IT3010

Network Design and Management

Introduction to Labs and Virtualization

Shashika Lokuliyana

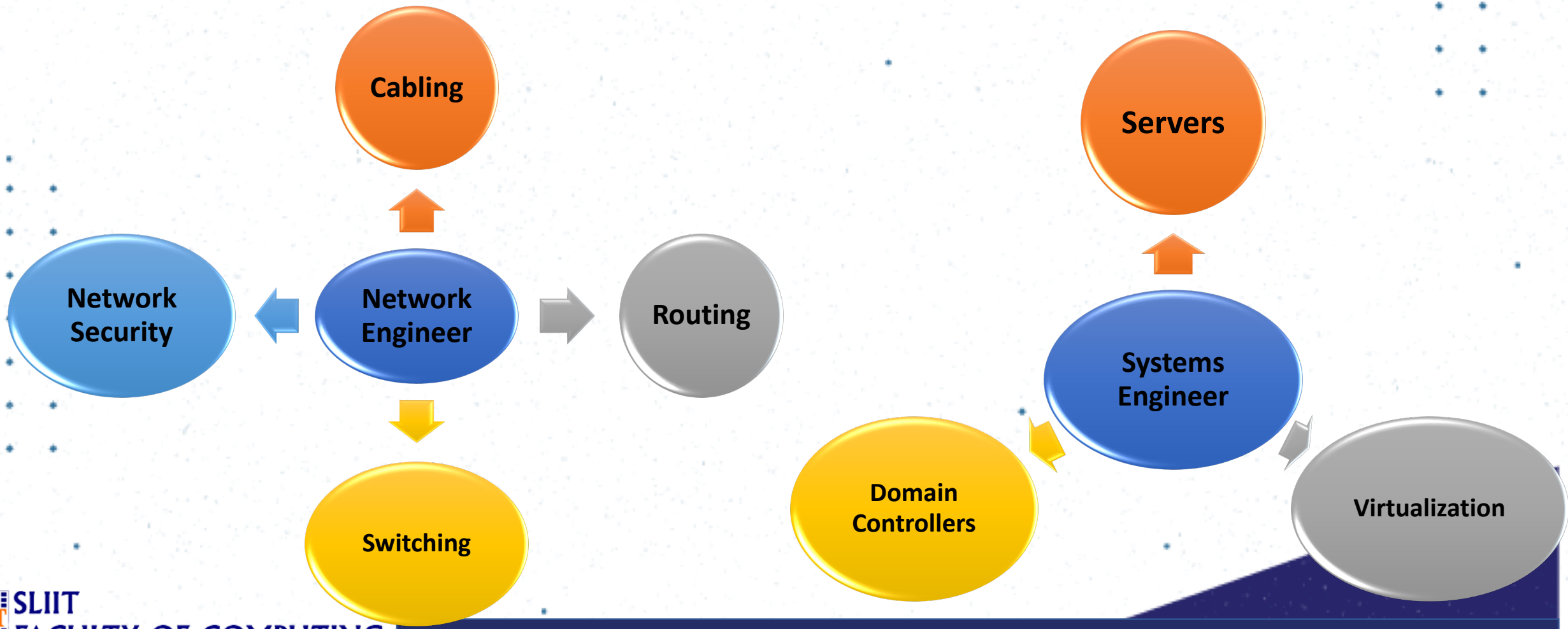
Faculty of Computing

Department of CSE

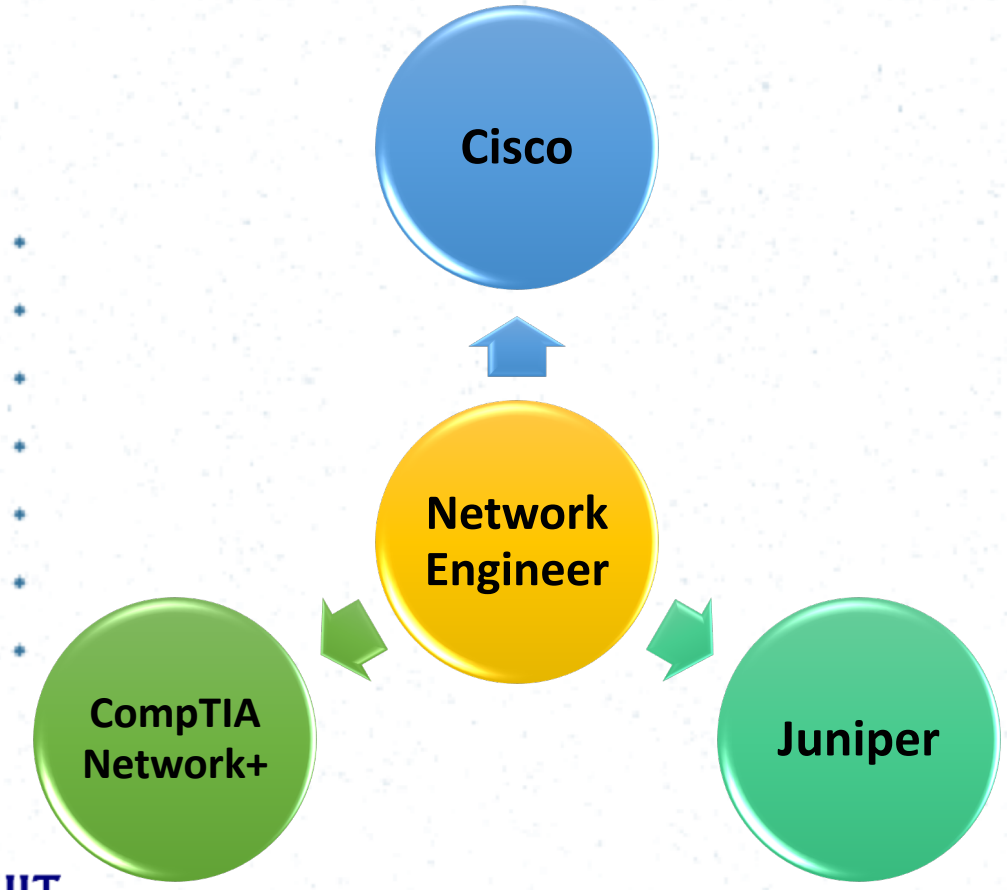
SLIIT

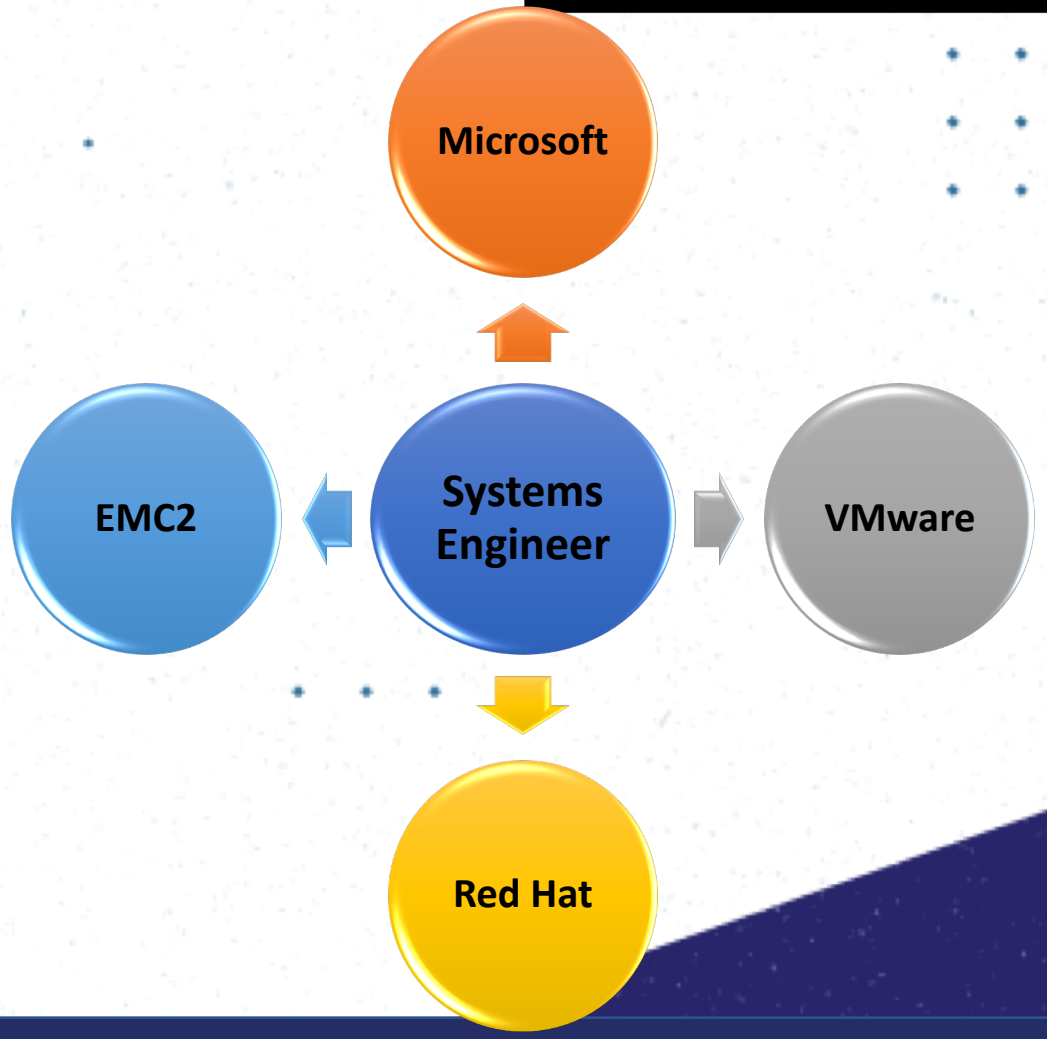
Discover Your Future

Network Engineer?? or Systems Engi



Certifications





Certifications

Cisco Path

For further details refer Cisco_Path.pdf included in the lab package.

Microsoft Path

For further details visit http://www.microsoft.com/learning/en/us/certification/cert-overview.aspx

Other certifications

Juniper

http://www.juniper.net/us/en/training/certification/

CompTIA Network+

http://certification.comptia.org/getcertified/certifications/network.aspx

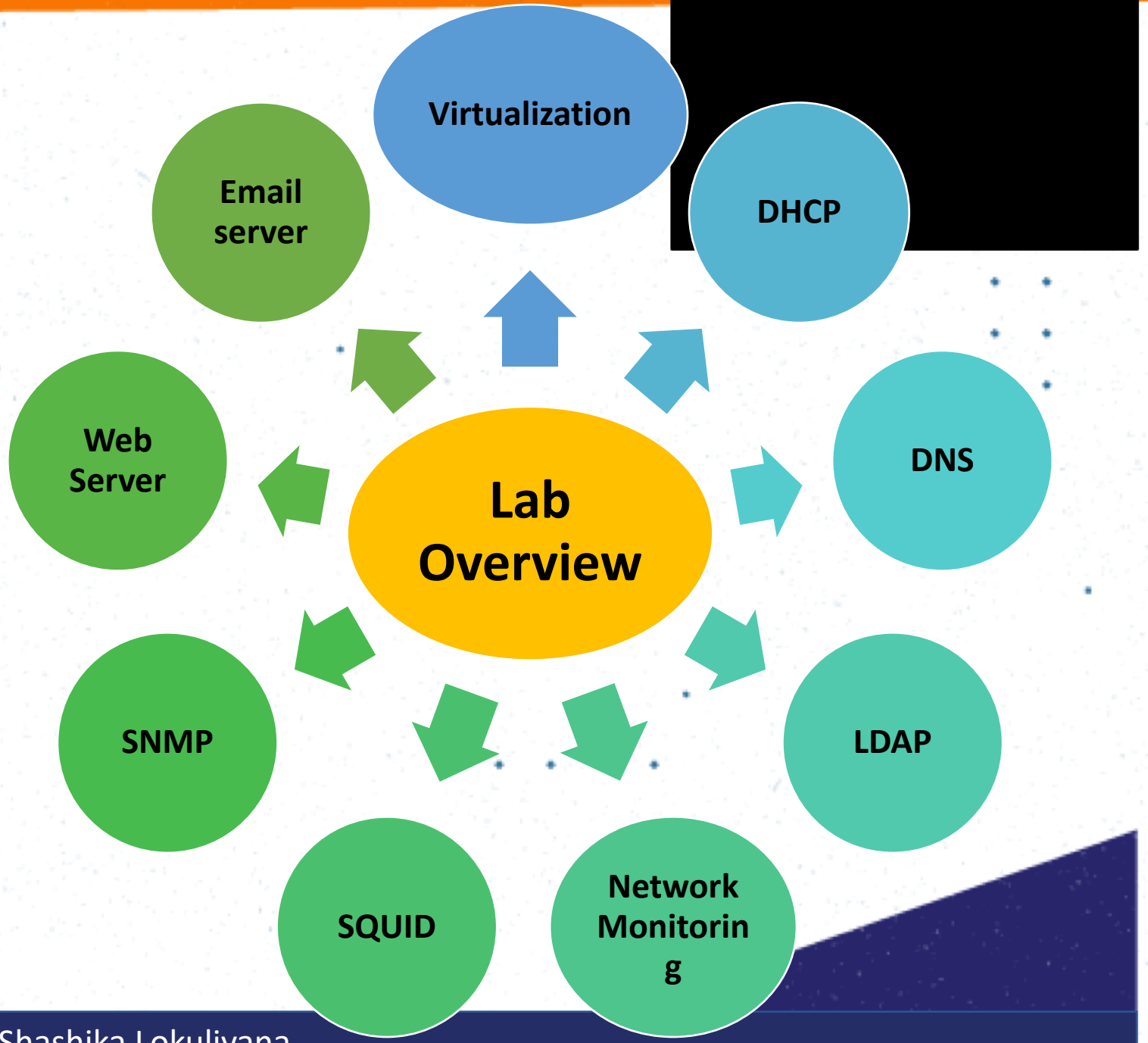
VMware

http://mylearn.vmware.com/portals/certification/

Red Hat

http://www.redhat.com/training/certifications/

NDM Lab Overview



“I create my lab sheets” policy… ☺

- Labs are for you to experiment..
- If I prepare the lab sheets,
  - ❑ Those will be my lab sheets..
  - ❑ Based on my level of understanding..
  - ❑ But sometime it will be difficult for you to cope up with my level of understanding.. ☺
- We will guide, instruct and provide support material..
- And it is your job to compile the lab sheet, the way you think it is best for you..!!
- Some general guidelines,
  - ❑ Make your lab sheet as we are doing the lab.. Don’t keep it for home work..
  - ❑ A picture is worth thousand words.. So make sure to take screenshots when needed..

Desktop Vs. Server OS

Desktop operating systems are typically installed in end user or standalone desktop and laptop PCs.

Features:

- Highly user-friendly and eye-catching GUI.
- Ability to run a wide range of applications.
- Low security.
- Minimal backup/automation capabilities.

Desktop Vs. Server OS

Server operating systems are typically installed in high end server machines (E.g. Blade systems).

Features:

- GUI not available or optional.
- Ability to reconfigure and update both hardware and software to some extent without restart.
- Advanced backup facilities to permit regular and frequent online backups of critical data.
- Transparent data transfer between different volumes or devices.
- Flexible and advanced networking capabilities.
- Automation capabilities such as daemons in UNIX and services in Windows.
- Tight system security, with advanced user, resource, data, and memory protection.

Desktop Vs. Server OS

Examples..

Desktop

- Windows XP, Vista, 7.
- Mac OS X Snow Leopard, Lion.
- Ubuntu Desktop.

Server

- Windows Server 2003, 2008.
- OS X Server.
- Ubuntu Server.
- Fedora, Debian, CentOS.

Open-source Vs. Closed-source OS

Open-source OS

- The source code of the operating system is exposed to the general public.
- Community development.
- Mostly free to use and distribute.

Closed-source OS

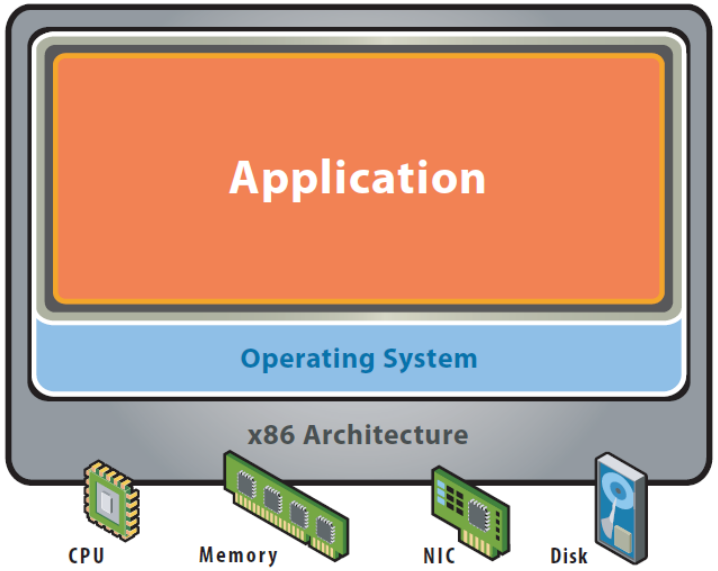
- Only a binary version of the OS is released to users.
- Licensing based usage.

Please read the Open-Source versus Closed-Source Sytems.html web page included in the lab package for further details.

Virtualization

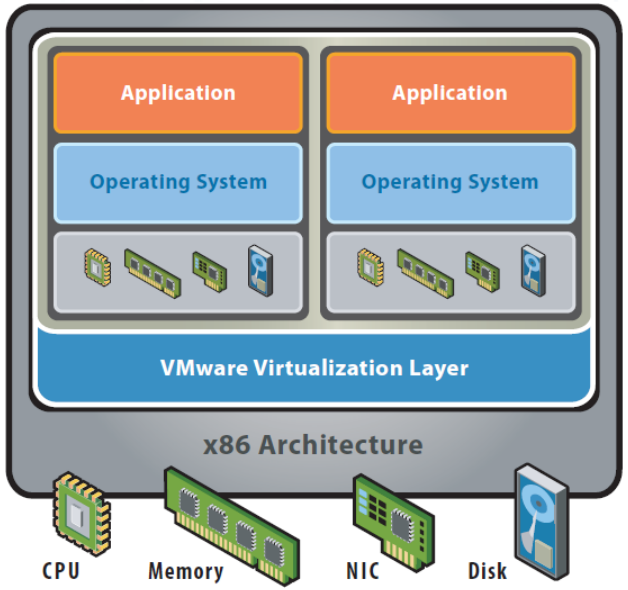
The term *virtualization* broadly describes the separation of a resource or request for a service from the underlying physical delivery of that service.

Virtualization cont..



Before Virtualization:

- Single OS image per machine
- Software and hardware tightly coupled
- Running multiple applications on same machine often creates conflict
- Underutilized resources
- Inflexible and costly infrastructure



After Virtualization:

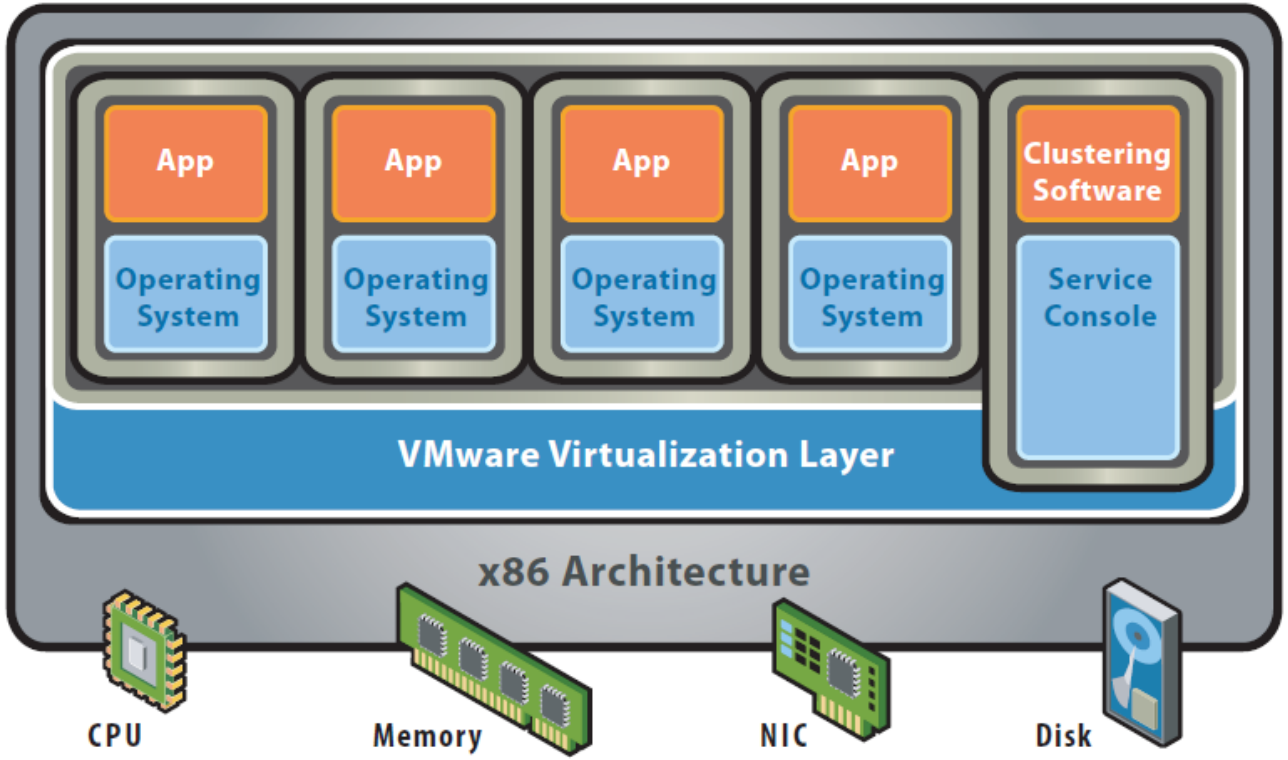
- Hardware-independence of operating system and applications
- Virtual machines can be provisioned to any system
- Can manage OS and application as a single unit by encapsulating them into virtual machines

Central to virtualization is the Virtual Machine Manager (VMM), aka Hypervisor. The VMM is responsible for monitoring and enforcing policy on the VMs for which it is responsible. This means that the VMM keeps track of everything that happens inside of a VM. When necessary, it provides resources, redirects the VM

Virtualization Approaches

- Virtualization can apply to a range of system layers,
    1. Hardware-level virtualization
    2. Operating system level virtualization
    3. High-level language virtual machines

1. Hardware-level virtualization



Bare-Metal (Hypervisor) Architecture

- Lean virtualization-centric kernel
- Service Console for agents and helper applications
- Higher virtualization efficiency by dealing directly with the hardware.

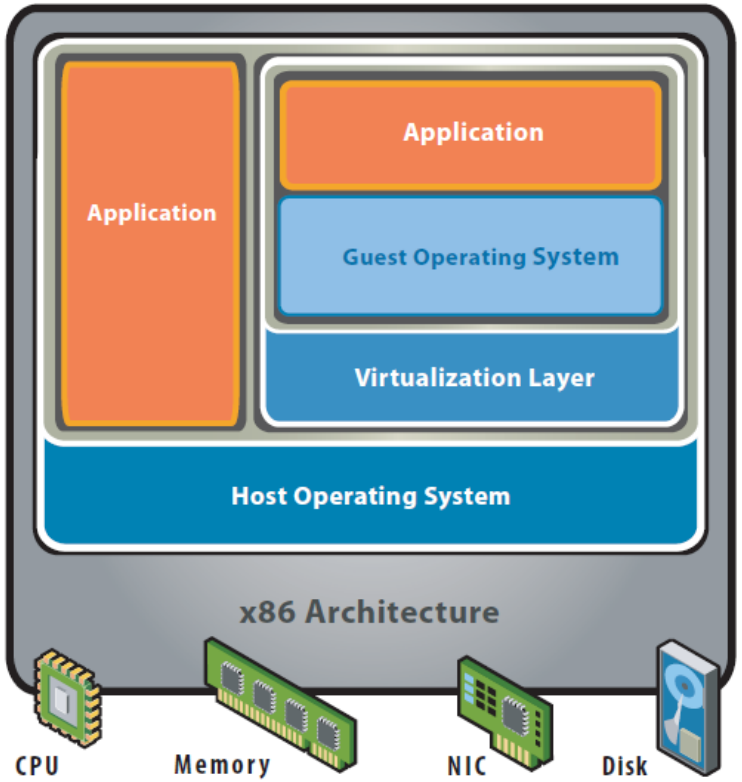
  E.g. Providers :

  Microsoft Hyper-V

  VMware ESX

  Xen

2. Operating system level virtualization

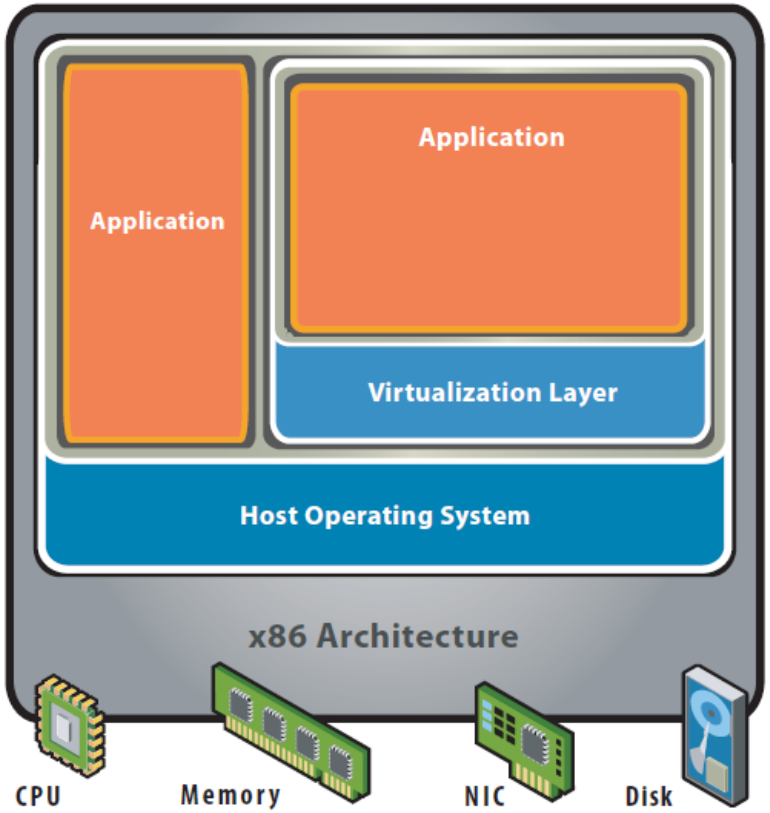


Hosted Architecture

- Installs and runs as an application
- Relies on host OS for device support and physical resource management
- Used mainly on systems where support for a broad range of I/O devices is important and can be provided by the host operating system.
- Used mainly on client systems where efficiency is less critical.

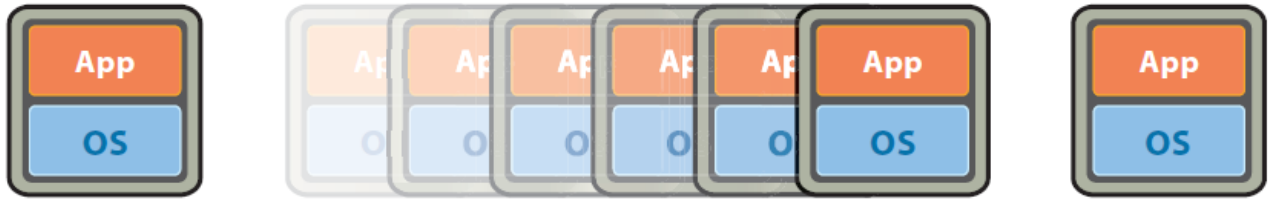
E.g. Providers :
Microsoft Virtual Server
Microsoft Virtual PC
VMware Workstation
VMware Player
Java Virtual Box

3. High-level language virtual machines



Application Architecture

- This VMM architecture is exemplified by Java Virtual Machines (JVMs) or .NET architecture.
- Can be considered more of an application framework than a hypervisor.
- Here, the goal of virtualization is to create a runtime environment within which the process can execute a set of instructions without relying on the host system (i.e. underlying OS).
- This is not actually a server virtualization category.



CONSISTENT VIRTUAL HARDWARE PLATFORM
Open Interfaces

VMware Infrastructure

ACE
Secured Enterprise Desktop

Workstation
Technical Desktop

VMware Server
Departmental Computing

ESX Server
Enterprise Computing

System Architecture & Highlights	Hosted on Windows	Hosted on Windows or Linux	Hosted on Windows or Linux	Bare Metal V-SMP Option	Mgmt Server, Console & APIs VMotion

IT3010

Network Design and Management

Lecture 02

ISO Network Management Framework

Shashika Lokuliyana

Faculty of Computing

Department of CSE

SLIIT

Discover Your Future

IT3010
NETWORK DESIGN MANAGEMENT

Lecture 1
Introduction to Network Design & Management

Today's lecture overview

- Design Methodology and Considerations
- Rationale for Network Management
- Network Management Process
- Network Management Systems

Introduction

Definition of a Data Network: A collection of devices and circuits for transferring data from one computer to another (or device, e.g. printer).

Purpose:

It enables users at different locations to share the resources of a computer stationed elsewhere.

E.g. : Automated Teller Machine (ATM)

Goals

Why bother about the network design..?

Primary goal of network design is to meet the organizations communication needs.

- Productivity 
- Budget 

Considerations

Achieving the goal..

Need to develop a comprehensive plan. Must take into account the following:

- Suitability
- Reliability
- Scalability
- Durability

Network Engineer/Administrator

Role of a Network Engineer/Administrator

Network engineers have the responsibility for installing, maintaining, troubleshooting, optimizing and expanding the network.

- As a network expands, so too the size and number of potential problems.
- The overall goal of network management is to help network engineers deal with the complexity of data networks.
- Design based on Network Management principles.

The Network Management Process

Network Management is the process of controlling complex data networks to maximize its efficiency and productivity.

ISO Framework for Network Management

- Configuration management
- Security management
- Performance management
- Accounting management
- Fault management

Configuration Management

Configuration management is the process of

- Gathering information about the current network environment.
- Using that data to modify the configuration of network devices.
- Storing the data, maintaining an up-to-date inventory of all network components and producing various reports.

Bridge Configuration Management Information	
Name	Software Version
Payroll Mainframe Subnet	A
Terminal Server Subnet	B
Engineerig Computer subnet	A

Data Collection, Modification and Stori

Data Collection

Two methods..

- Manual collection
  - Tedious, error prone, time consuming
- Auto-discovery/Auto-mapping
  - ICMP (ping, traceroute)
  - Network Management Protocol

Data Collection, Modification and Stori

Data Modifications

- Once configuration management information has been obtained, it will usually need to be updated.
- Network devices usually contain many pieces of modifiable parameters.
  - E.g. – routers (routing tables, network interfaces), servers (application services, operating systems).

Data Collection, Modification and Stori

Storing Information

Methods of storage:

- **Unstructured** (e.g. ASCII files)
  - Advantages:
    - Easily read.
    - Easily accessed from remote locations.
    - Easy to administer.
  - Disadvantages:
    - Inefficient storage.
    - Slow to search.
    - Unable to provide complex data relationships.

Data Collection, Modification and Stori

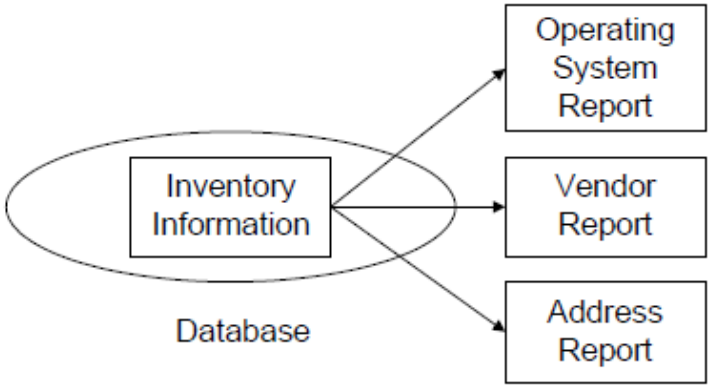
Storing Information

Methods of storage:

- **Structured** (e.g. DBMS)
  - Advantages:
    - Stores data efficiently.
    - Enables users to relate various types of information to one another.
    - Versioning.
  - Disadvantages:
    - Need to learn query language to access data (e.g. SQL).
    - Administrative overheads.

Configuration Management - Benefits

- Automatically gather and update data on network devices.
- Allows devices to be configured remotely.
- Provides central storage location for configuration data.
- Facilitates the production of network inventory and other reports.



Security Management

- Security management involves protecting sensitive information on devices attached to a data network by controlling access points to that information.
- Security management consists of the following aspects:
  - Identifying the sensitive information to be protected.
  - Finding the access points (vulnerabilities).
  - Securing the access points.
  - Maintaining the secure access points.

Security Management - Benefits

- Increases confidence in utilizing the network.
  - A lack of security may force drastic measures, such as eliminating network access of sensitive information altogether.
  - Properly set up and maintained security management can offer more practical alternatives.
- Some examples:
  - 1988: Internet worm
  - More recently: ICMP and TCP-based DoS attacks

Performance Management

Performance management involves ensuring that networks remain accessible and free from congestion:

- Monitoring network devices and their associated links to determine utilization and error rates.
- Helping the network provide consistent quality of service (QoS) by ensuring that the capacity of devices and links is not over taxed to the extent of adversely impacting performance.
  - Context-specific

Performance Management

Performance management entails the following steps:

1. Collecting data on current utilization of network devices and links.
2. Analyzing relevant data.
   - Statistical analysis
   - Workload modeling
3. Setting utilization thresholds.
4. Using simulation to determine how the network can be altered to maximize performance.

Performance Terms

- Availability
- Bandwidth/Throughput
- Propagation
- Congestion
- Latency
- Threshold
- Utilization

Performance Management - Benefits

- Reduces probability of network congestion and inaccessibility so as to provide a consistent level of service to users.
  - E.g. – Knowing the network's utilization workload can help one schedule large data transfers for non-peak times.
- Assist in examining network trends:
  - Content Creators
  - Content-hosting companies
  - Network operators
  - Networking researchers

Accounting Management

Accounting management is the process of gathering network statistics to help the network engineer make decisions about the allocation of network resources.

Accounting management involves the following tasks:

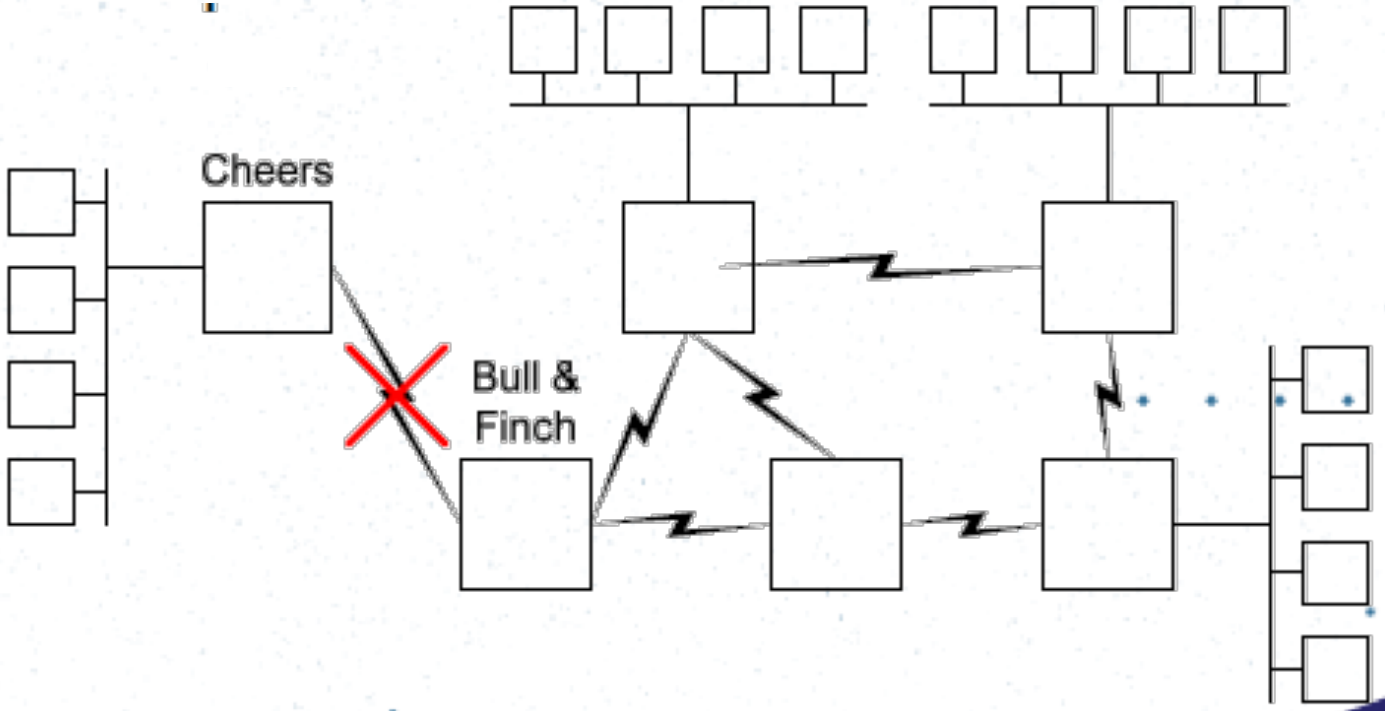
- Gathering data about the utilization of network resources.
  - Need to establish metrics -RFC 1272: "Internet Accounting Background"
    - E.g. Application layer – per-transaction, network layer – number of packets.
- Setting usage quotas using metrics.
- Billing users for their use of the network.

Accounting Management - Benefits

- Allows effective measurement and reporting of accounting information.
- Increases the engineer's understanding of user utilization.
  - Helps the network engineer make informed decisions about the allocation of network resources.
  - Ensure that users have a fair share of the network..

Fault Management

Fault management is the process of locating problems or faults, on the data network.



Fault Management

- The fault management process involves:
  - Detecting symptoms that may lead to a problem/fault
    - in the network.
  - Isolating the cause of the symptoms.
    - Find correlations between symptoms and potential problems.
      - Alarms do not usually include explicit information regarding the exact location of the fault.
  - Correcting the problem if possible.

Gathering Information for Fault Management

Two methods..

- **Interrupt driven**
  - Critical events (e.g. link failure).
  - Solely relying on such events may not facilitate effective fault management.
- **Polling**
  - Finds faults in a timely manner.
  - Higher bandwidth consumption.
  - Polling can be implemented using ICMP messages (ping).

Fault Management - Benefits

- Enhances network reliability by providing tools to aid/facilitate rapid fault detection, isolation and recovery.
- Maintains the illusion of complete and continuous connectivity between the users and the network.

Network Management Systems

A Network Management System (NMS) comprises:

- An underlying architecture (aka platform).
  - A software package that provides generic/basic functionality of network management for managing a variety of network devices.
- A set of applications built on top of the platform.

Network Management Systems

Example NMSs

- Commercial implementations
  - HP Openview
  - SunConnect SunNet Manager
  - IBM Netview
- Freeware implementations
  - Net-SNMP (formally UCD-SNMP, CMU-SNMP)
  - OpenNMS

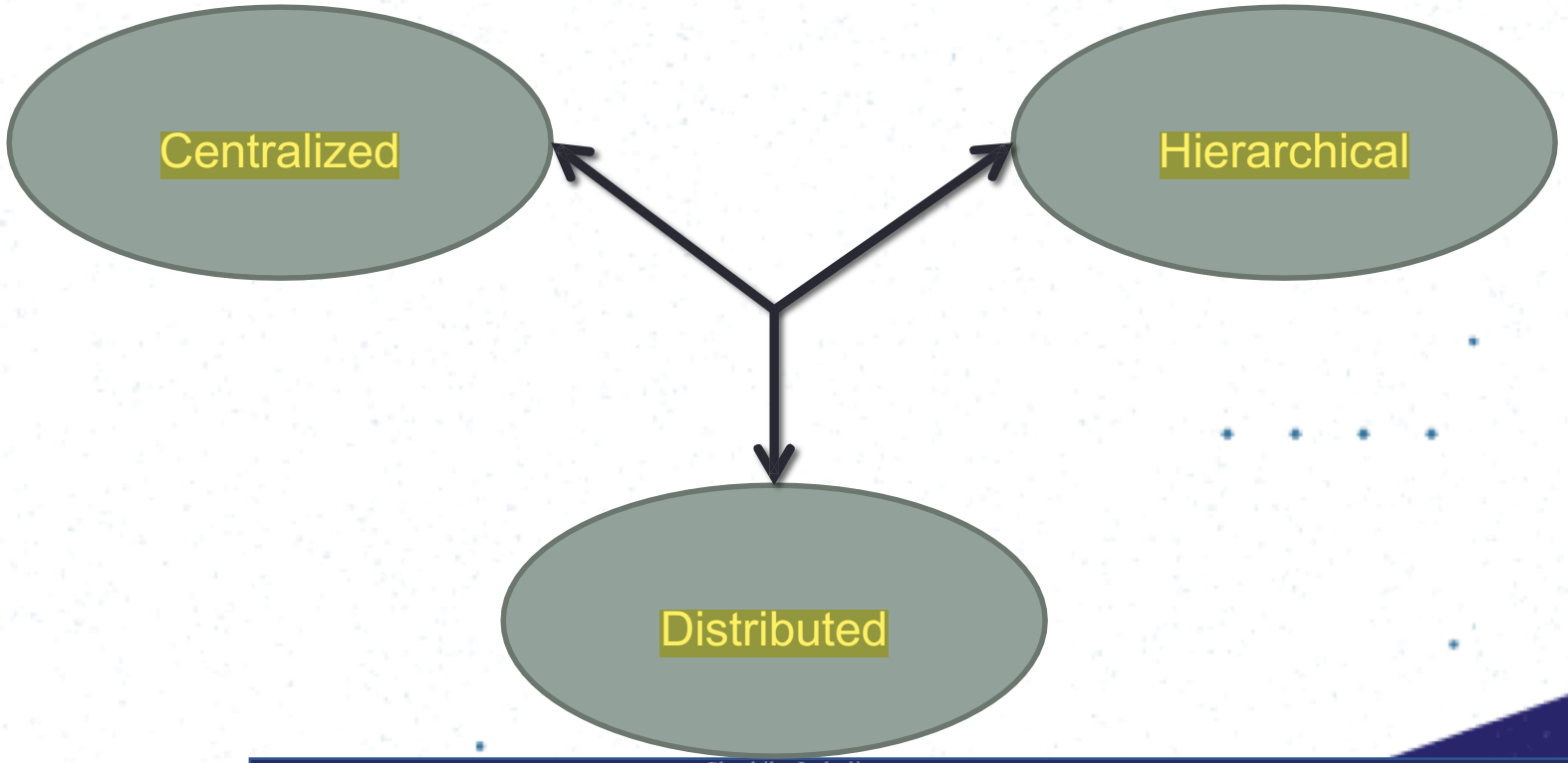
Network Management Systems

The platform should include the following functionality:

- A user interface
- A network map
- A **D**ata**b**ase **M**anagement **S**ystem (DBMS) / **M**anagement **I**nformation **B**ase (MIB)
- A query language
- A customizable menu system
- An event log

Network Management Architecture

An NMS platform can use three architectures to provide functionality.



Next Lecture...!!!

Network Mapping and Baselining

Thank You

IT3010

Network Design and Management

Lecture 03

Network Servers

Shashika Lokuliyana

Faculty of Computing

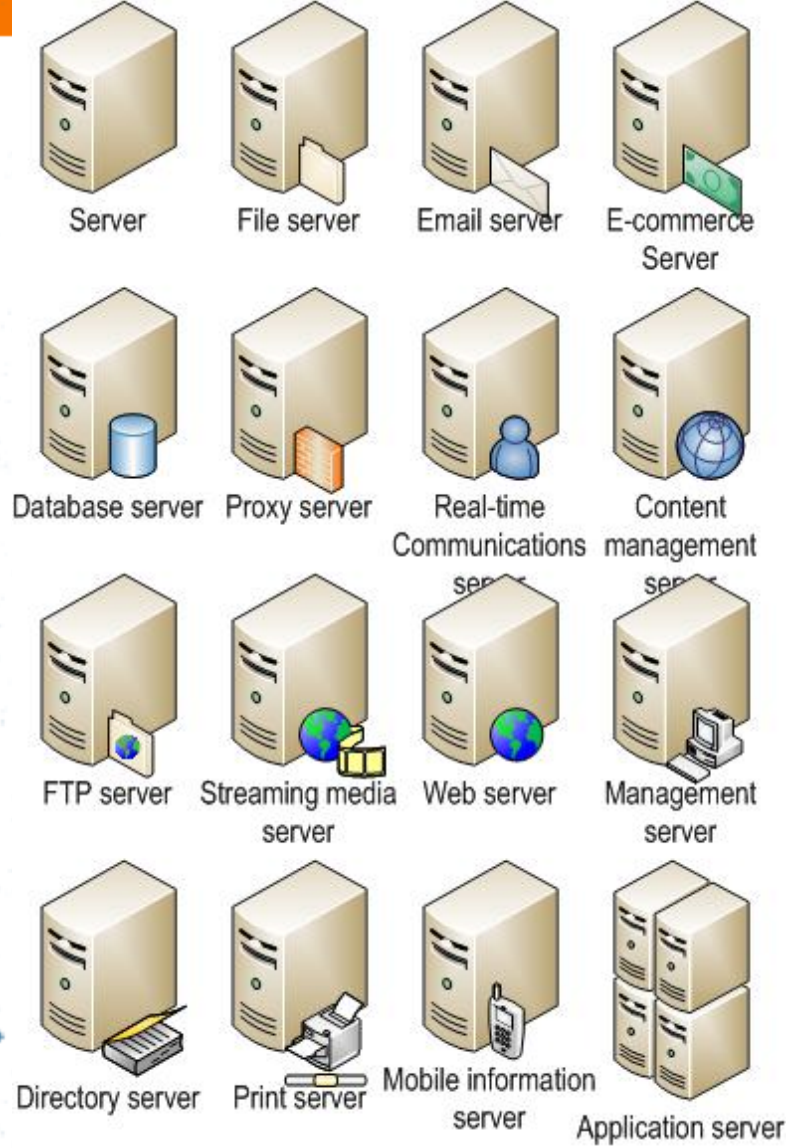
Department of CSE

SLIIT

Discover Your Future

To be Covered…!!!

- A day in the life of an application
- Client – Server Architecture
- Domain Name System (DNS)
- Dynamic Host Configuration Protocol
- Proxy Server
- Web Server
- Other Server types



A day in the life of an application

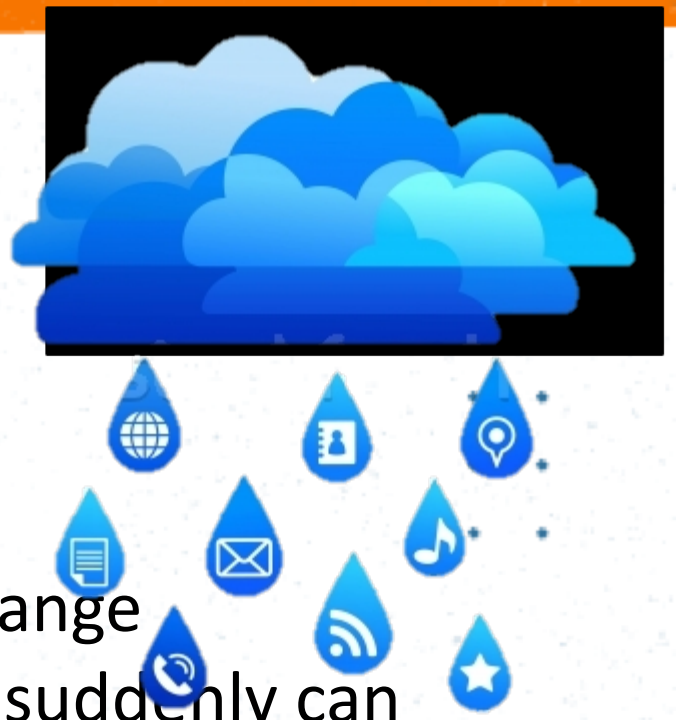
Networked applications

"The current exponential growth of the network seems to show that connectivity is its own reward, and it is more valuable than any individual application such as mail or the World-Wide-Web."

- David Clark

[A key contributor to the Internet's design]

Networked applications cont..

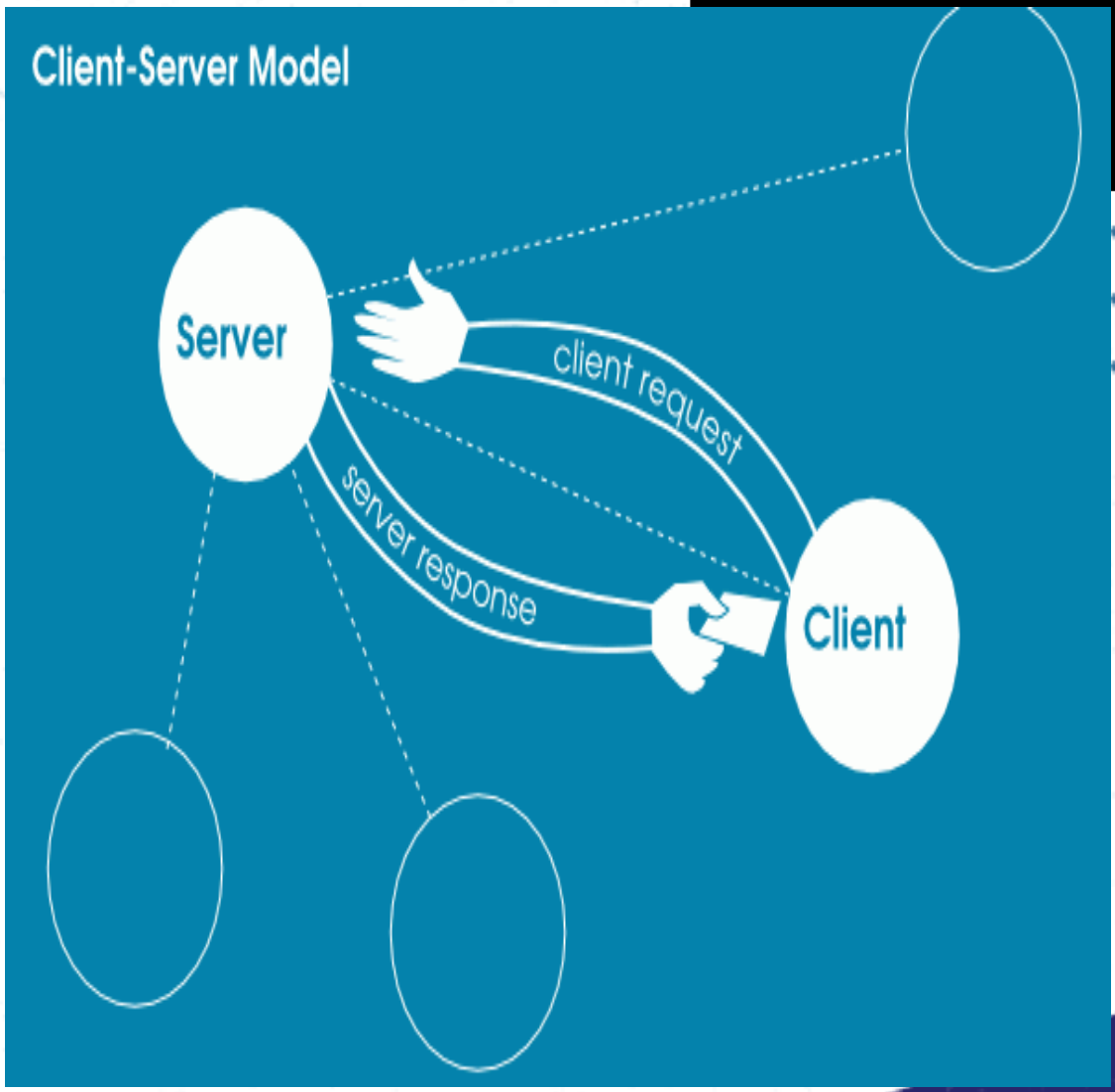


Connectivity is the idea that two computers in different parts of the world can connect to one another and exchange data. If you connect your computer to the Internet, you suddenly can talk with all of the other computers connected on the Internet. Well, at least the ones that want to talk with you too. Let’s look at what exactly that means,

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)

Client-server architecture



Server & Client

- **Server** is a piece of software that mange'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)
- The Domain Name System maintains the domain name hierarchy and provides translation services between it and the addre

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

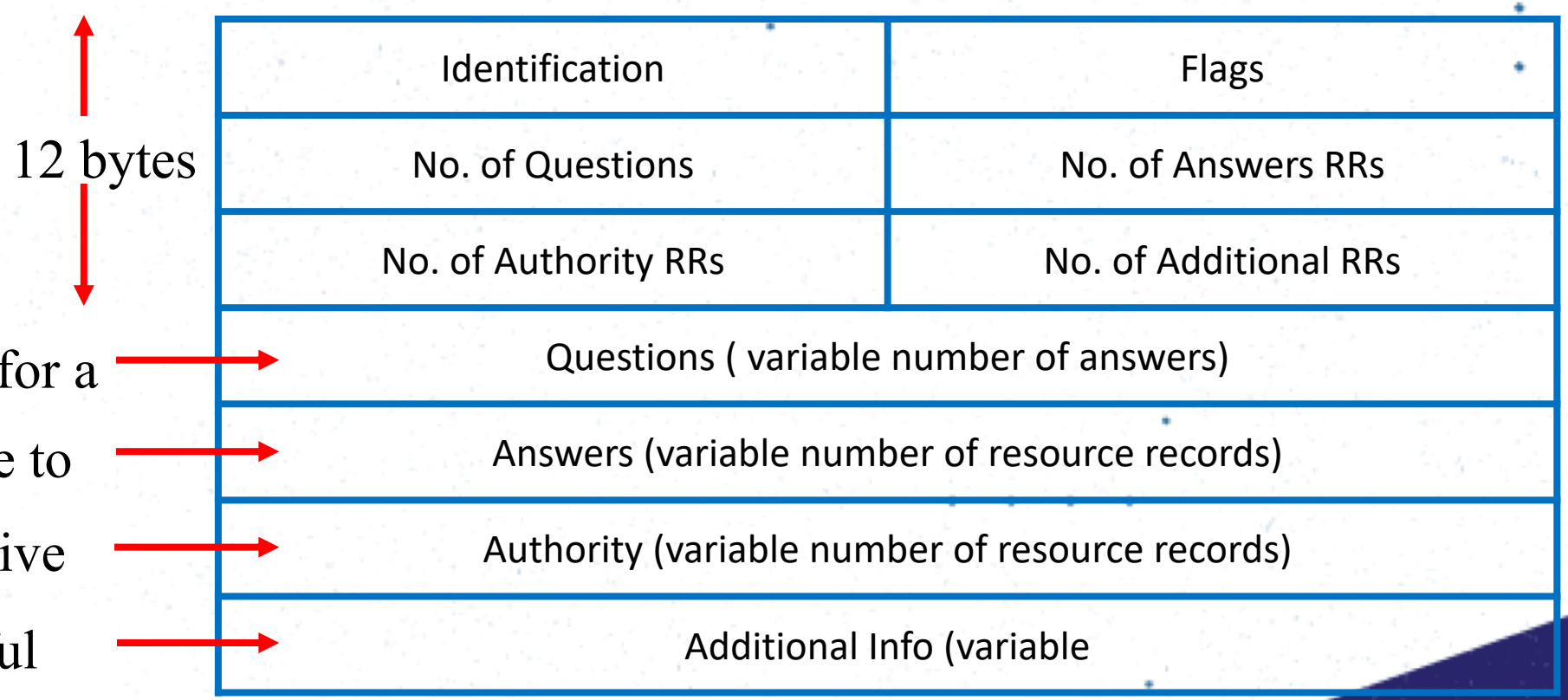
A ranked system (domain)

A certain kinds of partial ordered sets

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

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

DNS message format



- Name, type fields for a qu
- RRs in response to
- Records for authoritative servers
- Additional "helpful info that may be used

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

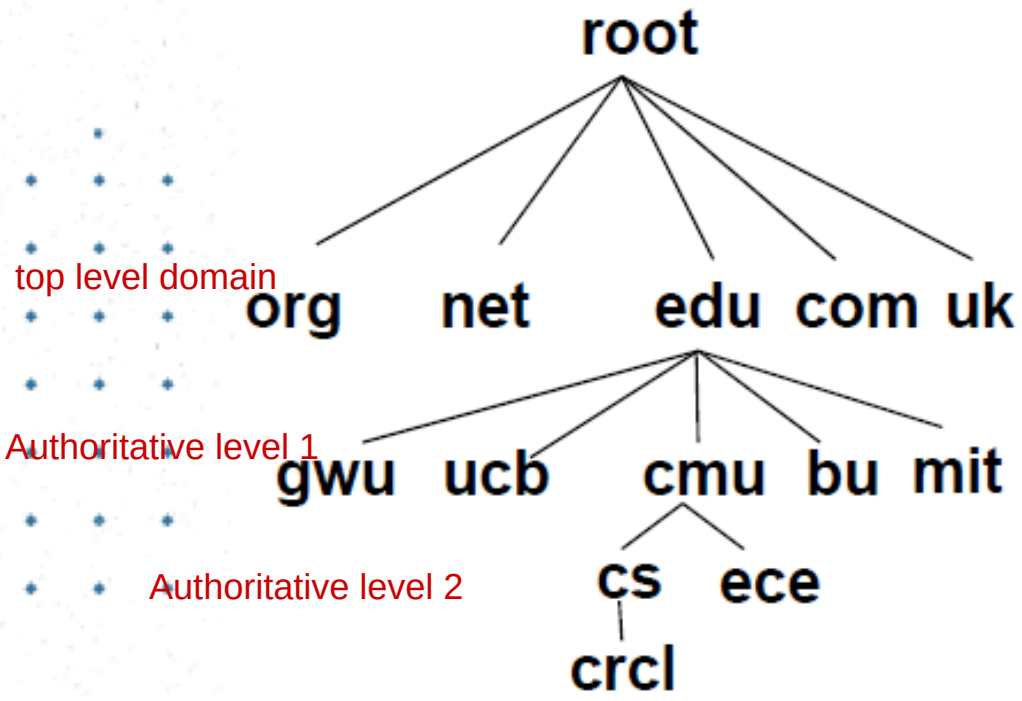
❖Single domain name maps to multiple IP addresses:

- www.google.com map to multiple IP addrs.

❖Some valid domain names don’t map to any IP addr:

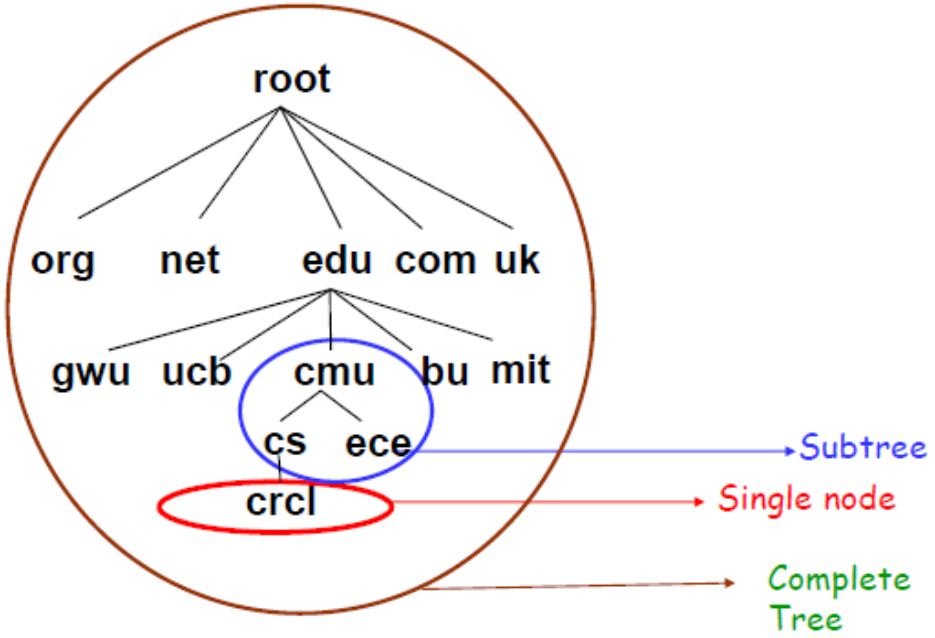
- crcl.cs.cmu.edu doesn’t have a host

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

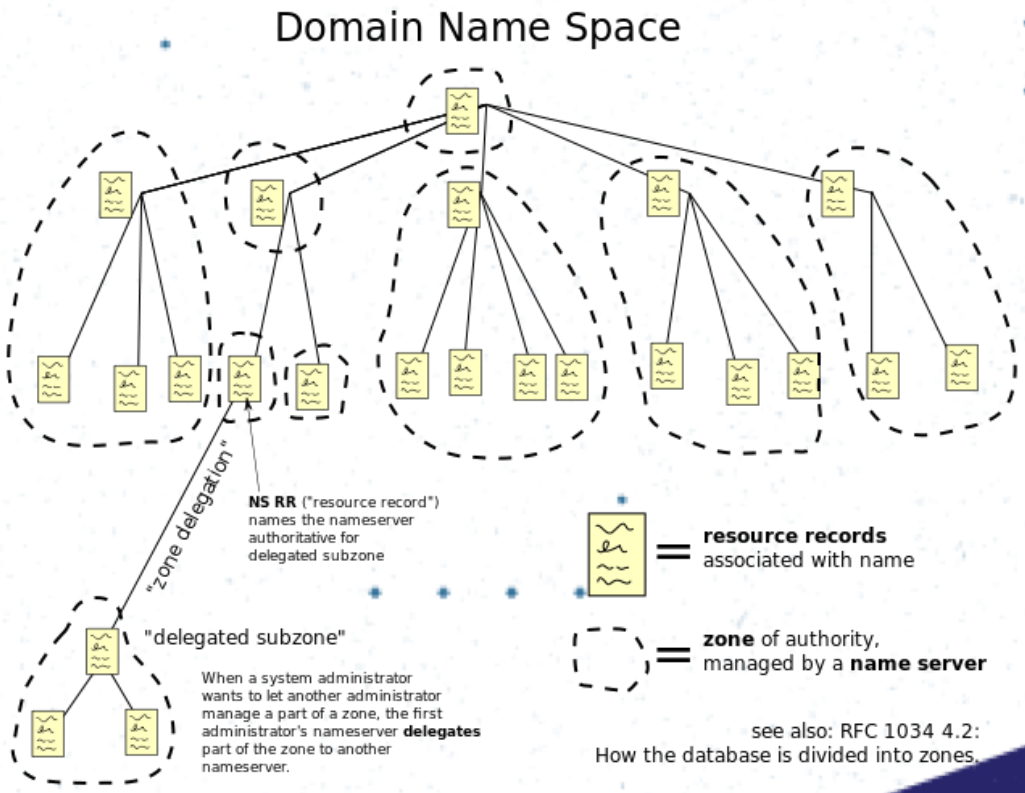
DNS Design: cont…

- 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?

http://www.root-servers.org/

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

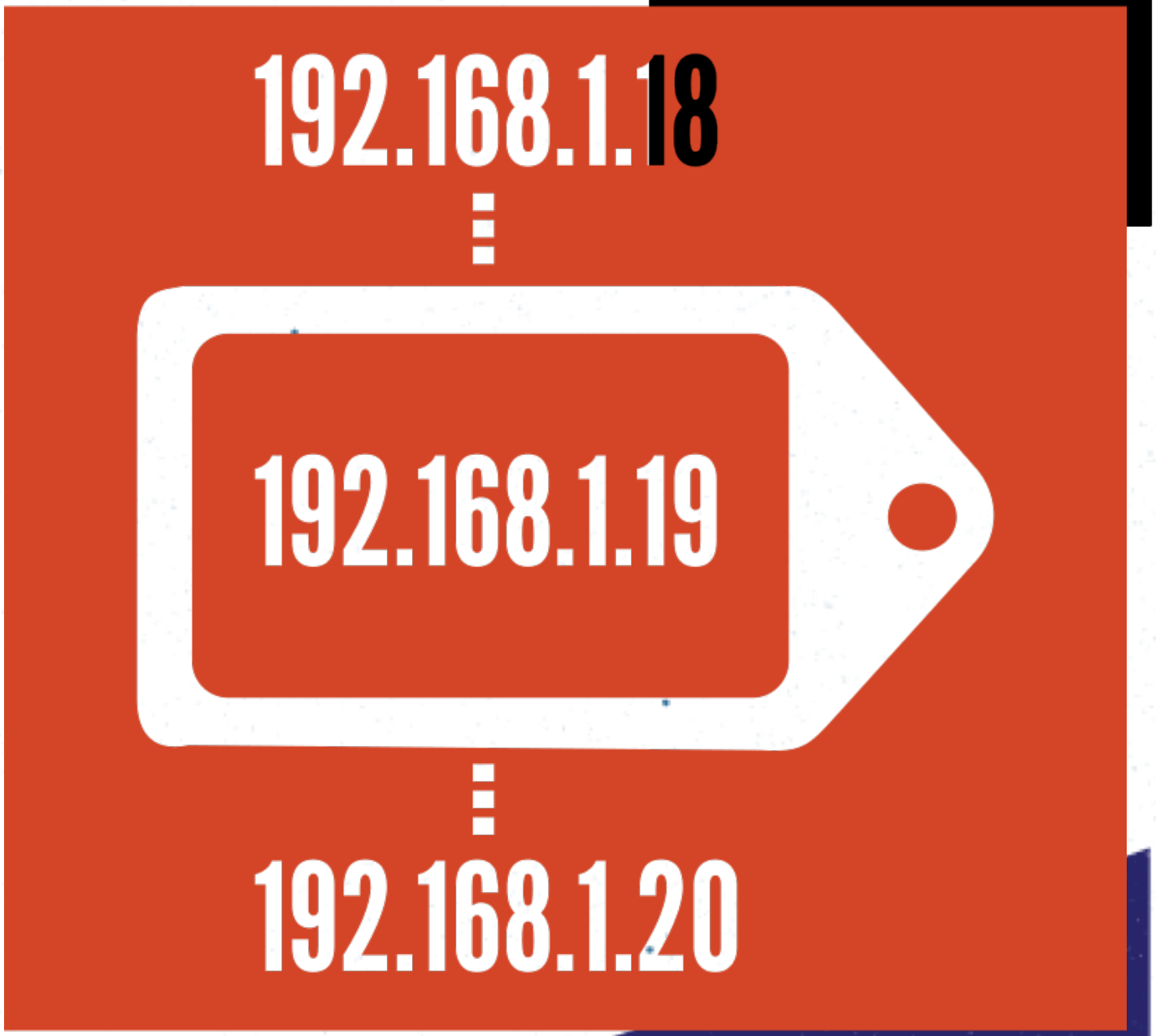
- ❖ Lifetime (TTL) of data controlled by owner of data
- ❖ TTL passed with every record

How do you handle upd

Reliability

- DNS servers are replicated
  - Name service available if ≥ 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)



Dynamic Host Configuration P

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

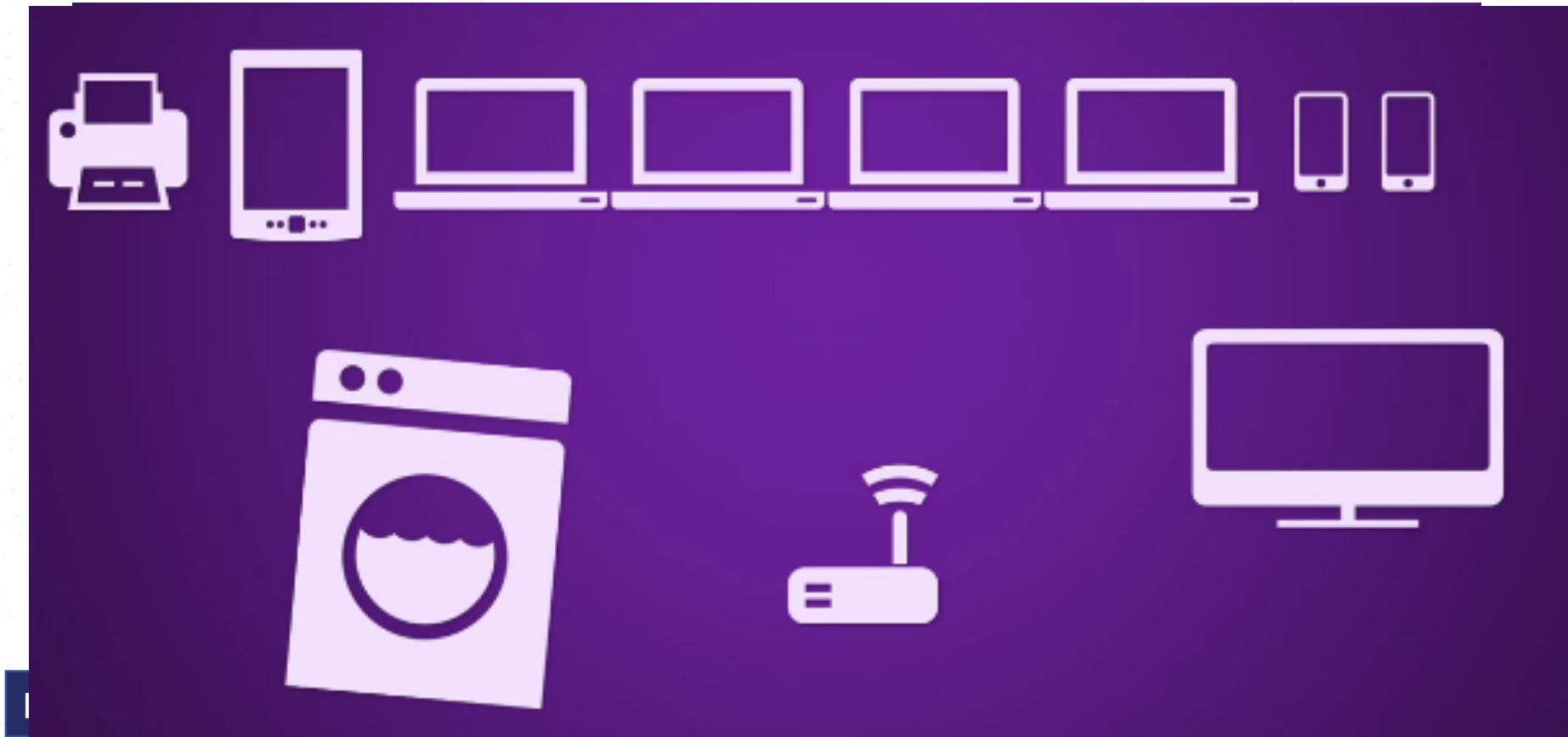
What a Device needs

- 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

[redacted]

- 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 clients 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 .

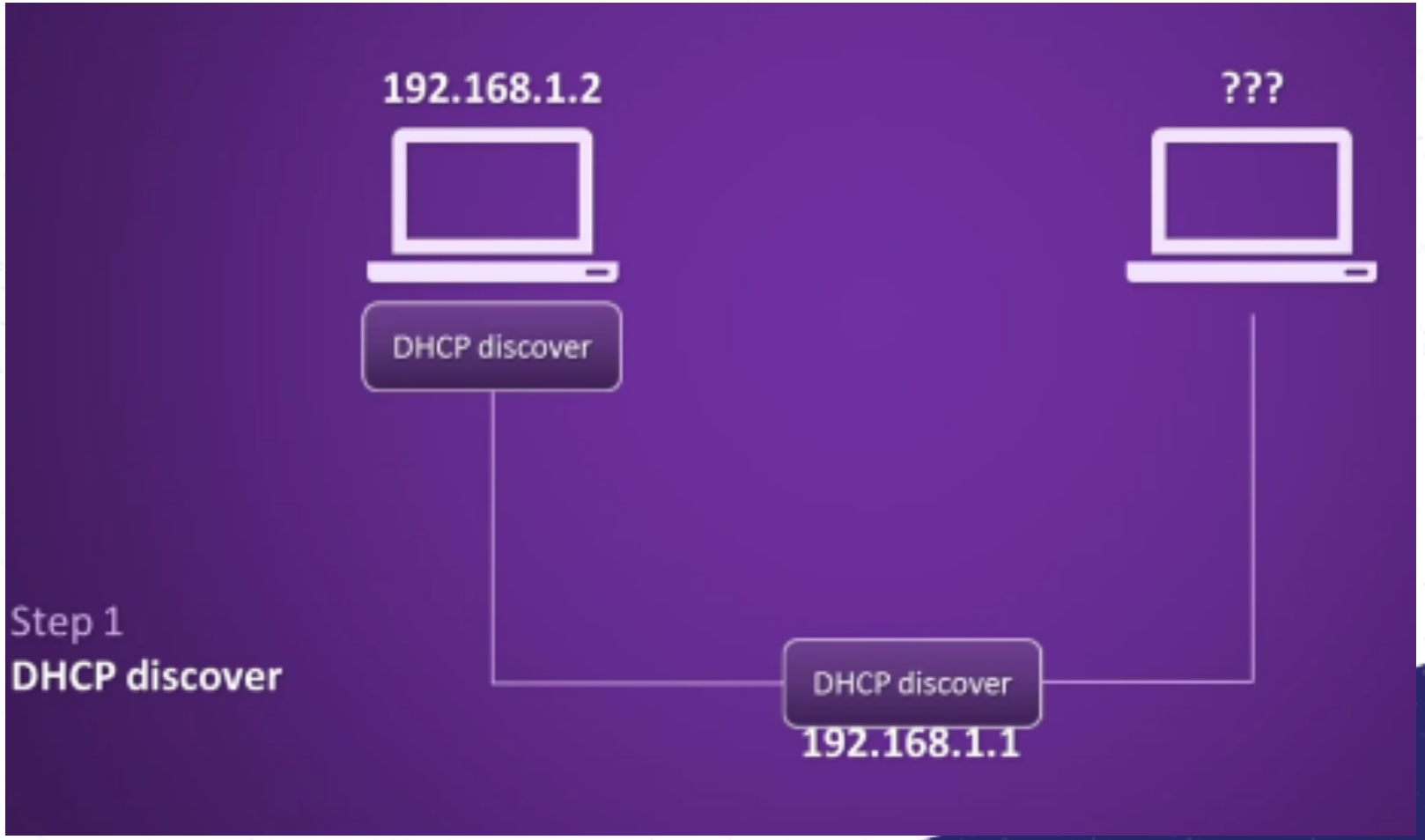
If a windows user:
A user can manually release and renew an IP address by typing the commands??
If Linux user??

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.



DHCP Client UDP port – 68

The host searches for a DHCP

Multiple DHCP servers

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

DHCP Server

DHCP Client

DHCP Message types

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

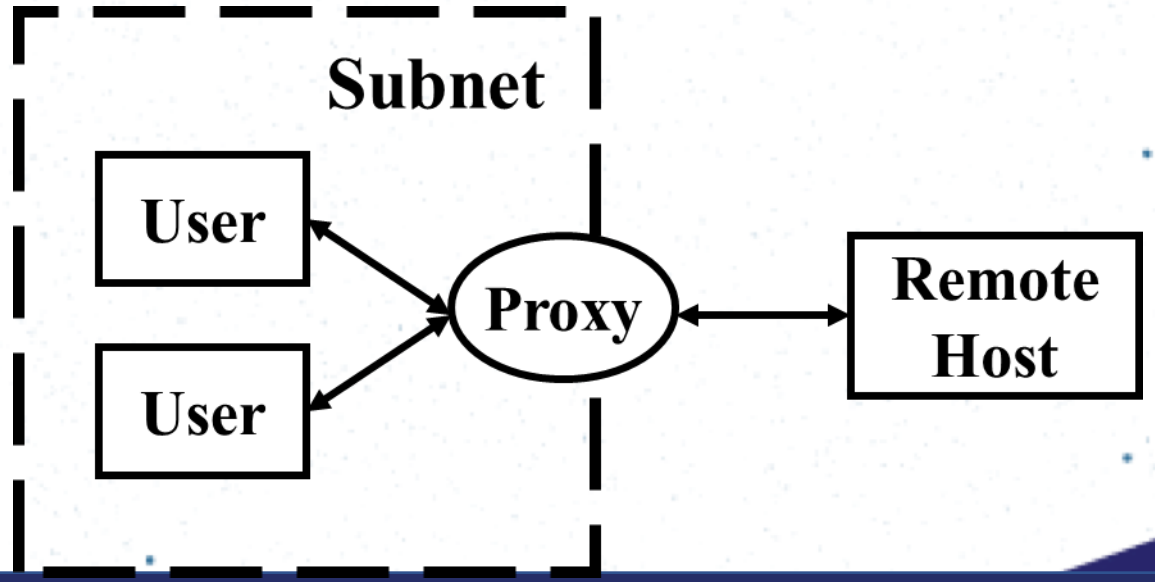
Proxy Server

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 anonymity.*

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.

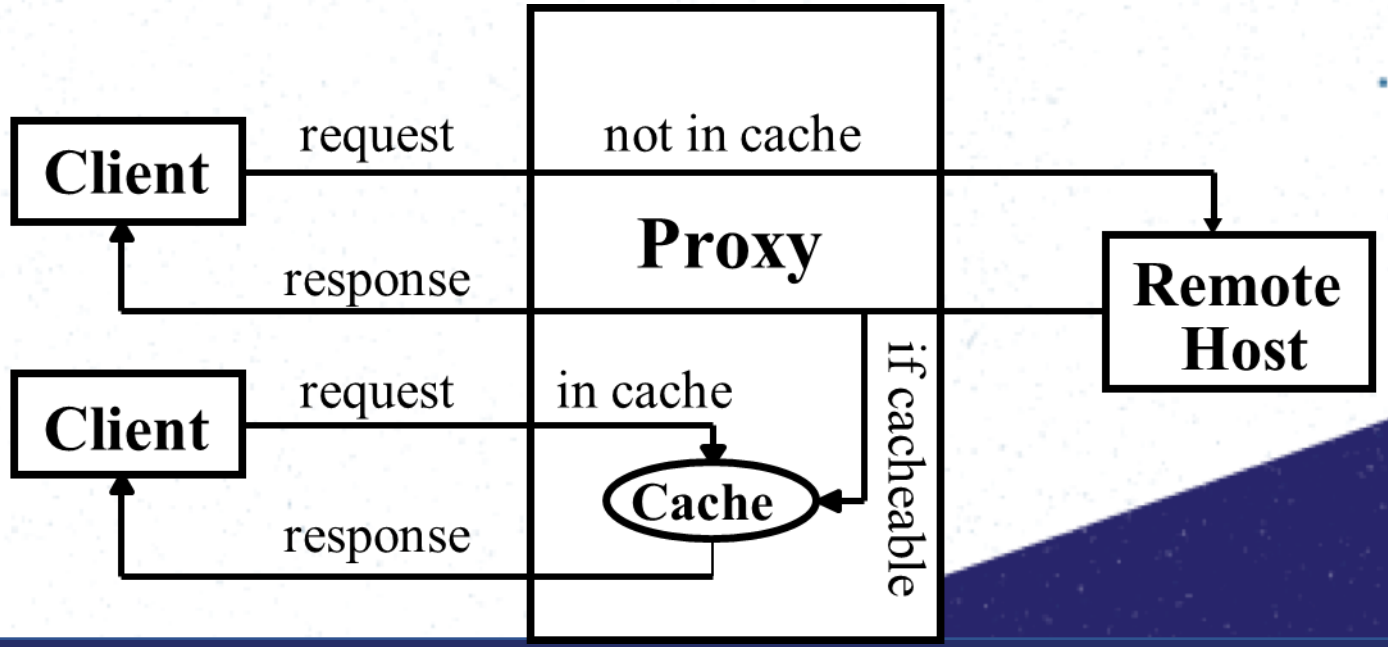
Types of proxy

- **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.

-

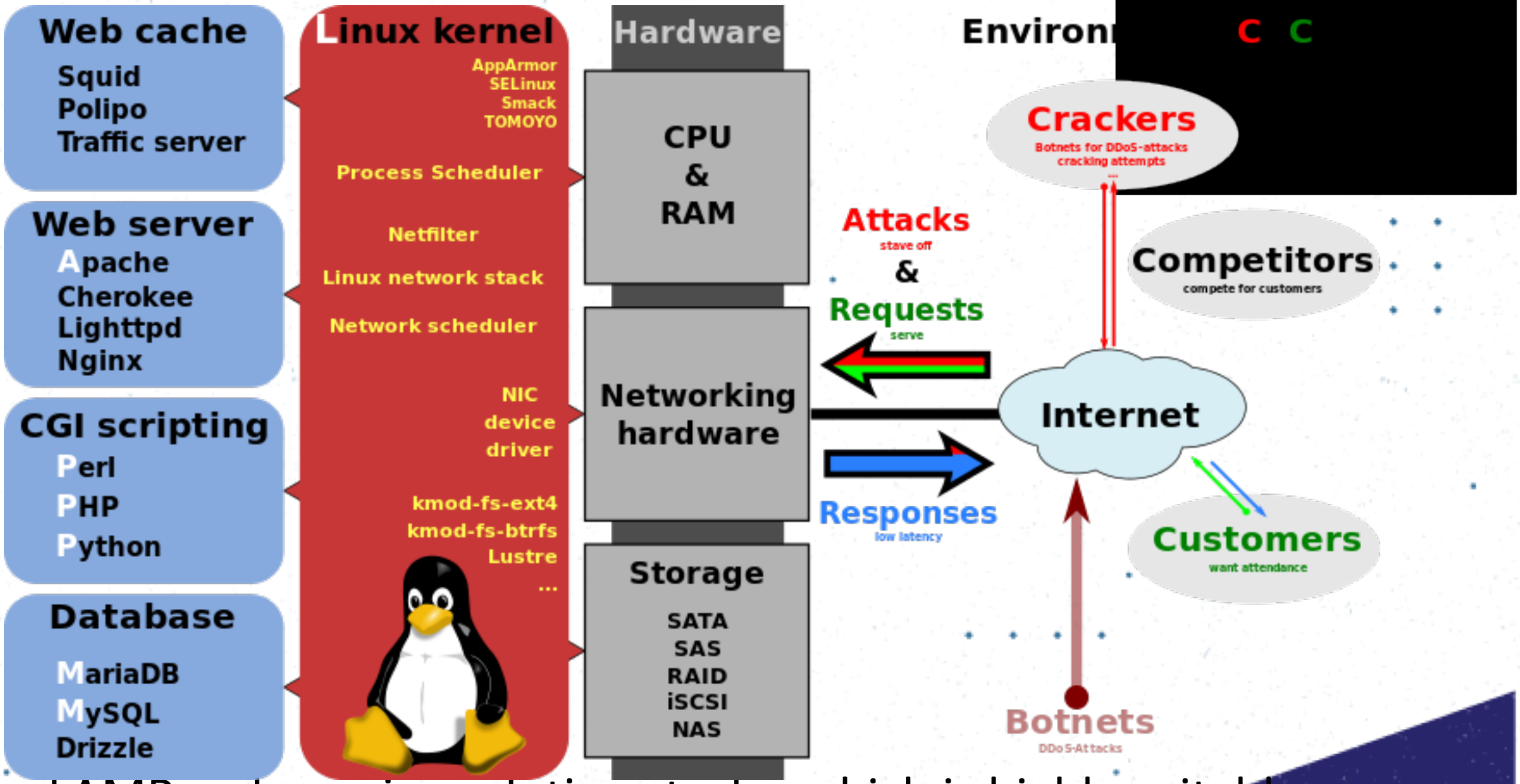
Wikipedia

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
- niginx
- GWS

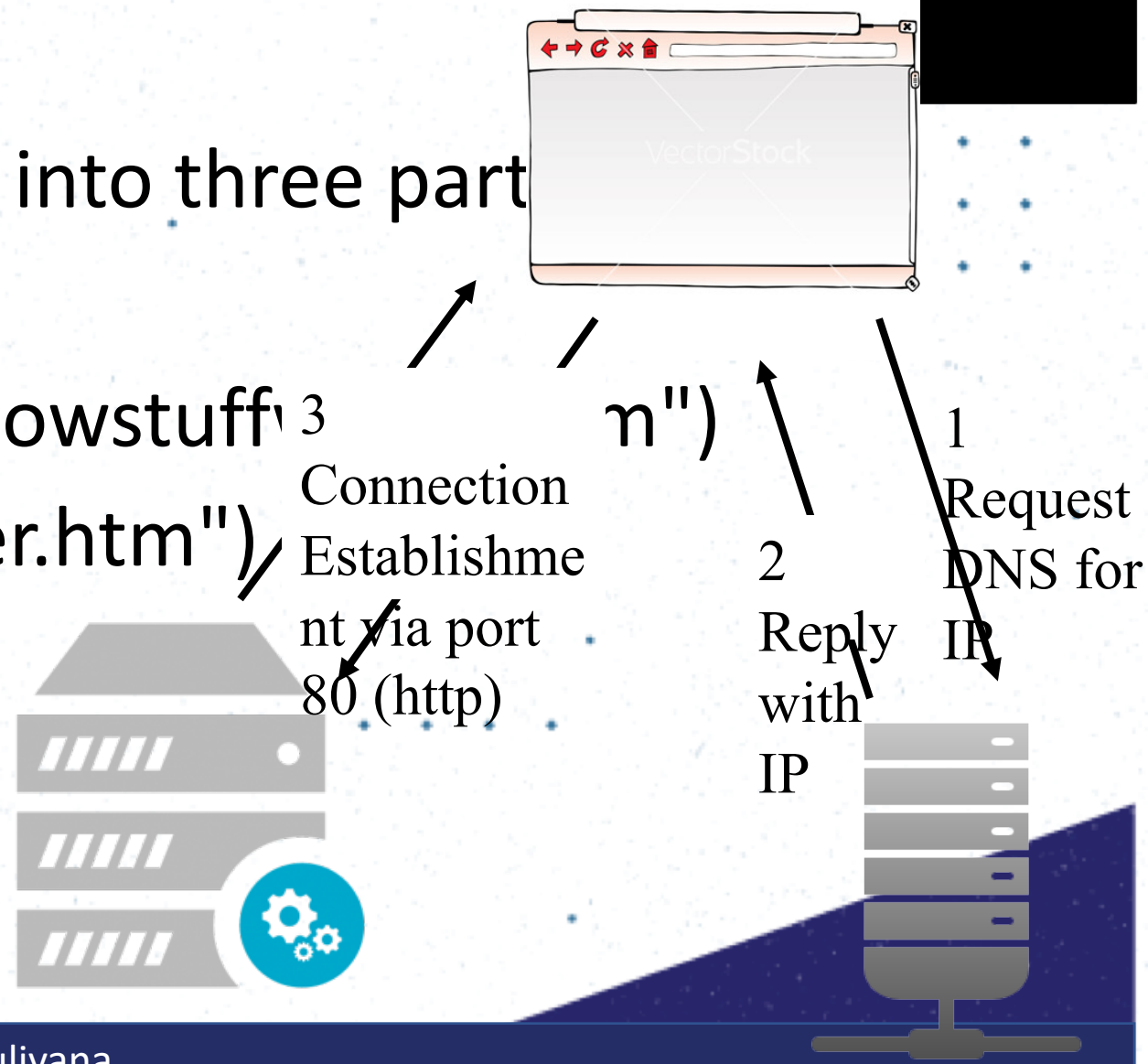


- LAMP web service solution stacks, which is highly suitable for building dynamic web sites and web applications.

Behind the Scenes

- The browser broke the URL into three part

1. The protocol ("http")
2. The server name ("www.howstuff[illegible]m")
3. The file name ("web-server.htm")



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.

-

Wikipedia

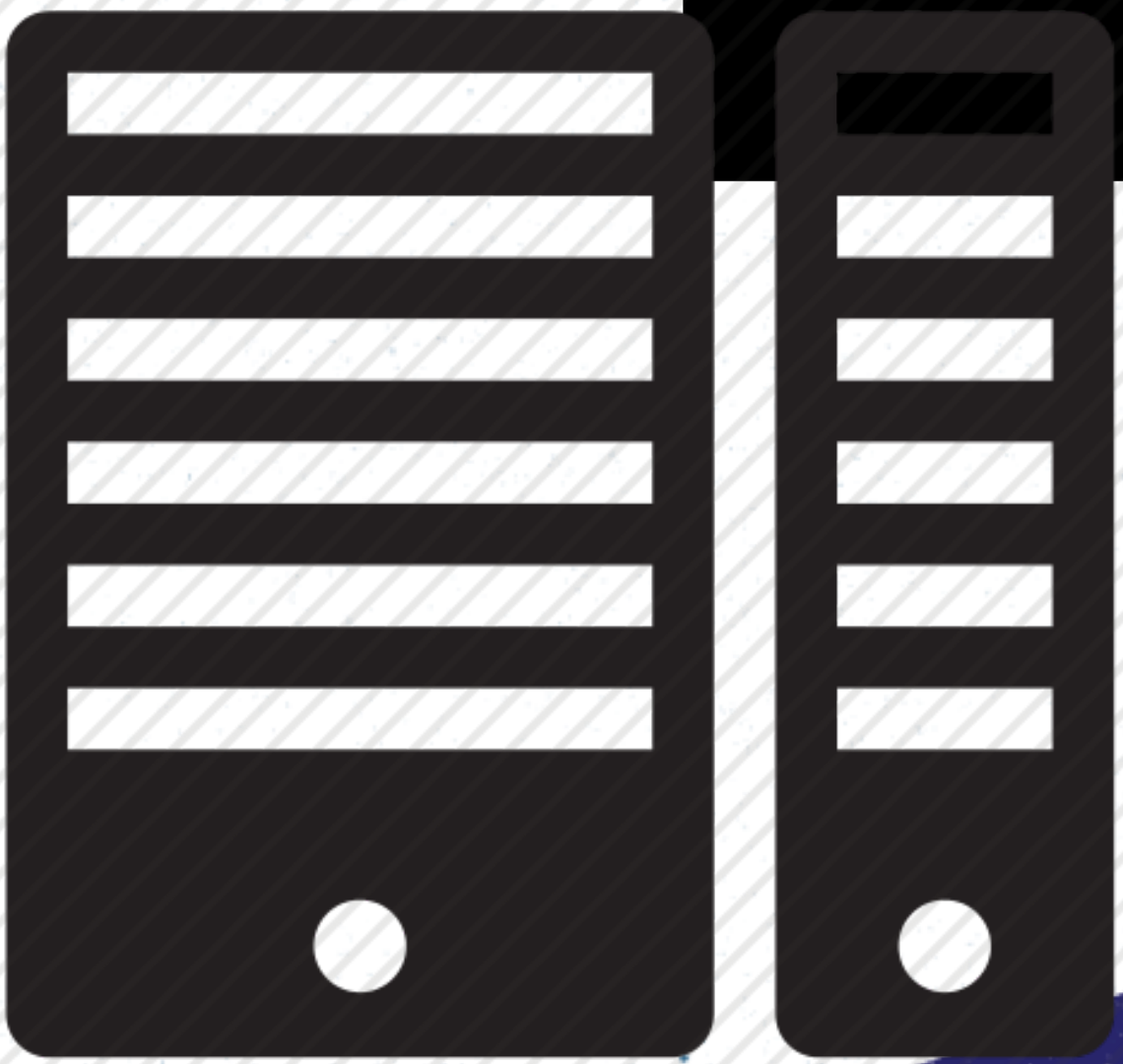
Mail server

- 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

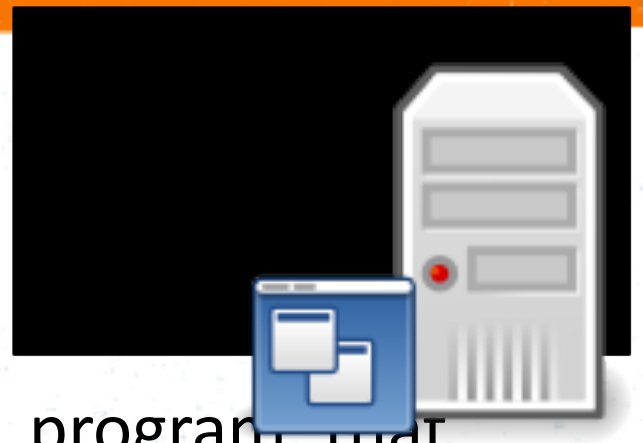
Popular Mail Servers:

- 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 respon 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 t 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.

Questions???

IT3010

Network Design and Management

Lecture 04

Network Mapping and Baselining

Shashika Lokuliyana

Faculty of Computing

Department of CSE

SLIIT

Discover Your Future

Today's lecture overview

- Audit
- Network Mapping
  - Definition
  - Goals
  - Benefits
  - Network mapping the OSI reference model
  - Non network information
  - Tools for performing network mapping
  - In the good old days
- Baselining
  - Why?
  - What?
  - When?
  - How?

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.

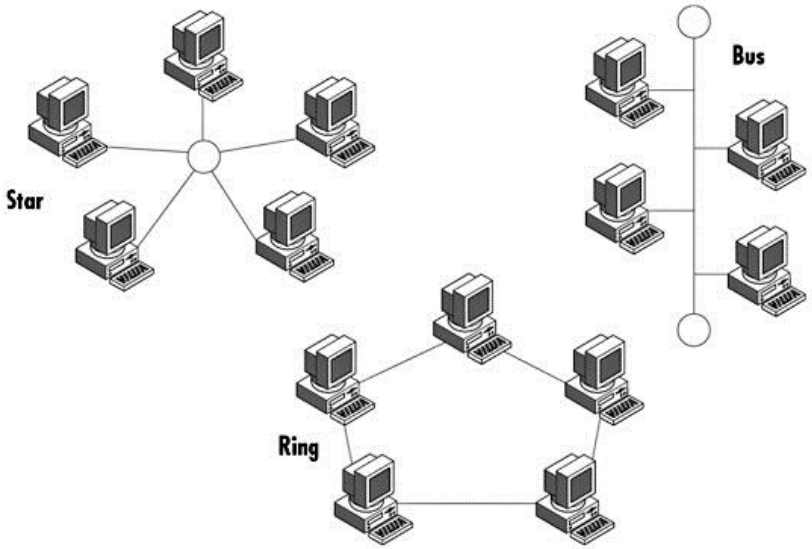
Key points:

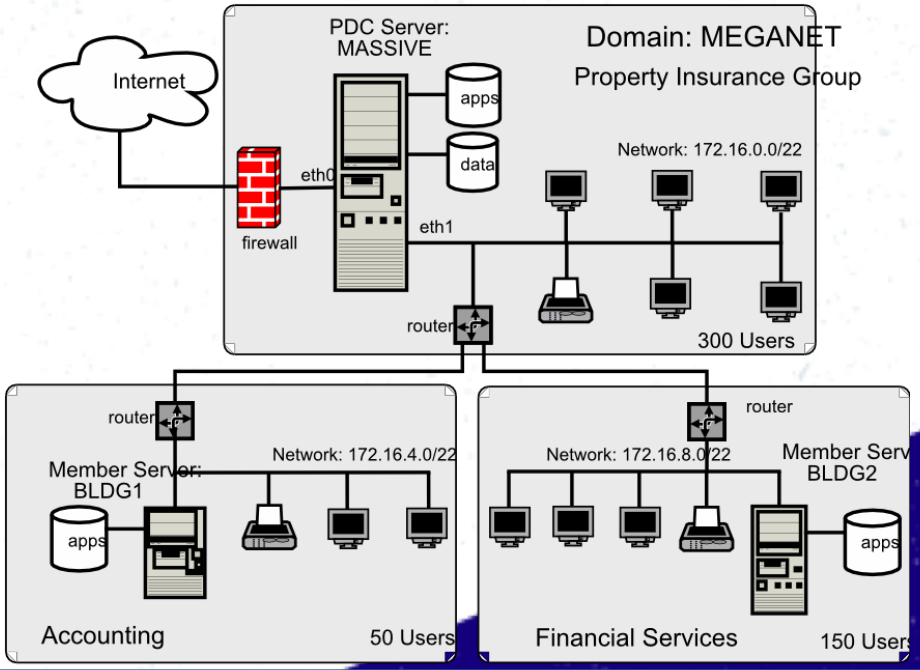
Physical characteristics of interfaces and media, Representation of bits, Data rate, Synchronization of bits, Line configuration, Physical topology, Transmission mode.

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.

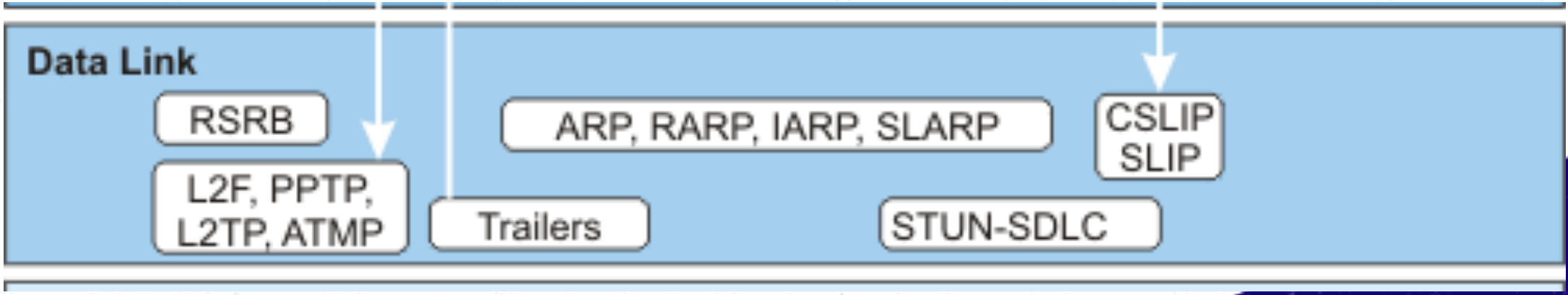
Key points:

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.



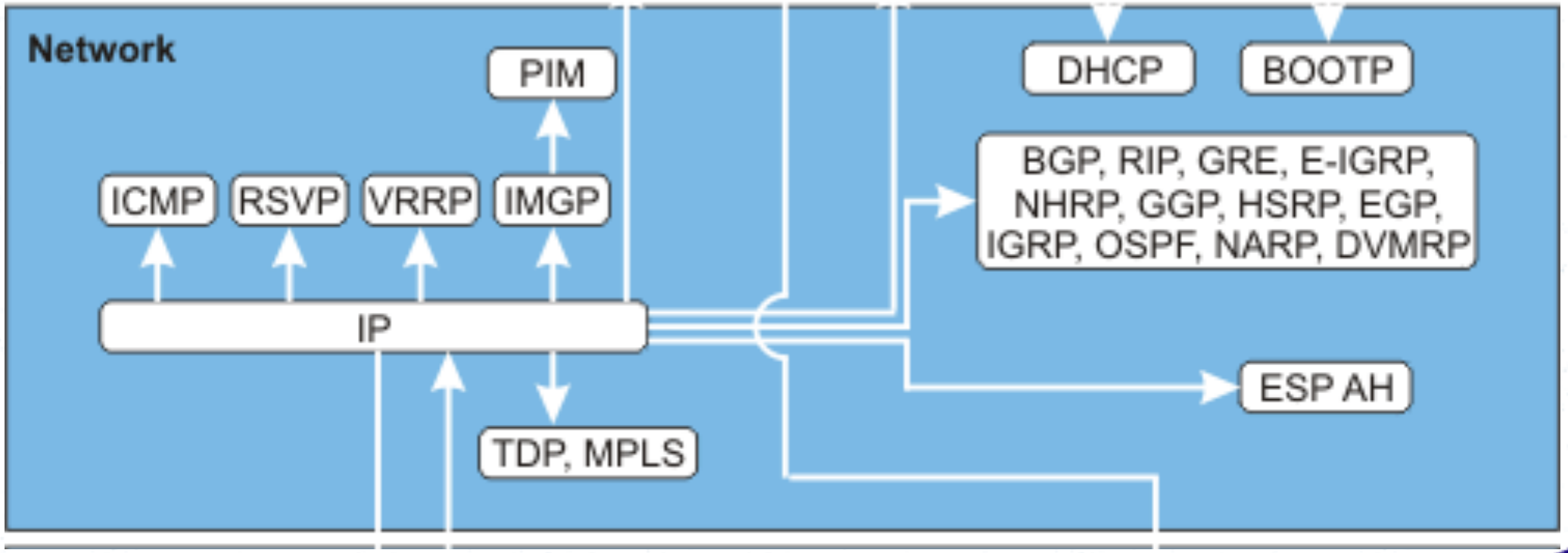
Network Layer

- 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



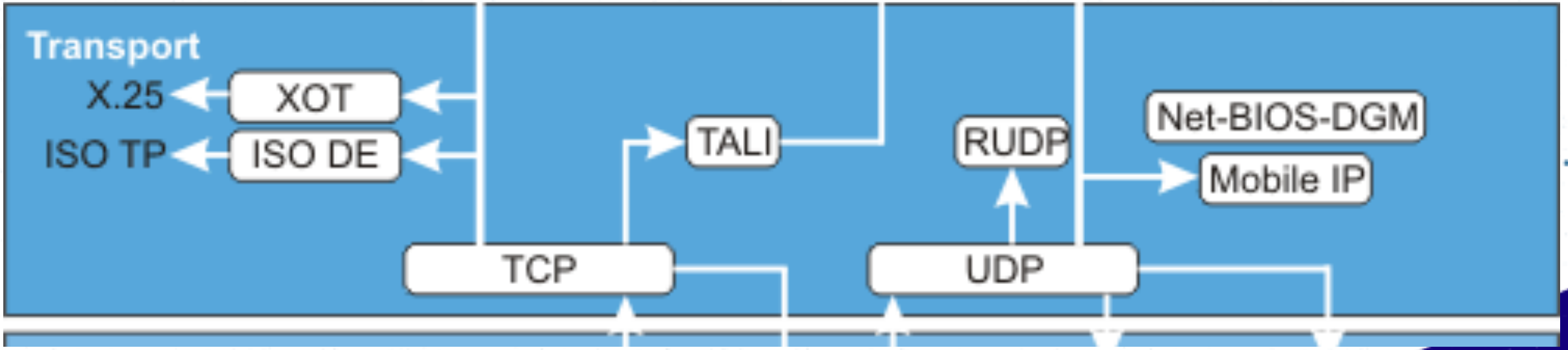
Transport Layer

- 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



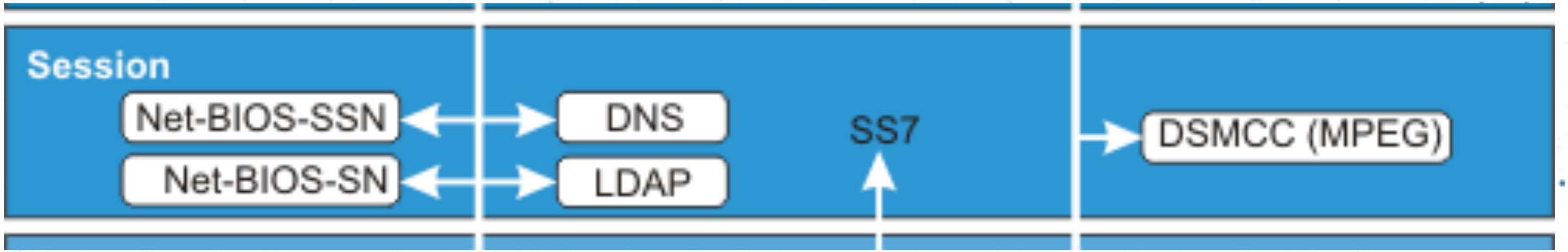
Session Layer

- 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.

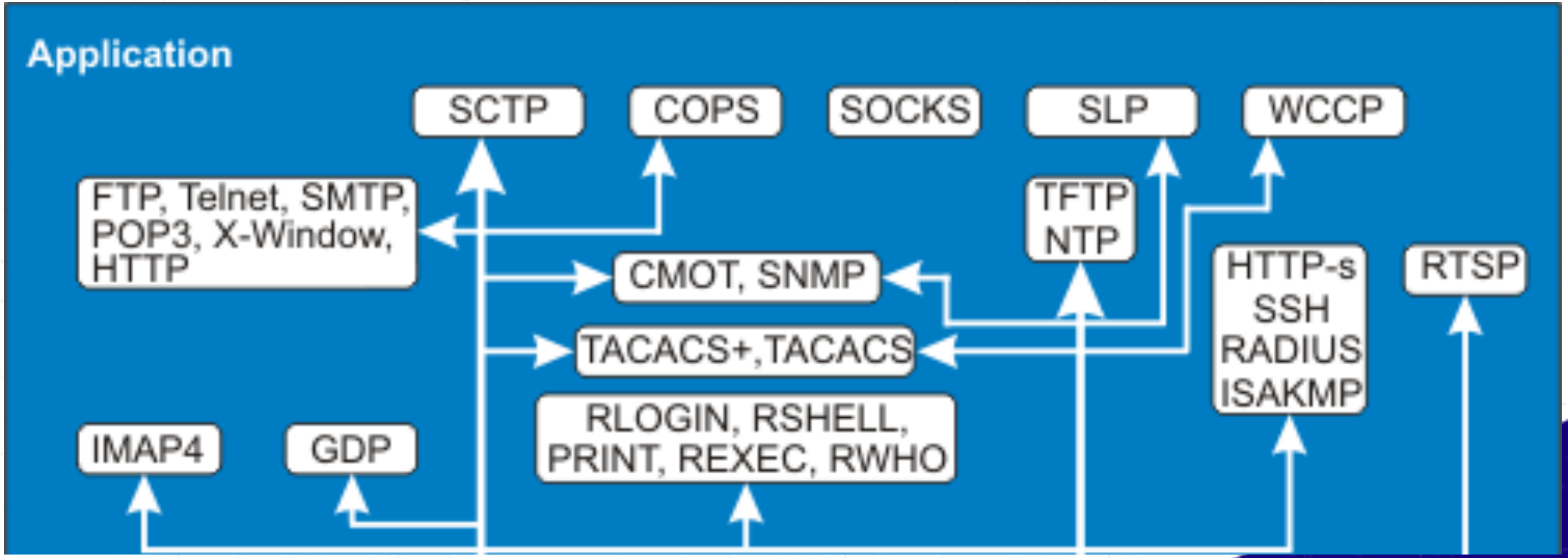
Application Layer

- 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".

Network Baselining

http://www.webopedia.com/TERM/n/network_baselining.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 Baselining

- 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?

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.

Next Lecture..

Network Monitoring

IT3010

Network Design and Management

Lecture 05

Network Monitoring

Shashika Lokuliyana

Faculty of Computing

Department of CSE

SLIIT

Discover Your Future

Network Design and Management

Network Monitoring

Lectuer 5

Today's lecture overview

- Definition of Network Monitoring
- Active vs. Passive monitoring
- Categories for monitoring
  - Network specifications: *Ethernet*
  - Network traffic and protocols
  - Platforms and operating systems (next week lecture)

A definition for Network Monitoring

WIKIPEDIA

The term network monitoring describes the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator (via email, SMS or other alarms) in case of outages. It is a subset of the functions involved in network management.

PCMAG.COM

oring an active communications rk in order to diagnose problems ather statistics for administration and fine tuning.

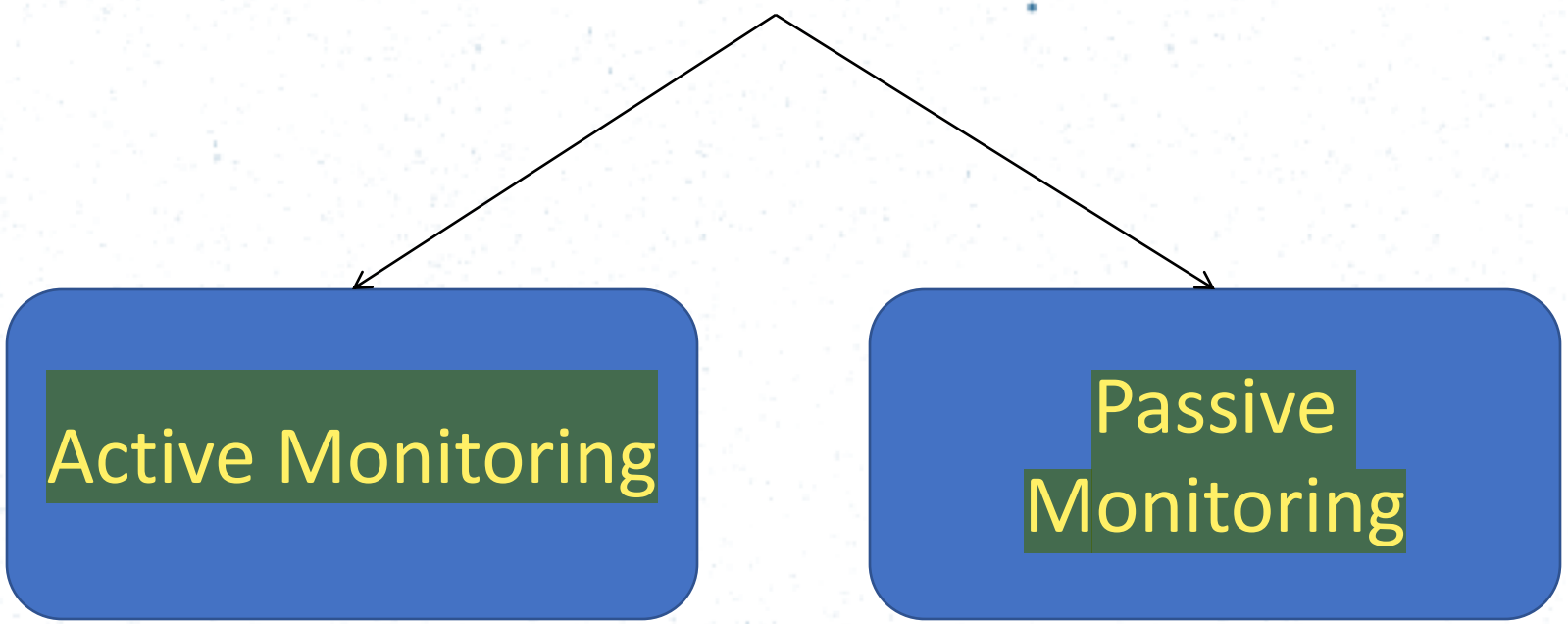
What is Network Monitoring??

- Write it in your terms.

Kevin had a funny feeling that his boss was monitoring his emails

Types of Network Monitoring

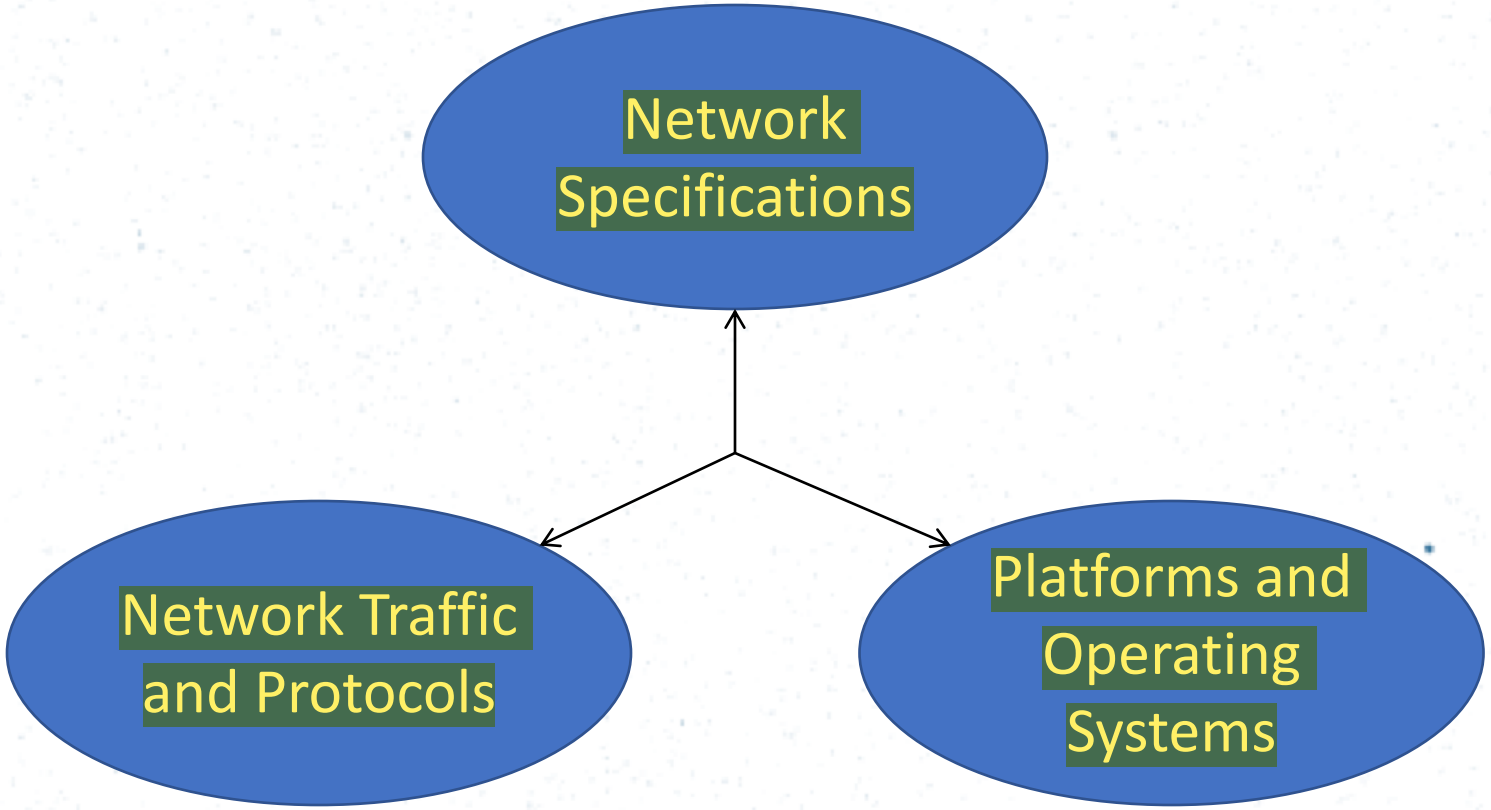
Two types of Network Monitoring



taking out sample/some traffic from the network & one by one analyze what have happened.

Monitoring Categories

Things we will need to monitor…



Monitoring and analysis of Network Specifications

Ethernet

Establishing an Ethernet Baseline

Things to monitor with respect to Ethernet..

- Network utilization
- …
- …
- Collision rate
- Errors

Where it all starts..

```
Router# show interfaces ethernet 0
Ethernet 0 is up, line protocol is up
   Hardware is MCI Ethernet, address is aa00.0400.0134 (via 0000.0c00.4369)
          Internet address is 131.108.1.1, subnet mask is 255.255.255.0
          MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
          Encapsulation ARPA, loopback not set, keepalive set (10 sec)
             ARP type: ARPA, PROBE, ARP Timeout 4:00:00
          Last input 0:00:00, output 0:00:00, output hang never
          Output queue 0/40, 0 drops; input queue 0/75, 2 drops
          Five minute input rate 61000 bits/sec, 4 packets/sec
          Five minute output rate 1000 bits/sec, 2 packets/sec
       2295197 packets input, 305539992 bytes, 0 no buffer
       Received 1925500 broadcasts, 0 runts, 0 giants
       3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
           0 input packets with dribble condition detected
       3594664 packets output, 436549843 bytes, 0 underruns
       8 output errors, 1790 collisions, 10 interface resets, 0 restarts
```

Ethernet Utilization

- Utilization is a network performance measure that specifies the amount of time a LAN spends successfully transmitting data.
- Many performance monitoring tools will provide a user with average and peak utilization times, which are reported as a percentage.

Fact => Delays occur 40% to 50%
Reason => Due to increased collisions
Solution => ……
Expectation => Should achieve 15% to 25%

Peak Utilization

Peak utilization means that, ...

....., a certain percentage of the LAN's capacity was utilized.

The peak utilization is the maximum bandwidth limit reached at any point in time on an interface

- Need to look at
  - Protocols
  - Devices
  - Users
- Determine when peaks occur

Average Utilization

average utilization provides an average bandwidth reading which gets calculated over a period of five minutes

Average utilization means that ……

……(e.g. 10 hours), on average, a certain percentage of the LAN's capacity is used for successfully transmitting data. In simple terms this is the calculated level over longer time.

- What are we averaging?

```
Last input 0:00:00, output 0:00:00, output hang never
Output queue 0/40, 0 drops; input queue 0/75, 2 drops
Five minute input rate 61000 bits/sec, 4 packets/sec
Five minute output rate 1000 bits/sec, 2 packets/sec
2295197 packets input, 305539992 bytes, 0 no buffer
```

  - What is bits-per-second?

Current Utilization

Current utilization is the moving average calculated over a small time period (e.g. 5 minutes).

$$\text{new average} = ((\text{average} - \text{interval}) * \exp(-t/C)) + \text{interval}$$

Where:

- t is five seconds, and C is five minutes. exp(−5/(60*5)) == .983. This value is known as the "weighting factor" or "decay factor".
- newaverage = the value we are trying to compute.
- average = the "newaverage" value calculated from the previous sample.
- interval = the value of the current sample.

Additional Resources for Utilization Monitoring

Please make sure to read the following PDF documents uploaded to the course web.

1. Extracted_from_Networking_Explained_Part_1.pdf *(2 pages)*
2. Extracted_from_Networking_Explained_Part_2.pdf *(2 pages)*
3. Understanding_the_bits_per_second.pdf *(3 pages)*

Note

Please note that the first two documents in the above list are two parts of the same document. You should refer starting from Ques #26 in part 1 and continue up to and including Ques #32 in part 2.

Broadcasts

```
2295197 packets input, 305539
Received 1925500 broadcasts,
3 input errors  3 CRC  0 fram
```

Broadcast + Multicast

- Excessive amounts of broadcast or multicast traffic,
- Broadcasts Rate should not exceed 5-10%

Multicasts

- Communication between small groups of devices.
- Same rules as broadcast.

Examining Ethernet Errors

- Collisions
- Short frames
- Bad FCS
- Long frames
- Ghosts

Collisions

```
ets output, 436549843 byte
ors, 1790 collisions, 10 i
```

If two frames are transmitted simultaneously by two stations, they overlap in time and the resulting signal is garbled. This event is known as a collision.

- Collisions are normal
- CSMA/CD
- Jam signal

In order to avoid this situation we have techniques with collision avoidance and collision detection methods.

Additional Resources for Collisions

- Please make sure to read chapter, “4.2.2 Carrier Sense Multiple Access Protocols (from Pg 255 to Pg 258)” of Tanenbaum’s book.

- Please make sure to read the following PDF documents uploaded to the course web.
  1. Causes_for_collisions.pdf *(1 page)*
  2. Troubleshooting_collisions.pdf *(6 pages)*

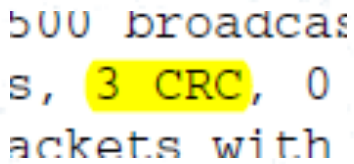
Short Frames

```
305539992 bytes, 0
asts, 0 runts, 0 gi
0 frame. 0 overrun.
```

- A short frame is a frame smaller than the minimum legal size of 64 bytes, with a good frame check sequence.
- Caused by,

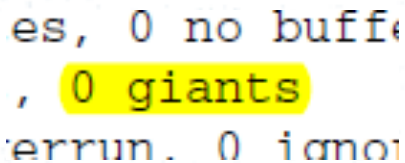
http://units.folder101.com/cisco/sem1/Notes/ch6-ethernet/eth-frames.htm

Bad FCS (Frame Check Sequence)



- A received frame that has a bad Frame Check Sequence, also referred to as a checksum or CRC error, differs from the original transmission by at least one bit.
- In an FCS error frame, the header information is probably correct and the frame may also have a valid size, but the checksum calculated by the receiving station does not match the checksum appended to the end of the frame by the sending station. The frame is then discarded.

Long Frames (Giant frame)



- A long frame is a frame larger than the maximum legal size of 1518 bytes.
- It does not consider whether or not the frame had a valid FCS checksum.
- Causes

Ghosts

- Ghosts are classified as energy (noise) detected on the cable that appears to be a frame, but is lacking a valid SFD.
- To qualify as a ghost, the frame must be at least 72 bytes long, including the preamble.
- Slows network, not increased utilization.
- Causes,

Documentation

Ethernet Baseline Statistics			
Network-Based		**Node-Based**	
% Utilization -Peak		% Utilization - Peak	
% Utilization - Average		% Utilization - Average	
Frames/Second - Peak		Frames/Second - Peak	
Frames/Second - Average		Frames/Second - Average	
Frame size - Peak		Frame size - Peak	
Frame size - Average		Frame size - Average	
Total Frame Count		Total Frame Count	
Total Byte Count		Total Byte Count	
Node count - Total		Node/Node Interaction - Total	
Top 10 Nodes		Node/Node Int. - Predominant	
Protocol count - Total		Protocol count - Total	
Protocol count - Top 3		Protocol count - Top 3	
Network Errors		**Station Errors**	
Collisions - Total		Collisions - Total	
Collisions/Second		Collisions/Second	
Runts/Fragments - Total		Runts/Fragments - Total	
Jabbers - Total		Jabbers - Total	
# of CRC/FCS Errors - Total		# of CRC/FCS Errors - Total	

Additional Resources for Monitoring the Ethernet

Please make sure to read the following PDF documents uploaded to the course web.

1. Ethernet_errors.pdf *(5 pages)*
2. Troubleshooting_ethernet.pdf *(12 pages)*

Monitoring and analysis of the Network Traffic

Network Traffic

What & how should we measure..?

- Measure amount and type
  - Need hardware tools

What are possible types to monitor..?

- Number of Nodes/Users
- Protocols
- Broadcast/Multicast/Unicast
- Conversations
- Errors

Number of Nodes/Users

- Workstations
- Servers
- Peripherals
- Routers and switches
- Who is on the network
- Physical access

Protocols

- Device dependent
- Segment dependent

How much of your traffic is overhead protocols

ARP – Address Resolution Protocol

To find the physical address for a given logical address.

DNS – Domain Name Service

To find the IP address for a given domain name.

ICMP – Internet Control Message Protocol

One of the core protocols of the Internet Protocol Suite used primarily for the purpose of sending error messages.

How much of your traffic is overhead protocols

LDAP – Lightweight Directory Access Protocol

For the purpose of accessing and maintaining distributed directory information services.

RIP, EIGRP, OSPF etc.

For the purpose of managing network devices.

Connections

- Who is talking to who?
  - ❑ How much?
    - ➢ Routers
    - ➢ Servers
- Applications
  - ❑ What applications are on the network
  - ❑ What protocols are they using
  - ❑ Which users access them

Where do errors occur?

- 65% to 75% of network errors occur in the first three layers

- Causes
  - ❑ Duplicate addresses
  - ❑ Host/Station/Network unreachable
  - ❑ Time-To-Live (TTL) exceeded

Monitoring and analysis of Platforms and Operating Systems

Determining Server Workload Characterization

What is workload characterization..?

- Within the confines of a network, workload is the amount of work assigned to, or done by, a client, workgroup, server, or internetwork in a given time period.

- Therefore, workload characterization is the science that observes, identifies and explains the phenomena of work in a manner that simplifies your understanding of how the client, workgroup, server, or internetwork is being used.

Determining Server Workload Characterization

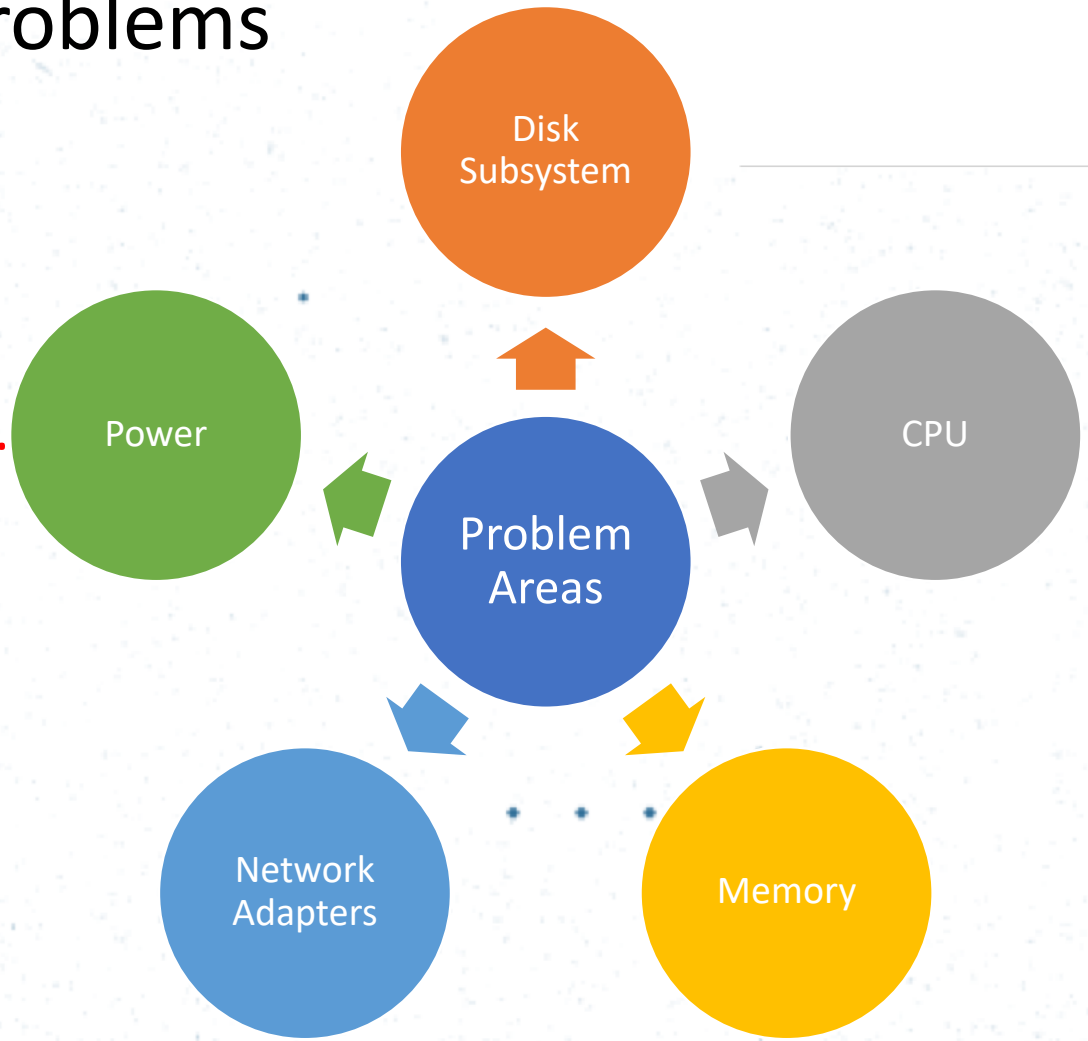
Things that should be considered..

- Server type
- Workload characterization
- Isolate components that restrict data flow
- Set expectations

What are common server problems

Problems can occur in..

Not covered.



What are common server problems

Disk Subsystem

- The disk subsystem is more than the disk itself.
- It will include,

- Problems can occur with any of the above components..!!

Note

In NT based windows server environments, the disk subsystem is divided into two part for ease of monitoring and troubleshooting.

- Physical disk - used for the analysis of the overall disk, despite the partitions that may be on the disk.
- Logical disk - analyzes information for a single partition.

What are common server problems

CPU

- Most server machines today, support 1-4, 1-8 or even 1-16 processors.
- And each processor can have up to 18 CPU cores.
- That is A LOT to monitor and troubleshoot..!!

Leads to common problems..

- Overheating due to not been correctly thermally bonded with heat sink during installation & replacement.
- Mismatches between CPU and memory speeds.
- Different CPUs populated with different number and size of memory modules.
- Etc.. Etc..

What are common server problems

Memory

- In server machines each processor can be populated with one or more memory modules.
- Some modern server stations even support up to 96 memory modules.

Leads to common problems..

- The number and size of modules not same for all CPUs in a server.
- Memory module not seated properly in the slot.
- Using modules having different speeds.
- Memory module not supported by the particular server model.
- Etc.. Etc..

What are common server problems

Network Adapters

- Some modern server stations can support a large number of NIC ports, even up to 16 ports.
- Larger the number of ports become, so does the complexity of troubleshooting..!!

Leads to common problems..

- Not loading the appropriate firmware version for the adapters.
- If/when using dual adapters, not following the restrictions on the supported combinations.
- Etc.. Etc..

File and Print Servers

- File and printer servers manage the storage of data and the various printers on the network.

  E.g. Windows Server 2008, Mac OS X Server, Red Hat Linux Server, Ubuntu Server Edition.

- **Key Concern**: Disk I/O or the number of user's attempting access to the server is the most critical concern.

- Focus on the number of users accessing server concurrently (also how they are accessing the server) and amount of resources demanded.

Web Servers

- Web servers allow Internet users to attach to your server to view and maintain web pages.

- Ordering of problem areas to focus,

  Memory > Network >

- Must fulfill requests from cache to achieve maximum performance.

Application Server

- Application server is a server that handles all application operations between users and an organization's backend business applications or databases. Aka *appserver*.
- Features include, built-in redundancy, monitor for high-availability, high-performance distributed application services and support for complex database access.
- Ordering of problem areas to focus,

  Memory >
- Application server usually has smaller, more frequent requests to it than File and Print Server environment.

Logon Server/System Services

- As the name implies, logon server is used for the purpose of authenticating users to the domain.
- Logon servers can provide convenient authentication features like Single Sign On (SSO), which enables the users to access multiple applications/services using the same username and password.
- Ordering of problem areas to focus,

  Processor > Disk
- Things to keep an eye on,
  - ❑ Activity generated between Servers.
  - ❑ Users - Peak activity more of a concern.

Why..?

Factors affecting performance

- Performance degradation is proportional to the problems.

- Hence, areas that problems can occur are the same areas that will affect performance.
  - ❑ Disk Subsystem
  - ❑ Memory
  - ❑ CPU
  - ❑ Network

Common Hard Disk Measurements

- Current Disk Queue Length
- % Disk Time
- Avg. Disk Queue Length
- Disk Reads/sec
- Disk Reads Bytes/sec
- Avg. Disk Bytes/Transfer
- Avg. Disk sec/Transfer

Paging and Swapping

Paging

- Move individual pages of process to the disk to reclaim memory.
- The paging algorithm keeps track of when each page was last used and tries to keep pages that were used recently in memory.

Swapping

- Move an entire process to disk to reclaim memory.
- Next time the system runs the process, it has to copy it from the disk swap space back into memory.

Revisit OS lecture slides..

Common Memory Measurements

- Page Faults/sec
- Pages Input/sec
- Pages Output/sec
- Pages/sec
- Page Reads/sec
- Page Writes/sec
- Available Memory
- Nonpageable memory pool bytes
- Pageable memory pool bytes
- Committed Bytes
- Pool Paged Bytes
- Pool NonPaged Bytes
- Working Set
- Paging File, %pagefile in use

Common Processor (CPU) Measurements

- % Processor Time
- Interrupts/sec
- % Interrupt Time
- % User Time
- % Privilege Time
- % DPC Time
- % Processor Time
- Processor Queue Length
- System Calls/sec
- % Total Processor Time
- % Total User Time
- % Total Privilege Time
- % Total Interrupt Time

Common Network Card Measurements

- Bytes Sent/sec
- Bytes Received/sec
- Bytes Total/sec
- % DPC Time
- DPCs queued/sec
- % Broadcasts
- % Multicasts
- Segments Sent/sec
- Segments Received/sec
- Segments/sec
- Segments Retransmitted/sec
- Connection Failures
- Connections Reset
- Connections Established
- Server Sessions
- Output Queue Length

Further reading..

If you are interested in knowing some further information about performance counters you can refer the following PDF uploaded to moodle,

Performance_Counters.pdf

Don’t overdo it…!!!

Excessive network monitoring (active) can and will slow your network…!!!

~ THE END ~