NORTHERN UNIVERSITY
BANGLADESH

An Internship report presented

on

Cisco Certified Network Associate(CCNA)

Supervised by

Mohammed Samsuddoha Alam

Assistant professor

Department of computer science & engineering

Northern University Bangladesh

Submitted by

Sourav Debnath

ID: CSE-04180101181

Department of computer science & engineering

Northern University Bangladesh

Date of submission:18 June,2022

LETTER OF TRANSMITTAL

18/ 06/ 2022

Muhammed Samsuddoha Alam
Assistant Professor
Department of Computer Science and Engineering
Northern University Bangladesh

Subject: Submission of Internship report.

Dear Sir,
I would like to inform you that I have submitted my internship report on "Cisco Certified Network Associate(CCNA) in CSL Training Center with due gratitude and appreciation and as per your instruction. I hope this report will be informative as well as comprehensive.

The internship program has given me the opportunity to learn about different aspect of netwroking. Before facing the Networking job sector I have gathered general idea about this course.

I also want to thank you for your support and patience for me and I appreciate the opportunity provided by you through assigning me to work in this thoughtful project.

I, therefore request and hope that you would be kind enough to me by providing acceptance of this report and oblige thereby.

Yours sincerely,
Sourav Debnath
ID: CSE-04180101181
Program: CSE
Northern University Bangladesh

Approval

The Industrial Training Report on “Cisco Certified Network Associate(CCNA)” submitted by **Sourav Debnath ID:CSE-04180101181** to the Department of Computer Science & Engineering has been accepted as satisfactory for the course **CSE 4389** titled **Field Work(Industrial Training).**

<u>Board of Examiners:</u>

1.Muhammed Samsuddoha Alam (Supervisor)

2.Md. Ruhul Amin (Examiner)

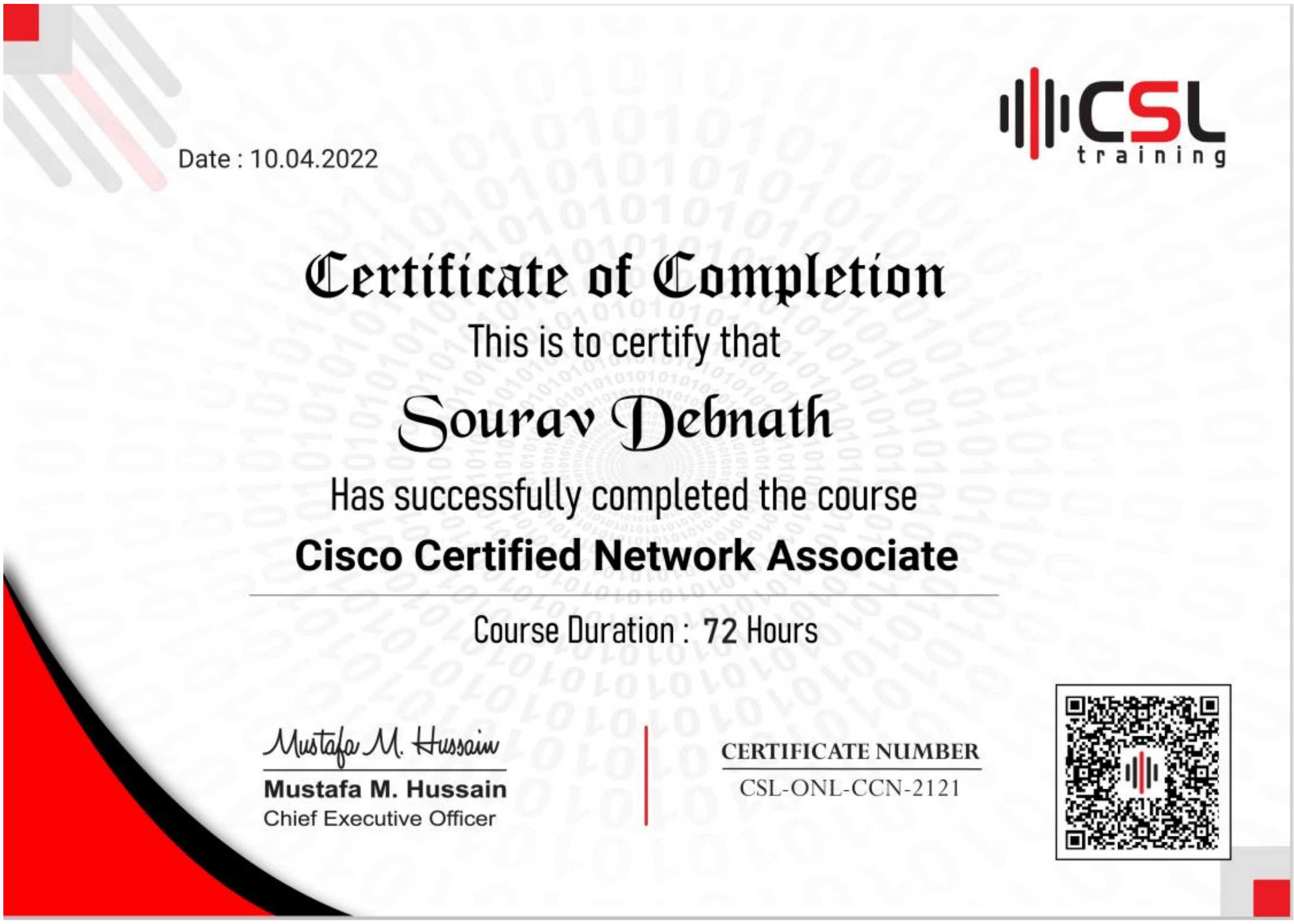
Md. Raihan-Ul-Masood
Associate Professor & Head
Department of Computer Science & Engineering
Northern University Bangladesh

ACKNOWLEDGEMENT

I take this opportunity to express my profound gratitude and deep regards to my guide “Utpal Kumar Ghose” for his exemplary guidance, monitoring and constant encouragement throughout the course of this training. The blessing, help and guidance given by him, time to time shall carry me a long way in the journey of life on which I am about to embark.

I also take this opportunity to express a deep sense of gratitude to Mohammed Samsuddoha Alam Sir & All Faculty Members of Department of Computer Science & Engineering, for their cordial support, valuable information and guidance, which helped me in completing this task through various stages.

I am obliged to staff members of Computer Department, for the valuable information provided by them in their respective fields. I am grateful for their cooperation during the period of my Project. Lastly, I thank almighty, my parents, brother, sisters and friends for their constant encouragement without which this assignment would not be possible.



CSL training

Date : 10.04.2022

Certificate of Completion

This is to certify that

Sourav Debnath

Has successfully completed the course

Cisco Certified Network Associate

Course Duration : 72 Hours

Mustafa M. Hussain

Mustafa M. Hussain
Chief Executive Officer

CERTIFICATE NUMBER
CSL-ONL-CCN-2121

INDEX

1. BASIC NETWORKING

1.1 What is a Network?

A network is any collection of independent computers that communicate with one another over a shared network medium. A computer network is a collection of two or more connected computers. When these computers are joined in a network, people can share files and peripherals such as modems, printers, tape backup drives, or CD-ROM drives. When networks at multiple locations are connected using services available from phone companies, people can send e-mail, share links to the global Internet, or conduct video conferences in real time with other remote users. As companies rely on applications like electronic mail and database management for core business operations, computer networking becomes increasingly more important.

Every network includes:

- At least two computers Server or Client workstation.
- Networking Interface Card's (NIC)
- A connection medium, usually a wire or cable, although wireless communication between networked computers and peripherals is also possible.
- Network Operating system software, such as Microsoft Windows NT or 2000, Novell NetWare, Unix and Linux.

Very common types of networks include:

1. Local Area Network (LAN)
2. Wide Area Network (WAN)
3. Metropolitan Area Network (MAN)
4. Personal Area Network (PAN)

1. Local Area Network

A Local Area Network (LAN) is a network that is confined to a relatively small area. It is generally limited to a geographic area such as a writing lab, school, or building.

Computers connected to a network are broadly categorized as servers or workstations. Servers are generally not used by humans directly, but rather run continuously to provide "services" to the other computers (and their human users) on the network. Services provided can include printing and faxing, software hosting, file storage and sharing,

messaging, data storage and retrieval, complete access control (security) for the network's resources, and many others.
On a single LAN, computers and servers may be connected by cables or wirelessly. Wireless access to a wired network is made possible by wireless access points (WAPs). These WAP devices provide a bridge between computers and networks. A typical WAP might have the theoretical capacity to connect hundreds or even thousands of wireless users to a network, although practical capacity might be far less.

2. Wide Area Network

Wide Area Networks (WANs) connect networks in larger geographic areas, such as Florida, the United States, or the world. Dedicated transoceanic cabling or satellite uplinks may be used to connect this type of global network.

Using a WAN, schools in Florida can communicate with places like Tokyo in a matter of seconds, without paying enormous phone bills. Two users a half-world apart with workstations equipped with microphones and a webcams might teleconference in real time. A WAN is complicated. It uses multiplexers, bridges, and routers to connect local and metropolitan networks to global communications networks like the Internet. To users, however, a WAN will not appear to be much different than a LAN.

3. Metropolitan area network

A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN. The limits of Metropolitan cities are determined by local municipal corporations and we cannot define them. Hence, the bigger the Metropolitan city the bigger the MAN, smaller a metro city smaller the MAN. The IEEE 802-2002 standard describes a MAN as being.

4. Personal area network

A personal area network (PAN) is a computer network used or communication among computerized devices, including telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink). A wireless personal area network (WPAN) is a PAN carried over wireless network technologies such as IrDA, Wireless USB, Bluetooth, Z-Wave, ZigBee, or even Body Area Network. The reach of a WPAN varies from a few centimeters to a few meters. A PAN may also be carried over wired computer buses such as USB and FireWire.

5. VPN (Virtual Private Network)

VPN uses a technique known as tunneling to transfer data securely on the Internet to a remote access server on your workplace network. Using a VPN helps you save money by using the public Internet instead of making long–distance phone calls to connect securely with your private network. There are two ways to create a VPN connection, by dialing an Internet service provider (ISP), or connecting directly to Internet.

1.2 What is a Topology?

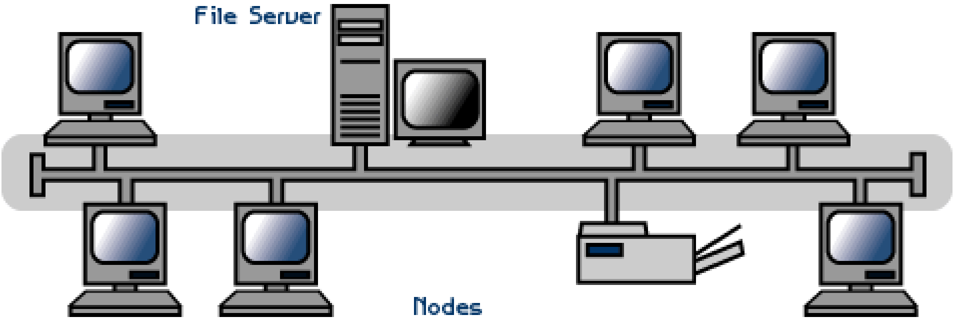
The physical topology of a network refers to the configuration of cables, computers, and other peripherals. Physical topology should not be confused with logical topology which is the method used to pass information between workstations. Logical topology was discussed in the Protocol chapter.

Main Types of Physical Topologies

1. Linear Bus Topology
2. Ring Topology
3. Star Topology
4. Mesh Topology
5. Tree (Expanded Star) Topology
6. Hybrid Topology

1. Linear Bus Topology

A linear bus topology consists of a main run of cable with a terminator at each end. All nodes (file server, workstations, and peripherals) are connected to the linear cable.



Advantages of a Linear Bus Topology

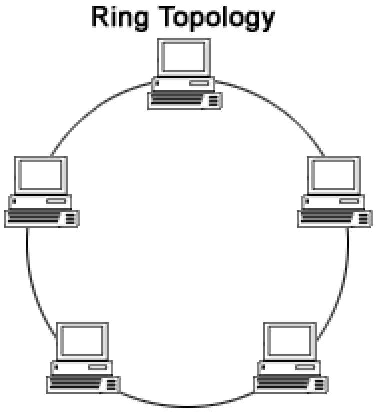
- Easy to connect a computer or peripheral to a linear bus.
- Requires less cable length than a star topology.

Disadvantages of a Linear Bus Topology

- Entire network shuts down if there is a break in the main cable.
- Terminators are required at both ends of the backbone cable.
- Difficult to identify the problem if the entire network shuts down.
- Not meant to be used as a stand-alone solution in a large building.

2. Ring Topology

Alternatively referred to as a ring network, the ring topology is a computer network configuration where each network computer and devices are connected to each other forming a large circle (or similar shape). Each packet is sent around the ring until it reaches its final destination. Today, the ring topology is seldom used. Below is a visual example of a simple computer setup on a network using a ring topology.



Advantages of Ring Topology

- This type of network topology is very organized. Each node gets to send the data when it receives an empty token. This helps to reduces chances of collision. Also in ring topology all the traffic flows in only one direction at very high speed.
- Even when the load on the network increases, its performance is better than that of Bus topology.
- There is no need for network server to control the connectivity between workstations.
- Additional components do not affect the performance of network.
- Each computer has equal access to resources.

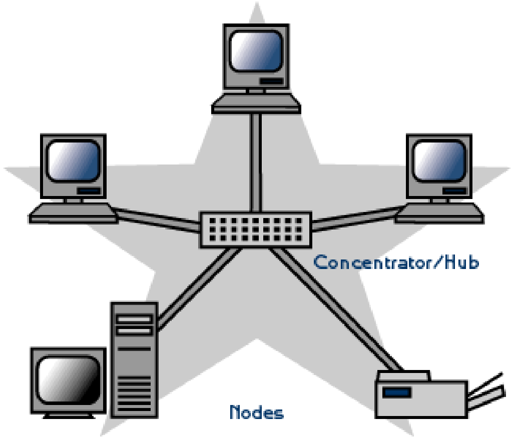
Disadvantages of Ring Topology

- Each packet of data must pass through all the computers between source and destination. This makes it slower than Star topology.
- If one workstation or port goes down, the entire network gets affected.
- Network is highly dependent on the wire which connects different components.
- MAU's and network cards are expensive as compared to Ethernet cards and hubs.

3. Star Topology

A star topology is designed with each node (file server, workstations, and peripherals) connected directly to a central network hub, switch, or concentrator.

Data on a star network passes through the hub, switch, or concentrator before continuing to its destination. The hub, switch, or concentrator manages and controls all functions of the network. It also acts as a repeater for the data flow. This configuration is common with twisted pair cable; however, it can also be used with coaxial cable or fiber optic cable.



Advantages of a Star Topology

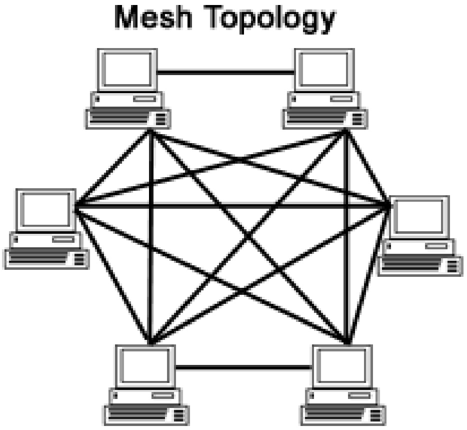
- Easy to install and wire.
- No disruptions to the network when connecting or removing devices.
- Easy to detect faults and to remove parts.

Disadvantages of a Star Topology

- Requires more cable length than a linear topology.
- If the hub, switch, or concentrator fails, nodes attached are disabled.
- More expensive than linear bus topologies because of the cost of the hubs, etc.

4. Mesh Topology

A network setup where each computer and network device is interconnected with one another, allowing for most transmissions to be distributed, even if one of the connections goes down. This topology is not commonly used for most computer networks as it is difficult and expensive to have redundant connection to every computer. However, this topology is commonly used for wireless networks. Below is a visual example of a simple computer setup on a network using a mesh topology.



Advantages of Mesh topology

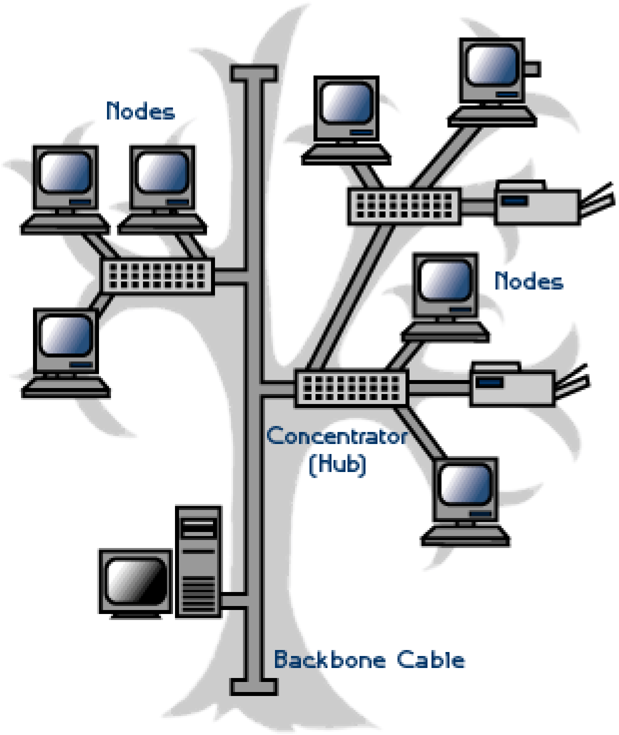
- Data can be transmitted from different devices simultaneously. This topology can withstand high traffic.
- Even if one of the components fails there is always an alternative present. So data transfer doesn't get affected.
- Expansion and modification in topology can be done without disrupting other nodes.

Disadvantages of Mesh topology

- There are high chances of redundancy in many of the network connections.
- Overall cost of this network is way too high as compared to other network topologies.
- Set-up and maintenance of this topology is very difficult. Even administration of the network is tough.

5. Tree or Expanded Star

A tree topology combines characteristics of linear bus and star topologies. It consists of groups of star-configured workstations connected to a linear bus backbone cable. Tree topologies allow for the expansion of an existing network, and enable schools to configure a network to meet their needs.



Advantages of a Tree Topology

- Point-to-point wiring for individual segments.
- Supported by several hardware and software venders.

Disadvantages of a Tree Topology

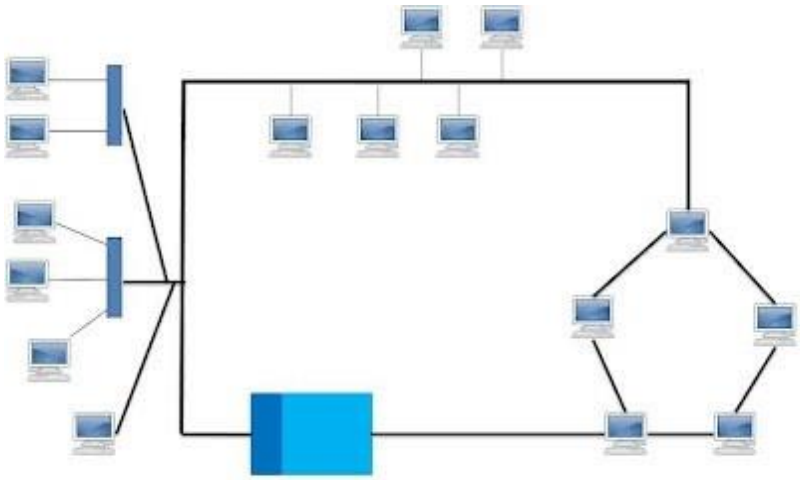
- Overall length of each segment is limited by the type of cabling used.
- If the backbone line breaks, the entire segment goes down.
- More difficult to configure and wire than other topologies.

6. Hybrid Topology

In this type of topology we integrate two or more different topologies to form a resultant topology which has good points (as well as weaknesses) of all the constituent basic topologies rather than having characteristics of one specific topology. This combination of topologies is done according to the requirements of the organization.

For example, if there exists a ring topology in one office department while a bus topology in another department, connecting these two will result in Hybrid topology. Remember connecting two similar topologies cannot be termed as Hybrid topology. Star-Ring and Star- Bus networks are most common examples of hybrid network.

Let's see the benefits and drawbacks of this networking architecture



Advantages of Hybrid Network Topology

- **Reliable**: Unlike other networks, fault detection and troubleshooting is easy in this type of topology. The part in which fault is detected can be isolated from the rest of network and required corrective measures can be taken, WITHOUT affecting the functioning of rest of the network.
- **Scalable**: It’s easy to increase the size of network by adding new components, without disturbing existing architecture.
- **Flexible**: Hybrid Network can be designed according to the requirements of the organization and by optimizing the available resources. Special care can be given to nodes where traffic is high as well as where chances of fault are high.
- **Effective**: Hybrid topology is the combination of two or more topologies, so we can design it in such a way that strengths of constituent topologies are maximized while there weaknesses are neutralized. For example we saw Ring Topology has good data reliability (achieved by use of tokens) and Star topology has high

tolerance capability (as each node is not directly connected to other but through central device), so these two can be used effectively in hybrid star-ring topology.

Disadvantages of Hybrid Topology

- Complexity of Design: One of the biggest drawbacks of hybrid topology is its design. It's not easy to design this type of architecture and it's a tough job for designers. Configuration and installation process needs to be very efficient.
- Costly Hub: The hubs used to connect two distinct networks, are very expensive. These hubs are different from usual hubs as they need to be intelligent enough to work with different architectures and should be function even if a part of network is down.
- Costly Infrastructure: As hybrid architectures are usually larger in scale, they require a lot of cables; cooling systems, sophisticate network devices, etc.

Considerations When Choosing a Topology

1. **Money:** A linear bus network may be the least expensive way to install a network; you do not have to purchase concentrators.
2. **Length:** Length of cable needed. The linear bus network uses shorter lengths of cable.
3. **Future growth:** With a star topology, expanding a network is easily done by adding another concentrator.
4. **Cable type:** The most common cable in schools is unshielded twisted pair, which is most often used with star topologies.

Summary Chart

Physical Topology	**Common Cable**	**Common Protocol**
Linear Bus	Twisted Pair or Coaxial Fiber	Ethernet
Star	Twisted Pair or Fiber	Ethernet
Tree	Twisted Pair or Coaxial Fiber	Ethernet

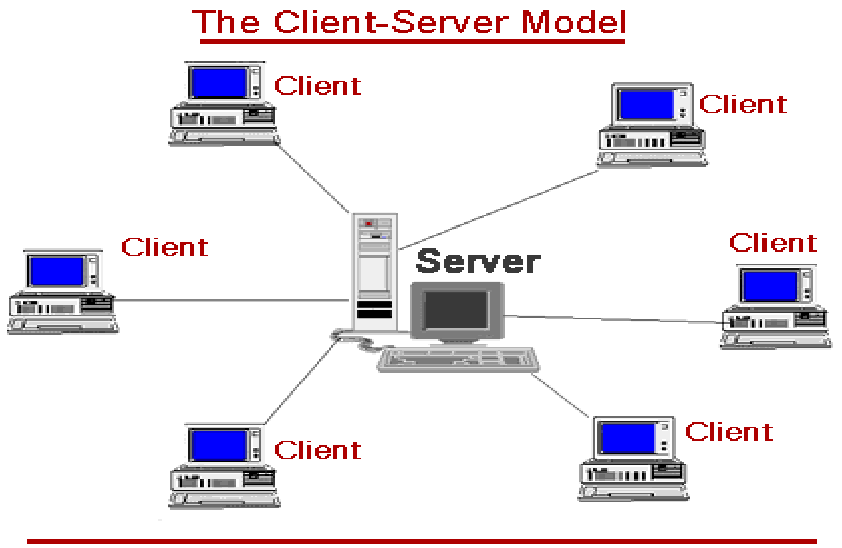
Collisions

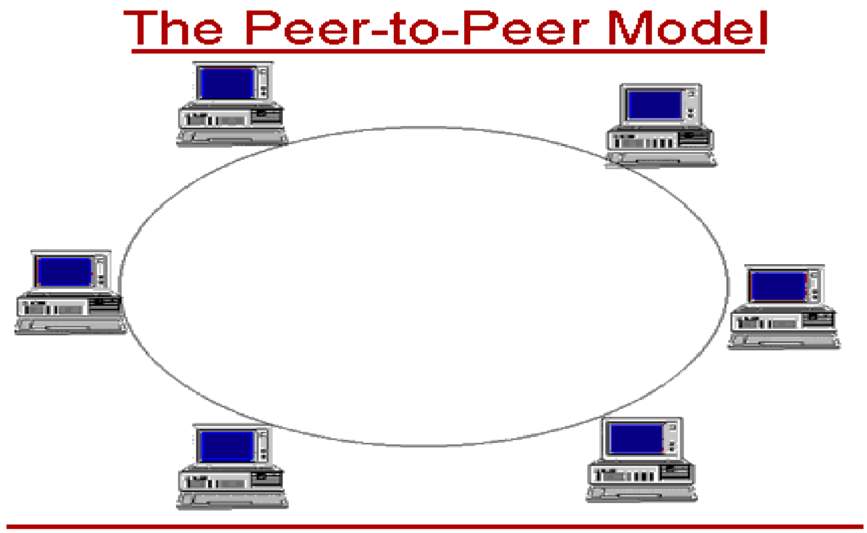
Ethernet is a shared media, so there are rules for sending packets of data to avoid conflicts and protect data integrity. Nodes determine when the network is available for sending packets. It is possible that two nodes at different locations attempt to send data at the same time. When both PCs are transferring a packet to the network at the same time, a collision will result

1.3 Categories of Network

Network can be divided in to two main categories:

1. Peer-to-peer.
2. Server-based.





In **peer-to-peer** networking there are no dedicated servers or hierarchy among the computers. All of the computers are equal and therefore known as peers. Normally each computer serves as Client/Server and there is no one assigned to be an administrator responsible for the entire network.

Peer-to-peer networks are good choices for needs of small organizations where the users are allocated in the same general area, security is not an issue and the organization and the network will have limited growth within the foreseeable future.

The term **Client/server** refers to the concept of sharing the work involved in processing data between the client computer and the most powerful server computer.

The **client/server** network is the most efficient way to provide:

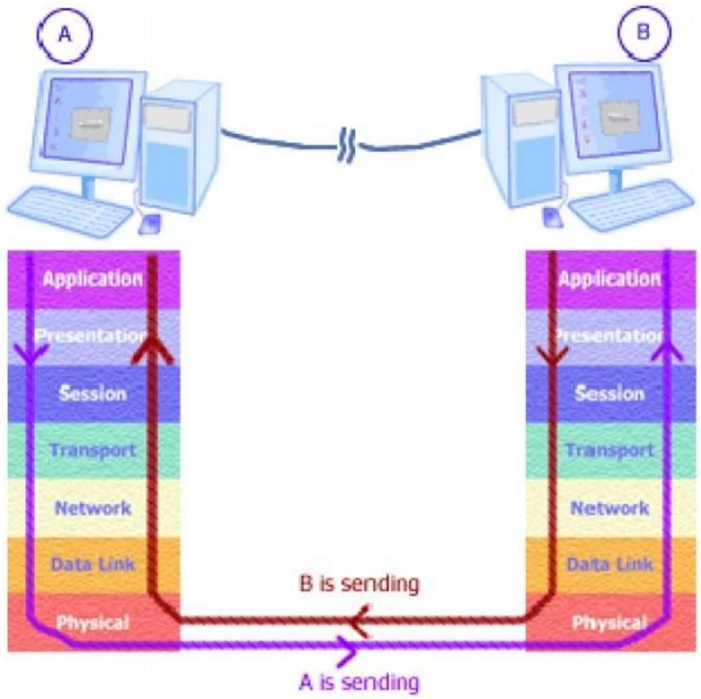
- Databases and management of applications such as Spreadsheets, Accounting, Communications and Document management.
- Network management.
- Centralized file storage.

The client/server model is basically an implementation of distributed or cooperative processing. At the heart of the model is the concept of splitting application functions between a client and a server processor. The division of labor between the different processors enables the application designer to place an application function on the processor that is most appropriate for that function. This lets the software designer optimize the use of processors--providing the greatest possible return on investment for the hardware.

Client/server application design also lets the application provider mask the actual location of application function. The user often does not know where a specific operation is executing. The entire function may execute in either the PC or server, or the function may be split between them. This masking of application function locations enables system implementers to upgrade portions of a system over time with a minimum disruption of application operations, while protecting the investment in existing hardware and software.

The OSI Model:

Open System Interconnection (OSI) reference model has become an International standard and serves as a guide for networking. This model is the best known and most widely used guide to describe networking environments. Vendors design network products based on the specifications of the OSI model. It provides a description of how network hardware and software work together in a layered fashion to make communications possible. It also helps with trouble shooting by providing a frame of reference that describes how components are supposed to function.



There are seven to get familiar with and these are the physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and the application layer.

1. **Physical Layer**, is just that the physical parts of the network such as wires, cables, and there media along with the length. Also this layer takes note of the electrical signals that transmit data throughout system.
2. **Data Link Layer**, this layer is where we actually assign meaning to the electrical signals in the network. The layer also determines the size and format of data sent to printers, and other devices. Also I don't want to forget that these are also called nodes in the network.

3. **Network Layer**, this layer provides the definition for the connection of two dissimilar networks.
4. **Transport Layer**, this layer allows data to be broken into smaller packages for data to be distributed and addressed to other nodes (workstations).
5. **Session Layer**, this layer helps out with the task to carry information from one node (workstation) to another node (workstation). A session has to be made before we can transport information to another computer.
6. **Presentation Layer**, this layer is responsible to code and decode data sent to the node.
7. **Application Layer**, this layer allows you to use an application that will communicate with say the operation system of a server. A good example would be using your web browser to interact with the operating system on a server such as Windows NT, which in turn gets the data you requested.

1.4 Network Architectures

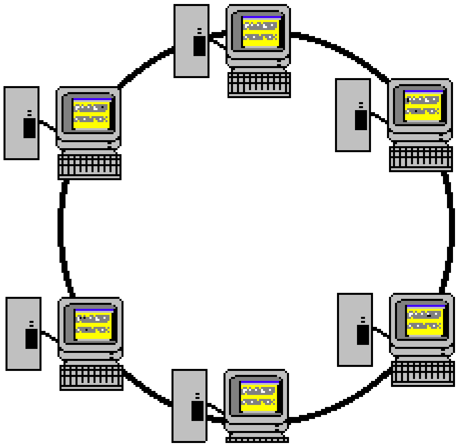
1. Ethernet

Ethernet is the most popular physical layer LAN technology in use today. Other LAN types include Token Ring, Fast Ethernet, Fiber Distributed Data Interface (FDDI), Asynchronous Transfer Mode (ATM) and LocalTalk. Ethernet is popular because it strikes a good balance between speed, cost and ease of installation. These benefits, combined with wide acceptance in the computer marketplace and the ability to support virtually all popular network protocols, make Ethernet an ideal networking technology for most computer users today. The Institute for Electrical and Electronic Engineers (IEEE) defines the Ethernet standard as IEEE Standard 802.3. This standard defines rules for configuring an Ethernet network as well as specifying how elements in an Ethernet network interact with one another. By adhering to the IEEE standard, network equipment and network protocols can communicate efficiently.

2. Fast Ethernet

For Ethernet networks that need higher transmission speeds, the Fast Ethernet standard (IEEE 802.3u) has been established. This standard raises the Ethernet speed limit from 10 Megabits per second (Mbps) to 100 Mbps with only minimal changes to the existing cable structure. There are three types of Fast Ethernet: 100BASE-TX for use with level 5 UTP cable, 100BASE-FX for use with fiber-optic cable, and 100BASE-T4 which utilizes an extra two wires for use with level 3 UTP cable. The 100BASE-TX standard has become the most popular due to its close compatibility with the 10BASE-T Ethernet standard. For the network manager, the incorporation of Fast Ethernet into an existing configuration presents a host of decisions. Managers must determine the number of users in each site on the network that need the higher throughput, decide which segments of the backbone need to be reconfigured specifically for 100BASE-T and then choose the necessary hardware to connect the 100BASE-T segments with existing 10BASE-T segments. Gigabit Ethernet is a future technology that promises a migration path beyond Fast Ethernet so the next generation of networks will support even higher data transfer speeds.

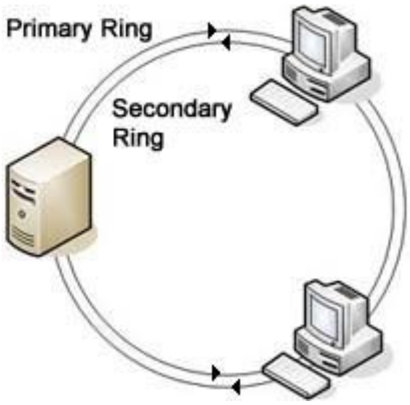
3. Token Ring



Token Ring is another form of network configuration which differs from Ethernet in that all messages are transferred in a unidirectional manner along the ring at all times. Data is transmitted in tokens, which are passed along the ring and viewed by each device. When a device sees a message addressed to it, that device copies the message and then marks that message as being read. As the message makes its way along the ring, it eventually gets back to the sender who now notes that the message was received by the intended device. The sender can then remove the message and free that token for use by others.

Various PC vendors have been proponents of Token Ring networks at different times and thus these types of networks have been implemented in many organizations.

4. FDDI



FDDI (Fiber-Distributed Data Interface) is a standard for data transmission on fiber optic lines in a local area network that can extend in range up to 200 km (124 miles). The FDDI protocol is based on the token ring protocol. In addition to being large geographically, an FDDI local area network can support thousands of users.

1.5 Protocols

Network protocols are standards that allow computers to communicate. A protocol defines how computers identify one another on a network, the form that the data should take in transit, and how this information is processed once it reaches its final destination. Protocols also define procedures for handling lost or damaged transmissions or "packets." TCP/IP (for UNIX, Windows NT, Windows 95 and other platforms), IPX (for Novell NetWare), DECnet (for networking Digital Equipment Corp. computers), AppleTalk (for Macintosh computers), and NetBIOS/NetBEUI (for LAN Manager and Windows NT networks) are the main types of network protocols in use today.

Although each network protocol is different, they all share the same physical cabling. This common method of accessing the physical network allows multiple protocols to peacefully coexist over the network media, and allows the builder of a network to use common hardware for a variety of protocols. This concept is known as "protocol independence,"

Some Important Protocols and their job:

Protocol	Acronym	Its Job
Transmission Control Protocol/internet Protocol	TCP/IP	The backbone protocol of the internet. Popular also for intranets using the internet
Internetwork Package Exchange/Sequenced Packet Exchange	IPX/SPX	This is a standard protocol for Novell Network Operating System
NetBIOS Extended User Interface	NetBEUI	This is a Microsoft protocol that doesn't support routing to other networks
File Transfer Protocol	FTP	Used to send and receive files from a remote host
Hyper Text Transfer Protocol	HTTP	Used for the web to send documents that is encoded in HTML.
Secured Hyper Text Transfer Protocol	HTTPS	Information transfer is encrypted and secured to encrypted information.
Network File Services	NFS	Allows network nodes or workstations to access files and drives as if they were their own.
Simple Mail Transfer Protocol	SMTP	Used to send Email over a network
Telnet		Used to connect to a host and emulate a terminal that the remote server can recognize
Post Office Protocol	POP	This protocol is used for transferring or downloading mails to your local system. So, that you can view/compose mails offline.
Internet Message Access Protocol	IMAP4	This is secured version of POP.
Routing Information Protocol	RIP	It is a protocol that is used to communicate b/w multiple routers for data transmission at a long distance.
Dynamic Host Configuration Protocol	DHCP	This protocol is used for assignment of dynamic IP address to the host systems.

Introduction to TCP/IP Networks:

TCP/IP-based networks play an increasingly important role in computer networks. Perhaps one reason for their appeal is that they are based on an open specification that is not controlled by any vendor.

What Is TCP/IP?

TCP stands for Transmission Control Protocol and IP stands for Internet Protocol. The term TCP/IP is not limited just to these two protocols, however. Frequently, the term TCP/IP is used to refer to a group of protocols related to the TCP and IP protocols such as the User Datagram Protocol (UDP), File Transfer Protocol (FTP), Terminal Emulation Protocol (TELNET), and so on.

The Origins of TCP/IP

In the late 1960s, DARPA (the Defense Advanced Research Project Agency), in the United States, noticed that there was a rapid proliferation of computers in military communications. Computers, because they can be easily programmed, provide flexibility in achieving network functions that is not available with other types of communications equipment. The computers then used in military communications were manufactured by different vendors and were designed to interoperate with computers from that vendor only. Vendors used proprietary protocols in their communications equipment. The military had a multi vendor network but no common protocol to support the heterogeneous equipment from different vendors

1.6 Transmission Media

Transmission Media is of two types:

1. Wired
2. Wireless

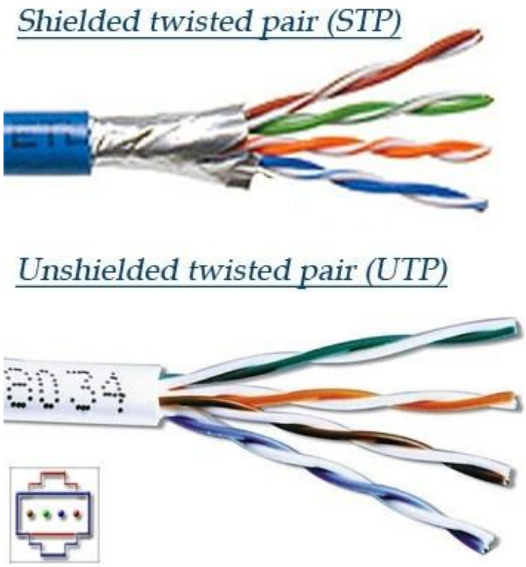
1. Wired Transmission

Cable is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with LANs. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

The following are the wired mediums:

- Unshielded Twisted Pair (UTP) Cable
- Shielded Twisted Pair (STP) Cable
- Coaxial Cable
- Fiber Optic Cable

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks.



The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot. The EIA/TIA (Electronic Industry Association/Telecommunication Industry Association) has established standards of UTP and rated six categories of wire (additional categories are emerging).

Categories of Unshielded Twisted Pair

Category	Speed	Use
1	1 Mbps	Voice Only (Telephone Wire)
2	4 Mbps	LocalTalk & Telephone (Rarely used)
3	16 Mbps	10BaseT Ethernet
4	20 Mbps	Token Ring (Rarely used)
5	100 Mbps (2 pair)	100BaseT Ethernet

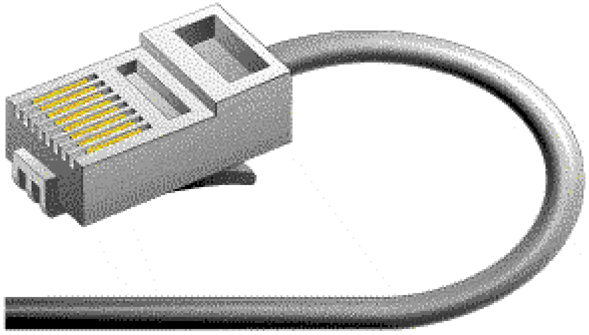
	1000 Mbps (4 pair)	Gigabit Ethernet
5e	1,000 Mbps	Gigabit Ethernet
6	10,000 Mbps	Gigabit Ethernet

Unshielded Twisted Pair Cabling Standards

- **Cat 1 :** Currently unrecognized by TIA/EIA. Previously used for POTS telephone communications, ISDN and doorbell wiring.
- **Cat 2 :** Currently unrecognized by TIA/EIA. Previously was frequently used on 4 Mbit/s token ring networks.
- **Cat 3 :** Currently defined in TIA/EIA-568-B; used for data networks utilizing frequencies up to 16MHz. Historically popular for 10 Mbit/s Ethernet networks.
- **Cat 4 :** Currently unrecognized by TIA/EIA. Provided performance of up to 20 MHz, and was frequently used on 16 Mbit/s token ring networks.
- **Cat 5 :** Currently unrecognized by TIA/EIA. Provided performance of up to 100 MHz, and was frequently used on 100 Mbit/s Ethernet networks. May be unsuitable for 1000BASE-T gigabit Ethernet.
- **Cat 5e :** Currently defined in TIA/EIA-568-B. Provides performance of up to 100 MHz, and is frequently used for both 100 Mbit/s and gigabit Ethernet networks.
- **Cat 6 :** Currently defined in TIA/EIA-568-B. Provides performance of up to 250 MHz, more than double category 5 and 5e.
- **Cat 6a :** Future specification for 10 Gbit/s applications.
- **Cat 7 :** An informal name applied to ISO/IEC 11801 Class F cabling. This standard specifies four individually-shielded pairs (STP) inside an overall shield. Designed for transmission at frequencies up to 600 MHz's.

1. Unshielded Twisted Pair Connector

The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector. A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.



RJ-45 connector

2. Shielded Twisted Pair (STP) Cable

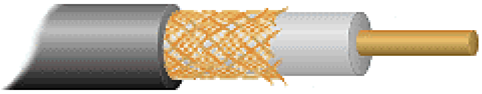
Although UTP cable is the least expensive cable, it may be susceptible to radio and electrical frequency interference (it should not be too close to electric motors, fluorescent lights, etc.). If you must place cable in environments with lots of potential interference, or if you must place cable in extremely sensitive environments that may be susceptible to the electrical current in the UTP, shielded twisted pair may be the solution. Shielded cables can also help to extend the maximum distance of the cables.

- Shielded twisted pair cable is available in three different configurations:
- Each pair of wires is individually shielded with foil.
- There is a foil or braid shield inside the jacket covering all wires (as a group).

There is a shield around each individual pair, as well as around the entire group of wires (referred to as double shield twisted pair).

3. Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield. The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.



Coaxial cable

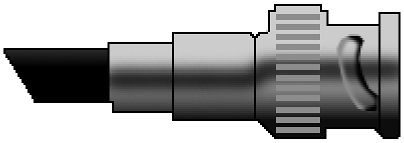
Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are **thick coaxial** and **thin coaxial**.

Thin coaxial cable is also referred to as thinnet. 10Base2 refers to the specifications for thin coaxial cable carrying Ethernet signals. The 2 refers to the approximate maximum segment length being 200 meters. In actual fact the maximum segment length is 185 meters. Thin coaxial cable has been popular in school networks, especially linear bus networks.

Thick coaxial cable is also referred to as thicknet. 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters. Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the center conductor. This makes thick coaxial a great choice when running longer lengths in a linear bus network. One disadvantage of thick coaxial is that it does not bend easily and is difficult to install.

Coaxial Cable Connectors

The most common type of connector used with coaxial cables is the Bayone-Neill-Concelman (BNC) connector. Different types of adapters are available for BNC connectors, including a T-connector, barrel connector, and terminator. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather screw, onto the cable.



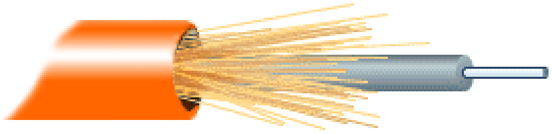
BNC connector

4. Fiber Optic Cable

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials. It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services. The cost of fiber optic cabling is comparable to copper cabling; however, it is more difficult to install and modify. 10BaseF refers to the specifications for fiber optic cable carrying Ethernet signals.

The center core of fiber cables is made from glass or plastic fibers (see fig 5). A plastic coating then cushions the fiber center, and kevlar fibers help to strengthen the cables and prevent breakage. The outer insulating jacket made of teflon or PVC.



Fiber optic cable

There are two common types of fiber cables -- single mode and multimode. Multimode cable has a larger diameter; however, both cables provide high bandwidth at high speeds. Single mode can provide more distance, but it is more expensive.

Specification	**Cable Type**
10BaseT	Unshielded Twisted Pair
10Base2	Thin Coaxial
10Base5	Thick Coaxial
100BaseT	Unshielded Twisted Pair
100BaseFX	Fiber Optic
100BaseBX	Single mode Fiber
100BaseSX	Multimode Fiber
1000BaseT	Unshielded Twisted Pair
1000BaseFX	Fiber Optic
1000BaseBX	Single mode Fiber
1000BaseSX	Multimode Fiber

Installing Cable - Some Guidelines

When running cable, it is best to follow a few simple rules:

1. Always use more cable than you need. Leave plenty of slack.
2. Test every part of a network as you install it. Even if it is brand new, it may have problems that will be difficult to isolate later.
3. Stay at least 3 feet away from fluorescent light boxes and other sources of electrical interference.
4. If it is necessary to run cable across the floor, cover the cable with cable protectors.
5. Label both ends of each cable.
6. Use cable ties (not tape) to keep cables in the same location together.

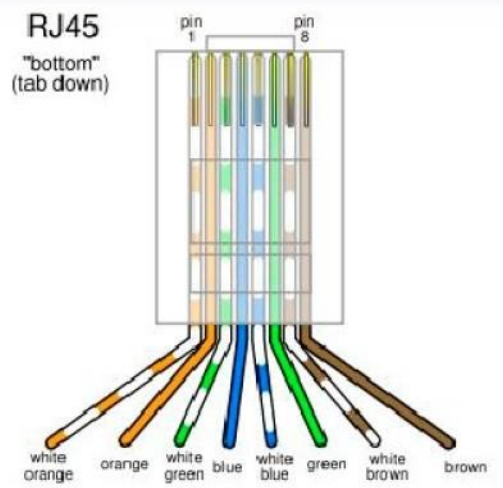
Ethernet Cable Connectors

- 8P8C - 8 positions, 8 conductor modular connector. Incorrectly referred to as RJ45.
- Cables available assembled, or connectors may be crimped on

cable. There are two types of Ethernet Cables:

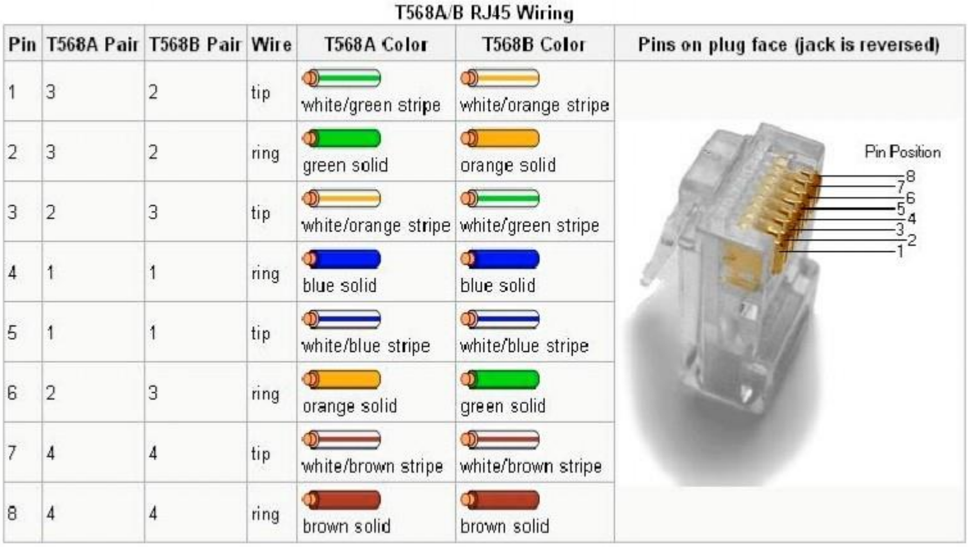
1. **Straight Cable :** To connect different kinds of devices. Eg, Switch to System,
2. **Cross Cable :** To connect similar kinds of devices. Eg, System to System

Ethernet RJ45 Pin Configurations



T568B RJ45 Connection

- Eight connections consist of four wire pairs.
- Pairs are solid and stripe of same color.
- Two pin configurations, T568A and T568B, which are interoperable.



T568A/B RJ45 Wiring

Pin	T568A Pair	T568B Pair	Wire	T568A Color	T568B Color	Pins on plug face (jack is reversed)
1	3	2	tip	white/green stripe	white/orange stripe	
2	3	2	ring	green solid	orange solid	
3	2	3	tip	white/orange stripe	white/green stripe	
4	1	1	ring	blue solid	blue solid	
5	1	1	tip	white/blue stripe	white/blue stripe	
6	2	3	ring	orange solid	green solid	
7	4	4	tip	white/brown stripe	white/brown stripe	
8	4	4	ring	brown solid	brown solid	

1.7 Ethernet Products

The standards and technology that have just been discussed help define the specific products that network managers use to build Ethernet networks. The following text discusses the key products needed to build an Ethernet LAN.

Transceivers

Transceivers are used to connect nodes to the various Ethernet media. Most computers and network interface cards contain a built-in 10BASE-T or 10BASE2 transceiver, allowing them to be connected directly to Ethernet without requiring an external transceiver. Many Ethernet devices provide an AUI connector to allow the user to connect to any media type via an external transceiver. The AUI connector consists of a 15-pin D-shell type connector, female on the computer side, male on the transceiver side. Thickwire (10BASE5) cables also use transceivers to allow connections.

For Fast Ethernet networks, a new interface called the MII (Media Independent Interface) was developed to offer a flexible way to support 100 Mbps connections. The MII is a popular way to connect 100BASE-FX links to copper-based Fast Ethernet devices.

Network Interface Cards

Network interface cards, commonly referred to as NICs, and are used to connect a PC to a network. The NIC provides a physical connection between the networking cable and the computer's internal bus. Different computers have different bus architectures; PCI bus master slots are most commonly found on 486/Pentium PCs and ISA expansion slots are commonly found on 386 and older PCs. NICs come in three basic varieties: 8- bit, 16-bit, and 32-bit. The larger the number of bits that can be transferred to the NIC, the faster the NIC can transfer data to the network cable.

Many NIC adapters comply with Plug-n-Play specifications. On these systems, NICs are automatically configured without user intervention, while on non-Plug-n-Play systems, configuration is done manually through a setup program and/or DIP switches.

Cards are available to support almost all networking standards, including the latest Fast Ethernet environment. Fast Ethernet NICs are often 10/100 capable, and will automatically set to the appropriate speed. Full duplex networking is another option, where a dedicated connection to a switch allows a NIC to operate at twice the speed.

Hubs/Repeaters

Hubs/repeaters are used to connect together two or more Ethernet segments of any media type. In larger designs, signal quality begins to deteriorate as segments exceed their maximum length. Hubs provide the signal amplification required to allow a segment to be extended a greater distance. A hub takes any incoming signal and repeats it out all ports.

Ethernet hubs are necessary in star topologies such as 10BASE-T. A multi-port twisted pair hub allows several point-to-point segments to be joined into one network. One end of the point-to-point link is attached to the hub and the other is attached to the computer. If the hub is attached to a backbone, then all computers at the end of the twisted pair segments can communicate with all the hosts on the backbone. The number and type of hubs in any one-collision domain is limited by the Ethernet rules. These repeater rules are discussed in more detail later.

Network Type	Max Nodes Per Segment	Max Distance Per Segment
10BASE-T	2	100m
10BASE2	30	185m
10BASE5	100	500m
10BASE-FL	2	2000m

Adding Speed

While repeaters allow LANs to extend beyond normal distance limitations, they still limit the number of nodes that can be supported. Bridges and switches, however, allow LANs to grow significantly larger by virtue of their ability to support full Ethernet segments on each port. Additionally, bridges and switches selectively filter network traffic to only those packets needed on each segment - this significantly increases throughput on each segment and on the overall network. By providing better performance and more flexibility for network topologies, bridges and switches will continue to gain popularity among network managers.

Bridges

The function of a bridge is to connect separate networks together. Bridges connect different networks types (such as Ethernet and Fast Ethernet) or networks of the same type. Bridges map the Ethernet addresses of the nodes residing on each network segment and allow only necessary traffic to pass through the bridge. When a packet is received by the bridge, the bridge determines the destination and source segments. If the segments are the same, the packet is dropped ("filtered"); if the segments are different, then the packet is "forwarded" to the correct segment. Additionally, bridges do not forward bad or misaligned packets. Bridges are also called "store-and-forward" devices because they look at the whole Ethernet packet before making filtering or forwarding decisions. Filtering packets and regenerating forwarded packets enable bridging technology to split a network into separate collision domains. This allows for greater distances and more repeaters to be used in the total network design.

Ethernet Switches

Ethernet switches are an expansion of the concept in Ethernet bridging. LAN switches can link four, six, ten or more networks together, and have two basic architectures: cut-through and store-and-forward. In the past, cut-through switches were faster because they examined the packet destination address only before forwarding it on to its destination segment. A store-and-forward switch, on the other hand, accepts and analyzes the entire packet before forwarding it to its destination.

It takes more time to examine the entire packet, but it allows the switch to catch certain packet errors and keep them from propagating through the network. Both cut-through and store-and-forward switches separate a network into collision domains, allowing network design rules to be extended. Each of the segments attached to an Ethernet switch has a full 10 Mbps of bandwidth shared by fewer users, which results in better performance (as opposed to hubs that only allow bandwidth sharing from a single Ethernet). Newer switches today offer high-speed links, FDDI, Fast Ethernet or ATM. These are used to link switches together or give added bandwidth to high-traffic servers. A network composed of a number of switches linked together via uplinks is termed a "collapsed backbone" network.

Routers

Routers filter out network traffic by specific protocol rather than by packet address. Routers also divide networks logically instead of physically. An IP router can divide a network into various subnets so that only traffic destined for particular IP addresses can pass between segments. Network speed often decreases due to this type of intelligent forwarding. Such filtering takes more time than that exercised in a switch or bridge, which only looks at the Ethernet address. However, in more complex networks, overall efficiency is improved by using routers.

What is a Network Firewall?

A firewall is a system or group of systems that enforces an access control policy between two networks. The actual means by which this is accomplished varies widely, but in principle, the firewall can be thought of as a pair of mechanisms: one which exists to block traffic, and the other which exists to permit traffic. Some firewalls place a greater emphasis on blocking traffic, while others emphasize permitting traffic. Probably the most important thing to recognize about a firewall is that it implements an access control policy. If you don't have a good idea of what kind of access you want to allow or to deny, a firewall really won't help you. It's also important to recognize that the firewall's configuration, because it is a mechanism for enforcing policy, imposes its policy on everything behind it. Administrators for firewalls managing the connectivity for a large number of hosts therefore have a heavy responsibility.

Network Design Criteria

Ethernets and Fast Ethernets have design rules that must be followed in order to function correctly. Maximum number of nodes, number of repeaters and maximum segment distances are defined by the electrical and mechanical design properties of each type of Ethernet and Fast Ethernet media.

A network using repeaters, for instance, functions with the timing constraints of Ethernet. Although electrical signals on the Ethernet media travel near the speed of light, it still takes a finite time for the signal to travel from one end of a large Ethernet to another. The Ethernet standard assumes it will take roughly 50 microseconds for a signal to reach its destination.

Ethernet is subject to the "5-4-3" rule of repeater placement: The network can only have five segments connected; it can only use four repeaters; and of the five segments, only three can have users attached to them; the other two must be inter-repeater links.

If the design of the network violates these repeater and placement rules, then timing guidelines will not be met and the sending station will resend that packet. This can lead to lost packets and excessive resent packets, which can slow network performance and create trouble for applications. Fast Ethernet has modified repeater rules, since the minimum packet size takes less time to transmit than regular Ethernet. The length of the network links allows for a fewer number of repeaters. In Fast Ethernet networks, there are two classes of repeaters. Class I repeaters have a latency of 0.7 microseconds or less and are limited to one repeater per network. Class II repeaters have a latency of 0.46 microseconds or less and are limited to two repeaters per network. The following are the distance (diameter) characteristics for these types of Fast Ethernet repeater combinations:

Fast Ethernet	Copper	Fiber
No Repeaters	100m	412m*
One Class I Repeater	200m	272m
One Class II Repeater	200m	272m
Two Class II Repeaters	205m	228m

* Full Duplex Mode 2 km

When conditions require greater distances or an increase in the number of nodes/repeaters, then a bridge, router or switch can be used to connect multiple networks together. These devices join two or more separate networks, allowing network design criteria to be restored. Switches allow network designers to build large networks that function well. The reduction in costs of bridges and switches reduces the impact of repeater rules on network design.

Each network connected via one of these devices is referred to as a separate collision domain in the overall network.

Comparison between Hub, Bridge, Switch & Router

Feature	Hub	Bridge	Switch	Router
Number of broadcast domains	Segment	1	1	1 per router interface
Number of collision domains	1	1 per bridge port	1 per switch port	1 per router interface
Forwards LAN	1	Yes	Yes	No
Forwards LAN multicasts	N/A	Yes	Yes; can be optimized for less forwarding	No
OSI layer used when making forwarding decision	N/A	Layer 2	Layer 2	Layer 3
Internal processing variants	N/A	Store- and-forward	Store-and- forward, cut-through, Fragment Free	Store- and-forward
Frame/packet fragmentation allowed?	N/A	No	No	Yes
Multiple concurrent equal-cost paths to same destination allowed?	N/A	No	No	Yes

1.8 Types of Servers

1. Device Servers

A device server is defined as a specialized, network-based hardware device designed to perform a single or specialized set of server functions. It is characterized by a minimal operating architecture that requires no per seat network operating system license, and client access that is independent of any operating system or proprietary protocol. In addition the device server is a "closed box," delivering extreme ease of installation, minimal maintenance, and can be managed by the client remotely via a Web browser.

Print servers, terminal servers, remote access servers and network time servers are examples of device servers which are specialized for particular functions. Each of these types of servers has unique configuration attributes in hardware or software that help them to perform best in their particular arena.

2. Print Servers

Print servers allow printers to be shared by other users on the network. Supporting either parallel and/or serial interfaces, a print server accepts print jobs from any person on the network using supported protocols and manages those jobs on each appropriate printer.

Print servers generally do not contain a large amount of memory; printers simply store information in a queue. When the desired printer becomes available, they allow the host to transmit the data to the appropriate printer port on the server. The print server can then simply queue and print each job in the order in which print requests are received, regardless of protocol used or the size of the job.

3. Multiport Device Servers

Devices that are attached to a network through a multiport device server can be shared between terminals and hosts at both the local site and throughout the network. A single terminal may be connected to several hosts at the same time (in multiple concurrent sessions), and can switch between them. Multiport device servers are also used to network devices that have only serial outputs. A connection between serial ports on

different servers is opened, allowing data to move between the two devices.
Given its natural translation ability, a multi-protocol multiport device server can perform conversions between the protocols it knows, like LAT and TCP/IP. While server bandwidth is not adequate for large file transfers, it can easily handle host-to-host inquiry/response applications, electronic mailbox checking, etc. And it is far more economical than the alternatives of acquiring expensive host software and special-purpose converters. Multiport device and print servers give their users greater flexibility in configuring and managing their networks.

Whether it is moving printers and other peripherals from one network to another, expanding the dimensions of interoperability or preparing for growth, multiport device servers can fulfill your needs, all without major rewiring.

4. Access Servers

While Ethernet is limited to a geographic area, remote users such as traveling sales people need access to network-based resources. Remote LAN access, or remote access, is a popular way to provide this connectivity. Access servers use telephone services to link a user or office with an office network. Dial-up remote access solutions such as ISDN or asynchronous dial introduce more flexibility. Dial-up remote access offers both the remote office and the remote user the economy and flexibility of "pay as you go" telephone services. ISDN is a special telephone service that offers three channels, two 64 Kbps "B" channels for user data and a "D" channel for setting up the connection. With ISDN, the B channels can be combined for double bandwidth or separated for different applications or users. With asynchronous remote access, regular telephone lines are combined with modems and remote access servers to allow users and networks to dial anywhere in the world and have data access. Remote access servers provide connection points for both dial-in and dial-out applications on the network to which they are attached. These hybrid devices route and filter protocols and offer other services such as modem pooling and terminal/printer services. For the remote PC user, one can connect from any available telephone jack (RJ45), including those in a hotel rooms or on most airplanes.

5. Network Time Servers

A network time server is a server specialized in the handling of timing information from sources such as satellites or radio broadcasts and is capable of providing this timing data to its attached network. Specialized protocols such as NTP or udp/time allow a time server to communicate to other network nodes ensuring that activities that must be coordinated according to their time of execution are synchronized correctly. GPS satellites are one source of information that can allow global installations to achieve constant timing.

1.9 IP Addressing

An IP (Internet Protocol) address is a unique identifier for a node or host connection on an IP network. An IP address is a 32 bit binary number usually represented as 4 decimal values, each representing 8 bits, in the range 0 to 255 (known as octets) separated by decimal points. This is known as "dotted decimal" notation.

Example: 140.179.220.200

It is sometimes useful to view the values in their binary form.

140 .179 .220 .200

10001100.10110011.11011100.11001000

Every IP address consists of two parts, one identifying the network and one identifying the node. The Class of the address and the subnet mask determine which part belongs to the network address and which part belongs to the node address.

Address Classes:

There are 5 different address classes. You can determine which class any IP address is in by examining the first 4 bits of the IP address.

Class A addresses begin with 0xxx, or 1 to 126 decimal.

Class B addresses begin with 10xx, or 128 to 191 decimal, because 127 is loopback address.

Class C addresses begin with 110x, or 192 to 223

decimal. **Class D** addresses begin with 1110, or 224 to

239 decimal. **Class E** addresses begin with 1111, or 240

to 254 decimal.

Addresses beginning with 01111111, or 127 decimal, are reserved for loopback and for internal testing on a local machine. [You can test this: you should always be able to ping 127.0.0.1, which points to yourself] Class D addresses are reserved for multicasting. Class E addresses are reserved for future use. They should not be used for host addresses.

Now we can see how the Class determines, by default, which part of the IP address belongs to the network (N) and which part belongs to the node (n).
Class A -- NNNNNNNN.nnnnnnnn.nnnnnnn.nnnnnnn
Class B --
NNNNNNNN.NNNNNNNN.nnnnnnnn.nnnnnnnn
Class C -- NNNNNNNN.NNNNNNNN.NNNNNNNN.nnnnnnnn

In the example, 140.179.220.200 is a Class B address so by default the Network part of the address (also known as the Network Address) is defined by the first two octets (140.179.x.x) and the node part is defined by the last 2 octets (x.x.220.200).

In order to specify the network address for a given IP address, the node section is set to all "0"s. In our example, 140.179.0.0 specifies the network address for 140.179.220.200. When the node section is set to all "1"s, it specifies a broadcast that is sent to all hosts on the network. 140.179.255.255 specifies the example broadcast address. Note that this is true regardless of the length of the node section.

Private Subnets

There are three IP network addresses reserved for private networks. The addresses are 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. They can be used by anyone setting up internal IP networks, such as a lab or home LAN behind a NAT or proxy server or a router. It is always safe to use these because routers on the Internet will never forward packets coming from these addresses.

Subnetting an IP Network can be done for a variety of reasons, including organization, use of different physical media (such as Ethernet, FDDI, WAN, etc.), preservation of address space, and security. The most common reason is to control network traffic. In an Ethernet network, all nodes on a segment see all the packets transmitted by all the other nodes on that segment. Performance can be adversely affected under heavy traffic loads, due to collisions and the resulting retransmissions. A router is used to connect IP networks to minimize the amount of traffic each segment must receive.

Subnet Masking

Applying a subnet mask to an IP address allows you to identify the network and node parts of the address. The network bits are represented by the 1s in the mask, and the node bits are represented by the 0s. Performing a bitwise logical AND operation between the IP address and the subnet mask results in the Network Address or Number.

For example, using our test IP address and the default Class B subnet mask, we get:

10001100.10110011.11110000.11001000 140.179.240.200 Class B IP Address
11111111.11111111.00000000.00000000 255.255.000.000 Default Class B Subnet Mask
10001100.10110011.00000000.00000000 140.179.000.000 Network Address

Default subnet masks

- Class A - 255.0.0.0 - 11111111.00000000.00000000.00000000
- Class B - 255.255.0.0 - 11111111.11111111.00000000.00000000
- Class C - 255.255.255.0 - 11111111.11111111.11111111.00000000

CIDR -- Classless InterDomain Routing.

CIDR was invented several years ago to keep the internet from running out of IP addresses. The "classful" system of allocating IP addresses can be very wasteful; anyone who could reasonably show a need for more that 254 host addresses was given a Class B address block of 65533 host addresses. Even more wasteful were companies and organizations that were allocated Class A address blocks, which contain over 16 Million host addresses! Only a tiny percentage of the allocated Class A and Class B address space has ever been actually assigned to a host computer on the Internet.

People realized that addresses could be conserved if the class system was eliminated. By accurately allocating only the amount of address space that was actually needed, the address space crisis could be avoided for many years. This was first proposed in 1992 as a scheme called Supernetting.

The use of a CIDR notated address is the same as for a Classful address. Classful addresses can easily be written in CIDR notation (Class A = /8, Class B = /16, and Class C = /24)

It is currently almost impossible for an individual or company to be allocated their own IP address blocks. You will simply be told to get them from your ISP. The reason for this is the ever-growing size of the internet routing table. Just 5 years ago, there were less than 5000 network routes in the entire Internet. Today, there are over 90,000. Using CIDR, the biggest ISPs are allocated large chunks of address space (usually with a subnet mask of /19 or even smaller); the ISP's customers (often other, smaller ISPs) are then allocated networks from the big ISP's pool. That way, all the big ISP's customers (and their customers, and so on) are accessible

via 1 networkroute on the Internet.

It is expected that CIDR will keep the Internet happily in IP addresses for the next few years at least. After that, IPv6, with 128 bit addresses, will be needed. Under IPv6, even sloppy address allocation would comfortably allow a billion unique IP addresses for every person on earth

CCNA TRAINING REPORT

2. DNS

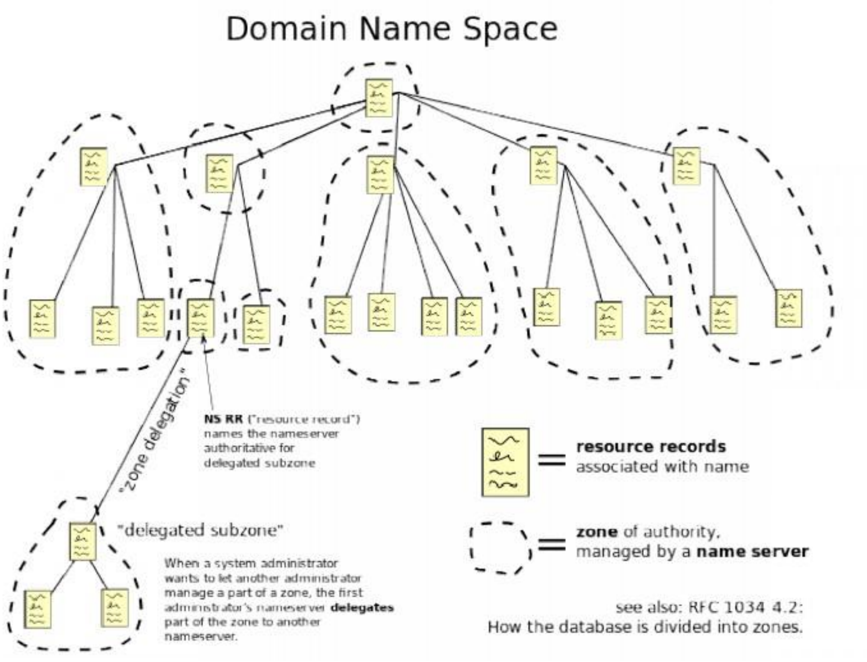
2.1 Introduction

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. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for the purpose of locating computer services and devices worldwide. By providing a worldwide, distributed keyword-based redirection service, the Domain Name System is an essential component of the functionality of the Internet.

An often-used analogy to explain the Domain Name System is that it serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses.
For example, the domain name www.example.com translates to the addresses 93.184.216.119 (IPv4) and 2606:2800:220:6d:26bf:1447:1097:aa7 (IPv6). Unlike a phone book, the DNS can be quickly updated, allowing a service's location on the network to change without affecting the end users, who continue to use the same host name. Users take advantage of this when they use meaningful Uniform Resource Locators (URLs), and e- mail addresses without having to know how the computer actually locates the services.

Domain name space

The domain name space consists of a tree of domain names. Each node or leaf in the tree has zero or more *resource records*, which hold information associated with the domain name. The tree sub-divides into *zones* beginning at the root zone. A DNS zone may consist of only one domain, or may consist of many domains and sub-domains, depending on the administrative authority delegated to the manager.


Domain Name Space
"zone delegation"
NS RR ("resource record") names the nameserver authoritative for delegated subzone
"delegated subzone"
When a system administrator wants to let another administrator manage a part of a zone, the first administrator's nameserver delegates part of the zone to another nameserver.
= resource records associated with name
= zone of authority, managed by a name server
see also: RFC 1034 4.2: How the database is divided into zones.

The hierarchical Domain Name System, organized into zones, each served by a name server

Administrative responsibility over any zone may be divided by creating additional zones. Authority is said to be *delegated* for a portion of the old space, usually in the form of sub-domains, to another name server and administrative entity. The old zone ceases to be authoritative for the new zone.

Domain name syntax

The definitive descriptions of the rules for forming domain names appear in RFC 1035, RFC 1123, and RFC 2181. A domain name consists of one or more parts, technically called *labels*, that are conventionally concatenated, and delimited by dots, such as example.com.

- The right-most label conveys the top-level domain; for example, the domain name www.example.com belongs to the top-level domain *com*.
- The hierarchy of domains descends from right to left; each label to the left specifies a subdivision, or subdomain of the domain to the right. For example: the label *example* specifies a subdomain of the *com* domain, and *www* is a sub domain of example.com. This tree of subdivisions may have up to 127 levels.
- Each label may contain up to 63 characters. The full domain name may not exceed the length of 253 characters in its textual representation. In the internal binary

representation of the DNS the maximum length requires 255 octets of storage, since it also stores the length of the name. In practice, some domain registries may have shorter limits.

- DNS names may technically consist of any character representable in an octet. However, the allowed formulation of domain names in the DNS root zone, and most other sub domains, uses a preferred format and character set. The characters allowed in a label are a subset of the ASCII character set, and includes the characters *a* through *z*, *A* through *Z*, digits *0* through *9*, and the hyphen. This rule is known as the *LDH rule* (letters, digits, hyphen). Domain names are interpreted in case- independent manner. Labels may not start or end with a hyphen. There is an additional rule that essentially requires that top-level domain names not be all-numeric.
- A hostname is a domain name that has at least one IP address associated. For example, the domain names www.example.com and example.com are also hostnames, whereas com is not.

Internationalized domain names

The limited set of ASCII characters permitted in the DNS prevented the representation of names and words of many languages in their native alphabets or scripts. To make this possible, ICANN approved the Internationalizing Domain Names in Applications (IDNA) system, by which user applications, such as web browsers, map Unicode strings into the valid DNS character set using Punycode. In 2009 ICANN approved the installation of internationalized domain name country code top-level domains. In addition, many registries of the existing top level domain names (TLD)s have adopted the IDNA system.

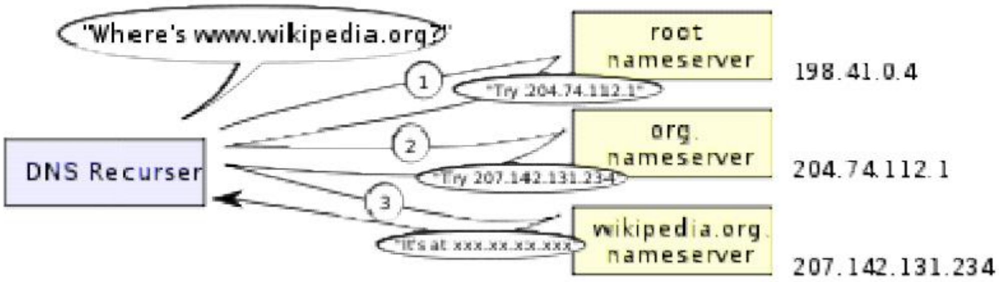
Name servers

The Domain Name System is maintained by a distributed database system, which uses the client-server model. The nodes of this database are the name servers. Each domain has at least one authoritative DNS server that publishes information about that domain and the name servers of any domains subordinate to it. The top of the hierarchy is served by the root name servers, the servers to query when looking up (*resolving*) a TLD.

2.2 Operations

Address resolution mechanism

Domain name resolvers determine the appropriate domain name servers responsible for the domain name in question by a sequence of queries starting with the right-most (top-level) domain label.



A DNS recursor consults three name servers to resolve the address www.wikipedia.org.

The process entails:

1. A network host is configured with an initial cache (so called *hints*) of the known addresses of the root name servers. Such a *hint file* is updated periodically by an administrator from a reliable source.
2. A query to one of the root servers to find the server authoritative for the top-level domain.
3. A query to the obtained TLD server for the address of a DNS server authoritative for the second-level domain.
4. Repetition of the previous step to process each domain name label in sequence, until the final step which returns the IP address of the host sought.

The diagram illustrates this process for the host www.wikipedia.org.

The mechanism in this simple form would place a large operating burden on the root servers, with every search for an address starting by querying one of them. Being as critical as they are to the overall function of the system, such heavy use would create an insurmountable bottleneck for trillions of queries placed every day .In practice caching is used in DNS servers to overcome this problem, and as a result, root name servers actually are involved with very little of the total traffic.

DNS resolvers

The client-side of the DNS is called a DNS resolver. It is responsible for initiating and sequencing the queries that ultimately lead to a full resolution (translation) of the resource sought, e.g., translation of a domain name into an IP address.

A DNS query may be either a non-recursive query or a recursive query:

- A *non-recursive query* is one in which the DNS server provides a record for a domain for which it is authoritative itself, or it provides a partial result without querying other servers.
- A *recursive query* is one for which the DNS server will fully answer the query (or give an error) by querying other name servers as needed. DNS servers are not required to support recursive queries.

The resolver, or another DNS server acting recursively on behalf of the resolver, negotiates use of recursive service using bits in the query headers.

Resolving usually entails iterating through several name servers to find the needed information. However, some resolvers function more simply by communicating only with a single name server. These simple resolvers (called "stub resolvers") rely on a recursive name server to perform the work of finding information for them.

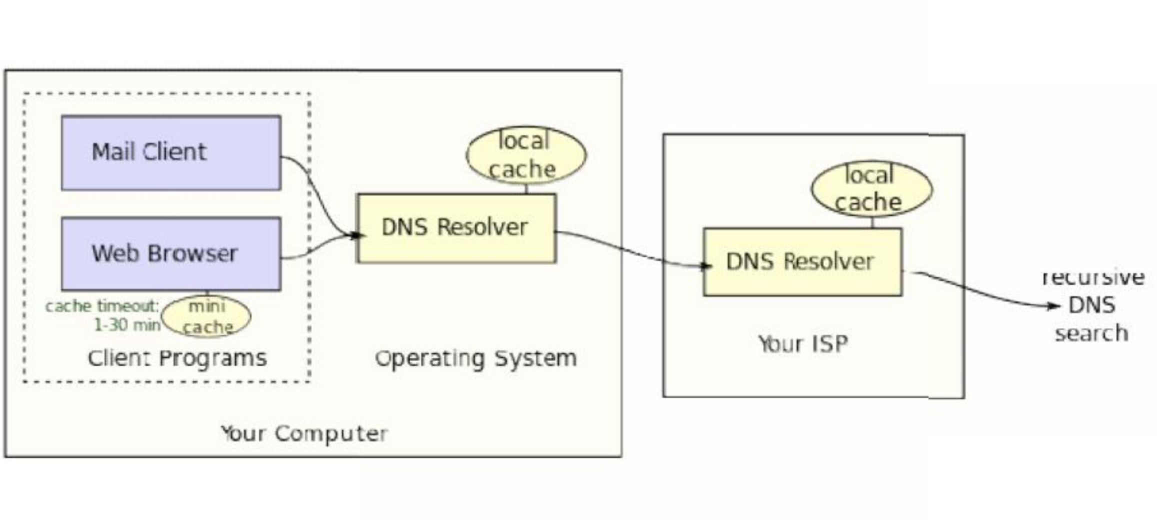
Reverse lookup

A reverse lookup is a query of the DNS for domain names when the IP address is known. Multiple domain names may be associated with an IP address. The DNS stores IP addresses in the form of domain names as specially formatted names in pointer (PTR) records within the infrastructure top-level domain arpa. For IPv4, the domain is in-addr.arpa. For IPv6, the reverse lookup domain is ip6.arpa. The IP address is represented as a name in reverse- ordered octet representation for IPv4, and reverse-ordered nibble representation for IPv6.

When performing a reverse lookup, the DNS client converts the address into these formats before querying the name for a PTR record following the delegation chain as for any DNS query. For example, assuming the IPv4 address 208.80.152.2 is assigned to Wikimedia, it is represented as a DNS name in reverse order: 2.152.80.208.in-addr.arpa.

When the DNS resolver gets a pointer (PTR) request, it begins by querying the root servers, which point to the servers of American Registry for Internet Numbers (ARIN) for the 208.in-addr.arpa zone. ARIN's servers delegate 152.80.208.in-addr.arpa to Wikimedia to which the resolver sends another query for 2.152.80.208.in-addr.arpa, which results in an authoritative response.

Client lookup



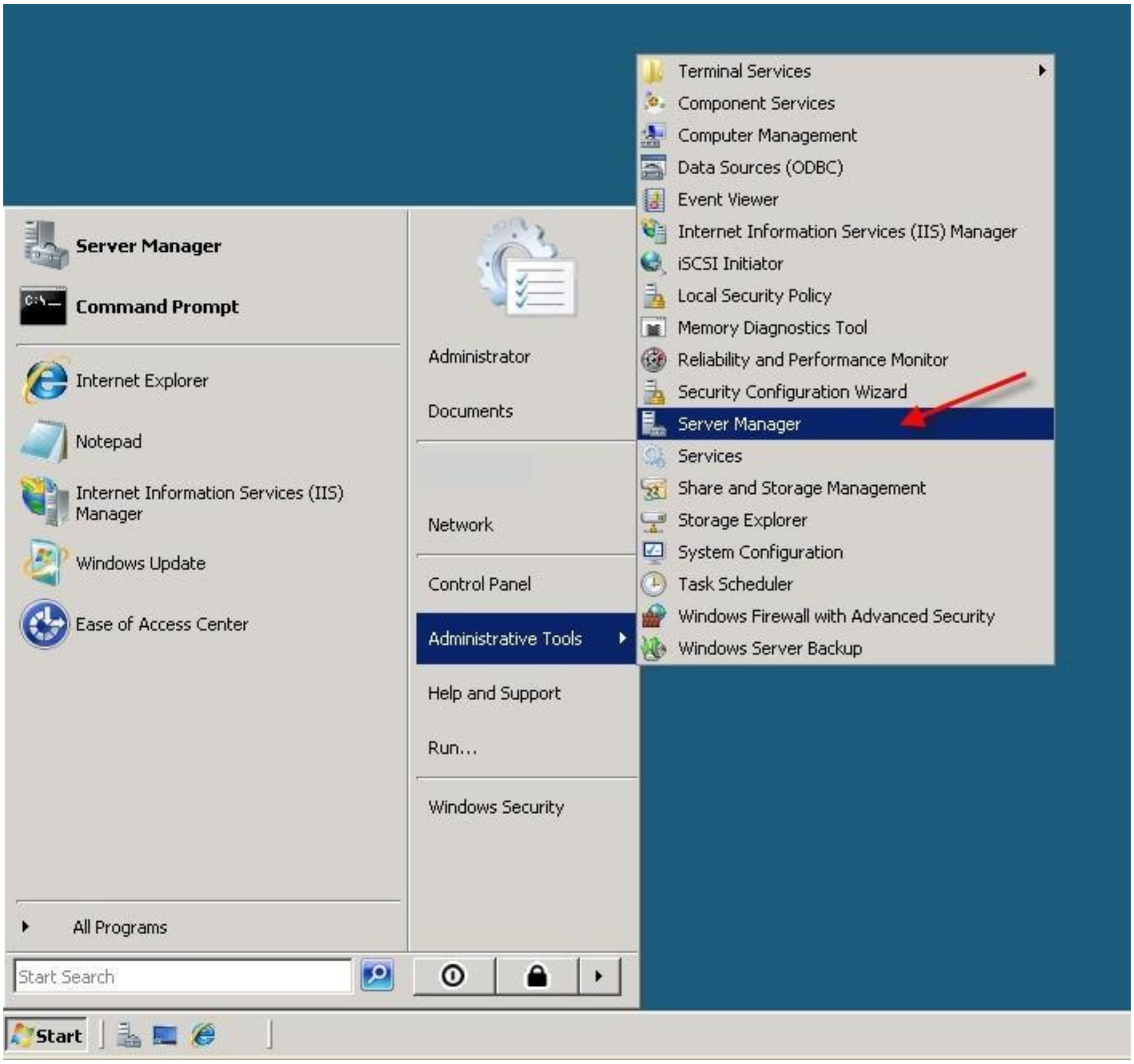
DNS resolution sequence

Users generally do not communicate directly with a DNS resolver. Instead DNS resolution takes place transparently in applications such as web browsers, e-mail clients, and other Internet applications. When an application makes a request that requires a domain name lookup, such programs send a resolution request to the DNS resolver in the local operating system, which in turn handles the communications required.

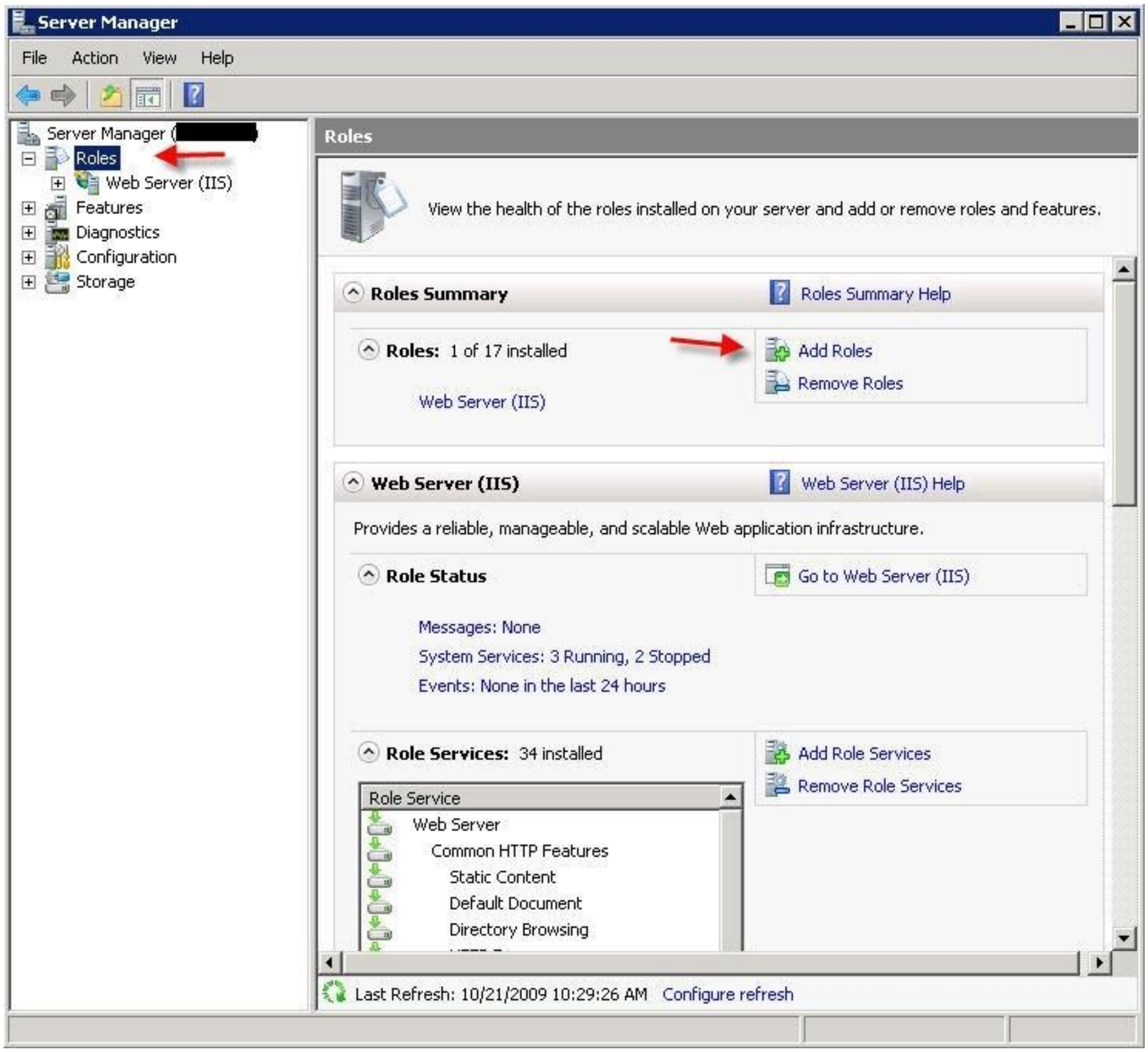
2.3 DNS Server Installation

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

From the Start menu, select ***Administrative Tools*** --> ***Server Manager***.



Expand and click ***Roles*** from the left window. Choose ***Add Roles***



View the health of the roles installed on your server and add or remove roles and features.

Roles: 1 of 17 installed

Web Server (IIS)

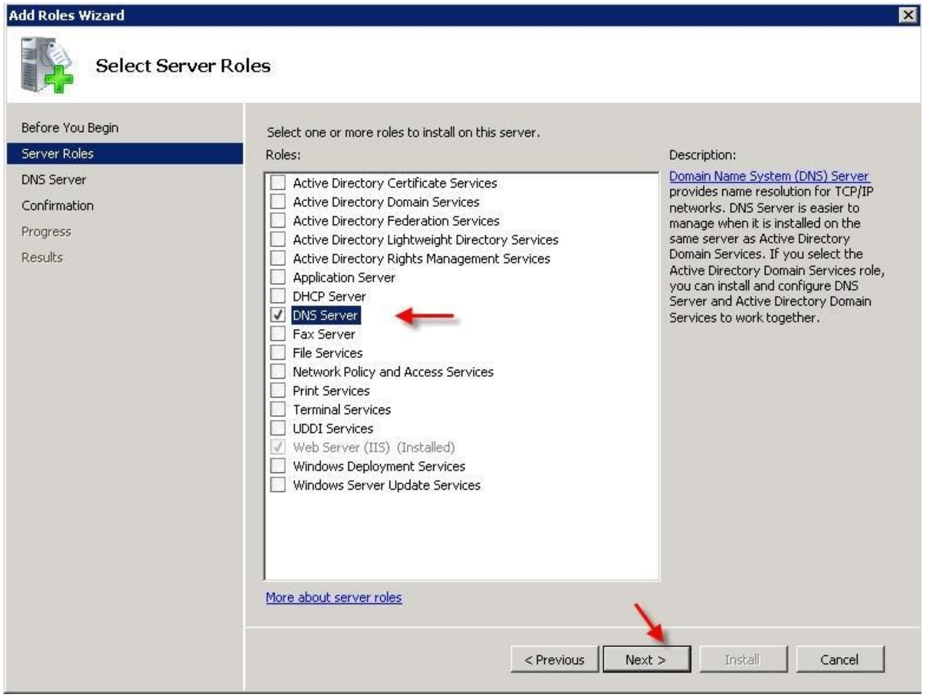
Provides a reliable, manageable, and scalable Web application infrastructure.

Messages: None
System Services: 3 Running, 2 Stopped
Events: None in the last 24 hours

Role Services: 34 installed

Last Refresh: 10/21/2009 10:29:26 AM

Follow the wizard by selecting the ***DNS Server*** role (leave any previously checked items checked)



Add Roles Wizard

Select Server Roles

Select one or more roles to install on this server.

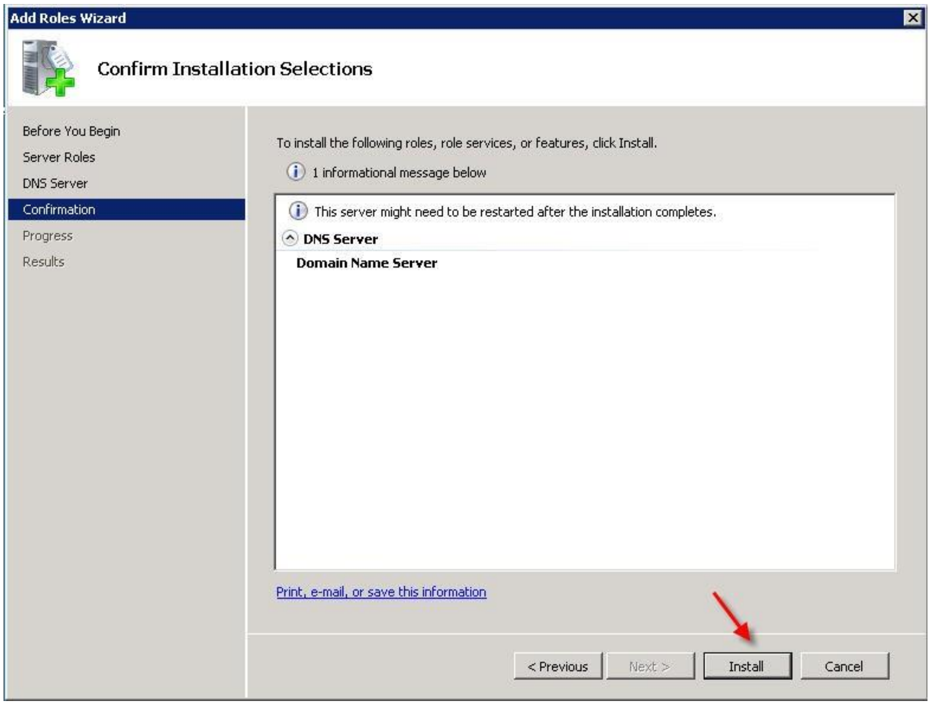
Roles:

- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- ☑ DNS Server
- □ Fax Server
- □ File Services
- □ Network Policy and Access Services
- □ Print Services
- □ Terminal Services
- □ UDDI Services
- ☑ Web Server (IIS) (Installed)
- □ Windows Deployment Services
- □ Windows Server Update Services

Description:

Domain Name System (DNS) Server provides name resolution for TCP/IP networks. DNS Server is easier to manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services role, you can install and configure DNS Server and Active Directory Domain Services to work together.

Click NEXT and then INSTALL to install DNS in Windows Server 2008



Add Roles Wizard

Confirm Installation Selections

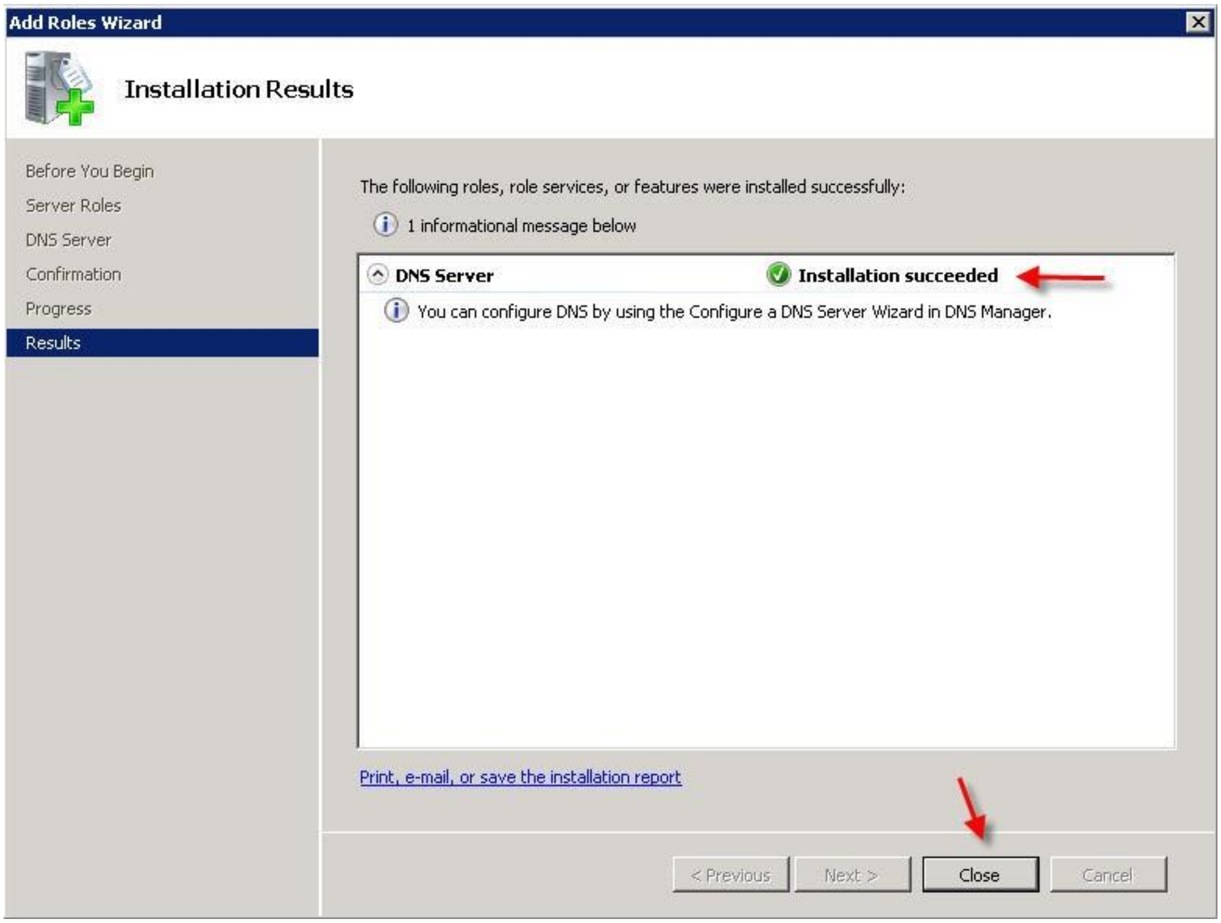
To install the following roles, role services, or features, click Install.

1 informational message below

This server might need to be restarted after the installation completes.

DNS Server

Domain Name Server



The following roles, role services, or features were installed successfully:

1 informational message below

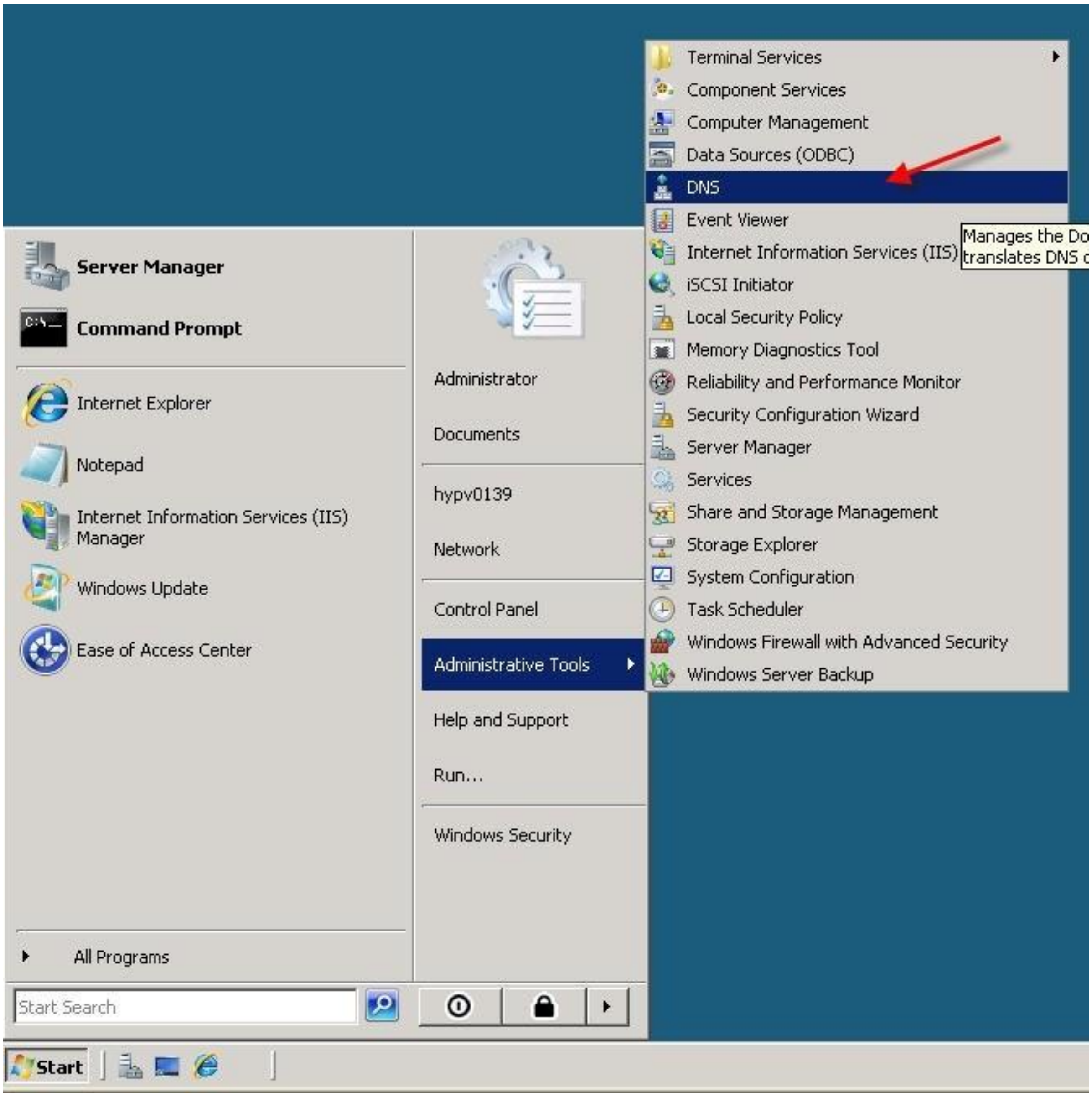
DNS Server ✓ Installation succeeded

You can configure DNS by using the Configure a DNS Server Wizard in DNS Manager.

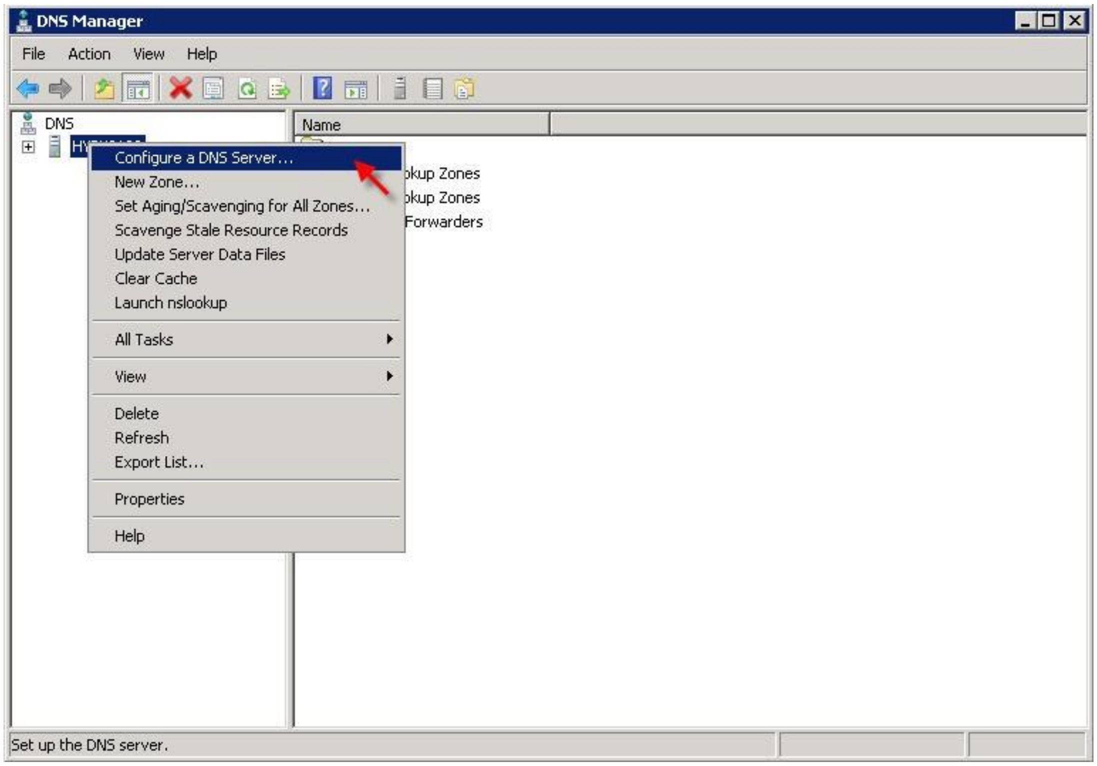
Print, e-mail, or save the installation report

2.4 DNS SERVER CONFIGURATION

From the Start menu, select ***Administrative Tools*** --> ***DNS*** to open the DNS console.

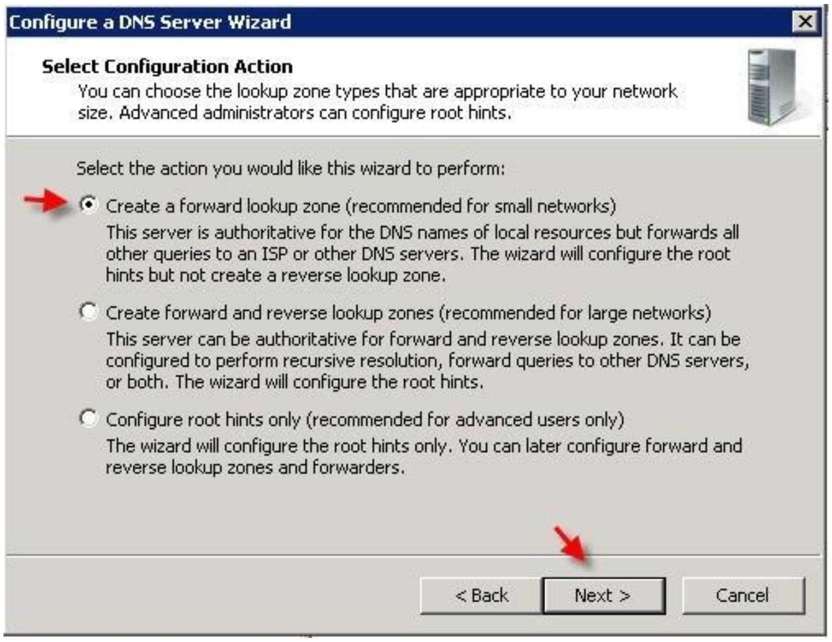


Highlight your computer name and choose **Configure a DNS Server** to launch the Configure DNS Server Wizard.



Set up the DNS server.

Click NEXT and then select the first option, ***Create a Forward lookup zone***



Select Configuration Action

You can choose the lookup zone types that are appropriate to your network size. Advanced administrators can configure root hints.

Select the action you would like this wizard to perform:

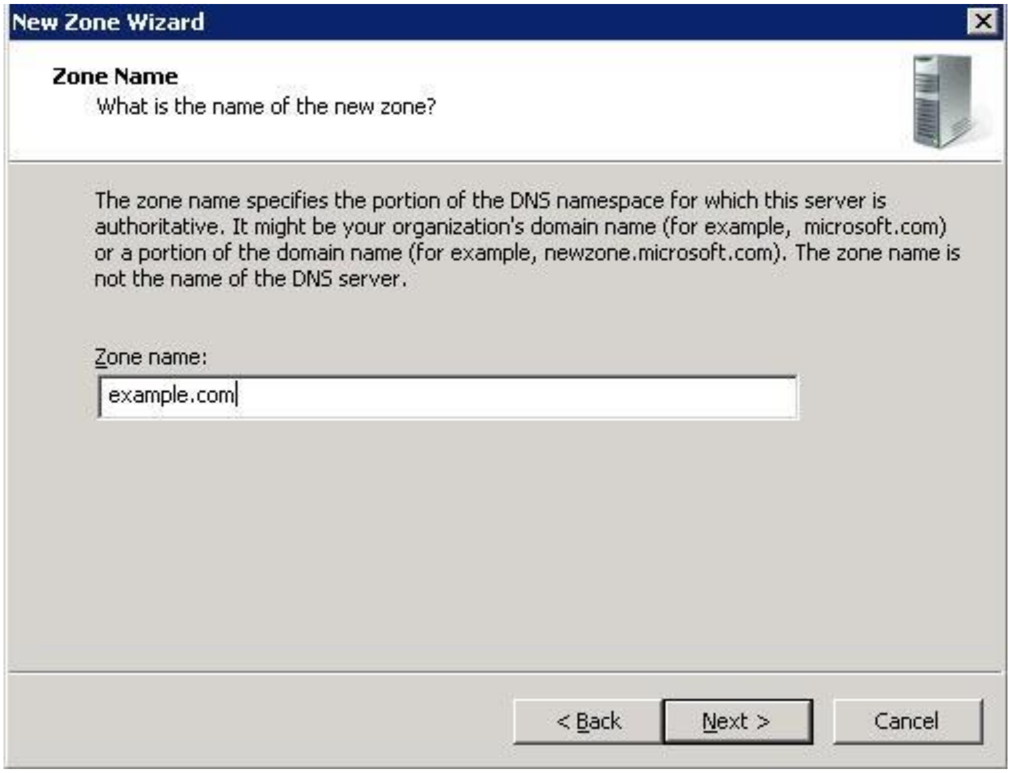
● Create a forward lookup zone (recommended for small networks)
This server is authoritative for the DNS names of local resources but forwards all other queries to an ISP or other DNS servers. The wizard will configure the root hints but not create a reverse lookup zone.

○ Create forward and reverse lookup zones (recommended for large networks)
This server can be authoritative for forward and reverse lookup zones. It can be configured to perform recursive resolution, forward queries to other DNS servers, or both. The wizard will configure the root hints.

○ Configure root hints only (recommended for advanced users only)
The wizard will configure the root hints only. You can later configure forward and reverse lookup zones and forwarders.

On the next screen, leave the default option selected, This Server maintains the zone, and click NEXT

Now you will need to enter the domain name that you want to create your first zone file for. We are using "example.com" in this tutorial:



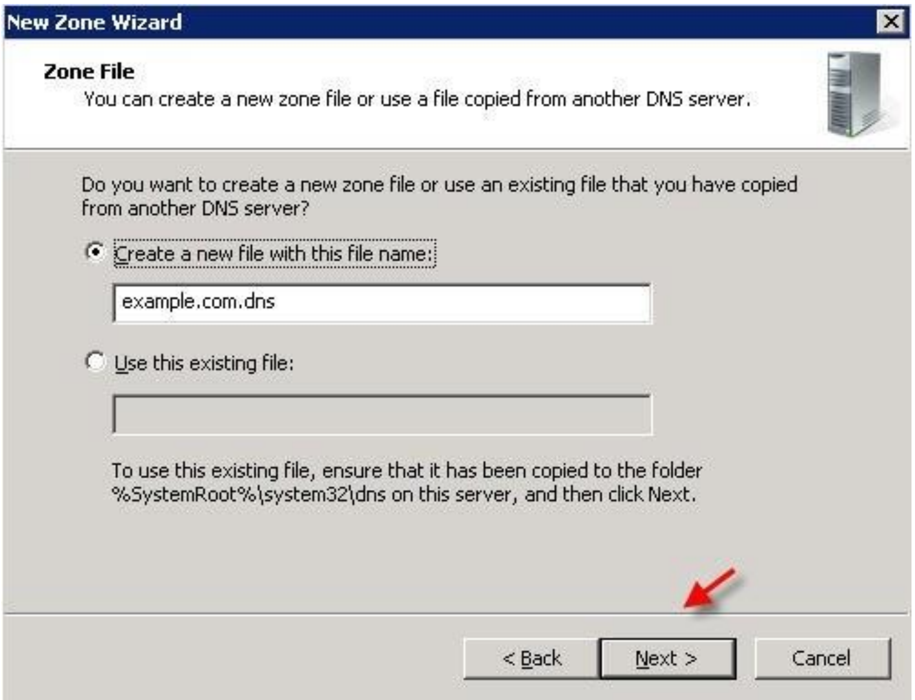
Zone Name

What is the name of the new zone?

The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.

Zone name: example.com

Click NEXT, and NEXT again on the next two screens



New Zone Wizard

Zone File

You can create a new zone file or use a file copied from another DNS server.

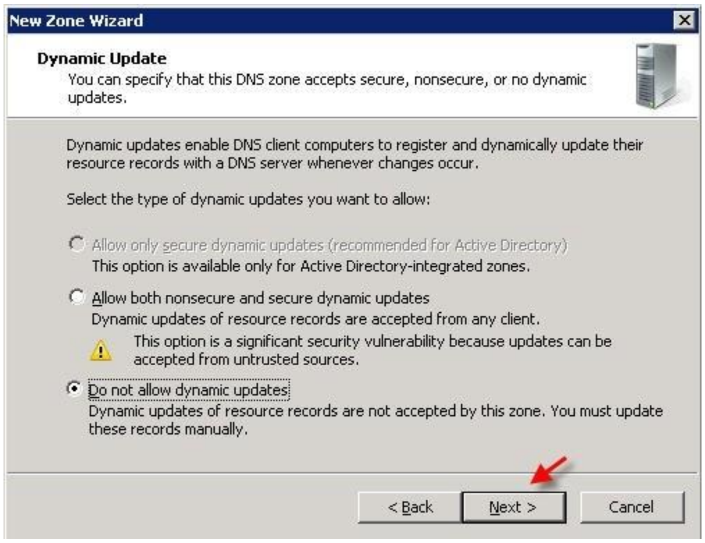
Do you want to create a new zone file or use an existing file that you have copied from another DNS server?

● Create a new file with this file name:

example.com.dns

○ Use this existing file:

To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.



New Zone Wizard

Dynamic Update

You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.

Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

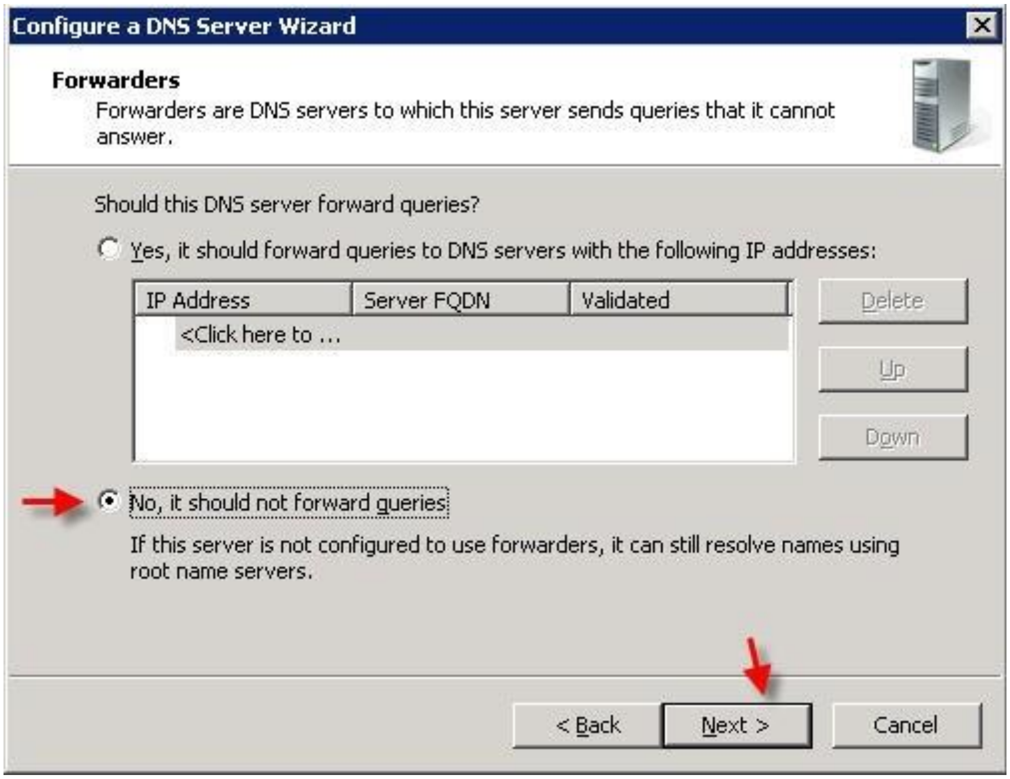
Select the type of dynamic updates you want to allow:

○ Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.

○ Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
⚠ This option is a significant security vulnerability because updates can be accepted from untrusted sources.

● Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

On the Forwarders screen, select the option "***No, it should not forward queries***



Forwarders

Forwarders are DNS servers to which this server sends queries that it cannot answer.

Should this DNS server forward queries?

○ Yes, it should forward queries to DNS servers with the following IP addresses:

IP Address	Server FQDN	Validated
<Click here to ...		

● No, it should not forward queries

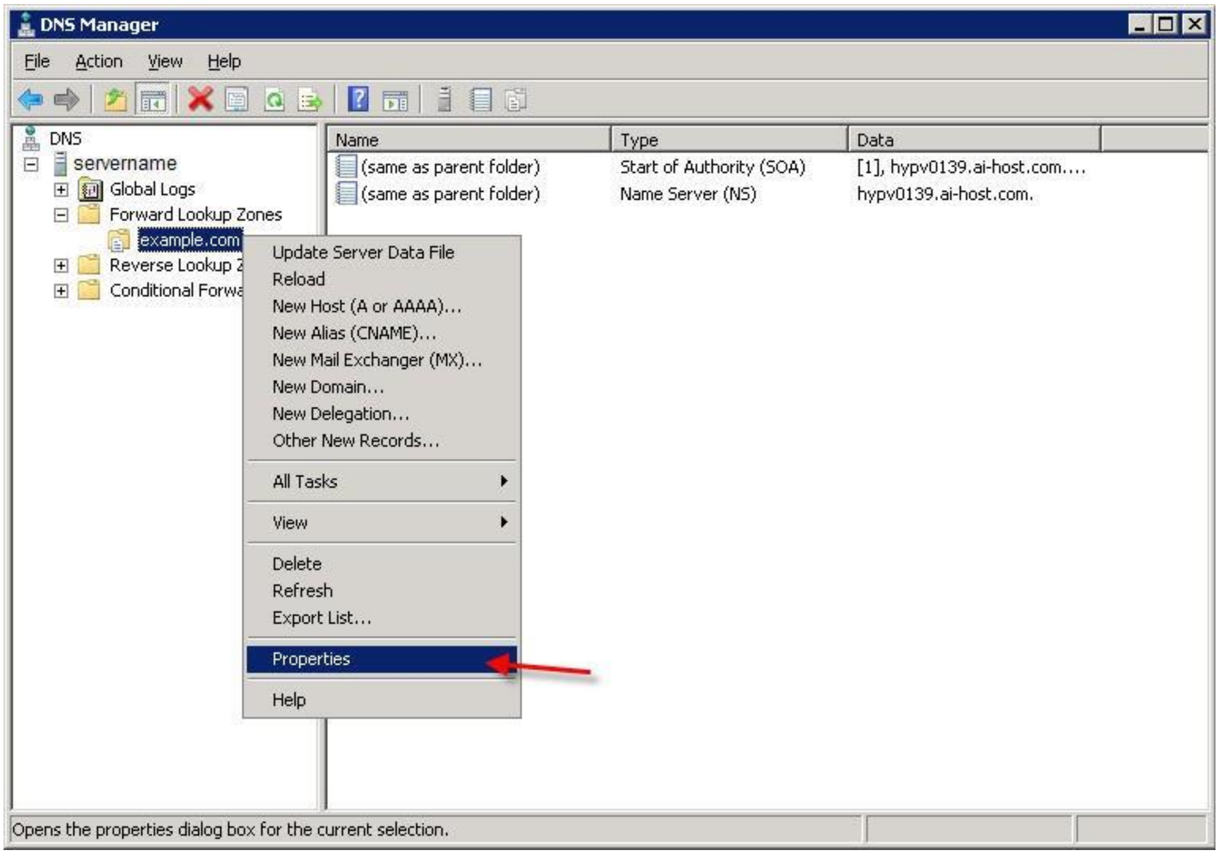
If this server is not configured to use forwarders, it can still resolve names using root name servers.

Click **FINISH**

2.5 MANAGING DNS RECORDS

There are many types of DNS records, this is a basic tutorial and will show you how to point your domain name to the IP address you assigned to your web site via an A record. You can also create other types of DNS records (MX, CNAME,etc) in a similar fashion.

In ***DNS Manager***, expand your server name, then expand the ***'Forward Lookup Zones'*** , right-click on your domain name and select ***Properties***

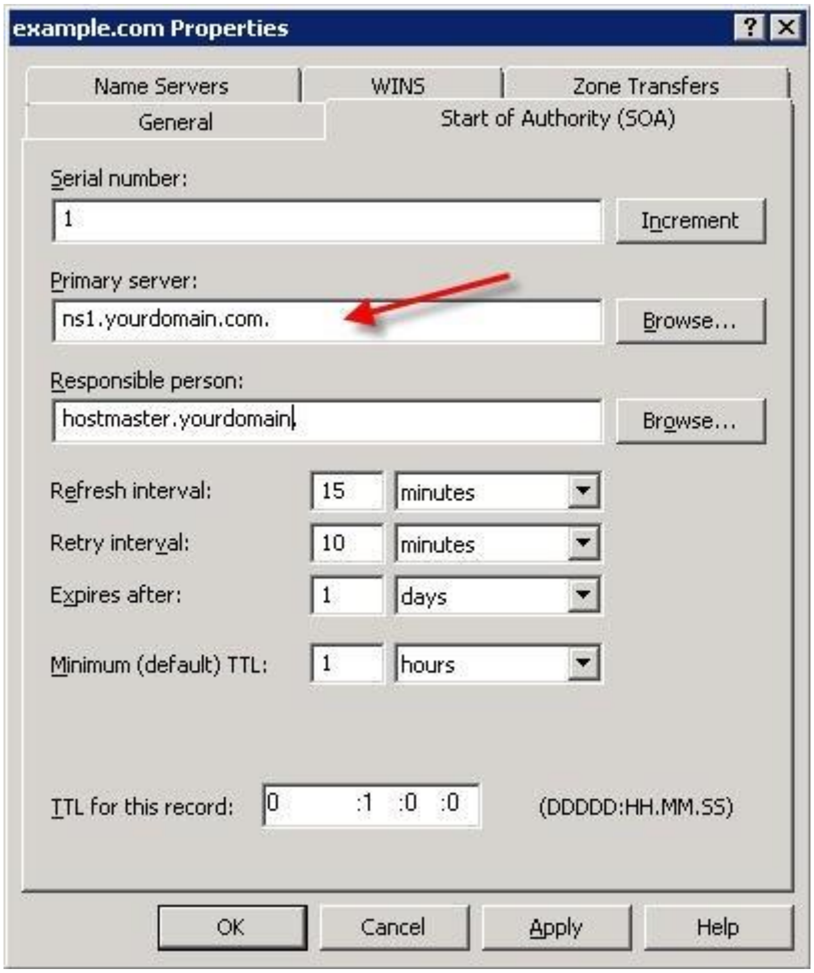


Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[1], hypv0139.ai-host.com....
(same as parent folder)	Name Server (NS)	hypv0139.ai-host.com.

Opens the properties dialog box for the current selection.

Click on the ***Start of Authority (SOA) tab***.

The SOA resource record is always the first record in a DNS zone. Set the Primary Server to your primary nameserver:



example.com Properties

Serial number: 1

Primary server: ns1.yourdomain.com.

Responsible person: hostmaster.yourdomain

Refresh interval: 15 minutes

Retry interval: 10 minutes

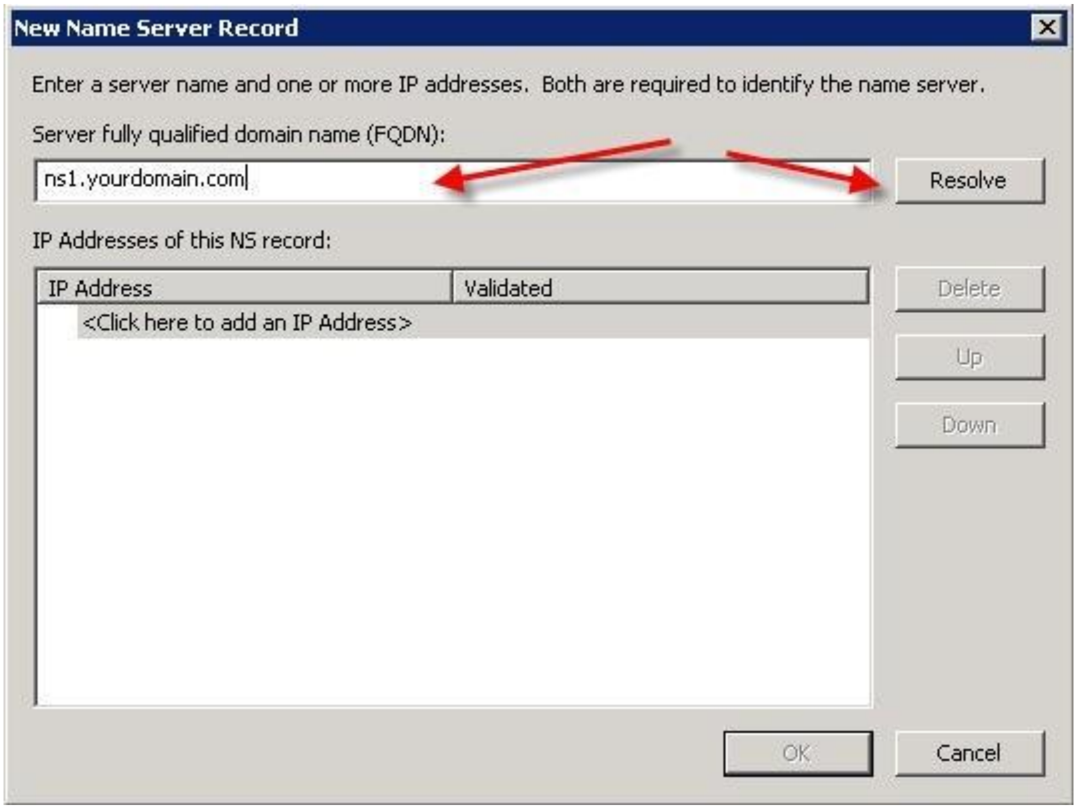
Expires after: 1 days

Minimum (default) TTL: 1 hours

TTL for this record: 0 :1 :0 :0 (DDDDD:HH.MM.SS)

Next, click on the ***Name Servers*** tab.

Remove anything currently listed, and click **Add** and enter your nameservers (i.e. - ns1.yourdomain.com , ns2.yourdomain.com)



New Name Server Record

Enter a server name and one or more IP addresses. Both are required to identify the name server.

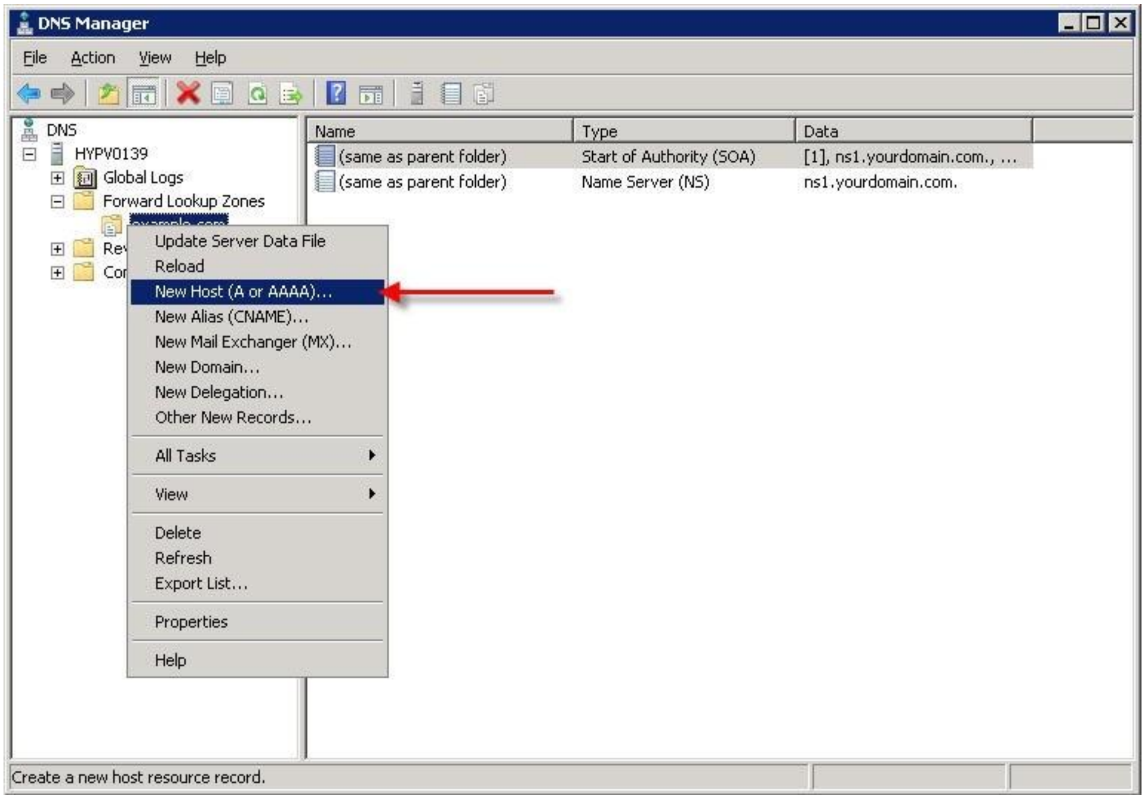
Server fully qualified domain name (FQDN): ns1.yourdomain.com

IP Addresses of this NS record:

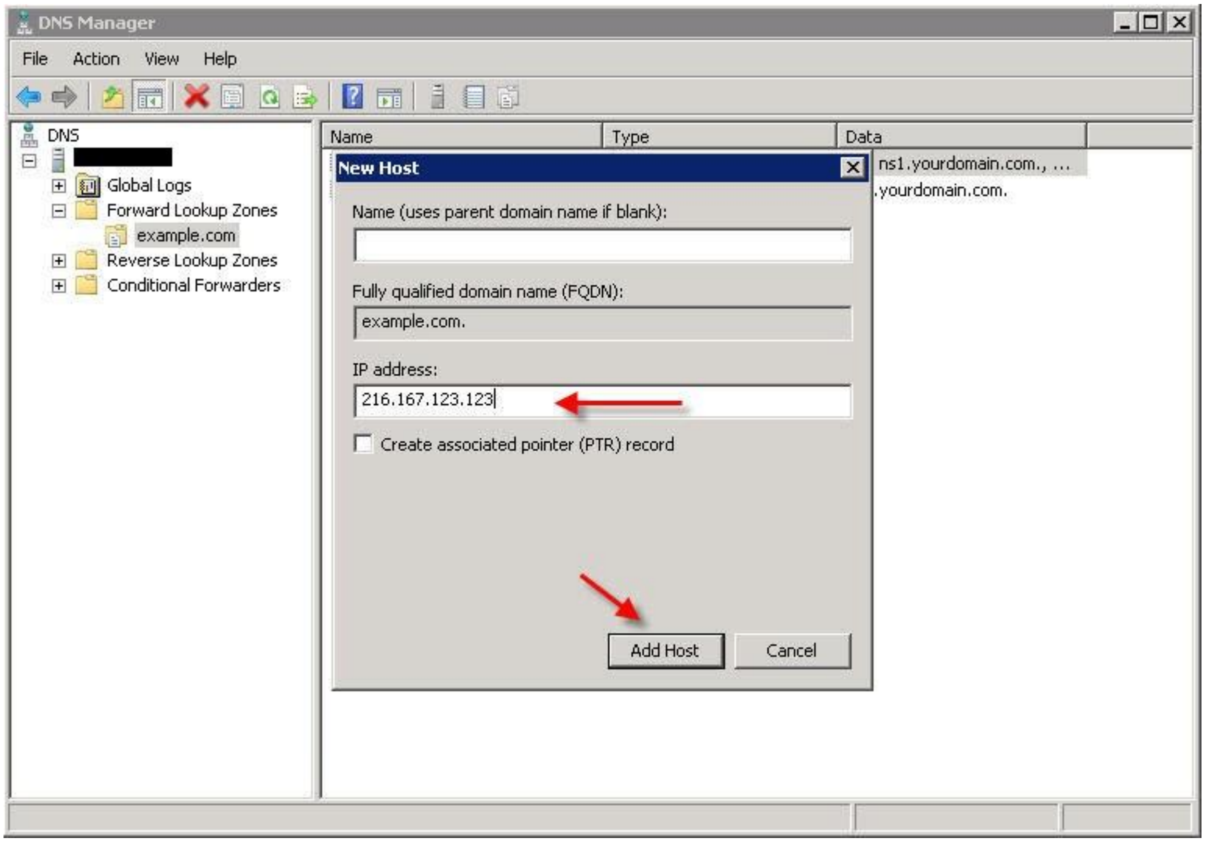
IP Address	Validated
<Click here to add an IP Address>	

When done, click OK to close the window. You are now ready to set up your zone records.

Right-click on your domain name under ***Forward Lookup Zones***, and select **New Host (A or AAAA)…**



Leave the ***Name*** field blank, and under ***IP Address***, enter the IP address you configured for this web site in IIS, and click **Add Host**.



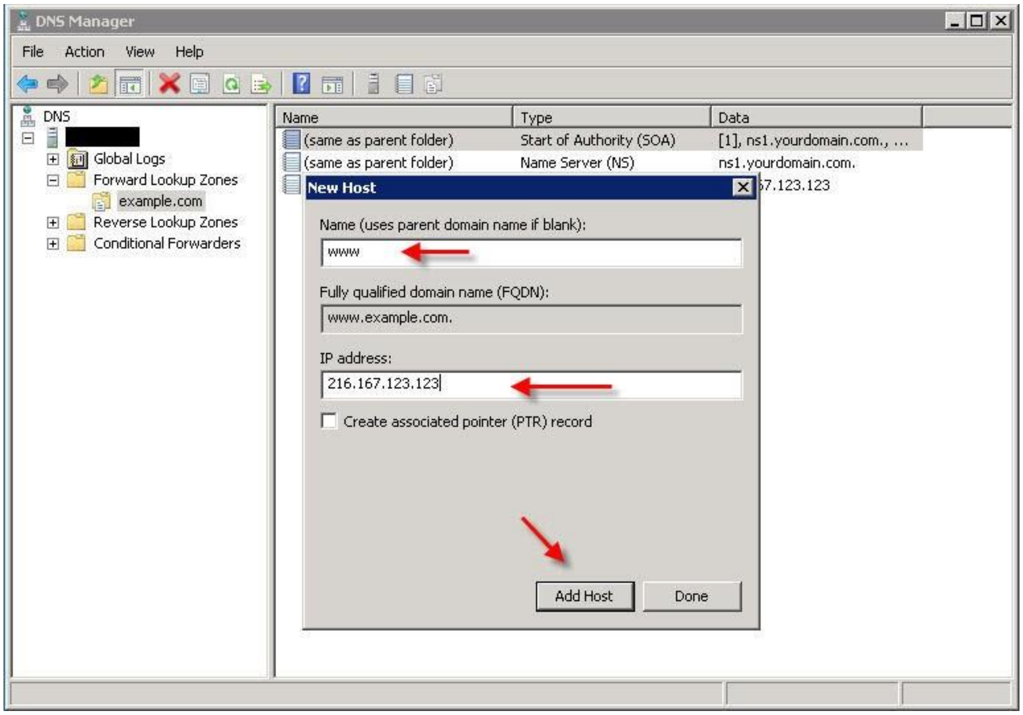
Name (uses parent domain name if blank):

Fully qualified domain name (FQDN): example.com.

IP address: 216.167.123.123

☐ Create associated pointer (PTR) record

You will most likely also want to make a record for 'www', so repeat the above step but this time instead of leaving the ***Name*** field blank, enter www in that field:



Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[1], ns1.yourdomain.com., ...
(same as parent folder)	Name Server (NS)	ns1.yourdomain.com.
		57.123.123

New Host

Name (uses parent domain name if blank): www

Fully qualified domain name (FQDN): www.example.com.

IP address: 216.167.123.123

☐ Create associated pointer (PTR) record

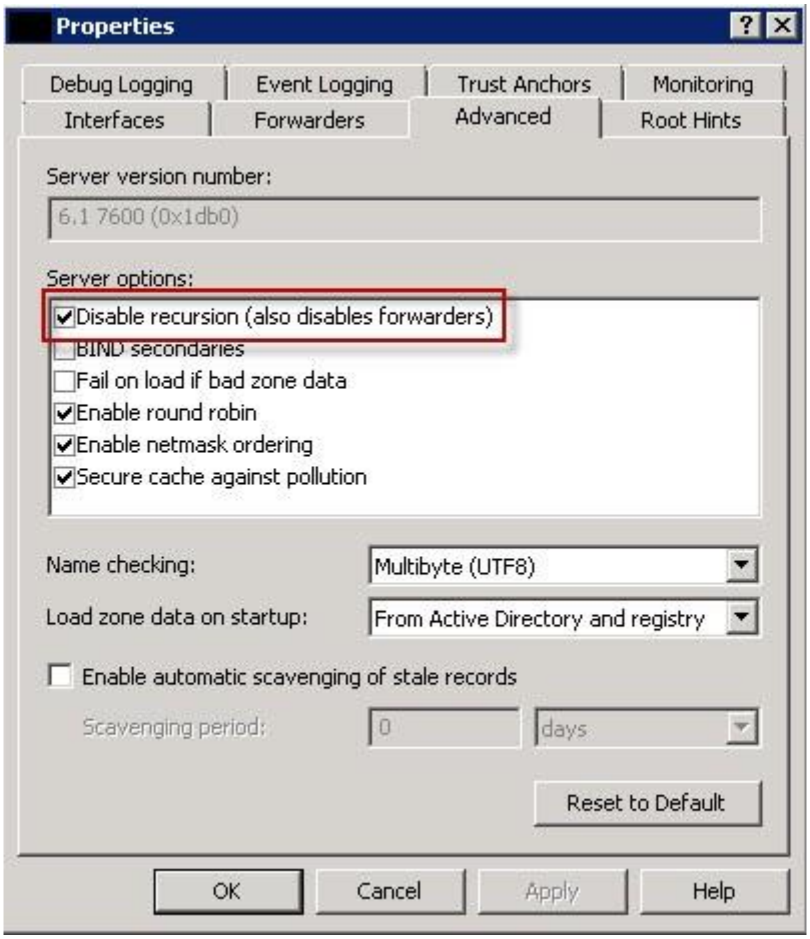
2.6 Disable DNS Recursion

The final step you'll want to perform is to disable DNS recursion. This will help secure your server from a variety of DNS recursion attacks.

To disable recursion, **right-click on your DNS server** and go to

'**Properties**'. Click the '**Advanced**' tab.

Then check the box labeled "**Disable recursion**"



Server version number: 6.1 7600 (0x1db0)

Server options:

- ☑ Disable recursion (also disables forwarders)
- ☐ BIND secondaries
- ☐ Fail on load if bad zone data
- ☑ Enable round robin
- ☑ Enable netmask ordering
- ☑ Secure cache against pollution

Name checking: Multibyte (UTF8)

Load zone data on startup: From Active Directory and registry

☐ Enable automatic scavenging of stale records

Scavenging period: 0 days

You have now set up DNS in Windows Server 2008 and have set up DNS records for your domain name.

You can create additional DNS records as needed (MX, CNAME, etc) by right-clicking on the domain under Forward Lookup Zones and selecting the appropriate type of record you wish to create.You can test that your DNS server is properly serving DNS from a Windows command prompt, by using the nslookup command in this format:

nslookup example.com ns1.yourdomain.com