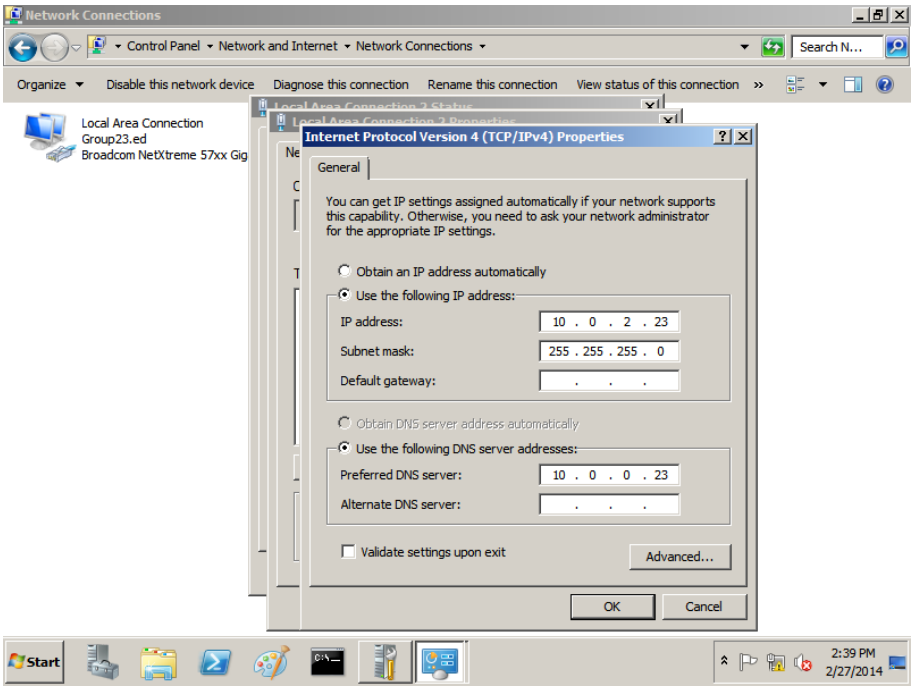
Advanced – Add beneath the IP address. TCP/IP address text box opens. Configure second IP address.



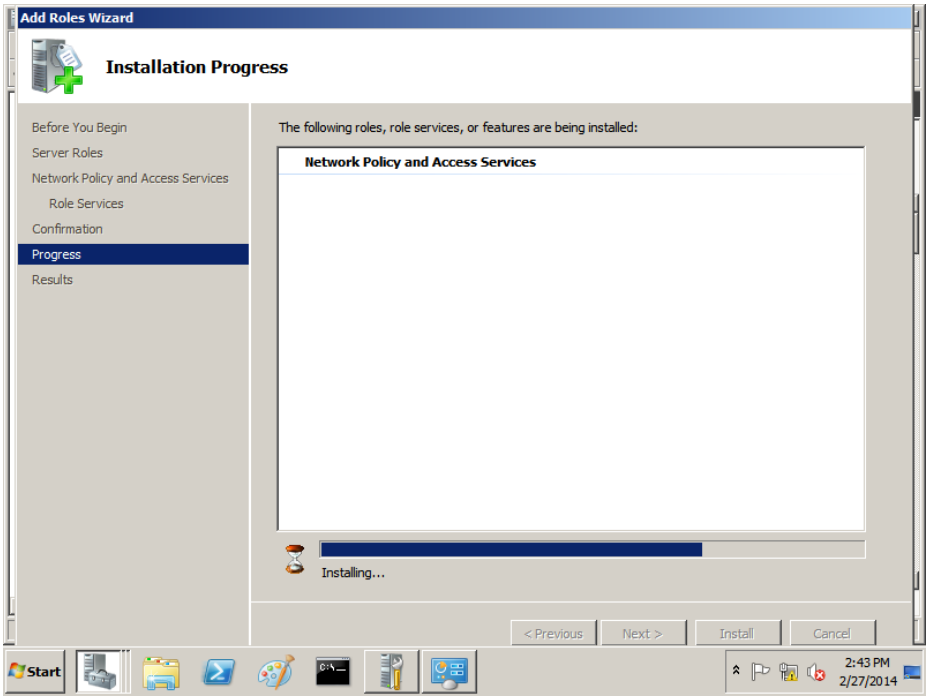
Add – OK. Double click Local Area Connection 2 – Properties

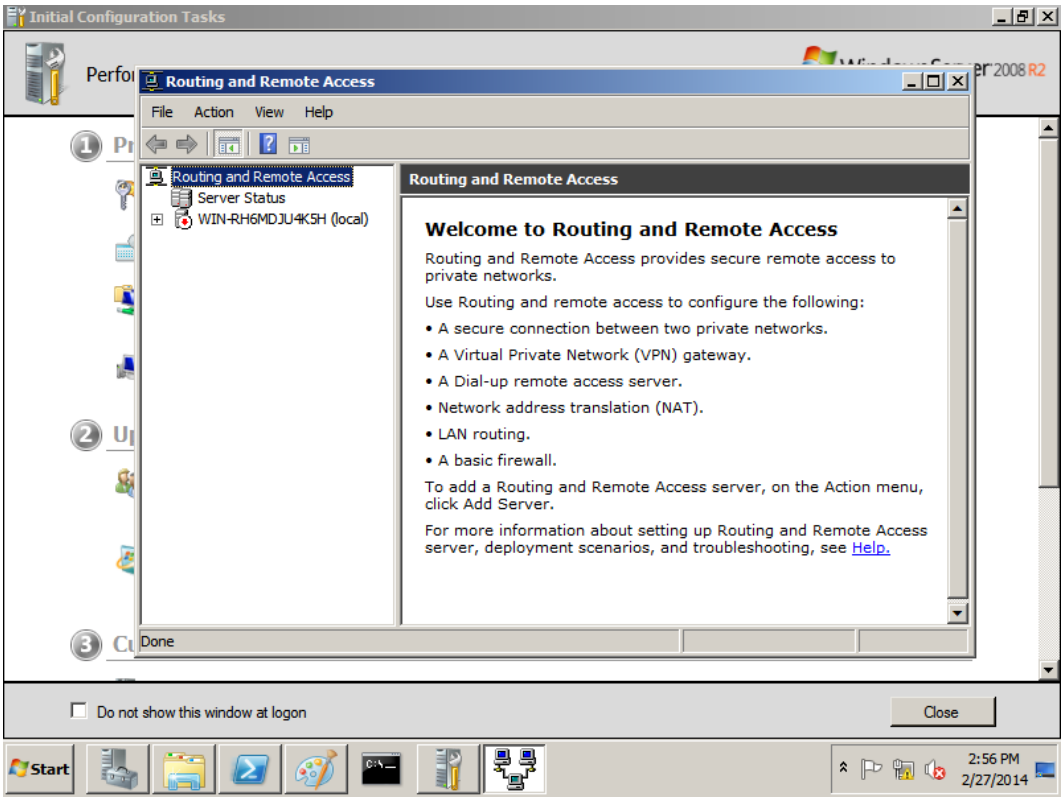


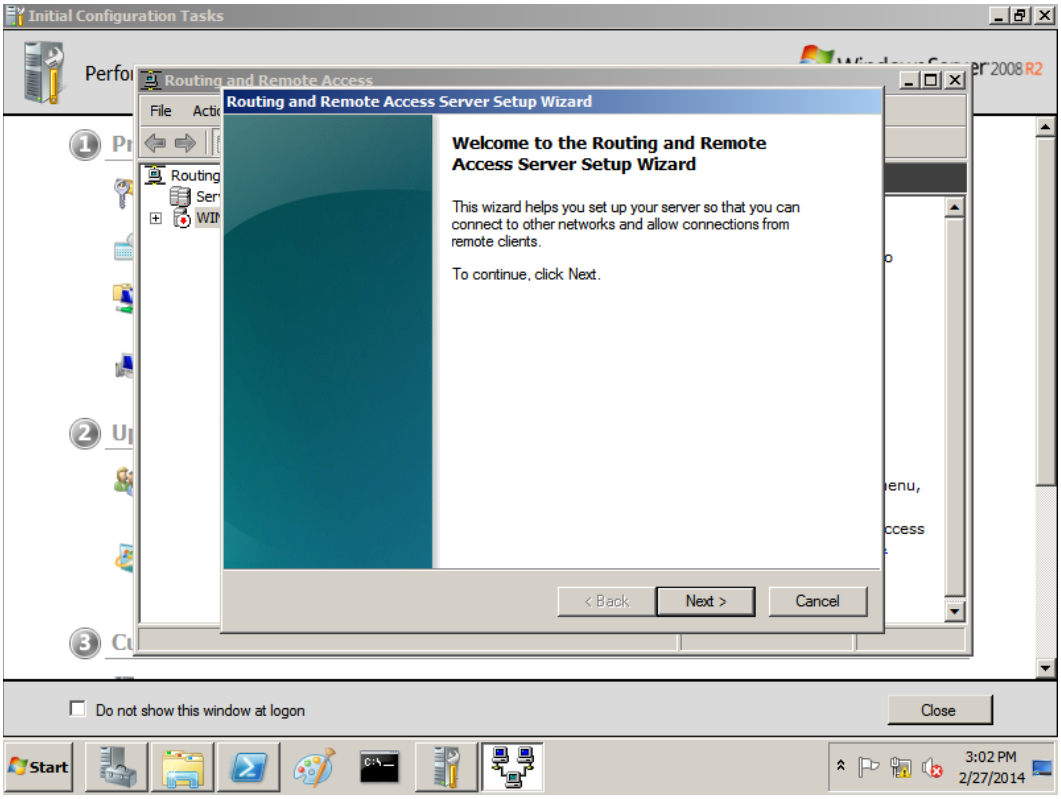
Double click Internet Protocol Version 4 (TCP/IPv4). Enter 10.0.2.23 in the IP address box and 255.255.0.0in the subnet mask box. Select Use the following DNS address and enter 10.0.0.23 (Other Server's IP address) in server DNS box. OK - Close



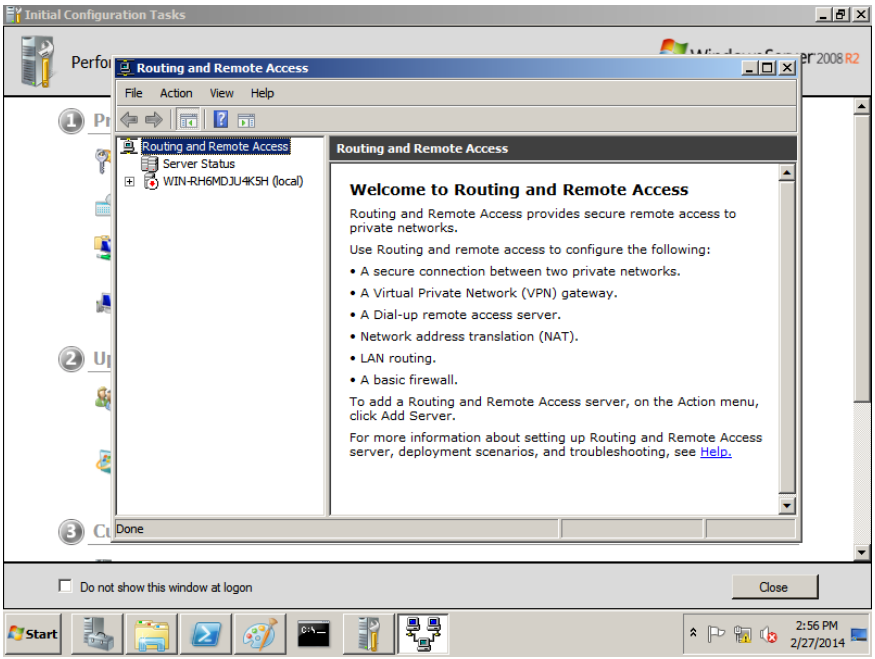
On Server 1 install and configure Routing and Remote Access.

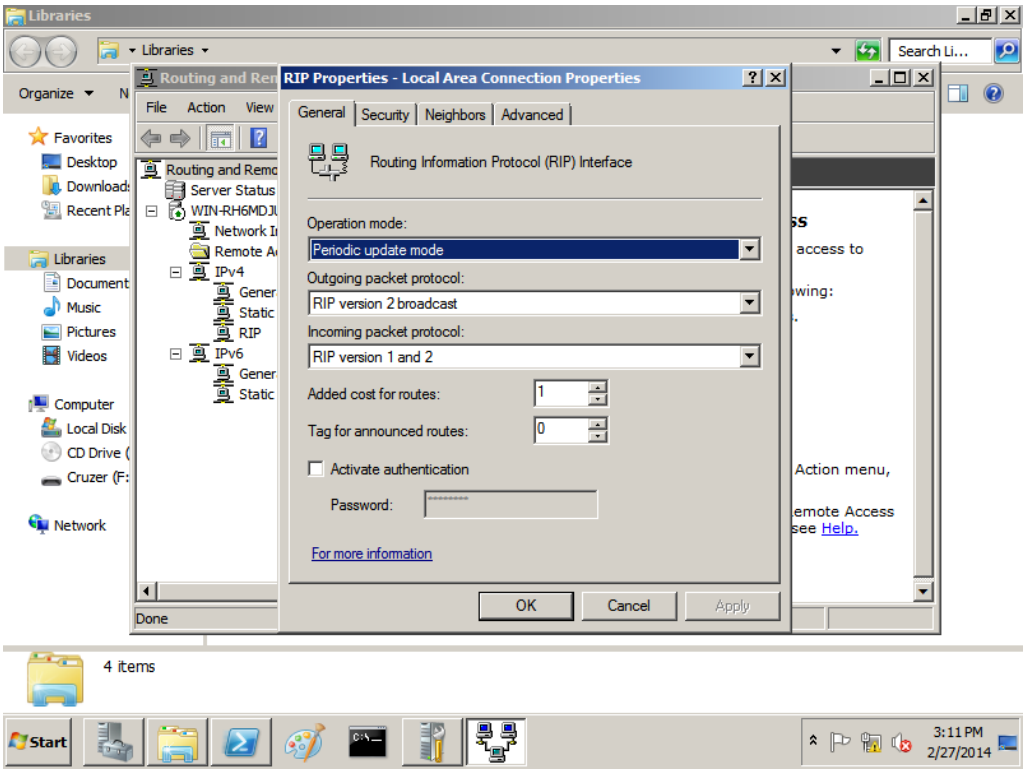



Initial Configuration Tasks
Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
WIN-RH6MDJU4K5H (local)
Routing and Remote Access
Welcome to Routing and Remote Access
Routing and Remote Access provides secure remote access to private networks.
Use Routing and remote access to configure the following:
• A secure connection between two private networks.
• A Virtual Private Network (VPN) gateway.
• A Dial-up remote access server.
• Network address translation (NAT).
• LAN routing.
• A basic firewall.
To add a Routing and Remote Access server, on the Action menu, click Add Server.
For more information about setting up Routing and Remote Access server, deployment scenarios, and troubleshooting, see Help.
Done
Do not show this window at logon
Close
Start
2:56 PM
2/27/2014

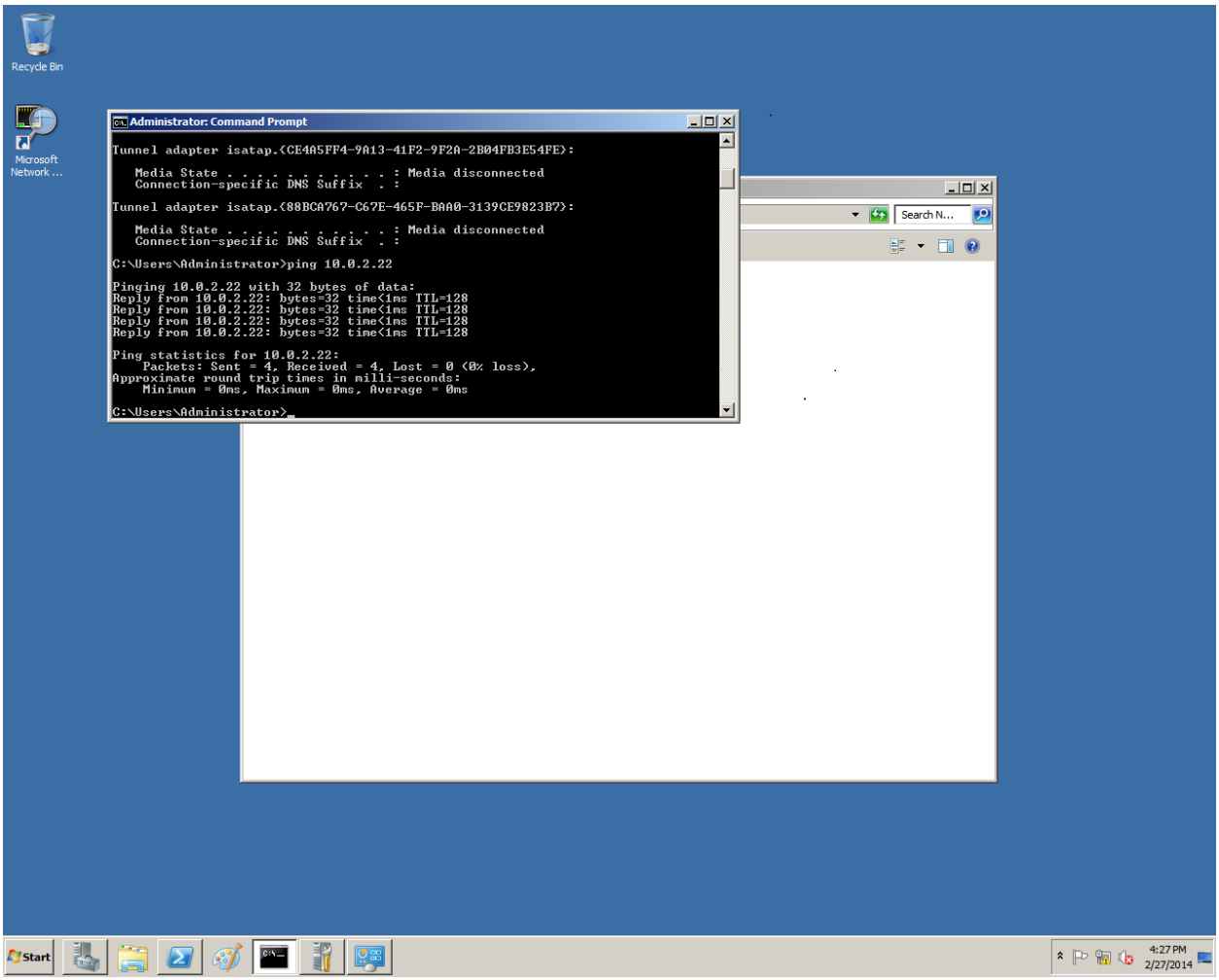

Initial Configuration Tasks
Routing and Remote Access
Routing and Remote Access Server Setup Wizard
Welcome to the Routing and Remote Access Server Setup Wizard
This wizard helps you set up your server so that you can connect to other networks and allow connections from remote clients.
To continue, click Next.
< Back
Next >
Cancel
Do not show this window at logon
Close
Start
3:02 PM
2/27/2014

Start – Administrator Tools – Routing and Remote Access – Wizard opens – Next – Finish – Start Service – click plus sign (+) next to Server 1- expand the tree – Ipv4 – right click General – Select New Routing Protocol.

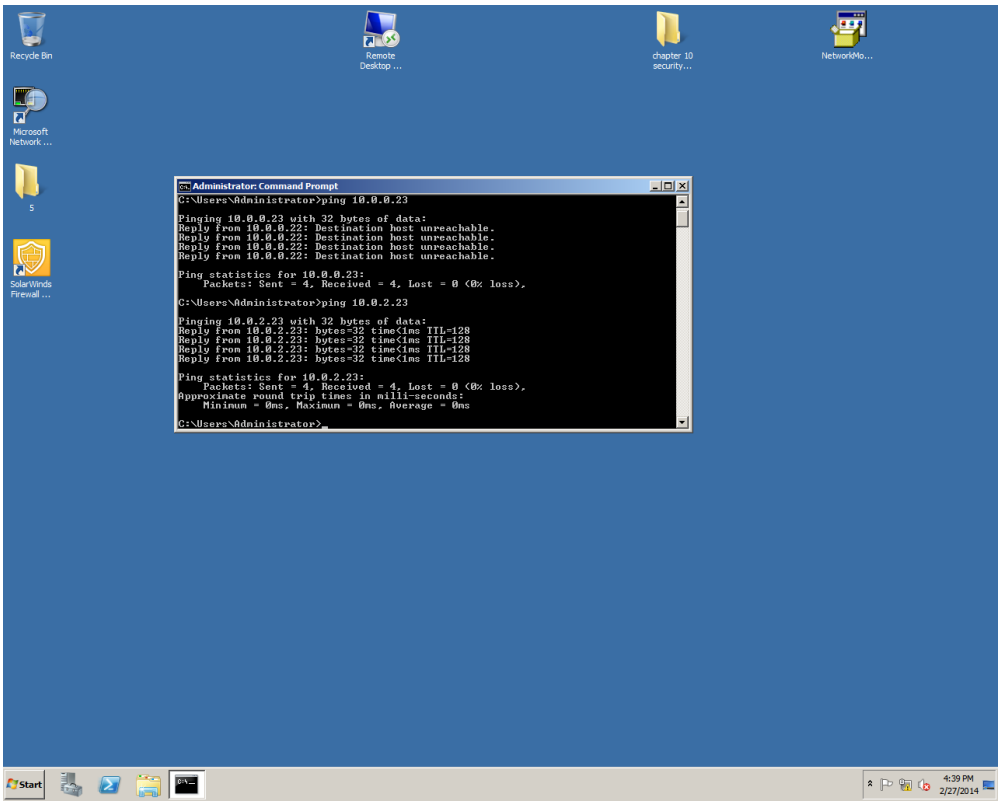




Double click RIP Version 2 for Internet Protocol – Click RIP – New Interface - Double click Local Area connection – OK – Repeat steps 29 through 31 for Local Area Connection 2. Server 2 repeat steps 6 through 10 and 15 through 33 – click OK twice – However use different IP address – Command Prompt – Ping Server1 from Server 2.



Ping Server 2 from Server 1.



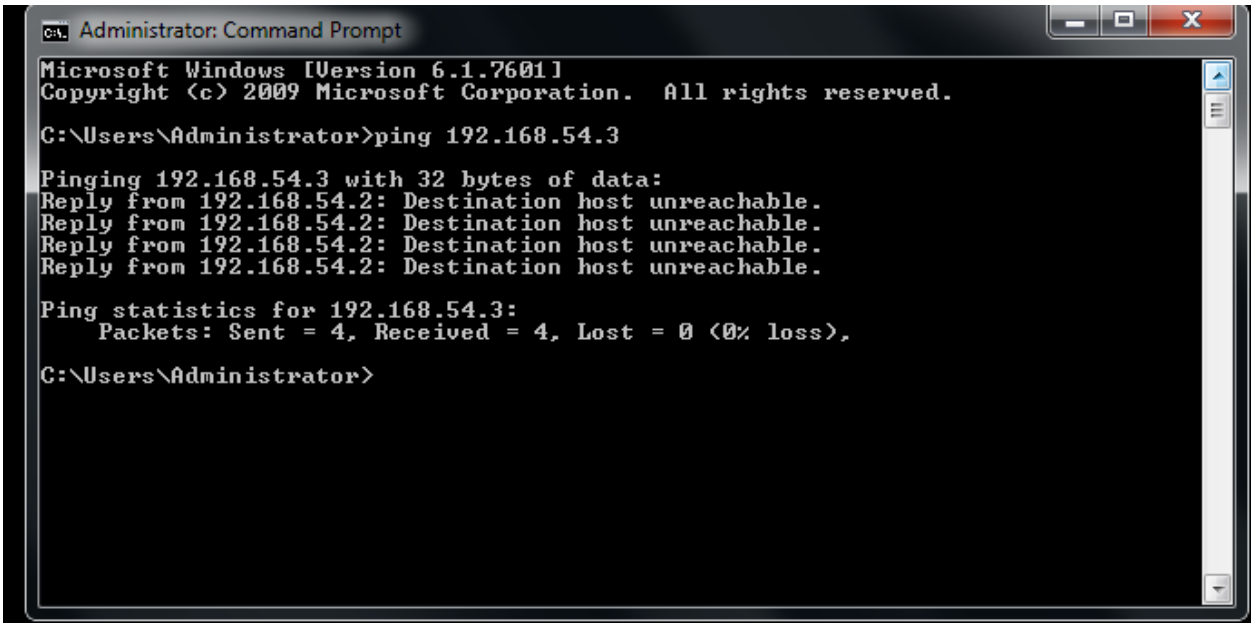
Log off.

Lab 5.2 Building a Daisy Chain

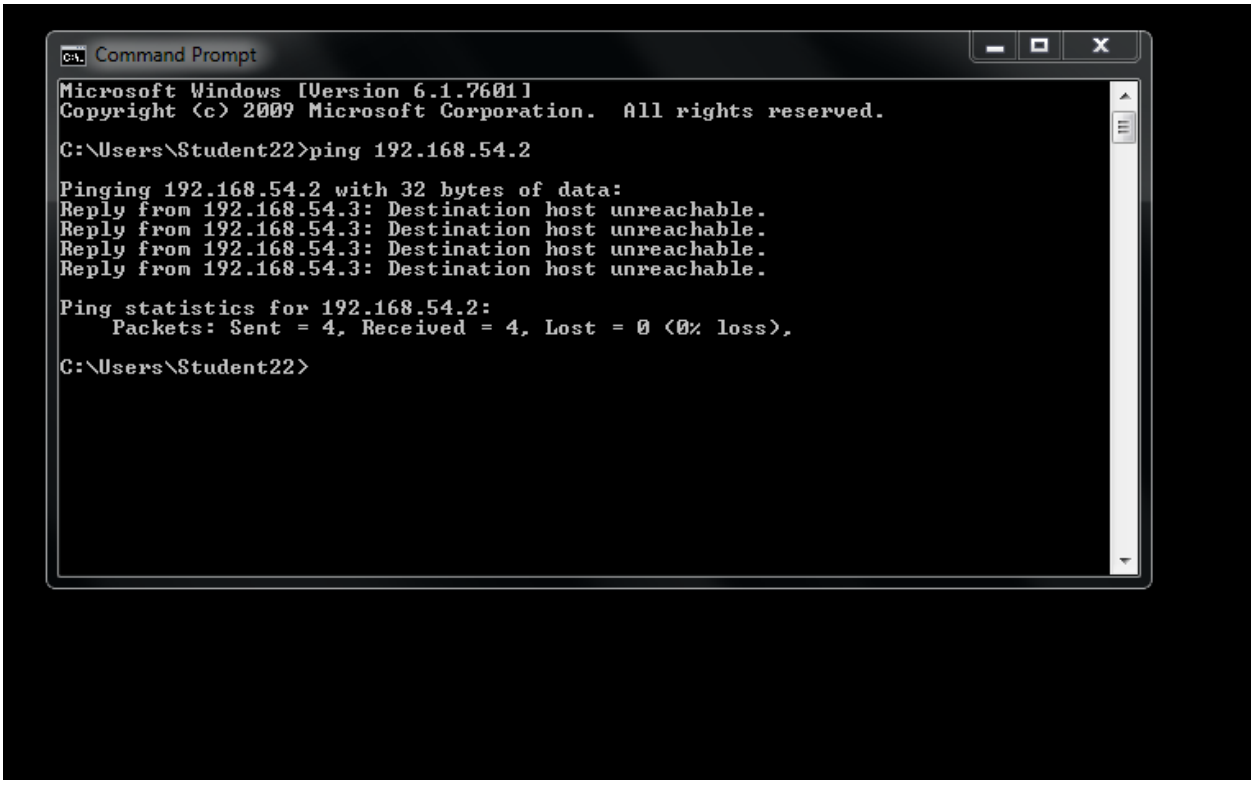
Connect two workstations with four switches.

Command Prompt

Ping workstation 1 from workstation 2

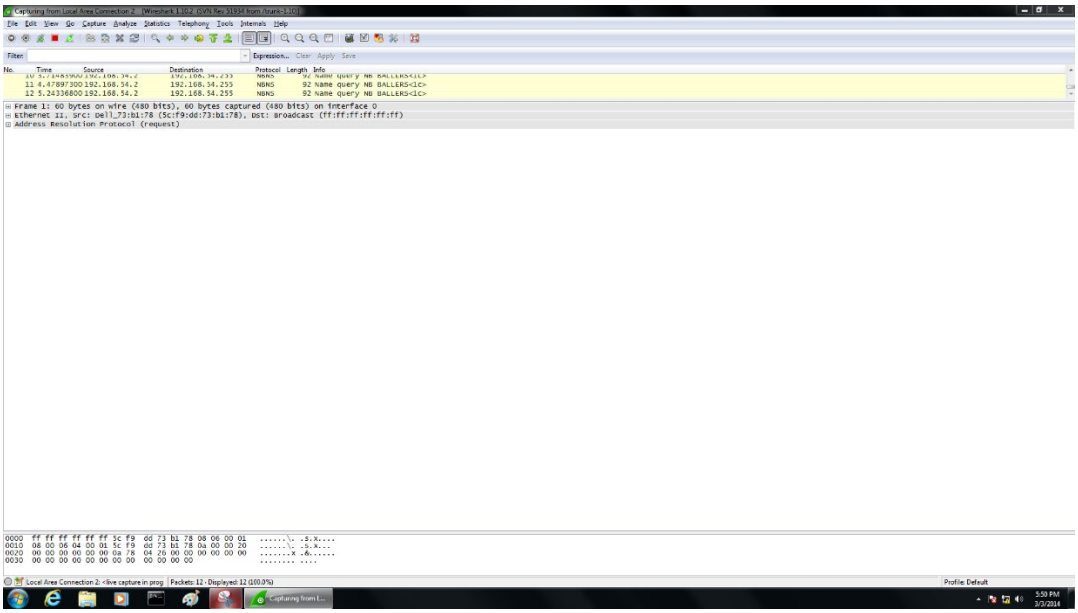


Ping workstation 2 from workstation 1

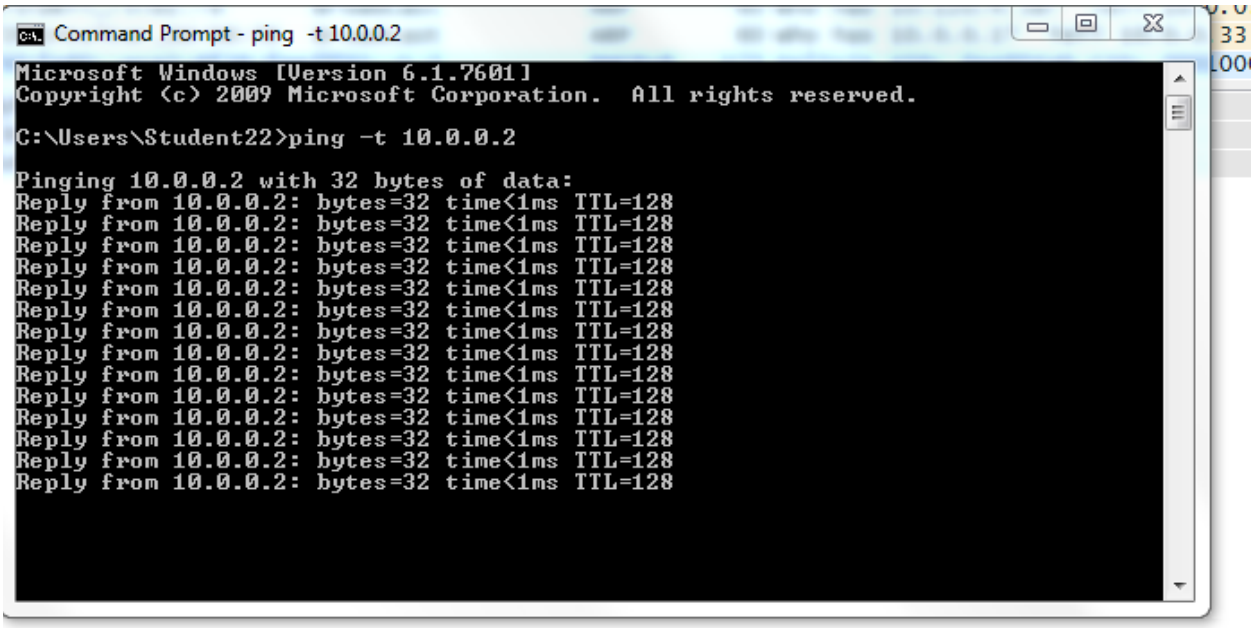


Lab 5.3 Examining Ethernet Frames

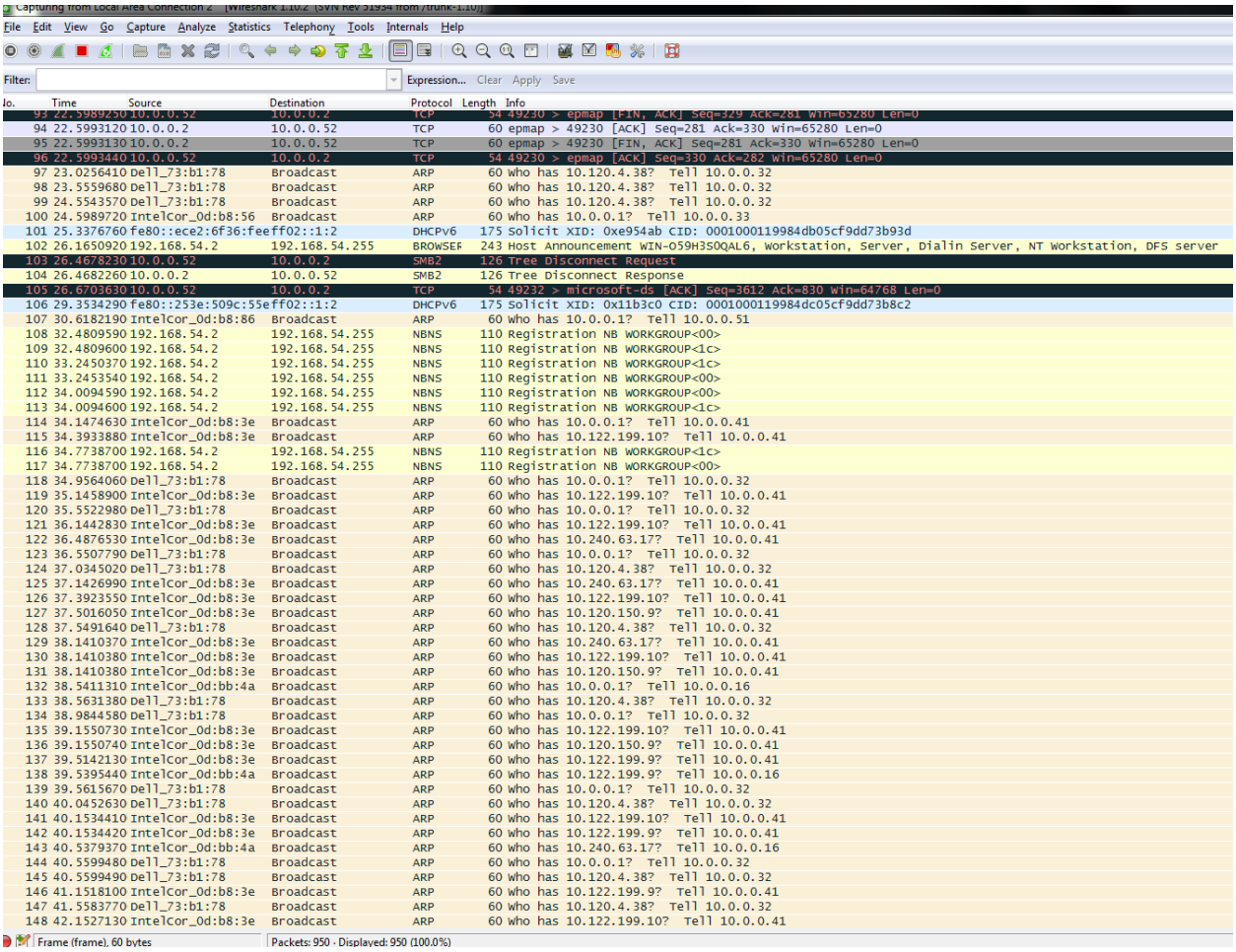
Log on to Server – Start – All Programs – Wireshark – Capture – Start – Command Prompt – **Ping -t** Workstation – Click Stop – Click a frame listed as ICMP – In the middle of the frame click the plus sign (+) to expand the tree

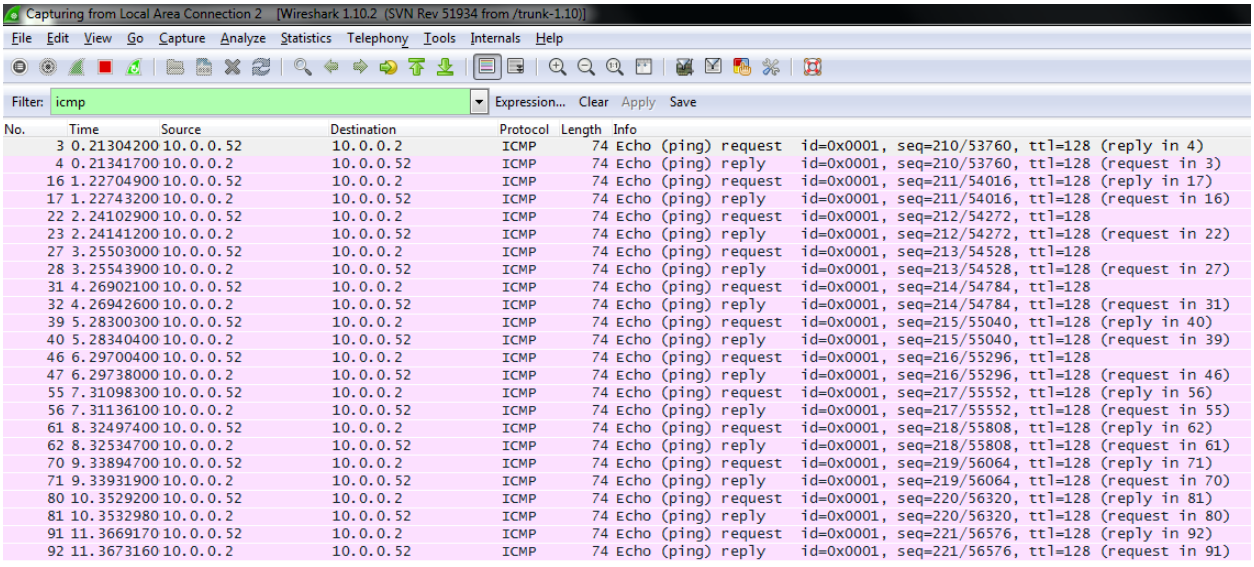


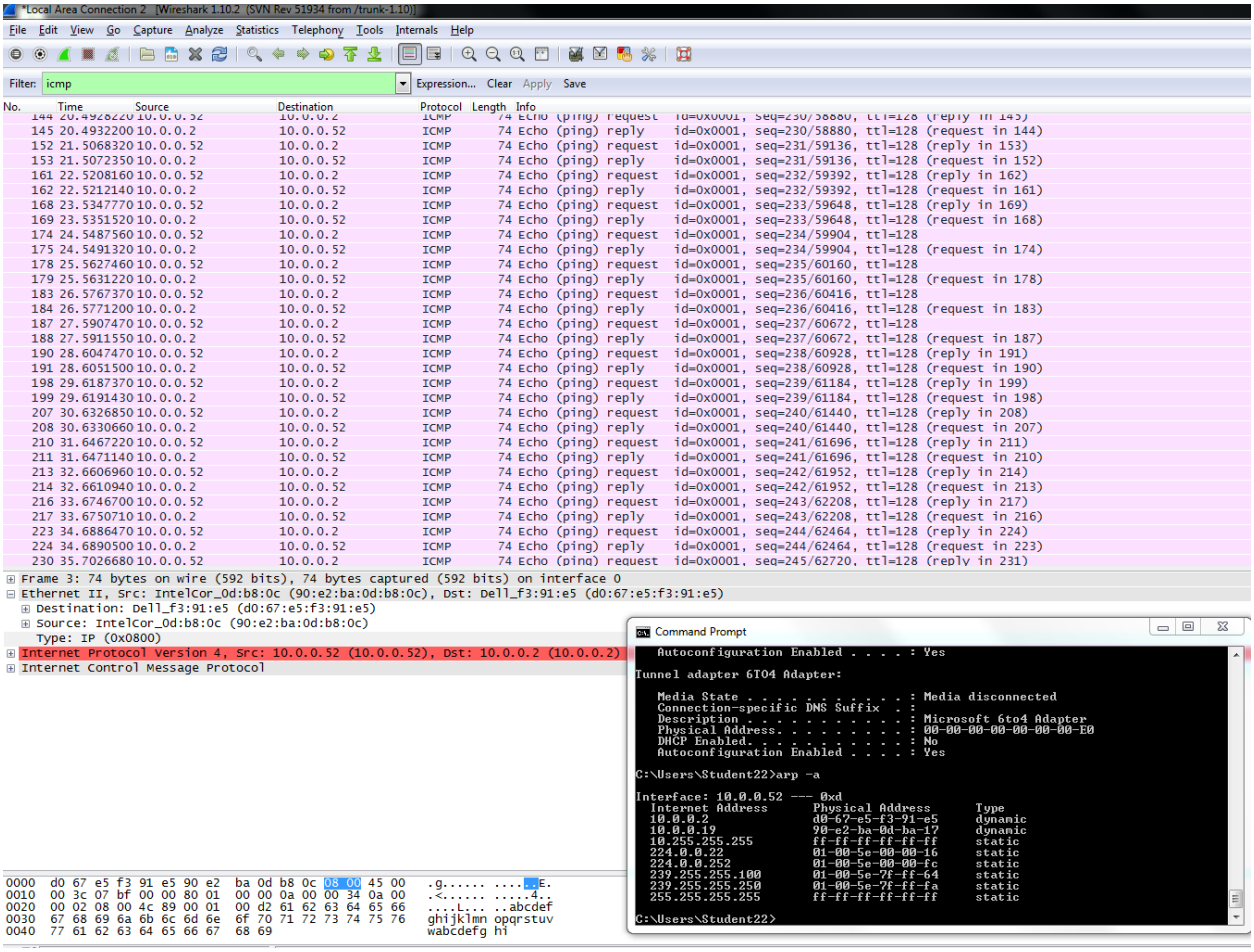
In the command prompt press **Crt+C** to stop the ping command. Then type **ipconfig/all** - Enter



Type arp –a – Enter


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
93 22.5989250 10.0.0.52 10.0.0.2 TCP 54 49230 > epmap [FIN, ACK] Seq=329 Ack=281 Win=65280 Len=0
94 22.5993120 10.0.0.2 10.0.0.52 TCP 60 epmap > 49230 [ACK] Seq=281 Ack=330 Win=65280 Len=0
95 22.5993130 10.0.0.2 10.0.0.52 TCP 60 epmap > 49230 [FIN, ACK] Seq=281 Ack=330 Win=65280 Len=0
96 22.5993440 10.0.0.52 10.0.0.2 TCP 54 49230 > epmap [ACK] Seq=330 Ack=282 Win=65280 Len=0
97 23.0256410 Dell_73:b1:78 Broadcast ARP 60 Who has 10.120.4.38? Tell 10.0.0.32
98 23.5559680 Dell_73:b1:78 Broadcast ARP 60 Who has 10.120.4.38? Tell 10.0.0.32
99 24.5543570 Dell_73:b1:78 Broadcast ARP 60 Who has 10.120.4.38? Tell 10.0.0.32
100 24.5989720 IntelCor_0d:b8:56 Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.33
101 25.3376760 fe80::ece2:6f36:feff02::1:2 DHCPv6 175 Solicit XID: 0xe954ab CID: 0001000119984db05cf9dd73b93d
102 26.1650920 192.168.54.2 192.168.54.255 BROWSER 243 Host Announcement WIN-O59H3SOQAL6, Workstation, Server, Dialin Server, NT Workstation, DFS server
103 26.4678230 10.0.0.52 10.0.0.2 SMB2 126 Tree Disconnect Request
104 26.4682260 10.0.0.2 10.0.0.52 SMB2 126 Tree Disconnect Response
105 26.6703630 10.0.0.52 10.0.0.2 TCP 54 49232 > microsoft-ds [ACK] Seq=3612 Ack=830 Win=64768 Len=0
106 29.3534290 fe80::253e:509c:55eff02::1:2 DHCPv6 175 Solicit XID: 0x11b3c0 CID: 0001000119984dc05cf9dd73b8c2
107 30.6182190 IntelCor_0d:b8:86 Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.51
108 32.4809590 192.168.54.2 192.168.54.255 NBNS 110 Registration NB WORKGROUP<00>
109 32.4809600 192.168.54.2 192.168.54.255 NBNS 110 Registration NB WORKGROUP<1c>
110 33.2450370 192.168.54.2 192.168.54.255 NBNS 110 Registration NB WORKGROUP<1c>
111 33.2453540 192.168.54.2 192.168.54.255 NBNS 110 Registration NB WORKGROUP<00>
112 34.0094590 192.168.54.2 192.168.54.255 NBNS 110 Registration NB WORKGROUP<00>
113 34.0094600 192.168.54.2 192.168.54.255 NBNS 110 Registration NB WORKGROUP<1c>
114 34.1474630 IntelCor_0d:b8:3e Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.41
115 34.3933880 IntelCor_0d:b8:3e Broadcast ARP 60 Who has 10.122.199.10? Tell 10.0.0.41
116 34.7738700 192.168.54.2 192.168.54.255 NBNS 110 Registration NB WORKGROUP<1c>
117 34.7738700 192.168.54.2 192.168.54.255 NBNS 110 Registration NB WORKGROUP<00>
118 34.9564060 Dell_73:b1:78 Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.32
119 35.1458900 IntelCor_0d:b8:3e Broadcast ARP 60 Who has 10.122.199.10? Tell 10.0.0.41
120 35.5522980 Dell_73:b1:78 Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.32
121 36.1442830 IntelCor_0d:b8:3e Broadcast ARP 60 Who has 10.122.199.10? Tell 10.0.0.41
122 36.4876530 IntelCor_0d:b8:3e Broadcast ARP 60 Who has 10.240.63.17? Tell 10.0.0.41
123 36.5507790 Dell_73:b1:78 Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.32
124 37.0345020 Dell_73:b1:78 Broadcast ARP 60 Who has 10.120.4.38? Tell 10.0.0.32
125 37.1426990 IntelCor_0d:b8:3e Broadcast ARP 60 Who has 10.240.63.17? Tell 10.0.0.41
126 37.3923550 IntelCor_0d:b8:3e Broadcast ARP 60 Who has 10.122.199.10? Tell 10.0.0.41
127 37.5016050 IntelCor_0d:b8:3e Broadcast ARP 60 Who has 10.120.150.9? Tell 10.0.0.41
128 37.5491640 Dell_73:b1:78 Broadcast ARP 60 Who has 10.120.4.38? Tell 10.0.0.32
129 38.1410370 IntelCor_0d:b8:3e Broadcast ARP 60 Who has 10.240.63.17? Tell 10.0.0.41
130 38.1410380 IntelCor_0d:b8:3e Broadcast ARP 60 Who has 10.122.199.10? Tell 10.0.0.41
131 38.1410380 IntelCor_0d:b8:3e Broadcast ARP 60 Who has 10.120.150.9? Tell 10.0.0.41
132 38.5411310 IntelCor_0d:bb:4a Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.16
133 38.5631380 Dell_73:b1:78 Broadcast ARP 60 Who has 10.120.4.38? Tell 10.0.0.32
134 38.9844580 Dell_73:b1:78 Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.32
135 39.1550730 IntelCor_0d:b8:3e Broadcast ARP 60 Who has 10.122.199.10? Tell 10.0.0.41
136 39.1550740 IntelCor_0d:b8:3e Broadcast ARP 60 Who has 10.120.150.9? Tell 10.0.0.41
137 39.5142130 IntelCor_0d:b8:3e Broadcast ARP 60 Who has 10.122.199.9? Tell 10.0.0.41
138 39.5395440 IntelCor_0d:bb:4a Broadcast ARP 60 Who has 10.122.199.9? Tell 10.0.0.16
139 39.5615670 Dell_73:b1:78 Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.32
140 40.0452630 Dell_73:b1:78 Broadcast ARP 60 Who has 10.120.4.38? Tell 10.0.0.32
141 40.1534410 IntelCor_0d:b8:3e Broadcast ARP 60 Who has 10.122.199.10? Tell 10.0.0.41
142 40.1534420 IntelCor_0d:b8:3e Broadcast ARP 60 Who has 10.122.199.9? Tell 10.0.0.41
143 40.5379370 IntelCor_0d:bb:4a Broadcast ARP 60 Who has 10.240.63.17? Tell 10.0.0.16
144 40.5599480 Dell_73:b1:78 Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.32
145 40.5599490 Dell_73:b1:78 Broadcast ARP 60 Who has 10.120.4.38? Tell 10.0.0.32
146 41.1518100 IntelCor_0d:b8:3e Broadcast ARP 60 Who has 10.122.199.9? Tell 10.0.0.41
147 41.5583770 Dell_73:b1:78 Broadcast ARP 60 Who has 10.120.4.38? Tell 10.0.0.32
148 42.1527130 IntelCor_0d:b8:3e Broadcast ARP 60 Who has 10.122.199.10? Tell 10.0.0.41
Frame (frame), 60 bytes
Packets: 950 · Displayed: 950 (100.0%)

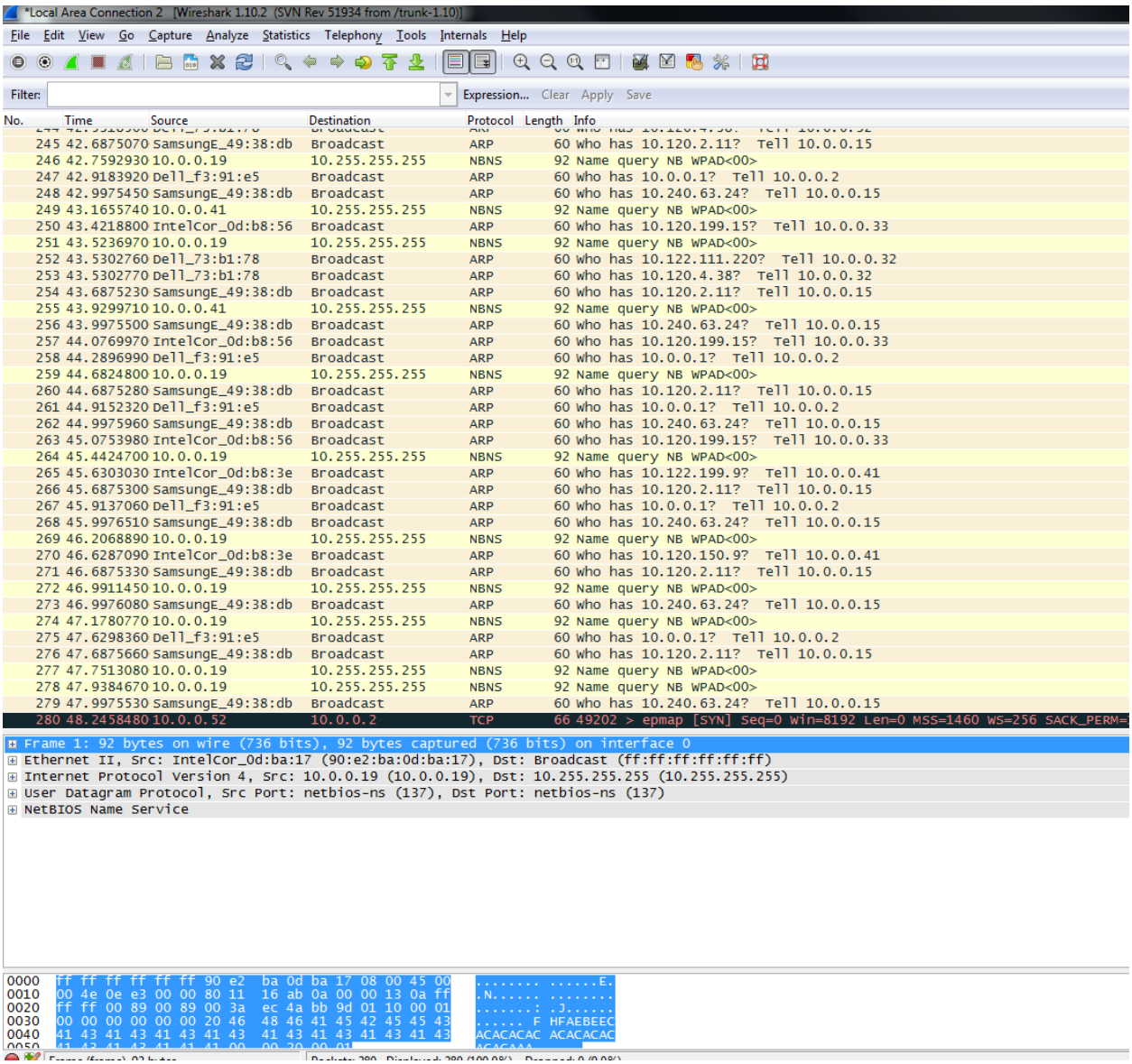

Capturing from Local Area Connection 2 [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: icmp
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
3 0.21304200 10.0.0.52 10.0.0.2 ICMP 74 Echo (ping) request id=0x0001, seq=210/53760, ttl=128 (reply in 4)
4 0.21341700 10.0.0.2 10.0.0.52 ICMP 74 Echo (ping) reply id=0x0001, seq=210/53760, ttl=128 (request in 3)
16 1.22704900 10.0.0.52 10.0.0.2 ICMP 74 Echo (ping) request id=0x0001, seq=211/54016, ttl=128 (reply in 17)
17 1.22743200 10.0.0.2 10.0.0.52 ICMP 74 Echo (ping) reply id=0x0001, seq=211/54016, ttl=128 (request in 16)
22 2.24102900 10.0.0.52 10.0.0.2 ICMP 74 Echo (ping) request id=0x0001, seq=212/54272, ttl=128
23 2.24141200 10.0.0.2 10.0.0.52 ICMP 74 Echo (ping) reply id=0x0001, seq=212/54272, ttl=128 (request in 22)
27 3.25503000 10.0.0.52 10.0.0.2 ICMP 74 Echo (ping) request id=0x0001, seq=213/54528, ttl=128
28 3.25543900 10.0.0.2 10.0.0.52 ICMP 74 Echo (ping) reply id=0x0001, seq=213/54528, ttl=128 (request in 27)
31 4.26902100 10.0.0.52 10.0.0.2 ICMP 74 Echo (ping) request id=0x0001, seq=214/54784, ttl=128
32 4.26942600 10.0.0.2 10.0.0.52 ICMP 74 Echo (ping) reply id=0x0001, seq=214/54784, ttl=128 (request in 31)
39 5.28300300 10.0.0.52 10.0.0.2 ICMP 74 Echo (ping) request id=0x0001, seq=215/55040, ttl=128 (reply in 40)
40 5.28340400 10.0.0.2 10.0.0.52 ICMP 74 Echo (ping) reply id=0x0001, seq=215/55040, ttl=128 (request in 39)
46 6.29700400 10.0.0.52 10.0.0.2 ICMP 74 Echo (ping) request id=0x0001, seq=216/55296, ttl=128
47 6.29738000 10.0.0.2 10.0.0.52 ICMP 74 Echo (ping) reply id=0x0001, seq=216/55296, ttl=128 (request in 46)
55 7.31098300 10.0.0.52 10.0.0.2 ICMP 74 Echo (ping) request id=0x0001, seq=217/55552, ttl=128 (reply in 56)
56 7.31136100 10.0.0.2 10.0.0.52 ICMP 74 Echo (ping) reply id=0x0001, seq=217/55552, ttl=128 (request in 55)
61 8.32497400 10.0.0.52 10.0.0.2 ICMP 74 Echo (ping) request id=0x0001, seq=218/55808, ttl=128 (reply in 62)
62 8.32534700 10.0.0.2 10.0.0.52 ICMP 74 Echo (ping) reply id=0x0001, seq=218/55808, ttl=128 (request in 61)
70 9.33894700 10.0.0.52 10.0.0.2 ICMP 74 Echo (ping) request id=0x0001, seq=219/56064, ttl=128 (reply in 71)
71 9.33931900 10.0.0.2 10.0.0.52 ICMP 74 Echo (ping) reply id=0x0001, seq=219/56064, ttl=128 (request in 70)
80 10.3529200 10.0.0.52 10.0.0.2 ICMP 74 Echo (ping) request id=0x0001, seq=220/56320, ttl=128 (reply in 81)
81 10.3532980 10.0.0.2 10.0.0.52 ICMP 74 Echo (ping) reply id=0x0001, seq=220/56320, ttl=128 (request in 80)
91 11.3669170 10.0.0.52 10.0.0.2 ICMP 74 Echo (ping) request id=0x0001, seq=221/56576, ttl=128 (reply in 92)
92 11.3673160 10.0.0.2 10.0.0.52 ICMP 74 Echo (ping) reply id=0x0001, seq=221/56576, ttl=128 (request in 91)



Log off.

Lab 5.4 Capturing Network Data

Log onto Server – Start – All Programs – Wireshark – The Wireshark Network Protocol Analyzer Opens – Click Capture – Start – Log onto the Workstation - Command Prompt – FTP 192.168.54.1 – Enter. You have connected and the computer is running the Microsoft FTP service. Atempt a failed log in. Now look at the Wireshark on Server – click Stop. To find the log in information click Edit – Find Packet click String – Find. Note that the frame contains both the username and the password you used while attempting to log in to FTP.


*Local Area Connection 2 [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
245 42.6875070 SamsungE_49:38:db Broadcast ARP 60 Who has 10.120.2.11? Tell 10.0.0.15
246 42.7592930 10.0.0.19 10.255.255.255 NBNS 92 Name query NB WPAD<00>
247 42.9183920 Dell_f3:91:e5 Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.2
248 42.9975450 SamsungE_49:38:db Broadcast ARP 60 Who has 10.240.63.24? Tell 10.0.0.15
249 43.1655740 10.0.0.41 10.255.255.255 NBNS 92 Name query NB WPAD<00>
250 43.4218800 IntelCor_0d:b8:56 Broadcast ARP 60 Who has 10.120.199.15? Tell 10.0.0.33
251 43.5236970 10.0.0.19 10.255.255.255 NBNS 92 Name query NB WPAD<00>
252 43.5302760 Dell_73:b1:78 Broadcast ARP 60 Who has 10.122.111.220? Tell 10.0.0.32
253 43.5302770 Dell_73:b1:78 Broadcast ARP 60 Who has 10.120.4.38? Tell 10.0.0.32
254 43.6875230 SamsungE_49:38:db Broadcast ARP 60 Who has 10.120.2.11? Tell 10.0.0.15
255 43.9299710 10.0.0.41 10.255.255.255 NBNS 92 Name query NB WPAD<00>
256 43.9975500 SamsungE_49:38:db Broadcast ARP 60 Who has 10.240.63.24? Tell 10.0.0.15
257 44.0769970 IntelCor_0d:b8:56 Broadcast ARP 60 Who has 10.120.199.15? Tell 10.0.0.33
258 44.2896990 Dell_f3:91:e5 Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.2
259 44.6824800 10.0.0.19 10.255.255.255 NBNS 92 Name query NB WPAD<00>
260 44.6875280 SamsungE_49:38:db Broadcast ARP 60 Who has 10.120.2.11? Tell 10.0.0.15
261 44.9152320 Dell_f3:91:e5 Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.2
262 44.9975960 SamsungE_49:38:db Broadcast ARP 60 Who has 10.240.63.24? Tell 10.0.0.15
263 45.0753980 IntelCor_0d:b8:56 Broadcast ARP 60 Who has 10.120.199.15? Tell 10.0.0.33
264 45.4424700 10.0.0.19 10.255.255.255 NBNS 92 Name query NB WPAD<00>
265 45.6303030 IntelCor_0d:b8:3e Broadcast ARP 60 Who has 10.122.199.9? Tell 10.0.0.41
266 45.6875300 SamsungE_49:38:db Broadcast ARP 60 Who has 10.120.2.11? Tell 10.0.0.15
267 45.9137060 Dell_f3:91:e5 Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.2
268 45.9976510 SamsungE_49:38:db Broadcast ARP 60 Who has 10.240.63.24? Tell 10.0.0.15
269 46.2068890 10.0.0.19 10.255.255.255 NBNS 92 Name query NB WPAD<00>
270 46.6287090 IntelCor_0d:b8:3e Broadcast ARP 60 Who has 10.120.150.9? Tell 10.0.0.41
271 46.6875330 SamsungE_49:38:db Broadcast ARP 60 Who has 10.120.2.11? Tell 10.0.0.15
272 46.9911450 10.0.0.19 10.255.255.255 NBNS 92 Name query NB WPAD<00>
273 46.9976080 SamsungE_49:38:db Broadcast ARP 60 Who has 10.240.63.24? Tell 10.0.0.15
274 47.1780770 10.0.0.19 10.255.255.255 NBNS 92 Name query NB WPAD<00>
275 47.6298360 Dell_f3:91:e5 Broadcast ARP 60 Who has 10.0.0.1? Tell 10.0.0.2
276 47.6875660 SamsungE_49:38:db Broadcast ARP 60 Who has 10.120.2.11? Tell 10.0.0.15
277 47.7513080 10.0.0.19 10.255.255.255 NBNS 92 Name query NB WPAD<00>
278 47.9384670 10.0.0.19 10.255.255.255 NBNS 92 Name query NB WPAD<00>
279 47.9975530 SamsungE_49:38:db Broadcast ARP 60 Who has 10.240.63.24? Tell 10.0.0.15
280 48.2458480 10.0.0.52 10.0.0.2 TCP 66 49202 > epmap [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=
Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
Ethernet II, Src: IntelCor_0d:ba:17 (90:e2:ba:0d:ba:17), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 10.0.0.19 (10.0.0.19), Dst: 10.255.255.255 (10.255.255.255)
User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
NetBIOS Name Service
0000 ff ff ff ff ff ff 90 e2 ba 0d ba 17 08 00 45 00 ....E.
0010 00 4e 0e e3 00 00 80 11 16 ab 0a 00 00 13 0a ff .N..... .....
0020 ff ff 00 89 00 89 00 3a ec 4a bb 9d 01 10 00 01 .....: .J.....
0030 00 00 00 00 00 00 20 46 48 46 41 45 42 45 45 43 ..... F HFAEBEEC
0040 41 43 41 43 41 43 41 43 41 43 41 43 41 43 41 43 ACACACAC ACACACAC

Log off.

Joseph Martinez

Networking I: Network +

CNG – 124

Chapter Six Labs

Networking Hardware, Switching and Routing

Lab 6.1 Configuring Transmission and Duplex Settings

Lab 6.2 Creating a Multi-Homed Computer by Installing Two NICs

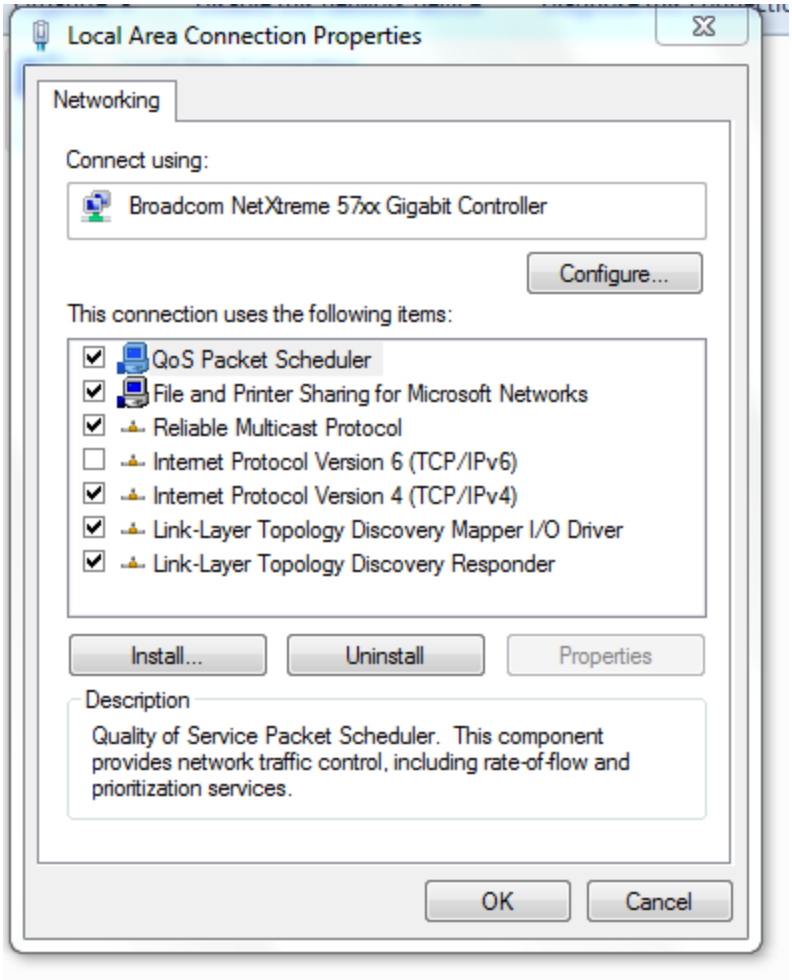
Lab 6.3 Activating Routing and Remote Access in Windows Server 2008

Lab 6.4 Activating a Routing Protocol in Windows Server 2008

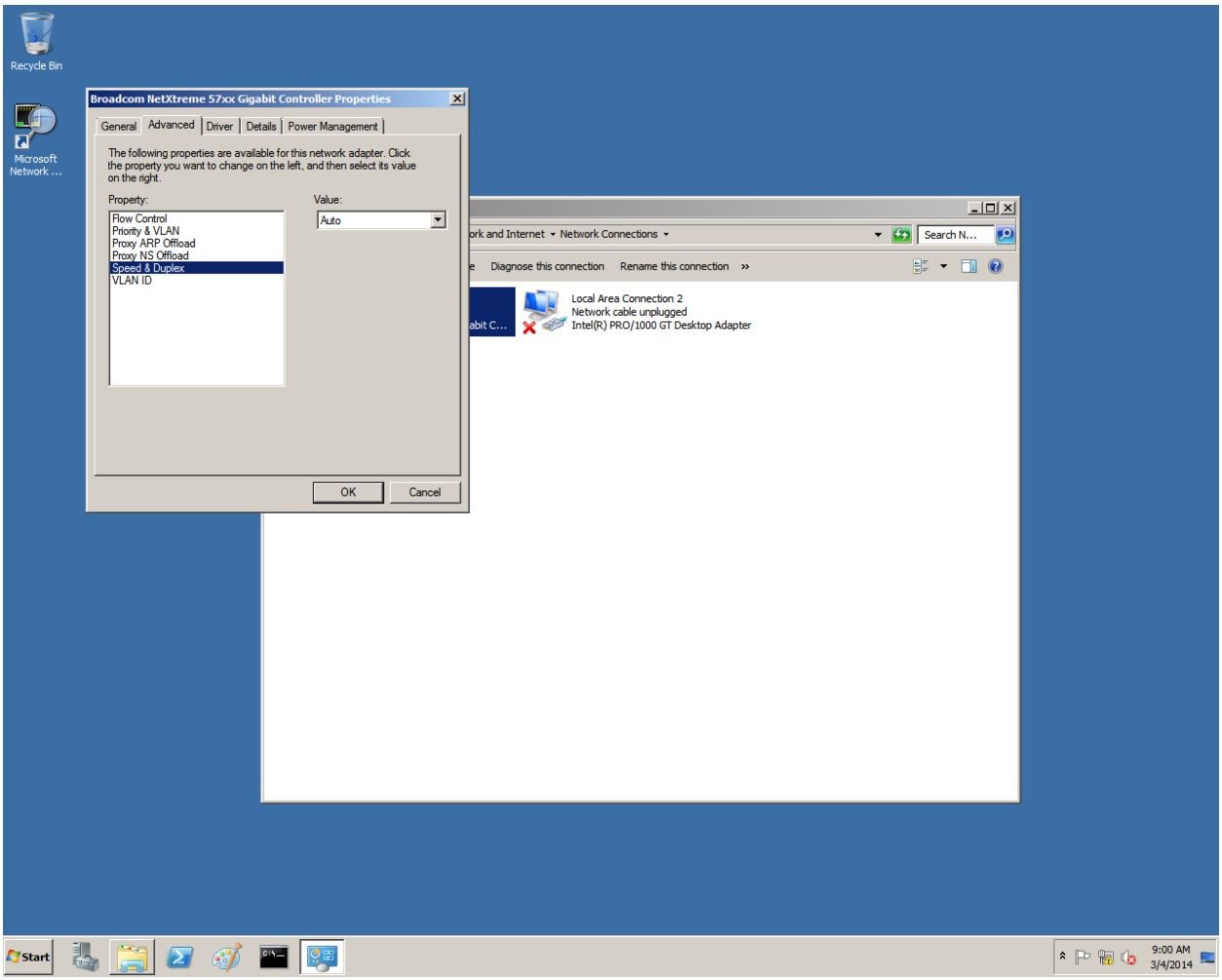
Lab 6.5 Configuring a Bridging Firewall

Lab 6.1 Configuring Transmission and Duplex Settings

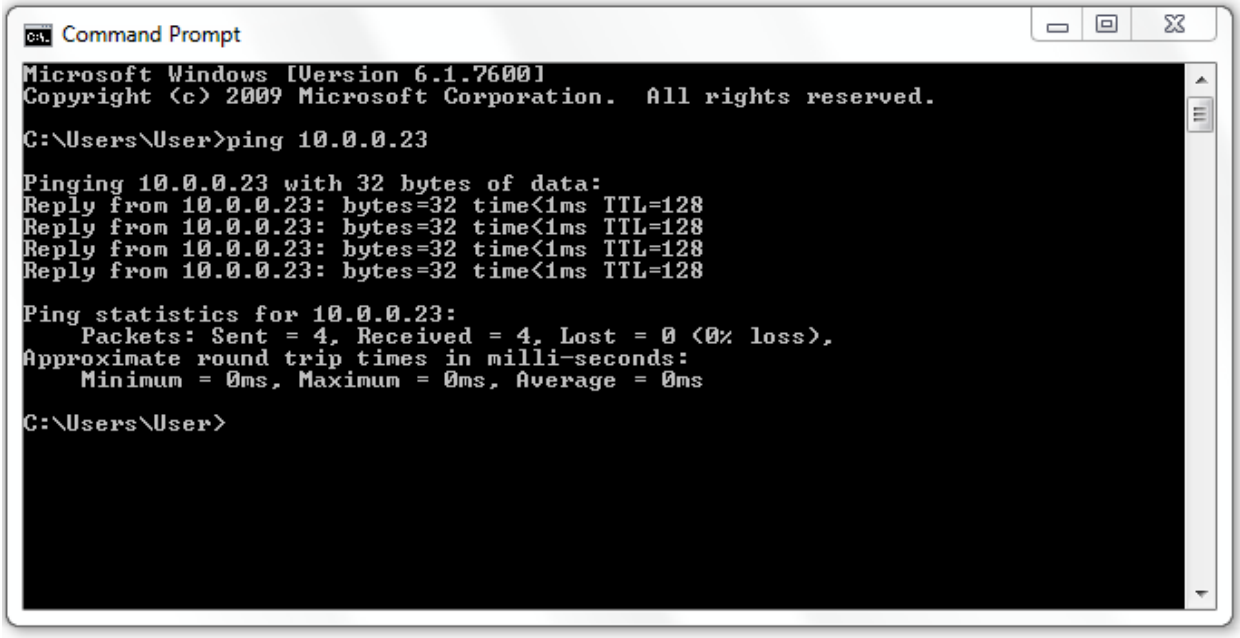
Plug one end of the cable into the switch. Plug the other end of the cable into the Server. – Log on – Local Area Connection – Properties – Configure



Click Advanced – It shows the properties dialog box for the NIC – select Speed and Duplex – In the value drop down box select **100 Mbps Full Duplex** – OK



Log on to Workstation – Ping

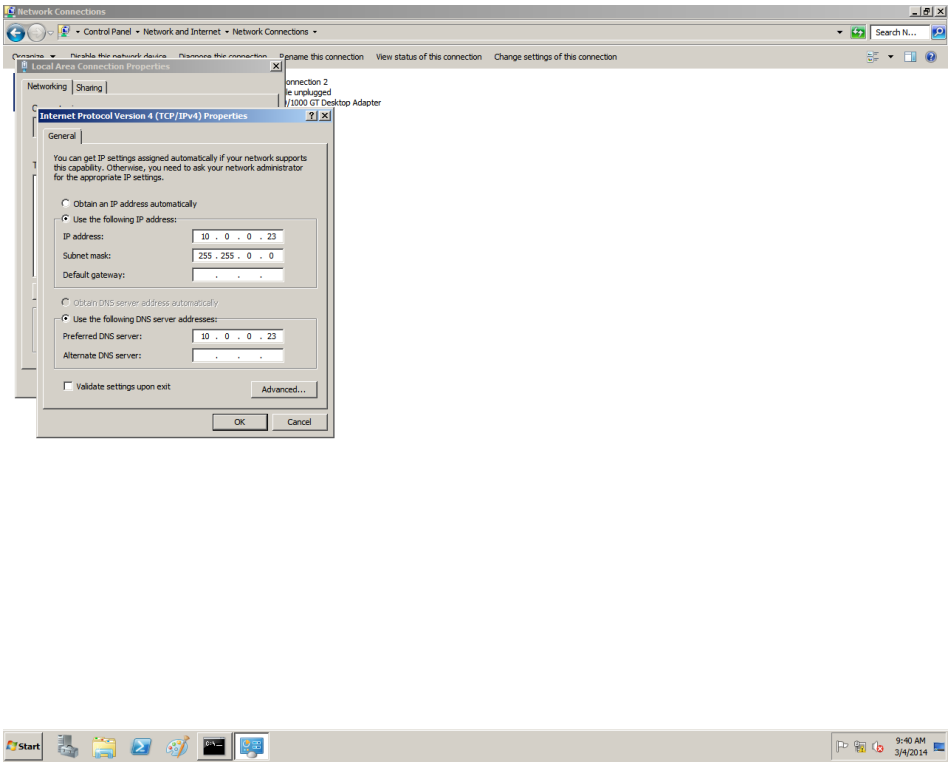


Repeat steps 3 through 9 and on step 8 use the value 100 Mbps Full Duplex

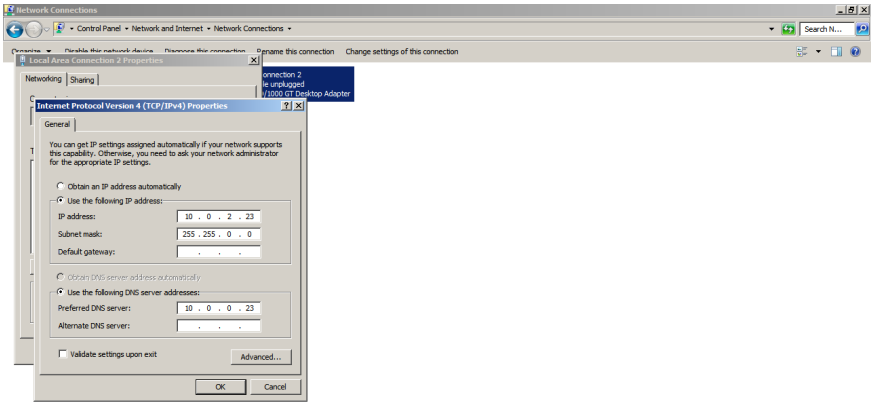
Lab 6.2 Creating a Multi-Homed Computer by Installing Two NICs

Examine the Windows Server Catalog Hardware Compatibility List (HCL) at www.windowsservercatalog.com

Install a NIC card on Server – Log onto the Server – Local Area Connections – Manage Network Connections – Local Area Connection – Properties – Internet Protocol Version 4 – Use the following IP address - 10.0.0.23 Subnet Mask 255.255.0.0 – Leave the default gateway boxes are enabled. OK – Close.



Repeat steps 1 through 24 with Local Area Connection 2 using IP address 10.0.2.23.

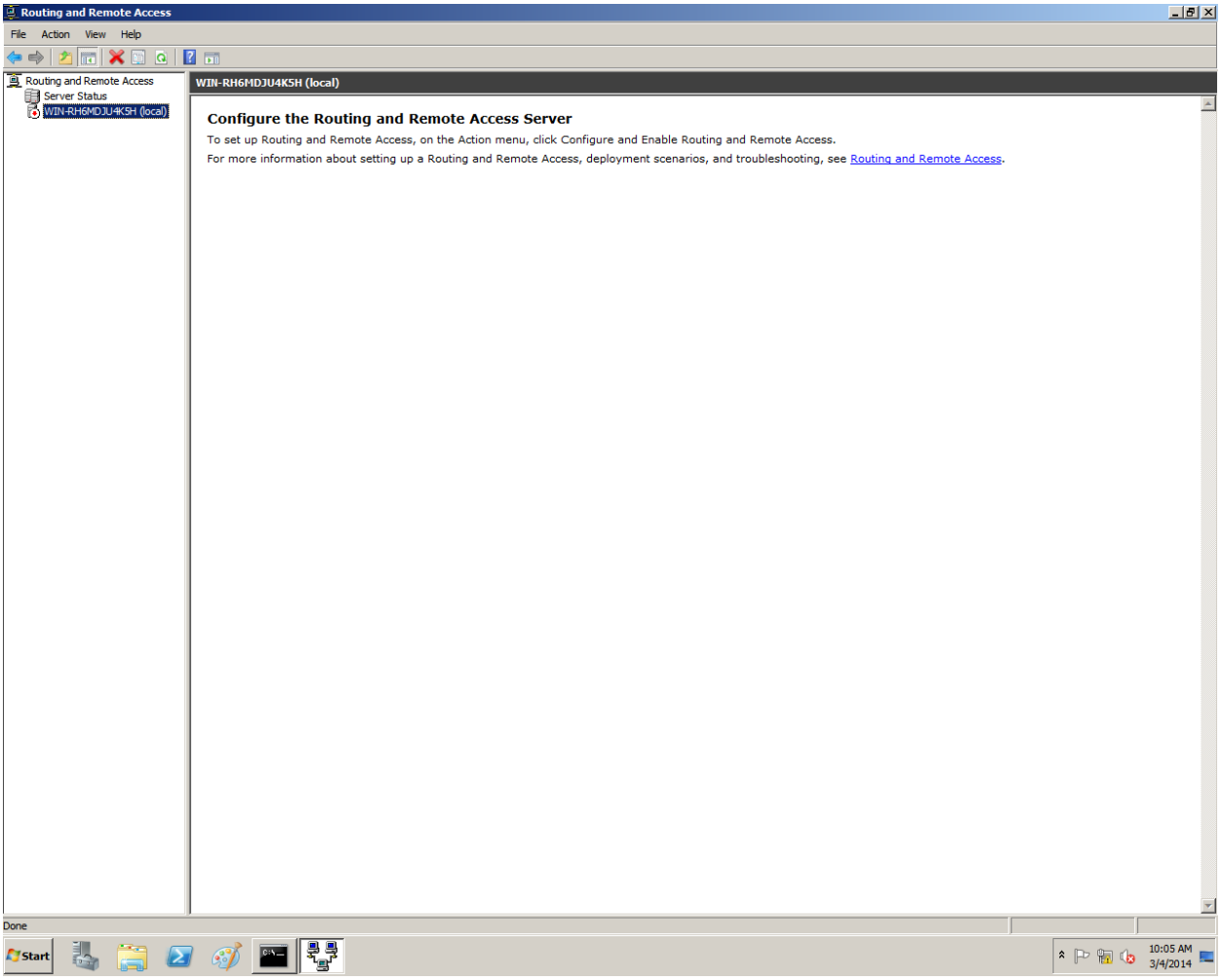


You have now built a multi-homed computer. Log off.

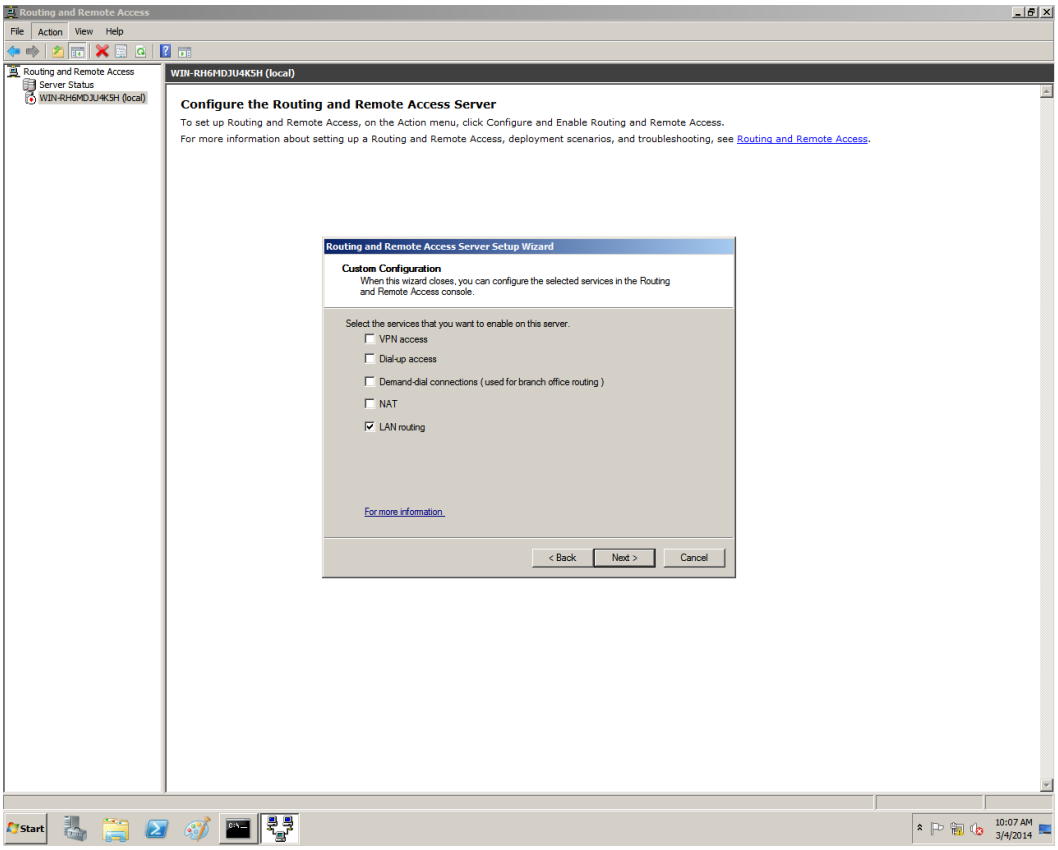
Lab 6.3 Activating Routing and Remote Access in Windows Server 2008

Connect Workstation 1 to a Switch – Connect Server to the same Switch – Connect other NIC on Server to second Switch – Connect Workstation 2 to second Switch. Configure both NICs on Server and each NIC on each Workstation to corresponding IPs

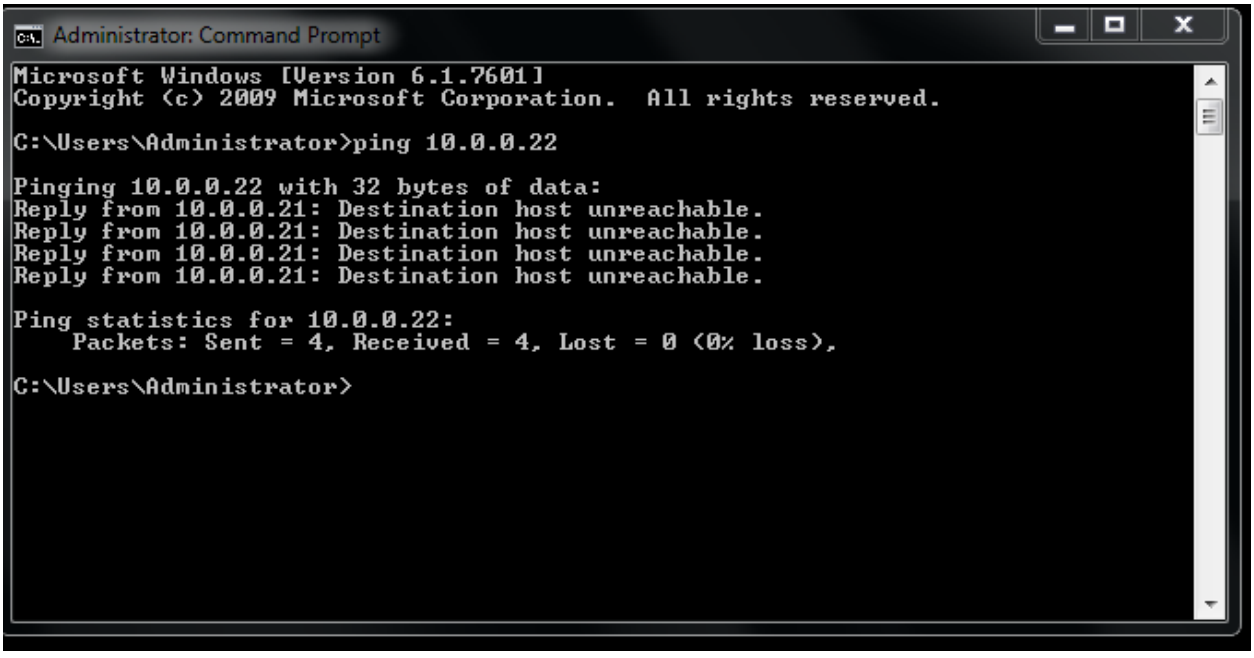
On Server – Start – Administrative Tools – Routing and Remote Access – Configure and Enable Routing and Remote Access Service.



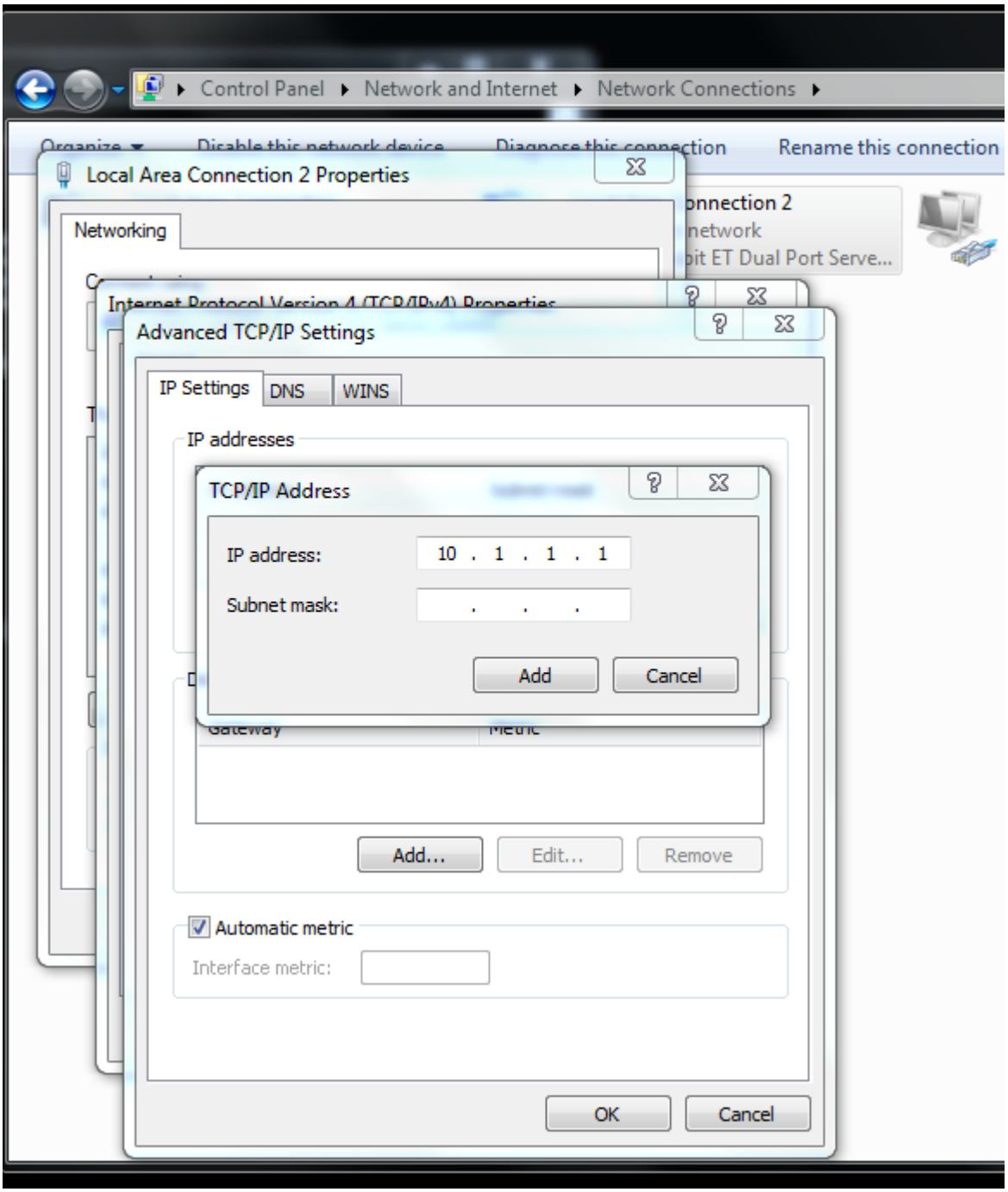
The Wizard opens – Next – Custom Configuration – Next – Click Lan Routing



Next – Finish – A dialog box opens, indicating that the Routing and Remote Access Service has been installed. Click Start Service – Log onto Workstation 1- Ping Workstation 2.

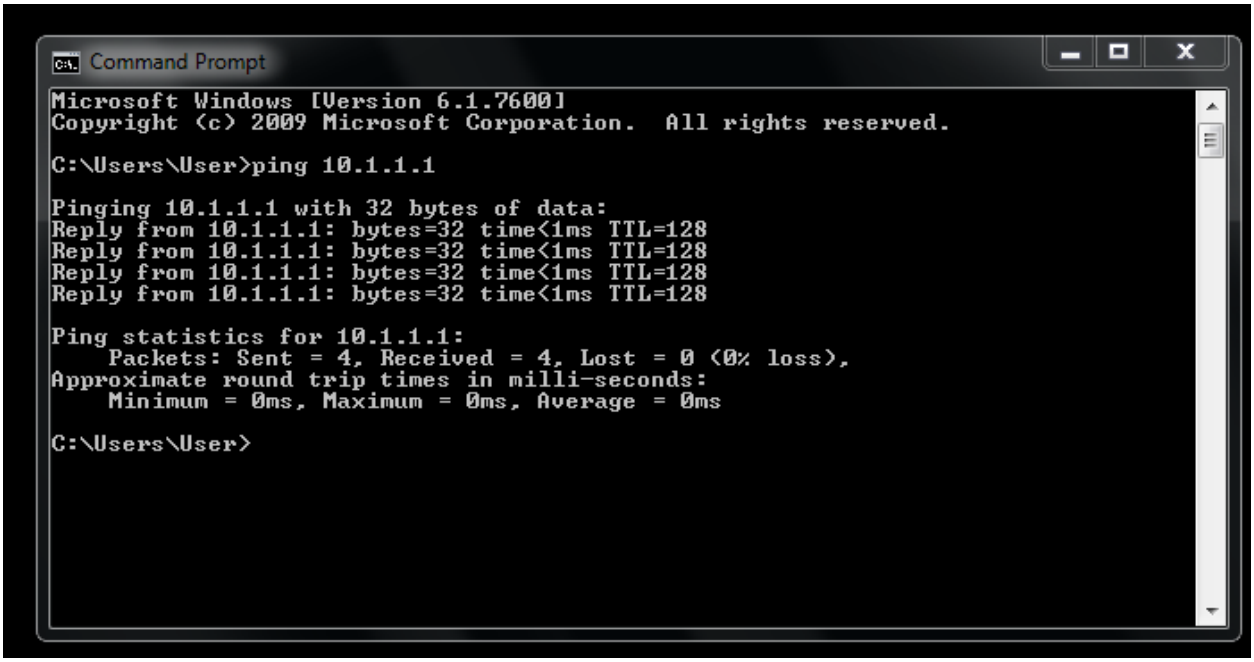


If the output does not indicate that the computer has received four replies repeat steps 9 and 10.Repeat steps 11 and 12 with Workstation 2. The Server is now acting as a router. Now configure IP address on Workstation 2. Double click TCP/IPv4 – Advanced – Add – Type 10.1.1.1 in the IP box.

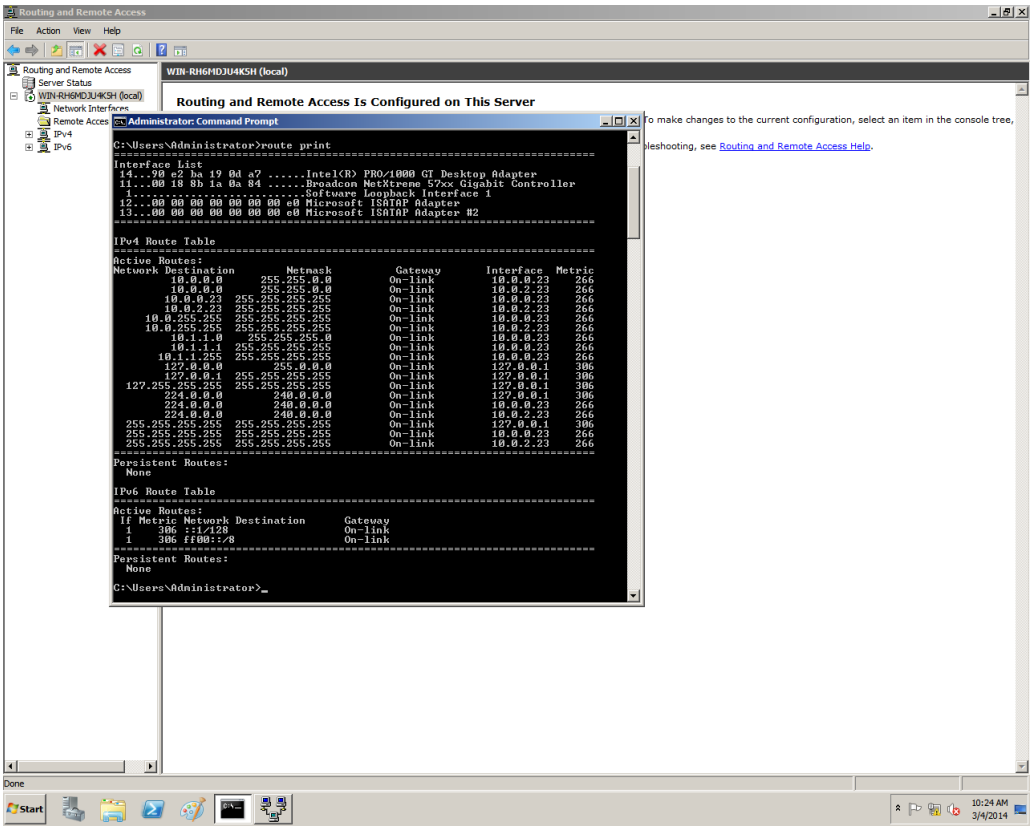


Add – OK

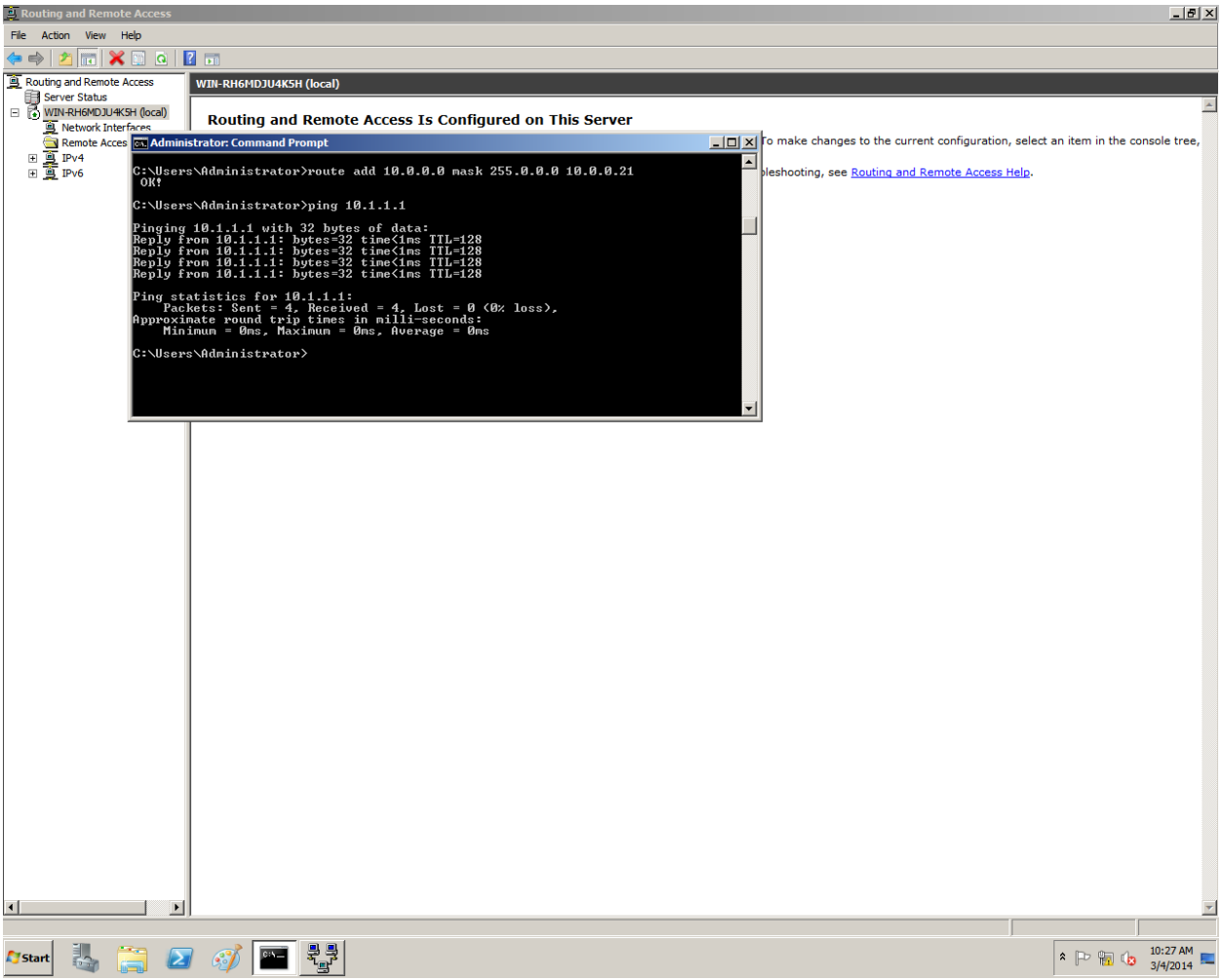
Workstation 1 – Ping 10.1.1.1 - Enter



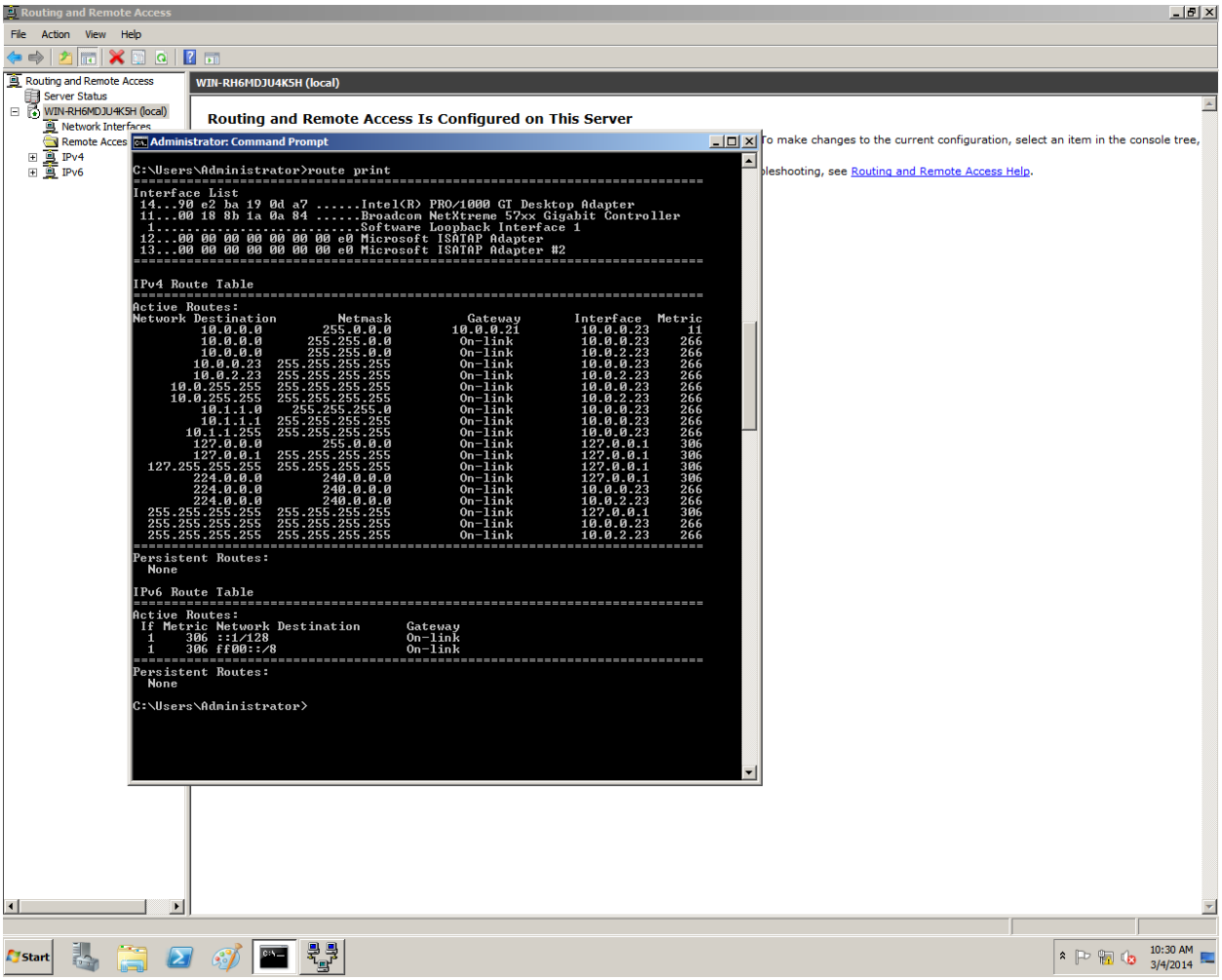
Workstation 2 – Command Prompt – **route print** – Enter



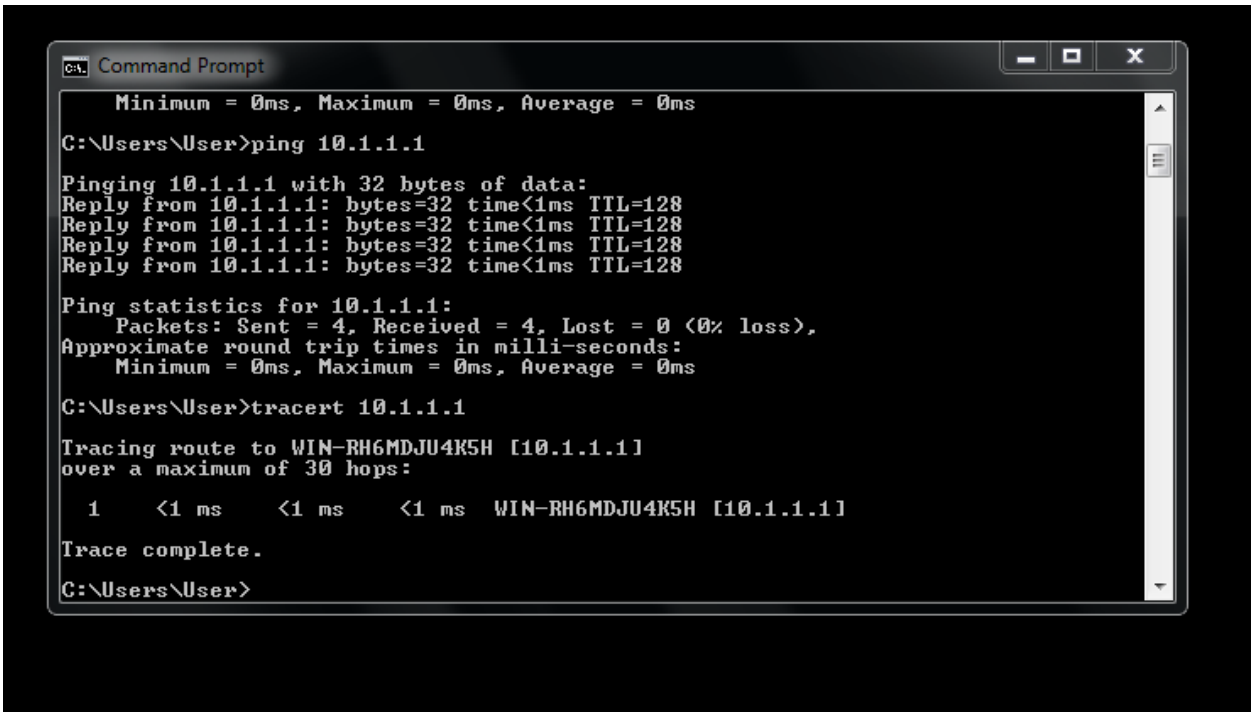
Recall that when you pinged in step 23 the computer responded with “Destination host unreachable” Now configure a static route on Server so that Workstation 1 can reach 10.1.1.1. **Type route add 10.0.0.0 mask 255.0.0.0 172.16.1.2** and Enter – Ping 10.1.1.1



Command Prompt – **route print** - Enter



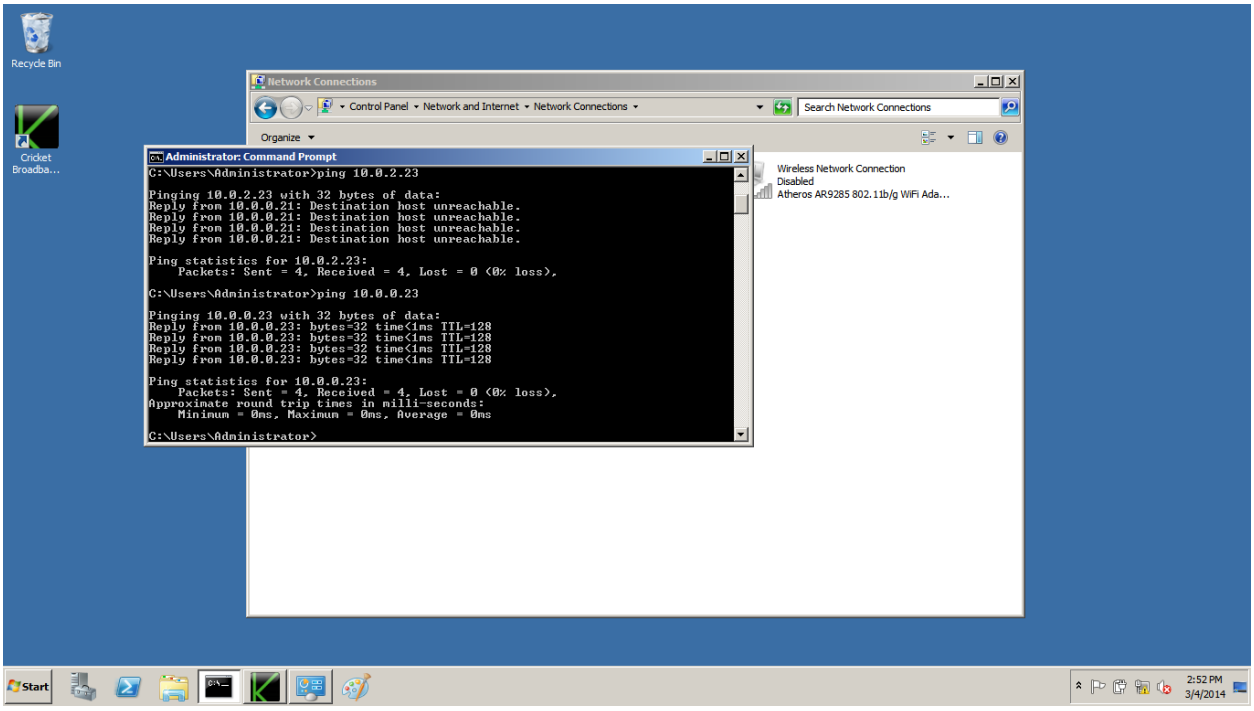
Workstation 1- Ping 10.1.1.1



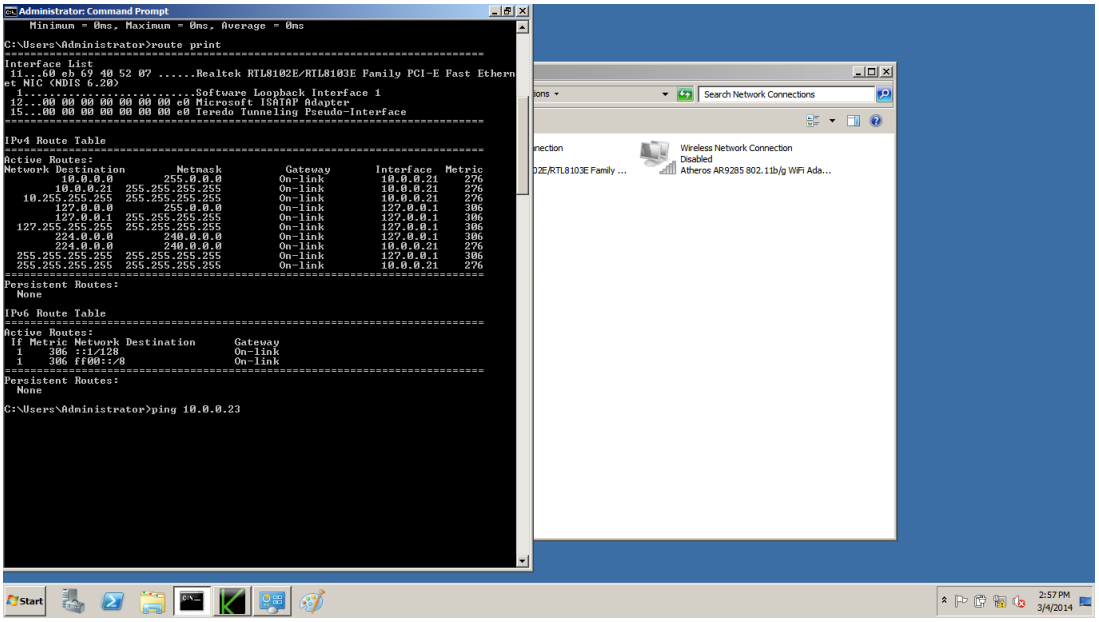
Log off the three computers

Lab 6.4 Activating a Routing Protocol in Windows Server 2008

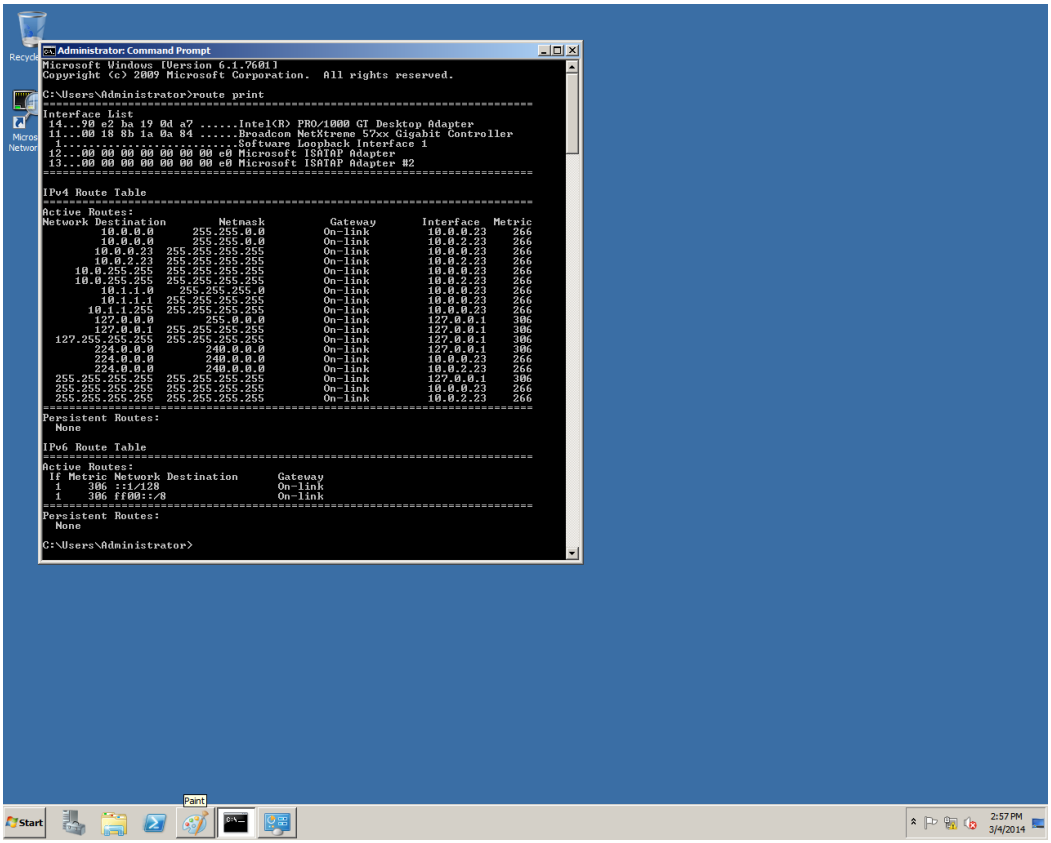
Connect each of the NICs in Server 1to separate switches. Connect the NIC in Server 2 to one of the switches. Server 2 Ping other server



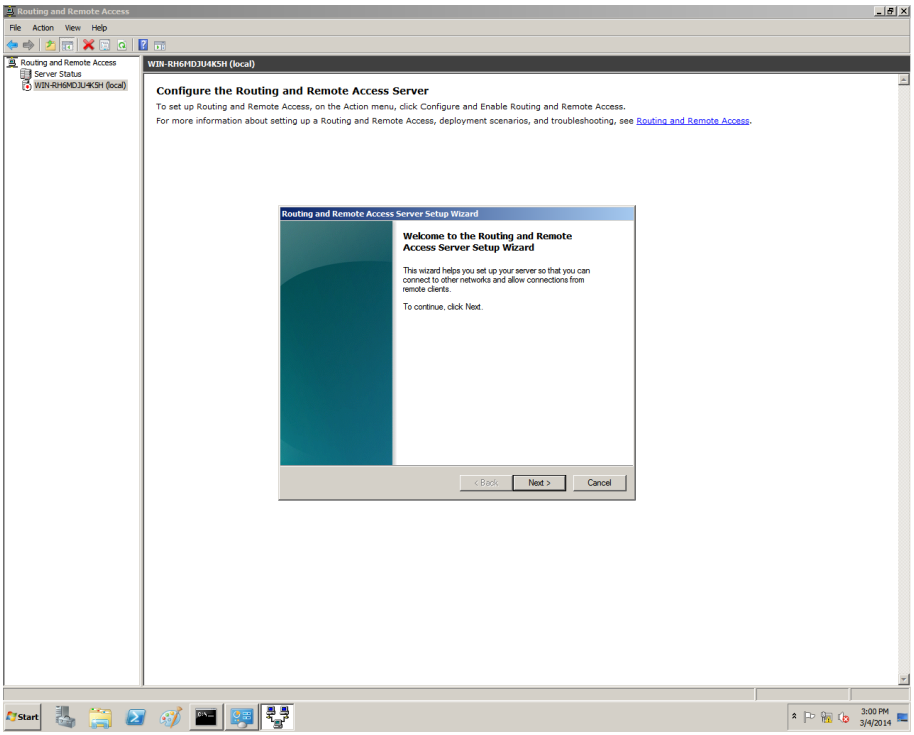
Server 2 is plugged into the wrong switch – Plug into other switch – Ping Server 1s other NIC, it is unreachable. **Type route print**



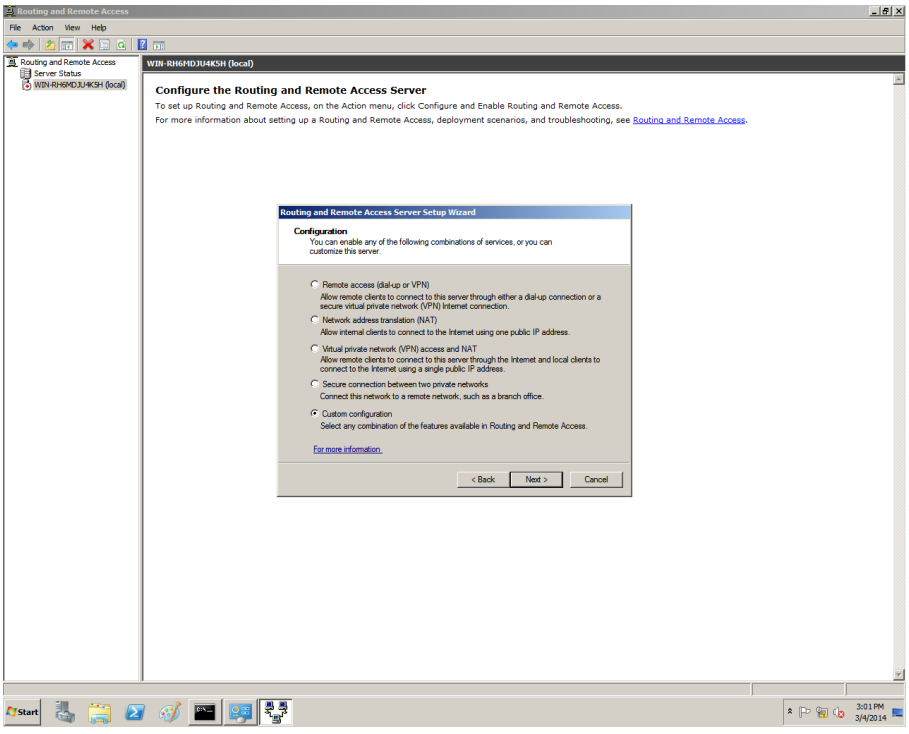
Server 1 – Command Prompt – Type **route print** –



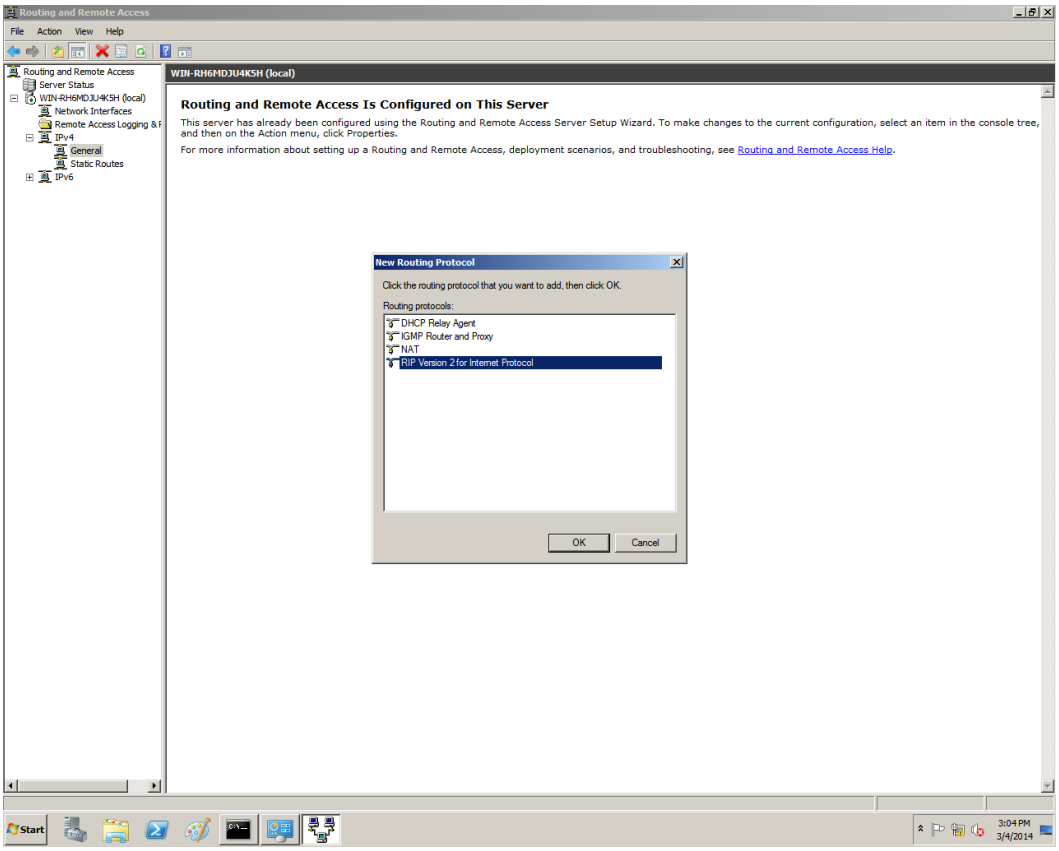
Click Start – Administrator Tools – Routing and Remote Access – In left pane select Server 1 – Action on the menu bar – Configure and Enable Routing and Remote Access. Setup wizard appears.



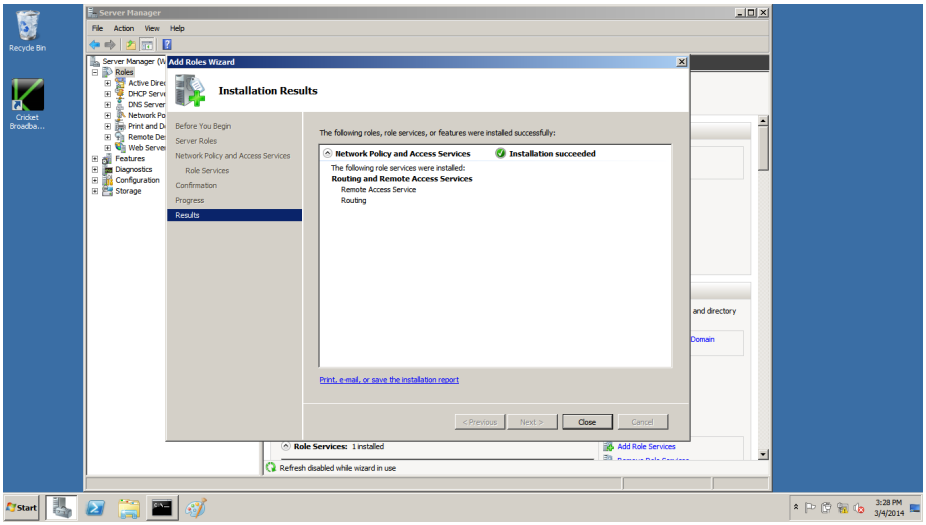
Next – select Custom Configuration – Next



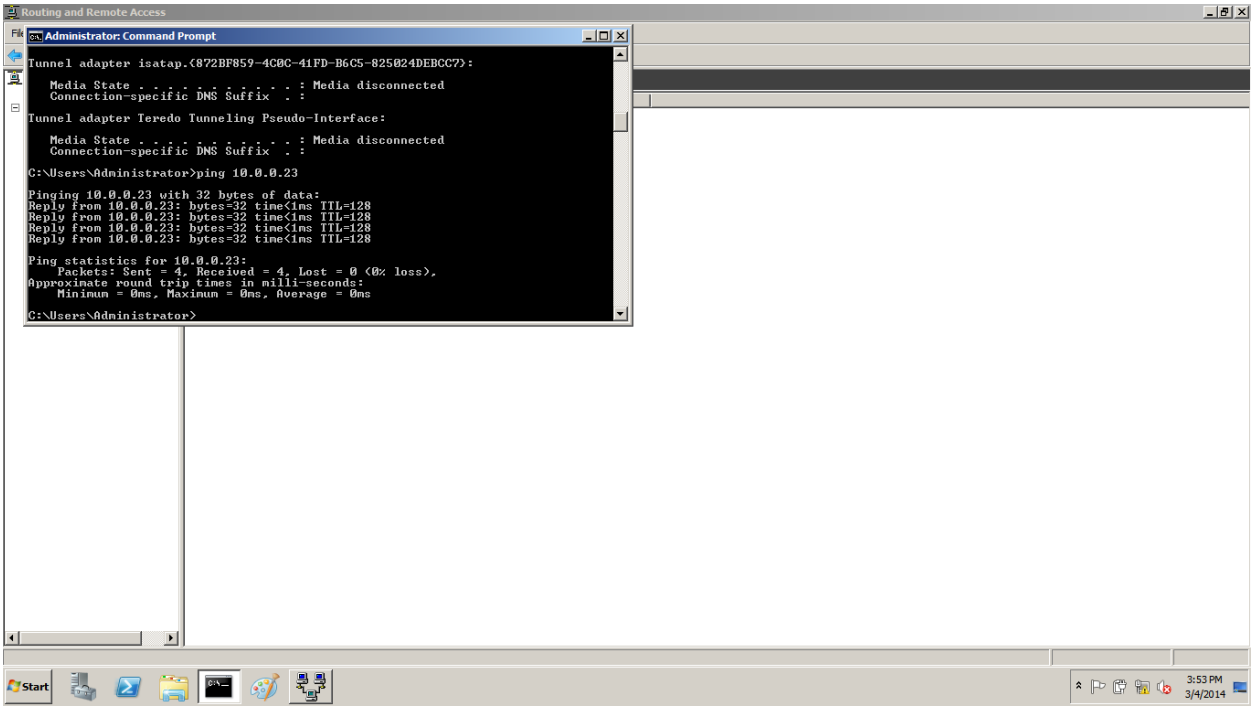
Click LAN routing check box –Next – Finish Click Start service – In left pane click plus sign (+) a tree appears – click plus sign (+) next to IPv4 node – right click General – New Routing Protocol



Click RIP Version 2 for Internet Protocol – OK –Right click the New RIP icon – New Interface – Click Local Area Connection – OK – Repeat steps 21 through 23 for Local Area Connection 2 –

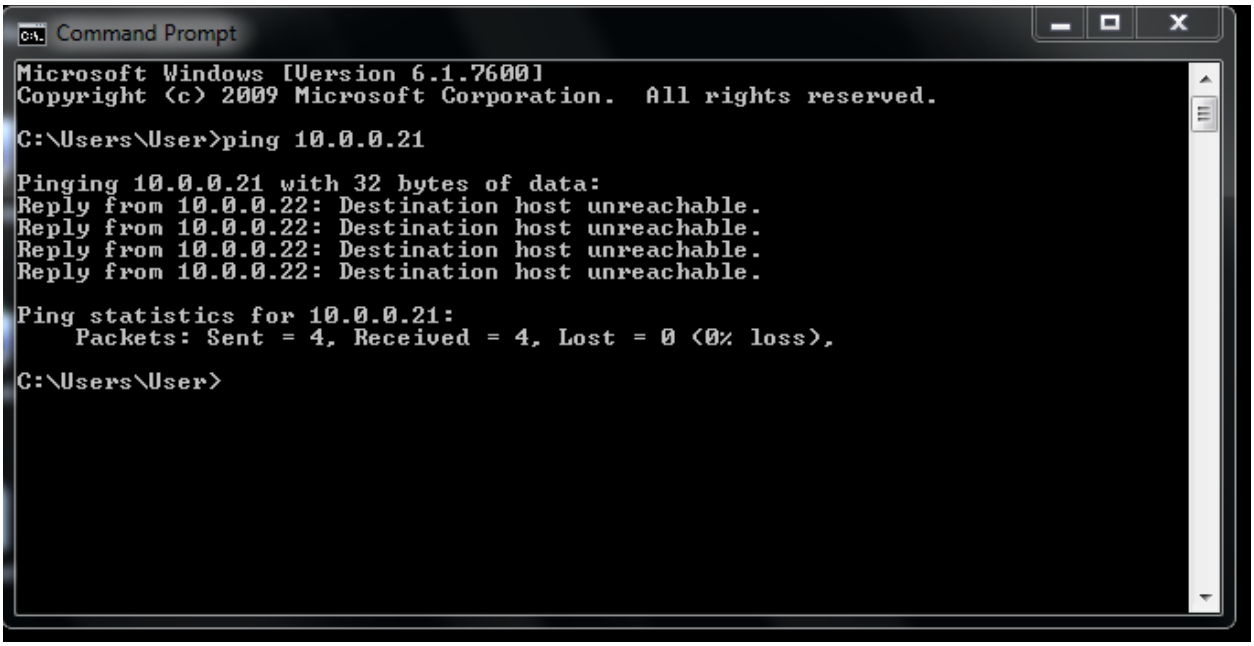


All Tasks – Restart – Enable Routing and Remote Access on Server 2 – Repeat steps 11 through 23 – RIP icon – Show Neighbors – Server 2 Ping

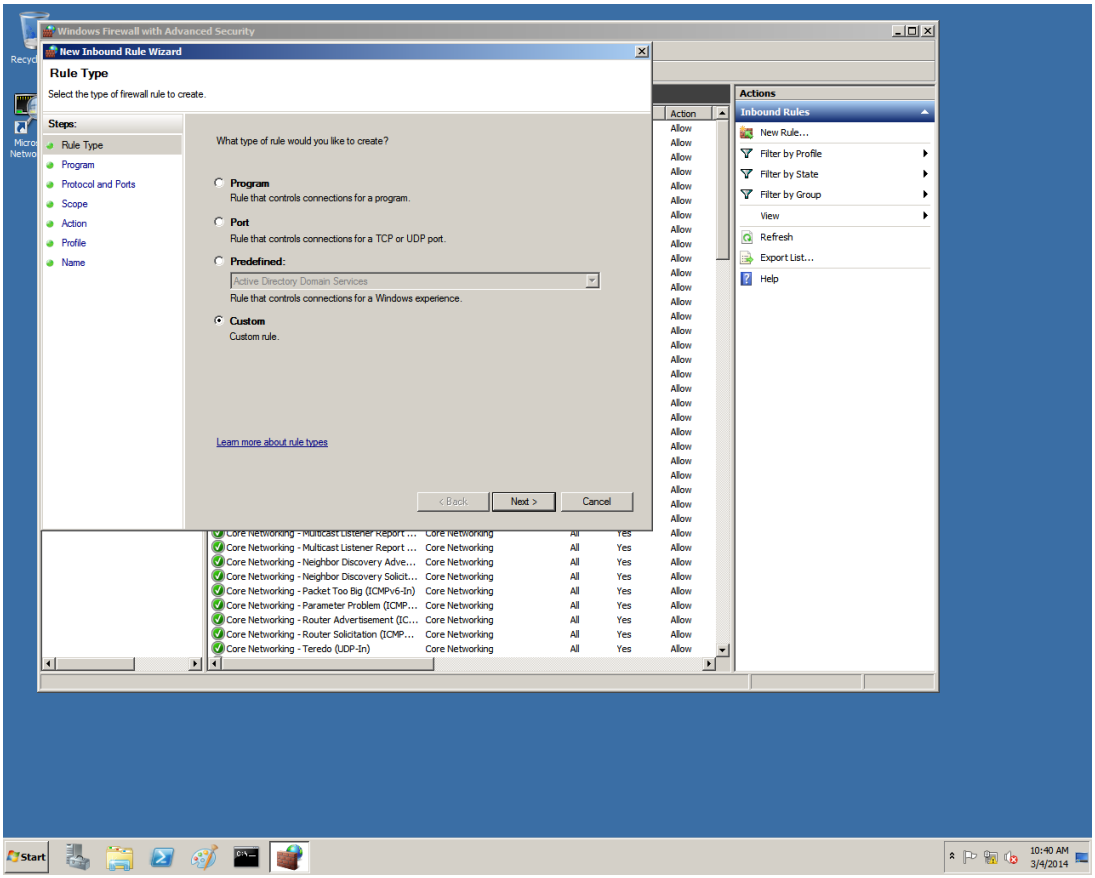


Lab 6.5 Configuring a Bridging Firewall

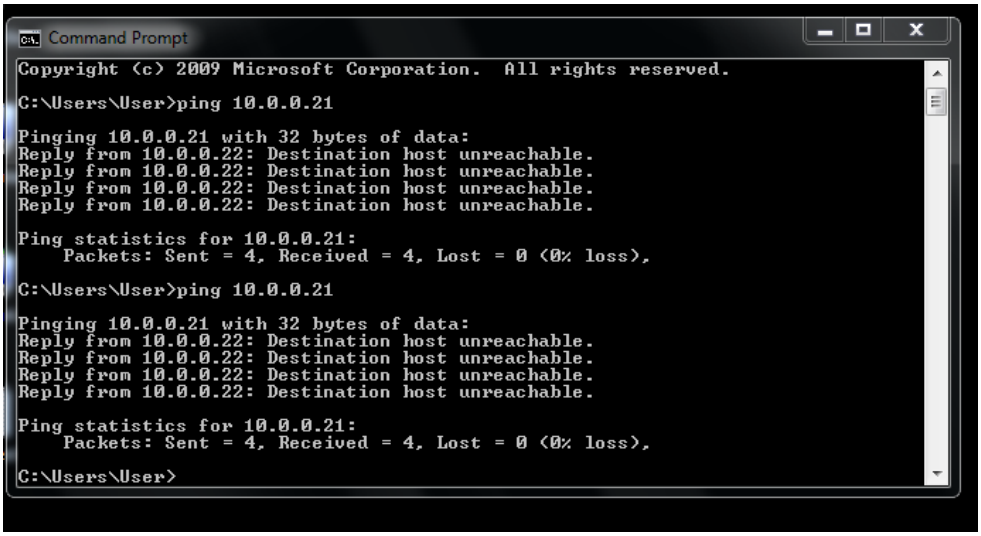
Ping Workstation 2 from workstation 1



Now configure Server 1 as a firewall. Administrative Tools – Windows Firewall with Advanced Security. Right click Inbound Rules and click New Rule – Custom –Next



– All Programs – Next – select ICMPv4 – Next – Block the connection – Next – Next – Name the Rule Ping Block – Finish - Workstation1 Ping



Joseph Martinez

Networking I: Network +

CNG – 124

Chapter Seven Labs

Topologies and Ethernet Standards

Lab 7.1 Pricing WAN Services

Lab 7.2 Connecting to an Internet Service Provider in Windows Server 2008

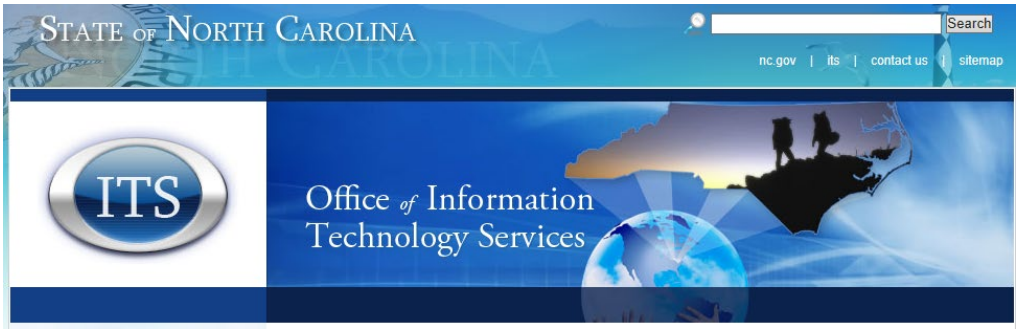
Lab 7.3 Connecting to a Cisco Router with Telnet

Lab 7.4 Configuring a Cisco Router with HyperTerminal

Lab 7.1 Pricing WAN Services

Silvernet Wide Area Network (WAN) Services

Tier	From	To	Rate	Amount
1	0	20	Monthly	$99.40
2	20.01	40 Gigabytes	Monthly	$198.82
3	40.01	80 Gigabytes	Monthly	$397.64
4	80.01	1600 Gigabytes	Monthly	$795.30
5	1600.01	320 Gigabytes	Monthly	$1,590.56
6	320.01	640 Gigabytes	Monthly	$3,181.13
7	640.01	1280 (1 TB) Gigabytes	Monthly	$6,362.25
8	1.25 TB	2.5 TB	Monthly	$12,724.50
9	2.5 TB	5+ TB	Monthly	$25,448.98



WAN Rate Summary

One-Time Charges	
Broadband Installation Fee	**$100.00**
FT1 — Nx10mb Installation Fee	**$500.00**

Recurring Charges				
	WAN Core	Transport*	Enterprise CPE	TOTAL**
DSL Broadband	—	$90.00	$76.00	**$166.00**
FR 256k	$182.00	$222.00	$166.00	**$570.00**
FR T1	$182.00	$423.00	$166.00	**$771.00**
Ethernet 10mb	$546.00	$620.00	$279.00	**$1,445.00**
Ethernet 20mb	$546.00	$834.00	$279.00	**$1,659.00**
Ethernet 50mb	$546.00	$1,012.00	$279.00	**$1,837.00**
Ethernet 100mb	$546.00	$1,115.00	$279.00	**$1,940.00**
MAN 100mb	$546.00	$94.00	$710.00	**$1,350.00**

Lab 7.2 Connecting to an Internet Service Provider in Windows Server 2008

Connect to the Internet Wizard

The Connect to the Internet Wizard simplifies the process of connecting an individual computer running Windows Server 2008 to the Internet. Through the Connect to the Internet Wizard, you can specify the name of an Internet Service Provider (ISP) along with information that the ISP provides, such as a telephone number, user name, and password.

There are a variety of ways to start the Connect to the Internet Wizard, including:

• Start any program that requires an Internet connection when no Internet connection has yet been configured. An example of such a program is Internet Explorer.

• Open Network and Sharing Center, click Set Up a Connection or Network, click Connect to the Internet, and then click Next. Network and Sharing Center can be opened in a variety of ways, including through Control Panel.

• Open Internet Options, and on the Connections tab, click the Setup button. Internet Options can be opened in a variety of ways, including through Internet Explorer (Tools menu) and through Control Panel\Network and Internet\Internet Options. You can use Group Policy to make this button unavailable.

Making the Setup Button (in Internet Options) Unavailable

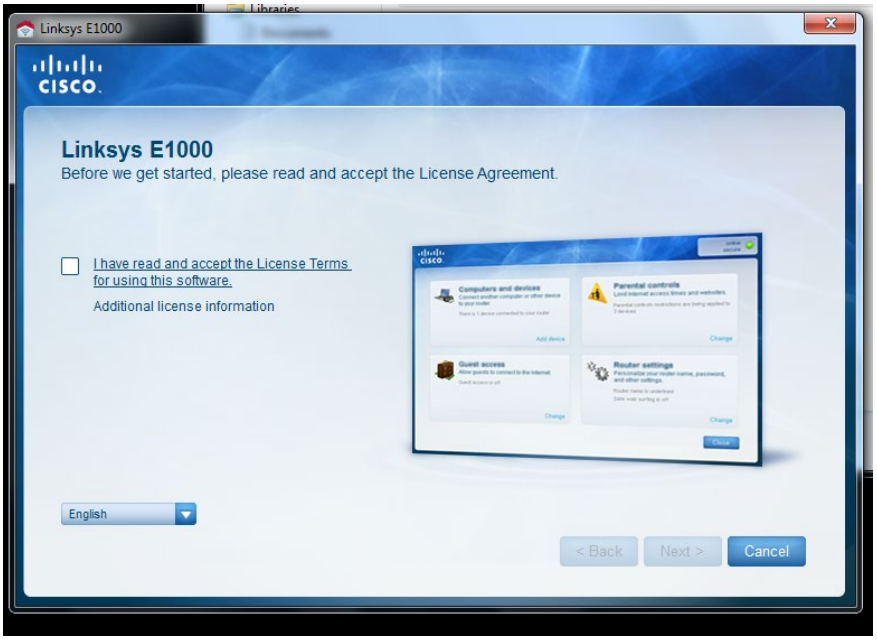
You can make the Setup button (on the Connections tab in Internet Options, as described in the previous list) unavailable. To make the Setup button unavailable, in Group Policy, in User Configuration under Policies (if present), in Administrative Templates\Windows Components\Internet Explorer, find the Group Policy setting, Disable Internet Connection Wizard. Enable this setting. Note that this policy makes the Setup button unavailable, but does not prevent the Connect to the Internet Wizard from running.

Lab 7.3 Connecting to a Cisco Router with Telnet

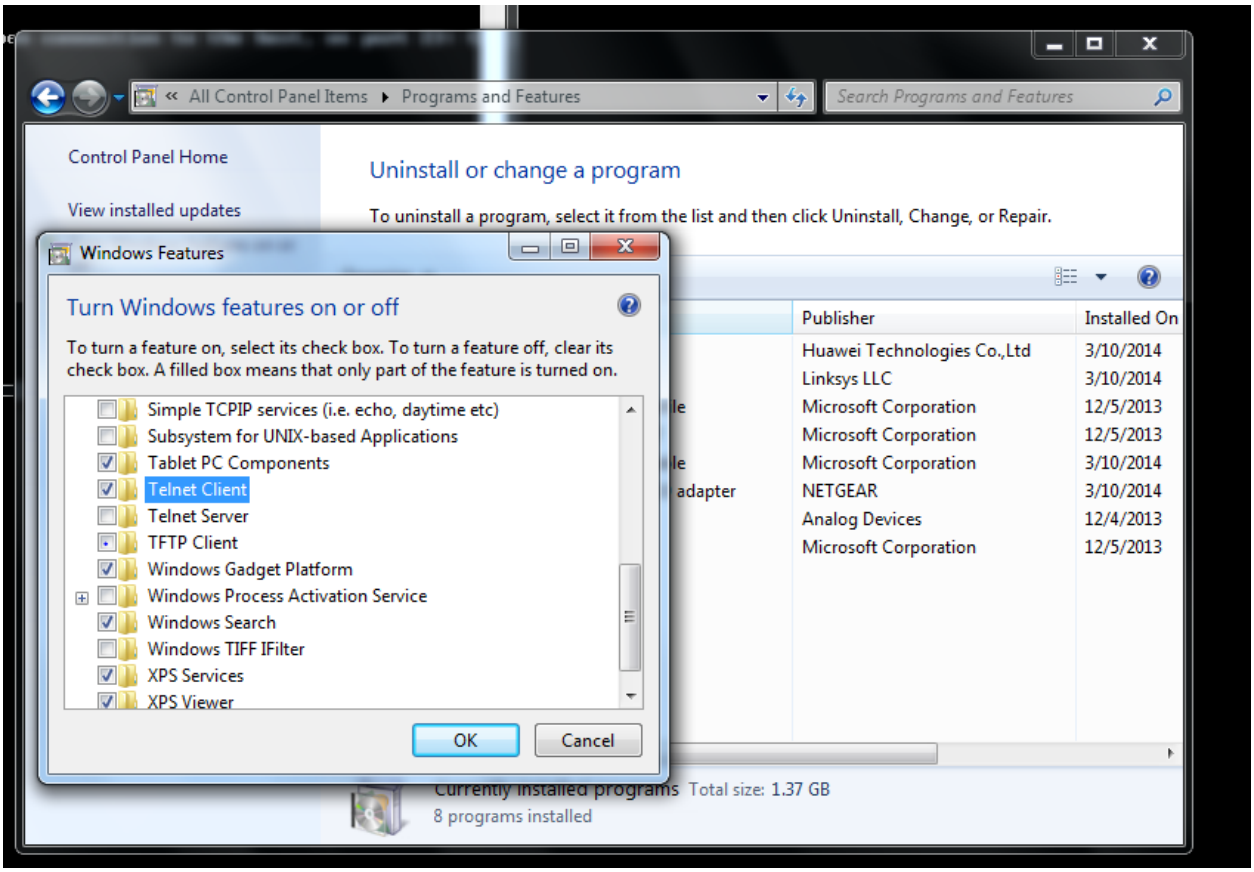
Connect one end of the straight-through cable to the Windows computer and connect the other end to the switch. Connect the other cable between the switch and the first Ethernet port on the

router.CMD – type **telnet**, the Telnet client opens. Connect to the router by typing routers IP address **open** 192.168.1.1. Enter. A password prompt appears. Enter the routers password – **Enter.**

Install software



Next – enter privileged mode – Enable – Enter – Type show running-config to examine the routers current running configuration.



Quit –Enter - Exit

Lab 7.4 Configuring a Cisco Router with HyperTerminal

Configuring a Cisco Router should not be a problem if one has had a bit of computer experience. GUI setup programs are included with the smaller routers. For the purposes of this article we will discuss using a terminal window to configure the Cisco Router.

1. Determine what type of network, WAN or VPN you need to configure. Gather IP addresses, the network protocol, subnet mask, and any addresses of gateways that may be needed, and write this information down. These are all bits of information that may be required for proper setup of a Cisco Router.
2. Connect the Cisco Router and the PC together with the cable provided. Turn the PC on.
3. Navigate to Hyperterminal if you are running Windows XP, this is done by going to Start >> Programs >> Accessories >> Communications >> Hyperterminal. For any other operating system, navigate to the appropriate Hyperterminal emulation program.
4. Configure the new connection by naming it Cisco and use the default Com 1 Port, set the baud rate to 9600. You will do this by filling out the appropriate boxes that appear.

5. Click OK and you are in the routers console. Power up the router and it will show the boot up screen in the console window. This is set up mode. You may use this set up mode to configure the router, or continue on to configure the router with a terminal window.
6. If you want to use the terminal window interface, type n and press enter. You will now see a screen with router shown. This is user mode which will not allow you to make changes. If a router name has been previously assigned, it will be shown. “Router” will be used in place of “router name” in these instructions.
7. Type enable and hit enter. You should now see router#, this means you are in privileged mode; however, you can only view information in this mode. You cannot change how the router works or what information it uses in this mode.
8. Type configure terminal and press enter, router(config)# should now be seen on your screen. This is Global Configuration Mode, you will use it to change the information the router operates with.
9. Type ? at the prompt and a list of commands will be shown. Type the name of the command ?, and a description of what the command does will appear. The first command typed should probably be show ?, this will show a list of show commands such as IP protocols and ARP.
10. You may now enter commands at this point to configure different aspects of the interface between the router and its components. It is beyond the scope of this article to explore all possible network scenarios and their configurations.

Review Questions

1. Which of the following elements of the PSTN is most likely capable of transmitting only analog signals?
   Local Loop
2. Which of the following WAN topologies comes with the highest availability and the greatest cost?
   Full Mesh
3. A customer calls your ISP's technical support line, complaining that his connection to the Internet usually goes as fast as 128 Kbps, but today it is only reaching 64 Kbps. He adds that he has tried dialing up three different times with the same result. What type of connection does this customer have?
   ISDN
4. What is the purpose of ISDN's D channel?
   To carry call session information
5. Suppose you work for a bank and are leasing a frame relay connection to link an automatic teller machine located in a rural grocery store with your bank's headquarters. Which of the following circuits would be the best option, given the type of use this automatic teller machine will experience?

SVC

6. On an ISDN connection, what device separates the voice signal from the data signals at the customer premises?
   Terminal Adapter
7. Which WAN technology operates at Layer 3 of the OSI model?
   None of the above
8. What technique enables DSL to achieve high throughput over PSTN lines?
   Data Modulation
9. Suppose you establish a home network and you want all three of your computers to share one broadband cable connection to the Internet. You decide to buy a router to make this sharing possible. Where on your network should you install the router?
   Between the cable modem and the workstations
10. How does ATM differ from every other WAN technology described in this chapter?
    It uses fixed-sized cells to carry data
11. You work for an Internet service provider that wants to lease a T3 over a SONET ring. What is the minimum Optical Carrier level that the SONET ring must have to support the bandwidth of a T3?
    OC1
12. Name two asymmetrical versions of DSL
    ADSL and VDSL
13. What technique does T1 technology use to transmit multiple signals over a single telephone line?
    Time Division Multiplexing
14. Where on the PSTN would you most likely find a DSLAM?
    In a remote switching facility
15. The science museum where you work determines that it needs an Internet connection capable of transmitting and receiving data at 12 Mbps at any time. Which of the following T-carrier solutions would you advise?
    Ten T1s
16. A local bookstore that belongs to a nationwide chain needs a continuously available Internet connection so that staff can search for the availability of customer requests in the database stored at the bookstore's headquarters. The maximum throughput the store needs is 768 Kbps. Which of the following options would best suit the store?
    ADSL
17. What part of a SONET network allows it to be self-healing?
    Its double-ring topology
18. Which of the following may limit a DSL connection's capacity?
    The distance from the customer to the carrier's switching facility
19. You work for a consulting company that wants to allow telecommuting employees to connect with the company's billing system, which has been in place for 10 years. What do

you suggest as the most secure and practical means of providing remote LAN access for this application?
Dialing into a terminal server that is connected to the same network as the billing system server

20. Why is broadband cable less commonly used by businesses than DSL or T-carrier services?
    Because most office buildings are not wired with coaxial cable
21. You're troubleshooting a problem with poor performance over a WAN connection at your office. Looking at the smart jack, you see the Tx light is blinking green and the Rx light is not illuminated. What can you conclude about the problem?
    It is likely due to faults in your service provider's network.
22. Your company has decided to order ADSL from its local telecommunications carrier. You call the carrier and find out that your office is located 17,000 feet from the nearest CO. Given ADSL's potential throughput and your distance from the CO, what is the maximum downstream throughput you can realistically expect to achieve through this connection?
    2 Mbps
23. In which of the following situations would you use RDP?
    To establish a VPN between your home workstation and your office LAN
24. You have decided to set up a VPN between your home and your friend's home so that you can run a private digital telephone line over your DSL connections. Each of you has purchased a small Cisco router for terminating the VPN endpoints. Which of the following protocols could you use to create a tunnel between these two routers?
    L2TP
25. A VPN is designed to connect 15 film animators and programmers from around the state of California. At the core of the VPN is a router connected to a high- performance server used for storing the animation files. The server and router are housed in an ISP's data center. The ISP provides two different T3 connections to the Internet backbone. What type of connection must each of the animators and programmers have to access the VPN?
    Any type of Internet connection

7.1 Lab Manual Review Questions

1. Which of the following best describes the function of a CSU?
   c. It determines a digital signal and ensures connection integrity.

2. Which of the following WAN topologies is the least expensive to build?

   d. Star

3. Which of the following WAN topologies gives the most redundancy? C. Full-mesh

4. What is the maximum number of channels that a single T1 can contain?

b. 24

5. What is the maximum throughput of a T3 line?

b. 45 Mbps

6. What does DSL use to achieve higher throughput than PSTN over the same lines?

b. Data modulation

7. Which of the following WAN links is most reliable?

d. Sonet

8. Which of the following is the most expensive type of connection to install and lease?

d. T3

Lab 7.2

1. What are the two differences between PPP and SLIP?
   a. SLIP can handle only asynchronous transmission, whereas PPP can handle both asynchronous and synchronous transmission. C. SLIP cannot carry Network layer protocols other than TCP/IP, whereas PPP can carry any Network Layer protocol.
2. Which of the following is one primary difference between PPP and PPTP?
   b. PPP encapsulates traffic according to its original Network layer protocol, whereas PPTP masks PPP traffic as IP-based data.
3. Which of the following is the most secure remote access protocol? d. PPTP
4. Which of the following best describes the asynchronous communications method? B. Data that is transmitted and received by nodes does not have to conform to any timing scheme.
5. If your ISP uses DHCP to assign TCP/IP information to a dial up connection, which of the following must you still specify in your connection parameters? C. The network's DHCP server address.

Lab 7.3

1. What CLI command would you use to test a connection between a router and another device on the network? B. ping
2. What direct serial connection can be used to access routers that are not already part of a network? B. Telnet

3. A router determines logical addressing information by interpreting the contents of an incoming _____. D. Frame
4. Routers operate at which layer of the OSI model? B. 3
5. Of the following task, which one are Routers incapable of performing? D. Interpreting MAC address information.

Lab 7.4

1. What symbol does the CLI use to show privileged mode? C. #
2. Why can't all routers just be configured through an Ethernet port? A. The Ethernet port must first be made a member of the network.
3. What kind of routers operate on the Internet backbone? D.Gateway
4. What CLI command is used to enter privileged mode? D. Enable
5. Which CLI command shows a list of available commands? A ?

Joseph Martinez

Networking II: Network +

CNG – 125

Chapter Eight Labs

Wireless Networking

Lab 8.1 Adding a Windows Client to a Wireless Network

Lab 8.2 Adding a Linux Client to a Wireless Network

Lab 8.3 Installing a Wireless Router

Lab 8.4 Investigating Wireless Access Points

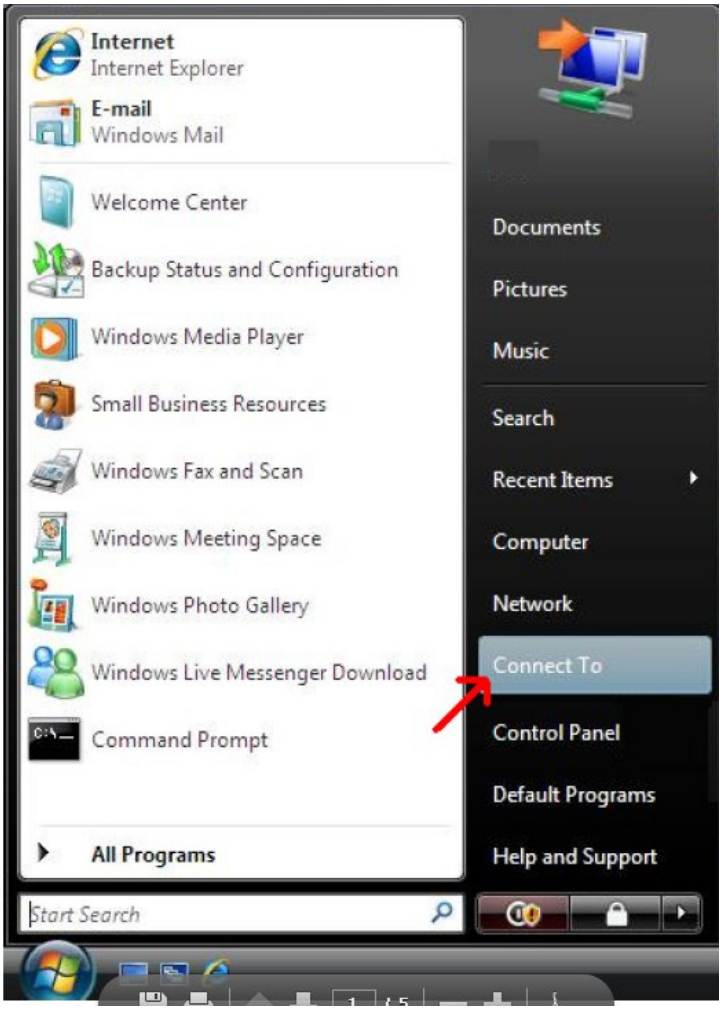
Lab 8.1 Adding a Windows Client to a Wireless Network

How To Install the Client for Microsoft Networks:

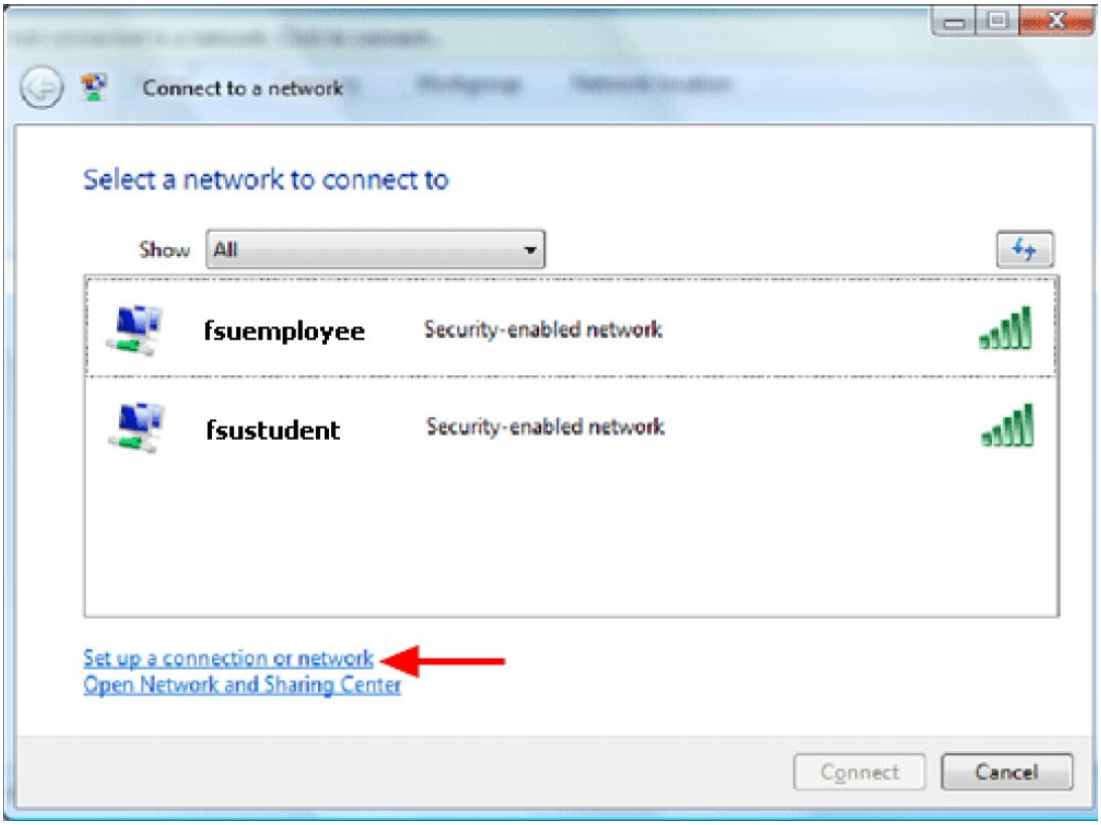
To function with FSU's wireless networks, it is recommended that users purchase a wireless network card that supports 802.11 a/b/g or 802.11a/g. FSU requires all network users to install and update an anti-virus program. A virus or spy-ware on a network will cause severe performance issues. You should also install the latest Windows Updates from Microsoft. For virus and software update information, visit: http://www.frostburg.edu/computing/cmpages

Windows Vista and Windows 7: Install the network card and install the drivers. Neither Windows Vista nor Windows 7 require the Wireless Utility that comes with your network card. However, if the utility has already been installed, the following instructions can still be used to configure your system.

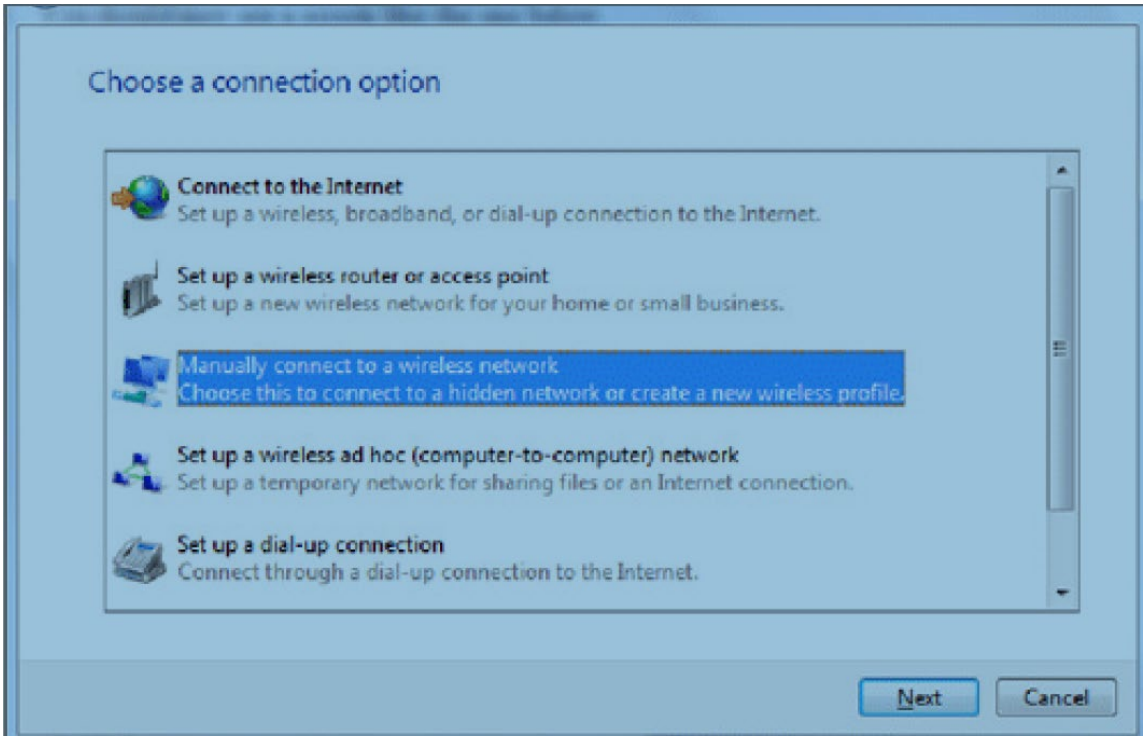
Click on Start then choose Connect To from the Windows Vista or Windows 7 Desktop



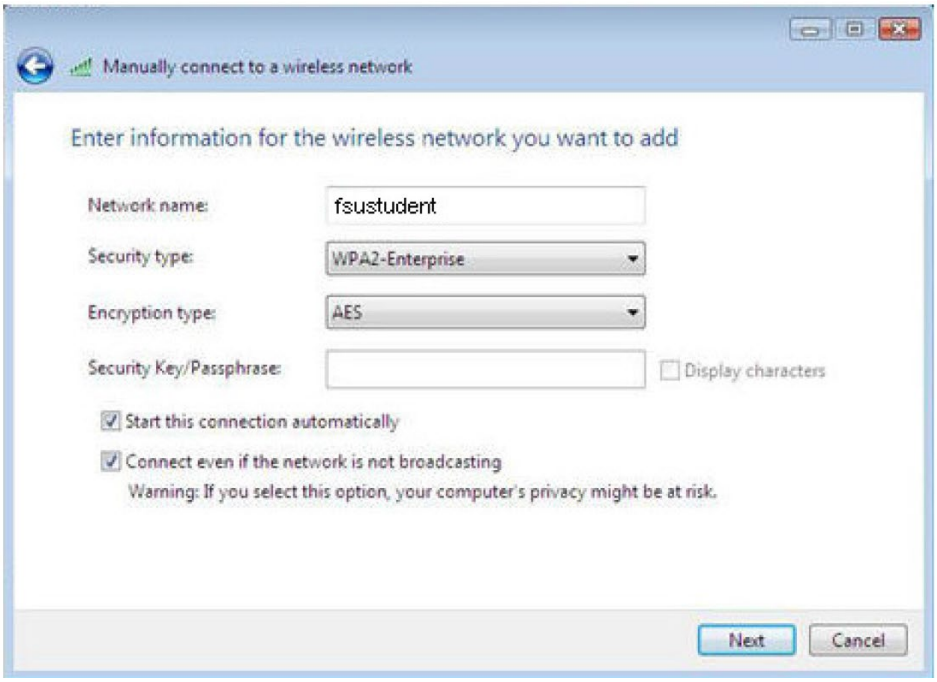
You will then see a screen similar to the one below:



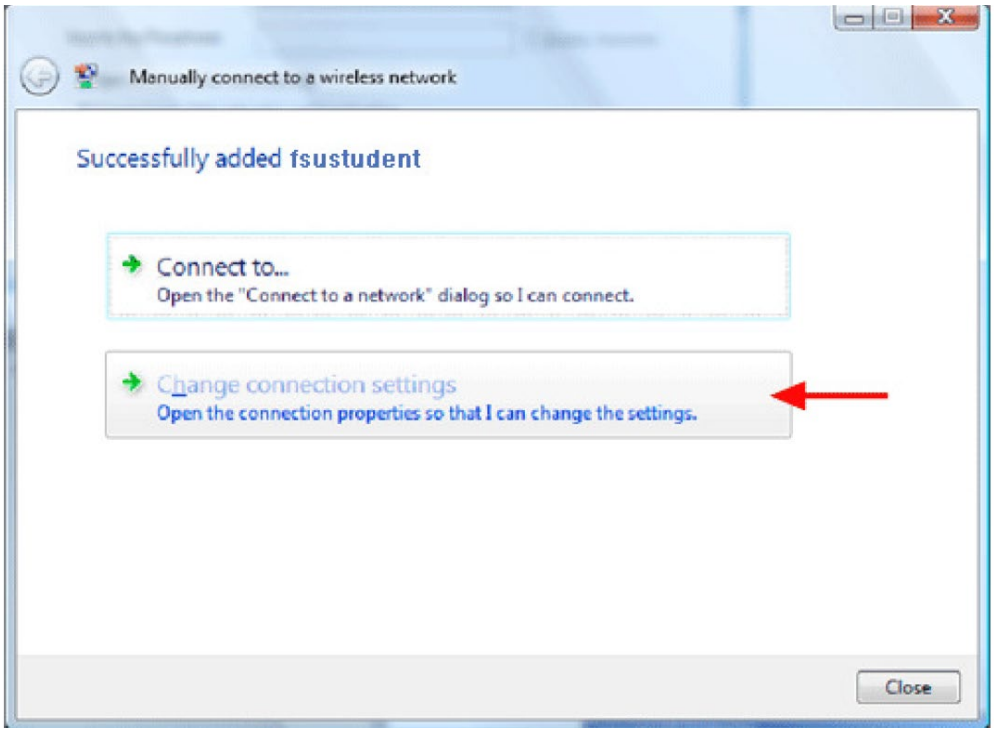
Click on Set up a connection or network, then click on Manually connect to a wireless network



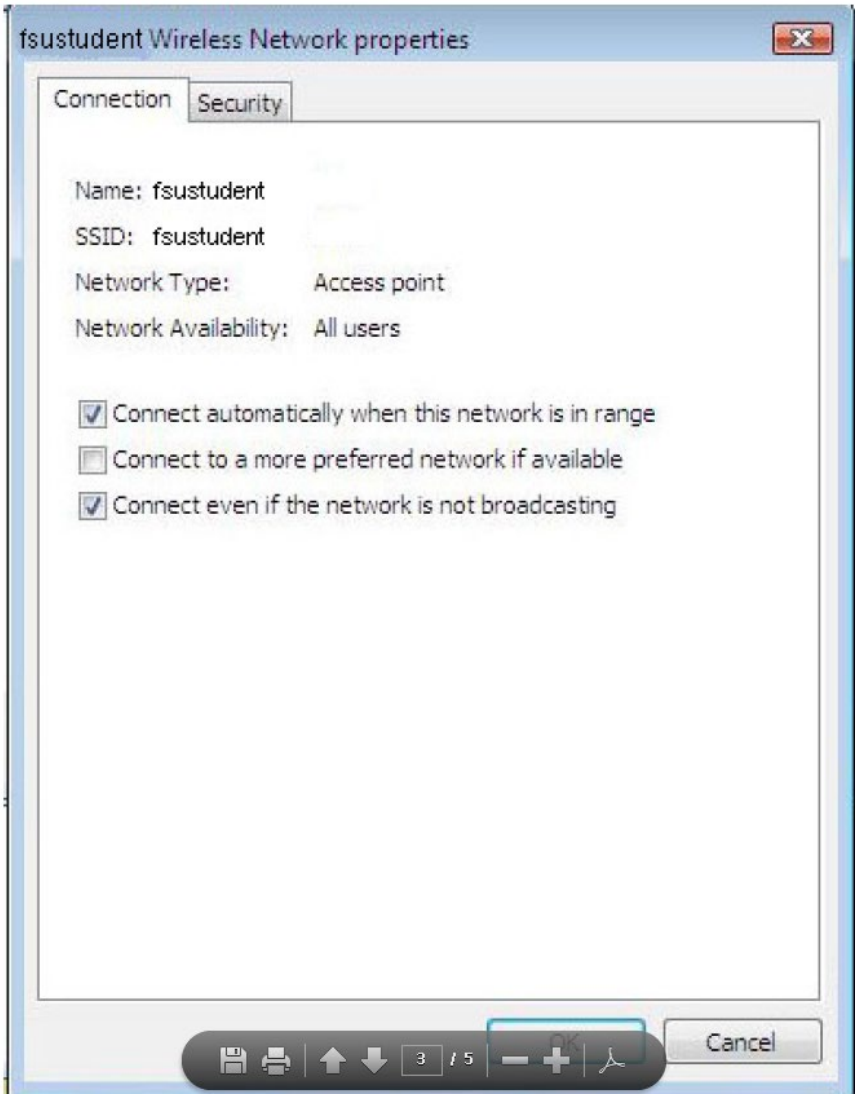
Type fsustudent (lower case) in the Network name field. Choose WPA2-Enterprise as the Security type. Choose AES (or TKIP if your wireless card doesn't support AES) as the Encryption type. Then click Next to continue.



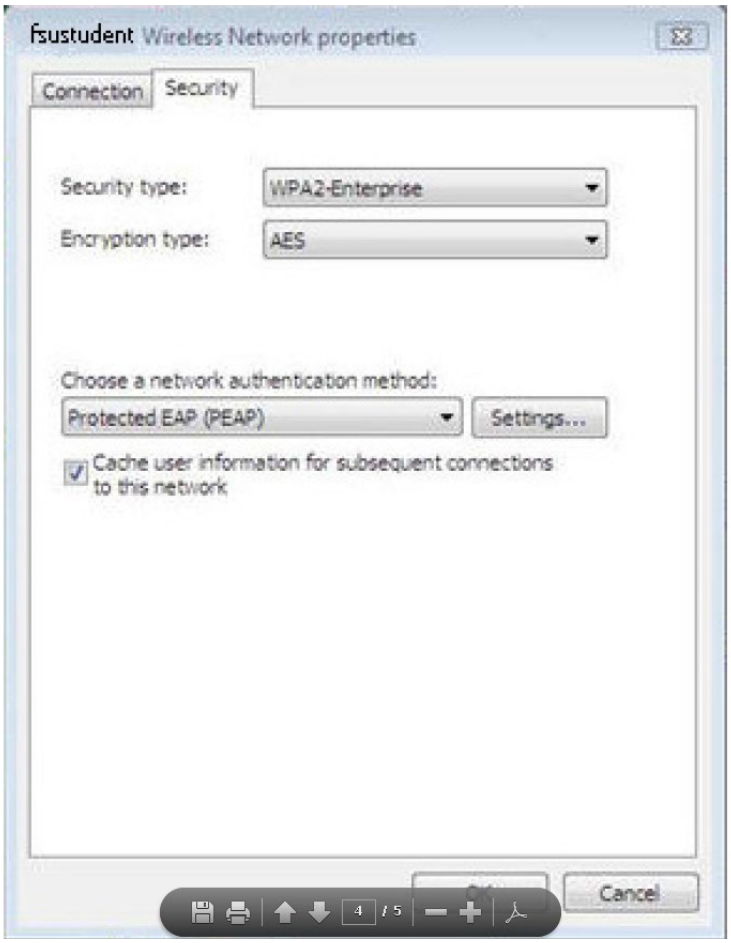
You will see a message that you have successfully added fsustudent. On this screen, click Change connection settings



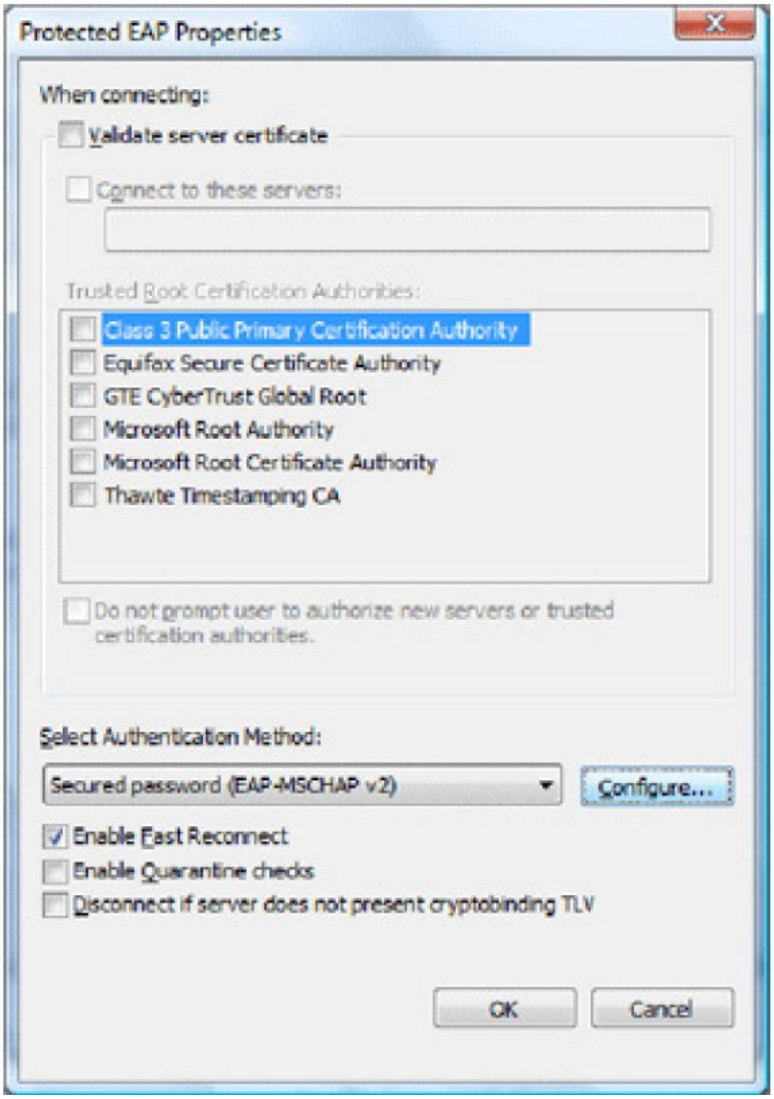
Uncheck the box next to Connect to a more preferred network is available then click on the Security tab.



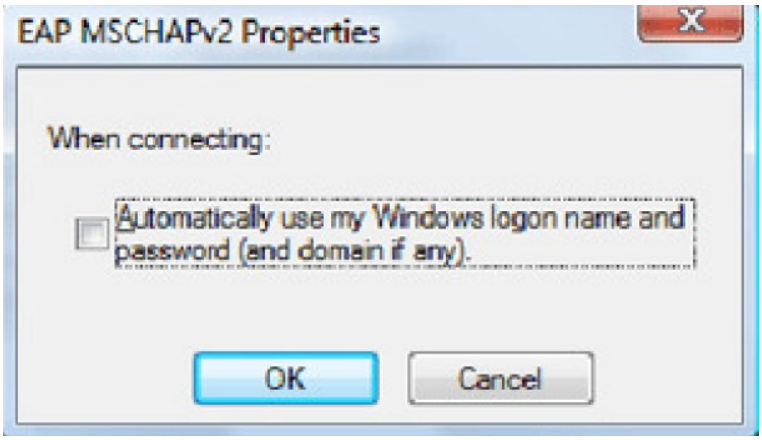
Choose Protected EAP (PEAP) as the authenication method. If more than one person will be using the computer you are configuring, uncheck the box next to Cache user information for subsequent connections to this network. Next, click the Settings button



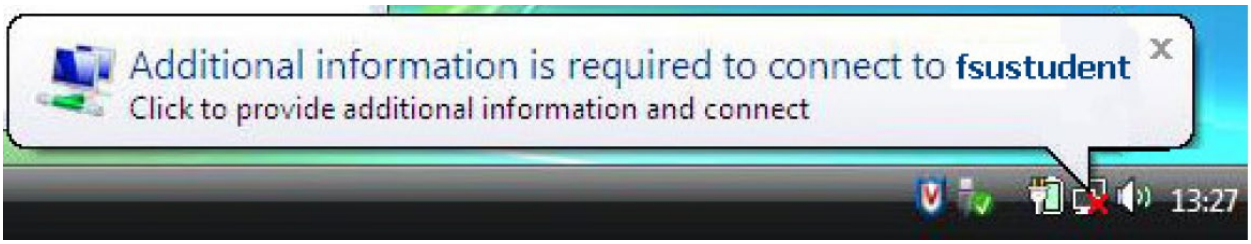
On the following screen, remove the check mark in the box next to Validate server certificate, check the box next to Enable FastReconnect, and in the Select Authentication Method box, select Secure password (EAP-MSCHAP v2). Then click the Configure button.



It is very IMPORTANT that you UNcheck the box next to the Automatically use my Windows logon name and password. If you fail to remove this check you will not be able to connect to the wireless.



Click the OK button until you have closed all dialog boxes. To finish connecting to the fsustudent wireless network, you will need to enter your FSU credentials. You will see a connection bubble appear near your System Tray. Click on this bubble and enter your username (ex: jdoe) and password to connect. Enter FROSTBURG or frostburg.edu as the Logon domain.



Please visit http://www.frostburg.edu/computing/cmpages to register your wireless computer on the network. The registration process will ensure that your system is clean of viruses and spyware. If you have already registered the computer via the wired port, you may not need to re-register.

Lab 8.2 Adding a Linux Client to a Wireless Network

Not all wireless NIC cards work with Linux. For this reason, do your homework. You can find hardware compatibility lists for Wireless Tools quite easily on popular search engines.

Wireless NIC manufacturers are notorious for changing the chip sets on their cards depending on the price of the components. They then supply different drivers with each new card to make them work. It is possible to buy cards with the same model number from the same vendor with very different circuitry. Frequently Linux drivers for the new cards are unavailable. Always check the compatibility lists before buying your wireless hardware.

The Linksys WMP11 wireless card is a good example of this confusion. The original version of the card used the Intersil Prisim chip set, which worked with Linux, but the newer version 2.7 (Broadcom chip set) and version 4 (InProComm chip set) do not. Even so, the original WMP won't work without upgrading the firmware.

In recent years it has become possible to use regular Windows drivers with Linux NICs. This is discussed in more detail in the section titled "Configuring Linux with Incompatible Wireless NICs". The method requires an understanding of Linux Wireless Tools which is covered beforehand, but first, let's cover some wireless networking essentials to provide some background

Note: Don't be fooled. The fact that your Linux system can detect your NIC doesn't mean that it is compatible. Always check the Internet for Linux compatibility listings so that you'll know how to proceed.

A wireless access point (WAP) is a device that acts as the central hub of all wireless data communications. In the most common operating mode (Infrastructure mode), all wireless servers communicate with one another via the WAP, which is usually connected to a regular external or integrated router for communication to the Internet. WAPs are, therefore, analogous to switches in regular wired networks.

Servers can communicate with one another without a WAP if their NICs are configured in Ad Hoc mode, but this prevents them from communicating with any other communications path. For that, you need a WAP on your network.

Lab 8.3 Installing a Wireless Router

Setting up a wireless router is straightforward as long as you have a PC with a wireless network adapter, as well as an active high-speed Internet connection. You might also need a computer with a wired network adapter and router-specific setup software, which is typically included on a disc packaged with your router or available for download on the router manufacturer's support site.If you have a router labeled with a Windows 7 logo and you are using Windows 7, setting things up should be quick if you follow the steps below.

1. Connect the wireless router to your modem using an ethernet cable. 2. Connect your wireless router to a power source. Wait about a minute, and then continue to the next step. 3. Click the network icon in the notification area; the icon should look like a series of vertical bars, or a tiny PC with a network adapter alongside it. 4. Select your wireless network from the list of available networks to complete the setup process. By default, your network name will be the name of your router manufacturer.

Although newer routers connected to Windows 7 PCs are generally simple to set up, some problematic wireless routers might require a little more attention. If you can't set up your wireless router as explained above, follow the directions included with it. **Chances are, you'll need to use one of the following two strategies.**

Set Up Your Router Using the Setup Software

1. Make sure that your wireless router is completely disconnected from the modem, the computer, and the power source. 2. On your PC, insert the disc that came with your router, or download and run the latest version of the router's software from the vendor website. 3. Follow the on-screen instructions. The setup routine will ask you to connect components (including your modem and PC) in a certain order, and it may request that you temporarily connect your wireless router to a computer via an ethernet cable. You will also create a wireless network name and password at this point. If something goes wrong, you may want to consider manually configuring your wireless router. Manually

Manually Configure Your Router Without Setup Software

1. Connect your wireless router to the modem, using an ethernet cable. 2. Connect the wireless router to a power source. Wait about a minute to ensure that your router is fully operational. 3. Connect the wireless router to your computer using an ethernet cable. 4. Log in to your router's Web interface by opening a browser and entering the IP address of your router into the address bar. The IP address should be listed within your router's documentation; if you can't find it, most routers use a common IP address such as http://192.168.1.1, http://192.168.0.1, or http://192.168.2.1. 5. Enter the default username

and password, which you should find within your router's documentation. Alternatively, visit Port Forward's Default Router Passwords page. 6. Use the Web interface to set up a network name and password. 7. Disconnect your computer from the wireless router and then reconnect wirelessly. Finally, check out our router tips to speed up your wireless connection.

Lab 8.4 Investigating Wireless Access Points

In computer networking, a wireless Access Point (AP) is a device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards. The AP usually connects to a router (via a wired network) as a standalone device, but it can also be an integral component of the router itself.

Chapter Eight Review Questions

1. To transmit and receive signals to and from multiple nodes in a three-storey house, what type of antenna should an access point use? A. Omnidirectional
2. Which of the following is not true about multipath signaling? B. Multipath signaling uses less energy and results in clearer reception than line-of-sight signaling.
3. You are setting up a WLAN for an insurance agency. The network includes 32 clients, three printers, two servers, and a DSL modem for Internet connectivity. What type of WLAN architecture would best suit this office? C. Infrastructure
4. Which of the following 802.11 transmission requirements contributes to its inefficiency? C. A destination node must issue an acknowledgment for every packet that is received intact.
5. In the 802.11 standard, IEEE specifies what type of access method? D. CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)
6. Suppose a user on your office network has changed the channel on which his wireless NIC communicates. Assuming the wireless connection is his only access to the LAN, what will happen when he next tries to send an e-mail? B. The e-mail program will respond with a message indicating it could not connect to the mail server.
7. What is the theoretical maximum throughput for 802.11b? 11 Mbps
8. What frequency band is used by Bluetooth, 802.11b, and 802.11g? b. 2.4 GHz
9. Your office currently runs a mix of 802.11b and 802.11g clients. Rumor has it that your company is about to merge with another company that uses a different wireless

technology. Which of the following would be compatible with what your WLAN currently runs? B. 802.11n

10. If your wireless stations are configured to perform passive scanning, what do they need from an access point to initiate association? C. A beacon frame
11. You're working on a school district's 802.11g WLAN. Within each school, several access points serve students, teachers, and administrators. So that users can move about the school with their laptops and not lose network connectivity, each of the access points must share which of the following? A. The same ESSID (extended service set identifier)
12. When a mobile user roams from access point A's range into access point B's range, what does it do automatically to maintain network connectivity? B. Reassociate with access point B
13. Which two of the following techniques help to reduce overhead in 802.11n wireless transmission? C&E. Frame aggregation and Channel bonding
14. Your organization is expanding and plans to lease 3000 square feet of space in a nearby building. Your supervisor asks you to conduct a site survey of the space. If conducted properly, which of the following will your site survey reveal? A,B,C,D. The optimal quantity and locations of access points for the WLAN, All potential sources of EMI, and The distance between each workgroup area and telco room. (All of the above)
15. Which of the following wireless technologies boasts the highest maximum theoretical throughput? D. 802.11n
16. Which of the following will help an access point's transmissions reach farther? B. Boosting its signal strength
17. Why are the 802.11b and 802.11g wireless transmission technologies more commonly used on business LANs than Bluetooth? (Choose two answers.) 802.11 signals travel farther than Bluetooth signals and 802.11 technologies transmit data at higher throughputs than Bluetooth.
18. Suppose you work for a telecommunications carrier who is looking into providing WiMAX in a suburb of a large city. A colleague suggests that your company reserve licensed frequencies from the FCC for your service. Why? A. Licensed frequencies will suffer less interference than unlicensed frequencies.
19. On your Linux workstation, you open a terminal window and type at the command prompt iwconfig eth0 key 5c00951b22. What have you done? C. Established the credentials the wireless interface will use to communicate securely with the access point
20. Which of the following types of satellites is used to provide satellite Internet access? A. Geosynchronous orbit

Lab 8.1 Review Questions

1. In which of the following ways does a wireless LAN differ from an Ethernet LAN: C. A wireless LAN uses different techniques at the Physical layer to transmit data.
2. Which of the following are potential disadvantages of wireless LANs as compared with cabled LANs? B,D. Issues such as the location of buildings and the weather can affect connectivity to wireless LAN. & Signal strength can be affected by many sources of electric noise.
3. How is a wireless NIC different from a NIC that requires a cable? A. A wireless NIC contains an antenna.
4. You have been hired as a network consultant by the East Coast Savings bank. East Coast Savings would like to implement a wireless LAN but with high standards of security. What sort of restrictions would you recommend placing on the wireless LAN? C. Wireless LAN users may surf the web, but may not access the rest of the banks network without special security software.
5. Why is a wireless signal susceptible to noise? B. Wireless transmissions cannot be shielded like transmissions along an Ethernet cable.

Lab 8.2

1. What is the administrators default account called in Linux? D. Root
2. What command line utility is replaced with Network Manager? C. ifconfig
3. Describe how you could use Network Manager to switch between networks? NetworkManager provides automatic network detection and configuration for the system. Once enabled, the NetworkManager service also monitors the network interfaces, and may automatically switch to the best connection at any given time. Applications that include NetworkManager support may automatically switch between on-line and off-line modes when the system gains or loses network connectivity.
4. What Linux command is used to test Network connections? C. ping
5. What term is used to describe when a mobile user moves out of one access points range and into the range of another? A. Reassociation

Lab 8.3

1. How is a wireless router's configuration utility usually accessed? B. Through a Web browser.
2. Why is it a good idea to change your wireless router's password? A. So other people cannot change your wireless router's settings
3. What type of connection is used to attach to the network port on a wireless router? A. None, it is wireless
4. Which of the following Wi-Fi standards has the highest effective throughput? A. 802.11g
5. Wireless access points are assigned a unique name or _____. D. SSID

Lab 8.4

1. Which network is the fastest? D. 802.11n
2. What feature eliminates the need for a separate electrical outlet for your WAP? A.PoE
3. Why is plenum-rated cable often a requirement for ceiling-mounted access point? D. In the case of a fire, they do not give off toxic fumes.
4. In an enterprise-wide WLAN, coverage can be extended across multiple access points by joining them to the same _____. D. MIM)
5. Some wireless access points can associate a client's MAC address with a port switch allowing a client to stay connected to an _____as they move throughout an area. C. RTS/CTS.

Joseph Martinez

Networking II: Network +

CNG – 125

Chapter Nine Labs

In-Depth TCP/IP Networking

Lab 9.1 Subnetting a Network

Lab 9.2 Understanding the Purpose of the Default Gateway

Lab 9.3 Understanding the TCP/IP Hosts File

Lab 9.4 Setting up an FTP Server

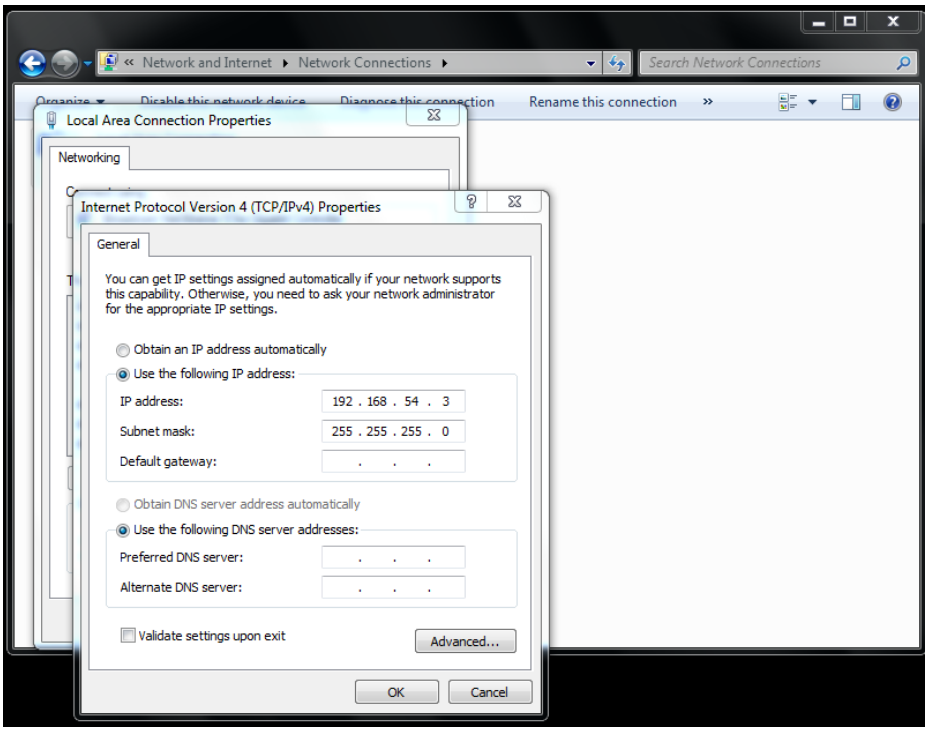
Lab 9.5 Configuring a Mail Server

Lab 9.1 Subnetting a Network

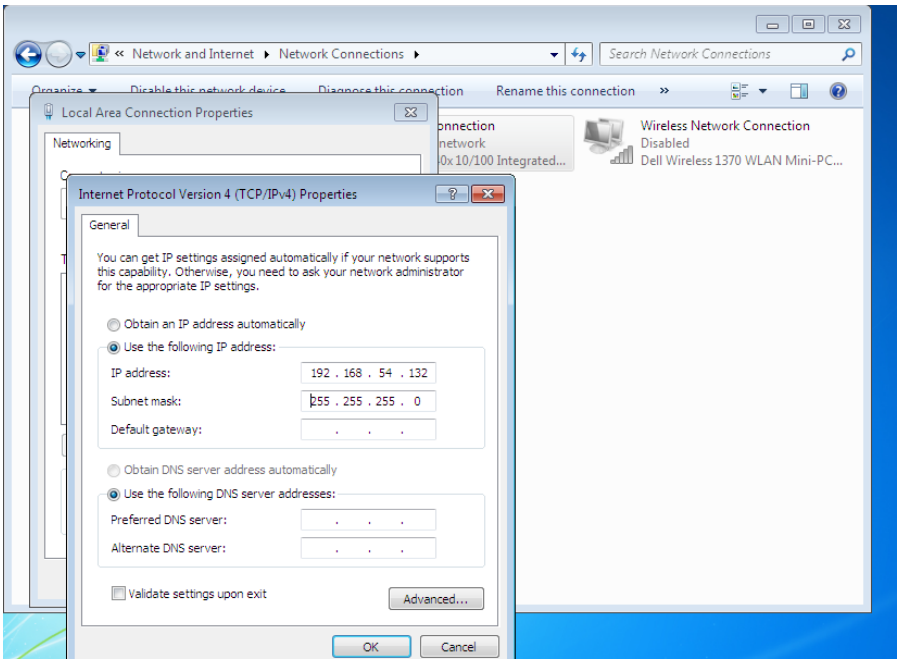
An IP address has two components, the network address and the host address. A subnet mask separates the IP address into the network and host addresses (<network><host>). Subnetting further divides the host part of an IP address into a subnet and host address (<network><subnet><host>). It is called a subnet mask because it is used to identify network address of an IP address by performing bitwise AND operation on the netmask.

A subnet mask neither works like an IP address, nor does it exist independently from them. Instead, subnet masks accompany an IP address and the two values work together. Applying the subnet mask to an IP address splits the address into two parts, an "extended network address" and a host address.

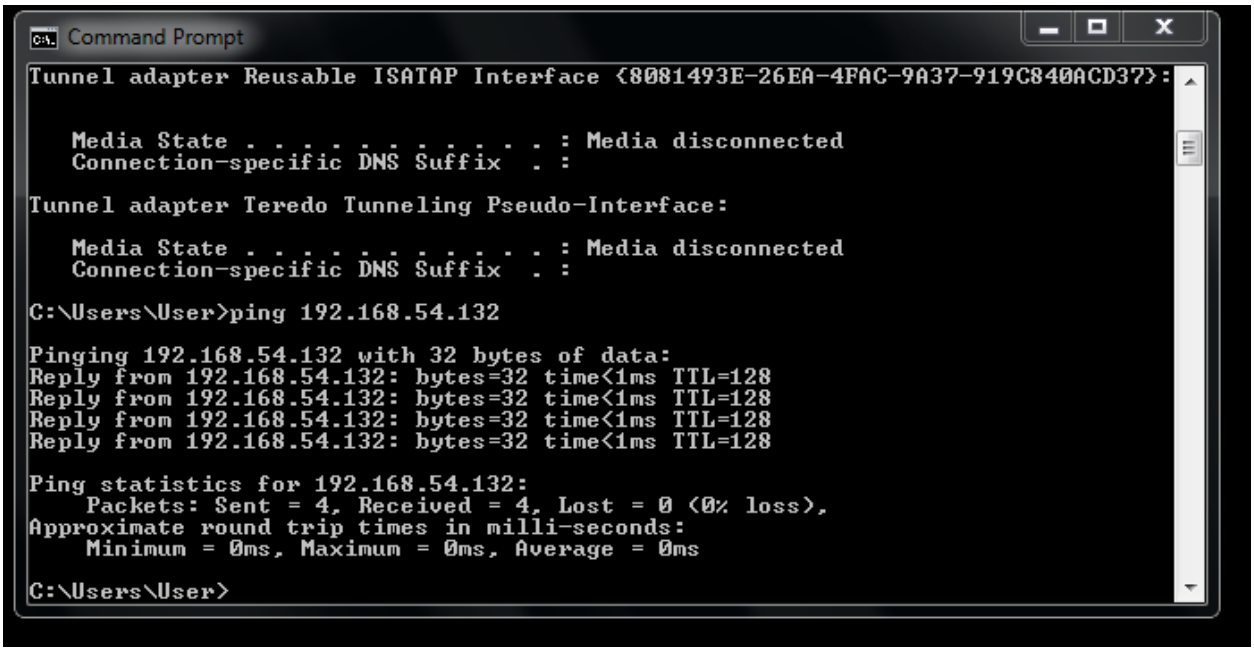
Configure workstation 1 with an IP address of 192.168.54.3, a subnet mask of 255.255.255.0, no default gateway and Firewall turned off.



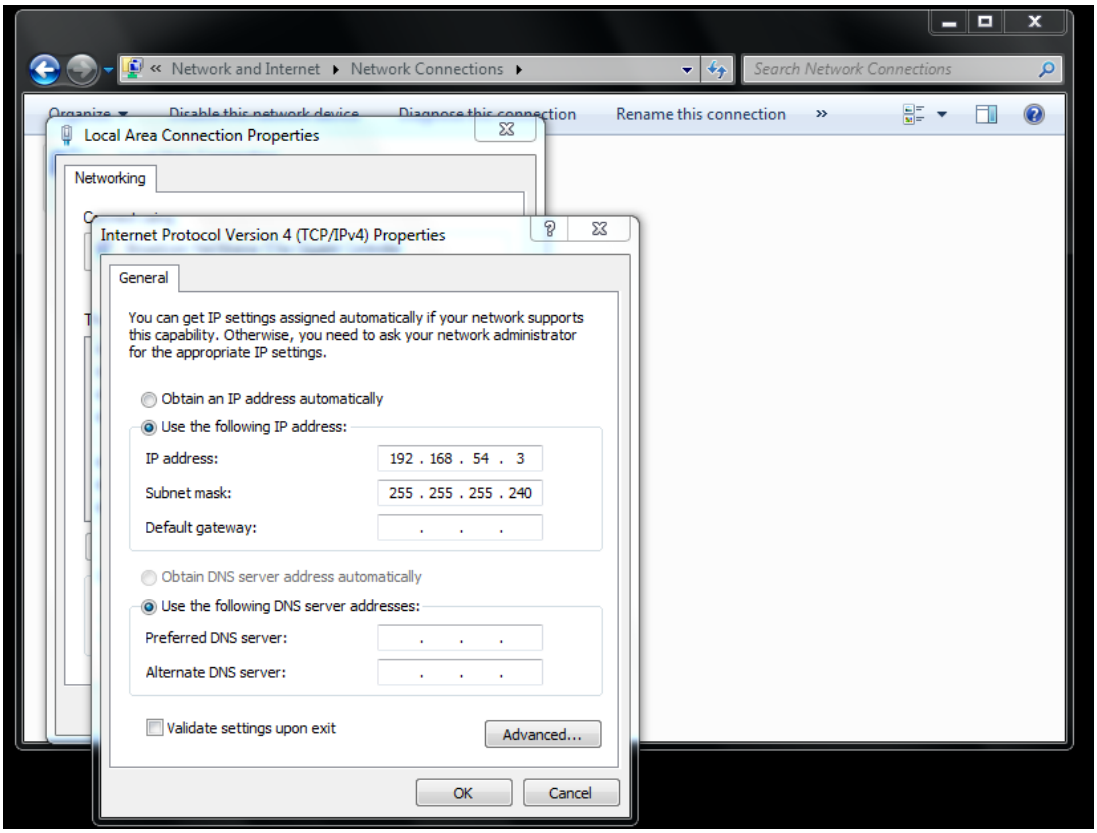
Workstation 2 with an IP address of 192.168.54.132 with subnet mask, default gateway and Firewall the same as Workstation 1.



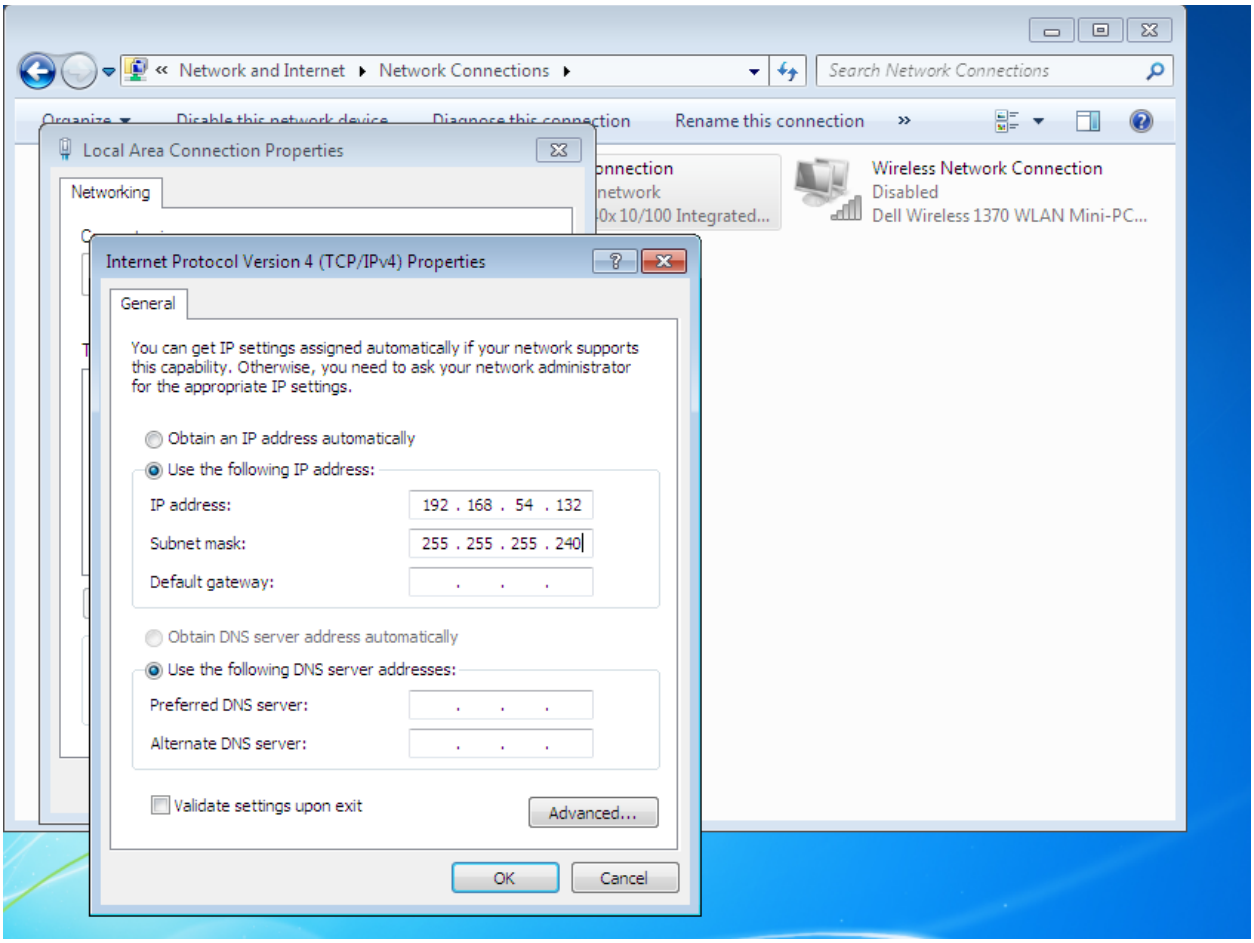
Workstation 1: **Ping** 192.168.54.132



Workstation 1: Click (TCIP/IPv4) - **Change the subnet mask** – 255.255.255.240



Repeat steps 4 through 7 on Workstation 2 – Ping both workstations



Ping – the ping is not successful because they are on separate networks. Workstation 1 is still on network 192.168.54.0 whereas Workstation 2 has been moved to network 192.168.54.128

Lab 9.2 Understanding the Purpose of the Default Gateway

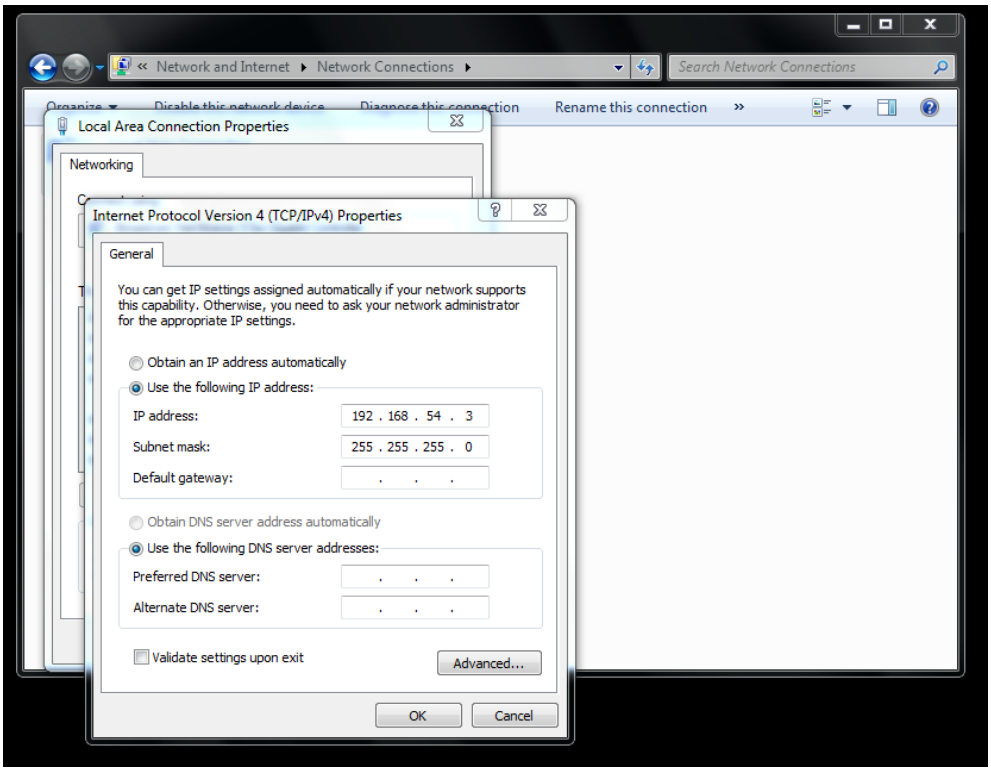
In computer networking, a gateway is a node (a router) on a TCP/IP network that serves as an access point to another network. A default gateway is the node on the computer network that the network software uses when an IP address does not match any other routes in the routing table. It is usually the IP address of the router to which your PC network is connected.

In home computing configurations, an ISP often provides a physical device which both connects local hardware to the Internet and serves as a gateway. Such devices include DSL routers and cable routers.

In organizational systems a gateway is a node that routes the traffic from a workstation to another network segment. The default gateway commonly connects the internal networks and the outside network (Internet). In such a situation, the gateway node could also act as a proxy server and a firewall. The gateway is also associated with both a router, which uses headers and forwarding tables to determine where packets are sent, and a switch, which provides the actual

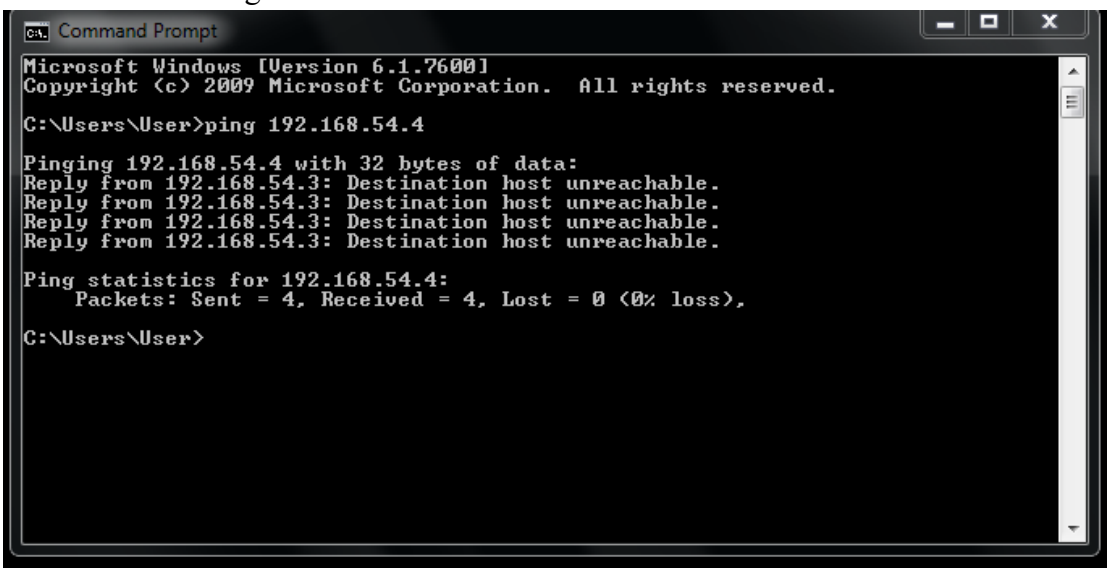
path for the packet in and out of the gateway. In other words, a default gateway provides an entry point and an exit point in a network.

Configure Workstation 1 with an IP address of 192.168.54.3, with a subnet mask of 255.255.255.0, no default gateway and the Firewall disabled.

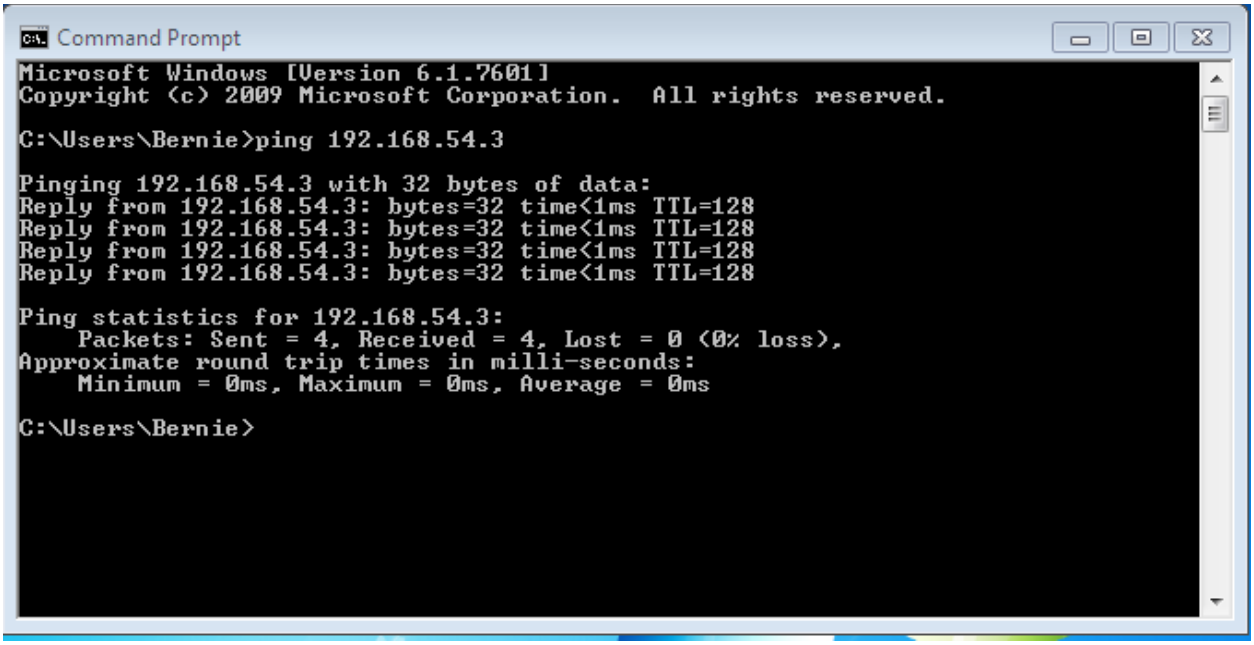


Configure Workstation 2 with an IP address of 192.168.54.4 and with the same subnet mask, default gateway and Firewall as Workstation 2.

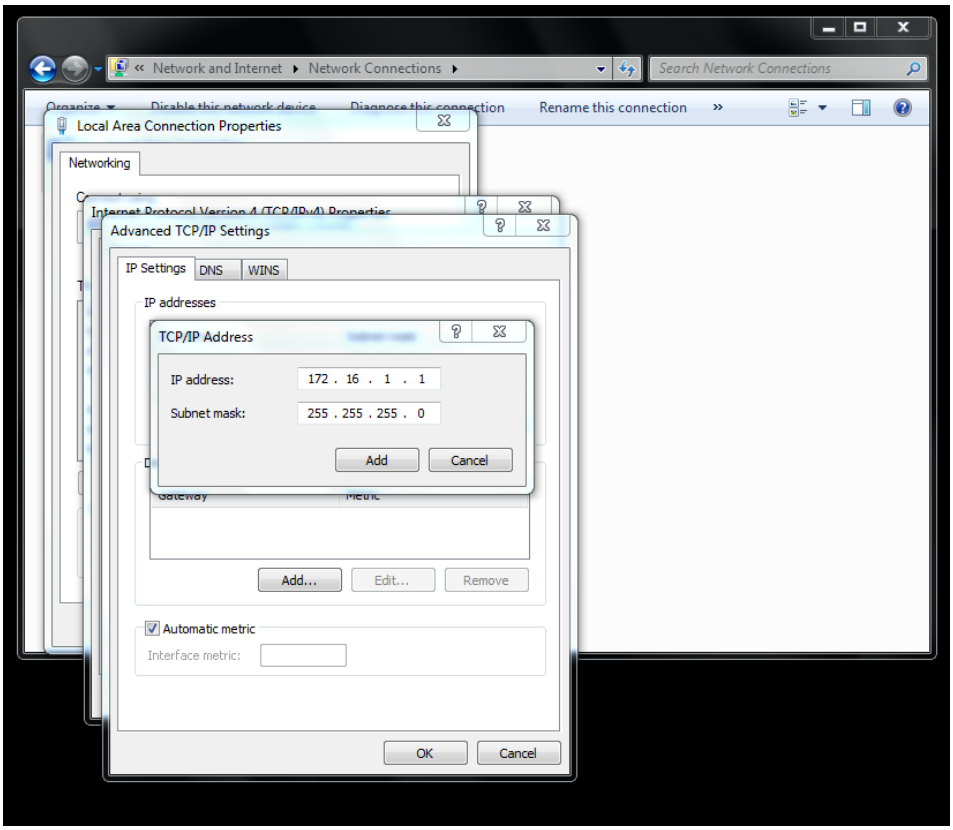
Workstation 1: Ping Workstation 2



Repeat steps 1 through 3 on Workstation 2 Ping Workstation 1

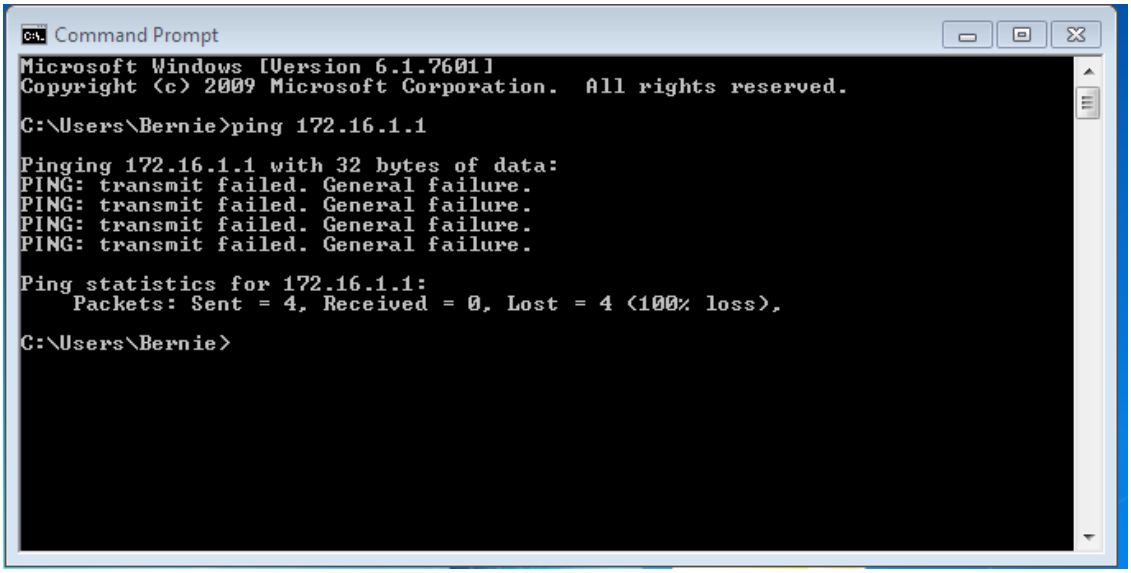


Now add a secondary IP address to Workstation 1 – Right click Local Area Connection – Properties – (TCP/IPv4) – Advanced – Click Add

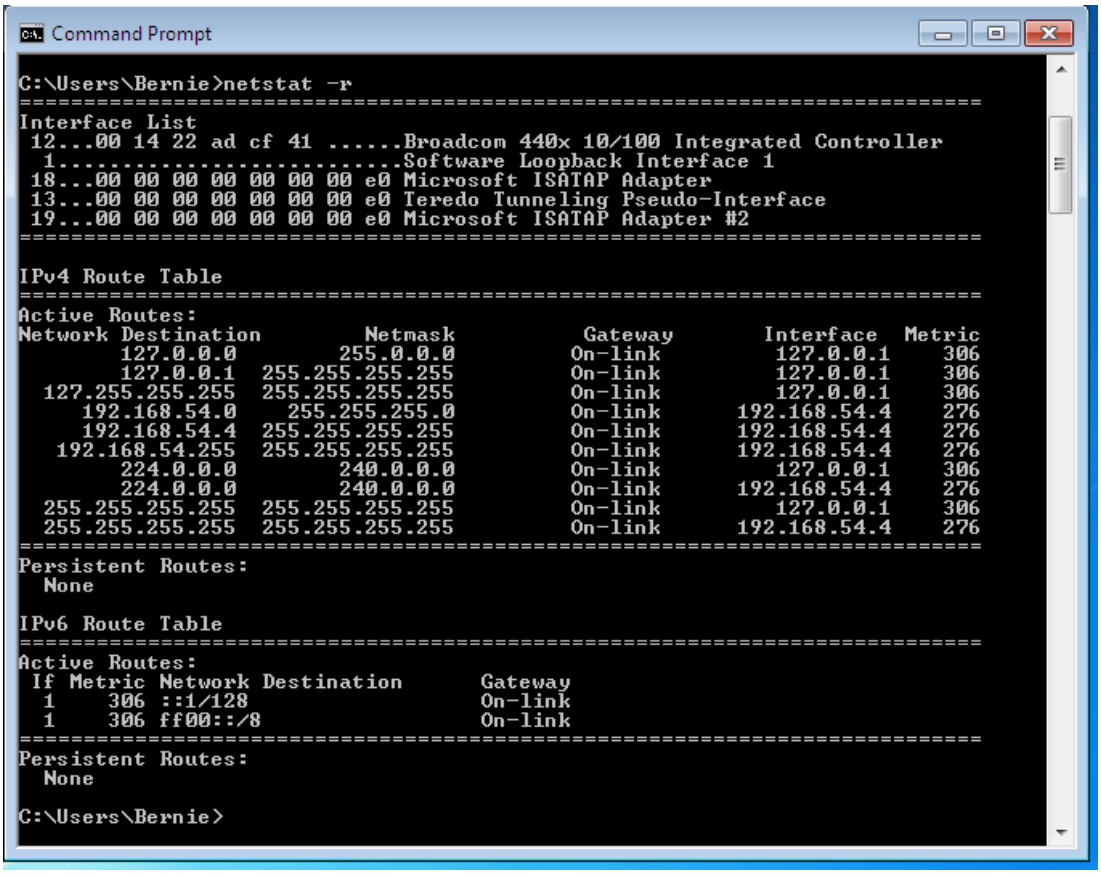


In the IP address text box, type 172.16.1.1 with a subnet mask of 255.255.255.0 – Add – O.K.

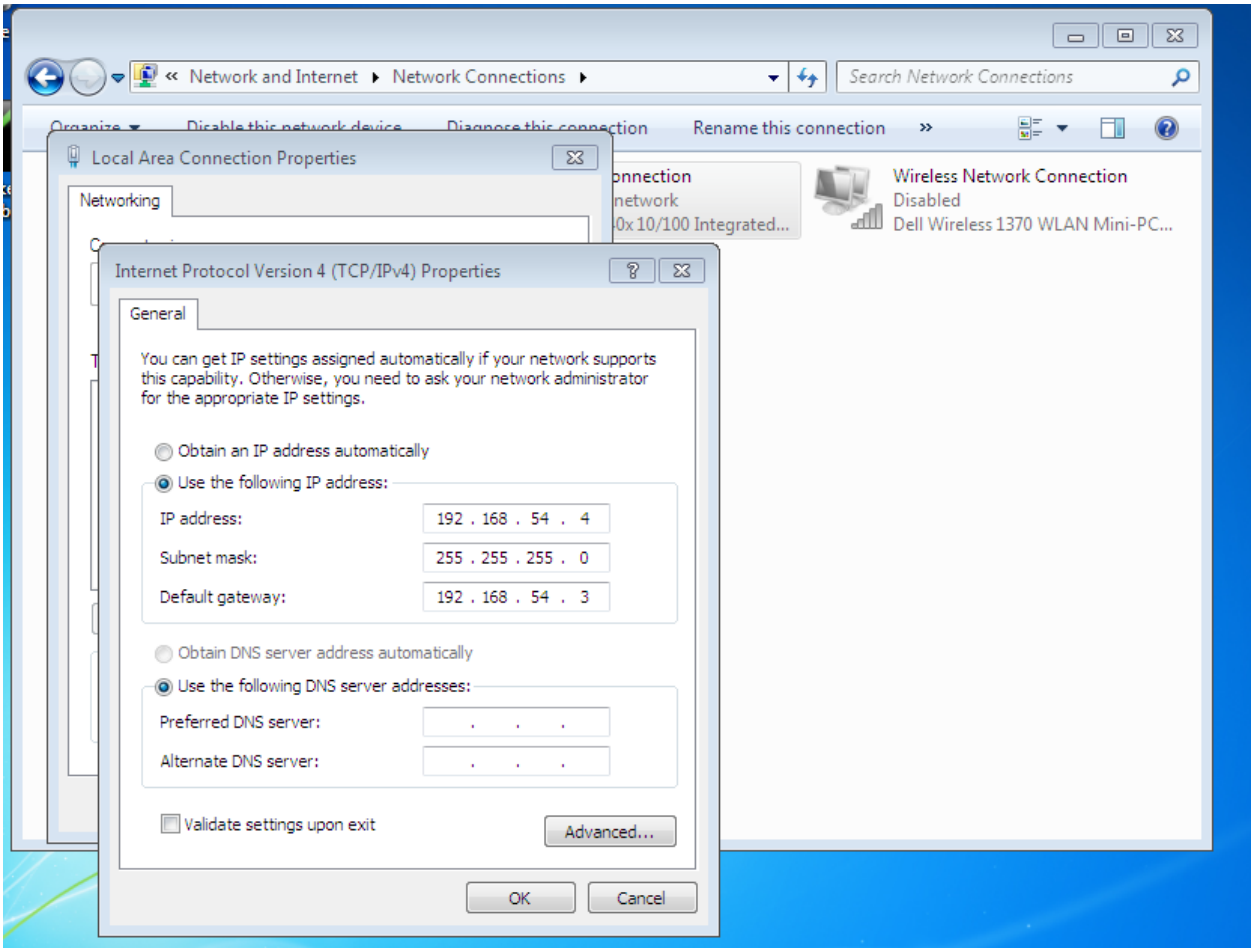
Workstation 2: Ping 172.16.1.1



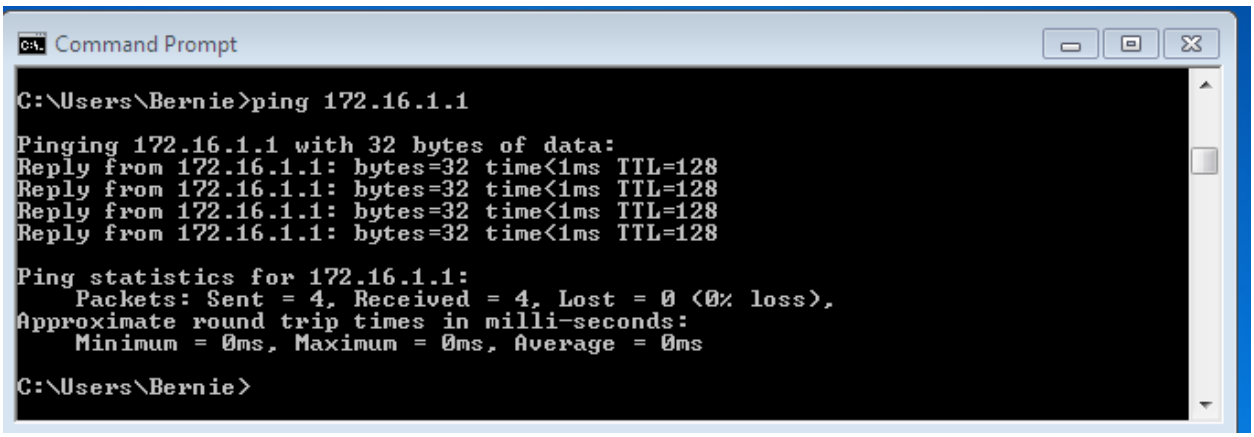
Ping is unreachable – it does not know where to send packets destined for 172.16.1.1 – Type **net stat –r** Press Enter to display the routing table.



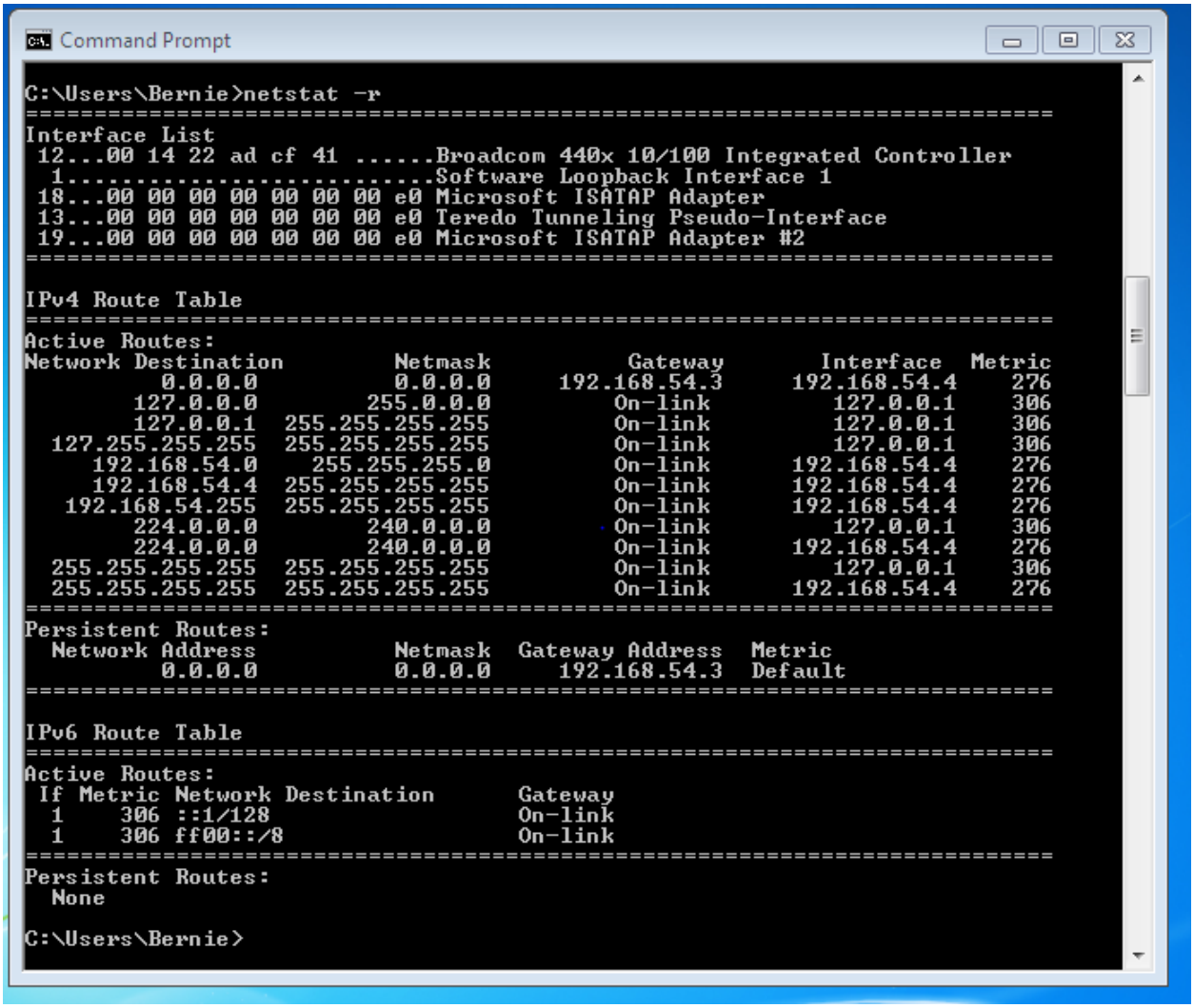
Now add a Default gateway to Workstation 2 – type 192.168.54.3



Ping Workstation 1 – 172.16.1.1- It receives 4 replies.



Type **netstst –r**



Compare the routing tables – Log off

Lab 9.3 Understanding the TCP/IP Hosts File

The hosts file is a computer file used by an operating system to map hostnames to IP addresses. The hosts file is a plain text file, and is conventionally named hosts. The hosts file is one of several system facilities that assists in addressing network nodes in a computer network. It is a common part of an operating system's Internet Protocol (IP) implementation, and serves the function of translating human-friendly hostnames into numeric protocol addresses, called IP addresses, that identify and locate a host in an IP network.

In some operating systems, the contents of the hosts file is used preferentially to other name resolution methods, such as the Domain Name System (DNS), but many systems implement name service switches, e.g., nsswitch.conf for Linux and Unix, to provide customization. Unlike

remote DNS resolvers, the hosts file is under the direct control of the local computer's administrator.

Review Questions

1. What is the purpose of a domain name?

In computer networking, a hostname (archaically node name) is a label that is assigned to a device connected to a computer network and that is used to identify the device in various forms of electronic communication such as the World Wide Web, e-mail or Usenet. Hostnames may be simple names consisting of a single word or phrase, or they may be structured.

On the Internet, hostnames may have appended the name of a Domain Name System (DNS) domain, separated from the host-specific label by a period ("dot"). In the latter form, a hostname is also called a domain name. If the domain name is completely specified, including a top-level domain of the Internet, then the hostname is said to be a fully qualified domain name (FQDN). Hostnames that include DNS domains are often stored in the Domain Name System together with the IP addresses of the host they represent for the purpose of mapping the hostname to an address, or the reverse process.

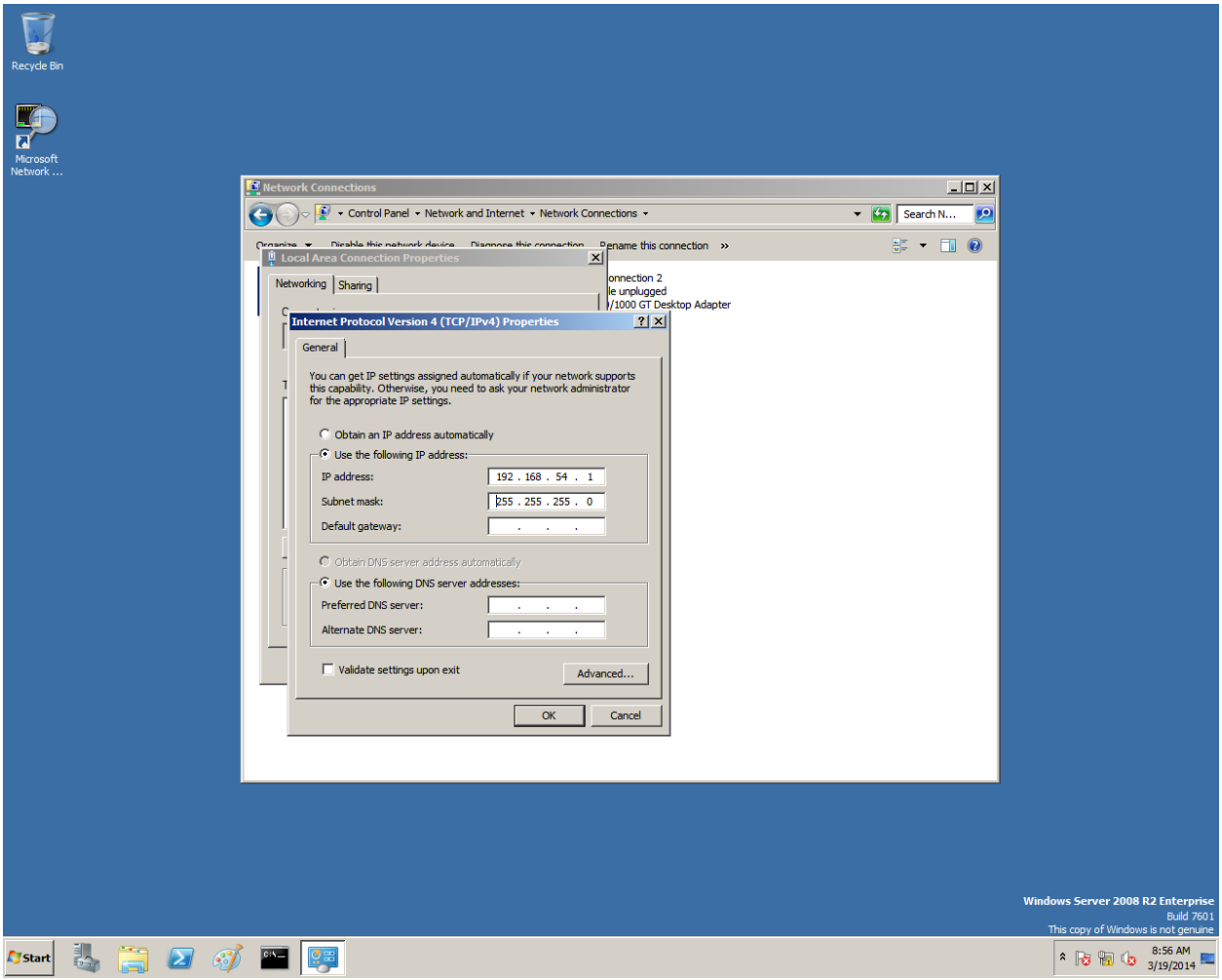
2. What is the purpose of a hosts file?

A host file is a plain-text computer file used to pair hostnames to IP addresses. The purpose of hosts files is to locate hosts in IP networks by converting hostnames into numeric data that can be read by an operating system. In Windows, hosts file is located in the drivers folder.

3. What file on a Linux system holds information about host names and their IP addresses?
a. /etc/hosts
4. Which of the following symbols indicates a comment in the hosts file? D. #
5. What is the alias of the host name “c2” in the following hosts file? A. CName

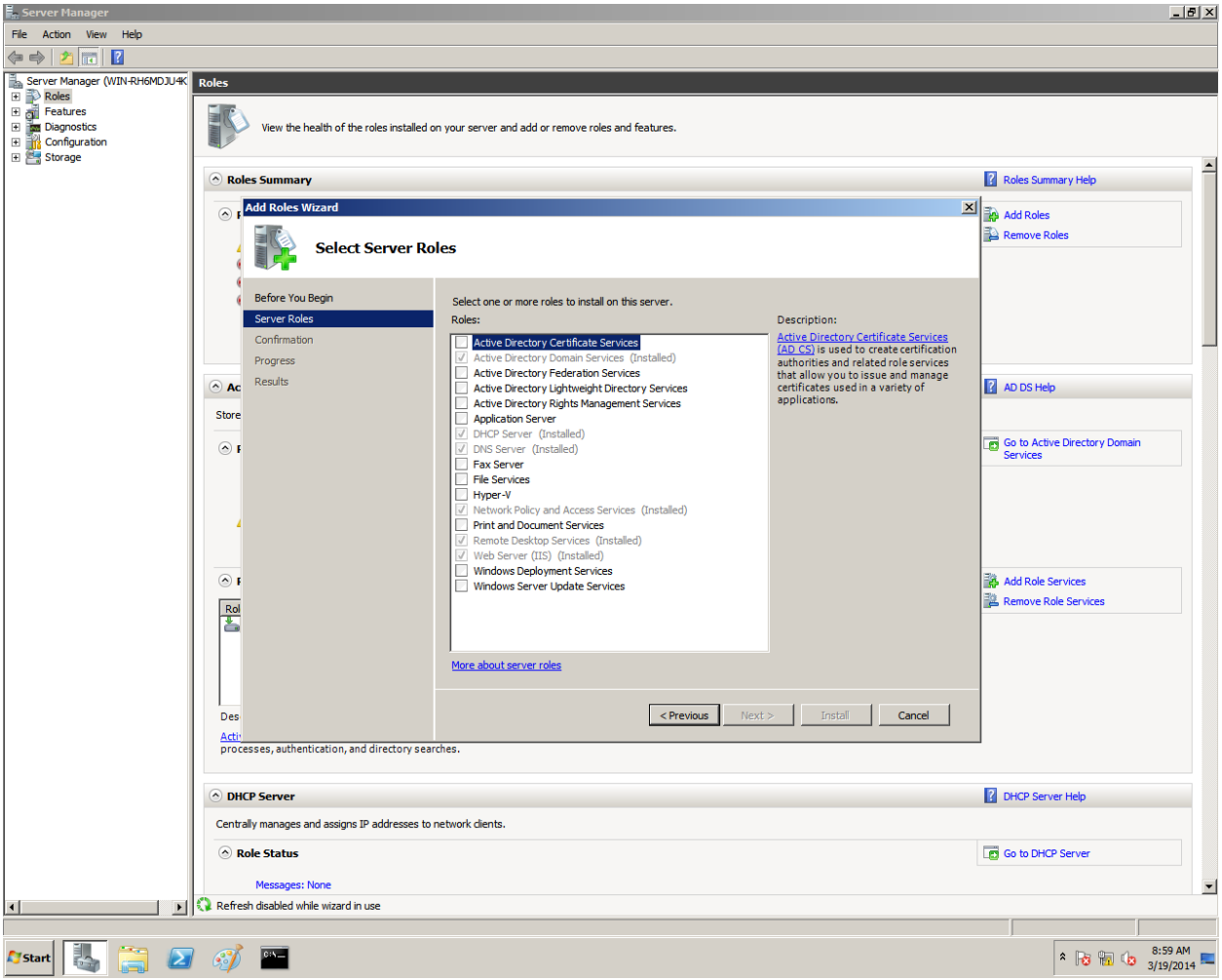
Lab 9.4 Setting up an FTP Server

Configure a computer running Windows Server 2008 with an IP address of 192.168.54.1 and a subnet mask of 255.255.255.0

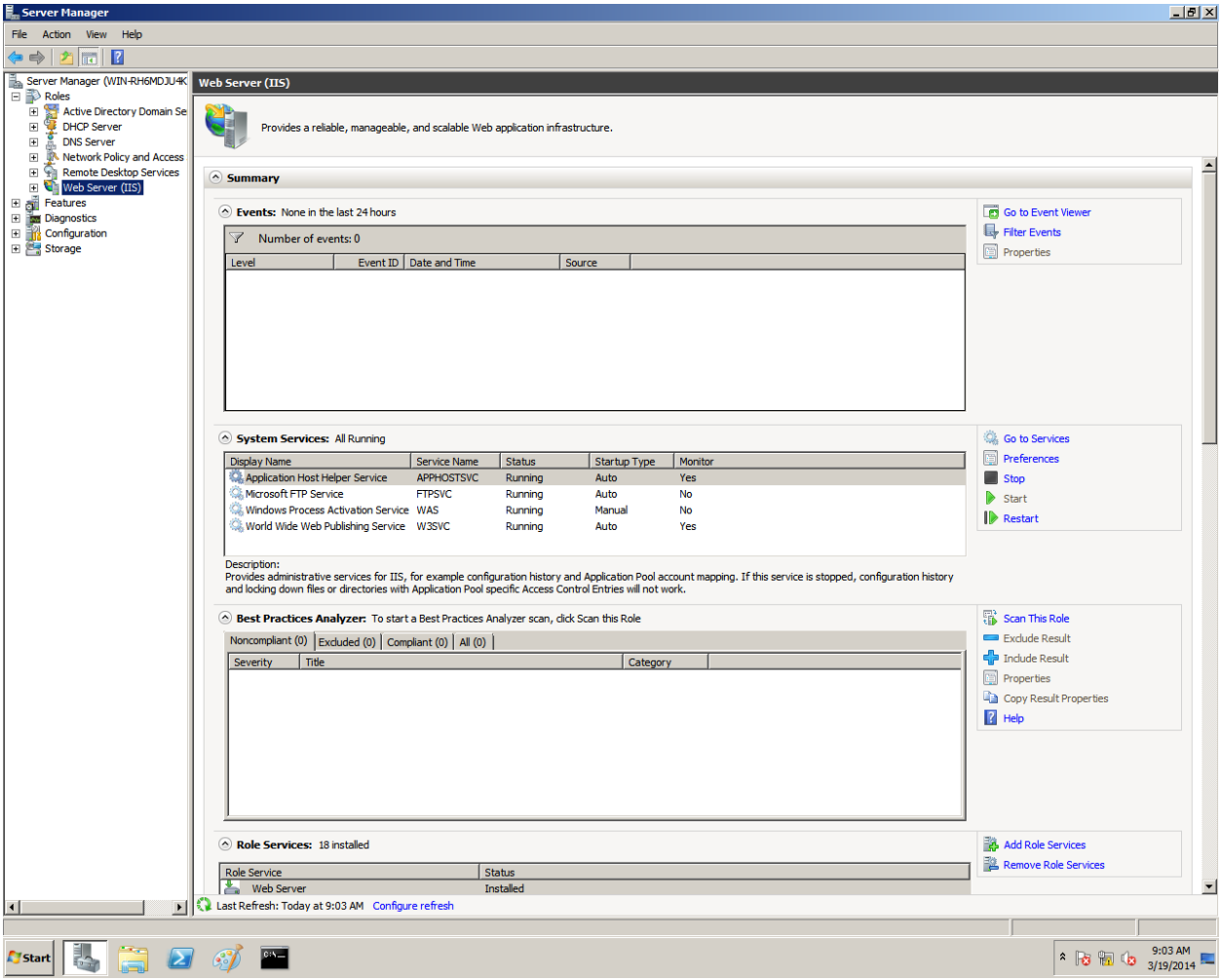


Configure a Workstation 1 with an IP address of 192.168.54.3 and a subnet mask of 255.255.255.0

On Server – Server Manager – Roles – Add Roles



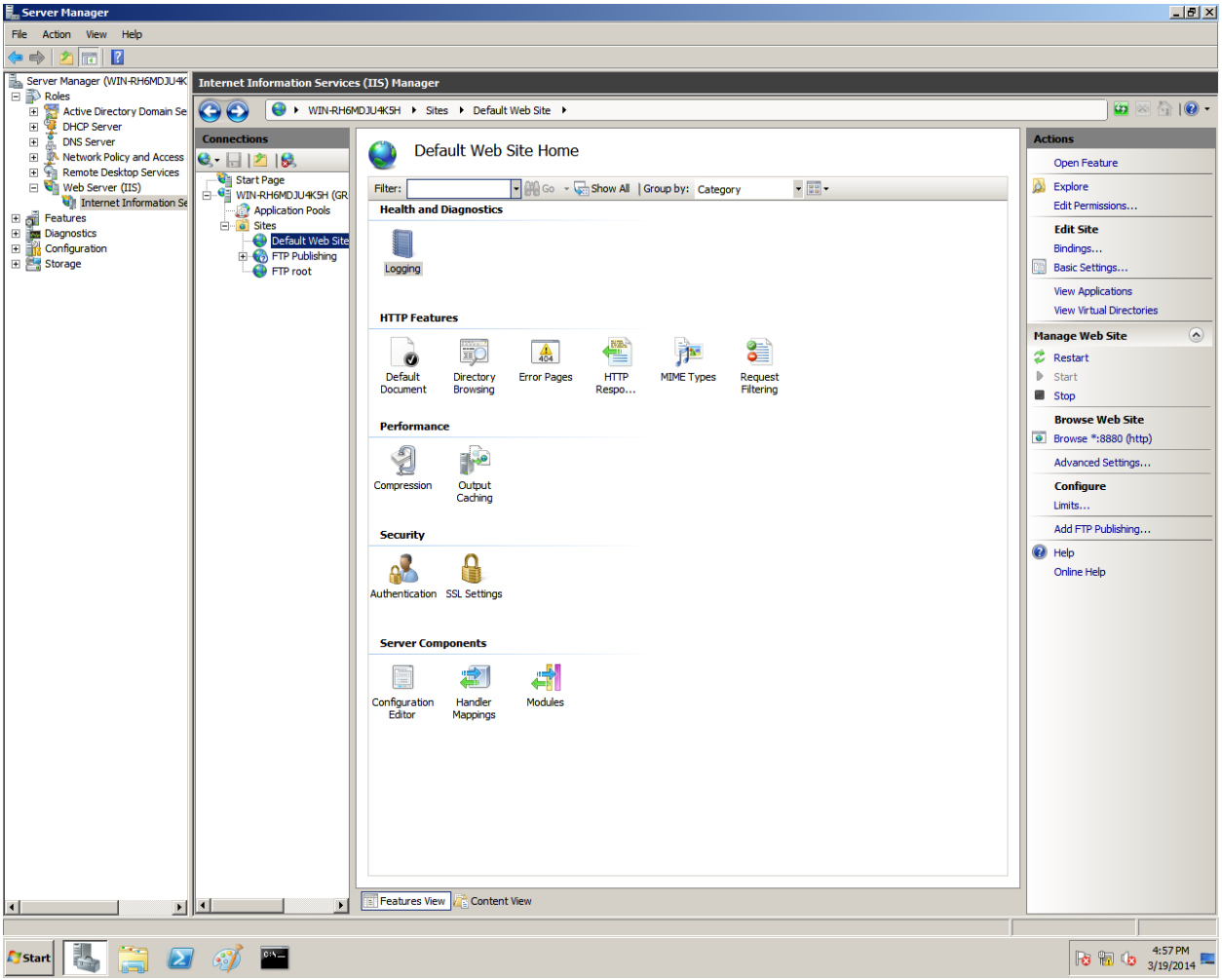
Place a check mark in the Web Server (IIS) check box – click Add Required Features in the Add Roles Wizard dialogue box that opens. Click next and then next again after reading the description of IIS. On the Select Role Services window, place a check mark in the FTP Publishing Service, click Add Required Role. – Next – Install.



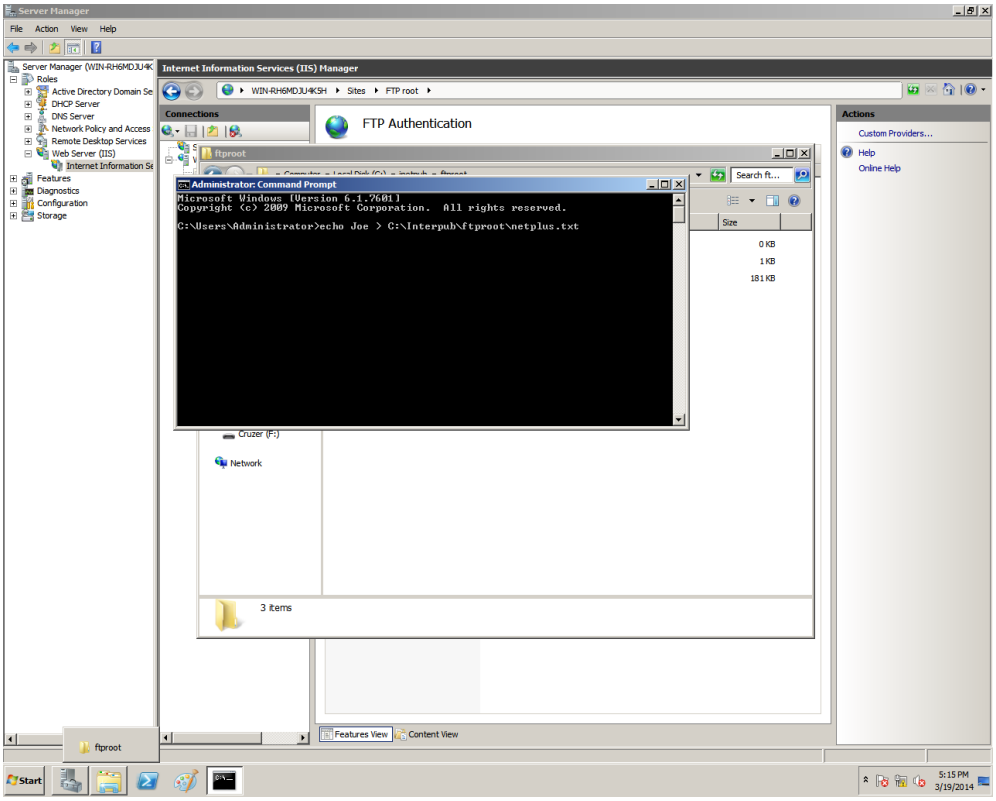
Click start – point to Administrative Tools – Services – right click FTP Publishing Service – Start

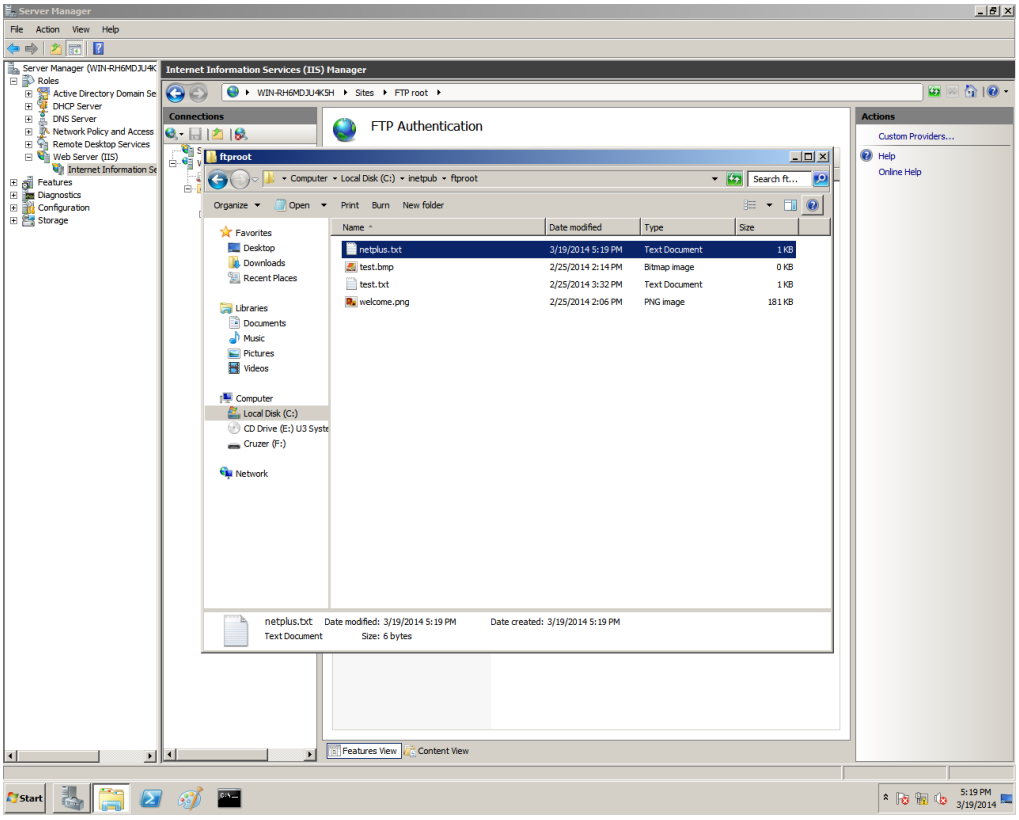
Click start –Administrative Tools –Internet Information Services (IIS) 6.0 Manager

Double click Server 1, double click FTP Sites, and right click Default FTP Site. – Yes – right click FTP Site – Properties



Click Security Accounts tab – select netplus user for anonymous access. A click browse I enter netplus as the username, - Check names – OK. Click the Home Directory tab and ensure that the local path to the ftproot directory is C:\inetpub\ftproot. In CMD type echo *your name* > C:\Inetpub\ftproot directory.


Server Manager
File Action View Help
Internet Information Services (IIS) Manager
WIN-RH6MDJU4KSH ▸ Sites ▸ FTP root ▸
Connections
FTP Authentication
Actions
Custom Providers...
Help
Online Help
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>echo Joe > C:\Inetpub\ftproot\netplus.txt
ftproot
3 items
Features View
Content View
5:15 PM
3/19/2014


Server Manager
File Action View Help
Internet Information Services (IIS) Manager
WIN-RH6MDJU4KSH ▸ Sites ▸ FTP root ▸
Connections
FTP Authentication
Actions
Custom Providers...
Help
Online Help
ftproot
Computer ▸ Local Disk (C:) ▸ inetpub ▸ ftproot
Search ft...
Organize Open Print Burn New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Cruzer (F:)
Network
Name Date modified Type Size
netplus.txt 3/19/2014 5:19 PM Text Document 1 KB
test.bmp 2/25/2014 2:14 PM Bitmap image 0 KB
test.txt 2/25/2014 3:32 PM Text Document 1 KB
welcome.png 2/25/2014 2:06 PM PNG image 181 KB
netplus.txt Date modified: 3/19/2014 5:19 PM Date created: 3/19/2014 5:19 PM
Text Document Size: 6 bytes
Features View
Content View
5:19 PM
3/19/2014

Lab 9.5 Configuring a Mail Server

Configure this computer as a mail server to install E-mail Services, which provides e-mail transfer and retrieval services. E-mail Services includes the POP3 service, which provides e-mail retrieval, and the SMTP service, which provides e-mail transfer. Administrators can use the POP3 service to store and manage e-mail accounts on the mail server. After configuring this computer as a mail server, users can connect to the mail server and retrieve e-mail to their local computer using an e-mail client that supports the POP3 protocol, such as Microsoft Outlook.

Before you configure your computer as a mail server, verify that:

•The server on which you intend to install e-mail services has a working Internet connection.

•There is an NTFS partition available. With an NTFS partition, you can take advantage of the increased security provided by disk quotas. For more information about disk quotas, see Configuring disk quotas for the POP3 service.

•You have a registered e-mail domain name. Contact your Internet Service Provider for assistance in registering an e-mail domain name.

•A Mail eXchanger (MX) record for your e-mail domain name exists and matches the name of your server. Contact your Internet service provider (ISP) to create an MX record.

•You have configured your server for static addressing. Contact your Internet Service Provider for the information necessary to configure your server for static addressing. For more information on how to configure your mail server with a static IP address, see Configure TCP/IP for static addressing.

•Windows Firewall is enabled. For more information, see Enable Windows Firewall with no exceptions.

•The Security Configuration Wizard is installed and enabled. For information about the Security Configuration wizard, see Security Configuration Wizard Overview.

The following table lists the information that you need to know to before you add a mail server role.

Determine the appropriate level of security for this server: A server in this role may be targeted by attackers because of its exposure to the Internet and other networks. To ensure the security of this server, it is recommended that you implement security precautions, such as firewalls and Internet Protocol security (IPSec), before placing it in a production environment. For more information, see Internet Protocol Security (IPSec) and Basic Firewall.

Determine the appropriate authentication method for your configuration: You must choose an authentication method before you create any e-mail domains on the mail server. The

authentication method can be changed only if there are no existing e-mail domains on the mail server. If the computer that you are configuring as a mail server is either a member server or a domain controller, the authentication method setting defaults to Active Directory authentication. Otherwise, the setting defaults to local Windows accounts authentication.

Determine that you have a registered e-mail domain name: The e-mail domain must be a registered domain name and it must match the Mail eXchanger (MX) record created by your ISP. If you do not already have an e-mail domain name, contact your ISP for assistance in registering a domain name.

Note

•The POP3 service supports top-level and third-level domain names. For example, example.com and mailserver.example.com are both supported.

Joseph Martinez

Networking II: Network +
CNG – 125

Chapter Ten Labs
Virtual Networking and Remote Access

Lab 10.1 Configuring a Remote Access Server

Lab 10.2 Creating VPN with the Point-to-Point Tunneling Protocol

Lab 10.3 Configuring Remote Desktop Services (Terminal Services) on Windows

Lab 10.4 Remotely Managing a Computer with Active Directory

Lab 10.5 Remotely Managing a Linux Server

Lab 10.1 Configuring a Remote Access Server

Routing and Remote Access Service (RRAS), a Microsoft API that makes it possible to create applications to administer the routing and remote access service capabilities of the operating system. RRAS makes it possible for a computer to function as a network router, and developers can also use RRAS to implement routing protocols.

To install the Routing and Remote Access service

1.In the Server Manager main window, under Roles Summary, click Add roles.

-- OR --

In the Initial Configuration Tasks window, under Customize This Server, click Add roles.

2.In the Add Roles Wizard, click Next.

3.In the list of server roles, select Network Policy and Access Services. Click Next twice.

4.In the list of role services, select Routing and Remote Access Services to select all of the role services. You can also select individual server roles.

5.Proceed through the steps in the Add Roles Wizard to complete the installation.

Note

After you complete the installation, the Routing and Remote Access service is installed in a disabled state. To enable and configure the remote access server, you must be logged on as a member of the Administrators group. After installing the Routing and Remote Access service, you need to enable the service to configure your server for routing and remote access.

To enable the Routing and Remote Access service

1.If this server is a member of an Active Directory domain and you are not a domain administrator, instruct your domain administrator to add the computer account of this server to the RAS and IAS Servers security group in the domain of which this server is a member. The domain administrator can add the computer account to the RAS and IAS Servers security group by using Active Directory Users and Computers or by using the netsh ras add registeredserver command. If this server is using local authentication or is authenticating against a RADIUS server, skip this step.

2.Open Routing and Remote Access.

3.By default, the local computer is listed as a server.

To add another server, in the console tree, right-click Server Status, and then click Add Server.

In the Add Server dialog box, click the applicable option, and then click OK.

4.In the console tree, right-click the server you want to enable, and then click Configure and Enable Routing and Remote Access.

5.Follow the instructions in the Routing and Remote Access Server Setup Wizard.

Protocol's

Protocol is an agreed-upon format for transmitting data between two devices. It determines type of error checking and data compression used.

SLIP

Short for Serial Line Internet Protocol, a protocol for connection to the Internet via a dial-up connection. Developed in the 80s when modem communications typically were limited to 2400 bps, it was designed for simple communication over serial lines.

PPP

Short for Point-to-Point Protocol, a method of connecting a computer to the Internet. PPP is more stable than the older SLIP protocol and provides error checking features.

MP

Short for Multilink Point-to-Point Protocol, an extension to the PPP protocol that allows multiple physical connections between two points to be combined into a single logical connection. The combined connections, called a bundle, provide greater bandwidth than a single connection.

PPTP

Short for Point-to-Point Tunneling Protocol, a new technology for creating Virtual Private Networks (VPNs) , developed jointly by Microsoft Corporation, U.S. Robotics, and several remote access vendor companies, known collectively as the PPTP Forum. A VPN is a private network of computers that uses the public Internet to connect some nodes.

Lab 10.1 Review Questions

1. Which of the following best describes a modems function?

To convert a source computer's digital pulses into analog signals for the PSTN, and then convert analog signals back into digital pulses for the destination of the computer.

2. What is another term for Public Switched Telephone Network?

Telephone service carried by the PSTN is often called plain old telephone service (POTS).

PSTN refers to the international telephone system based on copper wires carrying analog voice data. This is in contrast to newer telephone networks base on digital technologies, such as ISDN and FDDI.

3. Which of the following types of dial-up connections would result in the best performance from the clients perspective?

A PPP dial-up connection to an RRAS server that allowed the client to launch an application from the RRAS server.

4. What does RAS stand for?

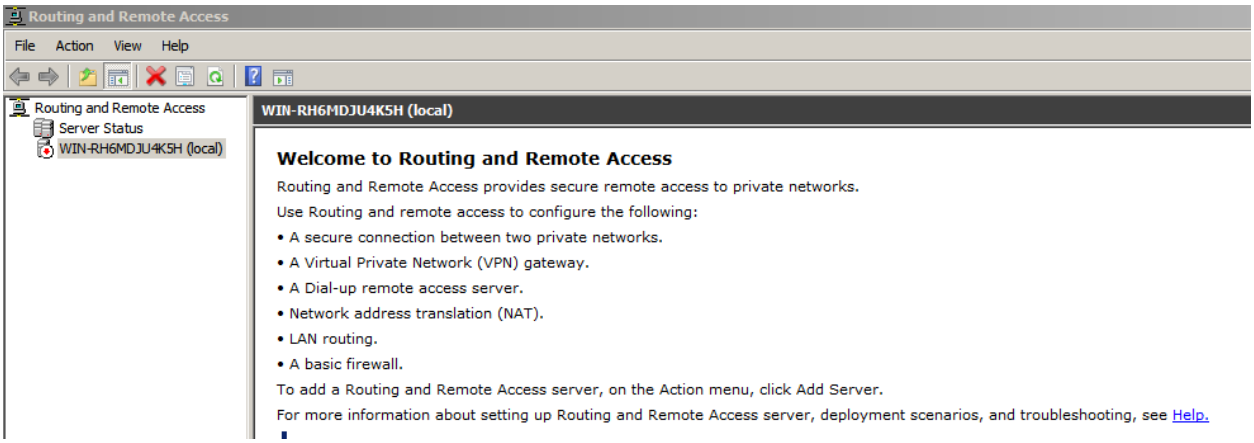
Short for remote access server.

5. Why do most remote clients (for example, those that dial in to an RRAS server) use DHCP and not static IP addressing?

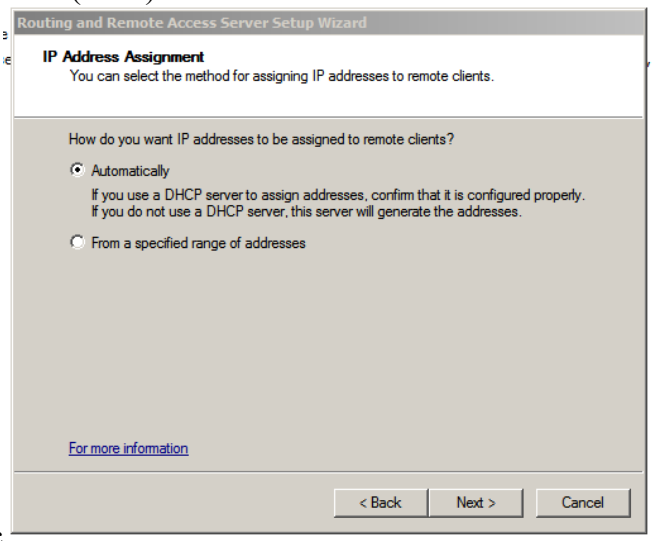
When Remote Access Service (RAS) uses Dynamic Host Configuration Protocol (DHCP) to obtain IP addresses for dial-in clients, only the IP address from the DHCP lease is passed to the RAS client. Other options in the DHCP scope are not. This article describes the behavior that occurs.

Lab 10.2 Creating VPN with the Point-to-Point Tunneling Protocol

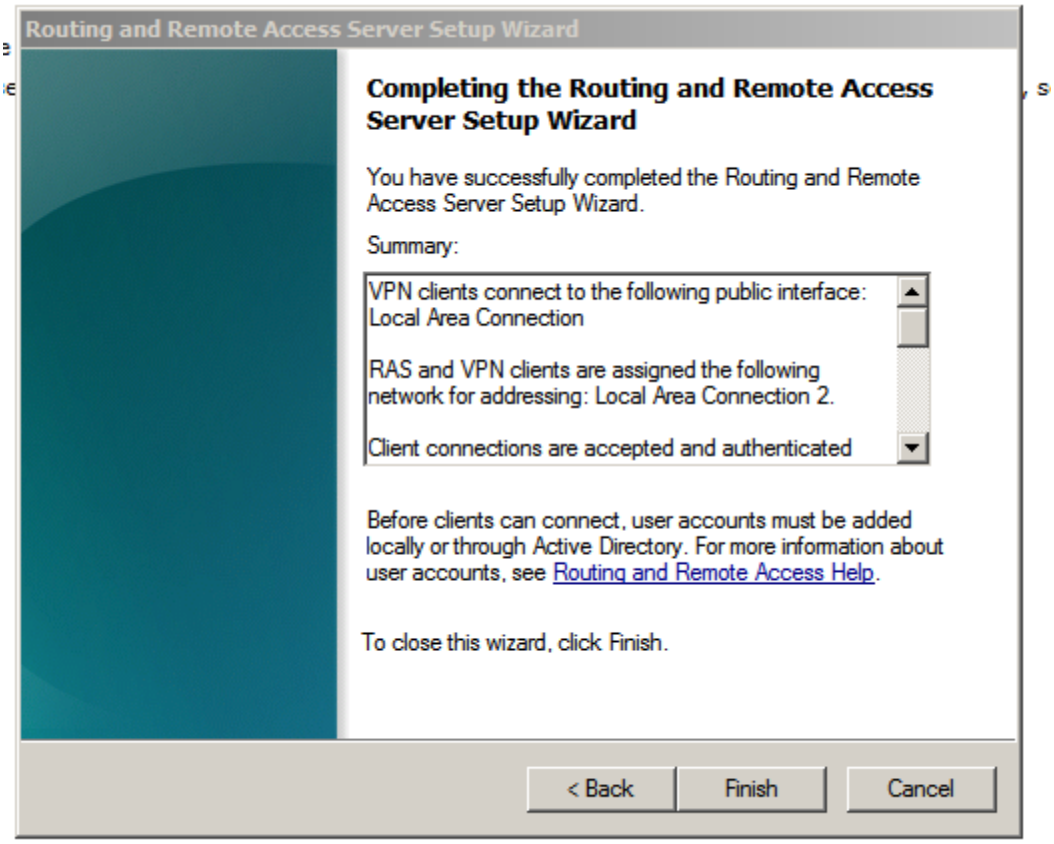
Log on to Server 1, click Start – Administrative Tool – Routing and Remote Access



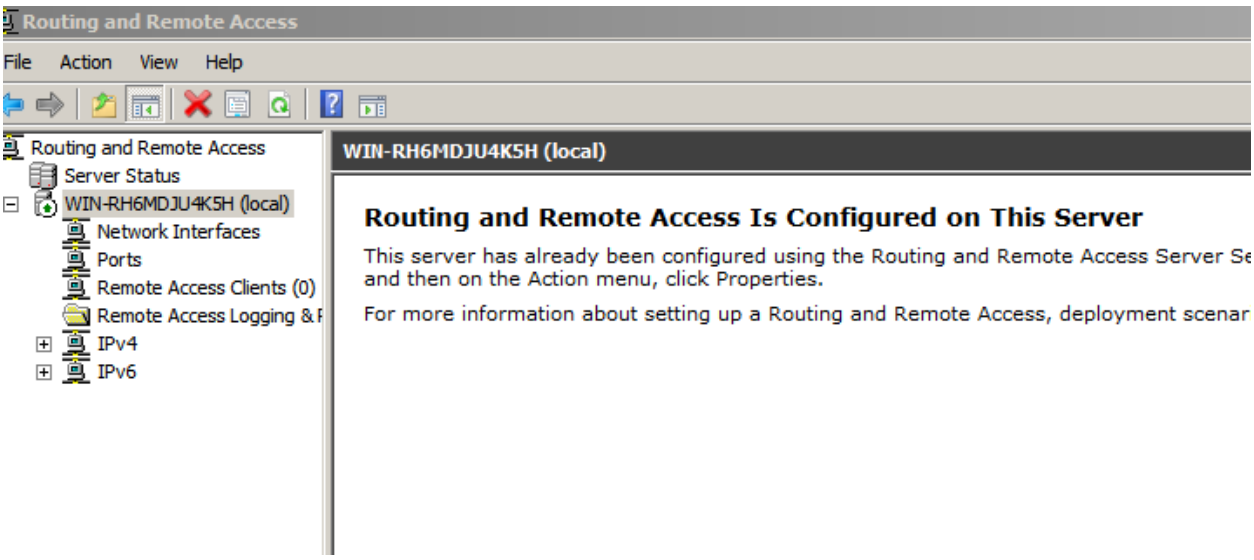
In the left pane of the dialogue box, right click Server 1 – Configure and Enable Routing and Remote Access – Next – Virtual private network (VPN) access and NAT – Next – select Local Area Connection – Next – Select Automatic



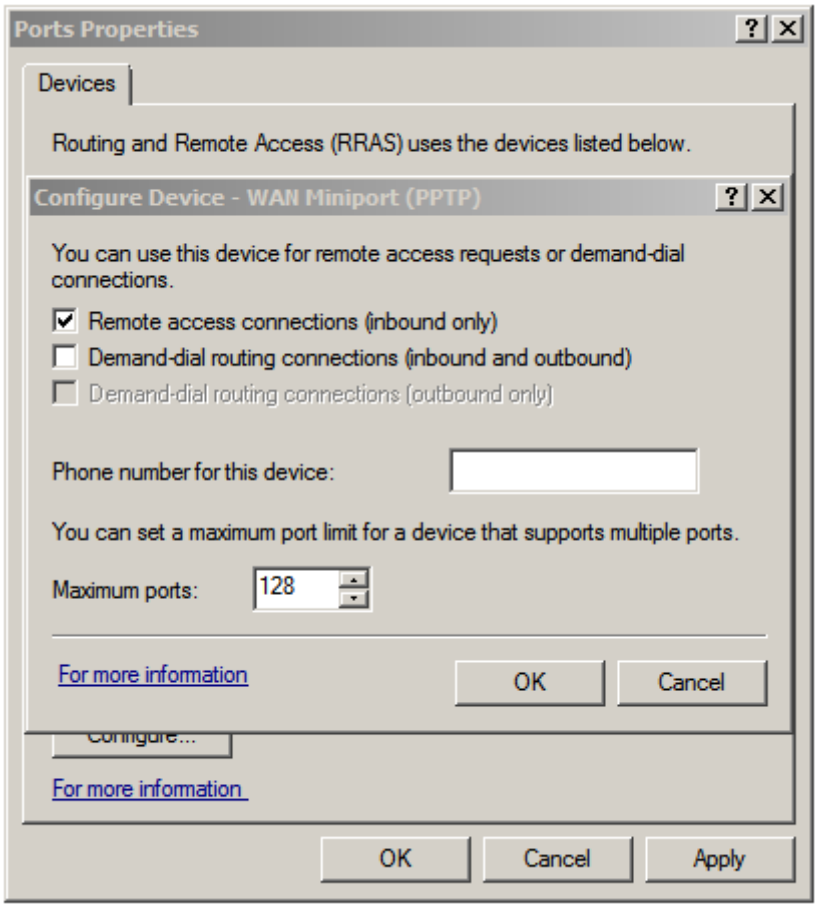
-Next – Select No, use Routing and Remote Access to authenticate connection requests – Next – Finish



Click OK. The tree underneath Server 1 has expanded.

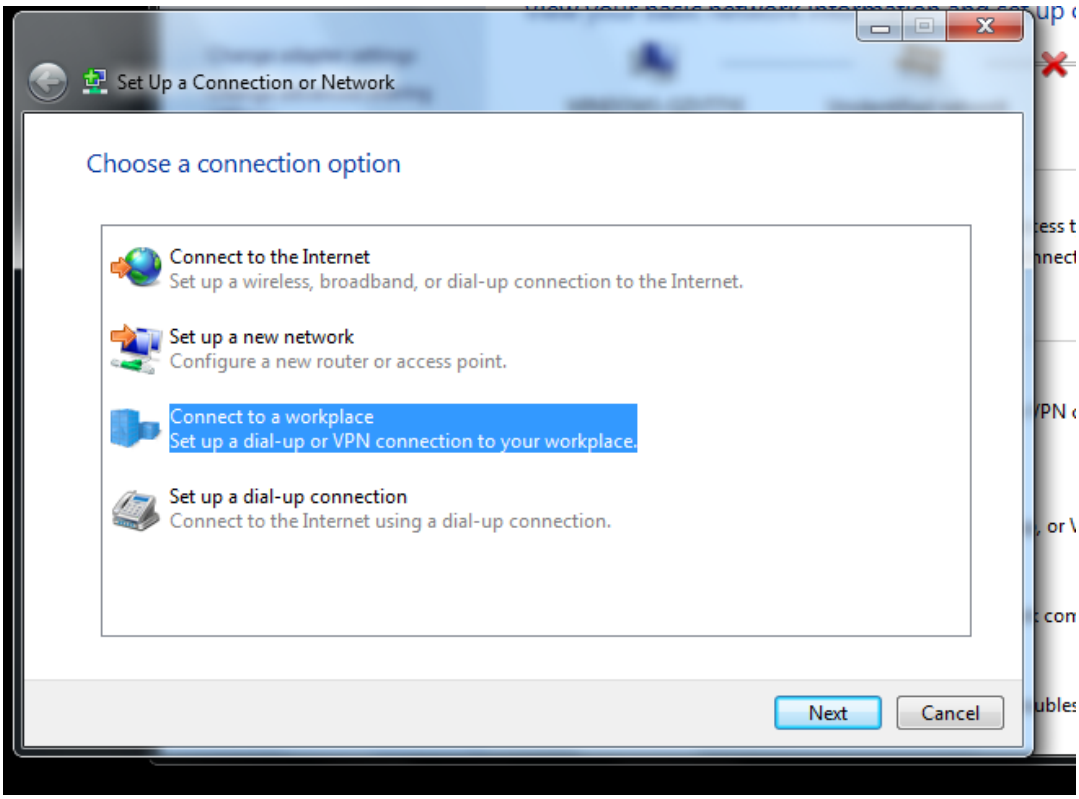


Right click Ports on the tree – select Properties – click WAN Miniport (PPTP) – Configure – Demand-dial routing connections

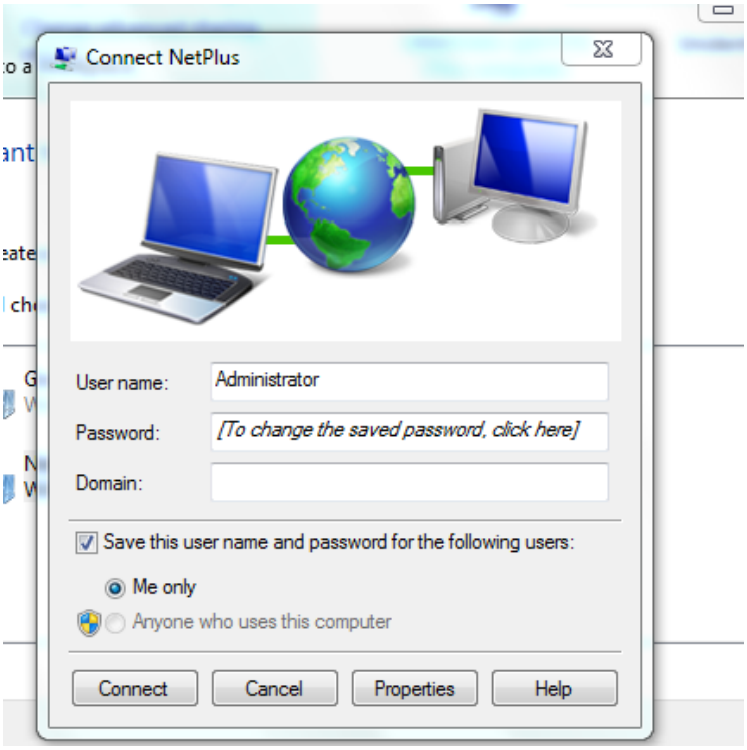


Click Demand-dial routing connections (inbound and outbound) Right click Server 1 – All Tasks – Restart

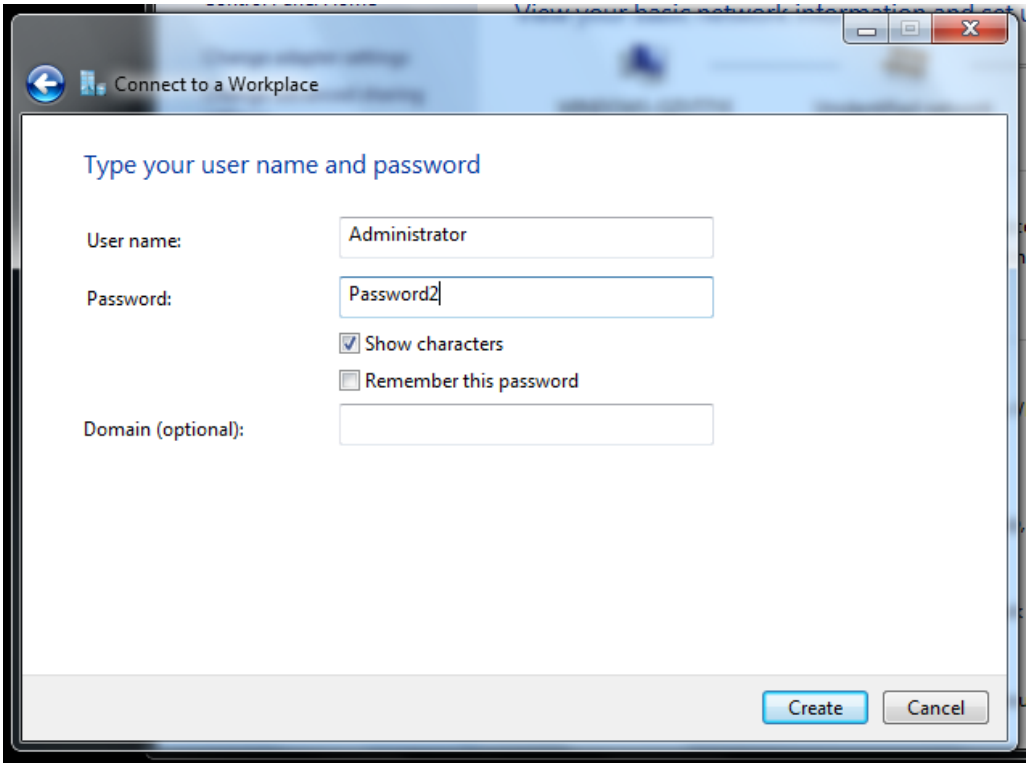
Log on to Workstation 1- Network and Internet – Network Sharing Center – Set up a new connection or network – connect to s workplace- Next – Select No, create a new connection option – Next



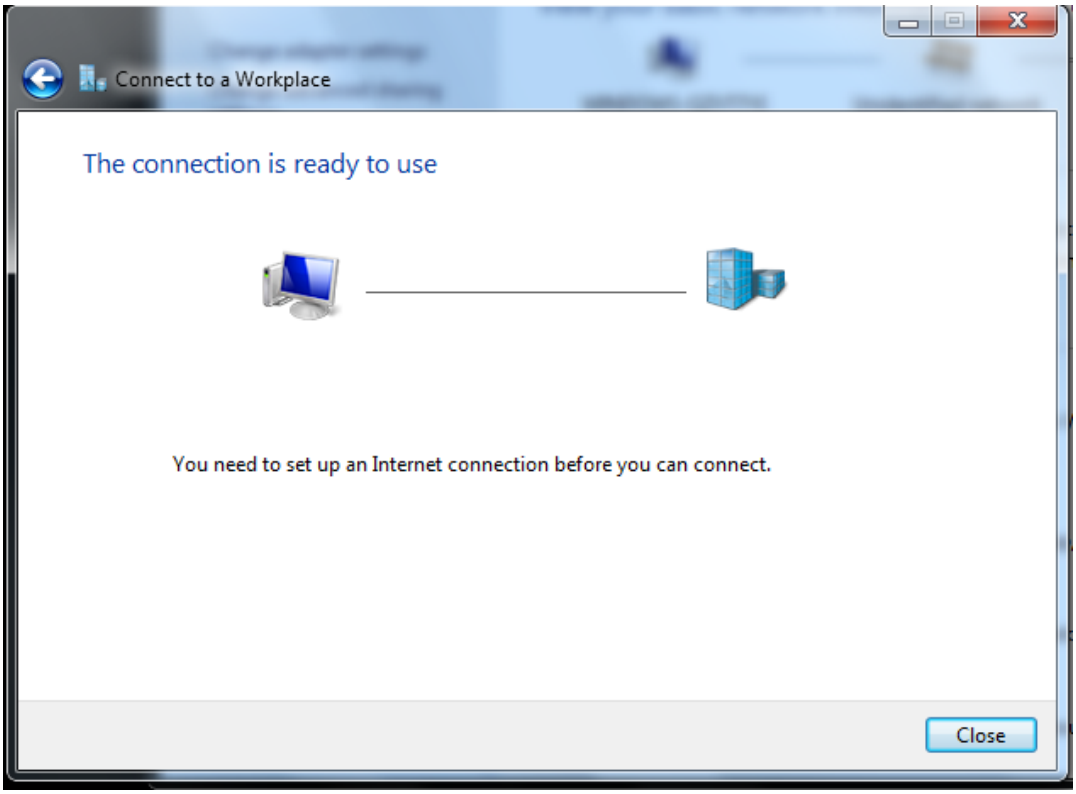
Enter 192.168.54.1 and NetPlus as the Destination name, and next.



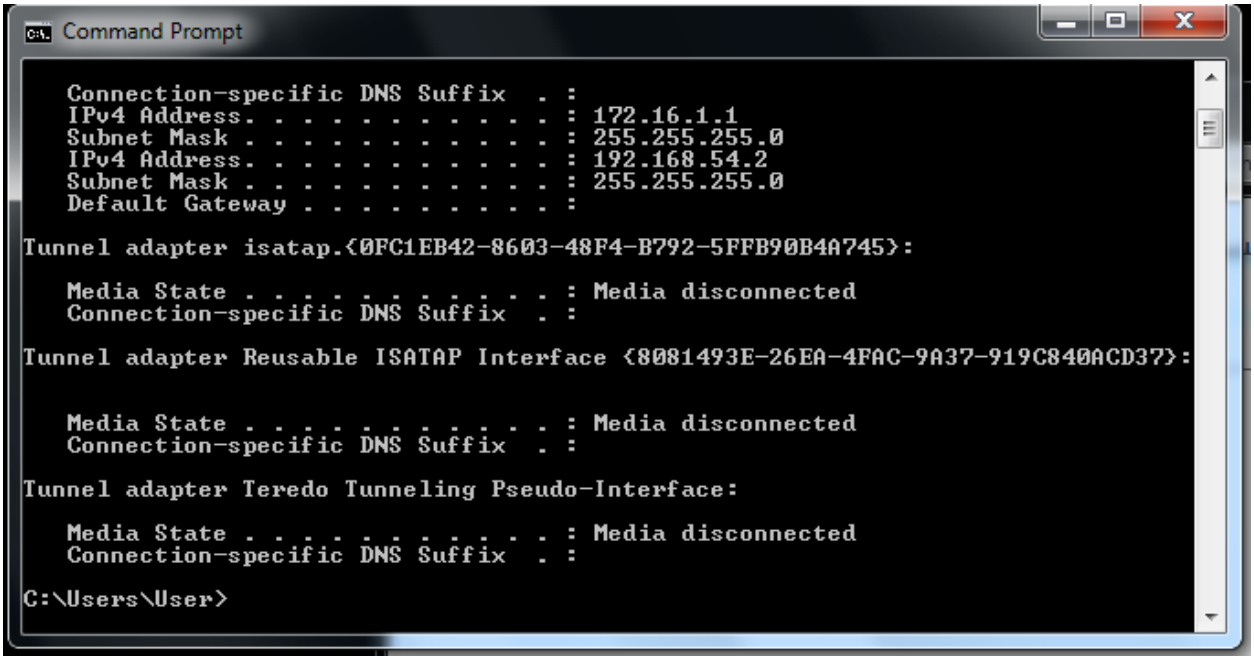
Enter the User name and Password



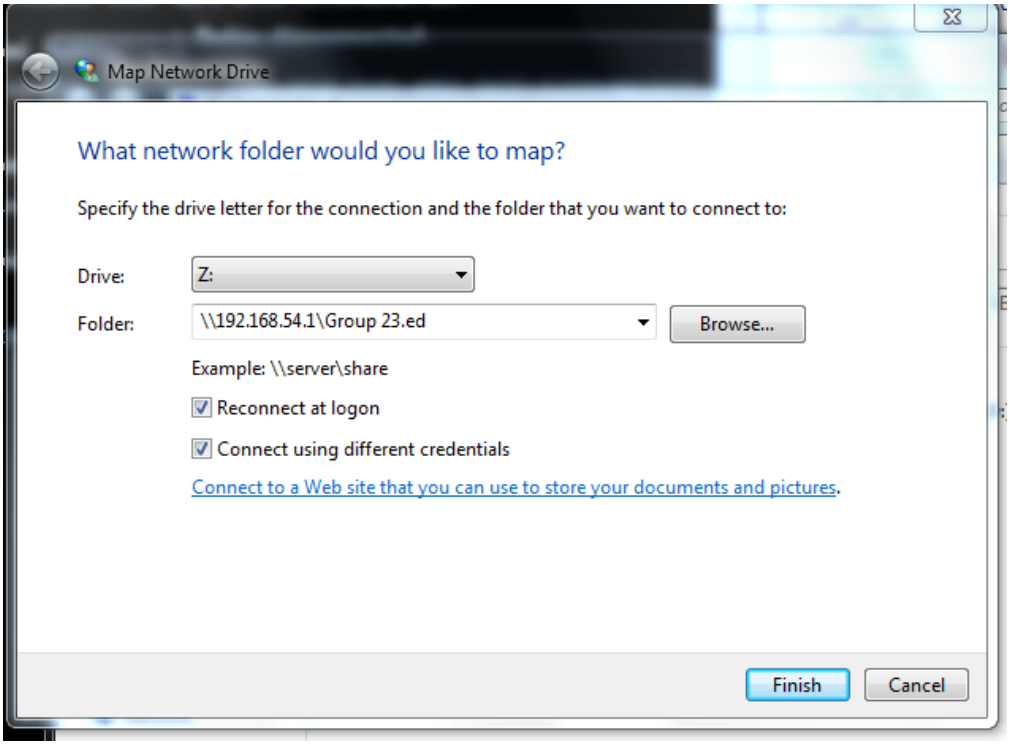
The NetPlus dialog box opens, indicating that the computer is being registered on the network.

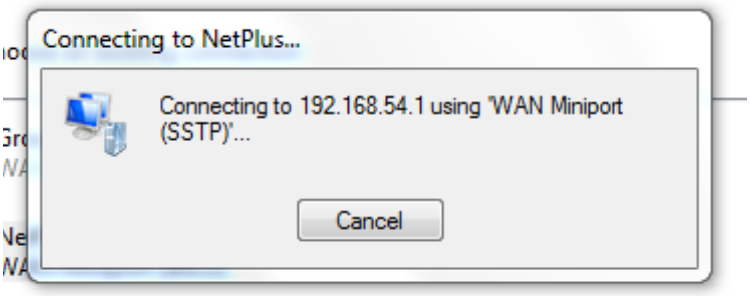


Skip to Step 39. – CMD – ipconfig – Enter



The computer displays the IP address for each NIC on the computer, including the virtual NIC for the VPN. – On workstation 1 – click Computer – on the menu bar, click Map Network Drive. The dialogue box opens. In the folder text box, enter \\192.168.54.1\NETPLUS. Click Connect using different credentials. Finish. The network password dialog opens. Type Administrator and password – OK. The map Network Drive dialog box opens

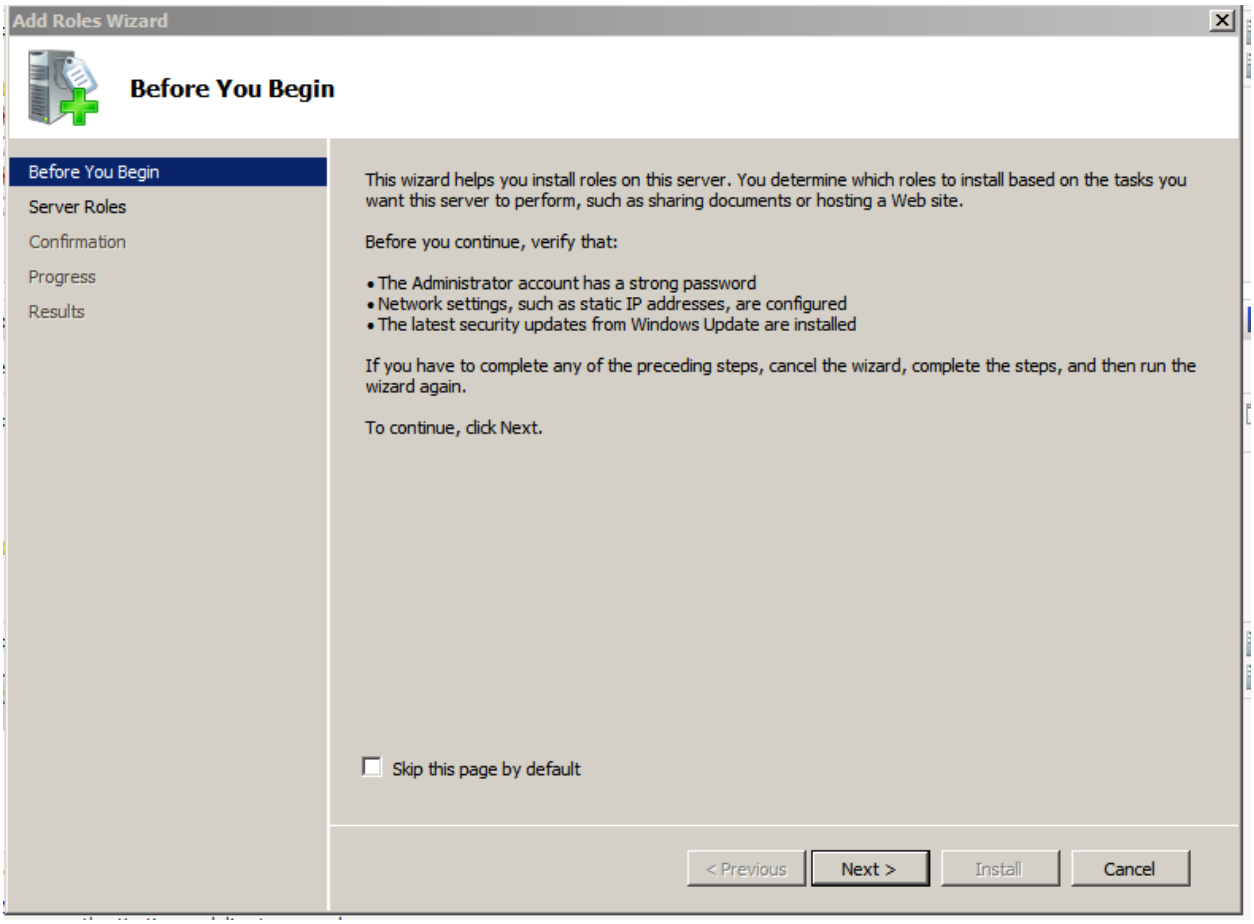




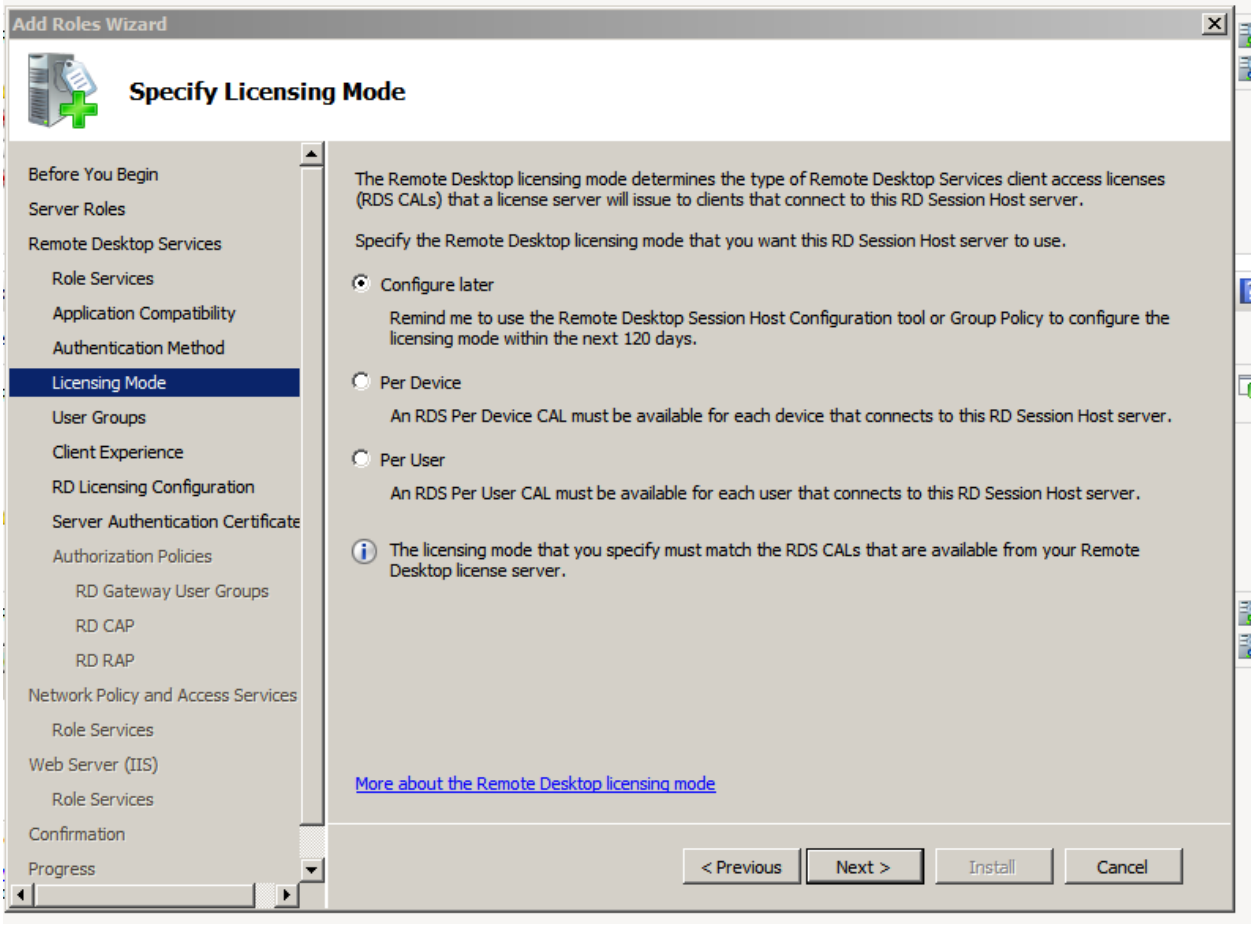
Double-click the icon for the mapped network drive. A folder containing the name of at least one text file appears. Double click the text file. The text file opens. Log off.

Lab 10.3 Configuring Remote Desktop Services (Terminal Services) on Windows

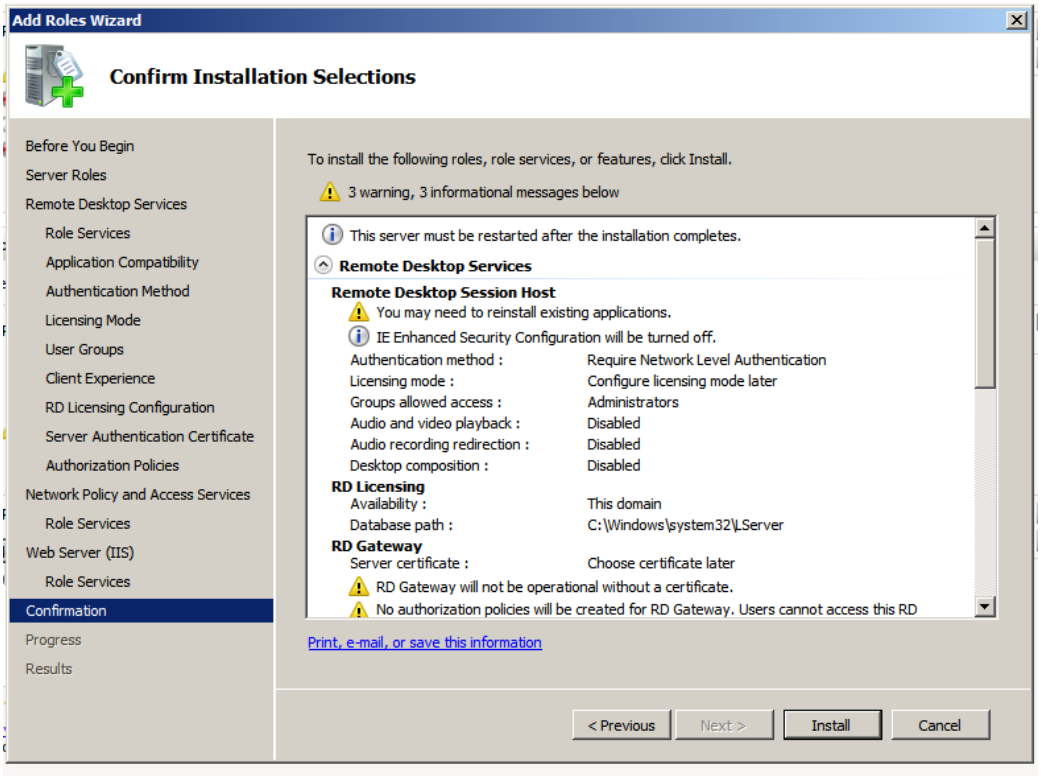
Log on to Server 1 2008, Server Manager – Roles – Add Roles – Wizard opens – If the you began window opens click Next



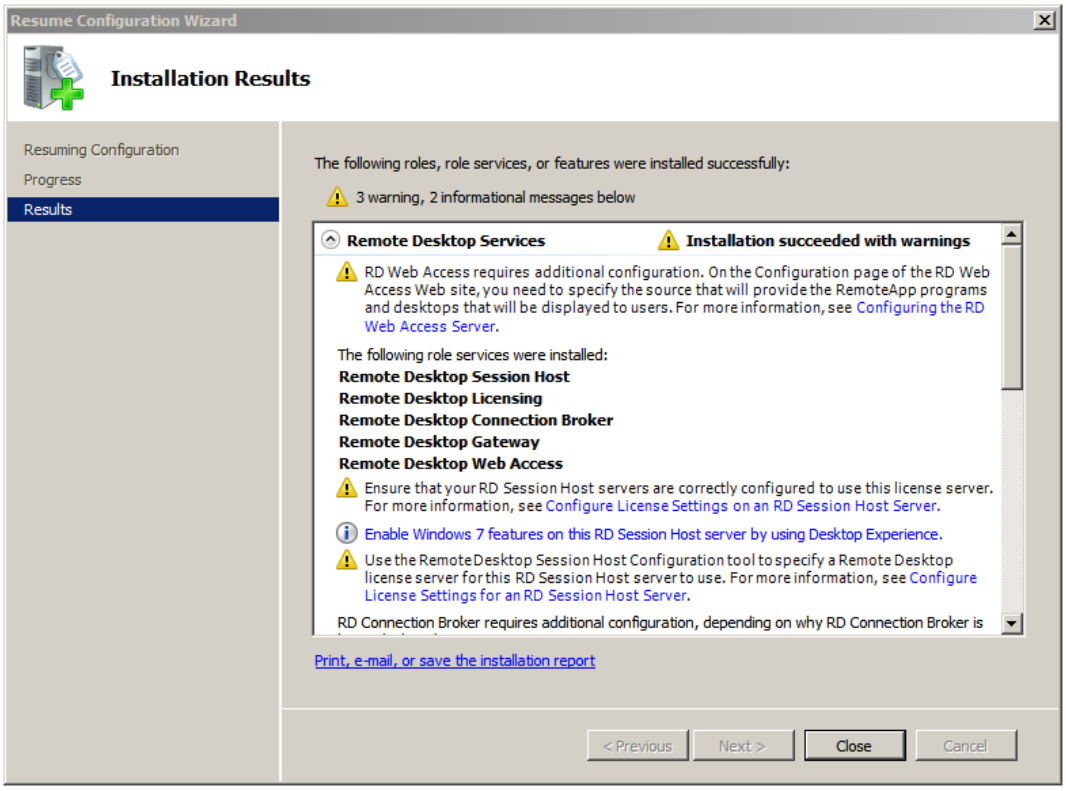
On Select Server Roles window click Routing and Remote Desktop. The next window in the wizard provides some information on the Terminal Server – Click Next to open the Select Role Services window. Check the Terminal Server and Licensing check boxes – Next – The next window in the wizard is used to select the kind of client access licenses that will be used. Select Configure later, and click Next. Select the Administrators groups and click Next.



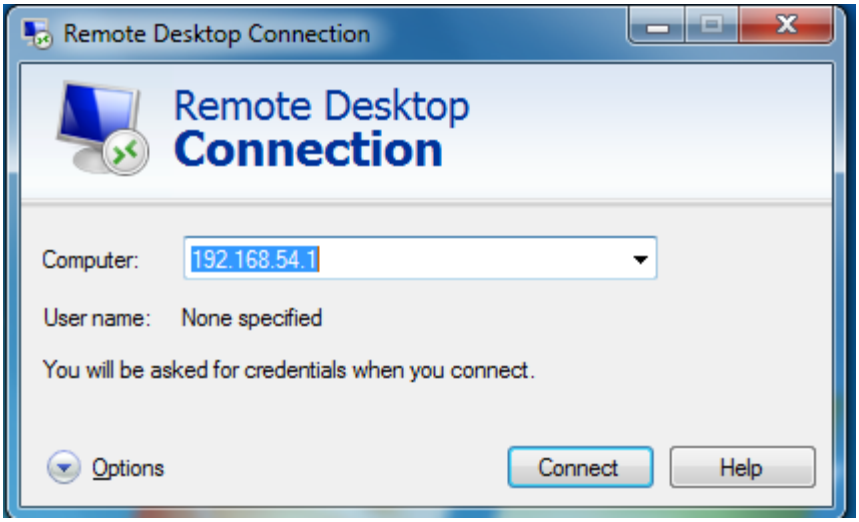
Click Install. – Close – The Add Roles Wizard dialog box opens, indicating that you must restart the computer. Click Yes and the computer reboots.

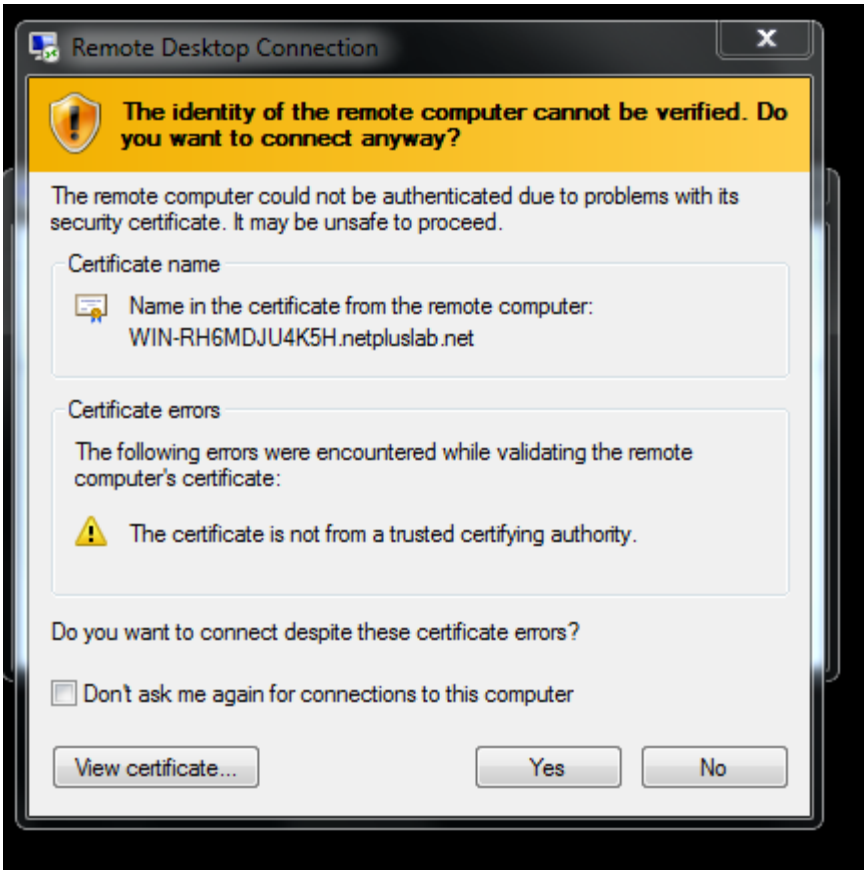


The Add Roles Wizard dialog box opens, indicating that you must restart the computer. Click Yes and the computer reboots.



Now you log onto Server 1 (from Workstation 1) while it is still configured in Remote Administration Mode. Log on to Workstation 1 - Start – All Programs – Accessories – Remote Desktop Connection. He Remote Desktop Connection dialog box opens.





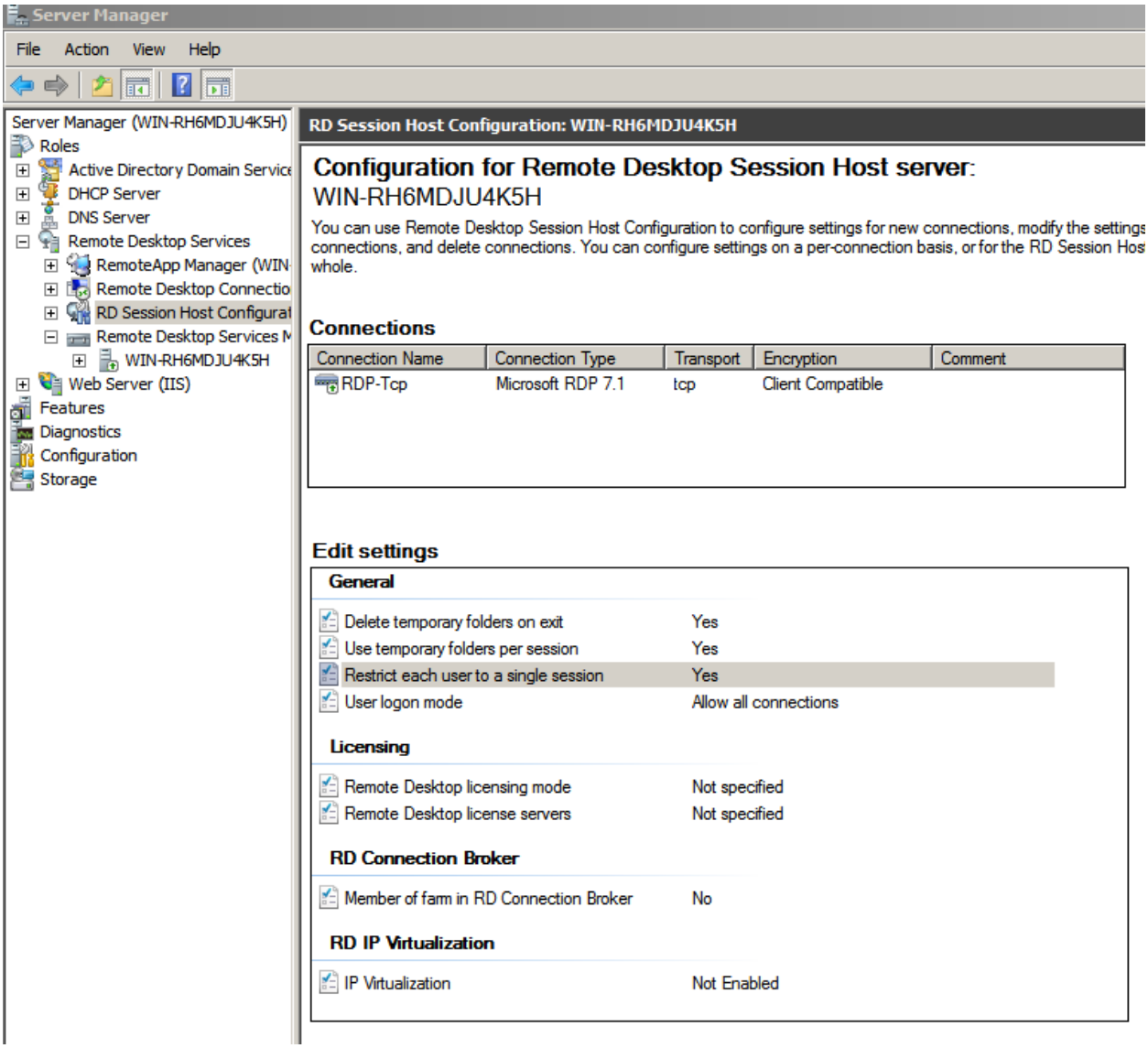
Select Yes. Log on to the remote computer as the Administrator. The Windows Server 2008 desktop appears. Minimize the Remote Desktop Connection. Repeat Steps 14 through 17. **Remote Desktop did not allow me to open two sessions.**

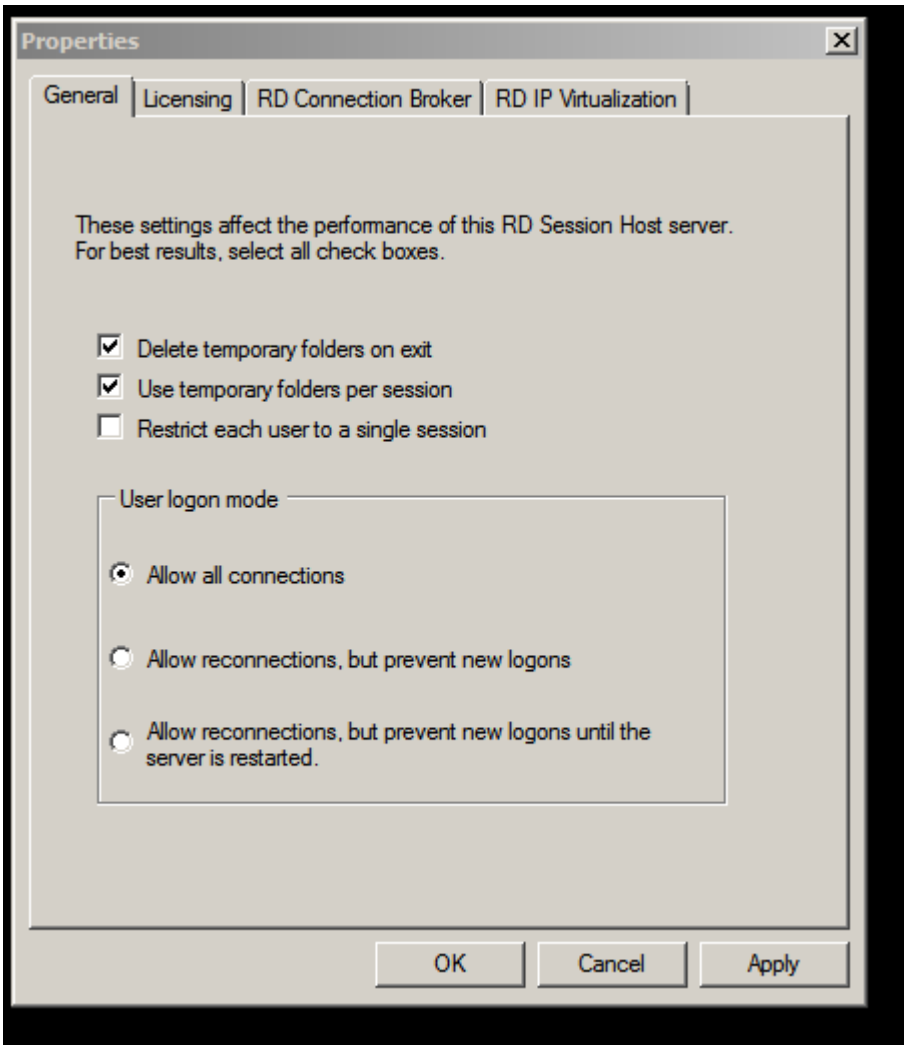
On Server 1 press CTRL+Alt+Del. Log on

Skip steps 20 through 31.

Now you configure the Server so that users can log on to multiple sessions. Right click the restrict each user to a single session icon.

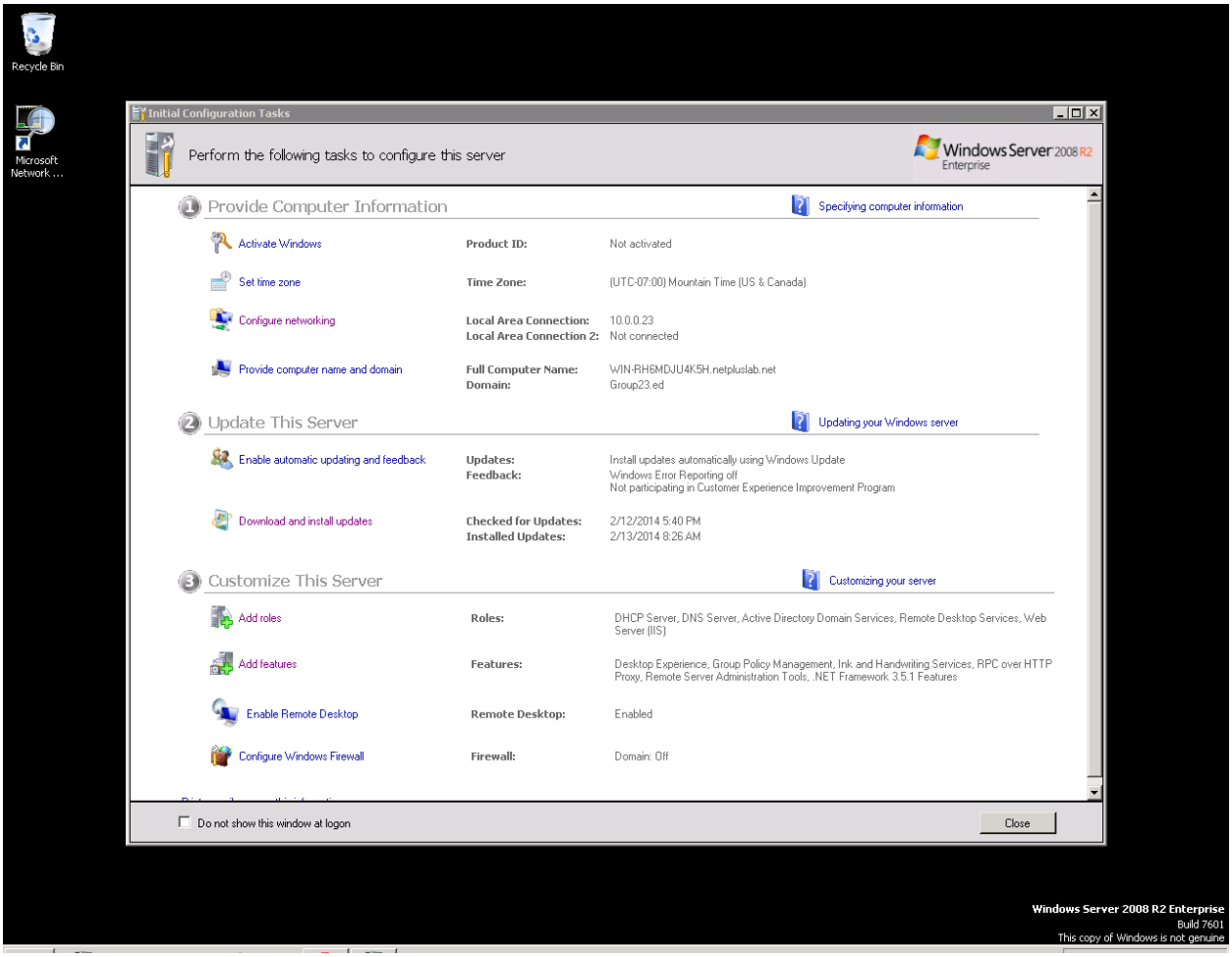
From the shortcut menu, click Properties. Restrict each user to a single session – OK



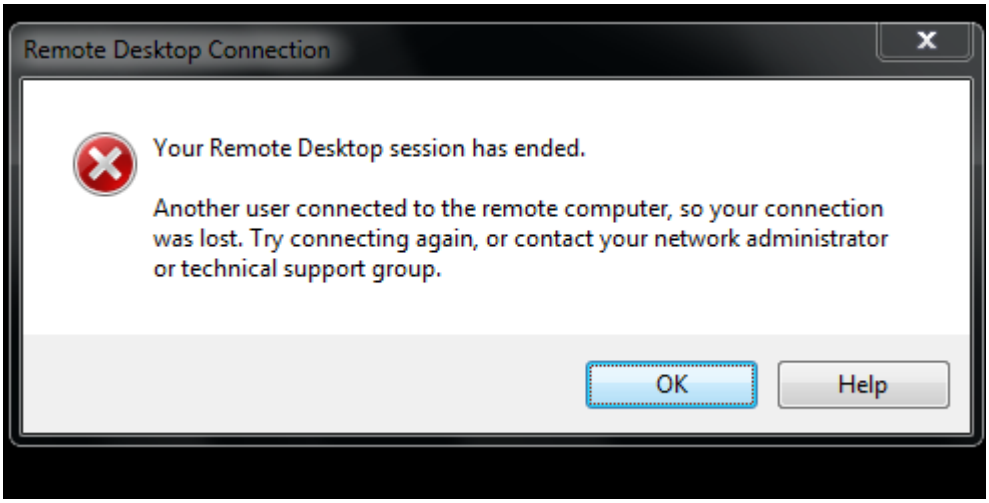


On Workstation 1 repeat steps 14 through 17. Repeat three more times, logging on each time as a different user.

The below picture is a snapshot of multiple sessions, it is a snapshot of the Server on the Workstation.

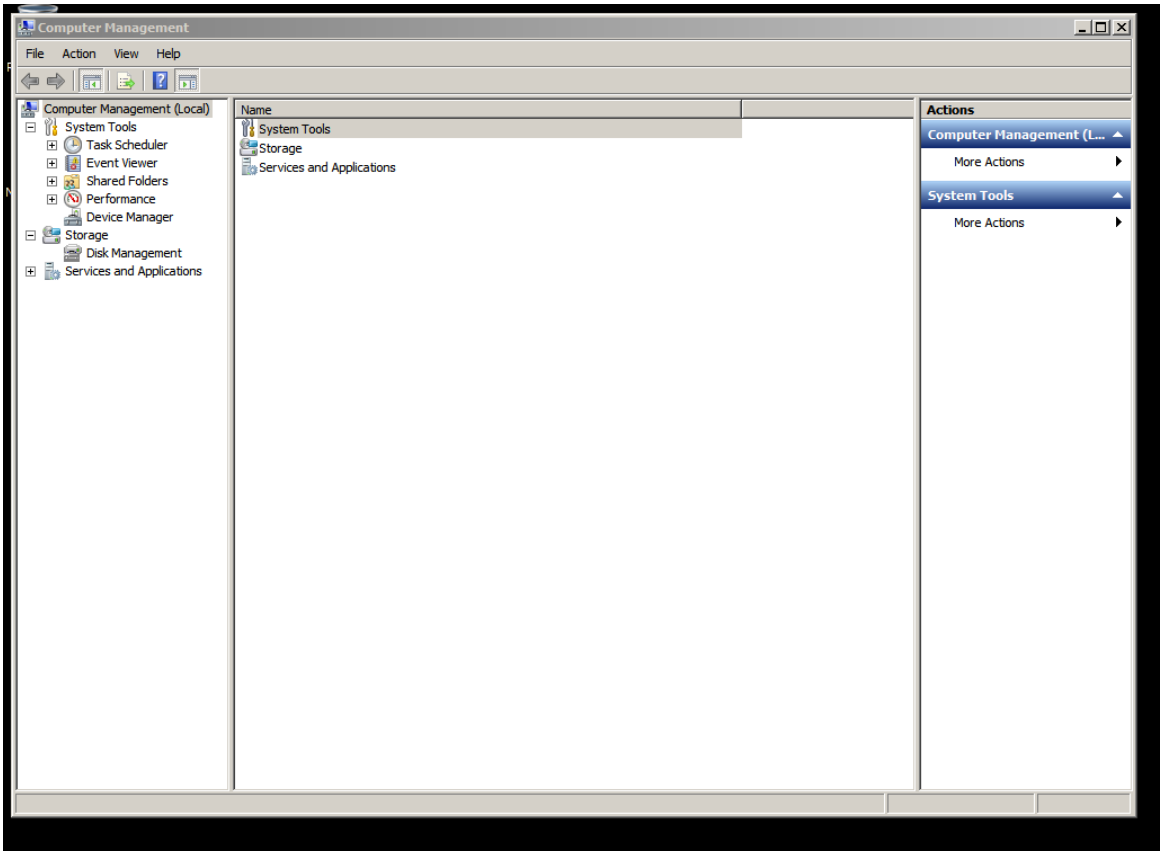


On Server 1, click the Start – Administrative Tools, point to Terminal Services, click Terminal Manager. The right pane of the window shows all the users currently logged on to the Server and their sessions. – Right click one of the sessions, and click, and click Disconnect from the short-cut menu. A Terminal Services Manager dialog box opens, indicating that each selected session will be terminated. Click OK. Repeat steps 35 and 36 for each remaining session.

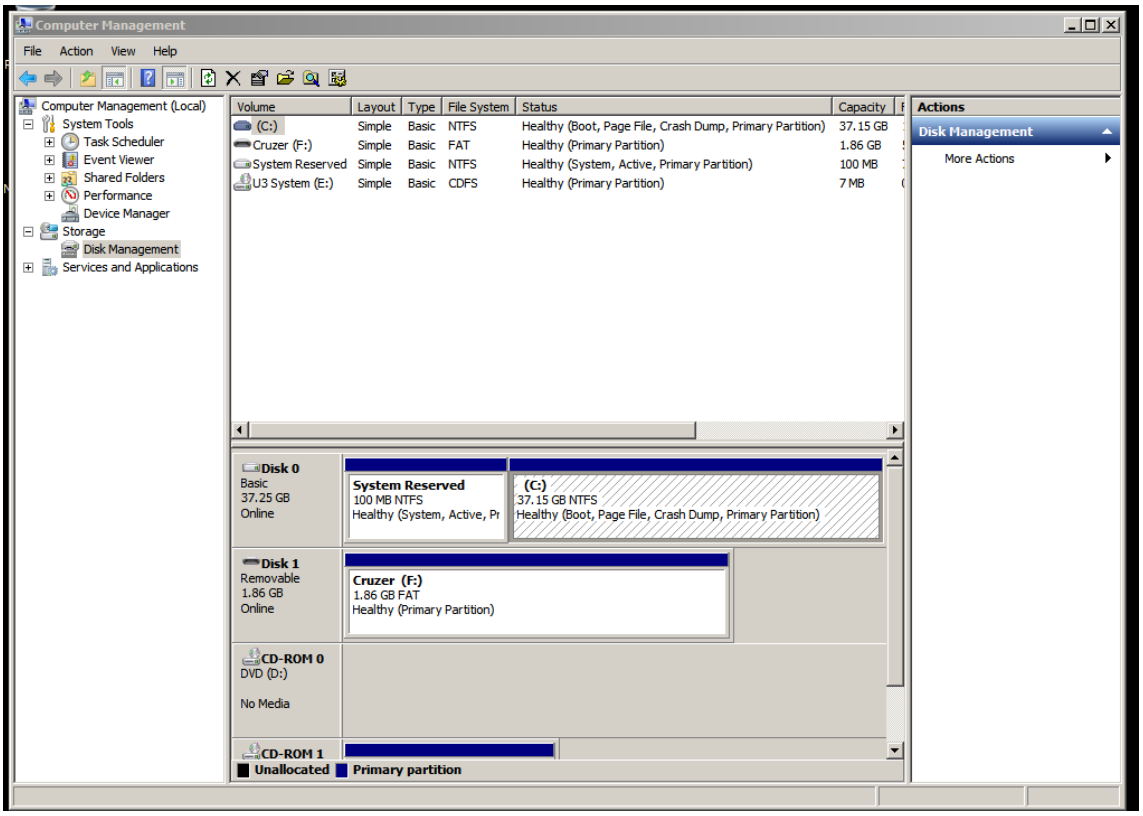


Lab 10.4 Remotely Managing a Computer with Active Directory

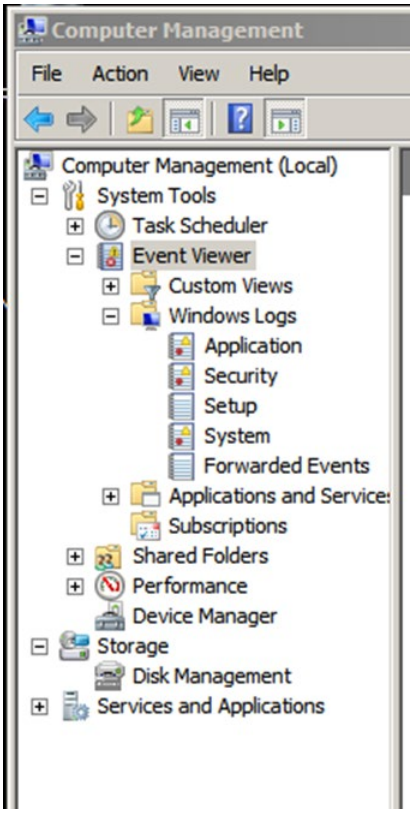
Log on to Server 1 – Start – Administrative Tools – Computer Management

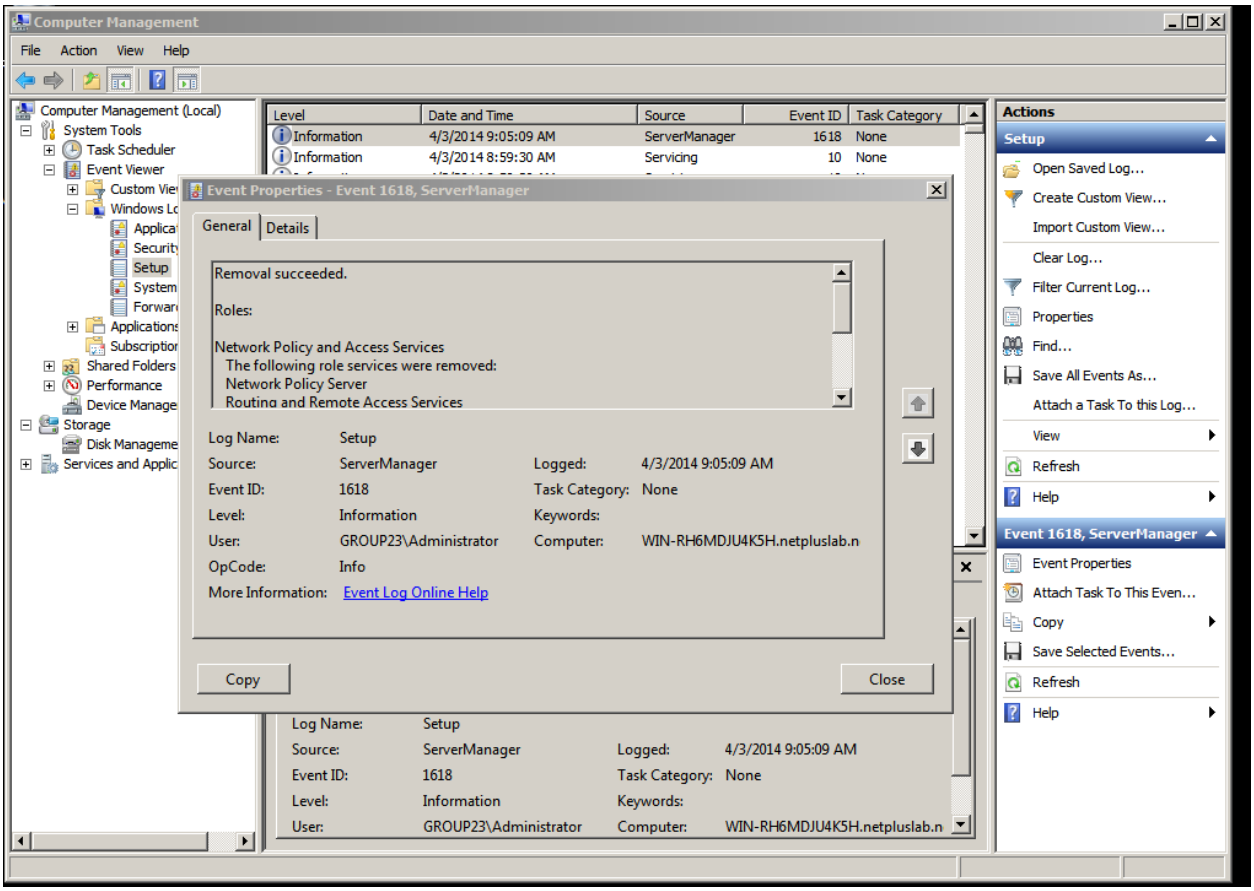


Click the Disk Management icon below Storage. How many hard disks are on the Server, how large are they, and with what file system have they been configured? **1 hard disk, 37.15 GB and NTFS.**

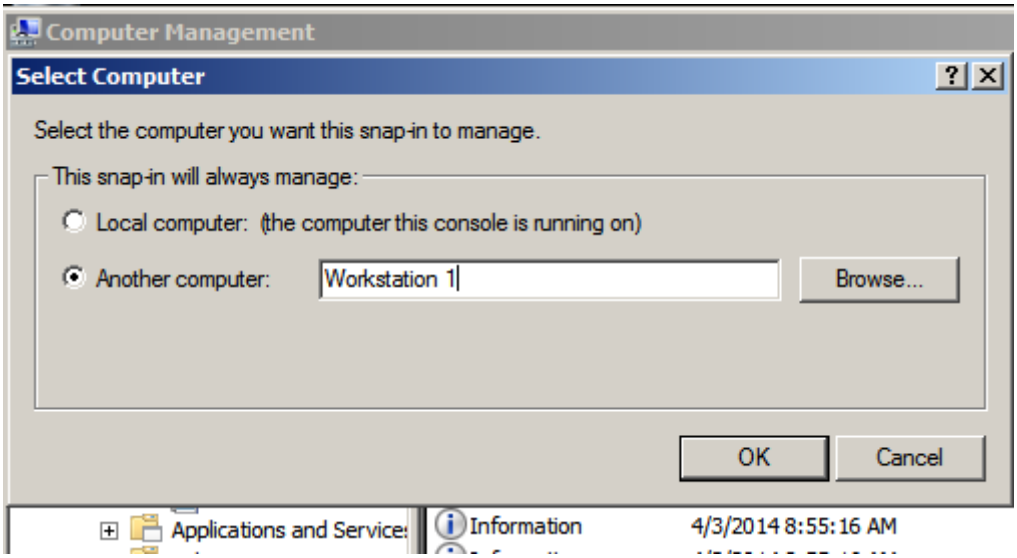


Click the Event Viewer and Windows Logs, and then double-click the System node.

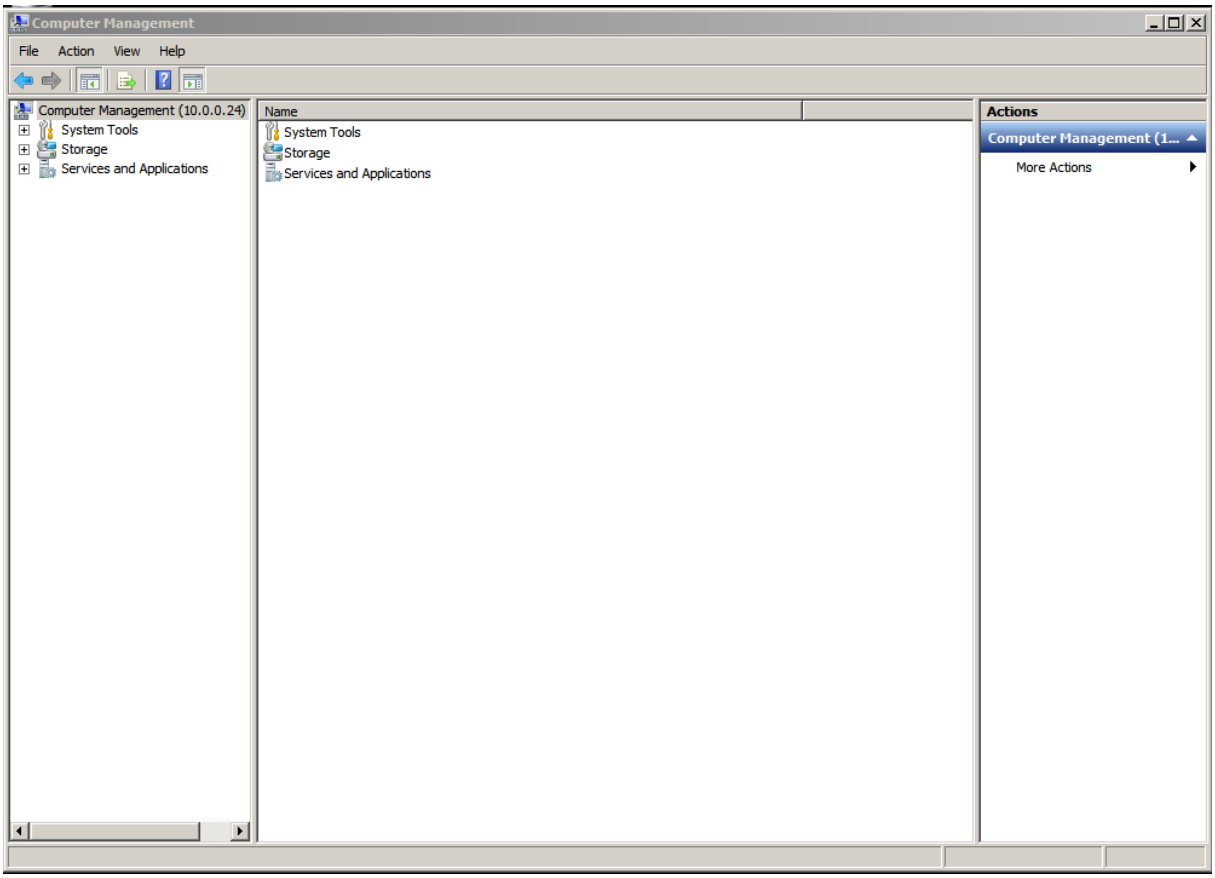




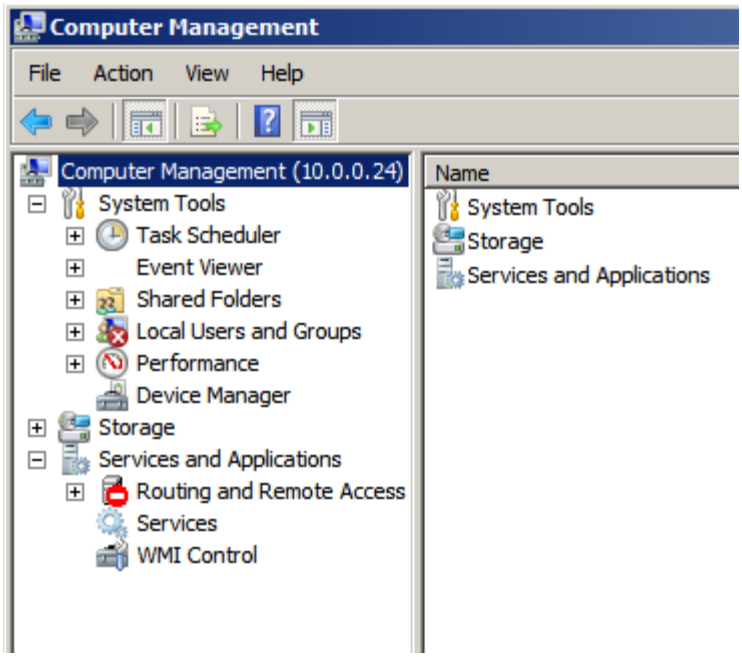
Scroll the arrow to view the events. – Close – Right click Computer Management – Select Connect to another computer – In the computer text box type the IP address of Workstation 1 – OK.



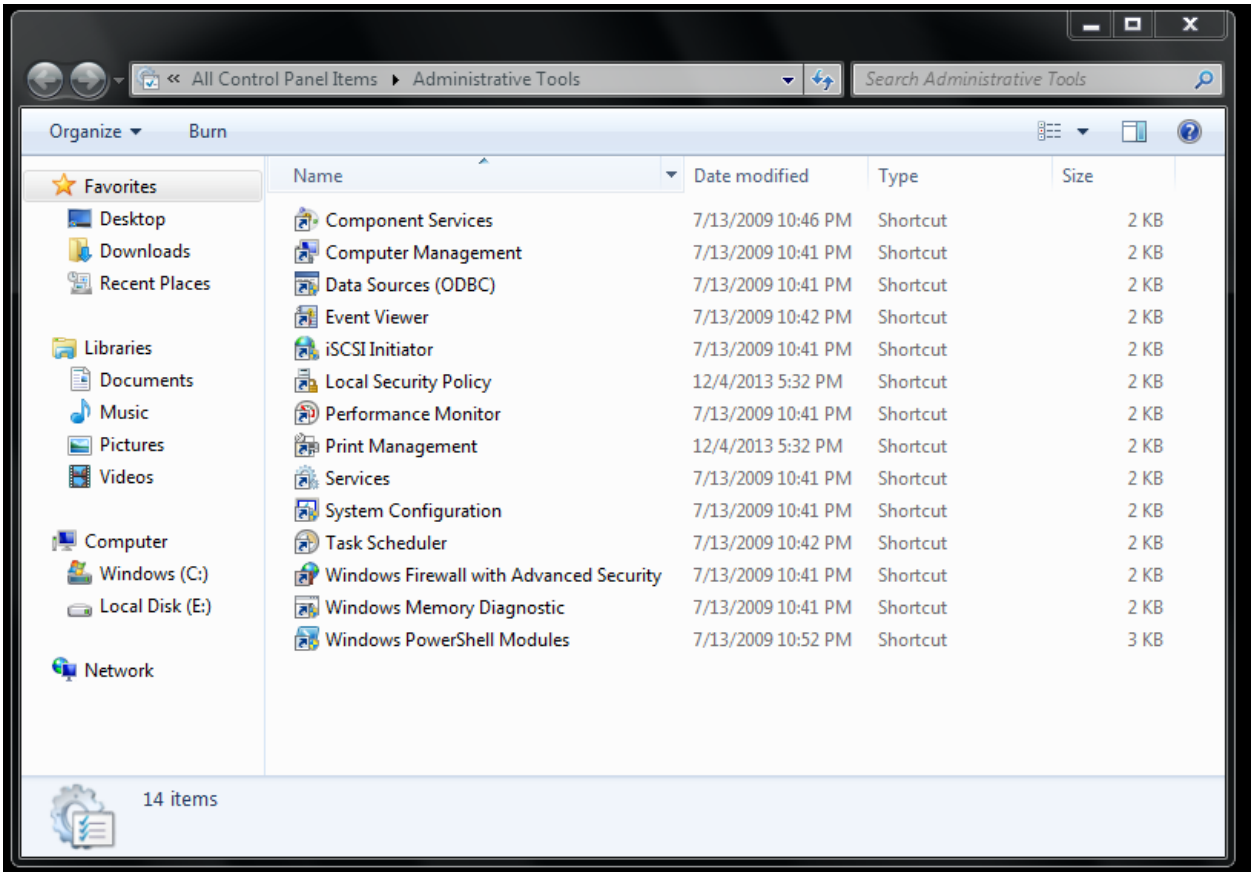
The icon at the top of the left pane changes to the Computer Management dialog box for Workstation 1 as you **manage the computer remotely**.



Click the plus sign (+) next to System Tools to expand the tree underneath it. Repeat this step with the Services the Services and Applications icon.



Repeat Steps 4 through 7 on Workstation1.



Administrative Tools

Administrative Tools is a folder in Control Panel that contains tools for system administrators and advanced users. The tools in the folder might vary depending on which version of Windows you are using.

- Component Services. Configure and administer Component Object Model (COM) components. Component Services is designed for use by developers and administrators.

• Computer Management. Manage local or remote computers by using a single, consolidated desktop tool. Using Computer Management, you can perform many tasks, such as monitoring system events, configuring hard disks, and managing system performance.

• Data Sources (ODBC). Use Open Database Connectivity (ODBC) to move data from one type of database (a data source) to another. For more information, see

• Event Viewer. View information about significant events, such as a program starting or stopping, or a security error, which are recorded in event logs.

• iSCSI Initiator. Configure advanced connections between storage devices on a network. Microsoft iSCSI Initiator is a tool that connects external iSCSI-based storage to host computers with an Ethernet network adapter.

• Local Security Policy. View and edit Group Policy security settings.

• Performance Monitor. View advanced system information about the central processing unit (CPU), memory, hard disk, and network performance.

• Print Management. Manage printers and print servers on a network and perform other administrative tasks.

• Services. Manage the different services that run in the background on your computer.

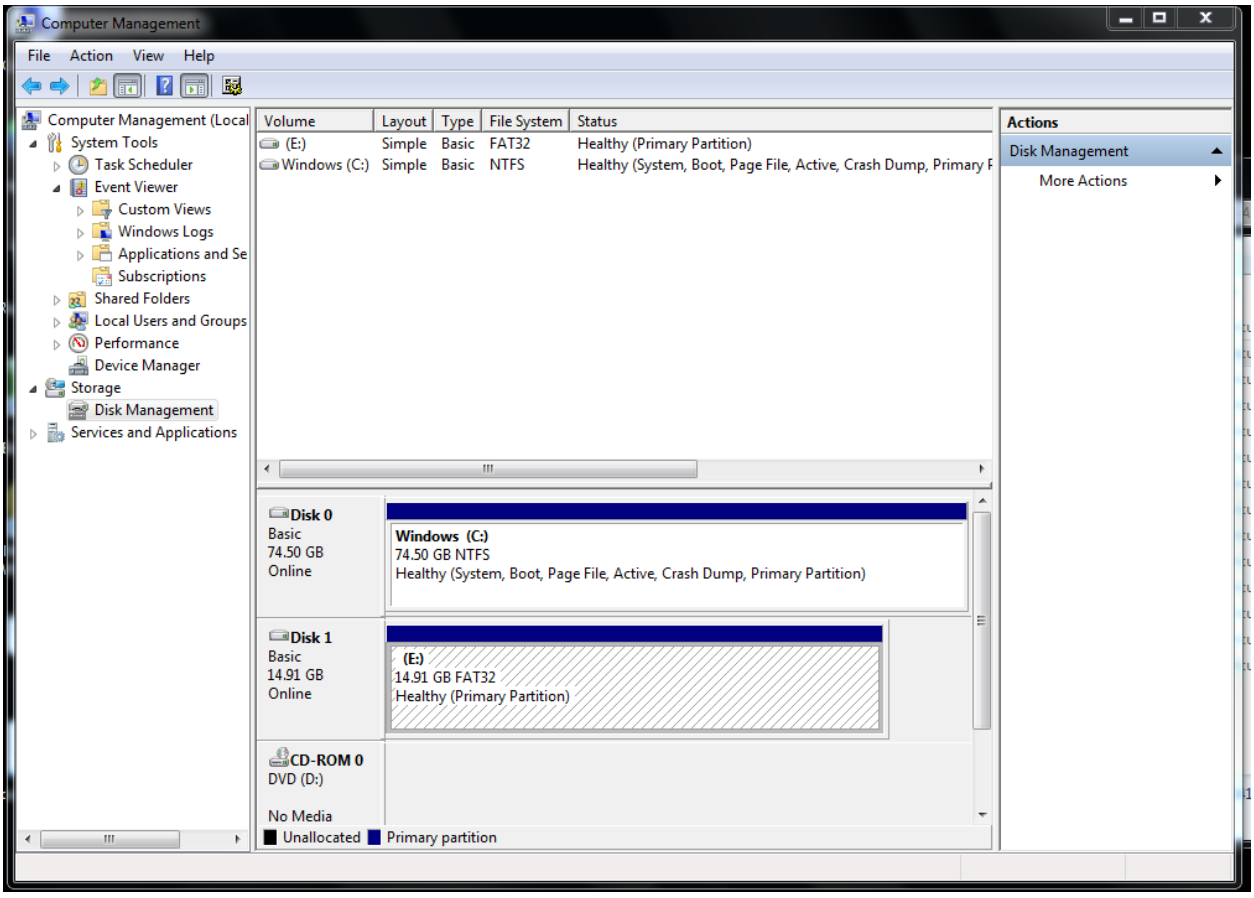
• System Configuration. Identify problems that might be preventing Windows from running correctly.

• Task Scheduler. Schedule programs or other tasks to run automatically.

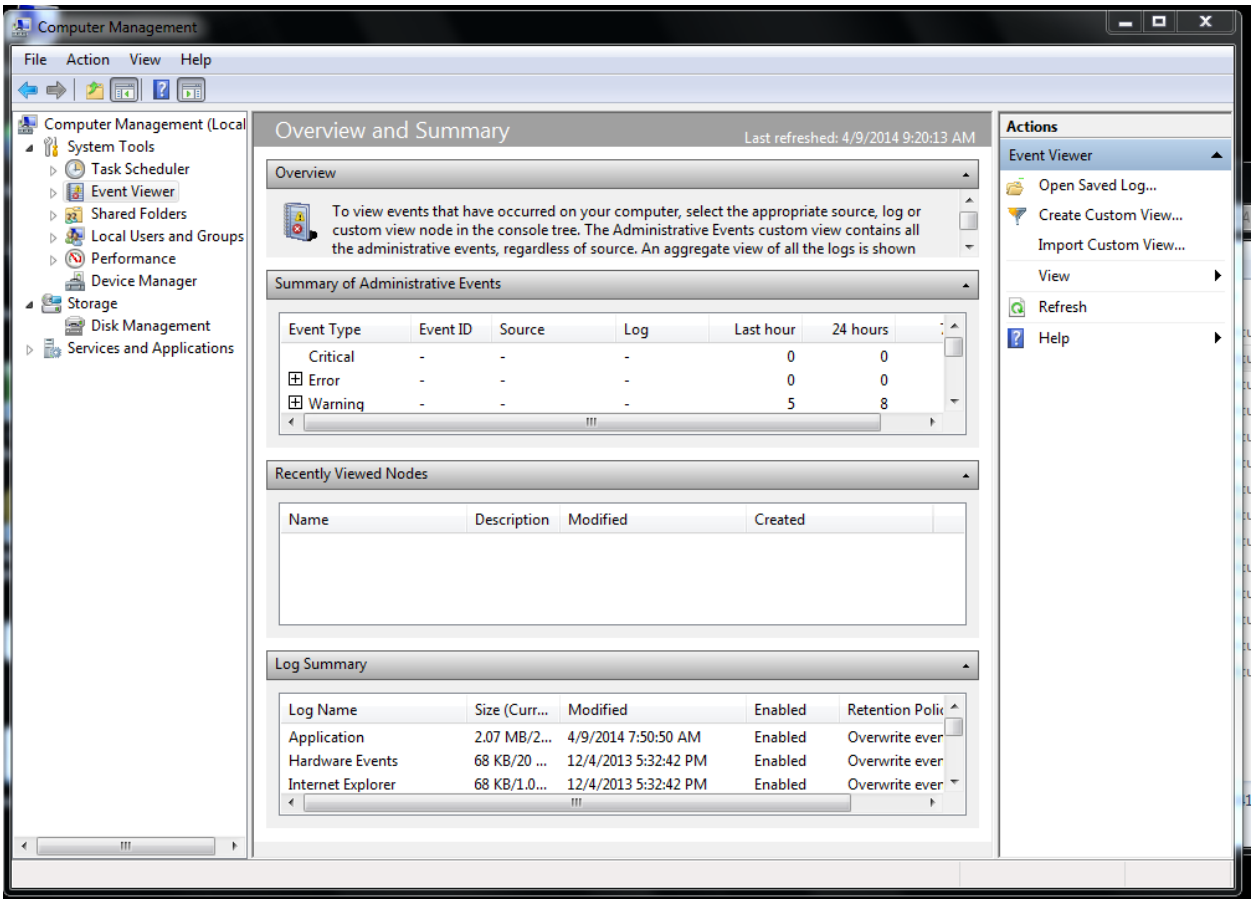
• Windows Firewall with Advanced Security. Configure advanced firewall settings on both this computer and remote computers on your network.

• Windows Memory Diagnostic. Check your computer's memory to see if it's functioning properly.

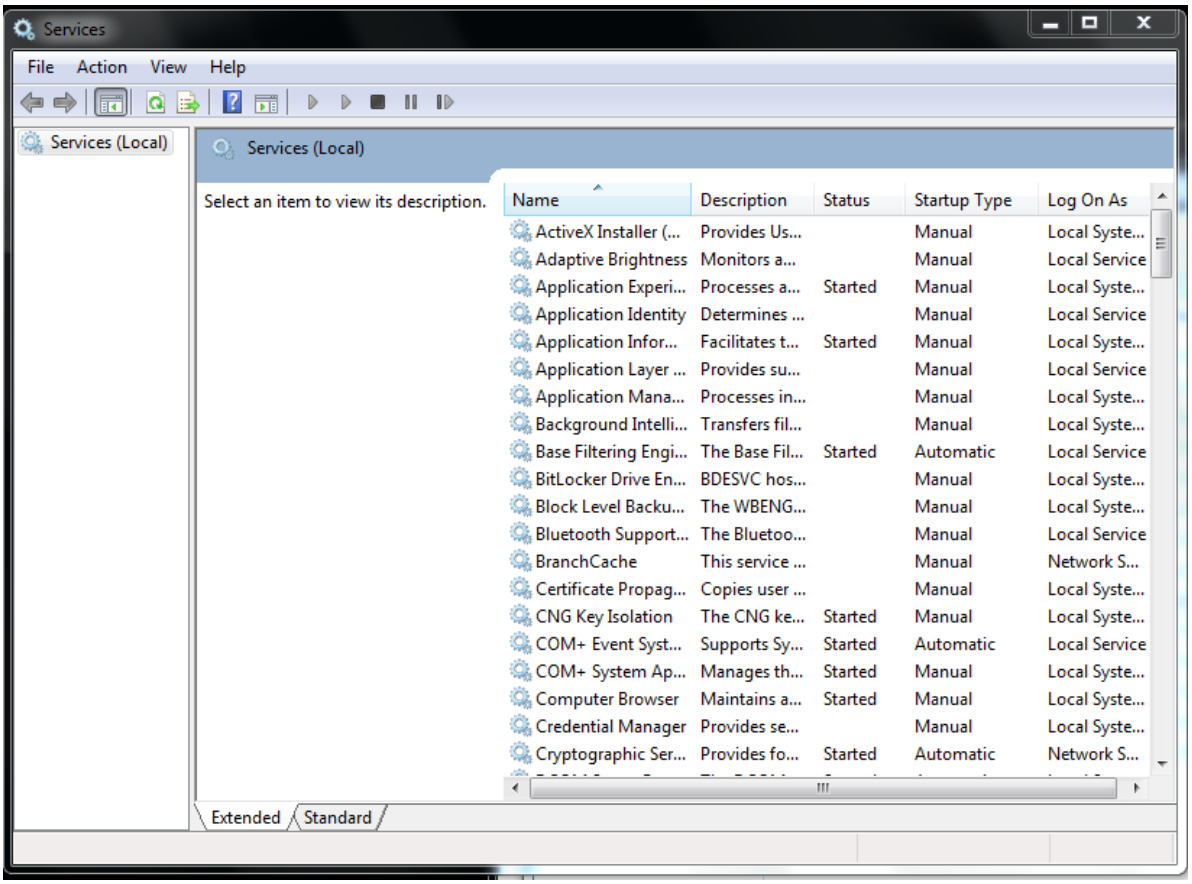
The Workstation has 1 disk drive, 74.50 GB and NTFS filing system



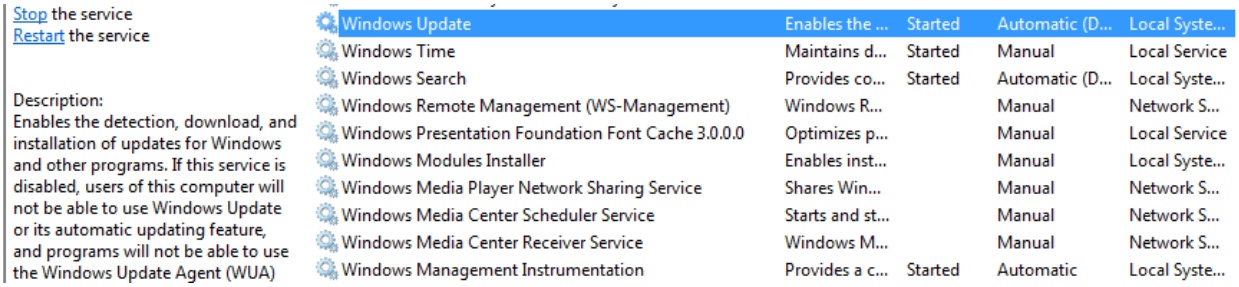
Double-click the System node. A list of events in the A System event log spears in the center pane.



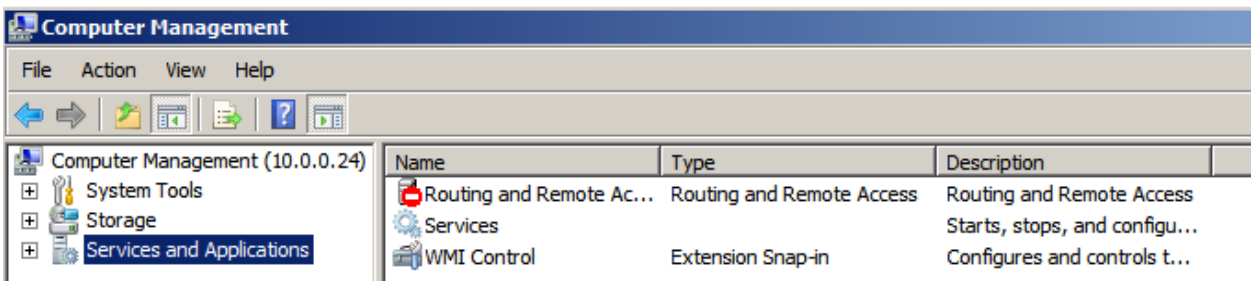
Log on to Workstation 1 – Control Panel – System and Security – Click Administrative Tools icon. The Services window opens.



Look for the Automatic Updates icon. Its status is started.

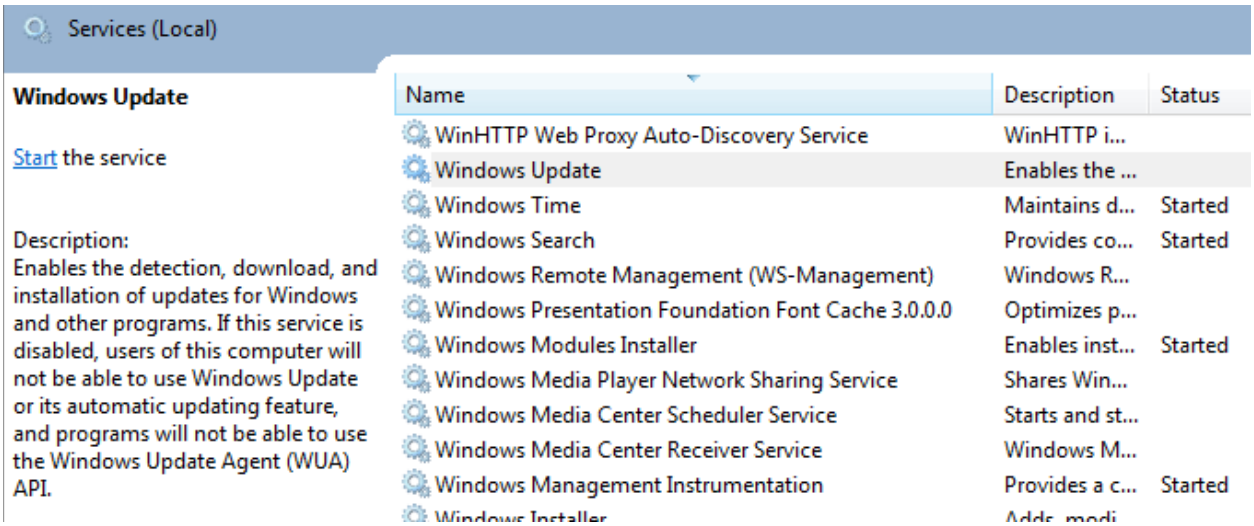


On Server 1 click Services icon in the left pane of the Computer Management window. A list of the services running in Workstation 1 appears.

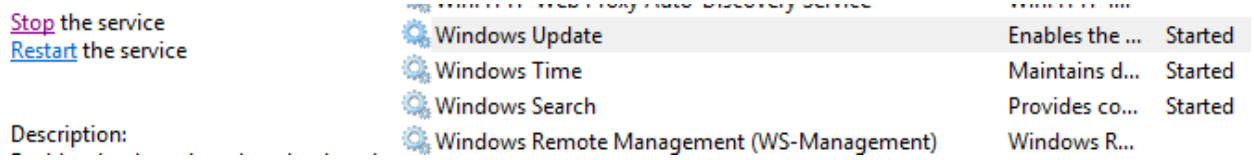


Right click the Windows Update icon, from the shortcut menu select Stop.

On Workstation 1, press F5 to refresh the Services window. The window is now blank, indicating that the service is not running.



Right-click the Windows Update icon, select start.



Log off both computers.

Lab 10.5 Remotely Managing a Linux Server

No matter how hard you try, you can't be everywhere at once. Servers and workstations that you need to support can be based in various locations, sometimes even thousands of miles away. Physical access to these systems on short notice is impossible. Fortunately, there are several widely used remote administration methods for Linux that let you cross that distance in little more than a few mouse clicks. Here are four major Linux remote administration utilities and some pluses and minuses for each.

Using Secure Shell

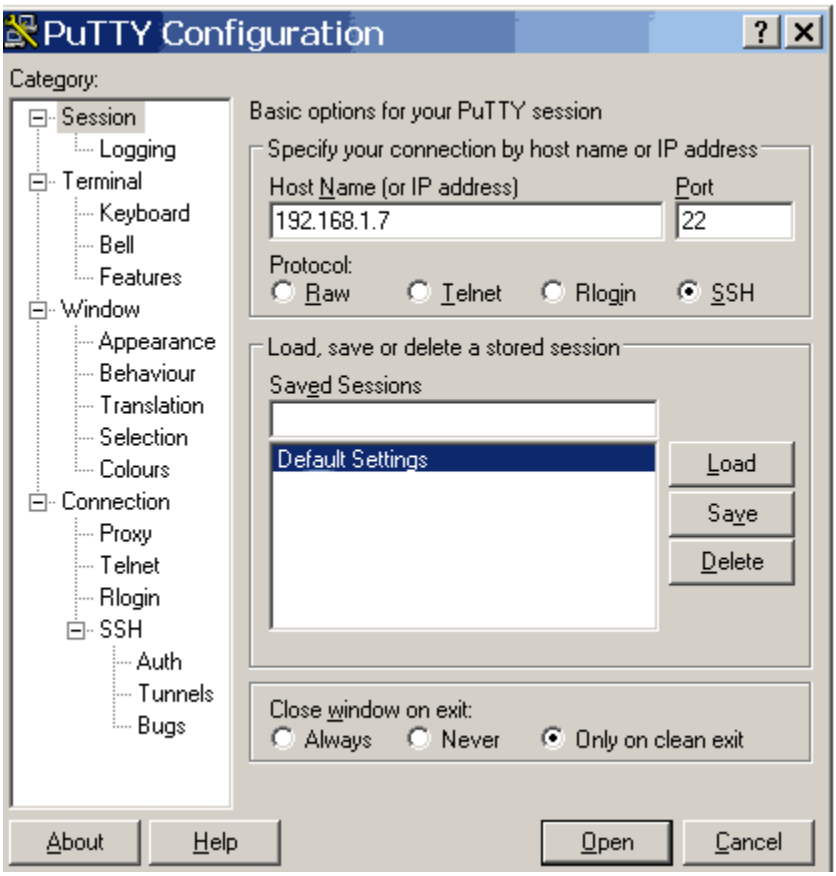
Secure Shell (SSH) is probably the most popular remote administration tool. SSH offers command line access over an encrypted tunnel. Many Linux distributions come with an SSH server already installed. As with any tool, patches must be installed and restrictions should be put in place to keep unauthorized users from using the service.

Once you have an SSH server installed, configuring it is fairly easy. There are a couple of major settings that you should have in place to minimize risk, including:

PermitRootLogin—This value should be set to No, since root should never log in remotely. If you want to administer the box, create a normal user and SSH in with that account. Once in, you can use the su command to log in as root.

X11 Forwarding—This value will be used for getting a graphical connection. If you just want to use the console, you can set this value to No; otherwise, set it to Yes.

If you don't have an SSH server installed, you can use your Linux distribution's RPM installer to get it up and running. Once you've accomplished that, connecting is fairly simple. First, you need to obtain a client. My favorite free SSH client is PuTTY, which you can download from the PuTTY Web site. PuTTY is a great little utility that allows you to connect to remote systems using various protocols, including SSH and Telnet. Configuring PuTTY is very easy. To connect to a remote system, all you have to do is fill in the host name or IP address to connect to, and select SSH for the connection type, as shown in Figure A.



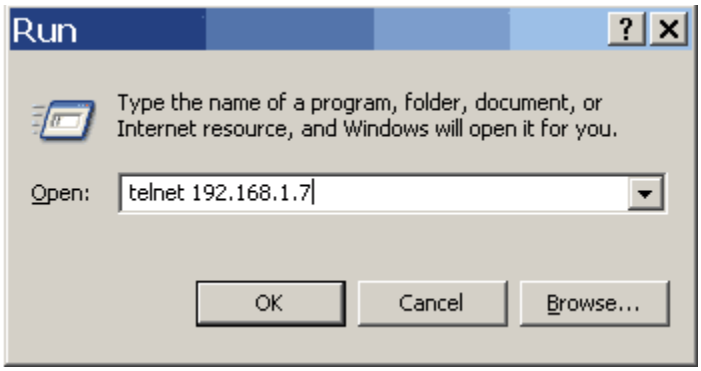
Once you connect to the remote system, you have full shell access allowing you to issue commands as you would from the console.

Using Telnet

Telnet, much like SSH, allows for remote console-level access to a system. The major difference between these two is that Telnet is not encrypted, meaning it is open for all to see. Most major Linux distributions come with a Telnet package that can be installed, but is not by default.

You can install a Telnet daemon using your distribution's RPM installer. Because of the inherent insecurity in using an unencrypted connection, most distributions have the Telnet service disabled. Most Telnet daemons run through Xinetd, a management system for services. To enable a Telnet daemon that runs through Xinetd, edit the /etc/xinetd.d/telnet file and change the value for Disable to No. Then, type service xinetd restart to have the changes take effect.

Connecting to a server with Telnet is even easier than with SSH. Nearly every operating system has a built-in Telnet client, including such obscure operating systems as OS/2. If you prefer, you can still use PuTTY and just select Telnet instead of SSH. To connect using the built-in Windows client, use the Run dialog box from the Start menu, as shown in Figure B.



Once connected, you'll be presented with a standard logon prompt. You can remotely manage your system from the console, as you can with SSH.

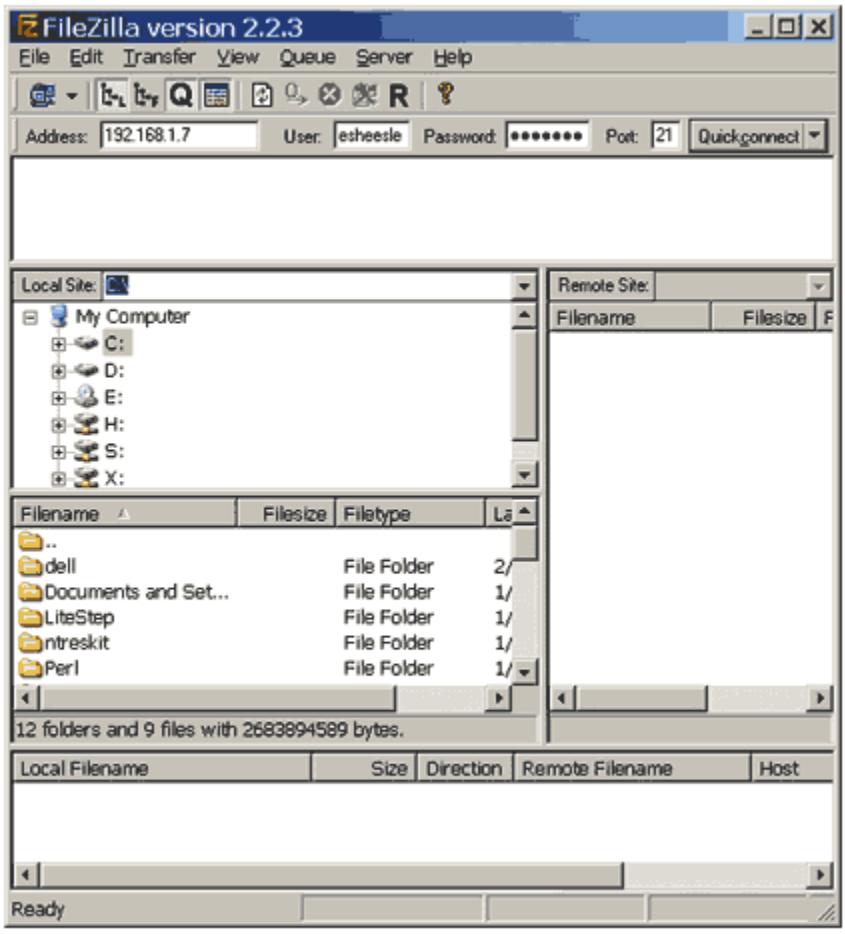
Using FTP

FTP, a file transfer mechanism, can’t be used for major remote administration but is great for transferring files that you may need on the remote workstation. FTP is not encrypted, but there's an encrypted alternative, SFTP.

Most distributions come with an FTP service that you can install by using the RPM installer. Note that most of the major Linux FTP servers have had major vulnerabilities found, so make sure to get the latest version. If you have an SSH server installed, you can also use SFTP through it.

My favorite file transfer program is FileZilla. It's free and supports both FTP and SFTP. You can download it from the FileZilla Web site. Connecting to your FTP server using FileZilla is fairly simple. You need to fill in the host name to connect to, your username, password, and finally the

port, as shown in Figure C. The port to connect to depends on whether you're using FTP or SFTP to connect. FTP is commonly run on port 21, whereas SFTP is on port 22 with SSH.



Once connected, you can use the FileZilla graphical interface to move files between your local system and the remote system. If you're uploading many files, FileZilla will automatically establish multiple connections to minimize upload or download time.

Using X

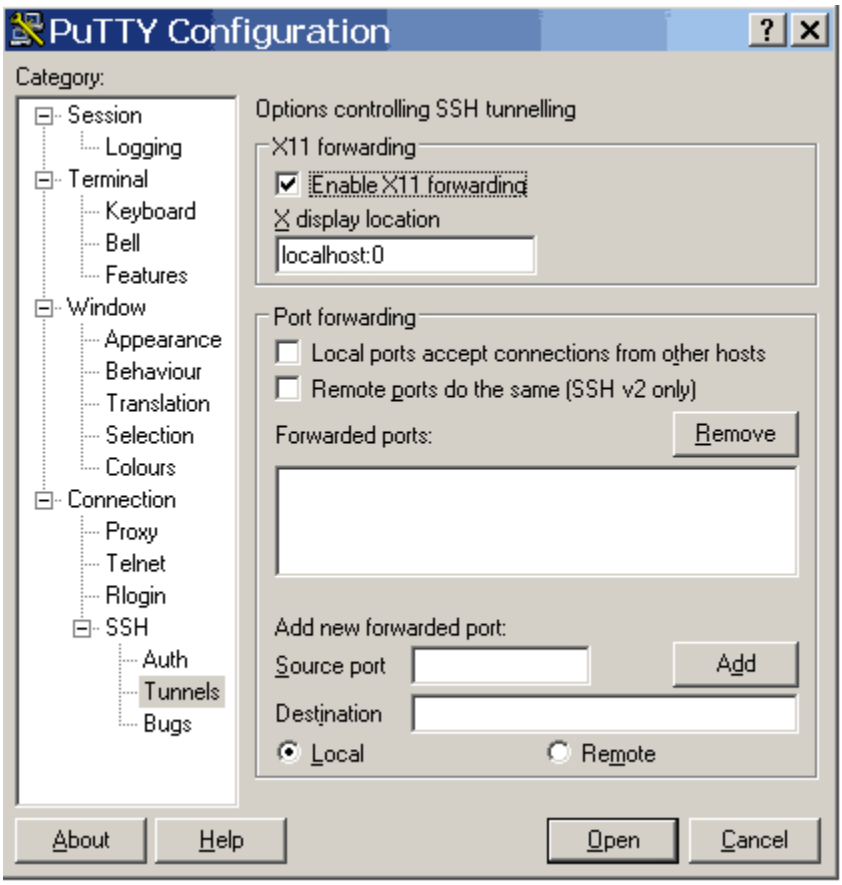
Using an X Server to manage a system remotely allows you full graphical access to the remote machine. X is the graphical interface used by most Linux distributions. It can function as both a local and remote graphical server.

There are several ways to establish an X session, but the most secure of these is to connect to your server with SSH or Telnet and spawn back your X window. This method prohibits users that are not authenticated from getting access. X sessions are a fairly secure and very efficient method for managing remote servers. However, many corporate firewalls block outbound X traffic.

Several components are needed to make remote X sessions work. The first of these is an X Server. Linux has the native X Server, but to get a connection on a Windows system, you need an X Server for that as well. Cygwin has an X Server that can be installed, along with support for many other features similar to Linux. You can get Cygwin from Red Hat.

When you install Cygwin, make sure to include the X Server. You also need to have some way to connect to the remote machine (such as using SSH). Once you start Cygwin, you'll get a prompt; just type startx. This will open another window with several local xterms running in it. Now that you have X Server up and listening, you can spawn back windows from your remote server.

The next step is to connect to your server. For the purposes of this article, I'll use PuTTY to connect via SSH and spawn back a shell. To set up PuTTY to automatically forward X requests back to your X Server, go to the SSH | Tunnels configuration option and check the Enable X11 Forwarding option, as shown in Figure D.



Connect to the remote host, type xterm, and press [Enter]. After several seconds, a new window will appear in Cygwin's X window. This new window gives you full access to your server. From this window, you can run most applications that you could run locally on the server.

Review Questions

1. What is the difference between the SSH protocol and the Telnet protocol?

SSH is encrypted

Telnet vs SSH

Secure Shell, commonly known as SSH, and Telnet are two network protocols that have been used widely at one point in time or another. They are both used to connect to remote servers in order to facilitate some sort of communications. The primary difference, which also led to one superseding the other, is in security. SSH offers security mechanisms that protect the users against anyone with malicious intent while Telnet has no security measures whatsoever.

Telnet was designed to work within a private network and not across a public network where threats can appear. Because of this, all the data is transmitted in plain text, including passwords. This is a major security issue and the developers of SSH used encryptions to make it harder for other people to sniff the password and other relevant information. Telnet also omits another safety measure called authentication. This ensures that the source of the data is still the same device and not another computer. Without authentication, another person can intercept the communication and do what he wishes. This is also addressed in SSH as it uses a public key to authenticate the source of the data.

2. Which of the following commands could you use to display a Linux computer's IP address?

ifconfig

3. Why might a virtual NIC be configured on a Linux computer?

For the computer to act as a router between two networks.

4. The **ssh** command allows you to open a remote terminal window on another computer. What is the major difference between working in an **ssh** session on a remote computer in another city and working directly at the console of a remote computer?

You cannot power cycle the remote computer.

5. In this lab, how could you tell whether a terminal window was for the local computer or for an SSH session on a remote computer ?

The prompt indicated the name of the remote computer.

`

Joseph Martinez

Networking II: Network +

CNG – 125

Chapter Eleven Labs

Network Security

Lab 11.1 Auditing

Lab 11.2 Checking for Vulnerable Software

Lab 11.3 Implementing Network Address Restrictions on a Linux Server

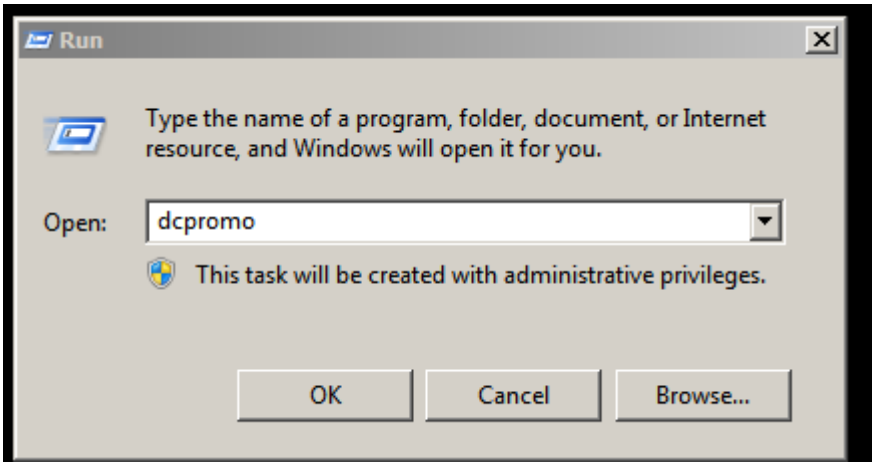
Lab 11.4 Plaintext versus Encrypted Protocols

Lab 11.5 Securing a Wireless Network

Lab 11. 6 Delegating Administrative /rights

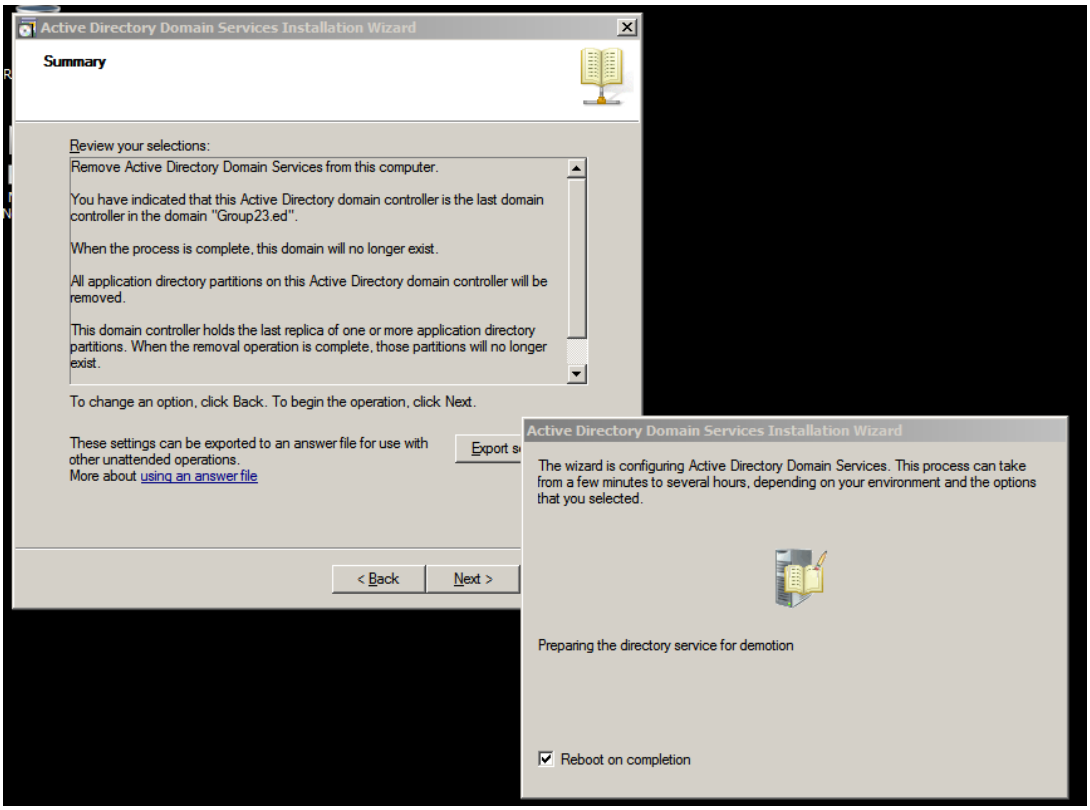
Lab 11.1 Auditing

Log on to Server – open Run dialog box – type **dcpromo** – Enter

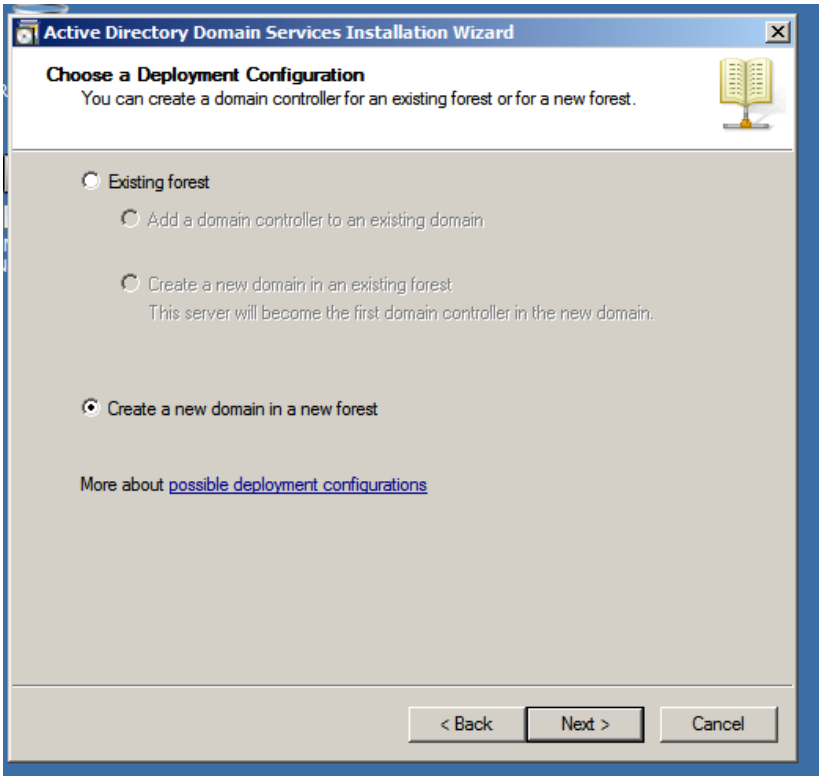


If Terminal Services is installed on the computer, Active Directory Services Wizard dialog box opens.

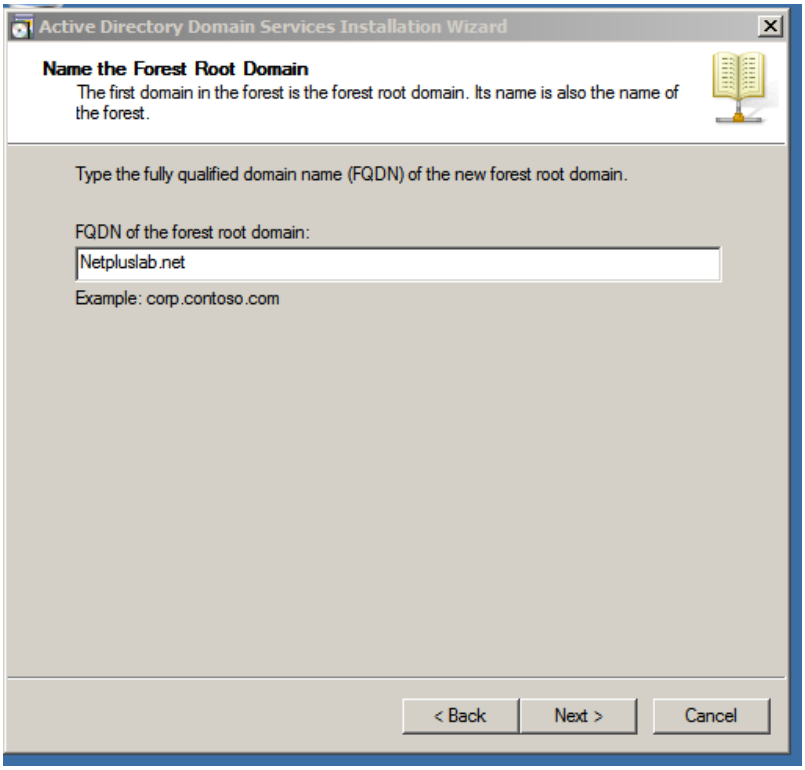
Click Next -



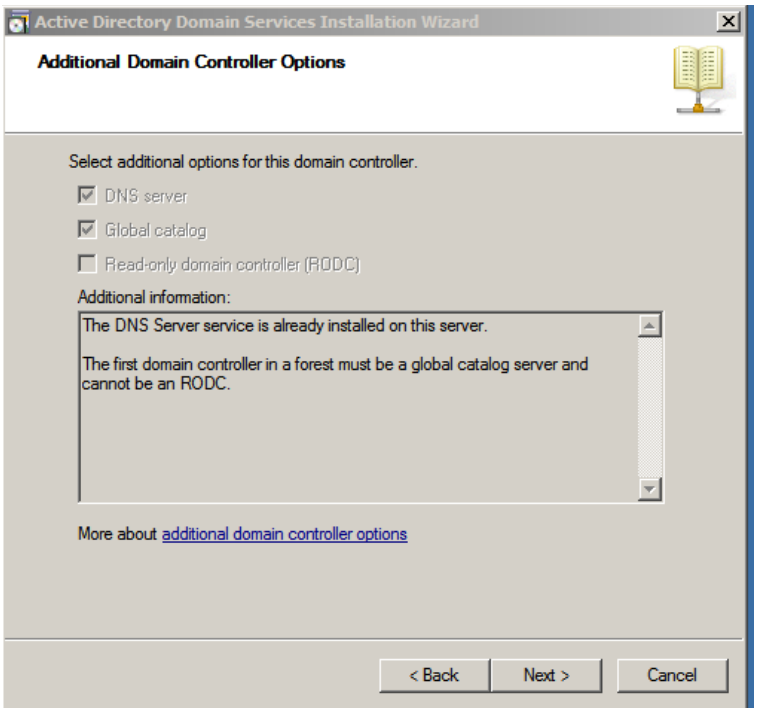
Make sure that the Create a new domain in new forest option is selected –



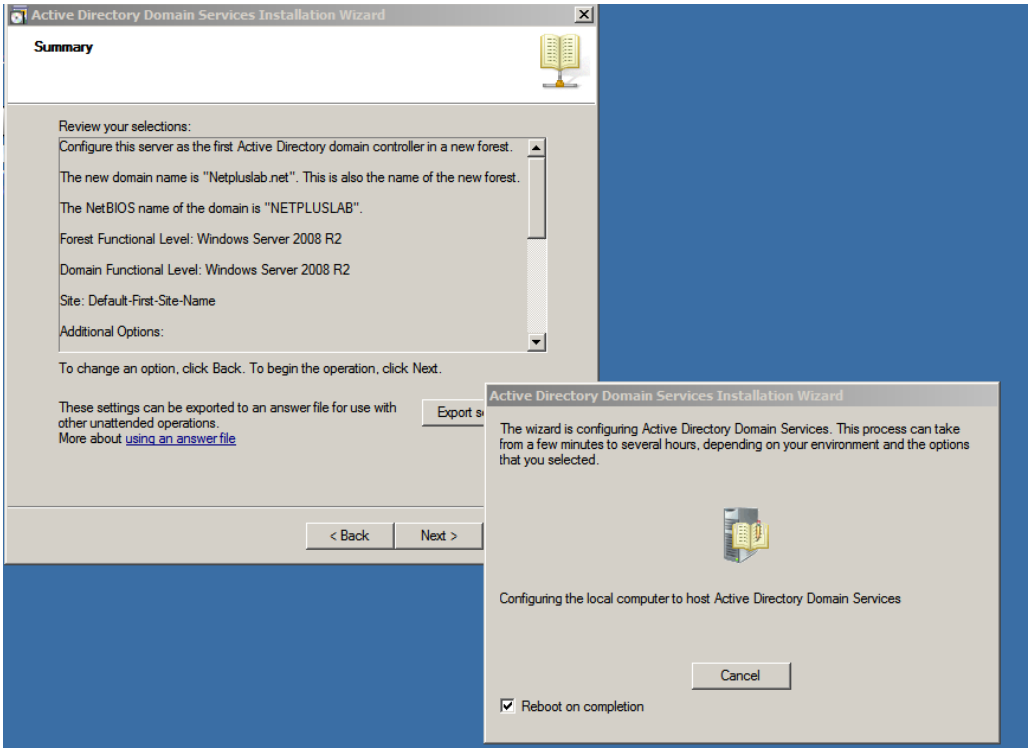
Next – Type Netpluslab.net



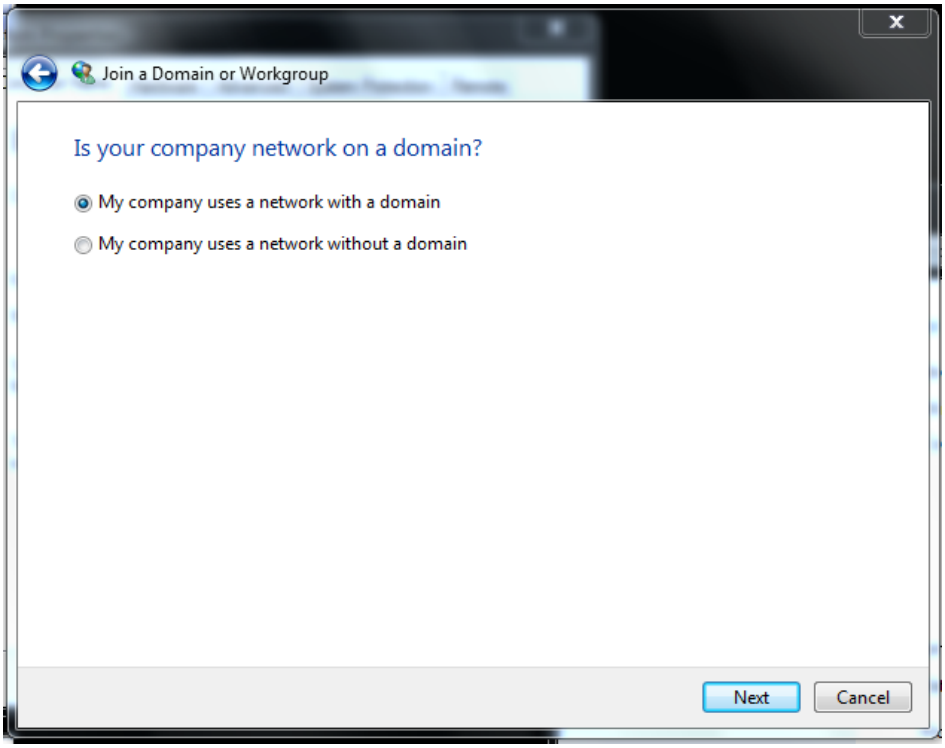
After several moments, the wizard asks you to select the forest functional level. Select Windows Server 2008, and click Next. The wizard then asks you to select additional options for the domain controller. Make sure DNS server is selected, and click next.

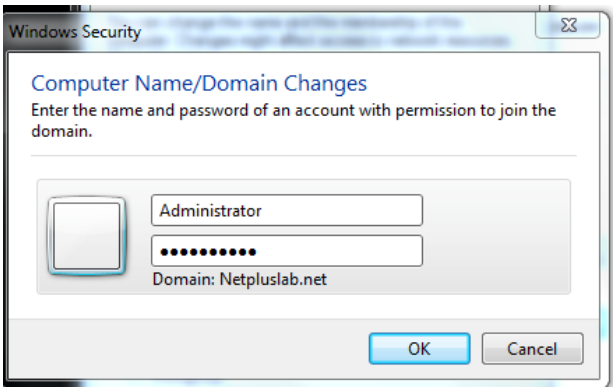


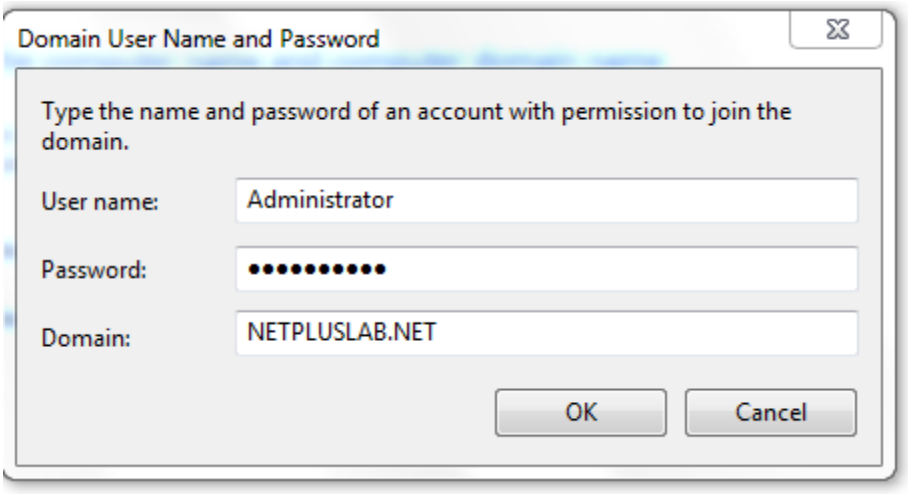
The wizard asks you to specify the location of database and log files for Active Directory.



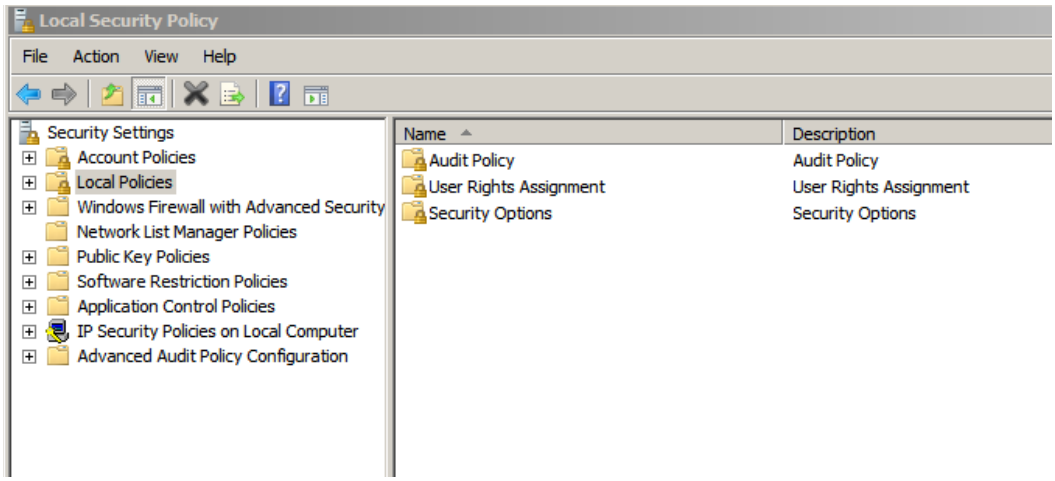
Select defaults – Next – Next – Restart now. Log on – Properties – Change Settings – Network ID – Next – My company uses a network domain - Next



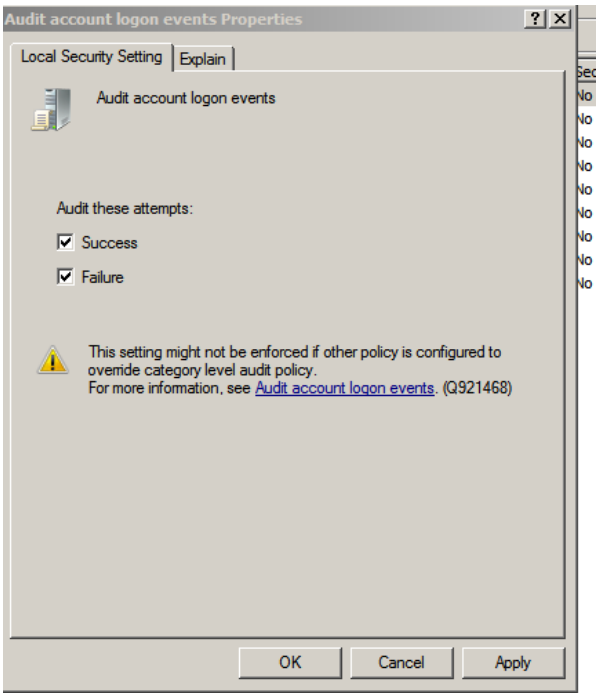




Next. Click do not add a domain user account. Next – Finish – OK – Reboot – Log on to the NETPLUSLAB domain as the domain administrator. – Skip to Step 33 – Log on to the Server – Administrator Tools – Local Security Policy

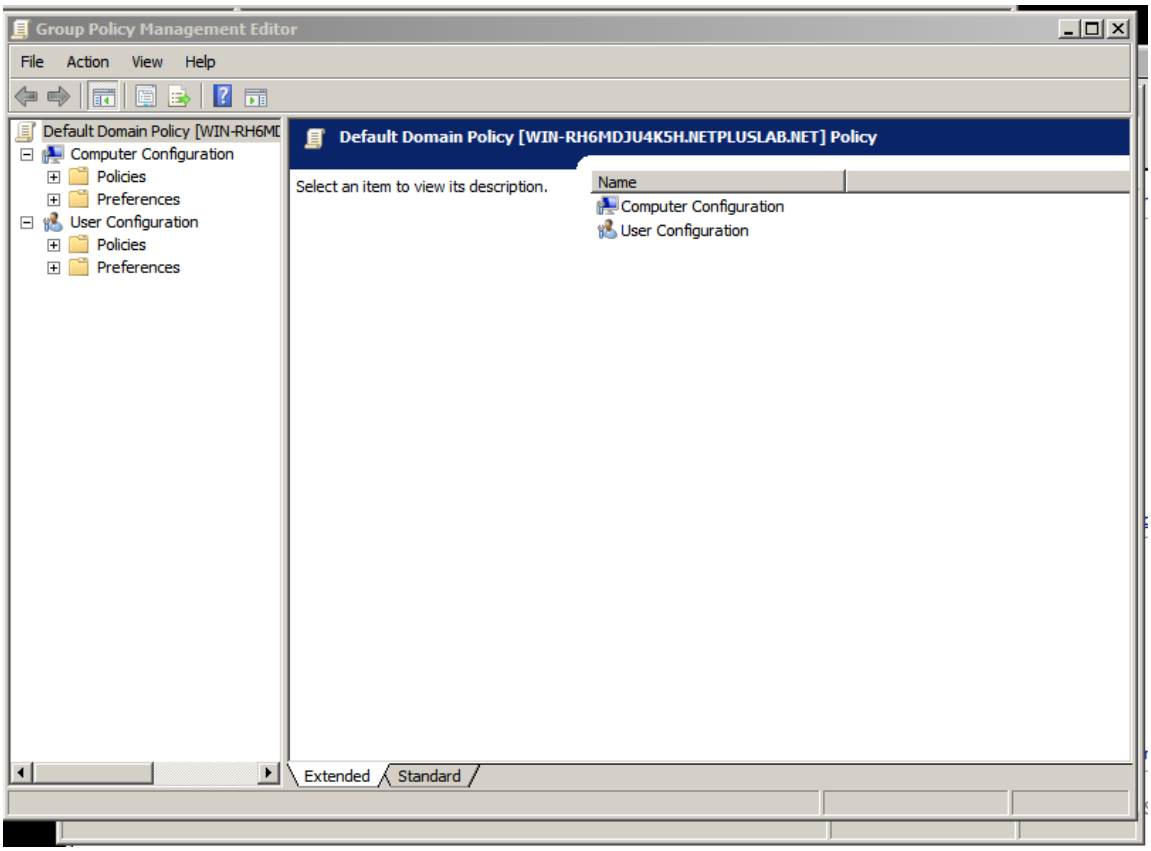


Click Local Area Policies in the left pane. Double click Audit Policy – double click Audit account logon events. - Click Success and Failure check boxes - OK

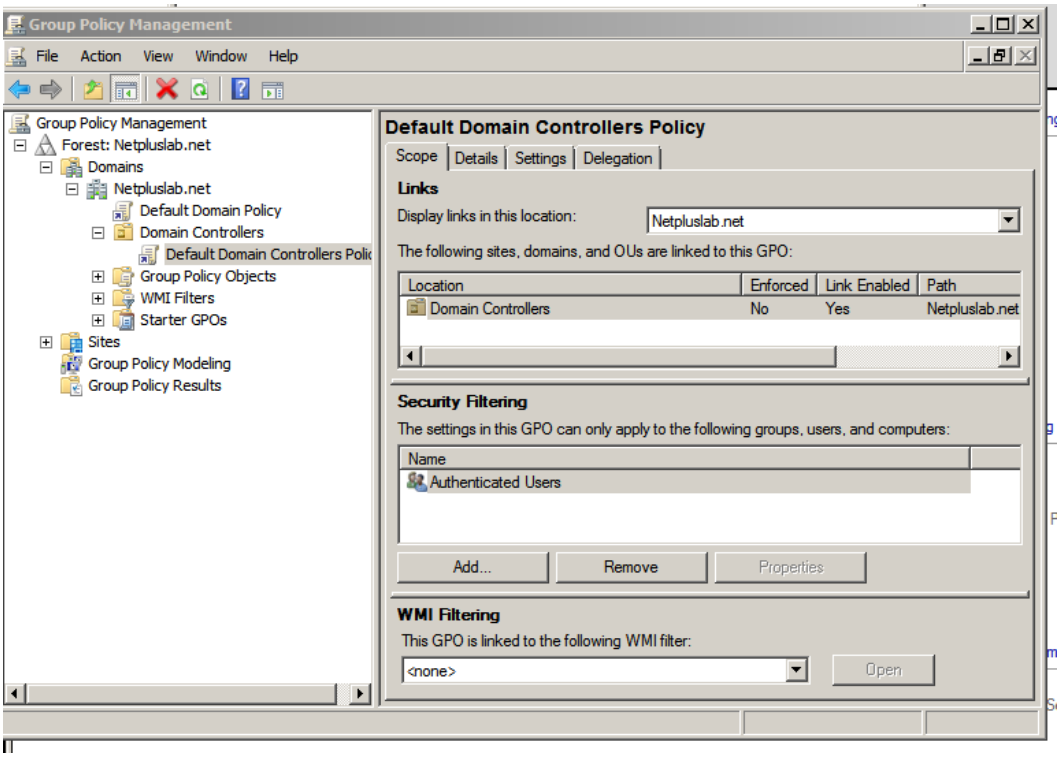


Repeat steps 37 and 38 for Audit logon events – In the left pane right click Reload.

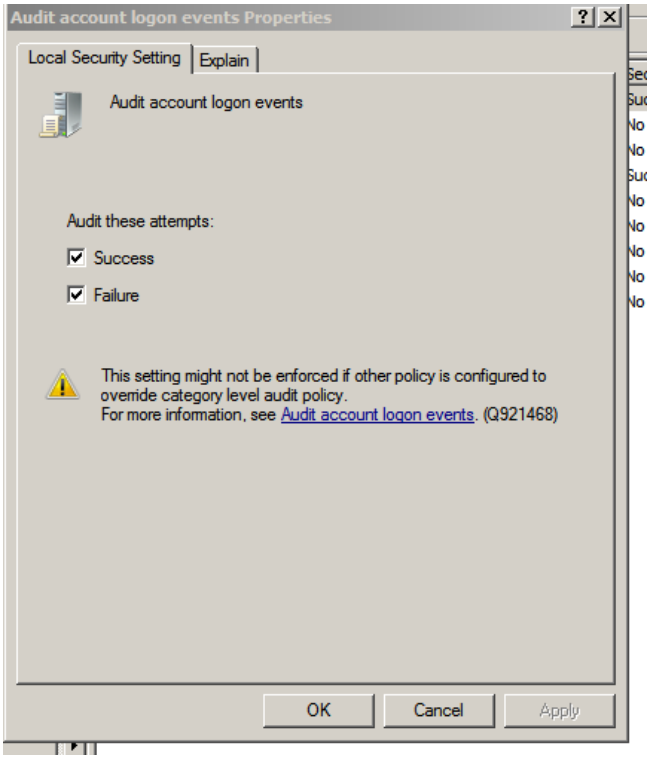
Administrative Tools – Group Policy Management



Group Policy Management Forest – netpluslab.net – Domains – netpluslab.net – Domain Controllers Policy



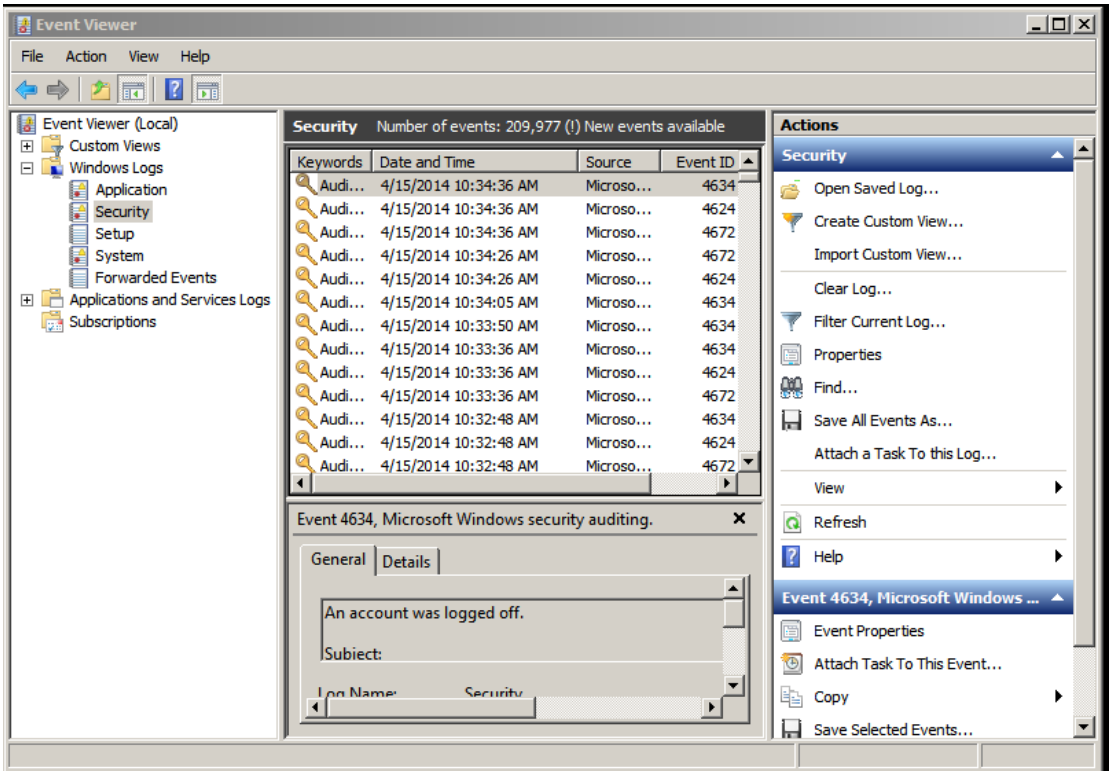
Edit – Local Policies – Audit Policy



Audit account logon events – OK

Log on to the Workstation using an invalid password – error message appears – OK

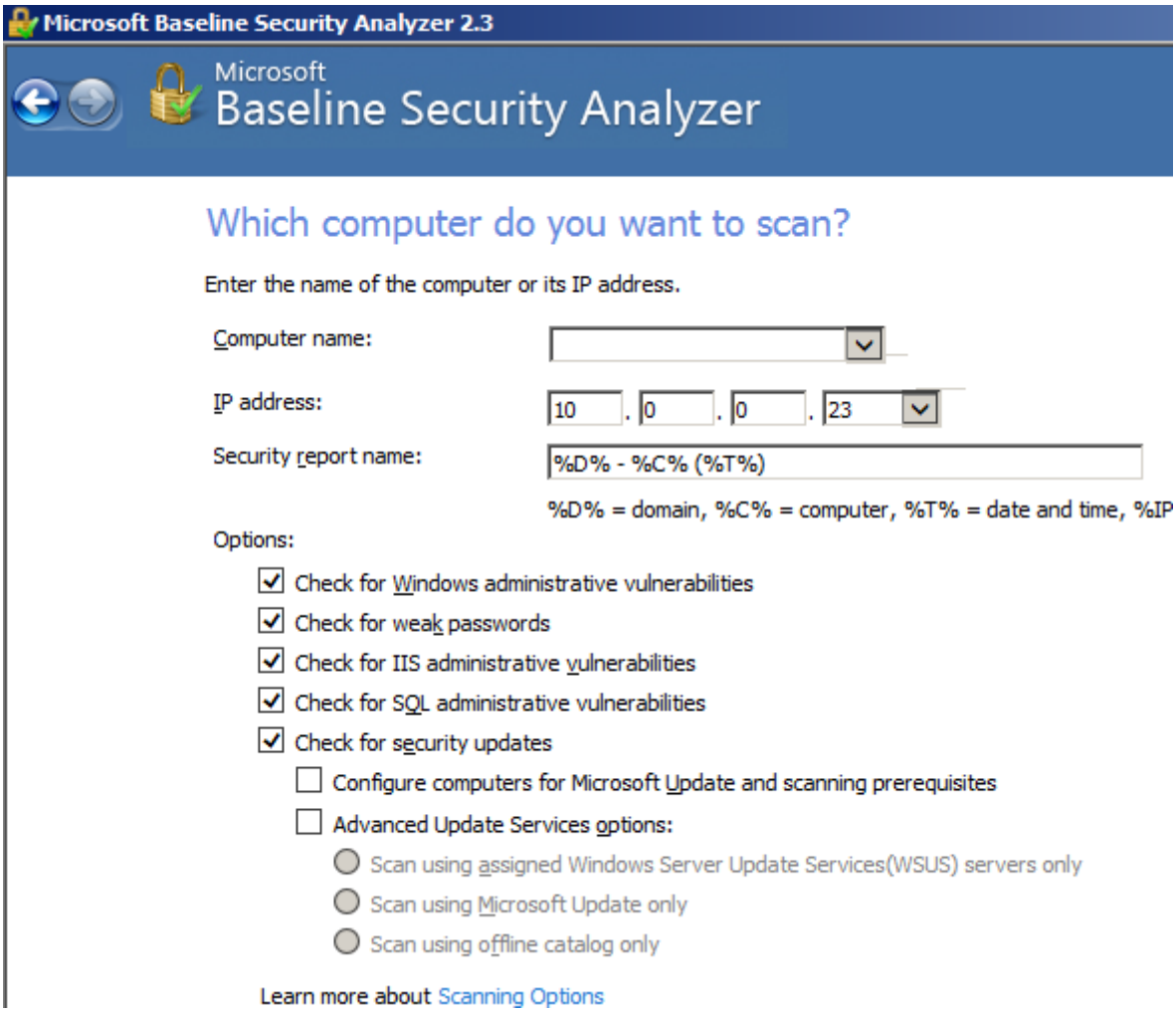
Log on with correct password – Administrative Tools – Event Viewer – Expand Windows logs – Click Security – Double click Audit Failure – Repeat previous step – log off.

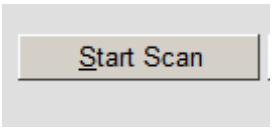


Lab 11.2 Checking for Vulnerable Software

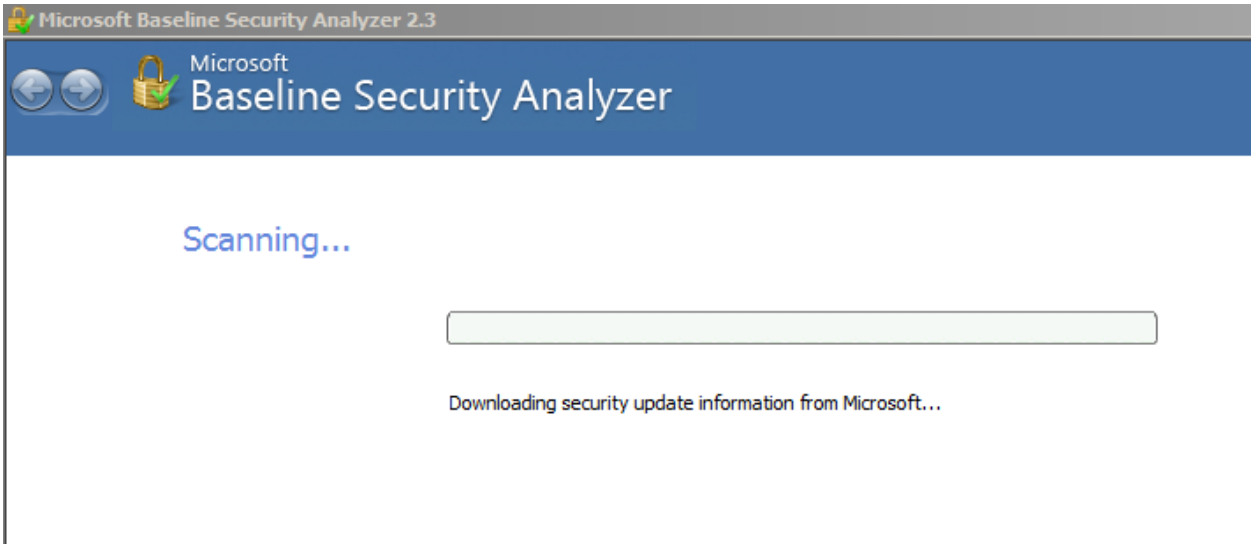
Download Microsoft Baseline Security Analyzer 2.2 and install on Server – Open –

Make sure that the name or the local computer is selected in the Computer name drop-down box, and that the Check for windows administrative vulnerabilities, Check for passwords, Check for IIS administrative vulnerabilities, and Check for SQL administrative vulnerabilities check box.

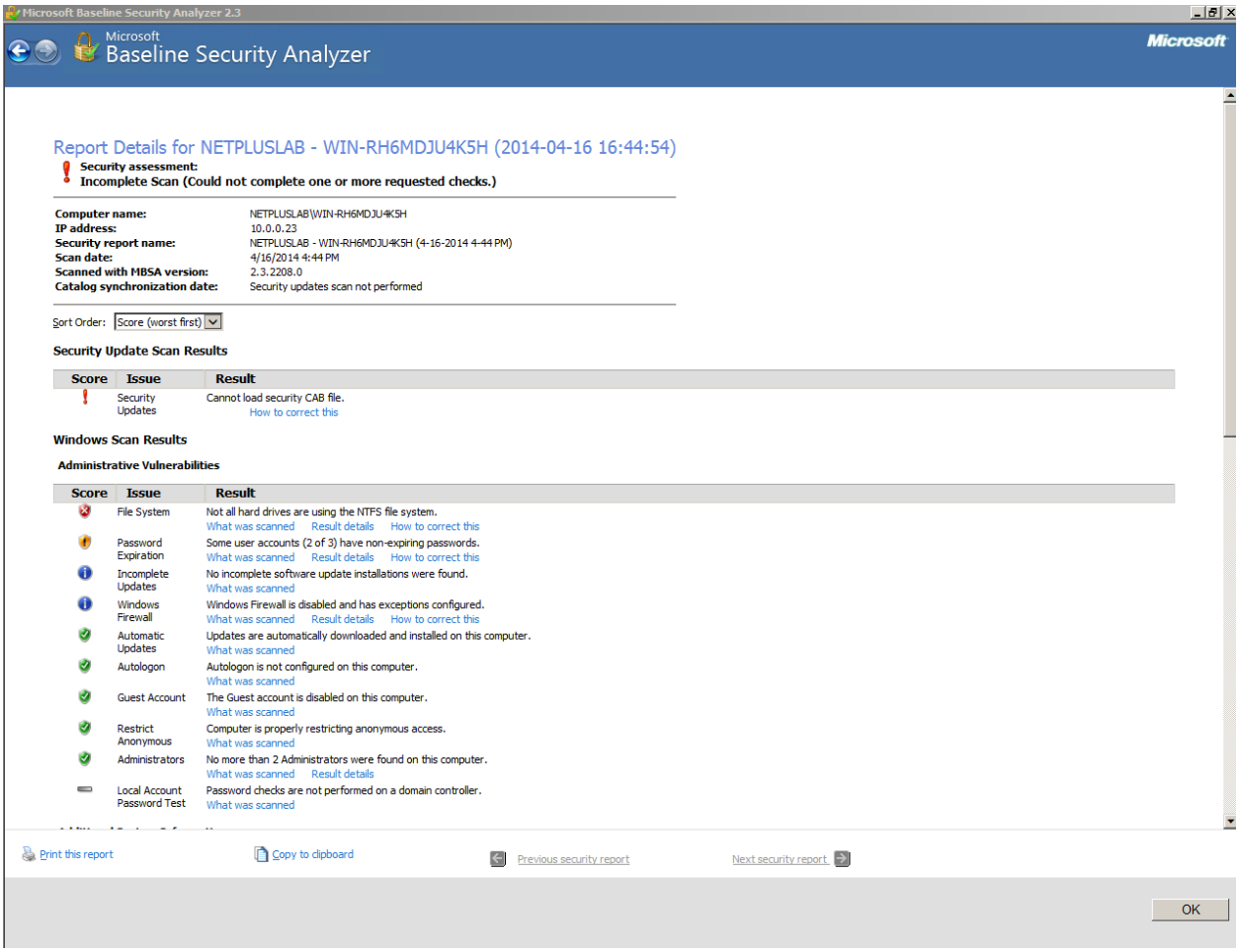




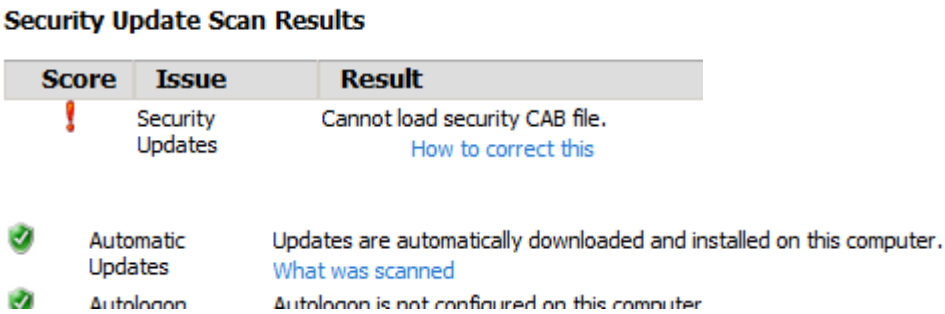
Start Scan

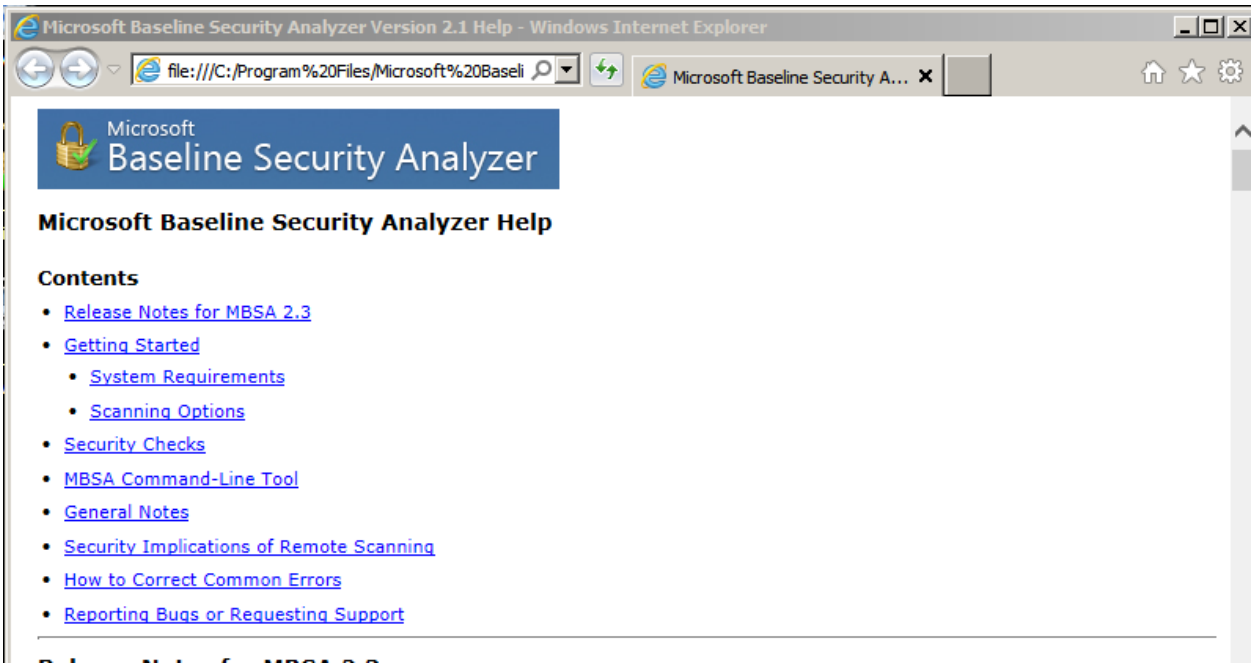


At the top of the report is a summary of the security status of the computer. Check the security assessment.



Scroll down to the security update scan results section. A red stop sign is for security risks, a green check mark for any item that does not pose a risk, a white I in a blue circle for any informational items, a yellow explanation points for items that need to be changed and a blue star for items that can be changed.





Log off.

Lab 11.3 Implementing Network Address'

Network address translation (NAT) is a methodology of modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device for the purpose of remapping one IP address space into another.

Originally used to simply map each address of one address space to a corresponding address in another space, most often today, NAT is used in conjunction with network masquerading (or IP masquerading) which is a technique that hides an entire IP address space, usually consisting of private network IP addresses (RFC 1918), behind a single IP address in another, usually public address space. This mechanism is implemented in a routing device that uses stateful translation tables to map the "hidden" addresses into a single IP address and readdresses the outgoing Internet Protocol packets on exit so they appear to originate from the routing device. In the reverse communications path, responses are mapped back to the originating IP addresses using the rules ("state") stored in the translation tables. The translation table rules established in this fashion are flushed after a short period unless new traffic refreshes their state.

Lab 11.4 Plaintext versus Encrypted Protocols

Plaintext: A text-based protocol or plain text protocol is a communications protocol whose content representation is in human-readable format. The immediate human readability stands in contrast to binary protocols which have inherent benefits for use in a computer environment (such as ease of mechanical parsing and improved bandwidth utilization).

Text-based protocols are typically optimized for human parsing and interpretation, and are therefore suitable whenever human inspection of protocol contents is required, such as during debugging and during early protocol development design phases.

FTP: File Transfer Protocol is a standard network protocol used to transfer files from one host to another host over a TCP-based network, such as the Internet. FTP is built on a client-server architecture and uses separate control and data connections between the client and the server. FTP users may authenticate themselves using a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that hides (encrypts) the username and password, and encrypts the content, FTP is often secured with SSL/TLS ("FTPS"). SSH File Transfer Protocol ("SFTP") is sometimes also used instead, but is technologically different.

In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption doesn't prevent hacking but it reduces the likelihood that the hacker will be able to read the data that is encrypted. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm, that usually requires a

secret decryption key, that adversaries do not have access to. For technical reasons, an encryption scheme usually needs a key-generation algorithm to randomly produce keys.

Lab 11.5 Securing a Wireless Network

1.Connect to your router via your browser, by inputting something called a Gateway IP Address.

•Click Start > Run > type 'cmd' > Click 'Enter'

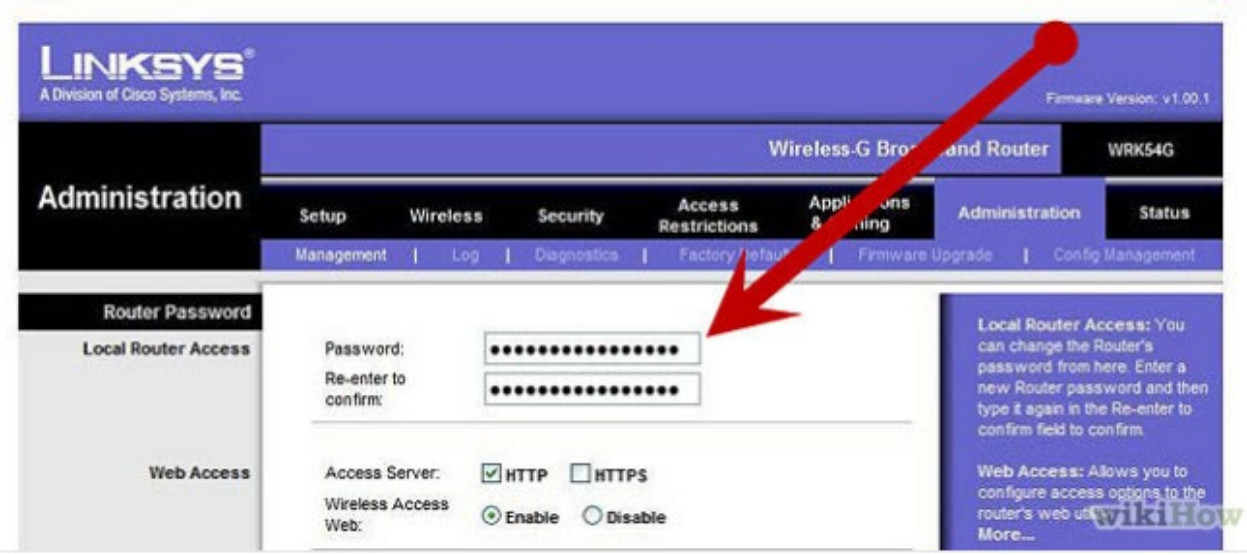
•Once the Command Prompt window opens, type 'ipconfig /all' and hit 'Enter'

•Locate the line labeled 'Gateway' and make note of the number that follows. It will look similar to '192.168.1.1'

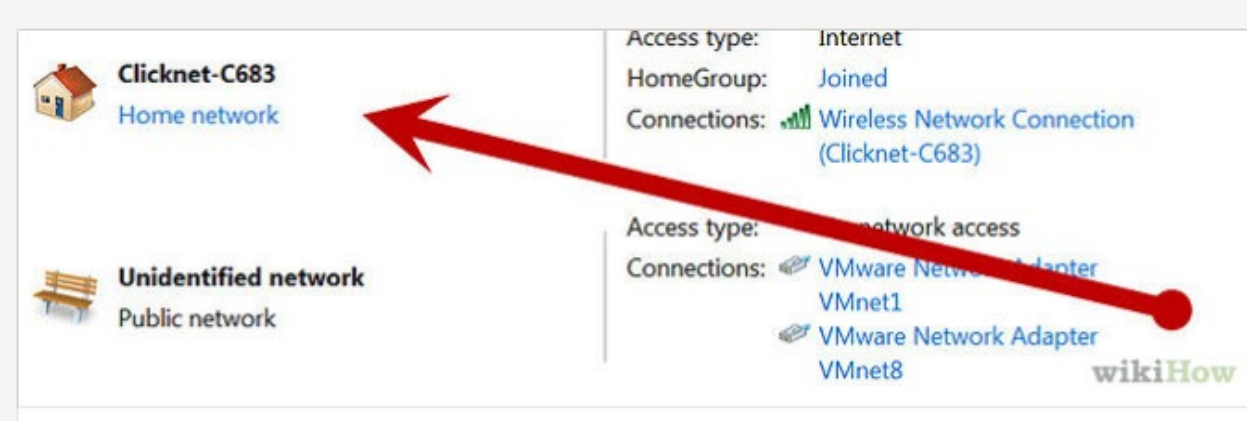
•Open Internet Explorer (or your favorite browser)

•Enter the Gateway IP Address into the address bar and click 'Enter

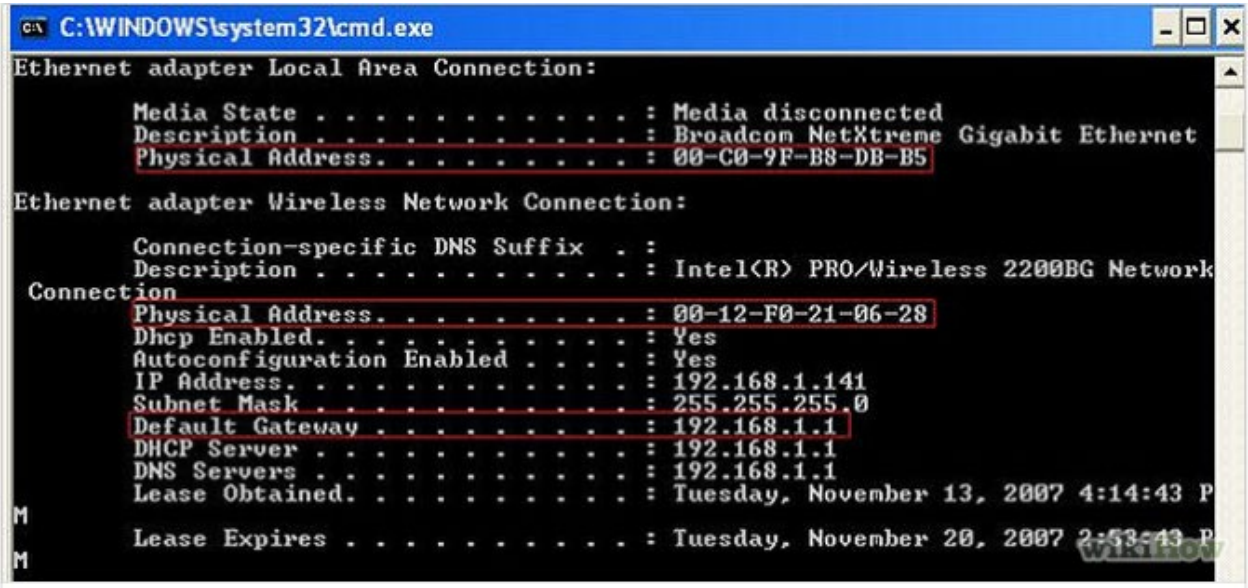
2. Enable encryption on your access point. Using 128-bit encryption or higher makes your Wireless Network more secure. WEP and WPA are entirely different encryption schemes. WEP has been proven insecure and can be cracked in a few minutes using free utilities that can be downloaded from the Internet. Using at least WPA is recommended, because it is much more secure, but is sometimes a bit harder to set up correctly than WEP is, and isn't completely secure.Some older access points or wireless cards do not support WPA2. If you have one of these, it is recommended that you purchase a newer one that supports **WPA2**, depending on how important you consider your security.



3. Set the router access password. Anybody who gains access to the router configuration settings can disable the security you have set up. If you forget the password, most routers have a hardware reset that will restore all of the settings to factory defaults. The best option is to use a random sequence of the maximum length of characters - you only have to type that once, so it is not a big thing. When you connect to the router via LAN cable while setting it up, you can copy and paste the password onto the router and onto your local setting, so you never need to type it again.

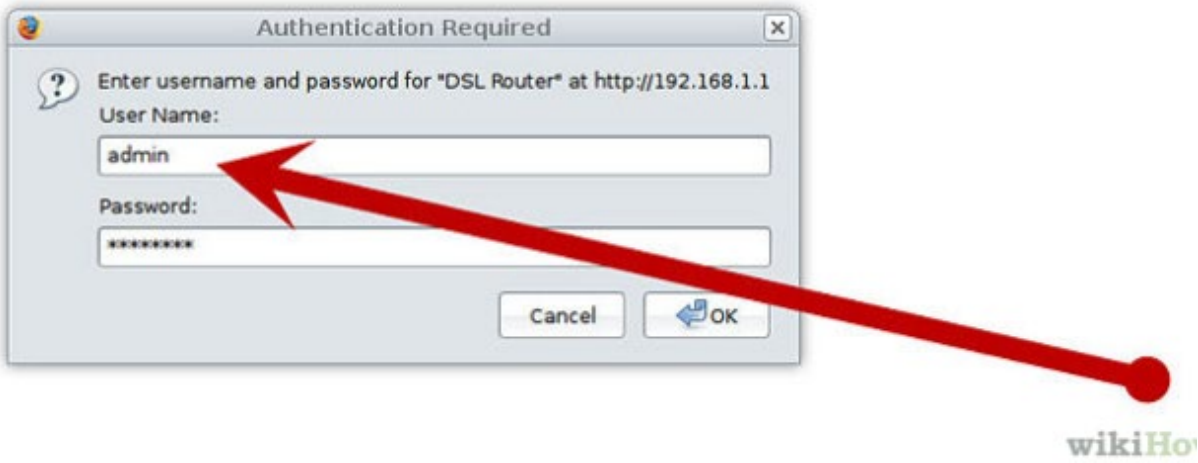


4. Change the Service Set Identifier (the network name or "SSID") from the default to something unique. A default SSID indicates to hackers that the network was set up by a novice and that other options (such as the password) are also left as the default. Use a name you can remember and identify, as the SSID has no influence on the security of your network (not even if you choose not to broadcast it).



5. Enable MAC Address filtering on your Access Point or router. A MAC (not to be confused with the computer model 'Mac') address is a code unique to every wireless networking card in existence. MAC Address filtering will register the hardware MAC Address of your networked devices, and only allow devices with known MAC Addresses to connect to your network. However, hackers can clone MAC addresses and still enter your network, so MAC address filtering should not be used in place of proper WPA2 encryption.

6. Don't disable the 'SSID Broadcast'. Do not disable the 'SSID Broadcast' feature of your Access Point or router. This seems counter-intuitive, but it is actually a bad idea.[3] Although this would make your network invisible to your neighbors, any determined hacker can still sniff out your SSID; and you are implicitly forcing your computer to shout out your SSID anywhere you are, while it is trying to connect to it. Anyone could then impersonate your router with that SSID, and get your credentials that way.



7. Disable remote login. The first router worm brute forces its way into the router in this manner. Most default usernames are set to Admin. It isn't hard for a virus/worm to crack the password if the username is known. The good thing is that routers normally have this disabled by default. Be sure to confirm that it is disabled when you first set up your router and periodically thereafter. If you need to update your router setting remotely, only set up access for the time you are going to be connected.

8. Disable wireless administrating. Finally, change the setting that allows administrating the router through a wireless connection to 'off' (meaning that you need to connect with a LAN cable for administration). This disables any wireless hacking into the router.

Tips

•You need to set the same WPA2 Settings on your computer and router.

•Check your Access Point or Routers' documentation on how to enable or disable security features.

•You may need to upgrade the Firmware of your Access Point or Router if it doesn't have any of these features. In some situations, you will need to purchase a new Access Point.

warnings

•A user with a 'cantenna' can access your wireless network from a very long way off. Just because your notebook doesn't get a signal on the porch doesn't mean someone else can't access or monitor your network from a mile away, meaning that even though you don't think anyone in your neighborhood would break into your network, someone far away might.

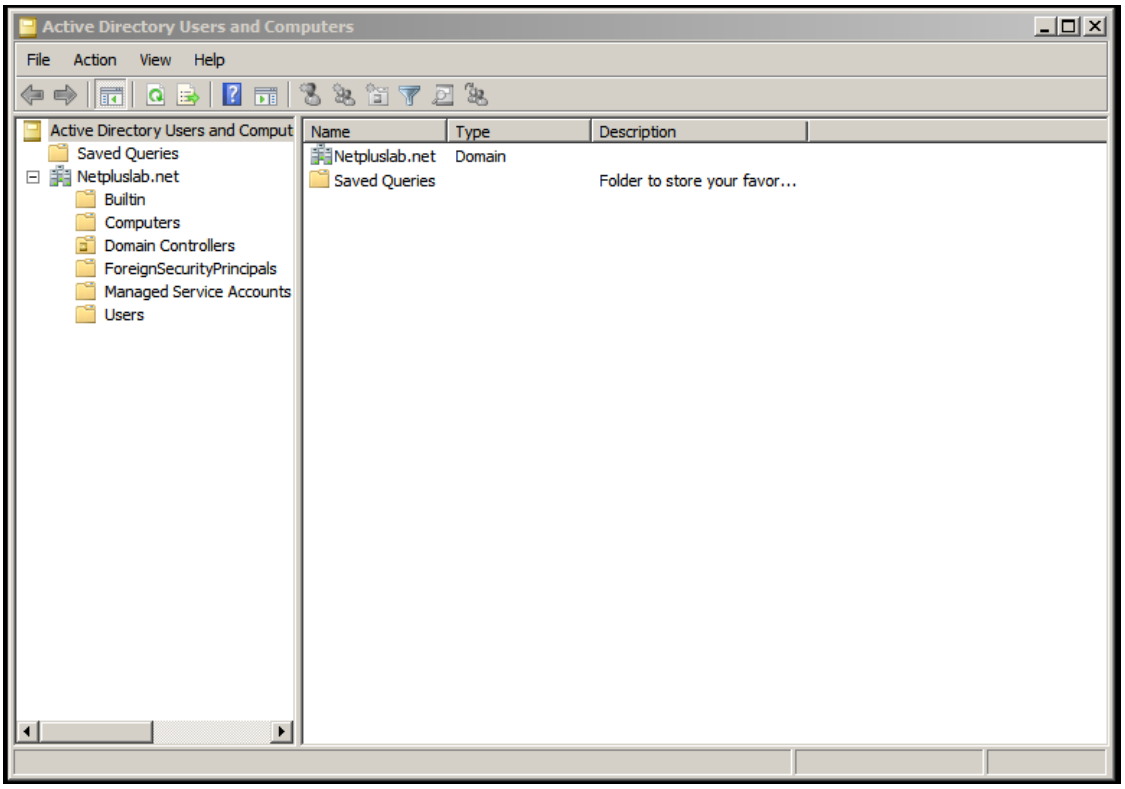
•Disable 'File and Printer Sharing' in the wireless 'Connection Properties' for your portable computer. Only use the 'Client for Microsoft Networks' half of Microsoft's file sharing. This means that your portable must connect to a machine that shares file/folders in order to access things, and that OTHER computers can't ask to connect to your portable to access files on your machine. At least not through Microsoft's 'File Sharing'. Other running services and back doors may exist.

•Certain versions of Windows don't have individual wireless settings for different wireless domains. This means that the settings that 'share' files at home with your LAN will 'share' files with anybody else's wireless network, even a wireless network masquerading as one you trust.

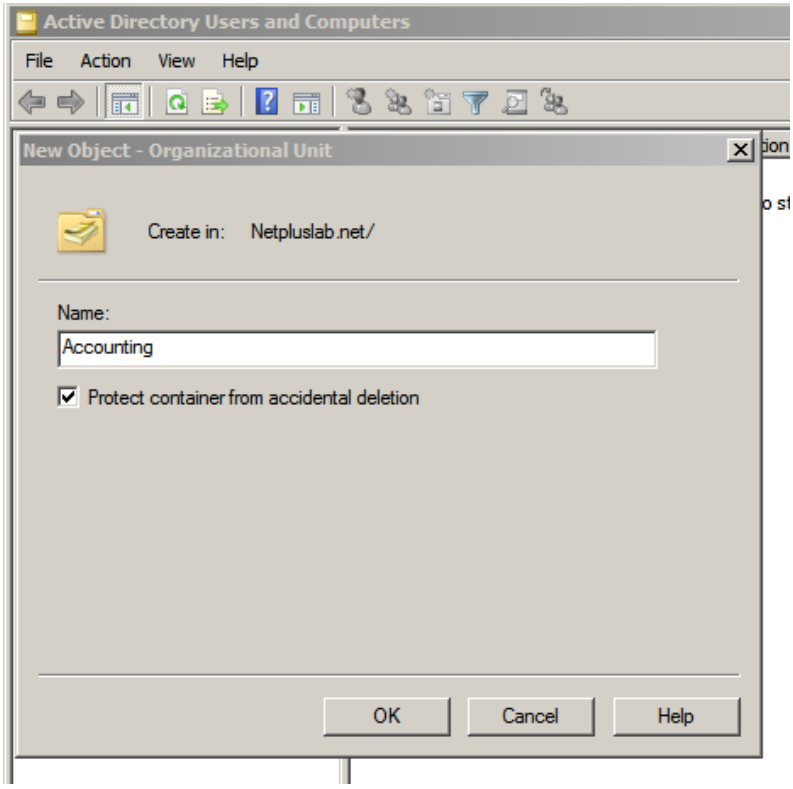
•Be sure to register all devices on your network, including computers, laptops, media players, and networked storage if you are using MAC filtering. Also, be sure to enter the MAC addresses correctly as if you enter the wrong ones, you will not be able to connect the computer to the router to change them back and you will need to reset the router. Some routers allow you to save them while they are connected.

Lab 11. 6 Delegating Administrative /rights

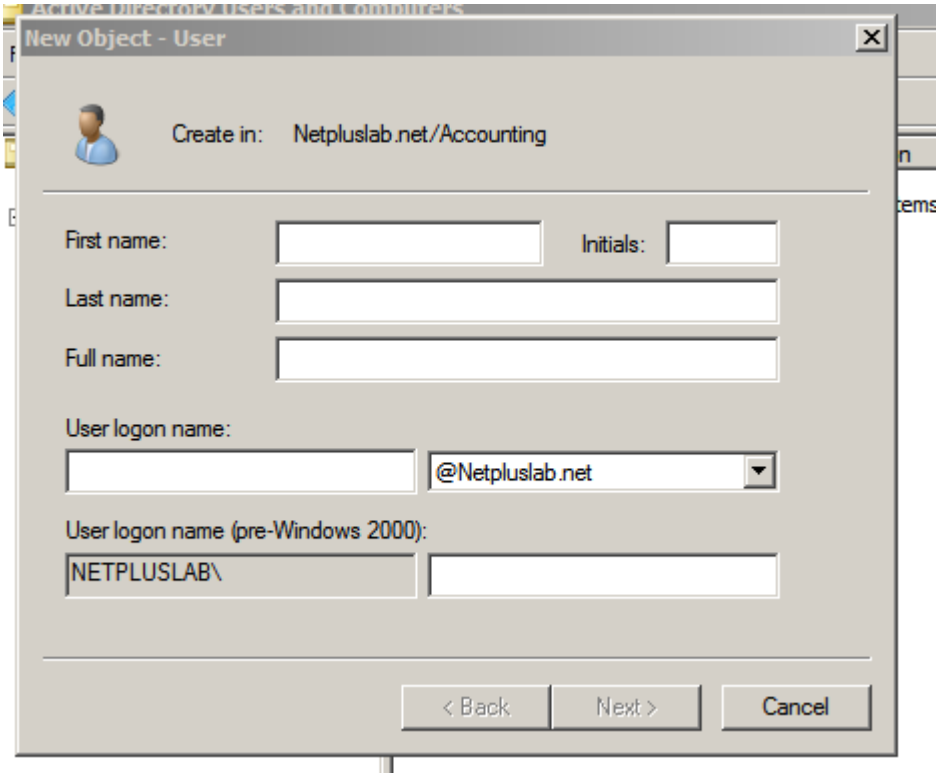
Server – Administrative Tools – Active Directory Users and Computers –



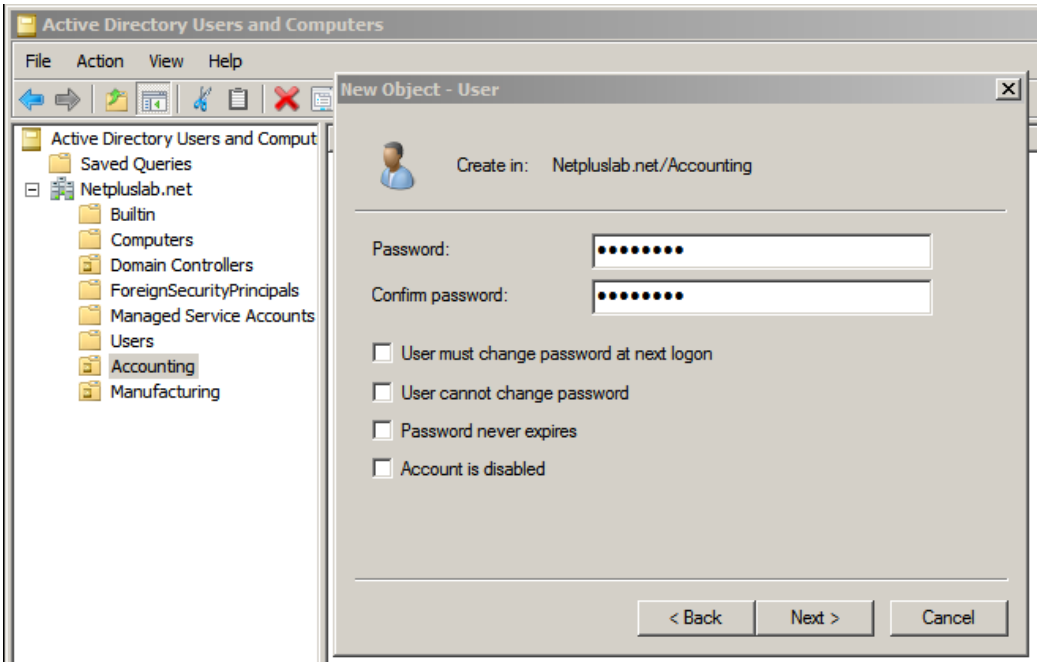
Right click netpluslab.net – New – Organizational Unit - Type Accounting – OK



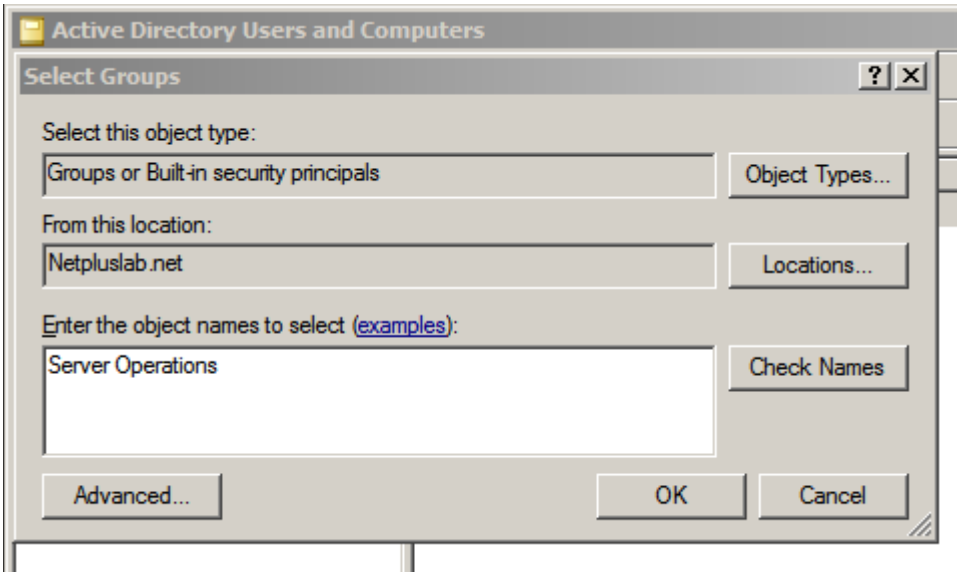
Repeat steps 3 & 4,creating an organizational unit named Manufacturing. Right click Accounting object – short-cut menu – New – User



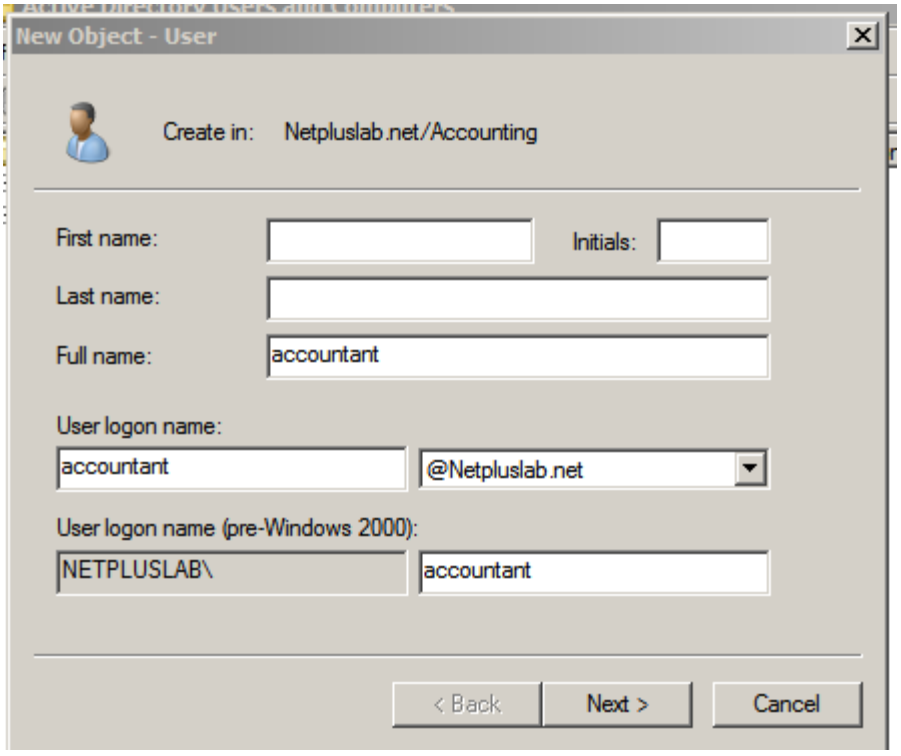
In the Text boxes enter accounting – admin – Next – Password boxes (1234QWer) – Click User must change password at next logon – Next



Finish – Click Accounting in the left pane – Right click the Accounting – admin object – Select Add to group

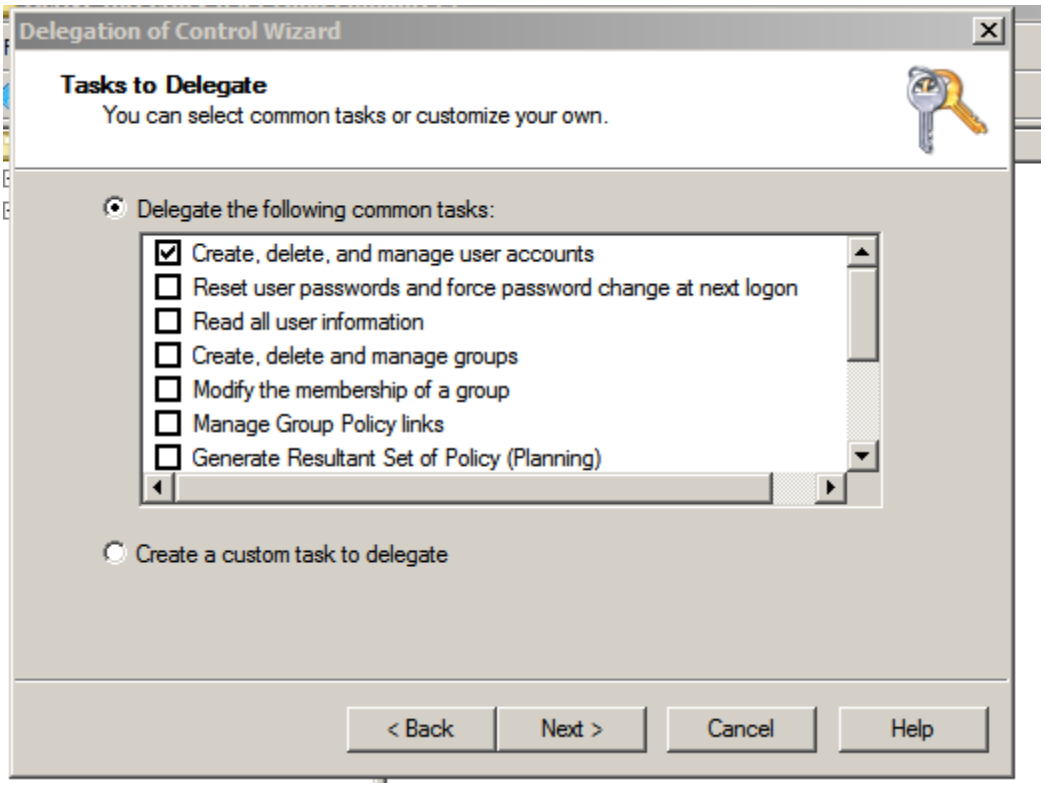


In the 'Enter the object names to select' text box, type Server Operations – Click OK – Repeat steps 6 through 10, creating a user account named manufacturer –

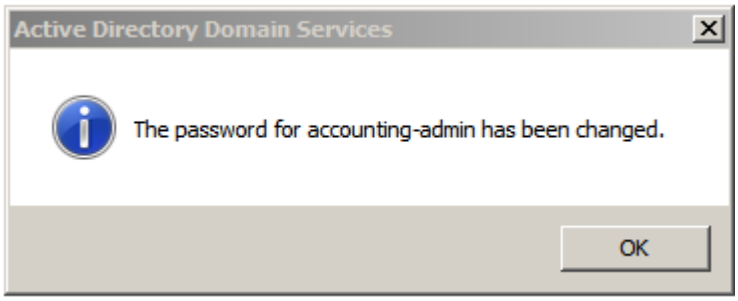


Right click Accounting object and select Delegate Control – Wizard opens

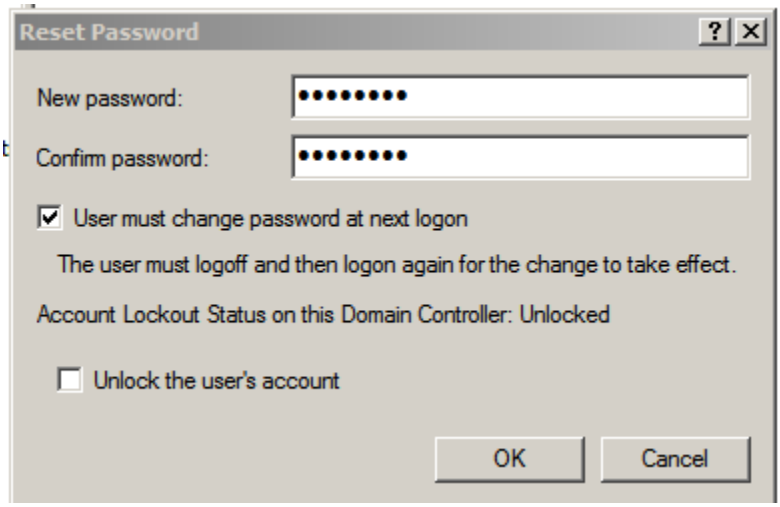
Click Next – The wizard offers you the option of selecting users or groups – Add - In the 'Enter the object names to select' text box, type accounting – admin – OK – Next – The wizard lists a series of tasks you could delegate. Place a check in the Create, delete, and manage user accounts – Next – Finish



Log off Server – Log on Server as the accounting-admin – Start – Administrative Tools – Active Directory Users and Computers – Click the Accounting object – Right click the accountant user icon, select Reset Password – Enter a new password – Click OK



Repeat steps 6 through 10 for the Accounting object, create a user named bills – Click icon for Manufacturing – Reset Password –



Right click the Manufacturing icon in the left pane of the window – Select delegate Control – OK – On Workstation log on to the netpluslab.net domain as the bills user account. Log off

Joseph Martinez

Networking II: Network +

CNG – 125

Chapter Thirteen Labs

Troubleshooting Network Problems

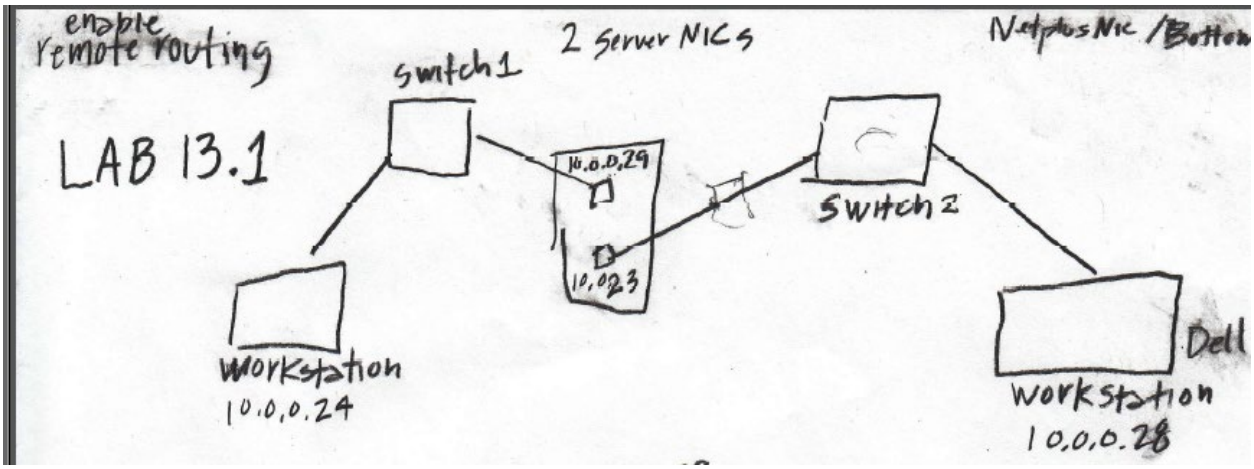
Lab 13.1 Using the Ping Utility to Troubleshoot a TCP/IP Network

Lab 13.2 Using the Traceroute Utility to Troubleshoot a TCP/IP Network

Lab 13.3 Troubleshooting Client Logon Problems

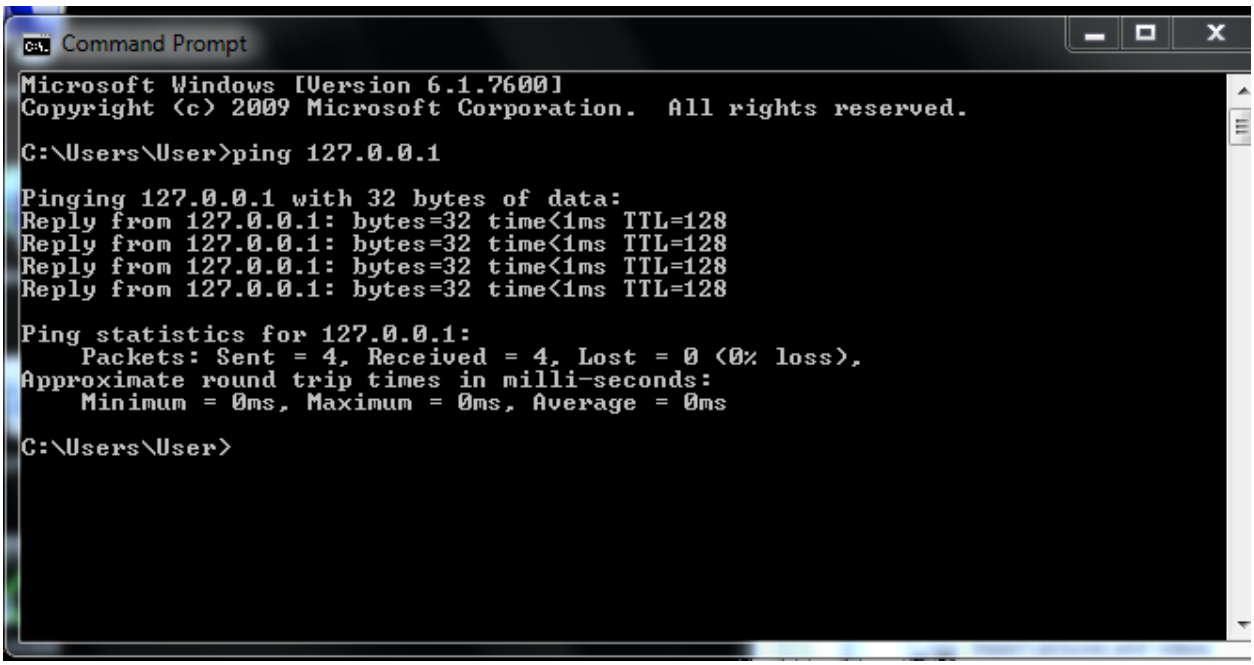
Lab 13.4 Troubleshooting Web Client Problems

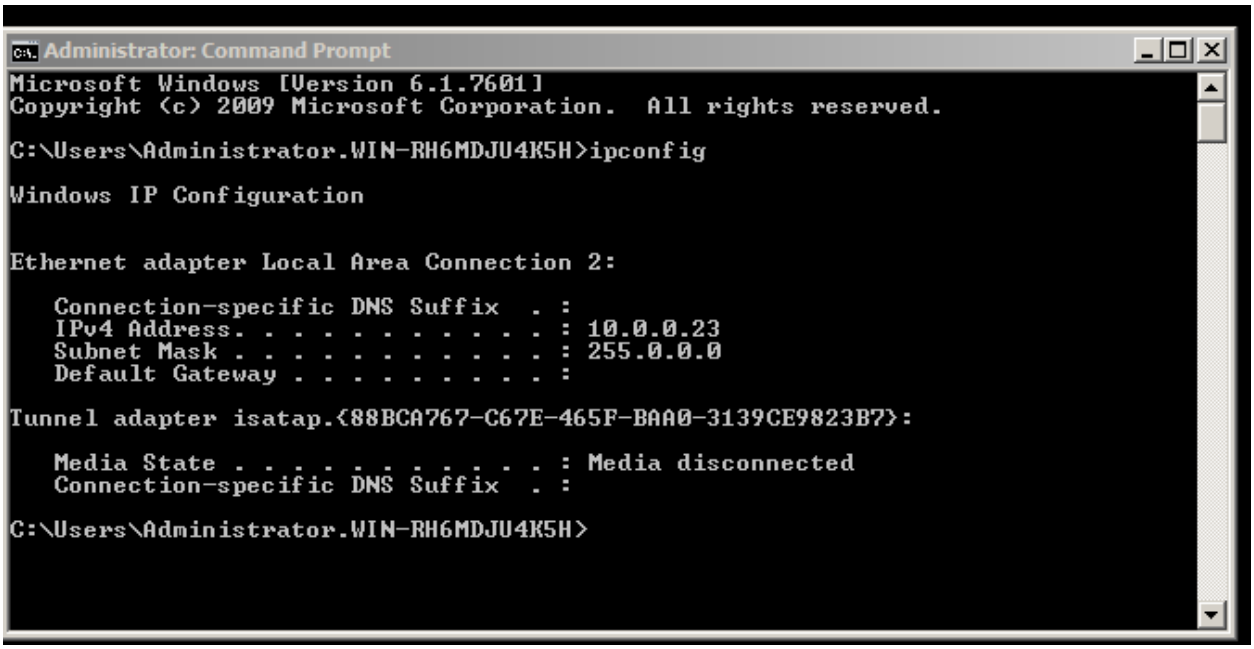
Lab 13.1 Using the Ping Utility to Troubleshoot a TCP/IP Network



Perform Lab with a faulty cable, after determining the problem, fix it.

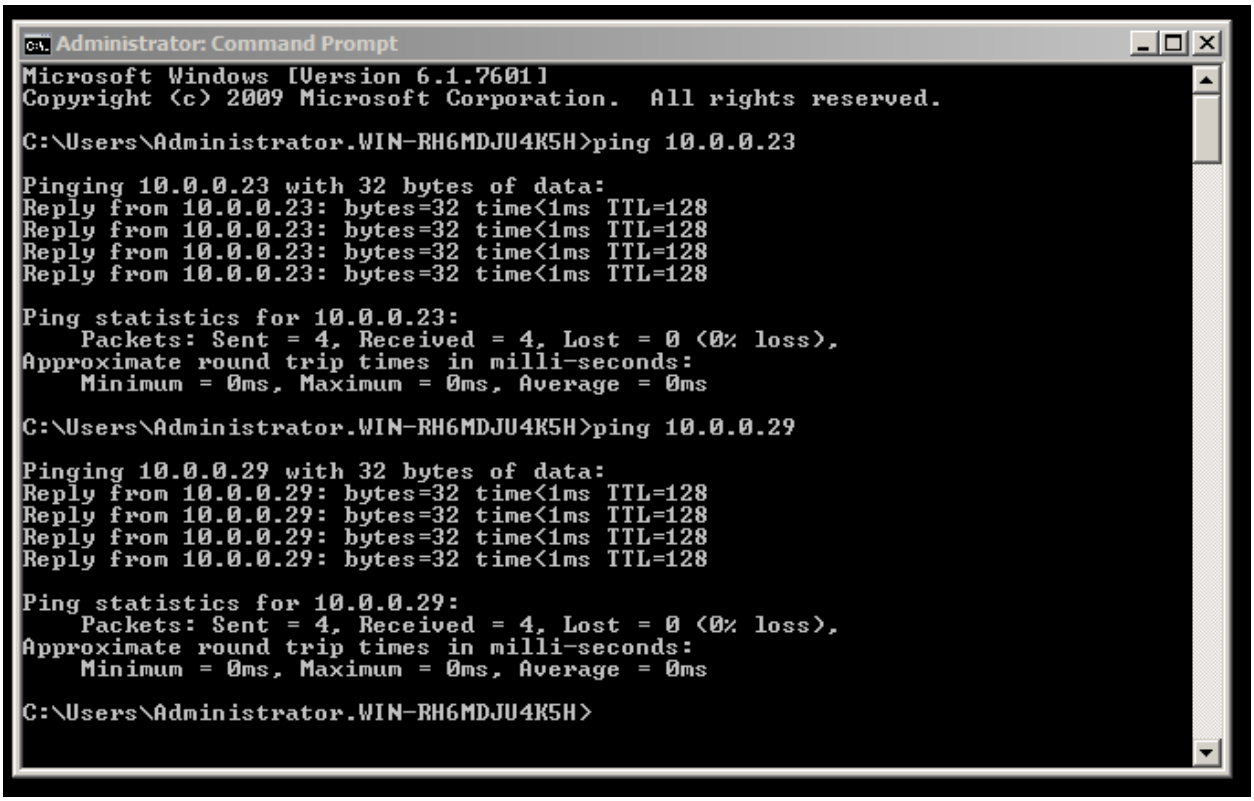
Log on to Workstation 1 – Command Prompt – To determine if the TCP/IP is operating properly
Ping 127.0.0.1



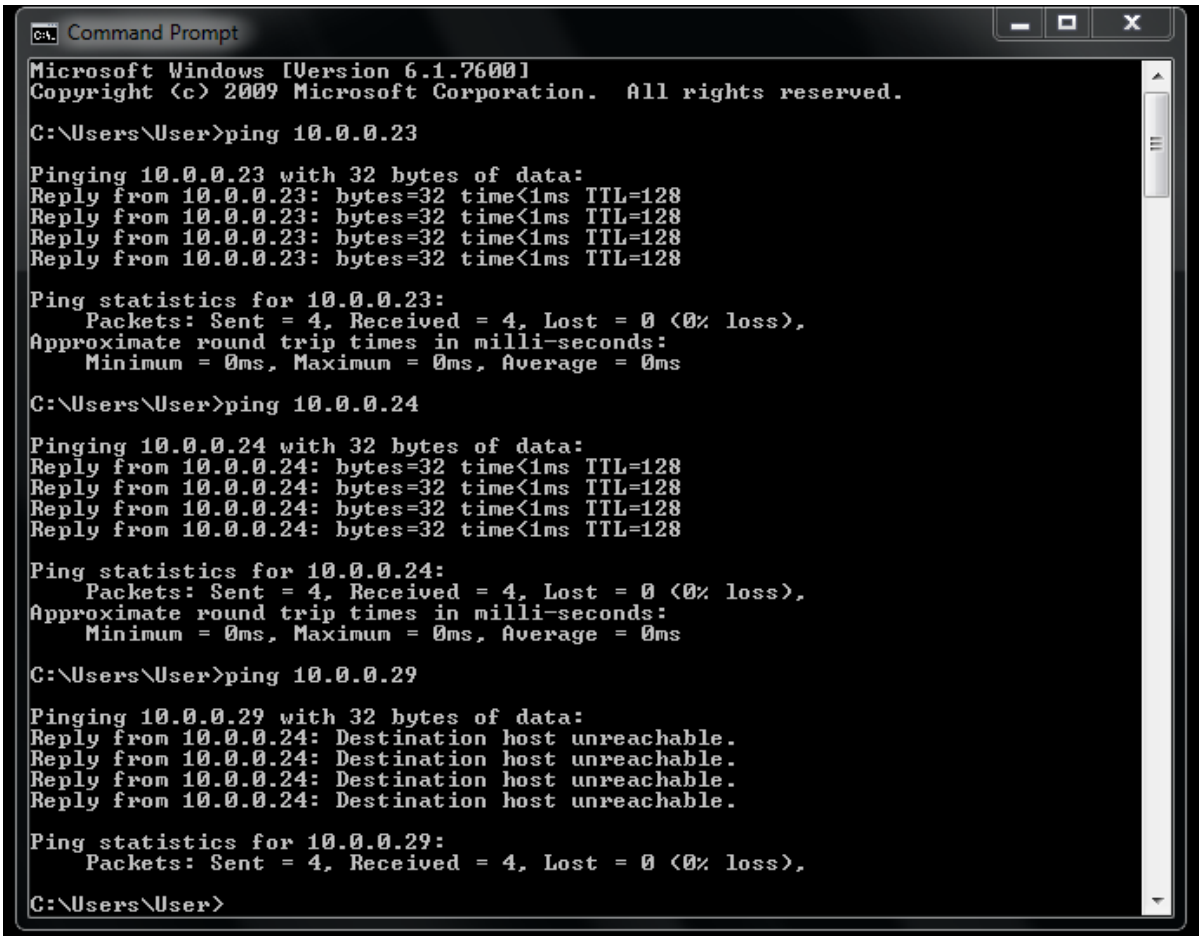


To determine if the computers NIC is operating properly Ping 10.0.0.23

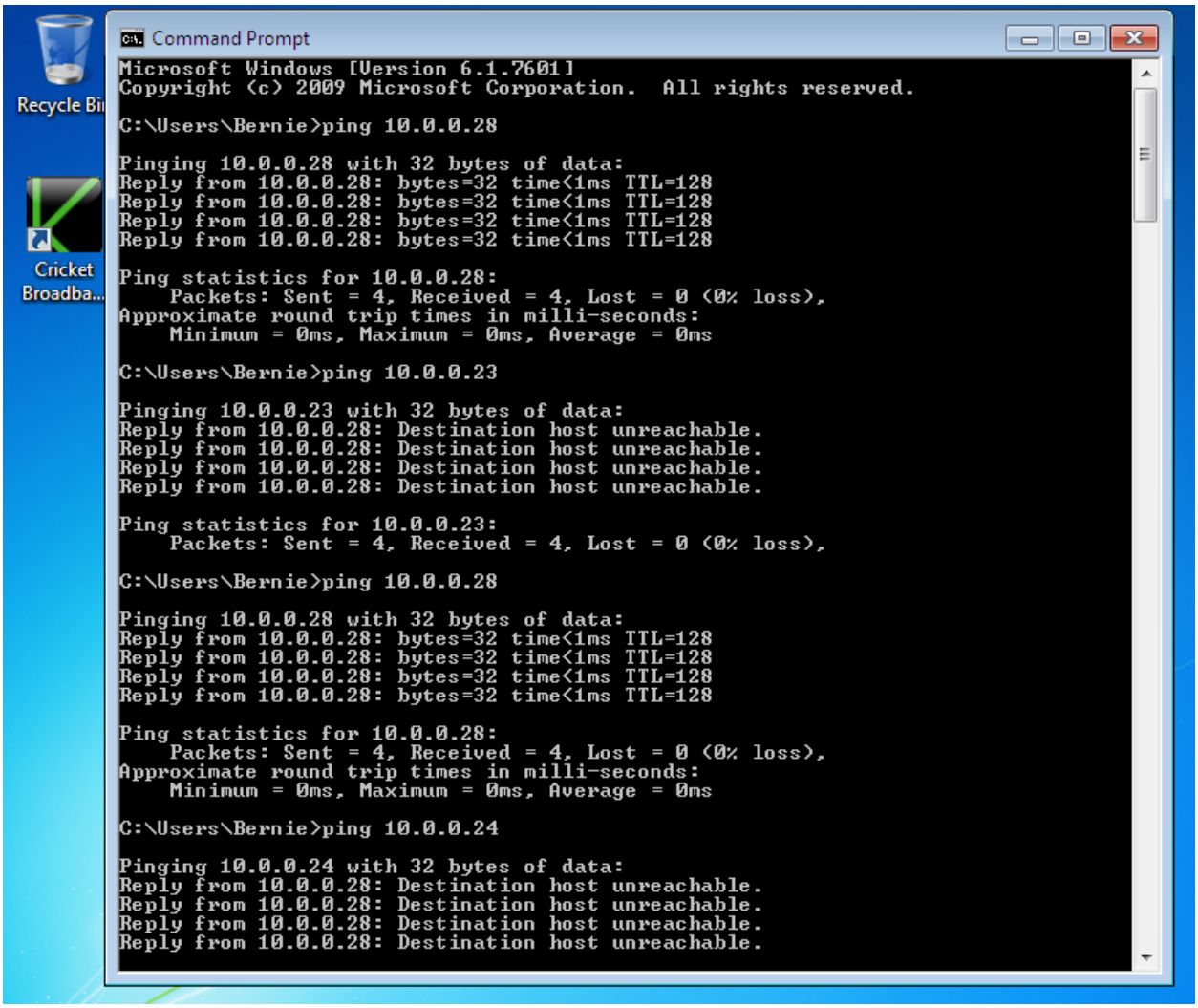
To determine if the connection to the near side of the Switch is operating properly Ping 10.0.0.29



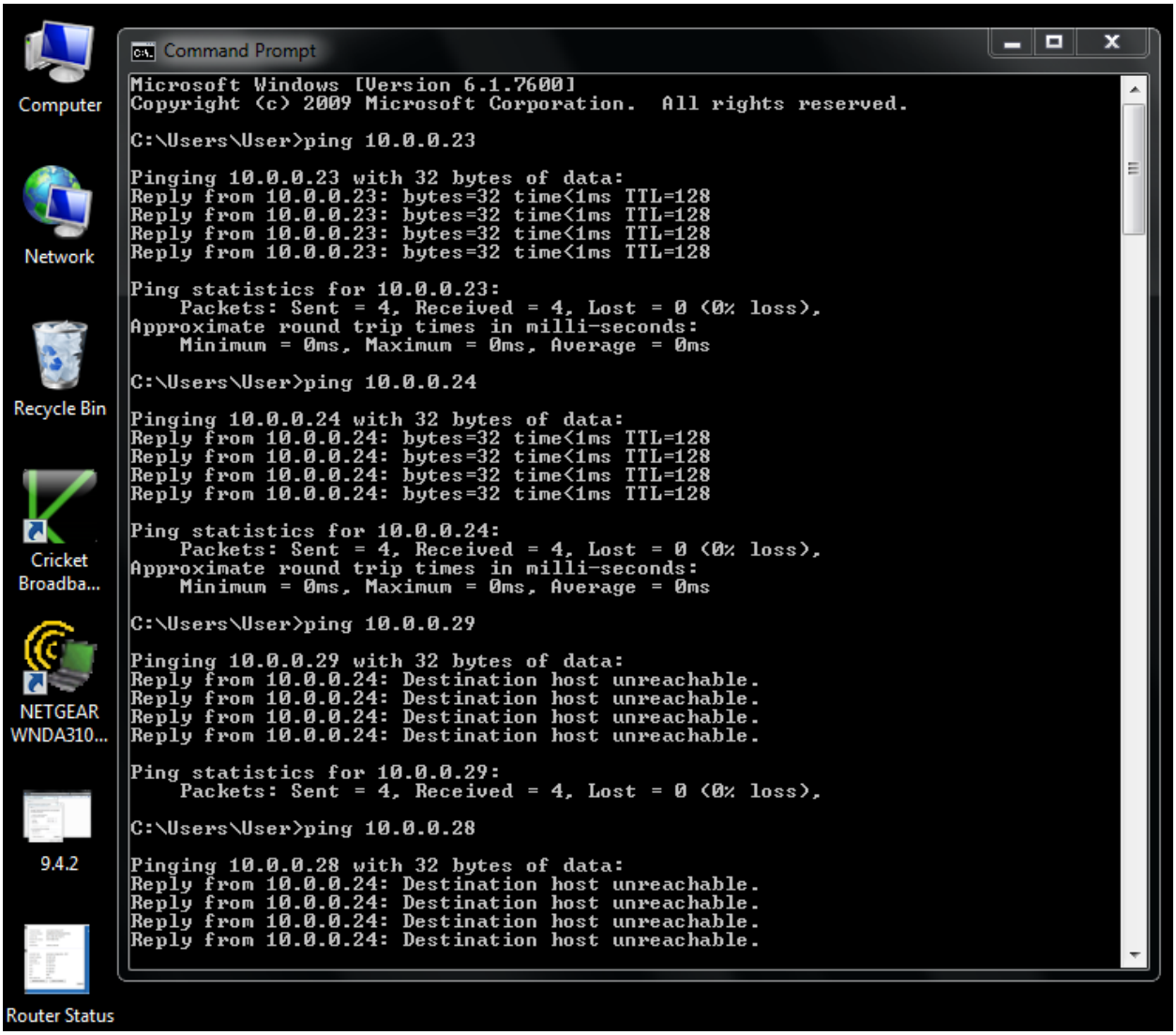
To determine if the router is operating properly Ping 10.0.0.24



Ping Workstation 1 and 2 Server NIC's


Recycle Bi
Cricket Broadba...
Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Bernie>ping 10.0.0.28
Pinging 10.0.0.28 with 32 bytes of data:
Reply from 10.0.0.28: bytes=32 time<1ms TTL=128
Reply from 10.0.0.28: bytes=32 time<1ms TTL=128
Reply from 10.0.0.28: bytes=32 time<1ms TTL=128
Reply from 10.0.0.28: bytes=32 time<1ms TTL=128
Ping statistics for 10.0.0.28:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\Bernie>ping 10.0.0.23
Pinging 10.0.0.23 with 32 bytes of data:
Reply from 10.0.0.28: Destination host unreachable.
Reply from 10.0.0.28: Destination host unreachable.
Reply from 10.0.0.28: Destination host unreachable.
Reply from 10.0.0.28: Destination host unreachable.
Ping statistics for 10.0.0.23:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
C:\Users\Bernie>ping 10.0.0.28
Pinging 10.0.0.28 with 32 bytes of data:
Reply from 10.0.0.28: bytes=32 time<1ms TTL=128
Reply from 10.0.0.28: bytes=32 time<1ms TTL=128
Reply from 10.0.0.28: bytes=32 time<1ms TTL=128
Reply from 10.0.0.28: bytes=32 time<1ms TTL=128
Ping statistics for 10.0.0.28:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\Bernie>ping 10.0.0.24
Pinging 10.0.0.24 with 32 bytes of data:
Reply from 10.0.0.28: Destination host unreachable.
Reply from 10.0.0.28: Destination host unreachable.
Reply from 10.0.0.28: Destination host unreachable.
Reply from 10.0.0.28: Destination host unreachable.

Ping Workstation 2, workstation 1 and both NIC's on Server



From Server Ping both NIC's and both Workstations

Lab 13.2 Using the Traceroute Utility to Troubleshoot a TCP/IP Network

The TRACERT (Trace Route) command is a route-tracing utility used to determine the path that an IP packet has taken to reach a destination.

Note: You can run this utility by typing tracert IPAddress or tracert HostName at the command prompt.

How the TRACERT Command Works

The TRACERT diagnostic utility determines the route taken to a destination by sending Internet Control Message Protocol (ICMP) echo packets with varying IP Time-To-Live (TTL) values to the destination. Each router along the path is required to decrement the TTL on a packet by at least 1 before forwarding it, so the TTL is effectively a hop count. When the TTL on a packet reaches 0, the router should send an ICMP Time Exceeded message back to the source computer.

TRACERT determines the route by sending the first echo packet with a TTL of 1 and incrementing the TTL by 1 on each subsequent transmission until the target responds or the maximum TTL is reached. The route is determined by examining the ICMP Time Exceeded messages sent back by intermediate routers. Note that some routers silently drop packets with expired TTLs and are invisible to TRACERT.

TRACERT prints out an ordered list of the routers in the path that returned the ICMP Time Exceeded message. If the -d switch is used (telling TRACERT not to perform a DNS lookup on each IP address), the IP address of the near- side interface of the routers is reported.

In the following example, the packet must travel through two routers (157.54.48.1 and 11.1.0.67) to get to host 11.1.0.1. In this example, the default gateway is 157.54.48.1 and the IP address of the router on the 11.1.0.0 network is at 11.1.0.67.

```
C:\>tracert 11.1.0.1

    Tracing route to 11.1.0.1 over a maximum of 30 hops

    1     2 ms     3 ms     2 ms  157.54.48.1
    2    75 ms    83 ms    88 ms  11.1.0.67
    3    73 ms    79 ms    93 ms  11.1.0.1

    Trace complete.
```

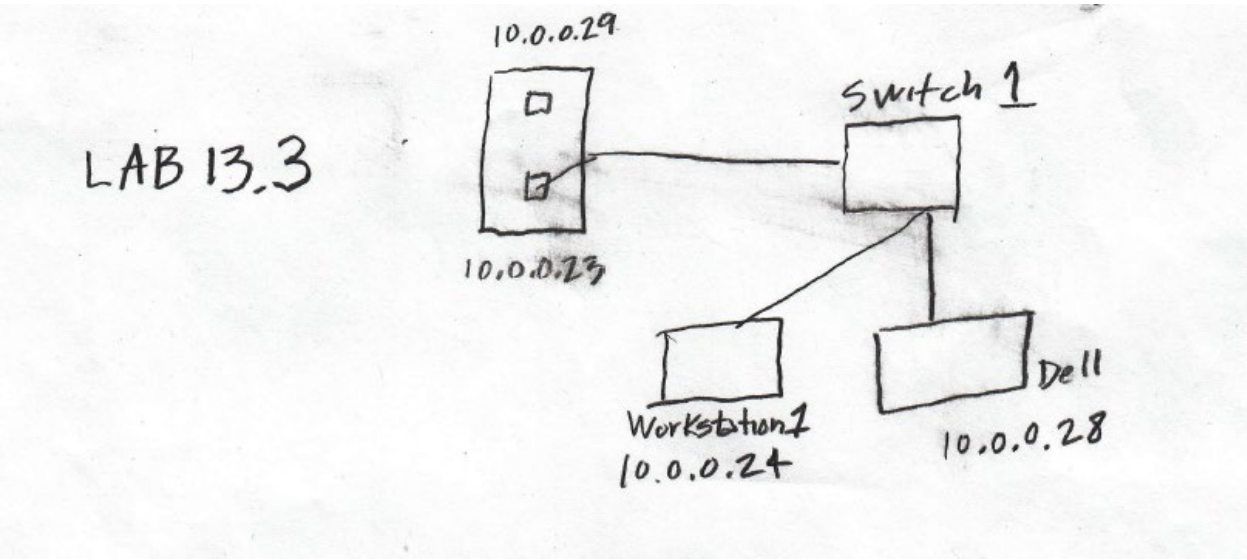
Troubleshooting with TRACERT

The TRACERT command can be used to determine where a packet stopped on the network. In the following example, the default gateway has determined that there is not a valid path for the host on 22.110.0.1. There is probably a router configuration problem or the 22.110.0.0 network does not exist (a bad IP address).

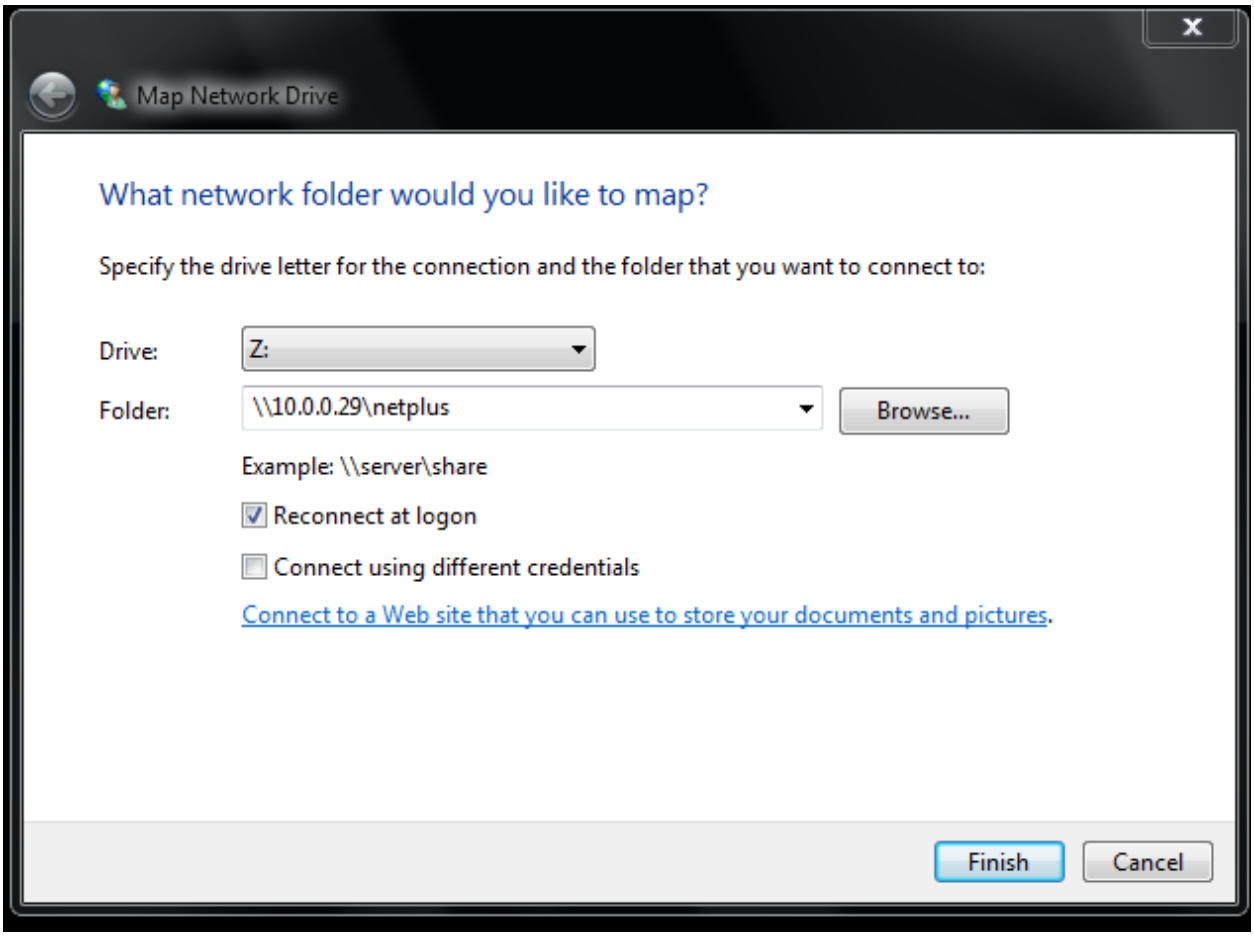
```
C:\>tracert 22.110.0.1

    Tracing route to 22.110.0.1 over a maximum of 30 hops

    1  157.54.48.1  reports: Destination net unreachable.

    Trace complete.
```

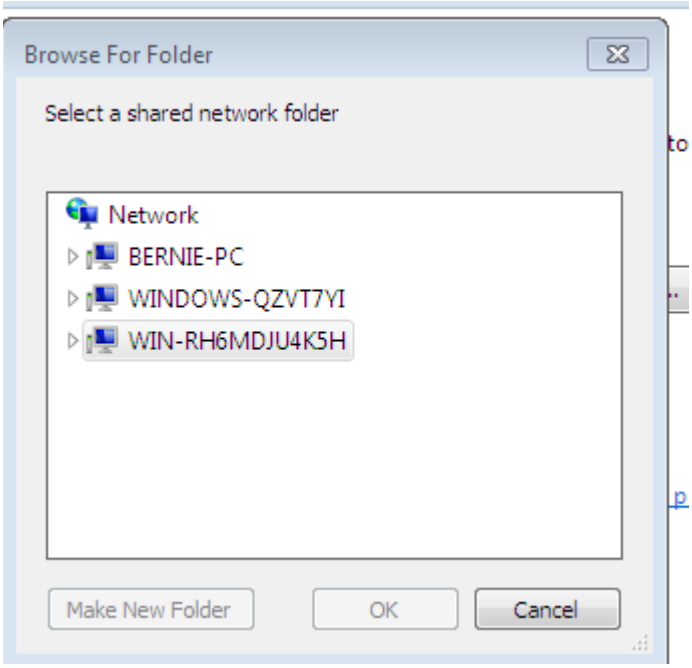
TRACERT is useful for troubleshooting large networks where several paths can be taken to arrive at the same point, or where many intermediate systems (routers or bridges) are involved.

Lab 13.3 Troubleshooting Client Logon Problems

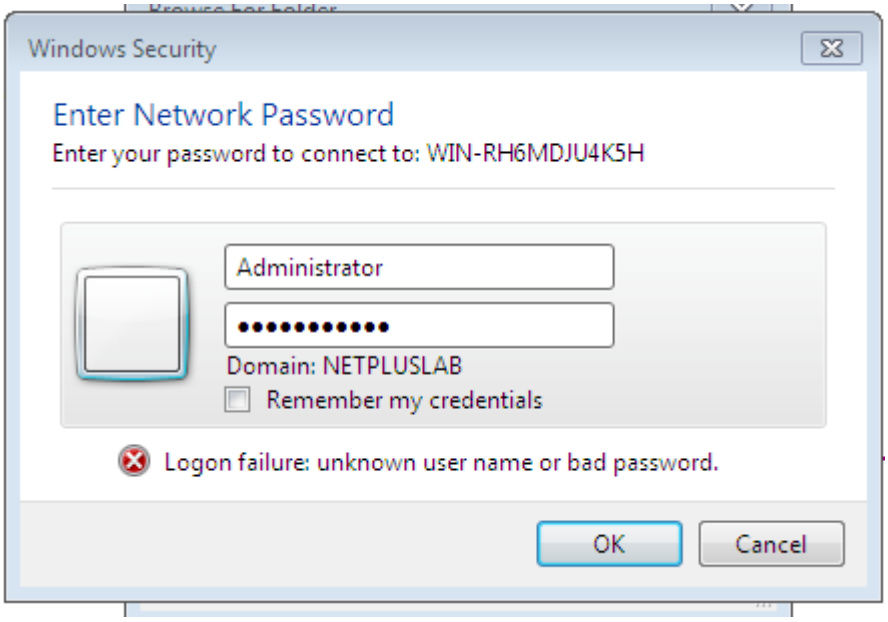


Log on to Workstation 1 – Start – Computer – Map Network Drive – In the folder text box, type \\10.0.0.29\netplus - Finish

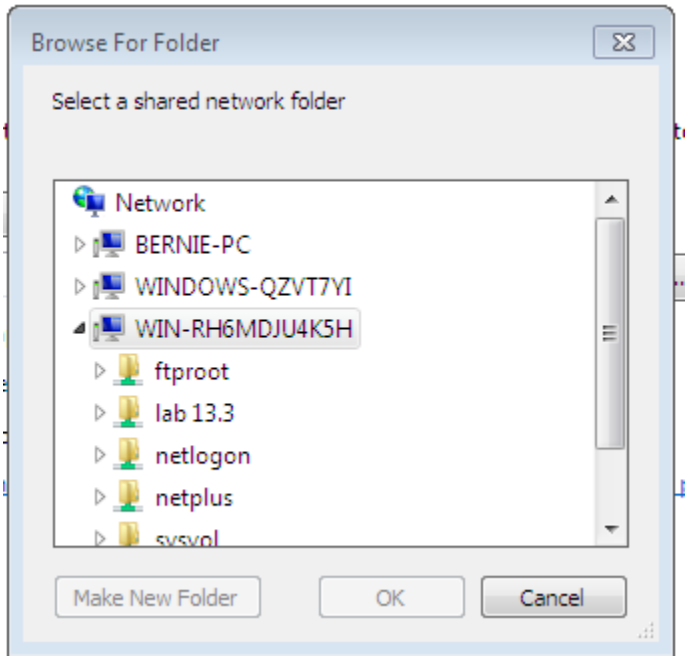

Map Network Drive
What network folder would you like to map?
Specify the drive letter for the connection and the folder that you want to connect to:
Drive:
Z:
Folder:
\\10.0.0.29\netplus
Browse...
Example: \\server\share
Reconnect at logon
Connect using different credentials
Connect to a Web site that you can use to store your documents and pictures.
Finish
Cancel


Browse For Folder
Select a shared network folder
Network
BERNIE-PC
WINDOWS-QZVT7YI
WIN-RH6MDJU4K5H
Make New Folder
OK
Cancel

Enter Administrator username and password



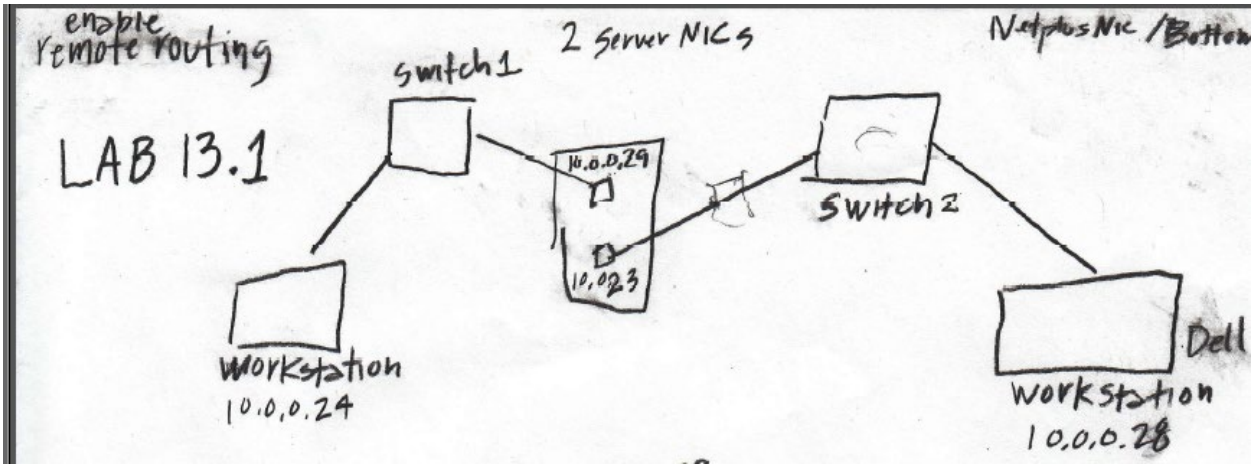
The computer maps the NETPLUS shared folder.



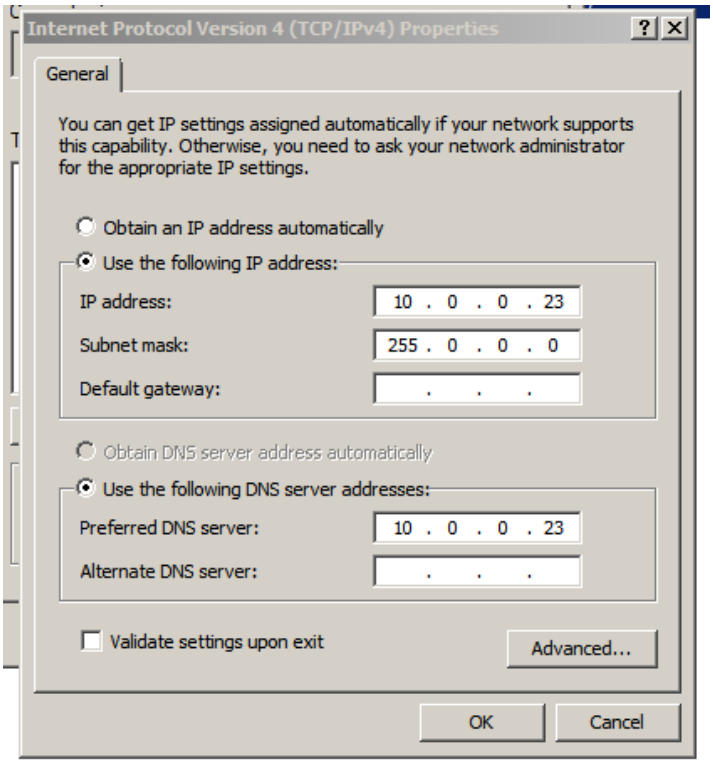
Repeat steps 1 through 5 on Workstation 2 - You have now verified that you can log on to Server 1 with both computers.

Leave the room while your instructor causes a network problem and shuts down the computers. Re-enter room, Log on and identify the problem – fix and log off.

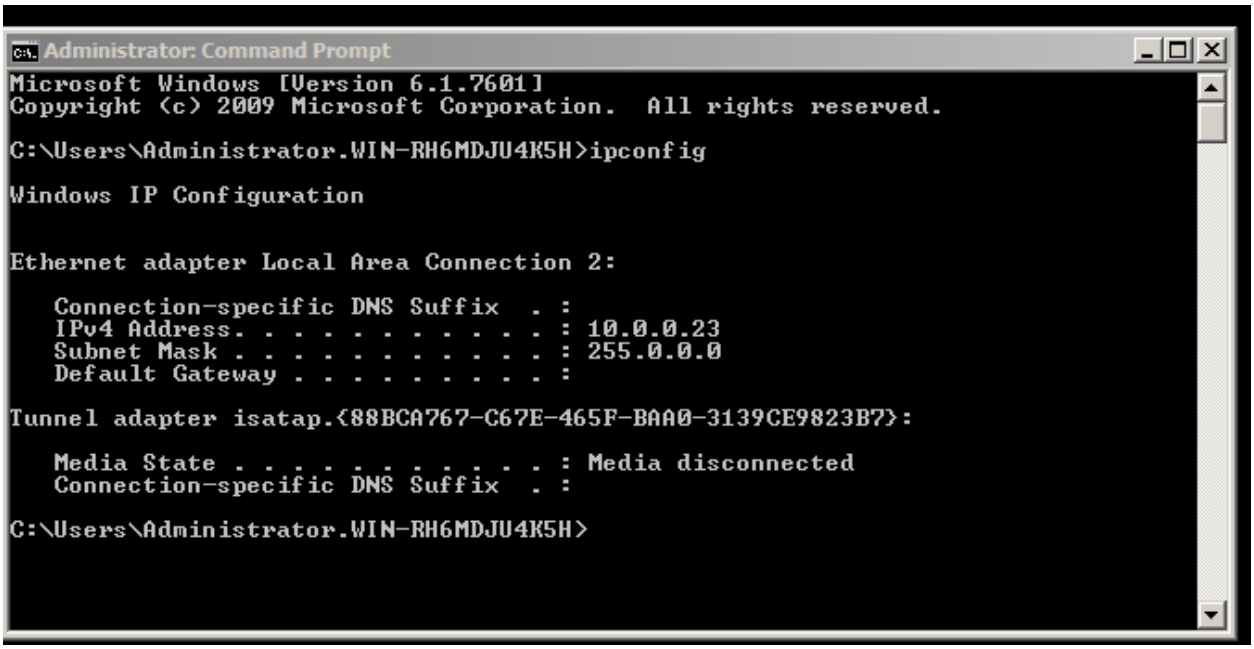
Lab 13.4 Troubleshooting Web Client Problems



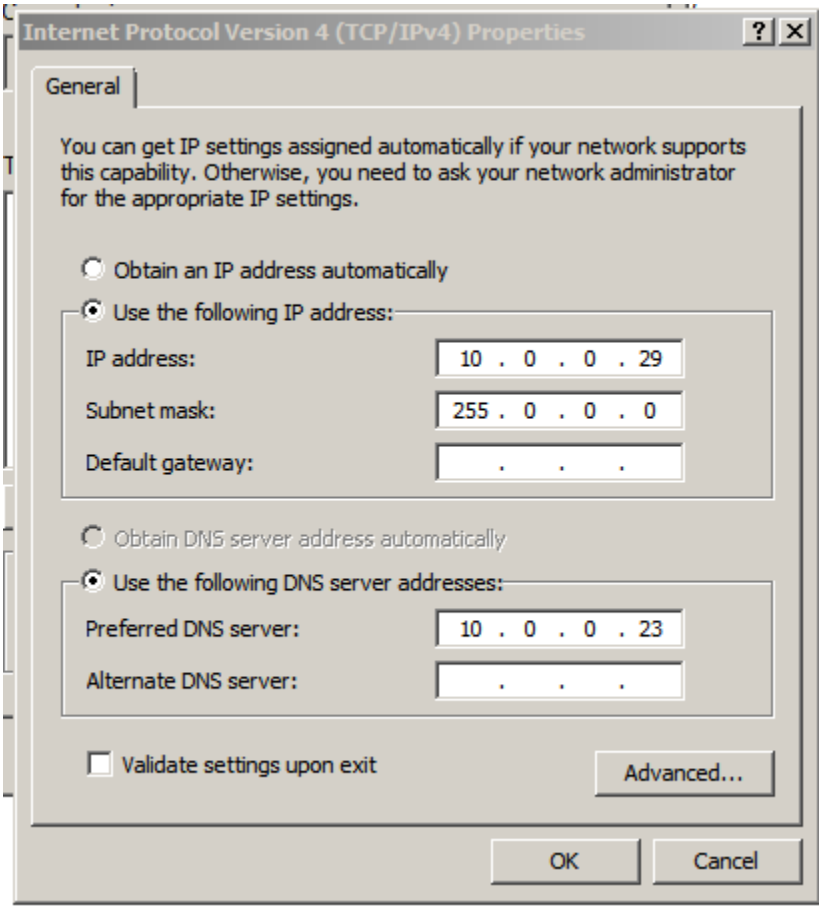
On Server, one NIC configured with an IP address of 10.0.0.23 and a subnet mask of 255.0.0.0



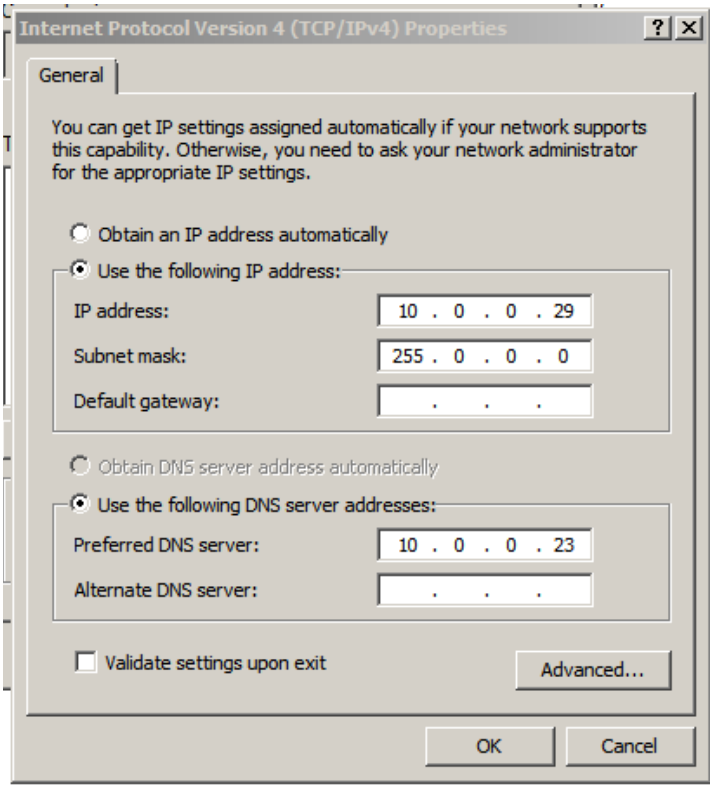
Ping NIC 1 on Server 1 from Server 1



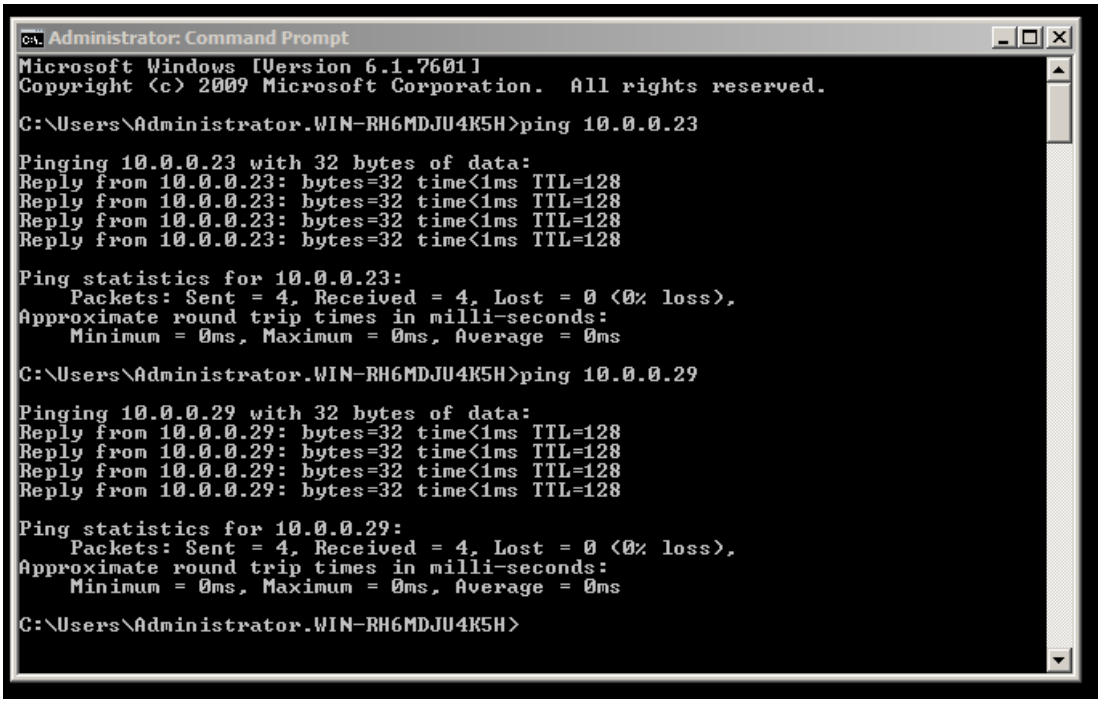
Configure NIC 2 with an IP address of 10.0.0.29 and a subnet mask of 255.0.0.0



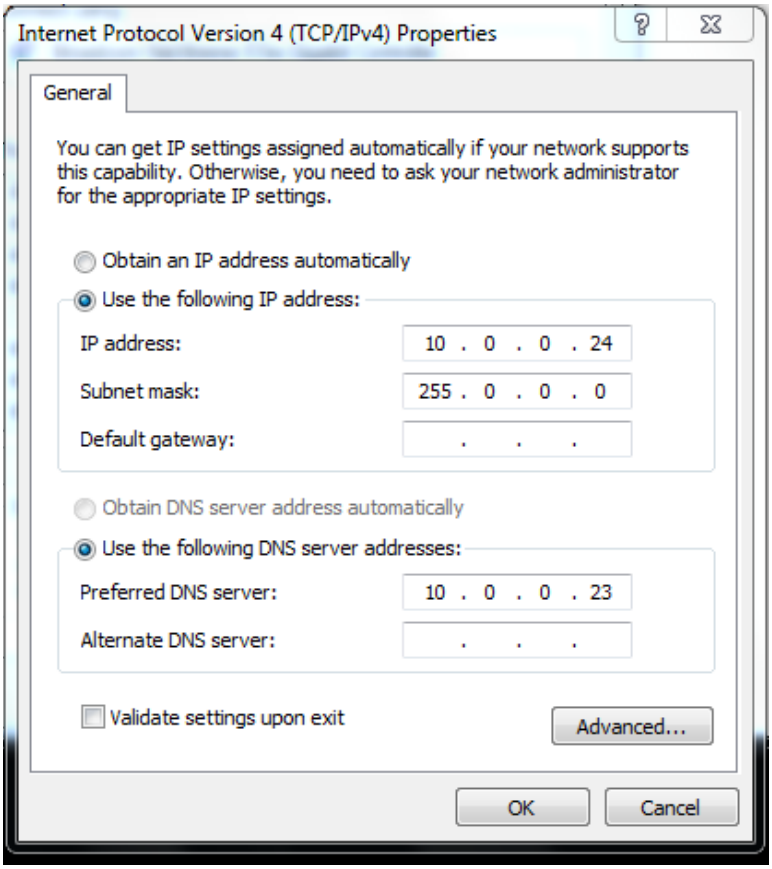
Routing and remote access configured on Server 1 so that it acts as a router. – A Switch named Switch 1 connected to NIC 1 (10.0.0.23). - Switch 2 connected to NIC 2 (10.0.0.29)

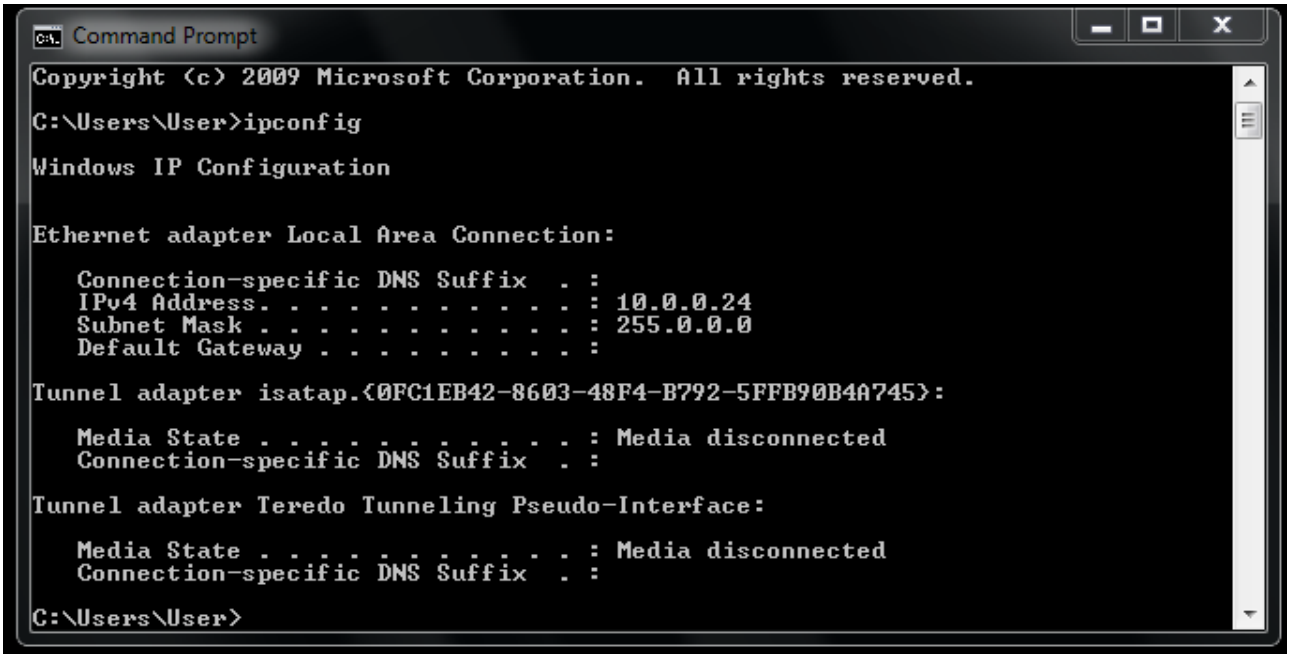


Ping both NIC's on Server 1

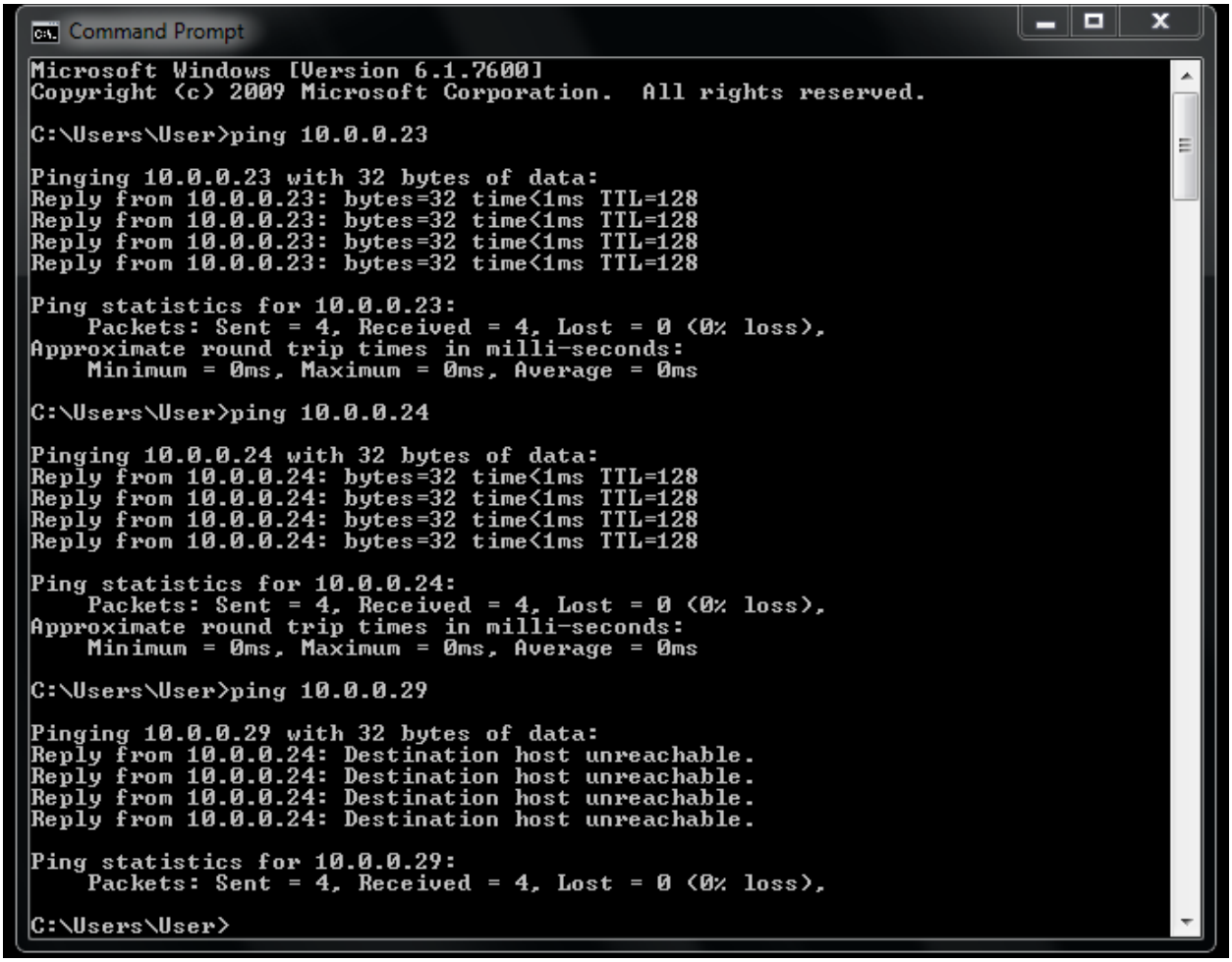


A computer running Windows 7 named workstation 1, configured with an IP address of 10.0.0.24 and a subnet mask of 25.0.0.0 connected to Server through Switch 1.

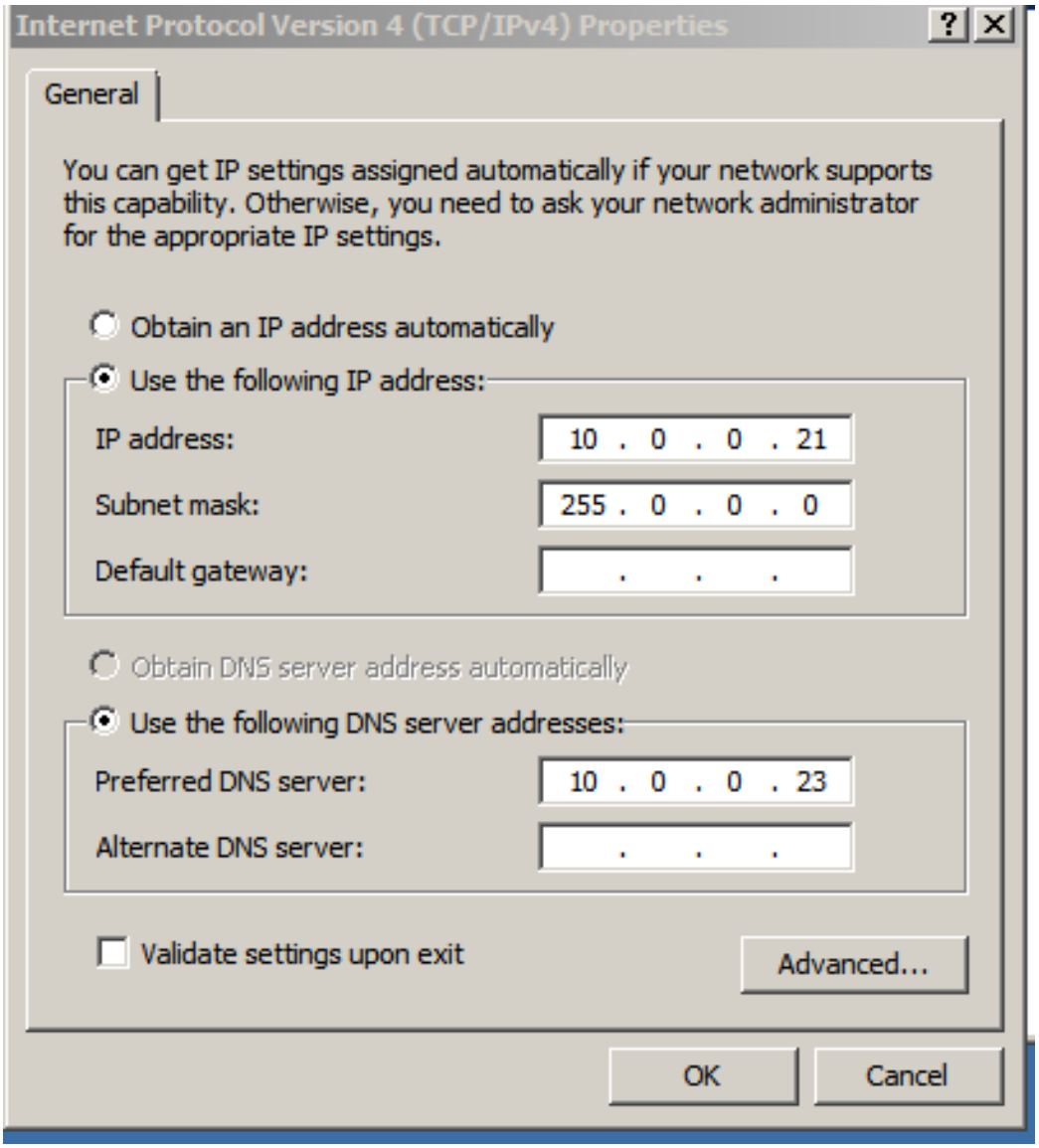




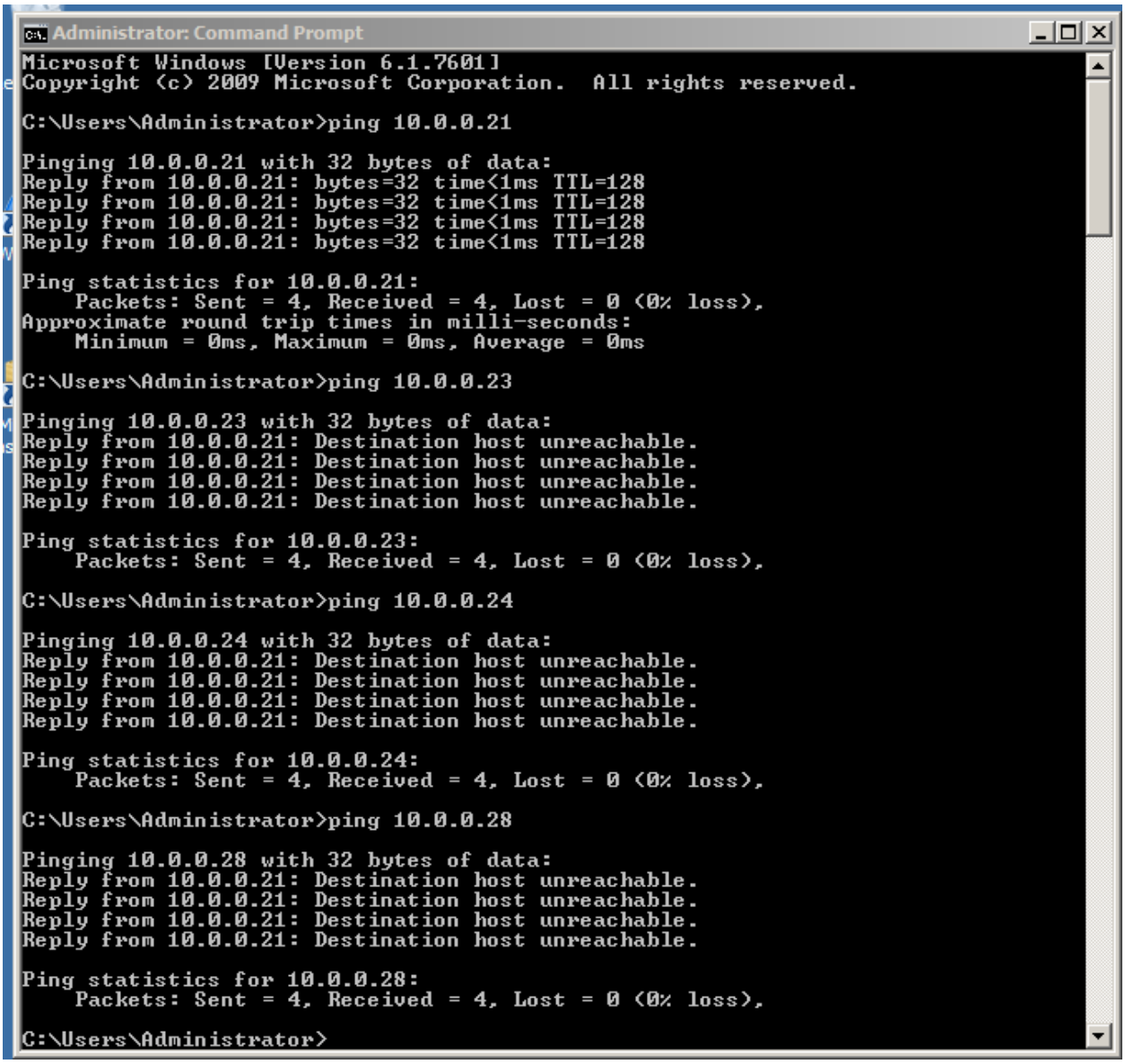
Ping both NIC's on Server and Ping its own NIC from Workstation 1.



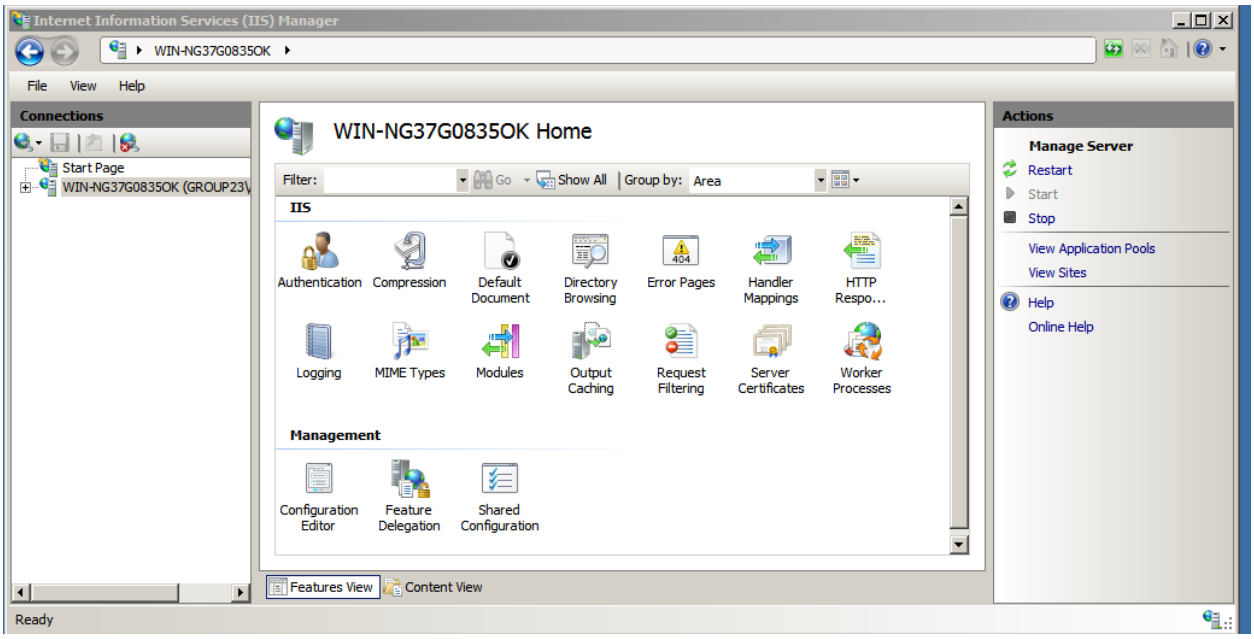
A computer running Windows Server 2008 named Server 2, configured with an IP address of 10.0.0.21 and a subnet mask of 25.0.0.0 connected to Server 1 NIC 10.0.0.29 through Switch 2.

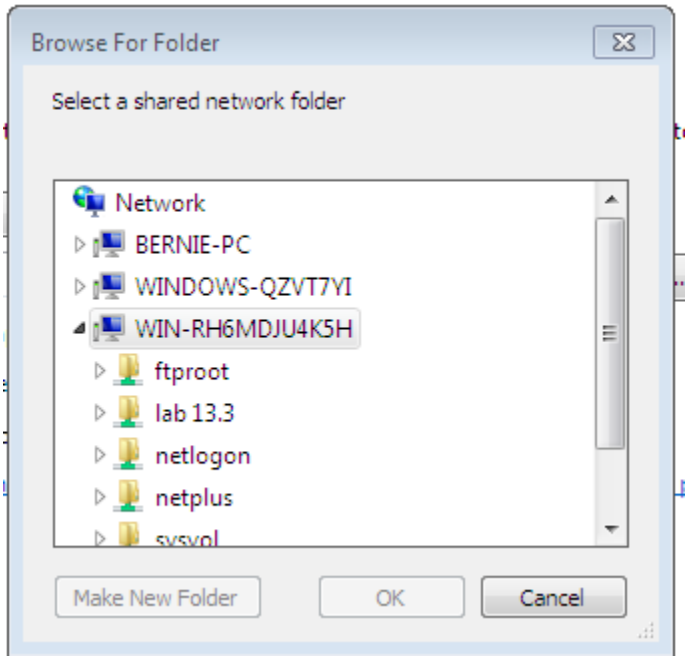


Ping both NIC's on Server, Workstation 1 and Server 2.



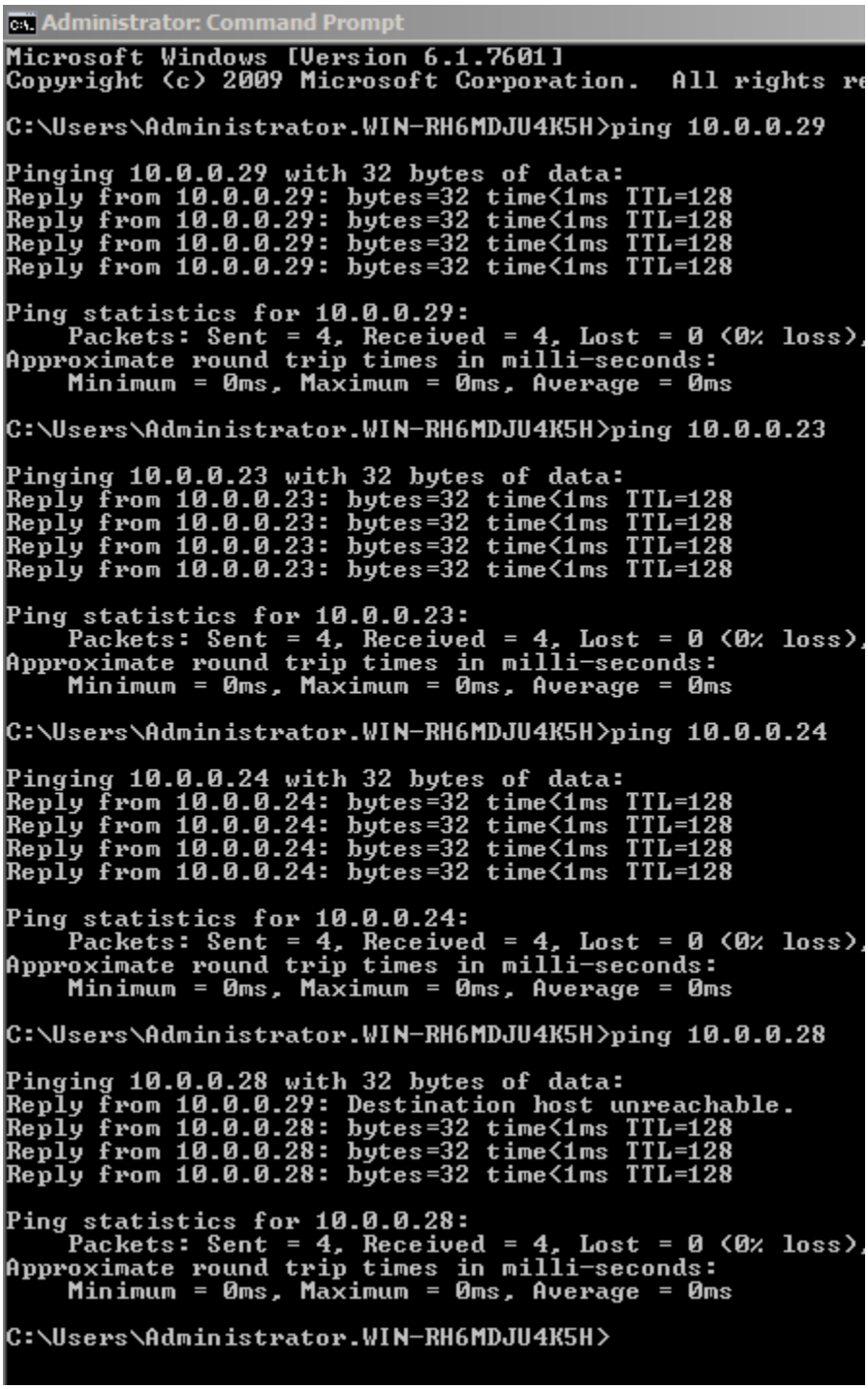
IIS installed and running on Server 2 with a file named “This is test page” in C:\Inetpub\wwwroot





The DNS server running on Server 1

Make sure all computers are communicating with routing and pings.



Log off the 2 Servers and Workstation.

Joseph Martinez

Networking II: Network +
CNG – 125

Chapter Fourteen Labs
Ensuring Integrity and Availability

Lab 14.1 Understanding Malware

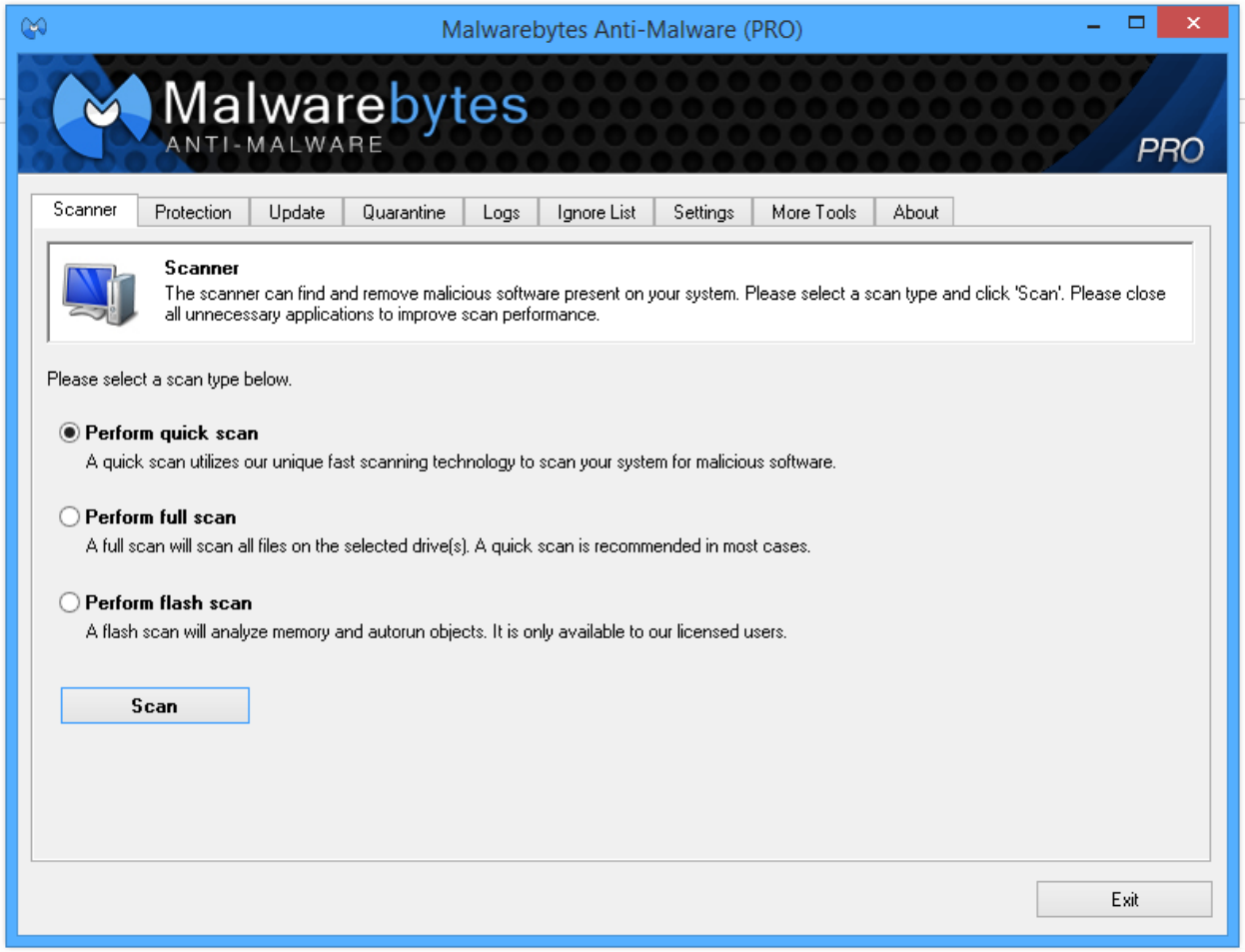
Lab 14.2 Using Uninterruptible Power Supplies (UPS's)

Lab 14.3 Configuring Raid

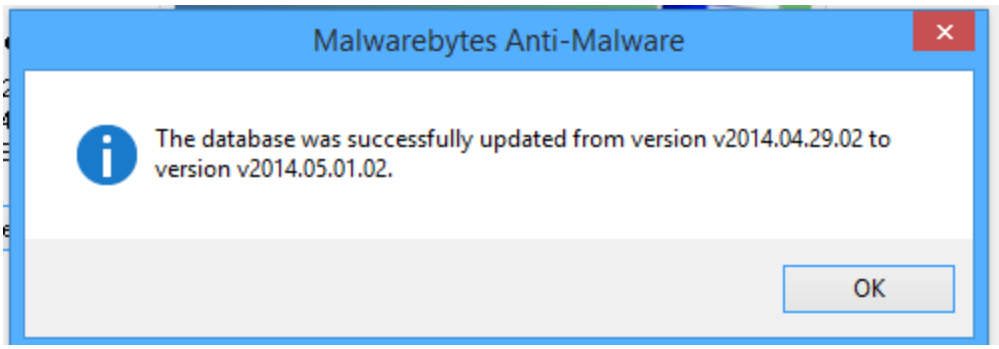
Lab 14.4 Backing up a Windows Server 2008 Computer

Lab 14.1 Understanding Malware

Log on to Workstation – Start – All Programs – Malware bytes Anti-Malware

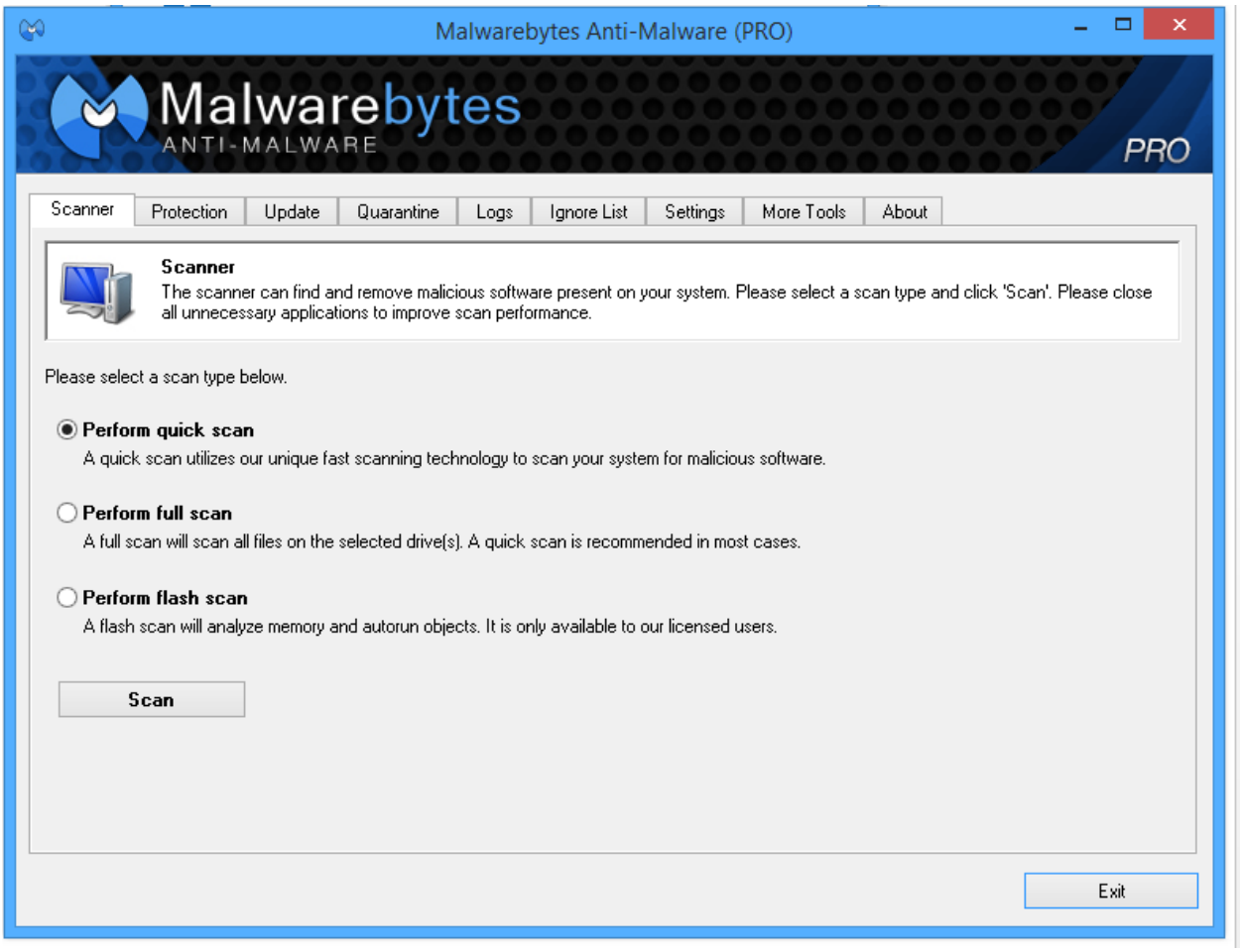


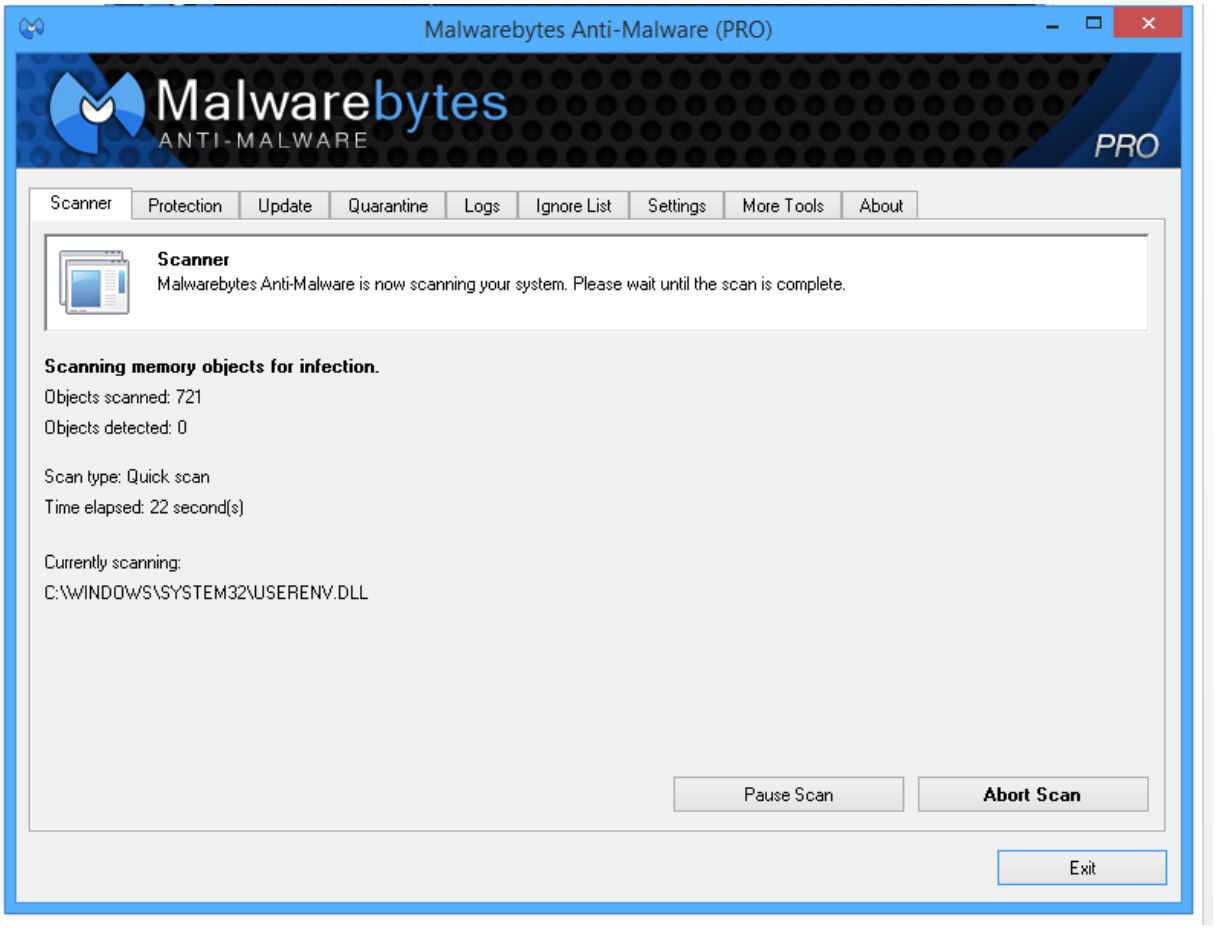
Click Update Now



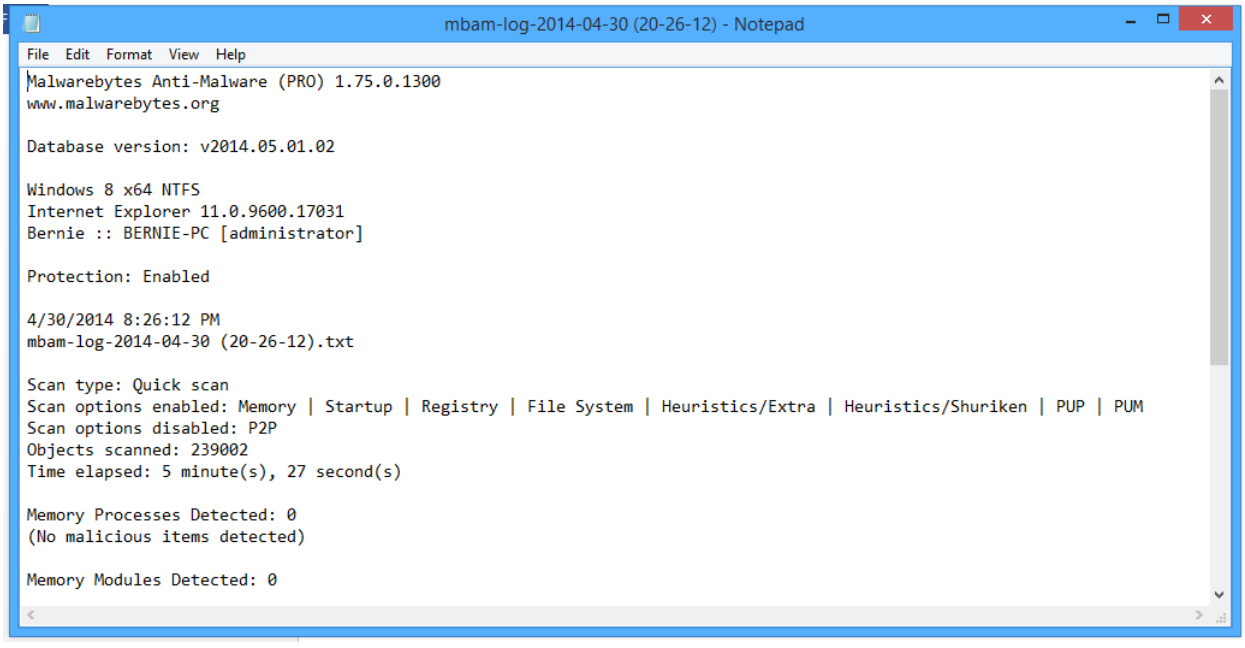
After updates are installed – Close.

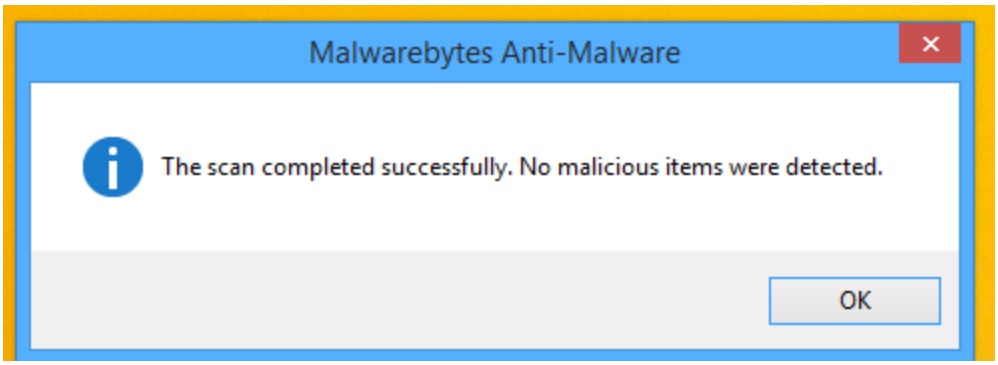
Click Scan for Threats





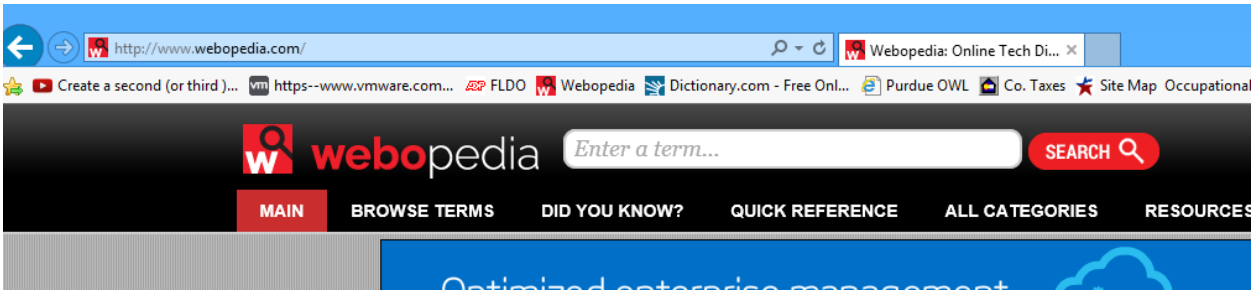
After the scan is finished, the computer shows a summary of the scan, including the number of files scanned, the number of viruses found, and the number of files repaired, quarantined, deleted or excluded.





Click OK

To gain an understanding of virus – related terms, access the Webopedia Web site.



Search Results: "macro virus"

1 2 3 4 5 » Last ›

macro virus

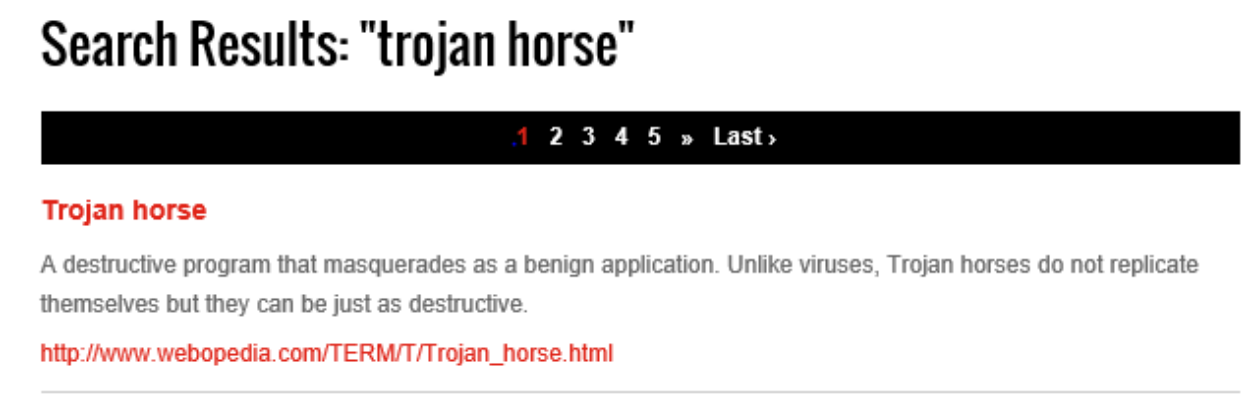
A type of computer virus that is encoded as a macro embedded in a document. Many applications, such as Microsoft Word and Excel, support powerful macro languages.
http://www.webopedia.com/TERM/M/macro_virus.html

Search Results: "worm"

1 2 3 4 5 » Last ›

worm

(1) A program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down. Also see virus



Log off

Lab 14.2 Using Uninterruptible Power Supplies (UPS's)

An uninterruptible power supply, also uninterruptible power source, UPS or battery/flywheel backup, is an electrical apparatus that provides emergency power to a load when the input power source, typically mains power, fails. A UPS differs from an auxiliary or emergency power system or standby generator in that it will provide near-instantaneous protection from input power interruptions, by supplying energy stored in batteries, supercapacitors, or flywheels. The on-battery runtime of most uninterruptible power sources is relatively short (only a few minutes) but sufficient to start a standby power source or properly shut down the protected equipment.

A UPS is typically used to protect hardware such as computers, data centers, telecommunication equipment or other electrical equipment where an unexpected power disruption could cause injuries, fatalities, serious business disruption or data loss. UPS units range in size from units designed to protect a single computer without a video monitor (around 200 volt-ampere rating) to large units powering entire data centers or buildings. The world's largest UPS, the 46-megawatt Battery Electric Storage System (BESS), in Fairbanks, Alaska, powers the entire city and nearby rural communities during outages.

A small free-standing UPS with one IEC 60320 C14 input and three C13 outputs

VA Rating

Volt-ampere (VA) is a measurement of power in a direct current (DC) electrical circuit. The VA specification is also used in alternating current (AC) circuits, but it is less precise in this application, because it represents apparent power , which often differs from true power .

In a DC circuit, 1 VA is the equivalent of one watt (1 W). The power, P (in watts) in a DC circuit is equal to the product of the voltage V (in volt s) and the current I (in ampere s):

P = VI

In an AC circuit, power and VA mean the same thing only when there is no reactance . Reactance is introduced when a circuit contains an inductor or capacitor . Because most AC circuits contain reactance, the VA figure is greater than the actual dissipated or delivered power in watts. This can cause confusion in specifications for power supplies. For example, a supply might be rated at 600 VA. This does not mean it can deliver 600 watts, unless the equipment is reactance-free. In real life, the true wattage rating of a power supply is 1/2 to 2/3 of the VA rating.

When purchasing a power source such as an uninterruptible power supply (UPS) for use with electronic equipment (including computers, monitors, and other peripherals), be sure the VA specifications for the equipment are used when determining the minimum ratings for the power supply. The VA figure is nominally 1.67 times (167 percent of) the power consumption in watts. Alternatively, you can multiply the VA rating of the power supply by 0.6 (60 percent) to get a good idea of its power-delivering capability in watts.

Lab 14.3 Configuring Raid

Setting up RAID 5 on Windows Server 2008

Pre-requisites

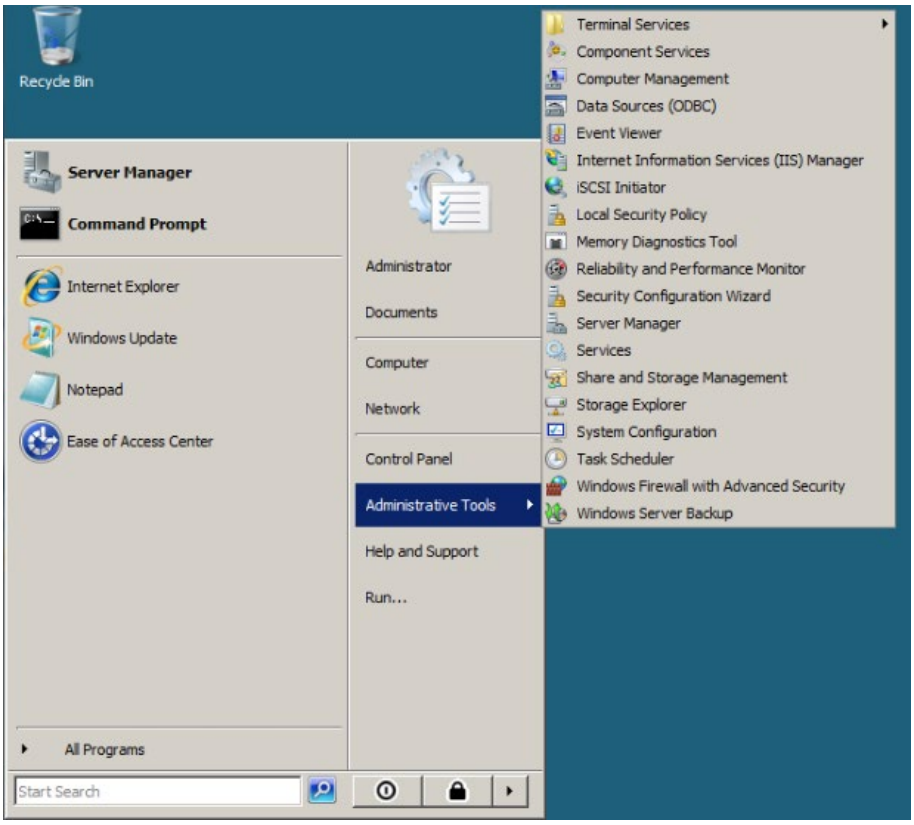
[_] Windows Server 2008

[_] Administrative account to above system

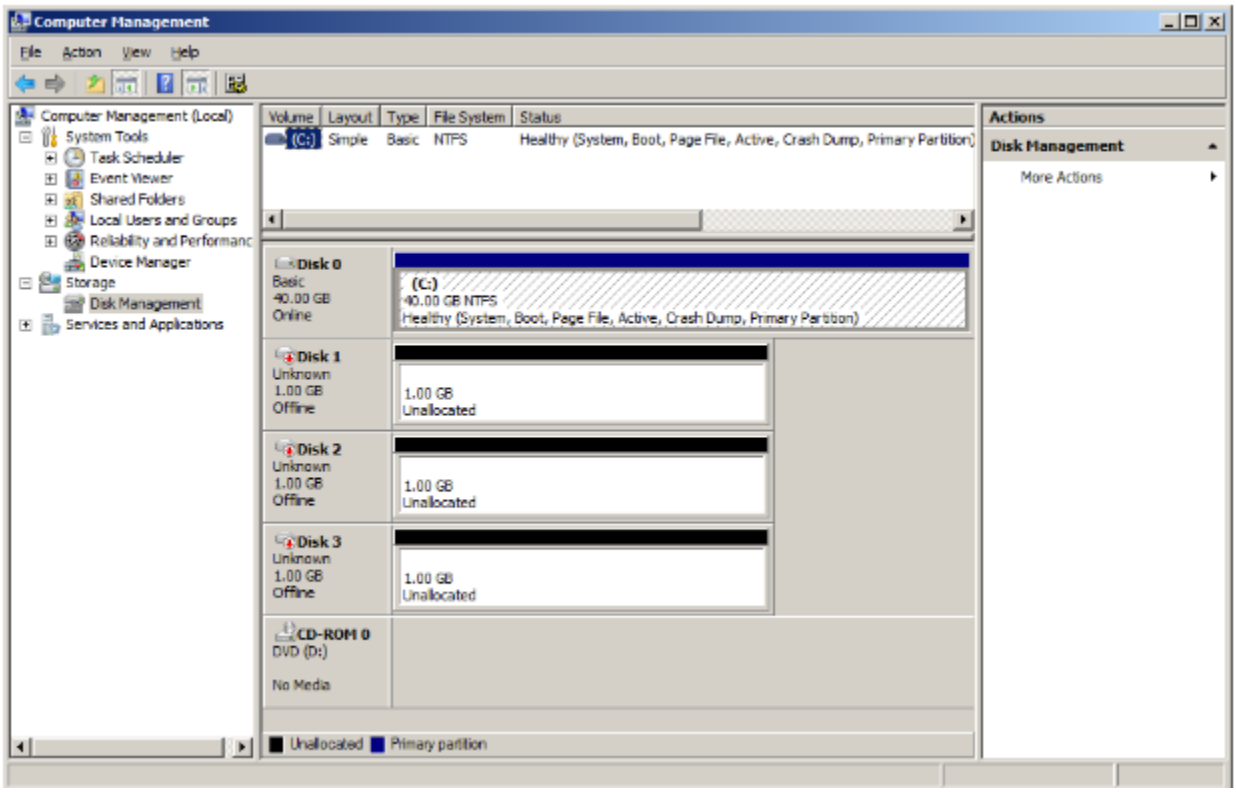
[_] At least three extra hard-drives(Min of three needed for RAID5)

Instructions

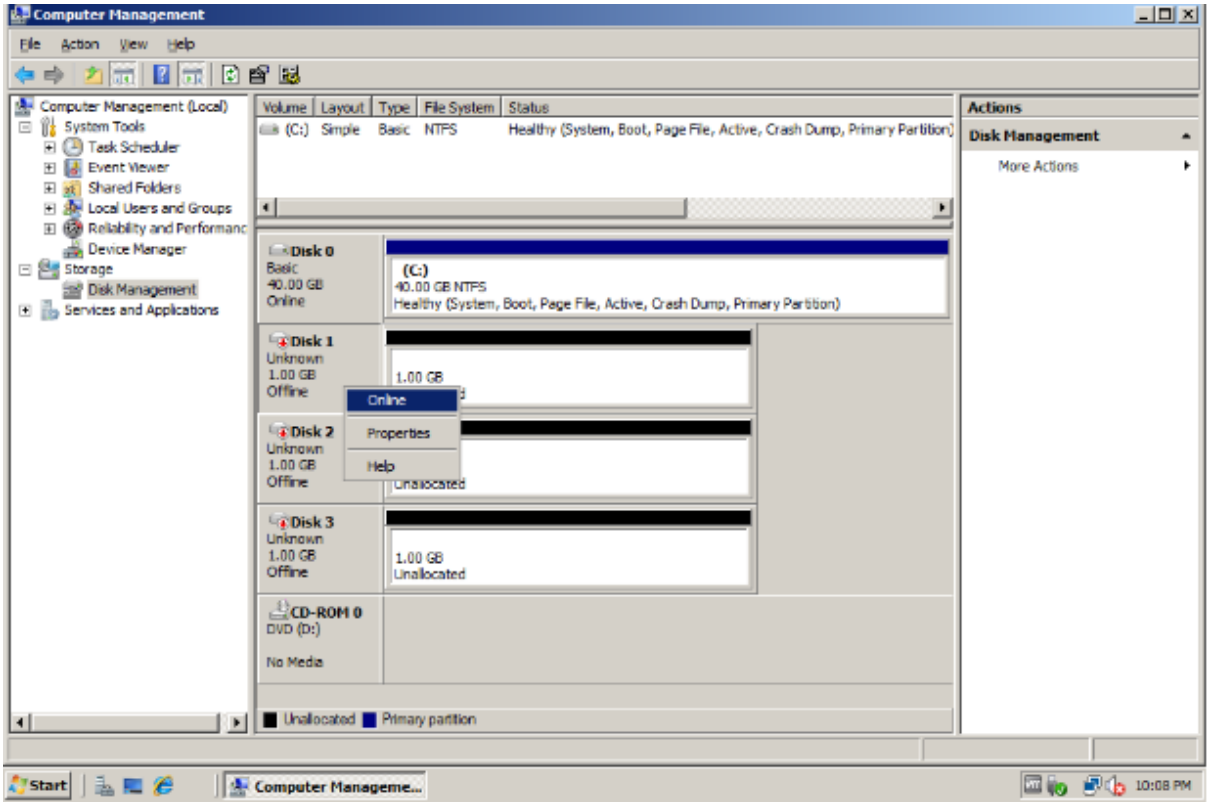
1. Login with the Administrative account
2. Navigate to 'Computer Management' (Start->Administrative Tools->Computer Management)



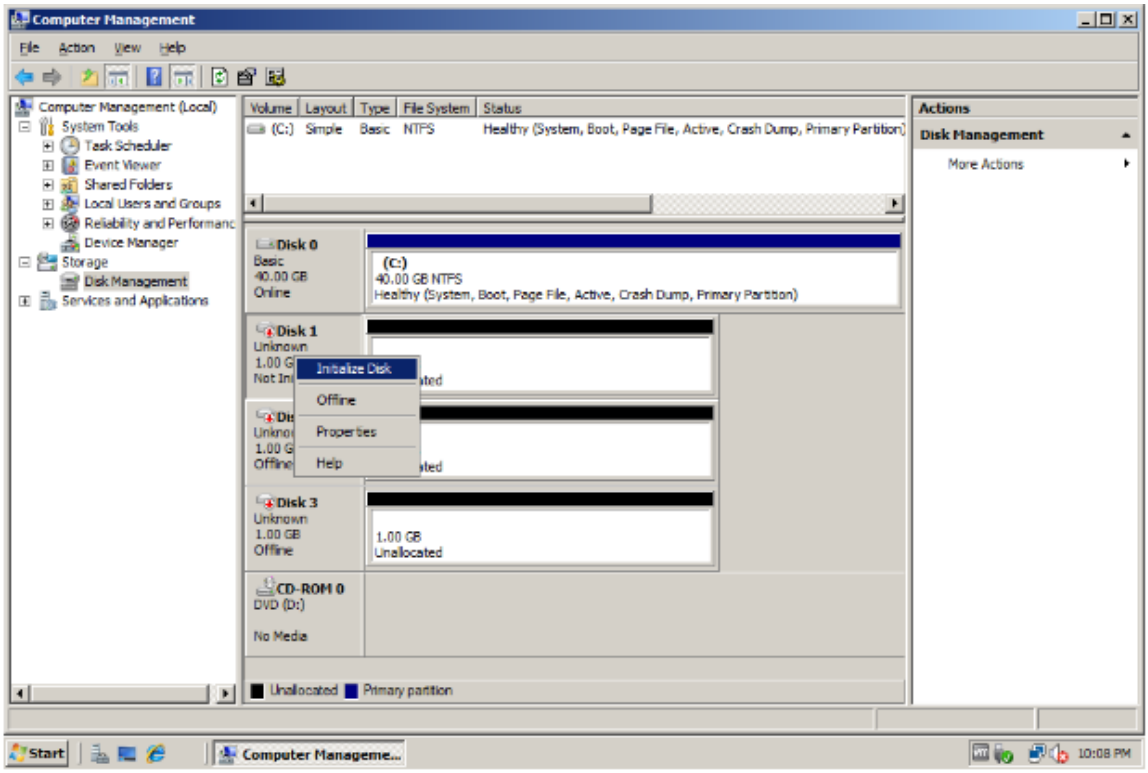
3. In 'Computer Management' click on 'Disk Management' and you should see something like the following:



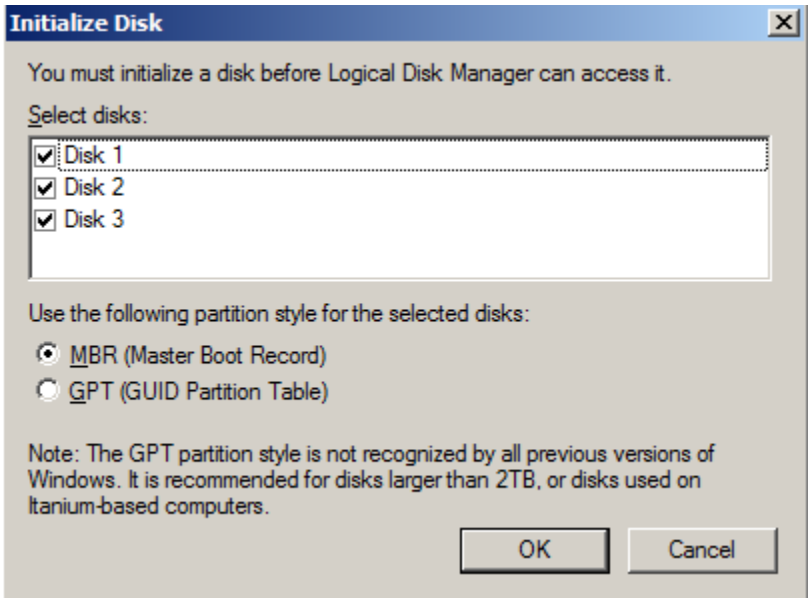
4. Right click on each of your new Disks, and select 'Online'



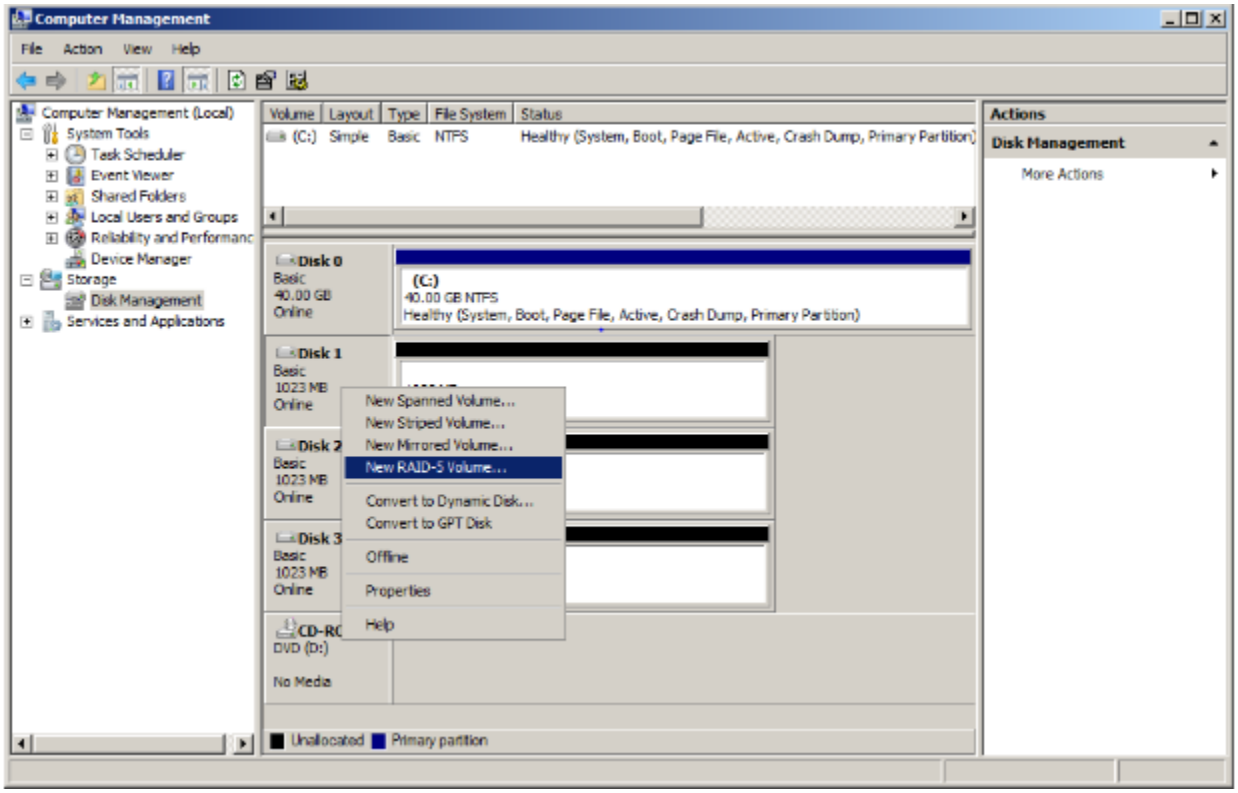
5. Now Right click on one of them again and select 'Initialize Disk'



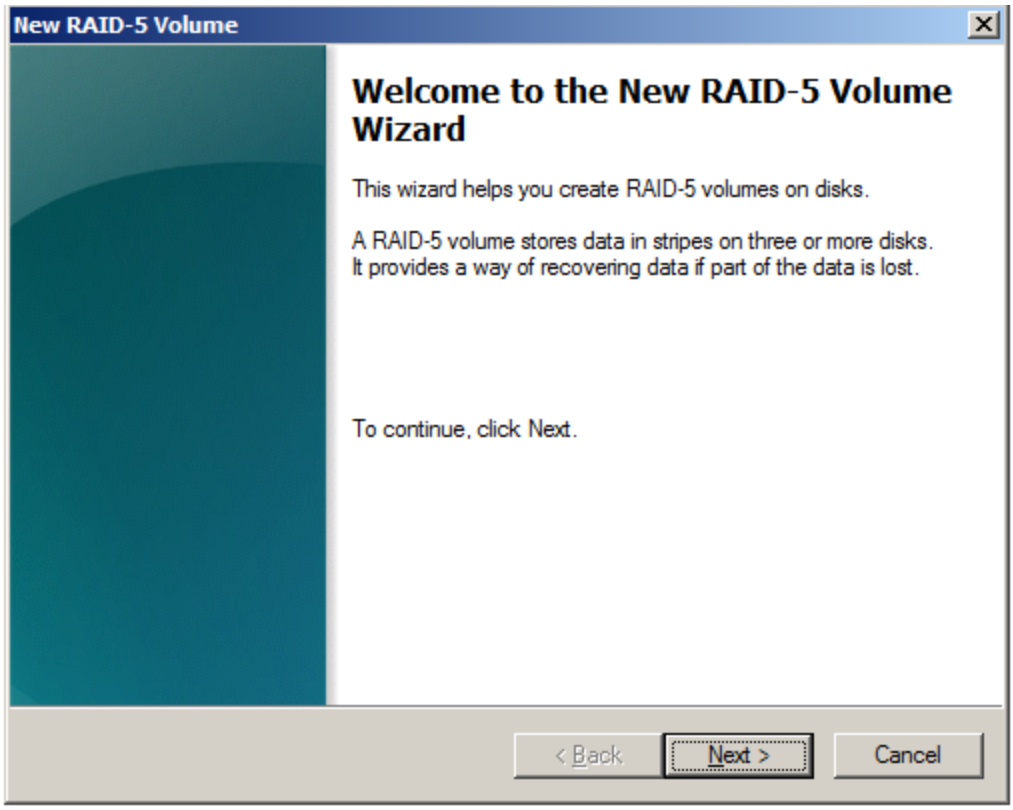
6. You can accept the default configurations and select [OK] (All three[or more] disks should already be selected)



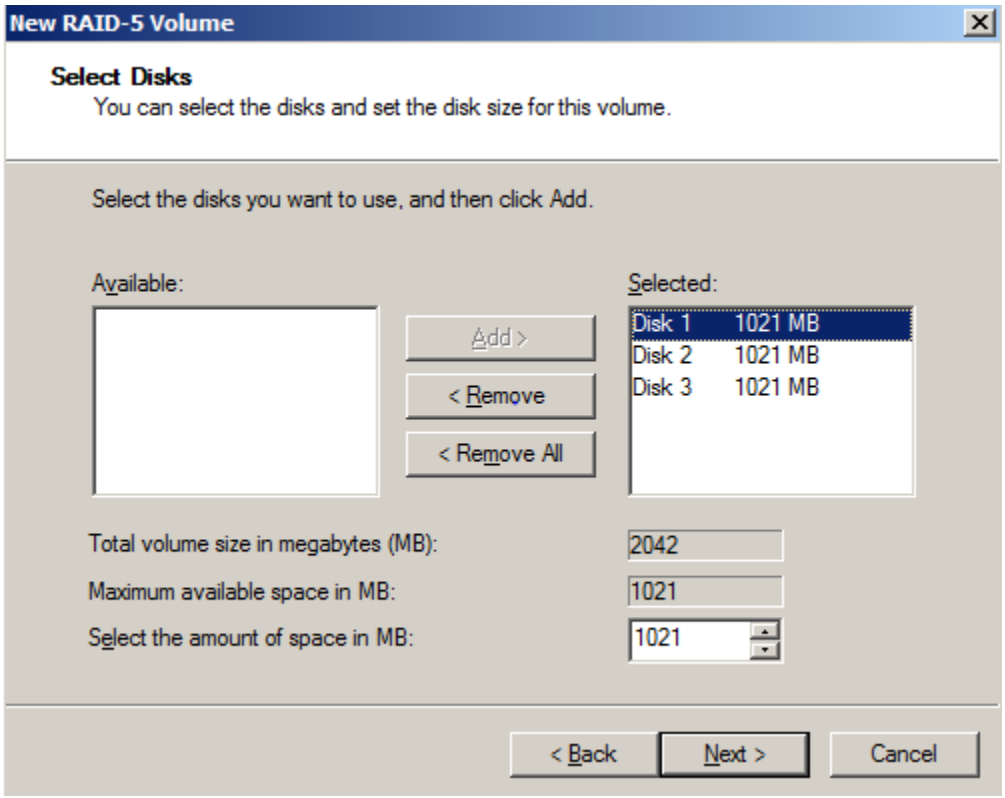
7. Now right click on one of the drives and select 'New RAID-5 Volume...'



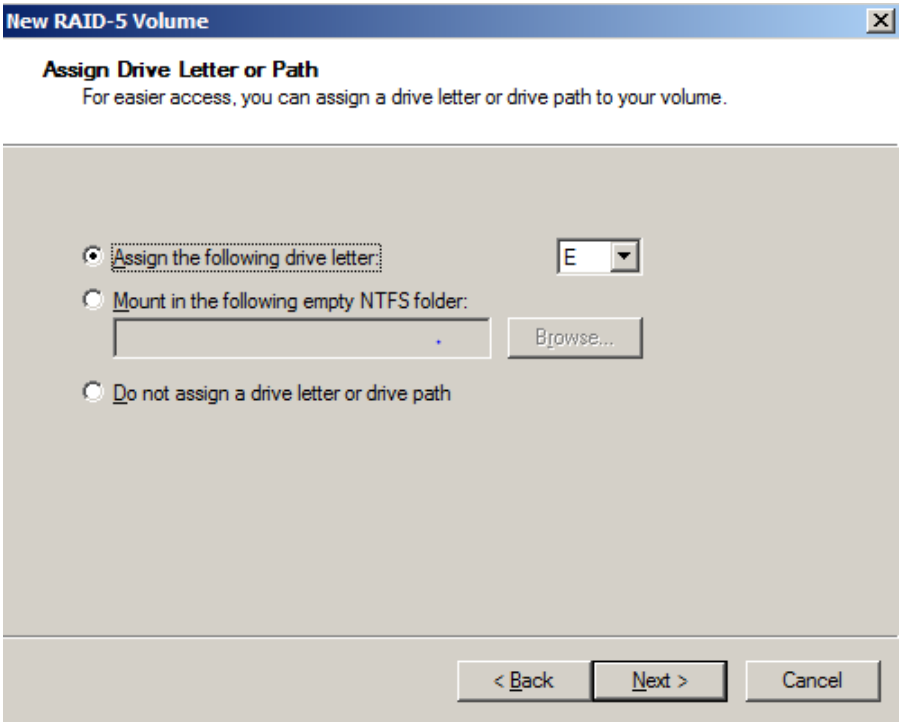
8. On the RAID-5 Wizard screen click [Next]



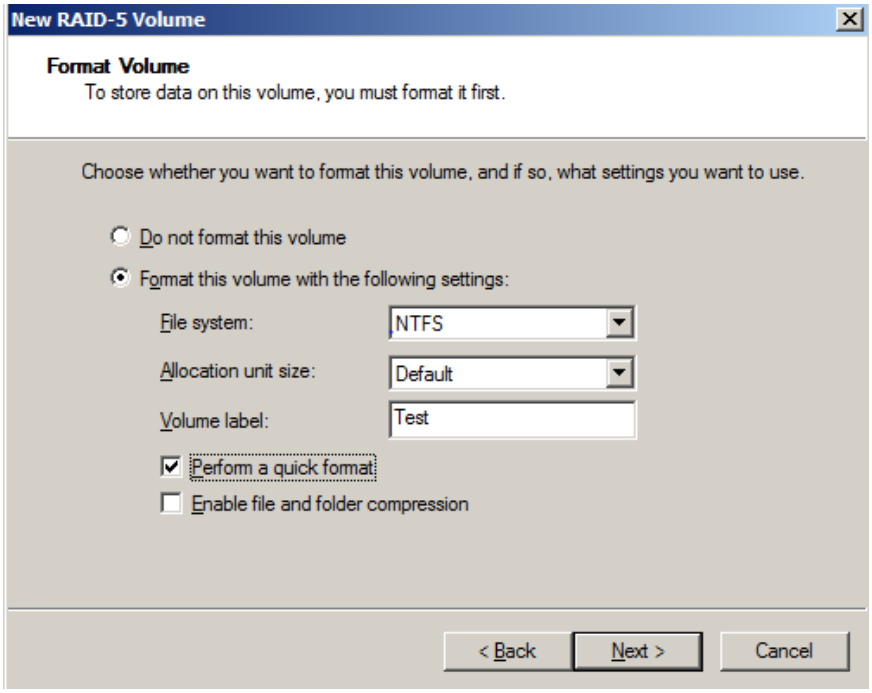
9. On the 'Select Disks' screen highlight and click [Add >] for the disks you wish to have added to the 'Selected' list. Then click [Next]



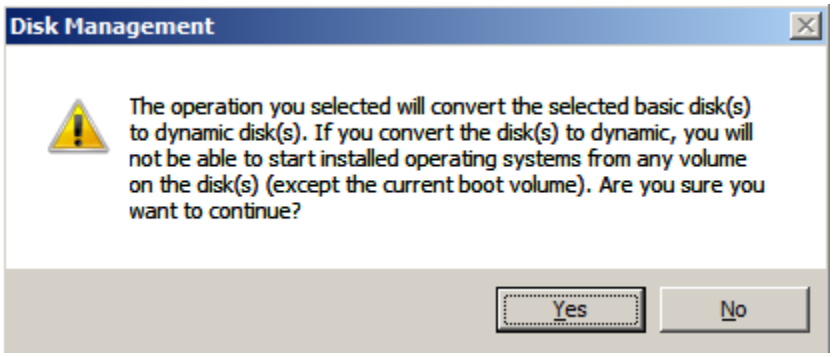
10. You'll now be asked to pick a drive letter for your new RAID5 volume, select what you would like then click [Next]



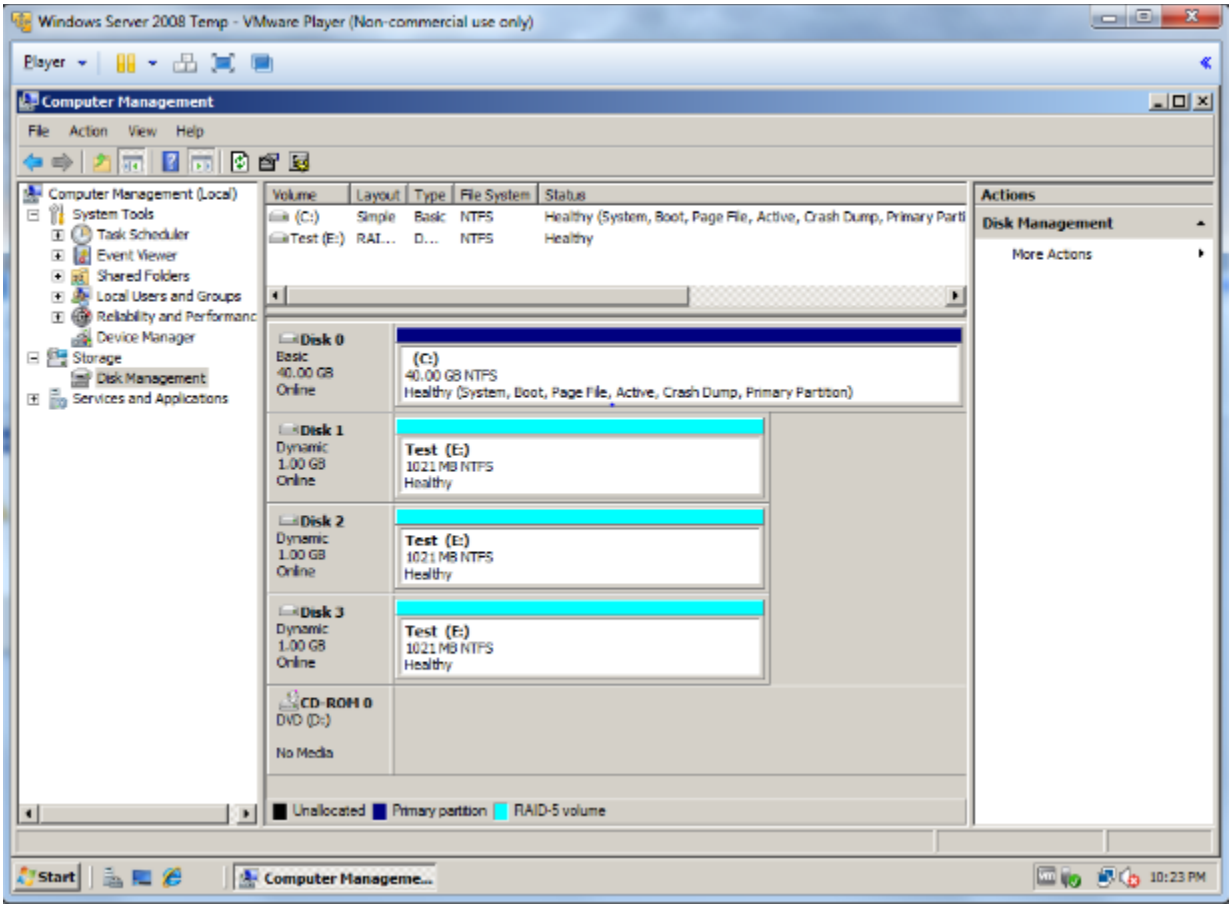
11. On the 'Format Volume' screen, change the features you would like to. (Large volumes will take a very long time to format, but is the best way to confirm that your disks are functioning.) For this test we're going to select 'Perform a quick format', and change the 'Volume Label' to "Test". Then click [Next]



12. On the 'Completing' screen click [Finish], you may then see the next popup click [Yes]



13. The setup may take some time, but when it completes you should now see your new drive letter in the area above the physical drive list.



14. You will now be able to go to your 'Computer' and access this new redundant storage. (Anything you put in here will now be protected against the loss of one of the three drives.)

Being able to setup RAID5 using software is an easy way to save money and get a redundant storage media. You will be able to have one disk fail and your data will still be safe. If you loose two disks your data is gone. For very important data always keep off system backups

Lab 14.4 Backing up a Windows Server 2008 Computer

How to install Windows Server Backup

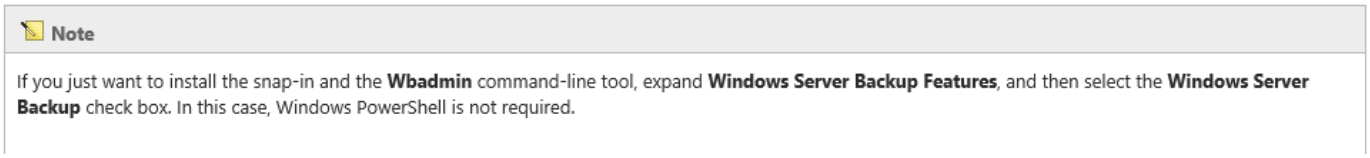
To access backup and recovery tools for Windows Server 2008, you must install the Windows Server Backup, Command-line Tools, and Windows PowerShell items that are available in the Add Features Wizard in Server Manager. This installs the following tools:

To install backup and recovery tools

1.Click Start, click Server Manager, in the left pane click Features, and then in the right pane click Add Features. This opens the Add Features Wizard.

2.In the Add Features Wizard, on the Select Features page, expand Windows Server Backup Features, and then select the check boxes for Windows Server Backup and Command-line Tools.

You will receive a message that Windows PowerShell is also required to be installed with these features.



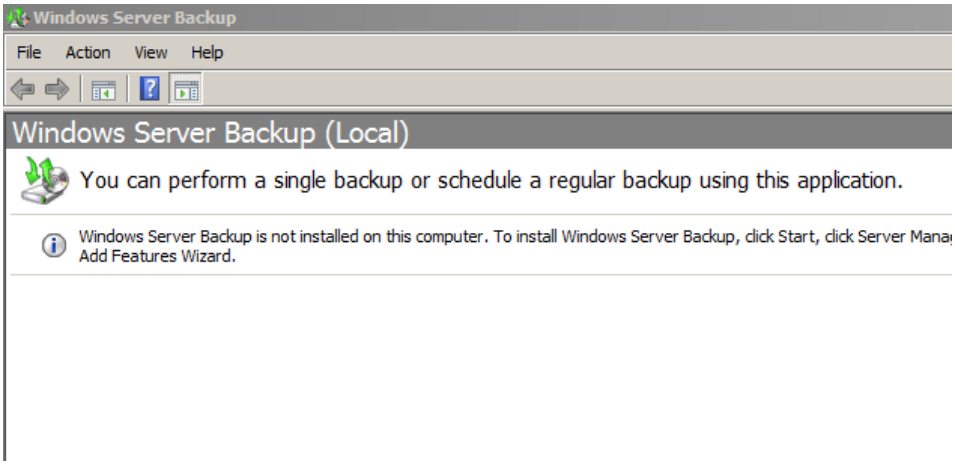
3.Click Add Required Features, and then click Next.

4.On the Confirm Installation Selections page, review the choices that you made, and then click Install. If there is an error during the installation, it will be noted on the Installation Results page.

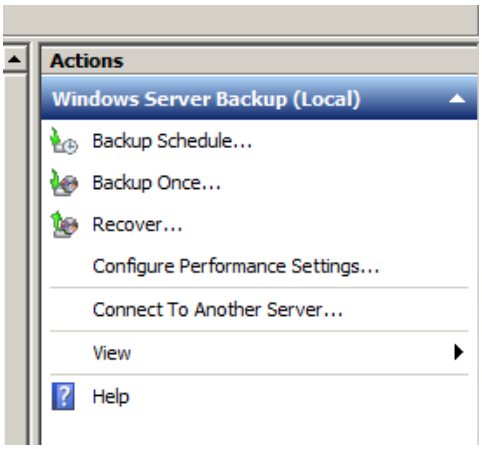
5.Then, to access these backup and recovery tools, do the following:

◦ To access the Windows Server Backup snap-in, click Start, click Administrative Tools, and then click Windows Server Backup.

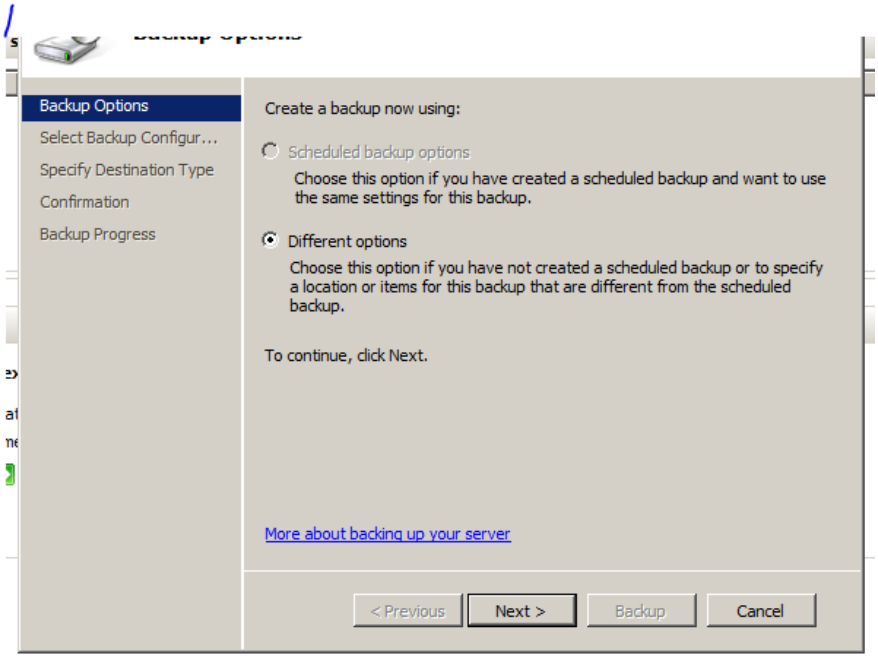
Log on to Server – Administrative Tools – Windows Server Backup –



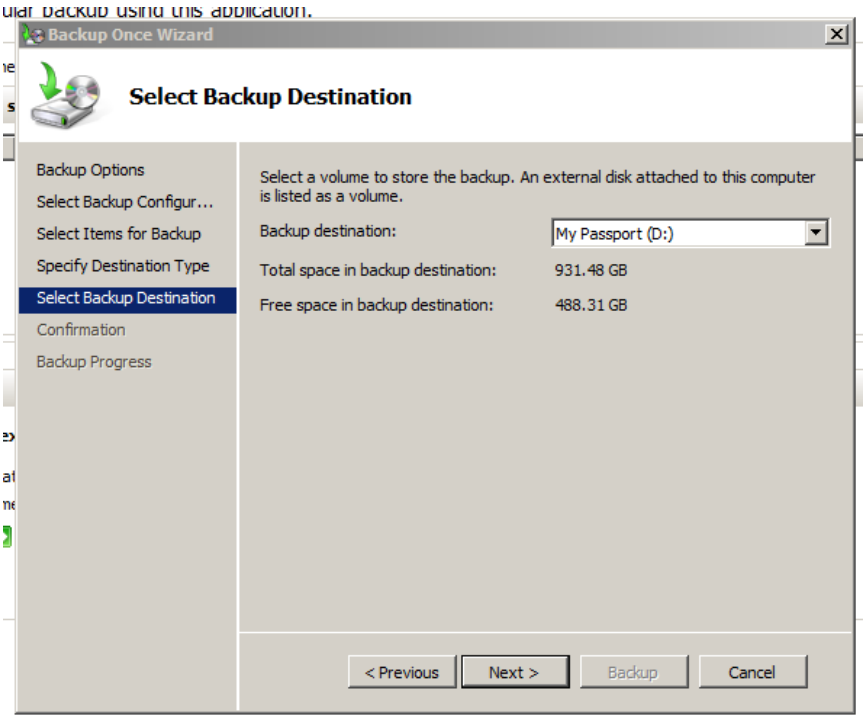
Click Backup Once –

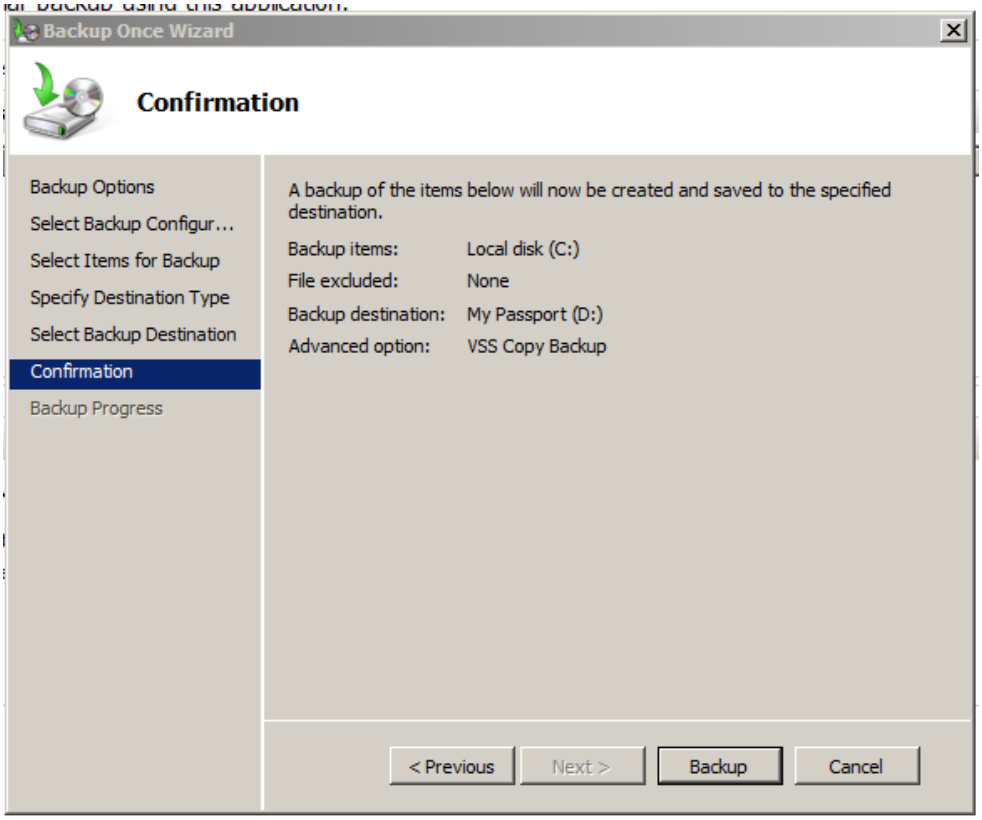


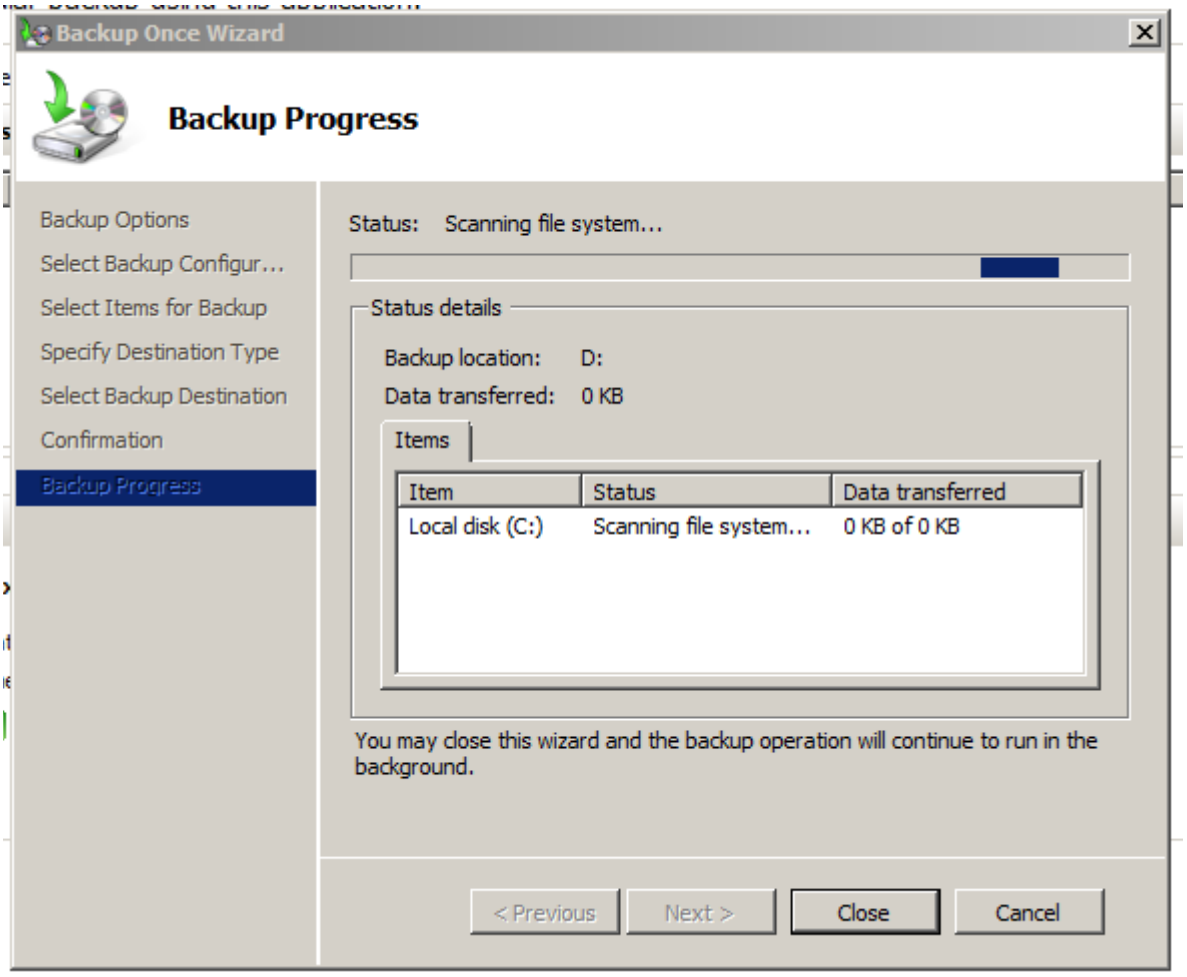
The Backup Once Wizard opens –



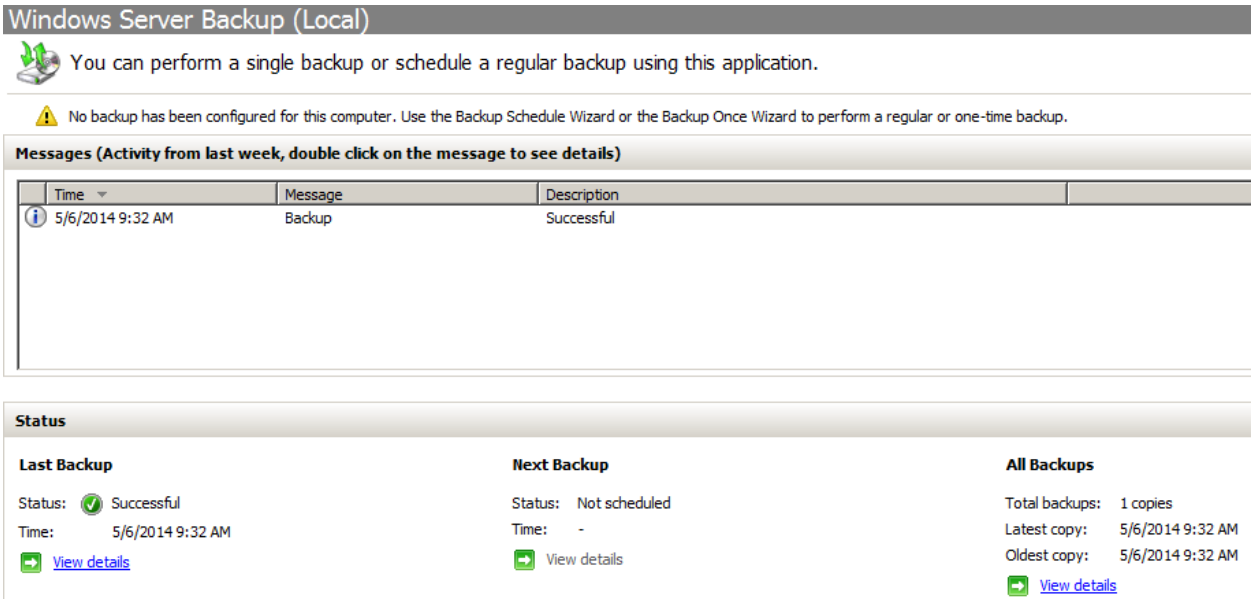
Make sure that the Different Options button is selected – The Wizard asks you what you want to backup – Click Custom – The wizard asks you what volumes you want to backup – The wizard asks you to choose the destination volume –







The Backup progress window opens and the status box indicates the various backup states being completed. After a few minutes, the Backup progress window indicates that the backup is complete. – Close – click Recover in the Actions pane – The Recovery Wizard opens – Choose the server you are on – Next –Select the date and time that the backup was made – Next – Click Files and folders – Next – Expand the Server 1 node – select autoexec.bat – Next - Click Next again to accept the Recovery – When the recovery has completed – Click Close – Log off.


Windows Server Backup (Local)
You can perform a single backup or schedule a regular backup using this application.
No backup has been configured for this computer. Use the Backup Schedule Wizard or the Backup Once Wizard to perform a regular or one-time backup.
Messages (Activity from last week, double click on the message to see details)
Time
Message
Description
5/6/2014 9:32 AM
Backup
Successful
Status
Last Backup
Status: Successful
Time: 5/6/2014 9:32 AM
View details
Next Backup
Status: Not scheduled
Time: -
View details
All Backups
Total backups: 1 copies
Latest copy: 5/6/2014 9:32 AM
Oldest copy: 5/6/2014 9:32 AM
View details

Joseph Martinez

05-01-14

Networking II: Network +
CNG – 125

Chapter Fifteen Labs
Implementing and Managing Networks

Lab 15.1 Creating a Project Plan

Lab 15.2 Planning an Upgrade

Lab 15.3 Observing a Network Upgrade

Lab 15.4 Installing and Removing Updates on Windows Server 2008

Lab. 15.5 Researching Network Solutions

Lab 15.1 Creating a Project Plan

Microsoft Project

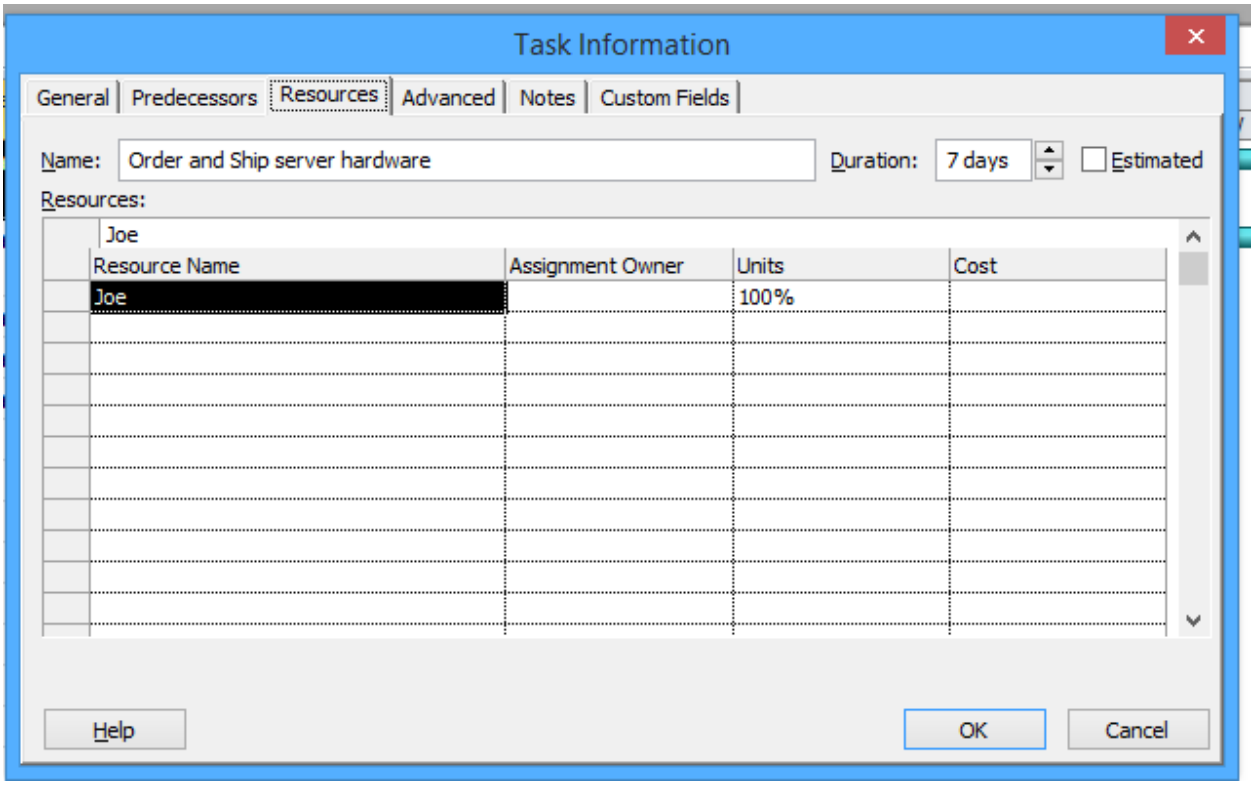
Microsoft Project is a project management software program, developed and sold by Microsoft, which is designed to assist a project manager in developing a plan, assigning resources to tasks, tracking progress, managing the budget, and analyzing workloads.

Microsoft Project was the company's third Microsoft Windows-based application, and within a couple of years of its introduction it became the dominant PC-based project management software.

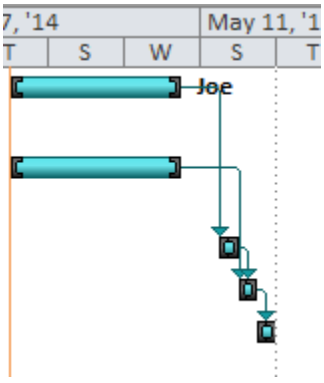
While part of the Microsoft Office family, it has never been included in any of the Office suites. It is available currently in two editions, Standard and Professional. Microsoft Project's proprietary file format is .mpp.

Microsoft Project and Microsoft Project Server are the cornerstones of the Microsoft Office enterprise project management (EPM) product.

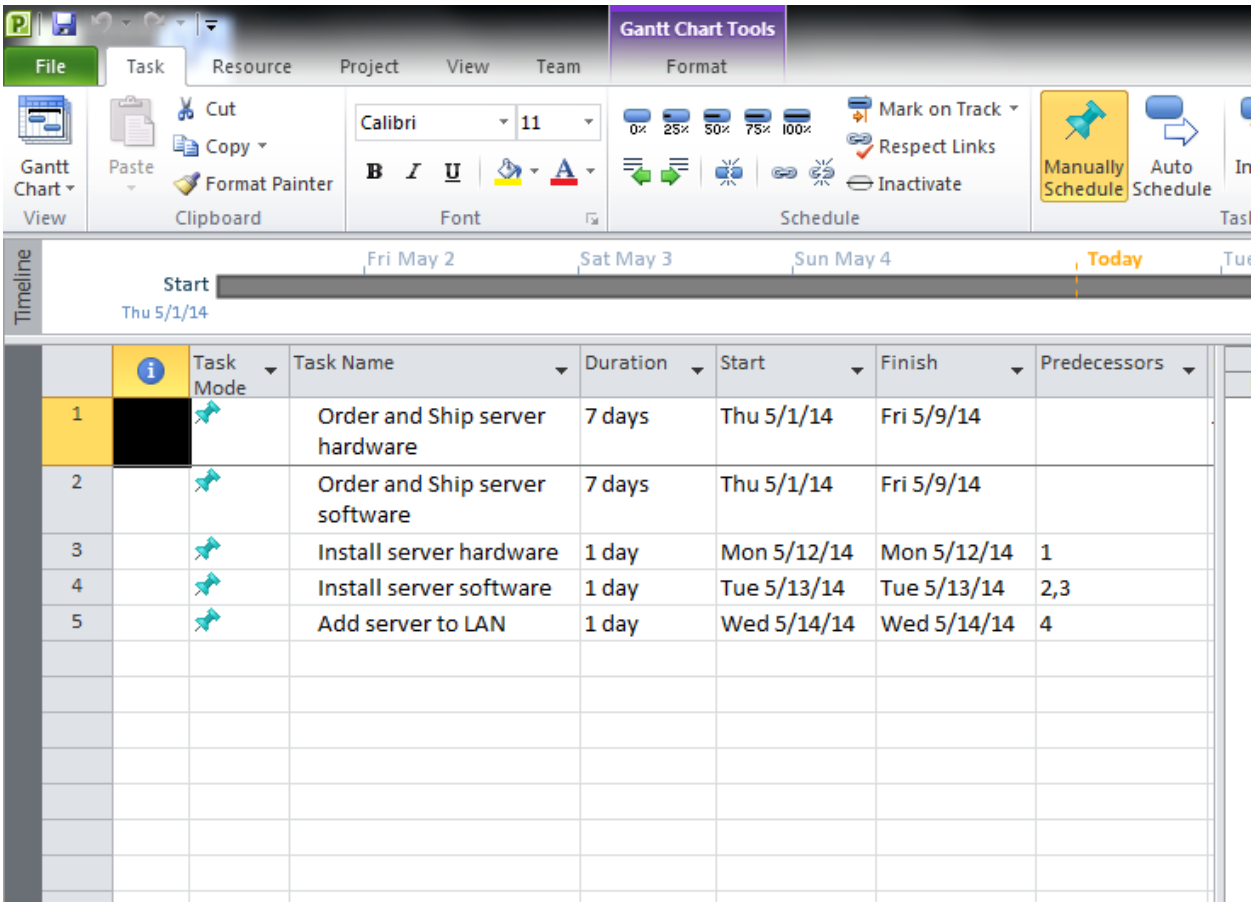
Log on to Windows 7 – Open Microsoft Project 2010 – On the left side of the windows, look for the Task Name column –



On the right side of the window, a chart appears after tasks have been entered, marking the tasks on the calendar with boxes and showing precedence information.



Enter the information contained in the book into the columns.



	Task Mode	Task Name	Duration	Start	Finish	Predecessors
1		Order and Ship server hardware	7 days	Thu 5/1/14	Fri 5/9/14	
2		Order and Ship server software	7 days	Thu 5/1/14	Fri 5/9/14	
3		Install server hardware	1 day	Mon 5/12/14	Mon 5/12/14	1
4		Install server software	1 day	Tue 5/13/14	Tue 5/13/14	2,3
5		Add server to LAN	1 day	Wed 5/14/14	Wed 5/14/14	4

Lab 15.2 Planning an Upgrade

How to Upgrade the Network Interface Card (NIC) Driver

The software that controls the network hardware — specifically, the network interface card (NIC) — is a driver. Rarely do you need to update this software. In fact, a routine or security update is included with the standard Windows Update. But you can upgrade a NIC driver manually if you must.

To specifically update a NIC driver, follow these steps:

1.Set a system restore point.

2.Open the PC's NIC Properties dialog box.

3.In the NIC Properties dialog box, click the Driver tab.

4.Click the Update Driver button.

5.Follow the directions onscreen to search the Internet, or use the Windows Update service to find the best or most current driver.

6.In Windows XP, choose to install the software automatically.

What happens next depends on whether you need a new driver.

If the driver is up-to-date, you see a message explaining as much. Otherwise, a newer driver is downloaded from the Internet and installed on your PC.

7.Close the NIC Properties dialog box as well as any other open windows when you're done.

You might have to restart your computer; do so, if prompted.

•When the new driver doesn't fix the problem, replace the NIC.

•If problems occur, restore the system: Restart the computer. Also, if you can, run System Restore and choose the most recent restore point.

•Updating the NIC driver may solve some problems. But mostly, when you have NIC problems, you should do a hardware analysis

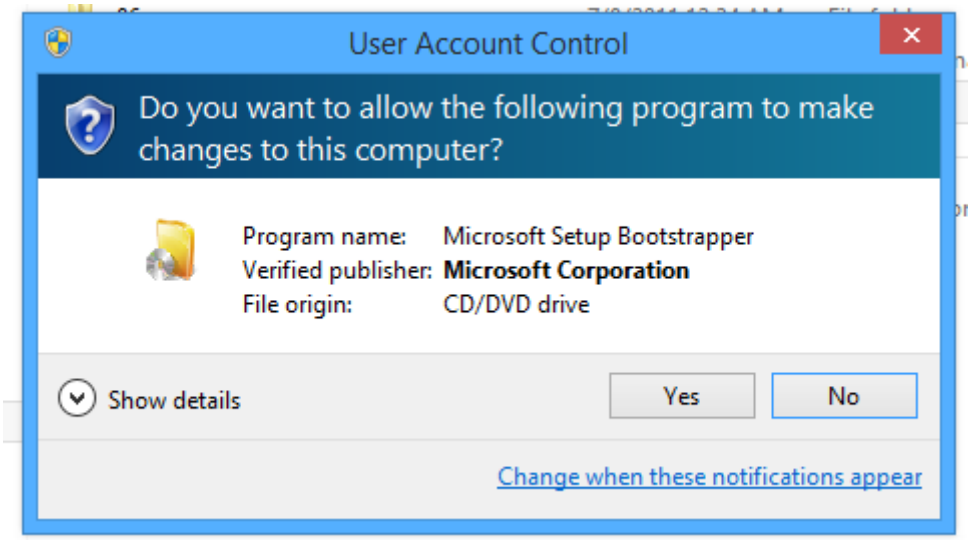
How to Install NIC Card

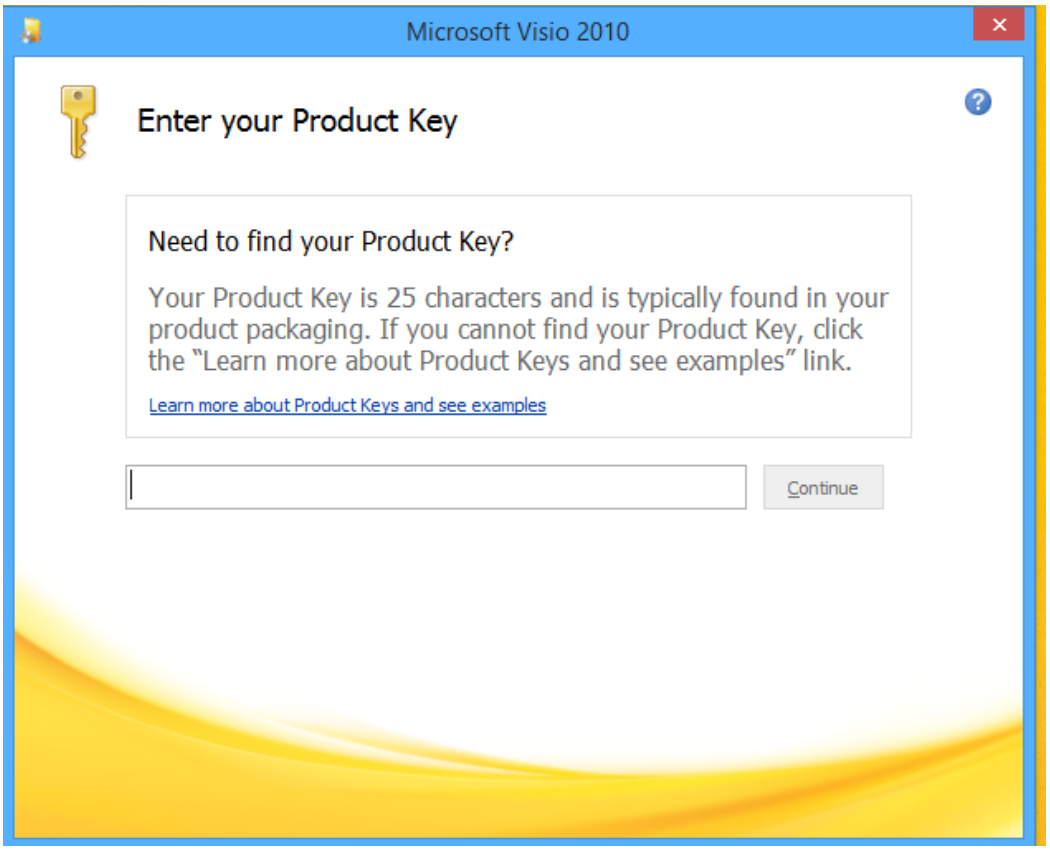
1. Open the PC case. The power should be off when you do this.

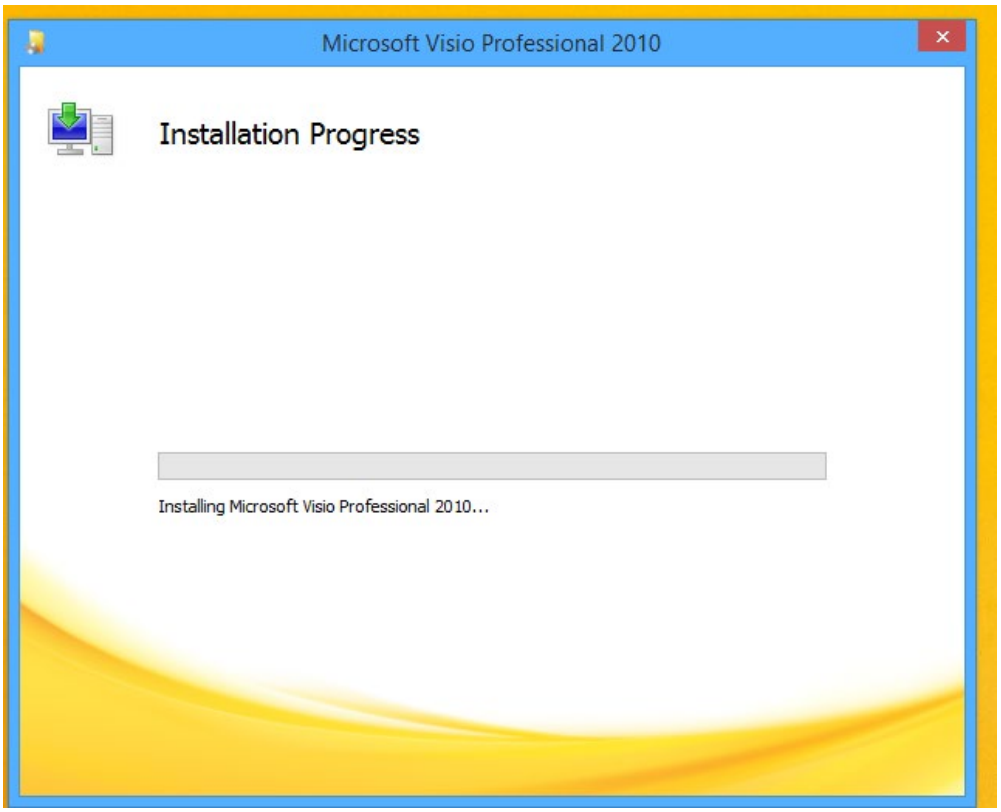
2. Ensure that you have an antistatic wrist strap attached to your wrist and grounded to the PC when working with it.
3. Ensure that you have an antistatic wrist strap attached to your wrist and grounded to the PC when working with it.
4. Now take the NIC card and install it into one of the PCI slots by aligning the guide notches with the PCI slot.
5. Press straight down with gentle pressure until the card snugly fits into the PCI slot.
6. Secure the card with a single screw used to attach the card to the PC.
7. Check the card whether it moves from its position. If it does, it could damage itself when the PC is turned on.
8. Close the PC case and turn on the power.

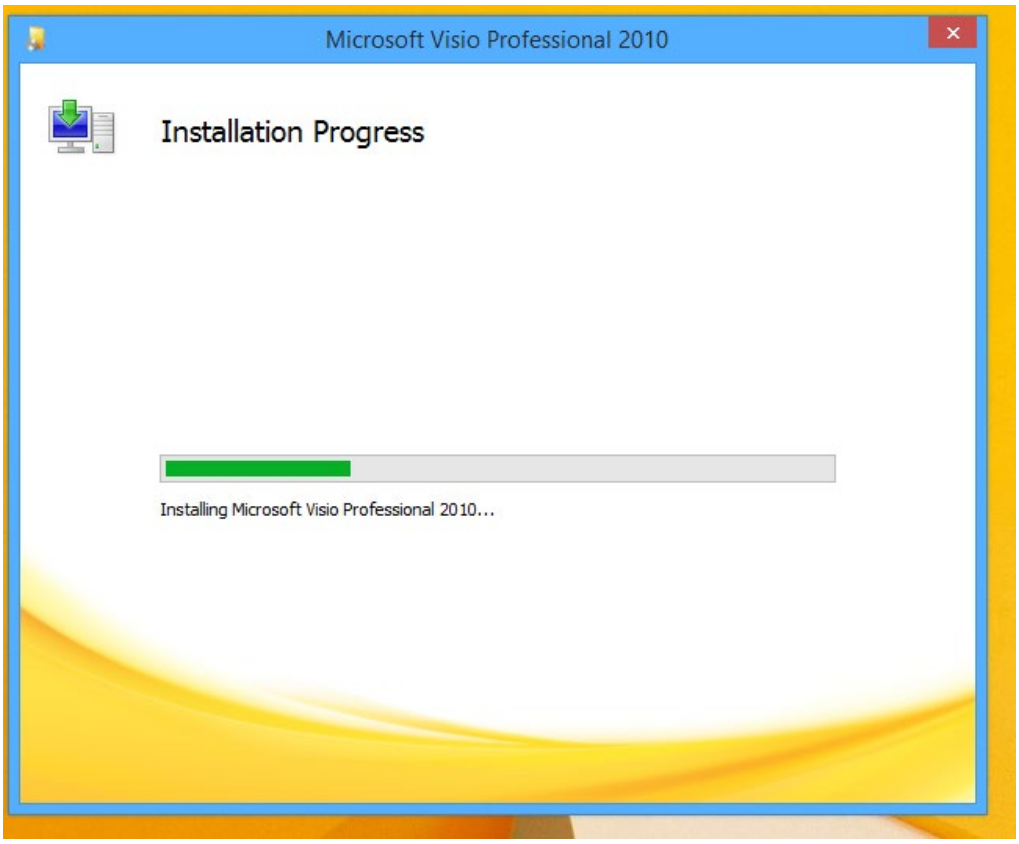
Lab 15.3 Observing a Network Upgrade

Installing Microsoft Visio 2010 and Project Pro 2013

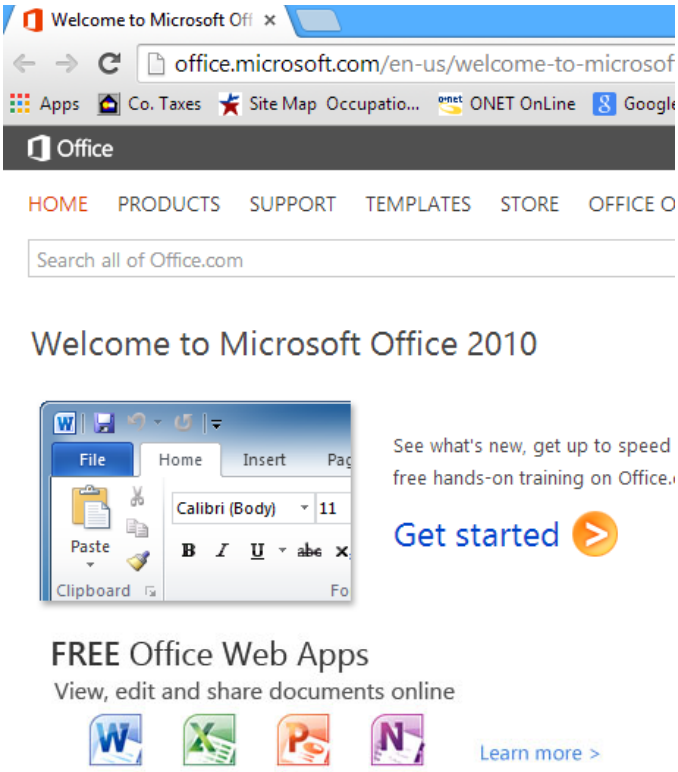


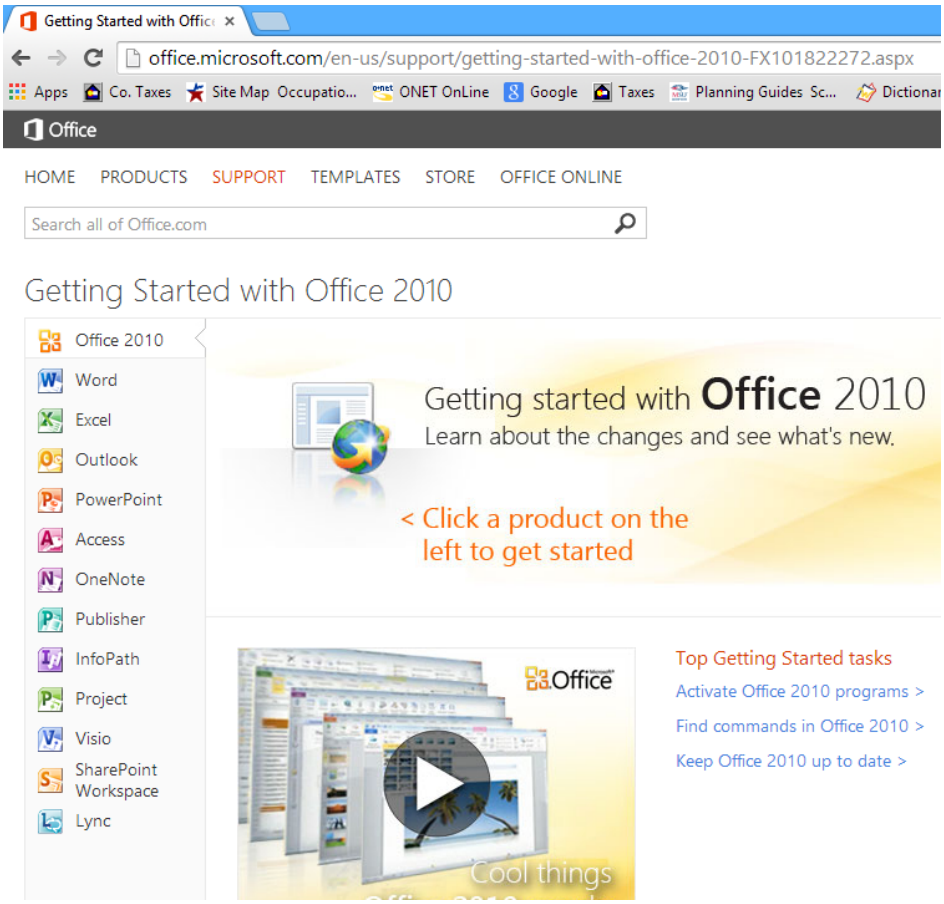

Microsoft Visio 2010
Enter your Product Key
Need to find your Product Key?
Your Product Key is 25 characters and is typically found in your product packaging. If you cannot find your Product Key, click the "Learn more about Product Keys and see examples" link.
Learn more about Product Keys and see examples
Continue

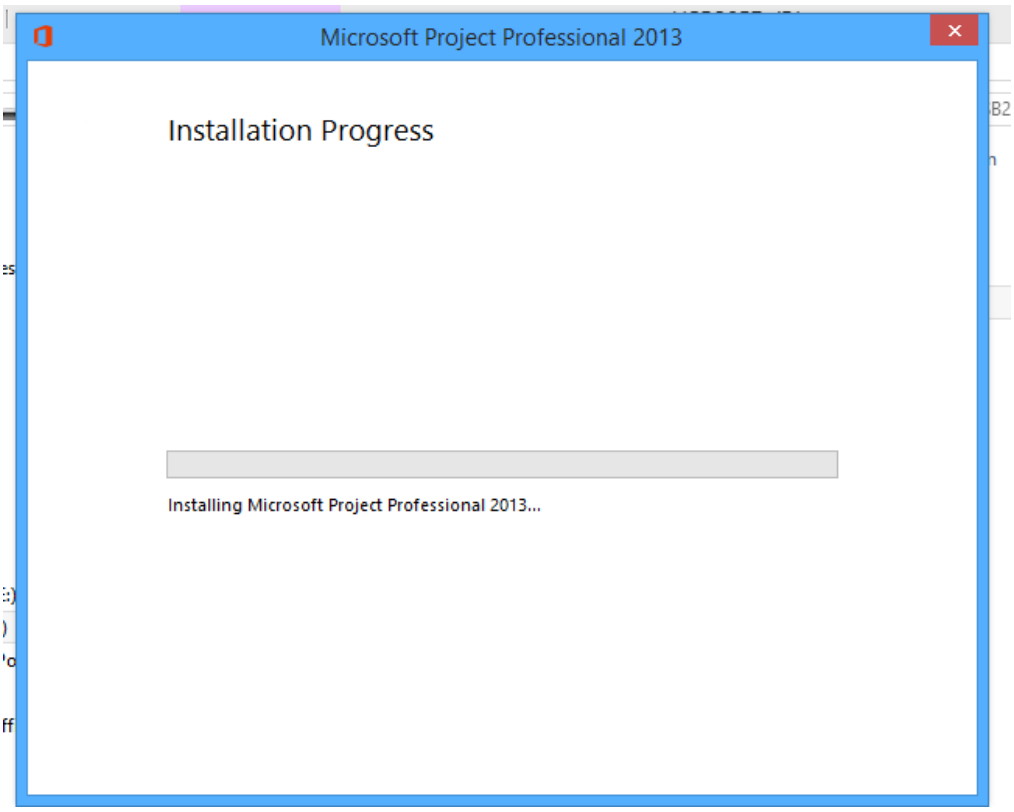

Microsoft Visio Professional 2010
Installation Progress
Installing Microsoft Visio Professional 2010...

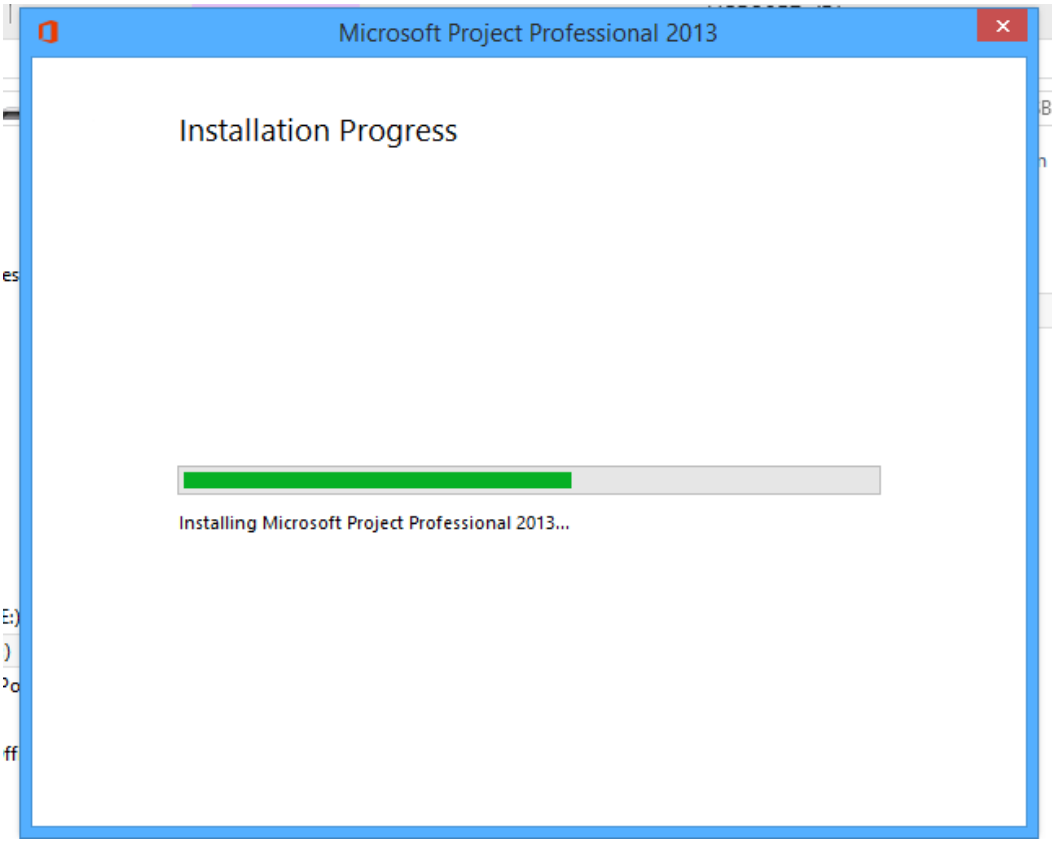

Microsoft Visio Professional 2010
Installation Progress
Installing Microsoft Visio Professional 2010...

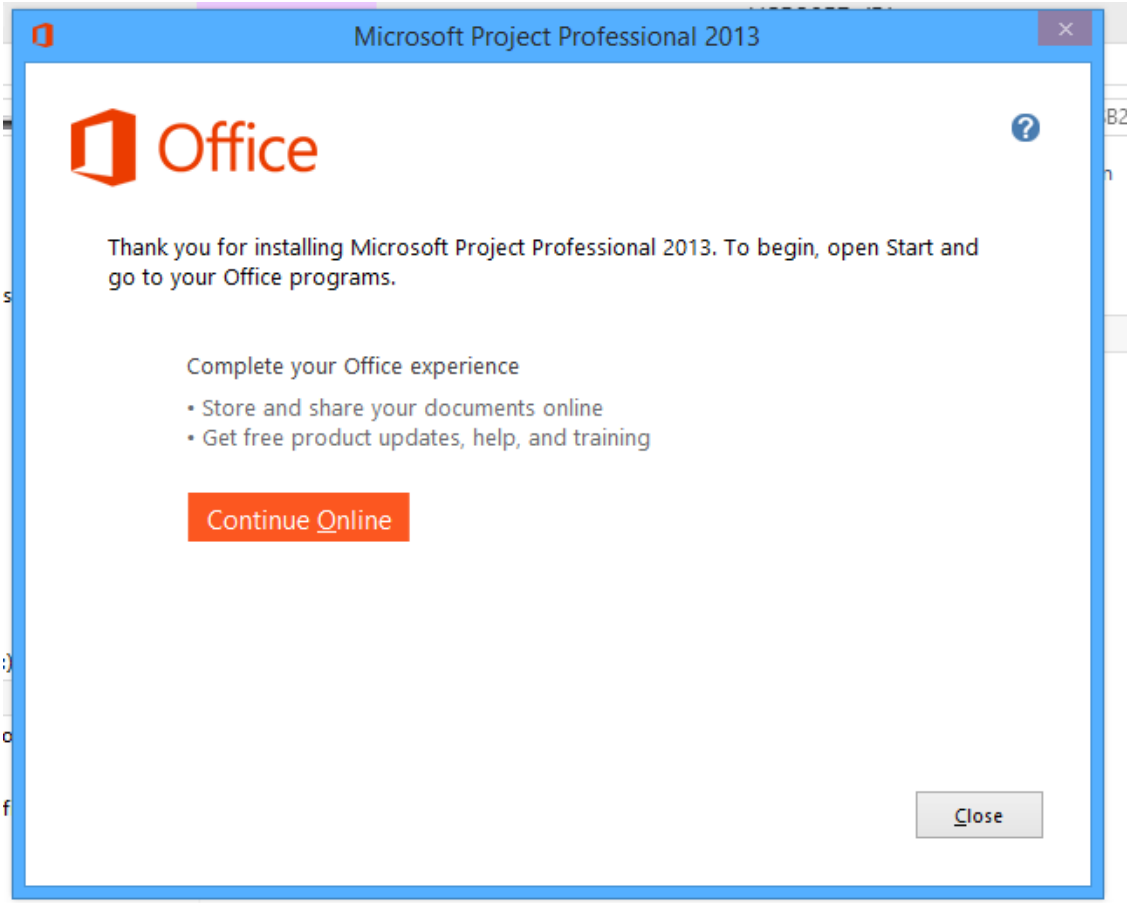

Microsoft Visio Professional 2010
Office
Some updates were not installed. To ensure your version of Microsoft Visio Professional 2010 is up to date, visit the Microsoft Update Web site.
Complete your Office experience
• Store and share your documents online
• Get free product updates, help, and training
Continue Online
Close

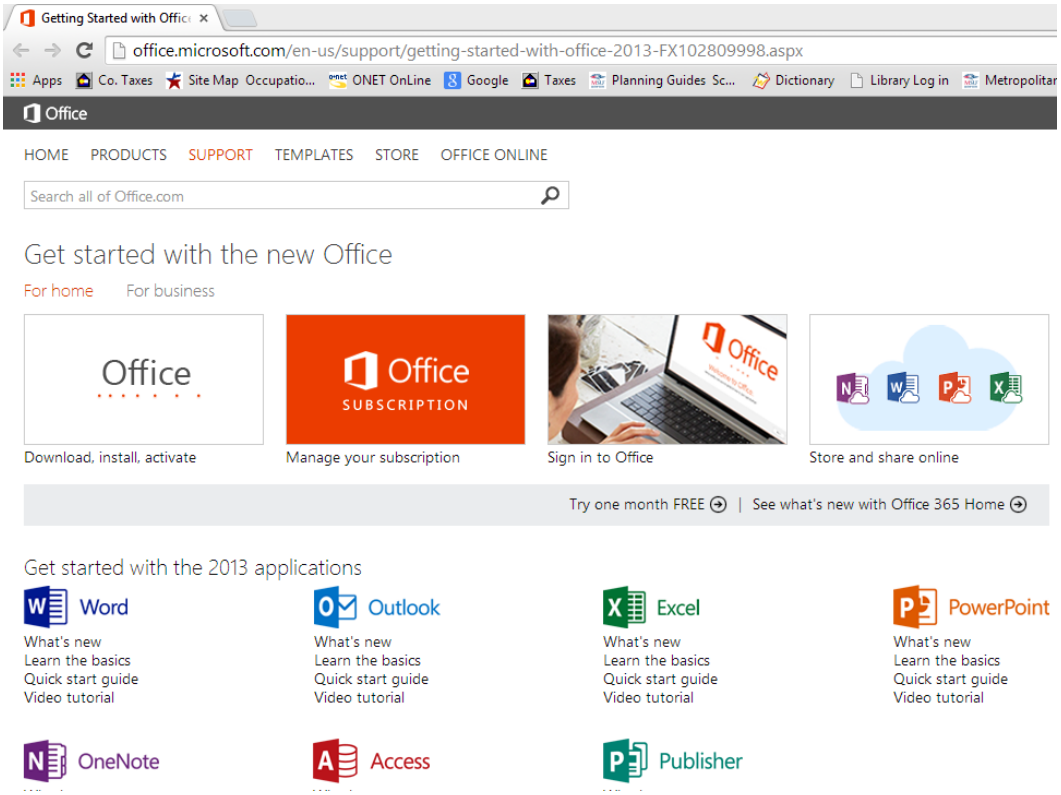

Welcome to Microsoft Off
office.microsoft.com/en-us/welcome-to-microsof
Apps
Co. Taxes
Site Map Occupatio...
ONET OnLine
Google
Office
HOME
PRODUCTS
SUPPORT
TEMPLATES
STORE
OFFICE O
Search all of Office.com
Welcome to Microsoft Office 2010
File
Home
Insert
Calibri (Body)
11
Paste
Clipboard
See what's new, get up to speed
free hands-on training on Office.
Get started
FREE Office Web Apps
View, edit and share documents online
Learn more >


Getting Started with Offic
office.microsoft.com/en-us/support/getting-started-with-office-2010-FX101822272.aspx
Apps
Co. Taxes
Site Map Occupatio...
ONET OnLine
Google
Taxes
Planning Guides Sc...
Office
HOME
PRODUCTS
SUPPORT
TEMPLATES
STORE
OFFICE ONLINE
Search all of Office.com
Getting Started with Office 2010
Office 2010
Word
Excel
Outlook
PowerPoint
Access
OneNote
Publisher
InfoPath
Project
Visio
SharePoint Workspace
Lync
Getting started with Office 2010
Learn about the changes and see what's new.
< Click a product on the left to get started
Office
Cool things
Top Getting Started tasks
Activate Office 2010 programs >
Find commands in Office 2010 >
Keep Office 2010 up to date >


Microsoft Project Professional 2013
Installation Progress
Installing Microsoft Project Professional 2013...

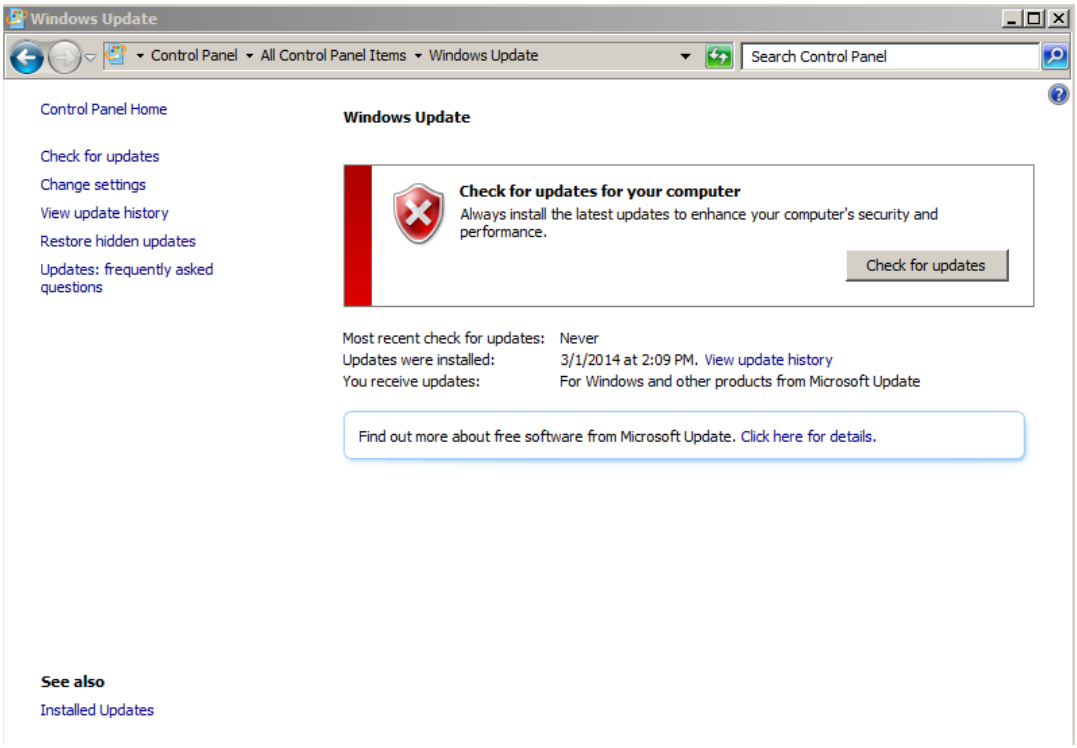

Microsoft Project Professional 2013
Installation Progress
Installing Microsoft Project Professional 2013...

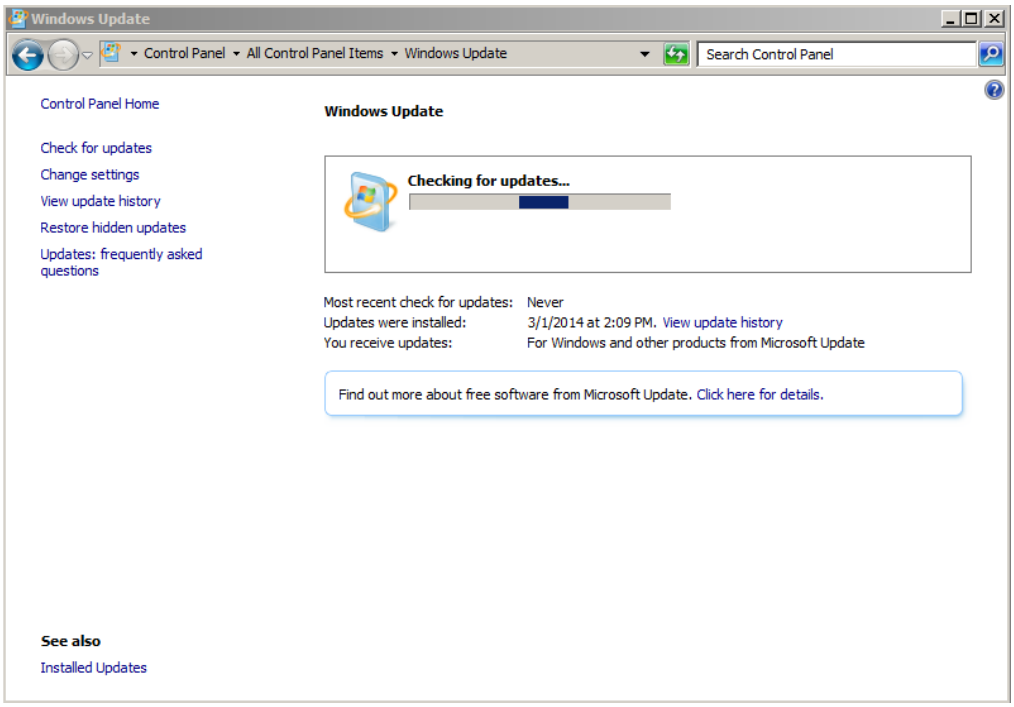

Microsoft Project Professional 2013
Office
Thank you for installing Microsoft Project Professional 2013. To begin, open Start and go to your Office programs.
Complete your Office experience
• Store and share your documents online
• Get free product updates, help, and training
Continue Online
Close

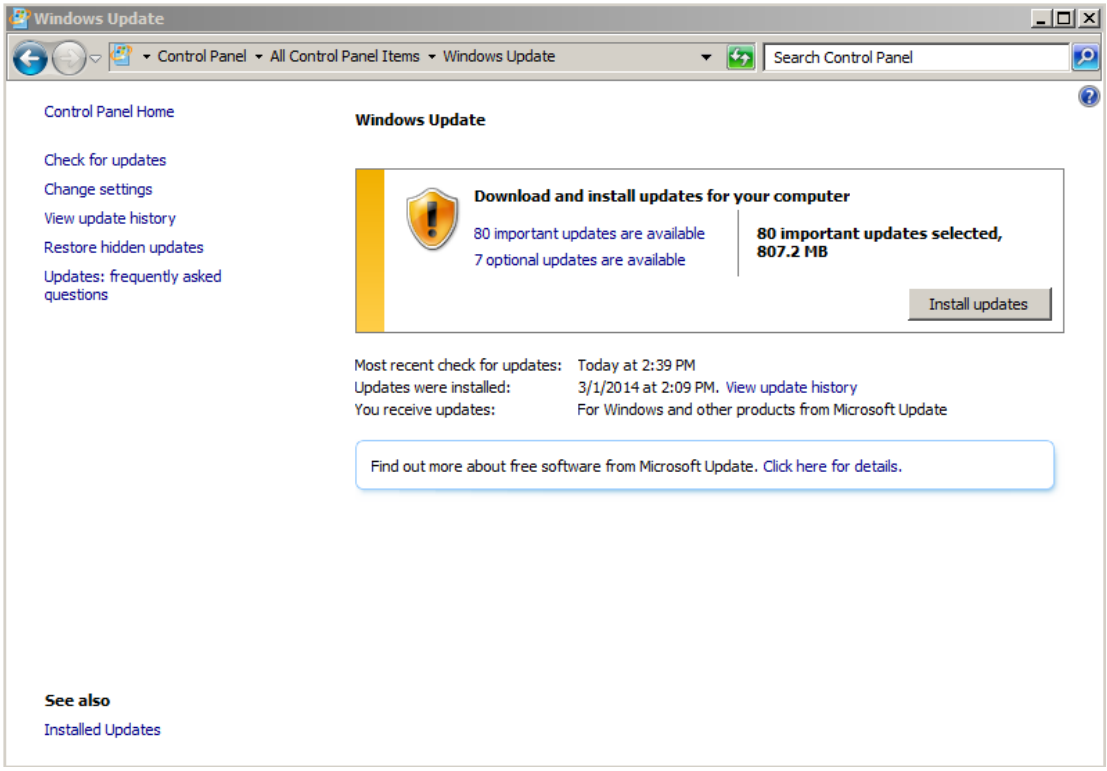

Getting Started with Offic
office.microsoft.com/en-us/support/getting-started-with-office-2013-FX102809998.aspx
Office
HOME PRODUCTS SUPPORT TEMPLATES STORE OFFICE ONLINE
Search all of Office.com
Get started with the new Office
For home For business
Office
Download, install, activate
Office SUBSCRIPTION
Manage your subscription
Sign in to Office
Store and share online
Try one month FREE | See what's new with Office 365 Home
Get started with the 2013 applications
Word
What's new
Learn the basics
Quick start guide
Video tutorial
Outlook
What's new
Learn the basics
Quick start guide
Video tutorial
Excel
What's new
Learn the basics
Quick start guide
Video tutorial
PowerPoint
What's new
Learn the basics
Quick start guide
Video tutorial
OneNote
Access
Publisher

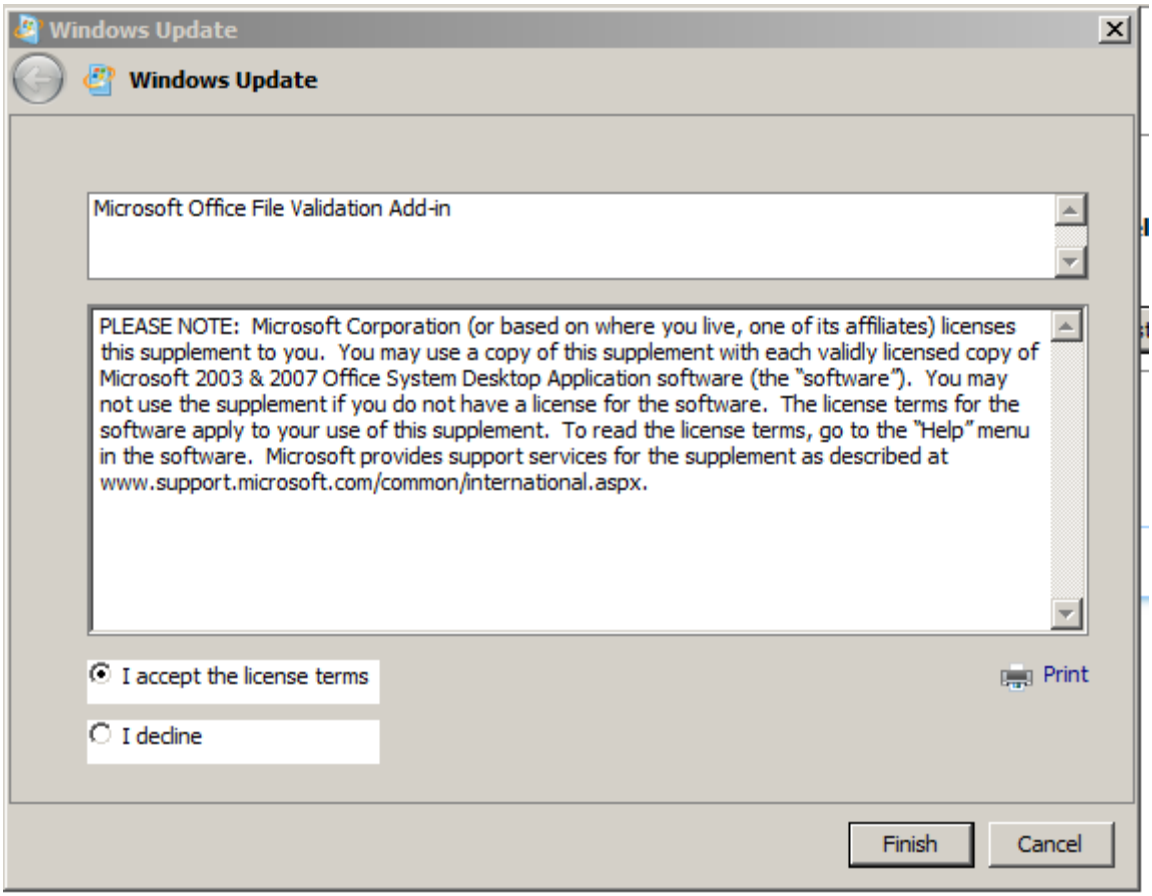
Lab 15.4 Installing and Removing Updates on Windows Server 2008

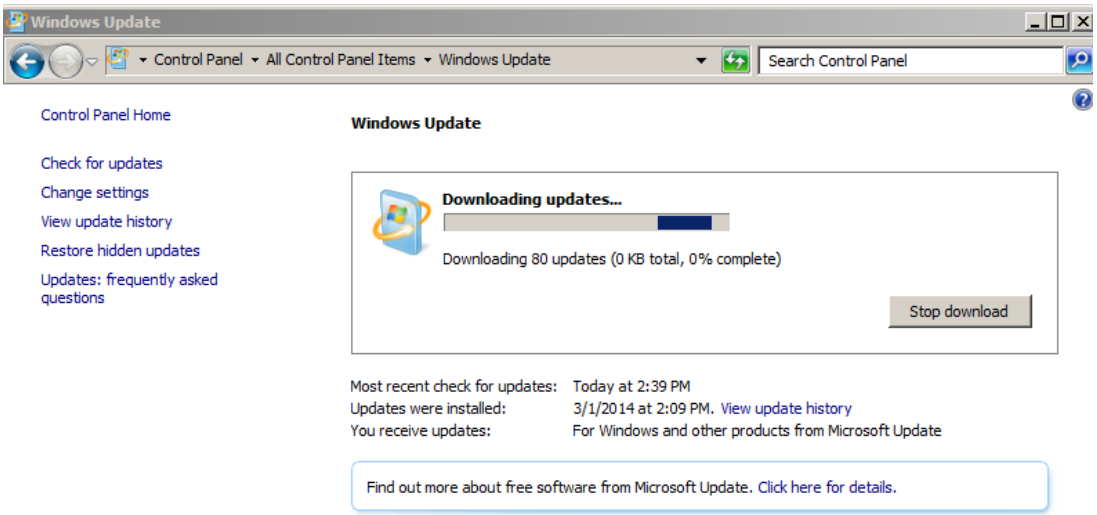
Start – Control Panel – double click Windows Update

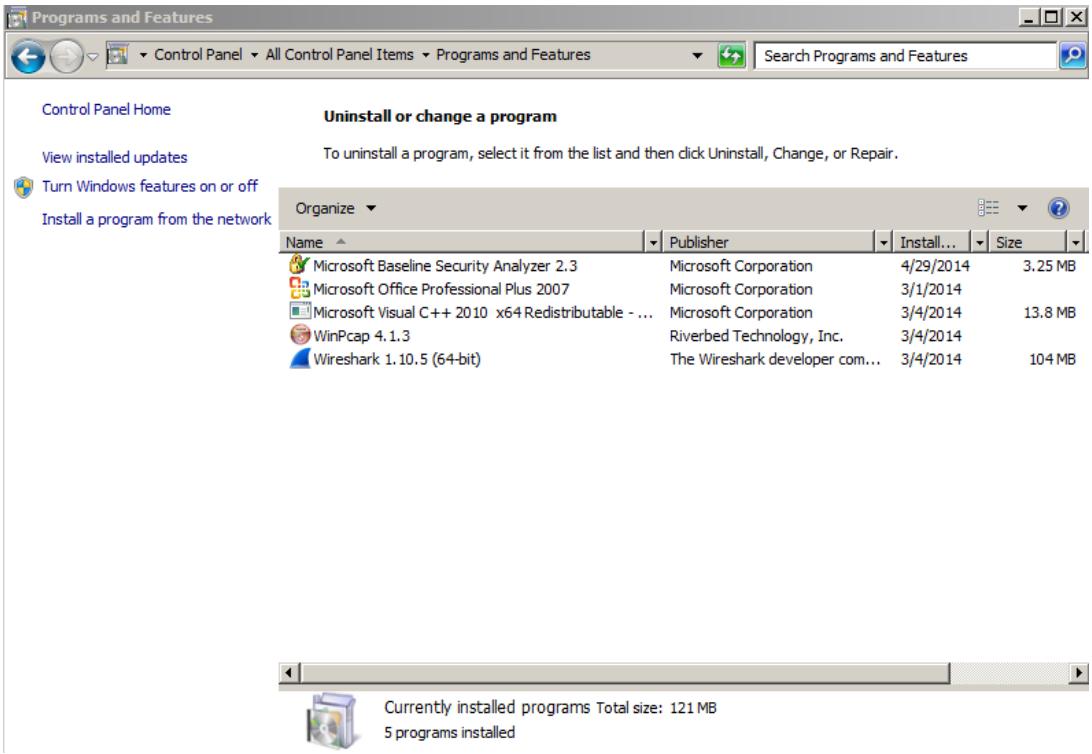





Windows Update
Control Panel ▸ All Control Panel Items ▸ Windows Update
Search Control Panel
Control Panel Home
Check for updates
Change settings
View update history
Restore hidden updates
Updates: frequently asked questions
Windows Update
Download and install updates for your computer
80 important updates are available
7 optional updates are available
80 important updates selected, 807.2 MB
Install updates
Most recent check for updates: Today at 2:39 PM
Updates were installed: 3/1/2014 at 2:09 PM. View update history
You receive updates: For Windows and other products from Microsoft Update
Find out more about free software from Microsoft Update. Click here for details.
See also
Installed Updates


Windows Update
Windows Update
Microsoft Office File Validation Add-in
PLEASE NOTE: Microsoft Corporation (or based on where you live, one of its affiliates) licenses this supplement to you. You may use a copy of this supplement with each validly licensed copy of Microsoft 2003 & 2007 Office System Desktop Application software (the "software"). You may not use the supplement if you do not have a license for the software. The license terms for the software apply to your use of this supplement. To read the license terms, go to the "Help" menu in the software. Microsoft provides support services for the supplement as described at www.support.microsoft.com/common/international.aspx.
I accept the license terms
I decline
Print
Finish
Cancel


Windows Update
Control Panel ▸ All Control Panel Items ▸ Windows Update
Search Control Panel
Control Panel Home
Check for updates
Change settings
View update history
Restore hidden updates
Updates: frequently asked questions
Windows Update
Downloading updates...
Downloading 80 updates (0 KB total, 0% complete)
Stop download
Most recent check for updates: Today at 2:39 PM
Updates were installed: 3/1/2014 at 2:09 PM. View update history
You receive updates: For Windows and other products from Microsoft Update
Find out more about free software from Microsoft Update. Click here for details.
See also
Installed Updates


Programs and Features
Control Panel ▸ All Control Panel Items ▸ Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Install a program from the network
Uninstall or change a program
To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.
Organize
Name
Publisher
Install...
Size
Microsoft Baseline Security Analyzer 2.3 Microsoft Corporation 4/29/2014 3.25 MB
Microsoft Office Professional Plus 2007 Microsoft Corporation 3/1/2014
Microsoft Visual C++ 2010 x64 Redistributable - ... Microsoft Corporation 3/4/2014 13.8 MB
WinPcap 4.1.3 Riverbed Technology, Inc. 3/4/2014
Wireshark 1.10.5 (64-bit) The Wireshark developer com... 3/4/2014 104 MB
Currently installed programs Total size: 121 MB
5 programs installed

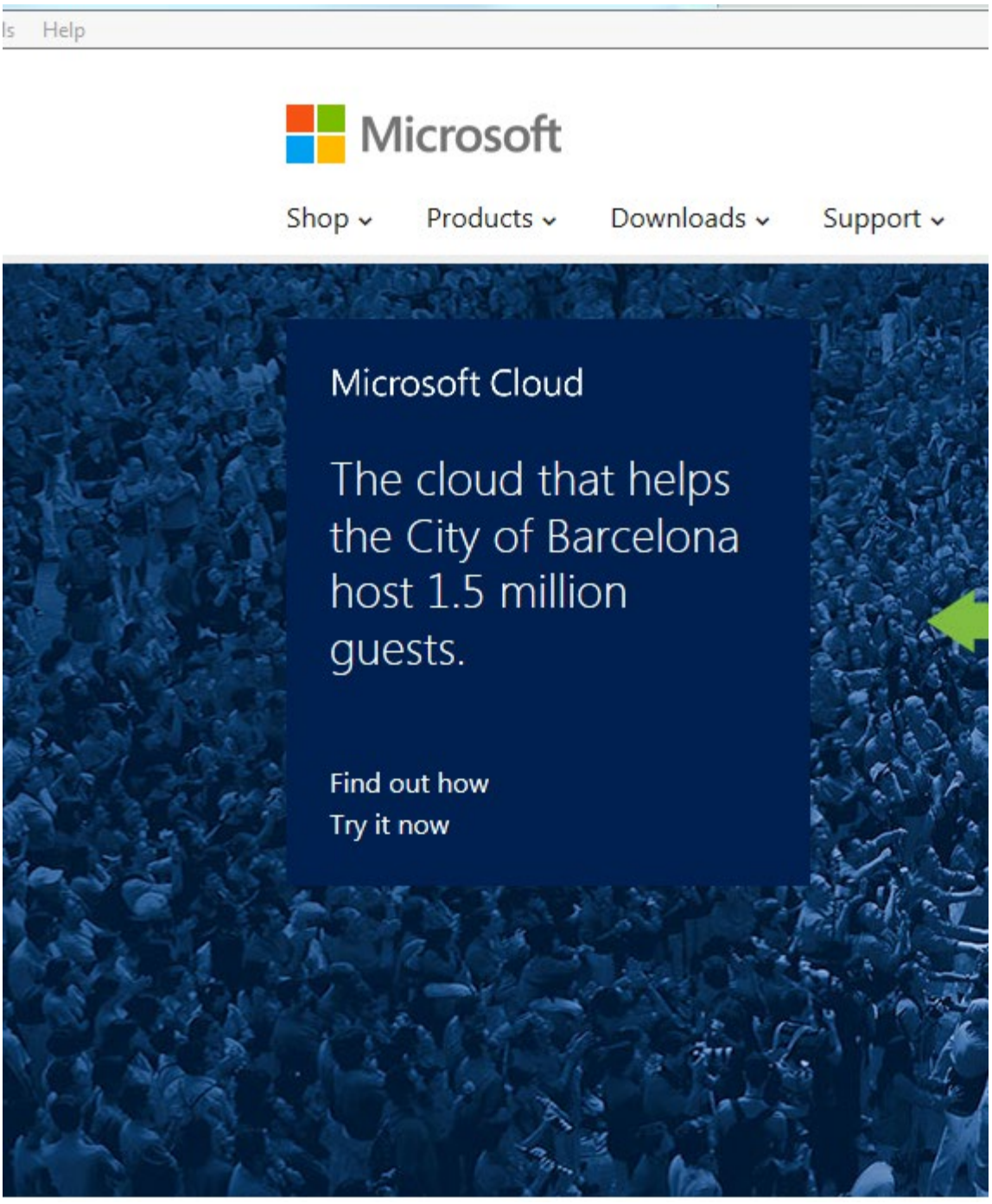
Uninstall an update

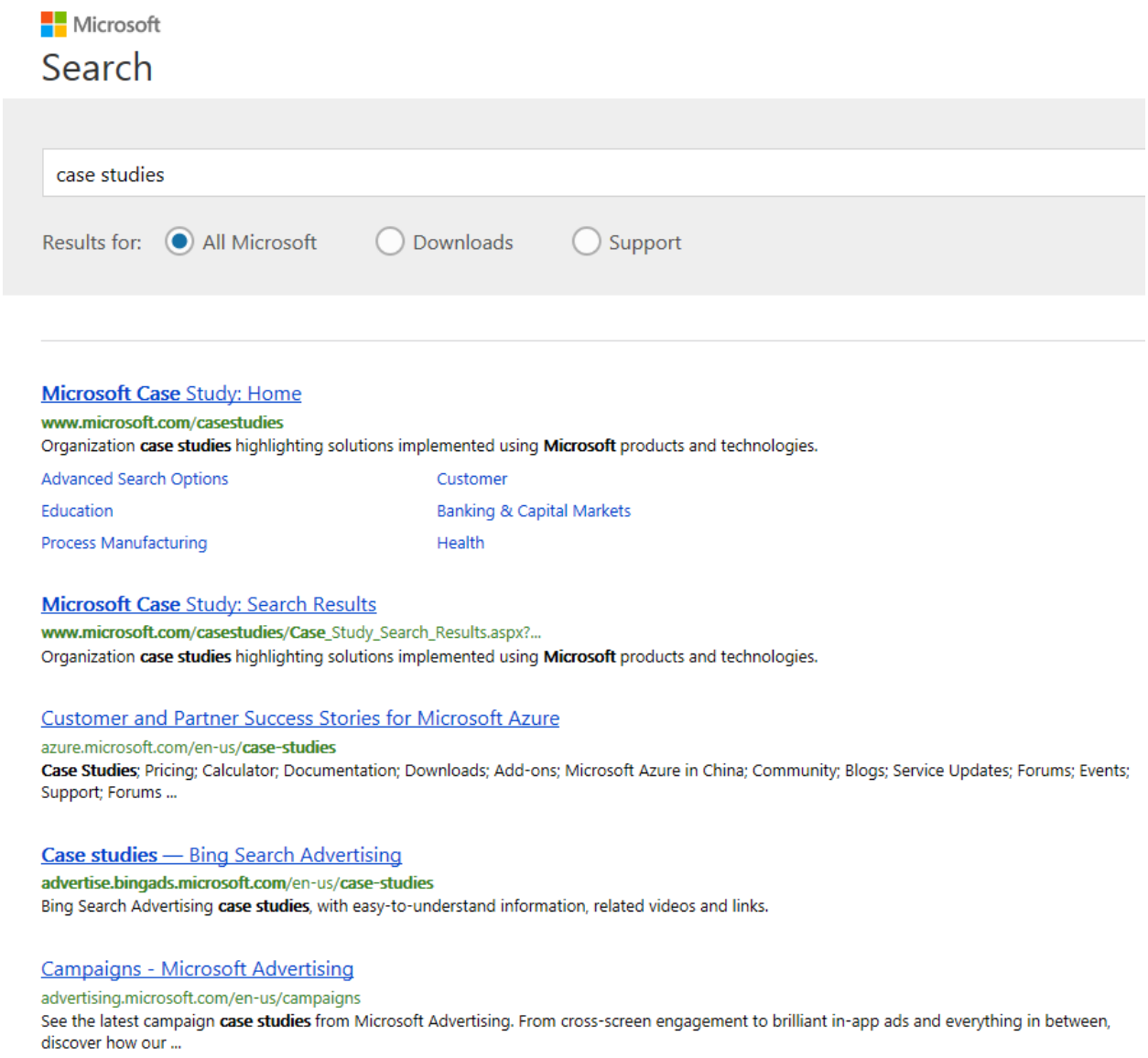
To uninstall an update, select it from the list and then click Uninstall or Change.

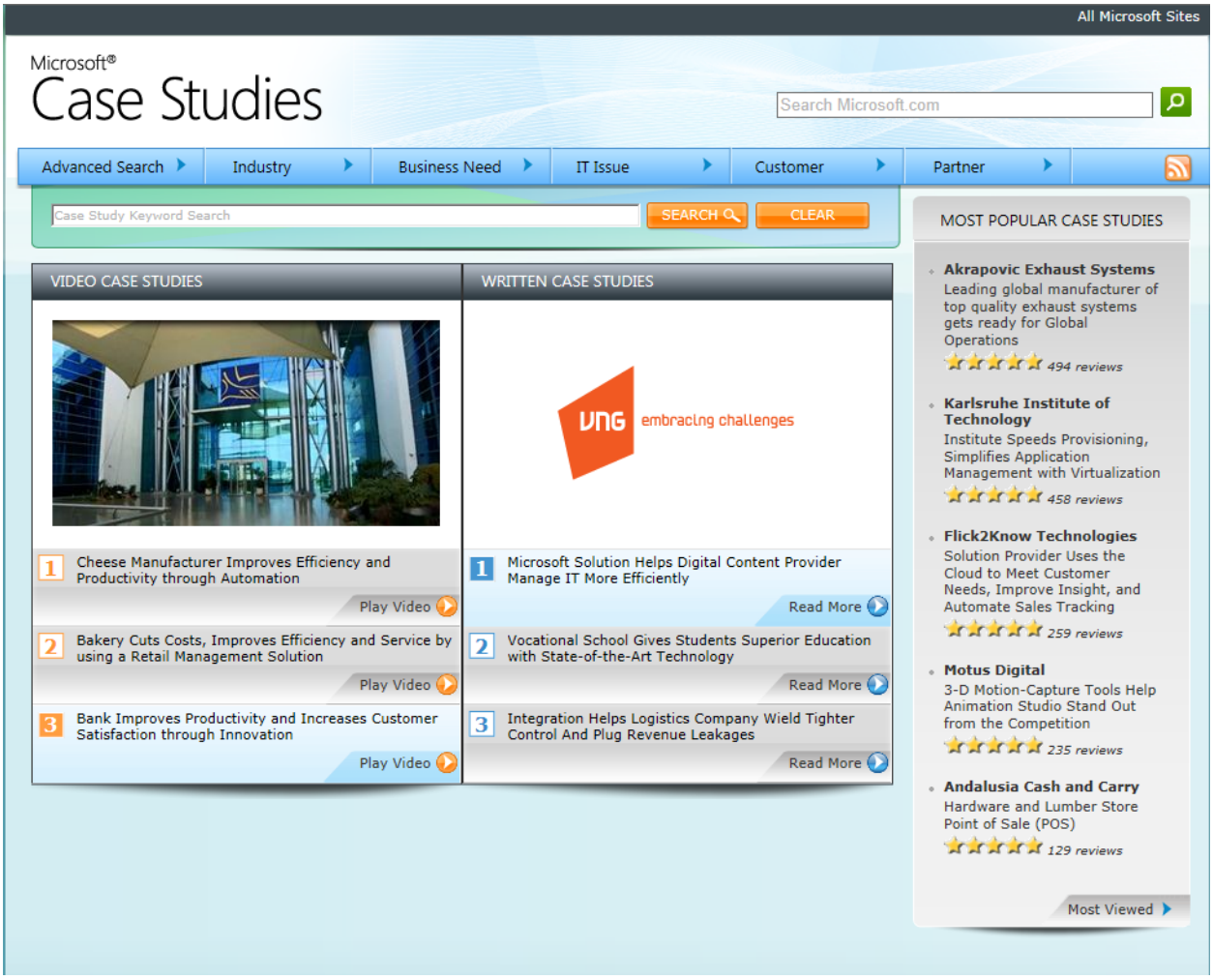
Organize

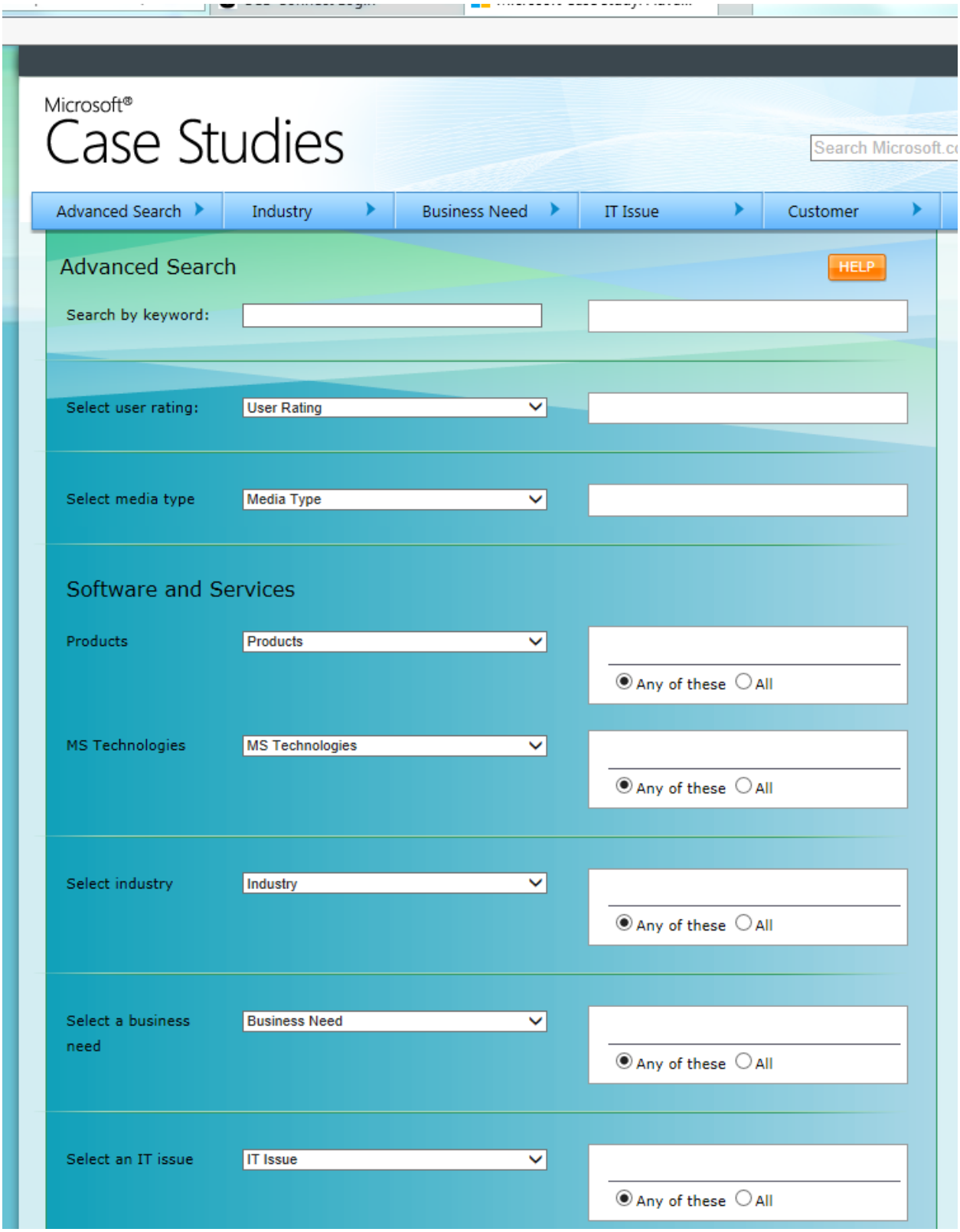
Name	Program	Version	Publisher	I...
Microsoft Office Professional Plus 2007 (1)				
2007 Microsoft Office Suite Service Pack 2 (SP2)	Microsoft Office P...		Microsoft	3/1/2014
Microsoft Windows (134)				
Streaming Media Services update (KB963697)	Microsoft Windows		Microsoft Corporation	3/14/2014
Update for Microsoft Windows (KB2670838)	Microsoft Windows		Microsoft Corporation	3/1/2014
Windows Internet Explorer 10	Microsoft Windows		Microsoft Corporation	3/1/2014
Microsoft Windows English Spelling Package	Microsoft Windows			3/1/2014
Microsoft Windows English Hyphenation Package	Microsoft Windows			3/1/2014
Update for Microsoft Windows (KB2533552)	Microsoft Windows		Microsoft Corporation	3/1/2014
Update for Microsoft Windows (KB2919469)	Microsoft Windows		Microsoft Corporation	3/1/2014
Security Update for Microsoft Windows (KB2916036)	Microsoft Windows		Microsoft Corporation	3/1/2014
Security Update for Microsoft Windows (KB2913602)	Microsoft Windows		Microsoft Corporation	3/1/2014
Update for Microsoft Windows (KB2913431)	Microsoft Windows		Microsoft Corporation	3/1/2014
Security Update for Microsoft Windows (KB2911501)	Microsoft Windows		Microsoft Corporation	3/1/2014
Security Update for Microsoft Windows (KB2909921)	Microsoft Windows		Microsoft Corporation	3/1/2014
Security Update for Microsoft Windows (KB2909210)	Microsoft Windows		Microsoft Corporation	3/1/2014
Update for Microsoft Windows (KB2904266)	Microsoft Windows		Microsoft Corporation	3/1/2014
Security Update for Microsoft Windows (KB2901112)	Microsoft Windows		Microsoft Corporation	3/1/2014
Security Update for Microsoft Windows (KB2900986)	Microsoft Windows		Microsoft Corporation	3/1/2014
Security Update for Microsoft Windows (KB2898857)	Microsoft Windows		Microsoft Corporation	3/1/2014
Update for Microsoft Windows (KB2893519)	Microsoft Windows		Microsoft Corporation	3/1/2014
Security Update for Microsoft Windows (KB2893294)	Microsoft Windows		Microsoft Corporation	3/1/2014
Security Update for Microsoft Windows (KB2892074)	Microsoft Windows		Microsoft Corporation	3/1/2014
Update for Microsoft Windows (KB2891804)	Microsoft Windows		Microsoft Corporation	3/1/2014

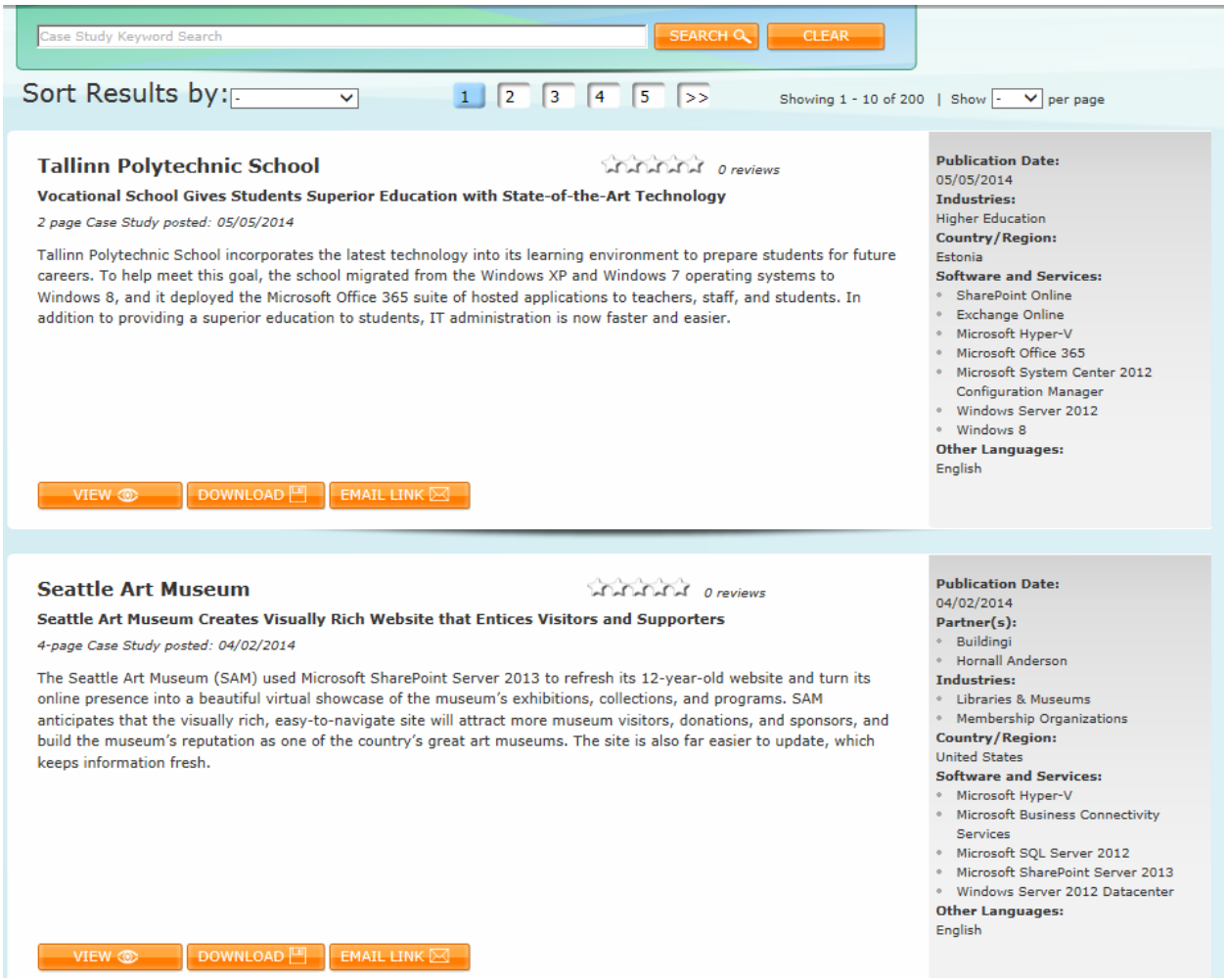
Lab. 15.5 Researching Network Solutions


ls Help
Microsoft
Shop
Products
Downloads
Support
Microsoft Cloud
The cloud that helps the City of Barcelona host 1.5 million guests.
Find out how
Try it now


Microsoft
Search
case studies
Results for:
All Microsoft
Downloads
Support
Microsoft Case Study: Home
www.microsoft.com/casestudies
Organization case studies highlighting solutions implemented using Microsoft products and technologies.
Advanced Search Options
Customer
Education
Banking & Capital Markets
Process Manufacturing
Health
Microsoft Case Study: Search Results
www.microsoft.com/casestudies/Case_Study_Search_Results.aspx?...
Organization case studies highlighting solutions implemented using Microsoft products and technologies.
Customer and Partner Success Stories for Microsoft Azure
azure.microsoft.com/en-us/case-studies
Case Studies; Pricing; Calculator; Documentation; Downloads; Add-ons; Microsoft Azure in China; Community; Blogs; Service Updates; Forums; Events; Support; Forums ...
Case studies — Bing Search Advertising
advertise.bingads.microsoft.com/en-us/case-studies
Bing Search Advertising case studies, with easy-to-understand information, related videos and links.
Campaigns - Microsoft Advertising
advertising.microsoft.com/en-us/campaigns
See the latest campaign case studies from Microsoft Advertising. From cross-screen engagement to brilliant in-app ads and everything in between, discover how our ...


All Microsoft Sites
Microsoft®
Case Studies
Search Microsoft.com
Advanced Search
Industry
Business Need
IT Issue
Customer
Partner
Case Study Keyword Search
SEARCH
CLEAR
VIDEO CASE STUDIES
WRITTEN CASE STUDIES
1 Cheese Manufacturer Improves Efficiency and Productivity through Automation
Play Video
2 Bakery Cuts Costs, Improves Efficiency and Service by using a Retail Management Solution
Play Video
3 Bank Improves Productivity and Increases Customer Satisfaction through Innovation
Play Video
VNG embracing challenges
1 Microsoft Solution Helps Digital Content Provider Manage IT More Efficiently
Read More
2 Vocational School Gives Students Superior Education with State-of-the-Art Technology
Read More
3 Integration Helps Logistics Company Wield Tighter Control And Plug Revenue Leakages
Read More
MOST POPULAR CASE STUDIES
Akrapovic Exhaust Systems
Leading global manufacturer of top quality exhaust systems gets ready for Global Operations
494 reviews
Karlsruhe Institute of Technology
Institute Speeds Provisioning, Simplifies Application Management with Virtualization
458 reviews
Flick2Know Technologies
Solution Provider Uses the Cloud to Meet Customer Needs, Improve Insight, and Automate Sales Tracking
259 reviews
Motus Digital
3-D Motion-Capture Tools Help Animation Studio Stand Out from the Competition
235 reviews
Andalusia Cash and Carry
Hardware and Lumber Store Point of Sale (POS)
129 reviews
Most Viewed


Microsoft®
Case Studies
Search Microsoft.c
Advanced Search
Industry
Business Need
IT Issue
Customer
Advanced Search
HELP
Search by keyword:
Select user rating:
User Rating
Select media type
Media Type
Software and Services
Products
Products
Any of these
All
MS Technologies
MS Technologies
Any of these
All
Select industry
Industry
Any of these
All
Select a business need
Business Need
Any of these
All
Select an IT issue
IT Issue
Any of these
All


Case Study Keyword Search
SEARCH
CLEAR
Sort Results by:
1 2 3 4 5 >>
Showing 1 - 10 of 200 | Show per page
Tallinn Polytechnic School
0 reviews
Vocational School Gives Students Superior Education with State-of-the-Art Technology
2 page Case Study posted: 05/05/2014
Tallinn Polytechnic School incorporates the latest technology into its learning environment to prepare students for future careers. To help meet this goal, the school migrated from the Windows XP and Windows 7 operating systems to Windows 8, and it deployed the Microsoft Office 365 suite of hosted applications to teachers, staff, and students. In addition to providing a superior education to students, IT administration is now faster and easier.
VIEW
DOWNLOAD
EMAIL LINK
Publication Date:
05/05/2014
Industries:
Higher Education
Country/Region:
Estonia
Software and Services:
SharePoint Online
Exchange Online
Microsoft Hyper-V
Microsoft Office 365
Microsoft System Center 2012 Configuration Manager
Windows Server 2012
Windows 8
Other Languages:
English
Seattle Art Museum
0 reviews
Seattle Art Museum Creates Visually Rich Website that Entices Visitors and Supporters
4-page Case Study posted: 04/02/2014
The Seattle Art Museum (SAM) used Microsoft SharePoint Server 2013 to refresh its 12-year-old website and turn its online presence into a beautiful virtual showcase of the museum's exhibitions, collections, and programs. SAM anticipates that the visually rich, easy-to-navigate site will attract more museum visitors, donations, and sponsors, and build the museum's reputation as one of the country's great art museums. The site is also far easier to update, which keeps information fresh.
VIEW
DOWNLOAD
EMAIL LINK
Publication Date:
04/02/2014
Partner(s):
Buildingi
Hornall Anderson
Industries:
Libraries & Museums
Membership Organizations
Country/Region:
United States
Software and Services:
Microsoft Hyper-V
Microsoft Business Connectivity Services
Microsoft SQL Server 2012
Microsoft SharePoint Server 2013
Windows Server 2012 Datacenter
Other Languages:
English