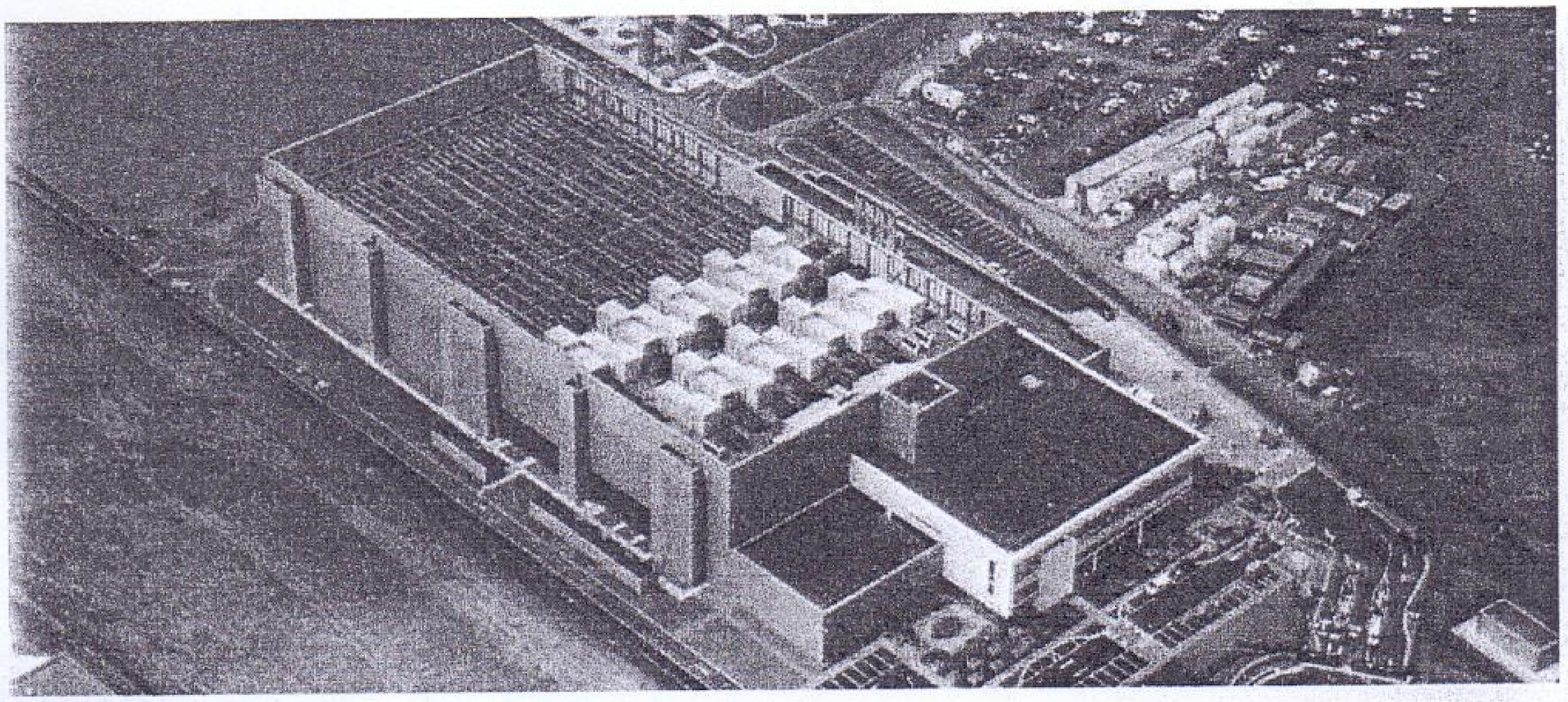
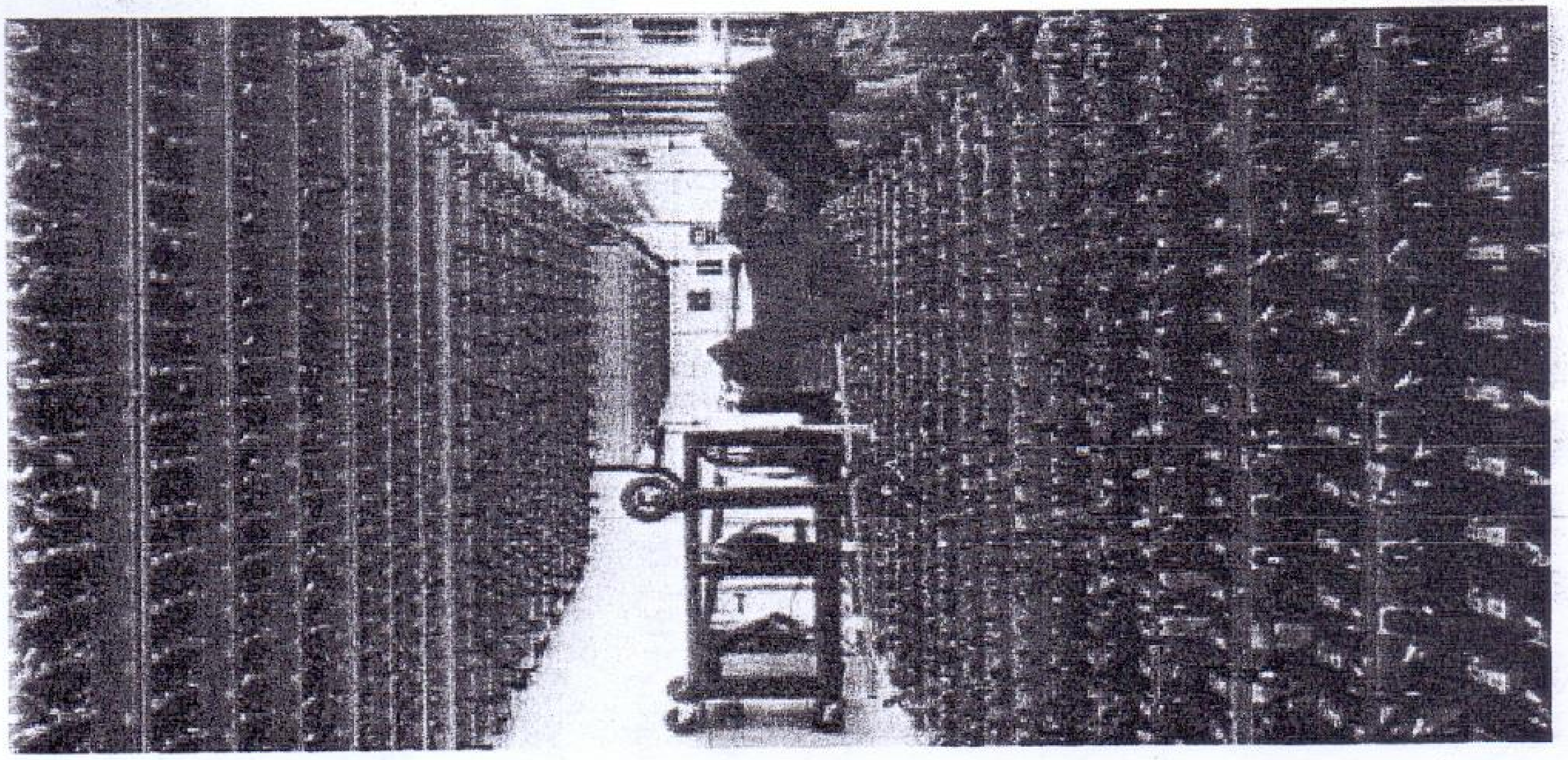
CCNA Book 3

Eng. Ahmed Nabil

(DoN)

Data Center
(Virtualization and cloud overview)





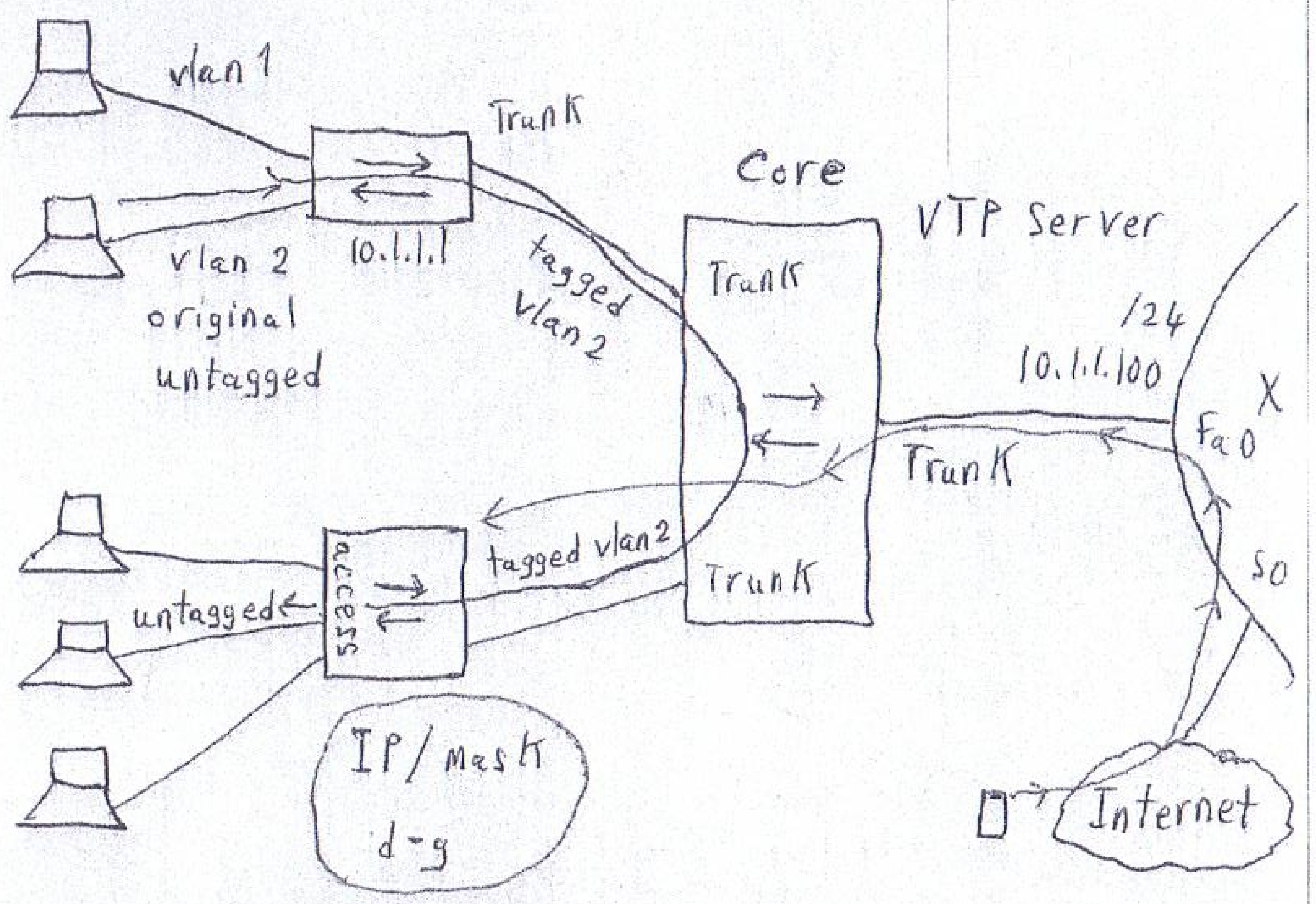
Session 1 /1

Managing the Switch Remotely:

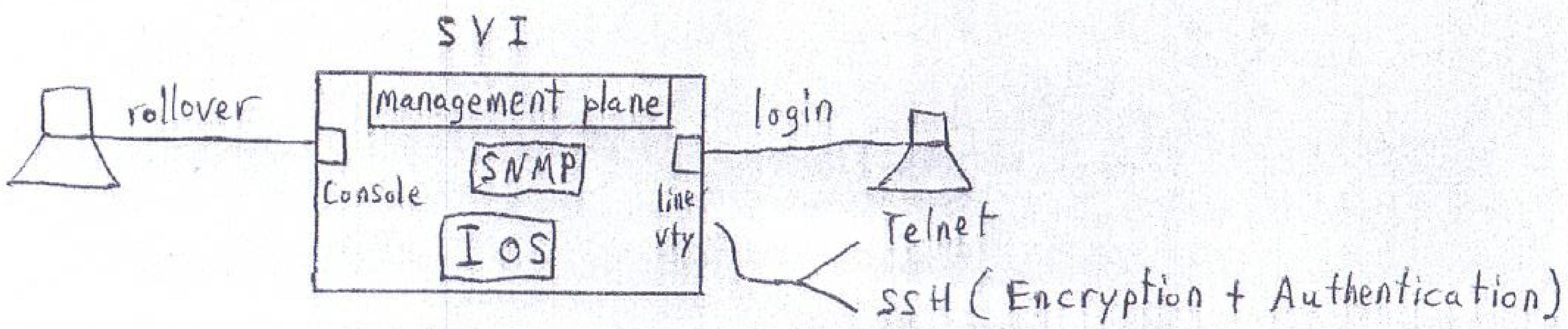
* Using Management Plane

(config)# line vty 0 15
(config-line)# password bisco
(config-line)# login
(config-line)# transport input SSH

(config)# interface vlan 1
(config-if)# ip address 10.1.1.1 255.255.255.0
(config-if)# no shutdown
(config)# ip default-gateway 10.1.1.100 (IP of Router)



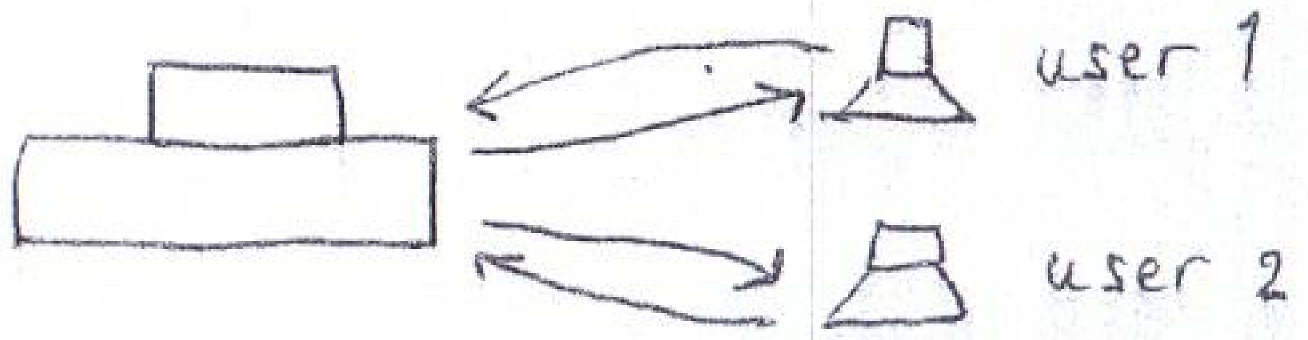
SVI = Switch Virtual Interface



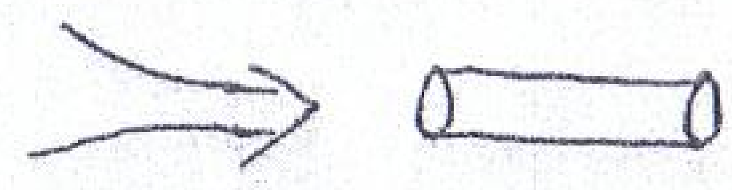
Session 1/2

Cloud Computing:

Basically, Cloud Computing was defined as one computer that can be used by two or more different users at the same time.

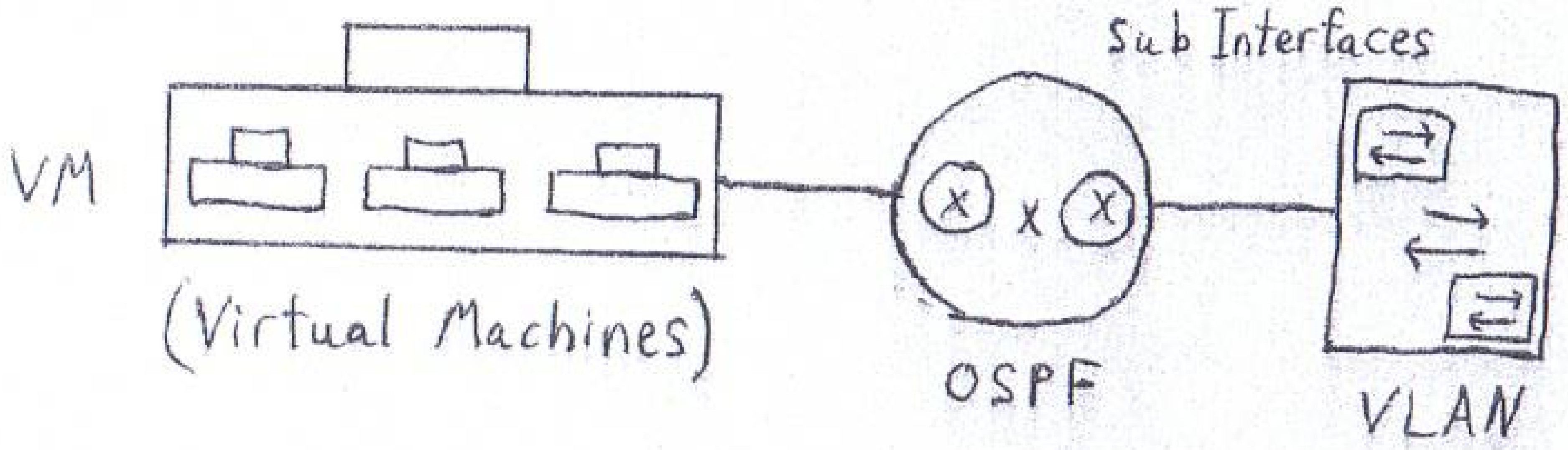


* Nowadays, Cloud Computing is Known as Virtualization



Virtualization:

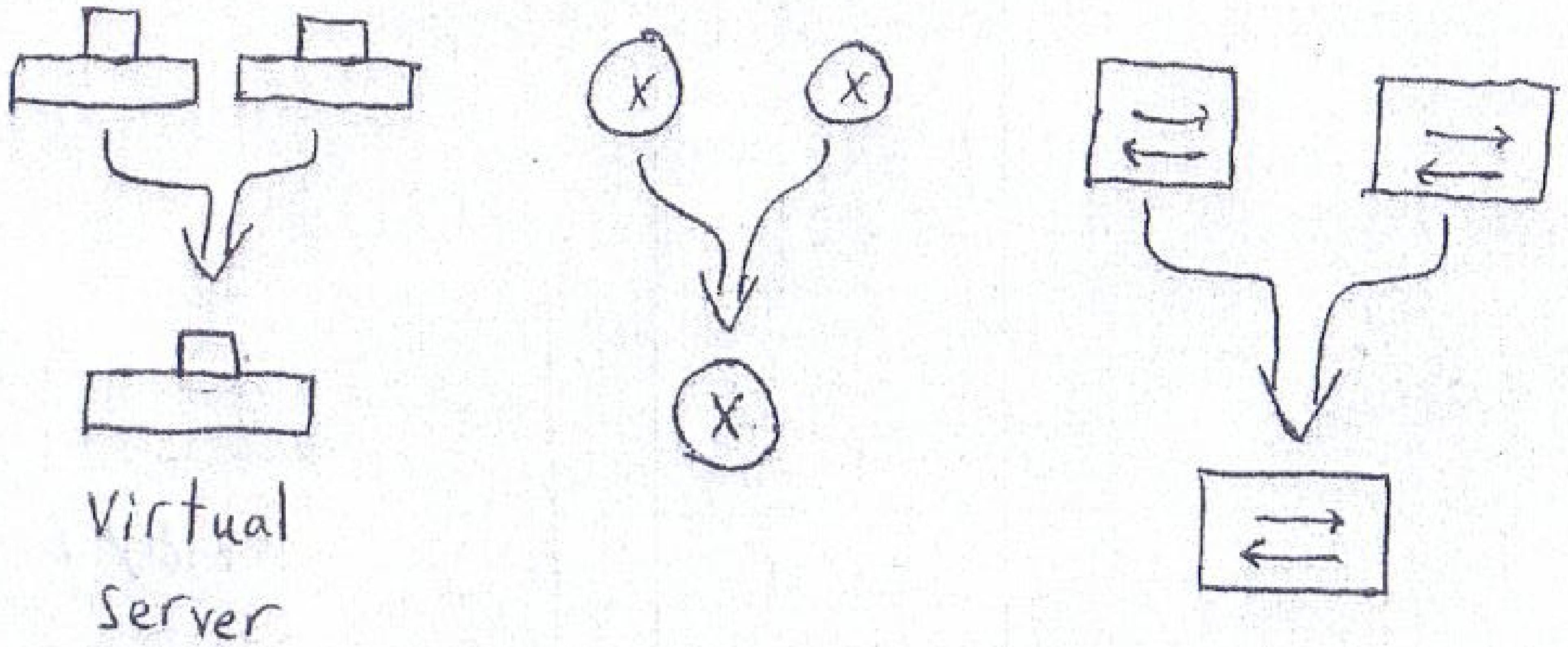
* It is dividing physical devices into smaller sub devices → to save resources



* It is merging many physical devices to act as one virtual bigger device ⌈ Redundancy
⌊ Load Sharing

Redundancy → (Active/Standby)

Load Sharing → (Active/Active)



Session 1/3

Cloud has 3 types of services:

[1] H/W Service: network rental
network hosting

IaaS: Infrastructure as a Service

Storage → icloud
Server
Cable
Router
Switch

M/W
[2] Midware Service: Use tools: (.NET/Java/Python)

Can help developers

PaaS: Platform as a Service
Midware as a Service

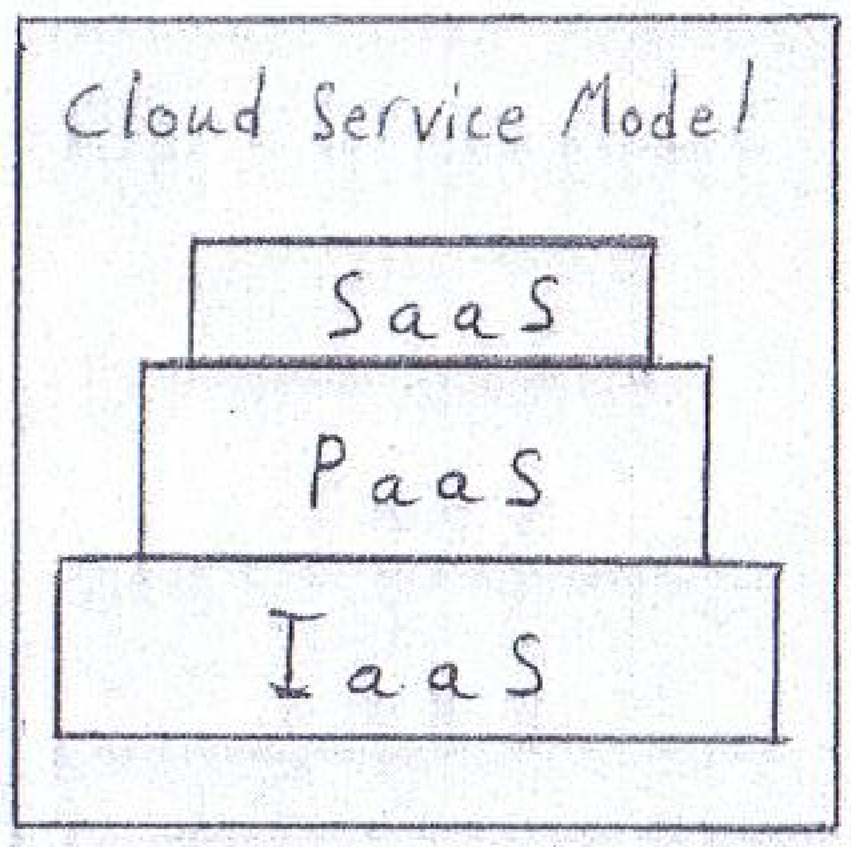
S/W
[3] Software Service: Applications

game, mail, soundcloud, playstore, ...

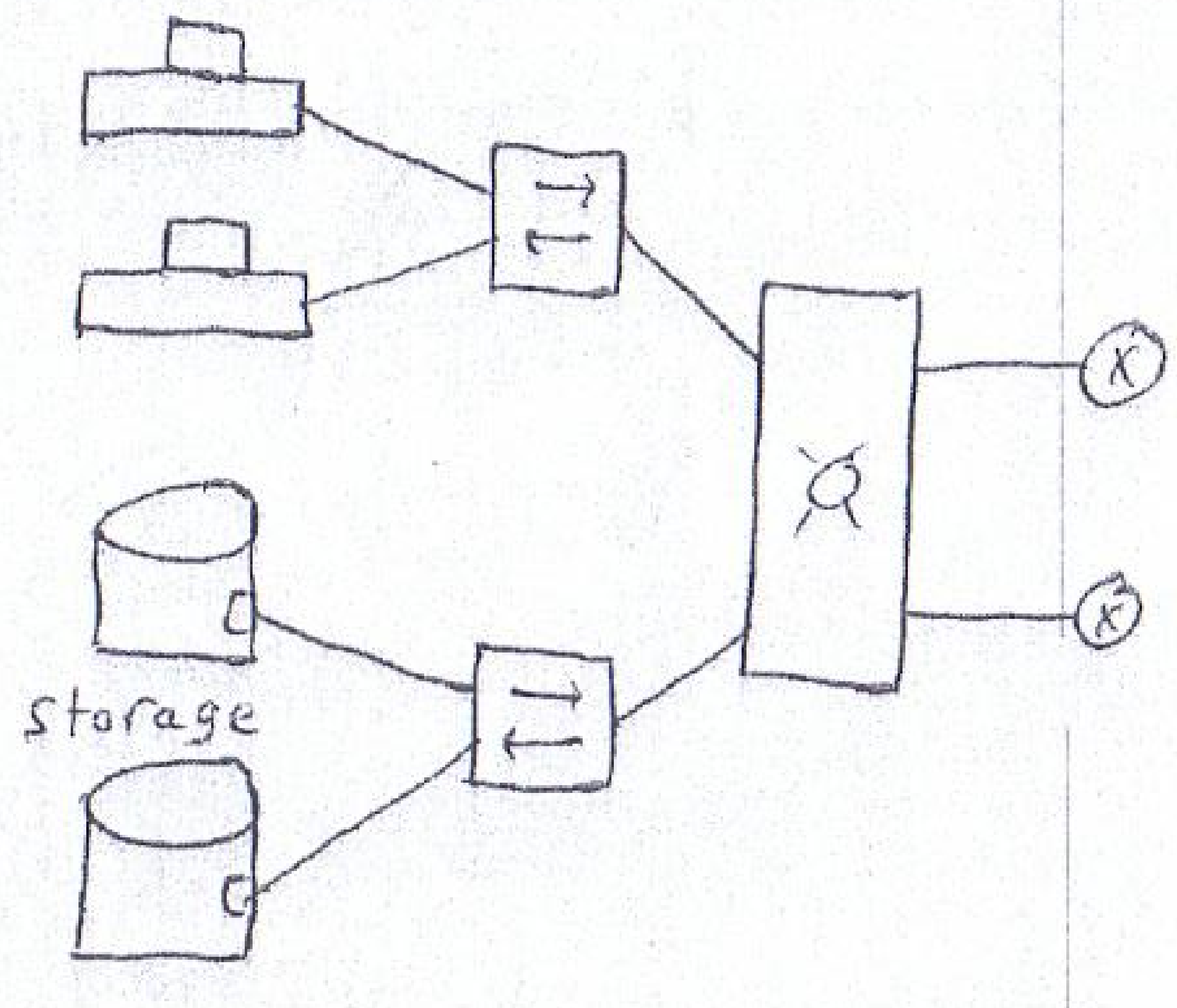
SaaS: Software as a Service

Cloud Service Providers:

- DELL-EMC
- IBM
- VMWare
- Google
- Amazon
- Microsoft



LAN



SAN = storage Area Network

Cloud < Flexibility, Scalability

Data Center

Network Cloud

Cloud Computing:

Basically it was defined as a Computer to be used by two or more People Simultaneously.

the Word Virtualization is now used to describe this Situation.

Computing Services include Servers, Storage, databases, networking, Software & midware.

tools & Programing used to build applications.

Virtualization is:

either
- Merging Many Physical devices to act as one bigger Virtual device, to help in Redundancy & Load sharing

or

- Dividing main device into Smaller Sub devices, to Save Costs & use resources in a better & efficient way.

There are three types of Cloud Services. Forming Cloud Computing Stack.

- H/W Cloud Service.
- Midware Cloud Service.
- Software /applications Cloud Service

* all these services maintarget is network flexibility & scalability.

S/w as a Service	SaaS	S/w & apps
Platform as a Service	PaaS	M/w & tools
Infrastructure as a Service	Iaas	H/w (Servers, Storage , network)

Switches Cables routers

1- Iaas: Infrastructure as a Service

A virtualized Computer environment delivered over network & Internet by Cloud Provider.

It includes Servers, Storage & network equipment.

Can also be Called Haas (H/w as a service).

It includes renting IT infrastructure using Virtual Machines (VM) ≡ Virtual Server ≡ Sub Server , Virtual Storage , Virtual Switches, Cables & Virtual Routers.

2- Paas (Platform as a Servile)

it makes things easy for developers to Create applications & Softwares.

So mainly used for development, testing, delivering & managing S/w applications.

So its final target is writing S/w for Computer Systems using Python, Java & .NET, --- to build S/w Codes.

these Codes will then be loaded on the infrastructure of Cloud Provider.

Paas Can also be Called Maas (Midware as a Service)

3- Saas (S/w as a Service)

Cloud Providers Can host S/w applications, Customer Can manage maintainance, upgrades & add security patches to the existing applications.

Saas example is PlayStore, app store, gaming, gmail, office tools (Microsoft office 365 & Calendering, ----

Top Cloud Providers are:

- Amazon
- Dell EMC
- Google
- Microsoft
- Oracle
- VMWare
- IBM
- SAP
- Salesforce

each has it own huge data Center

& now we will discuss how to build a datacenter for Providing a Cloud Service using infrastructure Virtualization.

Cloud Can exist in 3 fashions:

- Private cloud:

Used by Private Enter-prises & Companies by locating Company's data Center

at the Cloud Provider Premises

- Public Cloud:

Used by internet users

Like iCloud, Sound Cloud, Playstore, appStore & gmail, ---

- Hybrid Cloud.

Mix between Private & Public Cloud

Like Visa & Master Card users, ---

Virtualization :

Data Center & Cloud fundamentals

- Switch virtualization
- Link Virtualization
- Router Virtualization
- Server Virtualization

- Switch virtualization:

* Dividing Switch into Sub Switches Can be done using VLANs, other methods is not Covered in our Course

* Merging the activity of many Physical Switches Can be done in So many ways, but our Course only Covers Per VLAN STP.

- PVST will help achieving loadsharing between many Core Switches.

Session 2 / 1

* Switch Virtualization:

Merging switch for Redundancy & Load Sharing

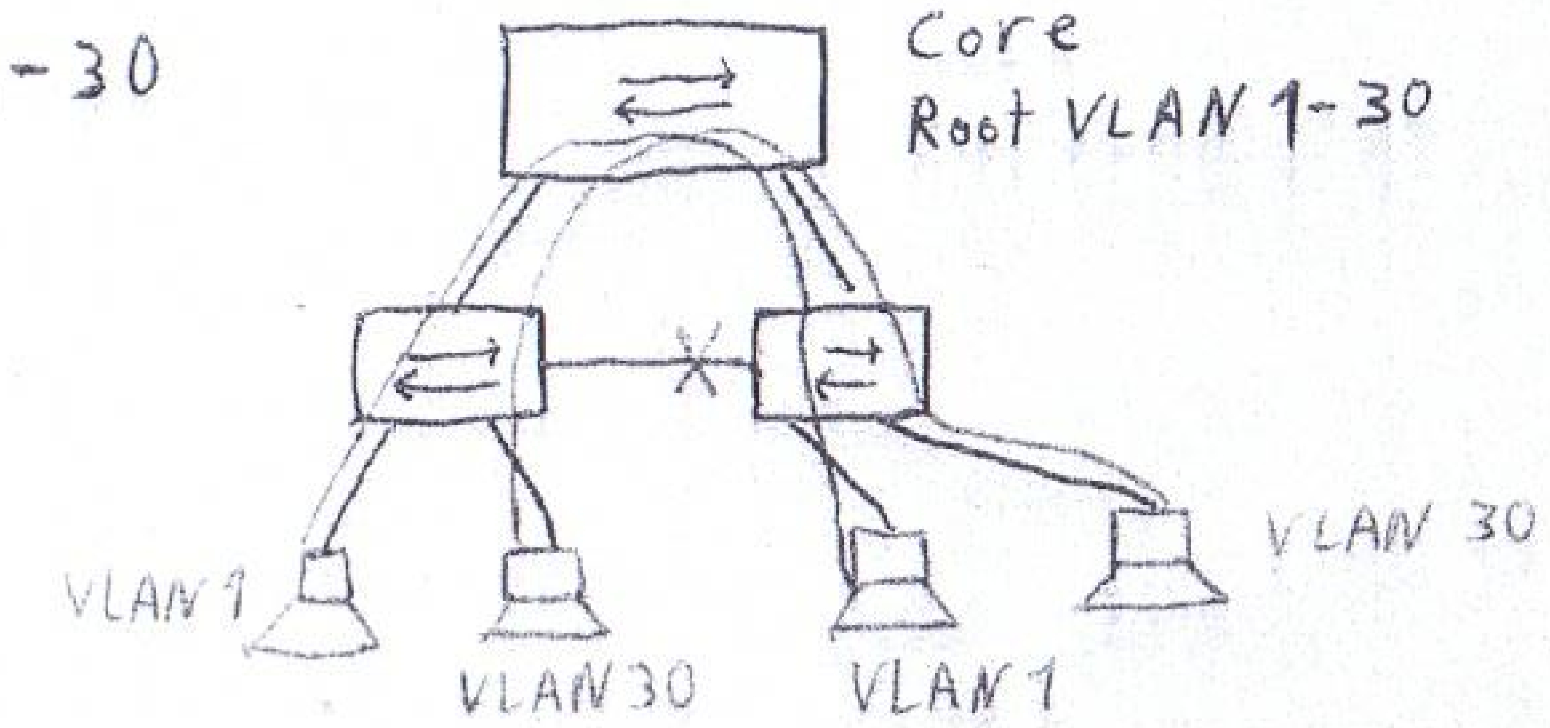
Core 1 (config)# spanning-tree vlan 1-15 root primary
Core 1 (config)# spanning-tree vlan 16-30 root secondary

Core 2 (config)# spanning-tree vlan 16-30 root primary
Core 2 (config)# spanning-tree vlan 1-30 root secondary

STP Types:

[1] STP version 1: (IEEE 802.1d)
↓ One Core

VLAN
1-30



[3] RSTP (Rapid STP): Version 2 - (IEEE 802.1w)
only one core is available

[4] Cisco Rapid - PVST: Fast & Multiple Cores

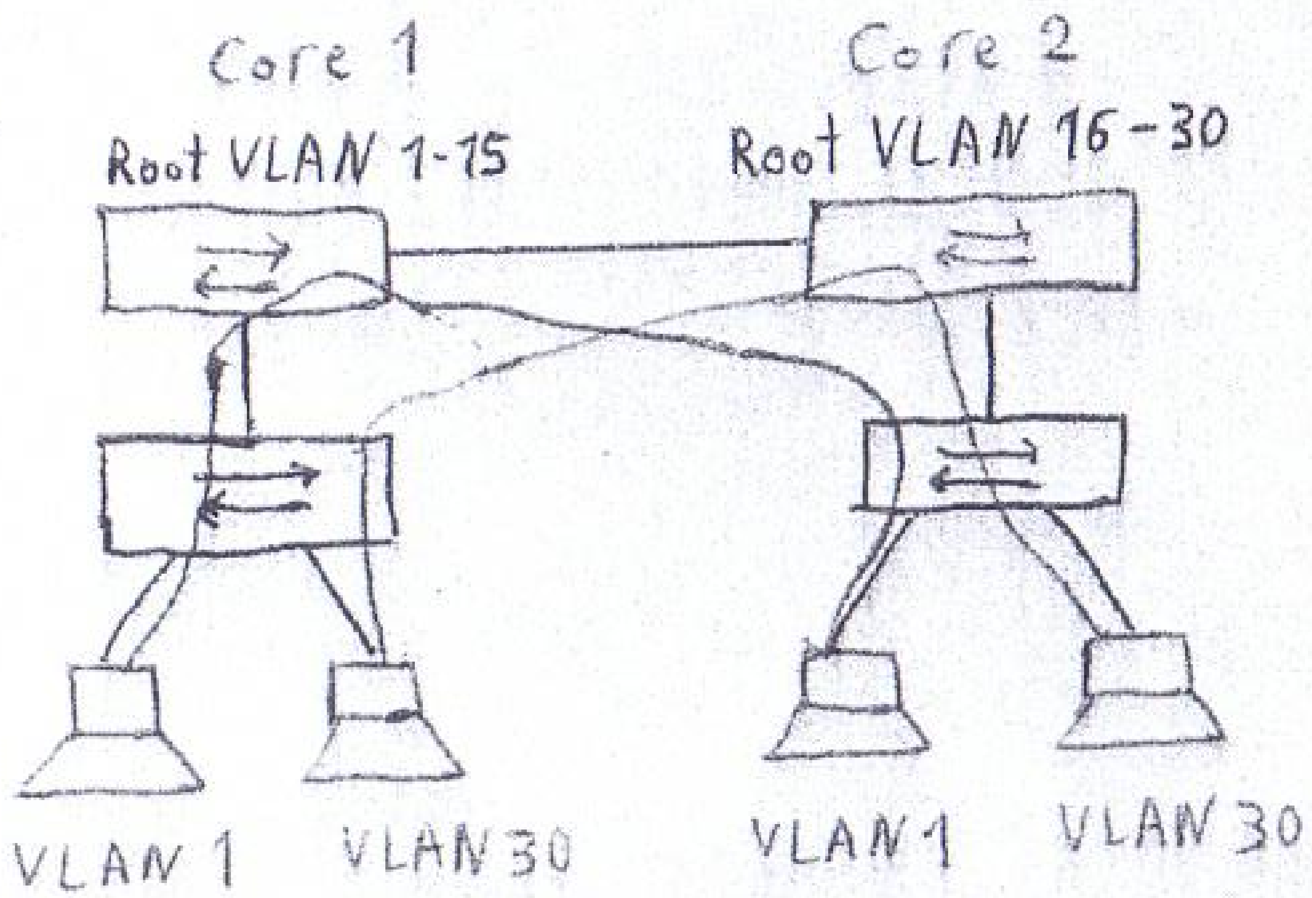
[5] MSTP: Multiple STP - Version 3 - (IEEE 802.1S)

[multiple VLANs
multiple Cores

* It is rapid PVST but Standard

[2] Cisco PVST:

Per VLAN STP



(config)#
spanning-tree mode

- STP → slow + 1 core default
- RSTP → fast + 1 core
- MST → fast + multiple cores

} Standard

- PVST → slow + multiple cores
- Rapid-PVST → fast + multiple cores

} Cisco

Session 2/2

* Switch Virtualization:

It is dividing / merging physical switches

VLAN

- VSS : Virtual Switch System
- Switch stacking
- PVST : Per VLAN STP

* VSS = Virtual Switch System

It's merging many $\boxed{\text{core switches}}$ Catalyst 6500

to act as one virtual switch,

one Active switch control the group of

switches, while all forwards.

PVST
rapid-PVST
MST

* Switch Stacking: "Stackwise"

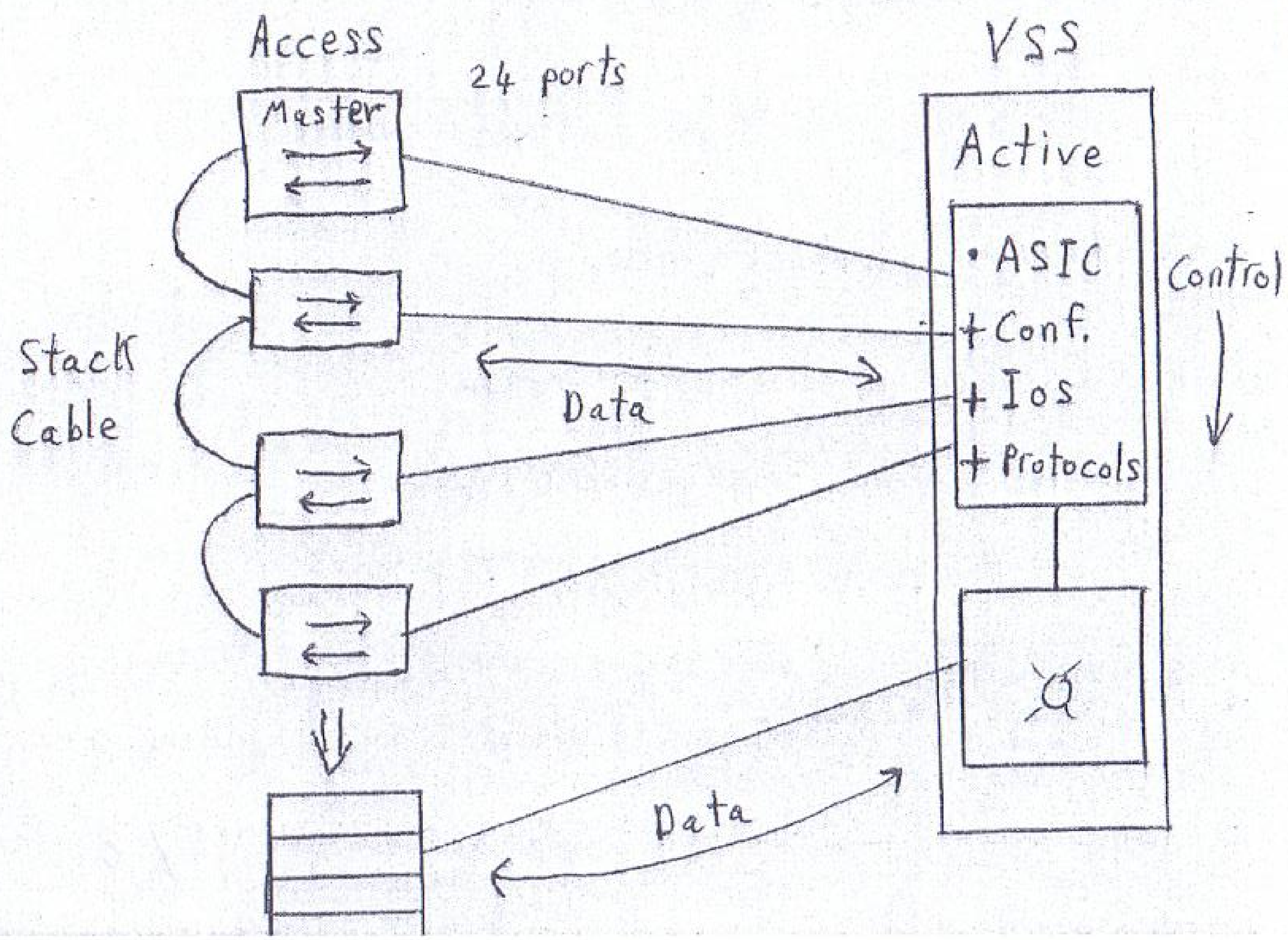
It is merging many $\boxed{\text{Access switches}}$ Catalyst 2960 X

to act as one virtual switch,

one Master switch control the stack of

switches, while all forwards,

* Stacking can be done for up to 9 switches

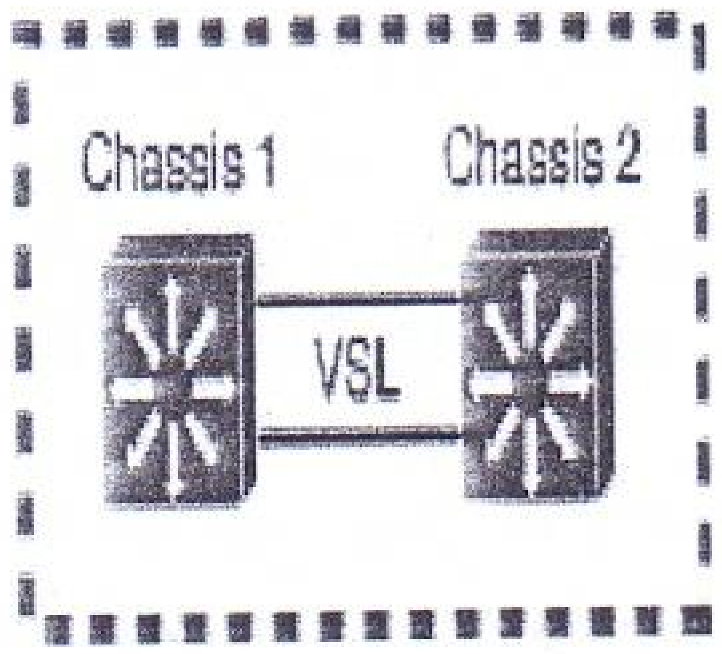


Redundancy between devices:

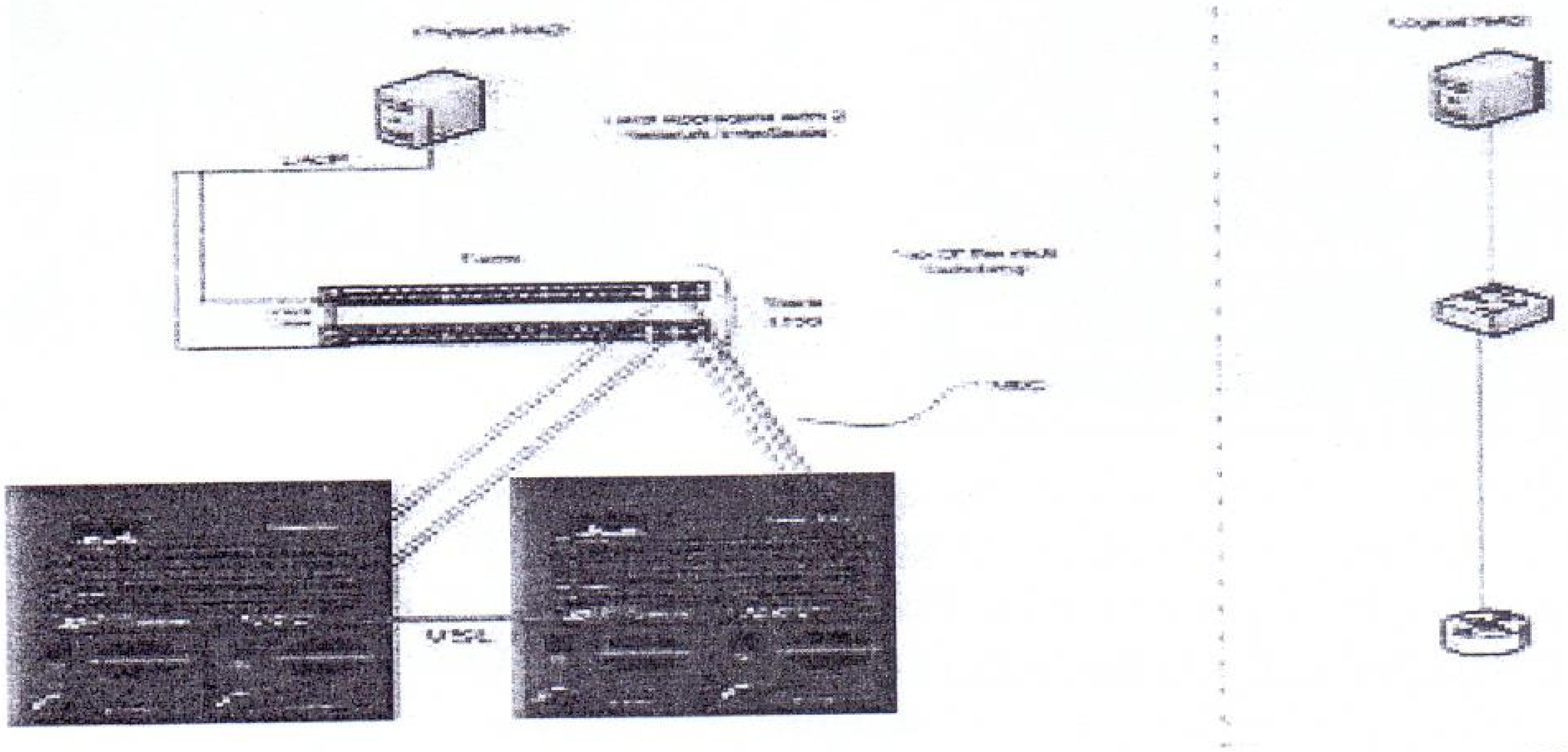
VSS (Virtual Switching System)

A VSS is a network system virtualization technology that pools Multiple **(up to two)** Cisco Catalyst 4500/6500 switches into one virtual switch, working in active/hotstandby fashion, increasing operational efficiency, offering non stop communication and scaling system bandwidth capacity to 1.4 Tbps (for sup 720), 2Tbps (for Sup 1T) and so on.

One supervisor in one of the chassis controls the operation of the logical switch. If it fails, a supervisor in the other chassis can take over. To build the logical switch, the two chassis must be linked together by multiple interfaces that have been configured as a virtual switch link (VSL)



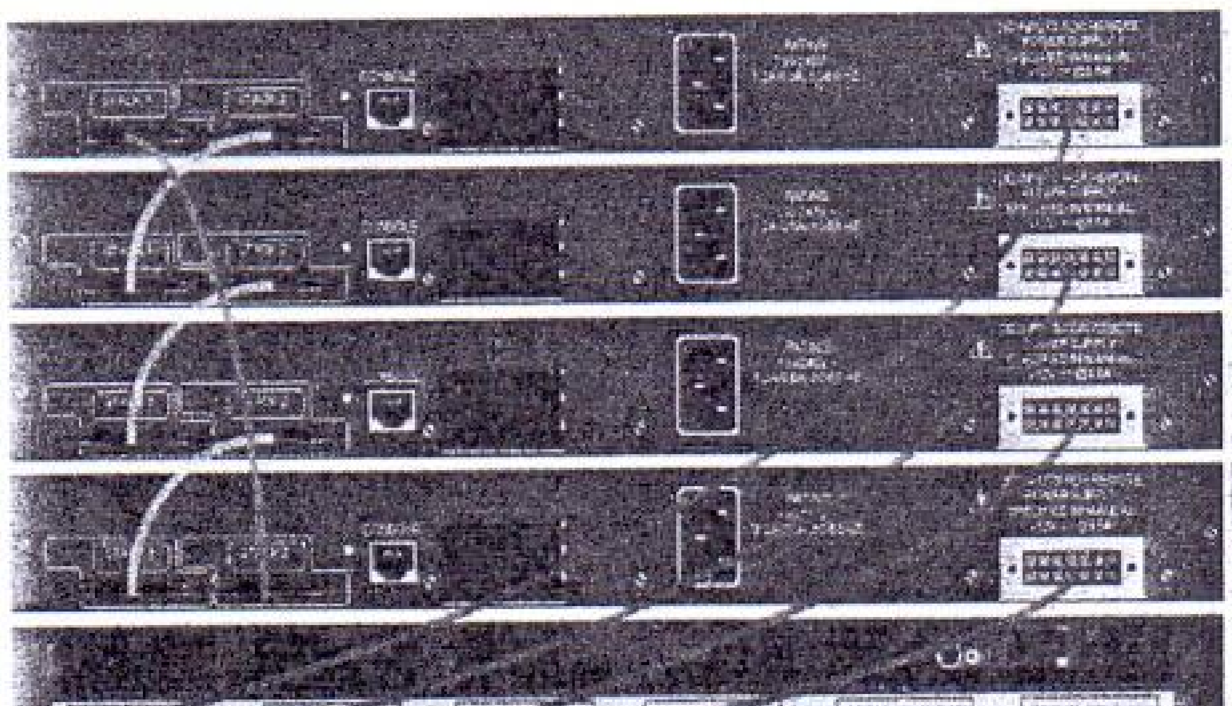
The two supervisor engines on the two different switch need to be connected together with one or more (up to 8) 10GbE link (this link is called VSL (Virtual Switch Link), this link will carry control signals between the two switches and in the same time can be used for sending data between the two switches.

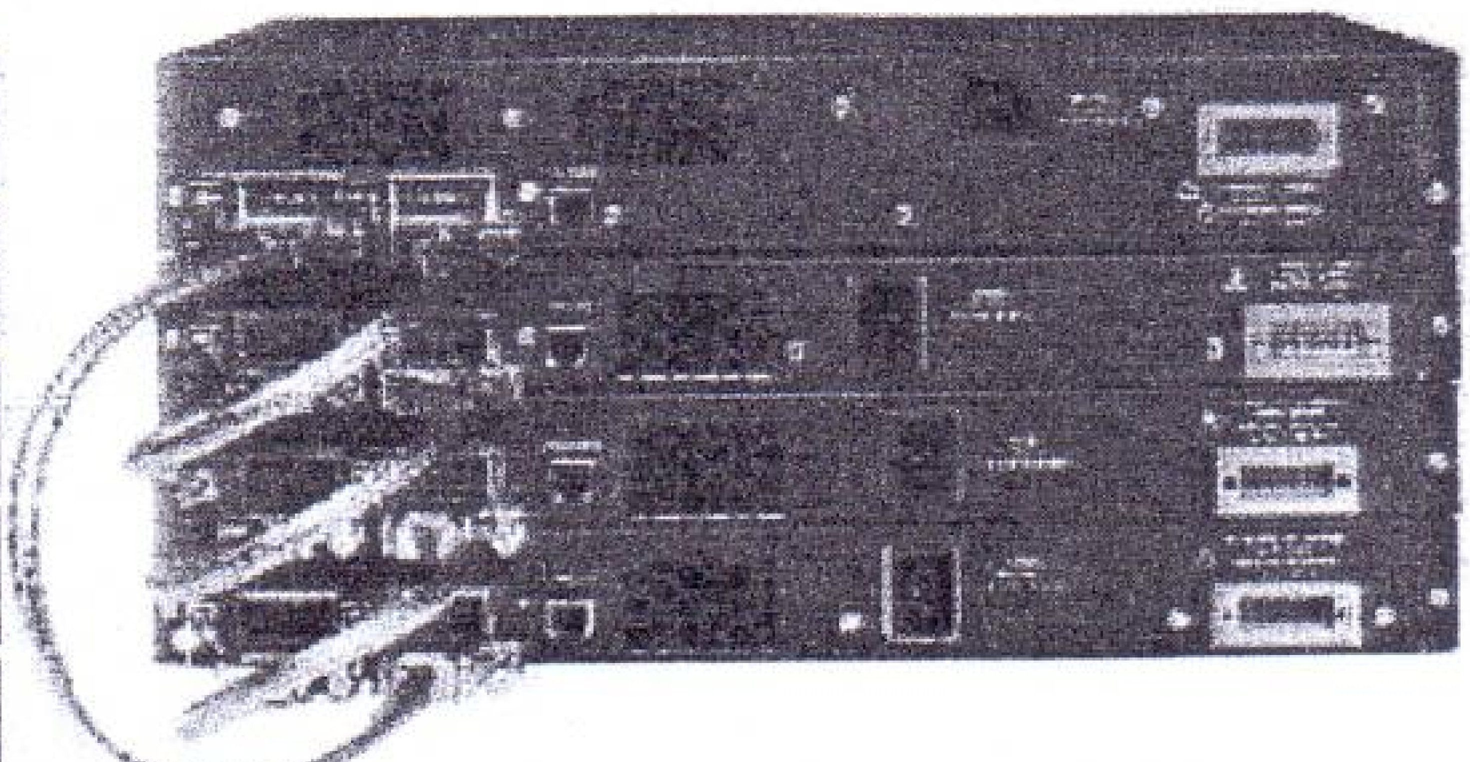


AHMED NABIL

Switch Stacking (Stackwise):

Traditionally, access layer switches have been independent physical devices. If you needed multiple switches in one location, you had to configure links between them. Cisco introduced the StackWise and StackWise Plus technologies to enable separate physical switches to act as a single logical switch. This is a similar feature as VSS but for non modular switches, its target is to logically merge many switches as one switch unit in order to gain higher performance, you should select one switch as stack master (highest priority, default 1, can vary from 1-15), stack master performs all of the management functions, all other are called stack members, If the master switch fails, other member switches can take over the role. When the physical switches are not part of a stack, each one operates independently and manages its own functions.
The most famous stackable switches is available on switch models such as the Cisco Catalyst 2960-X, 3750-E, 3750-X, and 3850 platforms.
To create a logical "stacked" switch, individual physical switches must be connected to each other using special-purpose stacking cables. Each switch supports two stack ports; switches are connected in a daisy-chain fashion, one switch to the next, and one final connection connects the chain into a closed
loop. You can think of the stacking cables as an extension of the switching fabric. When frames need to be moved from one physical switch to another, they are sent across the bidirectional stacking cable loop to get there. Figure illustrates how physical switches are cabled to become one logical stack.
The same daisy-chain scheme can be used to connect up to nine physical switches in a closed ring fashion providing a speed of 32Gbps (stackwise) and 64Gbps (stackwise plus).

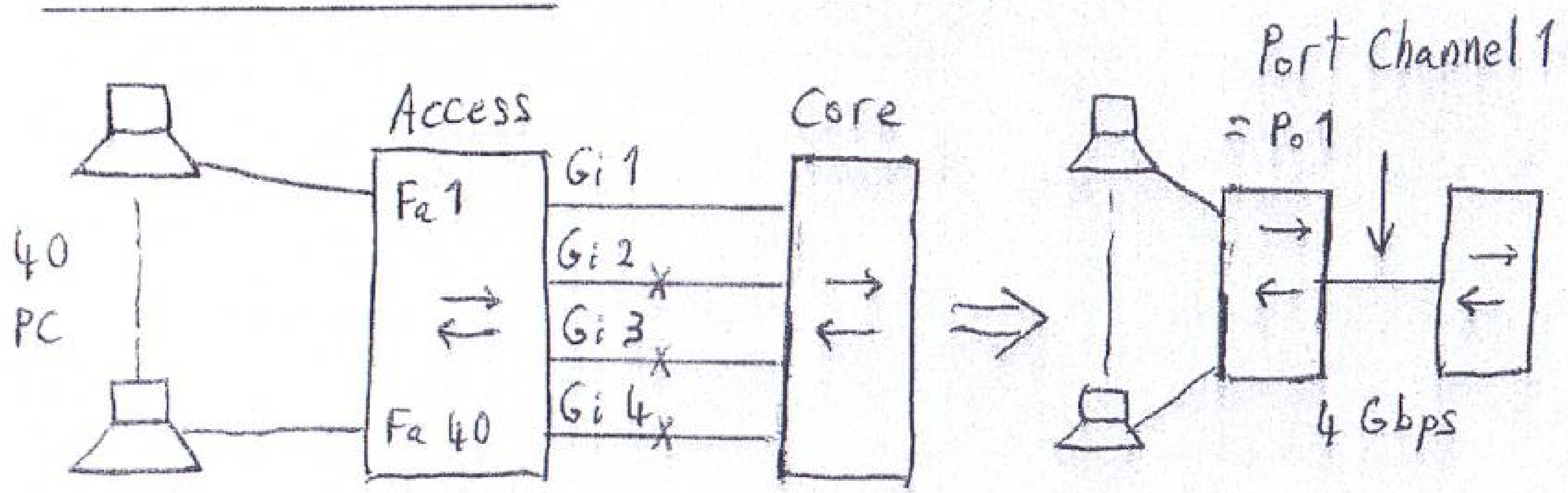




One advantage of the closed stacking loop is that individual switches can be inserted or removed without breaking the path between switches completely. The ring can be broken to add or remove a switch, But if stack cable is broken bandwidth percentage is reduced by 50%, but the remaining switches stay connected over the rest of the ring.

* Cable Virtualization:

Link Aggregation: EtherChannel (EC)



40 PC X 100 Mbps = 4000 Mbps = 4 Gbps

* no. of BP = 4 - 2 + 1 = 3

EtherChannel Benefits:

1 Logical grouping of many physicals ports:

Use
- PAgP: Port Aggregation Protocol
- LACP: Link Aggregation Control Protocol

PAgP: Cisco → merge 2 - 8 Links

LACP: Standard → merge 2 - 16 Links
- 8 Active
- 8 standby

(IEEE 802.3ad)

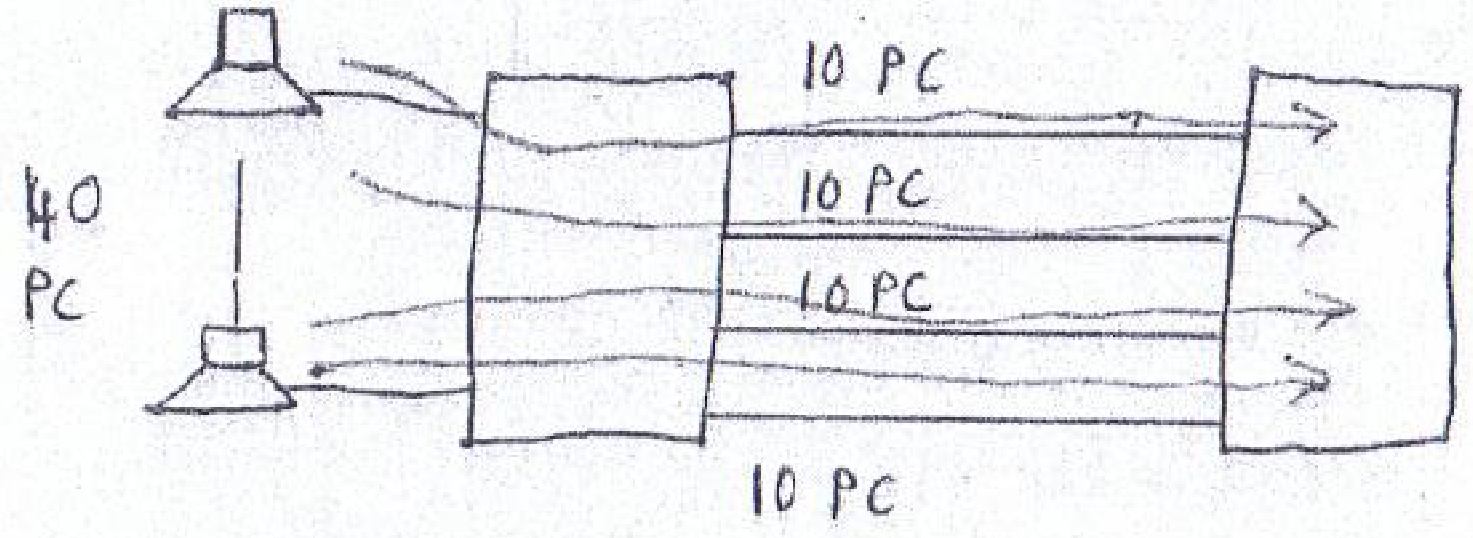
(config)# interface range G 1-4

(config-if-range)# channel-protocol {LACP / PAgP}

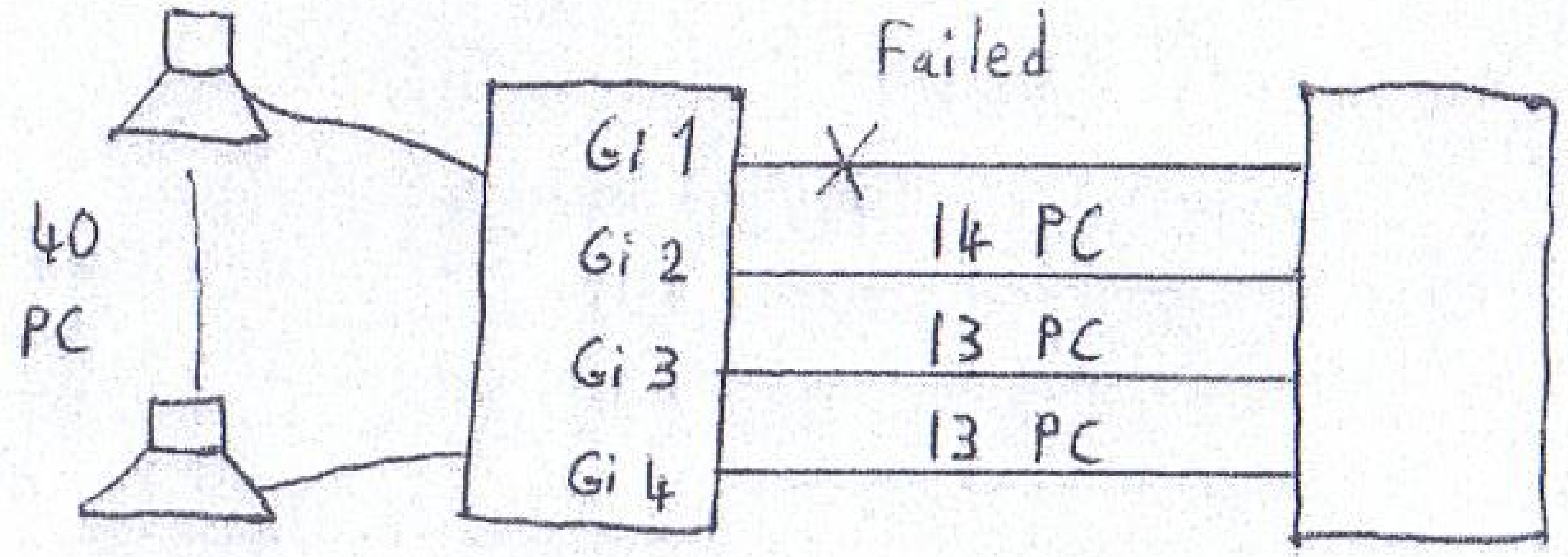
(config-if-range)# channel-group # {Active / desirable, Passive / auto}

Po #

2 Load Distribution: Increase BW

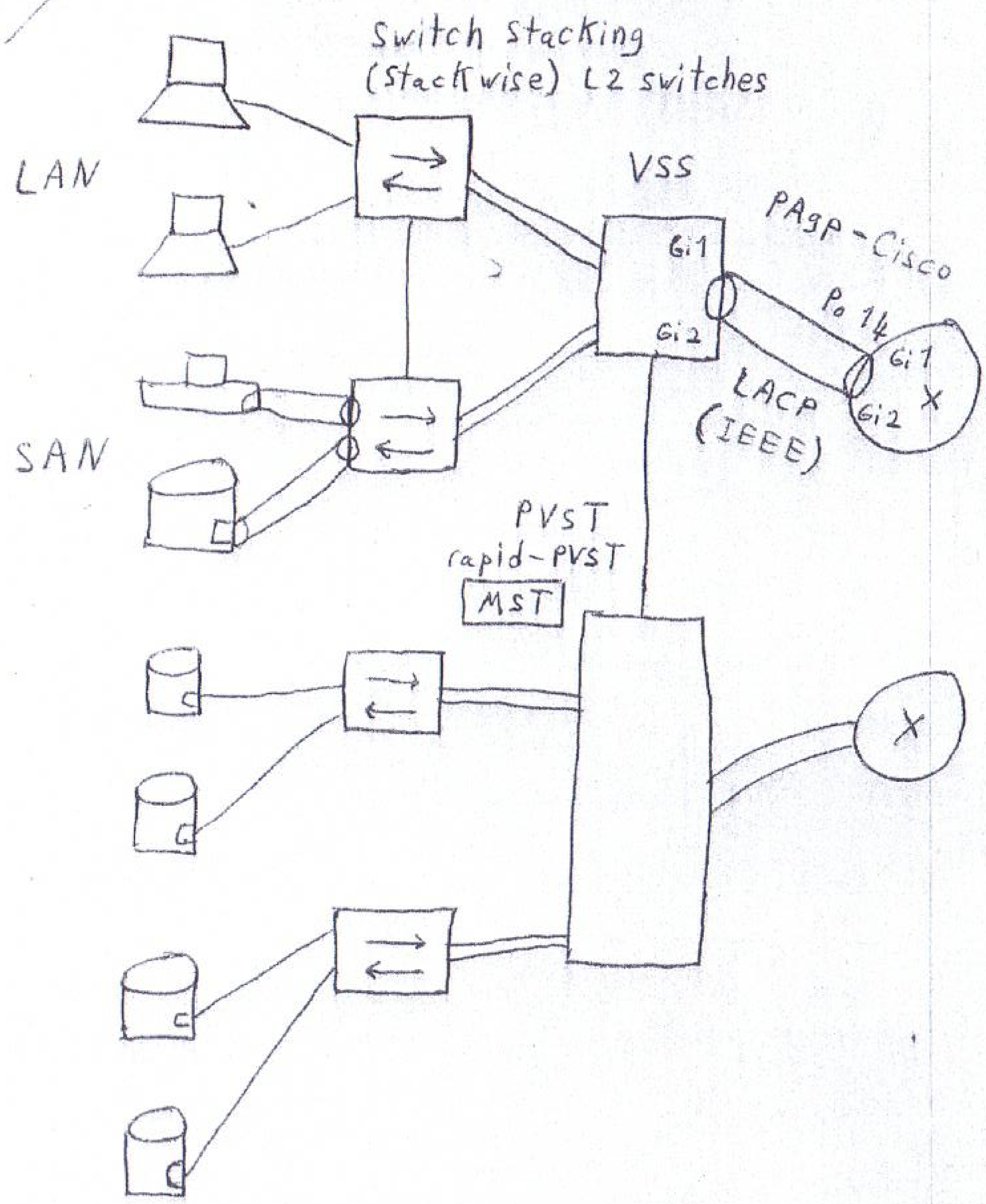


3 Link Level Redundancy:



Session 3/2

Building a Data Center:



Router:

(config)# int. Gi 1

(config-if)# channel-protocol lacp

(" -if)# channel-group 14 mode active

(config)# int. Gi 2

(config-if)# channel-protocol lacp

(" - if)# channel-group 14 mode active

#show etherchannel summary

Po 6	Gi 1, Gi 2

(config)# int. Po 14

(config-if)# ip address 192.168.1.1 255.255.255.0

Switch: (config)# interface range Gi1-2

(config-if-range)# channel-protocol lacp

(" - " - range)# channel-group 6 mode active

EC Conditions: VTAS DS NS NS D

VTAS → same — vlan conf. / trunk conf. / stp conf.

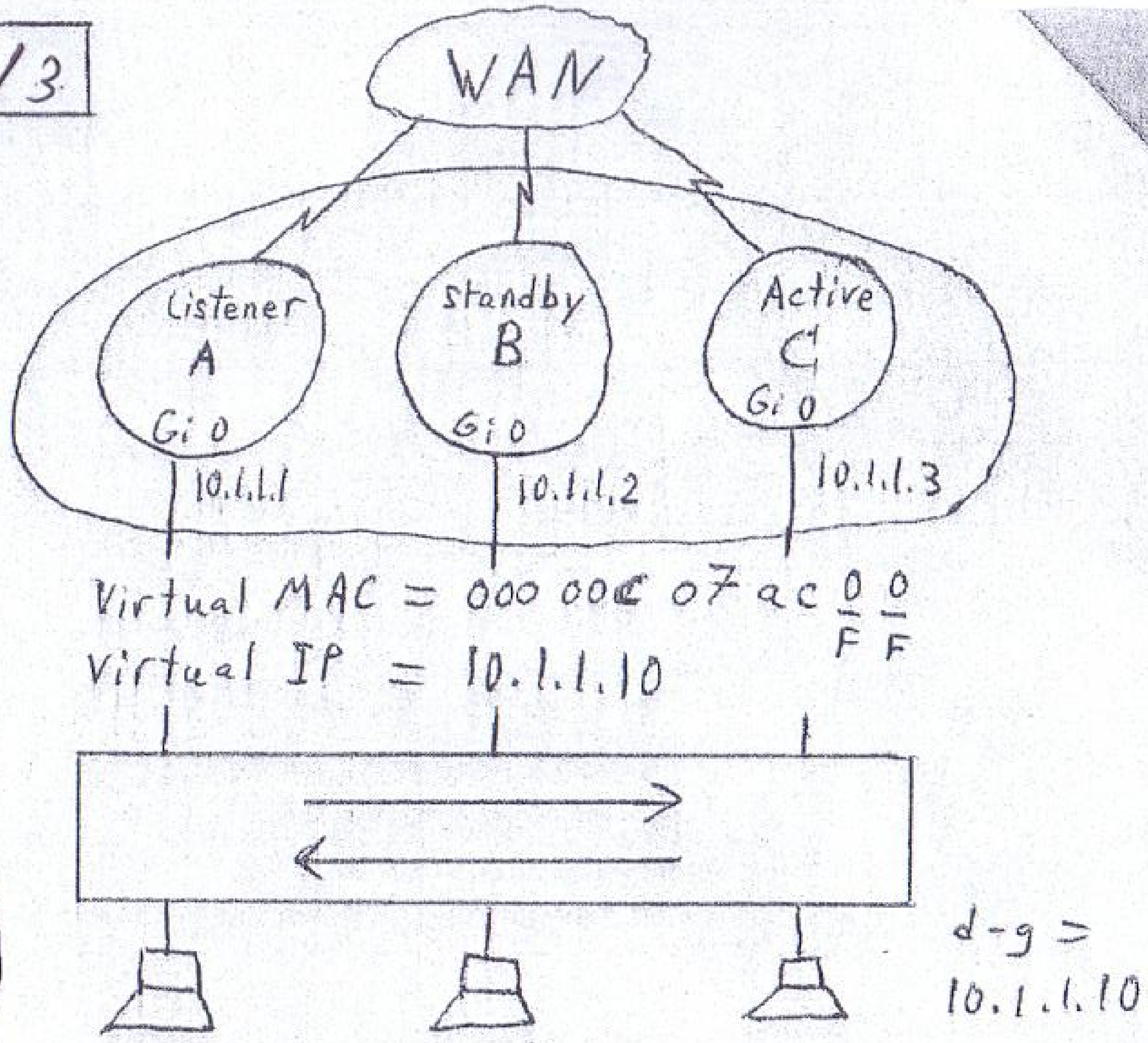
no port security conf.

DS → Same speed — same duplex

FHRP (First Hop Redundancy Protocol)

Session 3/3

* HSRP: Hot Standby Redundancy Protocol – Cisco
  - Active / standby
* VRRP: Virtual Router Redundancy Protocol – Standard
  - Master / Backup
* GLBP: Gateway Local Balancing Protocol – Cisco
  - Active / Active



Elections:
1 Active router / 1 Standby router — highest priority, highest IP
All others are listeners

HSRP Operation:

@Startup:

A B C (config)# int. Gi 0

(config-if)# standby # (group no, 8 bit, (0–255)) ip 10.1.1.10 (virtual IP)

C (config-if)# standby 1 priority >100

(config-if)# standby 1 track S0/0

(config-if)# standby 1 Preempt

Preempt
#show standby

Neighbor Discovery: "Exchange of Hello"

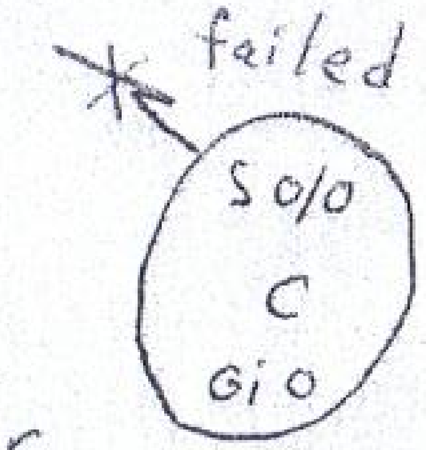
Each router sends hello every 3 sec on multicast 224.0.0.2

@Change:

If Active fails ⇒ Standby will be new active

(Hold time = dead time = 10 sec) ⇒ Listener will be new standby

If Active, WAN Link fail



Object Tracking:

If WAN link failed, Active Router will decrement its priority.

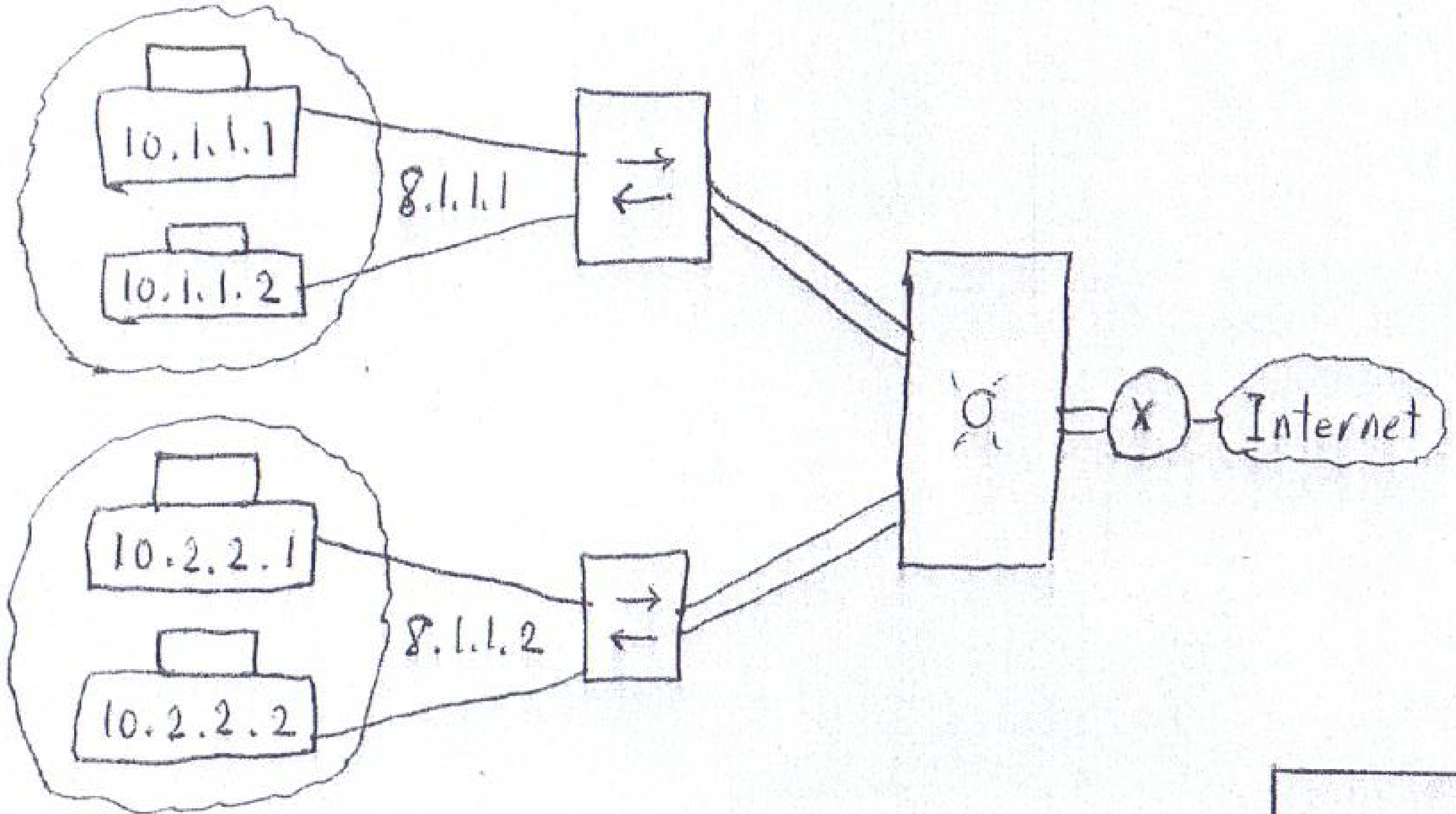
Immediately ⇒ Standby is new active
Listener is new standby

Session 3 / 4

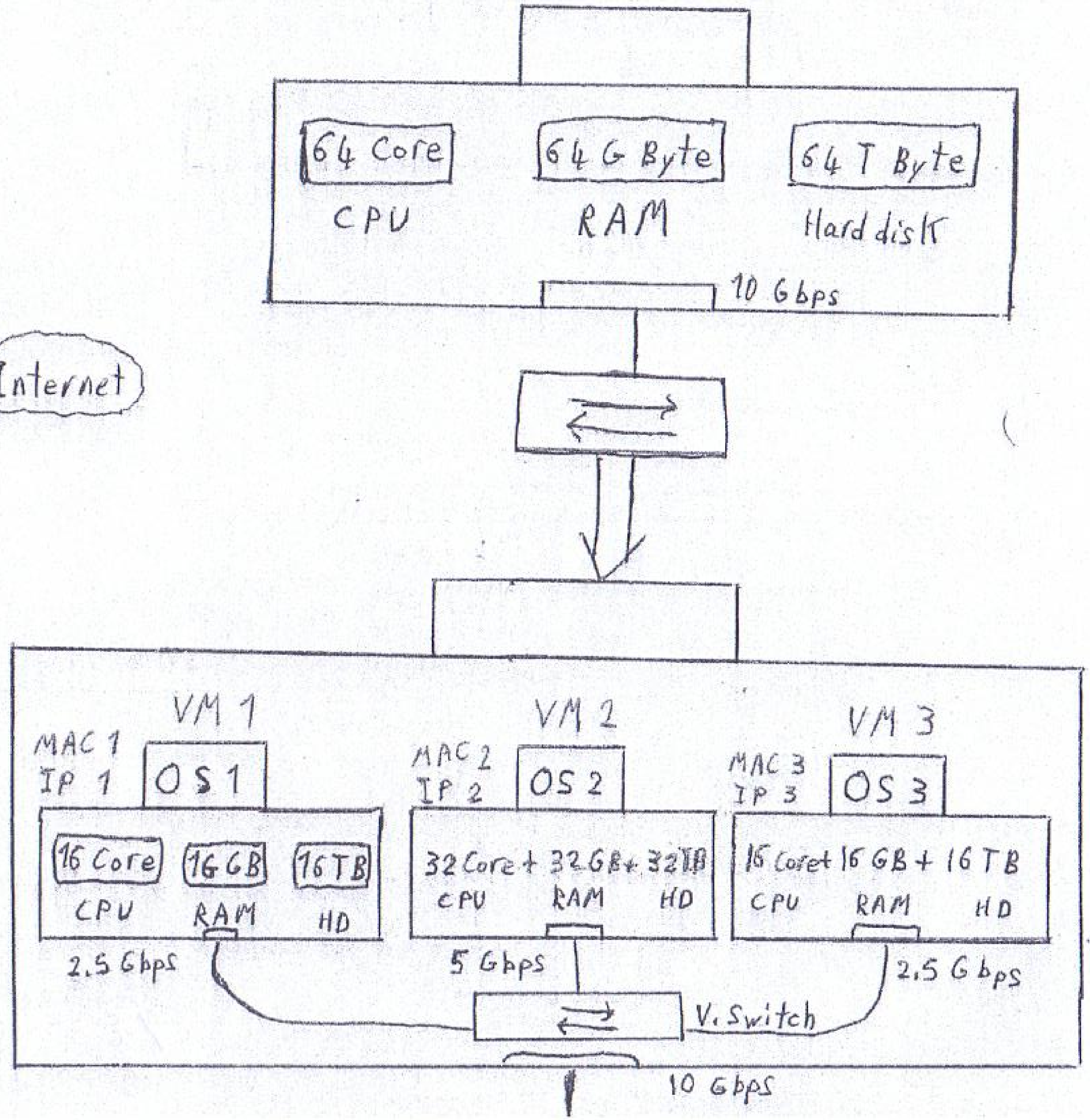
Server Virtualization:

It is merging many servers to act as virtual server using SLB (Server Load Balancing)

Redundancy   Load Balancing



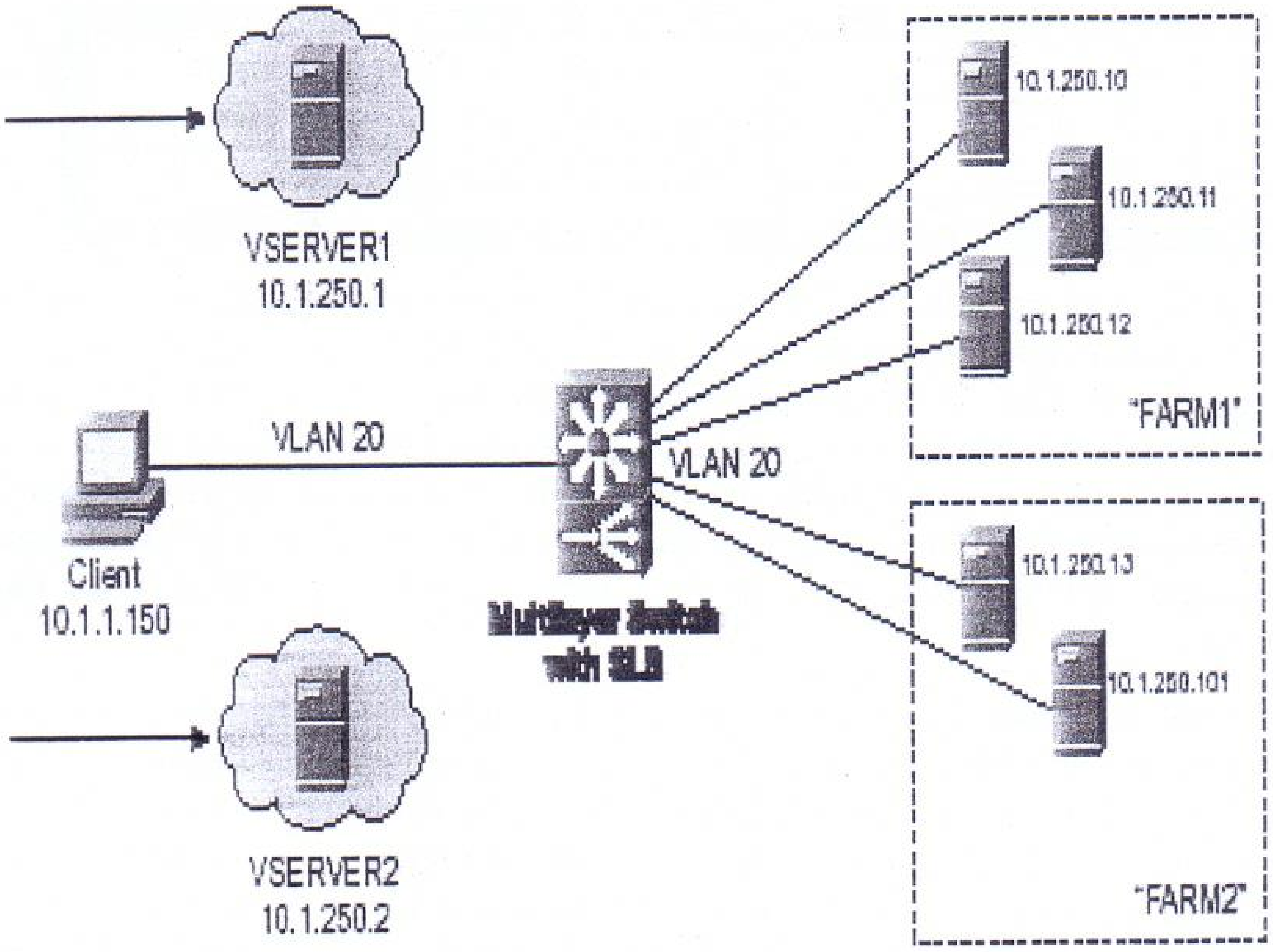
It is dividing Main Server into smaller sub Servers called VM (Virtual Machines)



Server Virtualization & Cloud Fundamentals:

SLB: (server load balancing)

- It is grouping many physical servers to act as one virtual server.
- Each of the router redundancy protocols allows a router to take the identity of one or more others.
- This can also be used to intelligently forward traffic to multiple destinations, in other words one or more physical destination s can hide behind a single virtual address.
- SLB provide virtual server IP address to a group of real physical servers organized as a server farm.
- The client never knows which real server it is connecting with, only the SLB router knows that for sure, the client knows the virtual server IP address.



Advantages of SLB:

1-Extra layer of security is possible

2-Taking one of the servers for maintenance can happen at any time with no effect on transmission

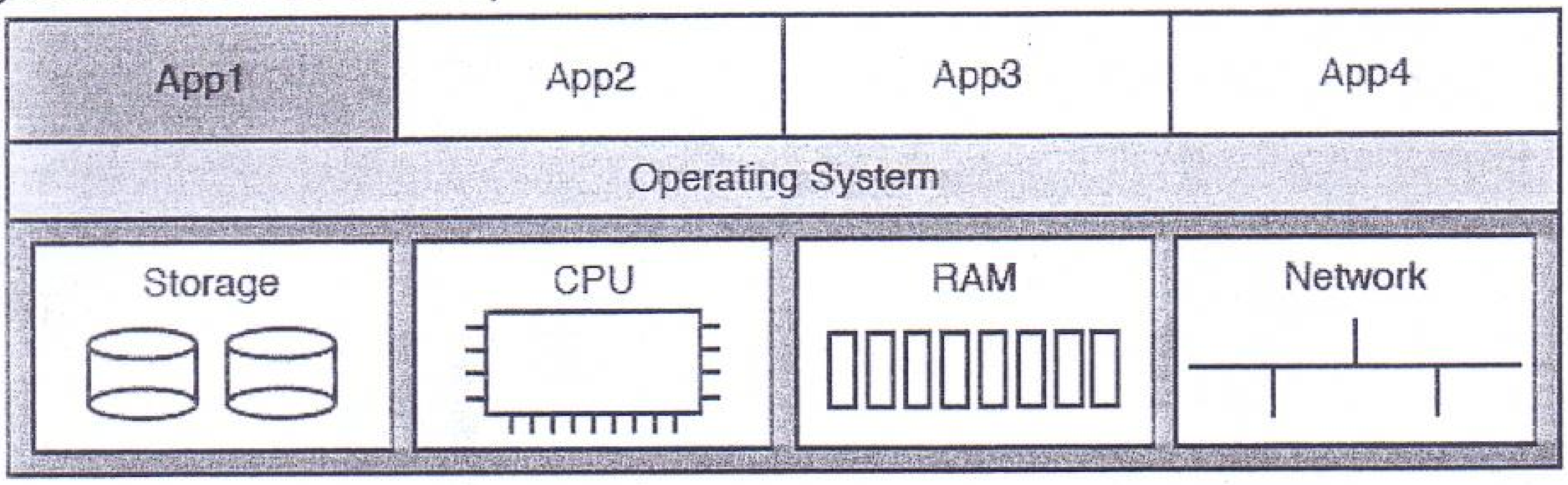
Server Virtualization

When you think of a server, what comes to mind? Is it a desktop computer with a fast CPU? A desktop computer with lots of RAM? Is it hardware that would not sit upright on the floor, but could be easily bolted into a rack in a data center? When you think of a server, do you not even think of hardware, but of the server operating system (OS), running somewhere as a virtual machine (VM)?

VM (Virtual Machine):

It is dividing physical server into subservers called VM.

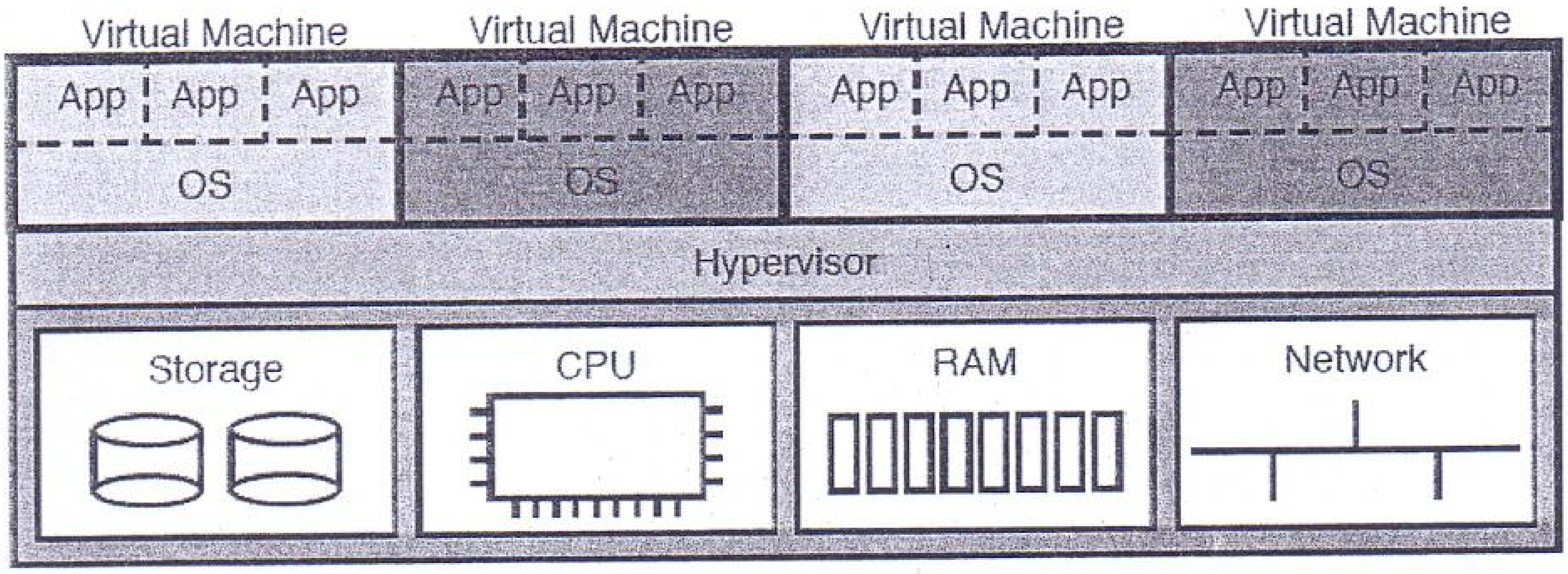
Think of a server as a computer having a big memory (RAM), CPU (processor with many cores), storage (hard disk) and fast NIC (ten gigaethernet or more)

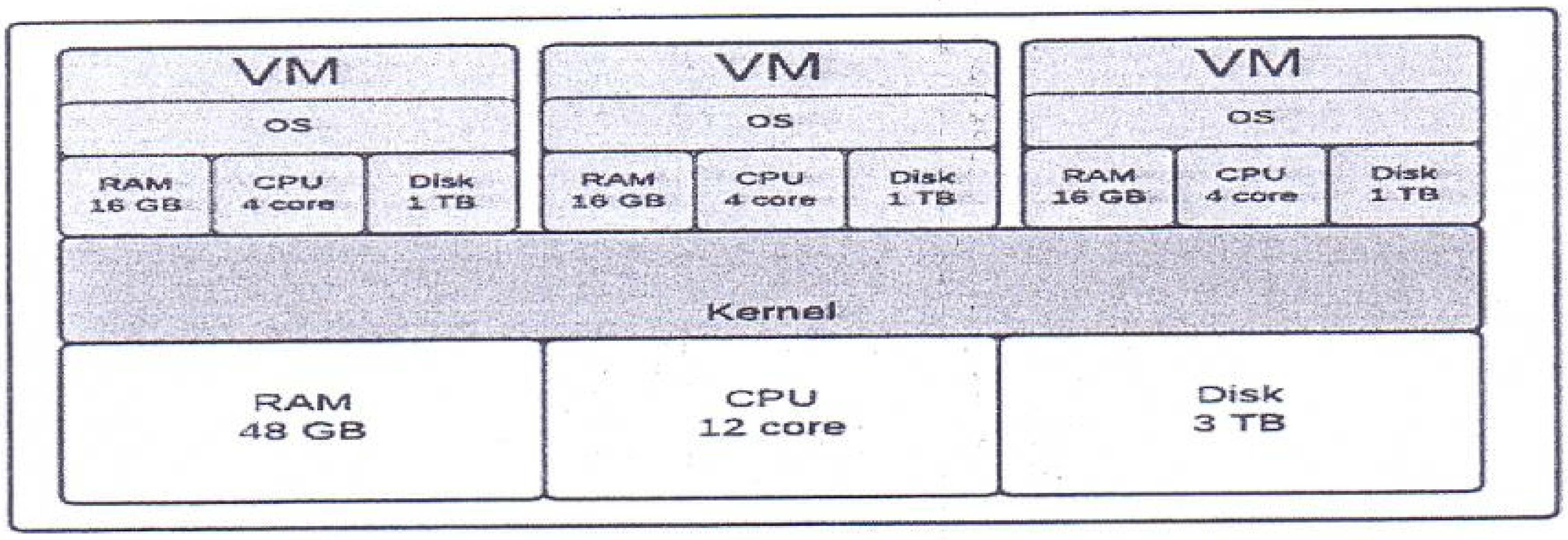


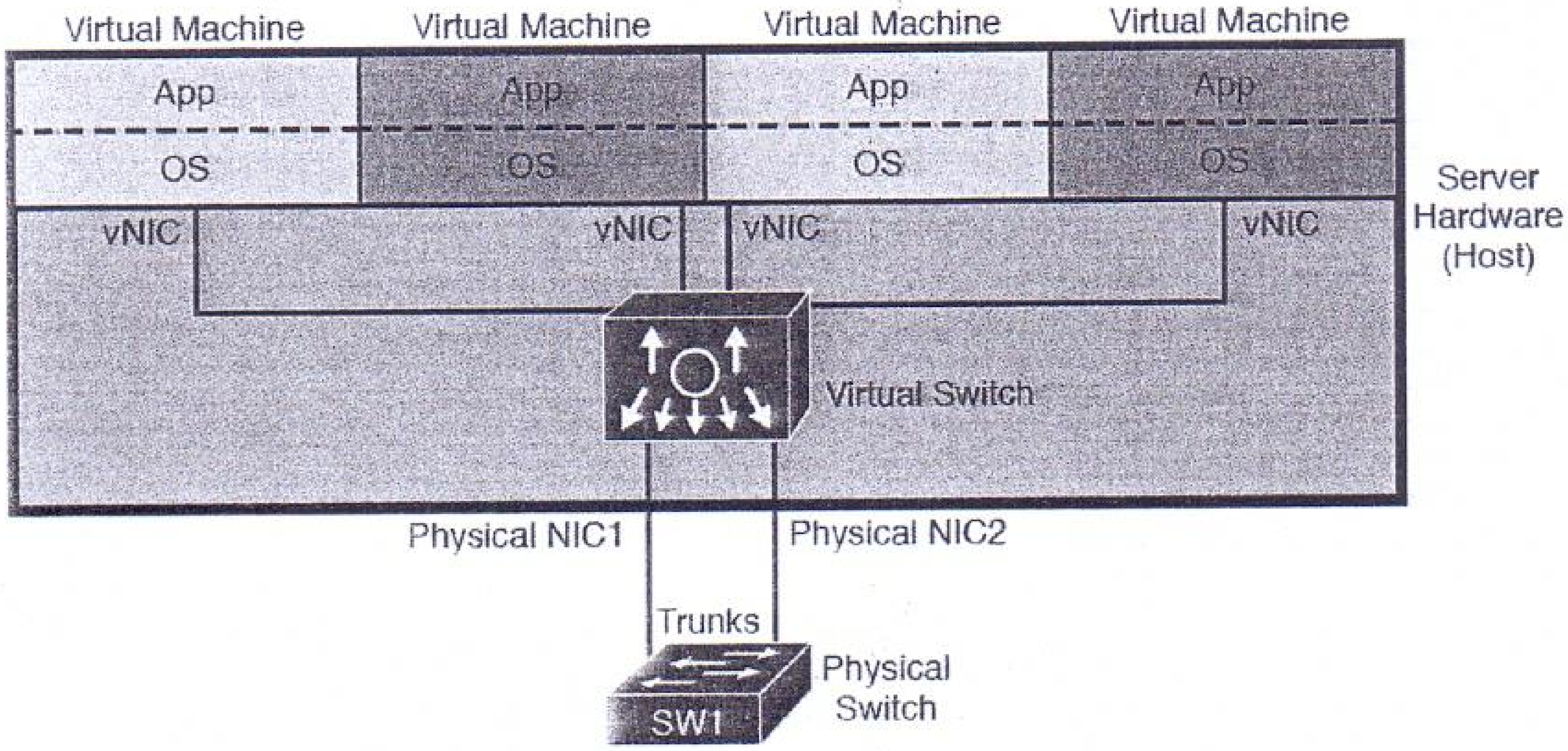
A single physical host (server) often has more processing power than you need for one OS. Thinking about processors for a moment, modern server CPUs have multiple cores (processors) in a single CPU chip. Each core may also be able to run multiple threads with a feature called *multithreading*. So, when you read about a particular Intel processor with 8 cores and multithreading (typically two threads per core), that one CPU chip can execute 16 different programs concurrently. The hypervisor (introduced shortly) can then treat each available thread as a virtual CPU (vCPU), and give each VM a number of vCPUs, with 16 available in this example.

A VM—that is, an OS instance that is decoupled from the server hardware—still must execute on hardware. Each VM has configuration as to the minimum number of vCPUs it needs, minimum RAM, and so on. The virtualization system then starts each VM on some physical server so that enough physical server hardware capacity exists to support all the VMs running on that host. So, at any one point in time, each VM is running on a physical server, using a subset of the CPU, RAM, storage, and NICs on that server. Figure 27-3 shows a graphic of that concept, with four separate VMs running on one physical server.

To make server virtualization work, each physical server (called a *host* in the server virtualization world) uses a *hypervisor*. The hypervisor manages and allocates the host hardware (CPU, RAM, etc.) to each VM based on the settings for the VM. Each VM runs as if it is running on a self-contained physical server, with a specific number of virtual CPUs and NICs and a set amount of RAM and storage. For instance, if one VM happens to be configured to use four CPUs, with 8 GB of RAM, the hypervisor allocates the specific parts of the CPU and RAM that the VM actually uses.







To connect the marketplace to the big ideas discussed thus far, the following list includes a few of the vendors and product family names associated with virtualized data centers:

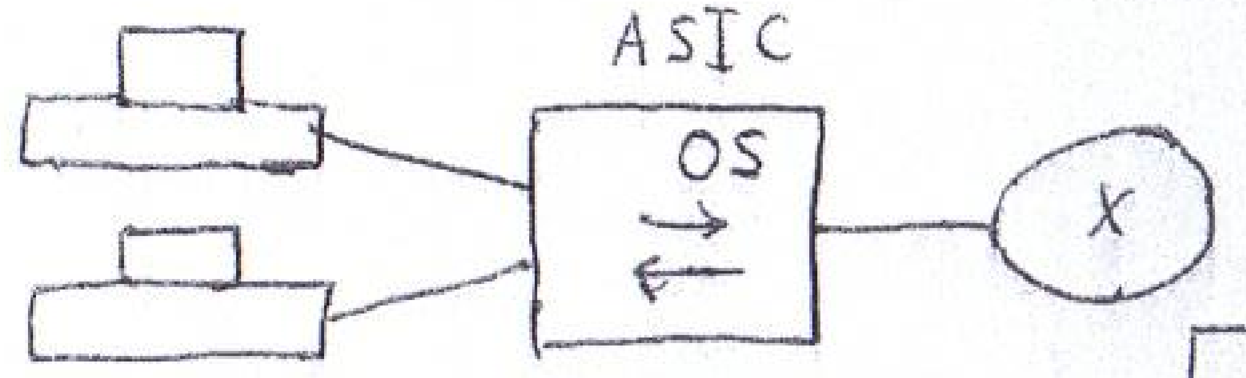
- VMware vCenter (new is VMware VSphere)
- Microsoft HyperV
- Citrix XenServer
- Red Hat KVM

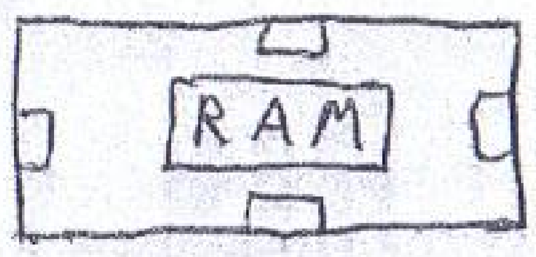
Session 4/1

SDN (Software Defined Network):

Network Programability = Network Automation = Network Orchestration

* new generation of networks are SDN based

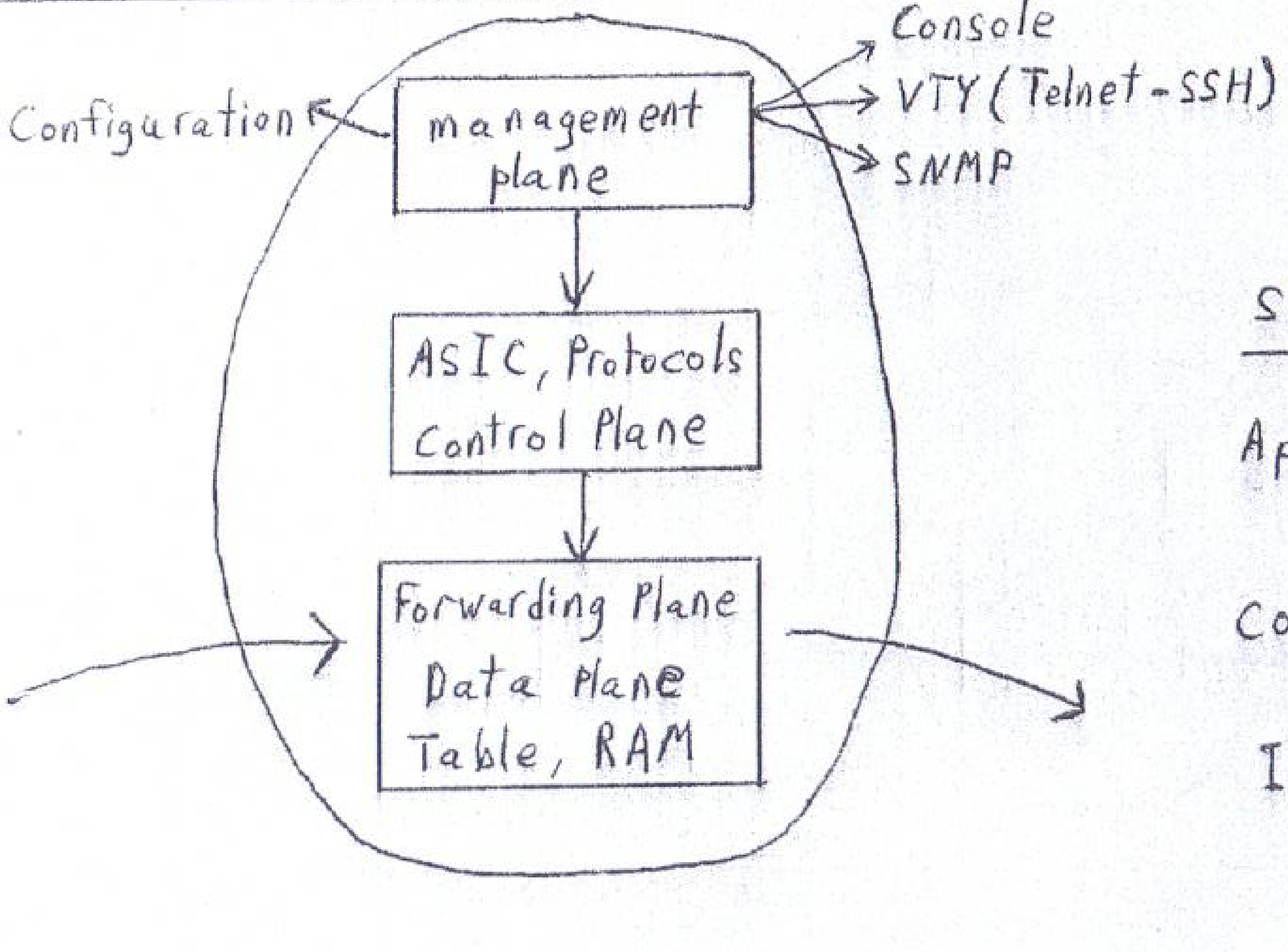


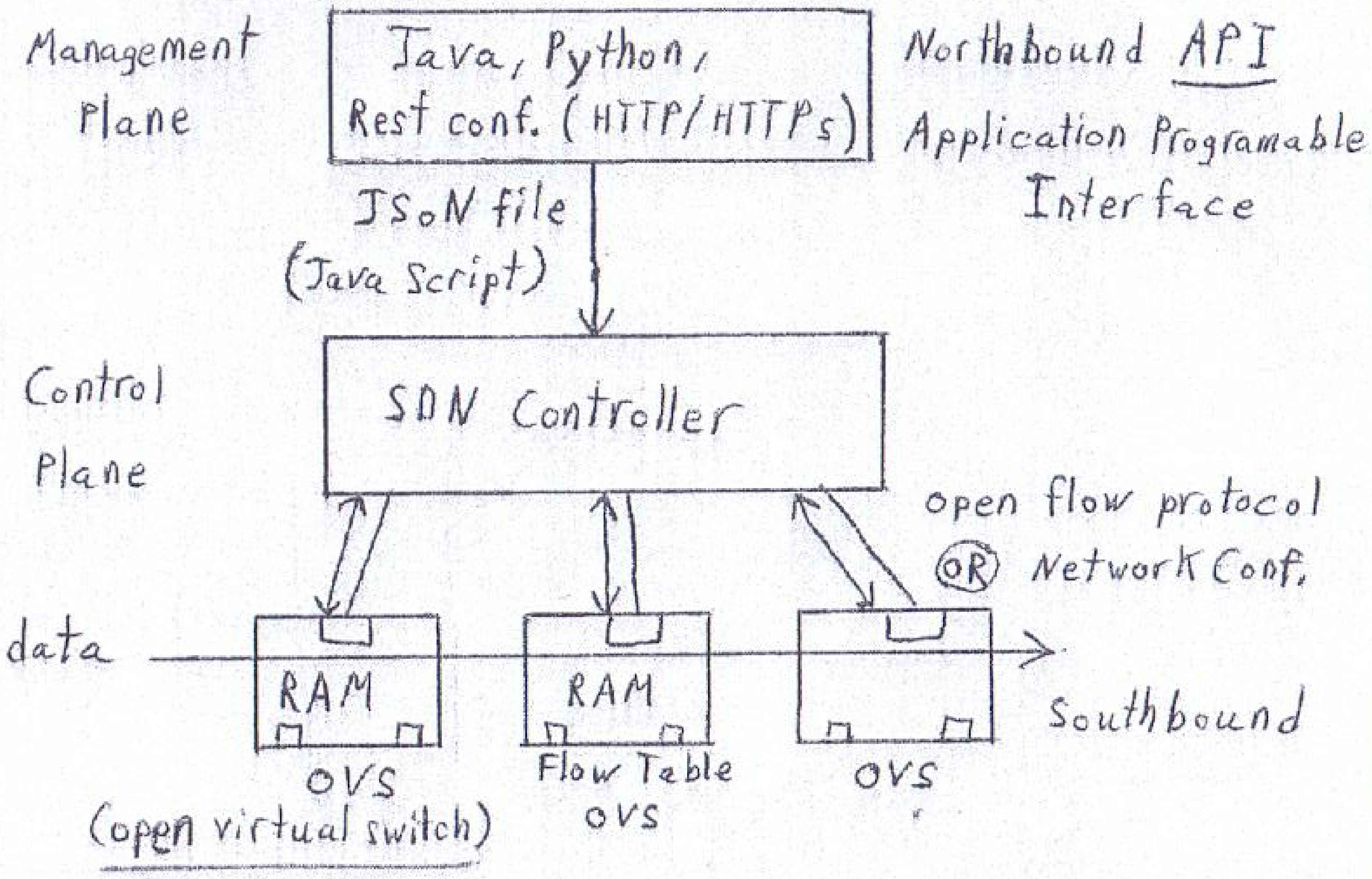


Light Weight Device:

- no IOS
- no conf. file
- no ASIC
- only RAM & Interface

Traditional Network:





SDN Model:

Application Layer	Northbound API	rest conf.
Control Layer	Controller	open flow
Infrastructure Layer	Southbound	

SDN Famous Controllers

1. ODL (Open Day Light) → standard
   (Open Network Foundation) → ONF
2. HPE VAN
3. VMWare
4. Cisco
   - Meraki SD LAN
   - Viptela SD WAN - APIC - EM
   - ACI Servers Data Center - Cisco DNA
5. Juniper

SDN: Software Defined Network

"Network Programability"
"Network Automation"
"Network Orchestration"

- traditional networks require Switches, routers, Firewalls & etc...

all these devices need 3 planes to work Properly:

- Management Plane.

It is all S/W & H/W inside each device that makes the device managable, like Console, VTy (Telnet) Lines, SNMP & etc...

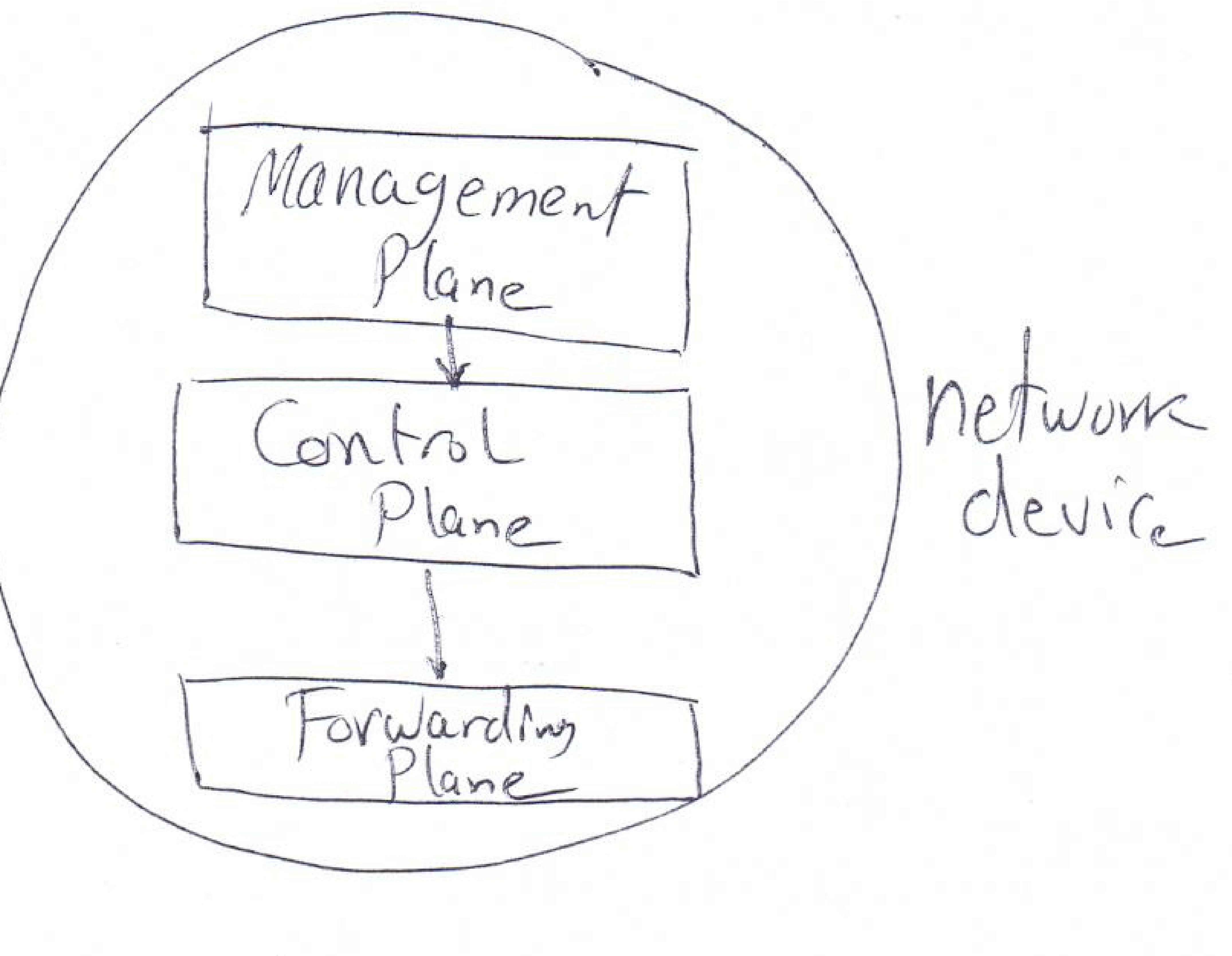
- Control Plane:

It is all the ASICs, S/w, Protocols & Operating System | Configuration file needed by the device to Provide its functionality.

Like Learning ASICs, forwarding ASICs, Security ASICs, QoS ASICs, Switching Protocols (STP | DTP | CDP | ...), Routing Protocols (OSPF / BGP / ---), Routing ASICs (CEF).

- Forwarding Plane:

It is all interfaces (WICs/NICs), memories (RAM) & tables (routing table, Switch table (MAC table), NAT Table & Inspection Table (for firewall & other Security devices)

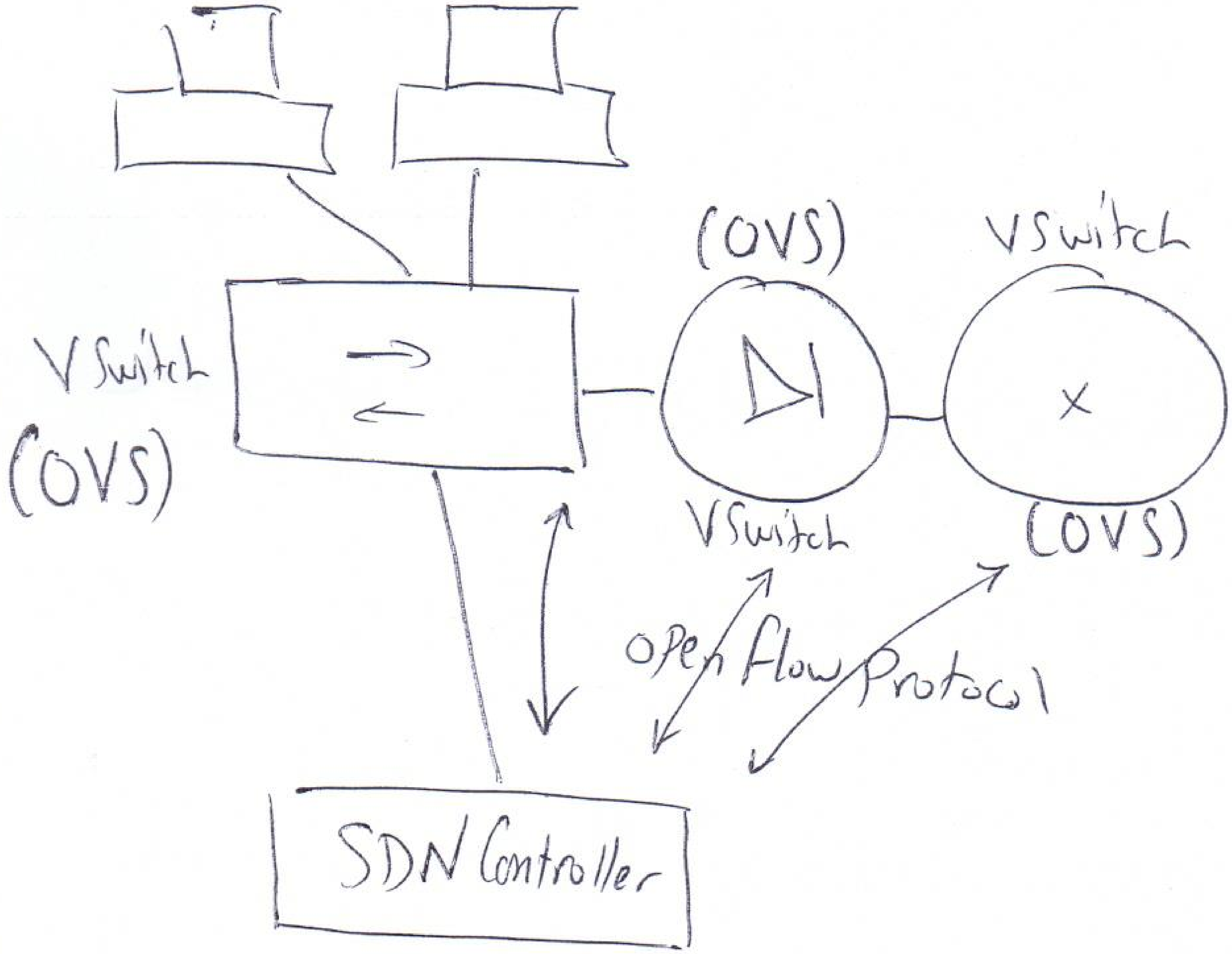


SDN is a new Cloud trend (Iaas) that will split functionality, So Some devices have the Management plane & Control Plane & Some other devices have the forward Plane.

- SDN Controller will form all required Management & Control plane tasks

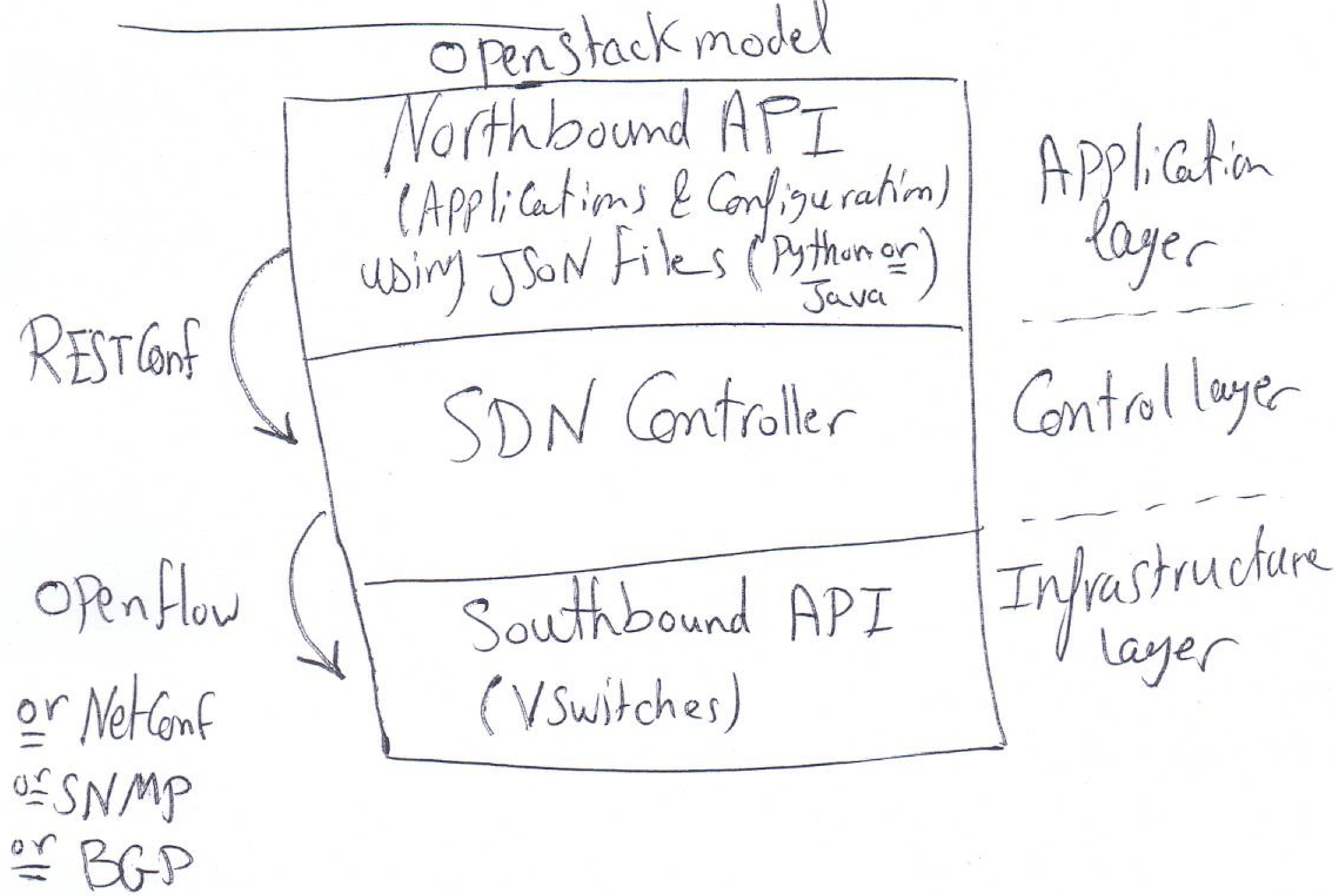
- OVS (open virtual switch
= VSwitch (V Box) = Virtual Switch will form all required forwarding Plane tasks.

- the Communication between SDN Controllers (recommend minimum of 3 Controllers) & the VSwitch will be Performed Using the "Open flow" Protocol



SDN standards are introduced by ONF (Open Network Foundation)

SDN model:



- **Northbound API** (Application Programable Interface)

It is the interface between network admin. & the SDN Controller.

the admin. makes all the required Programing & Configuration using Python or Java to Create JSON Files (Java Script files)

- Southbound API:

All the SDN management & Control Planes instructions are then Sent to the VSwitches using OpenFlow Protocol.

⇒ Southbound devices recive a flow table that Contains how data flow will be forwarded.

- Standard SDN Controller is ODL (OPen Day Light)

- Cisco has a lot of SDN Controllers
(Meraki For LAN (SD-LAN),
ViPtela for WAN (SD-WAN), APIC-EM (Enterprise Module)
ACI for Data Center (SD-Servers)
& Major Controller is Cisco DNA (Digital Network Architecture)

- Cisco Currently provides Hybrid SDN devices.

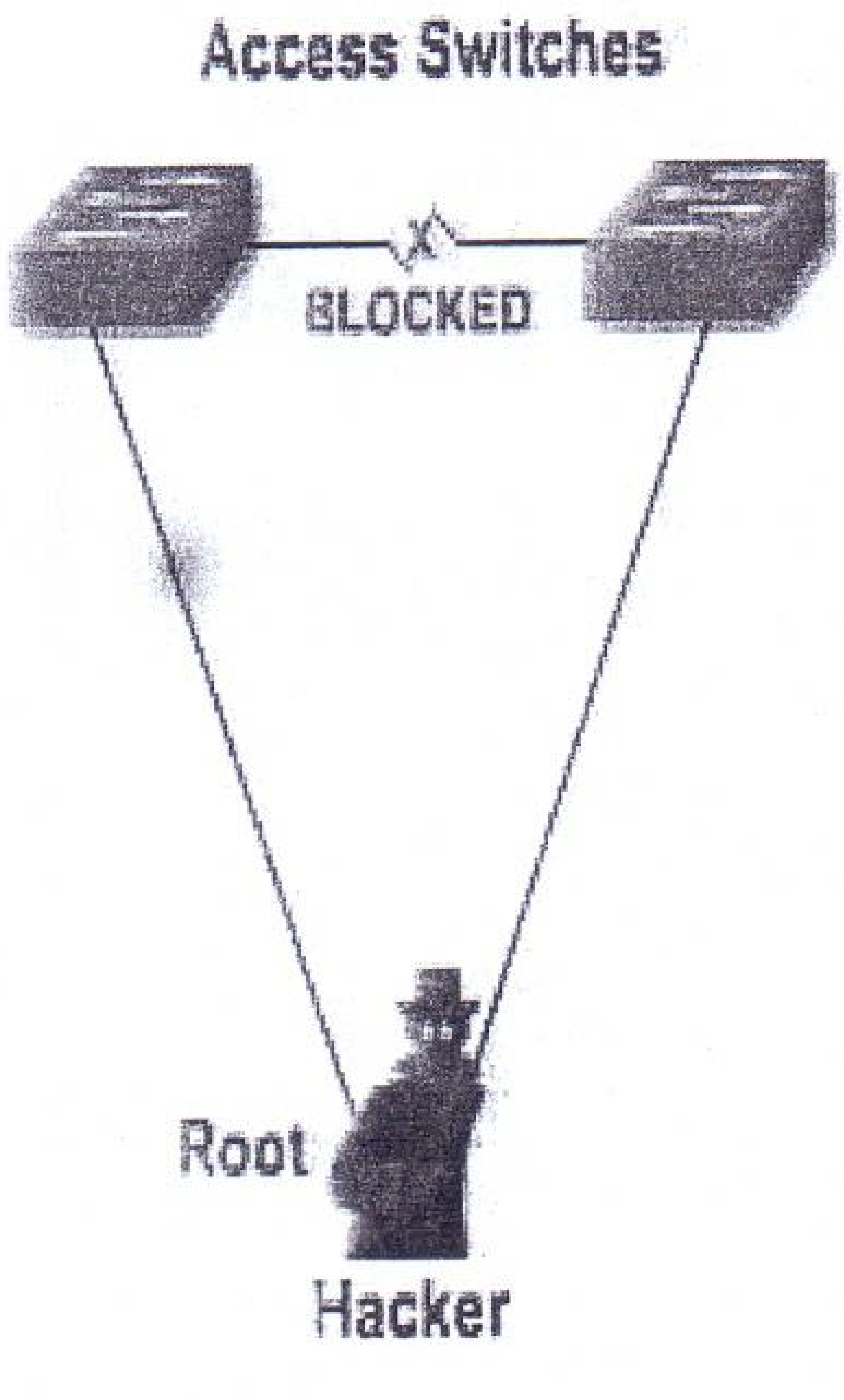
these Hybrid devices first attempt to work with SDN Controller, but if SDN Controller fails, it will work in the traditional fashion, where each device will standalone depends on its management & Control planes to form the data forwarding plane.

& if the Controller is back again, it will work as a lightweight device depending on the Controller to form the forwarding decisions.

Top SDN Controllers are:

1. OpenDaylight (ODL) → Standard
2. VMWare/NiCira
3. HP (HPE VAN) Virtual Application Network
   → Enterprise
4. Juniper (Contrail)
5. Cisco (DNA Center) also APIC-EM/ViPtela
   Meraki / ACI
6. BroCade (Vyatta)

Securing Network Access



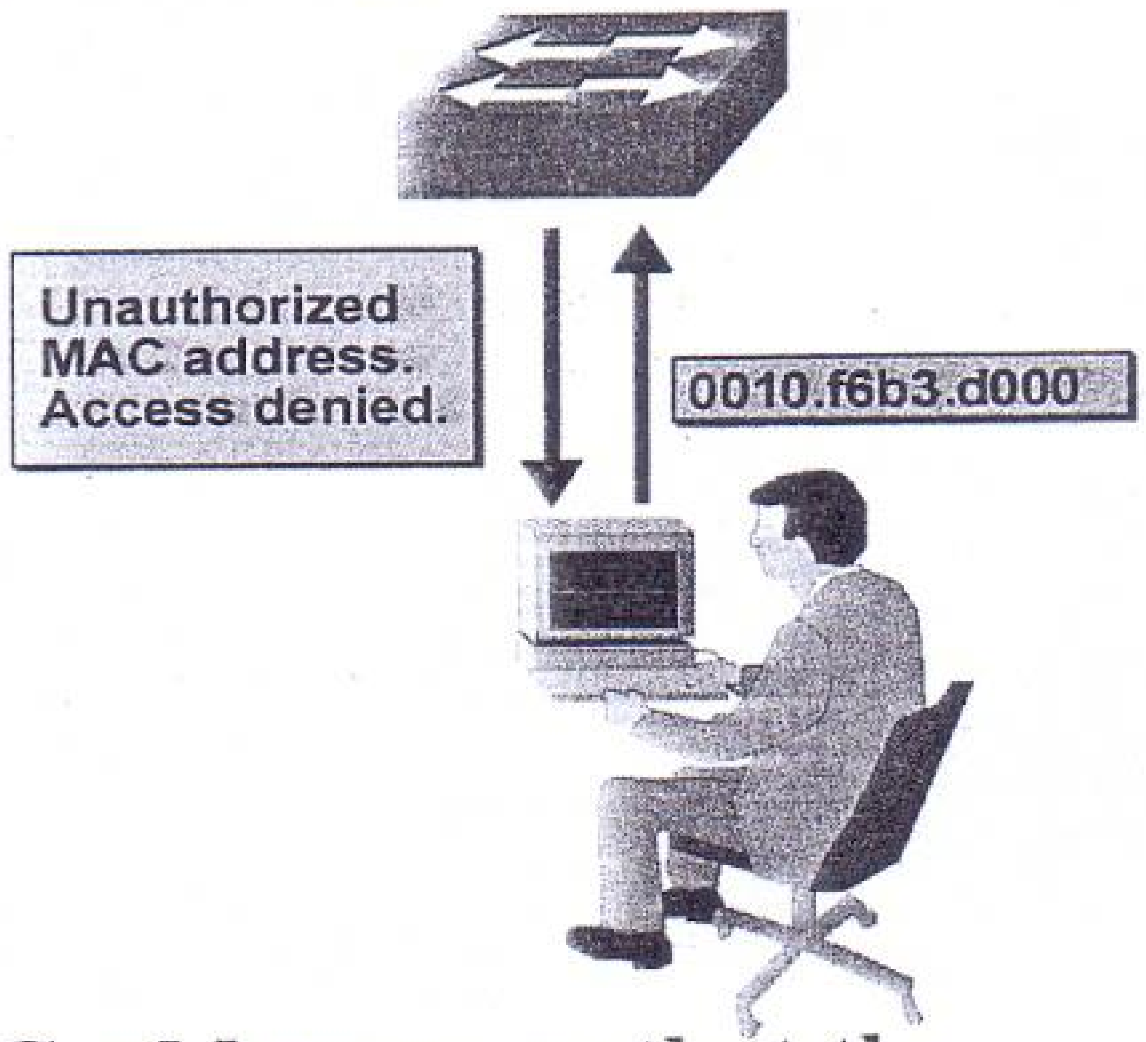
MAC table overflow attack

MAC Flooding

MAC flooding is the attempt to exploit the fixed hardware limitations of the MAC table of a switch, so switch will flood all traffic after that attack (act as a hub)

Mitigating the MAC table overflow attack

The MAC table-overflow attack can be mitigated by configuring **port security** on the switch . This option provides for either the specification of the MAC addresses on a particular switch port or the specification of the number of MAC addresses that can be learned by a switch port. When an invalid MAC address is detected on the port, the switch can either block the offending MAC address or shut down the port.



- **Enable port security feature**

Switch(config-if)# switchport port-security

- **you must identify a set of allowed MAC addresses so that the port can grant them access.**

Switch(config-if)# switchport port-security maximum <u>max-address-no.</u>

- **You can also statically define one or more MAC addresses on an interface.**

Switch(config-if)# switchport port-security mac-address <u>mac-address</u>

Switch(config-if)# switchport port-security mac-address sticky

- **Violation action**

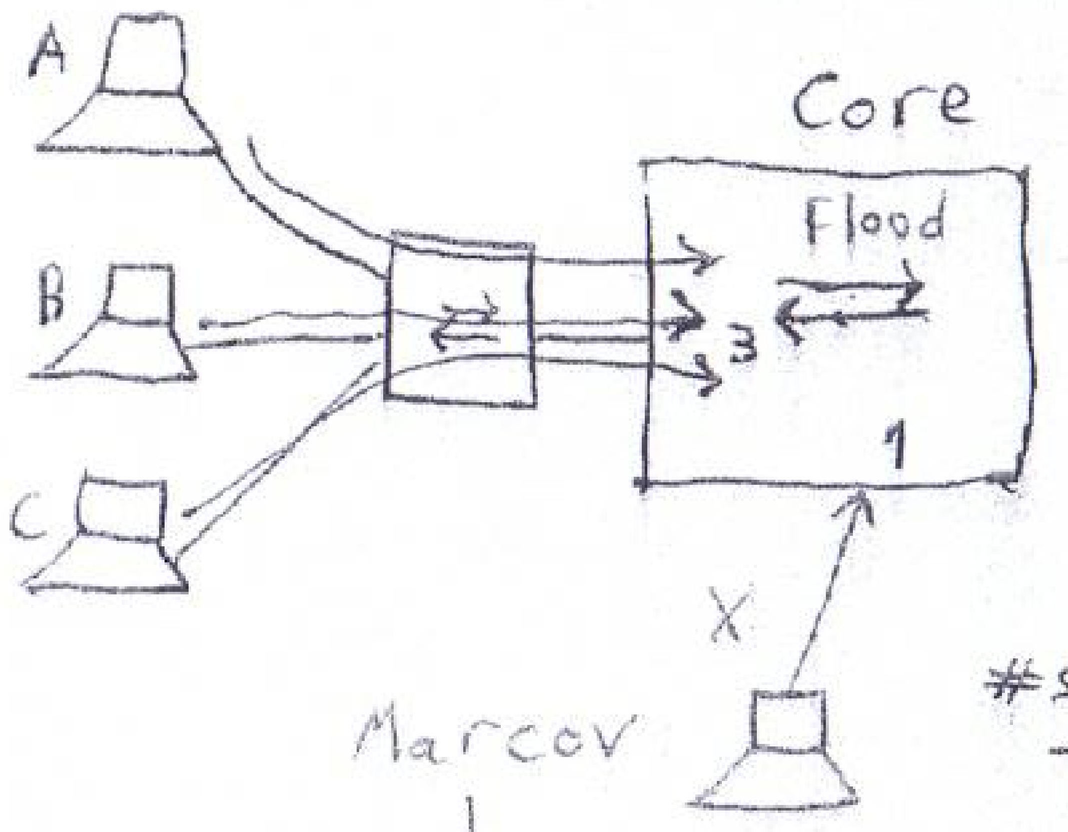
Switch(config-if)# switchport port-security violation {shutdown | restrict | protect}

Ahmed Nabil

Maged Abd El-Wareth

Security Attacks:

1. MAC table flooding/overflow: Converts switch to hub
   - Sniffering Attack
   - DOS attack (Denial Of Service)



RAM

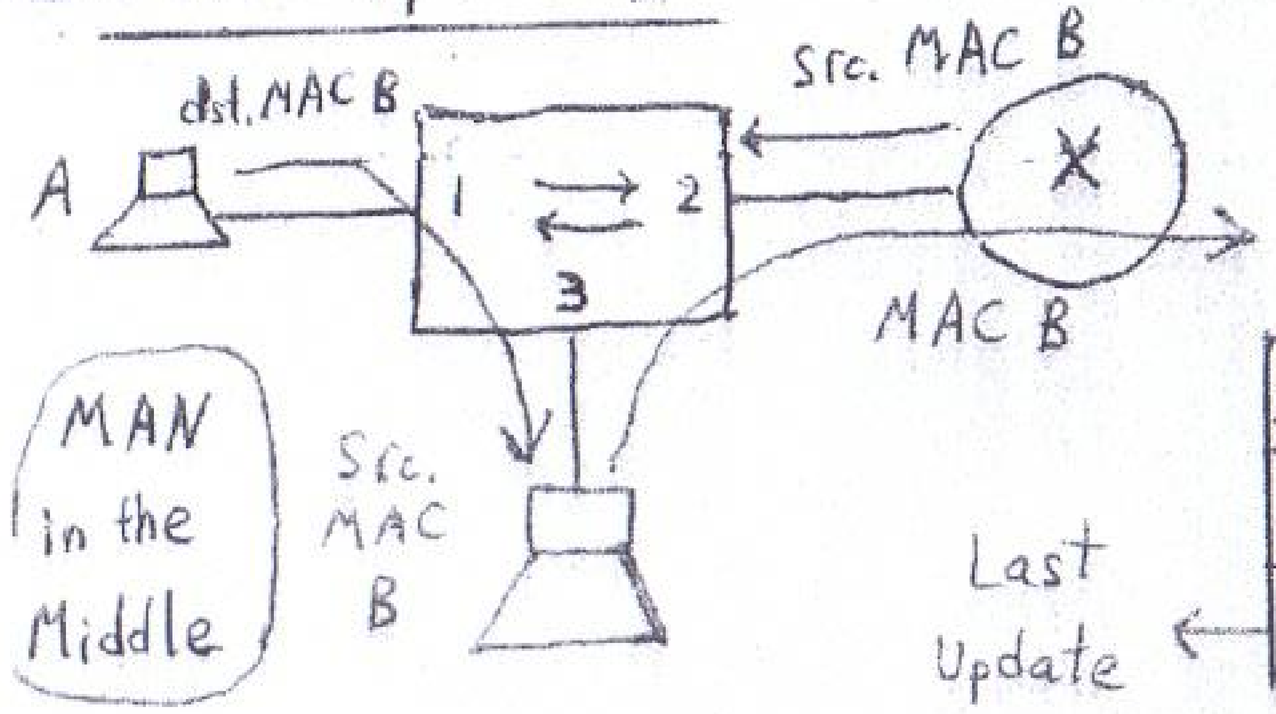
MAC	Port
X	1
Y	1
Z	1
⋮	⋮

#show mac-address -table

Bogus frames — src. mac X | src. mac Y | src. mac Z

frames with headers only, doesnt carry data. → 100,000 frames/sec

2. MAC Spoofing:



MAC	Port
~~B~~	~~2~~
B	3

Last Update

Mitigation

MAC	Port	
B	2	→ Static
~~B~~	~~3~~	→ Dynamic

Mitigation < MAC Flooding → Port Security; MAC Spoofing → Port Security + Sticky

Mitigation

Port Security:

(config)# interface fa 3

(config-if)#switchport port-security — only one MAC allowed on that Port; Port vill shutdown

err-disable state ← in case of voilation

(config-if)#switchport port-security maximum 3
(" -if)#switchport port-security mac A
(" -if)#switchport port-security mac B
(" -if)#switchport port-security mac C

(" - ")#switchport port-security mac sticky

(" - ")#switchport port-security violation { Restrict / Protect }

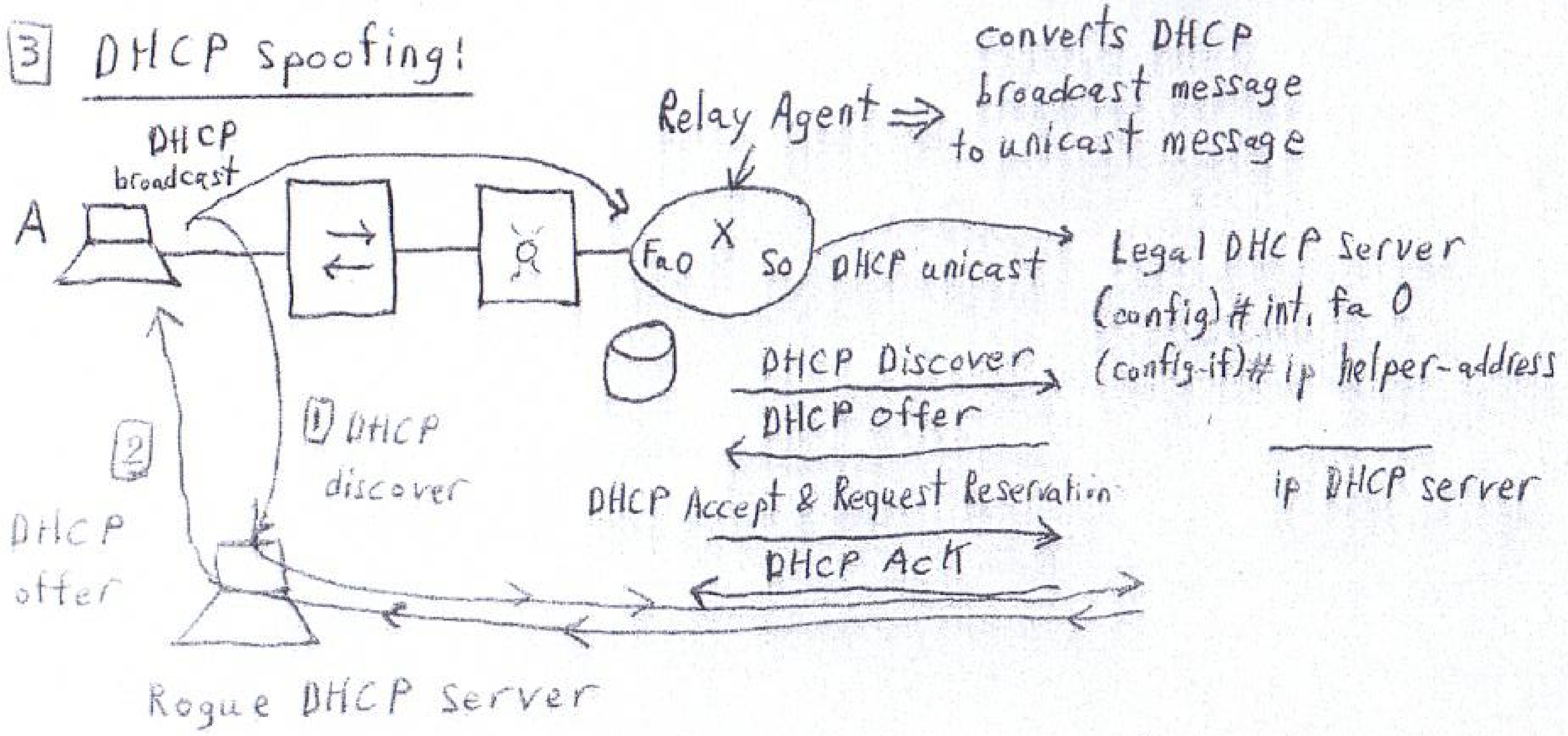
Deny unknow MAC
Permit Known MAC

#show port-security Interface

Session 5/2

Security Attacks:

3 DHCP Spoofing:



* Device A receives Hacker's DHCP offer first before DHCP Server as (first offer is the best offer).

Mitigation:

DHCP Snooping:

(config)# ip dhcp snooping

↓

* Switch will make all switch ports untrusted: deny DHCP Server msg. / offer

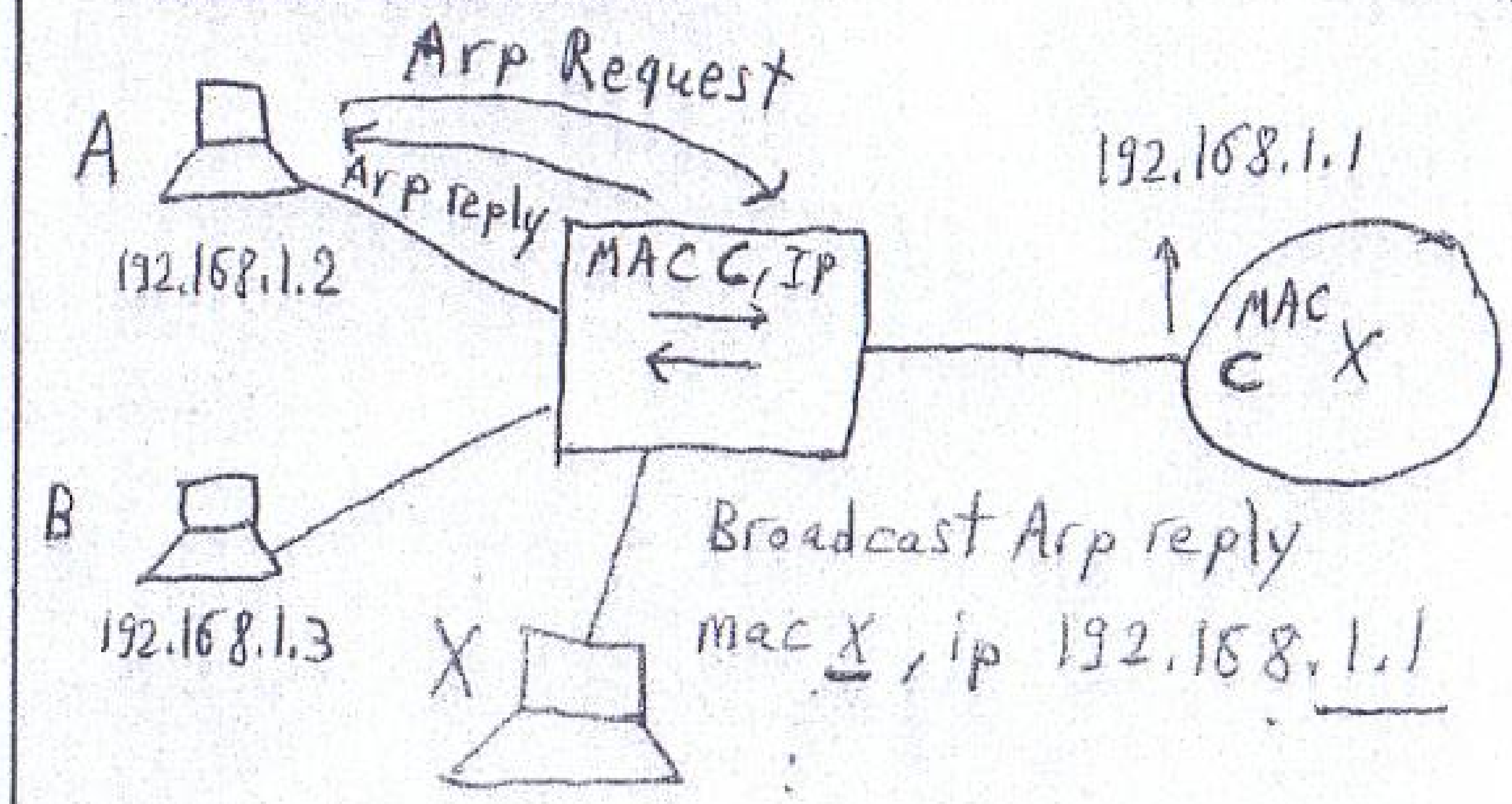
(config) # int. Gi 1

(config-if)# ip dhcp snooping trust

DHCP Snooping Table

IP	MAC	Port	Lease
192.168.1.2	A	fa 1	24 hrs
192.168.1.3	B	fa 2	24 hrs
192.168.1.1	C	fa 3	

4 ARP Spoofing:



Arp Cache

MAC	IP
~~C~~	~~192.168.1.1~~
X	192.168.1.1 → last update is best update

Mitigation:

DAI: Dynamic Arp Initiation

(config)# ip arp inspect

↓

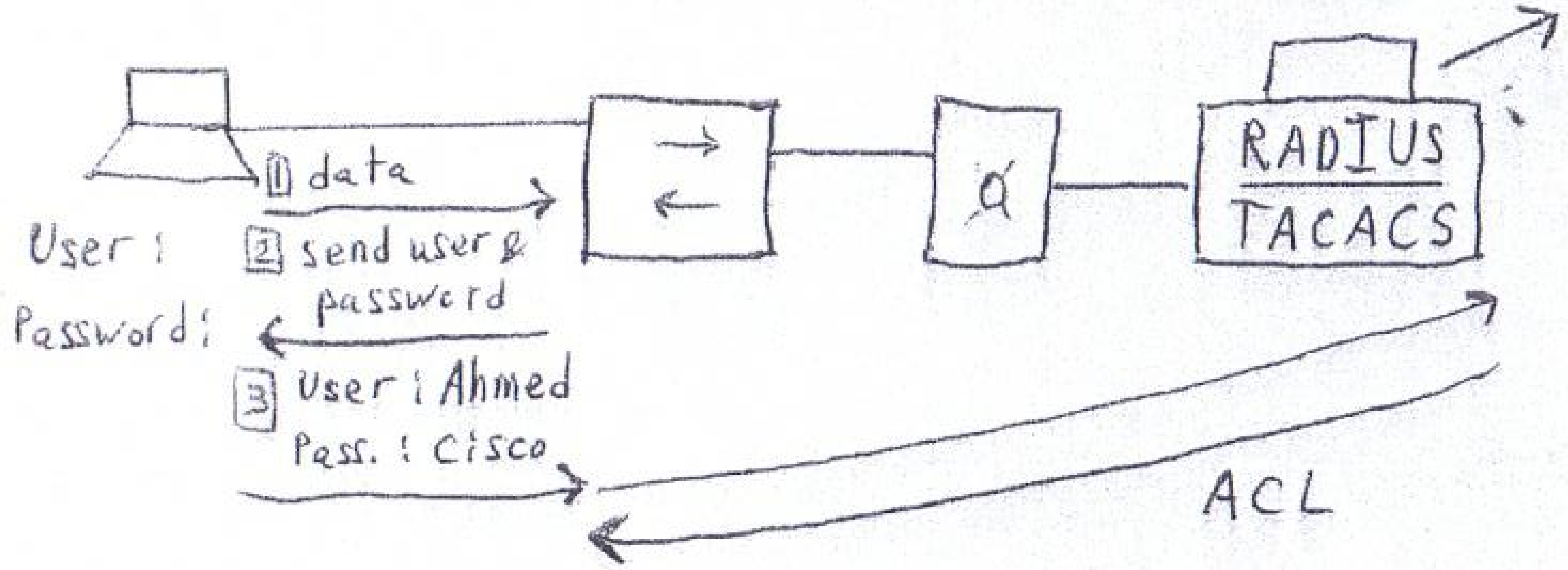
* Switch will open all arp messages and compare arp reply to DHCP Snooping Table.

Session 5 /3

AAA (Authentication, Authorization, Accounting)

controlling users' access with IEEE 802.1X

EAPoL = Extensive Authentication Protocol over LAN



(Privil

User	Password	Authorization	Accounting
Ahmed	Cisco	ACL < permit / deny	start time end time
Omar	Bisco	ACL < permit / deny	
Kiro	Disco	ACL : permit any	

1 Local Database:

(config)# username Ahmed password Cisco
(config)# username Omar password Bisco
(config)# username Kiro password Disco

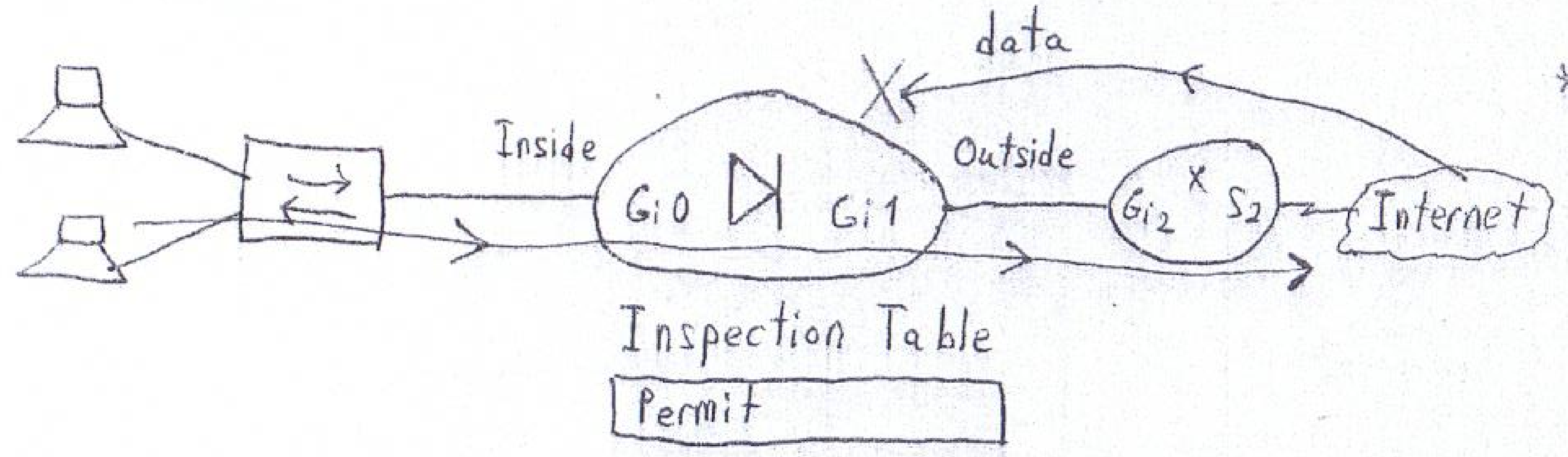
2 RADIUS Server → Standard

3 TACACS Server → Cisco

TACACS	RADIUS
Cisco	Standard
TCP	UDP
Can separate A, A, A on different server	Should combine A, A, A on same server
Encrypt entire packet	Encrypt password only
Limited Accounting	Extended Accounting

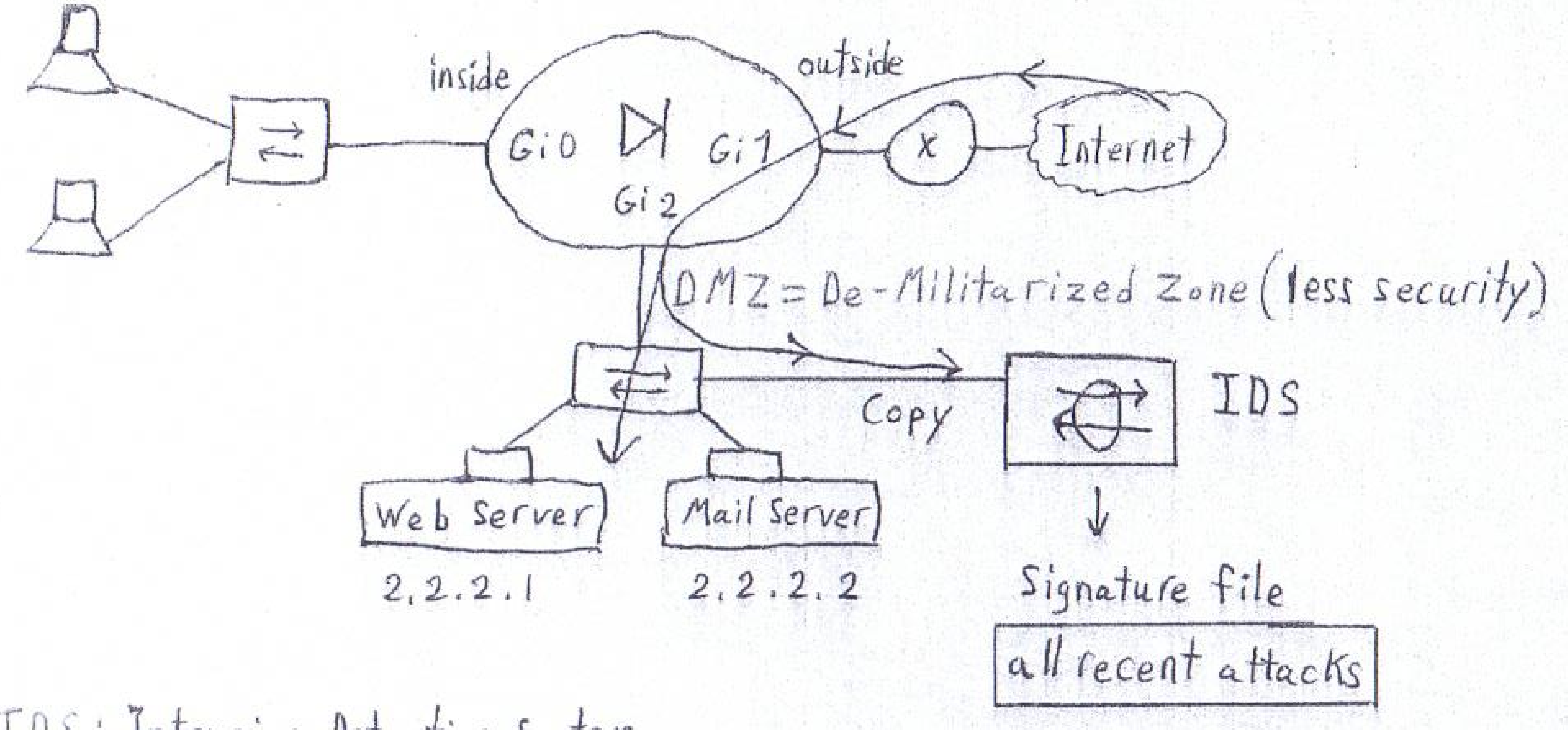
Session 5/4

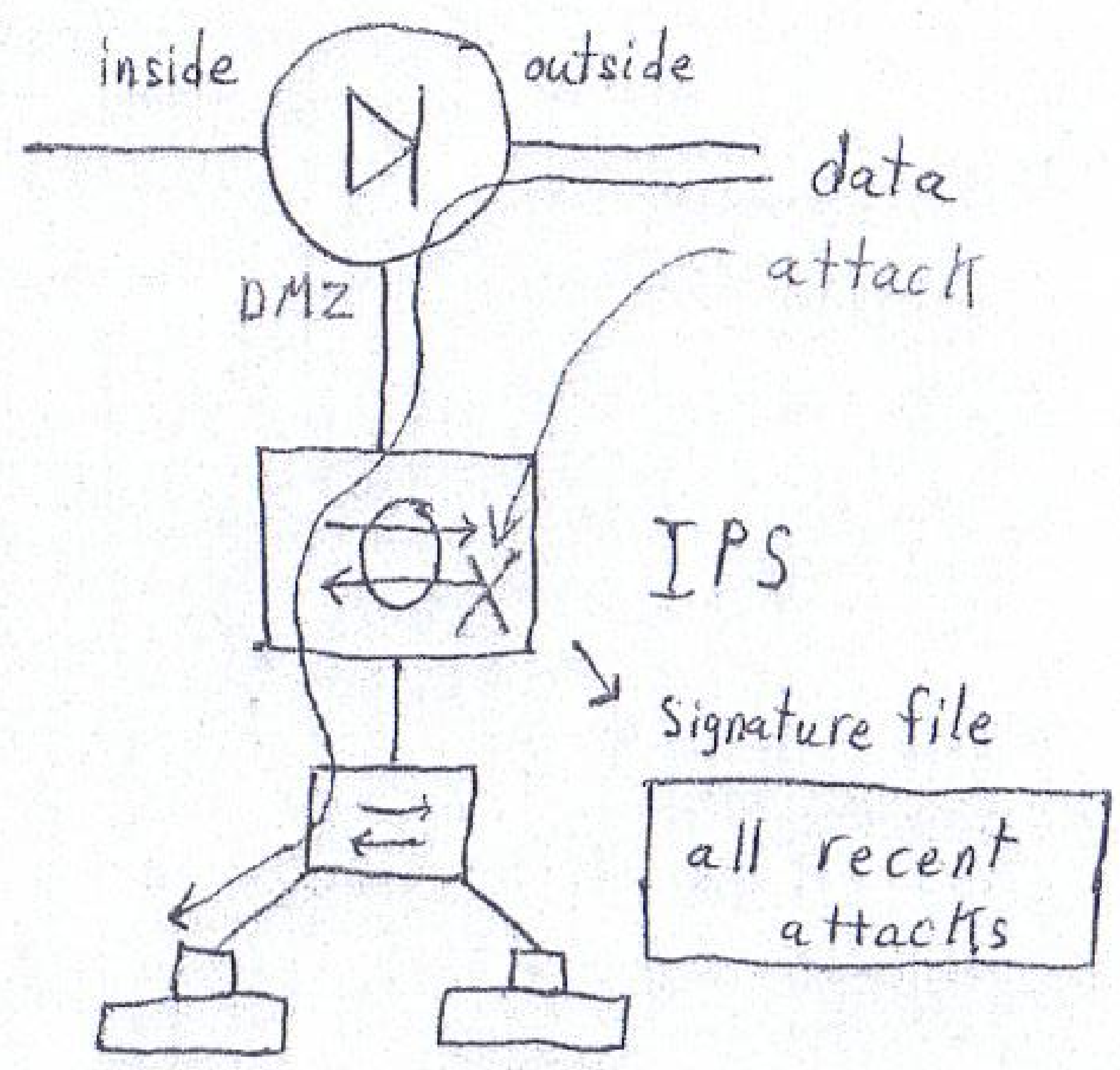
* Firewall:



* Rule 1: Data from outside are not allowed to go inside.

* Rule 2: Data from inside are allowed to go outside





IDS: Intrusion Detection System

IPS: Intrusion Prevention System

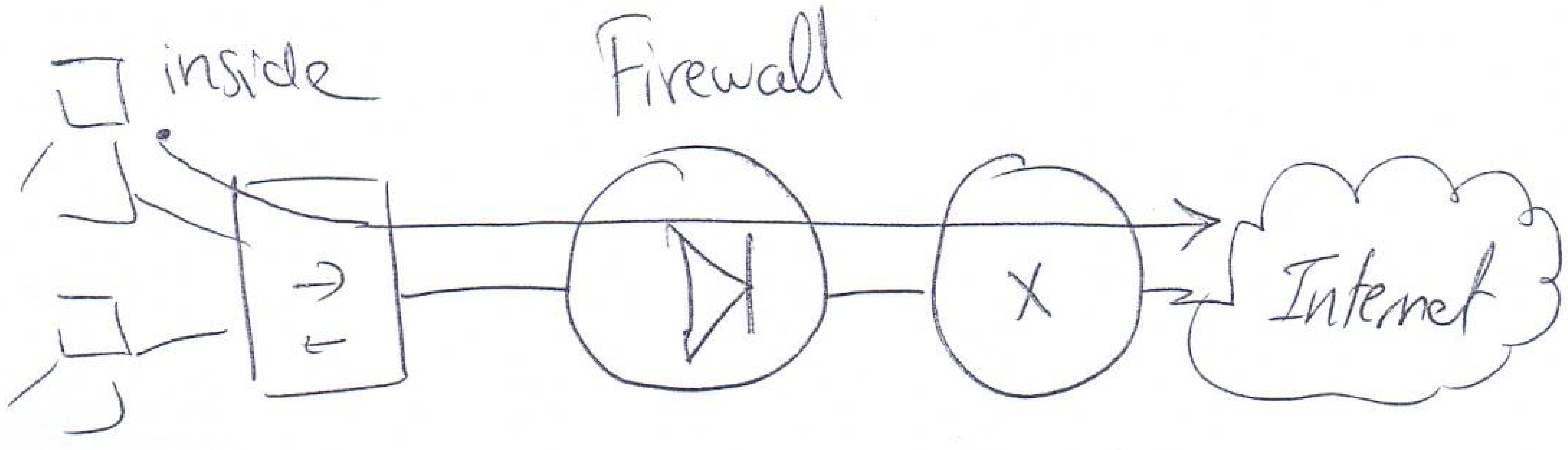
Network Security appliances:

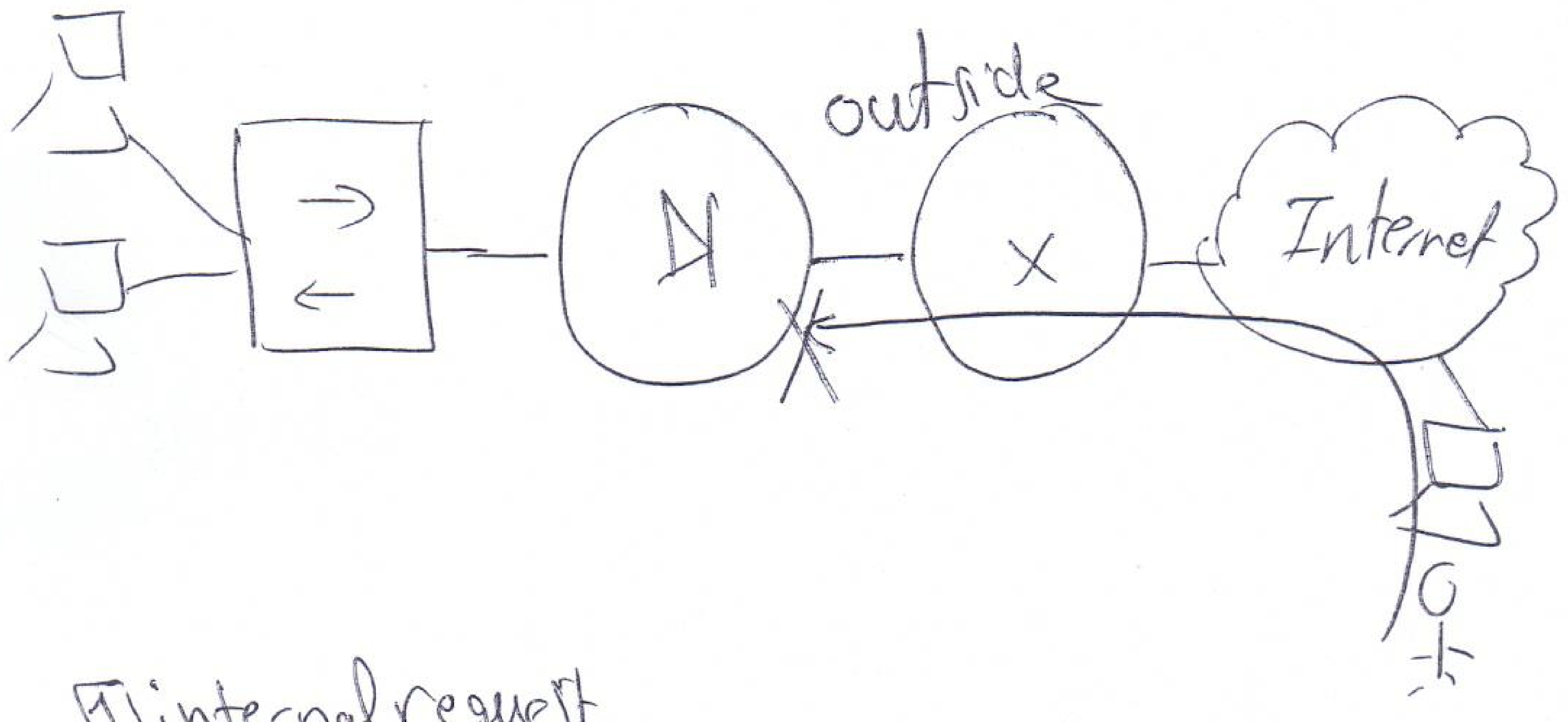
1 Firewall:

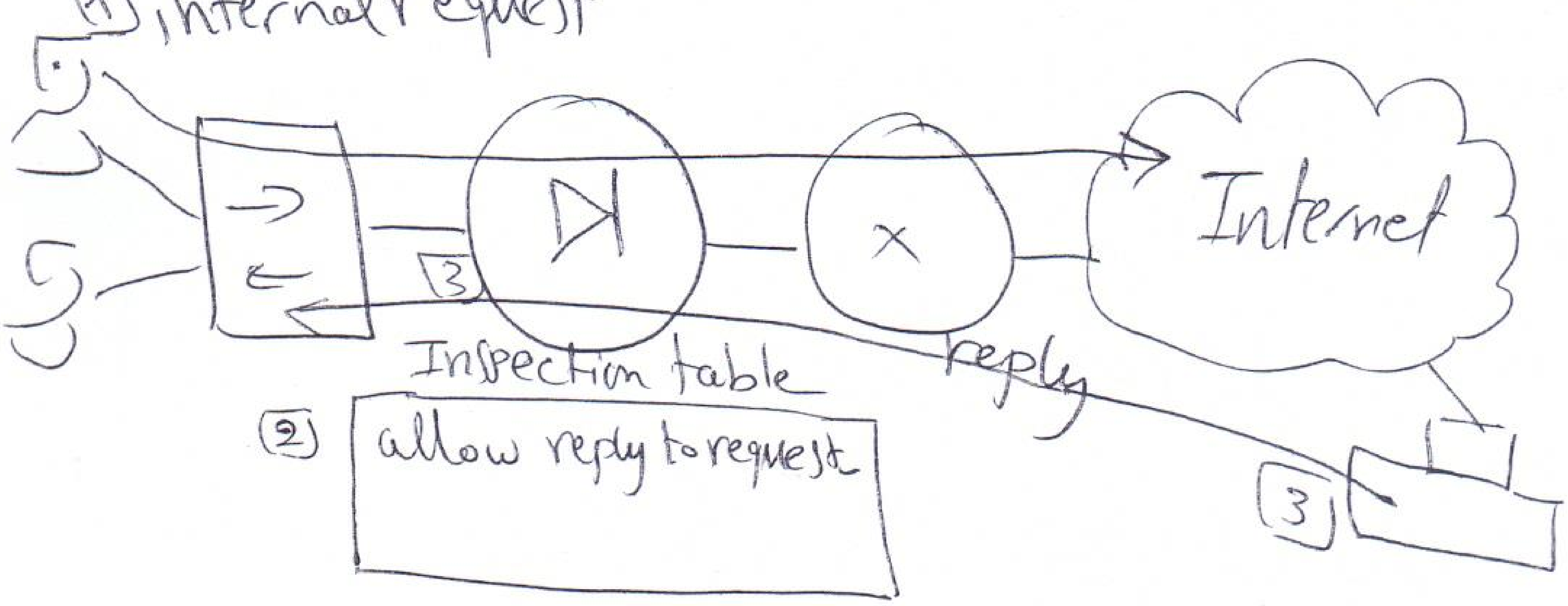
It is a Security H/w or S/w feature that has rules to restrict non required network access.

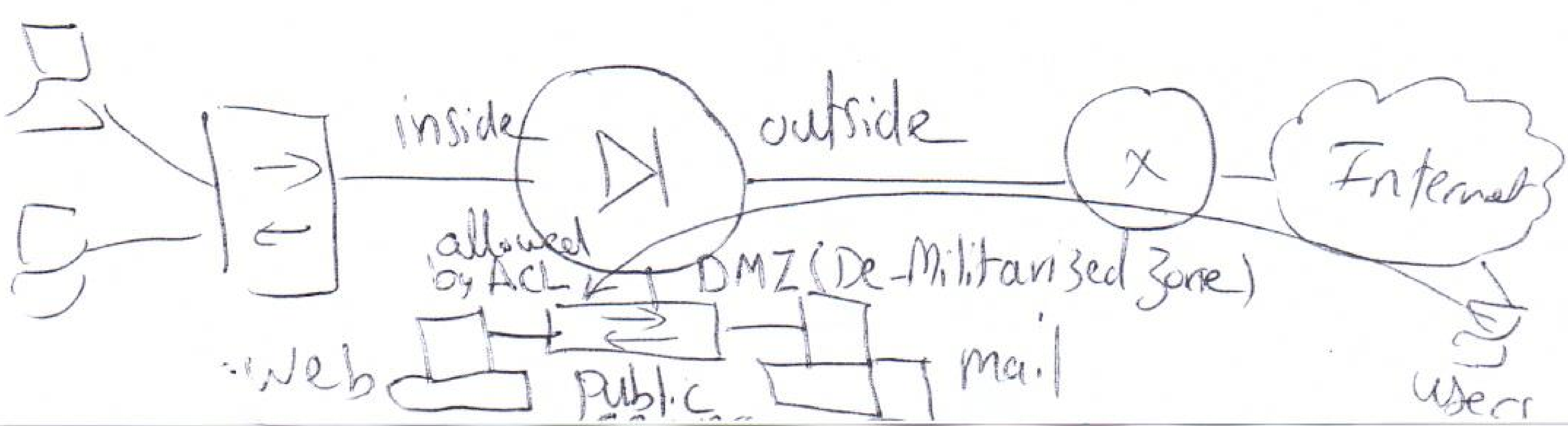
rule a: users from inside (LAN) are allowed to go outside (WAN/Internet) by default. defaults are changed using ACL

rule b: users from outside are not allowed to go inside, unless it is a reply to internal request, by default. defaults are changed using ACL


inside
Firewall
Internet


outside
Internet


1 internal request
3
Internet
Inspection table
reply
2
allow reply to request
3

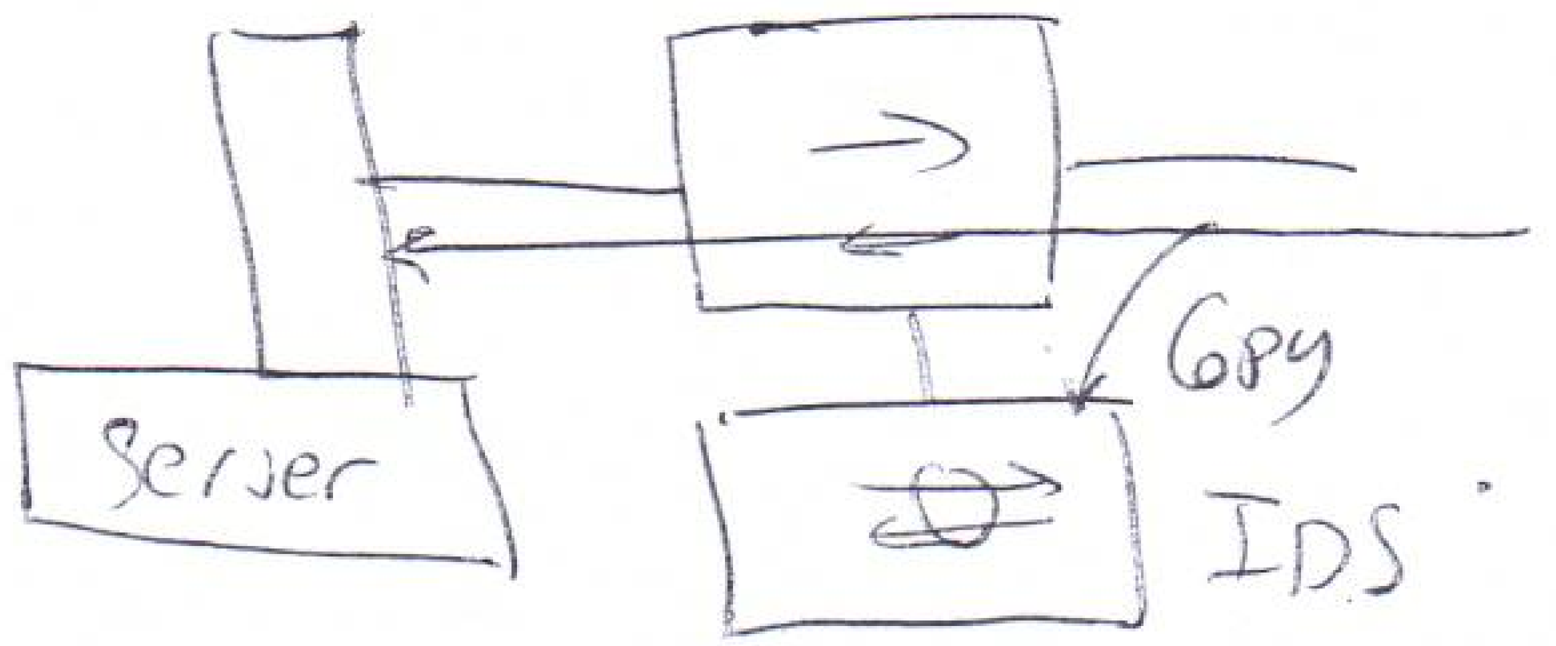

inside
outside
Internet
allowed by ACL
DMZ (De-Militarized Zone)
web
Public
mail
user

2 IDS (Intrusion Detection System)

It is a device that has a Signature file that Contains all Know attacks & hacks ideas till last update of the Signature file.

It Compares Copy of all received Packets (using deep inspection) against its Signature file.

If packet is an attack, it just Send notification to network administrator.



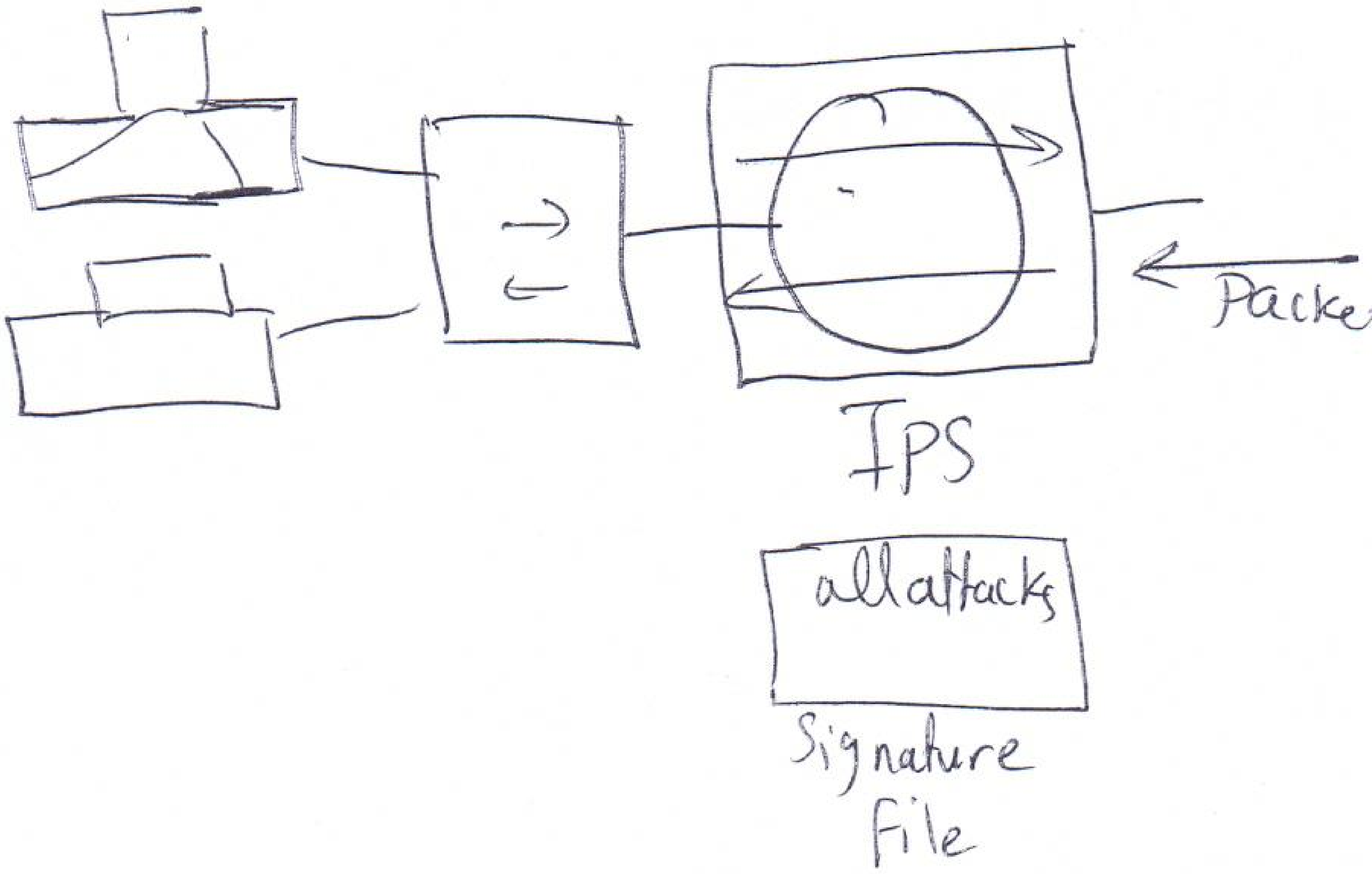
3 IPS: Intrusion Prevention System

It is also Called inline IDS.

It Compares original packet received to the Signature file.

If packet is an attack it sends alarm & stop the attack.

notify the network admin.



Famous Security appliances are:

- Cisco ASA (Adaptive Security Appliance)

  Firewall | IDS | IPS | VPN Concentrator
  Creator

- Palo Alto Firewall

- Fortigate firewall

- Sophos Firewall

Session 6/1

IP Telephony: Voice over IP

It is implementing human voice calls using same infrastructure as data

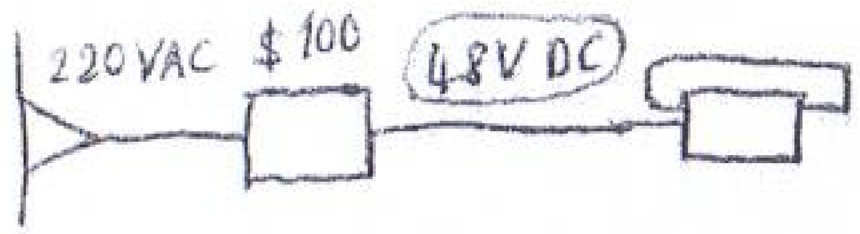
- Router
- Switch
- Cables
- Protocols

VoIP Requirements:

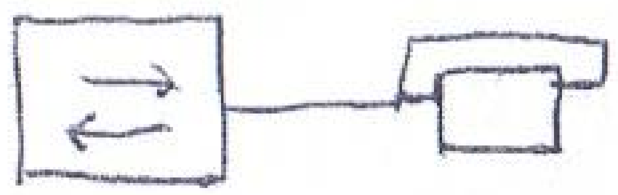
1. Physical requirement:
   cables min. Cat 5e

2. Power requirement:
   IP Phone Max. needs 48V DC

- External Adapter



- POE Switch (Power Over Ethernet)



3. BW requirement:

* Signaling:
  - call establishment
  - call termination

H 323, SIP (Session Initiation Protocol)

* Voice Carrier:

RTP = Real time Transport Protocol

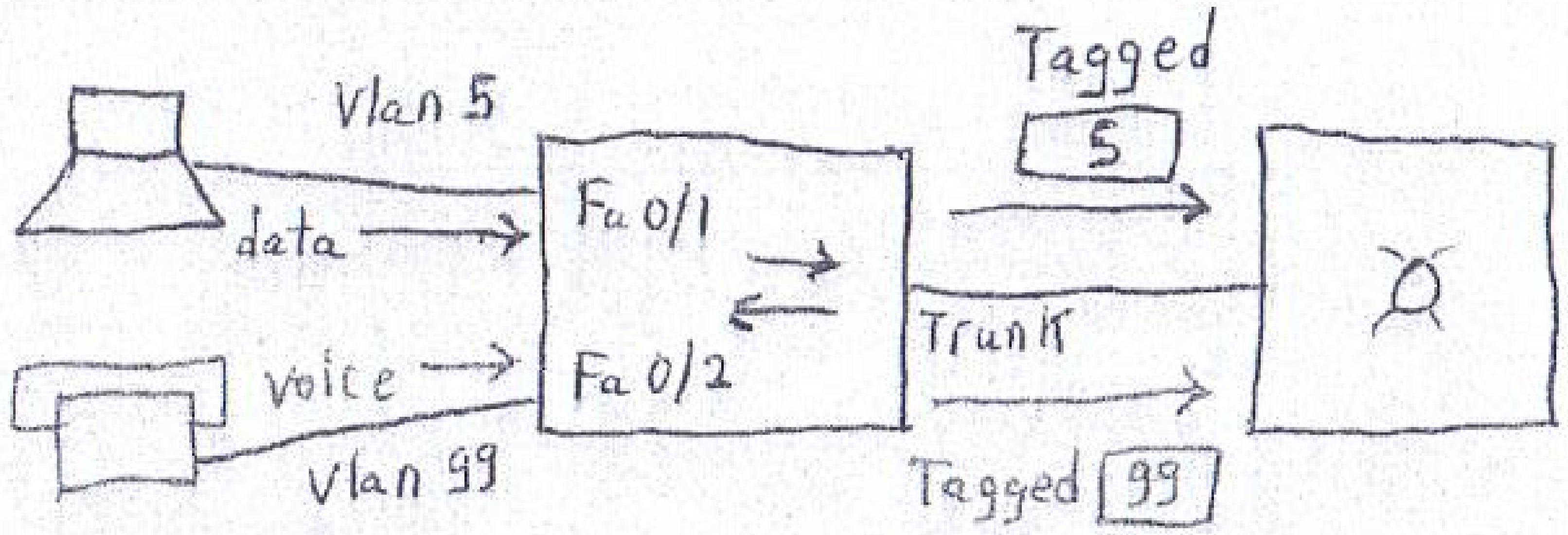
- HD voice call ⇒ 64 Kbps
- Normal quality ⇒ 8 Kbps

1000 IP Phone X 8 Kbps = 8000 Kbps
8 Mbps

Voice Packet $\boxed{\text{150 byte}}$

Data Packet $\boxed{\text{1500 byte}}$

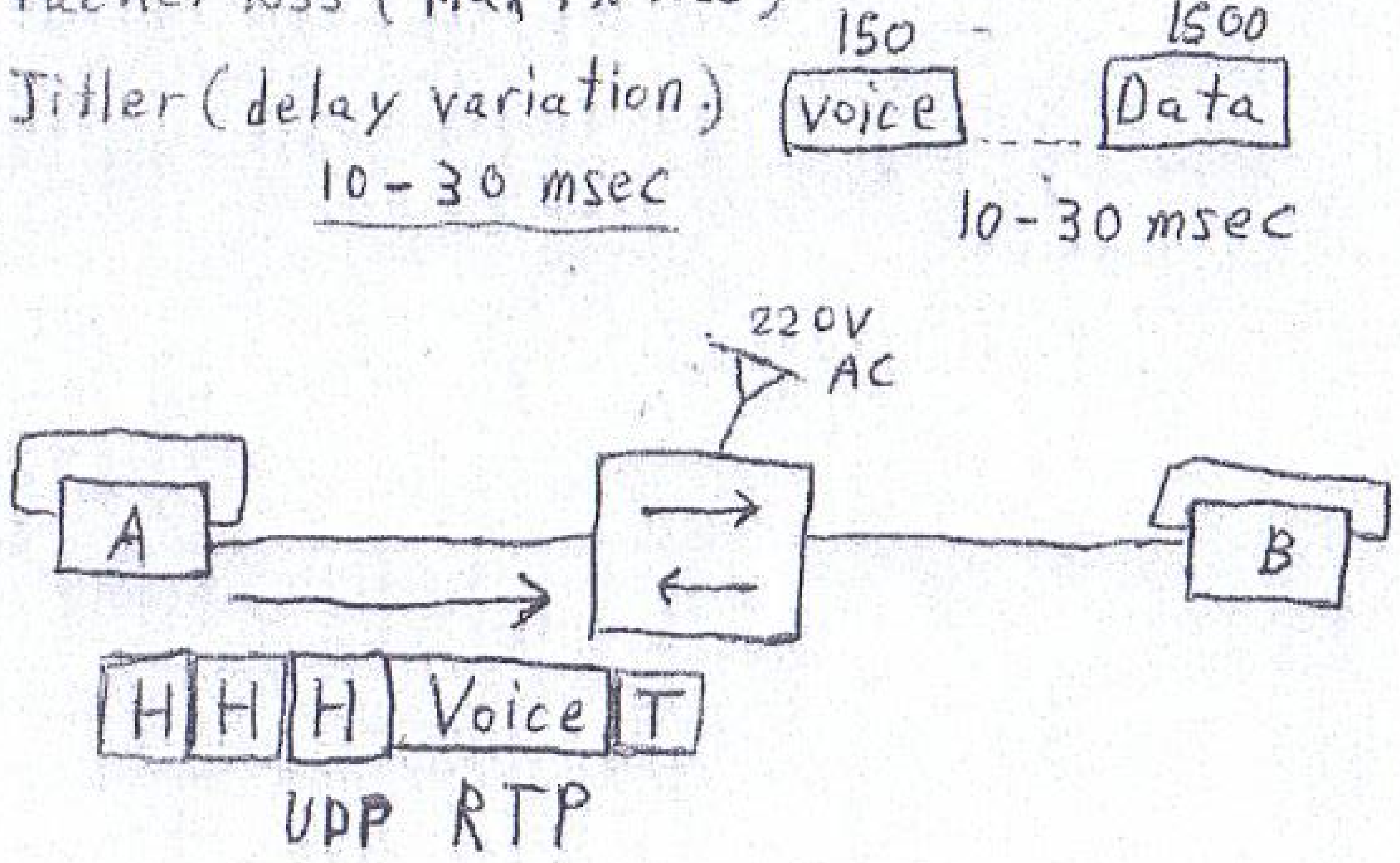
4. Voice VLAN:




```
(config)# interface fa 0/1
(config-if)# switchport access vlan 5
(config)# interface fa 0/2
(config-if)# switchport access voice Vlan 99
```

5. QOS (Quality Of Service): Delay (Latency) max : 150 msec

* Packet loss (max 1% loss)
* Jitter (delay variation) 10 - 30 msec



Session 6/12

QOS: (Quality of Service)

It is giving certain type of traffic priority < voice / video

over other types of traffic.
data

Service Types:

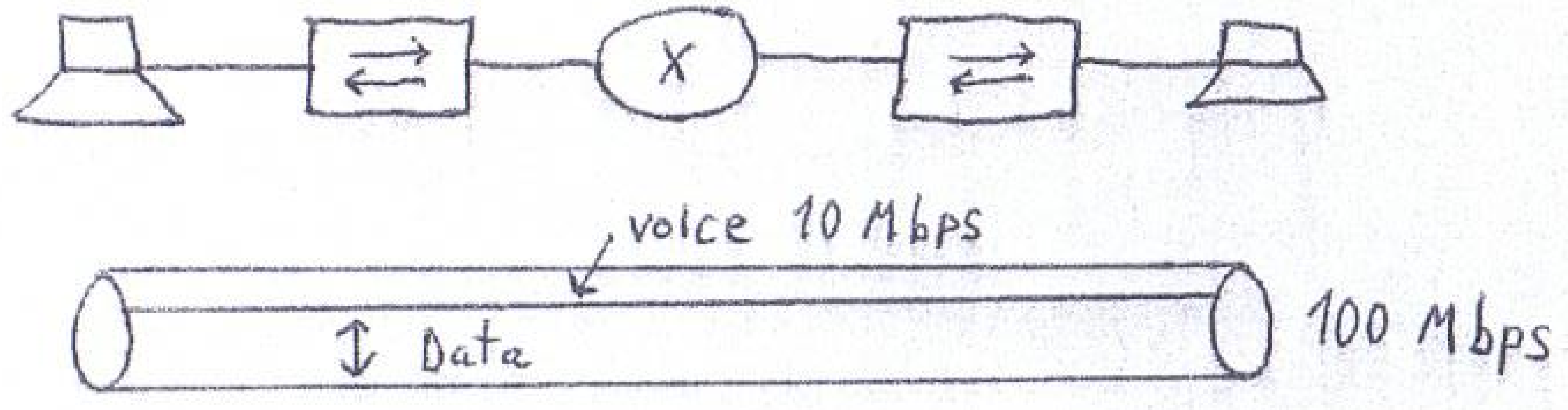
1. Best offer: FIFO

   no QoS (default)

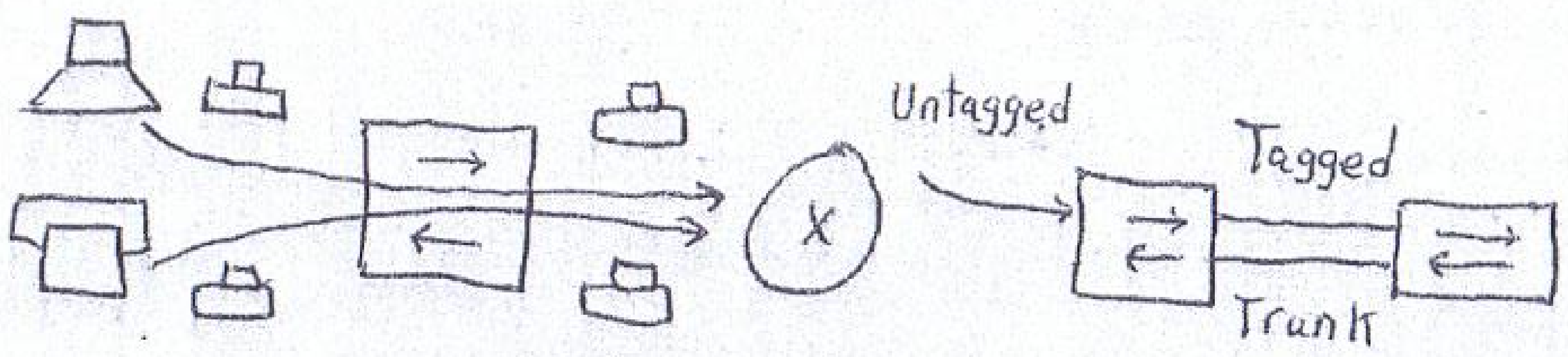
2. Integrated Service QOS:

   (End to End Service)

use RSVP: Resource Reservation Protocol
CPU BW Memory



3. Differentiate Service QOS: hop to hop QOS



How to detect Priority < IP Packet / L2 Frame

* IP Packet: TOS: 8 bit, Use 6 bit DSCP (Different Service Code Point) (0 - 63)

(0-7) Use 3 bit IP Precedense: 0,1,2,3 → data 4 → video 5 → voice
6 → Router protocols 7 → switch protocols

* L2 Frame:
dot 1q tag

tagged (dot 1q) = 802.1q

Pre	dst. MAC	src MAC	dot 1q Tag	Type	Packet	T

4 byte

12 bit	3 bit	-----

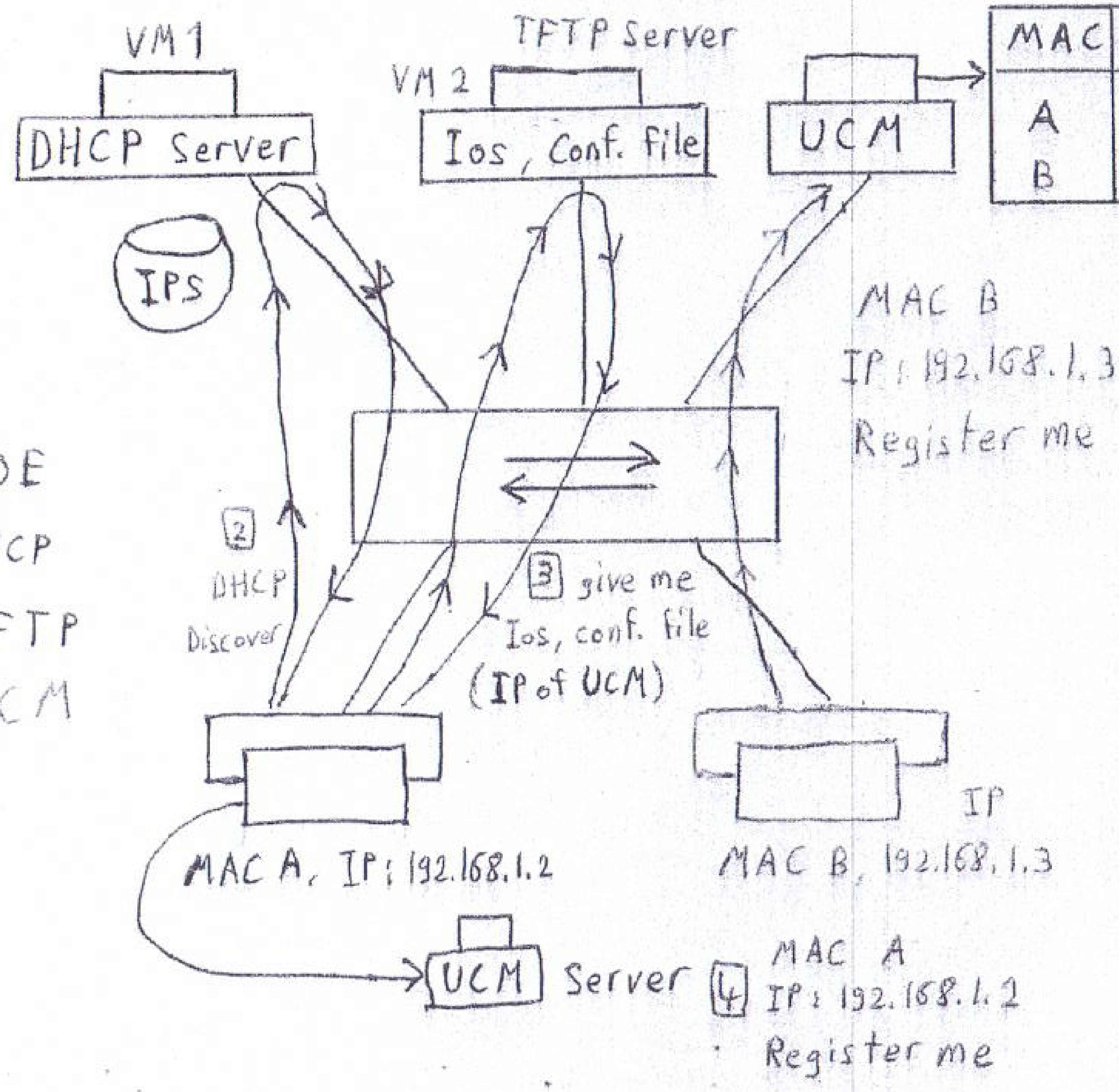
12 bit : VLAN ID 0-4095

3 bit : class of Source 0,1,2,3 → data 4 → video 5 → voice

Session 6/3

IP Telephony: Voice Over IP

[6] Voice Call Manager: (VOIP Server)



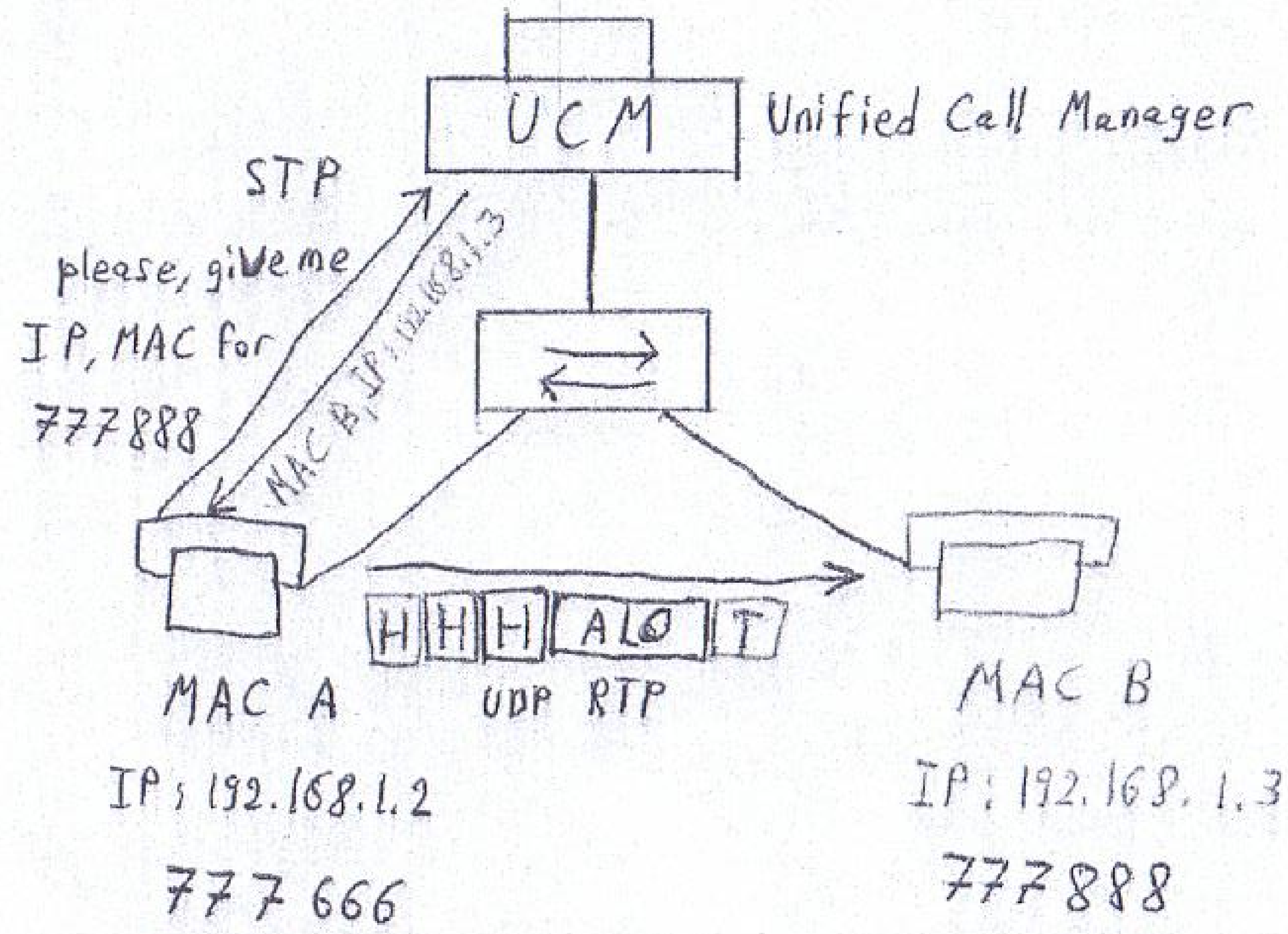
MAC	IP	Phone
A	192.168.1.2	777 666
B	192.168.1.3	777 888

[1] POE

[2] DHCP

[3] TFTP

[4] UCM



Light Weight
- no power supply
- no IC
- no conf. file
- no Ios

VOIP (Voice over IP):

It is implementing Telephony Voice Calls using IP network Infrastructure (Same Switches & Routers and Cables that Carry data)

· Implementing IP telephony:

IP Phone requires the following for a good quality Voice Communication Session.

1 Physical layer requirements:

IP Phone requires a minimum of Cat 5e UTP Cables.

2 Power requirement:

IP Phone as any network device needs Power to activate S/W (IOS) & H/W (ICs).

Power can be provided using External adapter or by Providing PoE (Power over Ethernet)

Note: IP Phone needs only DC Power (mostly 48V DC)

3 Bandwidth requirement:

A VoIP Call requires two types of traffic:

- Voice Carrier traffic stream, which is the human Voice Call carried using RTP ~~(Retransmission~~ (Real-time Transport Protocol) (Real-time Transmission Protocol)

  RTP requires max. 64 kbps & min. 8 kbps BW to carry human voice (Based on voice Codec) Convert human analog Voice to digital

- Voice Signaling (Protocols used for session management, establishment & termination)

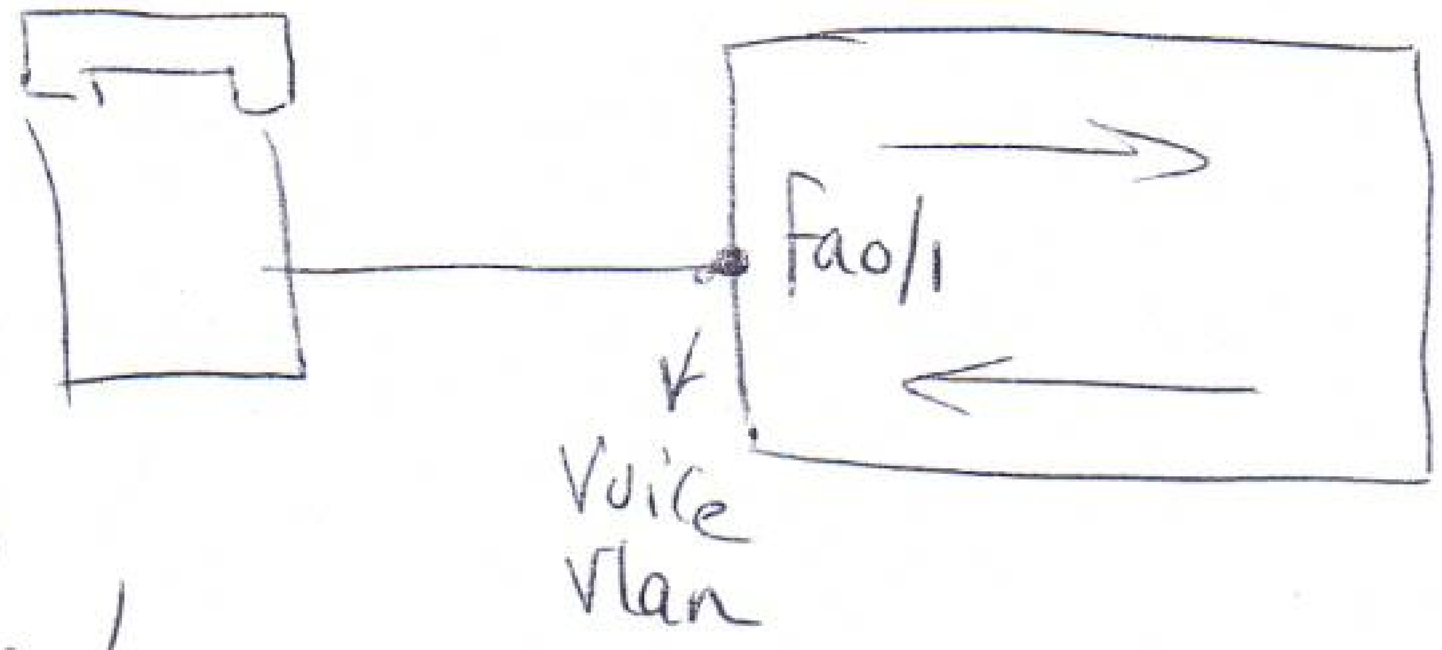
  ex: RTCP (Real-time Transmission Control Protocol)

  SIP (Session Initiation ربط المشغل Protocol)

these Protocols help IP Phones to discover each others & also help to produce statistics about Call quality.

4 Voice VLAN:

It is Preffered to dedicate a Specific VLAN for IP Phones & their supplementary device (ex: VoIP servers, Call manager, VoIP gateways)



(Config)# interface fa0/1
(Config-if)# Switchport Voice Vlan vlan no.

5 Voice QoS:

~~discussed next~~

Voice is very Sensitive to:

- delay (Latency) - max. 150 msec
- Jitter (delay Variation) - Should not exceed 30 msec
- Loss (packet drop) - more than 1% Packet loss Can Cause bad session quality

QoS Types:

1. Best-effort delivery: default QoS is also called FIFO (First In First out) delivery, which means no QoS.

2. Integrated Service QoS: (IntServ QoS)
It is end to end QoS using RSVP (ReSource ReSerVation Protocol), implemented by reserving Resources (BW, memory & CPU) from all devices from end to end to important traffic.

3. Differentiated Service QoS: (Diffserv QoS)
It is hop to hop QoS, implemented by checking CoS or ToS @ each hop to give high Priority data a better service.

QOS (Quality of Service): Ladies first

- It is giving diffent types of traffic a different types of Priorities.
- Priority can be added to frames & Packets

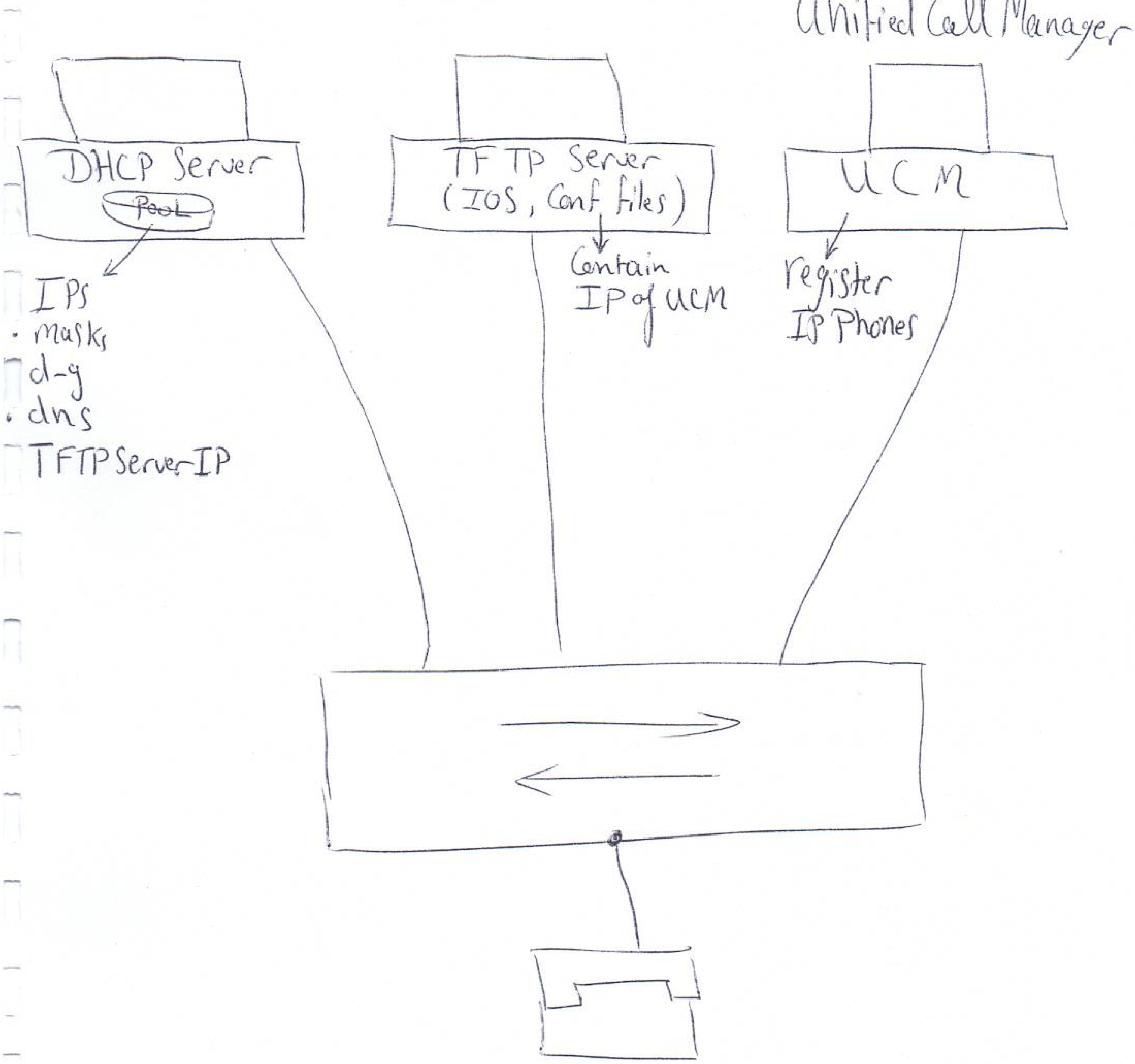
Using:- COS (Class of Service) bits in dot1q frame Tag
- TOS (Type of Service) bits in L3 IP packet

Using 3 bits is called IP Precedence bits

Using 6 bits is called DSCP bits (Diff Serv Code Point)

depending on CoS in frames or ToS in Packets data can move better & faster inside network to avoid
- delay
- Jitter
- Loss

IP Phone Startup operation:



Steps:

[1] Switch Provides the IP Phone with PoE So as for the Phone to be activated

[2] Switch Sends to the IP Phone information about its VLAN.

Switch Knows Phone VLAN from:
(Config-if)# Switchport Voice Vlan #

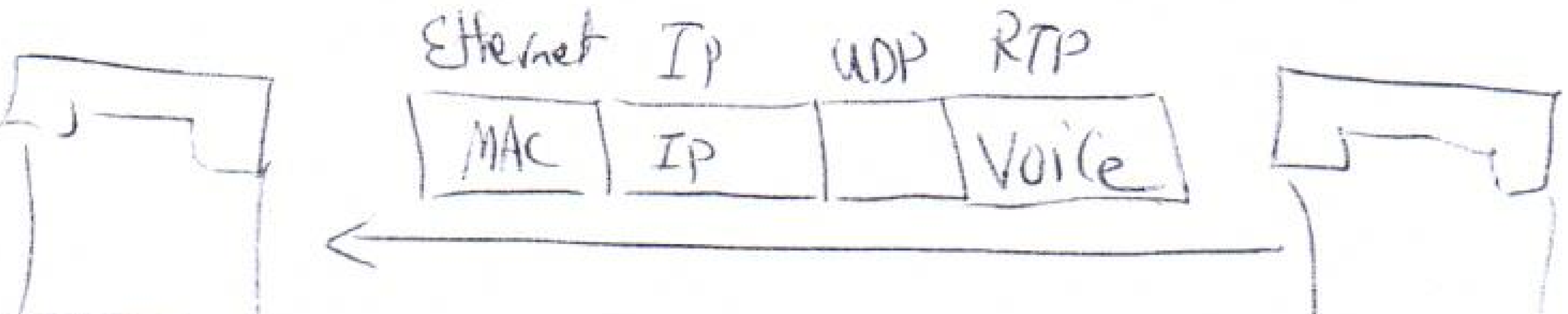
[3] Phone Sends BroadCast targeting DHCP Server (DHCP disCovery) asking for DHCP offer (IP, mask, dg, dns, TFTP IP)

[4] After DHCP Server replies to IP Phone, Phone asks the TFTP Server for recent IOS image (firmware = factory operating System) & full Configuration file Containing IP of UCM

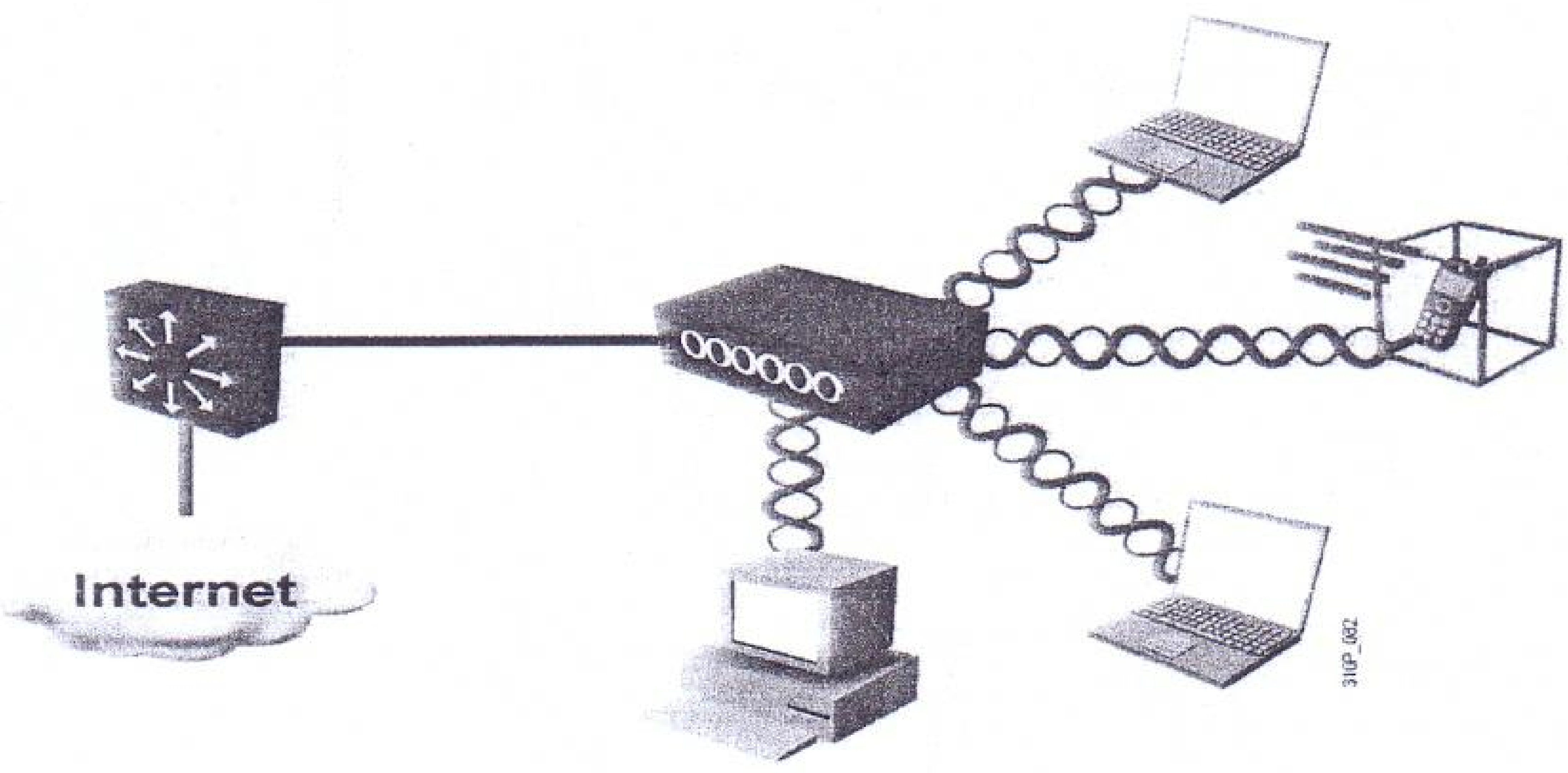
[5] The Phone registers its MAC with UCM & takes from UCM its Phone number.

Now IP Phone has MAC, IP & Phone number & also UCM has a table of Same info.

[6] Finally when any human on other Phone Calls the Phone number of our Phone, its Phone will go to UCM & tell it Phone & takes from it our Phone Mac & IP in order for RTP to Send all voice Packets to our Phone using its IP.



Wireless LANs



Maged Abd El-Wareth

Session 7/1

Wireless LAN: WiFi = Wireless Ethernet

IEEE 802.11

IEEE 802.11 b → 11 Mbps → 2.4 GH3
IEEE 802.11 a → 54 Mbps → 5 GH3
IEEE 802.11 g → 54 Mbps → 2.4 GH3
IEEE 802.11 n → 84 Mbps → 2.4 GH3
IEEE 802.11 ac → up to 1 Gbps → 2.4 GH3

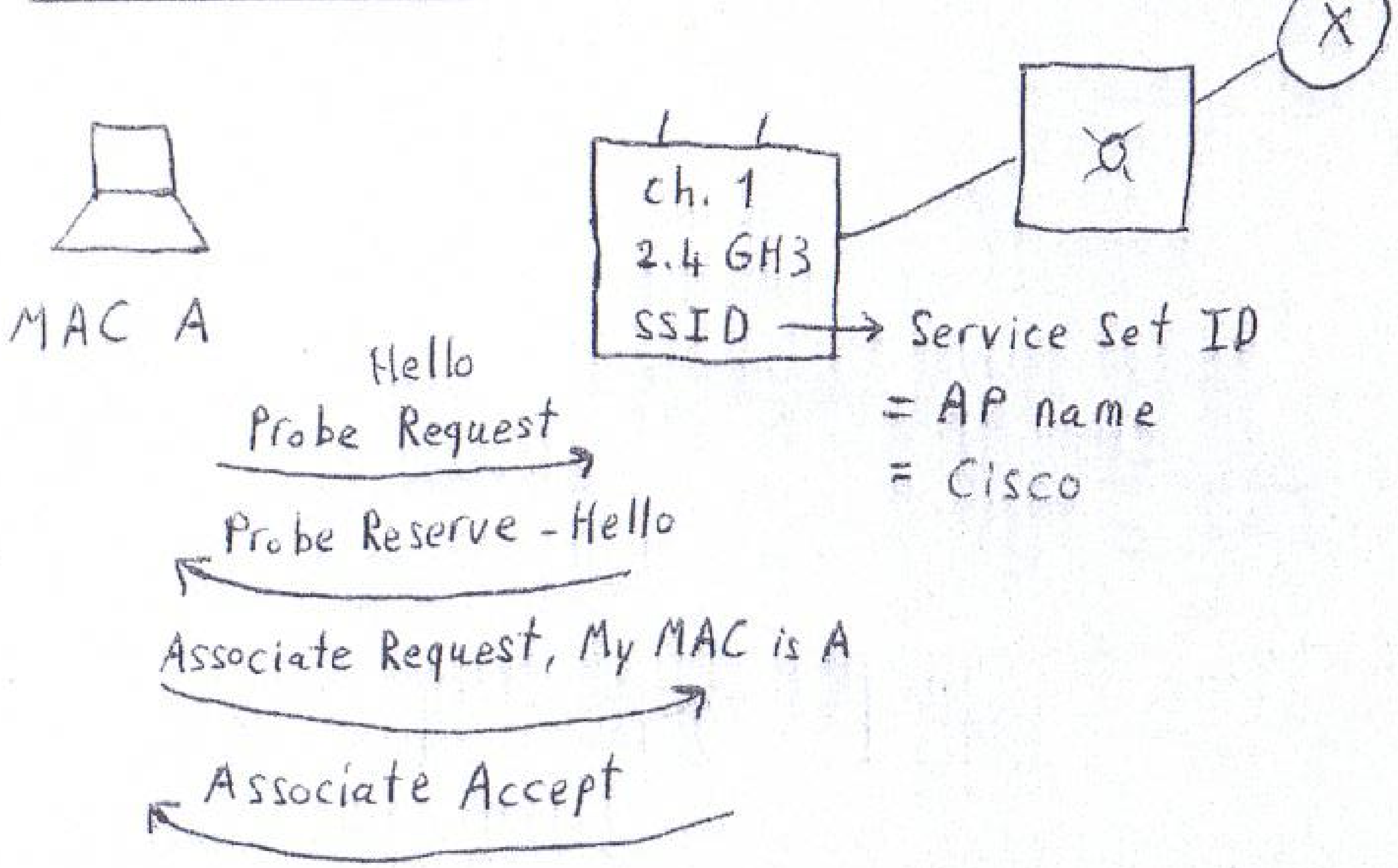
100 m

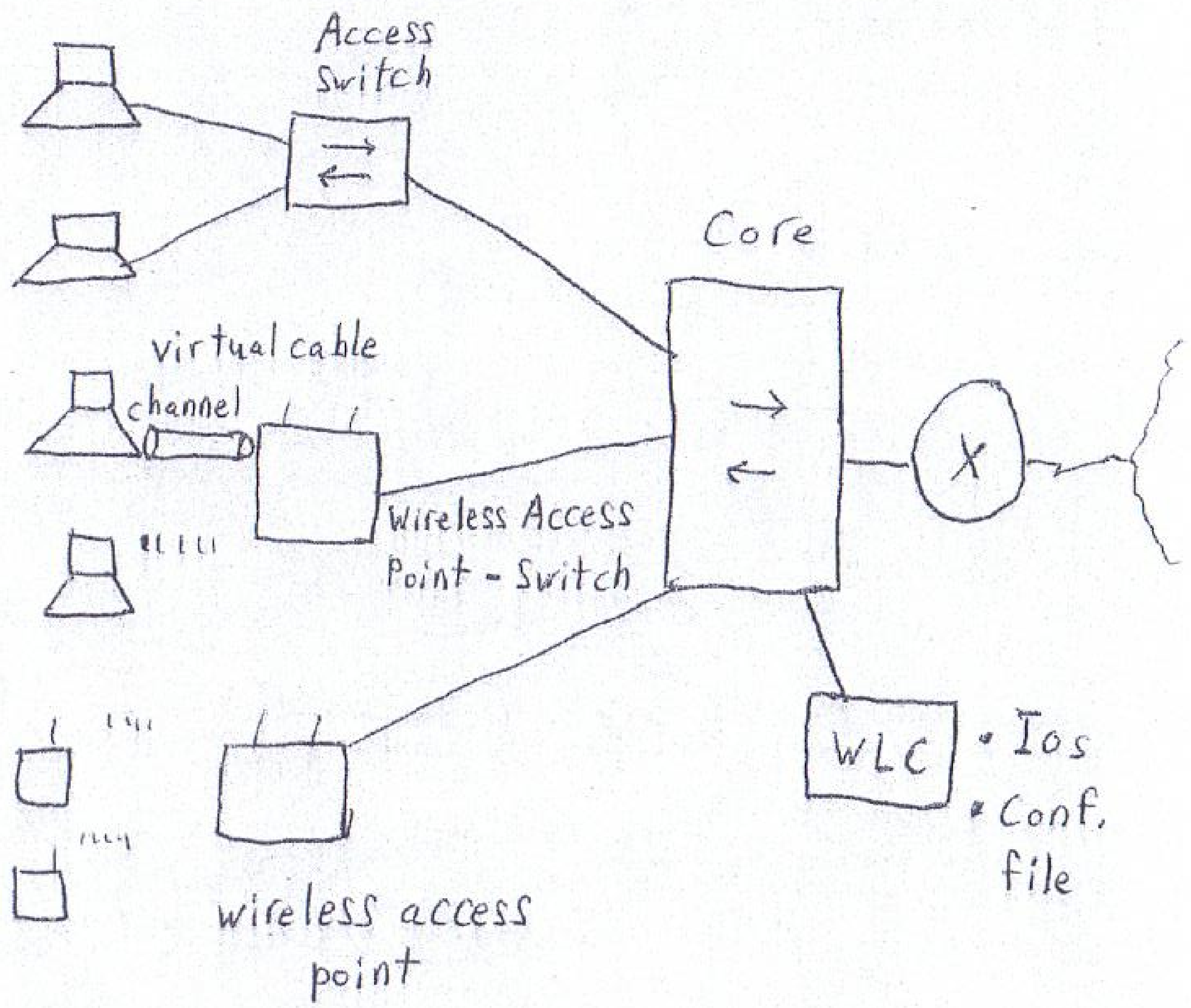
Wireless LAN Controller

+ Light weight AP

- no power supply
- no conf. file
- no Ios

WiFi Operation:





Wireless LANs:

- It is forming Communication between devices in LAN without need for Cable Connectivity, only Using wireless Channels.

- Wireless LANs Standard is Sponsored by IEEE

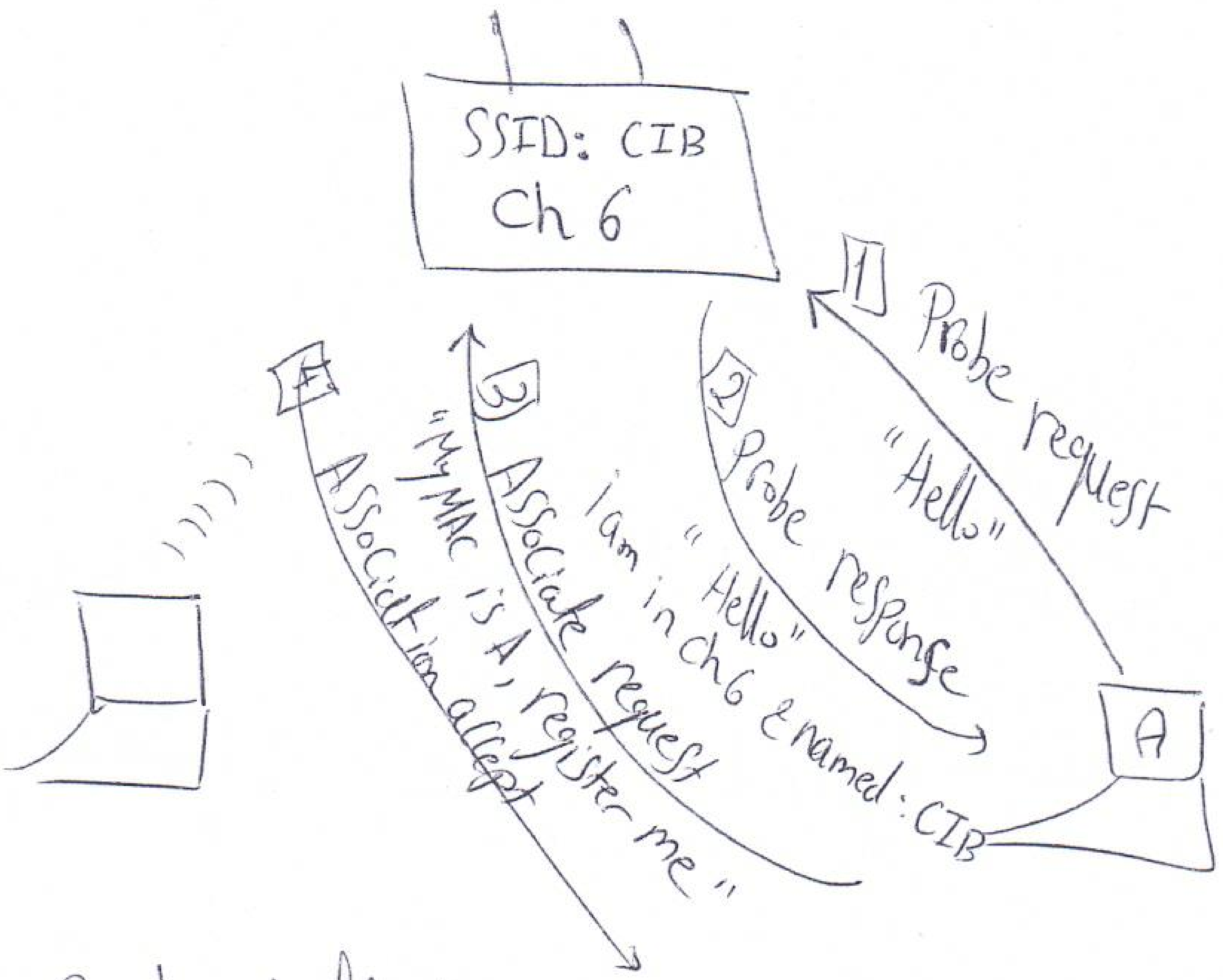
IEEE 802.11 a → up to 54 MbPs LAN speed
IEEE 802.11b → up to 11 MbPs LAN Speed
IEEE 802.11g → up to 54 MbPs LAN Speed
IEEE 802.11n → up to 384 MbPs LAN Speed
IEEE 802.11ac → up to 1 GbPs & more LAN Speed

Some Standards use Channels on 2.4 GHz Band & others use 5GHz and Some use both.

Covarage Can reach from 100m to 300m in free space.

& Wireless transmission Can use one of 14 available Channels mostly we use Ch 1, Ch6 & Ch 11 for best Performance.

ACCess Point & users operation:



1 PC Sends hello "Probe request" msg on all available channels in band.

2 AP replies with its SSID (name) & Channel Configured

3 PC Sends a registration request to AP

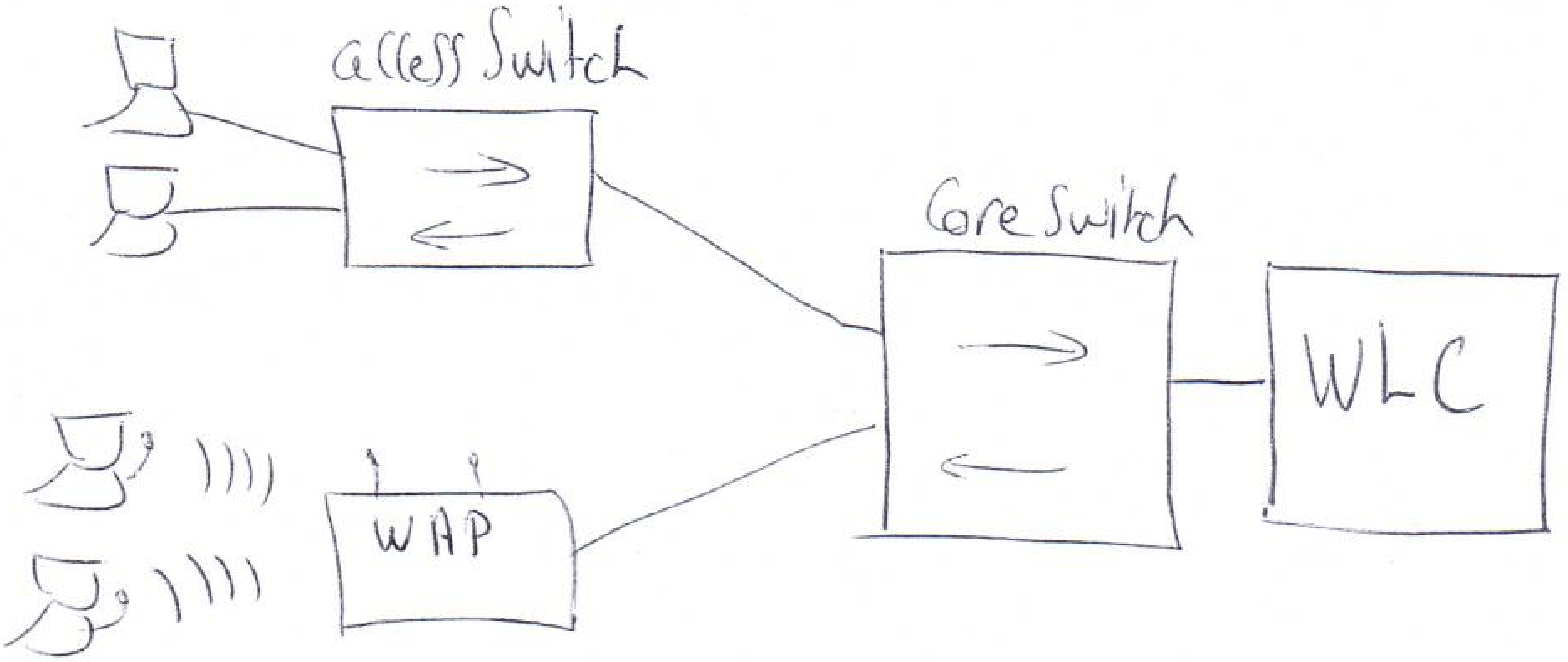
4 AP add MAC of end device to its Associates table & Send acceptance msg.

5 Now end device Can Send data frames to AP.

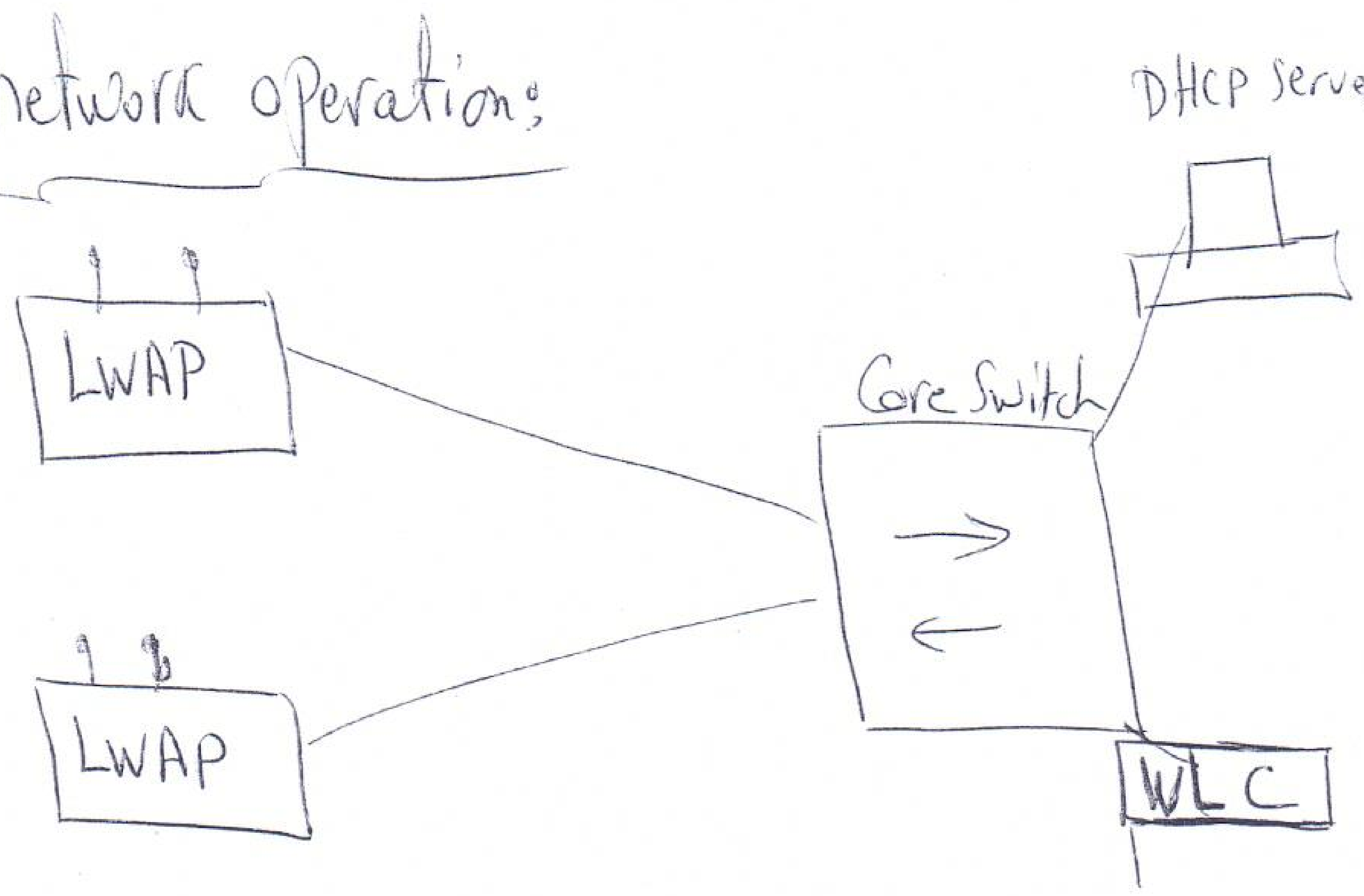
Wireless LAN Implementation:

For Large networks, the best wireless Solution is using WLC (wireless LAN Controller) +
LWAP (Light Weight Access Point)
instead of old implementation which was using only Autonomus access Points that require manual Configuration from network admin.

Wireless access Point is wireless Switch (as access switch) & wireless LAN Controller reacts as Core switch for APs.



Wireless network operation:



[1] Light Weight Access Point take PoE from Switch

[2] LWAP Comes empty with H/w but no S/w (IOS, Conf. file)

~~2~~ , So LWAP Send Broad Cast Searching for DHCP offer

[3] DHCP replies with IP, mask, d-g, dns & IP of WLC

[4] LWAP goes to ask WLC for IOS & Conf. file
, the most important info in Conf. file is
LWAP Channel & SSID (Service Set ID)
AP ID = Access Point ID

[5] now LWAP is ready to deal with end users.

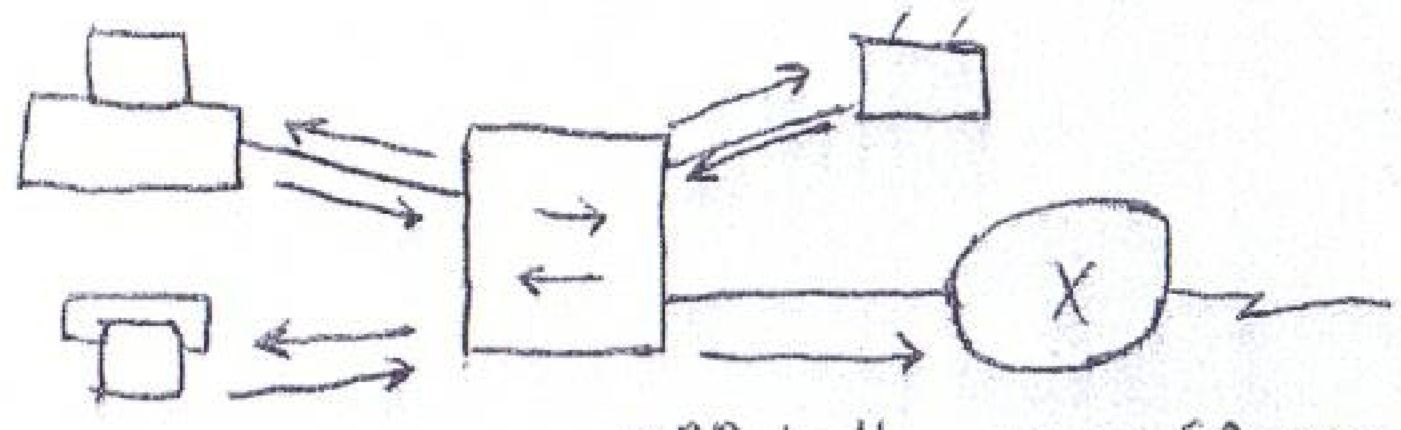
Network Management.

- CDP /LLDP
- NTP
- Syslog
- SNMP
- IP SLA
- SDN

Session 7 /2

Network Management:

* CDP: Cisco Discovery Protocol
  ↳ L2 Protocol



CDP hello every 60 sec.
(قمعتة)

* on by default

(config)# cdp run

(config-if)# cdp enable

CDP msg. contains:

1. Device ID (host name)
2. Platform (model
3. Capability (router, switch, server, IP phone)
4. Interface ⟹ # show cdp neighbors
5. IP & MAC
6. IOS version
7. Native VLAN
8. Duplex (half - full)
9. VTP domain # show cdp neighbors details

* LLDP: Link Layer Discovery Protocol
  ↳ Layer 2 = direct neighbor only

- It is standard version of CDP

* disabled by default

(config)# lldp run

OR (config-if)# lldp {transmit/receive/both}

show lldp neighbors

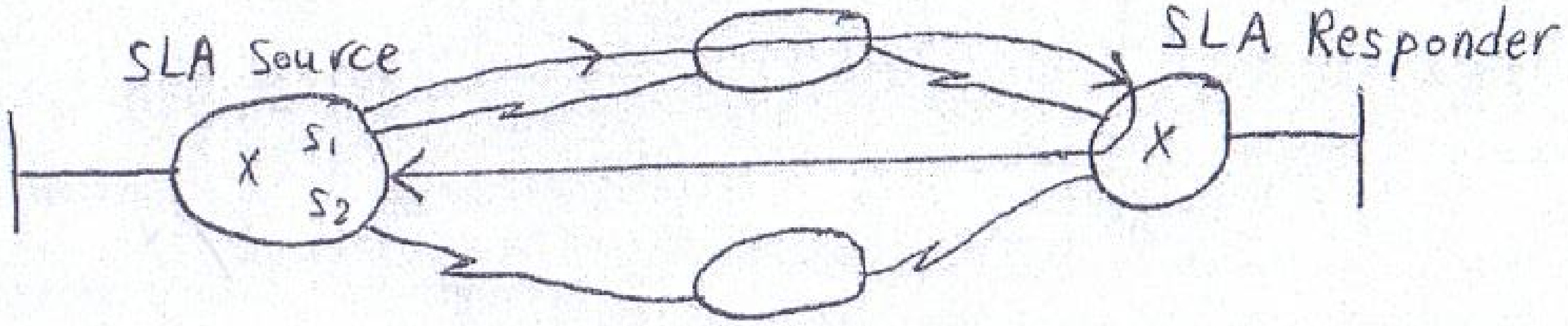
show lldp neighbors details

---

* IP SLA: IP Service Level Agreement (Cisco feature)

It is used to generate bogus traffic ∠ echo msg, FTP - RTP - HTTP - .....
in order to test link quality:

- Delay (max 150 msec)
- Jitter (10 - 30 msec)
- Packet loss (1%)

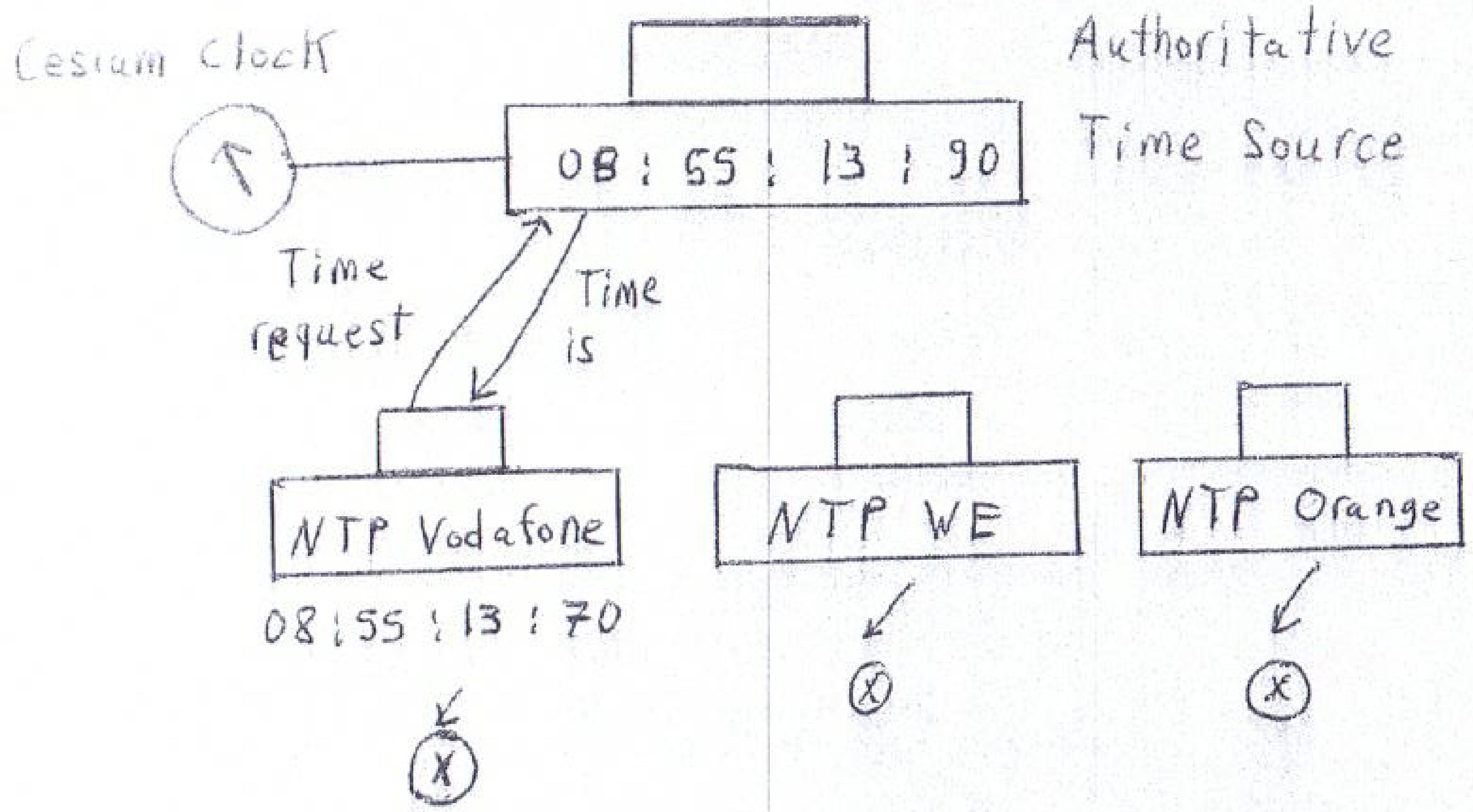


Network Management:

Session 7/3

* NTP: Network Time Protocol

It is an application using UDP Port 123 used to adjust time & date on network devices.



stratum 0

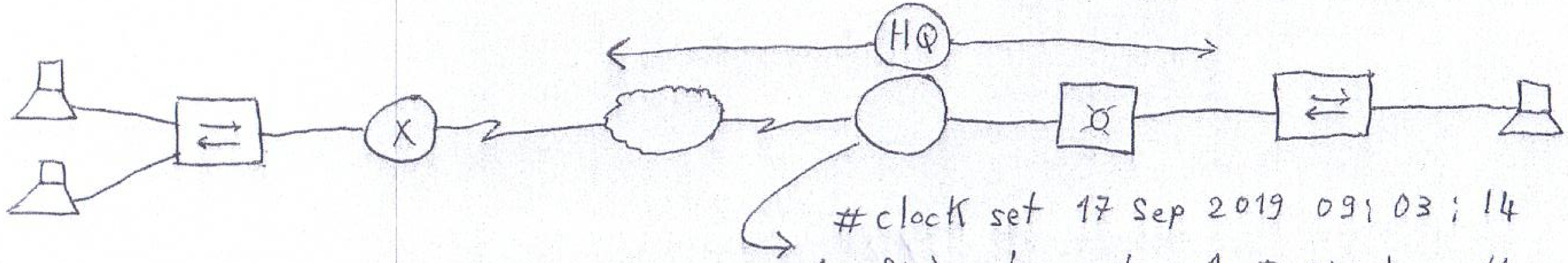
stratum 1

stratum 2

* Clock still accurates till stratum 15

* Stratum 16 is inaccurate

Time is ✓ every 5 mins



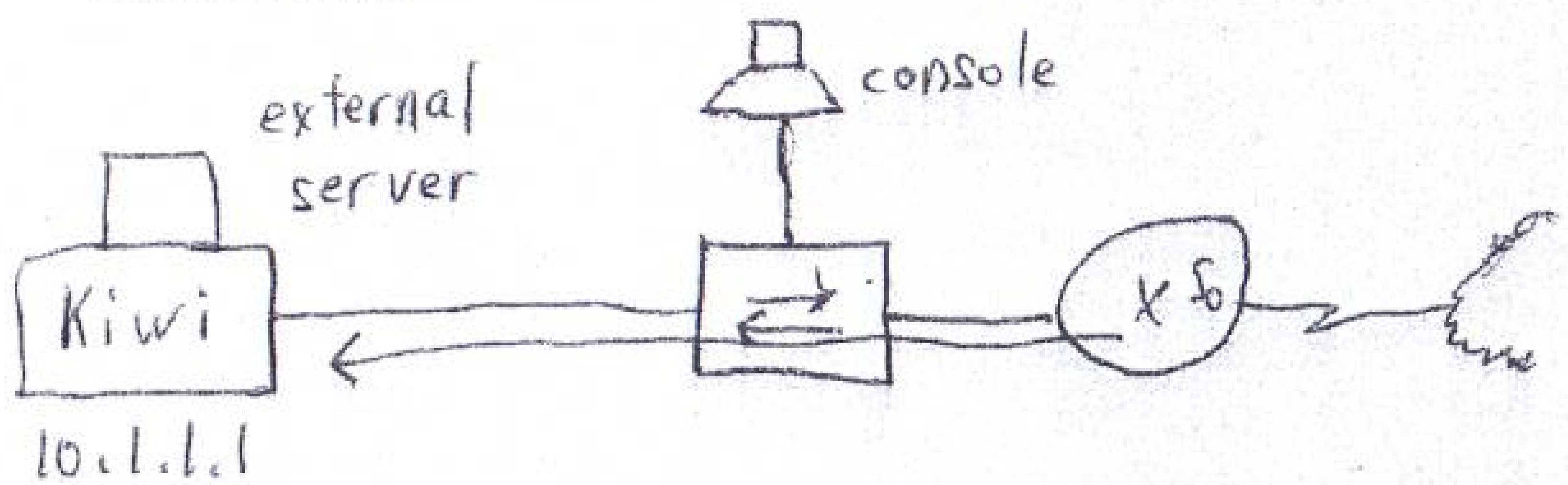
\#clock set 17 Sep 2019 09 : 03 : 14

(config)# ntp master 1 ≠ stratum #

Session 7/4

* Syslog: System logging

It is an application using UDP called System logging used to notify network administrator about network devices changes.



09:30:13. Interface So changed state to up

Notification: EIGRP neighbor is up

Syslog msg. appear:

1. on console interface (CLI) (default)
2. Store on internal RAM
   (config)# logging buffered   # show log
3. external server
   (config)# logging 10.1.1.1 ⇒ Server IP

* Syslog msgs are called Traps:

(8 Levels of Severity)

EACE
- Emergency — 0
- Alert — 1
- Critical — 2
- Error — 3

WNID
- Warning — 4
- Notification — 5
- Informational — 6
- Debugging — 7

(must run manually)

\# debug ip rip

\# debug ppp negotiation

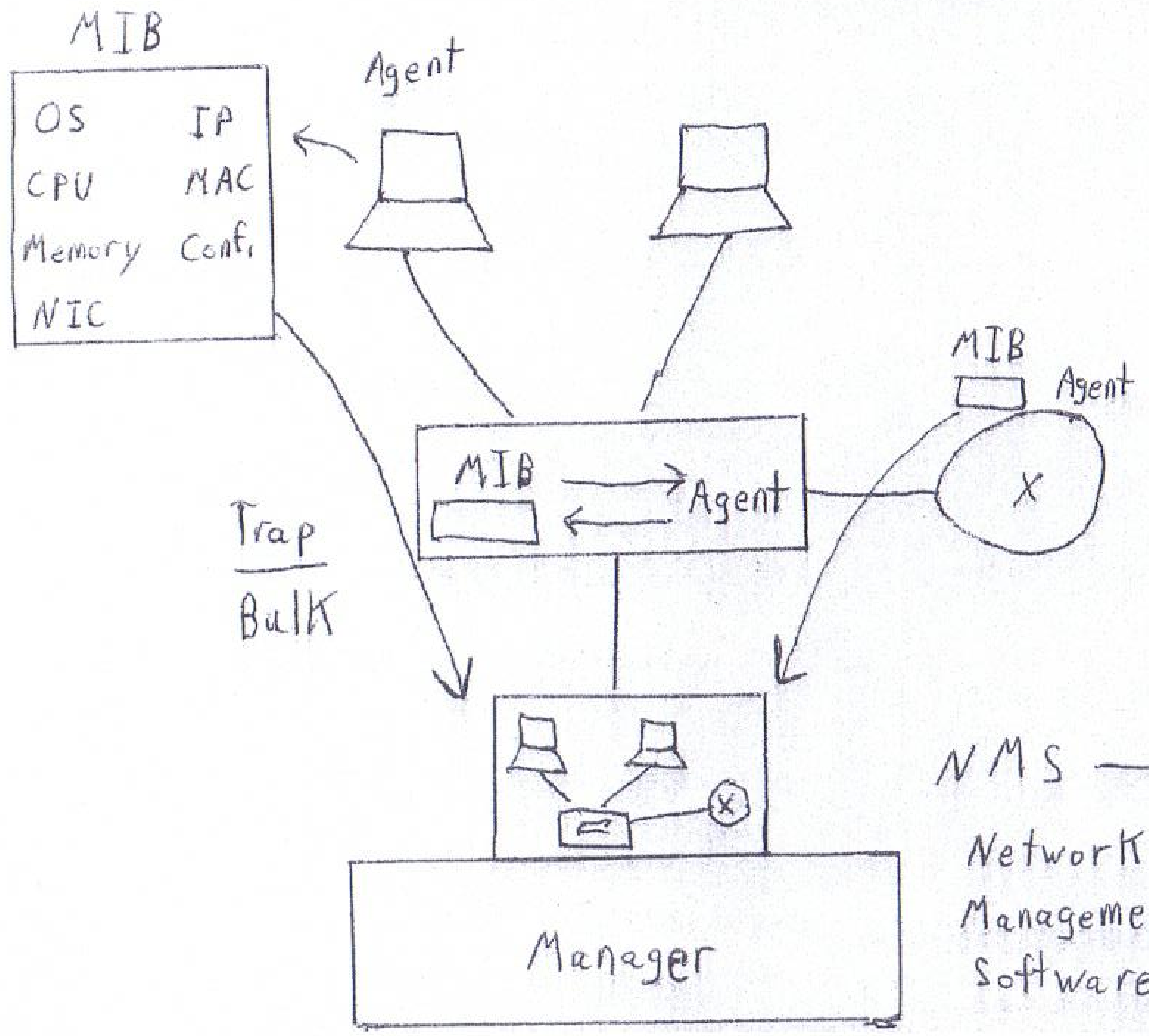
Session 7 / S

*SNMP: Simple Network Management Protocol

It is an application using UDP Port 161, 162 used to monitor all network devices in order to draw graphical network topology (Read & write)
↓
configure

SNMP Operation:

Trap is sent from MIB = Management Inf. Base of Agent to Manager NMS.



NMS — Network Management Software
- Whats up gold
- Cisco Prime
- IBM Tivoli
- HP open view
- Cisco Works

Session 7/6

SNMP Versions:

* Version 1:

- Limited MIB
- Limited Security: Community String
  Domain Name

* Version 2:

- Extra MIB using Bulk msg.
- Limited Security

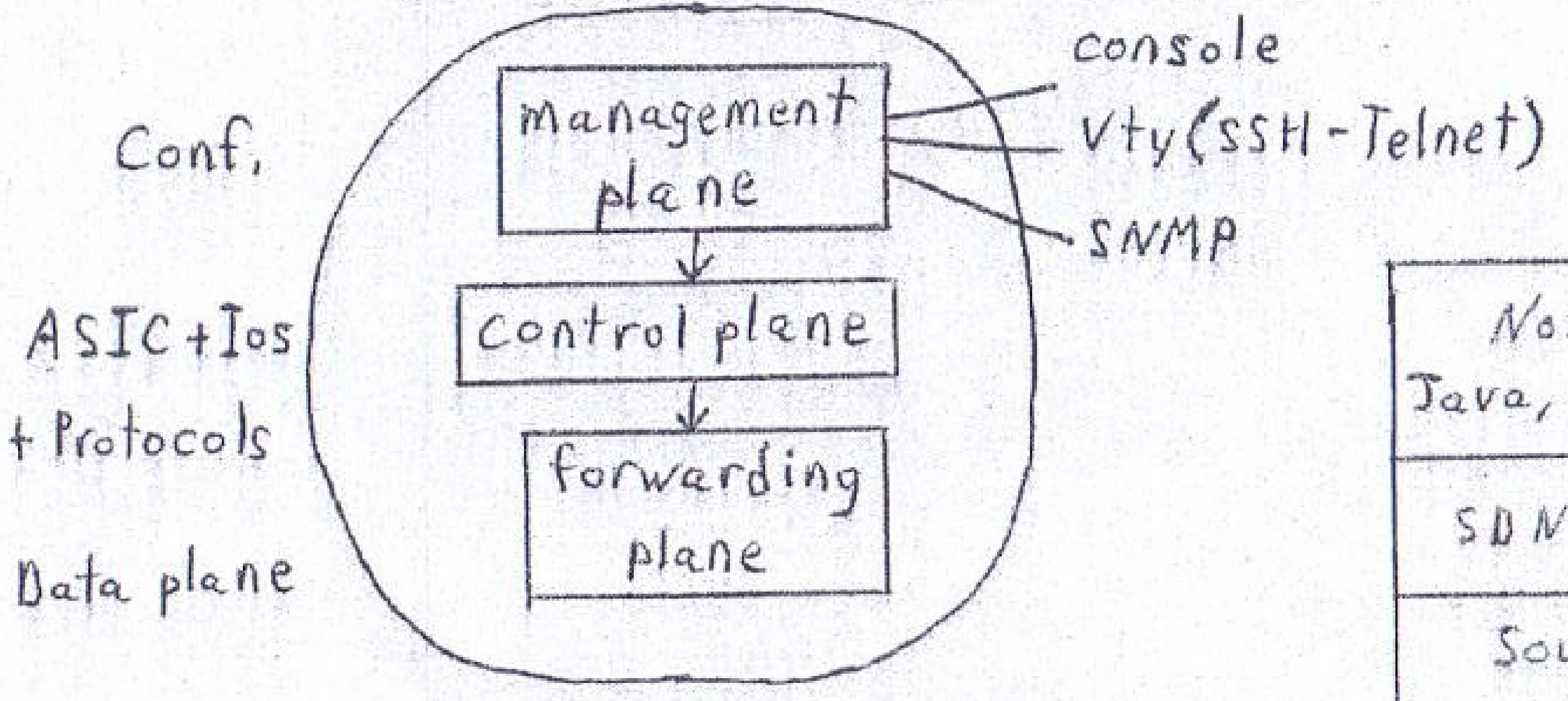
* Version 3:

- Extra MIB
- Extra Security < Authentication / Confidentialy (Encryption)

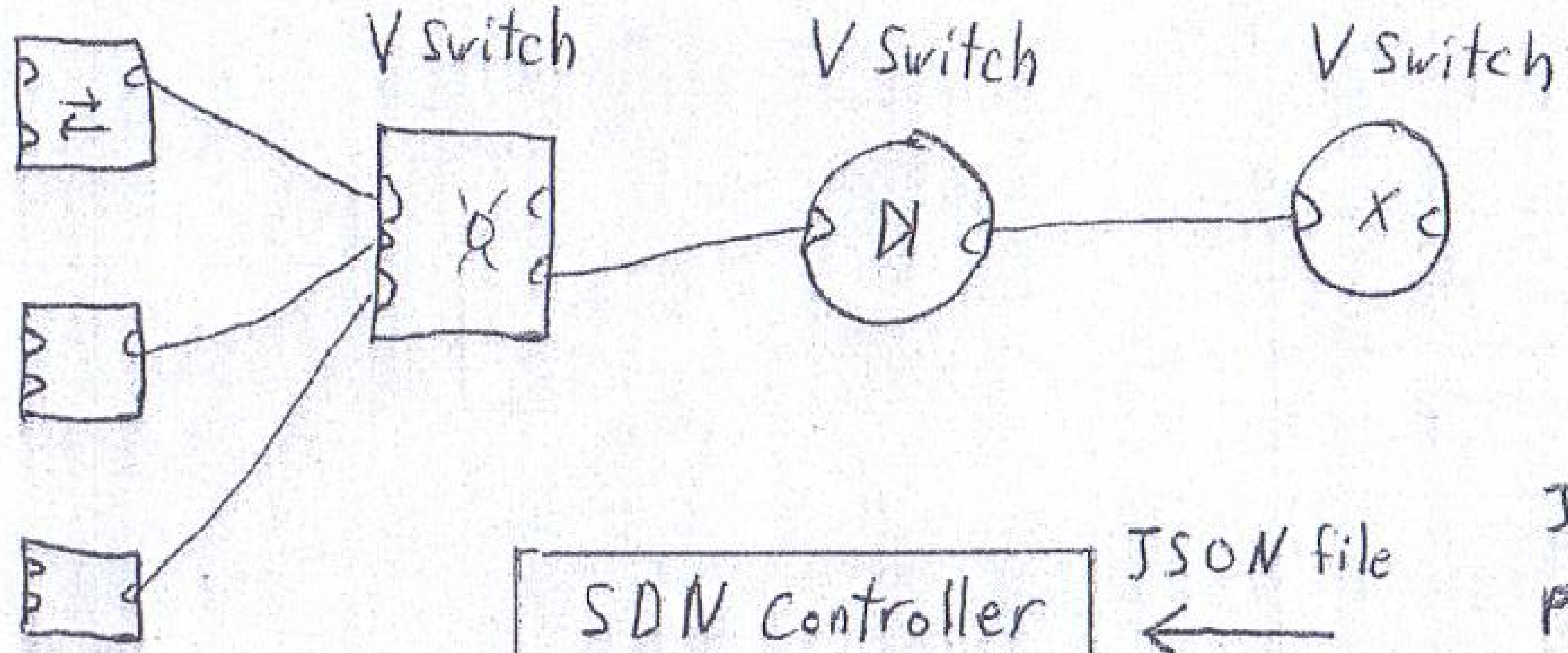
* SDN: Software Defined Network

Network Programability/Authentication/Orchestration

Traditional Devices: Standalone



Northbound Java, Python, REST conf.
SDN controller
Southbound V Switch



SDN Controller ← JSON file — Java, Python, REST Conf.

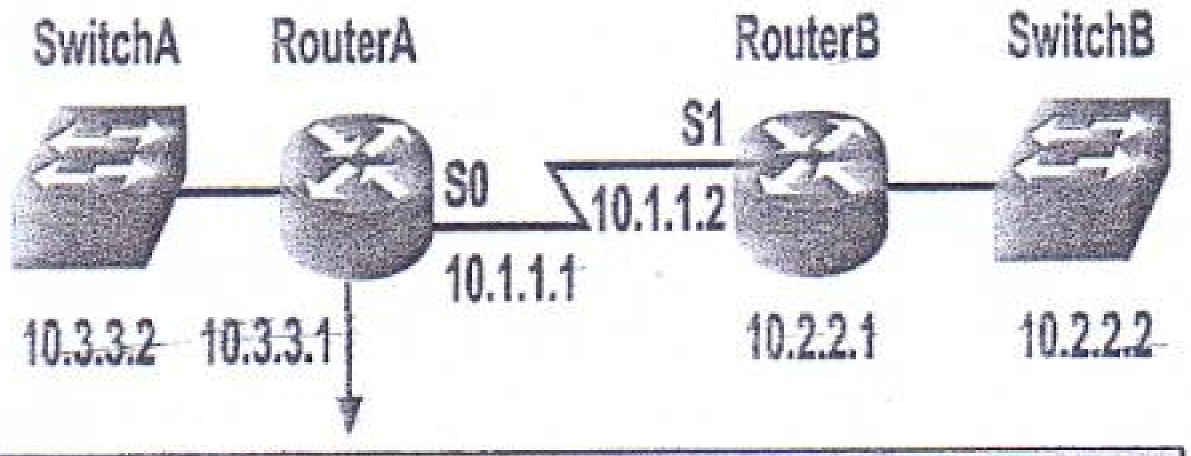
Management & Control

CDP (Cisco Discovery Protocol) & LLDP (Link Layer Discovery Protocol)

- CDP run by default on Cisco switches & send message every 60 sec on multicast MAC 0100.0ccc.cccc, Cisco Switches regard CDP as special address that should no be flooded (received only by neighbors), LLDP is same to CDP but standard.
- To disable CDP

(config)#[no] cdp run

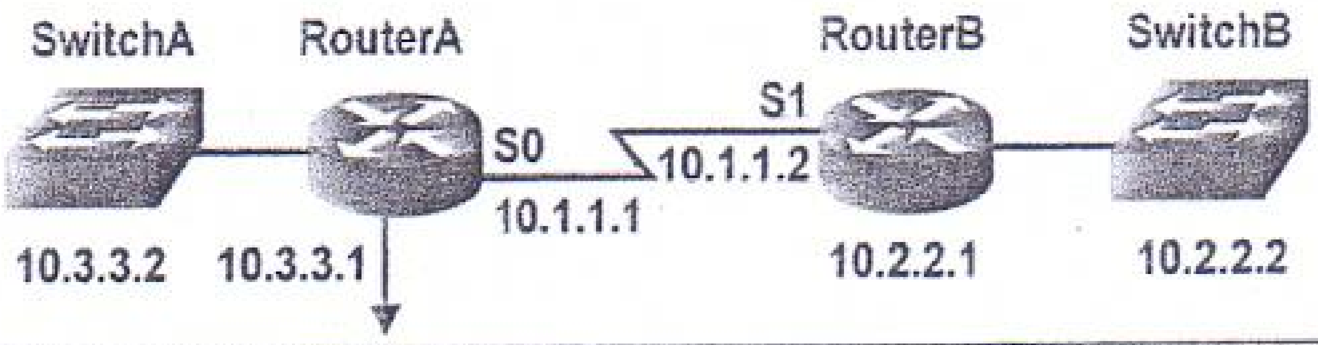
(config-if)#[no] cdp enable




```
RouterA#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID           Local Intrfce    Holdtme    Capability  Platform  Port ID
RouterB                Ser 0         148           R        2522      Ser 1
SwitchA0050BD855780 Eth 0            167          T S       1900      2
```

SwitchA also provides its MAC address (Catalyst 1900 only).




```
RouterA#Sh cdp Neighbor detail
-------------------------
Device ID: RouterB
Entry address(es):
  IP address: 10.1.1.2
Platform: cisco 2522,  Capabilities: Router
Interface: Serial0,  Port ID (outgoing port): Serial1
Holdtime : 168 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-JS-L), Version 12.0(3), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Mon 08-Feb-99 18:18 by phanguye
```

CDP (Cisco Discovery Protocol)

Send message every 60 seconds containing:

- Device name
- H/W Platform (model)
- S/W Platform (IOS version)
- Device Capabilities (Router, switch, IP Phone, Host, …)
- Local interfaces and neighbor interfaces
- Device IP and Sometimes MAC address

In CDP ver 2:

Added to the message:

- VTP Domain
- Native VLAN
- Duplex
- Rapid error tracking for (nativeVLAN mismatch,duplex mismatch,..)

Link Layer Discovery Protocol

~~The Link Layer Discovery~~ Protocol ~~(LLDP)~~ is similar to CDP, but is based on the IEEE 802.1ab standard. As a result, LLDP works in multivendor networks. It is also extensible because information is advertised.

LLDP also supports additional (messages) that are unique to audio-visual devices such as VoIP phones. The LLDP Media Endpoint Device carry useful ~~device information like a network policy~~ with ~~VLAN numbers~~ and ~~quality~~ of service information needed for voice traffic, power management, inventory management, and physical location data.

By default, LLDP is globally disabled on a Catalyst switch. To see if it is currently running or not, use the show lldp command. You can enable or disable LLDP with the lldp run ~~and no lldp run configuration commands,~~ respectively.

(config)#lldp run

On interface:

(config-if)#[no] lldp {transmit|receive}

Use the following command to display information about LLDP advertisements that have been received by a switch.

Switch# show lldp neighbors [*type member/module/number*] [*detail*]

Use the show lldp neighbors command to see a summary of neighbors that have been discovered.

```
[illegible] show lldp neighbors
Capability codes:
    [illegible]
    [illegible]
Device ID    Local Intf    Hold-time  Capability    Port ID
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
```

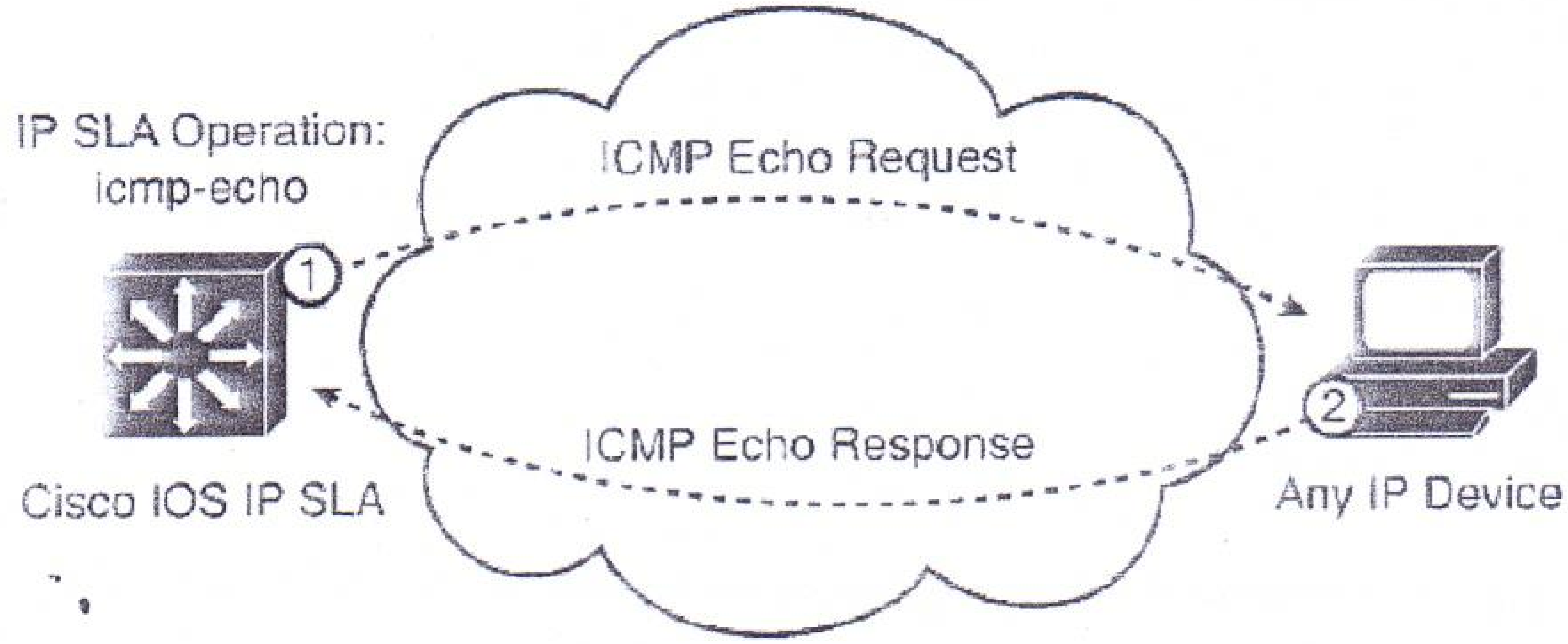
IP SLA (Service Level of Agreement)

IP SLA is a feature that enables a Cisco router or switch to simulate specific types of traffic and send it to a receiver called a *responder, to be used for measurement, monitoring and testing. IP SLA probes can simulate various types of traffic, such as HTTP, FTP, DHCP, UDP jitter, UDP* echo, HTTP, TCP connect, ICMP echo, ICMP path echo, ICMP path jitter, and DNS, and can report statistics such as path jitter, packet loss and delay. It has highly granular application configuration options such as TCP/UDP port numbers, TOS byte, and IP prefix bits. This is useful for measuring application performance end-to-end across your network. It can also be used to track reachability and then decrement HSRP priority values or bring up secondary links. Additionally, IP SLA can also be used as a measure of reliability and continuous availability. SNMP traps can be generated from events such as connection loss, timeout, roundtrip time threshold, average jitter threshold, one-way packet loss, one-way jitter, and one-way latency. There two parts of IP SLA, our testing source and the responder, the tester sends traffic and the responder only reply back.

To enable IP SLA, configure the source to send the required type of data probes. The receiver can be a computer, or it can be another Cisco device. The configuration of a Cisco responder is simple and only that command: Use the global ip sla responder command.

One benefit of using a Cisco device as the responder is that it can add time stamps to help measure latency and jitter.

The configuration of the IP SLA source is more complex. You must create a monitor session, list the traffic type, responder IP address, and any other desired variables such as DSCP value. Then you schedule the probes. Optionally configure tracking using the IP SLA session.



NTP (Network Time Protocol)

It is an application using UDP port 123 used for dynamic time adjustement and synchrinization, latest version is 4.
Imagine that you are reviewing device logs collected in a router's buffer and are attempting to correlate the events in the device logs with an issue that you are troubleshooting. To make that correlation, the logged events need to have accurate timestamps.

Although you could individually set the clock on each of your routers, those clocks might drift over time and not agree. You might have heard the saying that a man with one watch always knows what time it is, but a man with two watches is never quite sure. This implies that devices need to have a common point of reference for their time. Such a reference point is made possible by Network Time Protocol (NTP), which allows routers to point to a device acting as an NTP server. Because devices in different time zones might reference the same NTP server, each device has its own time zone configuration, which indicates how many hours its time zone differs from Greenwich Mean Time (GMT).

NTP uses a value, called a stratum value, to indicate the believability of a time source. Valid stratum values are in the range 0–15, with a value of 16 being used to indicate that a device does not have its time synchronized. However, Cisco IOS only permits you to set stratum values in the range 1–15.
Lower stratum values are considered more authoritative than higher stratum values, with a stratum value of 0 being the most authoritative. Stratum calculations work much like a hop count.
For example, an Internet-based time source using a cesium clock might have a stratum value of a 0. If one of your routers learns time from this stratum 0 time source, your router will have a stratum level of 1.
If other devices (for example, servers, switches, and other routers) in your network get their time from your stratum 1 router, they will each have a stratum level of 2.

NTP Synchronization modes:
-Clients listen to NTP server btroadcasts to synchronize and adjust its clock.
- Clients polls NTP server for time.

For NTP to Synchronize time, ther are two methods:

Method1:

-Clients listen to NTP server btroadcasts to synchronize and adjust its clock.

Server(config)#ntp master 3
Server(config)#int fa0
Server(config-if)#ntp broadcast …. Allow server to send broadcast packet containing the time.

Clinet(config)#int fa1
Client(config-if)# ntp broadcasts client ..allow ntp client to receive ntp broadcasts on that interface

Method2:

- Clients polls (request & wait reply) NTP server for time.

Server(config)#ntp master 3

Client(config)#ntp server ip of server

ROUTER R1 (Server) CONFIGURATION for authentication:
R1# conf term
Enter configuration commands, one per line. End with CNTL/Z.

R1(config)# ntp master 1 ...defines router as stratum 1

ROUTER R2 (client) CONFIGURATION for authentication
R2# conf term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)# ntp server 172.16.0.1

For troubleshooting NTP use:
#show ntp status
#show ntp associations

Syslog (System Message Logging):

Syslog is a protocol that is used to permit network devices to send their system messages across the network to a syslog server, so events as interface up or down, routing protocol neighborship established or tear down, or any debug lines can be saved to that server.

Also syslog messages can be sent to the logging buffer inside a router or a switch, and it can be displayed using

show logging or famously #show log

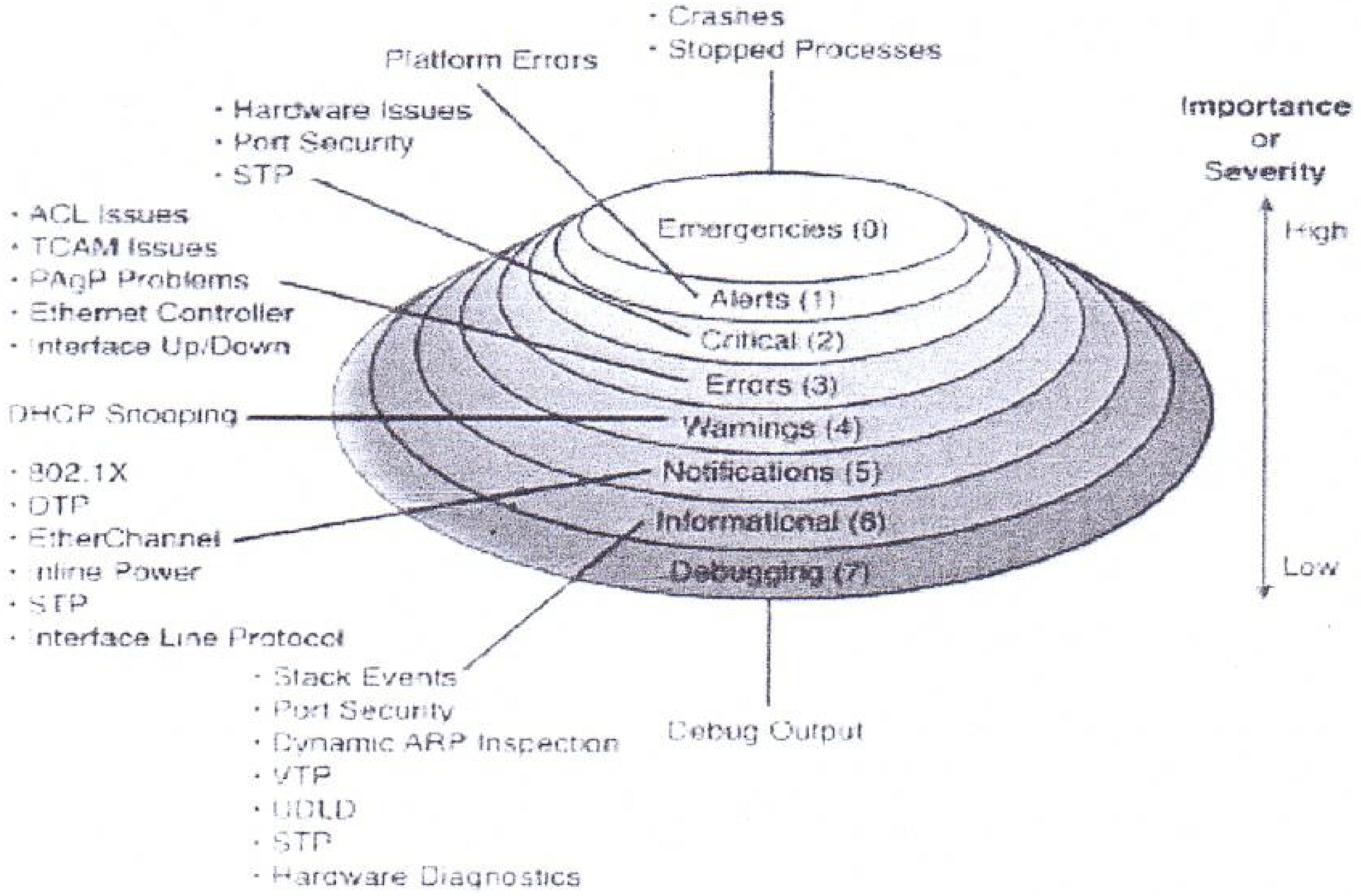
And to ~~order the device to buffer~~ logs in internal memory of router or switch use (config)#logging buffer

To tell ~~router or~~ switch the IP address of a syslog server, use (config)#logging ip of server

One of the very famous syslog server softwares is called KIWI

Syslog messages have 8 types called:

Emergency (0), Alert (1), Critical (2), Error (3), Warning (4),



* Network management:

* Syslog:

It is an application called systemlogging used to send alarms about major network changes.

Interface up/down   Protocol change   Remote login info.   Debug

01:12:13   serial a/o changed state to up

02:15:10   EIGRP neighbor is up

03:17:23   10.1.1.10 exit from VTyo

04:19:00   STP changed from listen to learn state

By default all these msgs appears on console

Terminal monitor

law nta 7abeb w nta 3amal Telnet t-shot l syslog msgs.

SNMP (Simple Network Management Protocol):

It is an application that provide a mean of sending management messages (called SNMP traps) from various network device needed to be monitored to a SNMP server, the device which is needed to be managed is called SNMP agent, and the managing device is called Manager, and the database collected is called MIB (Management Information Base) and the software installed on Manager is called NMS (Network Management Station Software), of the most famous NMSs are Cisco Works, Cisco Prime, HP open view, IBM Tivoli.

Most commonly a network administrator gathers and stores statistics over time using NMS, this info may contain devices processing(#show process cpu), memory utilization(#show process memory), interface status changes, any protocol state, also SNMP can used to make remote configuration.

Simply SNMP operation is TIMAMN

Trap/Inform message is sent from MIB of Agent to Manager NMS

Network Programability or SDN (S/W Defined Network):

A new trend in networks now is using Lightweight devices with least amount of S/w & H/w, & that is now happening even with routers & switches.

ALL required Calculations, decisions & functions is implemented on a Network Controller.

From that Controller we Can Program (Configure) all network devices & help them take Correct forwarding decisions with minimum amount of H/w, S/w & Cost.

- Cisco new tool APIC-EM is used for SDN Purpose. & also Cisco DNA is used for large Scaled networks.
- ALL SDN Controllers has Management Plane for high scalability network management.

Session 8 /1

Router Startup:

1. Run POST Program — Power On Self Test } H/W Test

2. Router check configuration register

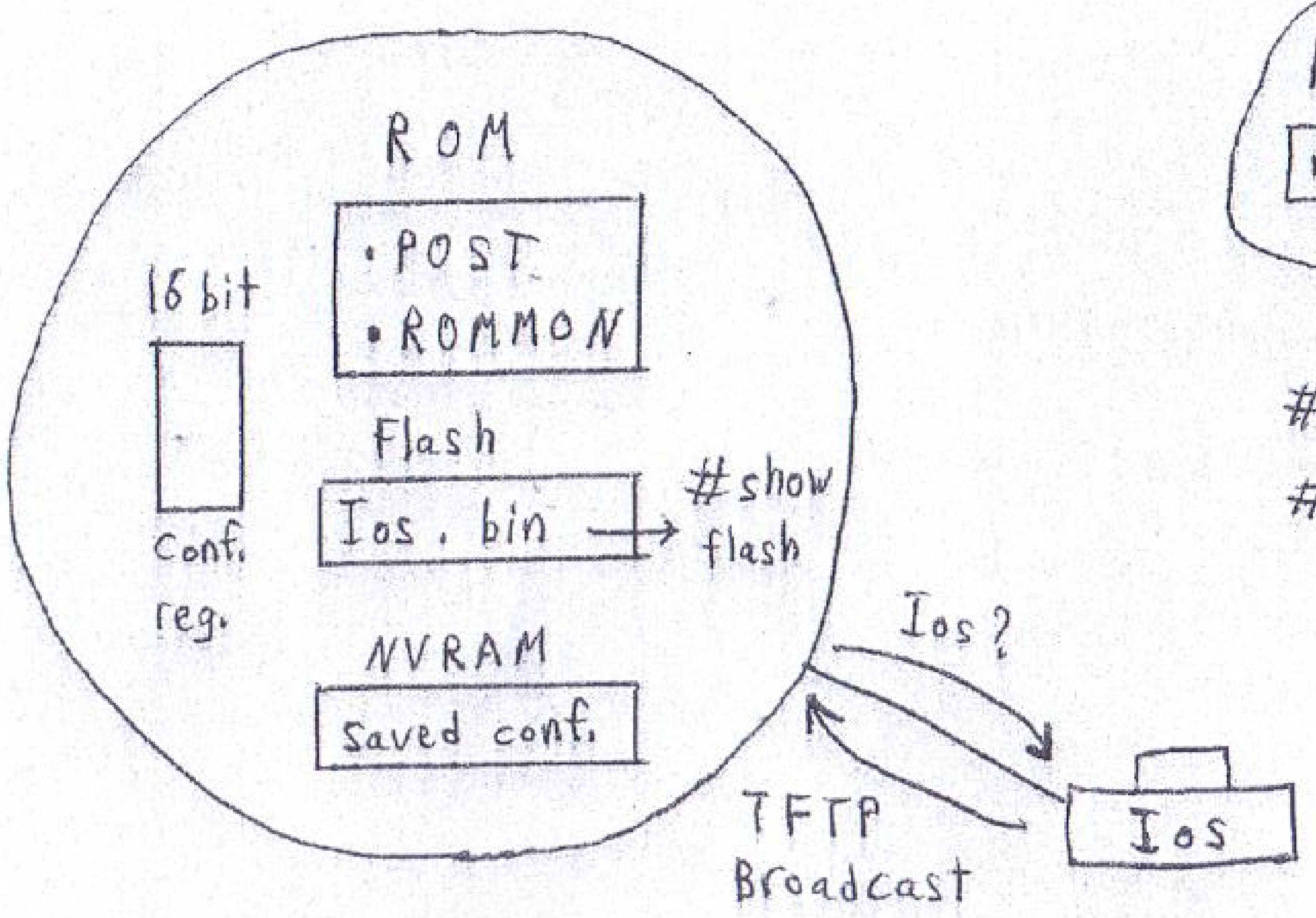
   OX 2102 (Hexa) < load Ios normally / load conf. file normally

3. Load Ios

Flash
TFTP
mini os Rommon

4. Load Conf. file

NVRAM
TFTP
Setup mode [y/n]



Password Recovery: by Console only

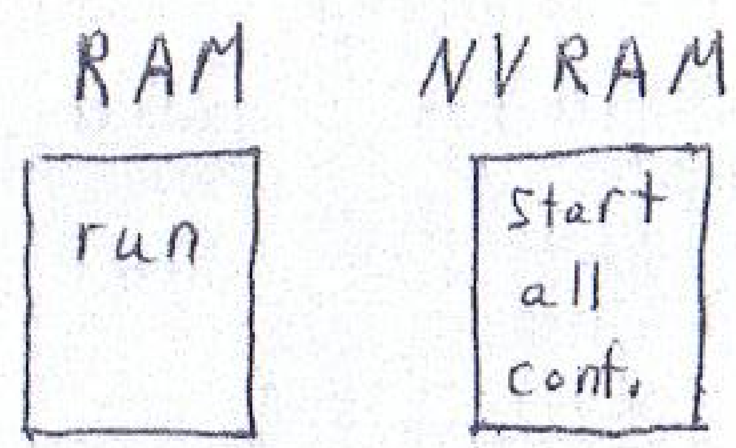
x

1. Power off / on

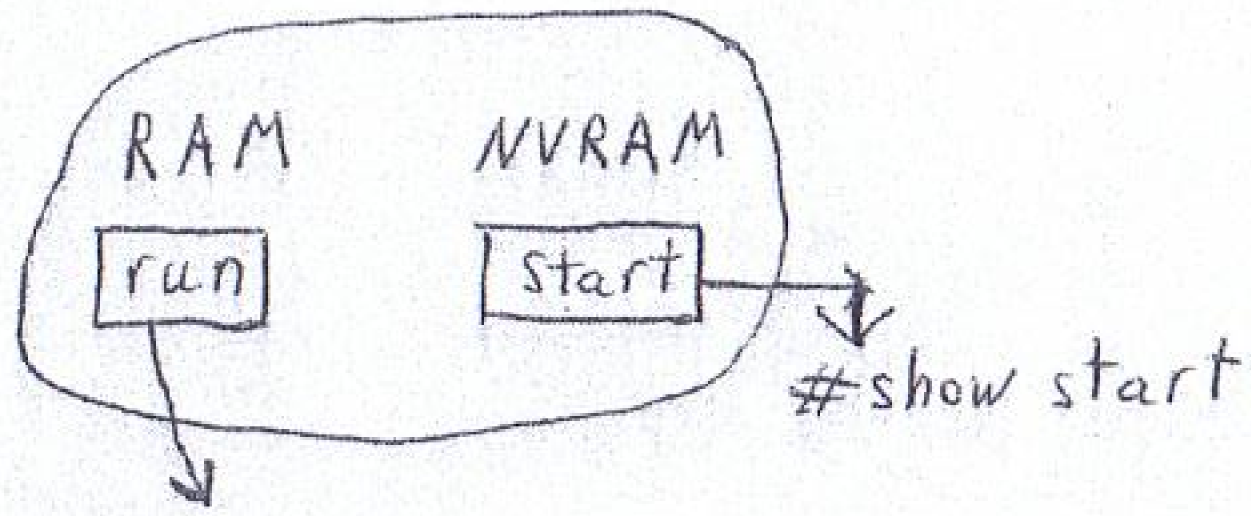
2. Press Ctrl / Break

3. Rommon > Conf. reg.

   OX 2102 < load Ios normally / bypass NVRAM



4. Power off/on → (config)# conf. - register OX2142



#show run

#copy run start

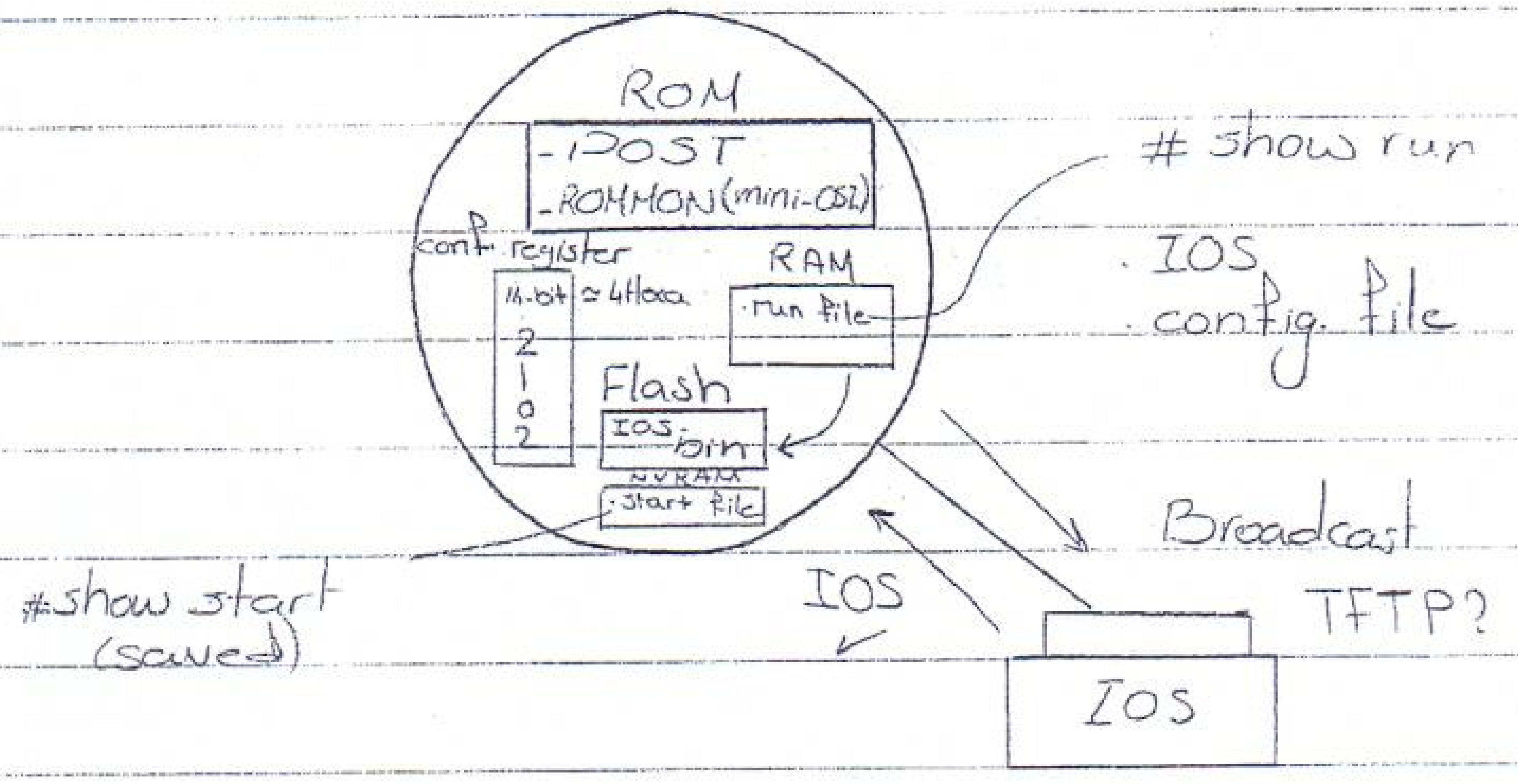
save conf.

* Router boot up sequence:

When power on Router:

1- Router run program called POST from ROM
(Test H/W)

Power on Self Test



2- Router consult configuration register (0x 2102) 2142

Hexa

Load IOS normally

Load config file normally

bypass config

3- Load IOS.

ⓐ	Flash
ⓑ	TFTP
ⓒ	ROMMON

4- Load config. file.

ⓐ	NVRAM	→ RAM
ⓑ	TFTP	
ⓒ	setup mode(Y/N)	

copy run start

To save configuration

* Password recovery: by console (not VTY)

1- Power off / on.

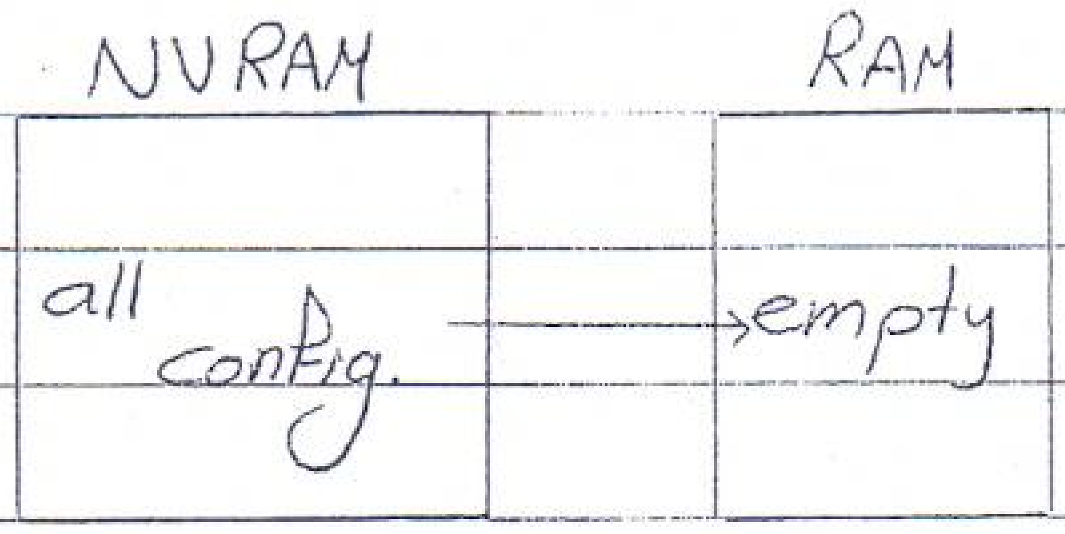
2. Press ctrl / break.

3. ROMMON > config 0x2142

load IOS normally

bypass configuration

4. Power off / on



5. # copy start run.

(config) # enable secret new

copy run start

Session 8/2

IP_{V4} : 32 bit

* Represented in dotted decimal octets

192 . 168 . 7 . 3

IP_{V6} : 128 bit

Q : Why we need IP_{V6} ?

A : Because we need larger address space

No. of $IP_{V6} = 2^{128} = 3.4 \times 10^{38}$ IP_{V6}

$\cong 5 \times 10^{28}$ IP_{V6} / human

* Represented in Coloned Hexa decimal fields

203B : FACE : B00C : 0003 : 0001 : 2345 : 6789 : ABCD

4 Hexa = 16 bit = Field   8 Fields = 128 bit

Rule 1:

Leading zeros in a field are optional

ex: 203B : 0003 : 000C : 00B7 : ____

= 203B : 3 : C : B7 : ____

Rule 2: Field of all zeros = :0:

ex: 203B : 0003 : 0000 : 000C : ____

= 203B : 3 : 0 : C : ____

Rule 3: Successive fields at all zeros = ::

ex: 203B : 0000 : 0000 : 0000 : 1234 : 0000 : 0000 : ABCD

= 203B :: 1234 :: ABCD X - used only once

= 203B :: 1234 : 0 : 0 : ABCD ✓

Ex: FF02 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 00005

= FF02 :: 5 ⟷ 224.0.0.5

(OSPF v3)   (OSPF v2)

Ex: 0 : 0 : 0 : 0 : 0 : 0 : 0 : 1

= 0 :: 1 ≅ ::1 ⟷ 127.0.0.1

(TCP/IP_{V6} loopback Test)   (Test TCP/IP_{V4} loopback)

Ex: 0:0:0:0:0:0:0:0

= 0::0 = 0:: = ::0

= :: ⟷ 0.0.0.0

(All IP_{V6} networks)   (All IP_{V4} networks)

IP_{v6} Classes: Only one class called Defaut class

Session 8/3

Prefix	Interface ID
Network Part	Host Part
64 bit	64 bit

Default Mask = (Prefix length) = /64

/24

no. of $IP = 2^{32-24}$

$= 2^8 = 256$ IP

/120

no. of $IP_{v6} =$

$2^{128-120} = 2^8 = 256$ IP

/30

no. of $IP = 2^{32-30}$

$= 2^2 = 4$ IP

/126

no. of $IP_{v6} =$

$2^{128-126} = 2^2 = 4$ IP

Assigning IP_{v6} address to hosts:

- Static (manual)
- $DHCP_{v6}$ (statefull → full conf.)
- SLAAC (Stateless Address Auto Configuration)

$\underbrace{AAAAAA}_{\text{OUI: Vendor}}\ \underbrace{AAAAAA}_{\text{Host}} = 48$ bit

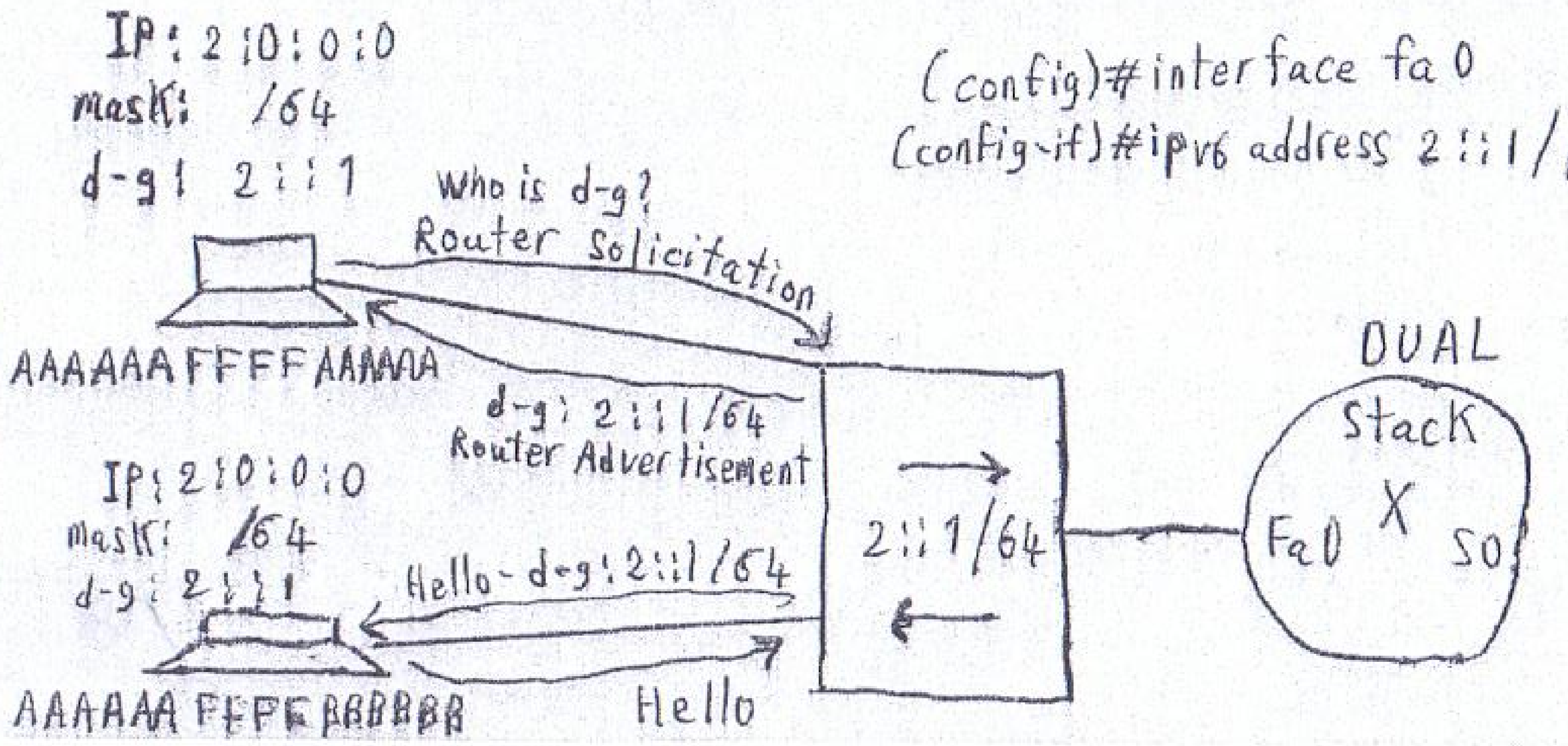
⇓

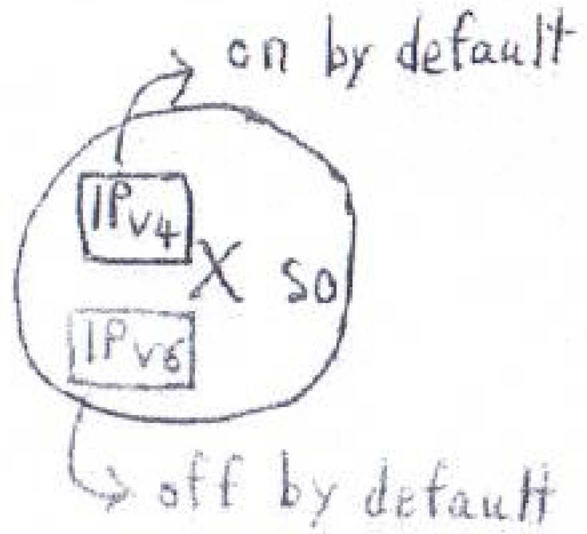
$\boxed{EUI-64}$ External Universal ID = 64 bit

⇓

$\underbrace{AAAAAA}_{24\ bit}\ \underbrace{FFFF}_{16\ bit}\ \underbrace{AAAAAA}_{24\ bit} = 64$ bit

(config)#interface fa0
(config-if)#ipv6 address 2::1/64





Activate IP_{v6} Router,

(config)# IP_{v6} unicast routing

(config)# ip route $\underbrace{0.0.0.0}_{network}$ $\underbrace{0.0.0.0}_{mask}$ S0

(config)# ipv6 route :: /0 S0

Session 8/4

IPv4 Addresses' Types

UniCast

- Loopback
  127.0.0.1
- LAN only (APIPA)
  169.254.X.X/16
- Private LAN/WAN
  10.X.X.X
  172.16.X.X - 172.31.X.X
  192.168.0.X
- Public/Real IP

MultiCast

Class D
224.X.X.X-239.X.X.X

224.0.0.2] All IPv4 Routers

224.0.0.5] OSPF
224.0.0.6] Ver. 2

224.0.0.9] RIP v2

224.0.0.10] EIGRP v4

Broadcast

255.255.255.255
DHCP
RIP v1
IGRP

IPv6 Addresses' Types

Broadcast

(N/A)

MultiCast

FF XX:X___

FF02::2] All IPv6 Routers

FF02::5] OSPF
FF02::6] Ver. 3

FF02::9] RIP ng
next generation

FF02::A] EIGRP v6

Unicast

loopback
::1

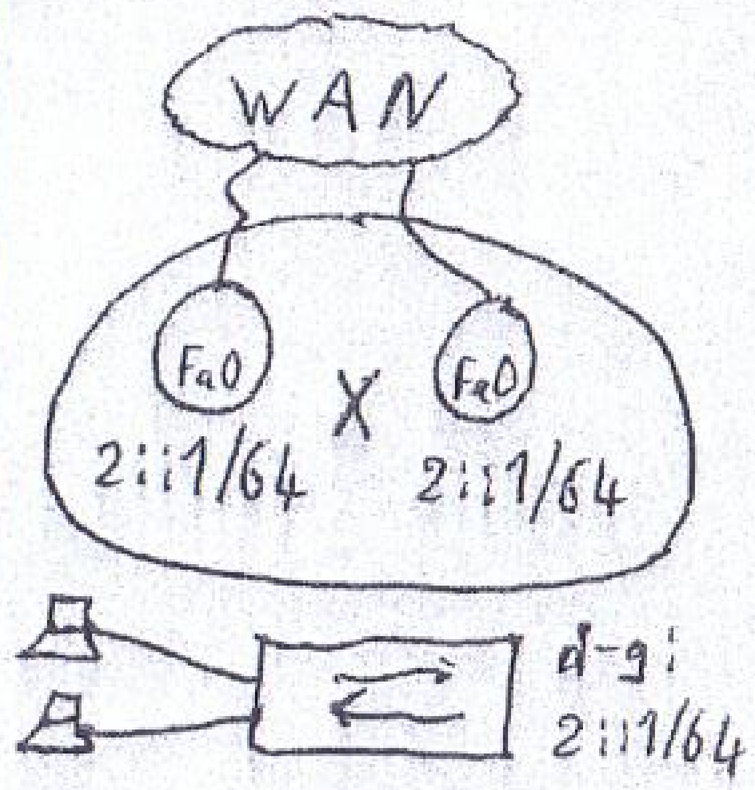
Link Local
FE80:___

Site Local
(Local Branches)
FEC0:___
FC00:___

Global IP
2XXX:___
3XXX:___

AnyCast

one to nearst
one to any



HSRP - VRRP - GLBP

(config)# int fa0

(config-if)# ipv6 address 2::1/64 anycast

OSPF version 3:

```
(config)# ipv6 router ospf 1
(config-rtr)# router-id 1.1.1.1

(config)# int fa0
(config-if)# ipv6 ospf 1 area 0

(config)# Int S0
(config-if)# ipv6 ospf 1 area 0
```

IPv6 Routing :

. Activate IPv6 Router Processor

(Config) # ipv6 unicast-routing

. Create routing Process

(Config) # ipv6 router ospf 1

. Activate routing Protocol on interface

(Config) # interface fa0/0

(Config-if) # ipv6 ospf 1 area 0
Process id

→ exit

(Config) # interface S0/0

(Config-if) # ipv6 ospf 1 area 0

The End :)