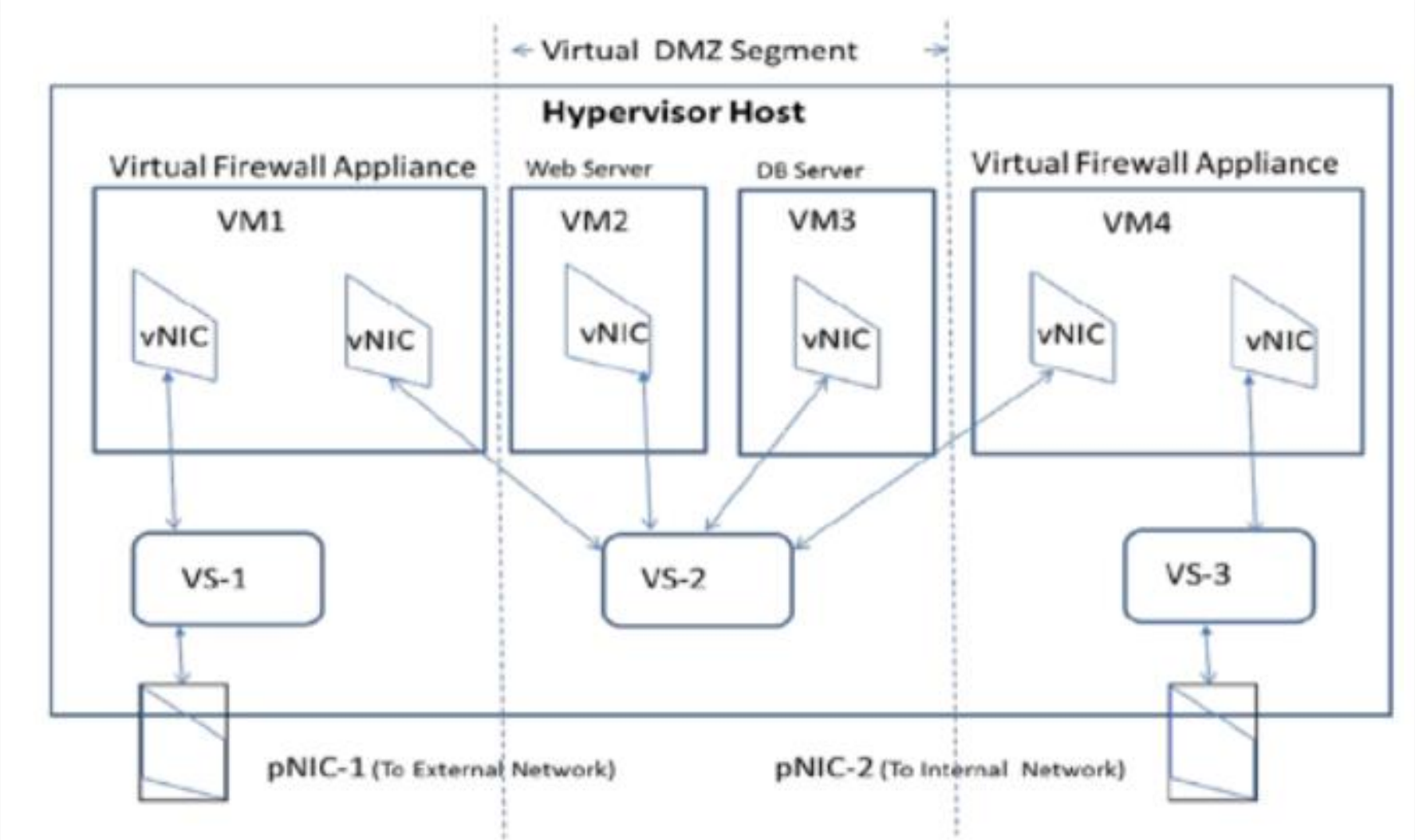
Module – III:

Secure Virtual Networking

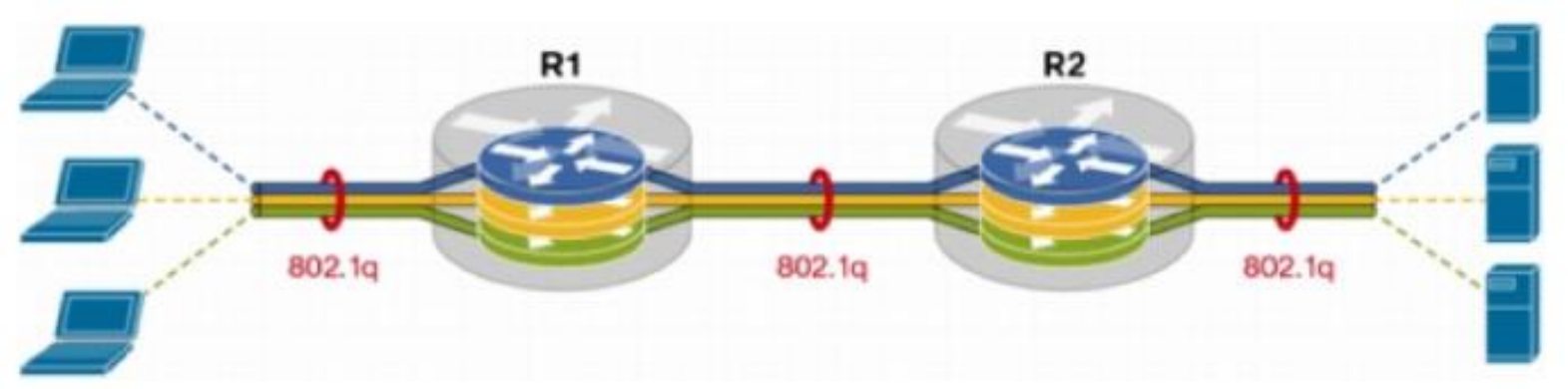
Security Architecture for VM Network



Courtesy of NIST

Terms to understand:

- DMZ
- Virtual Identity and Access Control
- virtual tunnel endpoints (VTEP)
- Network Integrity
- VLAN
- VPN
- Protocol Based Approaches
- Machine Virtualized Based Approaches
- Programmable Networks (SDN)



Access Control List:

Basically ACL is the integrated feature of IOS software that is used to filter the network traffic passing through the IOS devices. Network traffic flows in the form of packets. A packet contains small piece of data and all necessary information which are required to deliver it. By default when a router receives a packet in interface, it takes following actions:-

- Grab destination address from the packet
- Find an entry for destination address in routing table
- If match found, forwards the packet from associate interface
- If no match found, discard the packet immediately.

Types of ACLs

- Standard ACLs (1 – 99 and 1300 - 1999)
- Extended ACLs (100 – 199 and 2000 - 2699)

A packet interacts with three locations during its journey from router:-

- Packet arrives in interface (Entrance)
- Router makes forward decision
- Packet outs from interface (Exit)

Table 1 Virtualization techniques

Technique	Description	Examples
Full virtualization	The Virtual Machine Monitor emulates a complete machine, based on the underlying hardware architecture. The guest Operating System runs without any modification.	VMware Workstation, VirtualBox
Paravirtualization	The Virtual Machine monitor emulates a machine which is similar to the underlying hardware, with the addition of a hypervisor. The hypervisor allows the guest Operating System to run complex tasks directly on non-virtualized hardware. The guest OS must be modified in order to take advantage of this feature.	VMware ESX, Xen
Container-based virtualization	Instead of running a full Virtual Machine, this technique provides Operating System-level containers, based on separate userspaces. In each container, the hardware, as well as the Operating System and its kernel, are identical to the underlying ones.	OpenVZ, Linux VServer

Categories of Threats:

Threats into four categories, namely ***disclosure, deception, disruption, and usurpation***.

Unauthorized ***disclosure*** is defined as gaining unauthorized access to protected information. Sensitive data may be erroneously exposed to unauthorized entities, or acquired by an attacker that circumvents the system's security provisions.

Deception is characterized by intentionally attempting to mislead other entities. For example, a malicious entity may send false or incorrect information to others, leading them to believe that this information is correct. Fake identities may be used in order to incriminate others or gain illegitimate access.

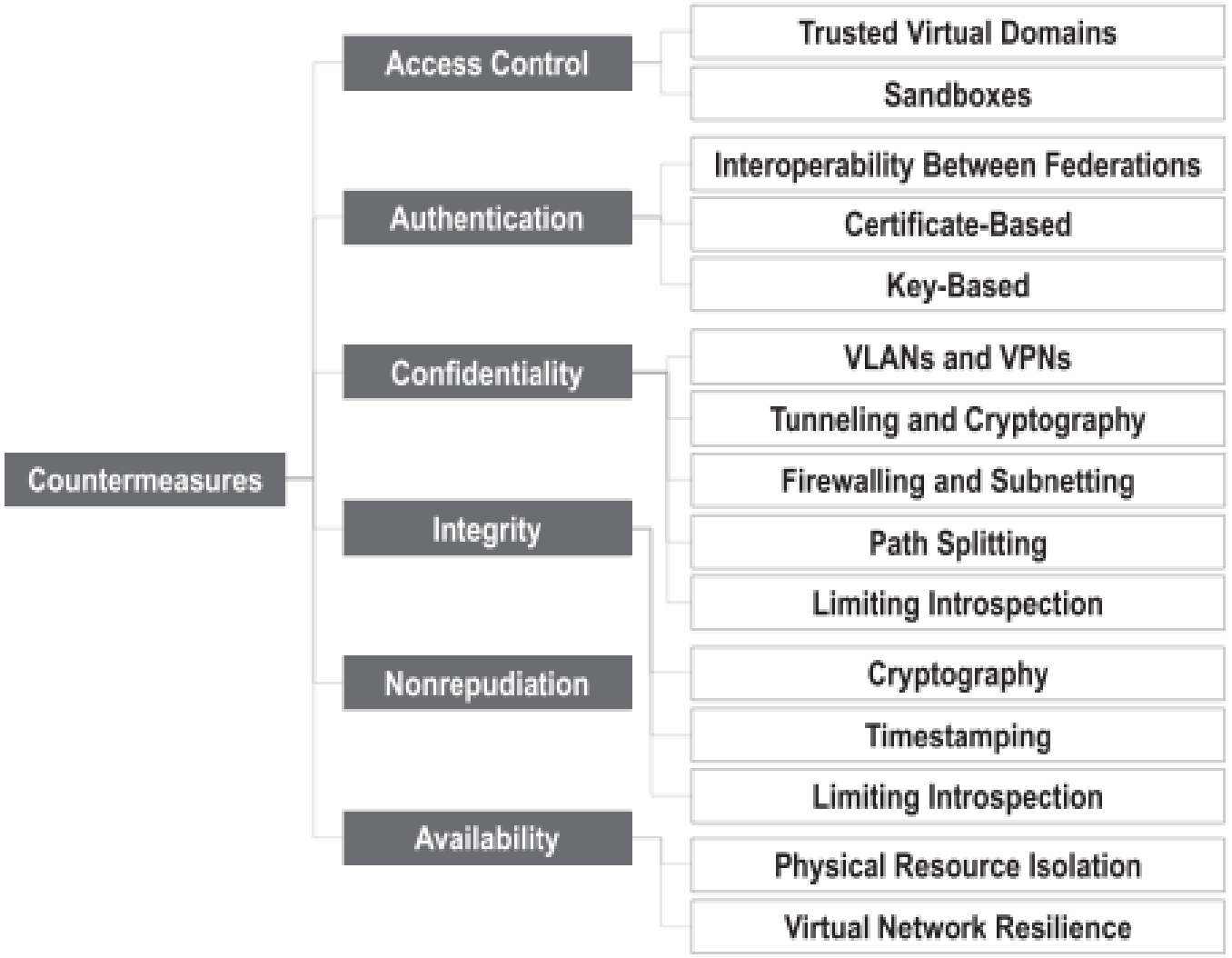
Disruption means causing failure or degradation of systems, negatively affecting the services they provide. This may be done by directly incapacitating a system component or the channel through which information is delivered, or by inducing the system to deliver corrupted information.

Last, through ***usurpation***, an attacker may gain unauthorized control over a system. This unauthorized control may allow the attacker to illegitimately access protected data or services, or tamper with the system itself in order to cause incorrect or malicious behavior.

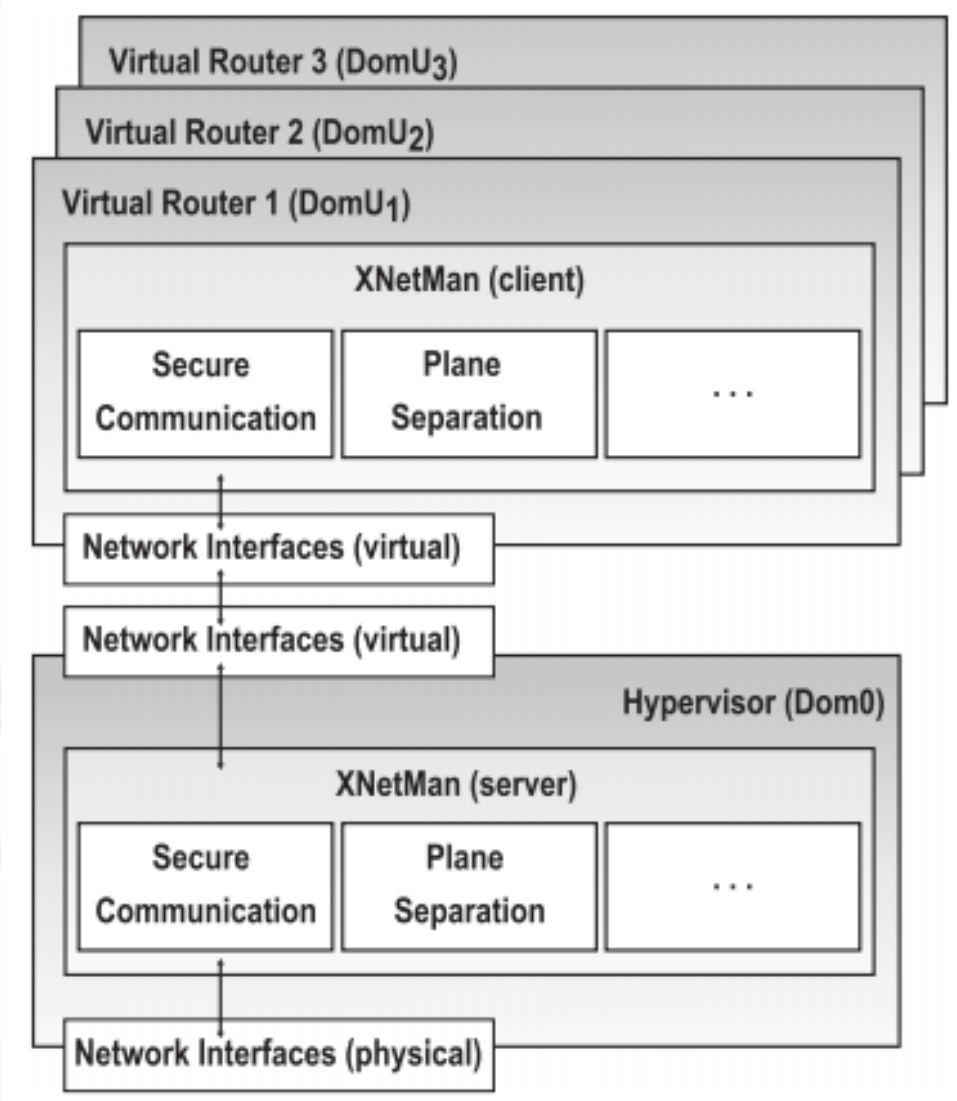
Table 2 Relationships between vulnerabilities and threats in network virtualization environments

Threat categories		Vulnerabilities	Threats
Disclosure	Information Leakage	Lack of ARP table protection	ARP table poisoning
		Placement of firewall rules inside virtual nodes	Subversion of firewall rules
	Information Interception	Lack of ARP table protection	ARP table poisoning
		Transmission of data in predictable patterns	Traffic Analysis attacks
		Uncontrolled handling of multiple, sequential virtual network requests from a single entity	Inference and disclosure of sensitive topological information
		Unprotected exchange of routing information among virtual routers	Disclosure of sensitive routing information
	Introspection Exploitation	Uncontrolled Introspection	Data theft
Deception	Identity Fraud	Improper handling of identities: - within individual networks;	Injection of malicious messages with forged sources
		- among federated networks;	Privilege escalation
		- during migration procedures.	Abuse of node removal and re-addition in order to obtain new (clean) identities
	Loss of registry entries	Uncontrolled rollback operations	Loss of registry entries
	Replay attacks	Lack of unique message identifiers	Replay attacks
Disruption	Physical Resource Overloading	Uncontrolled resource allocation	Performance degradation
			Abusive resource consumption
		Uncontrolled handling of virtual network requests	Exhaustion of resources in specific parts of the infrastructure
		Lack of proactive or reactive recovery strategies	Denial of Service attacks
	Physical Resource Failure	Lack of proactive or reactive recovery strategies	Failure of virtual routers/networks
		Uncontrolled resource reallocation after failures	Overloading of remaining virtual routers after failures
Usurpation	Identity Fraud	Improper handling of identities and associated privileges	Privilege escalation
	Software Vulnerability Exploitation	Privilege escalation in Virtual Machine Monitors	Unauthorized control of physical routers

Countermeasure Activities:



Simplified Architecture:



Network Segmentation

Methods

1. Subnet
2. VLAN

Classification of segmentation

1. Perimeter Segmentation
2. Data Center Segmentation
3. Micro Segmentation

Benefits of Segmentation

1. Allow us to organize and secure networks
2. Increased restrictions to comply with least privilege and Zero – Trust
3. Securing operating systems and applications that we do not control
4. Creating network bulkheads to limit propagation
5. Micro segmentation provides visibility into areas of the network we previously could not see

Subnetting:

Subnetting is the process of breaking down a single network into one or more smaller networks called “sub-networks” or “subnets” for short. The process of subnetting was initially created to solve the shortage of IP addresses over the internet but has since evolved into an IP management best practice for IP network utilization.

Subnet mask:

A subnet mask is a 32-digit number determining the possible range of IP addresses available in a network. One subnet mask limits how many IP addresses can exist on a single network, but multiple subnet masks can be used to organize an entire network into sub-subnets.

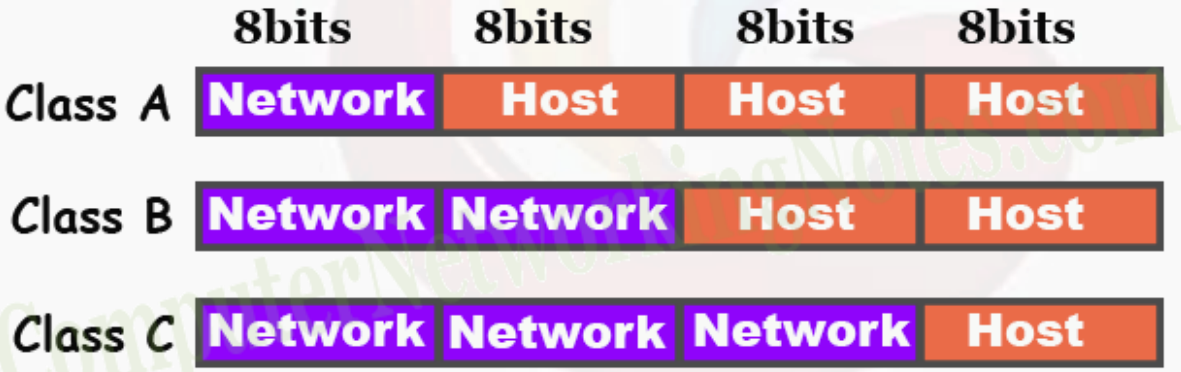
Calculate a subnet:

Without a subnet calculator, you can subnet any IP address manually using the binary method. To make a Class A, B or C default subnet mask larger, convert the subnet mask to a binary number and borrow bits from the host ID portion of the IP address to create a subnetwork ID. After your calculations, you'll be left with a list of possible subnets to use in your network.

If you don't need the exact IP addresses of possible subnets but instead need to know how many subnets are contained within a given IP address, you only need a simple equation. Two to the power of x equals the number of subnets, in which x is the number of subnet bits. If the IP address has 3 subnet bits, means you can have 2 to the 3rd power of subnets or 8 total subnets.

In class A, B and C: -

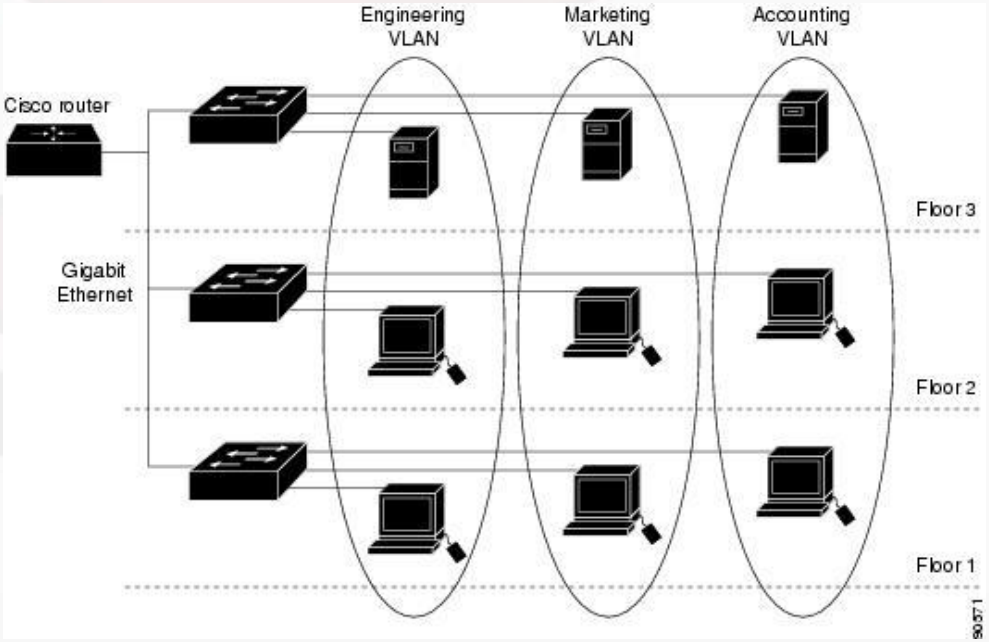
1. First 8, 16 and 24 bits are reserved for network portion respectively.
2. Last 2 bits (31 & 32) are reserved for host portion.



IP Class	First IP Address of class	Last IP Address of class	Default Subnet Mask	Default Network bits	Host bits	Reserved host bits
A	0.0.0.0	127.255.255.255	255.0.0.0	First 8 bits	9 to 30	31, 32
B	128.0.0.0	191.255.255.255	255.255.0.0	First 16 bits	17 to 30	31, 32
C	192.0.0.0	223.255.255.255	255.255.255.0	First 24 bits	25 to 30	31, 32

Virtual LAN (VLAN):

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch module port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN.



Configuring switches and routers for VLAN:

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# name test20
Switch(config-vlan)# end

Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config

Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# end

Switch# configure terminal
Switch(config)# interface fastethernet0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 33
Switch(config-if)# end
```