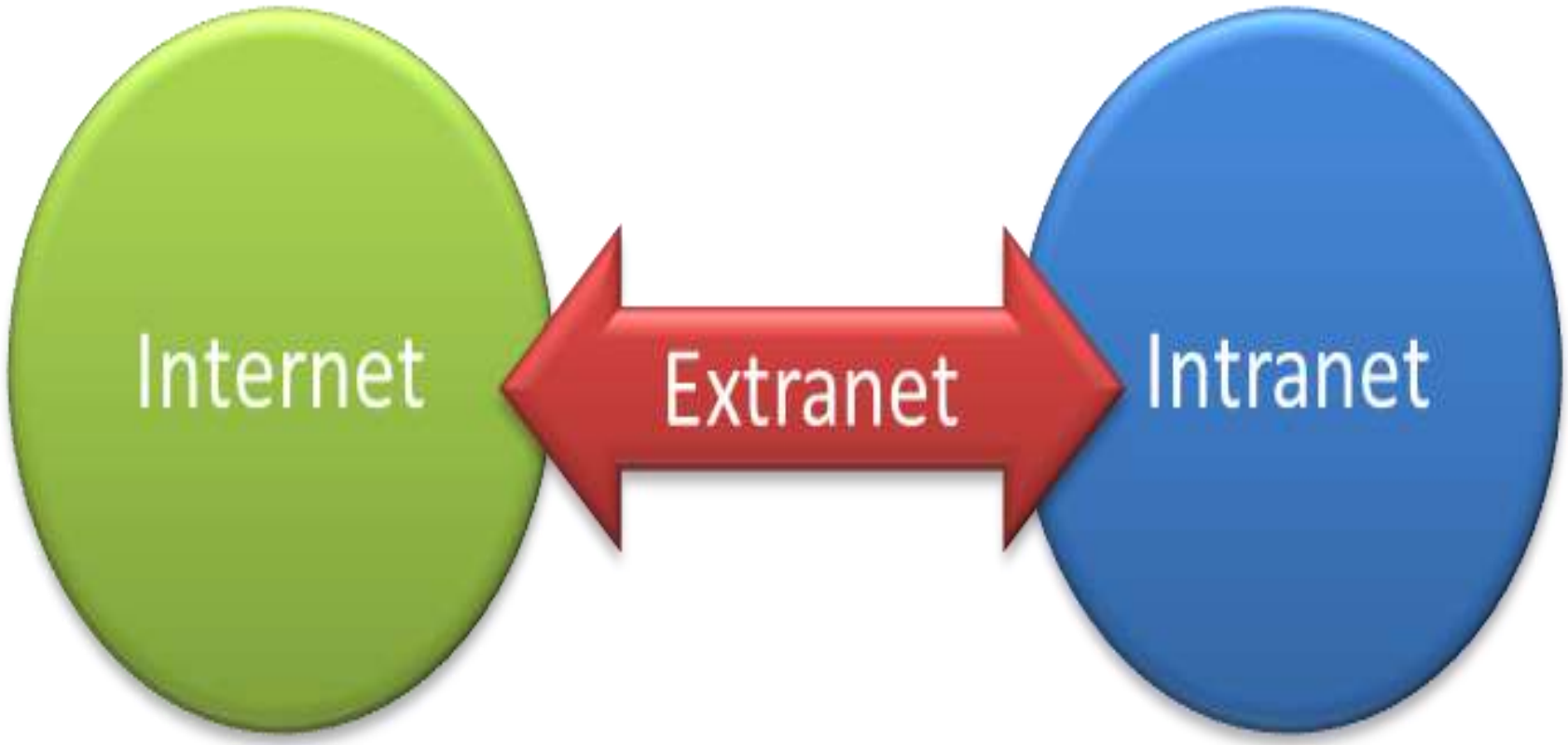

Internet
Extranet
Intranet

Presented by
Name: Subrata Paul
Roll: 13015411 **Session:** 2012-13
Year: 3rd **Semester:** 1st

Department of Computer Science
and Engineering, Rajshahi University

Definition

- The Internet generally allows everyone to access all network resources.
- An Intranet allows for restricted access to only members of an organization.
- An Extranet expands that access by allowing non-members such as suppliers and customers to use company resources.

The main difference between the three is accessibility.

Internet

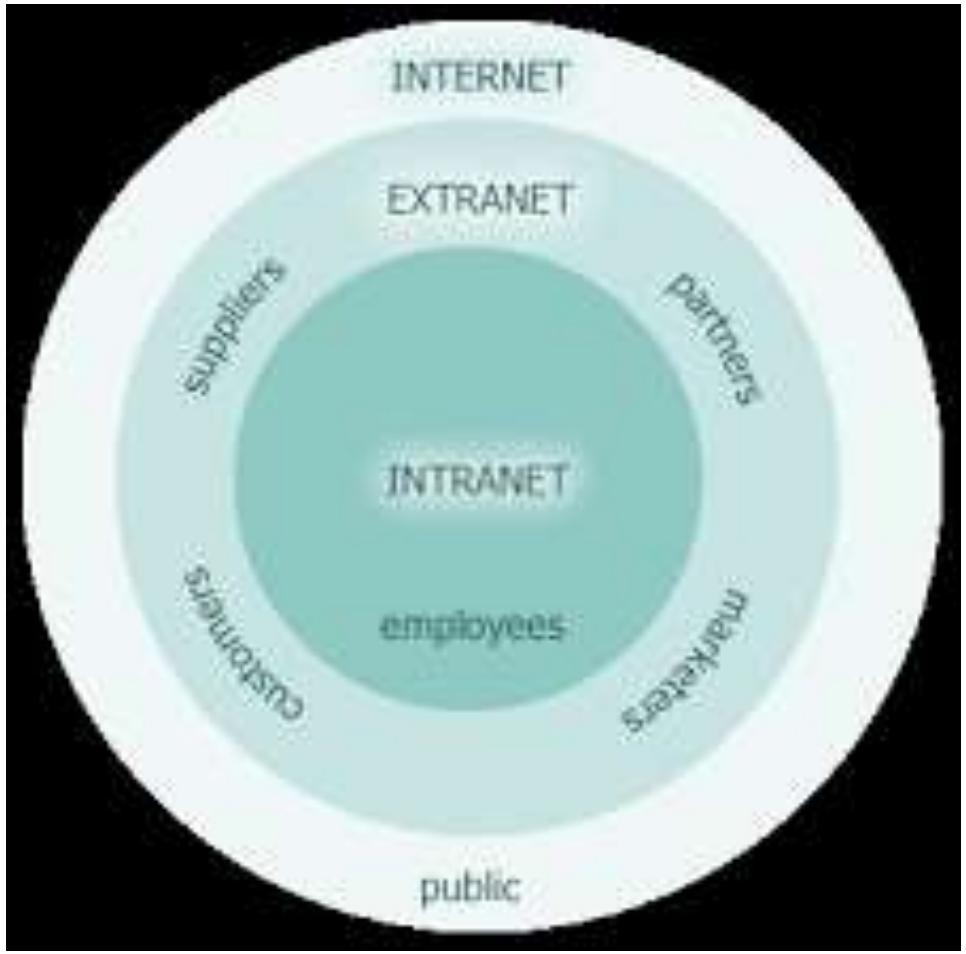
- This is a *network* that is accessible to a person who knows their **IP** address.
- **It** is global communication accessed through the Web and literary world wide.

Intranet

- This is a network that is not available to the world outside of the Intranet.
- **It** is shared content accessed by members within a single organization.

Extranet

- This is actually an Intranet that is partially accessible to authorized outsiders.
- **It** is shared content accessed by groups through cross-enterprise boundaries.



- ✓ Intranet is only available to a small group of people.
- ✓ Extranet allows limited access to non-members of an organization.
- ✓ Internet is known as world-wide web

Internet

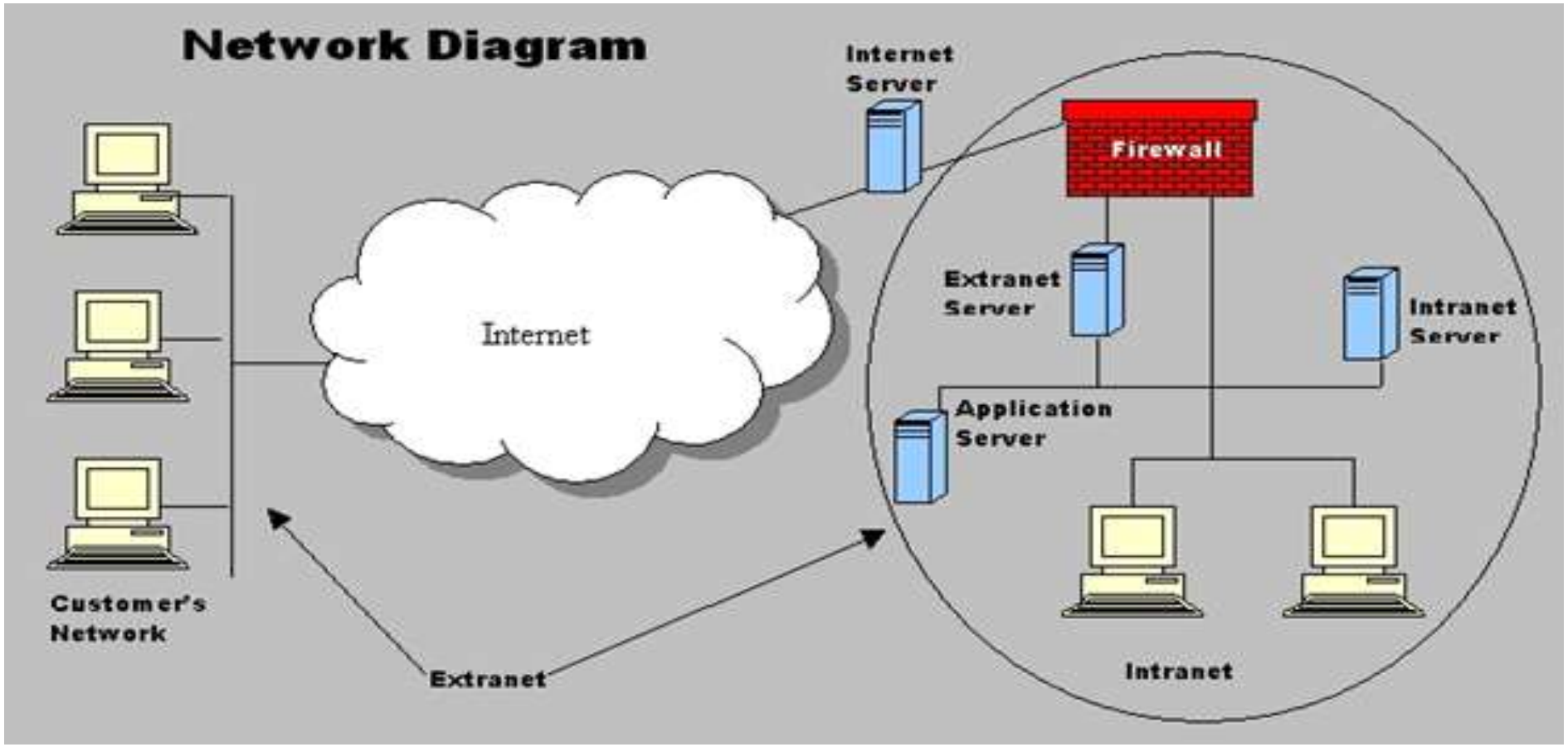
- Internet can be accessed with a computer using a domain name that needs to be translated into an IP address.

Intranet

- The firewall helps to control access between the Intranet and Internet to permit access to the Intranet only to the members

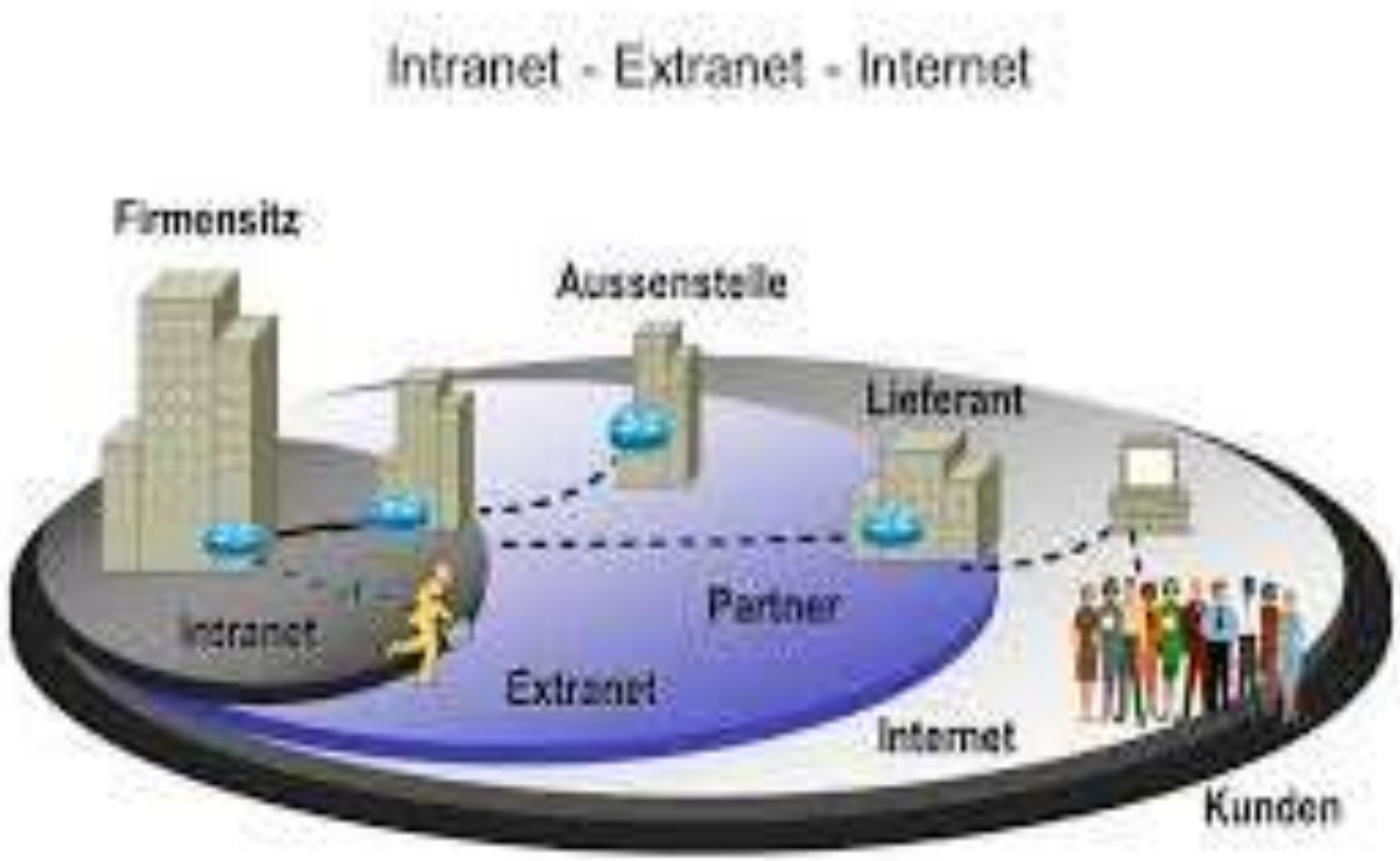
Extranet

- If the firewall allows access from the Internet, then it will be an Extranet.


Network Diagram
Internet Server
Firewall
Extranet Server
Intranet Server
Application Server
Internet
Customer's Network
Extranet
Intranet

Applications:

- Home users typically use the Internet for searching and sharing information. It is available to anyone with an Internet-connected device.
- Home users use an intranet to share files between computers Businesses and organizations use it to restrict access to confidential data.
- The purpose of Extranet is to allow collaboration and sharing of resources not only in-house but with a select group of outside users.



The **Internet**, **extranets**, and **intranets** all rely on the same **TCP/IP** technologies.

However, they are different in terms of the levels of access they allow to various users inside and outside the organization and the size of the network.

Why we use the terms intranet and extranets why not as Internet?

Cause this terms has benefits in today's business environment, to communicate more effectively, both internally with employees and externally with trading partners and customers.

- An intranet enables employees to share information, collaborate, and improve their communications.
- Extranet enables in business to communicate and collaborate more effectively with selected business partners, suppliers and customers.

VPN and VLAN

Definition

- A virtual private network (VPN) is a network that is constructed by using public wires (usually the Internet) to connect to a private network such as a company's internal network.

- A virtual local area network (VLAN) is a logical group of workstations, servers and network devices that appear to be on the same LAN despite their geographical distribution.

VLAN configuration:

The VLANs must be configured independently on each vlan supporting switch or router using any of the following methods

1. Manually via the command line interface (CLI) or web interface.
2. With a VLAN management tool provided by the vendor.
3. Automatically with a standard protocol like GVRP (GARP VLAN Registration Protocol), which works in conjunction with 802.1Q.
4. Automatically with a proprietary protocol like Cisco's VTP (Virtual Trunking Protocol), which works in conjunction with Cisco's proprietary ISL (Inter-Switch Link) trunking protocol.

VPN components:

There are four components to a VPN network.

1. The Internet
   - Fundamental plumbing for the network
2. Security Gateways
   - Sit between public and private networks preventing unauthorized intrusion
   - May provide tunneling and encrypt private data.
3. Security Policy Servers
   - Maintains Access control lists that the security gateway uses to determine which traffic is authorized.
4. Certificate Authorities
   - Used to confirm the authenticity of shared keys among sites.

Types:

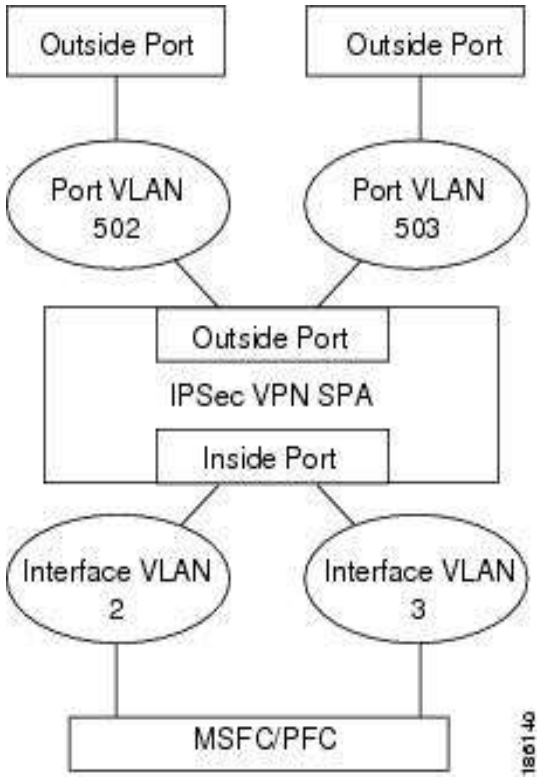
VLAN types

1. Port Based
   -Configured at each switch port
2. MAC Address Based
   - Uses the end stations MAC address for VLAN Assignment
3. Protocol Based
   - Uses LAN protocol to determine VLAN assignment
4. Dynamic Based
   - A User Profile determine VLAN assignment

VPN types

1. A special purpose device consisting of a network interface, operating system and hardware based cryptographic support
2. A software solution that works with the OSI layers to provide encryption
3. A hybrid in which the VPN application runs on standard computing platforms that may use an outboard cryptographic processor

A VLAN is created to cover and to relocate computers geographically, need not be belonging to same LAN.



A **VPN** is designed to allow connection from outside a network, to the inside of the network, by using VPN services

VLAN

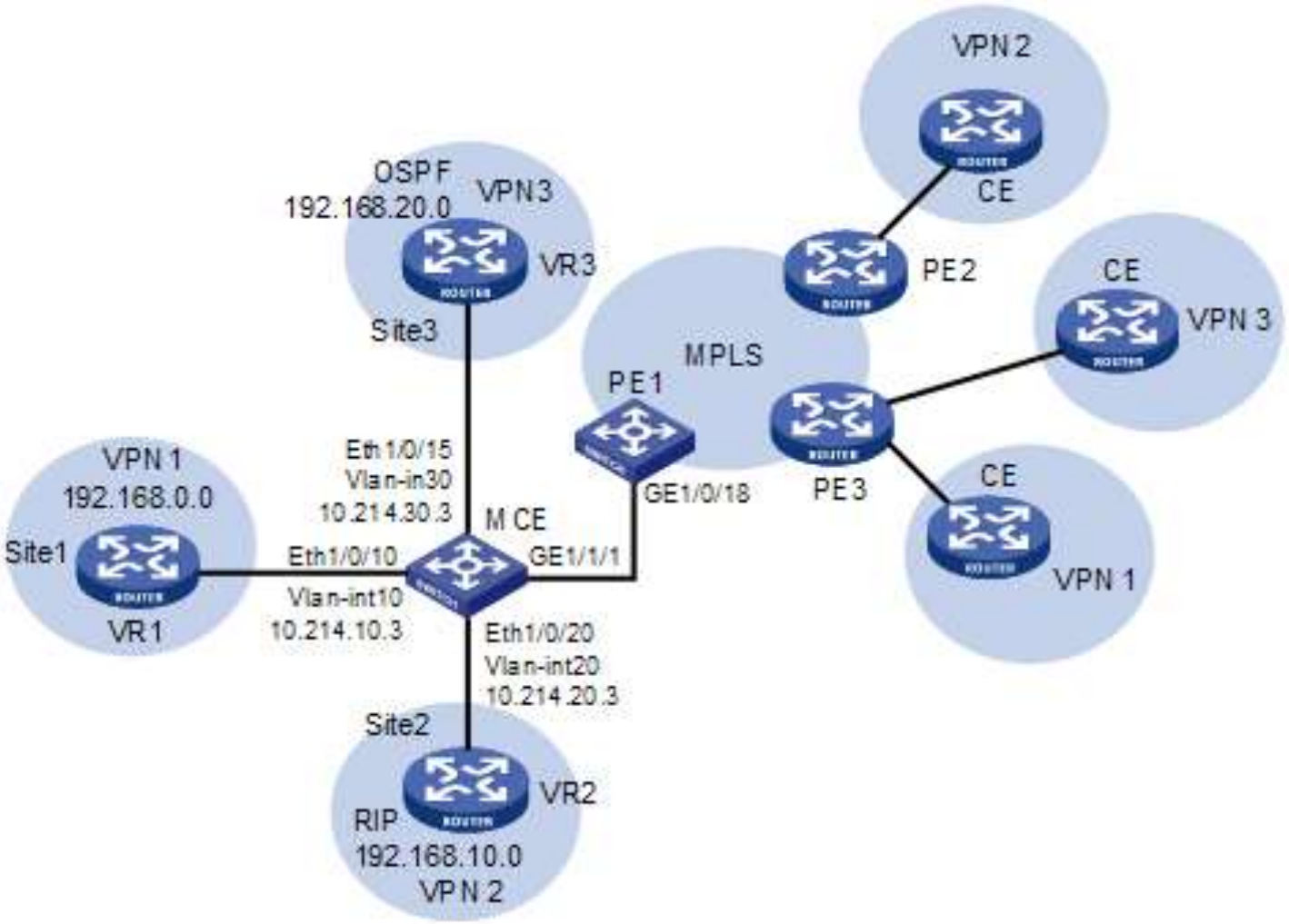
- The **VLAN** slices up a large network into smaller, more manageable pieces.
- It is purely a layer 2 construct.

VPN

- To access a LAN through a different LAN all together we need **VPN** access software (in fact authentication and client) to 'remotely' access the computers on the other networks.
- It constructs range from Layer 1 to Layer 3

Applications:

- VPNs are used to create a secure "channel" to transfer information through insecure channels. It is needs to provide the following 4 critical functions
  - Authentication
  - Access Control
  - Confidentiality
  - Data Integrity
- A VLAN is used to group computers that are not usually within same geography into the same broadcast domain
  - Used to alleviate traffic congestion without adding more bandwidth
  - Used to separate out users into logical groups of workers, regardless of actual physical location.



VPN is a method of creating a smaller sub- network on top of an existing bigger network while VLAN is a subcategory of VPN.

while VPN is most commonly related to remote access to a company’s network