

## Slide#1

### 1. Enterprise Application ?

Data consistency, access concurrency, polymorphism  
Reliability, Availability and Scalability  
Authorization, Authentication and Accounting

### 2. Enterprises? *the open group architecture framework* TOGAF--> organization having common set of goals

### 3. Why need enterprise architecture?

Business efficiency  
IT operational efficiency  
Better return on investment, reduce risk

### 4. Operating System (MAC OS, windows, Linux..)

OSGi: open gateway service initiative

### 5. Administration Tools (Ansible, Nagios)

### 6. Virtualization: *Bare metal, docker, hardware assisted, software virtual* *NFV network function virtualization*

### 7. Application Framework

community based resilience analysis      Simple Object Access Protocol  
Legacy client/server framework: COBRA, SOAP, REST...  
Modern: KARAF, KUBERNATES, HADOOP, MESOS  
App container: OSGi ; containerized appl. framework      representational state transfer

### 8. Groupware-->collaborative software

CRM customer relation management

### 9. SW development process and model

Continuous delivery  
Agile vs Waterfall  
SCRUM  
Tools: Git, ANT/maven, jenkins

ERP enterprise resource planning

### 10. Databases and Query Language

RDBMS vendors: MySQL, Oracle, Informix  
Major noSQL types: graph, document store, object...  
Major noSQL database: MongoDB, Redis (most popular key-value store)

### 11. Enterprise messaging and transaction

Ent. Message Bus  
Messaging Framework and Integration Platform: Apache Camel, Kafka, java Message service, Mule

### 12. Business Intelligence and Ent. Management Tools

Languages: Scala, Wolfram  
Data mining and Ent Analytic Tool: tableau, splunk,...  
Contiv: container networking

*data analysis*

### 13. Enterprise Cloud and Security

Cloud Service Model (XaaS-anything as a service)  
Cloud Vendor(Google, Akamai, AWS, Microsoft)

RPC: remote procedure call

International organizations for standardization

14. Ent. Standard open system interconnection  
 ISO/OSI  
 IEEE, IETF internet engineering task force

15. TOGAF EA framework enterprise architecture

Cisco's ACI (SDN)  
 ↓ application centric infrastructure  
 Ieee -institute of electronics and electrical  
 engineers  
 SOA service oriented architecture

Slide#2

1.OS

system software-->manage hardware and provide services to user programs

2.OS structure

Early OSes: monolithic

Two mode of executions: user mode and privilege mode

Trap: invoking kernel mode from user code

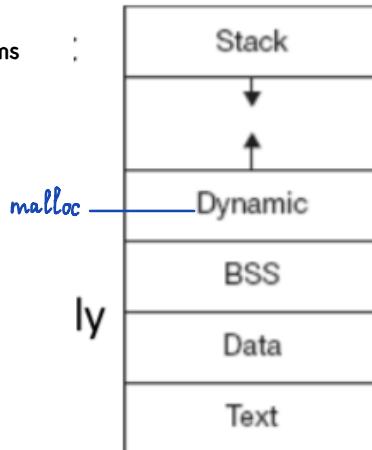
Interrupts: request for a response from processor

3.Process, address space and thread

Text--> code

Dynamic-->Malloc

BSS--> block started by symbol/uninitialized data



4.Type of OS

Single, Multiuser, Distributed, Templatized (VM, container), Lightweight, Embedded

5.Compute Platform

Mainframe, Micro, Mini, Virtualized, Hyper-converged, White-box

6.Three classes of Integrated Systems

Integrated Stack System (ISS): Hardware integrated with application software

Integrated infrastructure System (IIS): hardware integrated to provide shared computer infrastructure

Hyper-converged integrated system (HCIS):

7.VCE (Vblock) *Virtual Computer Environment*

Vblock: VCE HCIS product family

Virtual Computing Environment-->data center machines with virtual desktop infrastructure

8. NetApp Flexpod

Reference Architecture for server, storage and networking components-->work together as an integrated infrastructure stack.

Includes NetApp FAS storage and Cisco's switches,...

9.Converged Infrastructure-CISCO UCS

Unified Computing System--> data center server computer consisting of computing hardware, virtualization support,...

10. Hyper-Converged

Nutanix

## Cisco Hyperflex

### 11. Remote Management

CIMC, DRAC, iLOM, RMM, iLO

Common functions: reset server, power up server, remote console, mount remove physical CD, access server's integrated management log

KVM: kernel based virtual machine—>turning linux kernel into hypervisor

### 12. Linux

RedHat, CentOS, Ubuntu/Debian, SUSE

BSD/Berkeley SW distribution: used for OS X and iOS

Ubuntu: Debian based by Canonical

SUSE: for server, mainframes, popular in Europe

Unix INIT: being phased out, replaced by systemd

GNU-->free software distribution

### 13. Mac OS

Built on NeXT

### 14. OS services/ top level

Directory Services, OS, VPN, Patching, Web services,...

### 15. Windows Active Directory ?

--> services running on Windows server to manage permission and access to network resources

Store data as objects-categorized

Consists of: Domain Services, Federation Services, Certificate Services, Right Management and Lightweight directory services

Security: Log-in authentication and access control

Include: Scheme (rules for classes and objects), global catalog (info about every object), query and index mechanism, replication service (distribution of data over network)

Main service is Domain Service: storing directory information and handle interaction of user with domain

### 16. AD DS: a phone book making the info available/ directory service

scalable, centralized management,...

### 17. AD CS (cert services)

Public Key infrastructure

Managing digital cert.

### 18. AD FS

facilitating cross-organization access of system and info

Single Sign On

Microsoft's WS Federation Passive Requestor Profile protocol

implements SAML

### 19. AD RMS

Safeguard digital info

Allow specifying access permission to certain documents, prevent unauthorized access

## 20. AD LDS?

provide support for directory-enable apps without required dependencies for AD DS

LDAP

AD LDS users and groups: administrators, readers, users and instances

## 21.SAML Security Assertion Markup Language

XML based standard for authentication and authorization exchanging between security domains

## 22. How web services interact?

2 ways:

Choreography ?

Know what do do in real time

Decisions made individually between individual web services

No single controlling entity

Ex: routing

Orchestration

Telling others what to do

Used for service within a domain

One entity controlling others

Ex: SDN

## 23. File System

Types:

Local FS (Disk...)

Network distributed FS (stored on remote server)

Pseudo FS

List of FS

Note: SAMBA-->Windows/CIFS protocol

## 24.VFS Virtual FS

3 parts: metadata, super block (inode, dentry...), OO design

Super Block? --> segment of metadata

Inode: info about 1 file

Dentry (directory entry): look-up table to Inode

## 25.Optimization?

Based on characteristics of memory hierarchy and store devices

How to optimize (HDD)?--> Utilize RAM & CPU, prefer sequential IOs

## 26.HDD review

HDD--> seek time matters (time to move disk head from 1 place to another)

## 27. Ext4--> Unix FS concept

NTFS--Windows

ZFS--> the best concept

NFS-->Unix

GFS--> google

## 28.Storage Networking

# Glossary of Terms



- SAN – Storage Area Network. A network of switches, typically fibre channel used for carrying SCSI or FICON traffic
- FC – Fibre Channel. A protocol used to carry SCSI or FICON packets containing IO commands from a server to a storage array
- SCSI – Small Computer System Interface. A bus based system or protocol used to carry block based storage commands
- iSCSI – An IP based protocol capable of carrying SCSI commands to and from storage devices
- FICON – The protocol used to carry mainframe based IO
- MDS – The Cisco family of datacenter switches capable of carrying fiber channel traffic
- VSAN – Virtual SANs. A feature capable of creating logical SANs on a physical SAN infrastructure
- FCIP – Fibre Channel over IP. The protocol used to tunnel fiber channel packets over an IP infrastructure. Used for extending a Fibre Channel SAN over long distances

## 29.IT App model and system

App models: bare metal (archaic), Virtualization (Vmotion), Containers

## 30. Docker

Open source project--> automate deployment of SW in containers

-->wrapper of SW

-->build, ship, run anywhere

Better than Virtual Machine running apps

31. Docker File-->can be versioned in a version control system.

Docker tool: Kubernetes, Vagrant,...

## 32.Ansible?

Automation tool for configuration management, app deployment,....

Free, open-source

Yaml based

Flexible

#Slide 3

7 OSI layers

L#	Device Type	OSI Layer	TCP/IP Org.	TCP/IP New	Protocols	PDU
7	Gateway	Application	Application	Application	HTTP, FTP, POP, SMTP, DNS, RIP	Data
6		Presentation				Data
5		Session				Data
4		Transport	Transport	Transport	TCP/UDP	Segments
3	Router	Network	Internet	Network	IP, ARP, ICMP, IGMP	Packets
2	Switch/Bridge	Data Link	Link	Data Link	Ethernet,	Frames
1	Hubs/Repeater	Physical		Physical	Token Ring	Bits

### Enterprise Data Center

computer network built by companies

-->Most common architecture: Multi-tier: DC Core-DC aggregation/distribution-DC Access

### Enterprises Campus

The use of firewall is not recommended--> use layered architecture instead

Availability =  $\frac{MTBF}{MTBF + MTTR}$

MTBF = Mean Time Between Failure  
 MTTR = Mean Time To Repair

Sample architecture: Mobile devices (wired & wireless convergence), virtualization,...

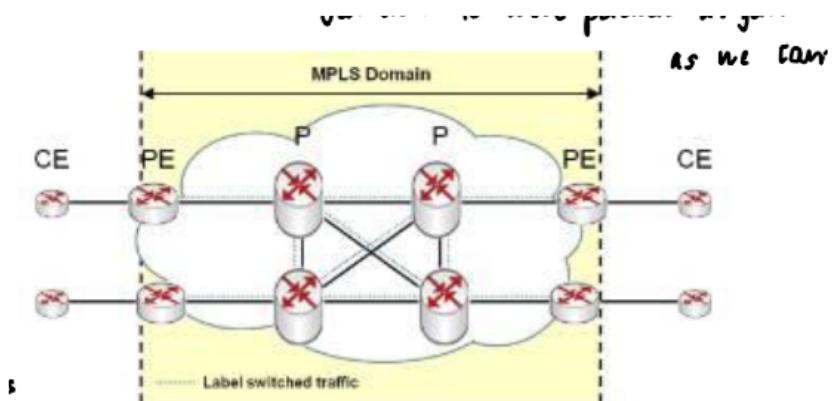
### Core Features (of what?)

High speed, low latency, low jitter (variable delay between data packets over a network--disruption in normal sequence of sending data packets), packet transport, reliability and fault tolerance

P: Service Provider Routers; talks to P or PE router  
 PE: Provider Edge  
 CE: Customer Edge  
 CPE: Customer Premises equipment

Layer 2 vs Layer 3: Bridging vs Routing

Bridging: L2, does not change the packet, need forwarding decision, uses switching



Routing: L3, changes the content of the packet (MAC DA address)

MAC learning: bridged and routed packets

Modern Ethernet switch: switching/L2 and routing/L3

Unicast: transfer packet to only 1 recipient

Broadcast: packet will be received by all devices in a network

Multicast: many to one or one to many; transmission to a group of hosts at the same time

Switching in Enterprises?

traditionally-->layer 2

Definition: hard-wired connection between 2 wires

if forwarding decision is determined-->packet is switched

Packet switching = label switching (ATM): early h/w forwarding implementation

label switching (hop-by-hop routing)--> layer 3

VLAN?

Layer 2

Group of interfaces configured such that they function as attach to the same wire (appeared to be on the same LAN but they are not physically)

VLANs--> to be partitioned by Mac address, Port or Protocol

Multi-layer Switching

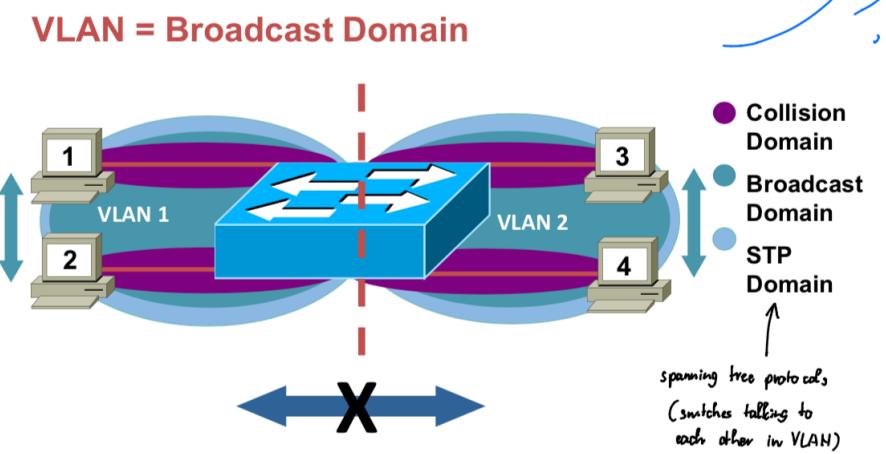
VLAN

using spanning tree protocol: switches talking to each other in VLAN

VLAN architecture

Native VLAN:

untagged VLAN on 802.1q trunked switchport



VLAN port types: Port based VLAN; tagged VLAN

VLAN number: 4094 maximum #num of VLANs on given Ethernet network

Switch Virtual Interface-->Forwarding between VLAN (slide)

Switches use L3 interface to route traffic to other L3 interface (No longer need a physical router)

Management domain (Spanning Tree Protocol Domain)

VLAN Trunk

A port carrying traffic of multiple VLANs through the use of encapsulation... (ISL, 802.1q)

Used as a link between forwarding devices

Each frame traveling on this will act as if it belongs to only 1 lane

### 802.1q

Both tagged and untagged frames allowed on this

Untagged frame-->Native LAN

Untagged frame: Null VLAN id with priority tagged frames.

### Layer2: VTP-->VLAN Trunk Protocol

Messaging protocol (layer 2) maintains VLAN configuration by managing addition, deletion and renaming of VLANs on a network-wide basis.

switches must be in same VTP domain to share information

### EtherChannel (Layer2)

Logical aggregation of similar links  
channels viewed as 1 logical links by  
protocols

IEEE802.3ad

Switch-1(config-if)#vlan 10



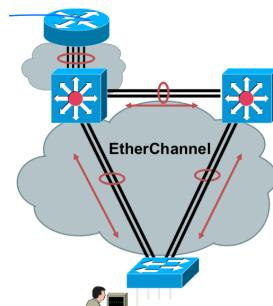
### Layer 3: SVI Switched Virtual Interface

A Switched Virtual Interface is a virtual LAN of switch ports represented by one interface to a routing or bridging system

Software based virtual interface

Used for VLAN to route traffic

SVI VLAN1 created by default



### Layer2: Forwarding

NO protocol to set up forwarding table.

Forwarding table built by source MAC address in data packets

Unicast flooding is sent if entry is not in CAM table

### Spanning Tree--> Layer 2

Invented by Radia Perlman

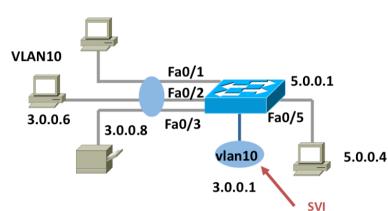
STP/ Spanning Tree protocol

Loop free topology for Ethernet

Prevent bridge loop (>2 layer 2 paths between 2 end points) and broadcast radiation (accumulation of broadcast and multicast on a computer network)

Fault tolerant

Newer version--> 802.1w

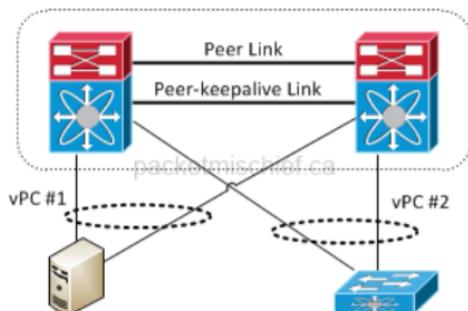


### Port Channel and VPC

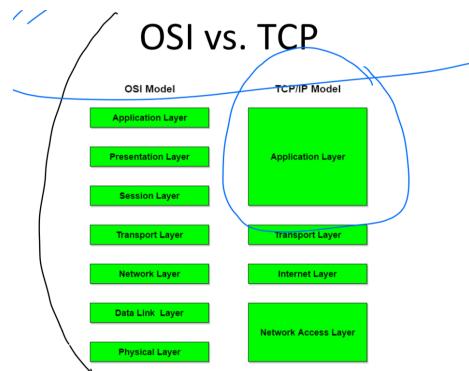
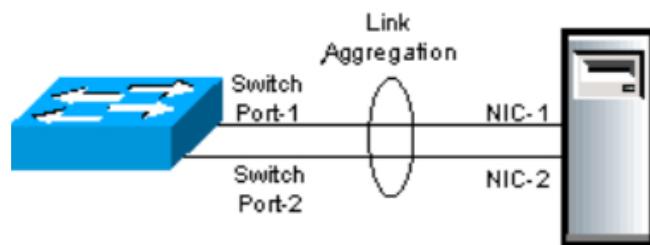
EtherChannel or link aggregation group (LAG)--> increase bandwidth, multiple path--> 1 logical path

Virtual Port Channel: same functionalities across multiple switches

**Linux bonding driver**  
 Aggregating multiple NIC into single bonded interface of NIC slaves.  
 Came with Linux distribution



OSI vs TCP



TCP vs UDP

TCP: connection oriented, reliable, error checked, deliver stream of bytes over IP, TCP sliding windows-->data transfer guarantee over a network.

UDP: connectionless, favors low latency over reliability, checksum, no handshaking, no data transfer guarantee

IGP vs EGP

Interior gateway protocol: RIP/RIPNG, EIGRP (self tuning/cisco), IS-IS  
 within AS (autonomous system)

OSPF--> companies

Exterior...: BGP

Between AS

Distance Vector and Link State Routing

Routing protocol: to compute best path to certain destination

Distance Vector?

Determine the best path based on distance (the cost of reaching 1 destination)

Example: RIFS

Link State?

Nodes share information, building up a network map updating through the whole network  
each node's table will eventually form the best paths to every other nodes it can reach

BGP-->the only EGP protocol

Classful vs classless routing

(Bellman - Ford algo.) RIP

Classful-->no longer popular now (RIPv1 & IGRP)

Do not send subnet mask information along with routing updates

OSPF , IS-IS (dijkstra algo.)

First implementation of IP had fixed class A, B, C, D subnet sized.

Sub netting allows Class A addresses to be subdivided into < 24 bit subnets

Classless routing is subnetting + almost complete elimination of A,B,C,D distinctions

Classless Routing (mainstreamed)

send subnet mask with their updates

RIVPv2, EIGRP, OSPF, IS-IS

Allow VLSM Variable Length Subnet Mask

CIDR-Classes Inter Domain Routing

Replaces class A, B or C. --> improve allocation of IP addressing scheme

Based on VLSM

RFC1918

Reserve some IPv4 addresses for private network

**IP address classes**

[<< Back](#)

Class	1 <sup>st</sup> Octet Decimal Range	1 <sup>st</sup> Octet High Order Bits	Network/Host ID (N=Network, H=Host)	Default Subnet Mask	Number of Networks	Hosts per Network (Usable Addresses)
A	1 – 126*	0	N.H.H.H	255.0.0.0	126 ( $2^7 - 2$ )	16,777,214 ( $2^{24} - 2$ )
B	128 – 191	10	N.N.H.H	255.255.0.0	16,382 ( $2^{14} - 2$ )	65,534 ( $2^{16} - 2$ )
C	192 – 223	110	N.N.N.H	255.255.255.0	2,097,150 ( $2^{21} - 2$ )	254 ( $2^8 - 2$ )
D	224 – 239	1110			Reserved for Multicasting	
E	240 – 254	1111			Experimental; used for research	

**Note:** Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for loopback and diagnostic functions.

**Private IP Addresses**

Class	Private Networks	Subnet Mask	Address Range
A	10.0.0.0	255.0.0.0	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.0.0	255.240.0.0	172.16.0.0 - 172.31.255.255
C	192.168.0.0	255.255.0.0	192.168.0.0 - 192.168.255.255

Hosted at [Novgorod State University](#)

### Sub netting

IPV4: 32bits --> N+M= 32 with N= #bits in network address; M= #bits in host address range  
 Classful routing: A(N=8), B(16), C(24): fixed !

Putting it together, a CIDR IP address would look like the following:

192.168.128.0/28      *how many bits are in the net mask!*

subnetting ----> class A from 8-32 bits fixed address bit size, B: 16-32, C: 24-32

### AS (autonomous System)

RFC1918 name	IP address range	number of addresses	largest CIDR block (subnet mask)	host id size	mask bits	<i>classful</i> description [Note 1]	a collection of connected Internet Protocol (IP)
24-bit block	10.0.0.0 – 10.255.255.255	16777216	10.0.0.0/8 (255.0.0.0)	24 bits	8 bits	single class A network	
20-bit block	172.16.0.0 – 172.31.255.255	1048576	172.16.0.0/12 (255.240.0.0)	20 bits	12 bits	16 contiguous class B networks	
16-bit block	192.168.0.0 – 192.168.255.255	65536	192.168.0.0/16 (255.255.0.0)	16 bits	16 bits	256 contiguous class C networks	

routing prefixes under the control of one or more network operators on behalf of a single administrative entity or domain that presents a common, clearly defined routing policy to the Internet

4 categories of AS

Multi-homed: AS connecting to more than 1 AS-->for reliability

Stub: AS connecting to only 1 AS (peering)

Transit: (service provider) provides connection through itself to other network

IX: connecting service providers to each other

BGP (border gateway protocol) properties.

- BGP routes are designated "internal" or "external"
- External routes come from a BGP peer in another AS
- Internal routes are specified in the "network" command or get redistributed from the IGP
- Internal routes are local to the AS; external are from outside the AS

## ↓ Multi-protocol label switching

MPLS and segment routing

MPLS: service provider uses for efficient traffic traveling through its network. Setting up a special lane for packets to travel through network encapsulated with a label (less than a tcp packet)

Ethernet VPN: encrypted with MPLS for better security

Internet Backbone

network connecting various pieces of the whole network.

NAPS: places which interconnects different internet carriers so that internet functions as one entity.

Peering: exchanging IP packets and BGP routes

ISP Tiers

Tier1: guarantee connection to any places on the Internet. Peer with all other Tier 1 ISPs

16 of them

Tier2: peer with >= 1 Tier 1.

Tier3: reach to the Internet via Tier2

Quality metrics of service

Throughput: traffic flow: bytes/sec or bit/sec

Delay: latency

Packet Jitter: variable delay

Error Rate

Packet Loss

Priority

Availability: percentage of time available

Security

Router and switch hardware

Content-addressable memory (CAM) is a special type of computer memory used in certain very- high-speed searching applications --> used to reduce switch latency for MAC look-up table

Ternary CAMs (TCAM) is a special type of CAM, used to speed up searches - A MAC Address is always an exact match and uses Binary CAM, but matching an IP Route or Access List requires partial matching --> found

in switches and routers to increase the speed of route look-up, packet classification, packet forwarding and access control list-based commands by enabling search on variable length prefixes

**Control Plane**  $\Rightarrow$  Routing! logically route packets between routers in a network!

- Makes decisions about where traffic is sent
- Control plane packets are destined to or locally originated by the router itself
- The control plane functions include the system configuration, management, and exchange of routing table information
  - The route controller exchanges the topology information with other routers and constructs a routing table based on a routing protocol, for example, RIP, OSPF or BGP
  - Control plane packets are processed by the router to update the routing table information.
  - It is the Signaling of the network
  - Since the control functions are not performed on each arriving individual packet, they do not have a strict speed constraint and are less time-critical

**Data Plane**  $\Rightarrow$  Forwarding! (the process of forward packets from input to output link within a router)

- Also known as Forwarding Plane
- Forwards traffic to the next hop along the path to the selected destination network according to control plane logic
- Data plane packets go through the router
- The routers/switches use what the control plane built to dispose of incoming and outgoing frames and packets

Clos network

Clos networks evolved into crossbar topologies and eventually into chassis-based Ethernet switches using a crossbar switching fabric. Now Clos networks are being used in modern data center networking architectures to achieve high performance and resiliency

Virtual networking

Computer network-->part of virtual network link.

Virtual link: not consist of physical link but from network virtualization

Virtual networking components

VNIC: network interface

Virtual Lan

Virtual forwarding and routing (VRF)

Virtual Network function (VNF)

VPN

L2 VPNs  $\Rightarrow$  emulation of point to point connection over a packet switching network

IEEE802.1Q VLANs

Pseudowire (PW) end-to-end service across MPLS network

Virtual private LAN service (VPLS) enables enterprises to link together their Ethernet-based LANs from multiple sites via the infrastructure provided by their service provider

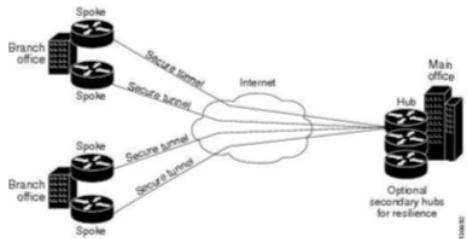
L3 VPN

Border gateway VPN (RFC2547)

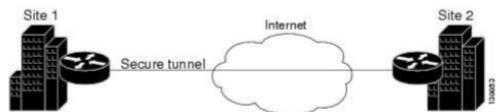
AMP-BGP + MPLS==> maintain separation between traffic from multiple subscriber networks as traffic is switched through a single shared core

### VPN topology

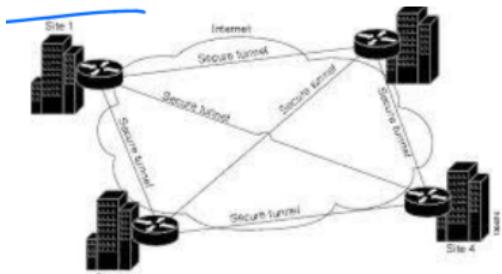
Hub and Spoke: 1 central VPN hub connects to multiple VPN routers



### Point-to-point VPN



### Full-mesh VPN



### Encryption Types:

#### IPSec (Internet Protocol Security)

Using layer 2 tunnel protocol to transfer IPsec packet

Provide AAA

Encapsulating an IP packet inside an IP Sec packet

De-encapsulating happens at the end of the tunnel

# Layered Security

Communication layers	Security protocols
Application layer	ssh, S/MIME, PGP, Kerberos, WSS
Transport layer	TLS, [SSL]
Network layer	IPsec
Data Link layer	[PPTP, L2TP], IEEE 802.1X, IEEE 802.1AE, IEEE 802.11i
Physical layer	<u>Quantum Communications</u>

can tunnel entire network traffic or secure an individual connection

DTLS Datagram Transport Layer Security  
used in Cisco AnyConnect VPN

Microsoft point-to-point encryption (MPPE)  
works with P-t-P tunneling protocol

SecureShell (SSH) VPN  
offer VPN Tunneling to secure remote connection to a network or inter-network links.

## Authentication

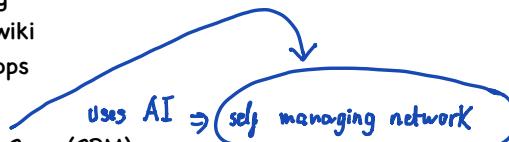
Tunnel endpoints must be authenticated before secure VPN tunnels can be established. User-created remote-access VPNs may use passwords, biometrics, two-factor authentication or other cryptographic methods.

Network-to-network tunnels often use passwords or digital certificates. They permanently store the key to allow the tunnel to establish automatically, without intervention from the administrator.

## Unified Communication

- Telepresence
- Conferencing
- Messaging
- Social / wiki
- Mobile Apps
- VoIP
- Customer Care (CRM)

(not include FTP)



## Intent Based Networking

Intent automation, real time analytic and intent assurance

Service Level Agreement → assure that I will get the service I pay for

## Cloud

VM cloud: data in private cloud

Public cloud: AWS, Azure

Hybrid cloud (private+ public cloud)

Cloud bursting: variable load (depends on user traffic—Relies on public cloud solutions)

## DNS Domain name service

convert a host name into IP address

DNS record stores: IP address, SMTP (email), NS (name server), Domain name aliases (CNAME)

## NTP (network time protocol)

for cloud synchronization between computer systems over packet switched, variable latency network

## Firewall

network security device → monitors and controls incoming and outgoing network traffic.

3 types:

1st gen: packet filter based on rules

2nd gen: stateful filter

2rd gen: application layer → prevent cross site scripting attack and SQL injection

## Access List

Black List: Accept all data, except for what must be blocked, lower maintenance and lower security

White List: Deny all data except what is allowed

NIST → recommend white list for high security environment

## NAT network translation

Type of NAT:

Static address translation: 1 to 1 mapping

Dynamic address translation: 1 to many (outside)

Overloading port address translation: extended version of dynamic address translation

ITU: International Telecommunication Union → UN org for information and communication technologies

ISO/OSI: International Organization for Standardization

TIA telecommunications industry association

NIST National institute of standard and technology

ONF: Open networking foundation

IETF: Internet Engineering Task Force

ICANN: Internet Corporation for Assigned Names and Numbers

IANA Internet Assigned Number Authority

ISOC Internet Society

IAB Internet Architecture Board

W3C World Wide Web Consortium

SNMP Simple Network Management protocol

Internet protocol for collecting and organizing information about managed devices on IP networks

NETCONF and Yang

NETCONF→ standard for installing, manipulating and deleting configuration of network devices

YANG → model for both configuration and state data of network elements.

Popular server and network monitoring software tools

(free) Cacti, Nagios (data management tool)

Slide#4

Legacy Client/Server: RPC(remote procedure protocol), COBRA, SOAP, REST, Web service...)

Modern application framework: Karaf (Apache Application container), Camel...

REST

Representational State Transfer

Performance, Scalability, Simplicity, Modifiability, Visibility, Portability and Reliability

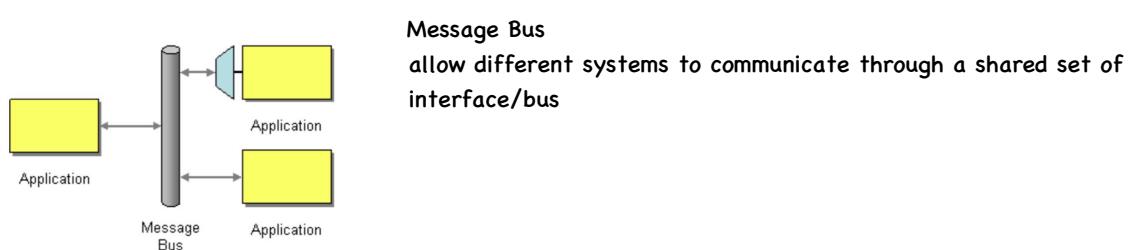
RAML

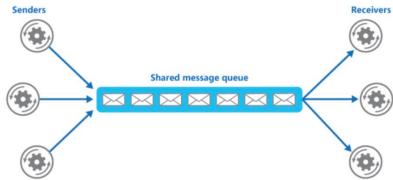
RESTful API modeling language

YAML based

REST constraints

Client-server, stateless, cacheable, layered system, code on demand, uniform interface





### Message Queue

>= 2 processes communicate/ exchange information via access to a common system message queue

Ajax-asynchronous Javascript and XML  
asynchronous: for interactive web services

XSLT Language for transforming XML doc to other XML

## OSGi Architecture

**Bundles** – Bundles are the OSGi components made by the developers.

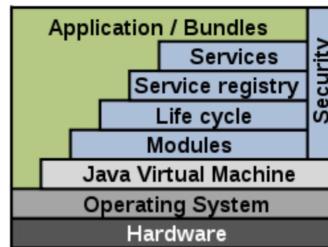
**Services** – The services layer connects bundles in a dynamic way by offering a publish-find-bind model for plain old Java objects.

**Life-Cycle** – The API to install, start, stop, update, and uninstall bundles.

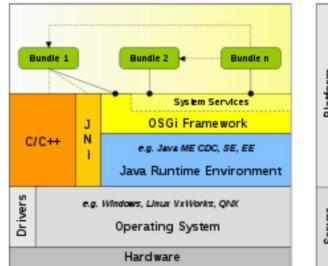
**Modules** – The layer that defines how a bundle can import and export code.

**Security** – The layer that handles the security aspects.

**Execution Environment** – Defines what methods and classes are available in a specific platform.



OSGi (open service gateway initiative)  
Java framework for developing and deploying modular software program and libraries  
OSGi has 2 parts: bundle specification and JVM (java virtual machine)



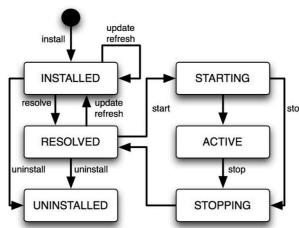
# Lifecycle

Reflects dynamic nature of OSGi

Resolve: Imported packages are bound to bundles that export them

Start: Activator start method is called

Stop: Activator stop method is called



Bundle State	Description
INSTALLED	The bundle has been successfully installed.
RESOLVED	All Java classes that the bundle needs are available. This state indicates that the bundle is either ready to be started or has stopped.
STARTING	The bundle is being started, the <a href="#">BundleActivator.start</a> method has been called but the start method has not yet returned. When the bundle has an activation policy, the bundle will remain in the STARTING state until the bundle is activated according to its activation policy.
ACTIVE	The bundle has been successfully activated and is running; its Bundle Activator start method has been called and returned.
STOPPING	The bundle is being stopped. The <a href="#">BundleActivator.stop</a> method has been called but the stop method has not yet returned.
UNINSTALLED	The bundle has been uninstalled. It cannot move into another state.

## Modules

Classes resolved on package level-not bundle level

Each bundle has its own class loader

## Bundle Lifecycle

# Apache Camel

open-source integration framework based on Enterprise Integration Patterns

The following projects can leverage Apache Camel as a routing and mediation engine:

- [Apache ServiceMix](#) - a popular distributed open source ESB and JBI container
- [Apache ActiveMQ](#) - a mature, widely used open source message broker
- [Apache CXF](#) - a smart web services suite (JAX-WS and JAX-RS)
- [Apache Karaf](#) - a small OSGi based runtime in which applications can be deployed
- [Apache MINA](#) - a high-performance [NIO](#)-driven networking framework

## Message Graphs (6 graphs in the slide)

# Apache Karaf

small OSGi runtime, lightweight container

Features: hot deployment, dynamic config, logging system, provisioning, native OS integration, remote access, security framework, managing instances

## **Spring Framework**

application framework and inversion of control container for the java platform.

### **Inversion of control**

Inversion of Control (IoC) is a design principle (although, some people refer to it as a pattern). As the name suggests, it is used to invert different kinds of controls in object oriented design to achieve loose coupling

## **Mule**

enterprise service bus (ESB) and integration framework

### **Java-based**

Allow different applications to communicate with each other by acting as a transit system for carrying data between applications within your enterprise or across the Internet.

Capabilities: service creation and hosting, service mediation, message routing, data transformation

Spark: based on hadoop

### **Kafka ?**

Enterprise service bus for collecting information during video streaming such as Netflix...

is an open-source stream-processing software platform developed by the Apache Software Foundation, written in Scala and Java

## **Kubernetes**

Clustering system to manage cluster of machines.

is an open-source container-orchestration system for automating deployment, scaling and management of containerized applications.[4] It was originally designed by Google and is now maintained by the Cloud Native Computing Foundation

## **Mesosphere**

Cloud scale OS/ distributed OS

Apache based project

→ to manage multiple machines or data center as a single computer

Hybrid environment

Application running in containers (fast healing/recovery)

## **Slide#5**

### **Enterprise System**

- Procurement process (buy)
- Production process (make)
- Fulfillment process (sell)
- Lifecycle data management process (design)
- Material planning process (plan)
- Inventory and warehouse management (IWM) process (store)
- Asset management and customer service processes (service)
- Human capital management (HCM) processes (people)
- Project management processes (projects)
- Financial accounting (FI) processes (track-external )
- Management accounting or controlling (CO) processes (track- internal )

**Architecture: Client-Server**

3 layers: presentation layer→application layer→data layer

Presentation Layer: interaction with the application

Application layer: what you are allowed to do

Data Layer: where to store client's work

**Architecture Service Oriented (SOA)**

Extension of client-server

"big apps composed out of smaller ones"

four properties: represent a business activity, self-contained, black-box for its consumers, may consist of other services

**ERP- enterprise resource planning**

consolidating enterprise's planning, manufacturing, sales...

automates the tasks involved in performing a business process

**ERP Magic Quadrant**

Top: SAP business all-in-one, IFS applications

check the graph !

Components: finance, HR (personnel related task), Manufacturing and logistics

**SCM (Supply chain management)**

Process of creating and fulfilling demands for goods and services.

Graph in slide

Types of SCM: Supply Chain Planning Software (SCP)→ predict inventory levels based on resources flow into supply chain; Supply chain execution software (SCE)→ automate different steps in supply chain

Supply Chain Planning Software top vendor: Oracle, JDA software

**CRM (customer relationship management CRM system)**

use technologies to help a business emerge from its customer base

major CRM vendor: Salesforce

**Human Resource Management**

activities used to attract & retain employees and maximize employee performance.

Including: recruitment, selection, training, development, performance...

serve as a link between human resources management and the strategic plan of the organization

**Business Intelligent Software**

Retail analytic→ Measurance (Cisco)

Data Analyzer→ Tableau

Combine multiple databases into 1→ Composite Software

Analyzing machine (log) data for the purpose of operational intelligence→ Splunk Enterprise

**HeatMap**

graphical representation of data where individual values contained in a matrix of colors.

**Content management system (CMS)**

application allows publishing, editing and modifying content, organizing and deleting them...  
used for website, shopping...  
goal to avoid hand-coding

### Enterprise Content management (ECM)

formalized mean of organizing' document, and other content...related to organization processes.

#### Directory Requirements:

- It must be **fast**. Sub-second responses are the norm.
- It must be **dynamic**. Updates must be real-time, with event-driven replication across directory instances.
- It must be **agile**. Reconfiguring the directory to accommodate organizational changes must be quick and easy.
- It must be **secure**. Directories contain data that must be both widely available and adequately protected.

## Directories vs. Databases

	Directory	Database
Records	Many short attributes	Fewer, longer, and more complex attributes
Access	Many fast reads, few writes	More updates; fewer, more complex reads
Performance	Fast, subsecond response	Less speed, more complex searches
Application	Lookup of small data sets that fit selected criteria	Transaction processes with commit and rollback facilities
Extensibility	Easy extension to accommodate organizational change	Typically more difficult to reconfigure to accommodate change
Security	Attribute-level security with read/write/encrypt constraints	Typically employs record-level constraints on read/write
Management	Focus on software configuration and schema design	Focus on data distribution on hardware and performance optimization

#### Identity Management

Top vendor: Okta, Microsoft

**Identity:** unique entity defined by a number of attributes  
**Domain:** environment in which the person and business has an identity definition.

Managing identities and identity store

Types of electronic identity stores:

Authentication directories

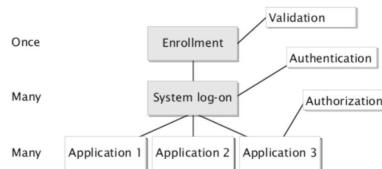
#### Authorization databases

## Authentication and Access Control

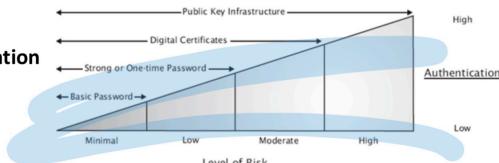
#### Directories vs Databases

#### Identification Protection

- One-time password
- Challenge response
- Digital certificate
- Biometrics



#### Levels of risk vs. authentication



#### Authentication and Access control

### **Role-based access control (RBAC)**

A user assigned with a role → allow to do something or access to certain resources.

### **Single sign-on and federated authentication**

Allow user to log in and gain access to multiple software systems without the need to log in again.

Ways to achieve SSO in enterprise:

Central storage of user names and password: store user's info in all systems in a secure vault within each system

Passing of user single sign on statuses between applications: save user's logon state and pass this state to the next system the user logs in to.

### **Public key infrastructure**

providing: digital signing of the document, encryption of document,...

### **Information technology management**

CIRBA-store defined infrastructure control

CyberARK, Venafi-priviledge account, crypto key

IP address management,...

### **Identity Management in active directory**

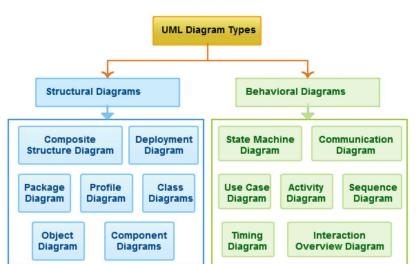
Windows Azure Authentication Library, W.A active directory graph, W.A access control service, W. identity foundation, Active Directory federation service

### **Apache Syncope**

Open source system for managing digital identities in enterprise environments

Provide: account and role administration, domain integration, approval and request management

## **UML Diagrams**



Commercial enterprise suites

Netsuite

Oracle: CRM, Service management,...

SAP business suite (based on Netweaver)

Slide#6

Cloud infrastructure market

Top vendor: Amazon and Microsoft

BPM (business process modeling)

representing processes of an enterprise such that current process may be analyzed, improved and automated.

UML created by Ivar Jacobson in 1992

UML

unified modeling language

Standardized, general purposed modeling

Core concepts in UML include: actor, attribute, class, interface, object, activity, event, message, state, use case, association, composition, depends, generalization, inheritance, multiplicity, role

**Class diagram**

most used UML diagram type.

used mostly by OOP

depicts classes, attributes and operations of each class

**Component diagram**

depicts the structural relationship of components of a system

**Deployment diagram**

depicts hardware and software of a system

**Object diagram (instance diagram)**

similar to class diagram

**Package diagram**

depicts dependencies between packages in a system

**Use case diagram**

depicts actors involved in a system, interactions between actors and system

**Activity Diagram**

depicts workflow in a graphical way

**State machine diagram**

similar to activity diagram

depicts behavior of objects at different moment in time

**Sequence diagram**

depicts how objects interact with each other and the other of interactions.

Communication diagram  
(collaboration diagram)  
Focuses on messages passed between objects

# Modeling Concepts in BPMN



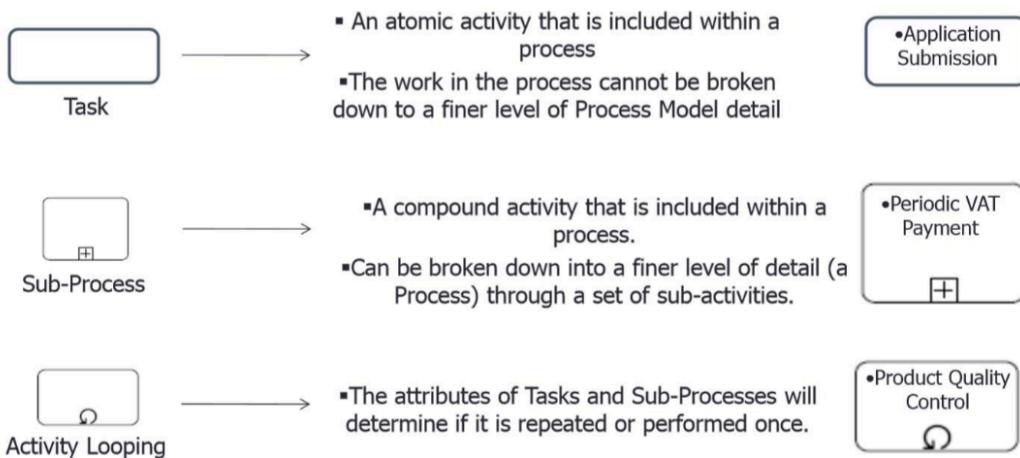
Interaction  
Overview Diagram  
collection of  
interaction  
diagram and the  
order they happen

BPM (Business  
Process  
Management)  
Provide notations  
for exception  
handling,  
transactions and  
compensation,...  
Used by business  
analysts, technical  
developers,  
business people,...

## BPMN Symbols Notation per Category

Flow Objects	Connecting Objects	Swimlanes	Artifacts
Event	Sequence Flow	Pool	Document
Task	Message Flow	Lane	Group
Gateway	Association		Comment

# Activities



## Sub-process markers

You can assign markers to sub-process. There are four markers: Loop, Multi-Instance, Ad-hoc and Compensation. A sub-process can have up to three markers, excluding the marker for collapsed: A loop/multi-instance marker, an Ad-hoc marker, and a Compensation marker. Assignment of markers is done through the specification dialog box of sub-process.

Name	Representation	Description
Loop	Process	This marker indicates that the sub-process will loop as long as the condition that defined in the loop is true. The condition is evaluated in each iteration, at either the beginning or the end of iteration. This marker can be used in combination with the ad-hoc and/or compensation marker.
Multi-instance (parallel instances)	Process	This marker indicates the execution of sub-process in a desired number of instances or in a data driven approach. The instances will be started at the same time.
Multi-instance (sequential instances)	Process	This marker indicates the execution of sub-process in a desired number of instances or in a data driven approach. The instances will be executed one after the other.
Ad-hoc	Process	This marker indicates that a sub-process is a group of activities that have no required sequence relationship. The sequence and number of performances for activities are determined by the performers of the activities.
Compensation	Process	To undo (cancel) the result of another activity that have already successfully completed. The execution of compensation sub-process is due to the undesired results and possibly side effects produced by another activity that need to be reversed.

Pools  
BPMN  
element-

->contains at most 1 business process, set boundaries of a business model

## Common Start Event Types

			Lanes
	None	<i>The modeler does not display the type of Event. It is also used for a Sub-Process that starts when the flow is triggered by its Parent Process.</i>	Sub partitions within a pool, used to organize and categorize activities of a process
	Message	<i>A message arrives from a participant and triggers the start of the Process.</i>	
	Timer	<i>A specific time-date or a specific cycle (e.g., every Monday at 9am) can be set that will trigger the start of the Process.</i>	
	Rule	<i>This type of event is triggered when the conditions for a rule such as "S&amp;P 500 changes by more than 10% since opening," or "Temperature above 300C" become true.</i>	
	Link	<i>A Link is a mechanism for connecting the end (Result) of one Process to the start (Trigger) of another. Typically, these are two Sub-Processes within the same parent Process.</i>	Hyperconvergence is an IT framework
	Multiple	<i>This means that there are multiple ways of triggering the Process. Only one of them will be required to start the Process. The attributes of the Start Event will define which of the other types of Triggers apply.</i>	Hyperconvergence is an IT framework

that combines storage, computing and networking into a single system in an effort to reduce data center complexity and increase scalability. Hyperconverged platforms include a hypervisor for virtualized computing, software-defined storage, and virtualized networking, and they typically run on standard, off-the-shelf servers

**check book example !**