NATIONAL UNIVERSITY OF COMPUTER & EMERGING SCIENCE
Computer Network Lab (CL-307)
Lab Session 08

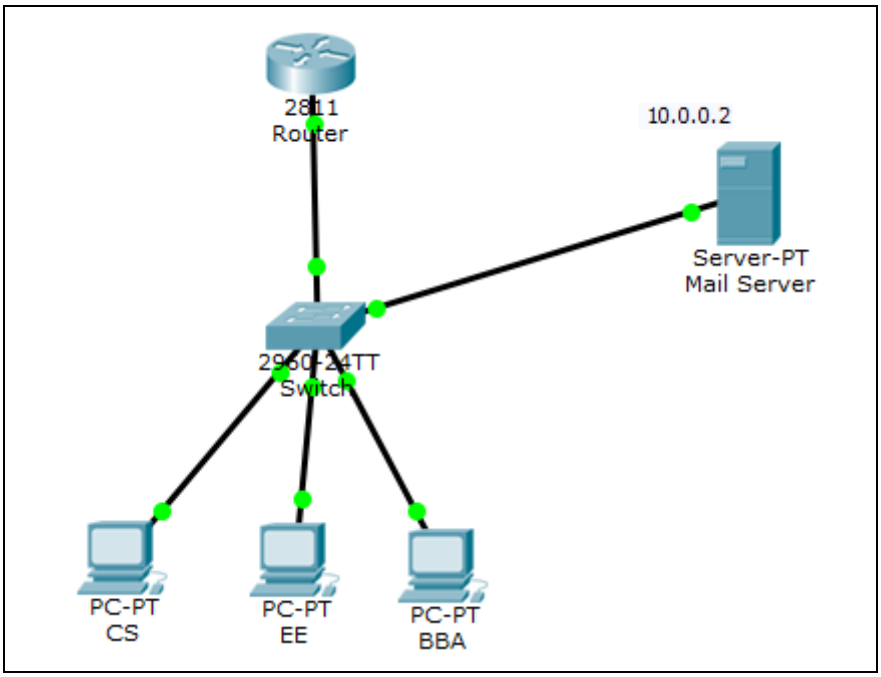
Application Layer Protocol

SMTP &POP3

Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (email) transmission. First defined by RFC 821 in 1982, it was last updated in 2008 with Extended SMTP additions by RFC 5321, which is the protocol in widespread use today. Although electronic mail servers and other mail transfer agents use SMTP to send and receive mail messages, user-level client mail applications typically use SMTP only for sending messages to a mail server for relaying. For retrieving messages, client applications usually use either IMAP or POP3.

SMTP communication between mail servers uses port 25. Mail clients on the other hand, often submit the outgoing emails to a mail server on port 587. Despite being deprecated, mail providers sometimes still permit the use of nonstandard port 465 for this purpose.

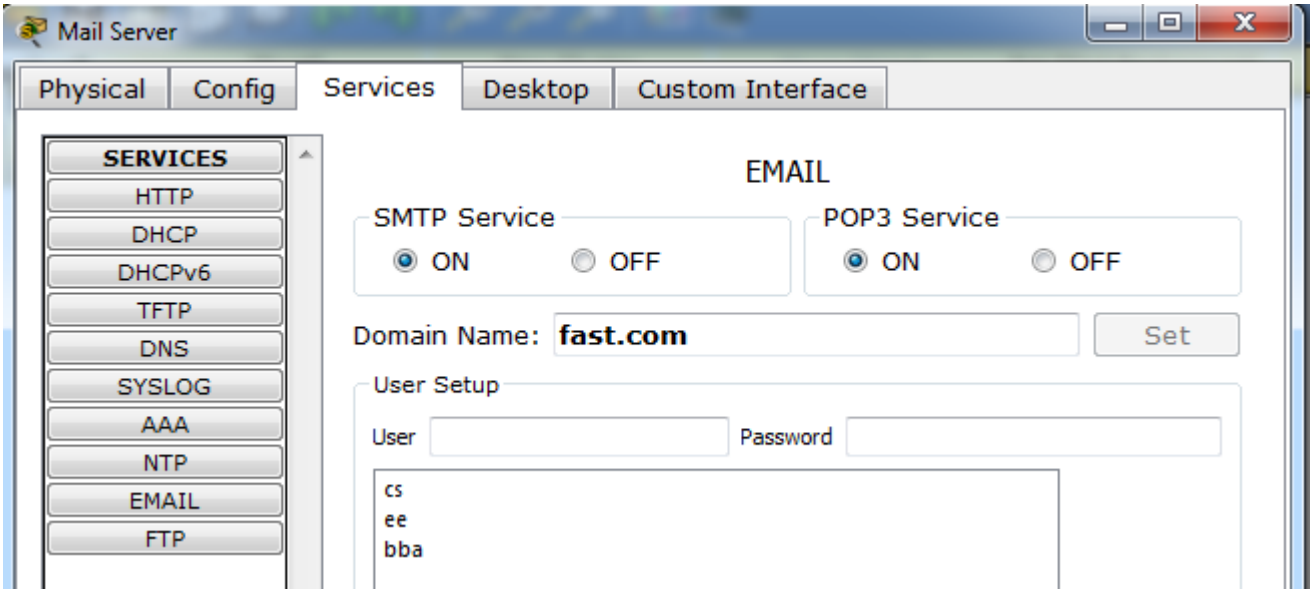
Topology



Objectives: Configure and Verify Email Services

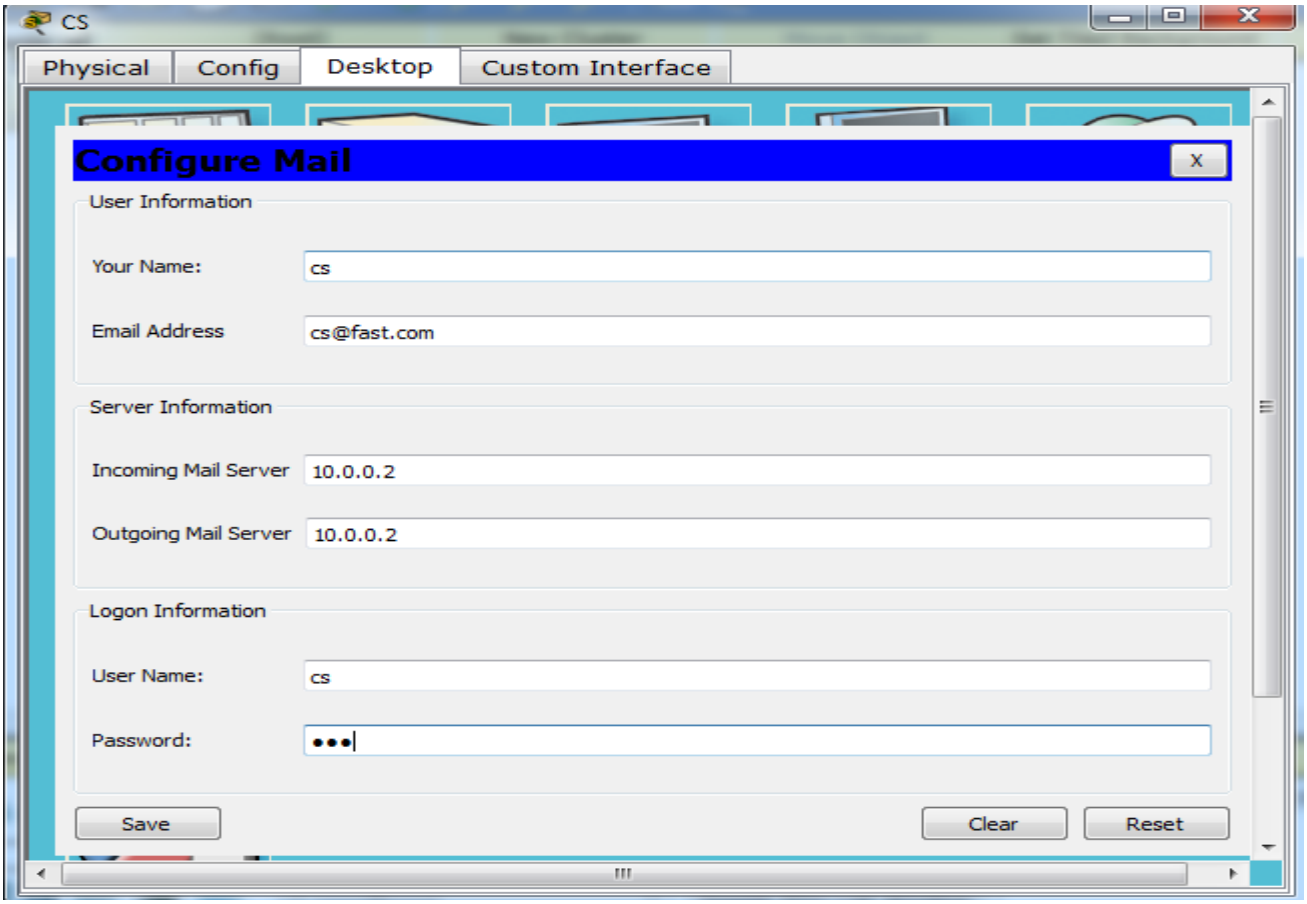
- Click on Mail server →services →EMAIL
- Enable SMTP & POP3 Service
- Set Domain Name:fast.com
- Add users.

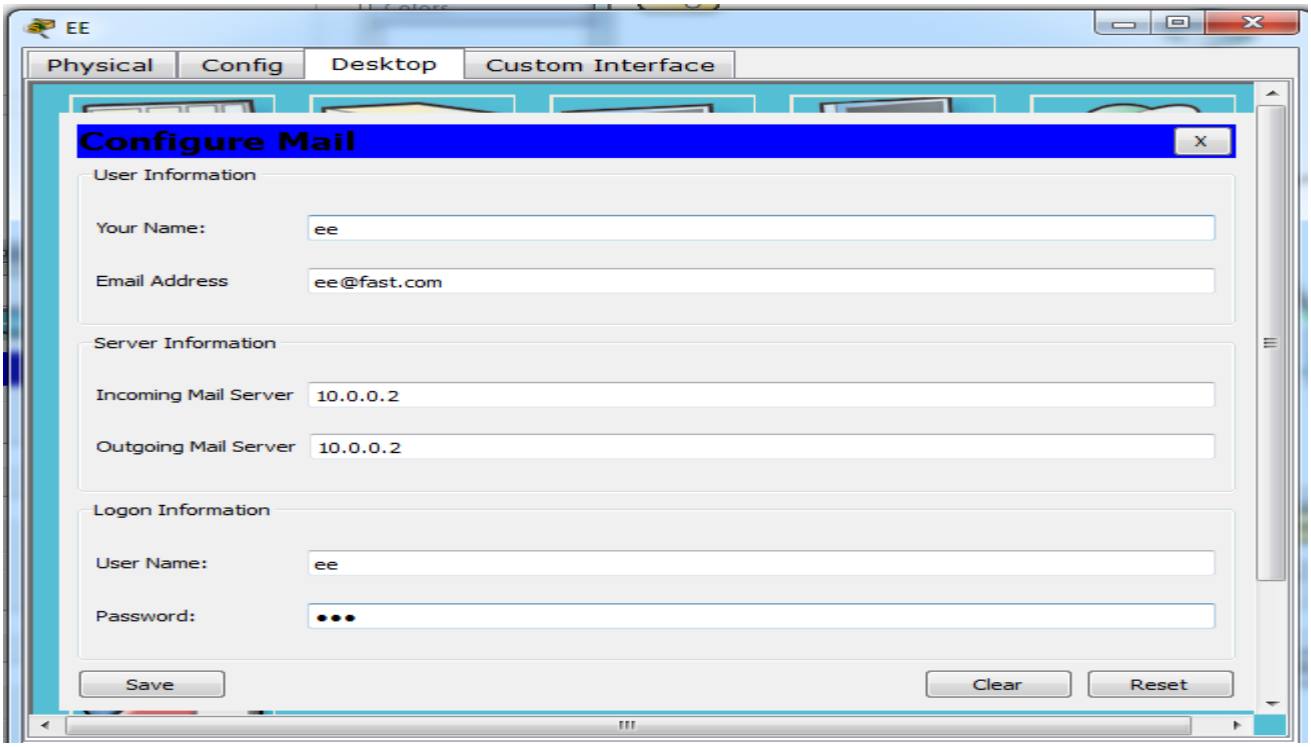
User name	password
cs	123
ee	123
bba	123

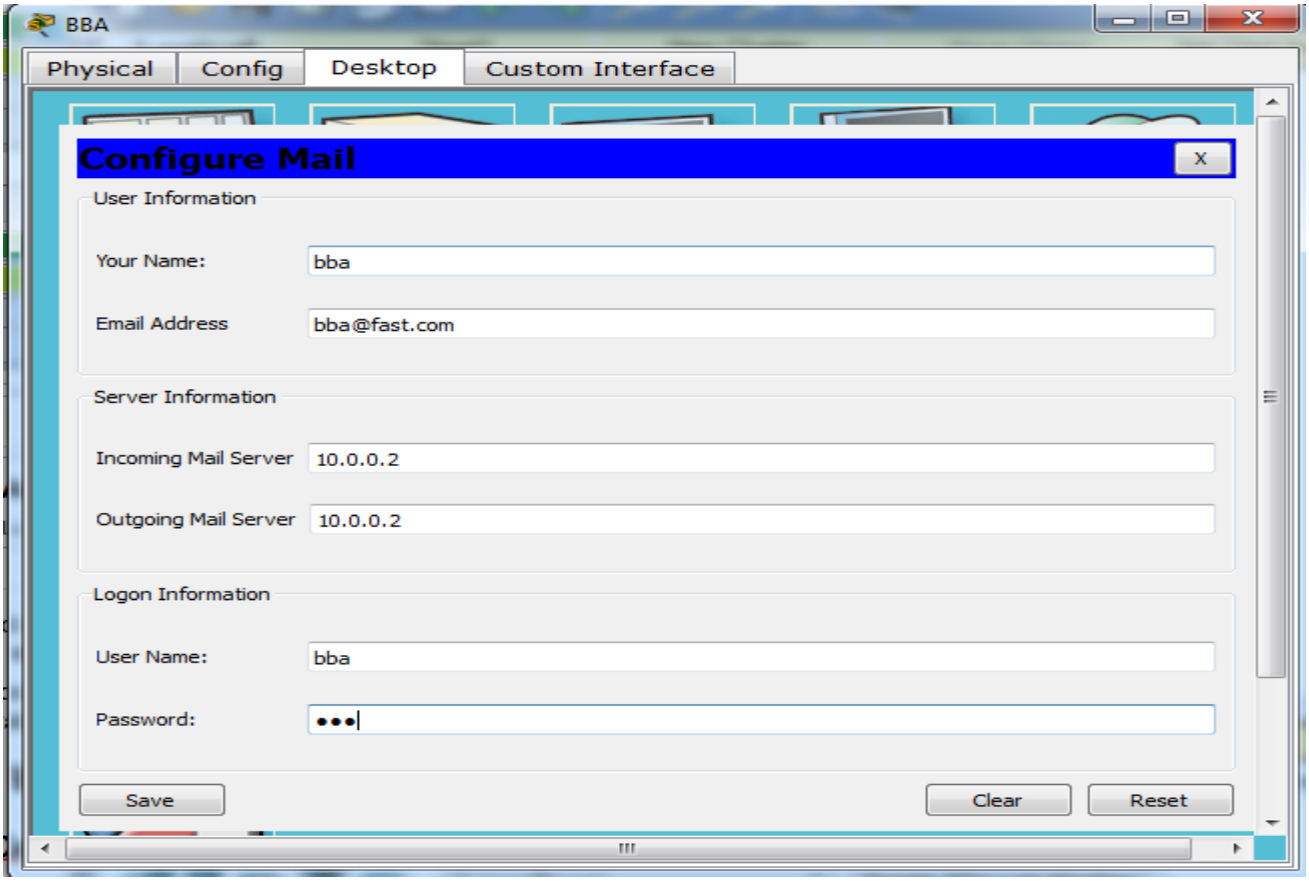


Now configuring user email account.

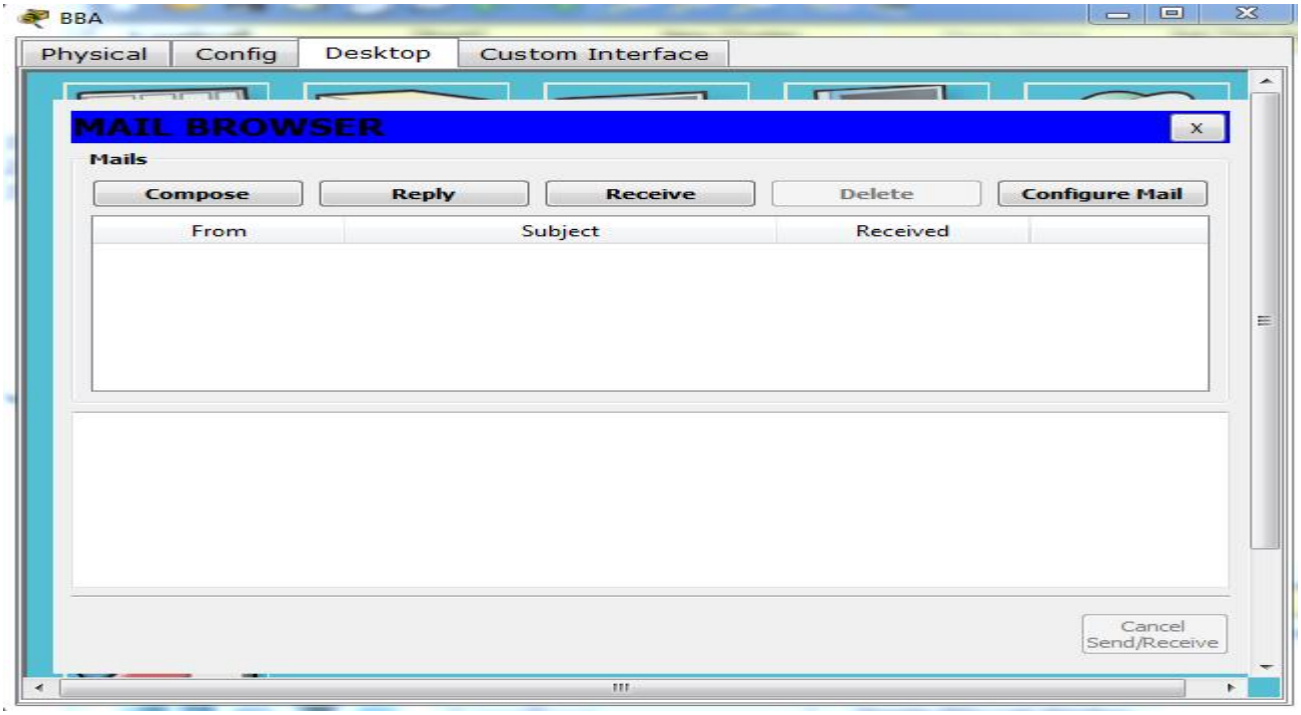
Go to pc →desktop →Email



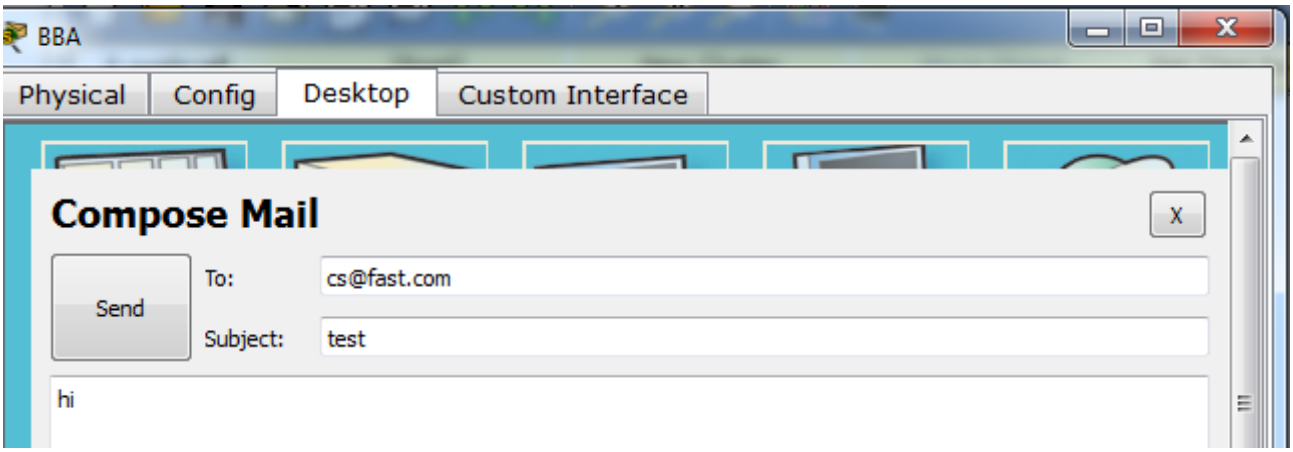

EE
Physical
Config
Desktop
Custom Interface
Configure Mail
X
User Information
Your Name:
ee
Email Address
ee@fast.com
Server Information
Incoming Mail Server
10.0.0.2
Outgoing Mail Server
10.0.0.2
Logon Information
User Name:
ee
Password:
Save
Clear
Reset


BBA
Physical
Config
Desktop
Custom Interface
Configure Mail
X
User Information
Your Name:
bba
Email Address
bba@fast.com
Server Information
Incoming Mail Server
10.0.0.2
Outgoing Mail Server
10.0.0.2
Logon Information
User Name:
bba
Password:
Save
Clear
Reset

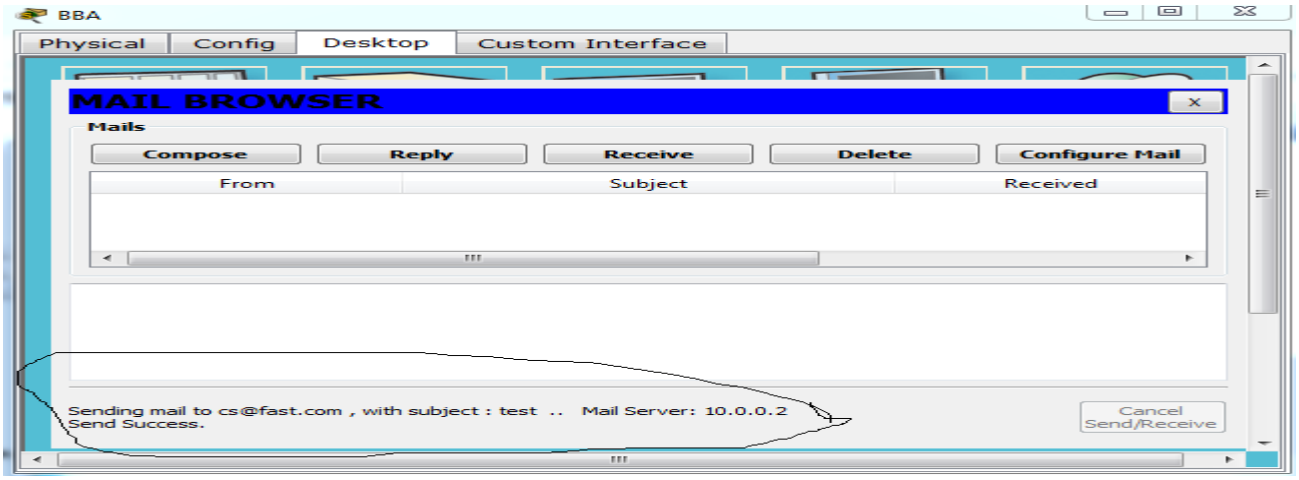
Click save



Now compose email → cs@fast .com

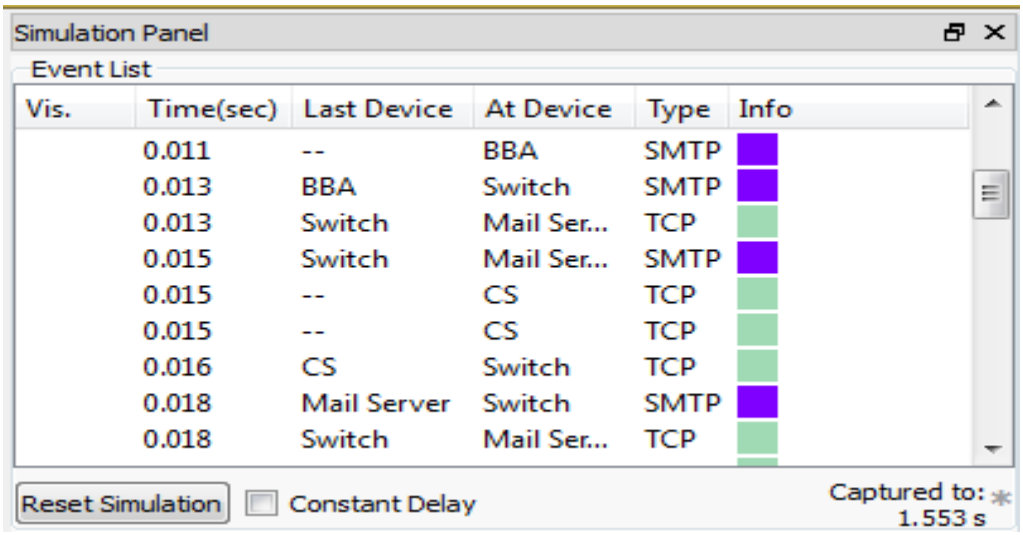


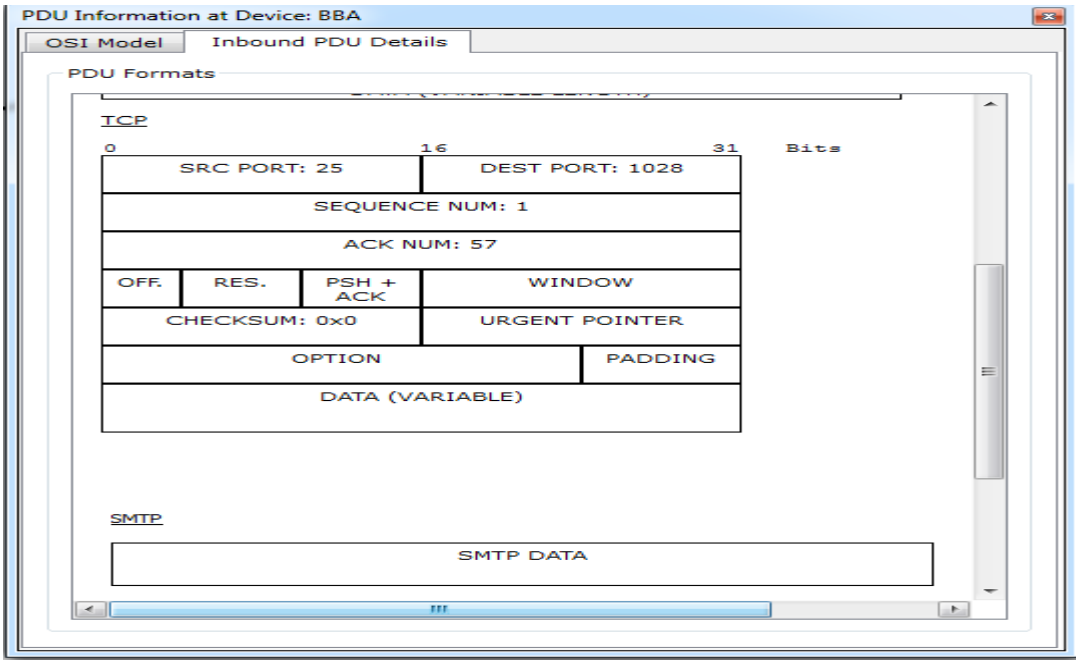
Click on send

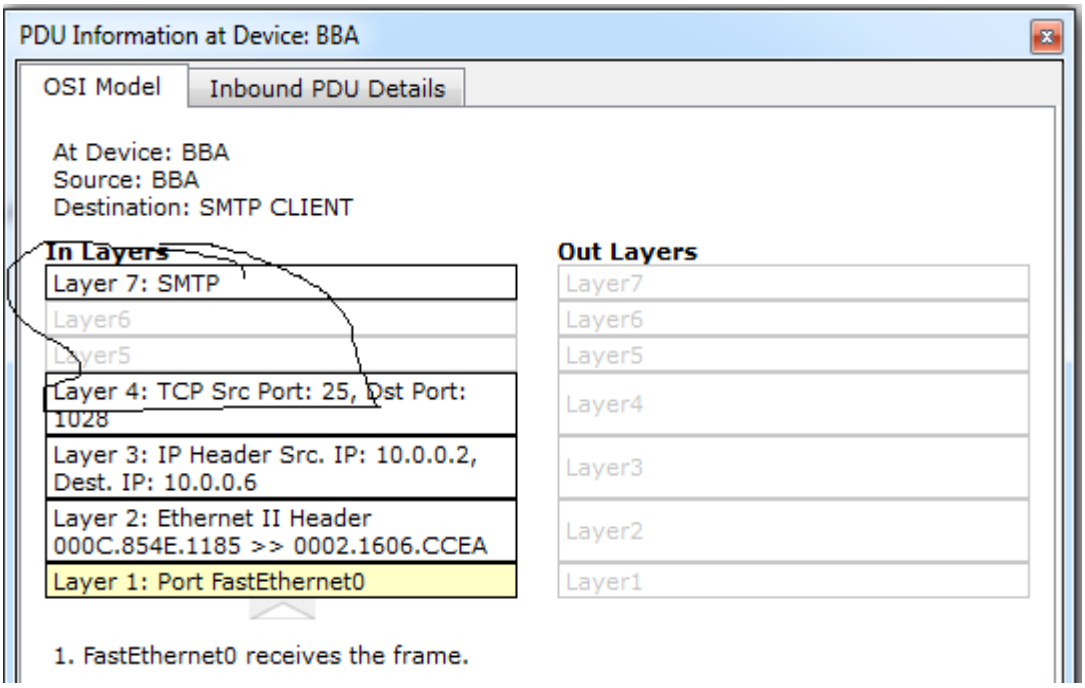


SIMULATION:

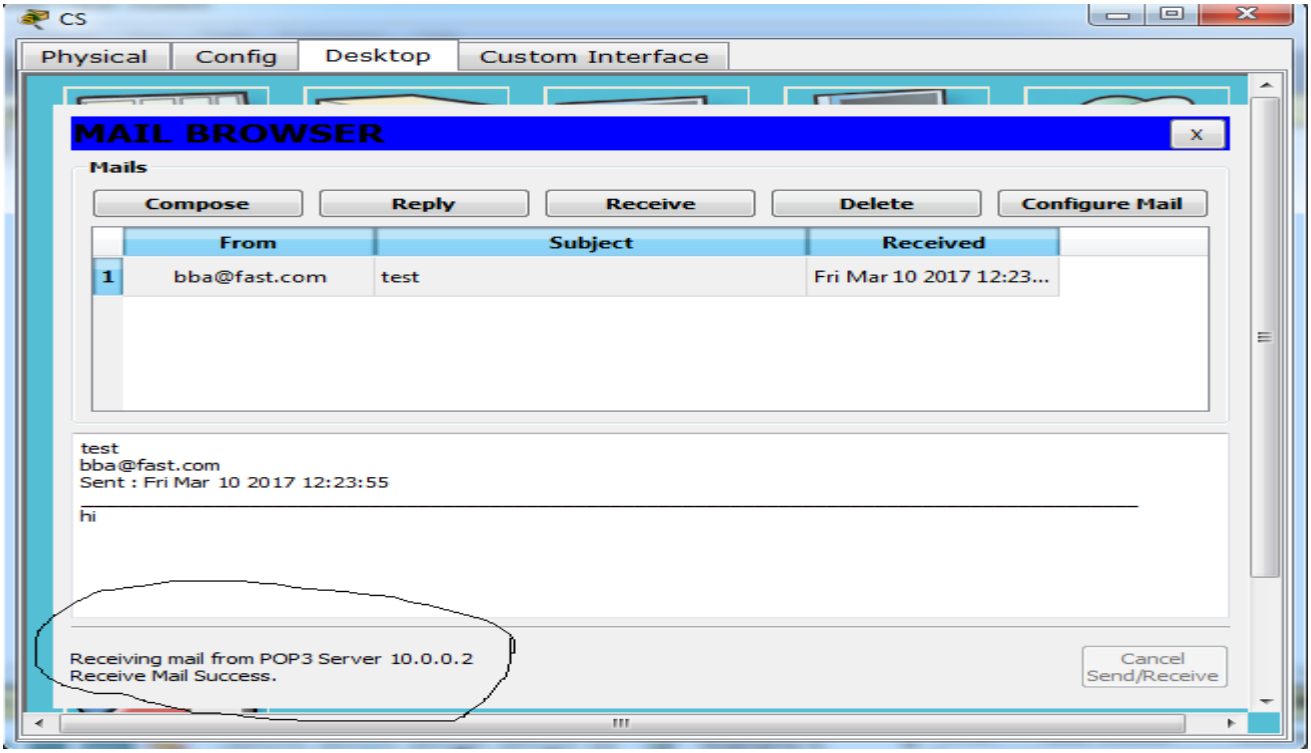
Now to note the POP3 header format information go to simulation mode →edit filters and click on SMTP &POP3 check box then click on capture/forward button. Now see how mail server works.

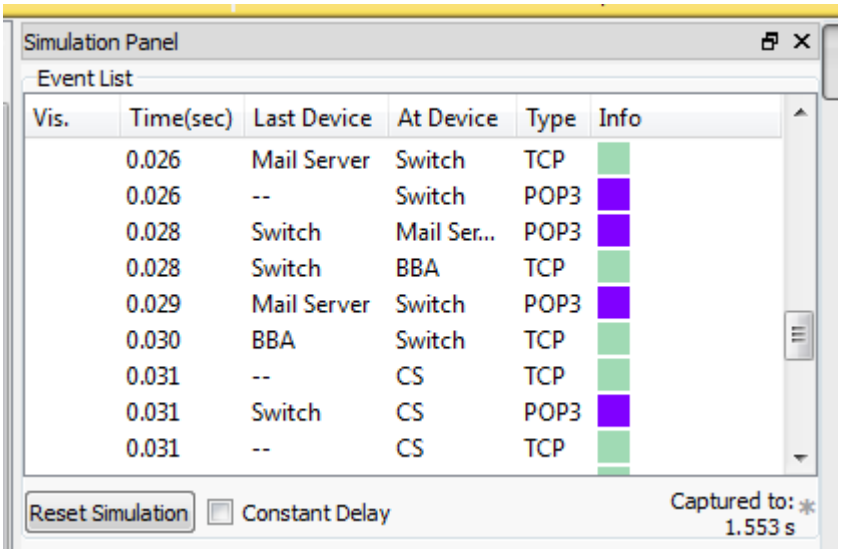


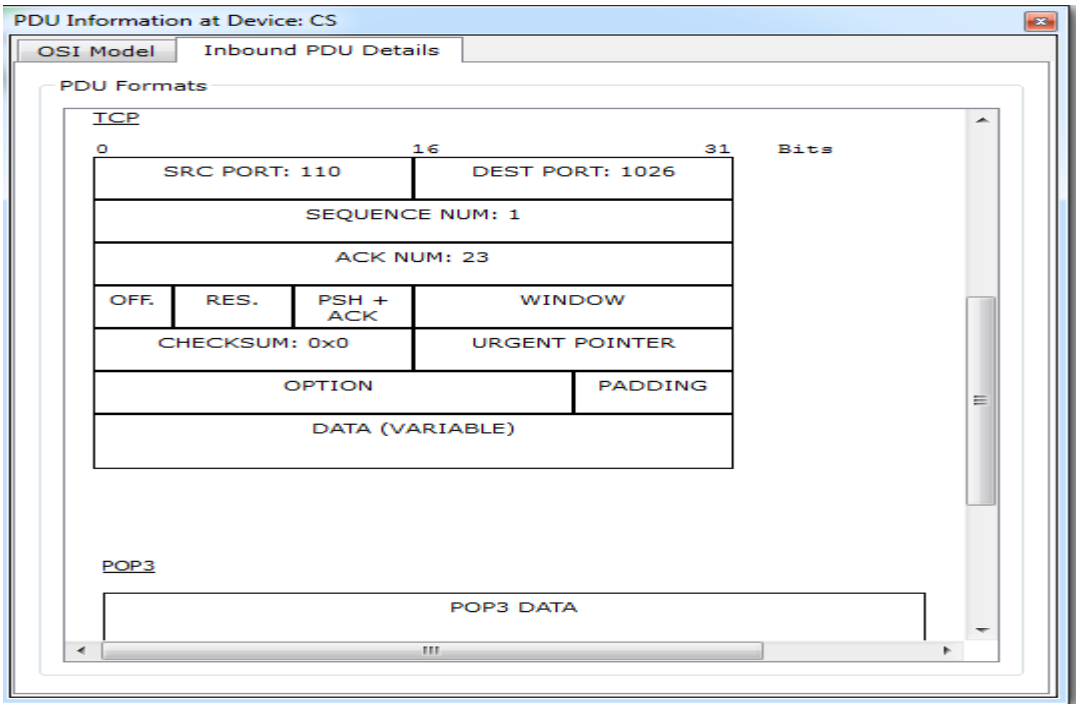


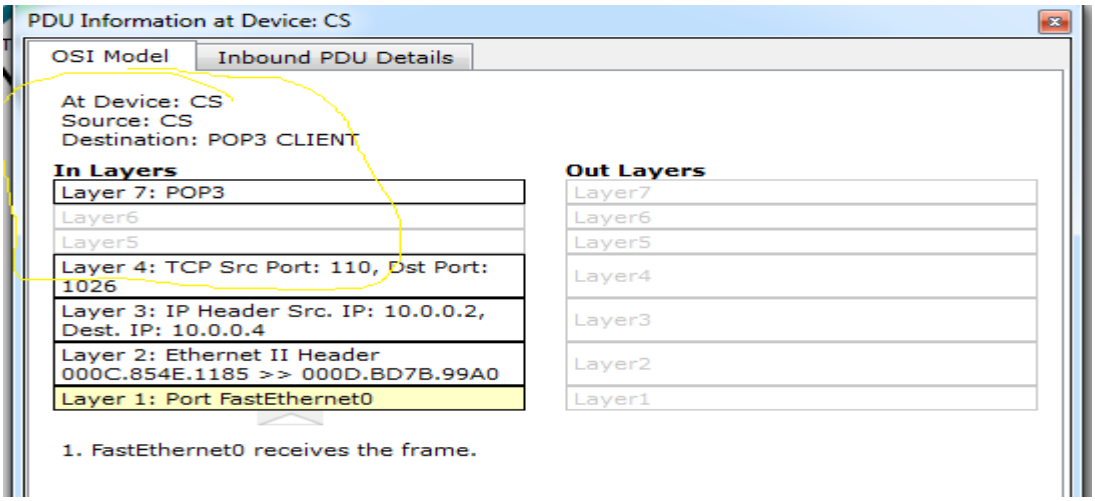


Now go CS account and click on receive:




Simulation Panel
Event List
Vis. Time(sec) Last Device At Device Type Info
0.026 Mail Server Switch TCP
0.026 -- Switch POP3
0.028 Switch Mail Ser... POP3
0.028 Switch BBA TCP
0.029 Mail Server Switch POP3
0.030 BBA Switch TCP
0.031 -- CS TCP
0.031 Switch CS POP3
0.031 -- CS TCP
Reset Simulation
Constant Delay
Captured to: 1.553 s


PDU Information at Device: CS
OSI Model
Inbound PDU Details
PDU Formats
TCP
0 16 31 Bits
SRC PORT: 110
DEST PORT: 1026
SEQUENCE NUM: 1
ACK NUM: 23
OFF.
RES.
PSH + ACK
WINDOW
CHECKSUM: 0x0
URGENT POINTER
OPTION
PADDING
DATA (VARIABLE)
POP3
POP3 DATA


PDU Information at Device: CS
OSI Model
Inbound PDU Details
At Device: CS
Source: CS
Destination: POP3 CLIENT
In Layers
Out Layers
Layer 7: POP3
Layer6
Layer5
Layer 4: TCP Src Port: 110, Dst Port: 1026
Layer 3: IP Header Src. IP: 10.0.0.2, Dest. IP: 10.0.0.4
Layer 2: Ethernet II Header 000C.854E.1185 >> 000D.BD7B.99A0
Layer 1: Port FastEthernet0
Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1
1. FastEthernet0 receives the frame.

VLAN & Inter-VLAN Routing

Objectives:

- To understand what is VLAN.
- To appreciate why VLANs are formed.
- To understand Inter-VLAN Routing.

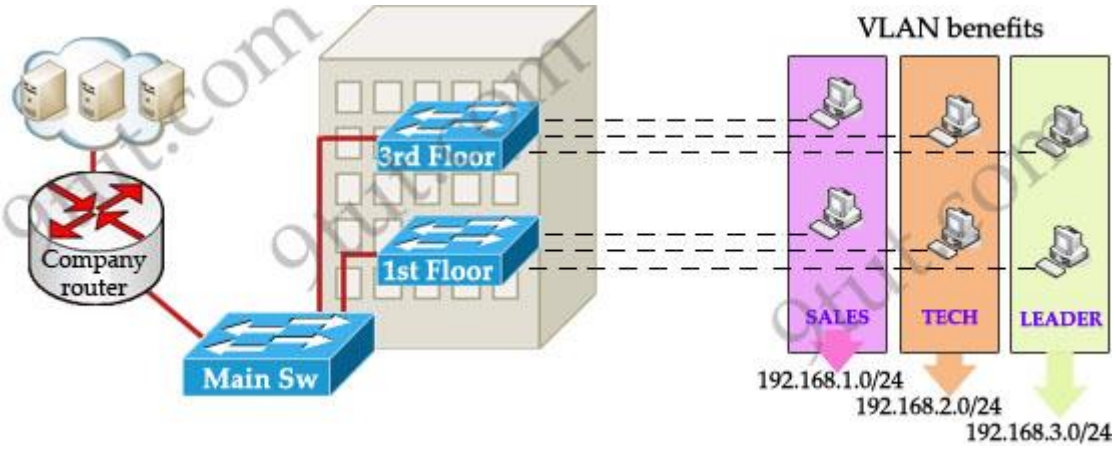
Introduction:

Virtual Local Area Networks-VLAN:

A traditional LAN comprising of workstations connected to each other by means of a hub or a repeater form a single collision and broadcast domains. Due to this, these devices propagate any incoming data throughout the network. To prevent collisions from traveling through all the workstations in the network, a bridge or a switch can be used. These devices will not forward collisions, but still will allow broadcasts and multicasts to pass through. A router, therefore, may be used to prevent broadcasts and multicasts from traveling through different networks. To stop broadcasts in a same LAN segment, VLAN's allow a network manager to logically segment a LAN into different broadcast domains so that packets are only switched between ports that are designated for the same VLAN.

A Virtual Local Area Network can be defined as a group of networking devices in the same broadcast domain, logically. Since this is a logical segmentation and not a physical one, it means that the devices in the same VLAN may be widely separated in the network; both by geography and location, workstations do not have to be physically located together.

VLAN helps you group users together according to their function rather than their physical location. This means Users on different floors of the same building, or even in different buildings can now belong to the same LAN. This makes the management much simpler.



As VLANs break up broadcast domains, so now if a computer in SALES broadcasts, only computers in SALES will receive that frame.

It is important to point out that you don't have to configure a VLAN until your network gets so large and has so much traffic that you need one. Many times, people are simply using VLAN's because the Network they are working on was already using them.

You need to consider using VLAN's in any of the following situations:

- **You have more than 200 devices on your LAN**
- **You have a lot of broadcast traffic on your LAN**
- **Groups of users need more security or are being slowed down by too many broadcasts?**
- **Groups of users need to be on the same broadcast domain because they are running the same applications. An example would be a company that has VoIP phones. The users using the phone could be on a different VLAN, not with the regular users.**
- **Or, just to make a single switch into multiple virtual switches.**

Another important fact is that, on a Cisco switch, VLAN's are enabled by default and ALL devices are already in a VLAN. The VLAN that all devices are already in is VLAN 1. So, by default, you can just use all the ports on a switch and all devices will be able to talk to one another.

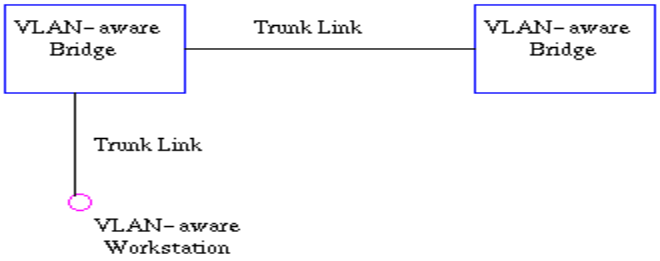
Types of Connections in VLAN:

Devices on a VLAN can be connected in three ways based on whether the connected devices are VLAN-aware or VLAN-unaware. Recall that a VLAN-aware device is one which understands VLAN memberships (i.e. which users belong to a VLAN) and VLAN formats.

- **Trunk Link:**

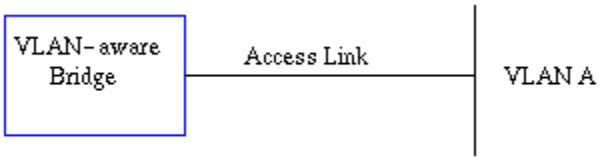
All the devices connected to a trunk link, including workstations, must be VLAN-aware. All frames on a trunk link must have a special header attached. These special frames are called tagged frames.

.



- **Access Link:**

An access link connects a VLAN-unaware device to the port of a VLAN-aware bridge. All frames on access links must be implicitly tagged (untagged). The VLAN-unaware device can be a LAN segment with VLAN-unaware workstations or it can be a number of LAN segments containing VLAN-unaware devices (legacy LAN).

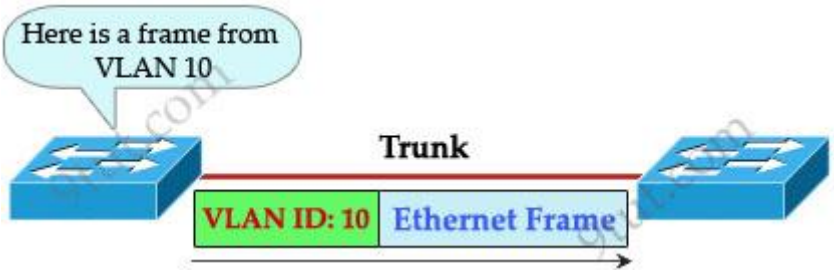


Communication in VLAN:

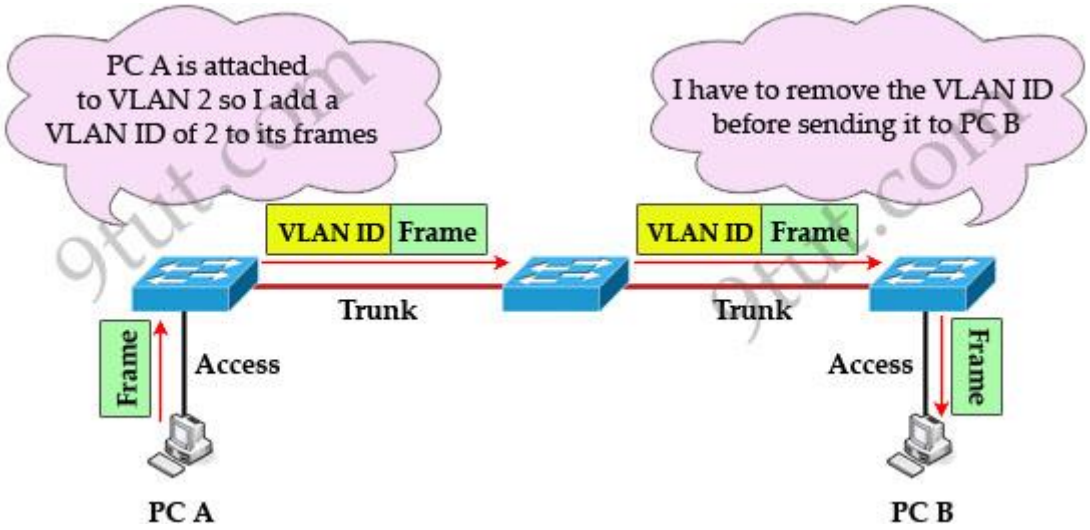
Hosts in the same VLAN can communicate normally even they are connecting to 2 or more different switches. When using multiple VLANs in networks that have multiple interconnected switches, we need to use VLAN Trunking between the switches. With VLAN trunking, the switches tag each frame sent between switches so that the receiving switch knows which VLAN the frame belongs to. This tag is known as a VLAN ID. A VLAN ID is a number which is used to identify a VLAN.

Inter-VLAN Routing:

To enable different VLANs to communicate with each otherwe need a router. Without a router, the computers within each VLAN can communicate with each other but not with any other computers in another VLAN. For example, we need a router to transfer file from LEADER to TECH. This is called "*inter-VLAN routing*".

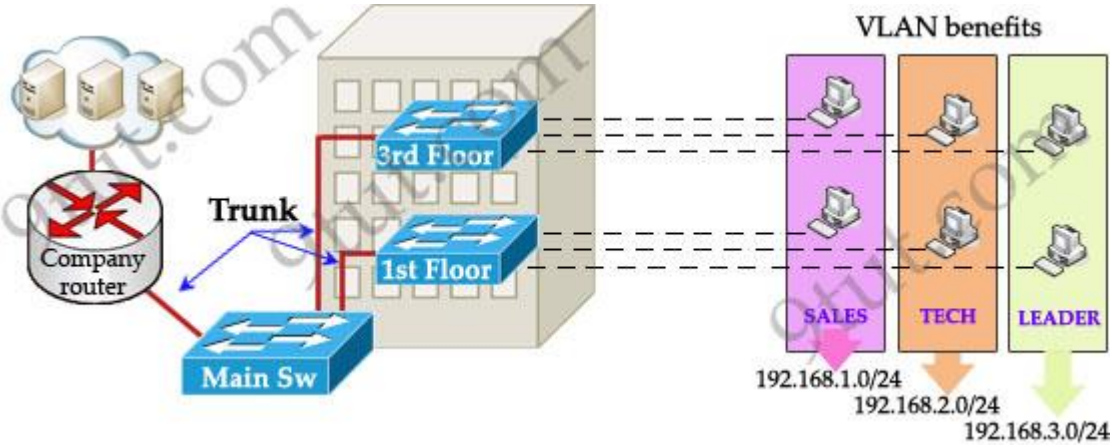


The tag is only added and removed by the switches when frames are sent out on the trunk links. Hosts don't know about this tag because it is added on the first switch and removed on the last switch. The picture below describes the process of a frame sent from PC A to PC B.



<u>Note:</u> Trunk link does not belong to a specific VLAN; rather it is a conduit for VLANs between switches and routers.

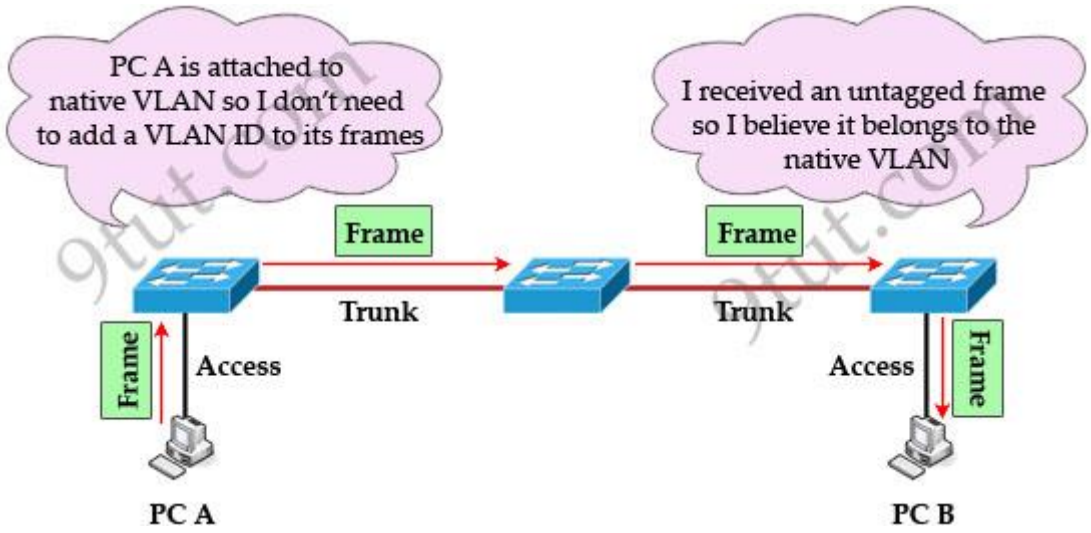
To allow inter-VLAN routing you need to configure trunking on the link between router and switch. Therefore in our example we need to configure 3 links as "trunk".



Cisco switches support two different trunking protocols, Inter-Switch Link (ISL) and IEEE 802.1q. Cisco created ISL before the IEEE standardized trunking protocol. Because ISL is Cisco proprietary, it can be used only between two Cisco switches. 802.1q is usually used in practical.

In 802.1q encapsulation, there is a concept called native VLAN that was created for backward compatibility with old devices that don't support VLANs. Native VLAN works as follows:

- **Frame belonging to the native VLAN is not tagged when sent out on the trunk links.**
- **Frame received untagged on the trunk link is set to the native VLAN.**



So if an old switch doesn't support VLAN it can still "understand" that frame and continue sending it (without dropping it).

Every port belongs to at least one VLAN. If a switch receives untagged frames on a trunk port, they are assumed to be part of the native VLAN. By default, VLAN 1 is the default and native VLAN but this can be changed on a per port basis by configuration.

VLAN Configuration:

Creating VLAN:

➔ **Step 1: Enter privileged EXEC mode:**

Switch>enable

➔ **Step 2: Enter global configuration mode.**

Switch#config terminal

➔ **Step 3: Create VLAN.**

Switch(config)#vlanX

➔ **Step 4: Give name to VLAN.**

Switch(config-vlan)#name XYZ

Notice that we don't need to exit out of "vlan mode" to create another VLAN.

Set VLAN Membership:

Assign VLAN to each port:

➔ **Step 5:Enter interface configuration mode.**

Switch(config)#interface *type port*

➔ **Step 6:Set the mode of port as trunk or access**

Switch(config-if)#switchportmode *access/trunk*

➔ **Step 7: If port is in access mode, assign a VLAN to the port.**

Switch(config-if)#switchport access vlan*number*

Notice that for port connecting to host we must configure it as access port.

<u>Allow Inter-VLAN Routing:</u>

➔ **Step 8: Enter interface configuration mode.**

Router(config)#interface *type port*

➔ **Step 9: Enter sub-interface configuration mode.**

Router(config-if)#interface *type port.subport*

➔ **Step 10. Set the ip address of the subinterface.**

Router(config-subif)#ip address X.X.X.X Y.Y.Y.Y

➔ **Step 11. Set the encapsulation type and vlan allowed on sub-interface.**

Switch(config-subif)# encapsulation dot1q*vlan number*

EXERCISE

Topology Diagram: