



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
- Abilities of data network

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
Engineering Computer subnet	A

Data Collection, Modification and Storing

Data Collection

Two methods..

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

Data Collection, Modification and Storing

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 Storing

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 Storing

Storing Information

Methods of storage:

- **Structured** (e.g. DBMS)

- Advantages:

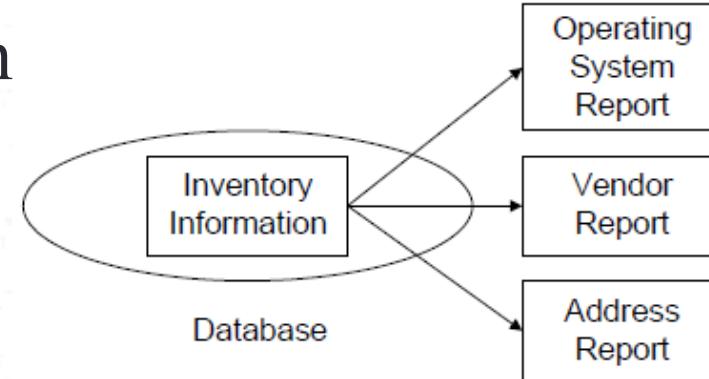
- Stores data efficiently.
 - Enables users to relate various types of information to one another.
 - Versioning.

- 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:

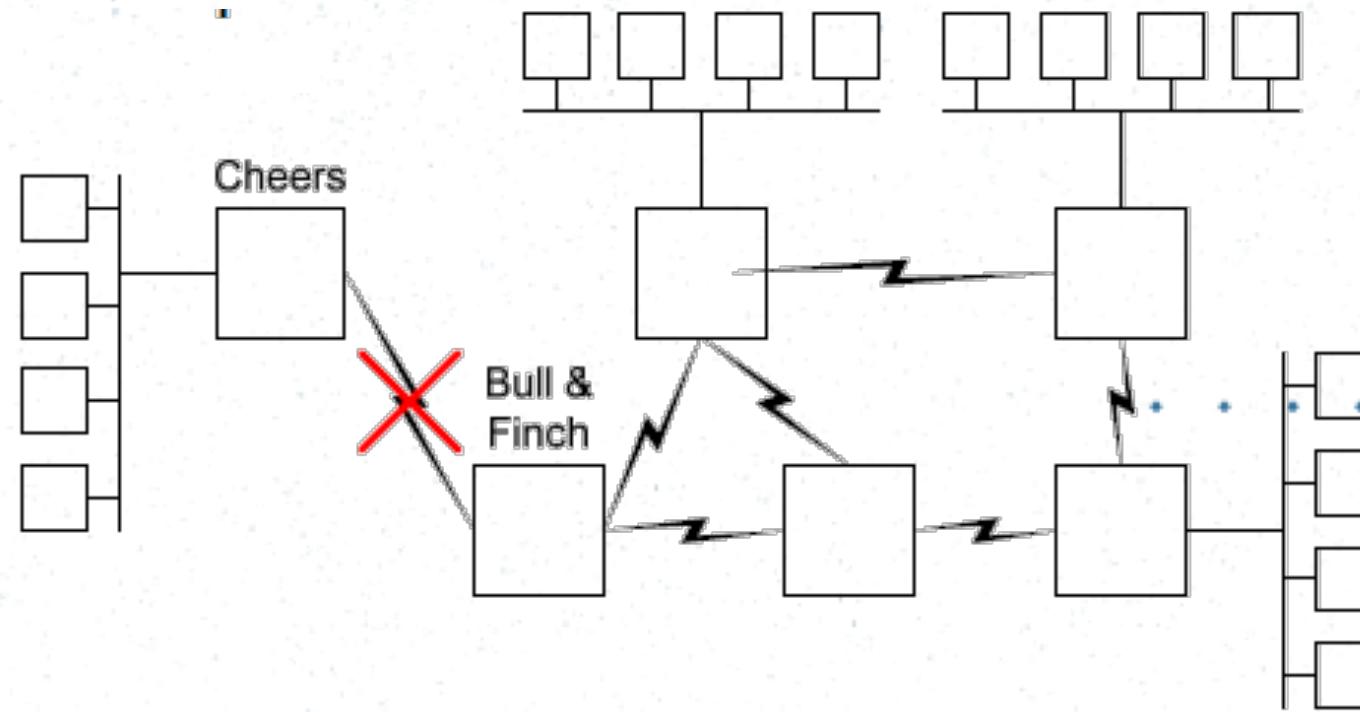
- ❑ Gathering data about the utilization of network resources.
 - Need to establish metrics -RFC 1272: “Internet Accounting Background”
 - E.g. Application layer – per-transaction, network layer – number of packets.
- ❑ Setting usage quotas using metrics.
- ❑ Billing users for their use of the network.

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

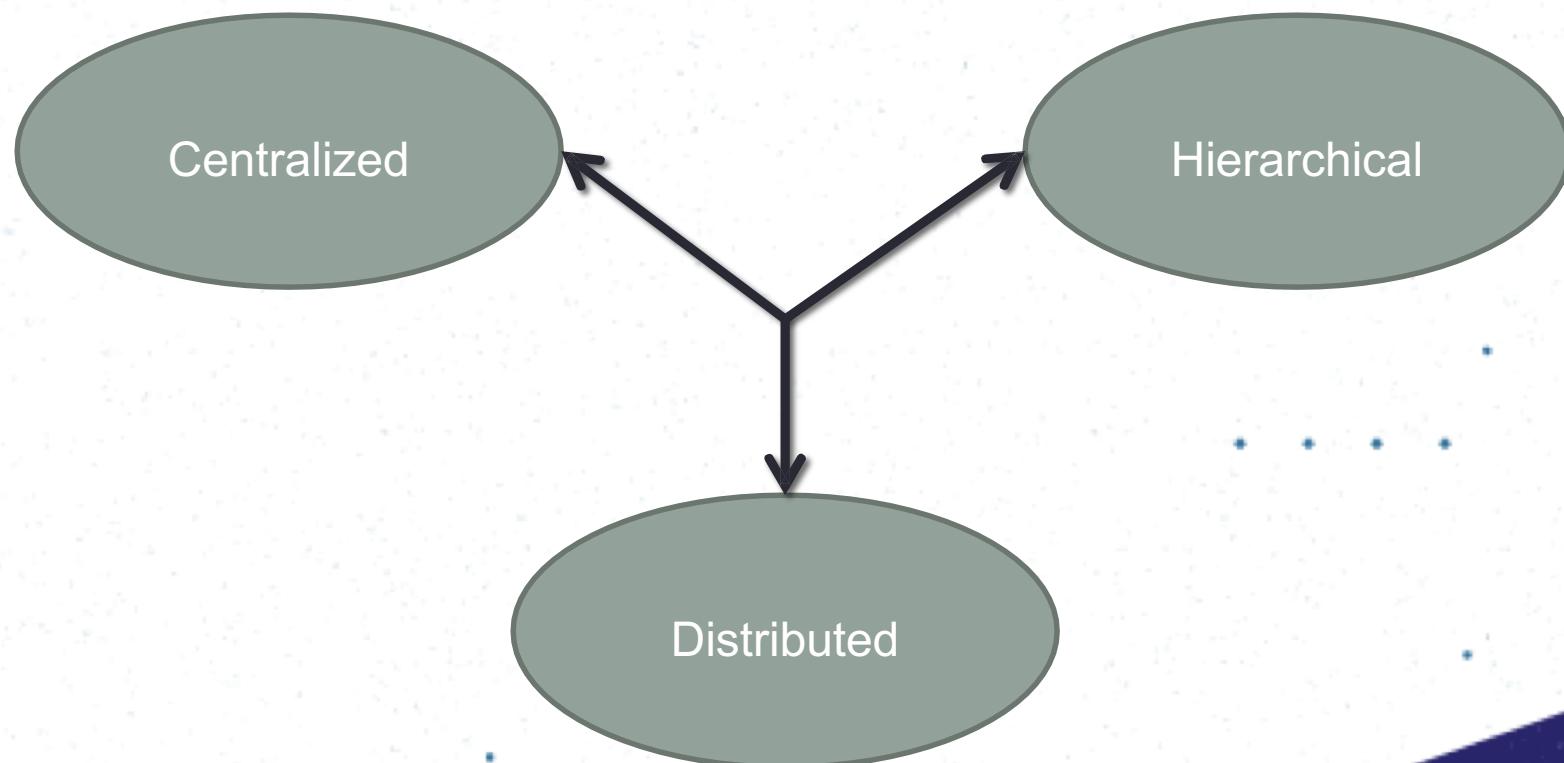
Network Management Systems

The **platform** should include the following functionality:

- A user interface
- A network map
- A **Database Management System (DBMS) / Management Information Base (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 Lokuliyan

Faculty of Computing
Department of CSE

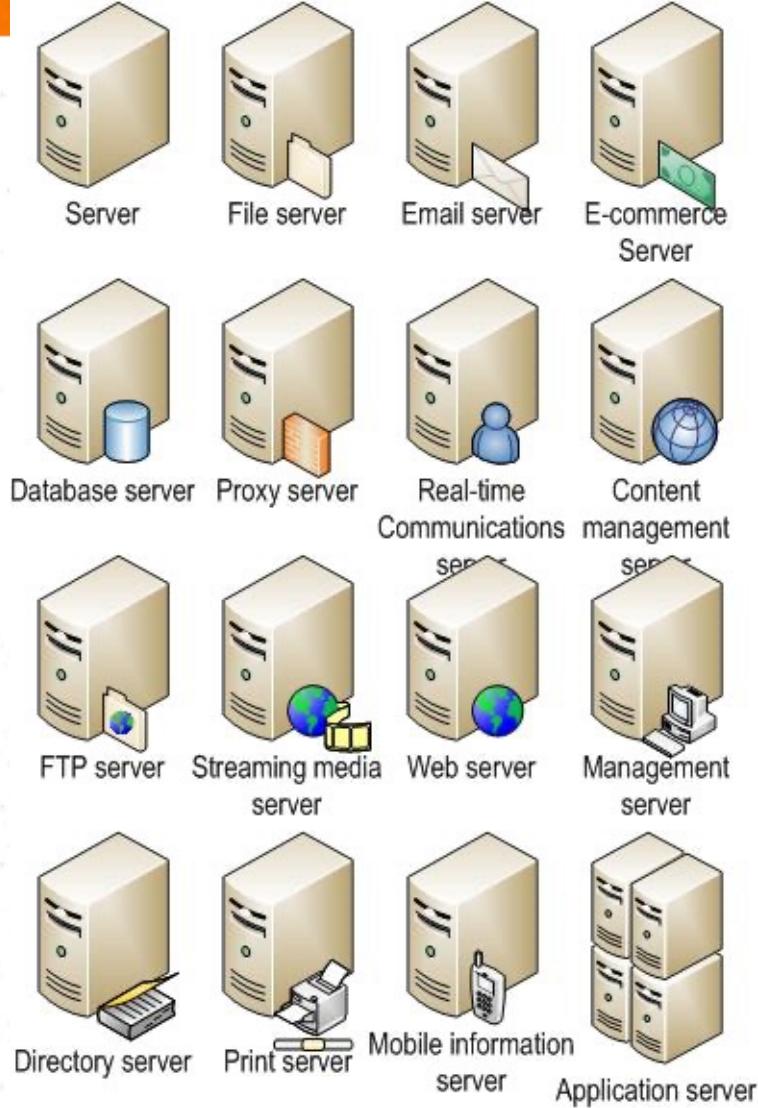


SLIIT

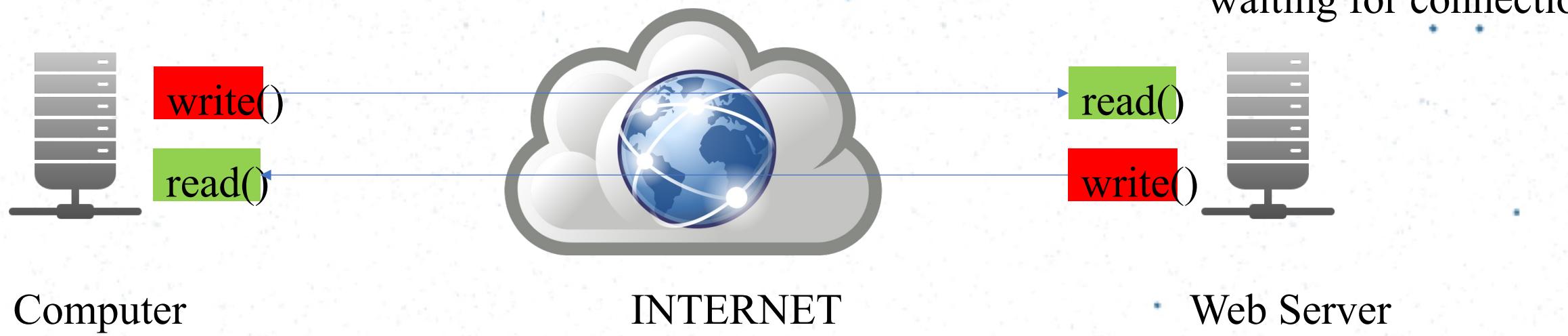
Discover Your Future

To be Covered...!!!

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



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 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)
 - A certain kinds of partial ordered sets
- The Domain Name System maintains the domain name hierarchy and provides translation services between it and the address spaces.

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

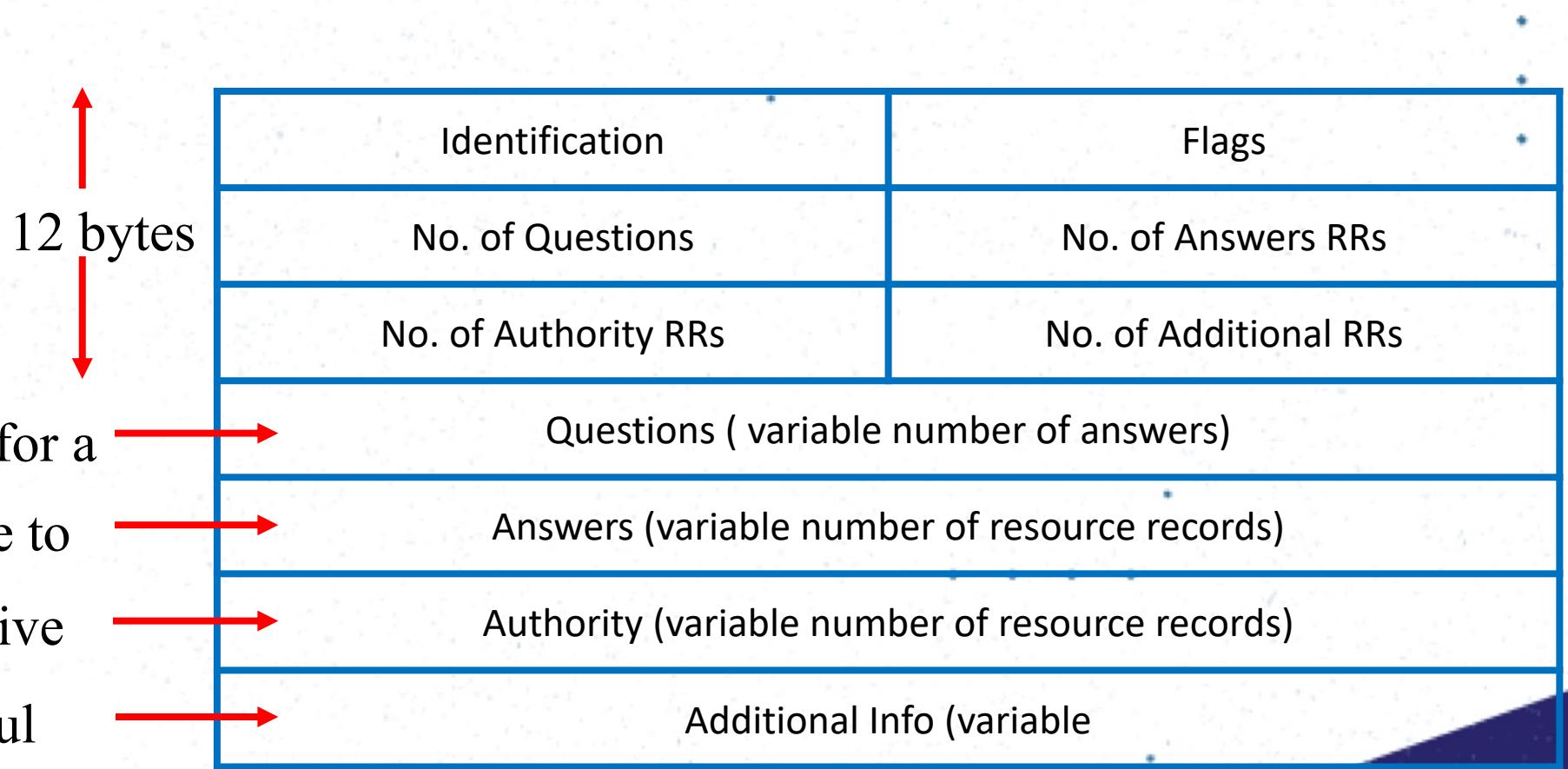
A ranked system

A unique name that identifies a website

(RFC-1034) - URL

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

hostname

Ip address

A

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

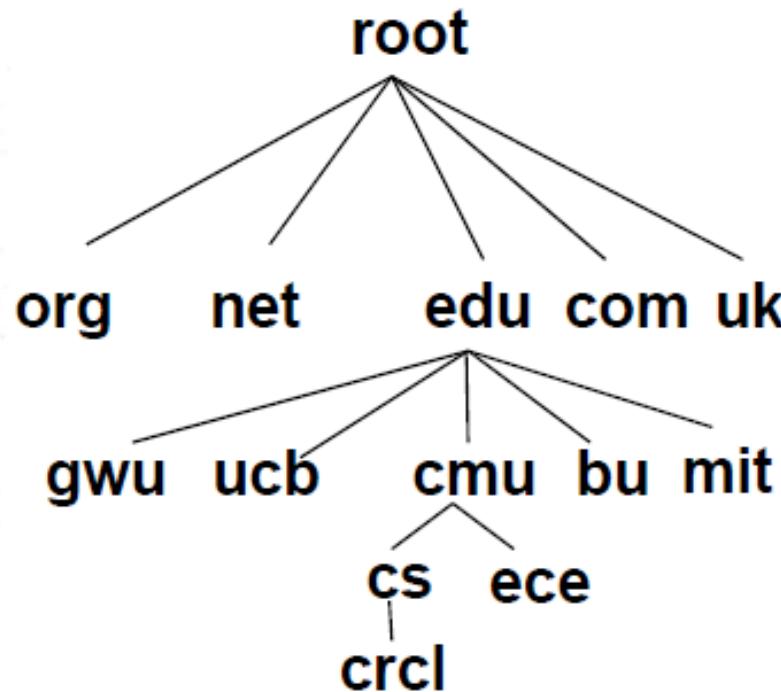
Type = MX

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

Properties of DNS Host Entries

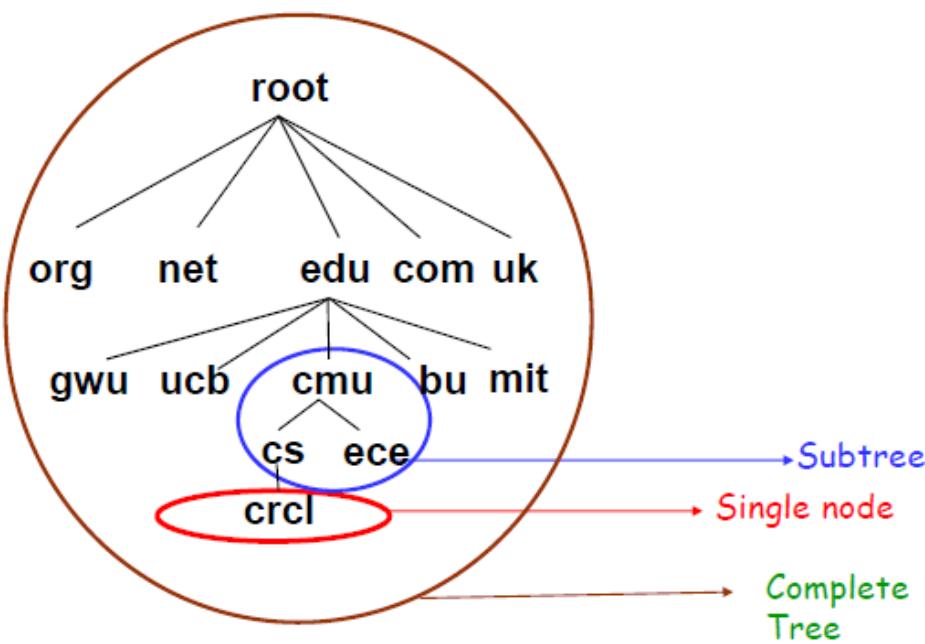
- Different kinds of mappings are possible:
 - ❖ 1-1 mapping between domain name and IP addr:
 - provolone.crcl.cs.cmu.edu maps to 128.2.218.81
 - ❖ Multiple domain names maps to the same IP addr:
 - www.scs.cmu.edu and www.cs.cmu.edu both map to 128.2.203.164
 - ❖ Single domain name maps to multiple 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



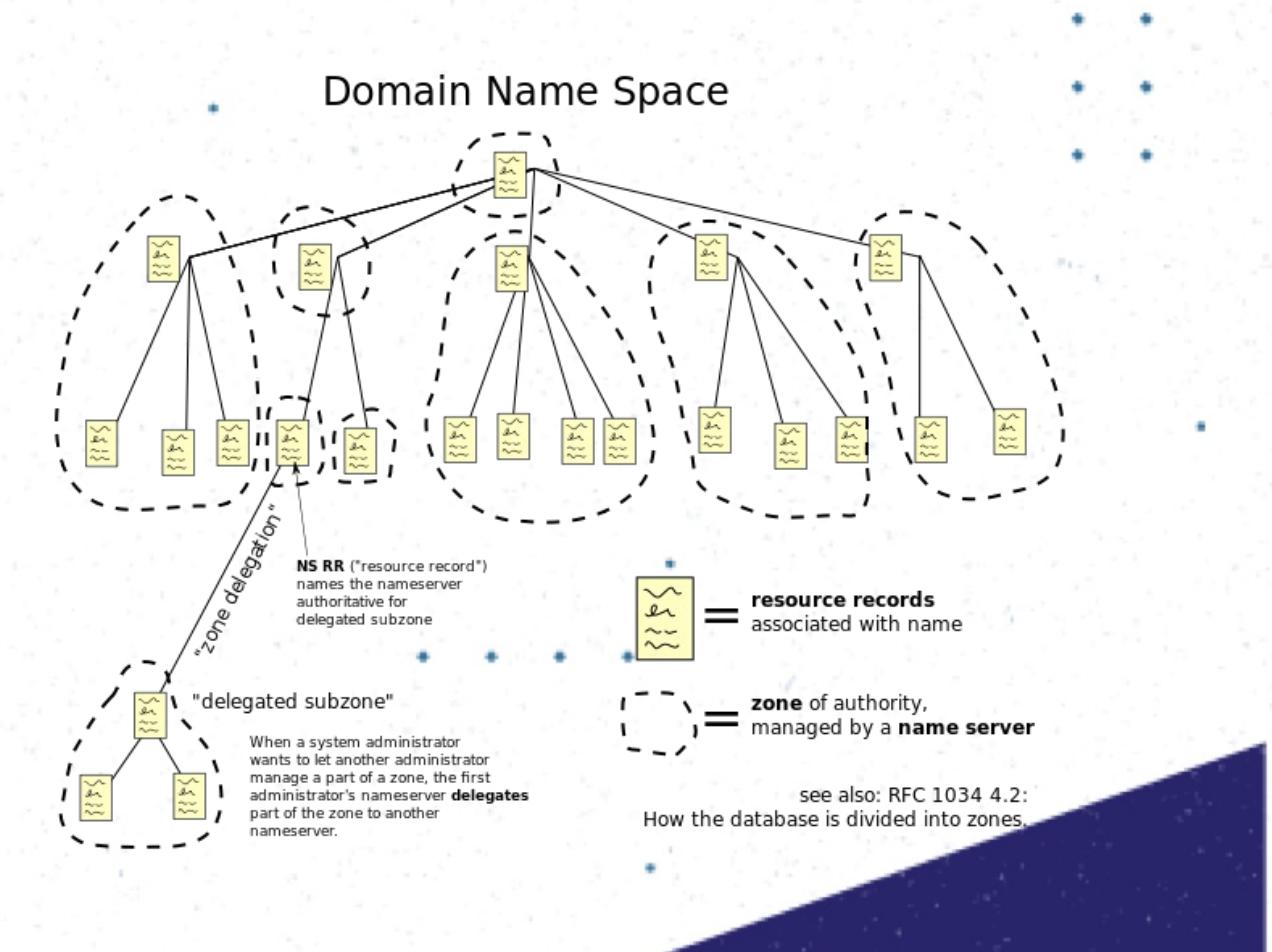
- Zone = contiguous section of name space
- E.g., Complete tree, single node or subtree
- A zone has an associated set of name servers
- Must store list of names and tree links

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?

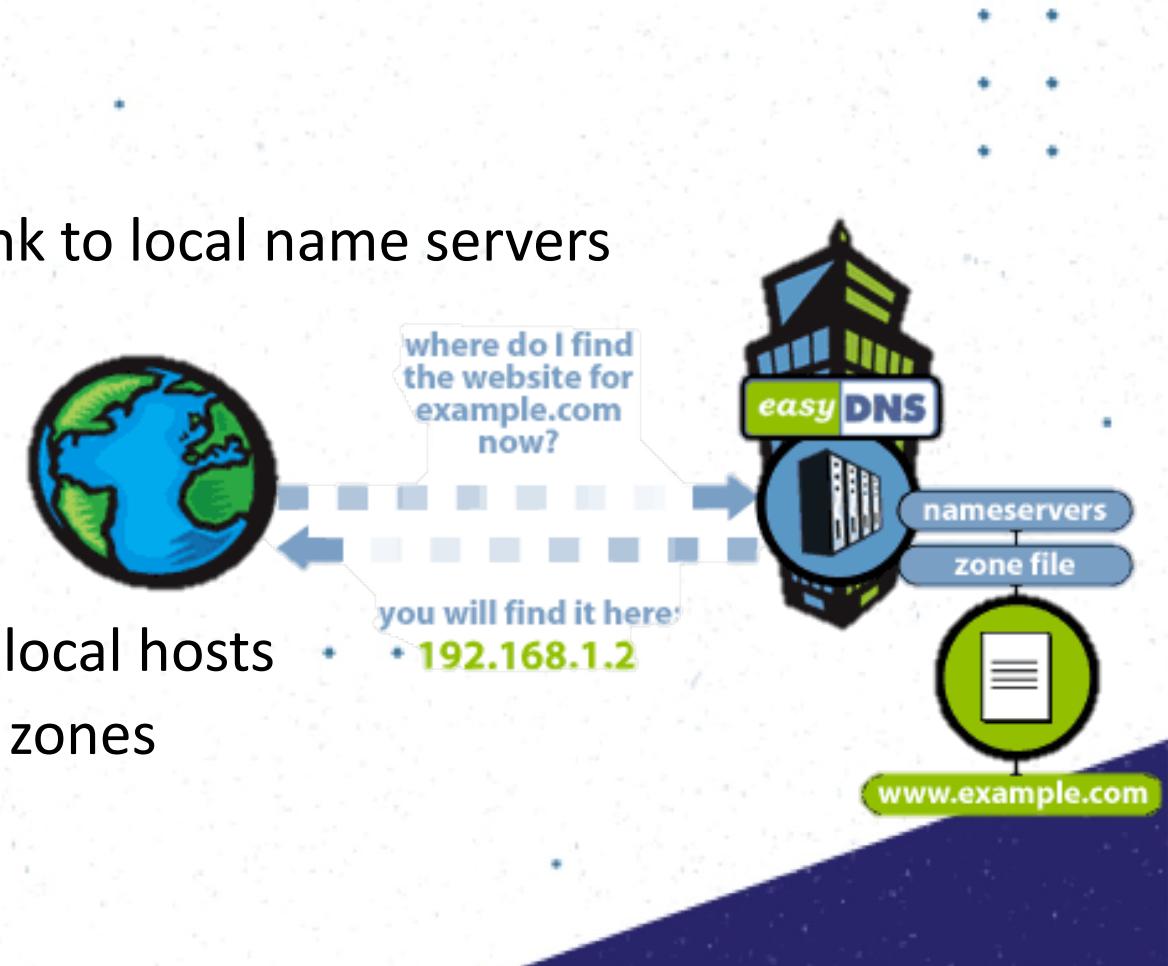
DNS: Root Name Servers

- ❖ 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*

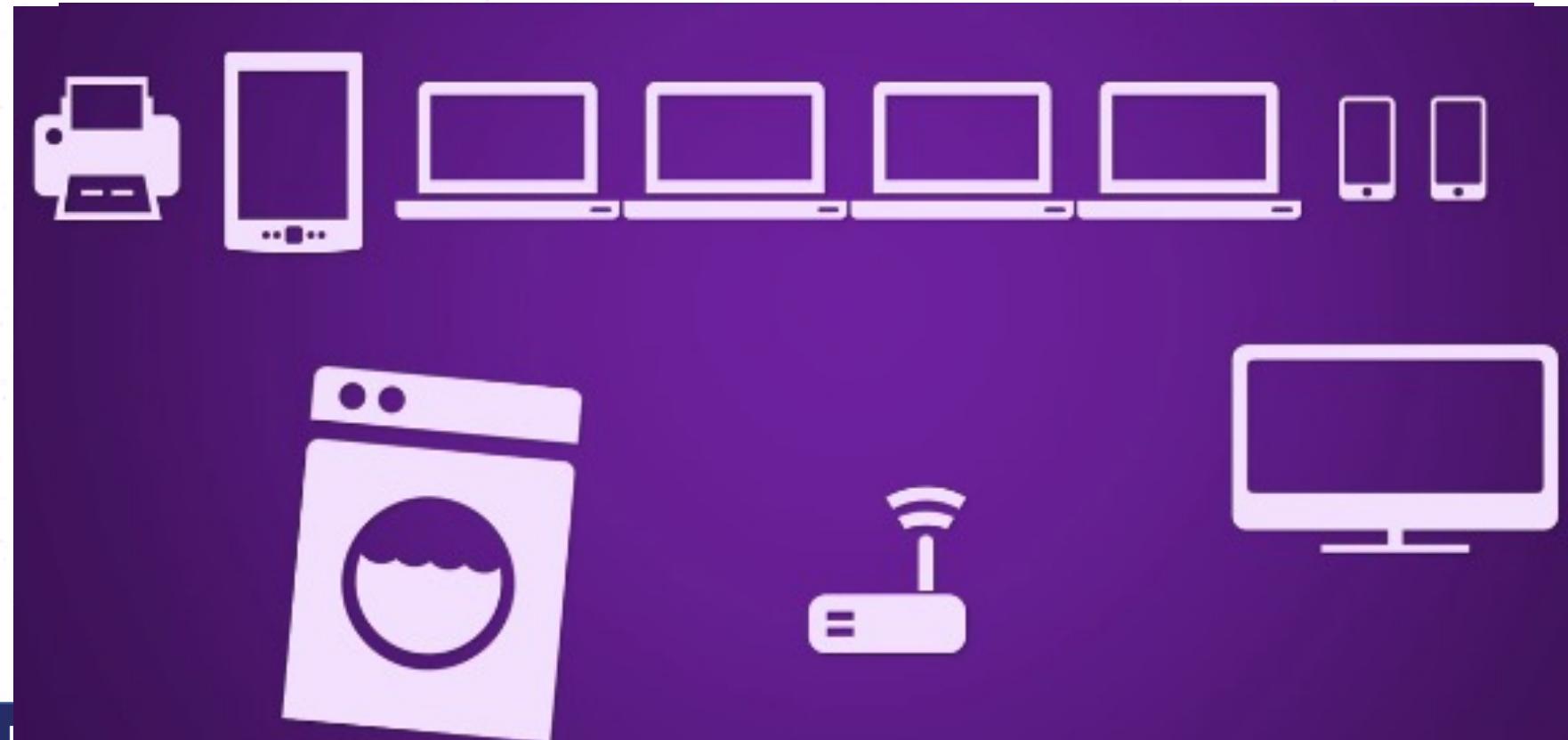
What a Device needs



- Most computers today need four pieces of information:
 - 1) IP address => to uniquely define itself in a 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??

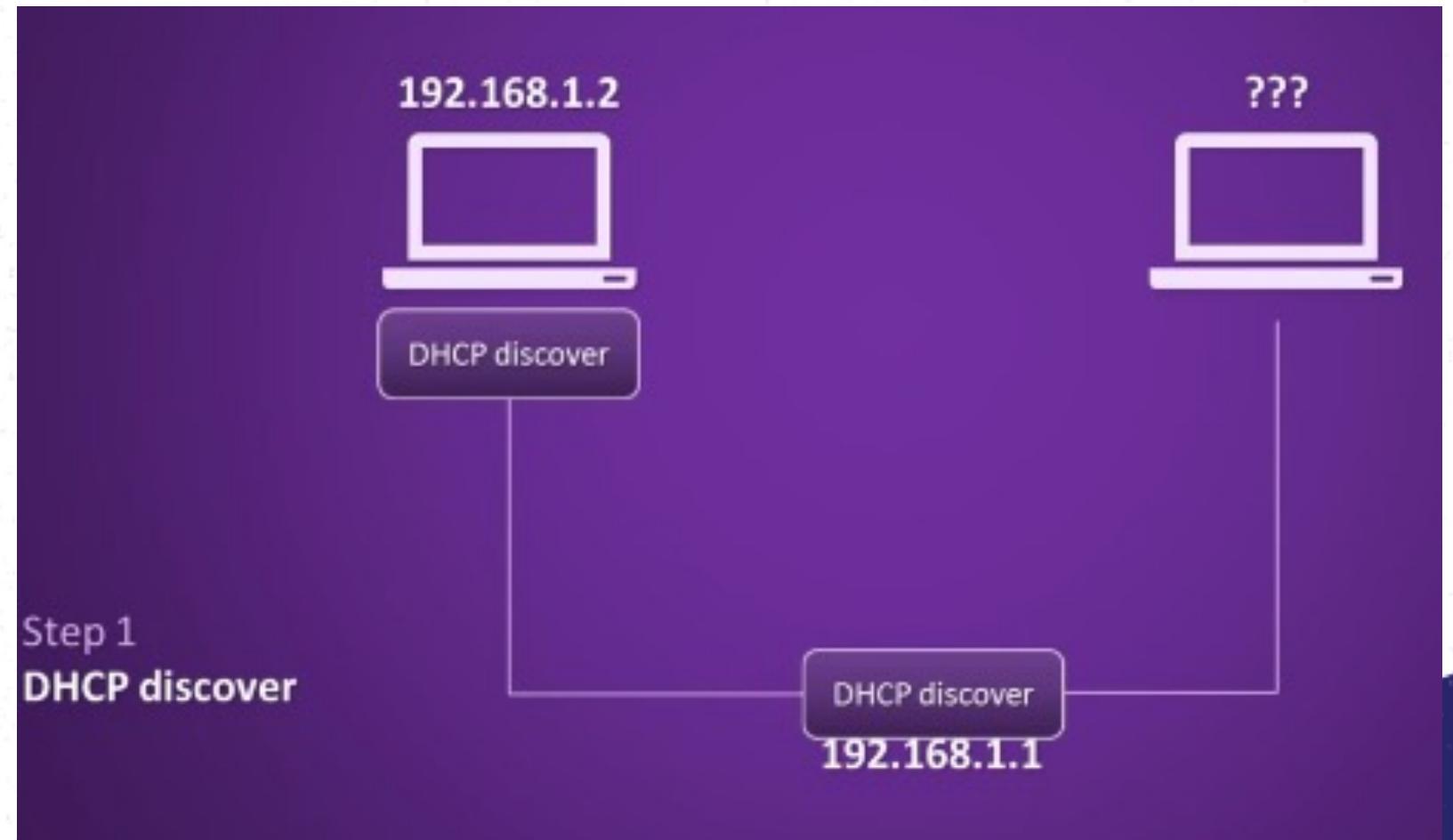


Assignment Conditions

- ❖ 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.



**DHCP Client UDP
port – 68**



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***
- ***DCHPREQUEST***
- ***DHCPACK***
- ***DHCPNAK***
- ***DHCPDECLINE***
- ***DHCPINFORM***
- ***DCHPRELEASE***

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 of 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.

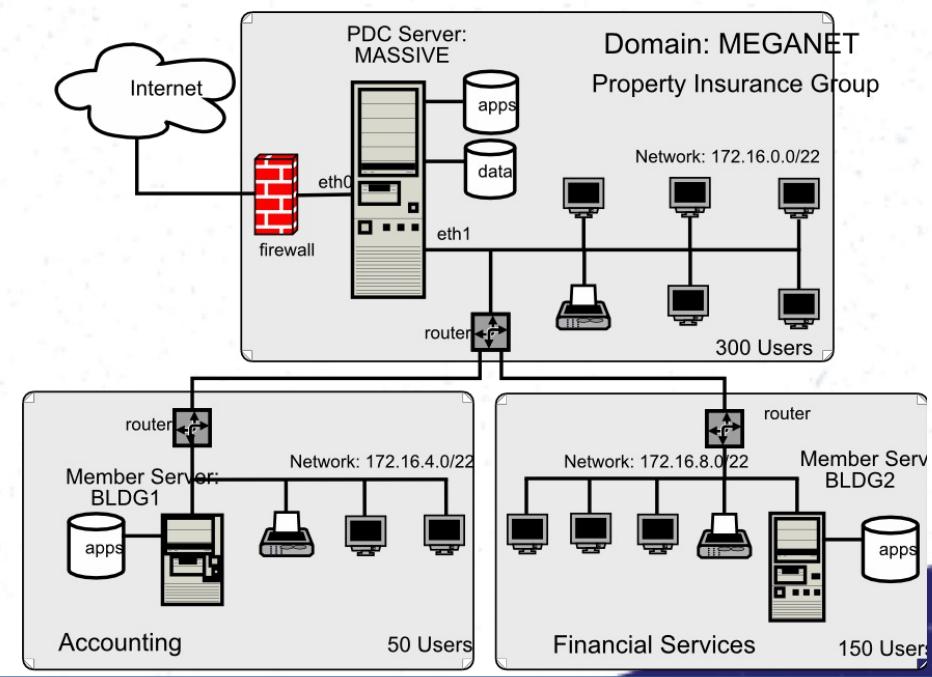
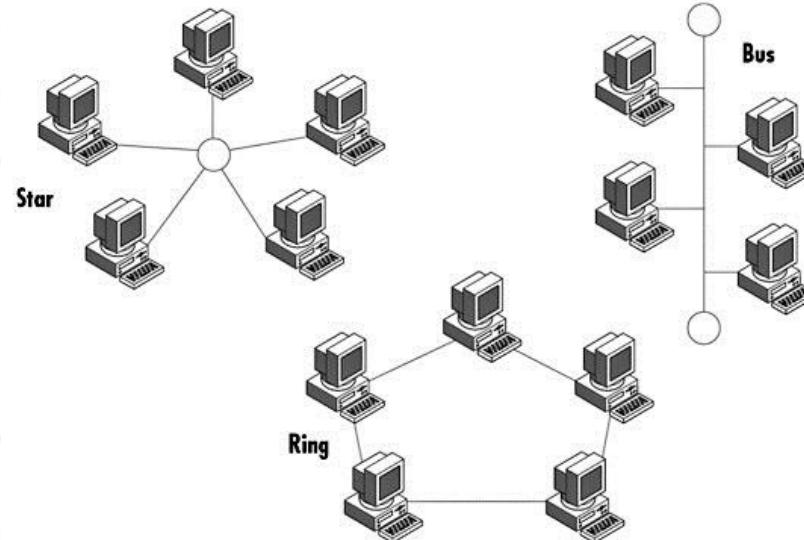
Key points:

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.

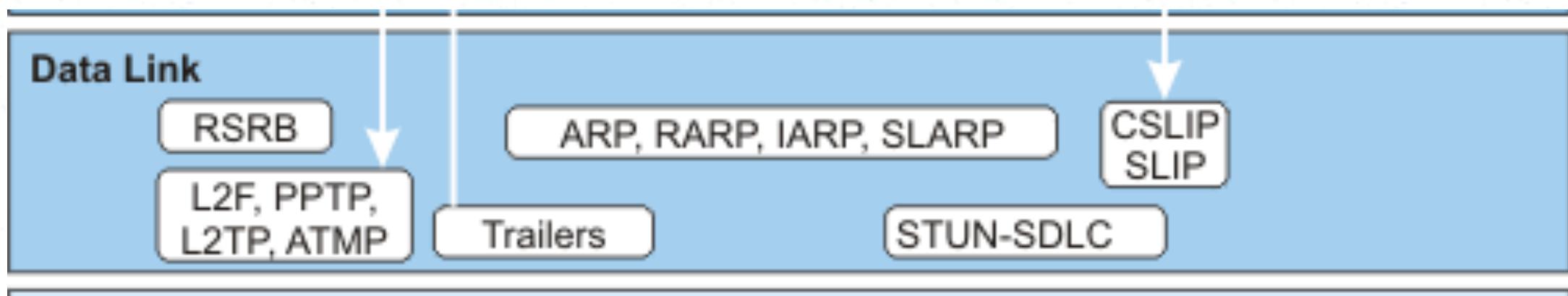
Key points:

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**.



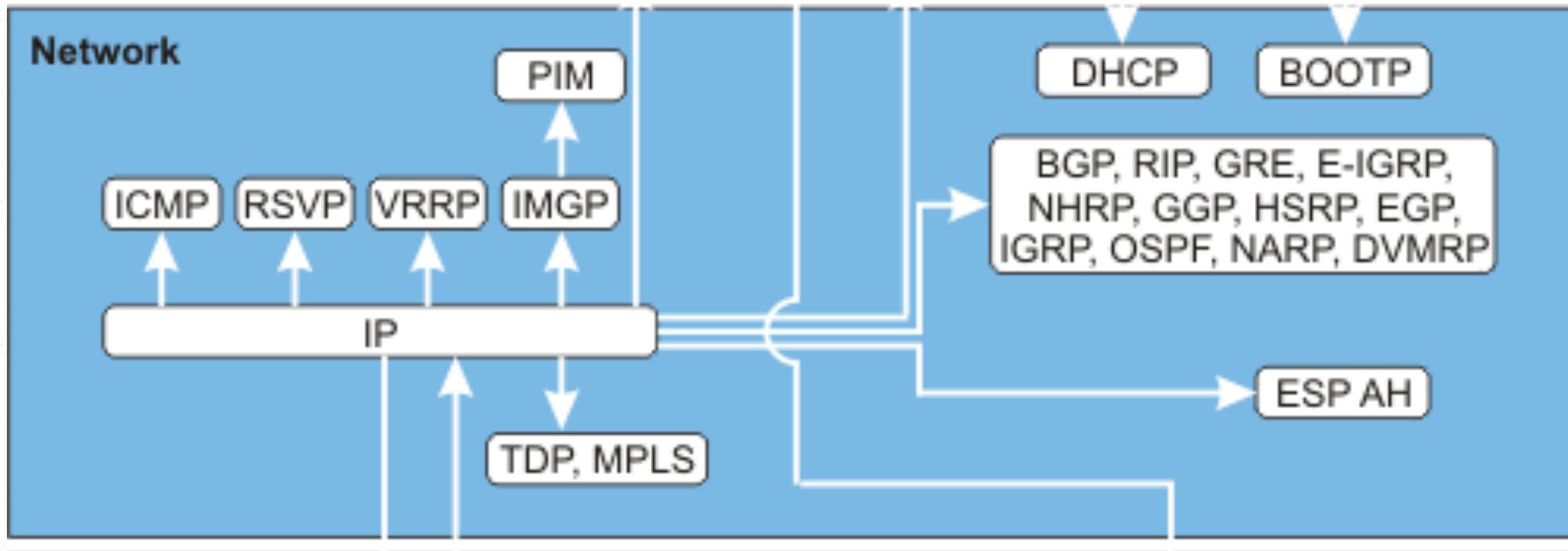
Network Layer

- 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



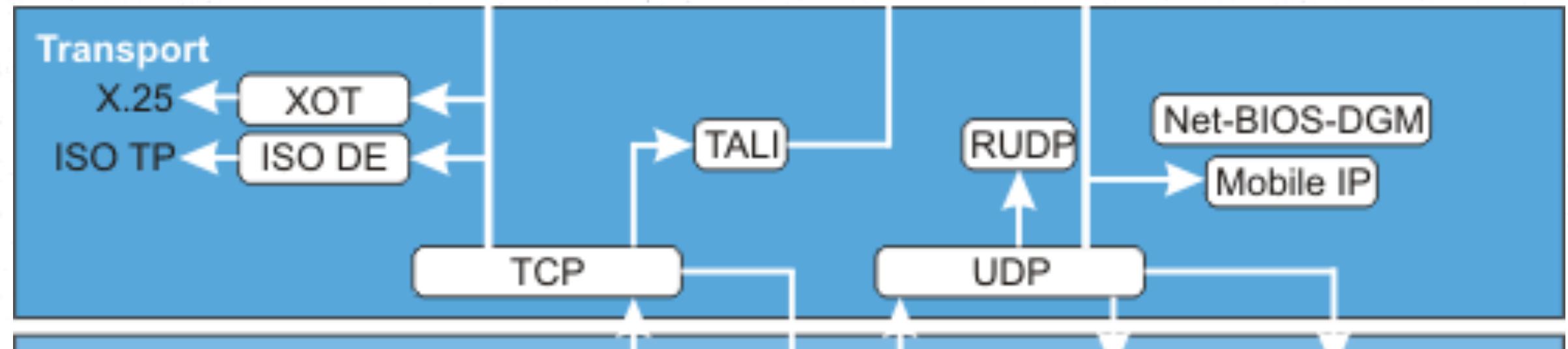
Transport Layer

- 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



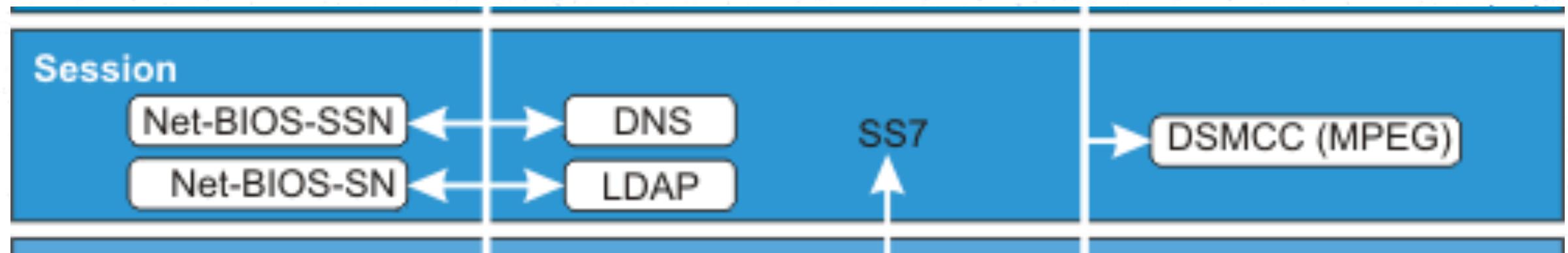
Session Layer

- 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.

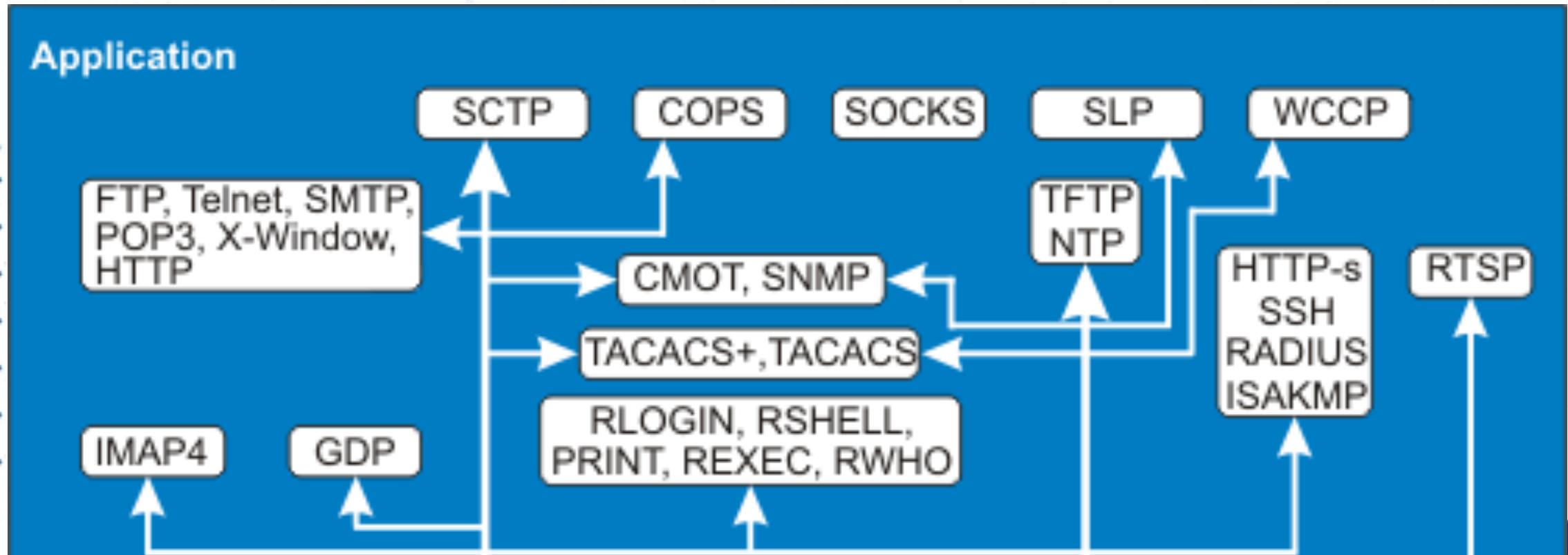
Application Layer

- 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 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

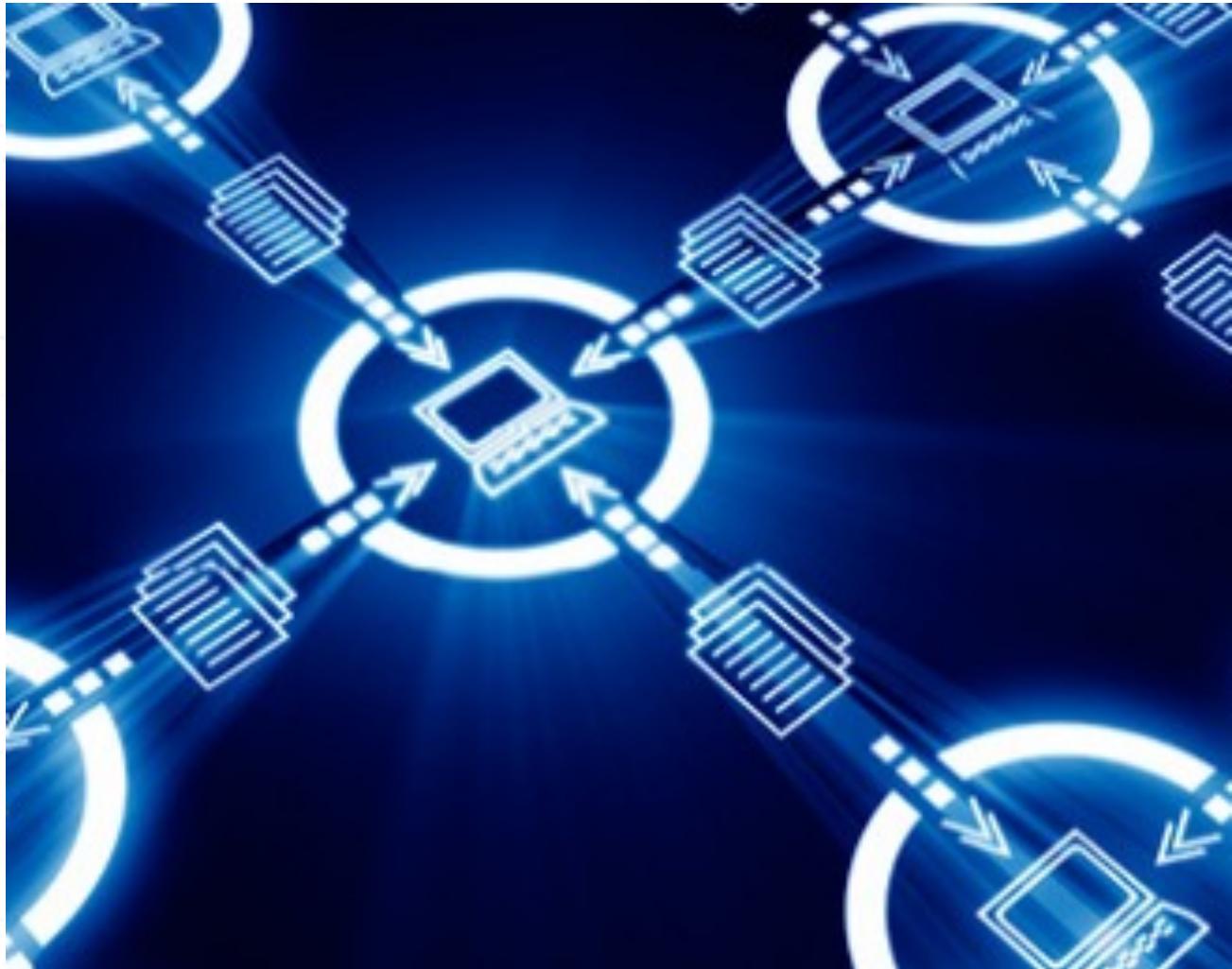
Care When Baselining

- 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?

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



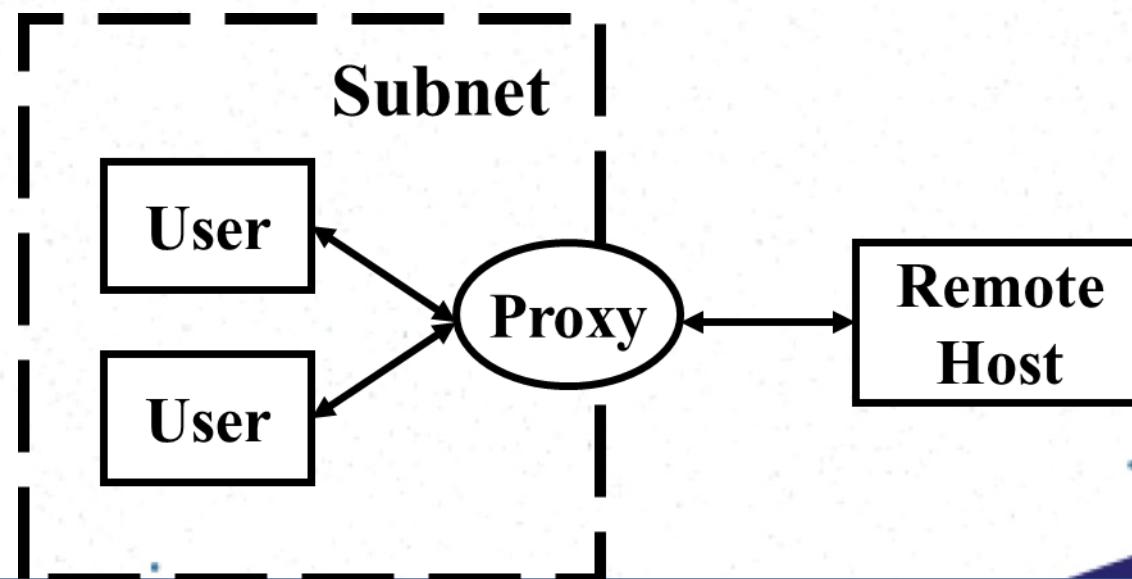
Proxy server



*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 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.

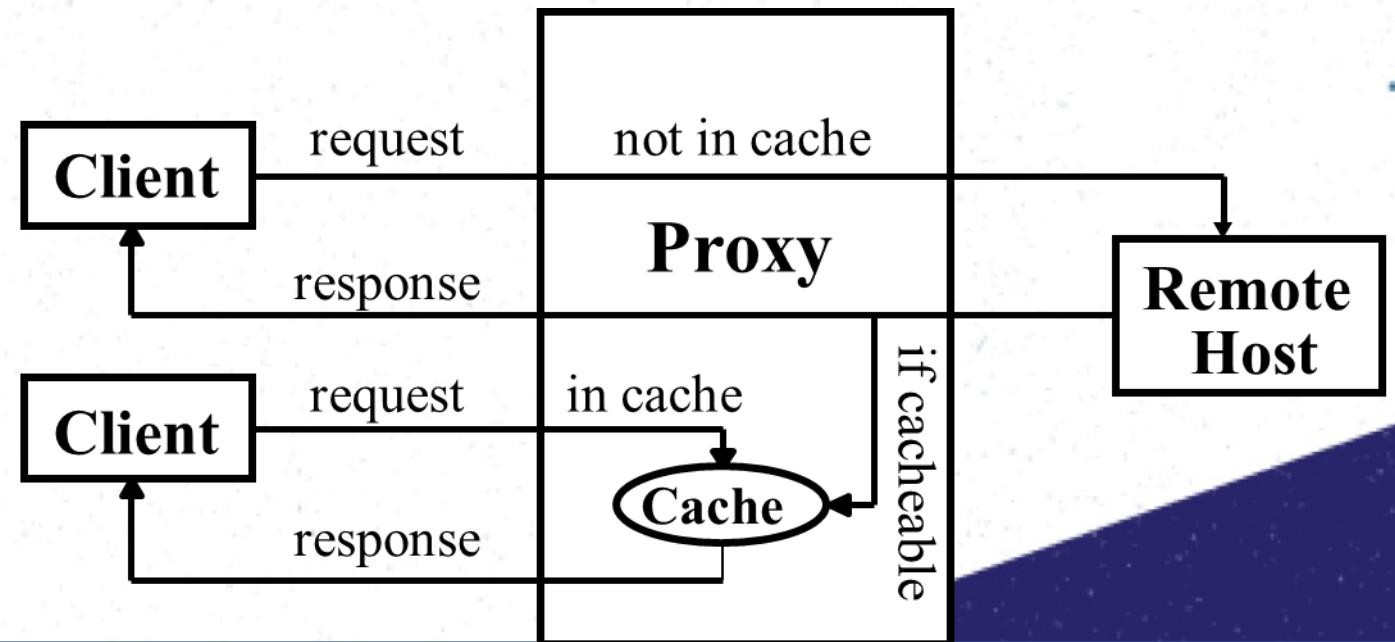
Types of proxy

- **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
- nginx
- GWS



Web cache

Squid
Polipo
Traffic server

Web server

Apache
Cherokee
Lighttpd
Nginx

CGI scripting

Perl
PHP
Python

Database

MariaDB
MySQL
Drizzle

Linux kernel

AppArmor
SELinux
Smack
TOMOYO

Process Scheduler

Netfilter

Linux network stack

Network scheduler

NIC
device
driver

kmod-fs-ext4
kmod-fs-btrfs
Lustre
...



Hardware

CPU
&
RAM

Networking
hardware

Storage

SATA
SAS
RAID
iSCSI
NAS

Environment: CCC

Crackers

Botnets for DDoS-attacks
cracking attempts

Competitors

compete for customers

Internet

Attacks
stave off
&
Requests
serve

Responses
low latency

Customers

want attendance

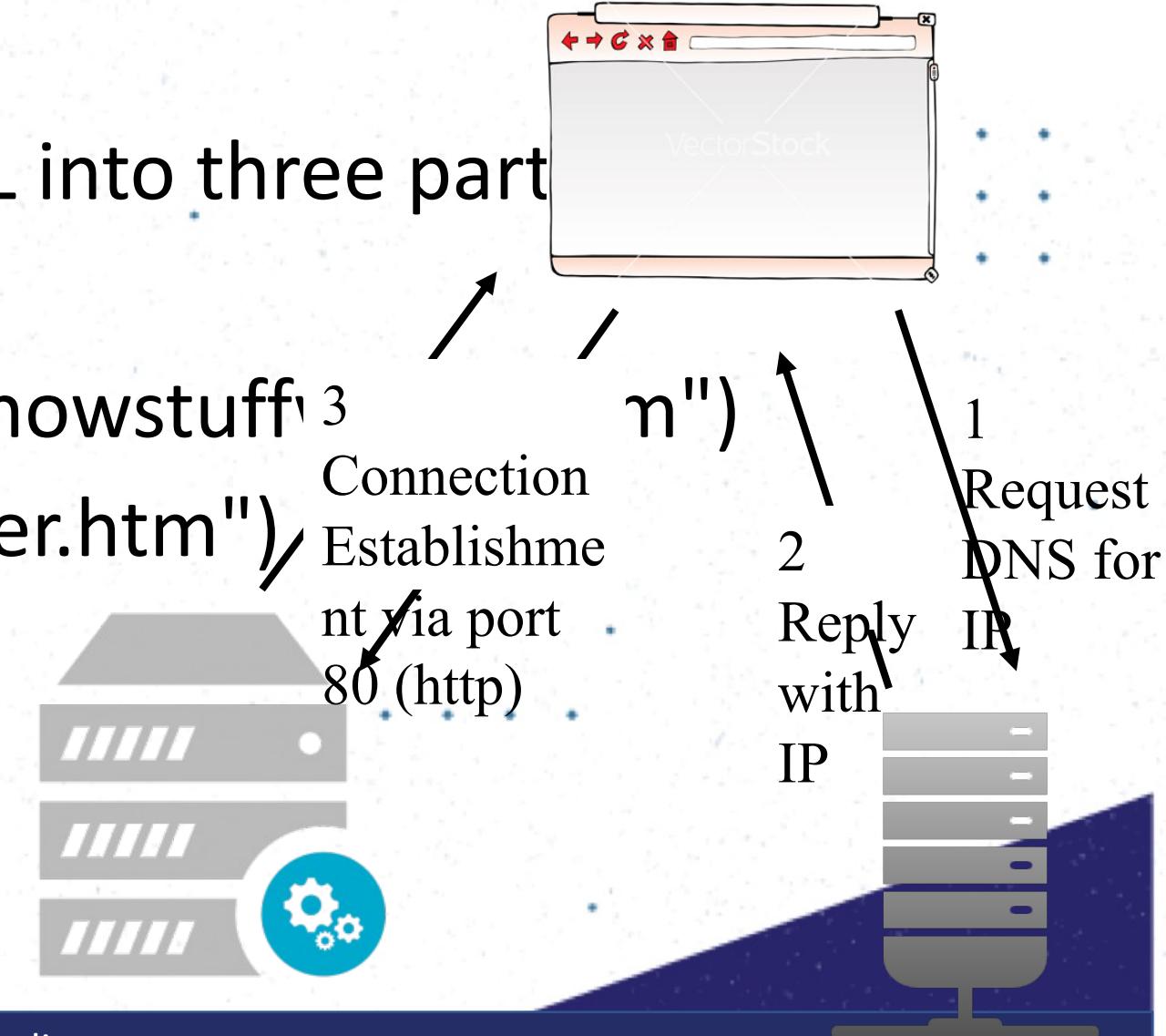
Botnets

DDoS-Attacks

- 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.howstuff")
 - 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.

Mail server



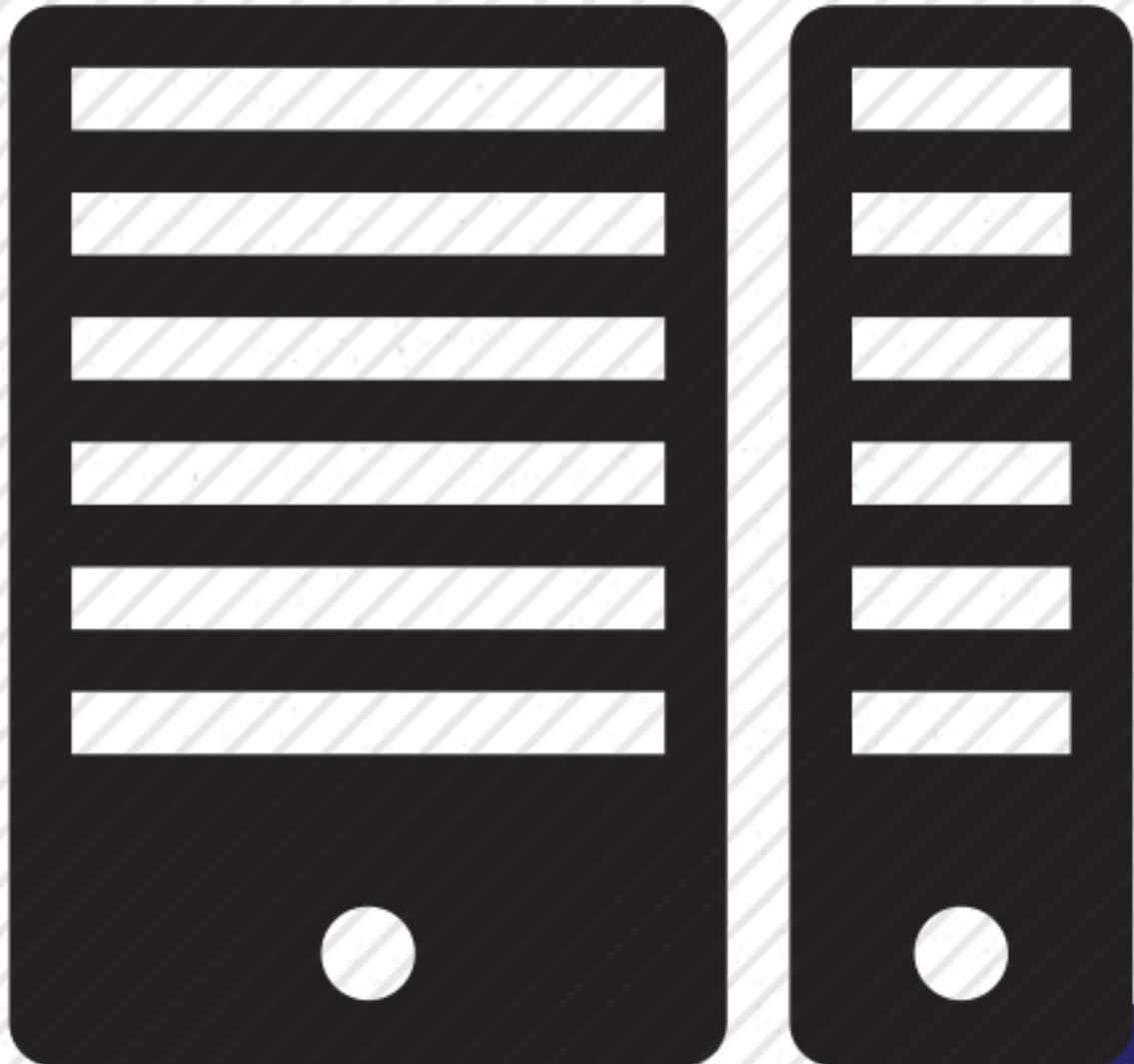
- ❖ Simple Mail Transfer Protocol (SMTP) is used to transfer mail between Mail Servers over Internet
- ❖ Post Office Protocol (PoP) and Interactive Mail Access Protocol (IMAP) is used between Client and Mail Server to retrieve mails
- ❖ The mail server of a domain is identified by the MX record of that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



IT3010

Network Design and Management

Lecture 03

Network Monitoring

Shashika Lokuliyan

Faculty of Computing
Department of CSE

Network Design and Management

Network Monitoring
Lecture 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.



Monitoring an active communications network in order to diagnose problems and gather statistics for administration and fine tuning.

monitor real time
gather statistics
fault diagnosis
alert



What is Network Monitoring??

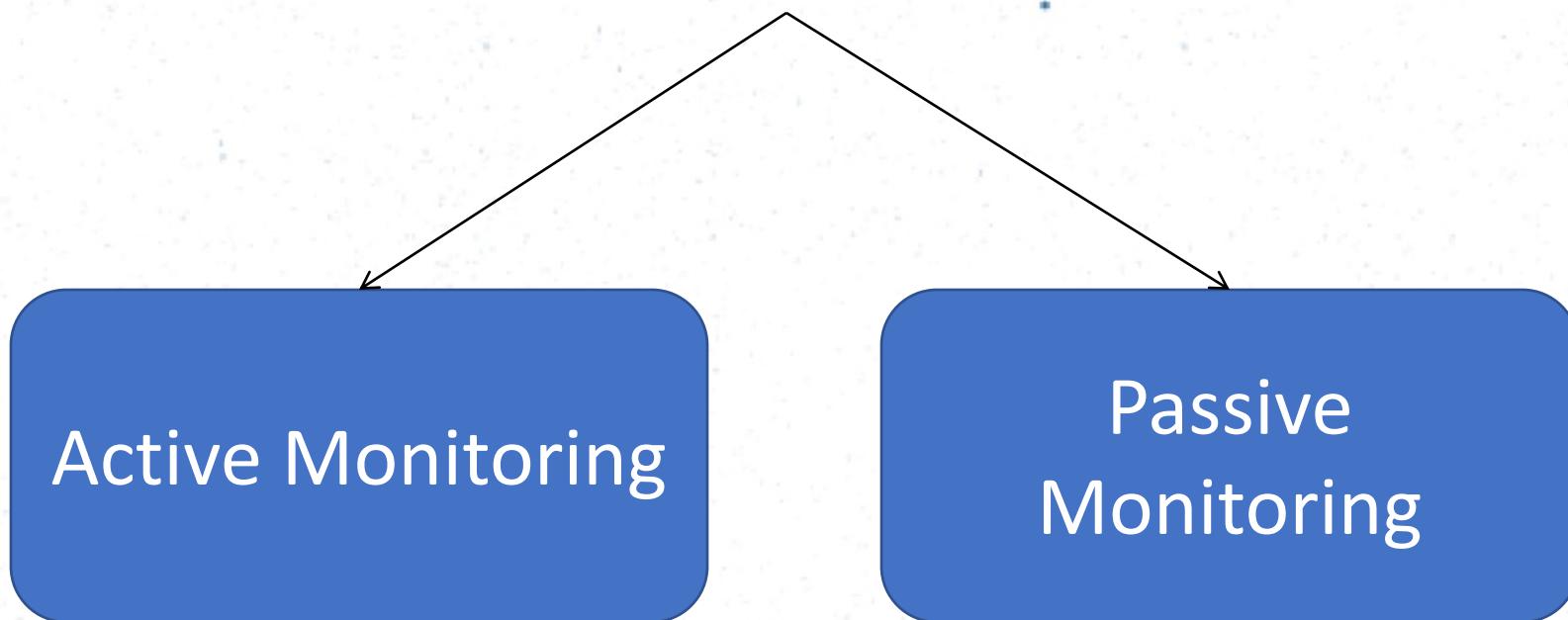
- Write it in your terms.



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

Types of Network Monitoring

Two types of Network Monitoring



Active Monitoring

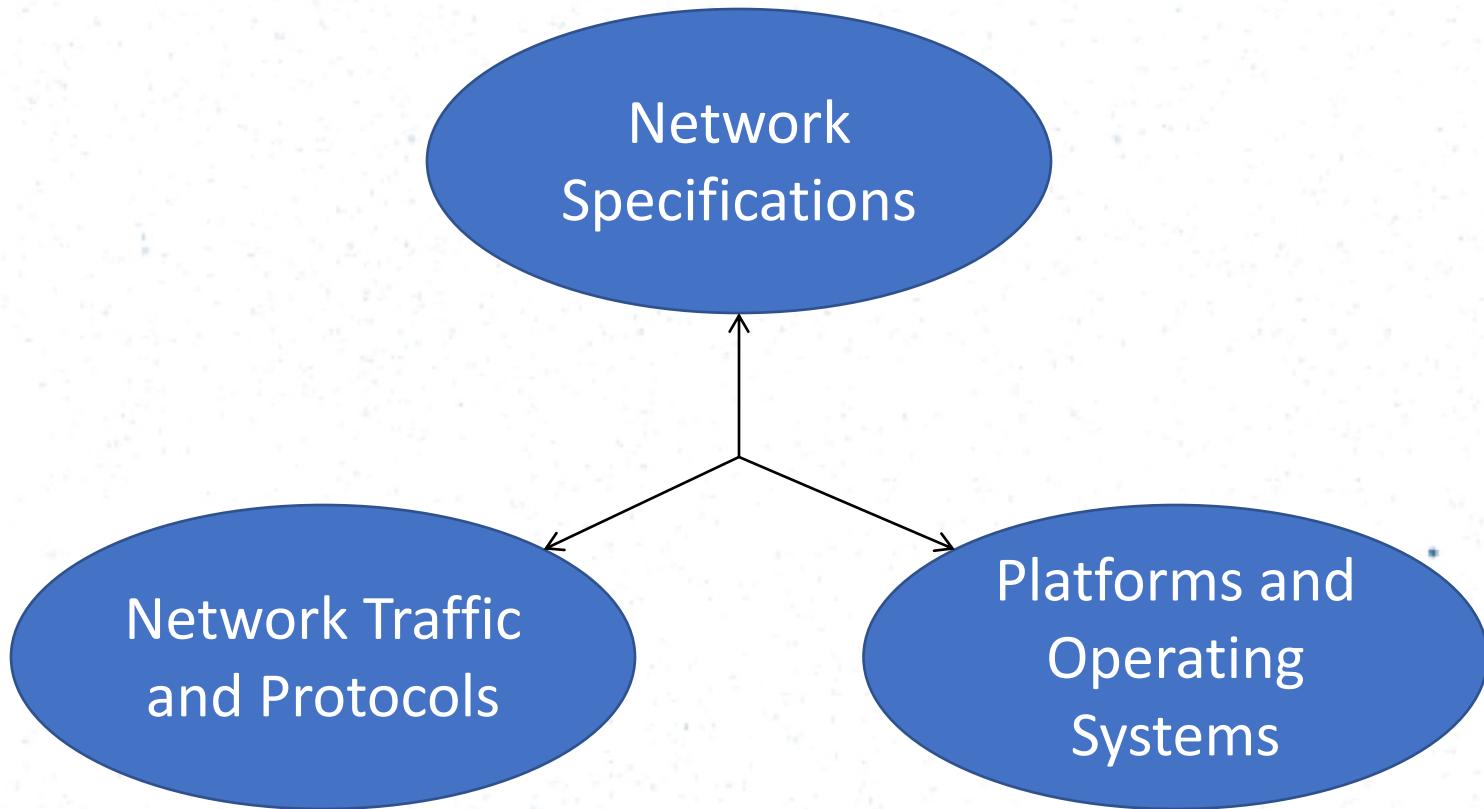
Passive Monitoring

performed by sending test traffic into network

carried out by observing network traffic

Monitoring Categories

Things we will need to monitor...



Monitoring and analysis of Network Specifications

Ethernet

IEEE 802.3

Establishing an Ethernet Baseline

Things to monitor with respect to Ethernet..

- Network utilization
 - ... broadcast
 - ... multicast
- 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 => **Partition network**

Expectation => Should achieve 15% to 25%

Peak Utilization

at a specific moment in time

Peak utilization means that,

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

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

Average Utilization

Average utilization means that **over some period of time**

.....(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

can occur based on

- Collisions / runts -> late collision
- Short frames
- Bad FCS
- Long frames
- Ghosts

Collisions

```
sets output, 436549843 bytes  
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

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,

collisions
Faulty NIC or software
Topology errors

Bad FCS (Frame Check Sequence)

500 broadcast
s, 3 CRC, 0
ackets with

- 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

- 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

faculty NIC
cabling
noise
software

```
es, 0 no buffer
, 0 giants
errun. 0 ignored
```

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,
 - earth loops
 - wiring
 - electrical interference

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**.

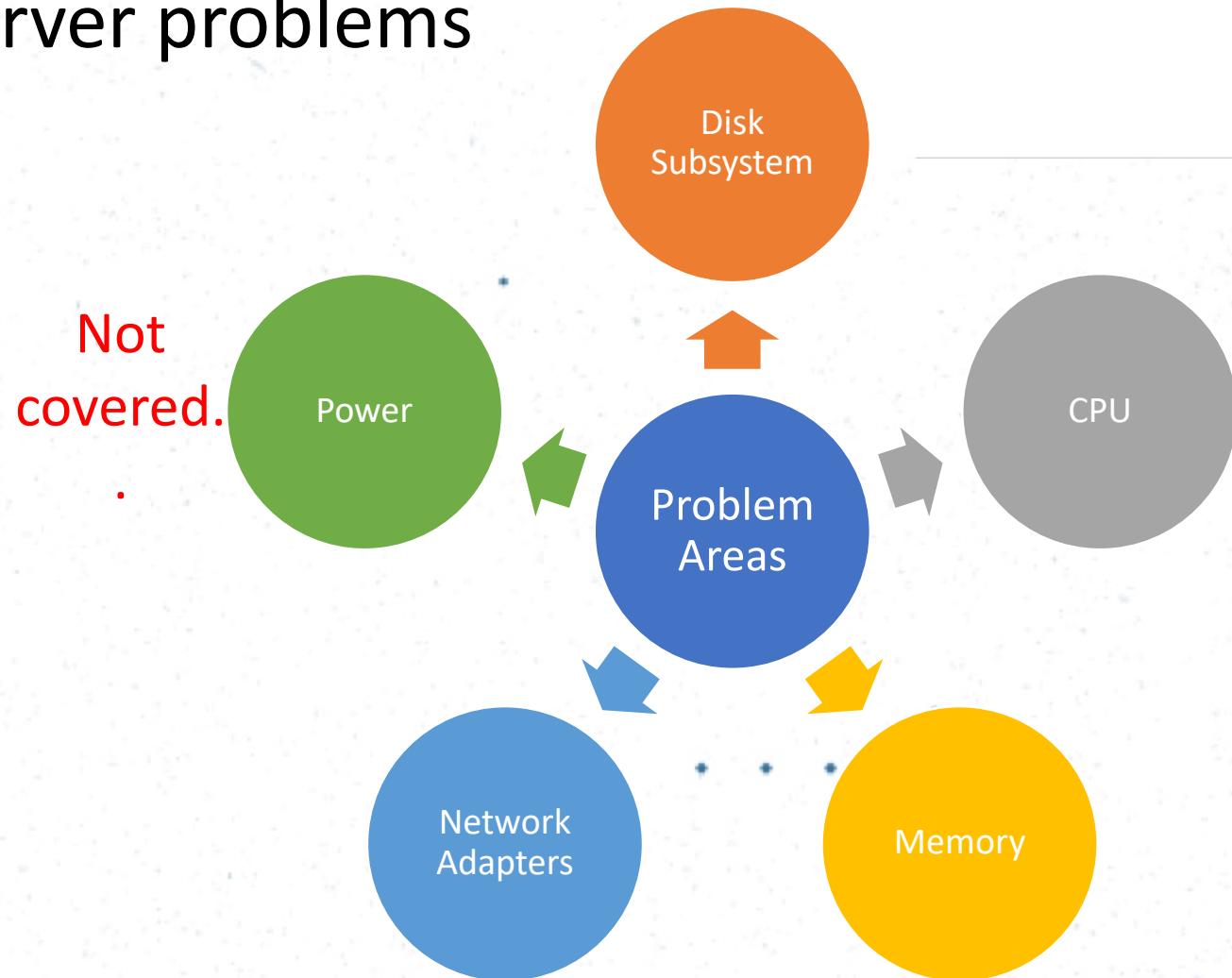
Determining Server Workload Characterization

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..



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 ~



IT3010

Network Design and Management

Lecture 04

Introduction to SNMP

Shashika Lokuliyan

Faculty of Computing
Department of CSE



SLIIT

Discover Your Future

SNMP

Simple Network Management Protocol

Network management

- In computer networks, network management refers to the **activities, methods, procedures, and tools** that pertain to the operation, administration, maintenance, and provisioning of **networked systems**. Network management is essential to **command** and **control** practices and is generally carried out of a network operations center.



network management

1. *Operation* deals with keeping the network (and the services that the network provides) up and running smoothly.
2. *Administration* deals with keeping track of resources in the network and how they are assigned.
3. *Maintenance* is concerned with performing repairs and upgrades.
4. *Provisioning* is concerned with configuring resources in the network to support a given service.

network management

- Data for network management is collected through several mechanisms.
 - *Agents* installed on infrastructure
 - Synthetic monitoring that simulates transactions
 - Logs of activity
 - Sniffers
 - Real user monitoring

In the past network management mainly consisted of monitoring whether devices were up or down; today performance management has become a crucial part of the IT team's role which brings about a host of challenges—especially for global organizations.

Need For Network Management Tools

- In the early days of the Arpanet, the predecessor of the Internet, the name service was accomplished by maintaining and distributing one file with all the IP addresses of the network. But no more ... DNS etc
- As networks increase in size
 1. The network becomes more indispensable to the organization.
 2. More things can go wrong, disabling or degrading the performance of portions of the network.
- Today a large network cannot be managed with software assistance.

SNMP & Network Management History

- **1983** - TCP/IP replaces ARPANET at U.S. Dept. of Defense, effective birth of Internet
- First model for net management - **HEMS** - High-Level Entity Management System (*RFCs 1021, 1022, 1024, 1076*)
- **1987** - ISO OSI proposes **CMIP** - Common Management Information Protocol, and **CMOT** (CMIP over TCP) for the actual network management protocol for use on the internet
- **Nov. 1987** - **SGMP** - Simple Gateway Monitoring protocol (*RFC 1028*)
- **1989** - Marshall T. Rose heads up **SNMP** working group to create a common network management framework to be used by both **SGMP** and **CMOT** to allow for transition to **CMOT**

SNMP & Network Management History

- Aug. 1989 - “Internet-standard Network Management Framework” defined (RFCs 1065, 1066, 1067)
- Apr. 1989 - **SNMP** promoted to **recommended** status as the de facto TCP/IP network management framework (RFC 1098)
- June 1989 - IAB committee decides to let **SNMP** and **CMOT** develop separately
- May 1990 - IAB promotes **SNMP** to a **standard protocol with a recommended status** (RFC 1157)
- Mar. 1991 - format of MIBs and traps defined (RFCs 1212, 1215)
- TCP/IP MIB definition revised to create **SNMPv1** (RFC 1213)

Technologies

- Main reason for having a standardized protocol was that without one in a heterogeneous environment, the network engineer would be spending too much time developing customized management tools instead of managing the network.
- A small number of accessory methods exist to support network and network device management. Access methods include,
 - SNMP
 - command-line interface
 - custom XML
 - CMIP
 - Windows Management Instrumentation (WMI)
 - Transaction Language 1
 - CORBA
 - NETCONF
 - Java Management Extensions (JMX)

Use of Standardized Protocol

- Goals:
 - Minimize complexity of management functions.
 - Flexible, extensible.
 - Independent of the architecture and mechanisms of particular hosts and gateways.
- • • •

SNMP – Simple Network Management Protocol

- "Internet-standard protocol for managing devices on IP networks"
- SNMP is a tool (protocol) that allows for remote and local management of items on the network including servers, workstations, routers, switches and other managed devices. It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

Key components

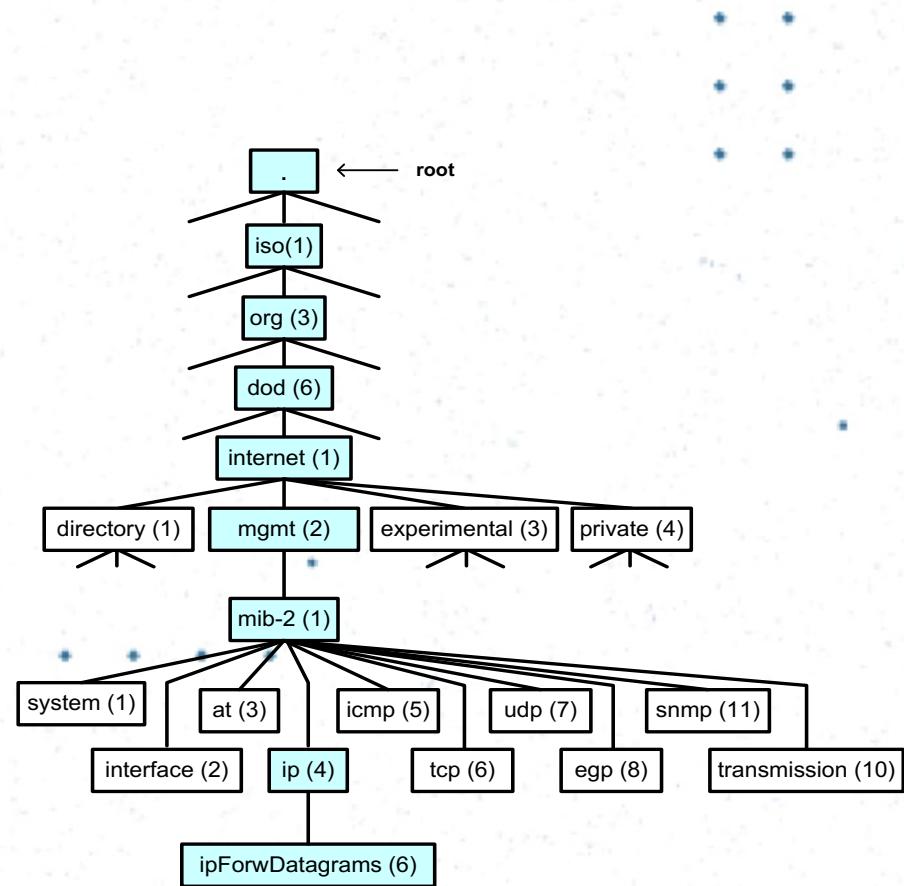
- ❖ **Manager** — an application program that contacts an SNMP agent to query or modify the database at the agent.
- ❖ **Agent** — software that runs on a piece of network equipment (host, router, printer, or others) and that maintains information about its configuration and current state in a database.
- ❖ **Network management station (NMS)** — executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs may exist on any managed network.
- ❖ **Management Information Bases (MIBs)** — describes the information in the database.
- ❖ **SNMP Protocol** — application layer protocol used by SNMP agents and managers to send and receive data.

Network management station (NMS)

- The one that executes network management applications (NMAs) that monitor and control network elements (NE) such as hosts, gateways and terminal servers.
- These network elements use a management agent (MA) to perform the network management functions requested by the network management stations.

Management information base (MIB)

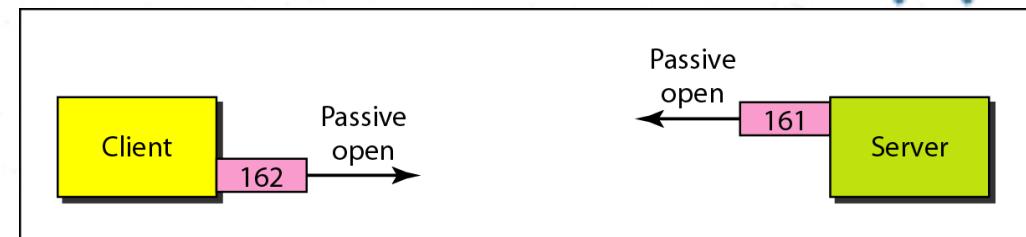
- MIBs describe the structure of the management data of a device subsystem; they use a **hierarchical namespace containing object identifiers (OID)**.
- Each OID identifies a variable that can be read or set via SNMP.
- MIBs use the notation defined by Structure of Management Information Version 2 (SMIv2, RFC 2578), a subset of ASN.1(Abstract Syntax Notation One).



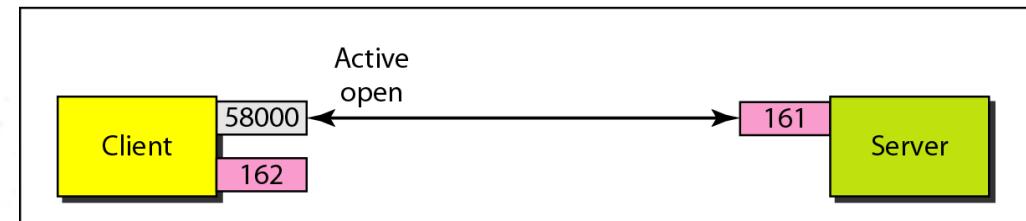
SNMP Protocol

- **SNMP versions**
 - SNMPv1
 - SNMPv2
 - SNMPv3

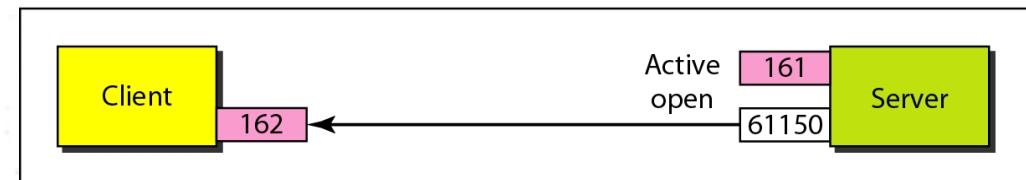
- Operates in the Application Layer.
- The SNMP Manager sends requests on UDP port 161.
- The SNMP Agent sends notifications on UDP port 162.
- SNMPv1 specifies five core protocol data units (PDUs). Two other PDUs were added in SNMPv2 and carried over to SNMPv3.



a. Passive open by both client and server



b. Exchange of request and response messages



c. Server sends trap message

SNMP PDU Format

Sending a Request

1. Appropriate PDU is constructed based on the **VarBindList** and the **operation type**.
2. The PDU, security information and agent identity are input to a security mechanism to apply authentication and encryption to the PDU (This is only conceptual in SNMPv1). The result from the security mechanism and the **community string** are used to generate an SNMP message.
3. PDU type –Get Request type
4. The message is then serialized and sent using a transport service (i.e. UDP) to the specified SNMP agent (serialization is done using the BER encoding scheme).

PDU Type used

Get-Request

Request ID	Error Status	Error Index	Name X	Value X	...
Not used	Not used	Not used			

Get-Response

Request ID	Error Status	Error Index	Name X	Value X	...
Copy value	Set to zero	Set to zero	Copy value	Current Value	

- **GetRequest**

- A manager-to-agent request to retrieve the value of a variable or list of variables. Desired variables are specified in variable bindings (values are not used). Retrieval of the specified variable values is to be done as an atomic operation by the agent. A *Response* with current values is returned.

SNMPv1

Receiving a Request

1. Incoming message is de-serialized to construct an **ASN.1** message.
2. **Version** number is verified.
3. The **community** name, security information and the data found in the SNMP message are input to a security mechanism.
4. The agent then performs a rudimentary parse of the ASN.1 object returned from the security service to build an ASN.1 object corresponding to an SNMP PDU object.

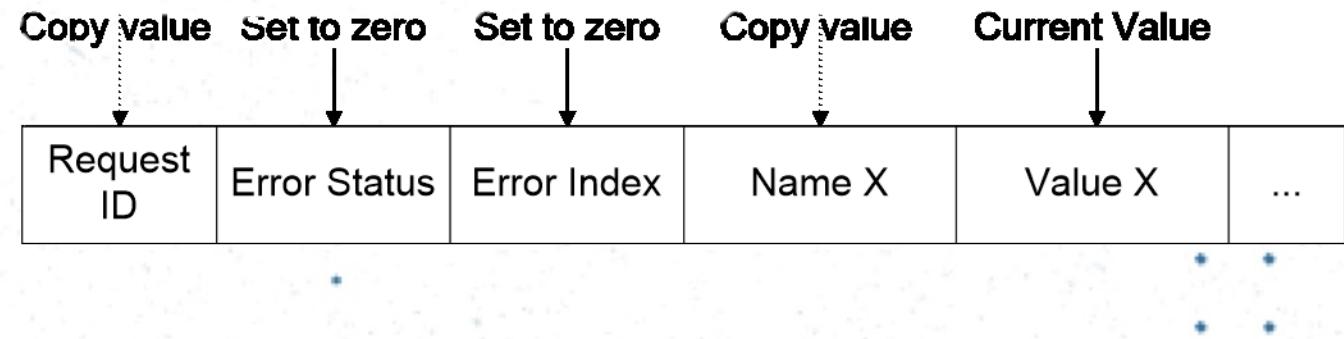
Sending a Response

1. It first constructs a **Response** PDU using as input, the saved **request-id value** and the values for **error-status**, **error-index** and **VarBindList** returned from processing the request.
2. The PDU, security information and agent identity are input to a security mechanism. The result from the security mechanism and the **community string** are used to generate an SNMP message.
3. The message is serialized and then sent to the manager address from the request.

Pdu type used

Get-Response

- **Response**
- Returns variable bindings and acknowledgement from agent to manager for *GetRequest* or any other request message type. Error reporting is provided by error-status and error-index fields. Although it was used as a response to both gets and sets, this PDU was called *GetResponse* in SNMPv1.



SNMPv1

Receiving a Response

1. Incoming message is de-serialized.
2. PDU **version** is verified.
3. The **community** name, security information and the data found in the SNMP message are input in the security mechanism.
4. The **ASN.1 object** is parsed.

GetRequest/GetResponse Errors

- **tooBig** – the size of the response would exceed a local limitation (and the error-index field has no additional information)
- **noSuchName** – a specified instance of the management information is not available to be accessed – due to access control settings or instance does not exist
- **genErr** – specified instance of the management information is not available due to some other reason

Since only one error indication is returned in a get-response message and each identified instance of management information in the request can cause an error, a manager may have to try the GET operation many times before a get-response message is retimed with no error.

Other Request PDU types

- **GetNextRequest**
- A manager-to-agent request to discover **available variables** and their **values**. Returns a Response with variable binding for the lexicographically **next variable in the MIB**. The entire MIB of an agent can be walked by iterative application of *GetNextRequest* starting at OID 0. Rows of a table can be read by specifying column OIDs in the variable bindings of the request.

SNMPv1

Other Request PDU types

- **GetBulkRequest**
- Optimized version of *GetNextRequest*. A manager-to-agent request for multiple iterations of *GetNextRequest*. Returns a Response with multiple variable bindings walked from the variable binding or bindings in the request. PDU specific non-repeaters and max-repetitions fields are used to control response behavior. *GetBulkRequest* was introduced in SNMPv2.

SNMPv2

Other Request PDU types

- **SetRequest**
- A manager-to-agent **request to change the value of a variable or list of variables**. Variable bindings are specified in the body of the request. Changes to all specified variables are to be made as an atomic operation by the agent. A Response with (current) new values for the variables is returned.

SNMPv1

SetRequest/GetResponse Errors

- **badValue** – the value provided for the field may not comply with the data types or standards defined
- **noSuchName** – a specified instance of the management information is not available to be accessed – due to access control settings or instance does not exist
- **genErr** – specified instance of the management information is not available due to some other reason

Since only one error indication is returned in a get-response message and each identified instance of management information in the request can cause an error, a manager may have to try the GET operation many times before a get-response message is retimed with no error.

Other PDU types

- Trap
- Asynchronous notification from agent to manager. SNMP traps enable an agent to notify the management station of significant events by way of an unsolicited SNMP message. Includes current *sysUpTime* value, an *OID* identifying the type of trap and optional variable bindings.
- No response is expected.

SNMPv1

TRAP types

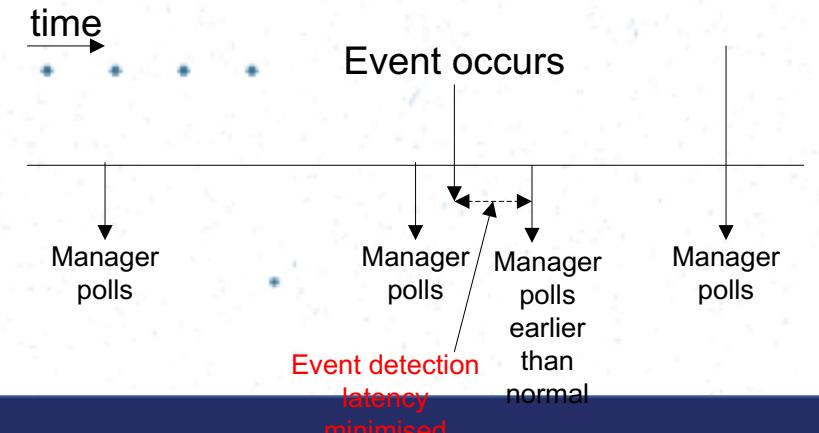
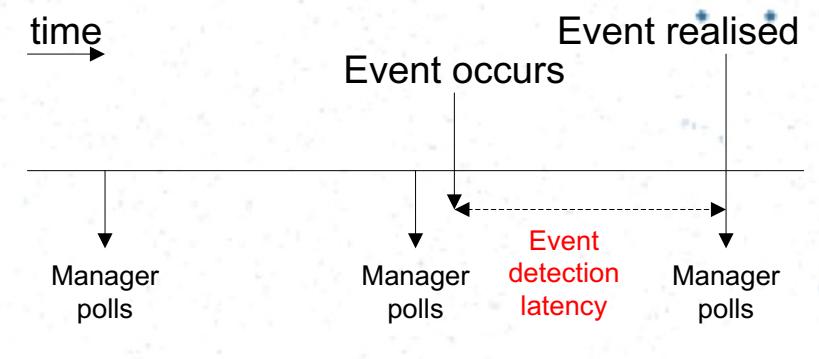
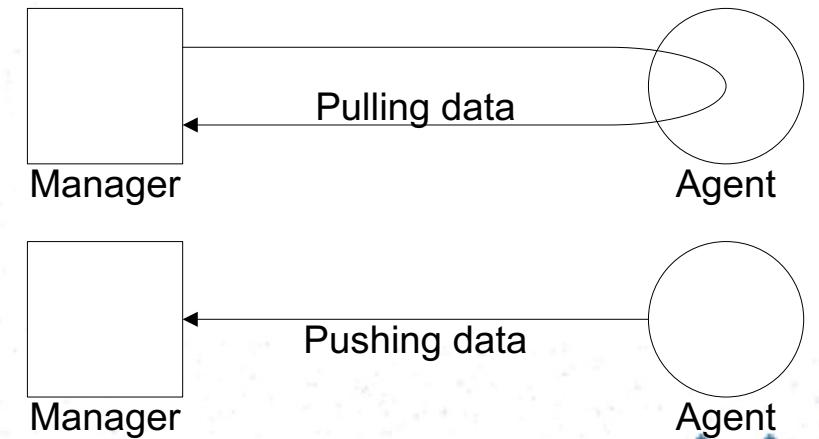
- **coldStart** - the sending protocol entity is reinitializing itself so that the agent's configuration or the protocol entity implementation can be altered.
- **warmStart** - the sending protocol entity is reinitializing itself so that neither the agent configuration nor the protocol entity implementation can be altered.
- **linkDown** - the sending protocol entity recognizes a failure in one of the communication links represented in the agent's configuration.
- **linkUp** - the sending protocol entity recognizes that one of the communication links represented in the agent's configuration has come up.

TRAP types

- **authenticationFailure** - the sending protocol entity is the addressee of a protocol message that is not properly authenticated.
- **egpNeighborLoss** - an EGP neighbor for whom the sending protocol entity was an EGP peer has been marked down and the peer relationship no longer exists.
- **enterpriseSpecific** - the sending protocol entity recognizes that some enterprise-specific event has occurred.

Use of Events

- Agents provide the specified data only when requested by managers.
 - This periodic gathering of data is called **polling**.
- Amount of time between an event and a manager realizing that an event has occurred is called the *event detection latency*.
- Another model of management is based on agents in managed systems sending data to configured managers.
 - Traps (**Pushing**).
 - However, during a communication failure, an event report would never reach a manager.



SNMP versions

1. **SNMPv1** - SNMP version 1 (SNMPv1) is the initial implementation of the SNMP protocol. Version 1 has been criticized for its poor security. Authentication of clients is performed only by a "*community string*".
2. **SNMPv2** - Revises version 1 and includes improvements in the areas of performance, security, confidentiality, and manager-to-manager communications. It introduced *GetBulkRequest*, an alternative to iterative *GetNextRequests* for retrieving large amounts of management data in a single request.
3. **SNMPv3** - SNMPv3 primarily added security and remote configuration enhancements to SNMP.

SNMP_v1

SNMPv1 - Limitations

- Limited data types
 - Reduction in complexity of SNMP has resulted in some increase in complexity of MIB understanding and design.
- Limited performance
 - Inefficient for large retrievals. (e.g. retrieving entire MIB or tables)
 - E.g. 2000 entry table with 4 columns 200ms RTT Using GETNEXT Requests: $2000 \times 4 \times 2 = 16000$ packets or $2000 \times 4 \times .2 = 1600$ seconds...!!!
- Limited error codes
- Lack of hierarchies
 - Inherently centralized
- Lack of security
 - Community strings

SNMP_v2

SNMPv2 - features

- ❖ New data types

SIMPLE TYPES:

SMIv1

INTEGER
OCTET STRING
OBJECT IDENTIFIER

SMIv2

INTEGER
OCTET STRING
OBJECT IDENTIFIER

- Integer32

APPLICATION-WIDE TYPES:

- Unsigned32
Gauge
Counter
-
TimeTicks
IpAddress
Opaque
NetworkAddress

Unsigned32
Gauge32
Counter32
Counter64
TimeTicks
IpAddress
Opaque
-

PSEUDO TYPES:

- BITS

SNMPv2 - features

- ❖ Community based (similar to SNMPv1).
- ❖ *GET* and *GETNEXT* operations are the same as SNMPv1.
- ❖ SET Request operation is a conceptual two phase commit;
 - ❖ PHASE 1 : Perform various checks.
 - ❖ PHASE 2 : Perform the actual set operation.
- ❖ SNMPv2 adds and enhances some protocol operations.
 - The *INFORM* Request.
 - The *GETBULK* Request.

GETBULK Request

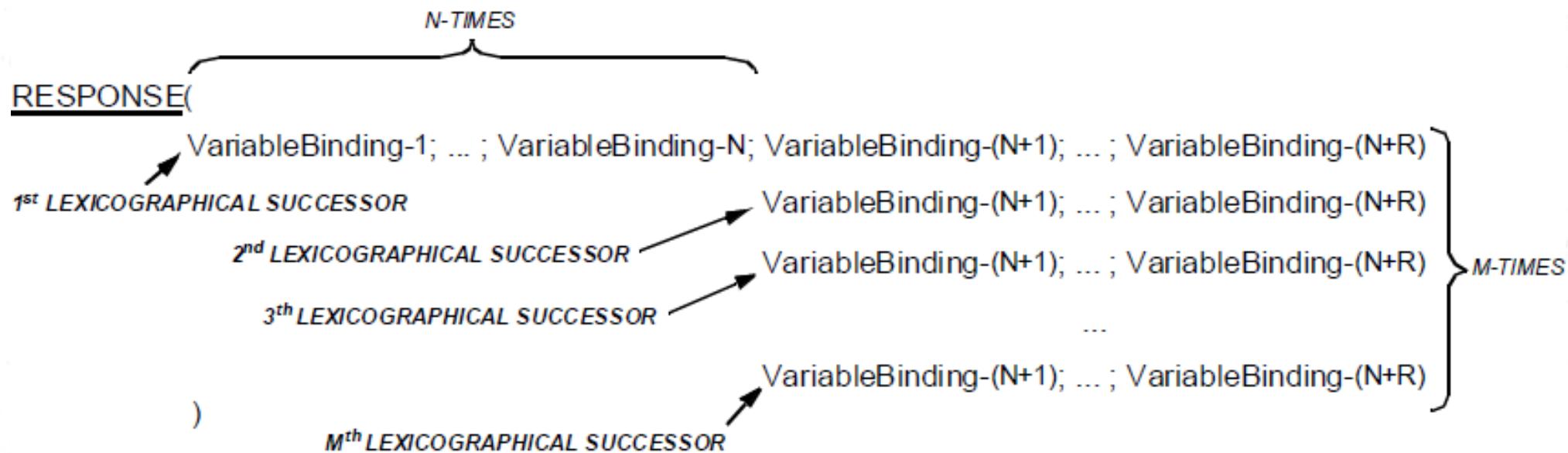
Some further insight...

- For efficient retrieval of many VarBinds.
- GETBULK Request has two additional parameters:
 - **non-repeaters**
 - The first N elements (non-repeaters) of the VarBind list are treated as if the operation was a normal GETNEXT Request operation.
 - **max-repetitions**
 - The next elements of the VarBind list are treated as if the operation consisted of a number (max-repetitions) of repeated GETNEXT Request operations.

GETBULK Request

Some further insight...

REQUEST(non-repeaters = N; max-repetitions = M;
VariableBinding-1; ... ; VariableBinding-N; VariableBinding-(N+1); ... ; VariableBinding-(N+R)
)



INFORM Request

Some further insight...

- Remember that for **SNMPv1 trap messages**, there is **no response sent by the manager**. Hence, **no guarantee** that the manager received the trap or not...!!!
- As a solution for this, SNMPv2 INFORM operation was introduced.
- In simple terms this is a confirmed trap.
 - Originally to INFORM a higher level manager
 - Same format as Trap PDU
 - Possible error: tooBig

SNMPv2 - features

- ❖ Additional error/exceptions
 - GET additional errors:
 - noSuchObject.
 - noSuchInstance.
 - GETNEXT additional errors:
 - endOfMibView.
 - Exceptions are coded within the VarBinds and do not raise Error Status and Index.

SNMPv2 - Limitations

- ❖ Too complex
- ❖ Overshoot problem - GETBULK does not stop when it reaches the end of a table.
- ❖ Although SNMPv2 was originally intended to overcome the security problem of SNMPv1 because of the high complexity, without the controversial new SNMP v2 security model, using instead the simple community-based security scheme of SNMPv1

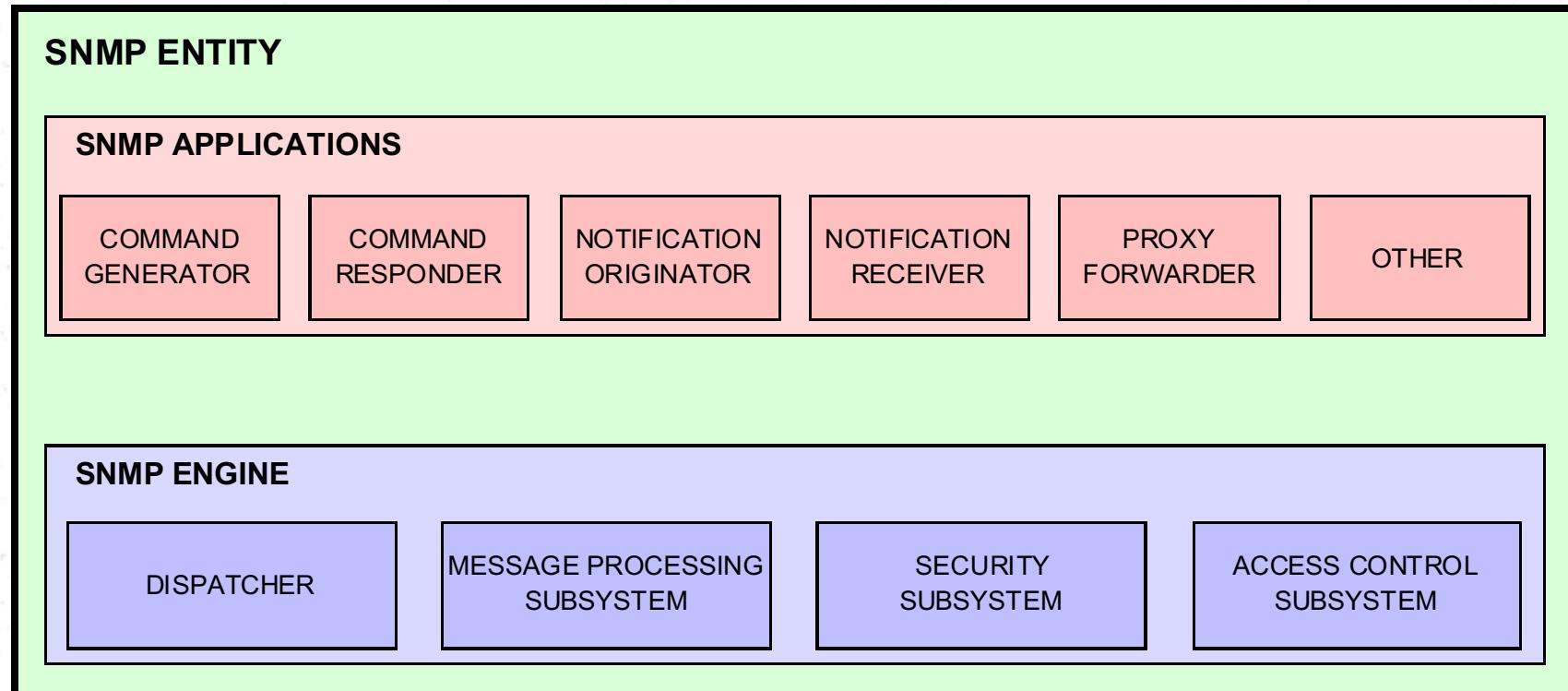
SNMP_v3

SNMPv3 - features

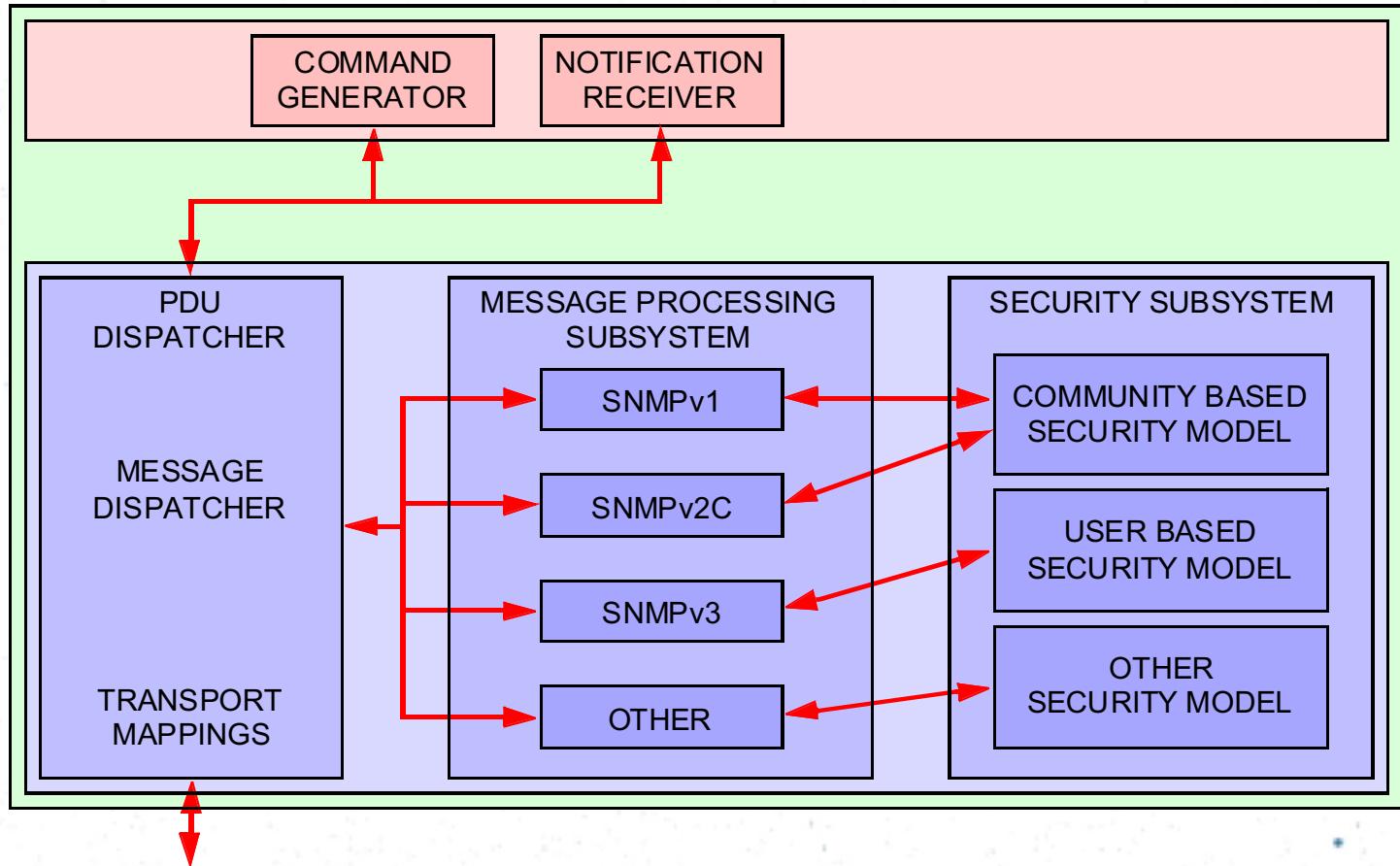
- ❖ Security.
- ❖ Remote configuration capabilities.
- ❖ Ability to control the agents via use of a newly defined specific management MIB.
- ❖ SNMPv3 contains all the functionality of SNMPv1 and SNMPv2.
- ❖ Incorporates the SNMPv2 data types.

SNMPv3 - Entities

- ❖ SNMP Manager and Agent is created as an SNMP Entity
 - Entity consists of an **SNMP engine** and **SNMP applications**.



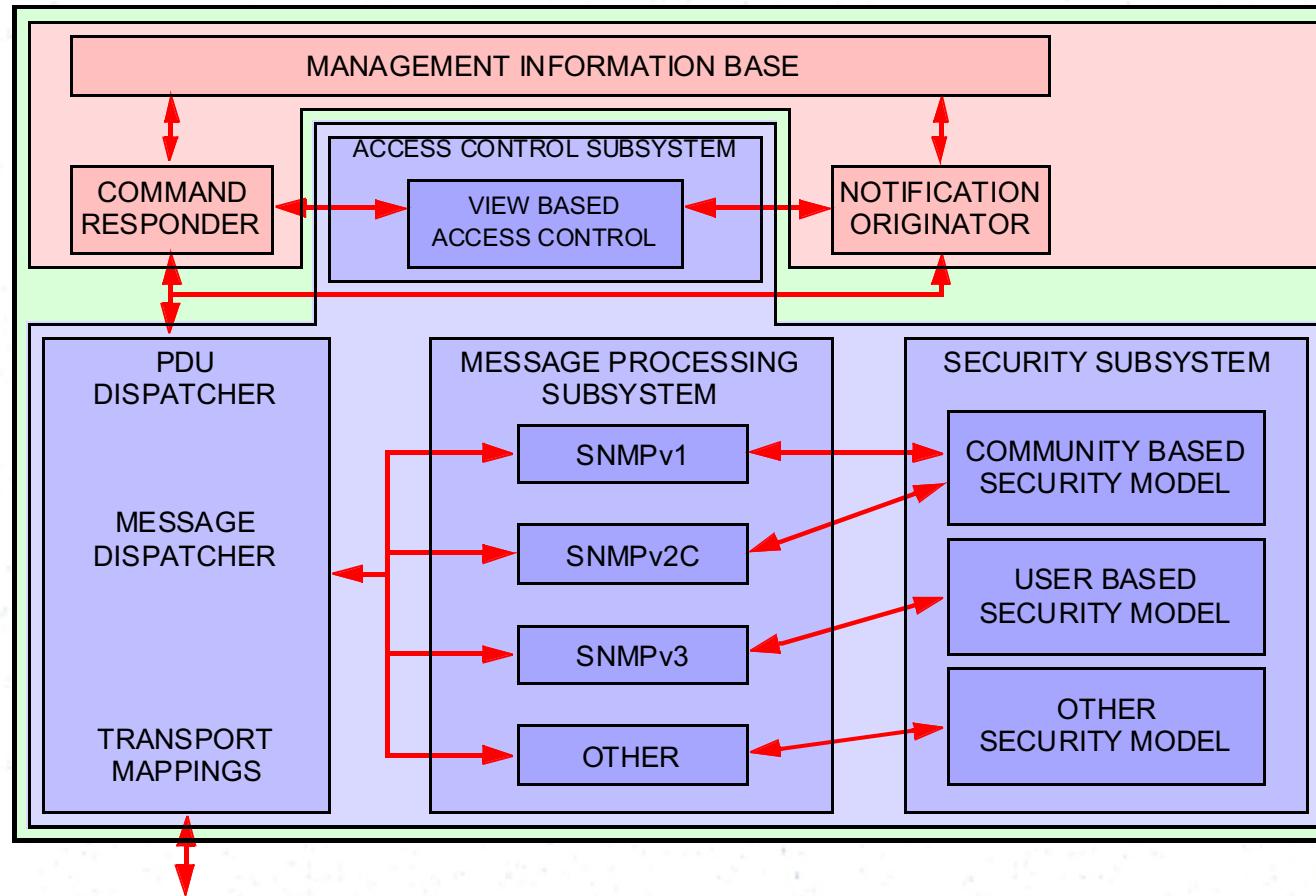
SNMPv3 – SNMP Manager entity



SNMP
Application

SNMP
Engine

SNMPv3 – SNMP AGENT entity



SNMP
Application

SNMP
Engine

SNMP Engine dispatcher

- ❖ The dispatcher is a **traffic manager** that sends and receives messages.
- ❖ Incoming messages
 - The dispatcher tries to **determine the version number** of the message and then **passes the message to the appropriate message processing model**.
- ❖ Outgoing messages
 - The dispatcher **selects the appropriate transports** for sending messages. Currently this is UDP in the TCP/IP world.
- ❖ The dispatcher is also responsible for dispatching PDUs to applications.

SNMP Engine

Message processing subsystem

- Outgoing messages
 - Accepts outgoing PDUs from the dispatcher and prepares them for transmission by wrapping them in a message header.
- Incoming messages
 - Accepts incoming messages from the dispatcher, processes each message header.
 - An implementation of the message processing subsystem may support a single message format corresponding to a single version of SNMP (SNMPv1, SNMPv2c, SNMPv3), or it may contain a number of modules, each supporting a different version of SNMP.

SNMP Engine

security subsystem

- Authenticates and encrypts messages.
- Outgoing messages are passed to the security subsystem from the message processing subsystem.
 - Depending on the services required, the security subsystem may encrypt the enclosed PDU and some fields in the message header.
 - The security subsystem may generate an authentication code and insert it into the message header.
- After encryption, the message is returned to the message processing subsystem.

SNMP Engine

security subsystem

- Incoming messages are passed to the security subsystem from the message processing subsystem.
 - If required, the security subsystem checks the authentication code and performs decryption.
 - The processed message is returned to the message processing subsystem.
 - An implementation of the security subsystem may support one or more distinct security models.

SNMP Engine

security subsystem

Consists of three sub modules,

1. Community Based Security Model
 - For SNMPv1 and SNMPv2
2. User Based Security Model
 - For SNMPv3 covering the CIA concepts
3. Other Security Model

SNMP Engine

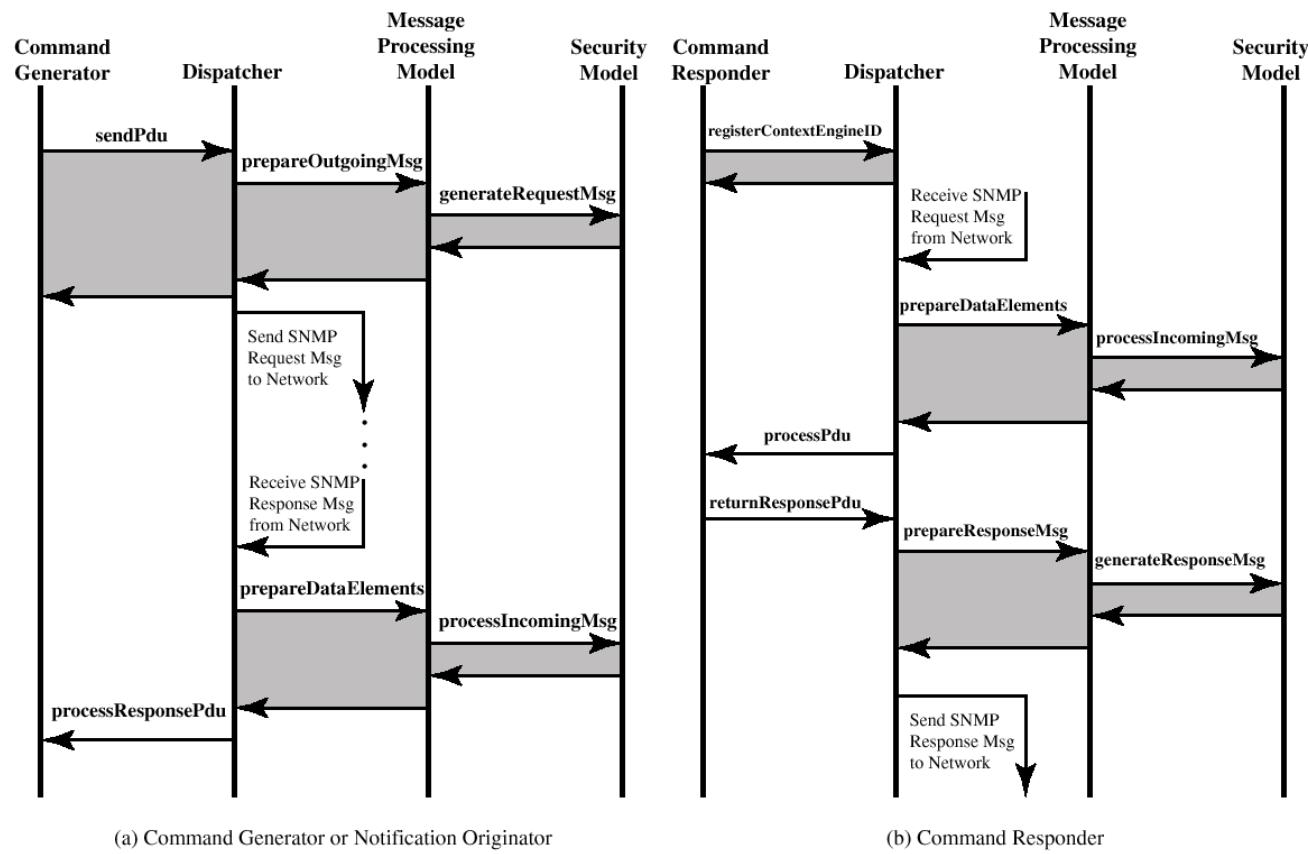
Access Control Subsystem

- Provides authentication.
 - Determine whether access to a managed object should be allowed.
- Can control which users and which operations can have access to which managed objects.

SNMP Application

- There are five types of applications.
 - **Command generators** - Generate SNMP commands to collect or set management data.
 - **Command responders** - Provide access to management data.
 - For example, processing get, get-next, get-bulk and set PDUs.
 - Commands are used in a command responder application.
 - **Notification originators** - Initiate Trap or Inform messages.
 - **Notification receivers** - Receive and process Trap or Inform messages.
 - **Proxy forwarders** - Forward messages between SNMP entities.

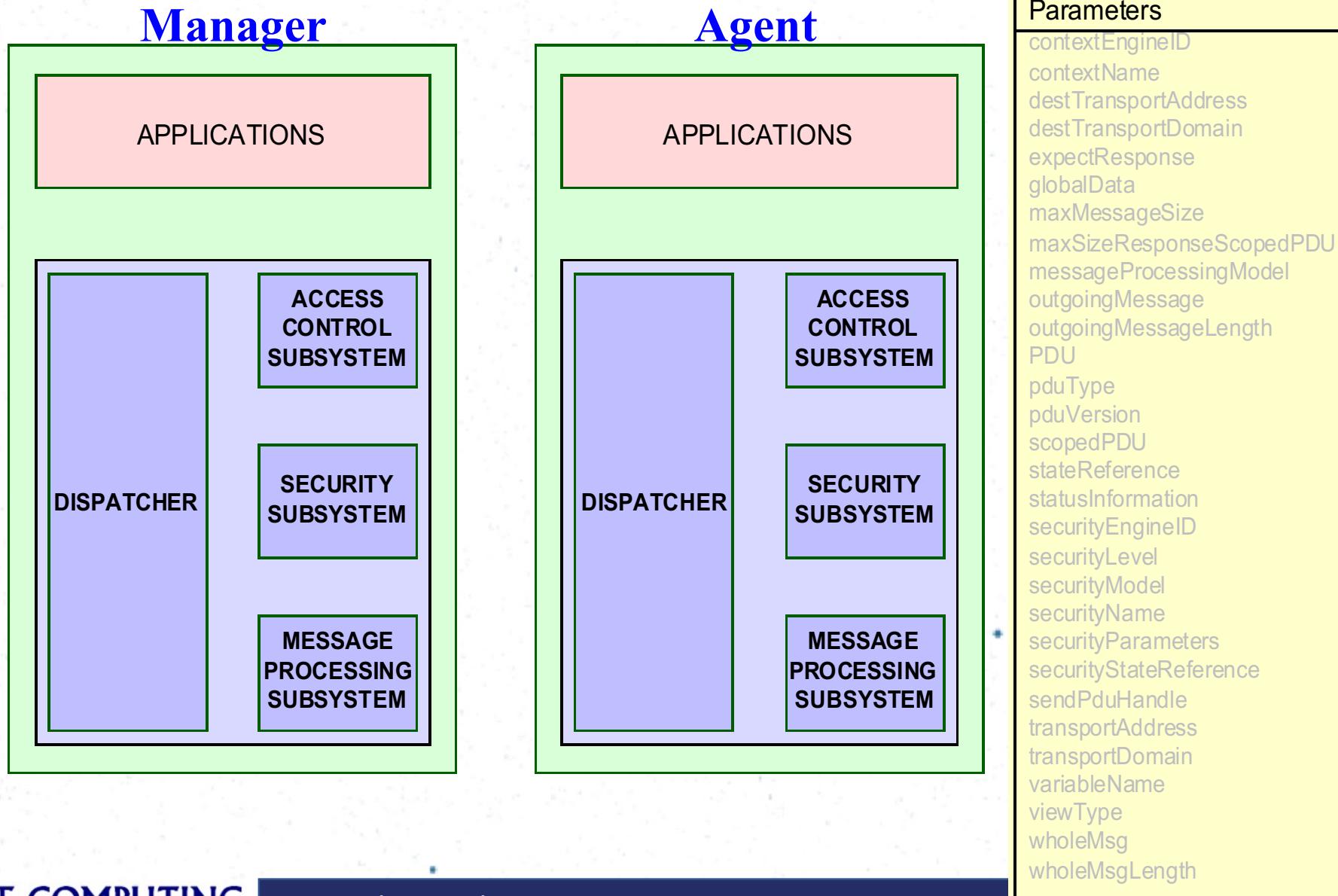
SNMPv3 flow



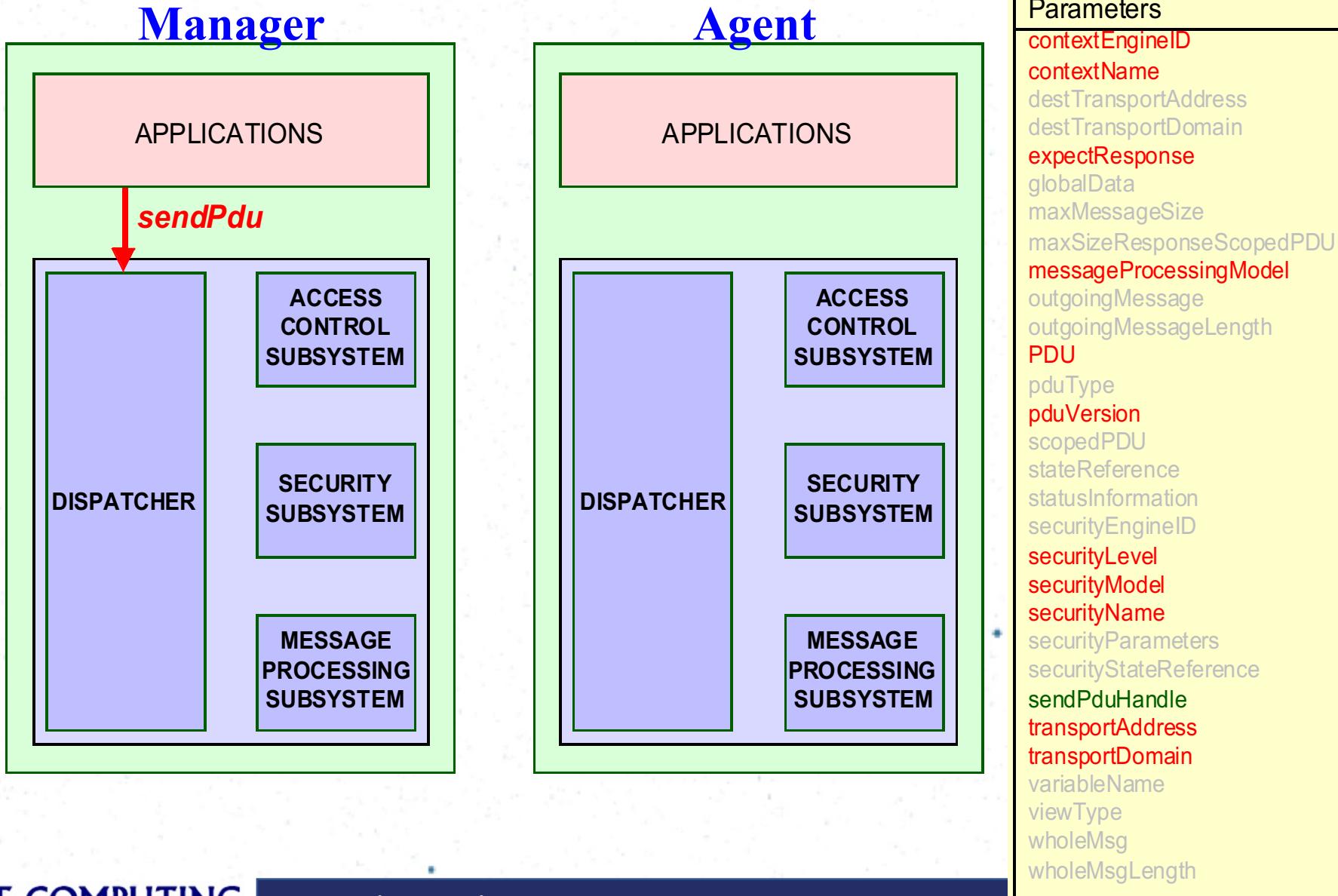
(a) Command Generator or Notification Originator

(b) Command Responder

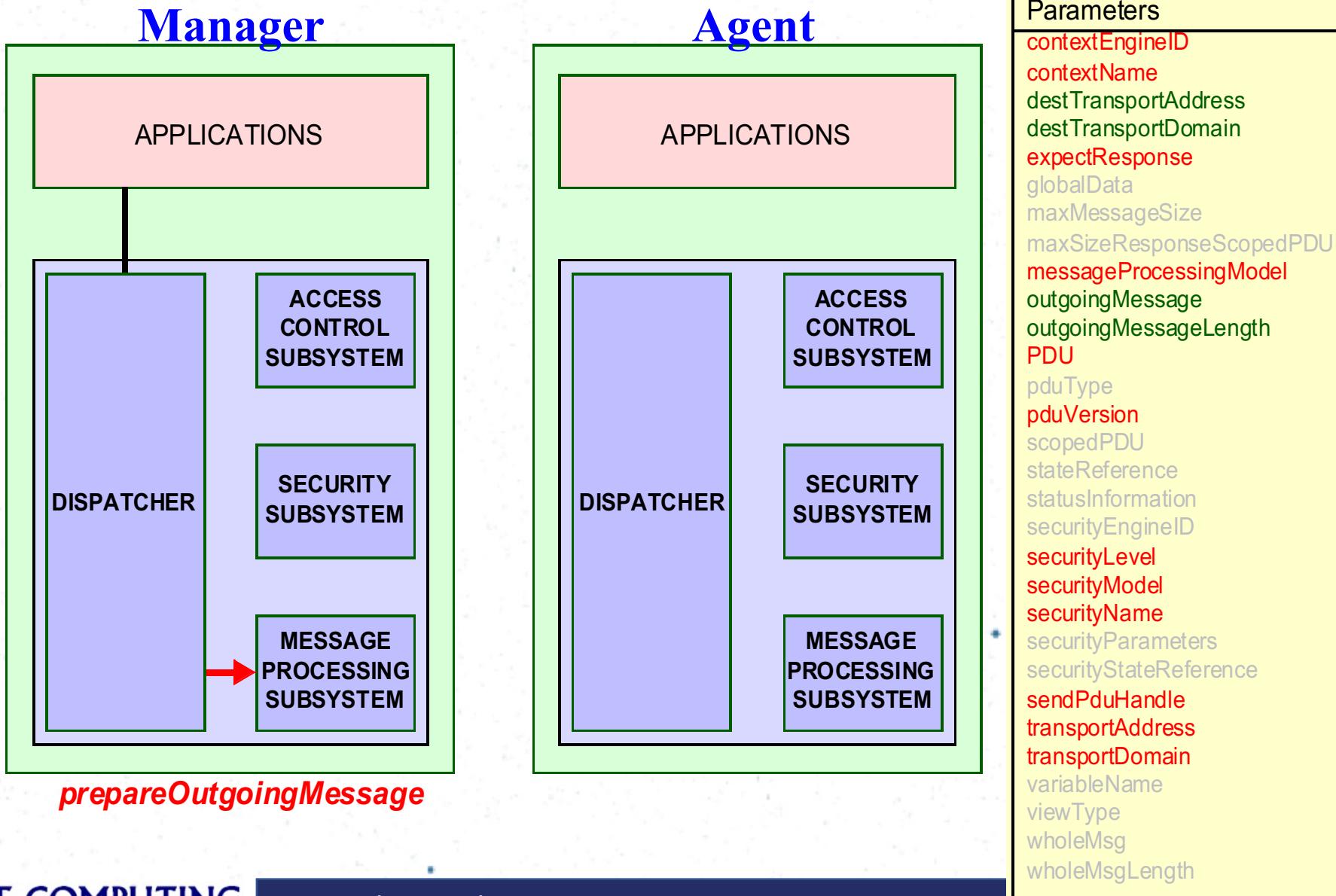
Primitives Between Modules



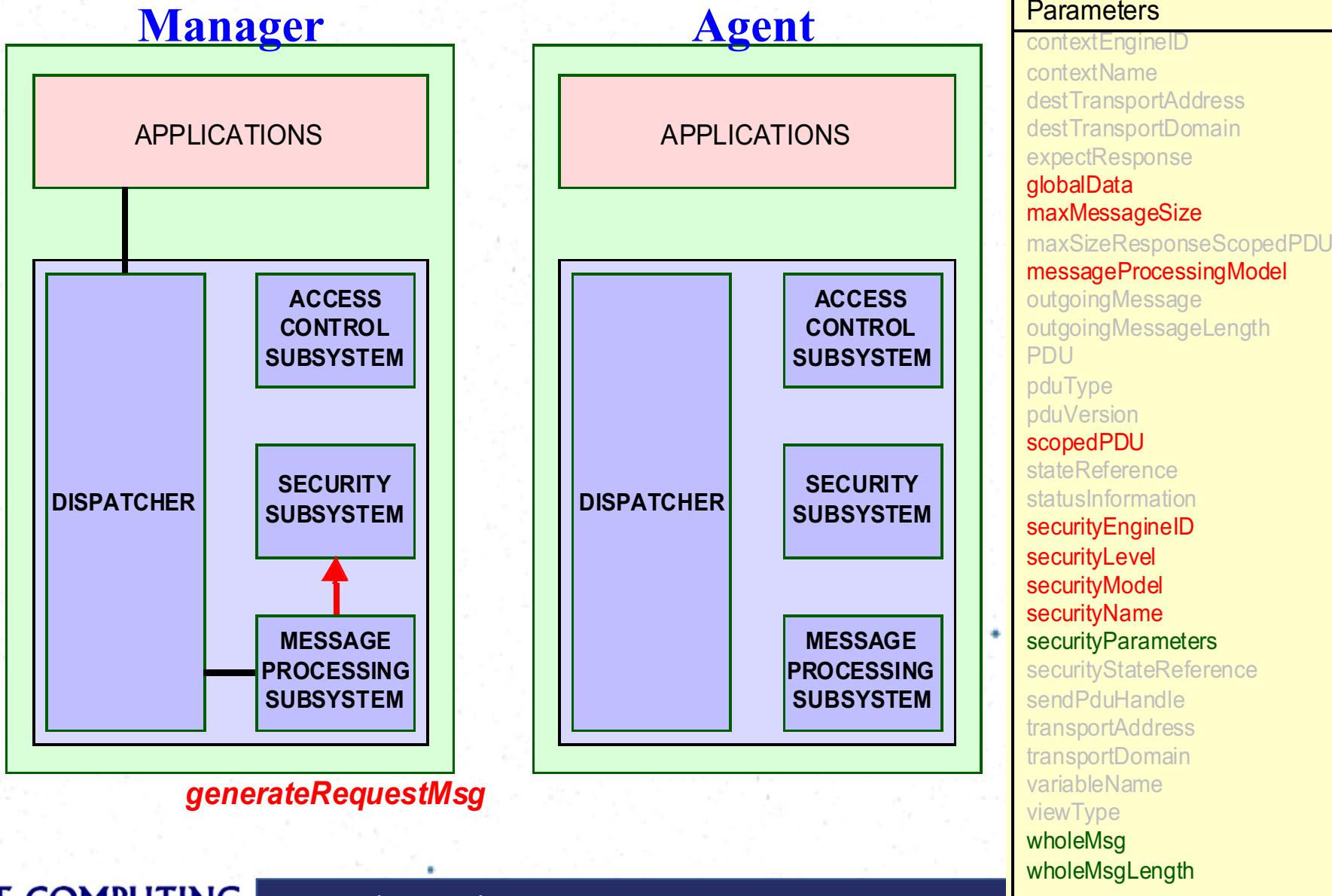
sendPdu



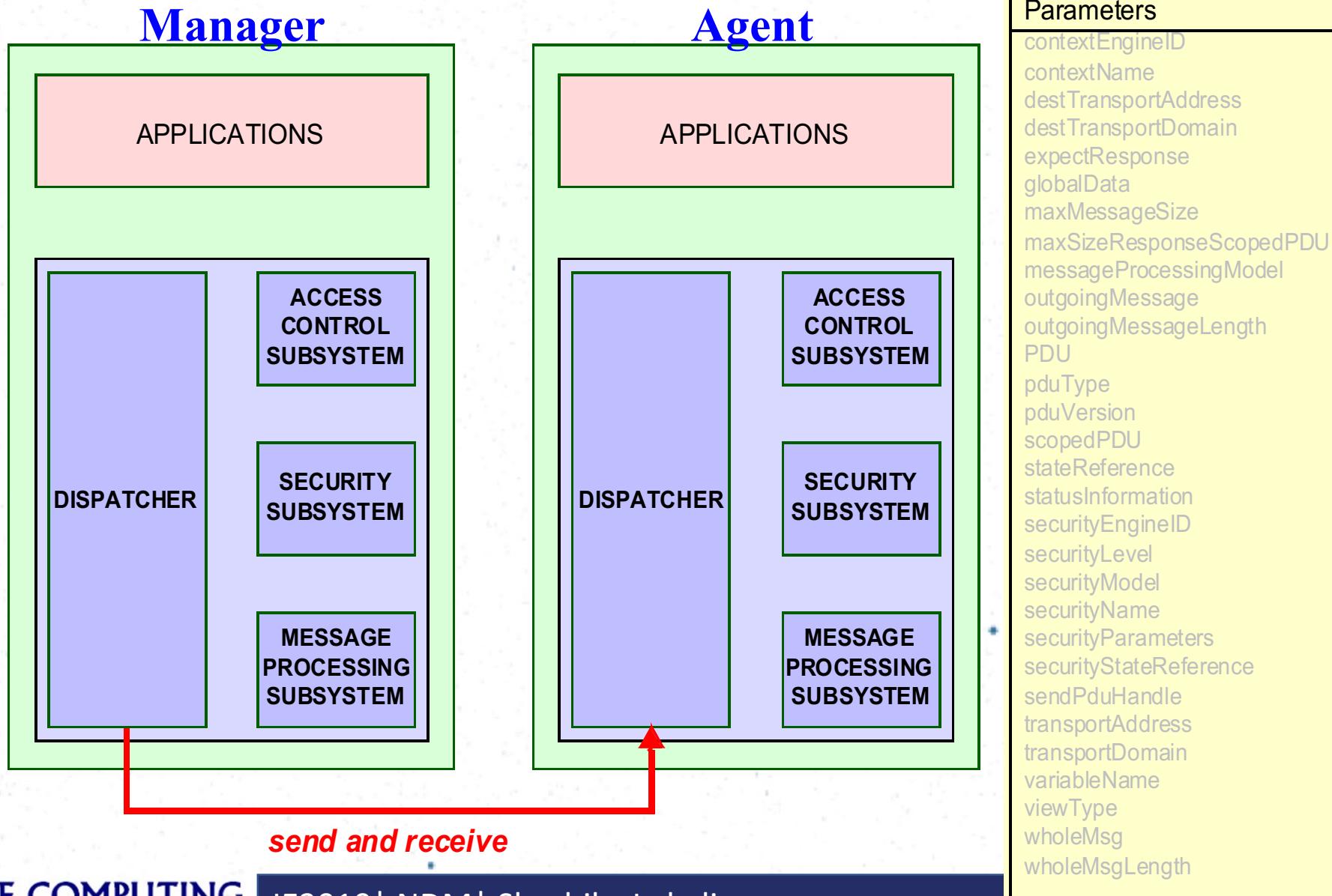
prepareOutgoingMessage



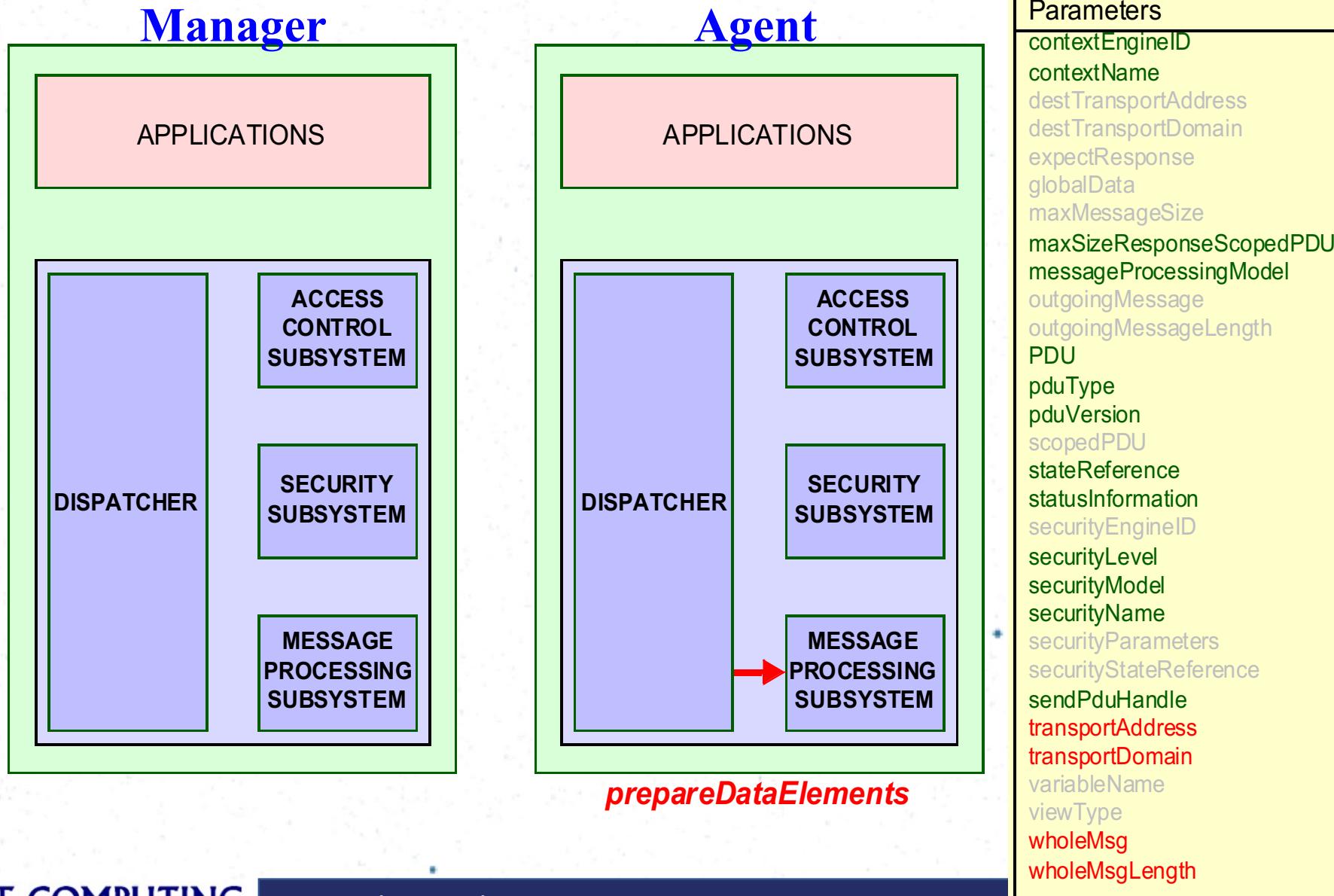
generateRequestMsg



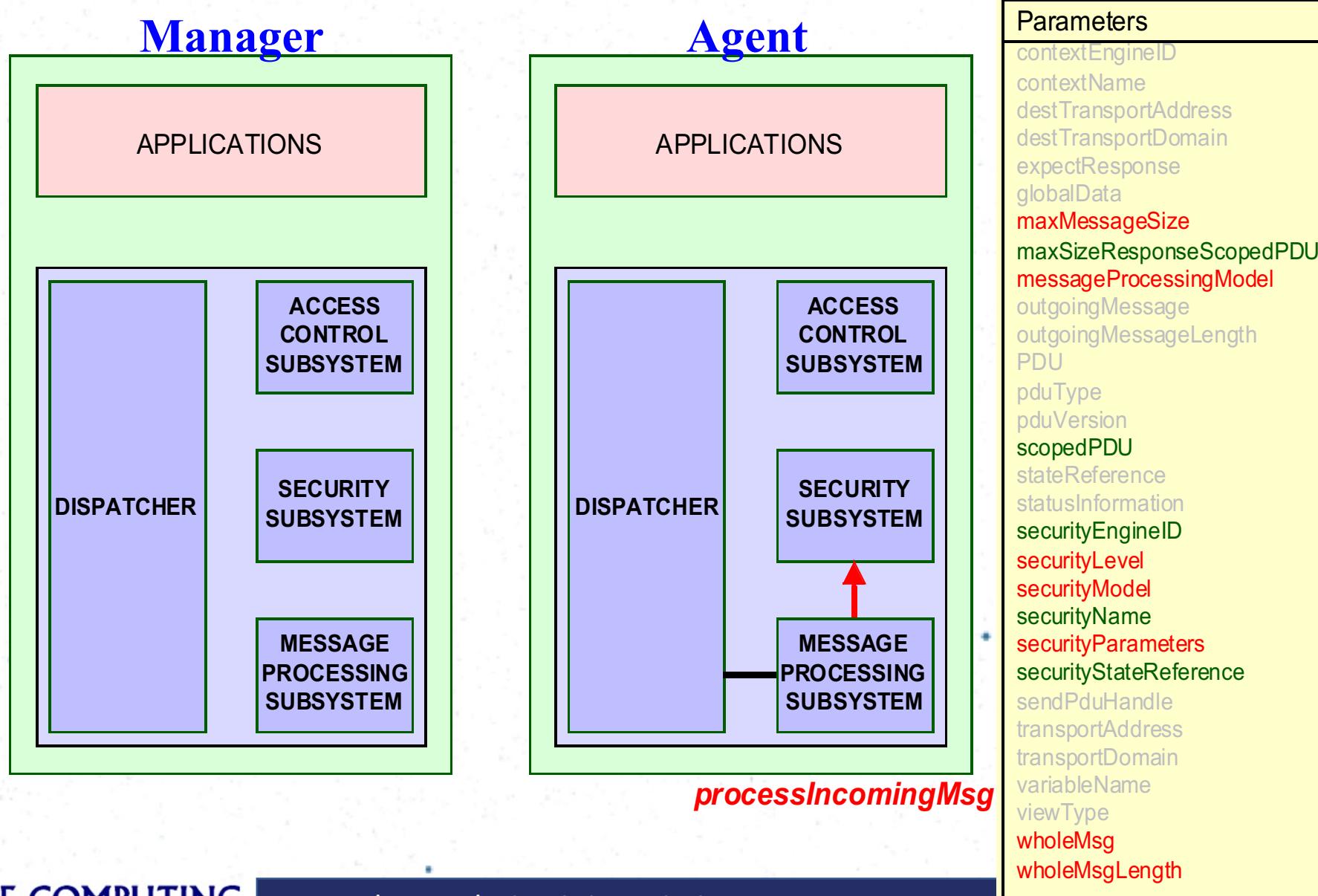
send / receive



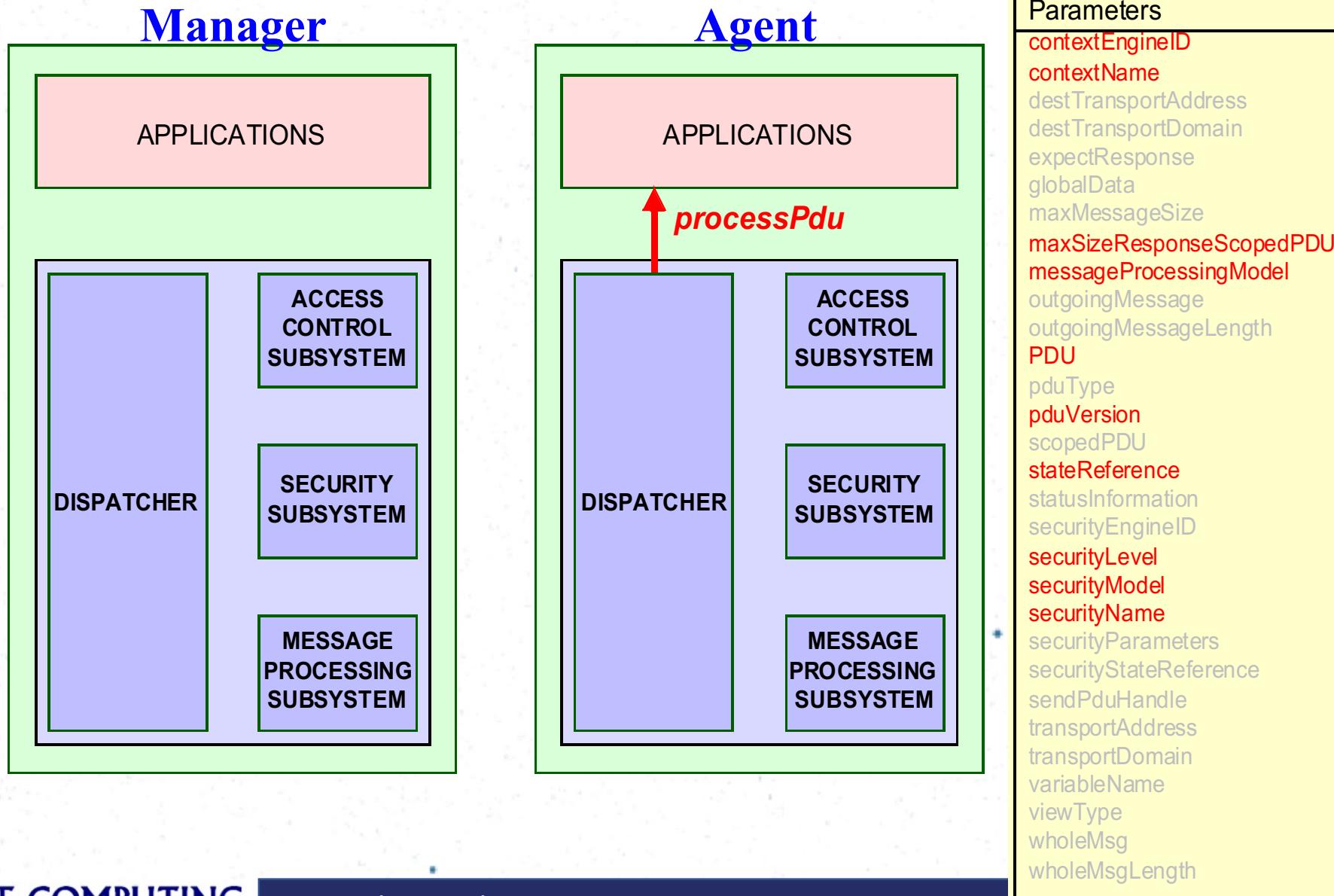
prepareDataElements



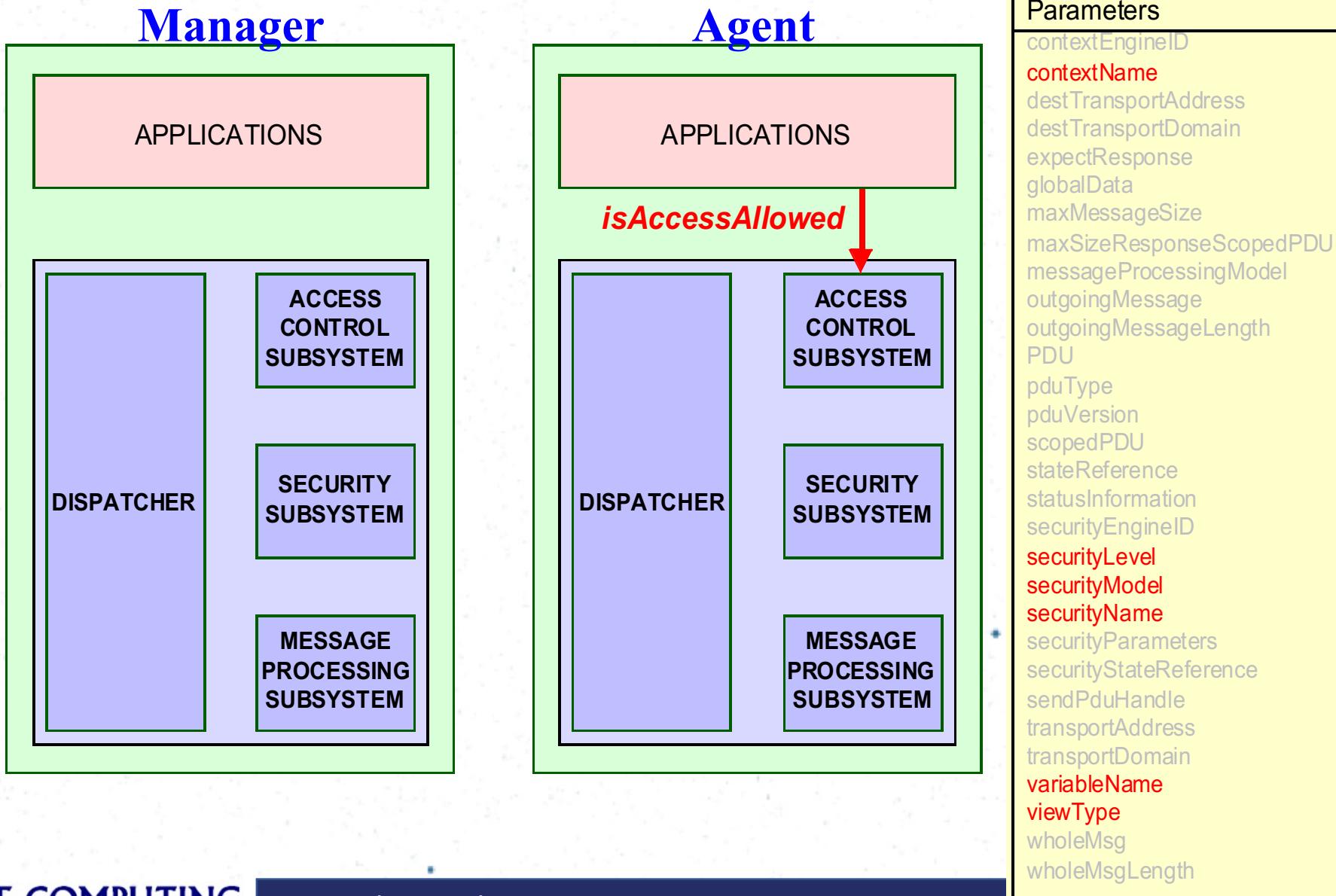
processIncomingMsg



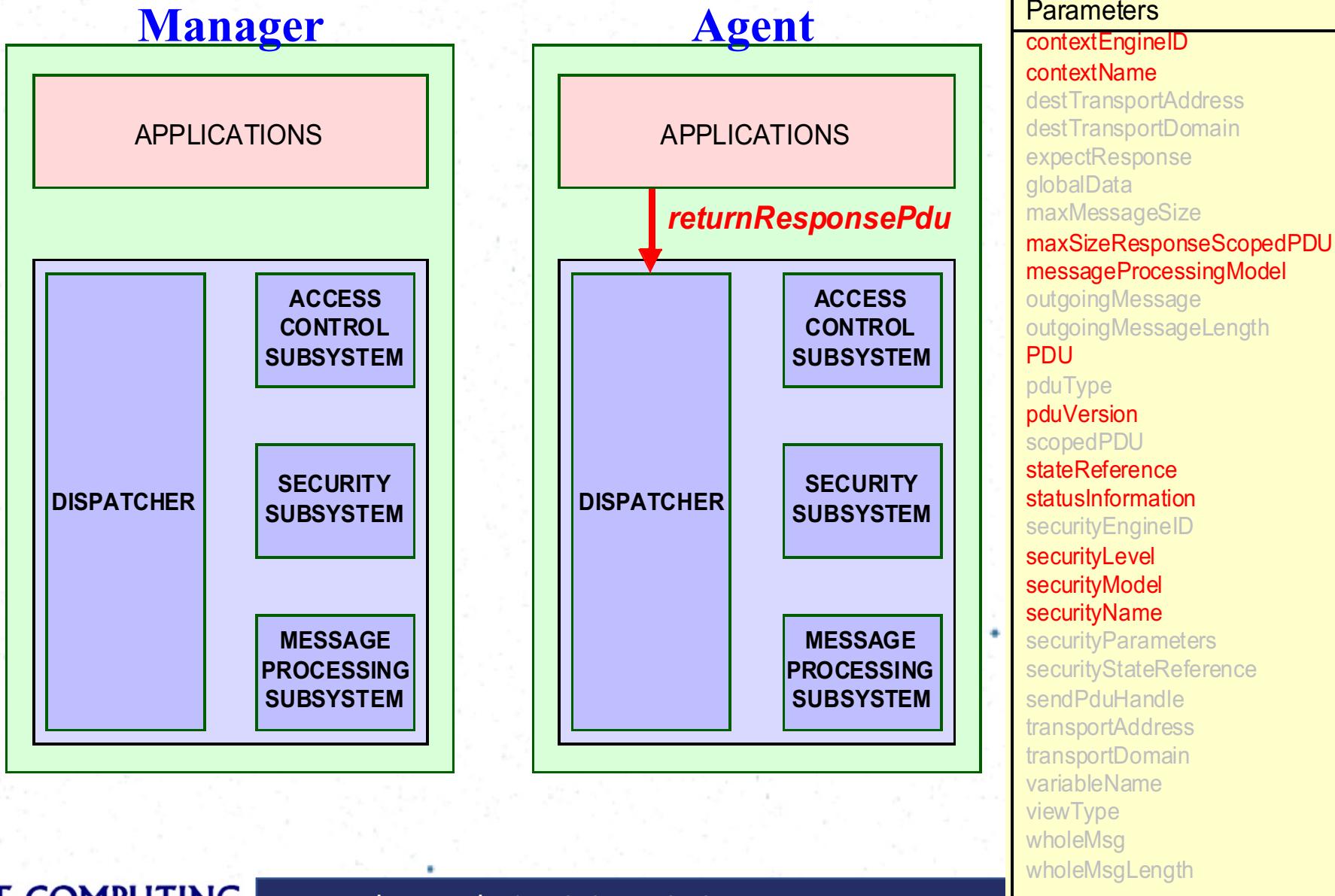
processPdu



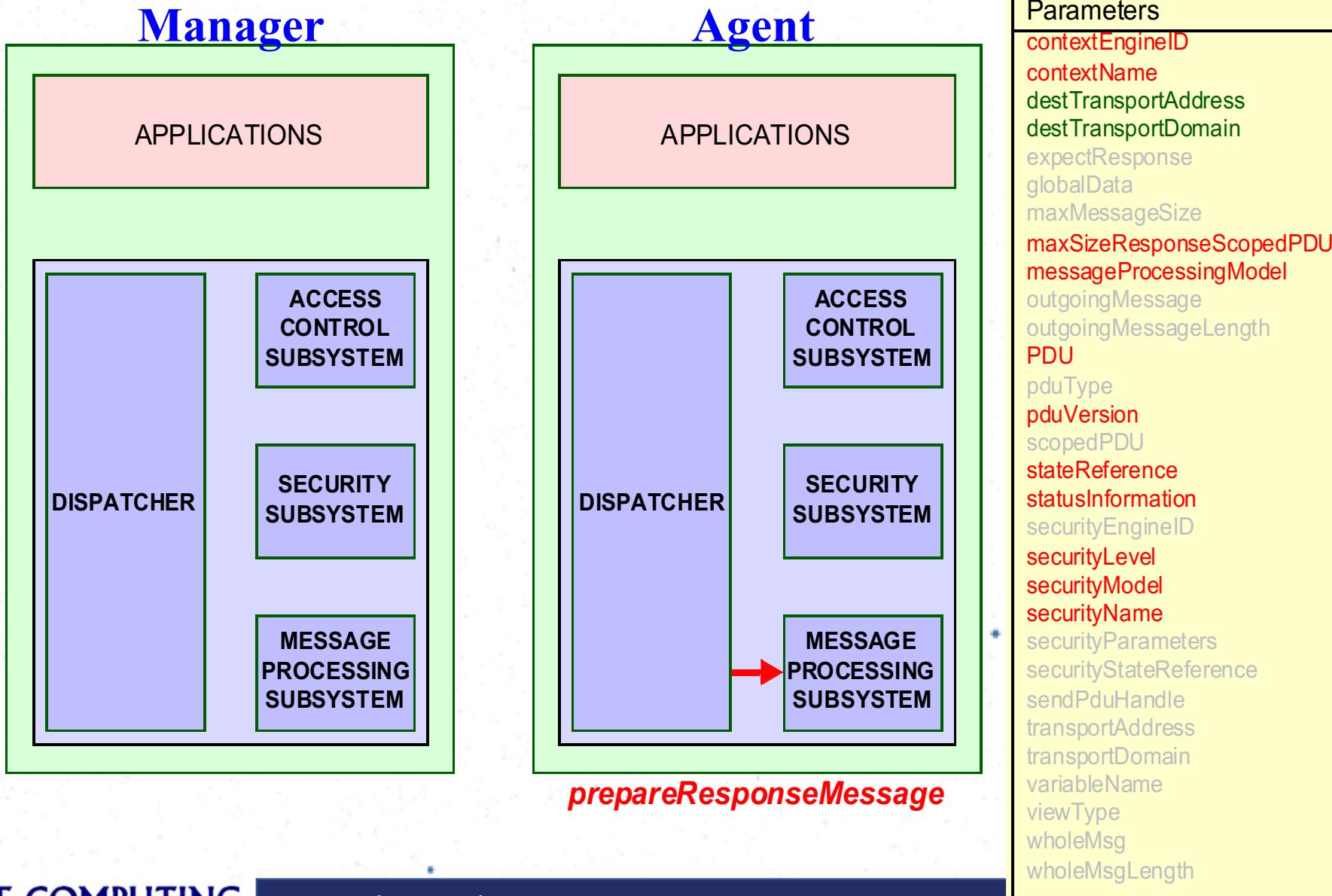
isAccessAllowed



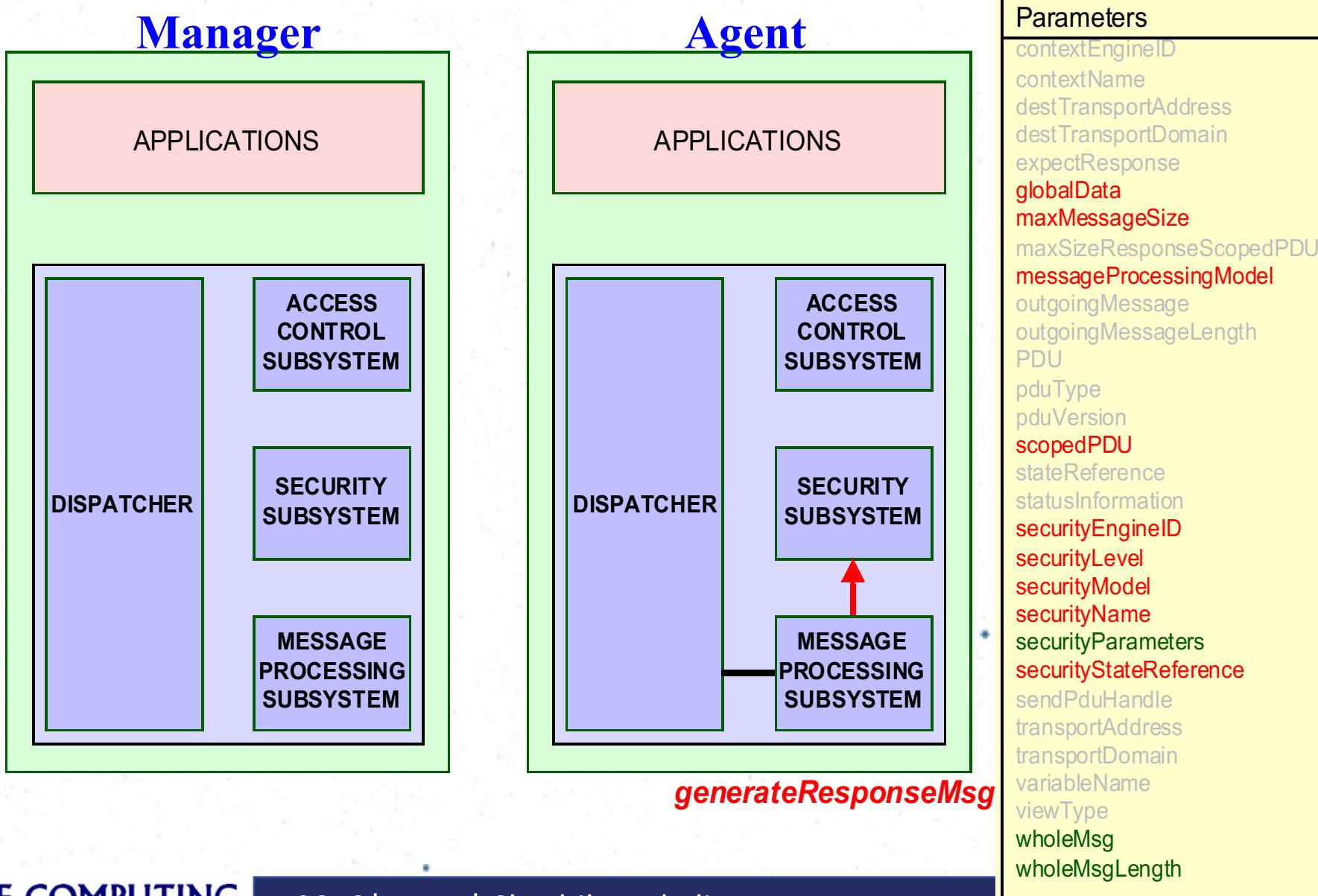
returnResponsePdu



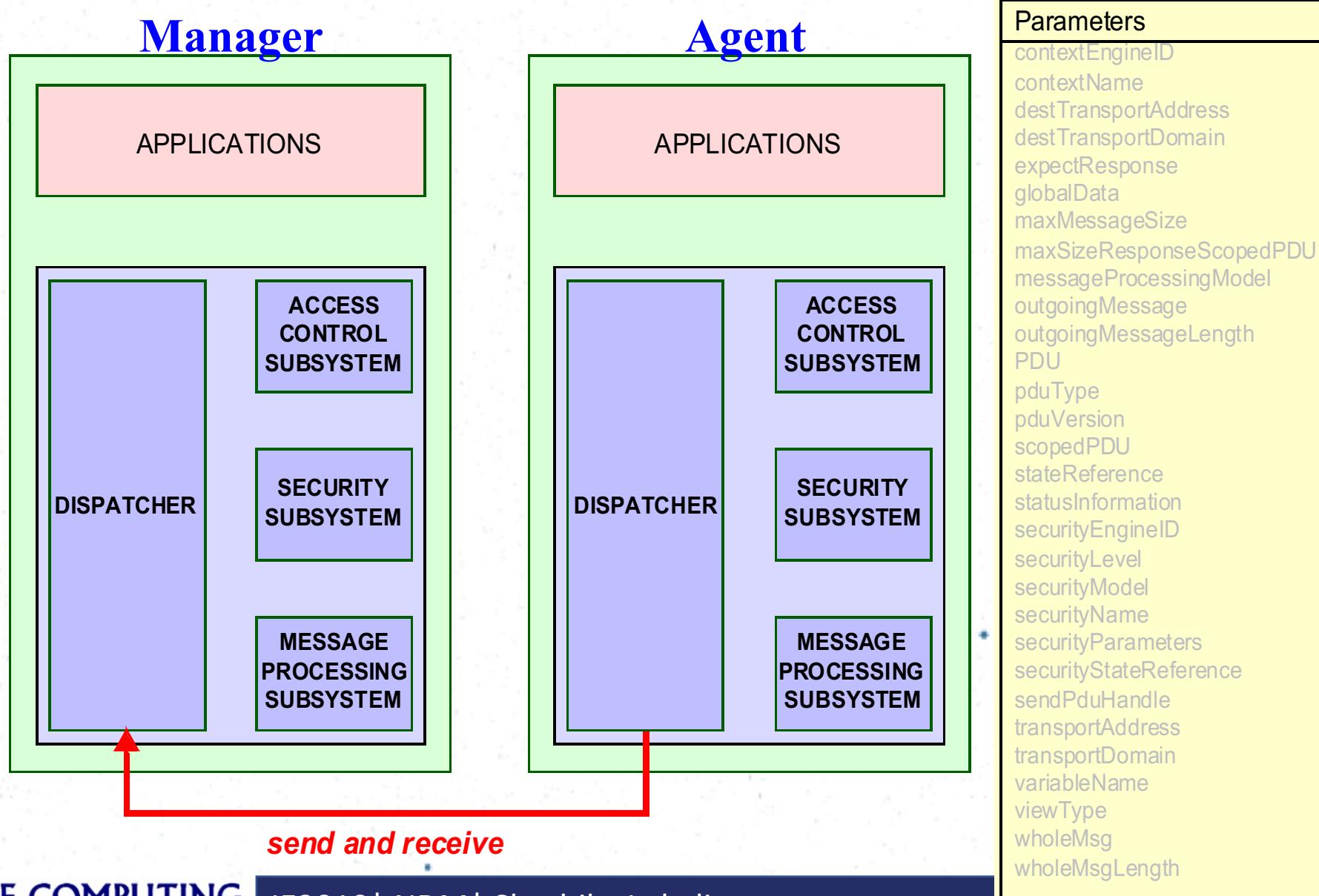
prepareResponseMessage



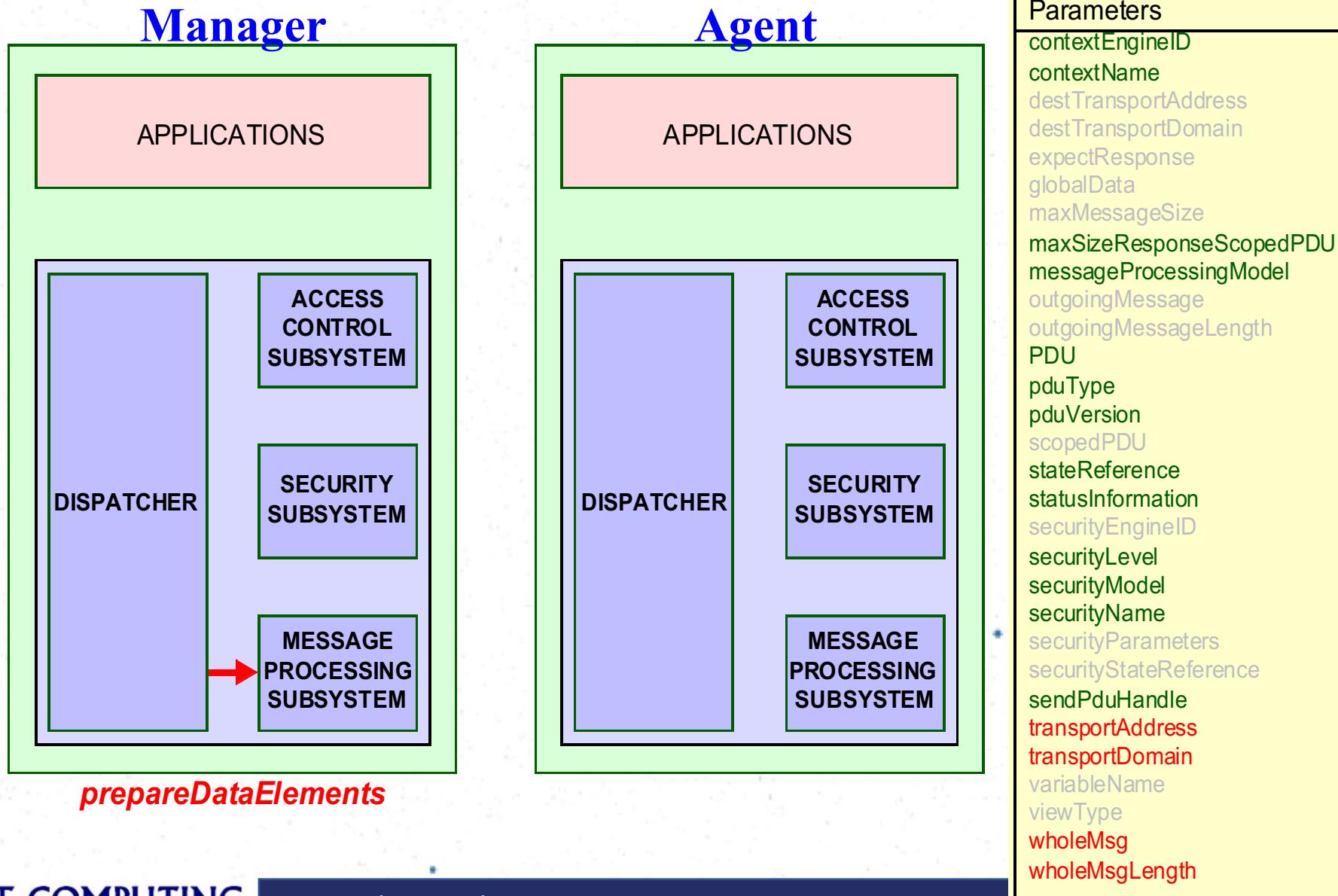
generateResponseMsg



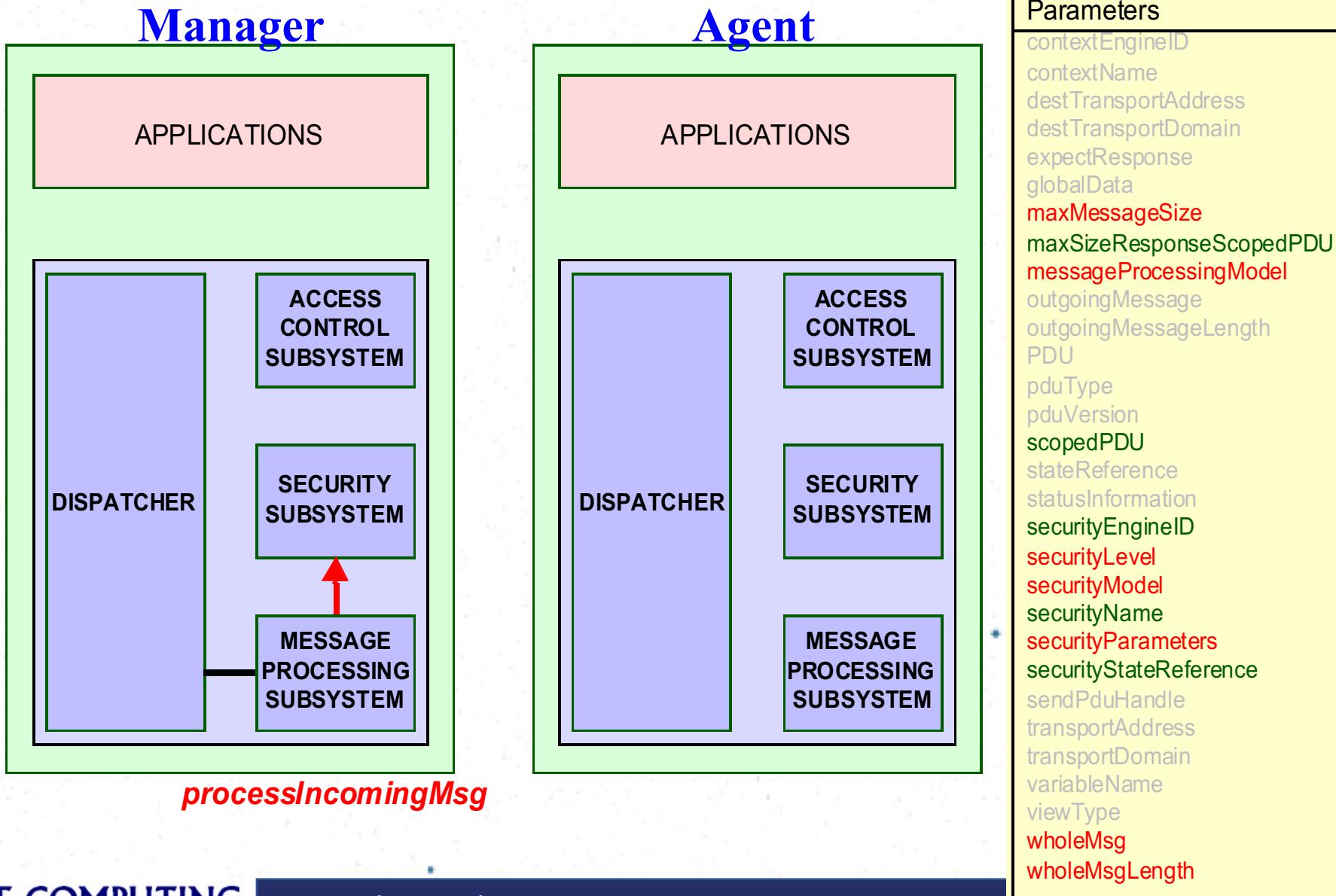
send / receive



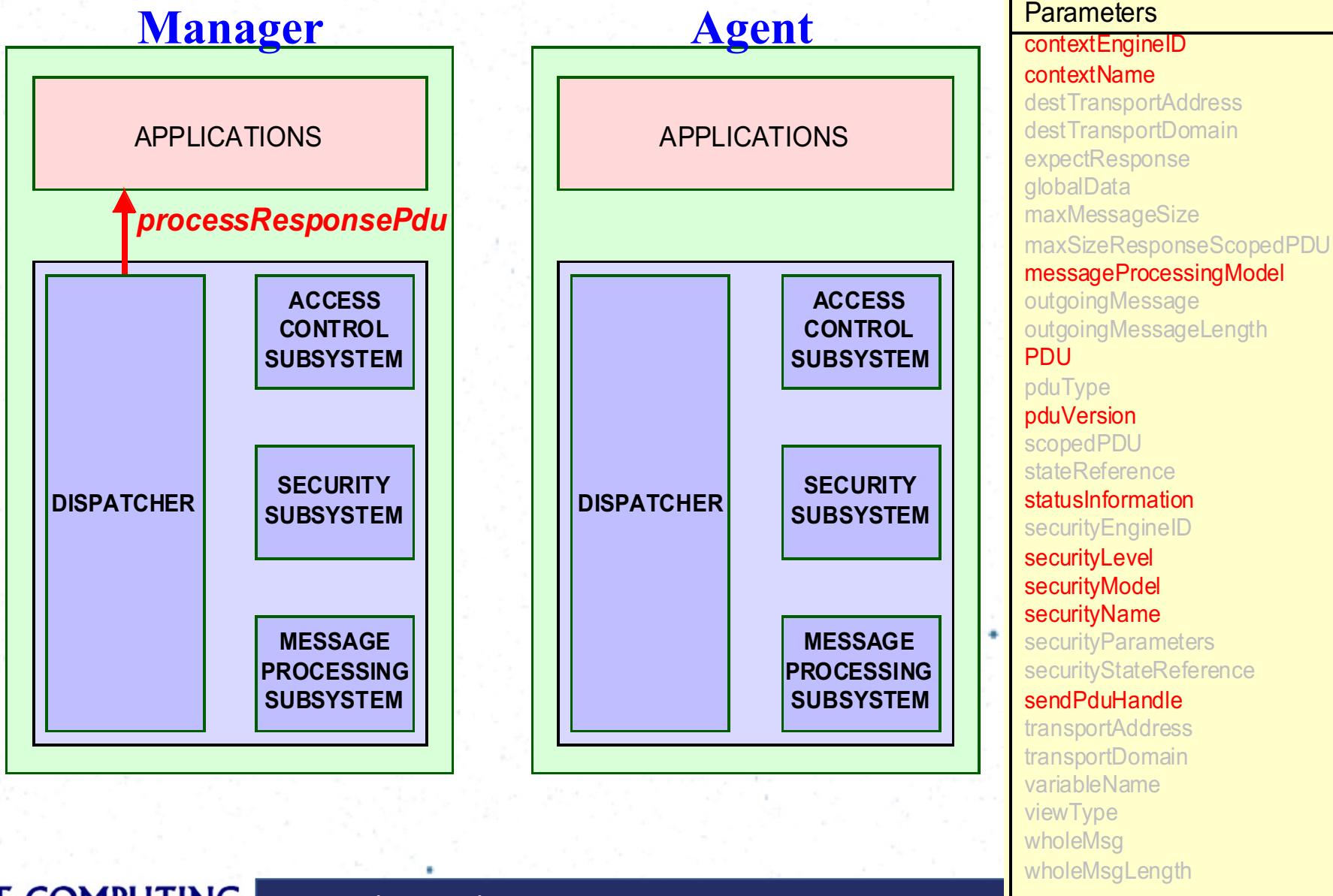
prepareDataElements



processIncomingMsg



processResponsePdu



SNMP RFC's

RFC	Description	Published	Current Status
1065	SMIv1	Aug-88	Obsoleted by 1155
1066	SNMPv1 MIB	Aug-88	Obsoleted by 1156
1067	SNMPv1	Aug-88	Obsoleted by 1098
1098	SNMPv1	Apr-89	Obsoleted by 1157
1155	SMIv1	May-90	Standard
1156	SNMPv1 MIB	May-90	Historic
1157	SNMPv1	May-90	Standard
1158	SNMPv1 MIB-II	May-90	Obsoleted by 1213
1212	SNMPv1 MIB definitions	Mar-91	Standard
1213	SNMPv1 MIB-II	Mar-91	Standard
1215	SNMPv1 traps	Mar-91	Informational
1351	Secure SNMP administrative model	Jul-92	Proposed Standard
1352	Secure SNMP managed objects	Jul-92	Proposed Standard
1353	Secure SNMP security protocols	Jul-92	Proposed Standard
1441	Introduction to SNMPv2	Apr-93	Proposed Standard
1442	SMIv2	Apr-93	Obsoleted by 1902
1443	Textual conventions for SNMPv2	Apr-93	Obsoleted by 1903
1444	Conformance statements for SNMPv2	Apr-93	Obsoleted by 1904
1445	SNMPv2 administrative model	Apr-93	Historic

RFC	Description	Published	Current Status
1448	SNMPv2 protocol operations	Apr-93	Obsoleted by 1905
1449	SNMPv2 transport mapping	Apr-93	Obsoleted by 1906
1450	SNMPv2 MIB	Apr-93	Obsoleted by 1907
1451	Manger-to-manger MIB	Apr-93	Historic
1452	Coexistence of SNMPv1 and SNMPv2	Apr-93	Obsoleted by 1908
1901	Community-Based SNMPv2	Jan-96	Experimental
1902	SMIv2	Jan-96	Draft Standard
1903	Textual conventions for SNMPv2	Jan-96	Draft Standard
1904	Conformance statements for SNMPv2	Jan-96	Draft Standard
1905	Protocol operations for SNMPv2	Jan-96	Draft Standard
1906	Transport mapping for SNMPv2	Jan-96	Draft Standard
1907	SNMPv2 MIB	Jan-96	Draft Standard
1908	Coexistence of SNMPv1 and SNMPv2	Jan-96	Draft Standard
1909	Administrative infrastructure for SNMPv2	Feb-96	Experimental
1910	User-based security for SNMPv2	Feb-96	Experimental

SNMP Security

- SNMPv1 uses plain text community strings for authentication as plain text without encryption
- SNMPv2 was supposed to fix security problems, but effort derailed (The “c” in SNMPv2c stands for “community”).
- SNMPv3 has numerous security features:
 - Ensure that a packet has not been tampered with (**integrity**),
 - Ensures that a message is from a valid source (**authentication**)
 - Ensures that a message cannot be read by unauthorized (**privacy**).



IT3010

Network Design and Management

Special Topics in SNMP

Shashika Lokuliyan

Faculty of Computing
Department of CSE



SLIIT

Discover Your Future

Structure of management information (SMI)

3

Goal of SNMP

Or at least the intention of the inventors...

- A world where a person's audio system, video system, HVAC system and toaster are all connected to the same network.
- To that end, computer scientists developed a protocol capable of managing **any network device**.
- The result was Simple Network Management Protocol (**SNMP**).

Problem 1

- Different software languages have slightly different sets of data types (integers, strings, bytes, characters etc.).
- But an SNMP manager sending a message full of Java data types may not be understood by an SNMP agent written in C.
- The solution for this problem is to use ASN.1 defined data types.
- Since ASN.1 is independent of any particular programming language, the SNMP agent/manager can be written in any programming language.

Problem 2

- When sending a particular data type over the wire, how should it be encoded?
- Should strings be null terminated as in the programming language C, or not? Should Boolean values be 8 bits as in C++ or 16 bits as in VB6?
- To address this problem ASN.1 includes Basic Encoding Rules (BER).
- To send a properly formatted message, the programmer must understand ASN.1 and BER encoding.

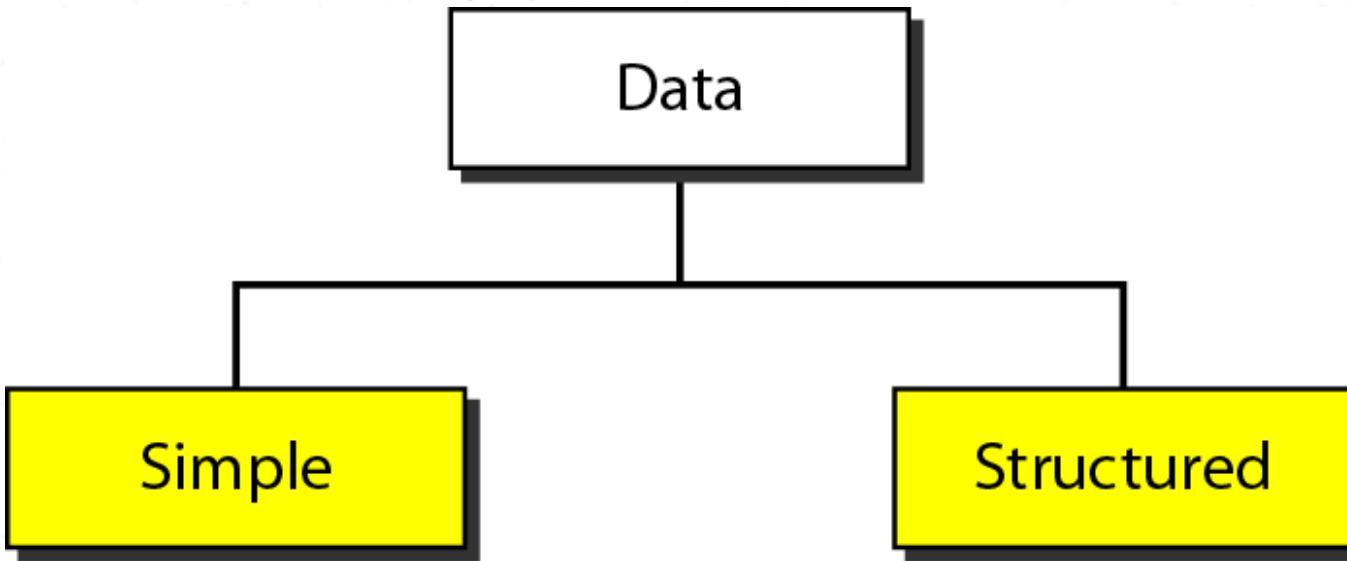
Structure of Management Information (SMI)

- Adapted subset of **ASN.1**
- Structure of Management Information (SMI) is used to define the objects in MIBs.
 - Module definitions
 - MODULE-IDENTITY
 - Object definitions
 - OBJECT-TYPE
 - Notification definitions
 - NOTIFICATION-TYPE

ASN.1

- Abstract syntax notation one
- Formal notation **for describing data structures and message formats**
- Type definitions, value definitions, combined
- Predefined basic types
 - BOOLEAN, INTEGER, OCTET STRING, BIT STRING, REAL, ENUMERATED, CHARACTER STRING, OBJECT IDENTIFIER
- Constructed types
 - SEQUENCE, SEQUENCE OF, CHOICE
 - Arbitrary nesting of types and sub-types
- Encoding

data type



Simple type

Type	Size	Description
INTEGER	4 bytes	An integer with a value between -2^{31} and $2^{31} - 1$
Integer32	4 bytes	Same as INTEGER
Unsigned32	4 bytes	Unsigned with a value between 0 and $2^{32} - 1$
OCTET STRING	Variable	Byte string up to 65,535 bytes long
OBJECT IDENTIFIER	Variable	An object identifier
IPAddress	4 bytes	An IP address made of four integers
Counter32	4 bytes	An integer whose value can be incremented from 0 to 2^{32} ; when it reaches its maximum value, it wraps back to 0.
Counter64	8 bytes	64-bit counter
Gauge32	4 bytes	Same as Counter32, but when it reaches its maximum value, it does not wrap; it remains there until it is reset
TimeTicks	4 bytes	A counting value that records time in $\frac{1}{100}$ s
BITS		A string of bits
Opaque	Variable	Uninterpreted string

Structured Types

Structured Types	Typical Use
SEQUENCE	Models an ordered collection of variables of different type
SEQUENCE OF	Models an ordered collection of variables of the same type
SET	Model an unordered collection of variables of different types
SET OF	Model an unordered collection of variables of the same type
CHOICE	Specify a collection of distinct types from which to choose one type
SELECTION	Select a component type from a specified CHOICE type
ANY	Enable an application to specify the type Note: ANY is a deprecated ASN.1 Structured Type. It has been replaced with X.680 Open Type.

ASN.1 types and values

- **Type definitions**

- NumberofStudents ::= INTEGER
- PassorFail ::= BOOLEAN
- GradeType ::= ENUMERATED {A, B, C}
- PointsScored ::= REAL
- Image ::= BIT STRING
- Data ::= OCTET STRING

- **Value definitions**

- studentsMonaySession
NumberofStudents ::= 9
- NDMCourse PassorFail ::= TRUE
- NumberofStudents ::= 10

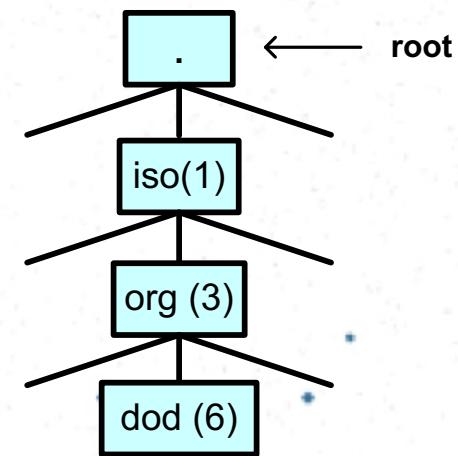
- **Combine type value definitions**

- StudentType ::= INTEGER {
 ugrad (0)
 ms (1)
 phd (2)
}
- NumberofStudents ::= 10

ASN.1 structured types and values

ASN.1 OBJECT IDENTIFIER (MIB)

- Define an information object that is managed at the international level
- internet OBJECT IDENTIFIER ::= { iso(1) org(3) dod(6) }



ASN.1 MACRO (MIB)

provide the capability of defining types and values that are not included in the standard repertoire.

```
OBJECT-TYPE MACRO ::=  
  BEGIN  
    TYPE NOTATION ::= "SYNTAX" type (TYPE  
ObjectSyntax)  
      "ACCESS" Access  
      "STATUS" Status  
    VALUE NOTATION ::= value (VALUE ObjectName)
```

```
Access ::= "read-only"  
        | "read-write"  
        | "write-only"  
        | "not-  
accessible"  
Status ::= "mandatory"  
        | "current"  
        | "optional"  
        | "obsolete"  
END
```

ASN.1 Encoding

- ASN.1 defines syntax and not how to encode them
- ASN.1 encoding rules
 - Basic encoding rules (BER) (will be discuss separately)
 - DER encoding rules (DER)
 - Canonical encoding rules (CER)
 - XML encoding rules (XER)
 - Packet encoding rules (PER)
 - Generic string encoding rules (GSER)

Management Information Base (MIB)

MIB

- A MIB specifies the managed objects
- MIB is a text file that describes managed objects using the syntax of ASN.1
- What is a managed object?
 - interface, TCP stack (RTO, congestion control alg.), ARP etc.
- In Linux, MIB files are in the directory */usr/share/snmp/mibs*
 - Multiple MIB files
 - MIB-II (defined in RFC 1213) defines the managed objects of TCP/IP networks

Managed Objects

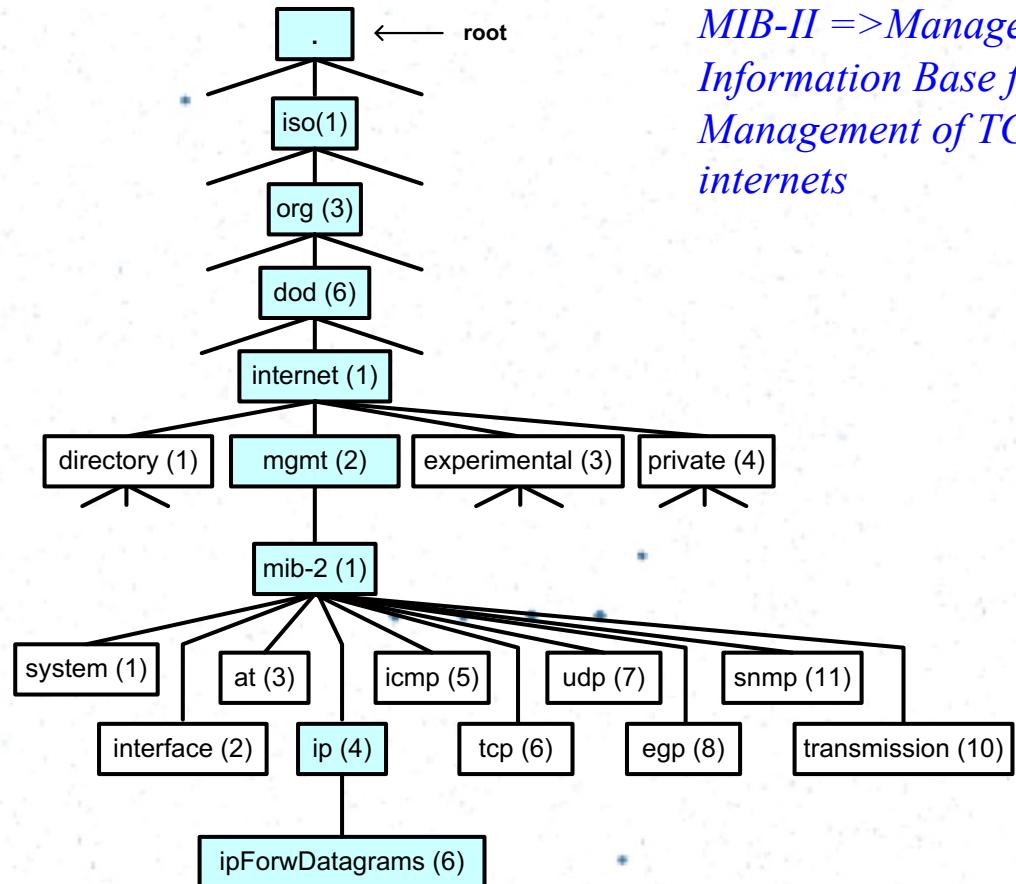
- Each managed object is assigned an *object identifier (OID)*
- The OID is specified in a MIB file.
- An OID can be represented as a sequence of integers separated by decimal points or by a text string:

Example:

- *1.3.6.1.2.1.4.6.*
- *iso.org.dod.internet.mgmt.mib-2.ip.ipForwDatagrams*
- When an SNMP manager requests an object, it sends the OID to the SNMP agent.

Organization of managed objects

- Organized in a **tree-like hierarchy**
- **OIDs reflect the structure of the hierarchy.**
- Each OID **represents a node** in the tree.
- The OID **1.3.6.1.2.1** (*iso.org.dod.internet.mgmt.mib-2*) is at the top of the hierarchy for all managed objects of the **MIB-II**.
- Manufacturers of networking equipment can add product specific objects to the hierarchy.

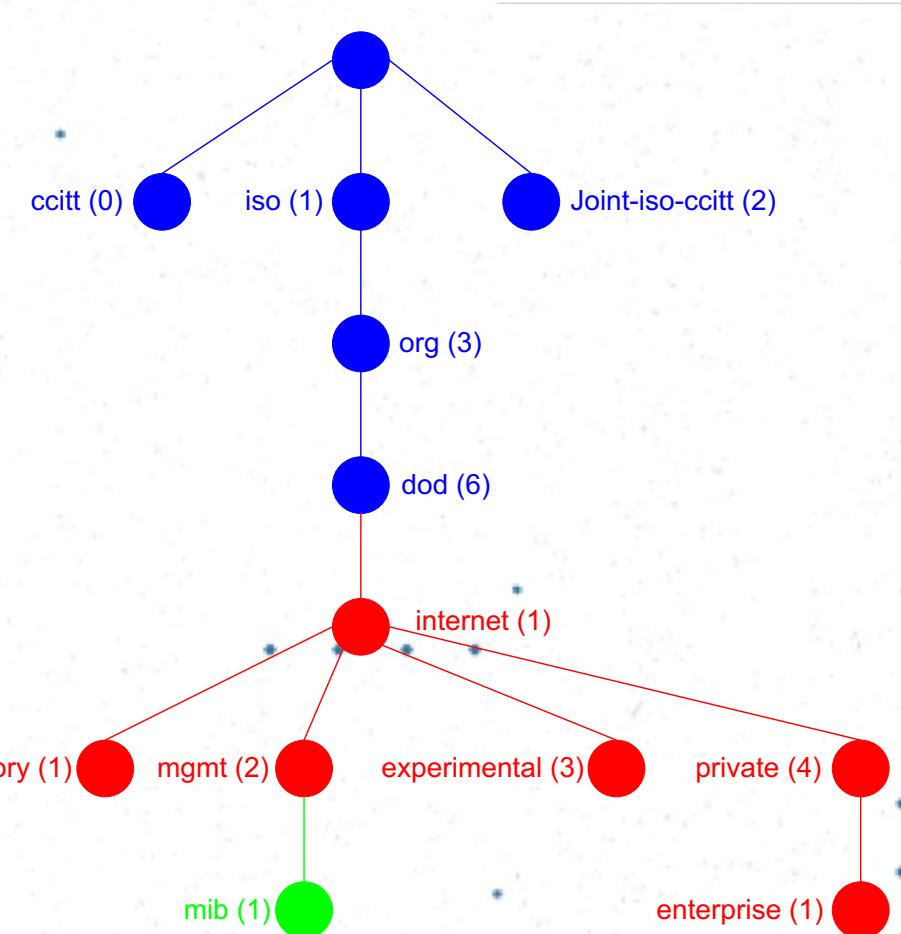


MIB-II => Management Information Base for Network Management of TCP/IP-based internets

Organization of managed objects

RFC 1155 defines **top of the administrative domain managed by the IETF**:

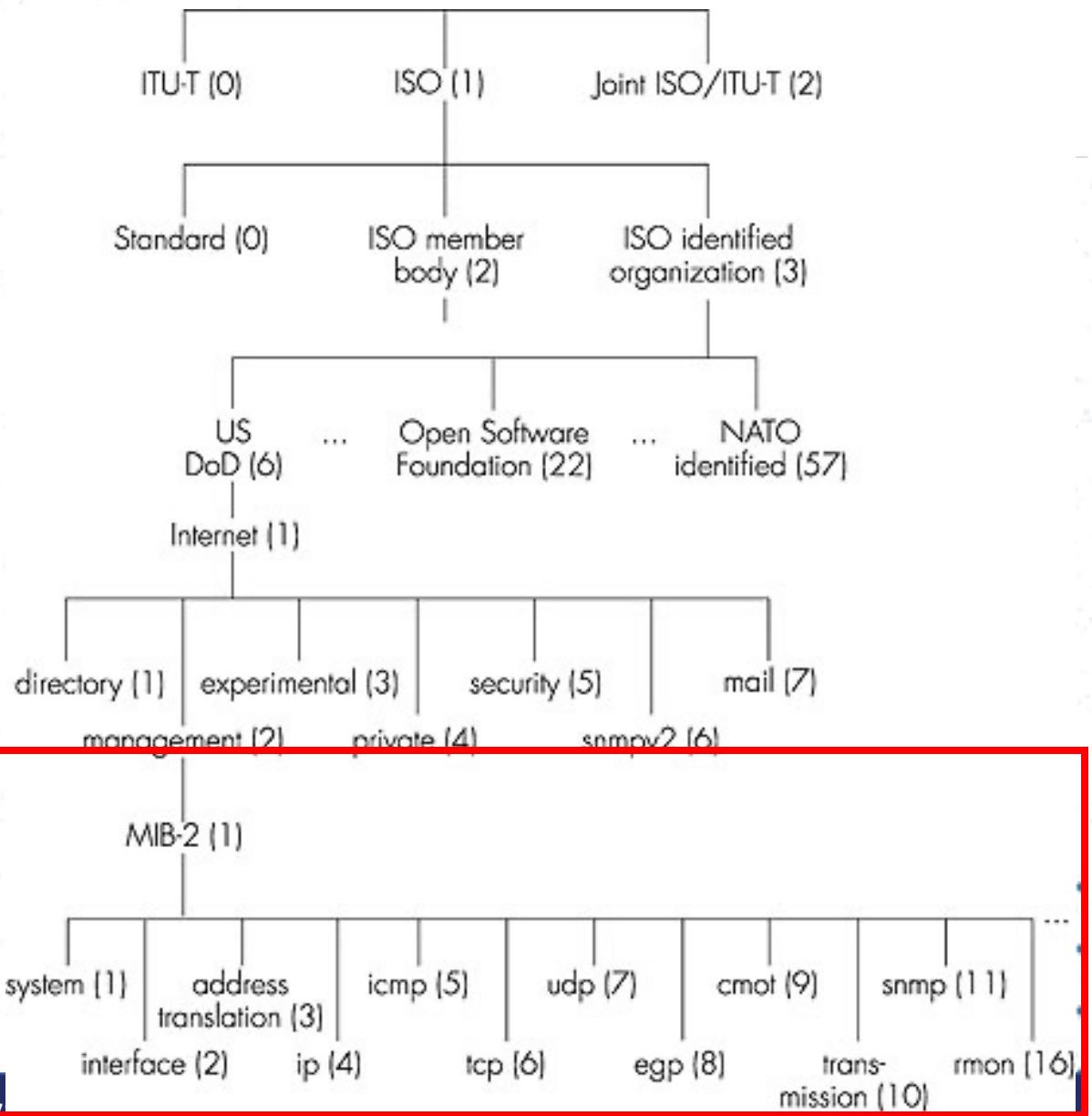
- 1.3.6.1 - Internet
 - ❑ **Directory** – reserved for use with a future memo that discusses how the OSI directory may be used in the Internet.
 - ❑ **Mgmt** – area for items defined in standards track documents.
 - ❑ **Experimental** – area for IETF experimental items.
 - ❑ **Private** – area for delegation of subtrees to **enterprises**, that is, anyone who asks for an enterprise number.



MIB-II (RFC1213)

MIB-II defines **11 separate groups** :

- system (1)
- interfaces (2)
- address translation (3)
- ip (4)
- icmp (5)
- tcp (6)
- udp (7)
- egp (8)
- cmot (9) CMIS over TCP (for historic reasons only)
- transmission (10)
- snmp (11)



System Group

- Contains **data pertaining to the system** where the agent is residing in.
- **Fault management objects:**
 - ❑ **SysObjectID** – System manufacturer.
 - ❑ **sysServices** – Protocol layers that device services, using formula $2^{(L-1)}$.
 - e.g. host that runs transport + application layer services.
 - $2^{(4-1)} + 2^{(7-1)} = 72$.
 - ❑ **sysUptime** – Amount of time system has been operational.
- **Configuration management objects:**
 - ❑ **sysDescr** – Description of the system.
 - ❑ **sysLocation** – System's physical location.
 - ❑ **sysContact** – System's name.

Interfaces Group

- The interfaces group provides information pertaining to each specific network interface (**ifTable**).
- Useful for configuration, performance, fault and accounting management.
- **ifNumber** - number of interfaces.
- **ifTable** example:

ifIndex	ifDescr	ifOperStatus	ifInUPackets	ifSpeed
0	DEC Ethernet 1	1	8169	8000000
1	SUN Ethernet 1	2	16184	100000

Interfaces Group cont.

Example – Determining Utilization

Total bytes = $(\text{ifInOctects}_y - \text{ifInOctects}_x) + (\text{ifOutOctects}_y - \text{ifOutOctects}_x)$

Total bytes per sec = Total bytes / (y-x)

Utilization = (Total bytes per sec * 8) / ifSpeed

IP Group

- Provides information about the IP layer in a systems network protocol stack.
 - Information pertaining to errors and types of packets seen.
 - Routing table (i.e. `ipRouteTable`).
- Configuration/Fault management objects:
 - `ipForwarding` – If device is set up to route IP packets.
 - `ipAddrTable` – Addresses on the device.
 - `ipRouteTable` – Routing table.
- Performance management objects:
 - `iplnDiscards` – Rate of input datagrams discarded.
 - `iplnHdrErrors` – Rate of input header errors.
 - `iplnAddrErrors` – Rate of input address errors.
- Accounting management objects:
 - `ipOutRequests` – Number of IP datagrams sent.
 - `iplnDelivers` – Number of IP datagrams received.

ICMP Group

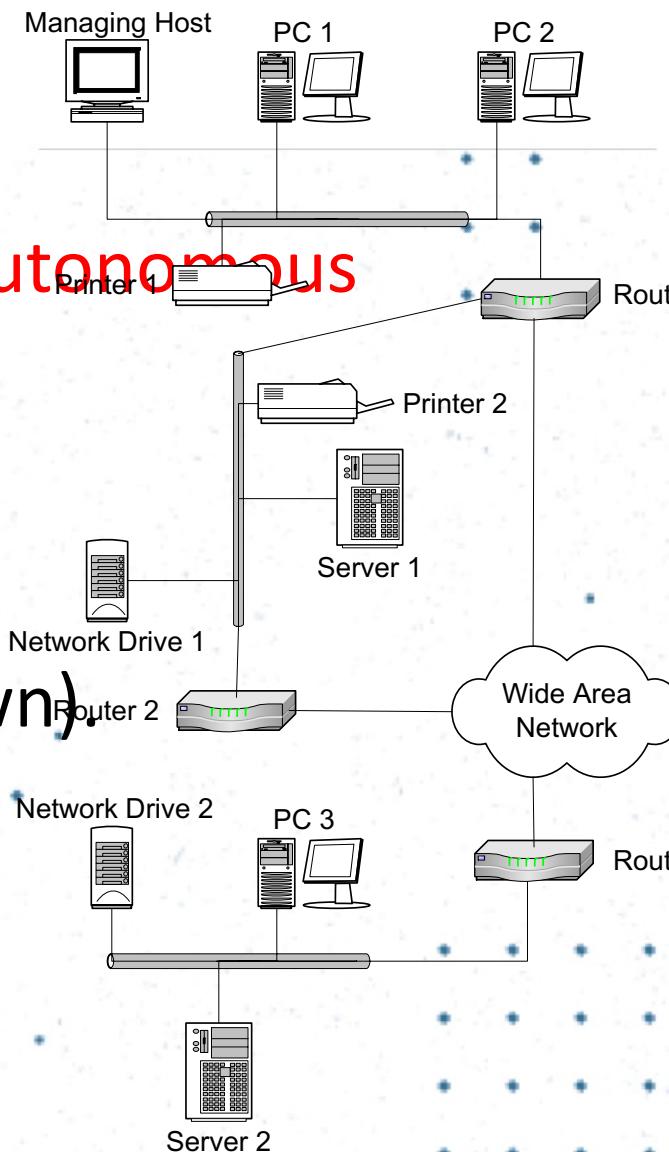
- Provides information pertaining to systems ICMP entity.
 - ❑ `icmpInRedirects` – rate of redirect messages received.
 - ❑ `icmpOutDestUnreachs` – rate of destination unreachable errors sent.
 - ❑ `icmpInSrcQuenches` – input rate of source quench messages (source quench msgs – requests that the sender decrease the rate of messages sent to a router or host).
 - ❑ `icmpOutEchos` – rate of output echo messages.
- Mainly useful for performance management.

TCP Group

- TCP – The Transmission Control Protocol (TCP) provides reliable transport services between applications (UDP is the unreliable transport service).
- Configuration management objects:
 - `tcpRtoAlgorithm` – Retransmission algorithm.
 - `tcpConnTable` – Connection table (i.e. `netstat`).
- Performance management objects:
 - `tcpAttemptFails` – Number of failed attempts to make a connection.
 - `tcpEstabResets` – Number of resets in established connections.
- Accounting management objects:
 - `tcpActiveOpens` – Number of times this system has opened a connection.
 - `tcpInSegs` – Number of TCP segments received.
- Security management objects:
 - `tcpConnTable` – Connection table (i.e. `netstat`).
- The User Datagram Protocol (UDP) group provides similar information. (e.g. `udpTable`)

EGP Group

- EGP (RFC 904) is a protocol that tests for the reachability of IP networks.
 - An IP network can be divided into networks of **autonomous systems**.
- **egpNeighTable** – information about this entity's EGP neighbors.
- **Fault management** objects:
 - **egpNeighState** – state of EGP neighbour (up,down).
- **Configuration management** objects:
 - **egpIntervalHello** – hello message interval.
 - **egpAs** – local EGP autonomous system.



Transmission Group

- Reserved for **information pertaining to specific media** underlying the interfaces of a system.
- Various RFCs:
 - RFC 1512 FDDI.
 - RFC 1493 Bridge.
 - RFC 1743 Token Ring.

SNMP Group

- Management protocols also need to be managed...!!!
 - Useful to all 5 areas of network management.
- Fault management objects:
 - **snmplnASNParseErrors** – Number of malformed SNMP messages.
 - **snmplnNoSuchNames** – Number of requests to invalid objects.
- Configuration management objects:
 - **EnableAuthenTraps** – Enables entity to send traps when authentication errors occur.
- Performance/Accounting management objects:
 - **snmplnPkts** – Rate of SNMP packets input.
 - **snmplnTraps** – Rate of traps input.
- Security management objects:
 - **snmplnBadCommunityNames** – Number of authentication failures.
 - **snmplnBadCommunityUses** – Number of requests without sufficient privileges.

Definition of managed objects in a MIB

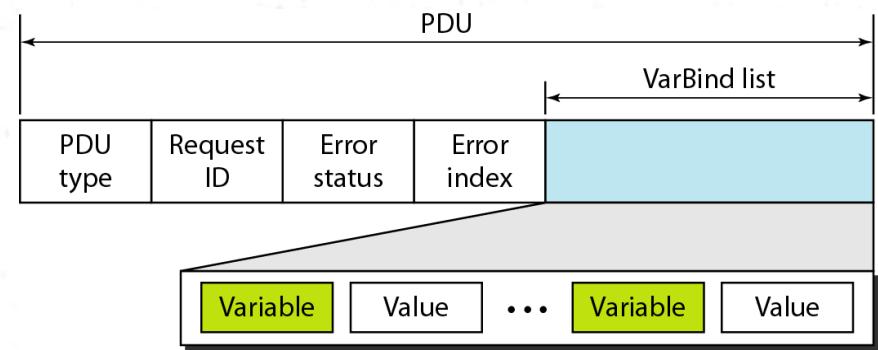
- Specification of **ipForwDatagrams** in MIB-II.

```
ipForwDatagrams OBJECT-TYPE
    SYNTAX  Counter
    ACCESS  read-only
    STATUS   current
    DESCRIPTION
        "The number of input datagrams for which this
        entity was not their final IP destination, as a
        result of which an attempt was made to find a
        route to forward them to that final destination.
        In entities which do not act as IP Gateways, this
        counter will include only those packets which were
        Source-Routed via this entity, and the Source-
        Route option processing was successful."
    ::= { ip 6 }
```

BER encoding

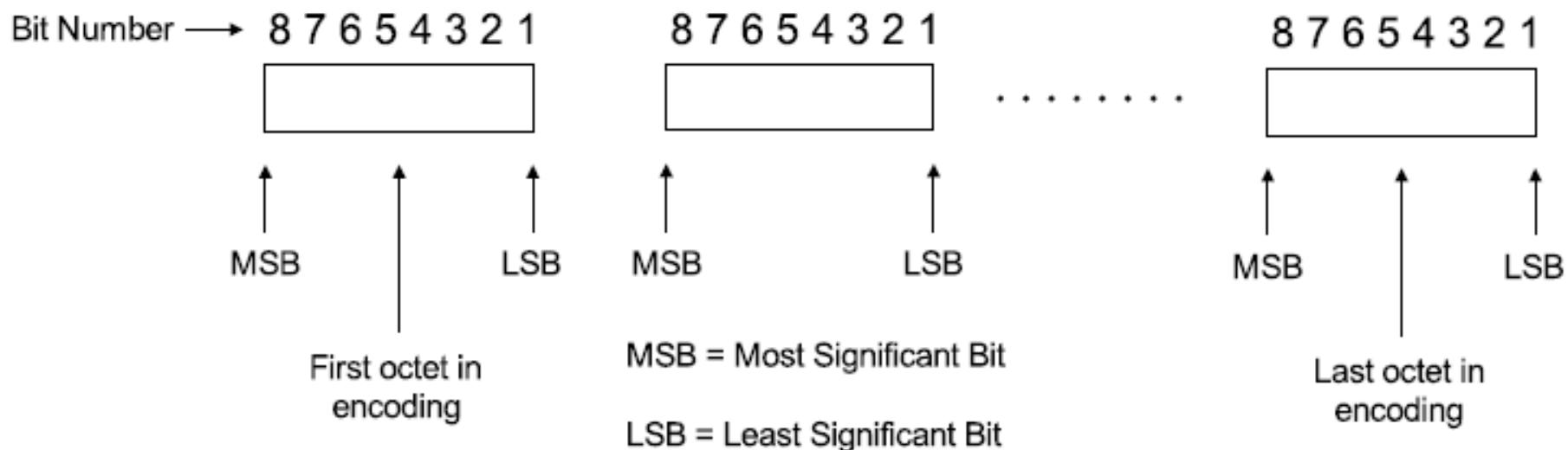
Format of a BER encoded message

- In BER encoding, the most fundamental rule states that each field is encoded in three parts:
 - Type (or Tag)
 - Length
 - Value
- Hence, this is also known as TLV encoding.



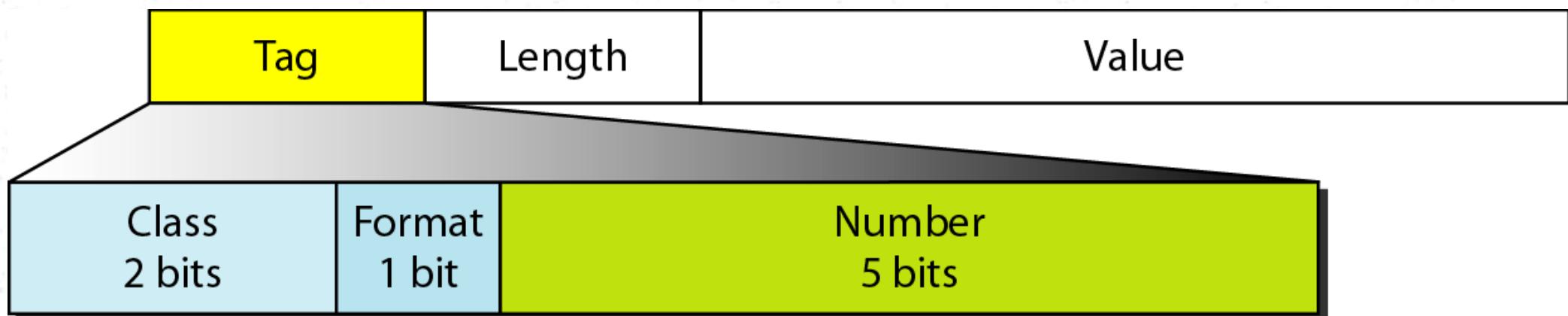
Format of a BER encoded message cont..

- Like in most protocols, in BER also the Most Significant Bit (MSB)/Octet is encoded on the left.



Type/Tag format

- Every BER encoded ASN.1 data type has a type field.
- This type can be one of four classes which is indicated by the first two bits of the type octet.



Data Type : class

Class	Bit 8	Bit 7	
Universal	0	0	Primitive/ Constructed types
Application	0	1	Primitive SNMP application types
Context-specific	1	0	...
Private	1	1	SNMP PDU types

Class
2 bitsFormat
1 bitNumber
5 bits

ASN.1 Primitive Types

Data Type	Class	Format	Number	Type/Tag (Binary)	Type/Tag (Hex)
BOOLEAN	00	0	00001	00000001	01
INTEGER	00	0	00010	00000010	02
BIT STRING	00	0	00011	00000011	03
OCTET STRING	00	0	00100	00000100	04
NULL	00	0	00101	00000101	05
OBJECT IDENTIFIER	00	0	00110	00000110	06

Class
2 bitsFormat
1 bitNumber
5 bits

ASN.1 Constructed Types

Data Type	Class	Format	Number	Type/Tag (Binary)	Type/Tag (Hex)
SEQUENCE and SEQUENCE OF	00	1	10000	00110000	30

Class
2 bitsFormat
1 bitNumber
5 bits

Primitive SNMP Application Types

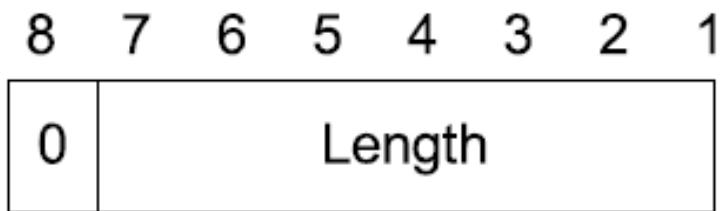
Data Type	Class	Format	Number	Type/Tag (Binary)	Type/Tag (Hex)
IpAddress	01	0	00000	01000000	40
Counter (Counter32)	01	0	00001	01000001	41
Gauge (Gauge32)	01	0	00010	01000010	42
TimerTicks	01	0	00011	01000011	43
Opaque	01	0	00100	01000100	44
NsapAddress	01	0	00101	01000101	45
Counter64	01	0	00110	01000110	46
UInteger32	01	0	00111	01000111	47



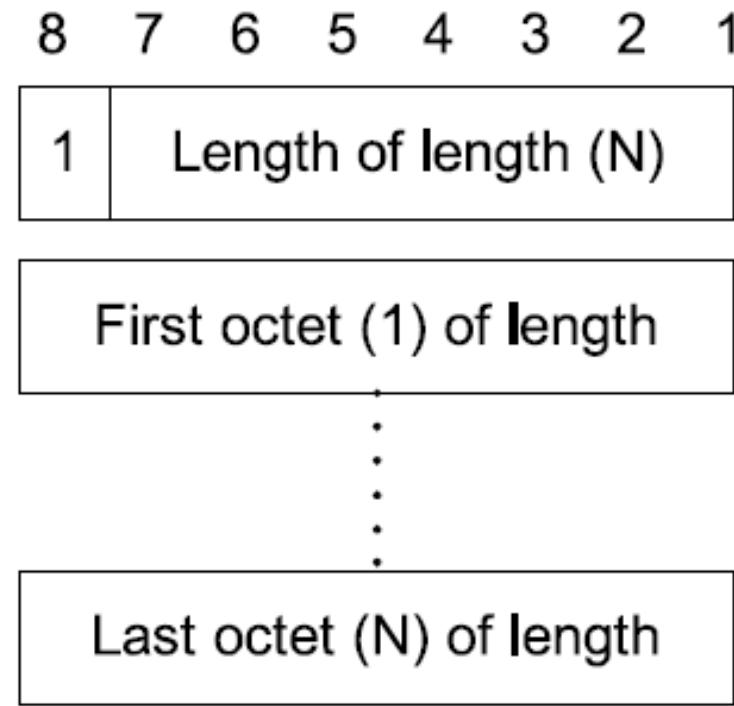
Context Specific SNMP PDU Types

Data Type	Class	Format	Number	Type/Tag (Binary)	Type/Tag (Hex)
GetRequest	10	1	00000	10100000	A0
GetNextRequest	10	1	00001	10100001	A1
Get/Response	10	1	00010	10100010	A2
SetRequest	10	1	00011	10100011	A3
Trap	10	1	00100	10100100	A4
GetBulkRequest	10	1	00101	10100101	A5
InformRequest	10	1	00110	10100110	A6
SNMPv2 Trap	10	1	00111	10100111	A7

Length format

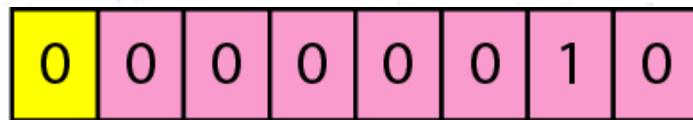


Short Form

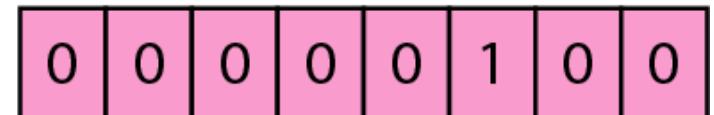
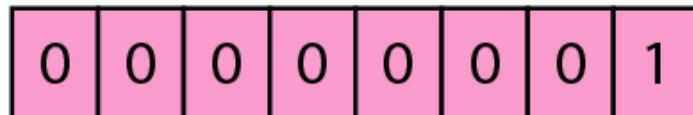
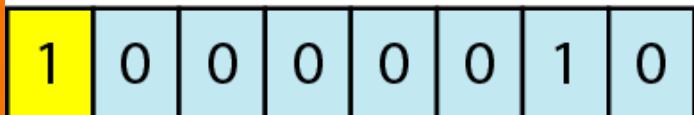


Long Form

Length format



a. The colored part defines the length (2).



b. The shaded part defines the length of the length (2 bytes);
the colored bytes define the length (260 bytes).

Value Format

- How to define an integer value;
- *integer INTEGER ::= 14*

02	04	00	00	00	0E
00000010	00000100	00000000	00000000	00000000	00001110
Tag (integer)	Length (4 bytes)	Value (14)			

Value Format

- How to define a string value;
- *Octetstring OCTET STRING ::= 'HI'*

04	02	48	49
00000100	00000010	01001000	01001001
Tag (String)	Length (2 bytes)	Value (H)	Value (I)

Value Format

- How to define a null value;

ASN.1

null NULL ::= NULL

BER

null

T
05

L
00

V
Empty

Value Format

- *How to define ObjectIdentifier 1.3.6.1 (iso.org.dod.internet).*

06	04	01	03	06	01
00000110	00000100	00000001	00000011	00000110	00000001
Tag (Objectld)	Length (4 bytes)	Value (1)	Value (3)	Value (6)	Value (1)

← 1.3.6.1 (iso.org.dod.internet) →

Encoding OBJECT IDENTIFIER

- Two rules apply when encoding OIDs using BER.
- The first rule states that, the first two numbers 'x.y' of the OID are encoded as a single value using the formula $(40*x)+y$.
- The first two numbers of any SNMP related OID is always 1.3. Therefore the first two numbers of an SNMP related OID is always encoded as 43 or 0x2B, because $(40*1)+3 = 43$.

Encoding OBJECT IDENTIFIER

- Second rule applies when encoding large numbers in OIDs that cannot be represented using one octet (i.e. one byte or 8 bits).
- For example, the OID 1.3.6.1.4.1.2680.1.2.7.3.2 contains 2680 which cannot be encoded using a single octet (since 8 bits can only represent 0-255).
- The rule indicates that, when encoding large numbers in OIDs, only the lower 7 bits of the octet are used for holding the actual value (0-127). The highest order bit is used as a flag to indicate that this number spans more than one byte.

Encoding OBJECT IDENTIFIER

- According to the rule discussed for large numbers in OIDs, value of 2680 will be encoded as 0x8A 0x78.
- And the fully BER encoded value for OID 1.3.6.1.4.1.2680.1.2.7.3.2 will be,

T	L	V
06	0C	2B 06 01 04 01 8A 78 01 02 07 03 02

Value Format

- How to define IPAddress 131.21.14.8

40	04	83	15	0E	08
01000000	00000100	10000011	00010101	00001110	00001000
Tag (IPAddress)	Length (4 bytes)	Value (131)	Value (21)	Value (14)	Value (8)

← 131.21.14.8 →

Value Format

- How to define SEQUENCE or SEQUENCE OF

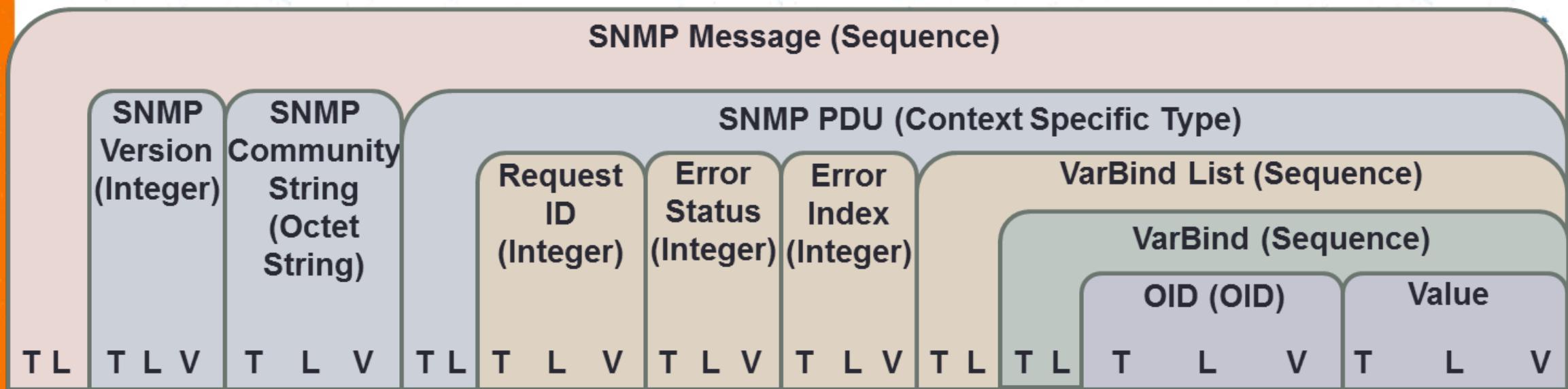
ASN.1

Temperature-each-day SEQUENCE (3) OF INTEGER
::= { 21, 15, -2}

BER

Temperature-each-day:	T	L	V				
	30	9		T	L	V	
				02	01	15	
				02	01	0F	
				02	01	FE	
							⋮ ⋮ ⋮ ⋮

BER encoded format of a SNMP message



You must remember this format...!!!

How to organize the decoded values

Tag (SNMP Message), Length,
Tag, Length, Version
Tag, Length, Community
Tag (PDU Type), Length
Tag, Length, Request ID
Tag, Length, Error Status
Tag, Length, Error Index
Tag (VarBind List), Length
Tag (VarBind), Length
Tag, Length, OID
Tag, Length, Value

Let's try an example

30 2B 02 01 00 04 08 53 65 63 75 72 69 74 79 A1 1C 02 04 3B 0B 16 36 02 01 00 02
01 00 30 0E 30 0C 06 08 2B 06 01 02 01 01 02 00 05 00

30 2B	=> SEQUENCE
02 01 00	=> INTEGER 0
04 08 53 65 63 75 72 69 74 79	=> OCTET STRING Security
A1 1C	=> Context Specific 1 Constructor
02 04 3B 0B 16 36	=> INTEGER 3B0B1636
02 01 00	=> INTEGER 0
02 01 00	=> INTEGER 0
30 0E	=> SEQUENCE
30 0C	=> SEQUENCE
06 08 2B 06 01 02 01 01 02 00	=> OBJECT IDENTIFIER
05 00	=> NULL

Example cont..

SEQUENCE => SNMP Message

INTEGER 0 => Version 0 (SNMPV1)

OCTET STRING Security => Community String

Context Specific 1 Constructor => GetNextRequest

INTEGER 3B0B1636 => Request ID (aka Sequence #)

INTEGER 0 => Error Status

INTEGER 0 => Error Index

SEQUENCE => VarBind List

SEQUENCE => VarBind

OBJECT IDENTIFIER => 1.3.6.1.2.1.1.2.0

NULL => Empty value

Try this by yourself...

- 30 2F 02 01 00 04 08 53 65 63 75 72 69 74 79 A2 20
02 04 3B 0B 16 36 02 01 00 02 01 00 30 12 30 10 06
08 2B 06 01 02 01 01 03 00 43 04 1B E1 55 80

~ THE END ~

SNMP Operations

SET Request

Initializes or changes the value of a network element.

GET Request

Sent by manager requesting data from agent.

GETNEXT Request

Sent by manager requesting data on the next managed object to the one specified.

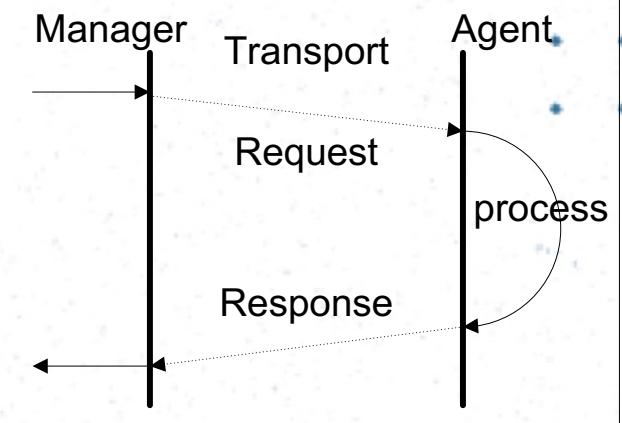
GET Response

Used by the agent to respond with data to get and set requests from the manager.

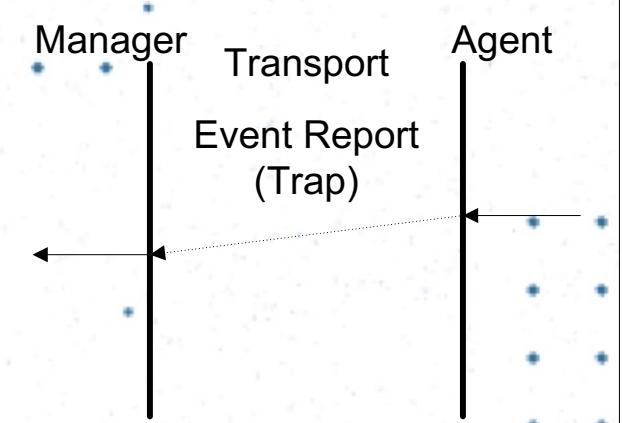
Trap

Alarm generated by agent.

Request/Response Messages



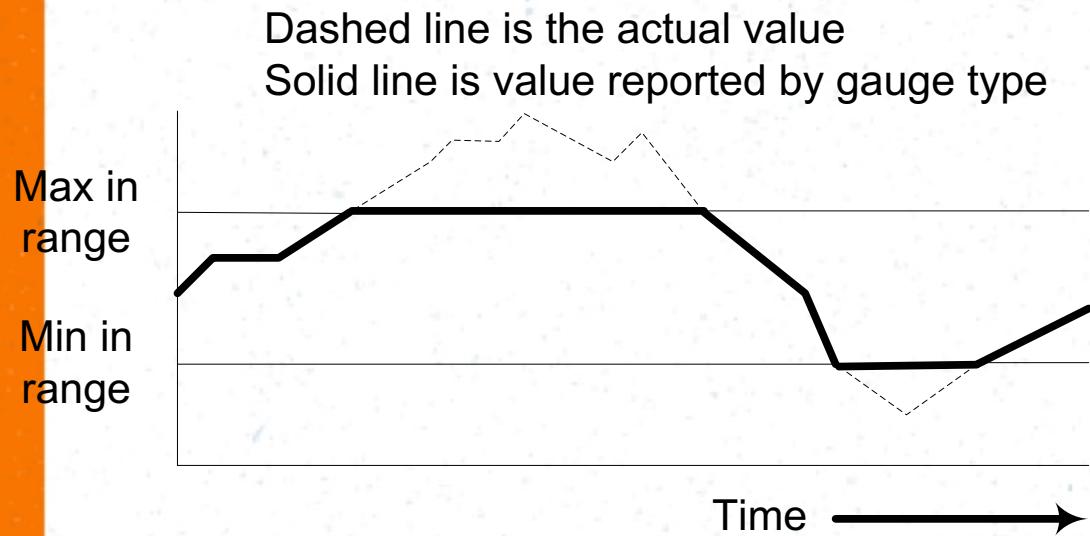
Trap Messages



SMI (RFC1155) Defined Data Types

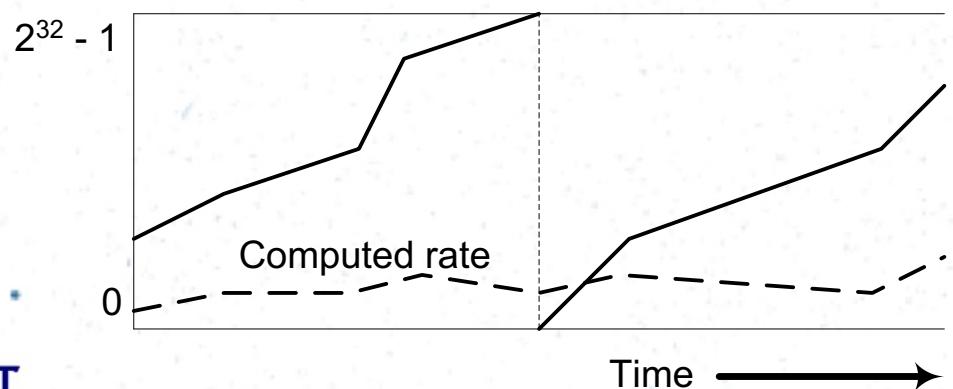
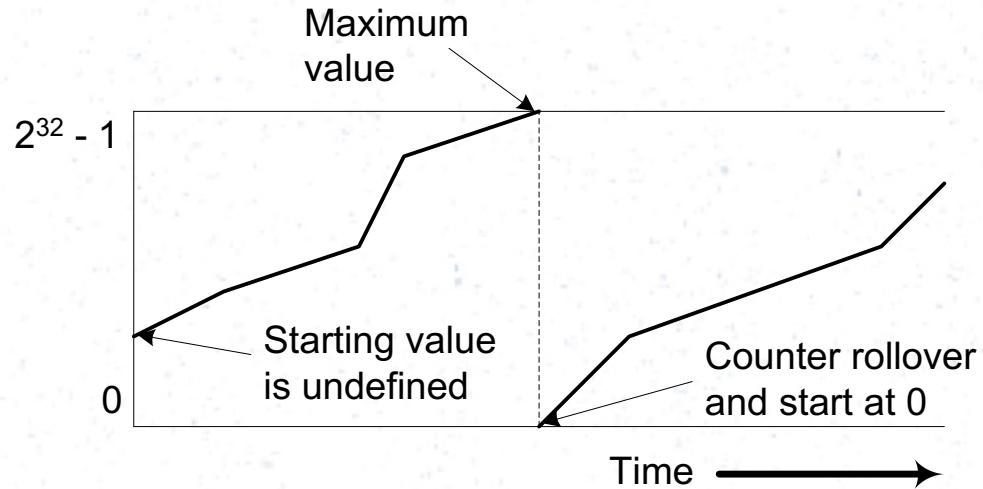
- Integer – Signed 32-bit integer.
 - Enumerated Integer.
- Octet String – String of bytes.
- Object Identifier.
- [NetworkAddress](#) – An address from one of possibly several protocol families.
- [IpAddress](#) – 32 bit IP address.
- [Gauge](#) – Non-negative integer from 0 to $2^{32} - 1$, which may increase or decrease.
- [Counter](#) – Non-negative monotonically increasing integer from 0 to $2^{32} - 1$.
- [Timeticks](#) – Non-negative integer which counts time in hundredths of a second.
- [Opaque](#) – Arbitrary syntax.

Gauge



- Used to specify a value whose range includes only **non-negative 32 bit integers**.
- RFC 1155 – *this application-wide type represents a non-negative integer, which **may increase or decrease**, but which **latches at a maximum value**.*

Counter



- Use to specify a non-negative value whose range includes only **positive 32-bit integers**.
- Values reported by counters are **not absolute**, since the **count is not required to start at 0 and the count may roll over**.
- Counters are used by obtaining a value v_0 at t_0 and then later obtaining a value v_1 at t_1 .

□ Difference between v_0 and v_1 is the count over the time period.

□ Counter rollover can be detected iff $v_0 > v_1$.

Other Types

- **Timeticks** — used to specify a non-negative value whose range includes only non-negative integers.
 - Units are in hundredths of seconds.
 - Length of time between rollovers is 497 days.
- **Network Address** – used to specify a string of 4 octets.
 - Currently used to store IPv4 addresses.
 - Was designed to allow a network address of any type to be specified.
 - **Obsolete – use IpAddress.**
- **Opaque** – used to specify octets of binary information.
 - Generic type.

ASN.1 Examples (MIB)

- RFC 1155
- internet OBJECT IDENTIFIER ::= { iso org(3) dod(6) 1 }
 - 1.3.6.1.
- Counter ::= [APPLICATION 1] IMPLICIT INTEGER (0..4294967295)
- TimeTicks ::= [APPLICATION 3] IMPLICIT INTEGER (0..4294967295)
- IpAddress ::= [APPLICATION 0] IMPLICIT OCTET STRING (SIZE (4))
- NetworkAddress ::= CHOICE { internet IpAddress }