Internet – interconnected network; network of networks that enables computers of all kinds to communicate and share services through the world.

ARPAnet – 1969; Advanced Research Project Agency Network; early packet-switching network and the first to implement TCP/IP protocol; It became the foundation of the internet; Other networks appeared as well: CSNET, BITNET.

Internet Characteristics

1. Complex Network – a network of networks; different types of protocols, computers, operating systems;
2. Disorganized – it is not organized, there are no rules by which websites should be made etc
3. Decentralized – no authority/organization controls the internet, www and internet society serve only as guidelines
4. Composed of billions of files – web sites, multimedia etc
5. Widely used – duh
6. International in Scope – duh
7. Dynamic – constantly changing, resources disappear, new data gets added
8. Expanding exponentially – duh

Internet Services

1. E-mail – 1970, most common service
2. Mailing lists – 1981 – group based messaging service through email
3. FTP – 1973 - duh
4. NewsGroups – 1979 – public messaging and bulletin board system
5. WWW – 1972 – web pages are created using HTML

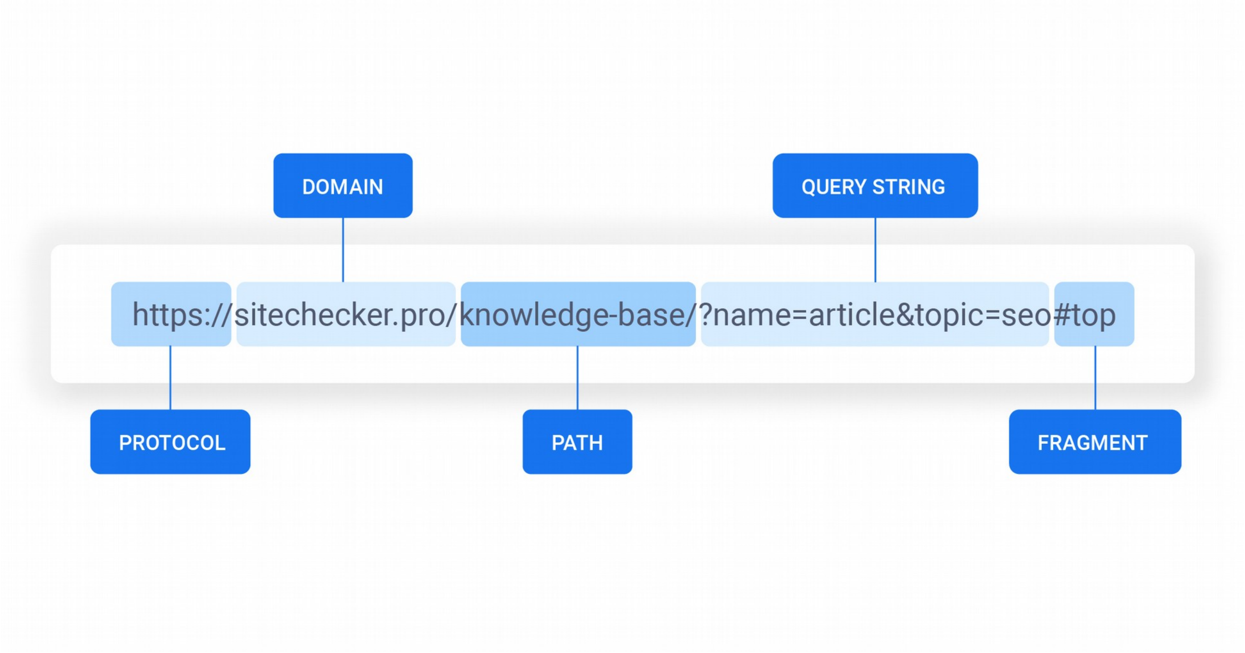
Elements of the Internet

A simplified hierarchical model of the internet includes: client, server, networks (composed of both clients and servers)

Hypertext – text with references (hyperlinks) to other text that the reader can immediately access. It allows navigation on a web page.
3 types of hyperlinks: text, image and image maps

Multimedia - A technology that facilitates an integration of text, audio, video, image, graphics and animation in digital form of computer.

URL – Uniform Resource Locator


DOMAIN
QUERY STRING
https://sitechecker.pro/knowledge-base/?name=article&topic=seo#top
PROTOCOL
PATH
FRAGMENT

Internet Protocol

Method by which data is sent from one computer over another over the network. Each computer has at least one IP address which uniquely identifies the computer from other computers. Responsible for addressing & sending of data from one to another computer.
Developed in 1970s, it is used together with TCP (TCP/IP).
Most networks use IPv4 (4 bytes), newer IPv6 standard has 16 bytes.

IPv4 – headers are minimum 20 octets (160 bits), define data length, flags, protocol, checksum, source and destination addresses etc.

IPv6 – bigger address space, enhancements over v4 for modern high speed networks, supports for multimedia data streams; not backwards compatible – all equipment and software must change;

Transmission Control Protocol (TCP) – Uses a set of rules to exchange messages with other internet points at the information packet level. Ensures a reliable connection by providing error control.

TCP PDU – Protocol Data Unit – single unit of information transmitted among peers of a network.

VAN (value added network) - a private network provider that focuses on offering network services such as secure email, message encryption and management reporting. Their goal is to facilitate EDI (electronic data interchange) among online companies, providing a convenient way for ecommerce businesses to securely communicate and share data.

How a VAN is created

When a common carrier such as a telecom company leases communication lines to a network provider and that provider then enhances those lines by adding additional services, it has created a Value Added Network. While EDI is the primary focus of VANs, the improvements or enhancements a network chooses to add is what differentiates networks.

Subnetting and Supernetting

In subnetting, a single big network is divided into multiple smaller subnetworks. In Supernetting, multiple networks are combined into a bigger network termed as a Supernetwork or Supernet.

SMTP – protocol for eMail delivery. Running on host provided by an ISP; Uses TCP; Used only for delivering mail.

Two ways of grabbing the messages from the server:

POP3 – Very simple protocol; Doesn't sync client and server; It deletes email from the server once it's downloaded, so if you download your mail on one computer, you won't be able to retrieve it on another, because it will already be deleted; It will only download mail from the Inbox folder; Folders aren't synced, so they may be different on different computers; It saves storage on the mail server;

IMAP – It keeps everything in sync, so what you see on one device will be identical to another; Doesn't delete email after downloading it;

MIME – standard which permits any kind of files and non-ASCII characters to be contained within eMail messages.

CGI – Common Gateway Interface - standard protocol for web servers to execute scripts which generates HTML, thus generating dynamic web pages. It allows an executable script to respond to an HTTP request, ex: POST request when submitting a form.

<u>Задачи:</u>

1) Given the IP address, find the beginning address (network address) – AND му прајш на IP адресата и на subnet mask. И то шо че го добијаш е одговоро.
2) What is the subnetwork address if the destination address is ____ and the subnet mask is ____ ? - исто ко погоре
3) Given the IP address ____ , design N subnets.
    1) Гледаш која е класата и според то одредуваш Default Subnet Mask

2) Го најдуваш најблискиио >= број шо е power of 2 (на пример 2^3) и додаваш 3 единици во Default Subnet Mask, така шо че добијаш Subnet Mask за subnet-ите

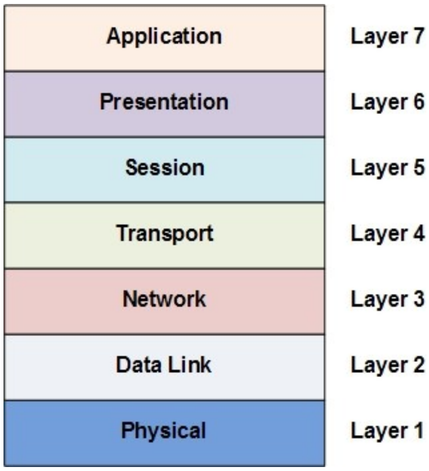
3) Number of subnets = 2^3 = 8
Number of addresses in each subnet = 2^(number of 0s in subnet mask)

4) A small organization is given a block with the beginning address and the prefix length ____/N (in slash notation). What is the range of the block?
- Number of addresses in the block = 2^Нулите од Subnet Mask (32-N)

5) What is the network address if one of the addresses is 167.199.170.82/27?
Смени ги последните 32 – 27 = 5 битој во нули и претвори ги пак во бројки.
=> 167.199.170.64/27

6) An organization is granted the block ______/N. The organization needs to have X subnets. What are the subnet addresses and the range of addresses for each subnet?
- Total number of addresses = 2^(32-N)
- Number of addresses in each subnet = total / X
- За секоја beginning и ending address of each subnet си додаваш после # of addresses

OSI Model - consists of seven different layers that are labeled from 1 through 7.



Application	Layer 7
Presentation	Layer 6
Session	Layer 5
Transport	Layer 4
Network	Layer 3
Data Link	Layer 2
Physical	Layer 1

The Physical Layer (Layer 1)

Layer 1 of the OSI model is named the physical layer because it is responsible for the transmission and reception of wire level data. For example, the physical layer is where it is dictated how bits are represented across a specific networking medium. The physical layer handles how data is physically encoded and decoded. Standards examples include IEEE 802.3 (Ethernet), IEEE 802.11 (Wireless Ethernet) and Synchronous optical networking (SONET) among others.

The Data Link Layer (Layer 2)

Layer 2 of the OSI model is named the data link layer and is responsible for link establishment and termination, frame traffic control, sequencing, acknowledgement, error checking, and media access management. The most familiar standards used at the data link layer include IEEE 802.3 (Ethernet) Media Access Control (MAC) and Logical Link Control (LLC) sublayers. The LLC acts as an interface between the physical layer and the MAC sublayer, and the MAC sublayer provides the ability for multiple terminals (computers) to communicate over the same physical medium. Other standards examples include Asynchronous Transfer Mode (ATM), High-Level Data Link Control (HDLC), Frame Relay and the Point to Point Protocol (PPP).

LLC – Logical Link Control – used to communicate with the upper layers of the application, and transition the packet to the lower layers for delivery.
It is implemented by software, typically the hardware part of the NIC / NIC driver (Network Interface Controller – aka network card).
The LLC sublayer takes the network protocol data, which is typically an IPv4 packet, and adds control information to help deliver the packet to the destination node.

MAC – Media Access Control - the lower sublayer of the data link layer.
It is implemented by hardware, i.e. the hardware part of the NIC.

The Network Layer (Layer 3)

Layer 3 of the OSI model is named the network layer and is where routing of network traffic begins. The network layer makes the traffic routing decisions and provides traffic control, fragmentation, and logical addressing (Internet Protocol (IP) addresses). The most common network layer protocol is IP, but other commonly used protocols include the Internet Control Message Protocol (ICMP) and Internet Group Message Protocol (IGMP).

The Transport Layer (Layer 4)

Layer 4 of the OSI model is named the transport layer and is responsible for message segmentation, acknowledgement, traffic control, and session multiplexing. The transport layer also has the ability to perform error detection and correction (resends), message reordering to ensure message sequence, and reliable message channel depending on the specific transport layer protocol used. The most common of the used transport layer protocols include the Transport Control Protocol (TCP) and User Datagram Protocol (UDP).

The Session Layer (Layer 5)

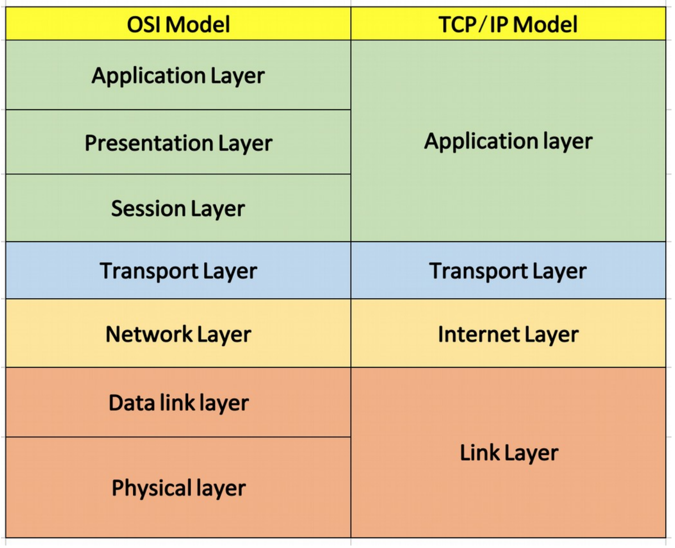
Layer 5 of the OSI model is named the session layer and is responsible for session establishment, maintenance and termination .

The Presentation Layer (Layer 6)

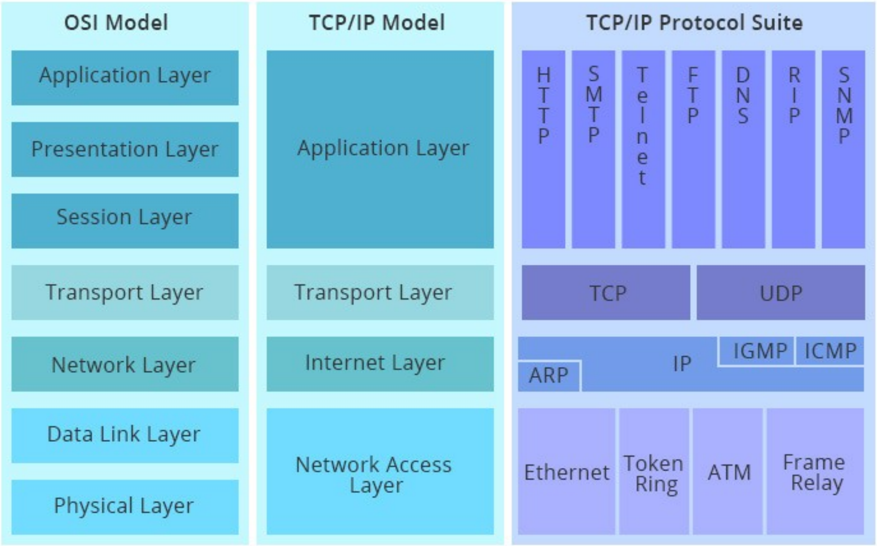
Layer 6 of the OSI model is named the presentation layer and is responsible for character code translation (i.e. ASCII vs. EBCDIC vs. Unicode), data conversion, compression, and encryption. Some common examples include Multipurpose Internet Mail Extensions (MIME), Transport Layer Security (TLS) and Secure Sockets Layer (SSL).

The Application Layer (Layer 7)

Layer 7 of the OSI model is named the application layer and is responsible for a number of different things depending on the application; some of these things include resource sharing, remote file access, remote printer access, network management, and electronic messaging (email). There are a large number of application layer protocols that are familiar to the common Internet user, including the File Transfer Protocol (FTP), Domain Name Service (DNS), Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP).

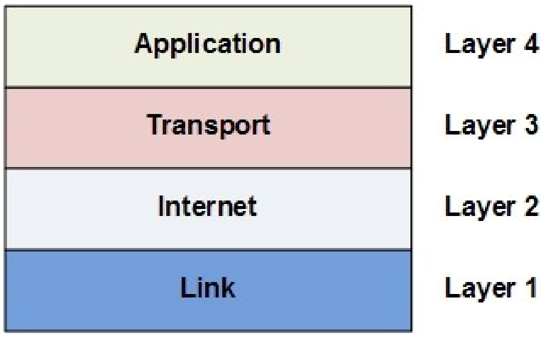


OSI Model	TCP/IP Model
Application Layer	Application layer
Presentation Layer	
Session Layer	
Transport Layer	Transport Layer
Network Layer	Internet Layer
Data link layer	Link Layer
Physical layer	



TCP/IP Model

Like the OSI model, the TCP/IP model is layered and is used in the same fashion as the OSI model but with fewer layers.



The Link Layer

The link layer is the lowest layer of the TCP/IP model. The link layer combines the physical and data link layer functions into a single layer. This includes frame physical network functions like modulation, line coding and bit synchronization, frame synchronization and error detection, and LLC and MAC sublayer functions. Common protocols include the Address Resolution Protocol (ARP), Neighbor Discovery Protocol (NDP), IEEE 802.3 and IEEE 802.11.

The Internet Layer

The Internet layer is the next layer up from the link layer and is associated with the network layer of the OSI model. Functions include traffic routing, traffic control, fragmentation, and logical addressing. Common protocols include IP, ICMP and IGMP.

The Transport Layer

The Transport layer is the next layer and is typically related directly with the same named layer in the OSI model. Functions include message segmentation, acknowledgement, traffic control, session multiplexing, error detection and correction (resends), and message reordering. Common protocols include the Transport Control Protocol (TCP) and User Datagram Protocol (UDP).

The Application Layer

The Application layer is the highest layer in the TCP/IP model and is related to the session, presentation and application layers of the OSI model. The application layer of the TCP/IP model is used to handle all process-to-process communication functions. Common protocols include Named Pipes, NetBIOS, MIME, TLS, SSL, FTP, DNS, HTTP, SMTP and many others.

Subnet Mask

A mask is a 32-bit binary number. Actually it's a 32-bit value that is used to distinguish the network ID from the host ID in an arbitrary IP address. The mask is AND with IP address to get the block address(Network address).

Mask AND IP address = Block Address

A network mask determines which portion of the address identifies the network and which portion of the address identifies the node. Class A, B, and C networks have default masks, also known as natural masks, as shown here:

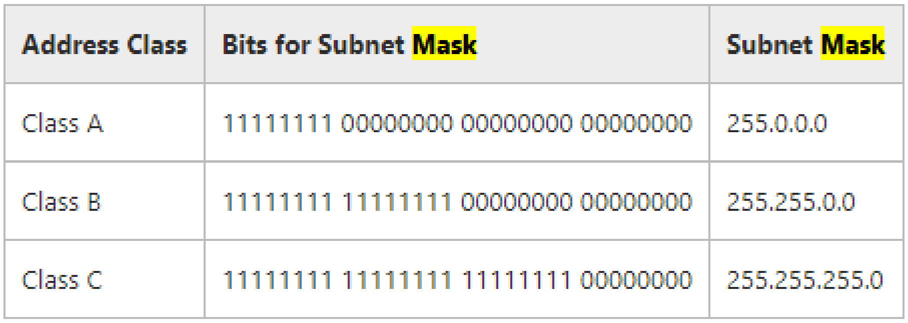
Class A: 255.0.0.0

Class B: 255.255.0.0

Class C: 255.255.255.0

Subnet masks are frequently expressed in dotted decimal notation. After the bits are set for the network ID and host ID portion, the resulting 32-bit number is converted to dotted decimal notation.

Example:



Address Class	Bits for Subnet Mask	Subnet Mask
Class A	11111111 00000000 00000000 00000000	255.0.0.0
Class B	11111111 11111111 00000000 00000000	255.255.0.0
Class C	11111111 11111111 11111111 00000000	255.255.255.0

Subnetting and Supernetting

(Subnetting) When a large network is subnetted, the network is divided into at least two smaller subnetworks, with each subnetwork (subnet) having its own subnetwork address (subnetid). In subnetting you borrow bits from the host part.

(Supernetting) When supernetting is performed, several networks are combined to create one large network, or supernetwork. Supernetting is done by borrowing bits from the network side.

Rules:

1. The number of blocks must be a power of 2 (1, 2, 4,8, 16, . . .).

2. The blocks must be contiguous in the address space (no gaps between the blocks).

3. The third byte of the first address in the superblockmust be evenly divisible by the number of blocks. Inother words, if the number of blocks is N, the third byte must be divisible by N.

The User Datagram Protocol (UDP) is called a connectionless, unreliable transport protocol. It does not add anything to the services of IP except to provide process-to-process communication instead of host-to-host communication. It's used primarily for establishing low-latency and loss tolerating connections between applications on the Internet.Both UDP and TCP run on top of the Internet Protocol (IP) and are sometimes referred to as UDP/IP or TCP/IP. Both protocols send short packets of data, called datagrams. UDP assumes that error-checking and correction is not required so it does not require

A datagram is "a self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network."

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Transmission Control Protocol (TCP) is a connection-oriented protocol; it creates a virtual connection between two TCPs to send data. In addition, TCP uses flow and error control mechanisms at the transport level. A connection is established and maintained until the application programs at each end have finished exchanging messages. It determines how to break application data into packets that networks can deliver, sends packets to and accepts packets from the network layer, manages flow control, and—because it is meant to provide error-free data transmission—handles retransmission of dropped or garbled packets as well as acknowledgement of all packets that arrive.

They are both build on top of the Internet protocol. In other words, whether you are sending a packet via TCP or UDP, that packet is sent to an IP address.

DNS (new)

- An iterative query is one where the DNS server may provide a partial answer to the query (or give an error). DNS servers must support non-recursive queries.
- A recursive query is one where the DNS server will fully answer the query (or give an error). DNS servers are not required to support recursive queries and both the resolver (or another DNS acting recursively on behalf of another resolver) negotiate use of recursive service using bits in the query headers.

DNS

- A DNS query is the process of a computer or networking device making an inquiry to get an IP address for a DNS name such as w3.org

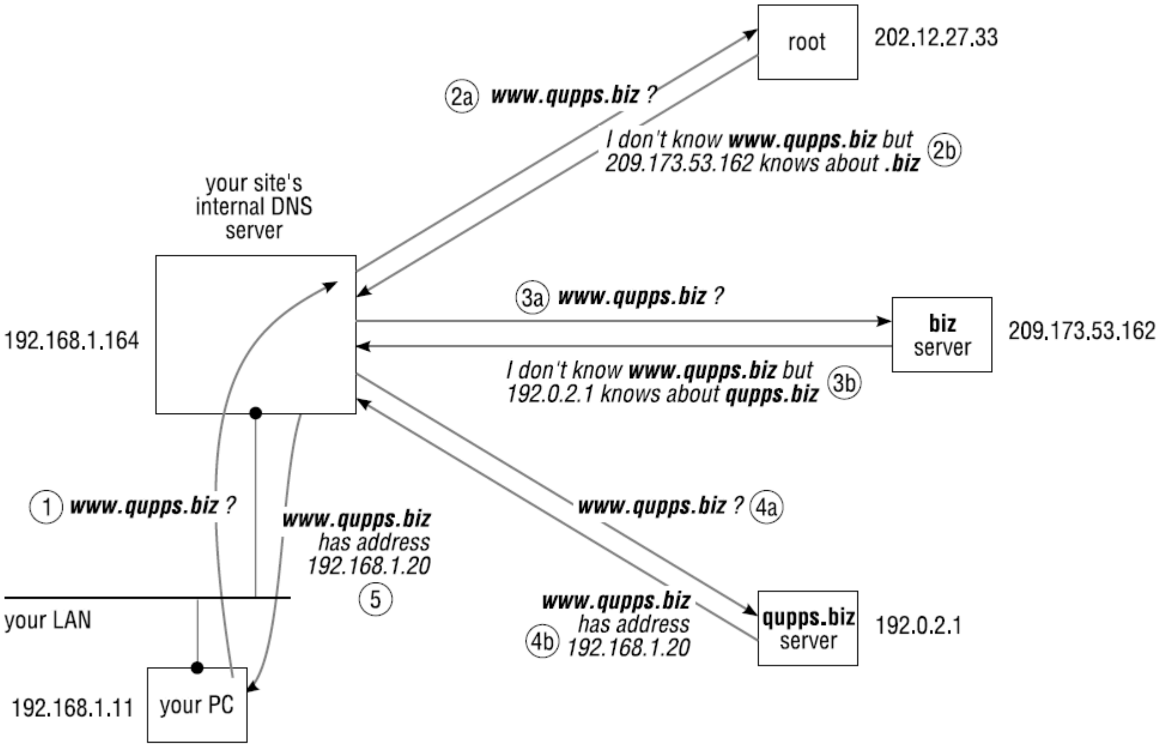
The client computer will send a DNS query to one of their internet service provider's DNS servers. The DNS server looks in it's DNS database to tell whether it can answer the query authoritatively. If the DNS server can answer authoritatively, the DNS server answers the query and the DNS query process is complete.

If the server cannot answer the query authoritatively it will look in its DNS cache of previous queries. If the DNS server finds a matching entry in its cache, it will answer the query with a non-authoritative answer based on the information in its cache and the DNS query process is complete.

- Types of DNS Resolutions:

Mapping a name to an address or an address to a name is called name-address resolution. It can be Recursive or Iterative Resolution.

Recursive: – The client machine sends a request to the local name server, which, if it does not find the address in its database, sends a request to the root name server, which, in turn, will route the query to an intermediate or authoritative name server. Note that the root name server can contain some hostname to IP address mappings. The intermediate name server always knows who the authoritative name server is.


root
202.12.27.33
2a www.qupps.biz ?
I don't know www.qupps.biz but 209.173.53.162 knows about .biz 2b
your site's internal DNS server
192.168.1.164
3a www.qupps.biz ?
biz server
209.173.53.162
I don't know www.qupps.biz but 192.0.2.1 knows about qupps.biz 3b
1 www.qupps.biz ?
www.qupps.biz has address 192.168.1.20
5
www.qupps.biz ? 4a
www.qupps.biz has address 192.168.1.20 4b
qupps.biz server
192.0.2.1
your LAN
192.168.1.11
your PC

- New domains are added to DNS is done through a registrar, a commercial entity accredited by ICANN. A registrar first verifies that the requested domain name is unique and then enters it into the DNS database. A fee is charged.

DDNS (Dynamic Domain Name Systems)

When the DNS was designed, no one predicted that there would be so many address changes. In DNS, when there is a change, such as adding a new host, removing a host, or changing an IP address, the change must be made to the DNS master file. The DNS master file must be updated dynamically. The Dynamic Domain Name System (DDNS) therefore was devised to respond to this need.

Dynamic DNS is a method of automatically updating a name server in the Domain Name System, often in real time, with the active DDNS configuration of its configured hostnames, addresses or other information

DNS SERVERS

Root name servers

- contacted by local name server that can not resolve name

– contacts authoritative name server if name mapping not known – gets mapping

– returns mapping to local name server

Top-level domain (TLD) servers:

– responsible for com, org, net, edu, etc., and all top-level country domains uk, fr, ca, jp.

– Network Solutions maintains servers for com TLD

– Educause for edu TLD

Authoritative DNS servers:

– organization’s DNS servers, providing authoritative hostname to IP mappings for organization’s servers (e.g.,Web, mail).

– can be maintained by organization or service provider

Local Name Server

-does not strictly belong to hierarchy

-each ISP (residential ISP, company, university) has one. – also called “default name server”

-when host makes DNS query, query is sent to its local DNS server – acts as proxy, forwards query into hierarchy

Ethernet is the most widely installed local area network (LAN) technology. Ethernet is a link layer protocol in the TCP/IP stack, describing how networked devices can format data for transmission to other network devices on the same network segment, and how to put that data out on the network connection.

An Ethernet cable is the most common type of network cable used on a wired network whether at home or in any other business establishment. This cable connects wired devices together to the local network for file sharing and Internet access.