Internship report

On Infolink

Networking and Solution

Prepared by

Q.M. Shahadat Hossain

2010-1-55-009

Supervised by

Mr. Mustafa Mahmud Hussain

Assistant Professor,
Dept. of Electronics and Communications Engineering

EAST WEST UNIVERSITY

Kamrul Shaker

System Admin, Infolink

Infolink

Declaration

This is to certify that, this Internship report prepared by me under the course Internship Program (ETE-498). It has not been submitted elsewhere for the requirement of any Diploma, Undergraduate or Graduate program or any other purposes.

Q.M. Shahadat Hossain

2010-1-55-009

Acceptance

An internship report is submitted to the department of Electronics and Communications Engineering, East West University in partial fulfillment of the requirement for the degree of Bachelor of Science in Electronics & Telecommunication Engineering.

Mr. Mustafa Mahmud Hussain
Assistant Professor
Department of ECE
East West University

Acknowledgement

First of all I wish to convey our heartfelt thanks and gratitude to Almighty Allah to complete the internship successfully and also those who all rendered their cooperation in making this report. Without their assistance I could not have completed our internship.

I thank and express my gratitude to **Mr. Mustafa Mahmud Hussain,** Assistant Professor, Department of Electronics and Communications Engineering (ECE), East West University, Dhaka. I have been working under his supervision, and he has been guiding me with a lot of effort and time. I would also like to thank for giving me opportunity to do internship with Infolink IT solution company Ltd. and all of my honorable colleagues.

I am very grateful to **Dr. Gurudas Mandal** Chairperson and Associate Professor, Department of Electronics and Communications Engineering (ECE), East West University, Dhaka for being so kind and helpful during the period of my Internship program as well as my academic period. For his kind effort I am going to complete our B.S.C. program.

I am also very grateful to all of my teachers and fellow friends for their encouragement and cooperation throughout my internship and my academic life. A special thank to those who were with me during the glorious years of learning and achieving this success.

Finally I am forever grateful to my parents for their patience and love.

Abstract

I've done my internship in **Network optimization center (NOC)** of **Infolink.** Focus of the department is network design, implementation, support and solution.

My task was configuring CPE; configuring Routers, switches; Site Survey and design of network structures of Corporate Clients. In the later portion of my internship I was also involved in Research and Development with particular topic.

Throughout my internship period I was always experiencing the practical implementation of networking topics covered in my academic courses. This internship helped me a lot. Now I'm confident that I could efficiently work in Networking Industry with my full dedication.

Infolink

Corporate Office: Road#12, House#19, (1st Floor), Baridhara, Dhaka-1212, Bangladesh.

Jamuna Office: Shop#4D-010, 4th Floor, Jamuna Future Park, KA-244,Kuril, Progoti Sharani, Baridhara, Dhaka-1229, Bangladesh.

Phone: +88-019-INFOLINK (46365465)
Phone: +88-096-10994998
Phone: +88-017-14420001

Support E-Mail: support@infolinkbd.com
Admin E-Mail: info@infolinkbd.com
Career E-Mail: career@infolinkbd.com

About Infolink

Infolink is an IT solution company. Infolink started its journey with aim of providing very high level software and technology support. The Company has developed with very talented force of IT experts who are creative and forward thinking in their approach. They are always ready to provide proper IT related solution based on clients demand. Infolink believe in quality and service because, quality and service creates its own demand. Infolink pricing is neither cheap nor high.

In Infolink members work like a family. Each member stands with his professional identity and also with lots of respect to others. In this Infolink Family everyone is very committed and responsible to his work. Regular weekly and monthly round table meetings enhance work speed and relationship. Infolink encourage their members to spend few portion of their time to develop creativity, planning ability etc. Infolink in all respect choose the simple and straight way.It try to makes everything clear to it's clients. Infolink software engineers and testing department ensure the highest level of work membership. Such transparency in operation pays back through giving a very strong foundation to the confidence of the people who deals with Infolink.

Upcoming Services of Infolink

- High-speedInternet service.
- Mobile IP Telephony.
- Live IP TV.
- E-Learning.
- Video Conferencing.
- Secured VPN
- ATM Connectivity
- IP PABX.
- Online Radio.
- Audio-Video Streaming.
- Tele Medicine.
- MAN for Corporate offices having presence in different locations.
- Remote Surveillance
- Online Gaming Service etc.

Round the Clock Customer Care

- 24x7 Hotline.
- Live Support.
- Quick response to queries.
- Dedicated support team.
- Web Based Self care

Table of Contents

Introduction

In the world of computers, **networking** is the practice of linking two or more computing devices together for the purpose of sharing data. Networks are built with a mix of computer hardware and computer software.

Network engineers are responsible for configuring devices, optimizing, installing, maintaining and supporting computer communication networks within an organisation or between organisations. Their goal is to ensure the smooth operation of communication networks in order to provide maximum performance, security of data transection and availability for their users, such as staff, clients, customers and suppliers.

This report is about my internship at **Infolink** covering a period of 3 months. I worked here as a Network Engineer. Especially I must say the project of Network Configuration and Implementation of jamuna future park were the big project of my Internship period. As I have a great interest in networking I enjoyed this period of internship at Infolink, IT Solution Company Limited and in this report I tried to describe thing I have learned from this internship.

In Infolink there is some device which is use to communicate between host and clients

I. DHCP Server.
II. AAA Server
III. DNS Server.
IV. Router and backup router
V. Switch and backup switch.
VI. Power stabilizer and backup batteries.

AAA Server

An AAA server refers to the process of authentication, authorization and accounting utilized by the Remote Authentication Dial In User Services (RADIUS) network protocol. RADIUS permits remote users or computers to access a computerized network server. When the AAA server process is not required, a server is called "open" or "anonymous." RADIUS and AAA server protocol is usually used by internet service providers (ISPs) to identify and bill their clients. It is also used by companies to identify and allow network access to their employees when they are working from a remote location.

When a user sends a request for access to a network server from a remote location, it must identify itself to the server. The request is usually composed of "credentials," which usually take the form of a username and password or passphrase. The request also sends information such as a dial-up phone number or network address for the network to verify the user's identity. The network checks the user's information against its database.

Once the user's identity is verified, the network sends back a response of either "access rejected," "access challenged" or "access accepted." If access is rejected, the user is totally denied access to the network, usually because of unconfirmed or invalid credentials. If access is challenged, the network will ask for additional information in order to verify the user. Usually, this occurs in networks with a higher level of security. If access is accepted, the user is authenticated, and given access to the network

Authentication types

Authentication has several purposes in networking:

1. Verify the user trying to connect (user authentication), to validate:

   (s)he really belongs to that Network Service Provider (NSP) and can be billed for the connection is really entitled to connect in that network and access the company intranet (orIP network), for non-billing networks.

2. For the user to verify (s)he connecting to the correct network, and not to a hacker's network (network authentication).

Optionally, device authentication. To verify the device (handset, CPE, PCMCIA card etc.) identity (Ethernet MAC address) is valid and hasn't been modified or tampered with. Based on this device ID (MAC) it can be decided to authorize that device into the network, if it is not in a black list (hasn't been stolen, for instance).

These air interface encryption keys are dynamically generated between the user and the AAA (RADIUS) server when the user starts the session. But in order to have the best possible security, these keys should be dynamically changed. This imply doing a user reauthentication periodically (every 30 min, every hour, etc.).

Configuring Login Authentication Using AAA

The AAA security services facilitate a variety of login authentication methods. Use the **aaa authentication login** command to enable AAA authentication no matter which of the supported login authentication methods you decide to use. With the **aaa authentication login** command, we create one or more lists of authentication methods that are tried at login. These lists are applied using the **login authentication** line configuration command.

To configure login authentication by using AAA, used the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# **aaa new-model**	Enables AAA globally.
Step 2	Router(config)# **aaa authentication login**{**default** | *list-name*} *method1* [*method2*	Creates a local authentication list.
Step 3	Router(config)# **line** [**aux** | **console** | **tty**| **vty**] **line-number** [**ending-line-number**]	Enters line configuration mode for the lines to which we want to apply the authentication list.
Step 4	Router(config-line)# **login authentication** {**default** | *list-name*}	Applies the authentication list to a line or set of lines.

DHCP Server

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway. RFCs 2131 and 2132 define DHCP as an Internet Engineering Task Force (IETF) standard based on Bootstrap Protocol (BOOTP), a protocol with which DHCP shares many implementation details. DHCP allows hosts to obtain necessary TCP/IP configuration information from a DHCP server.

Benefits of DHCP

- **Reliable IP address configuration**. DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, or address conflicts caused by the assignment of an IP address to more than one computer at the same time.
- **Reduced network administration.** DHCP includes the following features to reduce network administration:
  - Centralized and automated TCP/IP configuration.
  - The ability to define TCP/IP configurations from a central location.
  - The ability to assign a full range of additional TCP/IP configuration values by means of DHCP options.
  - The efficient handling of IP address changes for clients that must be updated frequently, such as those for portable computers that move to different locations on a wireless network.
  - The forwarding of initial DHCP messages by using a DHCP relay agent, thus eliminating the need to have a DHCP server on every subnet.

Why use DHCP

Every device on a TCP/IP-based network must have a unique unicast IP address to access the network and its resources. Without DHCP, IP addresses must be configured manually for new computers or computers that are moved from one subnet to another, and manually reclaimed for computers that are removed from the network.

DHCP enables this entire process to be automated and managed centrally. The DHCP server maintains a pool of IP addresses and leases an address to any DHCP-enabled client when it starts up on the network. Because the IP addresses are dynamic (leased) rather than static (permanently assigned), addresses no longer in use are automatically returned to the pool for reallocation.

The network administrator establishes DHCP servers that maintain TCP/IP configuration information and provide address configuration to DHCP-enabled clients in the form of a lease offer. The DHCP server stores the configuration information in a database, which includes:

- Valid TCP/IP configuration parameters for all clients on the network.
- Valid IP addresses, maintained in a pool for assignment to clients, as well as excluded addresses.
- Reserved IP addresses associated with particular DHCP clients. This allows consistent assignment of a single IP address to a single DHCP client.
- The lease duration, or the length of time for which the IP address can be used before a lease renewal is required.

A DHCP-enabled client, upon accepting a lease offer, receives:

- A valid IP address for the subnet to which it is connecting.
- Requested DHCP options, which are additional parameters that a DHCP server is configured to assign to clients. Some examples of DHCP options are Router (default gateway), DNS Servers, and DNS Domain Name. For a full list of DHCP options, see "DHCP Tools and Settings."

DHCP Terms and Definitions

Term	Definition
DHCP server	A computer running the DHCP Server service that holds information about available IP addresses and related configuration information as defined by the DHCP administrator and responds to requests from DHCP clients.
DHCP client	A computer that gets its IP configuration information by using DHCP.
Scope	A range of IP addresses that are available to be leased to DHCP clients by the DHCP Server service.

Subnetting	The process of partitioning a single TCP/IP network into a number of separate network segments called subnets.
DHCP option	Configuration parameters that a DHCP server assigns to clients. Most DHCP options are predefined, based on optional parameters defined in Request for Comments (RFC) 2132, although extended options can be added by vendors or users.
Lease	The length of time for which a DHCP client can use a DHCP-assigned IP address configuration.
Reservation	A specific IP address within a scope permanently set aside for leased use by a specific DHCP client. Client reservations are made in the DHCP database using the DHCP snap-in and are based on a unique client device identifier for each reserved entry.
Exclusion/exclusion range	One or more IP addresses within a DHCP scope that are not allocated by the DHCP Server service. Exclusions ensure that the specified IP addresses will not be offered to clients by the DHCP server as part of the general address pool.
DHCP relay agent	Either a host or an IP router that listens for DHCP client messages being broadcast on a subnet and then forwards those DHCP messages directly to a configured DHCP server. The DHCP server sends DHCP response messages directly back to the DHCP relay agent, which then forwards them to the DHCP client. The DHCP administrator uses DHCP relay agents to centralize DHCP servers, avoiding the need for a DHCP server on each subnet. Also referred to as a BOOTP relay agent.
Superscope	A configuration that allows a DHCP server to provide leases from more than one scope to clients on a single physical network segment.
Multicast IP addresses	Multicast IP addresses allow multiple clients to receive data that is sent to a single IP address, enabling point-to-multipoint communication. This type of transmission is often used for streaming media transmissions, such as video conferencing.

Multicast Scope	A range of multicast IP addresses that can be assigned to DHCP clients. A multicast scope allows dynamic allocation of multicast IP addresses for use on the network by using the MADCAP protocol, as defined in RFC 2730.
BOOTP	An older protocol with similar functionality; DHCP is based on BOOTP. BOOTP is an established protocol standard used for configuring IP hosts. BOOTP was originally designed to enable boot configuration for diskless workstations.

Configuring a DHCP Database Agent or Disabling Conflict Logging

Perform this task to configure a DHCP database agent.

A DHCP database agent is any host (for example, an FTP, TFTP, or rcp server) or storage media on the DHCP server (for example, disk0) that stores the DHCP bindings database. We can configure multiple DHCP database agents, and can configure the interval between database updates and transfers for each agent.

Automatic bindings are IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database. Automatic binding information (such as lease expiration date and time, interface index, and VPN routing and forwarding [VRF] name) is stored on a database agent. The bindings are saved as text records for easy maintenance.

An address conflict occurs when two hosts use the same IP address. During address assignment, DHCP checks for conflicts using ping and gratuitous Address Resolution Protocol (ARP). If a conflict is detected, the address is removed from the pool. The address will not be assigned until the administrator resolves the conflict.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enabl	Enables privileged EXEC mode. • Enter password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	Do one of the following • **ip dhcp database** *url* [**timeout** *seconds* | **write-delay** *seconds*] • or • **no ip dhcp conflict logging** **Example:** Router(config)# ip dhcp database ftp://user:password@172.16.1.1/router-dhcp timeout 80 **Example:** Router(config)# no ip dhcp conflict logging	Configures a DHCP server to save automatic bindings on a remote host called a database agent. or Disables DHCP address conflict logging.

Excluding IP Addresses

Perform this task to specify IP addresses (excluded addresses) that the DHCP server should not assign to clients.

The IP address configured on the router interface is automatically excluded from the DHCP address pool. The DHCP server assumes that all other IP addresses in a DHCP address pool subnet are available for assigning to DHCP clients.

We need to exclude addresses from the pool if the DHCP server should not allocate those IP addresses. An example usage scenario is when two DHCP servers are set up to service the same network segment (subnet) for redundancy. If the two DHCP servers do not coordinate their services with each other using a protocol such as DHCP failover, then each DHCP server must be configured to allocate from a nonoverlapping set of addresses in the shared subnet. Here the "Configuring Manual Bindings Example" section for a configuration example

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**ip dhcp excluded-address** *low-address* [*high-address*] **Example:** Router(config)# ip dhcp excluded-address 172.16.1.100 172.16.1.103	Specifies the IP addresses that the DHCP server should not assign to DHCP clients.

Configuring a DHCP Address Pool

Perform this task to configure a DHCP address pool. On a per-address pool basis, specify DHCP options for the client as necessary.

We can configure a DHCP address pool with a name that is a symbolic string (such as "engineering") or an integer (such as 0). Configuring a DHCP address pool also puts the router into DHCP pool configuration mode--identified by the (dhcp-config)# prompt--from which you can configure pool parameters (for example, the IP subnet number and default router list).

DHCP defines a process by which the DHCP server knows the IP subnet in which the DHCP client resides, and it can assign an IP address from a pool of valid IP addresses in that subnet. The process by which the DHCP server identifies which DHCP address pool to use to service a client request is described in the "Configuring Manual Bindings" task.

The DHCP server identifies which DHCP address pool to use to service a client request as follows:

- If the client is not directly connected (the giaddr field of the DHCPDISCOVER broadcast message is nonzero), the DHCP server matches the DHCPDISCOVER with a DHCP pool that has the subnet that contains the IP address in the giaddr field.
- If the client is directly connected (the giaddr field is zero), the DHCP server matches the DHCPDISCOVER with DHCP pools that contain the subnets configured on the receiving interface. If the interface has secondary IP addresses, the subnets associated with the secondary IP addresses are examined for possible allocation only after the subnet associated with the primary IP address (on the interface) is exhausted.

Cisco IOS DHCP server software supports advanced capabilities for IP address allocation. Here the "Configuring DHCP Address Allocation Using Option" section for more information.

STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter password if prompted.
Step 2	**configure terminal**	Enters global configuration mode.

	Example: Router# configure terminal	
Step 3	**ip dhcp pool** *name* **Example:** Router(config)# ip dhcp pool 1	Creates a name for the DHCP server address pool and enters DHCP pool configuration mode.
Step 4	**utilization mark high** *percentage-number* [**log**] **Example:** Router(dhcp-config)# utilization mark high 80 log	(Optional) Configures the high utilization mark of the current address pool size. • The **log** keyword enables the logging of a system message. A system message will be generated for a DHCP pool when the pool utilization exceeds the conigured high utilization threshold.
Step 5	**utilization mark low** *percentage-number* [**log**] **Example:** Router(dhcp-config)# utilization mark low 70 log	(Optional) Configures the low utilization mark of the current address pool size. • The **log** keyword enables the logging of a system message. A system message will be generated for a DHCP pool when the pool utilization falls below the configured low utilization threshold.
Step 6	**network** *network-number* [{*mask*| */prefix-length*} [**secondary**]]	Specifies the subnet network number and mask of the DHCP address pool.

	Example: Router(dhcp-config)# network 172.16.0.0 /16	
Step 7	**domain-name** *domain* **Example:** Router(dhcp-config)# domain-name cisco.com	Specifies the domain name for the client.
Step 8	**dns-server** *address [address2 ...address8]* **Example:** Router(dhcp-config)# dns server 172.16.1.103 172.16.2.103	Specifies the IP address of a DNS server that is available to a DHCP client. • One IP address is required; however, we can specify up to eight IP addresses in one command line. • Servers should be listed in order of preference.
Step 9	**bootfile** *filename* **Example:** Router(dhcp-config)# bootfile xllboot	(Optional) Specifies the name of the default boot image for a DHCP client. • The boot file is used to store the boot image for the client. The boot image is generally the operating system the client uses to load.
Step 10	**next-server** *address [address2 ...address8]*	(Optional) Configures the next server in the boot process of a DHCP client.

	Example: Router(dhcp-config)# next-server 172.17.1.103 172.17.2.103	• If multiple servers are specified, DHCP assigns them to clients in round-robin order. The first client gets address 1, the next client gets address 2, and so on. • If this command is not configured, DHCP uses the server specified by the **ip helper address** command as the boot server.
Step 11	**netbios-name-server** *address[address2 ... address8]* **Example:** Router(dhcp-config)# netbios-name-server 172.16.1.103 172.16.2.103	(Optional) Specifies the NetBIOS WINS server that is available to a Microsoft DHCP client. • One address is required; however, we can specify up to eight addresses in one command line. • Servers should be listed in order of preference.
Step 12	**netbios-node-type** *type* **Example:** Router(dhcp-config)# netbios-node-type h-node	(Optional) Specifies the NetBIOS node type for a Microsoft DHCP client.
Step 13	**default-router** *address [address2... address8]* **Example:** Router(dhcp-config)# default-router 172.16.1.100 172.16.1.101	(Optional) Specifies the IP address of the default router for a DHCP client. • The IP address should be on the same subnet as the client. • One IP address is required; however, we can specify up to eight IP addresses in one

		command line. These default routers are listed in order of preference; that is, *address* is the most preferred router, *address2* is the next most preferred router, and so on. • When a DHCP client requests an IP address, the router--acting as a DHCP server--accesses the default router list to select another router that the DHCP client is to use as the first hop for forwarding messages. After a DHCP client has booted, the client begins sending packets to its default router.
Step 14	**option** *code* [**instance** *number*] {**ascii** *string* | **hex** *string* | *ip-address*} **Example:** Router(dhcp-config)# option 19 hex 01	(Optional) Configures DHCP server options.
Step 15	**end** **Example:** Router(dhcp-config)# end	Returns to global configuration mode.

DNS

The DNS is a hierarchical 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 participants. Most importantly, it translates domain names meaningful to humans into the numerical (binary) identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide. 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, 209.191.122.70 as yahoo.com

The Domain Name System distributes the responsibility of assigning domain names and mapping those names to IP addresses by designating authoritative name servers for each domain. Authoritative name servers are assigned to be responsible for their particular domains, and in turn can assign other authoritative name servers for their sub-domains. This mechanism has made the DNS distributed, fault tolerant, and helped avoid the need for a single central register to be continually consulted and updated.

In general, the Domain Name System also stores other types of information, such as the list of mail servers that accept email for a given Internet domain. By providing a worldwide, distributed keyword-based redirection service, the Domain Name System is an essential component of the functionality of the Internet.

Hostnames for Network Devices

Each unique IP address can have an associated hostname. DNS uses a hierarchical scheme for establishing hostnames for network nodes. This allows local control of the segments of the network through a client-server scheme. The DNS system can locate a network device by translating the hostname of the device into its associated IP address.

Domains Names for Groups of Networks

IP defines a naming scheme that allows a device to be identified by its location in the IP. This is a hierarchical naming scheme that provides for domains. On the Internet, a domain is a portion of the naming hierarchy tree that refers to general groupings of networks based on organization type or geography. Domain names are pieced together with periods (.) as the delimiting characters. For example, Cisco is a commercial organization that the IP identifies by a com domain name, so its domain name is cisco.com. A specific device in this domain, the File Transfer Protocol (FTP) system, for example, is identified as ftp.cisco.com.

Name Servers

To keep track of domain names, IP has defined the concept of a name server. Name servers are programs that have complete information about their namespace portion of the domain tree and may also contain pointers to other name servers that can be used to lead to information from any other part of the domain tree. Name servers know the parts of the domain tree for which they have complete information. A name server may also store information about other parts of the domain tree. Before domain names can be mapped to IP addresses, we must first identify the hostnames, then specify a name server, and enable the DNS service.

Cache

To speed the process of converting names to addresses, the name server maintains a database, called a cache, of hostname-to-address mappings for use by the **connect**, **telnet**, and **ping** EXEC commands, and related Telnet support operations. The cache stores the results from previous responses. Upon receiving a client-issued DNS query, the name server will check this local storage to see if the answer is available locally.

Name Resolvers

Name resolvers are programs that extract information from name servers in response to client requests. Resolvers must be able to access at least one name server. The resolver either uses that name server's information to answer a query directly or pursues the query using referrals to other names servers. A resolver will typically be a system routine that is directly accessible to user programs. Therefore, no protocol is necessary between the resolver and the user program.

Zones

The domain namespace is divided into areas called zones that are points of delegation in the DNS tree. A zone contains all domains from a certain point downward, except those for which other zones are authoritative.

Authoritative Name Servers

A name server is said to be an authority for the parts of the domain tree for which it has complete information. A zone usually has an authoritative name server, often more than one. An authoritative name server has been configured with host table information or has acquired host table information though a zone transfer (the action that occurs when a secondary DNS server starts up and updates itself from the primary server).

DNS Operation

An organization can have many name servers, but Internet clients can query only those that the root name servers know. The other name servers answer internal queries only.

A name server handles client-issued queries to the DNS server for locally defined hosts within a particular zone as follows:

- An authoritative name server responds to DNS user queries for a domain name that is under its zone of authority by using the permanent and cached entries in its own host table. If the query is for a domain name that is under its zone of authority but for which it does not have any configuration information, the authoritative name server simply replies that no such information exists.
- A name server that is not configured as the authoritative name server responds to DNS user queries by using information that it has cached from previously received query responses. If no device is configured as the authoritative name server for a zone, queries to the DNS server for locally defined hosts will receive nonauthoritative responses.

Name servers answer DNS queries (forward incoming DNS queries or resolve internally generated DNS queries) according to the forwarding and lookup parameters configured for the specific domain.

When DNS queries are forwarded to name servers for resolution, some memory space is held for the corresponding DNS query until an appropriate response is received or until there is timeout. To avoid the free I/O memory from getting exhausted when handling queries at high rate, configure the maximum size for the queue.

HOW TO CONFIGURE DNS SERVER ON A CISCO ROUTER

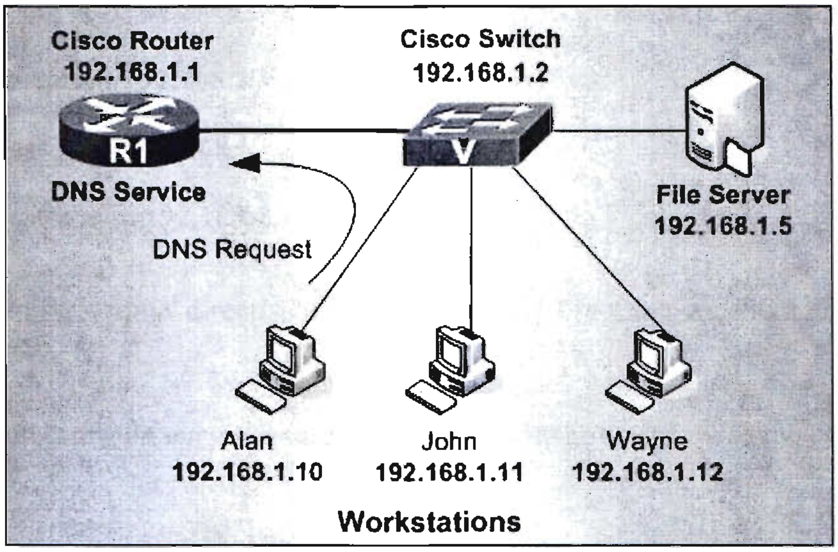
The DNS protocol is used to resolve FQDN (Fully Qualified Domain Names) to IP addresses around the world. This allows us to successfully find and connect to Internet websites and services no matter where they are. Its usefulness, however, local company and private networks also rely on DNS to operate efficiently and correctly.

In many cases, where a local DNS server is not available, we are forced to either use our ISP's DNS servers or some public DNS server, however, this can sometimes prove troublesome. Today, small low-end routers have the ability to integrate DNS functionality, making life easier, but so do Cisco routers - they simply have to be setup and we're done.

This article will show us how to configure our Cisco router to provide DNS services to our network, and make all clients use it as a DNS server. Our easy to follow step-by-step process ensures we'll understand the process and have it running within minutes.

EXAMPLE SCENARIO

Consider the following network diagram. This is our example network, we'd like to enable the DNS Service so our workstations can properly resolve Internet domains but also local network names.



First step is to enable the DNS service and domain lookup on the router:

```
R1# configure terminal
R1(config)# ip dns server
R1(config)# ip domain-lookup
```

Next, we need to configure the router with a public name-server, this will force the router to perform recursive DNS lookups, in other words, for every request it receives from our workstations the router will try to find the answer by asking as many DNS servers it needs, and finally return with an answer:

```
R1(config)#ipname-server4.2.2.5
R1(config)#ipname-server4.2.2.6
```

The cisco will allow us to enter up to 6 different name servers (essentially DNS servers). Usually we would use our ISP's DNS server to ensure you quick responses, then place a few free public

DNS servers such as the ones above. This will ensure that we'll get a DNS response from either our ISP or public DNS servers.

Next step is to configure your DNS server with the host names of our local network, this way when alan's PC trys to ping or connect to wayne, the router will successfully resolve its netbios name to the appropriate IP address:

```
R1(config)# ip host alan 192.168.1.10

R1(config)# ip host john 192.168.1.11

R1(config)# ip host wayne192.168.1.12
```

If you now try to ping 'wayne' directly from our router's CLI prompt, we should receive an answer:

At this point, we can configure our workstations to use our router's IP address as the primary DNS

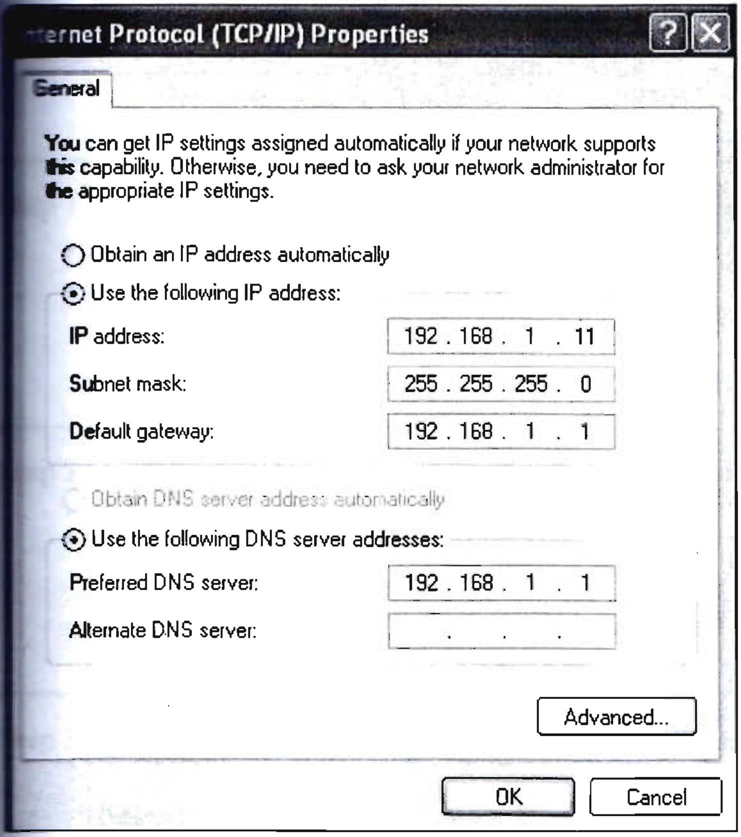
```
R1# ping wayne

Type escape sequence to abort

Sending 5, 100-byte ICMP Echos to 192.168.1.12, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

At this point, we can configure our workstations to use our router's IP address as the primary DNS

server



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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 11

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 1 . 1

Alternate DNS server: . . .

Configuring DNS Spoofing

Perform this task to configure DNS spoofing.

DNS spoofing is designed to allow a device to act as a proxy DNS server and "spoof" replies to any DNS queries using either the configured IP address in the **ip dnsspoofing** ip-address command or the IP address of the incoming interface for the query. This feature is useful for devices where the interface toward the Internet service provider (ISP) is not up. Once the interface to the ISP is up, the device forwards DNS queries to the real DNS servers.

This feature turns on DNS spoofing and is functional if any of the following conditions are true:

- The **no ip domain lookup** command is configured.
- IP name server addresses are not configured.
- There are no valid interfaces or routes for sending to the configured name server addresses.

If these conditions are removed, DNS spoofing will not occur.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**ip dns server** **Example:** Device(config)# ip dns server	Activates the DNS server on the device.
Step 4	**ip dns spoofing** [*ip-address*] **Example:** Device(config)# ip dns spoofing 192.168.15.1	Configures DNS spoofing. • The IP address used for DNS spoofing can be an IPv4 or IPv6 address. • The device will respond to the DNS query with the configured ip-address when queried for any hostname other than its own. • The device will respond to the DNS query with the IP address of the incoming interface when queried for its own hostname.

VLAN

A virtual local area network (VLAN) is a logical group of workstations, servers and network devices that appear to be on the same LAN despite their geographical distribution. A VLAN allows a network of computers and users to communicate in a simulated environment as if they exist in a single LAN and are sharing a single broadcast and multicast domain. VLANs are implemented to achieve scalability, security and ease of network management and can quickly adapt to change in network requirements and relocation of workstations and server nodes.

Higher-end switches allow the functionality and implementation of VLANs. The purpose of implementing a VLAN is to improve the performance of a network or apply appropriate security features.

How VLAN's work

When a LAN bridge receives data from a workstation, it tags the data with a VLAN identifier indicating the VLAN from which the data came. This is called explicit tagging. It is also possible to determine to which VLAN the data received belongs using implicit tagging. In implicit tagging the data is not tagged, but the VLAN from which the data came is determined based on other information like the port on which the data arrived. Tagging can be based on the port from which it came, the source Media Access Control (MAC) field, the source network address, or some other field or combination of fields. VLAN's are classified based on the method used. To be able to do the tagging of data using any of the methods, the bridge would have to keep an updated database containing a mapping between VLAN's and whichever field is used for tagging. For example, if tagging is by port, the database should indicate which ports belong to which VLAN. This database is called a filtering database. Bridges would have to be able to maintain this database and also to make sure that all the bridges on the LAN have the same information in each of their databases. The bridge determines where the data is to go next based on normal LAN operations. Once the bridge determines where the data is to go, it now needs to determine whether the VLAN identifier should be added to the data and sent. If the data is to go to a device that knows about VLAN implementation (VLAN-aware), the VLAN identifier is added to the data. If it is to go to a device that has no knowledge of VLAN implementation (VLAN-unaware), the bridge sends the data without the VLAN identifier.

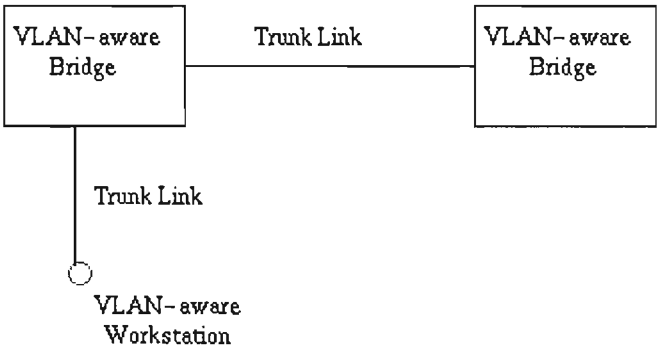
In order to understand how VLAN's work, we need to look at the types of connections between devices on VLAN's.

Types of Connections

Devices on a VLAN can be connected in three ways based on whether the connected devices are VLAN-aware or VLAN-unaware. Recall that a VLAN-aware device is one which understands VLAN memberships (i.e. which users belong to a VLAN) and VLAN formats.

1) Trunk Link

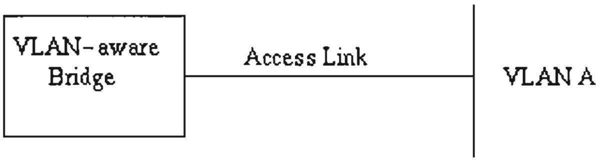
All the devices connected to a trunk link, including workstations, must be VLAN-aware. All frames on a trunk link must have a special header attached. These special frames are called tagged frames .



Trunk link between two VLAN-aware bridges.

2) Access Link

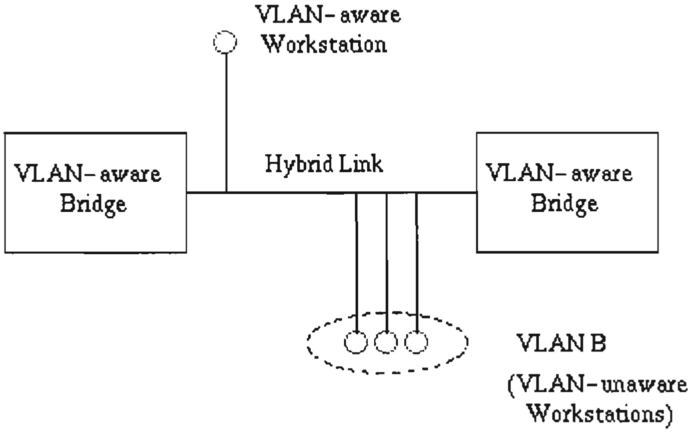
An access link connects a VLAN-unaware device to the port of a VLAN-aware bridge. All frames on access links must be implicitly tagged (untagged) . The VLAN-unaware device can be a LAN segment with VLAN-unaware workstations or it can be a number of LAN segments containing VLAN-unaware devices (legacy LAN).



Access link between a VLAN-aware bridge and a VLAN-unaware device.

3) Hybrid Link

This is a combination of the previous two links. This is a link where both VLAN-aware and VLAN-unaware devices are attached . A hybrid link can have both tagged and untagged frames, but all the frames for a specific VLAN must be either tagged or untagged.



Hybrid link containing both VLAN-aware and VLAN-unaware devices.

It must also be noted that the network can have a combination of all three types of links.

Adding and Verifying Data and Voice VLANs

```
Switch#configure terminal

Switch(config)#vlan 10

Switch(config-vlan)#name VOICE

Switch(config-vlan)#vlan 50

Switch(config-vlan)#name DATA

Switch(config-vlan)#end

Switch#show vlan brief

VLAN Name                          Status    Ports

---- ------------------------------ --------- -----------------------------

1    default                       active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
```

```
                                     Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                     Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                     Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                     Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                     Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                     Gi0/2
10   VOICE                         active
50   DATA                          active
1002 fddi-default                   act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                 act/unsup
1005 trnet-default                  act/unsup
```

Sure enough, VLANs 10 (VOICE) and 50 (DATA) now appear as valid VLANs on the switch. Now that the VLANs exist, we can assign the ports attaching to Cisco IP Phones (with PCs connected to the IP Phone) to the VLANs, as shown in Example

Assigning Voice and Data VLANs

```
Switch#configure terminal
Switch(config)#interface range fa0/2 - 24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#spanning-tree portfast
Switch(config-if-range)#switchport access vlan 50
Switch(config-if-range)#switchport voice vlan 10
Switch(config-if-range)#end
Switch#show vlan brief
VLAN Name                          Status    Ports
```

```
---- ------------------------------ --------- -------------------------------
1    default                   active    Gi0/1, Gi0/2
10   VOICE                       active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                           Fa0/6, Fa0/7, Fa0/8, Fa0/9
                               Fa0/10, Fa0/11, Fa0/12, Fa0/13
                               Fa0/14, Fa0/15, Fa0/16, Fa0/17
                               Fa0/18, Fa0/19, Fa0/20, Fa0/21
                               Fa0/22, Fa0/23, Fa0/24
50   DATA                        active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                               Fa0/6, Fa0/7, Fa0/8, Fa0/9
                               Fa0/10, Fa0/11, Fa0/12, Fa0/13
                               Fa0/14, Fa0/15, Fa0/16, Fa0/17
                               Fa0/18, Fa0/19, Fa0/20, Fa0/21
                               Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                 act/unsup
1003 token-ring-default              act/unsup
1004 fddinet-default                act/unsup
1005 trnet-default                 act/unsup
```

VPN

A virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A virtual private network can be contrasted with an expensive system of owned or leased lines that can only be used by one organization. The goal of a VPN is to provide the organization with the same capabilities, but at a much lower cost.

How VPN works

A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP). In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted. An additional level of security involves encrypting not only the data, but also the originating and receiving network addresses.

Many security protocols have been developed as VPNs, each offering differing levels of security and features. Among the more common are:

- **IP security (IPSec)**: IPSec is often used to secure Internet communications and can operate in two modes. Transport mode only encrypts the data packet message itself while Tunneling mode encrypts the entire data packet. This protocol can also be used in tandem with other protocols to increase their combined level of security.
- **Layer 2 Tunneling Protocol (L2TP)/IPsec**: The L2TP and IPsec protocols combine their best individual features to create a highly secure VPN client. Since L2TP isn't capable of encryption, it instead generates the tunnel while the IPSec protocol handles encryption, channel security, and data integrity checks to ensure all of the packets have arrived and that the channel has not been compromised.
- **Secure Sockets Layer (SSL)** and **Transport Layer Security (TLS)**: SSL and TLS are used extensively in the security of online retailers and service providers. These protocols operate using a handshake method. As IBM explains, "A HTTP-based SSL connection is always initiated by the client using a URL starting with https:// instead of with http://. At the beginning of an SSL session, an SSL handshake is performed. This handshake produces the cryptographic parameters of the session." These parameters, typically digital certificates, are the means by which the two systems exchange encryption keys, authenticate the session, and create the secure connection.

- **Point-to-Point Tunneling Protocol (PPTP)**: PPTP is a ubiquitous VPN protocol used since the mid 1990s and can be installed on a huge variety of operating systems has been around since the days of Windows 95. But, like L2TP, PPTP doesn't do encryption, it simply tunnels and encapsulates the data packet. Instead, a secondary protocol such as GRE or TCP has to be used as well to handle the encryption. And while the level of security PPTP provides has been eclipsed by new methods, the protocol remains a strong one, albeit not the most secure.
- **Secure Shell (SSH)**: SSH creates both the VPN tunnel and the encryption that protects it. This allows users to transfer information unsecured data by routing the traffic from remote fileservers through an encrypted channel. The data itself isn't encrypted but the channel its moving through is. SSH connections are created by the SSH client, which forwards traffic from a local port one on the remote server. All data between the two ends of the tunnel flow through these specified ports.
- These SSH tunnels are the primary means of subverting the government content filters described earlier. For example, if the filter prohibits access to TCP port 80, which handles HTTP, all user access to the Internet is cut off. However, by using SSH, the user can forward traffic from port 80 to another on the local machine which will still connect to the remote server's port 80. So as long as the remote server allows outgoing connections, the bypass will work. SSH also allows protocols that would otherwise be blocked by the firewall, say those for torrenting, to get past the wall by "wrapping" themselves in the skin of a protocol that the firewall does allow.

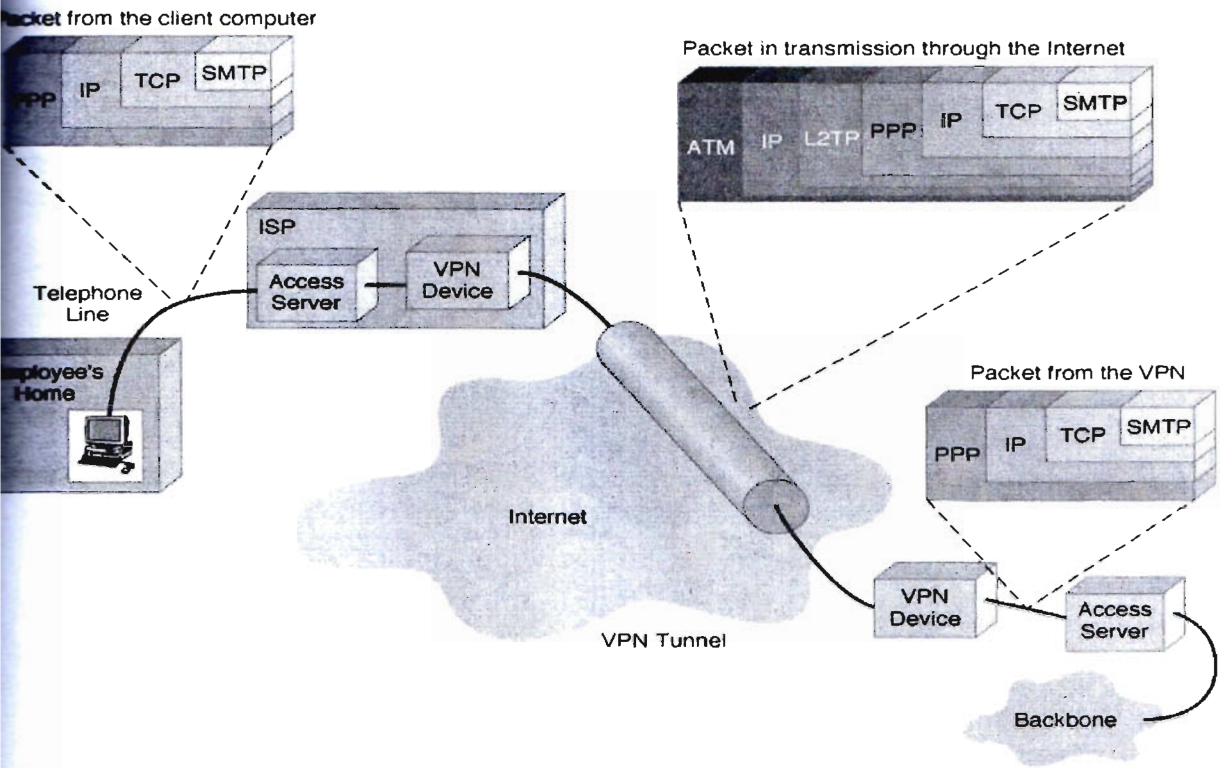


Figure: VPN encapsulation of packets

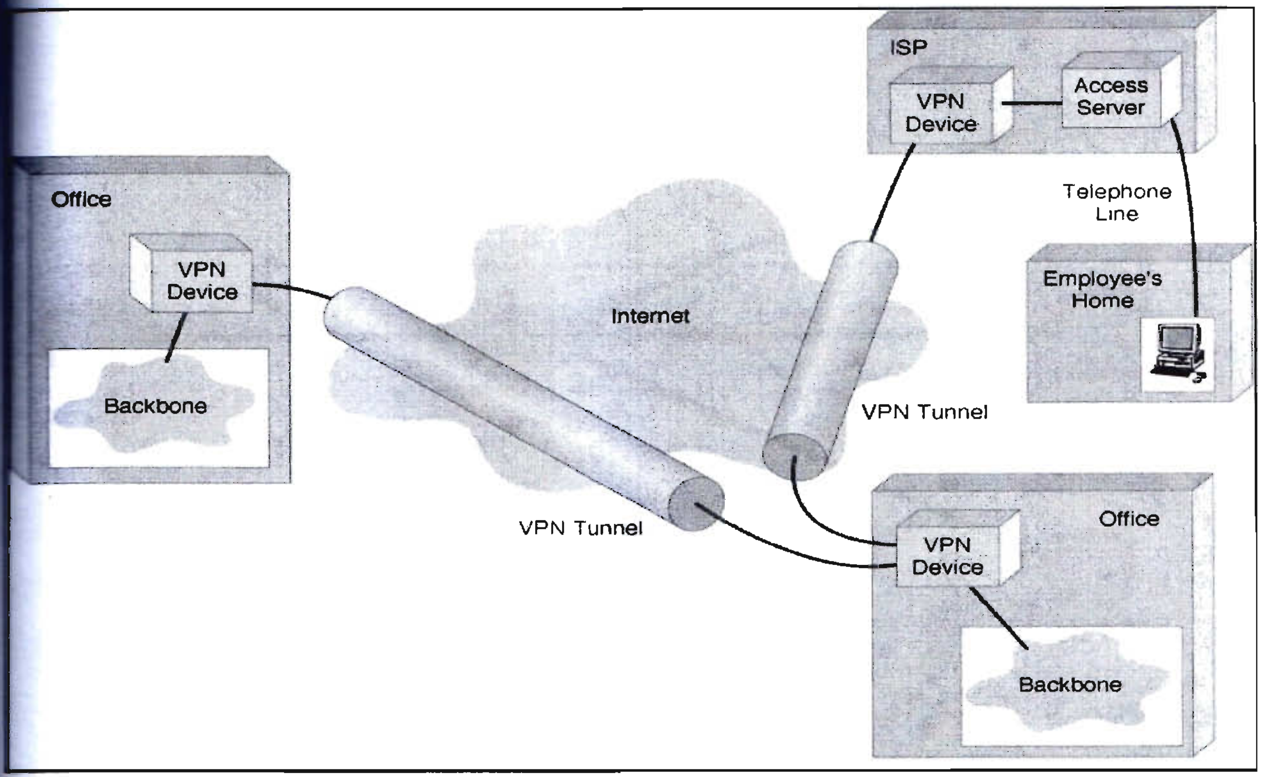


Figure: VPN Basic Architecture

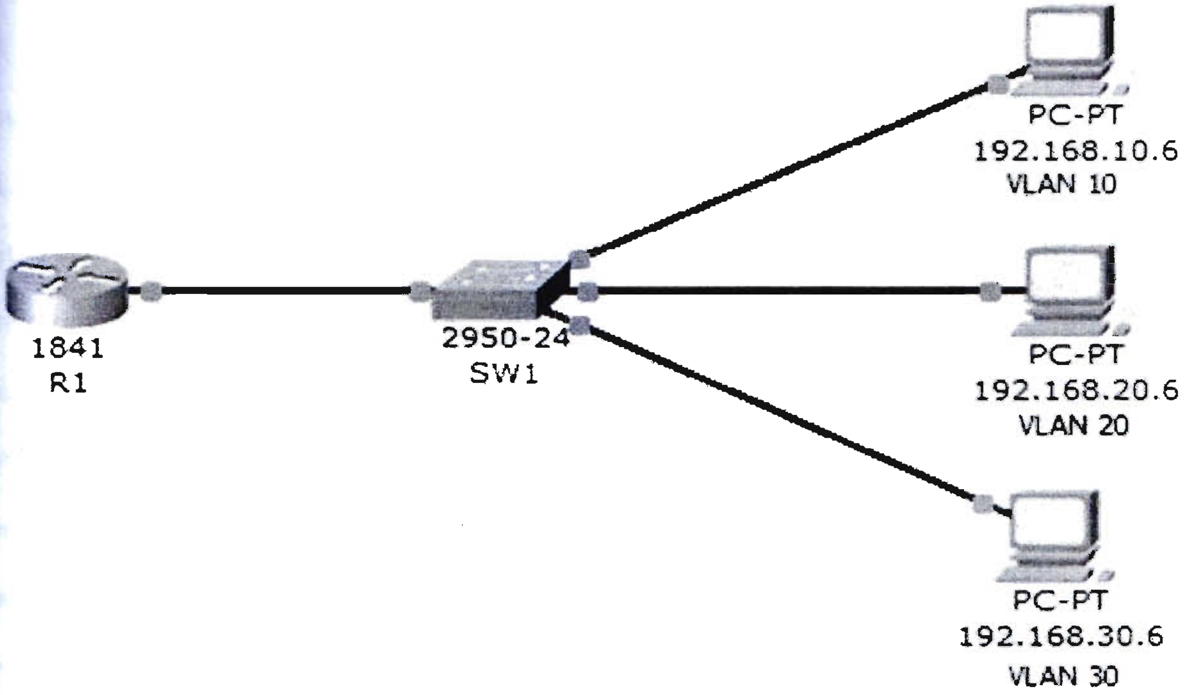
Data encapsulation process:

Original Datagram

Encrypted Inner Datagram

Datagram Header Outer Datagram Data Area

Data Encapsulation [From Comer]



Basic Router Configuration

```
Router>en

Router#conf t

Router#conf terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#int

Router(config)#interface giga

Router(config)#interface gigabitEthernet 0/0

Router(config-if)#ip add

Router(config-if)#ip address 172.16.0.1 255.255.254.0

Router(config-if)#no s

Router(config-if)#no sh
Router(config-if)#no shutdown


Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
exit
Router(config)#int
Router(config)#interface gig
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#ip add
Router(config-if)#ip address 172.16.4.33 255.255.255.224
Router(config-if)#no sh
Router(config-if)#no shutdown


Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up


%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to
up
exit
Router(config)#ho
Router(config)#hostname EWU
EWU(config)#line con
EWU(config)#line console 0
EWU(config-line)#pas
EWU(config-line)#password class
EWU(config-line)#lo

EWU(config-line)#log

EWU(config-line)#login

EWU(config-line)#exit

EWU(config)#banner m

EWU(config)#banner motd #Unauthorized Access Prohibited#

EWU(config)#en

EWU(config)#ena

EWU(config)#enable se

EWU(config)#enable secret cisco

EWU(config)#exit

EWU#

%SYS-5-CONFIG_I: Configured from console by console


EWU#conf t

EWU#conf terminal

Enter configuration commands, one per line.  End with CNTL/Z.

EWU(config)#ser

EWU(config)#service pa

EWU(config)#service password-encryption

EWU(config)#lin

EWU(config)#line vty 0 4

EWU(config-line)#pa

EWU(config-line)#pass

EWU(config-line)#password mango
EWU(config-line)#login
EWU(config-line)#exit
EWU(config)#ip do
EWU(config)#ip dom
EWU(config)#ip domain na
EWU(config)#ip domain name ciscolab.com
EWU(config)#cry
EWU(config)#crypto ke
EWU(config)#crypto key g
EWU(config)#crypto key generate rsa
The name for the keys will be: EWU.ciscolab.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

EWU(config)#lin
*Mar 1 0:20:26.981:  %SSH-5-ENABLED: SSH 1.99 has been enabled
EWU(config)#line vty 0 4
EWU(config-line)#no pas
EWU(config-line)#no password
EWU(config-line)#log
EWU(config-line)#login lo
EWU(config-line)#login local

EWU(config-line)#tra

EWU(config-line)#transport in

EWU(config-line)#transport input ssh

EWU(config-line)#use

EWU(config-line)#userna

EWU(config-line)#exit

EWU(config)#us

EWU(config)#username shuvo se

EWU(config)#username shuvo secret ab123

EWU(config)#log

EWU(config)#login

EWU(config)#login bl

EWU(config)#login block-for 300 a

EWU(config)#login block-for 300 attempts 4 w

EWU(config)#login block-for 300 attempts 4 within 30

EWU(config)#se

EWU(config)#sec

EWU(config)#security pas

EWU(config)#security passwords m

EWU(config)#security passwords min-length 7

EWU(config)#exit

EWU#

%SYS-5-CONFIG_I: Configured from console by console#
```

Basic Switch Configuration

```
Switch>en
Switch#conf t
Switch#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int
Switch(config)#interface vl
Switch(config)#interface vlan 1
Switch(config-if)#ip add
Switch(config-if)#ip address 172.16.0.2 255.255.254.0
Switch(config-if)#nosh
Switch(config-if)#no s
Switch(config-if)#no shu
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
exit
Switch(config)#lin
Switch(config)#line vt
Switch(config)#line vty 0 15
Switch(config-line)#pass
Switch(config-line)#password cisco
Switch(config-line)#log
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#
```

Firewall

Windows Firewall is a new feature of Microsoft Windows XP Service Pack 2 (SP2) that is turned on by default. It monitors and restricts the information that travels between our computer and a network such as the Internet. Windows Firewall helps to provide a line of defense against someone who might try to access our computer over a network without our permission. It also helps to block malicious software and worms and provides a means to log security events. Windows Firewall helps to protect our computer by blocking unsolicited traffic. Unsolicited traffic is any attempt to communicate with our computer over a network connection that was not specifically requested by programs running on our computer. Therefore programs such as Microsoft Internet Explorer or Outlook Express will continue to operate successfully with Windows Firewall enabled.

This document describes how to configure Windows Firewall on a single computer if the recommended default settings do not meet our requirements. For example, we might need to adjust settings if we use a program that needs an open connection to the Internet, or if I connect my mobile computer to a public network in a hotel or airport. This document focuses on:

Configuring Windows Firewall Advanced Settings

On the Advanced tab in Windows Firewall there are several settings that we can configure. These settings are divided into four sections:

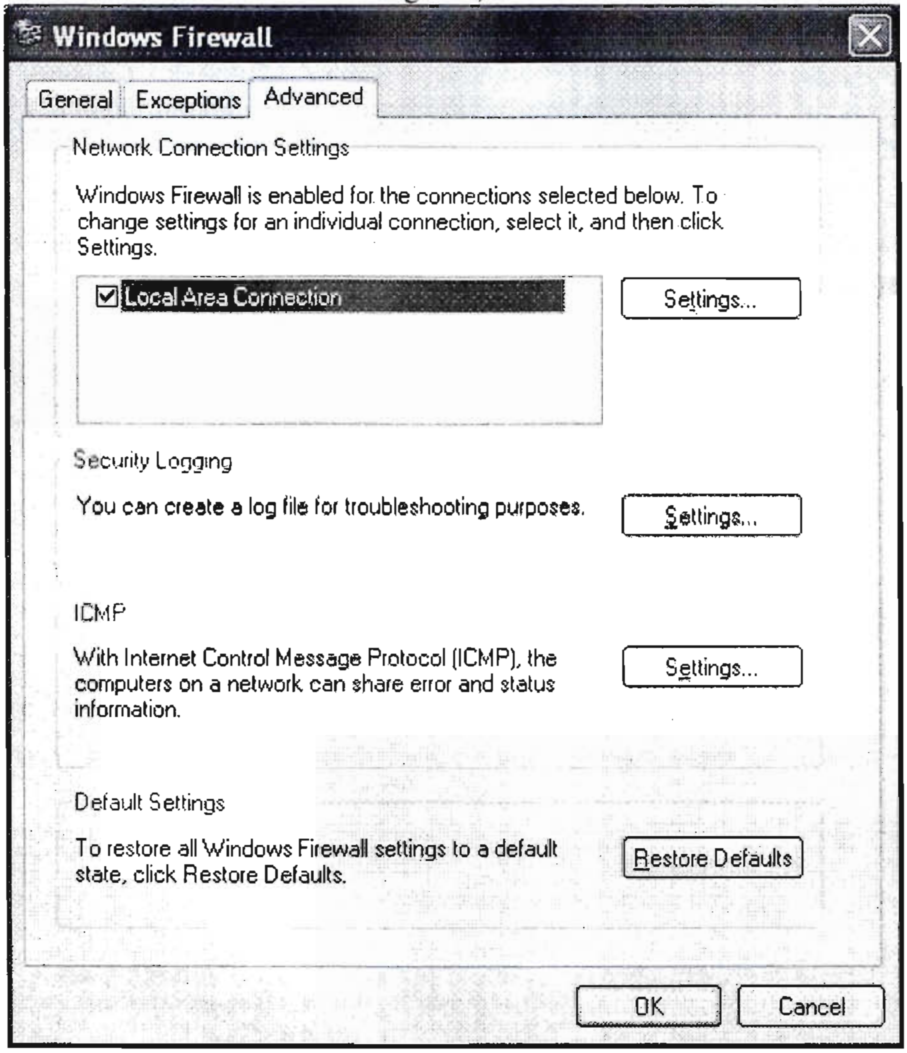
- **Network Connection Settings**. Advanced users modify these to define Windows Firewall settings for individual hardware connections that are available on a computer. For example, one could configure Windows Firewall to block connections only if s/he were attempted by a device attached to a USB port, and allow connections via his/her network card. The standard configuration on a standalone computer is for the Firewall to have the same settings for every hardware connection available.

- **Security Logging**. Advanced users can create a record of successful connections and unsuccessful connection attempts across Windows Firewall. When one choose to log unsuccessful attempts, information is collected about each connection attempt that is detected and blocked by Windows Firewall.
  When one choose to log successful connections, information is collected about each successful connection that travels across the firewall. Together these create a log of all the transactions going into and out of the computers environment.
- **ICMP**. Advanced users can select which parts of Internet Control Message Protocol (ICMP) can be used through Windows Firewall. To configure these settings requires in-depth knowledge of ICMP mechanisms. Incorrect configuration of ICMP can seriously affect our computers security.

.

To open the Windows Firewall Advanced Settings

1. In the **Windows Firewall** dialog box, click the **Advanced** tab.



Network Connection Settings

Windows Firewall is enabled for the connections selected below. To change settings for an individual connection, select it, and then click Settings.

☑ Local Area Connection

Security Logging

You can create a log file for troubleshooting purposes.

ICMP

With Internet Control Message Protocol (ICMP), the computers on a network can share error and status information.

Default Settings

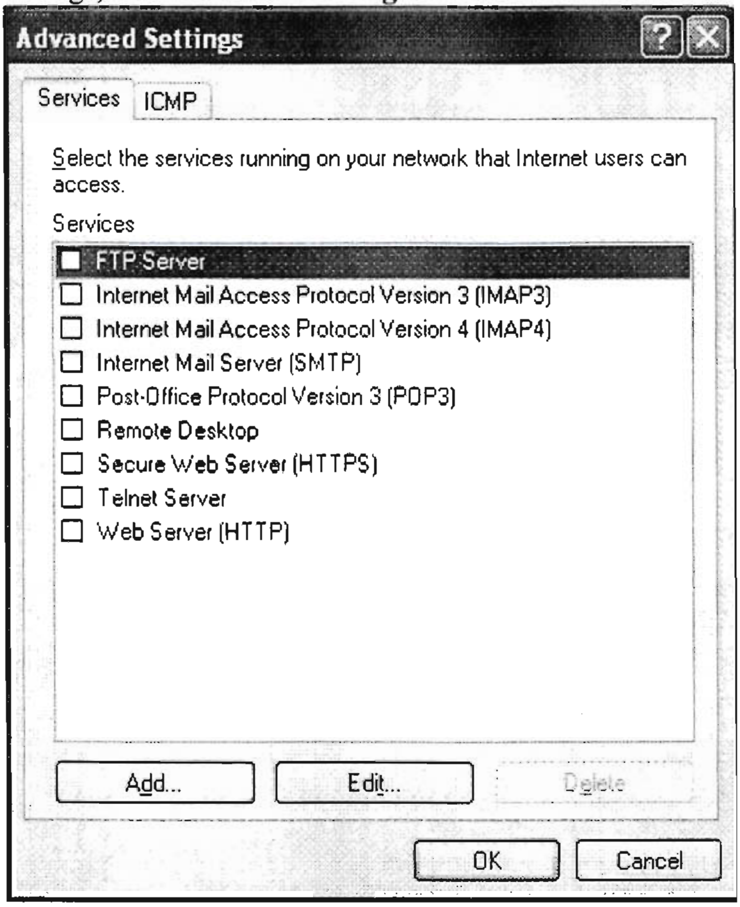
To restore all Windows Firewall settings to a default state, click Restore Defaults.

Windows Firewall Advanced settings

The default configuration for Windows Firewall is enabled for all connections. We can change this for individual connections, and can set a different configuration for each connection. For example, we might wish to disable email on our Internet connection, but allow email on our Local Area Connection.

To use Network Connection settings

1. In **Windows Firewall**, on the **Advanced** tab, under **Network Connection Settings**, clear all connections that we do not require Windows Firewall to protect.
2. Click to select the particular connection that we wish to change from the default firewall settings, and then click **Settings**.



Select the services running on your network that Internet users can access.

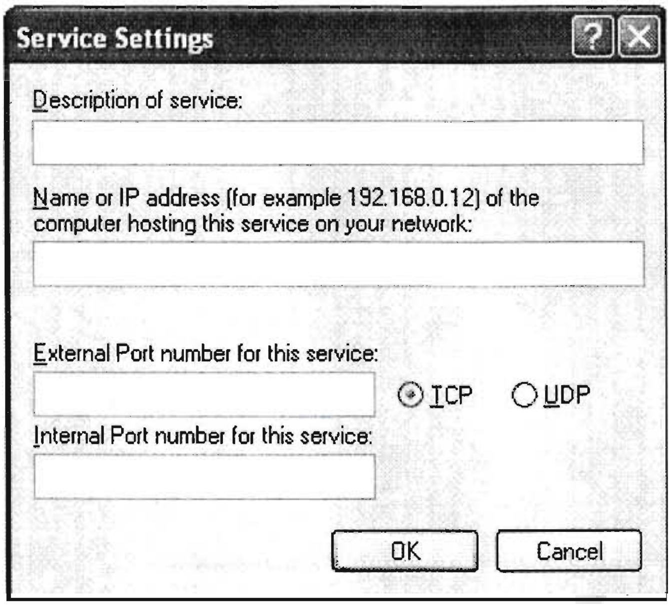
Services

- □ FTP Server
- □ Internet Mail Access Protocol Version 3 (IMAP3)
- □ Internet Mail Access Protocol Version 4 (IMAP4)
- □ Internet Mail Server (SMTP)
- □ Post-Office Protocol Version 3 (POP3)
- □ Remote Desktop
- □ Secure Web Server (HTTPS)
- □ Telnet Server
- □ Web Server (HTTP)

Windows Firewall Advanced settings per-network connection

3. Select or deselect the particular service that we wish to enable or disable for this connection.
4. If the service we wish to enable for this connection is not displayed, click **Add**.

5. Internet Protocol (IP) If the service we wish to enable for this connection is not displayed, click **Add**.


Service Settings
Description of service:
Name or IP address (for example 192.168.0.12) of the computer hosting this service on your network:
External Port number for this service:
Internal Port number for this service:
OK
Cancel

● TCP ○ UDP

Service Settings for a particular network connection

6. Type the specific connection details into each of the fields for the service that you wish to enable, and then click **OK**.

Windows Firewall can keep a log of successful connections that go through the firewall and any connections that are blocked.

When we choose to log dropped packets, information is collected about each attempt to cross the firewall that is detected and blocked. When we choose to log successful connections, information is collected about each successful connection that travels across the firewall. For example, when our computer successfully connects to a Web site using a Web browser, that connection is recorded in the log.

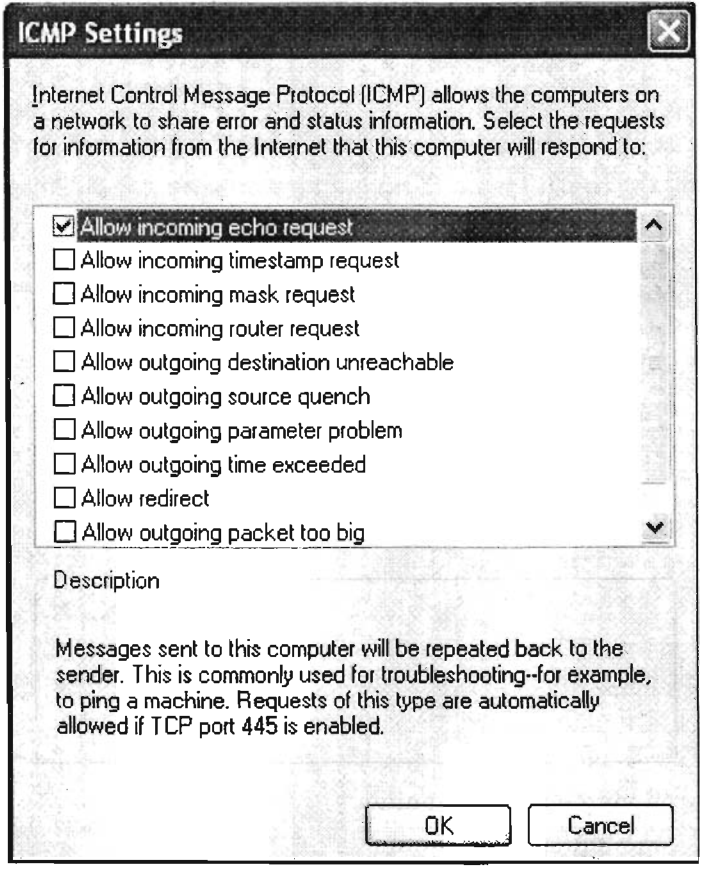
The security log has two sections:

- **Header**. This displays information about the version of the security log and the fields that are available to enter information into.
- **Body**. This is the complete report of all of the information gathered and recorded about the traffic across, or attempts to cross the firewall. The body of the security log is a dynamic list, which displays new data entries at the bottom of the log.

To configure Security Logging settings

1. In **Windows Firewall**, on the **Advanced** tab, under **Security Logging**, click **Settings**.

1. In **Windows Firewall** on the **Advanced** tab, under **ICMP**, click **Settings**.



Internet Control Message Protocol (ICMP) allows the computers on a network to share error and status information. Select the requests for information from the Internet that this computer will respond to:

☑ Allow incoming echo request
☐ Allow incoming timestamp request
☐ Allow incoming mask request
☐ Allow incoming router request
☐ Allow outgoing destination unreachable
☐ Allow outgoing source quench
☐ Allow outgoing parameter problem
☐ Allow outgoing time exceeded
☐ Allow redirect
☐ Allow outgoing packet too big

Description

Messages sent to this computer will be repeated back to the sender. This is commonly used for troubleshooting--for example, to ping a machine. Requests of this type are automatically allowed if TCP port 445 is enabled.

Figure 25 ICMP Settings

2. Select the appropriate requests that we want our computer to respond to and then
3. click **OK**.

Internet Protocol

An Internet Protocol (IP) address is a numerical label that is assigned to devices participating in a computer network that uses the Internet Protocol for communication between its nodes.

Each device on a network must be uniquely defined. At the Network layer, the packets of the communication need to be identified with the source and destination addresses of the two end systems.

These addresses are used in the data network as binary patterns. Inside the devices, digital logic is applied for their interpretation. For us in the human network, a string of 32 bits is difficult to interpret and even more difficult to remember. Therefore, we represent IPv4 addresses using dotted decimal format.

Dotted Decimal

Binary patterns representing IPv4 addresses are expressed as dotted decimals by separating each byte of the binary pattern, called an octet, with a dot. It is called an octet because each decimal number represents one byte or 8 bits.

For example, the address:

10101100000100000000010000010100

is expressed in dotted decimal as:

172.16.4.20

Keep in mind that devices use binary logic. The dotted decimal format is used to make it easier for people to use and remember addresses.

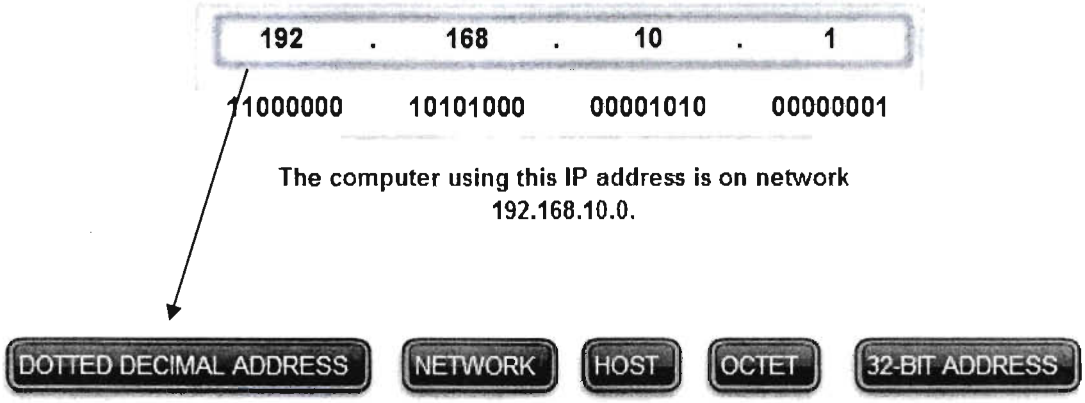
Network and Host Portions

For each IPv4 address, some portion of the high-order bits represents the network address. At Layer 3, we define a network as a group of hosts that have identical bit patterns in the network address portion of their addresses.

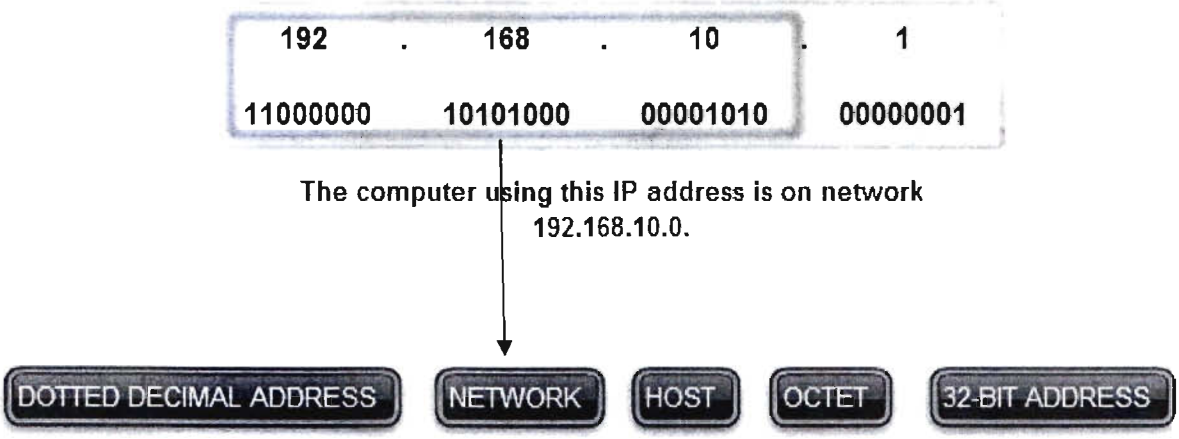
Although all 32 bits define the IPv4 host address, we have a variable number of bits that are called the host portion of the address. The number of bits used in this host portion determines the number of hosts that we can have within the network.

For example, if we need to have at least 200 hosts in a particular network, we would need to use enough bits in the host portion to be able to represent at least 200 different bit patterns.

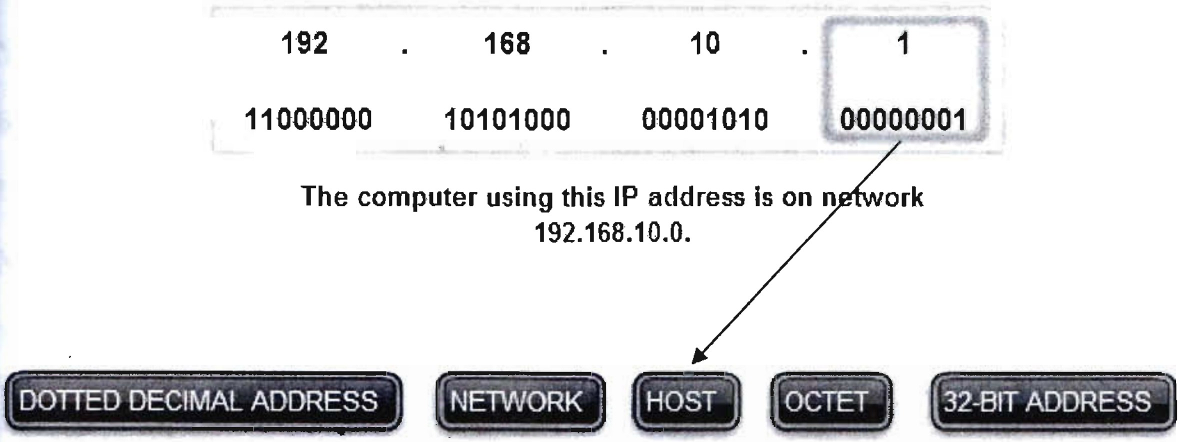
To assign a unique address to 200 hosts, we would use the entire last octet. With 8 bits, a total of 256 different bit patterns can be achieved. This would mean that the bits for the upper three octets would represent the network portion.



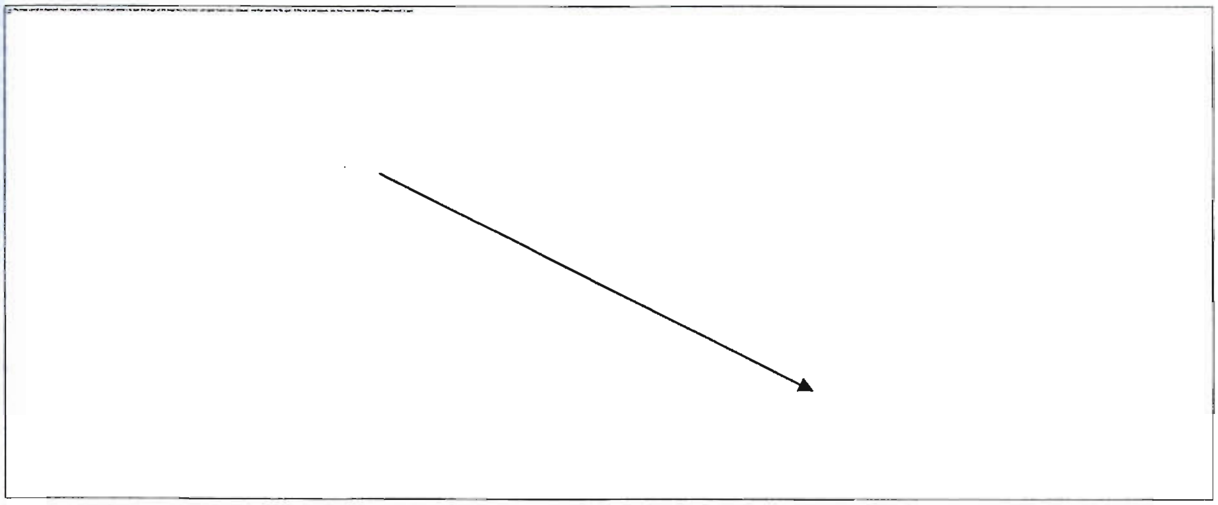
The computer using this IP address is on network 192.168.10.0.

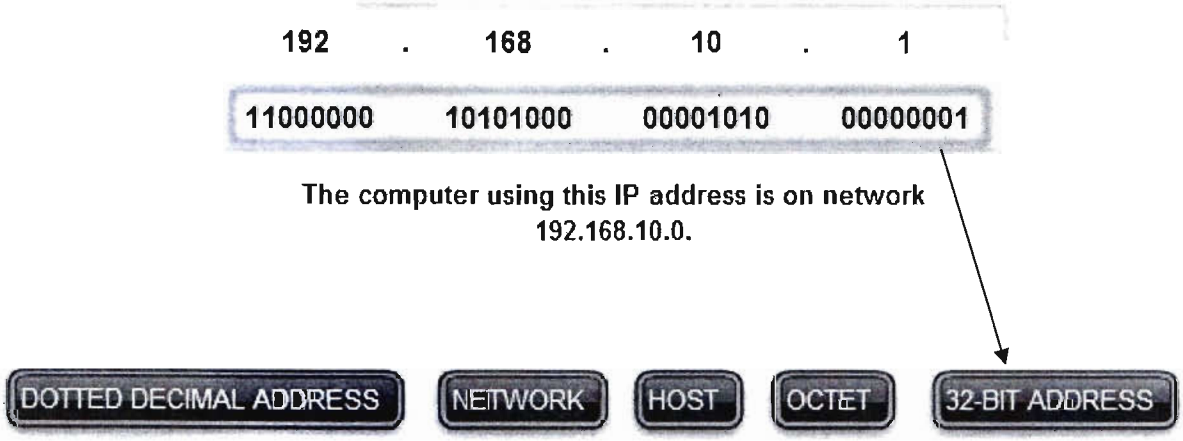


The computer using this IP address is on network 192.168.10.0.



The computer using this IP address is on network 192.168.10.0.





The computer using this IP address is on network 192.168.10.0.

Within the address range of each IPv4 network, we have three types of addresses:

Types of Addresses in an IPv4 Network

Network address - The address by which we refer to the network

Broadcast address - A special address used to send data to all hosts in the network

Host addresses - The addresses assigned to the end devices in the network

Network Address

The network address is a standard way to refer to a network. For example, we could refer to the network shown in the figure as "the 10.0.0.0 network." This is a much more convenient and descriptive way to refer to the network than using a term like "the first network." All hosts in the 10.0.0.0 network will have the same network bits.

Within the IPv4 address range of a network, the lowest address is reserved for the network address. This address has a 0 for each host bit in the host portion of the address.

Broadcast Address

The IPv4 broadcast address is a special address for each network that allows communication to all the hosts in that network. To send data to all hosts in a network, a host can send a single packet that is addressed to the broadcast address of the network.

The broadcast address uses the highest address in the network range. This is the address in which the bits in the host portion are all 1s. For the network 10.0.0.0 with 24 network bits, the broadcast address would be 10.0.0.255. This address is also referred to as the directed broadcast.

Host Addresses

As described previously, every end device requires a unique address to deliver a packet to that host. In IPv4 addresses, we assign the values between the network address and the broadcast address to the devices in that network.

In an IPv4 network, the hosts can communicate one of three different ways:

Unicast - the process of sending a packet from one host to an individual host

Broadcast - the process of sending a packet from one host to all hosts in the network

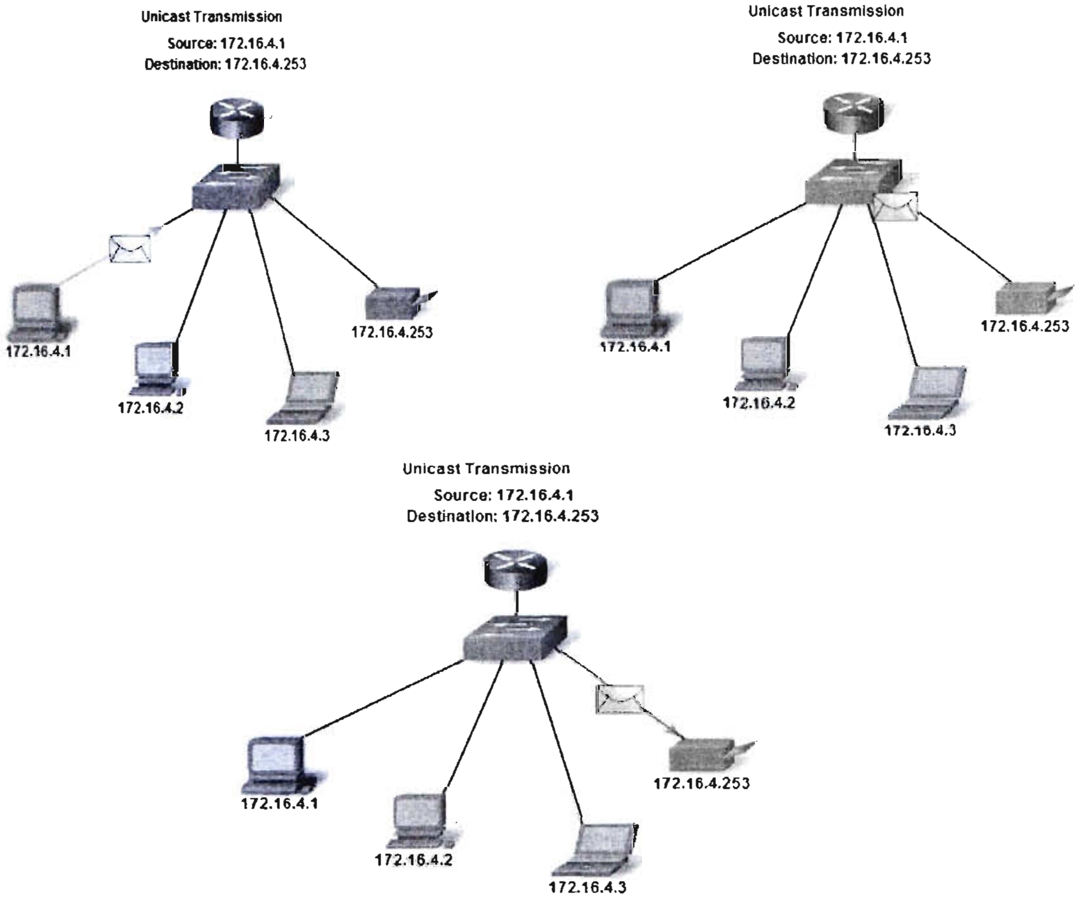
Multicast - the process of sending a packet from one host to a selected group of hosts

These three types of communication are used for different purposes in the data networks. In all three cases, the IPv4 address of the originating host is placed in the packet header as the source address.

Unicast Traffic

Unicast communication is used for the normal host-to-host communication in both a client/server and a peer-to-peer network. Unicast packets use the host address of the destination device as the destination address and can be routed through an internetwork. Broadcast and multicast, however, use special addresses as the destination address. Using these special addresses, broadcasts are generally restricted to the local network. The scope of multicast traffic also may be limited to the local network or routed through an internetwork.

In an IPv4 network, the unicast address applied to an end device is referred to as the host address. For unicast communication, the host addresses assigned to the two end devices are used as the source and destination IPv4 addresses. During the encapsulation process, the source host places its IPv4 address in the unicast packet header as the source host address and the IPv4 address of the destination host in the packet header as the destination address. The communication using a unicast packet can be forwarded through an internetwork using the same addresses.



Broadcast Transmission

Because broadcast traffic is used to send packets to all hosts in the network, a packet uses a special broadcast address. When a host receives a packet with the broadcast address as the destination, it processes the packet as it would a packet to its unicast address.

Broadcast transmission is used for the location of special services/devices for which the address is not known or when a host needs to provide information to all the hosts on the network.

Some examples for using broadcast transmission are:

Mapping upper layer addresses to lower layer addresses

Requesting an address

Exchanging routing information by routing protocols

When a host needs information, the host sends a request, called a query, to the broadcast address. All hosts in the network receive and process this query. One or more of the hosts with the requested information will respond, typically using unicast.

Similarly, when a host needs to send information to the hosts on a network, it creates and sends a broadcast packet with the information.

Unlike unicast, where the packets can be routed throughout the internetwork, broadcast packets are usually restricted to the local network. This restriction is dependent on the configuration of the router that borders the network and the type of broadcast. There are two types of broadcasts: directed broadcast and limited broadcast.

Directed Broadcast

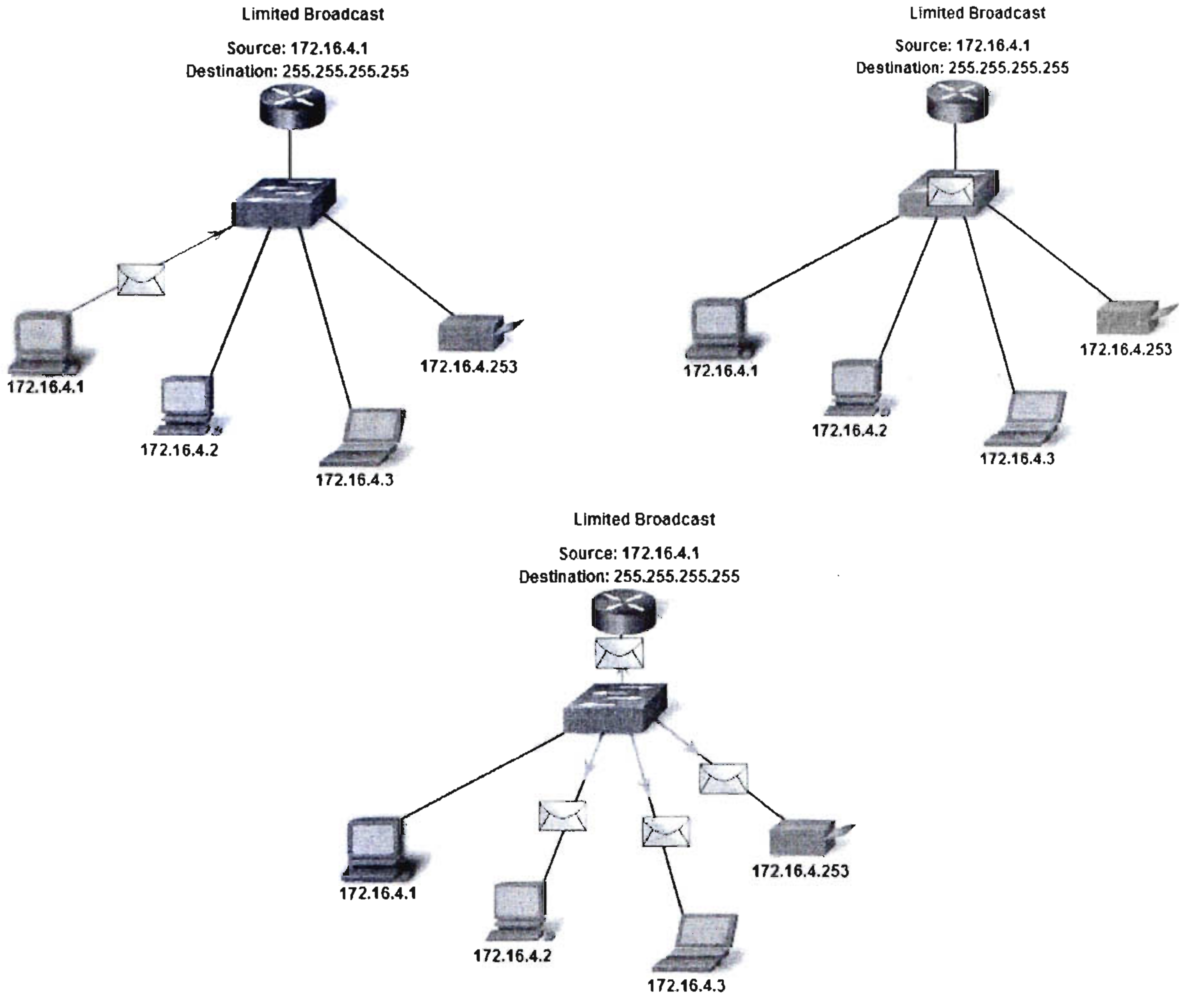
A directed broadcast is sent to all hosts on a specific network. This type of broadcast is useful for sending a broadcast to all hosts on a non-local network. For example, for a host outside of the network to communicate with the hosts within the 172.16.4.0 /24 network, the destination address of the packet would be 172.16.4.255. This is shown in the figure. Although routers do not forward directed broadcasts by default, they may be configured to do so.

Limited Broadcast

The limited broadcast is used for communication that is limited to the hosts on the local network. These packets use a destination IPv4 address 255.255.255.255. Routers do not forward this broadcast. Packets addressed to the limited broadcast address will only appear on the local network. For this reason, an IPv4 network is also referred to as a broadcast domain. Routers form the boundary for a broadcast domain.

As an example, a host within the 172.16.4.0 /24 network would broadcast to all the hosts in its network using a packet with a destination address of 255.255.255.255.

As you learned earlier, when a packet is broadcast, it uses resources on the network and also forces every host on the network that receives it to process the packet. Therefore, broadcast traffic should be limited so that it does not adversely affect performance of the network or devices. Because routers separate broadcast domains, subdividing networks with excessive broadcast traffic can improve network performance.



Multicast Transmission

Multicast transmission is designed to conserve the bandwidth of the IPv4 network. It reduces traffic by allowing a host to send a single packet to a selected set of hosts. To reach multiple destination hosts using unicast communication, a source host would need to send an individual packet addressed to each host. With multicast, the source host can send a single packet that can reach thousands of destination hosts.

Some examples of multicast transmission are:

Video and audio broadcasts

Routing information exchange by routing protocols

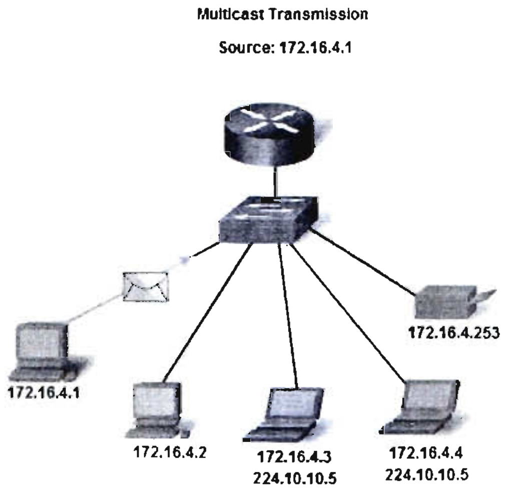
Distribution of software

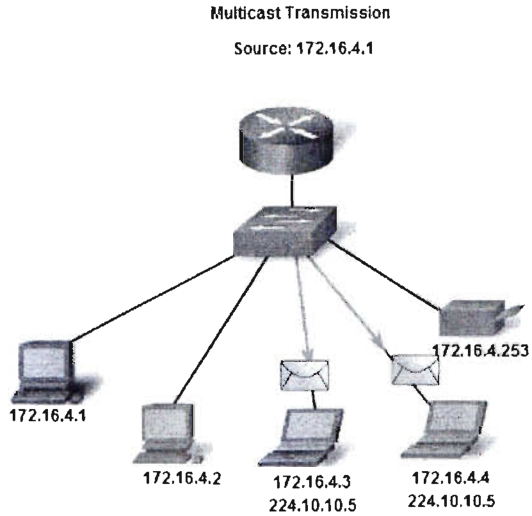
News feeds

Multicast Clients

Hosts that wish to receive particular multicast data are called multicast clients. The multicast clients use services initiated by a client program to subscribe to the multicast group.

Each multicast group is represented by a single IPv4 multicast destination address. When an IPv4 host subscribes to a multicast group, the host processes packets addressed to this multicast address as well as packets addressed to its uniquely allocated unicast address. As we will see, IPv4 has set aside a special block of addresses from 224.0.0.0 to 239.255.255.255 for multicast groups addressing.





Expressed in dotted decimal format, the IPv4 address range is 0.0.0.0 to 255.255.255.255. As you have already seen, not all of these addresses can be used as host addresses for unicast communication.

Experimental Addresses

One major block of addresses reserved for special purposes is the IPv4 experimental address range 240.0.0.0 to 255.255.255.254. Currently, these addresses are listed as reserved for future use (RFC 3330). This suggests that they could be converted to usable addresses. Currently, they cannot be used in IPv4 networks. However, these addresses could be used for research or experimentation.

Multicast Addresses

As previously shown, another major block of addresses reserved for special purposes is the IPv4 multicast address range 224.0.0.0 to 239.255.255.255. Additionally, the multicast address range is subdivided into different types of addresses: reserved link local addresses and globally scoped addresses, as shown in the graphic. One additional type of multicast address is the administratively scoped addresses, also called limited scope addresses.

The IPv4 multicast addresses 224.0.0.0 to 224.0.0.255 are reserved link local addresses. These addresses are to be used for multicast groups on a local network. Packets to these destinations are always transmitted with a time-to-live (TTL) value of 1. Therefore, a router connected to the local network should never forward them. A typical use of reserved link-local addresses is in routing protocols using multicast transmission to exchange routing information.

The globally scoped addresses are 224.0.1.0 to 238.255.255.255. They may be used to multicast data across the Internet. For example, 224.0.1.1 has been reserved for Network Time Protocol (NTP) to synchronize the time-of-day clocks of network devices.

Host Addresses

After accounting for the ranges reserved for experimental addresses and multicast addresses, this leaves an address range of 0.0.0.0 to 223.255.255.255 that could be used for IPv4 hosts. However, within this range are many addresses that are already reserved for special purposes.

Public & Private Addresses

Although most IPv4 host addresses are public addresses designated for use in networks that are accessible on the Internet, there are blocks of addresses that are used in networks that require limited or no Internet access. These addresses are called private addresses.

Private Addresses

The private address blocks are:

10.0.0.0 to 10.255.255.255 (10.0.0.0 /8)

172.16.0.0 to 172.31.255.255 (172.16.0.0 /12)

192.168.0.0 to 192.168.255.255 (192.168.0.0 /16)

Private space address blocks, as shown in the figure, are set aside for use in private networks. The use of these addresses need not be unique among outside networks. Hosts that do not require access to the Internet at large may make unrestricted use of private addresses. However, the internal networks still must design network address schemes to ensure that the hosts in the private networks use IP addresses that are unique within their networking environment.

Many hosts in different networks may use the same private space addresses. Packets using these addresses as the source or destination should not appear on the public Internet. The router or firewall device at the perimeter of these private networks must block or translate these addresses. Even if these packets were to make their way to the Internet, the routers would not have routes to forward them to the appropriate private network.

Public Addresses

The vast majority of the addresses in the IPv4 unicast host range are public addresses. These addresses are designed to be used in the hosts that are publicly accessible from the Internet. Even within these address blocks, there are many addresses that are designated for other special purposes.

Historic Network Classes

Historically, RFC1700 grouped the unicast ranges into specific sizes called class A, class B, and class C addresses. It also defined class D (multicast) and class E (experimental) addresses, as previously presented.

The unicast address classes A, B, and C defined specifically-sized networks as well as specific address blocks for these networks, as shown in the figure. A company or organization was assigned an entire class A, class B, or class C address block. This use of address space is referred to as classful addressing.

Class A Blocks

A class A address block was designed to support extremely large networks with more than 16 million host addresses. Class A IPv4 addresses used a fixed /8 prefix with the first octet to indicate the network address. The remaining three octets were used for host addresses.

To reserve address space for the remaining address classes, all class A addresses required that the most significant bit of the high-order octet be a zero. This meant that there were only 128 possible class A networks, 0.0.0.0 /8 to 127.0.0.0 /8, before taking out the reserved address blocks. Even though the class A addresses reserved one-half of the address space, because of their limit of 128 networks, they could only be allocated to approximately 120 companies or organizations.

Class B Blocks

Class B address space was designed to support the needs of moderate to large size networks with more than 65,000 hosts. A class B IP address used the two high-order octets to indicate the network address. The other two octets specified host addresses. As with class A, address space for the remaining address classes needed to be reserved.

For class B addresses, the most significant two bits of the high-order octet were 10. This restricted the address block for class B to 128.0.0.0 /16 to 191.255.0.0 /16. Class B had slightly more efficient allocation of addresses than class A because it equally divided 25% of the total IPv4 address space among approximately 16,000 networks.

Class C Blocks

The class C address space was the most commonly available of the historic address classes. This address space was intended to provide addresses for small networks with a maximum of 254 hosts.

Class C address blocks used a /24 prefix. This meant that a class C network used only the last octet as host addresses with the three high-order octets used to indicate the network address.

Class C address blocks set aside address space for class D (multicast) and class E (experimental) by using a fixed value of 110 for the three most significant bits of the high-order octet. This restricted the address block for class C to 192.0.0.0 /16 to 223.255.255.0 /16. Although it occupied only 12.5% of the total IPv4 address space, it could provide addresses to 2 million networks.

Limits to the Class-based System

Not all organizations' requirements fit well into one of these three classes. Classful allocation of address space often wasted many addresses, which exhausted the availability of IPv4 addresses. For example, a company that had a network with 260 hosts would need to be given a class B address with more than 65,000 addresses.

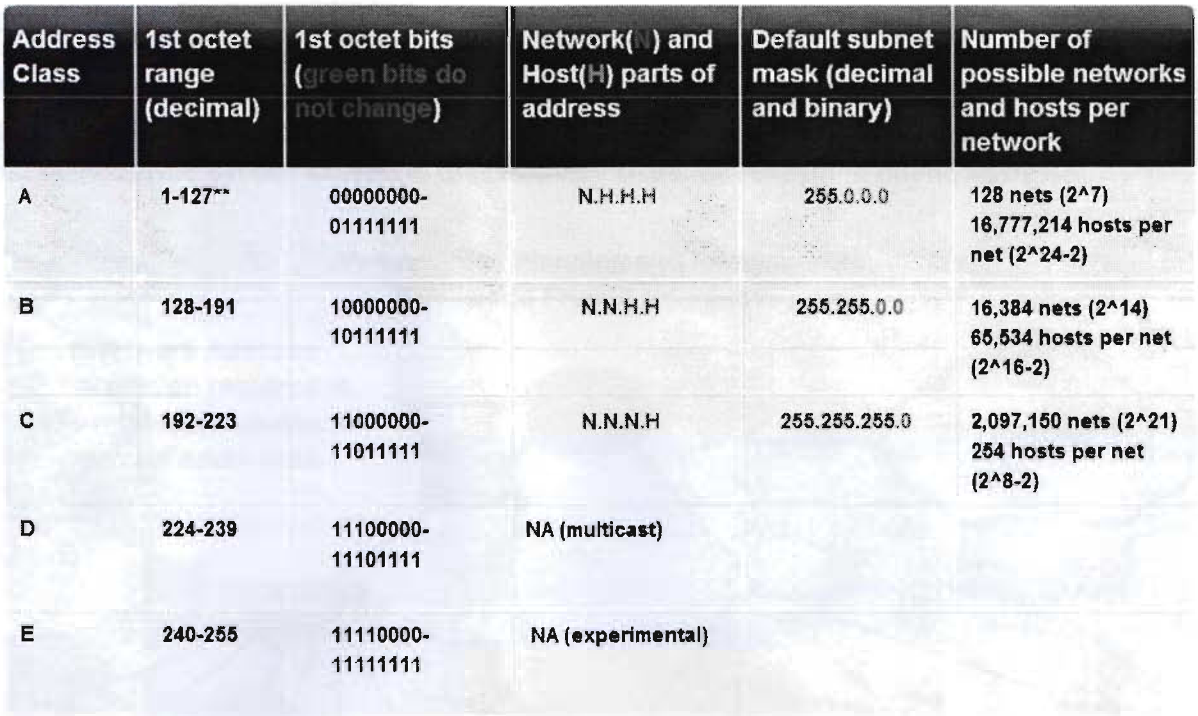
Even though this classful system was all but abandoned in the late 1990s, you will see remnants of it in networks today. For example, when you assign an IPv4 address to a computer, the operating system examines the address being assigned to determine if this address is a class A, class B, or class C. The operating system then assumes the prefix used by that class and makes the appropriate subnet mask assignment.

Another example is the assumption of the mask by some routing protocols. When some routing protocols receive an advertised route, it may assume the prefix length based on the class of the address.

Classless Addressing

The system that we currently use is referred to as classless addressing. With the classless system, address blocks appropriate to the number of hosts are assigned to companies or organizations without regard to the unicast class.

IP Address Classes



Address Class	1st octet range (decimal)	1st octet bits (green bits do not change)	Network(N) and Host(H) parts of address	Default subnet mask (decimal and binary)	Number of possible networks and hosts per network
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 nets (2^7) 16,777,214 hosts per net (2^24-2)
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16,384 nets (2^14) 65,534 hosts per net (2^16-2)
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2,097,150 nets (2^21) 254 hosts per net (2^8-2)
D	224-239	11100000-11101111	NA (multicast)		
E	240-255	11110000-11111111	NA (experimental)		

** All zeros (0) and all ones (1) are invalid hosts addresses.

Network Address Translation (NAT)

With services to translate private addresses to public addresses, hosts on a privately addressed network can have access to resources across the Internet. These services, called Network Address Translation (NAT), can be implemented on a device at the edge of the private network.

NAT allows the hosts in the network to "borrow" a public address for communicating to outside networks. While there are some limitations and performance issues with NAT, clients for most applications can access services over the Internet without noticeable problems.

Planning Address the Network

An important part of planning an IPv4 addressing scheme is deciding when private addresses are to be used and where they are to be applied.

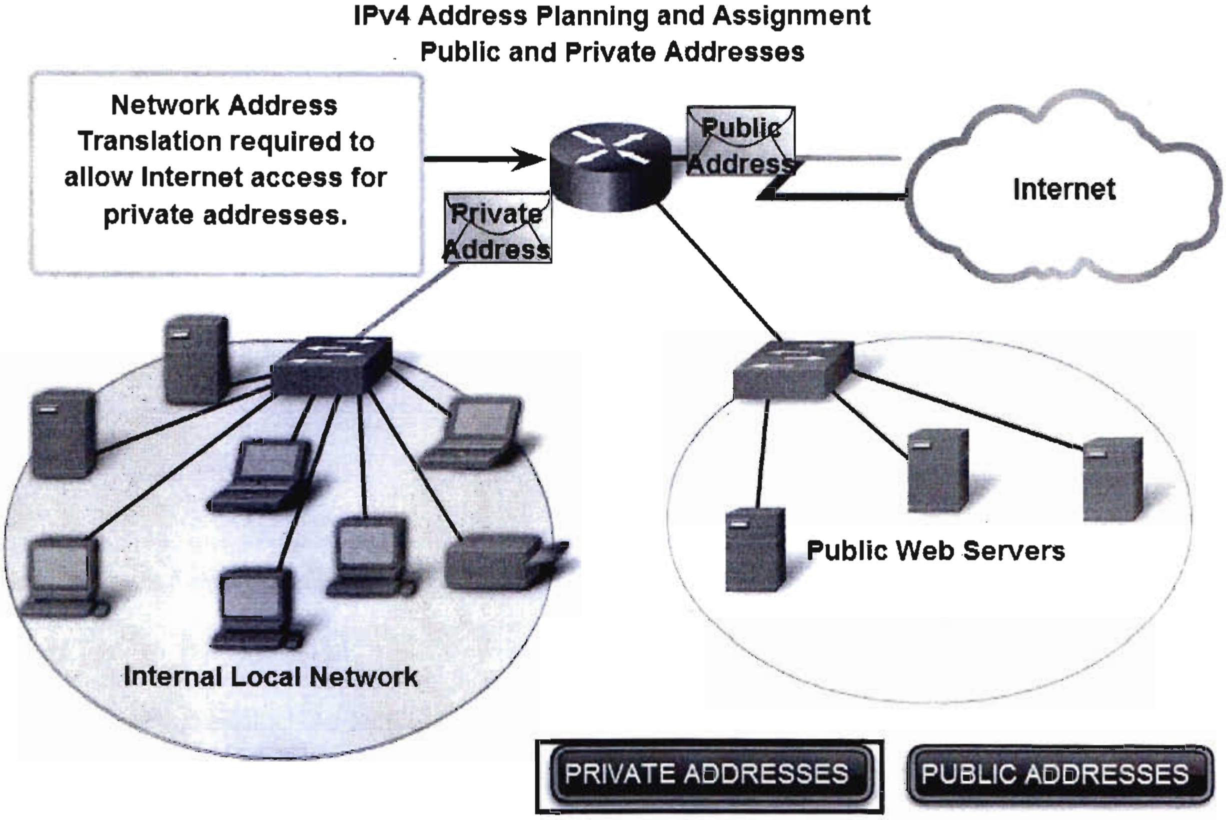
Considerations include:

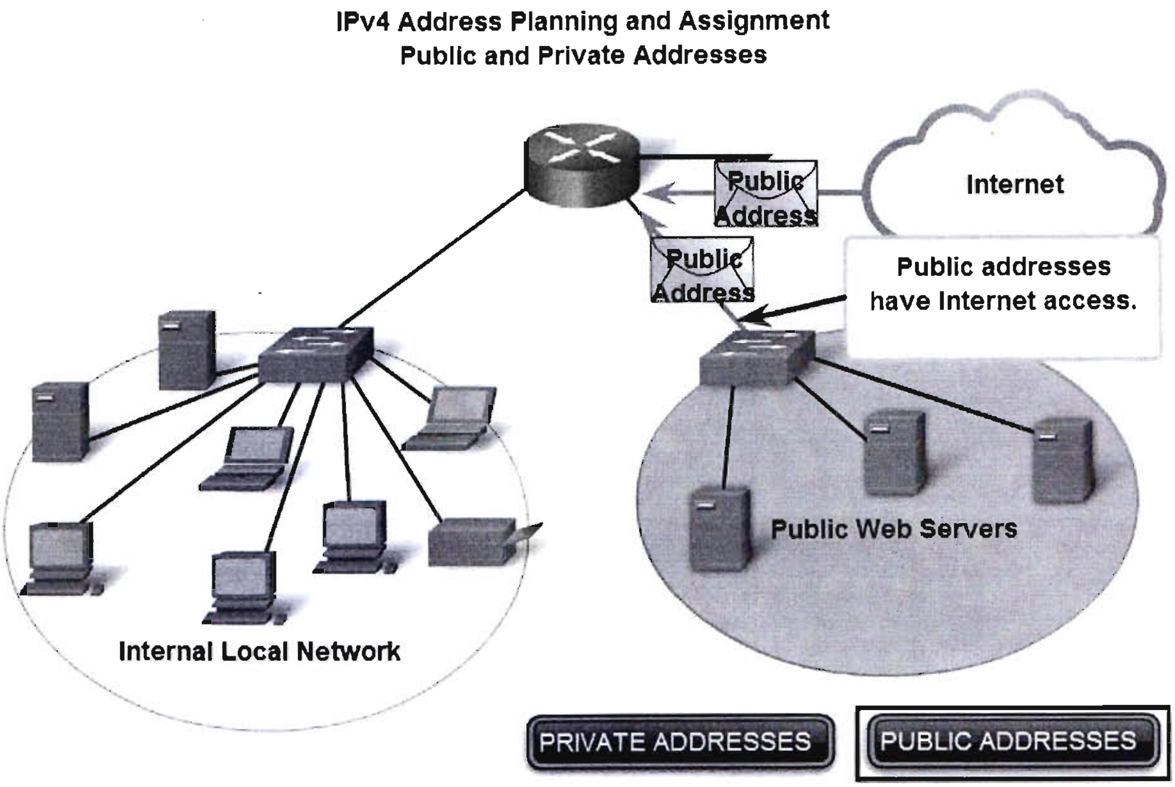
Will there be more devices connected to the network than public addresses allocated by the network's ISP?

Will the devices need to be accessed from outside the local network?

If devices that may be assigned private addresses require access to the Internet, is the network capable of providing a Network Address Translation (NAT) service?

If there are more devices than available public addresses, only those devices that will directly access the Internet - such as web servers - require a public address. A NAT service would allow those devices with private addresses to effectively share the remaining public addresses.


IPv4 Address Planning and Assignment
Public and Private Addresses
Network Address Translation required to allow Internet access for private addresses.
Public Address
Private Address
Internet
Public Web Servers
Internal Local Network
PRIVATE ADDRESSES
PUBLIC ADDRESSES



Static or Dynamic Addresses for End User Devices

Addresses for User Devices

In most data networks, the largest population of hosts includes the end devices such as PCs, IP phones, printers, and PDAs. Because this population represents the largest number of devices within a network, the largest number of addresses should be allocated to these hosts.

IP addresses can be assigned either statically or dynamically.

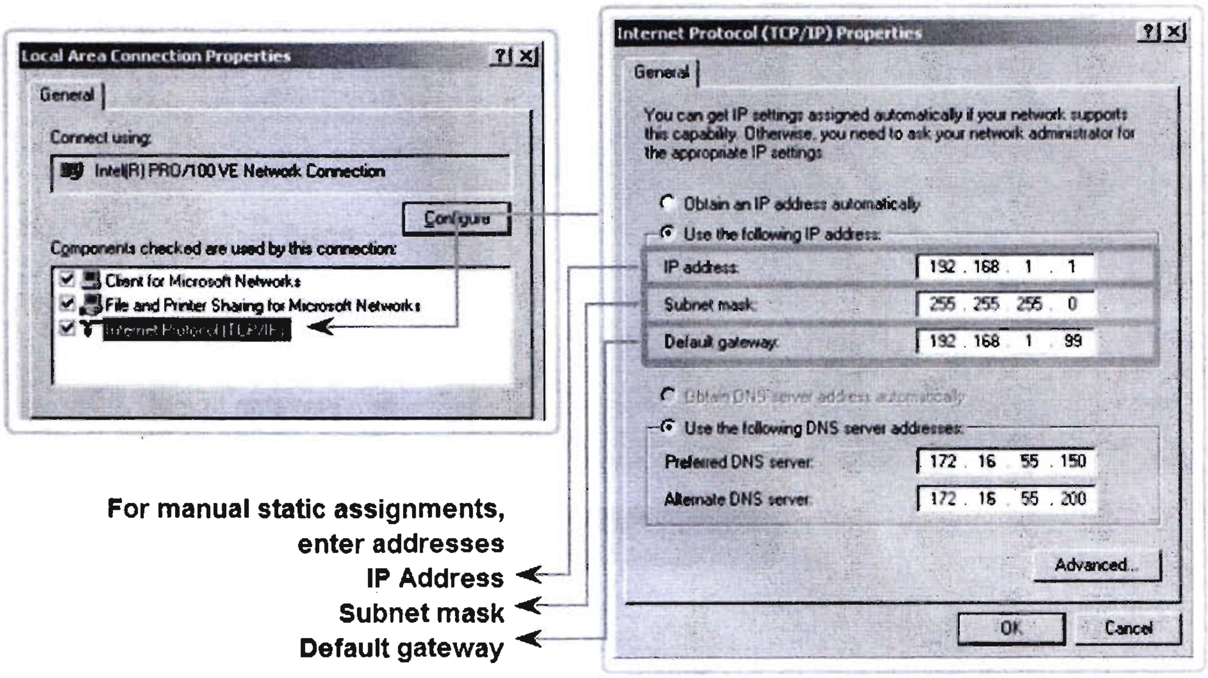
Static Assignment of Addresses

With a static assignment, the network administrator must manually configure the network information for a host, as shown in the figure. At a minimum, this includes entering the host IP address, subnet mask, and default gateway.

Static addresses have some advantages over dynamic addresses. For instance, they are useful for printers, servers, and other networking devices that need to be accessible to clients on the network. If hosts normally access a server at a particular IP address, it would cause problems if that address changed. Additionally, static assignment of addressing information can provide increased control of network resources. However, it can be time-consuming to enter the information on each host.

When using static IP addressing, it is necessary to maintain an accurate list of the IP address assigned to each device. These are permanent addresses and are not normally reused.

Addressing End Devices



Local Area Connection Properties

General

Connect using:

Intel(R) PRO/100 VE Network Connection

Configure

Components checked are used by this connection:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Internet Protocol (TCP/IP) Properties

General

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

○ Obtain an IP address automatically
● Use the following IP address:

IP address:	192 . 168 . 1 . 1
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 1 . 99

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server:	172 . 16 . 55 . 150
Alternate DNS server:	172 . 16 . 55 . 200

Advanced...

OK Cancel

For manual static assignments, enter addresses
IP Address
Subnet mask
Default gateway

Dynamic Assignment of Addresses

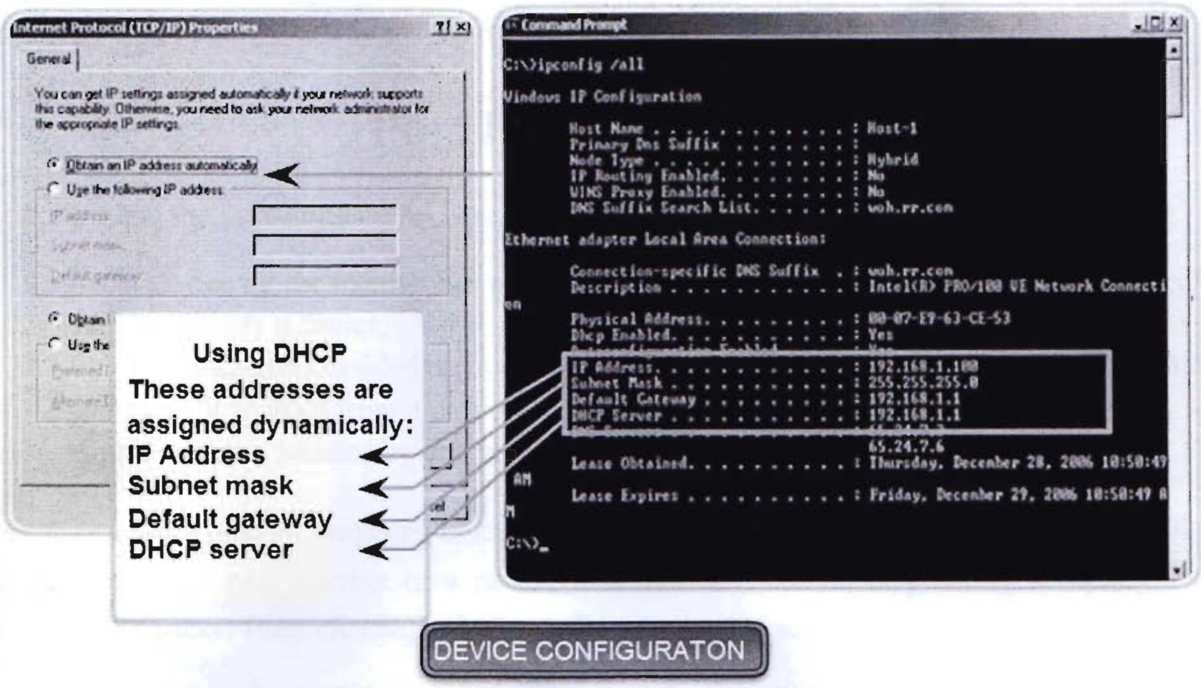
Because of the challenges associated with static address management, end user devices often have addresses dynamically assigned, using Dynamic Host Configuration Protocol (DHCP), as shown in the figure.

DHCP enables the automatic assignment of addressing information such as IP address, subnet mask, default gateway, and other configuration information. The configuration of the DHCP server requires that a block of addresses, called an address pool, be defined to be assigned to the DHCP clients on a network. Addresses assigned to this pool should be planned so that they exclude any addresses used for the other types of devices.

DHCP is generally the preferred method of assigning IP addresses to hosts on large networks because it reduces the burden on network support staff and virtually eliminates entry errors.

Another benefit of DHCP is that an address is not permanently assigned to a host but is only "leased" for a period of time. If the host is powered down or taken off the network, the address is returned to the pool for reuse. This feature is especially helpful for mobile users that come and go on a network.

Assigning Dynamic Addresses



Internet Protocol (TCP/IP) 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:
Subnet mask:
Default gateway:

● Obtain
○ Use the
Preferred
Alternate

Using DHCP
These addresses are assigned dynamically:
IP Address
Subnet mask
Default gateway
DHCP server

```
C:\>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : Host-1
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : woh.rr.com

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : woh.rr.com
        Description . . . . . . . . . . . : Intel(R) PRO/100 VE Network Connecti
on
        Physical Address. . . . . . . . . : 00-07-E9-63-CE-53
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DHCP Server . . . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . : 65.24.7.3
                                            65.24.7.6
        Lease Obtained. . . . . . . . . . : Thursday, December 28, 2006 10:50:49
 AM
        Lease Expires . . . . . . . . . . : Friday, December 29, 2006 10:50:49 A
M

C:\>_
```

Real IP

In data communication industry, there are some public IP blocks which are bought by some data communication company. When a client from different company needs public IP, some ISP or data communication company provides public static IP for which client has to pay a certain fee. Those public IPs are called “Real IP” or “Real Static IP”. Clients need Real IPs for several applications-

- For SMTP solution.
- For remote access to servers.
- For IP cameras.
- For remote bandwidth control etc.

For example, Infolink IT solution is a data communication company and it has three real IP blocks---

- 180.149.9.0 series.
- 180.149.13.0 series.
- 58.0.0.0 series.

Suppose one client needs to install IP camera and they already have our device. For that situation, if client asks for a Real IP to Infolink and Infolink will provide a real IP

180.149.13.129. For that real IP, client has to pay a certain yearly fee. With this real IP, client can access his IP camera through internet.

Port Forwarding

For understand the Port-Forwarding, we need to know couple of concepts. Those concepts are:

1. Every device on the internet has at least one ip address. The IP address is a number that is used to identify a device.
2. Every IP address is divided up into many ports. When one computer sends data to another computer, it sends it from a port on an ip address to a port on an ip address.
3. A port can only be used by one program at a time.

Port forwarding or **port mapping** is a name given to the combined technique of 1. translating the address and/or port number of a packet to a new destination, 2. possibly accepting such packet(s) in a packet filter (firewall), 3. forwarding the packet according to the routing table.

The destination may be a predetermined network port (assuming protocols like TCP and UDP, though the process is not limited to these) on a host within a NAT-masqueraded, typically private network, based on the port number on which it was received at the gateway from the originating host.

The technique is used to permit communications by external hosts with services provided within a private local area network.

Port forwarding, also known as tunneling, is basically forwarding a network port from one node to the other. This forwarding technique allows an outside user to access a certain port (in a LAN) through a NAT (network address translation) enabled router.

Advantages of Port Forwarding

Port forwarding basically allows an outside computer to connect to a computer in a private local area network. Some commonly done port forwarding includes forwarding port 21 for FTP access, and forwarding port 80 for web servers. To achieve such results, operating systems like the Mac OS X and the BSD (Berkeley Software Distribution) will use the pre-installed in the kernel, ipfirewall (ipfw), to conduct port forwarding. Linux on the other hand would add iptables to do port forwarding.

Disadvantages of Port Forwarding

There are a few downsides or precautions to take with port forwarding.

Only one port can be used at a time by one machine.

Port forwarding also allows any machine in the world to connect to the forwarded port at will, and thus making the network slightly insecure.

The port forwarding technology itself is built in a way so that the destination machine will see the incoming packets as coming from the router rather than the original machine sending out the packets.

Some well-known Ports

Name	Port(s)
FTP	21
Telnet	23
SMTP	25
DNS	53
HTTP	80
HTTPS	443

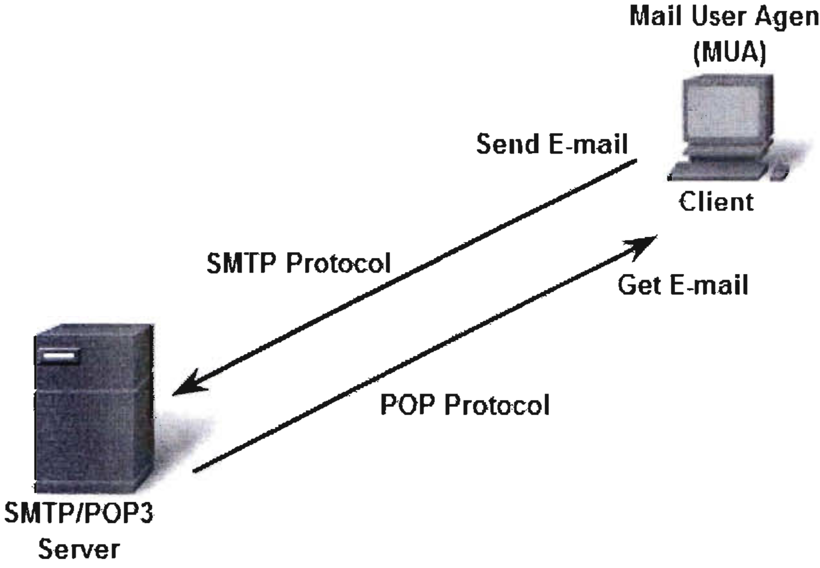
SMTP & POP

E-mail, the most popular network service, has revolutionized how people communicate through its simplicity and speed. Yet to run on a computer or other end device, e-mail requires several applications and services. Two example Application layer protocols are Post Office Protocol (POP) and Simple Mail Transfer Protocol (SMTP), shown in the figure. As with HTTP, these protocols define client/server processes.

When people compose e-mail messages, they typically use an application called a Mail User Agent (MUA), or e-mail client. The MUA allows messages to be sent and places received messages into the client's mailbox, both of which are distinct processes.

In order to receive e-mail messages from an e-mail server, the e-mail client can use POP. Sending e-mail from either a client or a server uses message formats and command strings defined by the SMTP protocol. Usually an e-mail client provides the functionality of both protocols within one application.

E-mail Client (MUA)



Clients send e-mails to a server using SMTP and receive e-mails using POP3.

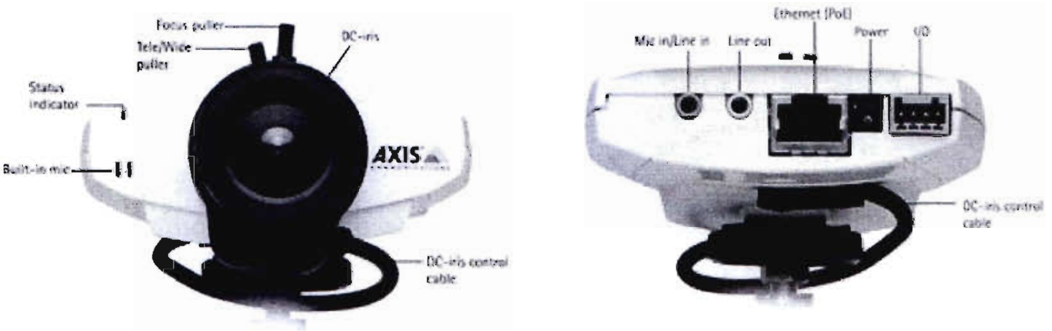
IP Camera

A network camera, often also called an IP camera, can be described as a camera and computer combined in one unit. The main components of a network camera include a lens, an image sensor, one or several processors, and memory. The processors are used for image processing, compression, video analysis and networking functionalities. The memory is used for storing the network camera's firmware (computer program) and for local recording of video sequences.

Like a computer, the network camera has its own IP address, is connected directly to a network and can be placed wherever there is a network connection. This differs from a web camera, which can only operate when it is connected to a personal computer (PC) via the USB or IEEE 1394 port, and to use it, software must be installed on the PC. A network camera provides web server, FTP (File Transfer Protocol), and e-mail functionalities, and includes many other IP network and security protocols.

A network camera connects directly to the network.

Front and back of a network camera.



Digital Video Recorder:

A **digital video recorder** (**DVR**) or **personal video recorder** (**PVR**) is a consumer electronics device or application software that records video in a digital format to a disk drive, USB flash drive, SD memory card or other local or networked mass storage device. The term includes set-top boxes with recording facility, portable media players (PMP) with recording facility, recorders (PMR as camcorders that record onto memory cards) and software for personal computers which enables video capture and playback to and from disk.

IP Camera Setup

Infolink Indoor modem and Outdoor modem supports IP Camera Solution. For this solution, there must need a Real IP. By this Real IP, user from remote place can access the IP Camera.

Requirements:

1. One DVR (Digital Video Recorder).
2. IP Camera.
3. An iphone or computer

This guide is for those who want to view a camera remotely. This guide will take you step by step through configuring a camera and an Iphone/computer. The reason behind this guide is to save you the hassle of figuring out what the dynamic address of your camera network is each time you want to view the camera.

Note: if you are on the same subnet as the camera than you will not need this guide.

Step 1: register a host name for dynamic DNS service

Step 2: Configure camera with a static IP address, DDNS profile, configure ports

Step 3: set up port forwarding on your router

Step 4: users and passwords

Step 5: configure an iphone or computer

Advantages

- Two-way audio via a single network cable allows users to communicate with what they are seeing (e.g. gas station clerk assisting a customer on how to use the prepay pumps).
- Flexibility: IP cameras can be moved around anywhere on an IP network
- Encryption & authentication: IP cameras offer secure data transmission through encryption and authentication methods such as WEP, WPA, WPA2, TKIP, AES.
- Remote accessibility: live video from selected cameras can be viewed from any computer, anywhere, and also from many mobile smart phones and other devices.
- IP cameras are able to function on a wireless network. Initial configuration has to be done through a router; after the IP camera is installed it can then be used on the wireless network. These cameras are used in navigation purpose in defence forces.
- PoE - Power over ethernet. Modern IP cameras have the ability to operate without an additional power supply. They can work with the PoE-protocol which gives power via the ethernet-cable.

Disadvantages

Higher initial cost per camera, except where cheap webcams are used.

- High network bandwidth requirements: a typical CCTV camera with resolution of 640x480 pixels and 10 frames per second (10 frame/s) in MJPEG mode requires about 3 Mbit/s.

- As with a CCTV/DVR system, if the video is transmitted over the public Internet rather than a private IP LAN, the system becomes open to hacking and hoaxing via internet. Criminals can hack into a CCTV system to observe security measures and personnel, thereby facilitating criminal acts and rendering the IP technology counterproductive.

Overview on Data Connectivity (Ether-CS)

Ethernet services represent a steadily growing portion of the fixed telecommunication market. To enable the provisioning of Ethernet services over IEEE 802.16e, the Mobile WiMAX network architecture supports transparent Ethernet transport as an optional extension to the IP services architecture. Ethernet support is tightly aligned to the IP services network model, and leverages many data path and control plane functions from its IP sibling to keep the implementation and operation overhead low for the Ethernet extension. Mobile WiMAX provides IP services as well as Ethernet services over the same mobile access network. The intrinsic mobility support may create new deployment opportunities for Ethernet services. Initially, the Ethernet extension may be mostly used to realize wireless access for DSL networks based on the same network interfaces defined for the wired Ethernet-based DSL aggregation. Ethernet services (often called carrier Ethernet services) have become common telecommunication services for establishing and connecting private networks of corporations, public authorities, or service providers, offering telecommunication services on top of the infrastructure of another network operator. Transparent layer 2 (L2) connectivity is provided based on Ethernet technologies due to its widespread availability, high scalability in terms of bandwidth as well as network size, excellent support of all kind of network layer protocols, and leading edge cost position.

Ethernet market in areas or cases when an appropriate wired infrastructure is not available. In particular, support of Ethernet services may be deployed by digital subscriber line (DSL) operators to extend their access networks based on Ethernet aggregation over a wireless infrastructure to customers without a phone line.

ETHERNET SERVICES

The Metro Ethernet Forum (MEF) has established a full set of specifications for the Introduction of Ethernet services, and the definition of the particular service attributes to facilitate commonly understood service level agreements between service providers and customers. Based on the concept of an Ethernet virtual connection (EVC), the MEF [1] distinguishes two kinds of Ethernet services (Next Fig.).

E-LINE SERVICE

E-Line service is a point-to-point connection carrying Ethernet frames between two customer interfaces of the network. It is frequently used for substituting legacy time-division multiplex (TDM) private lines with less expensive Ethernet private lines. When multiple point-to-point connections, each carrying its distinct service, are multiplexed onto a single Ethernet interface at the provider edge, the Ethernet private line service becomes an Ethernet virtual private line service, for example, Infolink used it to provide Internet service to multiple customers over a single Ethernet interface, a mode that is well supported by the bandwidth hierarchy of Ethernet interfaces.

E-LAN SERVICE

E-LAN service provides multipoint-to-multipoint connectivity for Ethernet frames across anumber of customer interfaces, essentially behaving like an extension to the customer's ownLAN. It is mostly deployed for creation of transparent LAN service (TLS), which enables full transparency for Ethernet control protocols and allows customers to establish new virtual LANs (VLANs) across their private networks without involvement of the Ethernet service provider.

Ether-CS Features

- Client can merge 2 or more LANs with their own IP as if all the branches are on the same LAN.
- Extra layer of security.
- Lower latency than our usual internet.

Ether-CS Advantages

- Provides more security.
- Flexibility and customizability.
- Makes really big networks manageable.

- Ideal for clients who requires data security and passage for intra-data volumes, or where many branches need to access one remote server.
- Target: Banks, Securities, Insurances, Financial Institutions, or any distributed network.

Ether-CS Common Problems

- Latency is too high (120-250 ms, unloaded) compared to other ISPs through fiber (2-20 ms).
- Upload constraint – it's 1/4th of assigned BW, also fluctuates a lot.
- Stability issues with Upload, Link.
- Not possible outside Dhaka and Chittagong at this moment.
- Impossible in situations where upload requirement is high.
- Can not go part-fiber .

Conclusion

In conclusion I have to attest my supervisor kamrul Shaker of Infolink . I really appreciate the way I have been guided through this internship program with **Infolink IT Solution company Ltd**, beginning from the opportunity to take the time I needed to refresh and expand my knowledge in several issues concerning Network Engineer, over a somehow protected period where I could discover and learn to value my new working environment, and finally earned the confidence to deal with assignments myself. It is through them that I did enjoy my work every day. Having a rare opportunity to use the knowledge and skills that I had acquired, I learned how to handle critical network problems and got new ideas. It was a great experience to work with networking devices practically and to troubleshoot different problems. According to my task of configuring router and switches; design of network structures of branches, I learned a lot about these.

Career-wise, the internship program undoubtedly will enrich my curriculum vitae (CV). Also, having gotten a chance to interact with most staff, I have had an insight on how to shape my career towards a humanitarian job in the near future.

The internship program gave me a chance not only to work with **INFOLINK IT SOLUTION LIMITED** but also a chance to learn from the good experts. This would reflect much onto my experience. Working with different business organizations was a rare chance for me.

Appendix

NAT	-	Network Address Translation
IP	-	Internet Protocol
LAN	-	Local Area Network
MAN	-	Metropolitan Area Network
WAN	-	Wide Area Network
VLAN	-	Virtual Local Area Network
DHCP	-	Dynamic Host Configuration Protocol
DNS	-	Domain Name System