



IT3010

Network Design and Management

Lecture 03 Network Servers

Shashika Lokuliyana

Faculty of Computing
Department of CSE

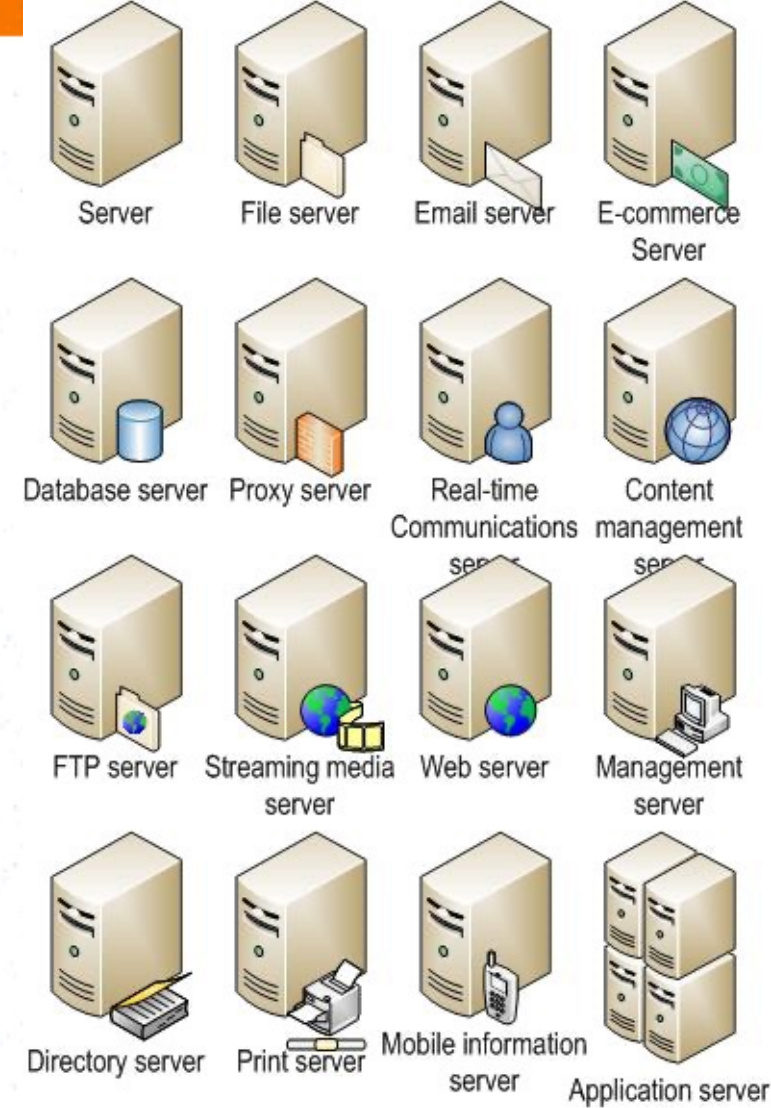


SLIIT

Discover Your Future

To be Covered...!!!

- ❖ Client – Server Architecture
- ❖ Domain Name System (DNS)
- ❖ Dynamic Host Configuration Protocol (DHCP)
- ❖ Audit
- ❖ Network Mapping
- ❖ Baselineing



Networked applications cont..



- ❖ Read write data over network
- ❖ Dominant model : bidirectional, reliable byte stream connection
 - On-side reads what the other writes
 - Operates in both directions
 - Reliable (unless connection breaks)

Server & Client



- **Server** is a piece of software that manage's a shareable resource.
- Usually the resource resides at one location in the network and the server is run on the computer at which the resource resides.
- The server offers acceptable level of service to the users.
- The mechanism of accessing this server are hidden from the network user by interface software which resides at the separate stations, usually referred to as the **client**.

Client-server model

- Standard model for developing network applications
- Notion of client and server:
 - A server is a process that is offering some service.
 - A client is a process that is requesting the service
 - Server or client may be running in different machines.
 - Server waits for requests from client(s).
- Roles of the client and the server processes are asymmetric.

Domain name system (DNS)



Domain Name System



*“The Domain Name System (**DNS**) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network.*

Wikipedia

Name server

- A name server is a computer hardware or software server that implements a network service for providing responses to queries against a directory service.
- It translates an often humanly-meaningful, text-based identifier to a system-internal, often numeric identification or addressing component.
- **What is Naming?**
 - A naming scheme must provide the facility to identify uniquely entities across the entire network.
 - Naming is associated with an addressing mechanism since it does not only provide a unique identifier but also the location of existence.

What is dns?

- The Internet maintains two principal namespaces, the domain name hierarchy and the Internet Protocol (IP) address spaces (RFC 781)

A container for a set of identifiers (aka symbols, names)

A ranked system

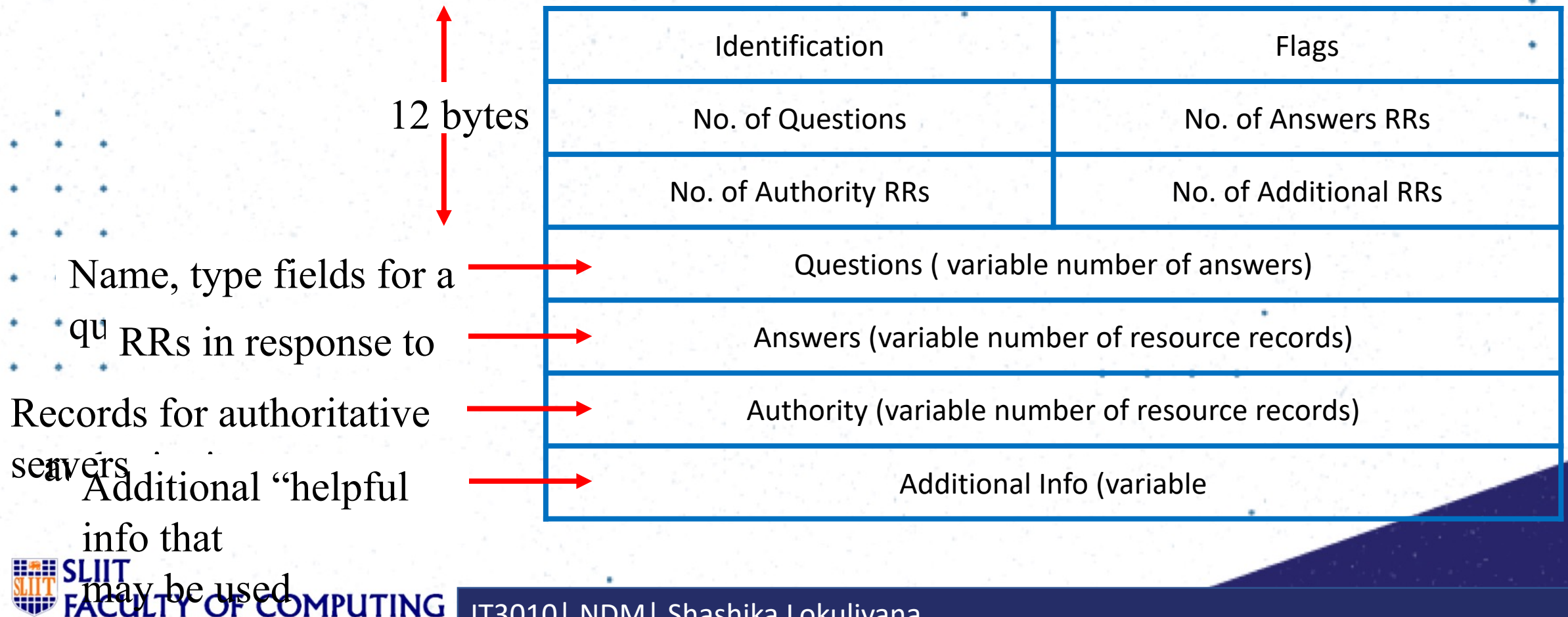
A certain kinds of partial ordered sets

*A unique name that identifies a website
(RFC-1034) - URL*

- The Domain Name System maintains the domain name hierarchy and provides translation services between it and the address

Why use a domain name (URL) and not the IP ???

DNS message format



DNS Header Fields

❖ Identification

- Used to match up request/response

❖ Flags 1-bit each to mark

- Query or response
- Authoritative or not
- Recursive resolution
- To indicate support for recursive resolution

DNS Record

RR format : *(class, name, value, type, ttl)*

- DB contains tuples called resource records (RRs)
- • Classes = Internet (IN), Chaosnet (CH), etc.
- • Each class defines value associated with type

DNS Record cont.....

For “IN” class:

- **Type = A**

- **name** is hostname
- **value** is IP address

- **Type = CNAME**

- **name** is an alias name for some “canonical” name
- **value** is canonical name

Type = NS

- **name** is domain (e.g. foo.com)
- **value** is name of authoritative name server for this domain

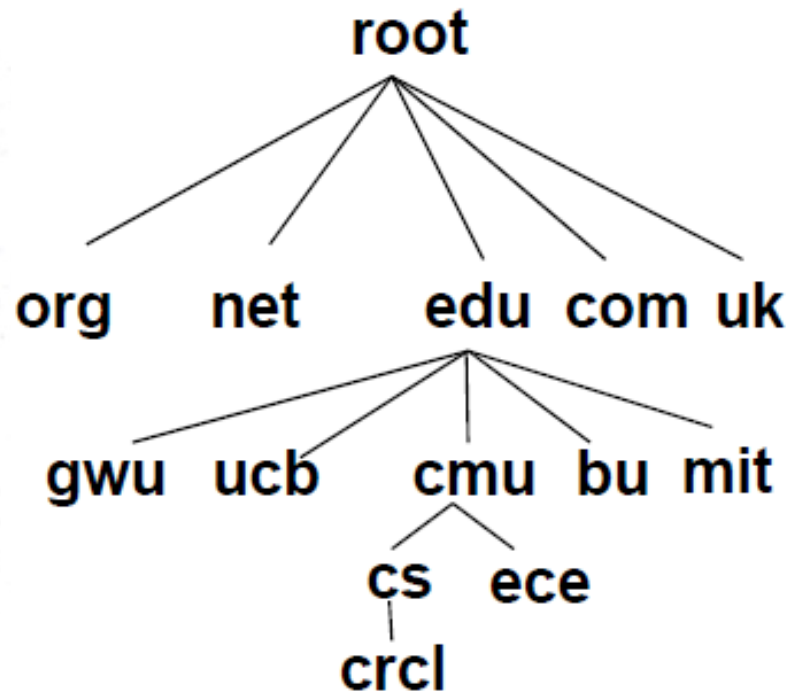
Type = MX

- **value** is hostname of mailserver associated with **name**

Properties of DNS Host Entries

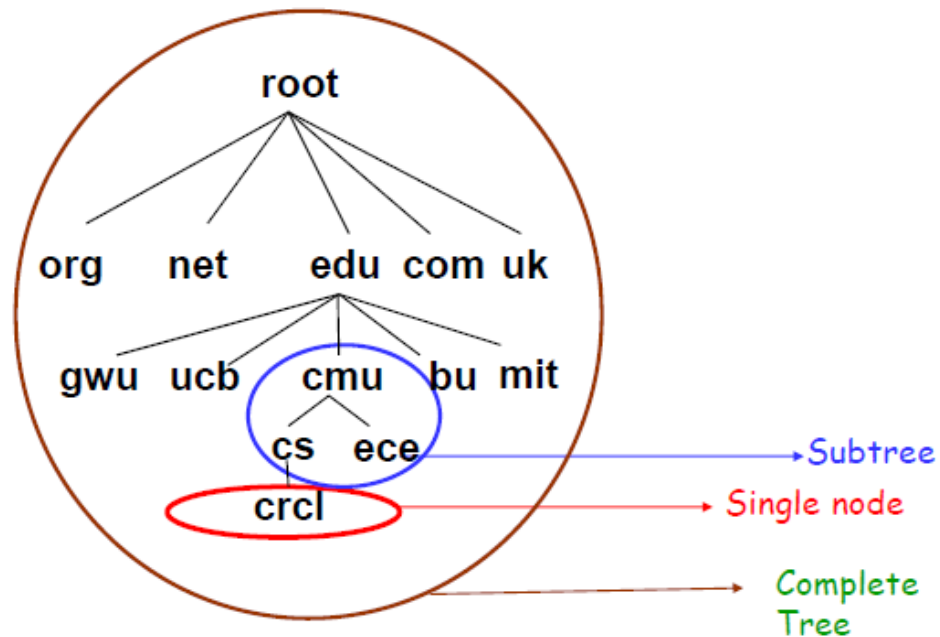
- Different kinds of mappings are possible:
 - ❖ 1-1 mapping between domain name and IP addr:
 - provolone.crcl.cs.cmu.edu maps to 128.2.218.81
 - ❖ Multiple domain names maps to the same IP addr:
 - www.scs.cmu.edu and www.cs.cmu.edu both map to 128.2.203.164
 - ❖ Single domain name maps to multiple IP addresses:
 - www.google.com map to multiple IP addrs.
 - ❖ Some valid domain names don't map to any IP addr:
 - crcl.cs.cmu.edu doesn't have a host

DNS Design: Hierarchy Definitions



- Each node in hierarchy stores a list of names that end with same suffix
- Suffix = path up tree
- E.g., given this tree, where would following be stored:
- Amal.com
- Amal.edu
- Amal.cmu.edu
- Amal.crcl.cs.cmu.edu
- Amal.cs.mit.edu

DNS Design: Zone Definitions



- Zone = contiguous section of name space
- E.g., Complete tree, single node or subtree
- A zone has an associated set of name servers
- Must store list of names and tree links

DNS Design: cont...

❖ Zones are created by convincing owner node to create/delegate a subzone

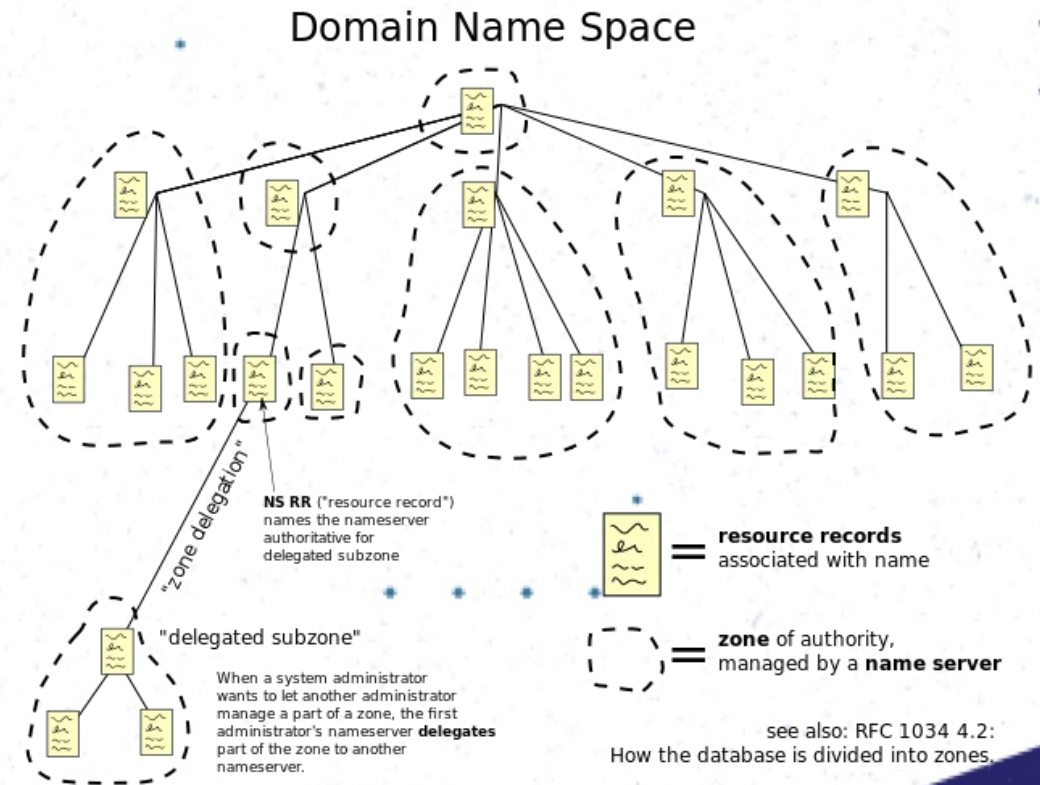
- Records within zone stored in multiple redundant name servers
- Primary/master name server updated manually
- Secondary/redundant servers updated by zone transfer of name space
 - Zone transfer is a bulk transfer of the “configuration” of a DNS server – uses TCP to ensure reliability

❖ Example:

- CS.CMU.EDU created by CMU.EDU admins
- Who creates CMU.EDU or .EDU?

DNS: Root Name Servers

- ❖ Responsible for “**root**” zone
- ❖ 13 root name servers
 - ❖ Currently
`{a-m}.root-servers.net`
- ❖ Local name servers contact root servers when they cannot resolve a name



Servers/Resolvers

- ❖ Each host has a resolver
 - Typically a library that application can link to local name servers (i.e. /etc/resolv.conf)
- ❖ Name server
 - Either responsible for some zone or
 - Local servers
 - Do lookup of distant host names for local hosts
 - Typically answer queries about local zones



Lookup Methods

- Recursive query:

- Server goes out and searches for more information
- Only returns the final answer or “not found”

- Iterative query:

- Server responds with as much as it knows.
- “I don’t know this name but ask this server”

Workload impact on choice?

- ❖ Root/distant server does
- ❖ Local server typically does

Workload and Caching

- **DNS responses are cached**
 - ❖ Quick response for repeated translations
 - ❖ Other queries may reuse some parts of lookup
 - E.g., NS records for domains
- **DNS negative queries are cached**
 - ❖ Don't have to repeat past mistakes
 - ❖ E.g., misspellings, search strings in resolv.conf

Cached data periodically times out

- ❖ Lifetime (TTL) of data controlled by owner of data
- ❖ TTL passed with every record

Reliability

- ❖ DNS servers are replicated
 - Name service available if \geq one replica is up
 - Queries can be load balanced between replicas
- ❖ UDP used for queries
 - Why not just use TCP?
- ❖ Try alternate servers on timeout
 - Exponential backoff when retrying same server
- ❖ Same identifier for all queries
 - Don't care which server responds

Dynamic Host Configuration Protocol (DHCP)

192.168.1.18

⋮

192.168.1.19

⋮

192.168.1.20

Dynamic Host Configuration Protocol



The Dynamic Host Configuration Protocol (**DHCP**) is a standardized networking protocol used on Internet Protocol (**IP**) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With **DHCP**, computers request IP addresses and networking parameters automatically from a **DHCP** server, reducing the need for a network administrator or a user to configure these



What a Device needs

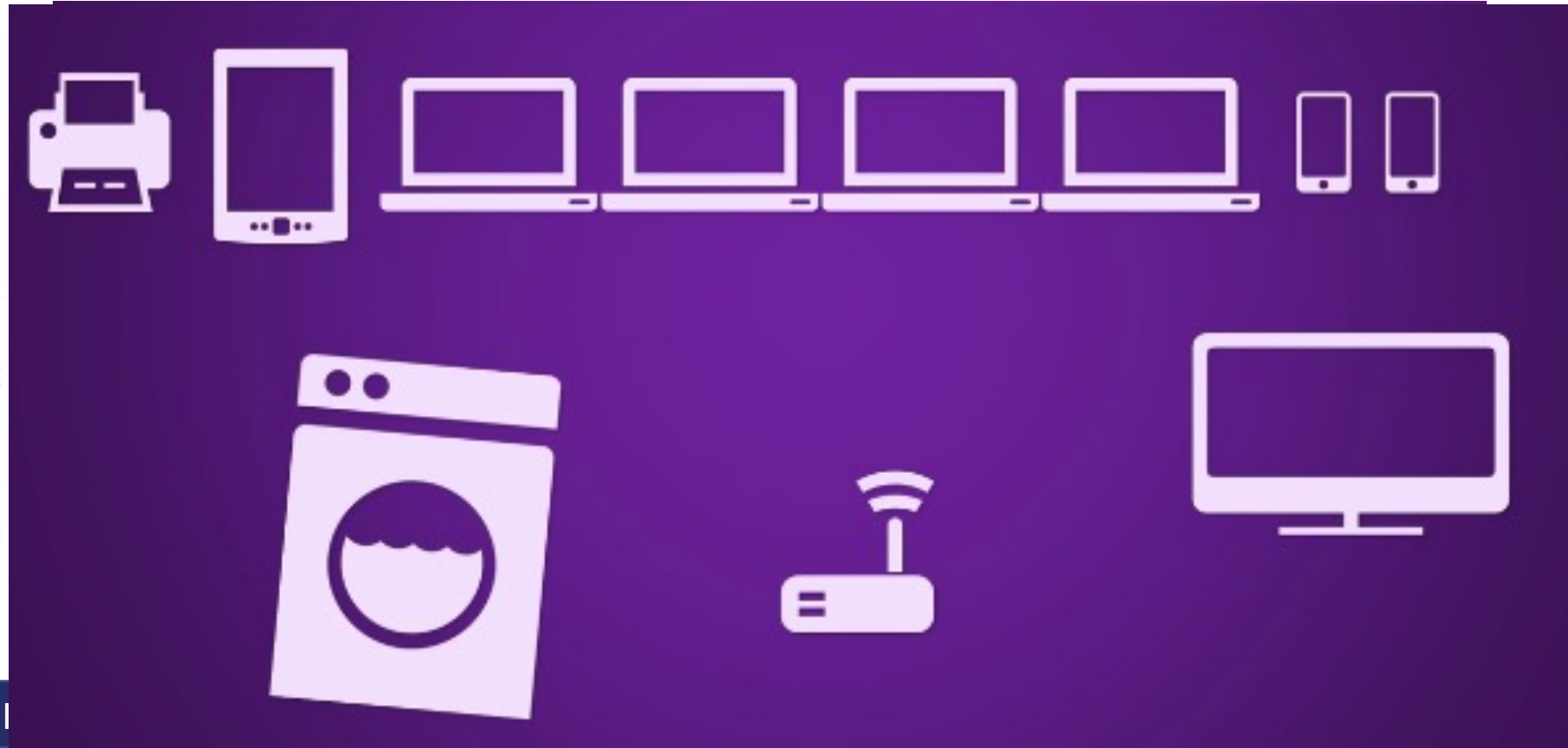
- Most computers today need four pieces of information:
 - 1) IP address => to uniquely define itself in an network
 - 2) Subnet mask => to define which network (or sub network) the device belongs to
 - 3) Address of a default router => to be able to communicate with other networks
 - 4) Address of a name server => to be able to use names instead of addresses

A world without DHCP

- Manual IP address allocation

**How much time it
would consume?**

**What if it was
wrongly configured
and had to
reconfigure again?**



DHCP – Dynamic Host Configuration Protocol

- ❖ Issues or leases dynamic IP addresses to clients in a network
- ❖ The lease can be subject to various conditions
 - Duration
 - Computer ID etc.





IP Address Assignment

- ❖ The DHCP server assigns or leases a client an IP address for a predetermined period of time
- ❖ In most cases, the IP address is automatically renewed when a client logs into a network
- ❖ The IP address assigned is taken from a pool of IP addresses defined as the scope of IP addresses available for assignment.

If a windows user:

A user can manually release and renew an IP address by typing the commands??

If Linux user??

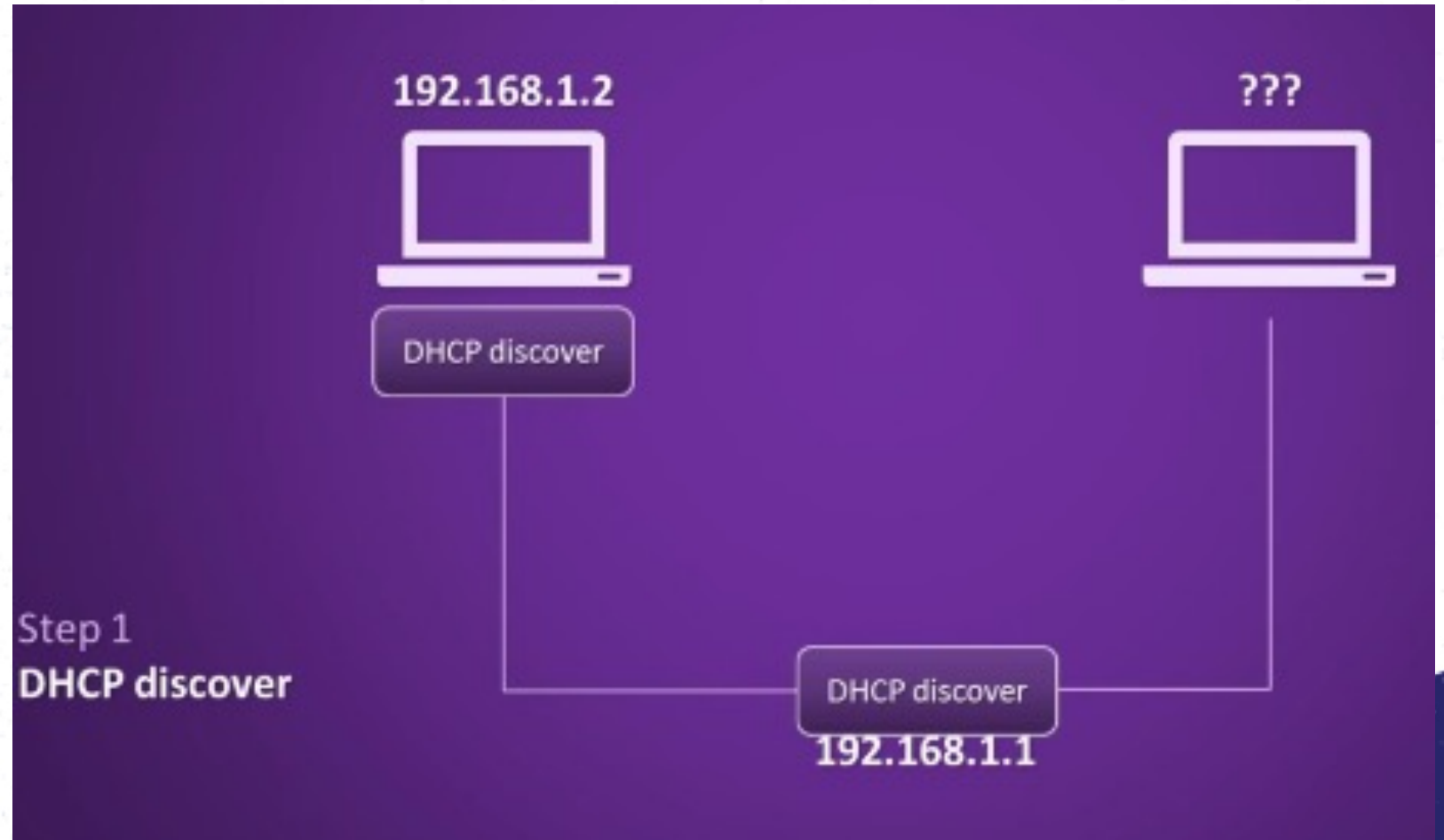


Assignment Conditions

- ❖ IP addresses can be reserved for clients based on MAC addresses and host names
- ❖ For security, the lease of IP addresses can be restricted to clients with known MAC addresses
- ❖ Some IP addresses may be excluded so that they could be reserved for assignment to servers as static addresses
 - Servers, in general, requires the assignment of static addresses
 - The router address is also normally excluded
- ❖ Specific or a range of IP addresses may be excluded in this manner

How DHCP server work

- Host searches for any available DHCP servers to get an address from.

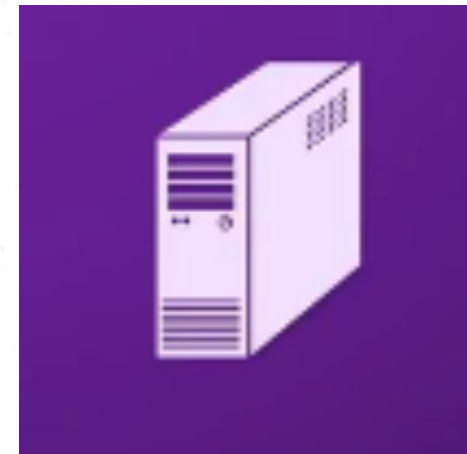


Multiple DHCP servers

- ❖ Multiple servers can respond with an address offer
- ❖ New host chooses one offer
- ❖ Servers see which offer the client picked.



DHCP Server



DHCP Client

DHCP Message types

- ***DHCPDISCOVER***
- ***DHCPOFFER***
- ***DHCPREQUEST***
- ***DHCPACK***
- ***DHCPNAK***
- ***DHCPDECLINE***
- ***DHCPINFORM***
- ***DHCPRELEASE***



Audit

Network management should **start** with an **audit**,

- ☐ Document/Map the entire network.
- ☐ Evaluate and baseline the physical and data link layer infrastructure.
- ☐ Evaluate and baseline network traffic and protocols.
- ☐ Evaluate and baseline platforms, operating systems and applications.
- ☐ Evaluate security

Network Mapping Definition

Network mapping in general is getting to know your network inside-out.

- ☐ Detailed description of everything
- ☐ Complex networks are difficult to visualize
- ☐ Big rewards
- ☐ Time consuming, boring!

Network Mapping OSI

- ☐ Physical Layer
- ☐ Data Link Layer
- ☐ Network Layer
- ☐ Transport Layer
- ☐ Session Layer
- ☐ Presentation Layer
- ☐ Application Layer

OSI model: Open Systems Interconnection model

- The OSI model defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.
- Forouzan, *TCP/IP Protocol Suite*, Section 2.2 provides a concise description about OSI model. Following subsections are a summary or this reference. You are required to read this section of the book.

Physical Layer

- Coordinates the functions required to **carry bit streams over the physical medium**.
- Deals with the mechanical and electrical specifications of the interface and transmission media.
- Defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur.

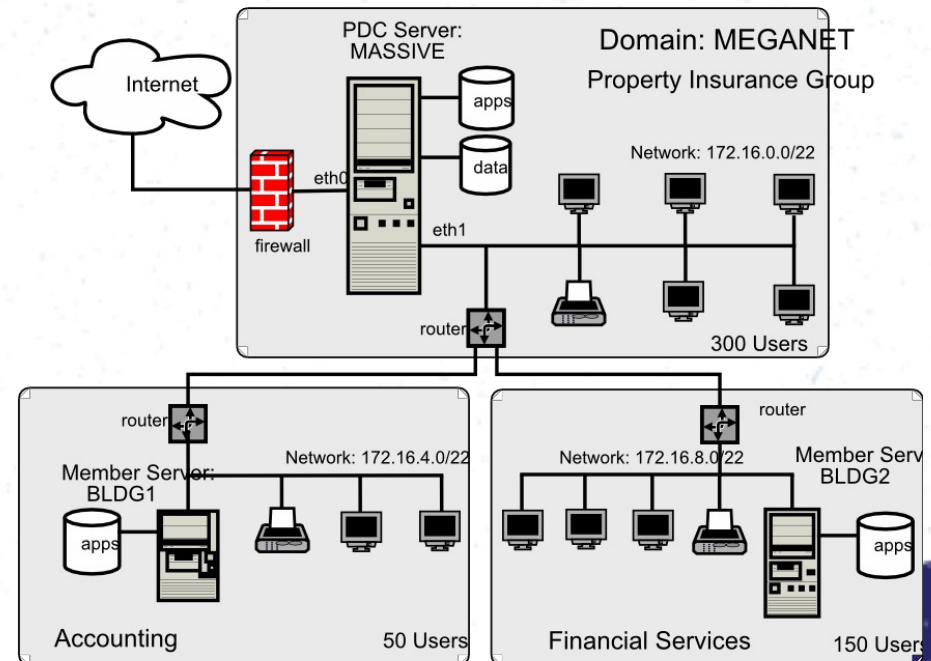
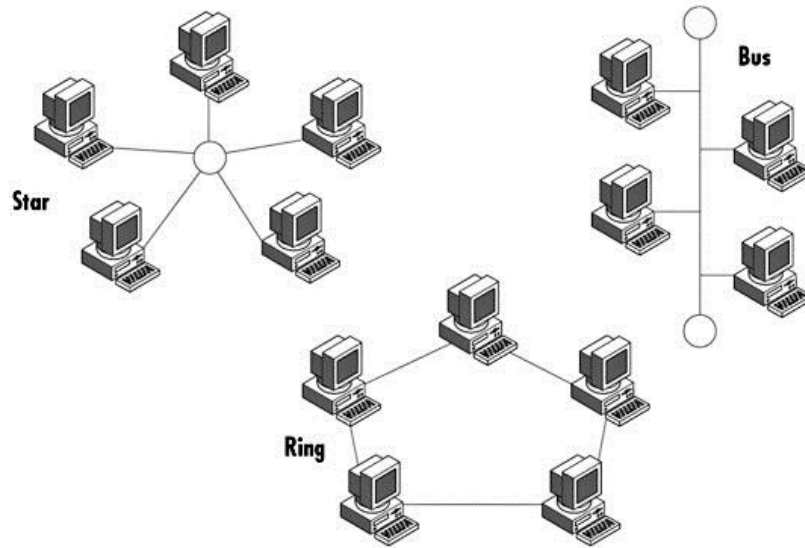
Key points:

Physical characteristics of interfaces and media,
Representation of bits, Data rate, Synchronization of bits,
Line configuration, Physical topology, Transmission mode.

Mapping the Physical Layer

- The Biggest Job
 - Every Device
 - Cabling Patch Panels
- Topology and Topography

Topology Vs. Topography



Data Link Layer

- This layer transforms the physical layer (a raw transmission facility), **to a reliable link**.
- It makes the physical layer appear **error free** to the upper layer (network layer).
- The data link layer is divided into two sub layers:
 - ❑ **The Media Access Control (MAC) layer**
The MAC sub layer controls how a computer on the network gains access to the data and permission to transmit it.
 - ❑ **Logical Link Control (LLC) layer**
The LLC layer controls frame synchronization, flow control and error checking.

Key points:

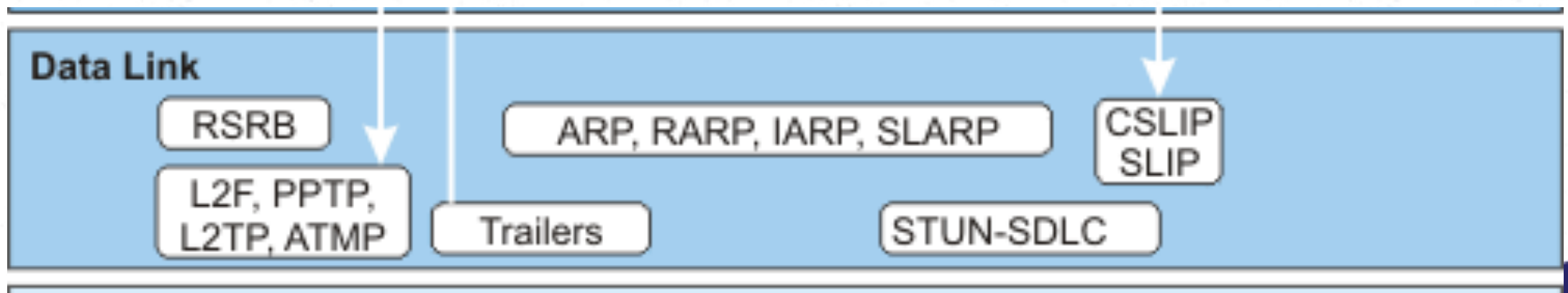
Framing, Physical addressing, Flow control, Error control, Access control to the link.



Mapping the Data Link Layer

- NIC (Network Interface Card)

A **network interface card (NIC)** is a hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called **network interface controller**, **network adapter** or LAN adapter.



Network Layer

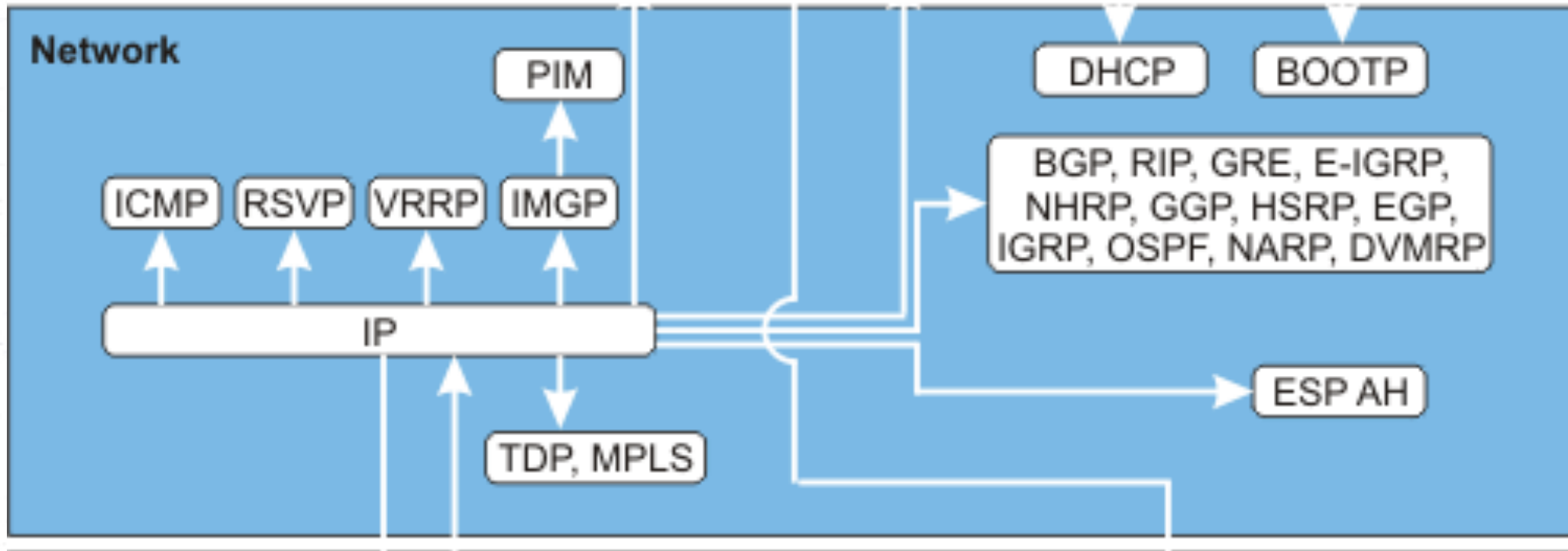
- Network layer is responsible for the **source-to-destination delivery** of a packet, whereas, the data link layer oversees the hop-to-hop delivery.
- Ensures that each packet gets from its point of origin to its final destination.

Key points:

Logical addressing, Routing.



Mapping the Network Layer



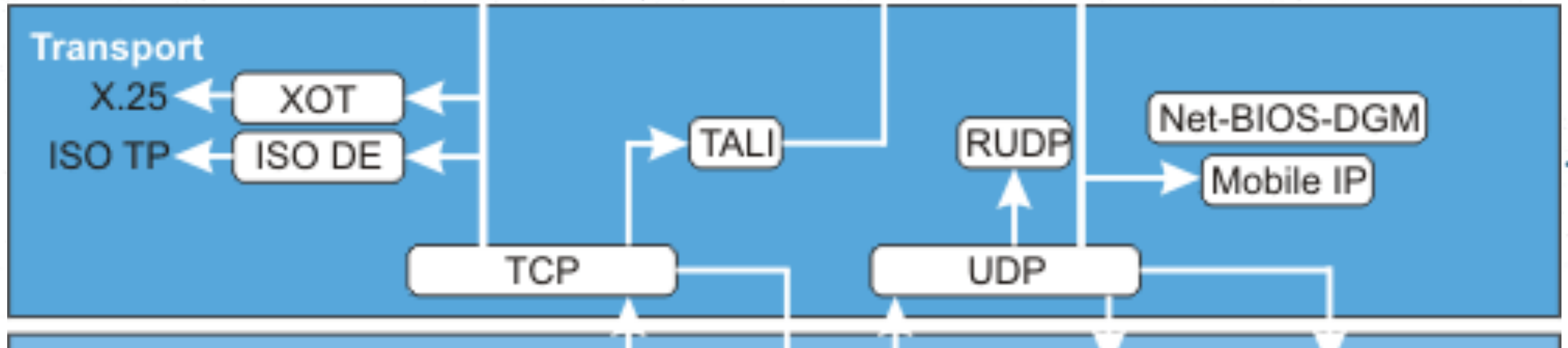
Transport Layer

- Transport layer is responsible for **process-to-process delivery of the entire message**.
- Ensures that the whole message arrives **intact and in-order**.

Key points:

Service-point addressing (aka port addressing),
Segmentation and reassembly, Connection control, Flow control, Error control.

Mapping the Transport Layer



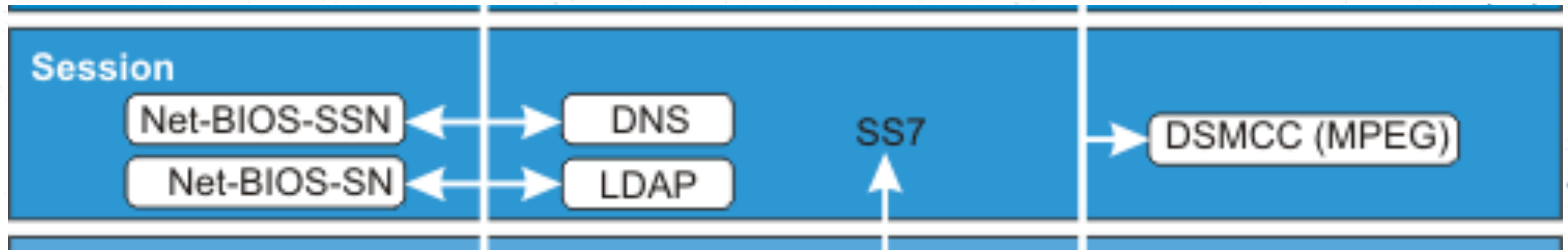
Session Layer

- This layer is considered as the network **dialog controller**.
- It establishes, maintains, and synchronizes the interaction between communicating systems.

Key points:

Dialog control, Synchronization.

Mapping the Session Layer



Presentation Layer

- Presentation layer is concerned with the **syntax and semantics** of the information exchanged between two systems.

Key points:

Translation, Encryption, Compression.

Mapping the Presentation Layer

- Type of encryption used.
- Type of compression used.

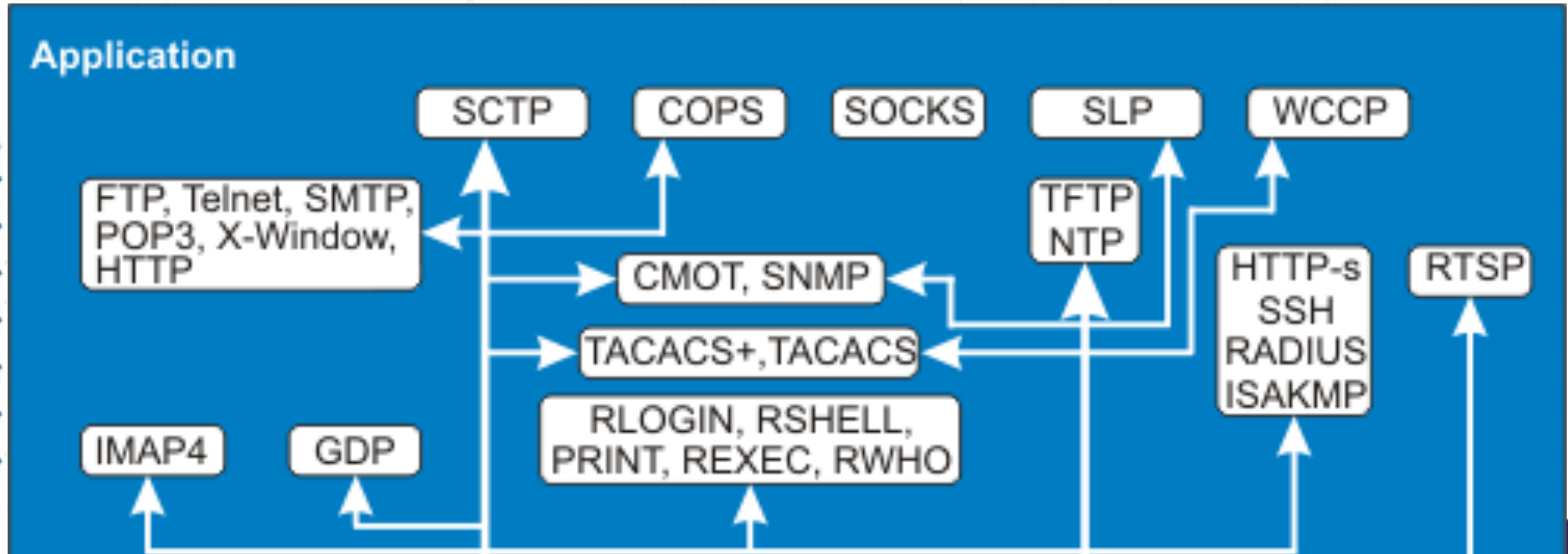
Application Layer

- Enables the users, human or software, to **access** the network.
- Provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.

Key points:

Network virtual terminal (aka remote terminal), File transfer, access and management (FTAM), Mail services, Directory services.

Mapping the Application Layer



Non Network Information

Non network information refers to the information that are directly not corresponding to you networking principles, BUT, is vital to the day-to-day management of the network related tasks. For example,

- ☐ **Network purpose statement.**
- ☐ **Network overview documentation.**
- ☐ Physical locations.
- ☐ Vendors.
- ☐ Signatories.
- ☐ Etc..

Non Network Information

Physical Locations

- Floor Plans
 - ☐ Pictures
 - ☐ Fire exits
- Addresses
 - ☐ Visitor entrances
 - ☐ Deliveries
 - ☐ Ship to
 - ☐ Driving directions
- Managers (with contact name and phone numbers)
 - ☐ IT Infrastructure
 - ☐ Non IT Infrastructure (e.g., HVAC - *heating, ventilation, and air conditioning*, hallways, offices, etc.)
 - ☐ Others

Non Network Information

Resources

- Account management
- Usernames and passwords for web resources you utilize

Signatories

- Who makes decisions?
- Who can authorize purchases?

Suppliers/Vendors

- List of all contractors who work on your network
- List of all vendors you purchase equipment from
- List of all service contracts (and/or warranty fulfillment)

Network Mapping Tools

Network mapping tools can make your life easy by assisting you with many network mapping related tasks.

Open source

- Nagios
- OpenNMS
- knetmap

Commercial

- SmartDraw™
- Visio
- netViz™
- Neon LANsurveyor



Baselining

- Why?
- What?
- When?
- How?

Baselining

- Optimize quality of service.
 - ❑ Gather performance data.
 - ❑ Analyze the data.
 - ❑ Determine appropriate performance thresholds.
- The act of measuring and rating the performance of a network in real-time situations.
 - http://www.webopedia.com/TERM/n/network_baselining.html
- Comparing current performance to a historical metric, or “baseline”.
 - <http://en.wikipedia.org/wiki/Baselining>

Network Baselineing

http://www.webopedia.com/TERM/n/network_baselineing.html

- Network baselining is the act of measuring and rating the performance of a network in real-time situations.
- Providing a network baseline requires testing and reporting of the physical connectivity, normal network utilization, protocol usage, peak network utilization, and average throughput of the network usage.
- Such in-depth network analysis is required to identify problems with speed and accessibility, and to find vulnerabilities and other problems within the network.
- Once a network baseline has been established, this information is then used by companies and organizations to determine both present and future network upgrade needs as well as assist in making changes to ensure their current network is optimized for peak performance.

Why Baseline

- To determine normal operating conditions
- To identify and forecast problems
- Troubleshooting
- Predict network operation
- Predict the ability to handle new tasks (scaling)
- Optimization

When to Baseline

- Begin immediately
- Long term
- Use the baseline to determine the baseline schedule
- Special attention areas
- All levels of system activity

How to Baseline

- Determine what we have (inventory)
- Determine what needs to be measured
- Determine when it needs to be measured
- Use the long term baseline to determine how often items need to be measured
- Repeat the measurements regularly
- Implement a way of obtaining alerts
- Implement a way of detecting trends
- Create a data repository

Care When Baselineing

- The very act of recording data for a baseline can skew the results
 - ❑ Known as **measurement degradation**, it may occur
 - Because the act of measuring an object's performance may increase its workload
 - If too short a time interval is used when measuring
 - When measuring multiple objects on a single system
- A base line is not an analysis, it is a tool that can be used to do analysis
 - ❑ **Do not start the analysis until you map the network**

Analysis

- What are normal operating conditions?
- What are the peak operating conditions?
- Why are the conditions the way they are?
- How will problems be assessed?
- How will modifications be assessed?

Questions???



Self Review

Glossary (aka *Vocabulary*)

ROI – Return On Investment

ROI is an accounting formula used to obtain an actual or perceived future value of an expense or investment.

SPOF – Single Point Of Failure

A generic phrase for any component of a system that upon failure will cause a malfunction in the entire system. A SPOF can be a hardware or electrical component or a software component. Each time a system expands (e.g., adding a workstation to a network or adding a new application to a network of workstations) the number of places where an SPOF can occur also expands.

Glossary (aka *Vocabulary*)

- MTBF – Mean Time Between Failures
- The average time a device will function before failing. MTBF ratings are measured in hours and indicate the sturdiness of hard disk drives and printers.
- Typical disk drives for personal computers have MTBF ratings of about 500,000 hours. This means that of all the drives tested, one failure occurred every 500,000 hours of testing. Disk drives are typically tested only a few hours, and it would be unlikely for a failure to occur during this short testing period. Because of this, MTBF ratings are also predicted based on product experience or by analyzing known factors such as raw data supplied by the manufacturer.

Glossary (aka *Vocabulary*)

MTTR – Mean Time To Repair

In data storage, MTTR is the average time before an electronic component can be expected to require repair.

AFR – Annualized Failure Rate

Is the relation between the MTBF and the hours that a number of devices are run per year, expressed in percent. AFR does not specifically apply to a single component, but rather to a population of like components.

Glossary (aka *Vocabulary*)

Uptime

Amount of time the utility is available to users.

Downtime

Amount of time the utility is unavailable to users.

Availability

Percentage of time the utility is available to the user.

Proxy Server



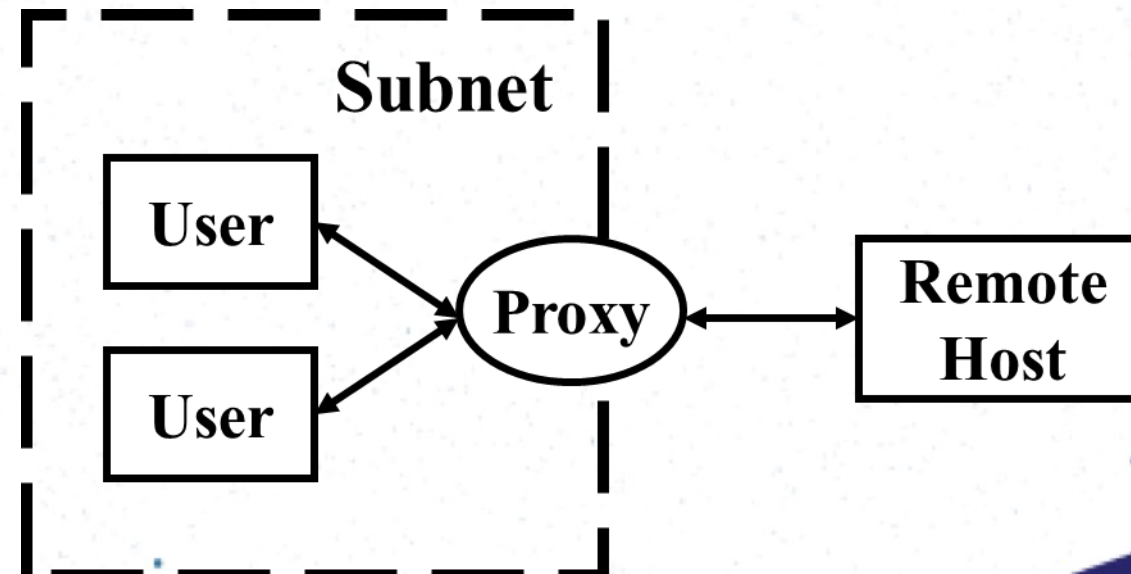
Proxy server



*In computer networks, a **proxy server** is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. Proxies were invented to add structure and encapsulation to distributed systems. Today, most proxies are web proxies, facilitating access to content on the World Wide Web and providing*

Basic concept

- A proxy server is usually associated with or part of a gateway server that separates the subnet from the outside network and a firewall server that protects the subnet from outside intrusion



Proxy Servers

- ❖ Part of an overall Firewall strategy
- ❖ Sits between the local network and the external network
 - Originally used primarily as a caching strategy to minimize outgoing URL requests and increase perceived browser performance
 - Primary mission is now to insure anonymity of internal users
 - Still used for caching of frequently requested files
 - Also used for content filtering
- ❖ Acts as a go-between, submitting your requests to the external network
 - Requests are translated from your IP address to the Proxy's IP address
 - E-mail addresses of internal users are removed from request headers
 - Cause an actual break in the flow of communications

Types of proxy

- **Forwarding proxies**

- Forward proxies are proxies in which the client server names the target server to connect to. Forward proxies are able to retrieve from a wide range of sources (in most cases anywhere on the Internet).

Types of proxy

- **Open proxies**

- An open proxy is a forwarding proxy server that is accessible by any Internet user. According to estimates there are "hundreds of thousands" of open proxies on the Internet. An anonymous open proxy allows users to conceal their IP address while browsing the Web or using other Internet services.

Types of proxy

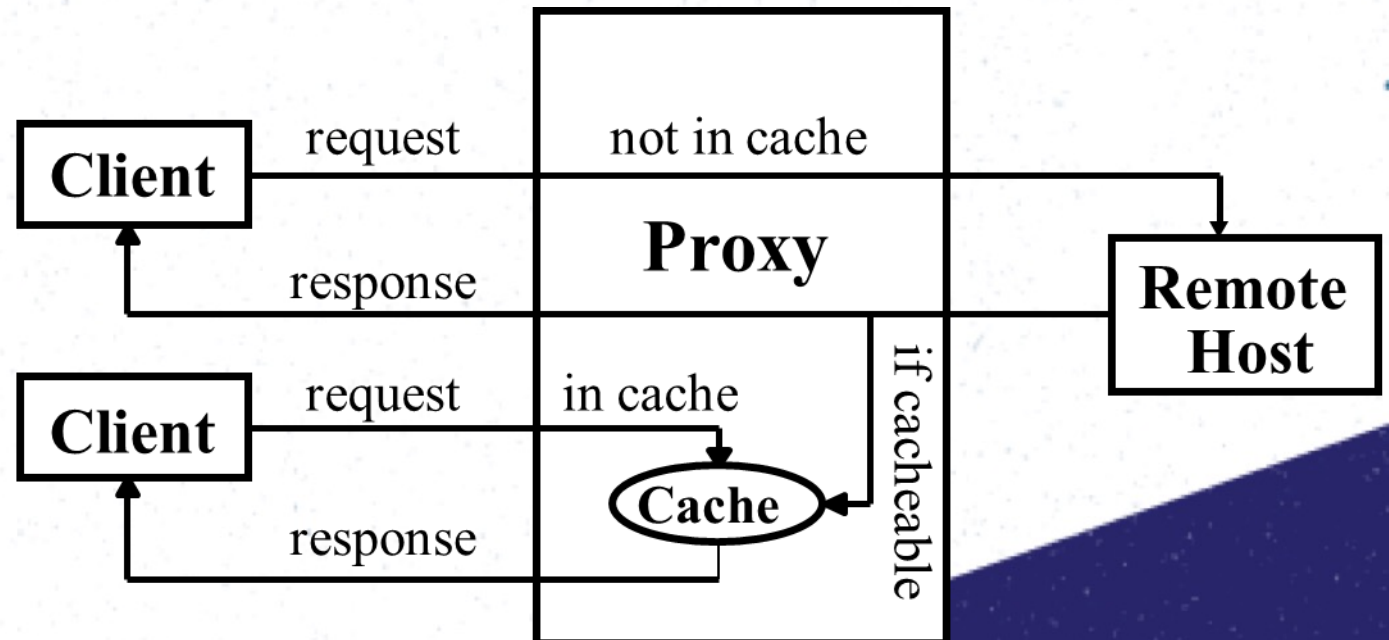
- **Reverse proxies**

- A reverse proxy (or surrogate) is a proxy server that appears to clients to be an ordinary server. Requests are forwarded to one or more proxy servers which handle the request. The response from the proxy server is returned as if it came directly from the origin server, leaving the client no knowledge of the origin servers.

Proxy Cache

- One of the most important uses of Proxy, is as a Cache Server. Cache mechanism allows saving some cacheable requests for later recall by any user and thus reduce both latency and Internet traffic.

- Browser caches
- Proxy caches
- Server cache





WEB Server

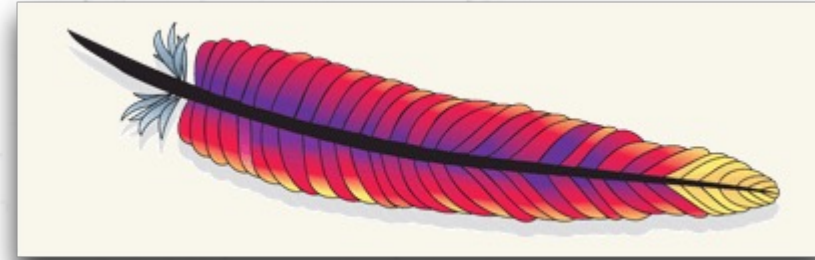


web server

The term web server, also written as Web server, can refer to either the hardware (the computer) or the software (the computer application) that helps to deliver web content that can be accessed through the Internet.

Wikipedia

Web server

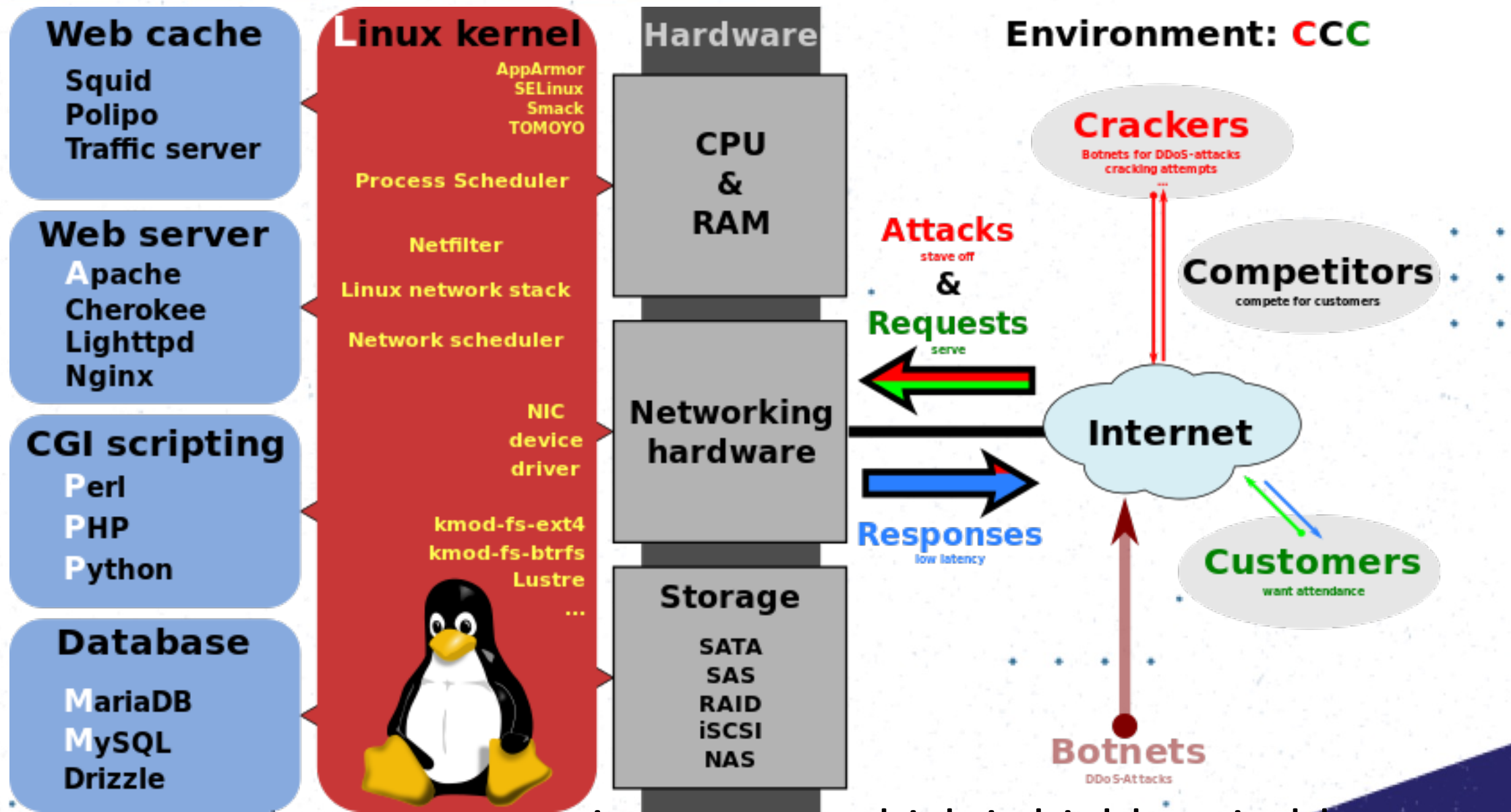


- ❖ HTTP (Hyper Text Transfer Protocol) is used to transfer web pages from a Web Server to Web Client (Browser)
- ❖ Web Pages are arranged in a directory structure in the Web Server
- ❖ HTTP supports CGI (Common Gateway interface)
- ❖ HTTP supports Virtual Hosting (Hosting multiple sites on the same server)

Popular Web Servers

- Apache
- Windows IIS
- nginx
- GWS





- LAMP web service solution stacks, which is highly suitable for building dynamic web sites and web applications.

Behind the Scenes

- The browser broke the URL into three parts

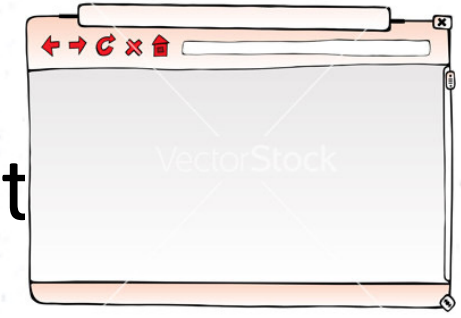
1. The protocol ("http")

2. The server name ("www.howstuffworks.com")

3. The file name ("web-server.htm")

Connection
Establishment
via port
80 (http)

1 Request
DNS for
IP
2 Reply
with
IP



MAIL Server



mail server

Within Internet message handling services (MHS), a message transfer agent or mail transfer agent (MTA) or mail relay is software that transfers electronic mail messages from one computer. An MTA implements both the client (sending) and server (receiving) portions of the Simple Mail Transfer Protocol.

Mail server



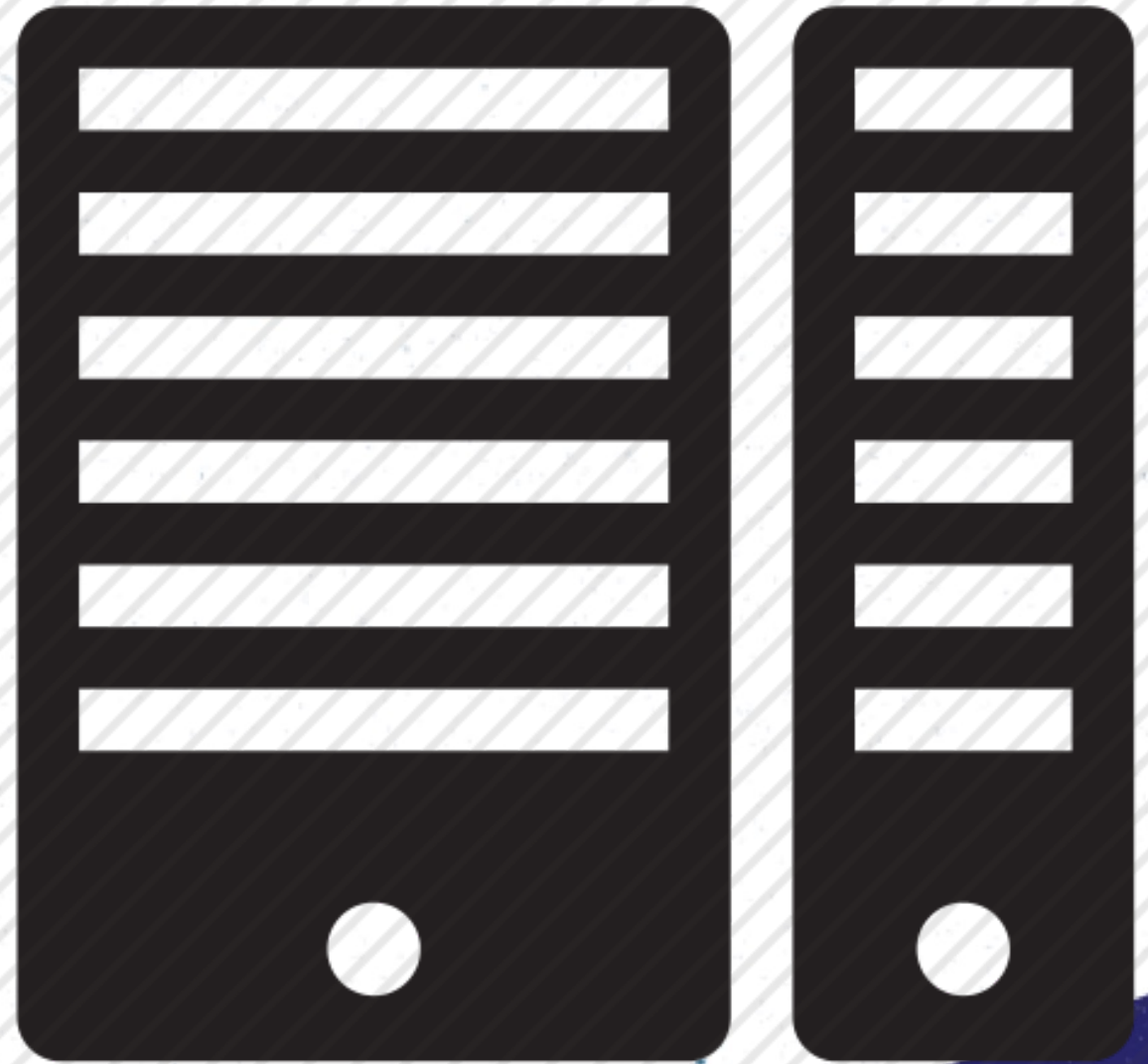
- ❖ Simple Mail Transfer Protocol (SMTP) is used to transfer mail between Mail Servers over Internet
- ❖ Post Office Protocol (PoP) and Interactive Mail Access Protocol (IMAP) is used between Client and Mail Server to retrieve mails
- ❖ The mail server of a domain is identified by the MX record of that domain

Popular Mail Servers:

- Sendmail/Postfix
- Microsoft Exchange Server
- IBM Lotus



OTHER Server types



Application server



- Also called an appserver, an application server is a program that handles all application operations between users and an organization's backend business applications or databases.
- An application server is typically used for complex transaction-based applications. To support high-end needs, an application server has to have built-in redundancy, monitor for high-availability, high-performance distributed application services and support for complex database access.

File server



- In the client/server model, a file server is a computer **responsible for the central storage and management of data files so that other computers on the same network** can access the files.
- A file server allows users to share information over a network without having to physically transfer files by floppy diskette or some other external storage device.

Ex. ://public drive at sliit

File server



- A file server may be :
 - An ordinary PC that handles requests for files and sends them to the network.
 - A dedicated network-attached storage (NAS) device that also serves as a remote hard disk drive for other computers, allowing anyone on the network to store files on it as if to their own hard drive.

Print server



- A print server, or printer server, is a device that connects printers to client computers over a network. It accepts print jobs from the computers and sends the jobs to the appropriate printers, queuing the jobs locally to accommodate the fact that work may arrive more quickly than the printer can actually handle it.
- Print servers may support a variety of industry-standard or proprietary printing protocols including Internet Printing Protocol, Line Printer Daemon protocol, NetWare, NetBIOS/NetBEUI, or JetDirect.