جامعة الأهرام الكندية
AHRAM CANADIAN UNIVERSITY

Lecture (05)
TCP/IP related issues

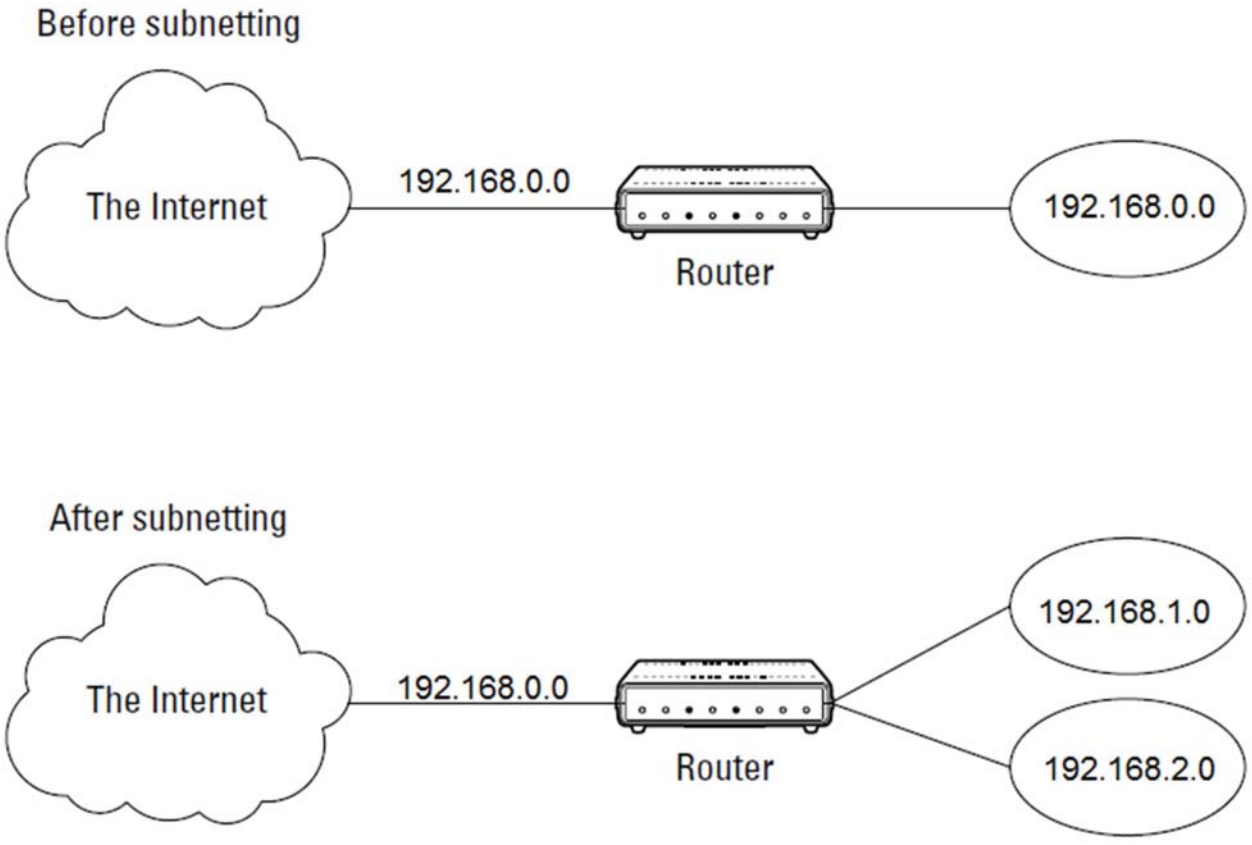
Dr. Ahmed M. ElShafee

Agenda

- Subnetting
- Subnet masks
- Private and public addresses
- Network Address Translation
- Virtual Private Network (VPN)
- VLANs
- Dynamic Host Configuration Protocol (DHCP)
- Proxy servers
- Gateway
- Firewalls

Subnetting

- A *subnet* is a network that falls within a Class A, B, or C network.
- Subnets are created by using one or more of the Class A, B, or C host bits to extend the network ID.
- Thus, instead of the standard 8-, 16-, or 24-bit network ID, subnets can have network IDs of any length.
- Following Figure shows an example of a network before and after subnetting has been applied.
- In the unsubnetted network, the network has been assigned the Class B address 192.168.0.0.
- All the devices on this network must share the same broadcast domain.

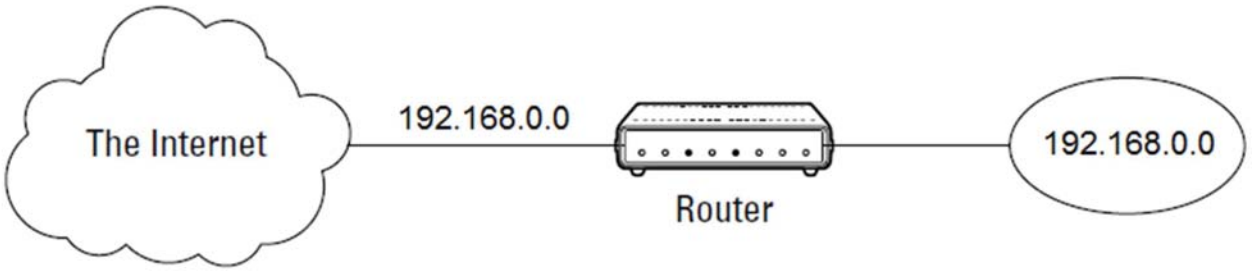


- In the second network, the first four bits of the host ID are used to divide the network into two small networks, identified as subnets 16 and 32.
- To the outside world (that is, on the other side of the router), these two networks still appear to be a single network identified as 192.168.0.0.
- For example, the outside world considers the device at 192.168.1.2 to belong to the 192.168.0.0 network.
- As a result, a packet sent to this device will be delivered to the router at 192.168.0.0.
- The router then considers the subnet portion of the host ID to decide whether to route the packet to subnet 1 or subnet 2.

Subnet masks

- For subnetting to work, the router must be told which portion of the host ID should be used for the subnet network ID.
- That is accomplished by using another 32-bit number, known as a *subnet mask.*
- Those IP address bits that represent the network ID are represented by a 1 in the mask, and those bits that represent the host ID appear as a 0 in the mask.

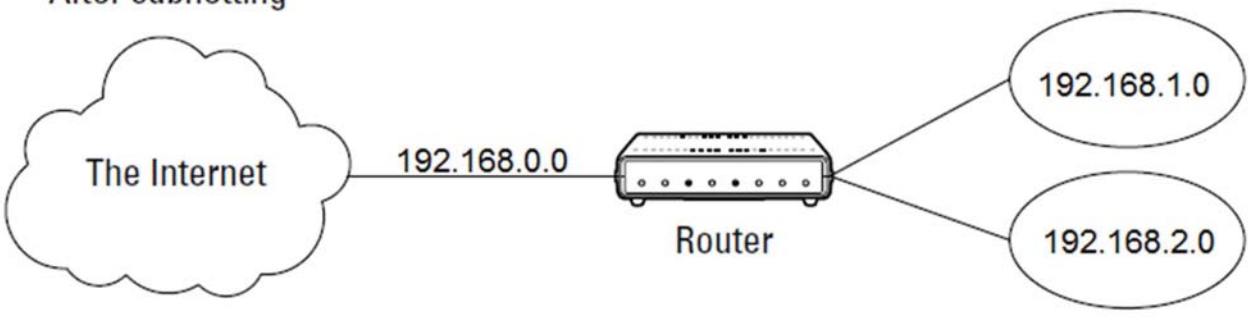
Before subnetting



- Subnet mask here

11111111	11111111	00000000	00000000
255	255	0	0

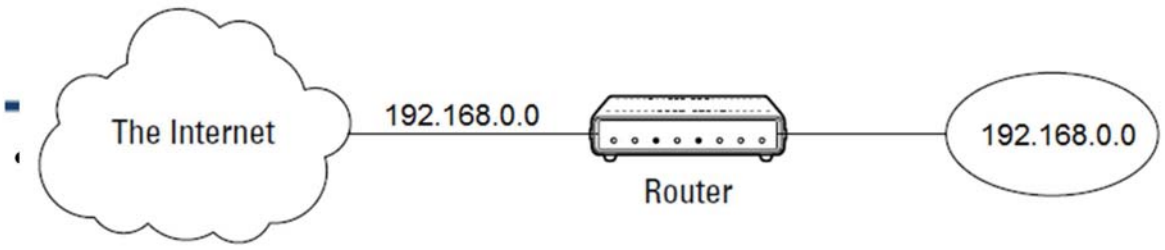
After subnetting



Router	11111111	11111111	11111100	00000000
	255	255	252	0

PCs	11111111	11111111	11111100	00000000
	255	255	252	0

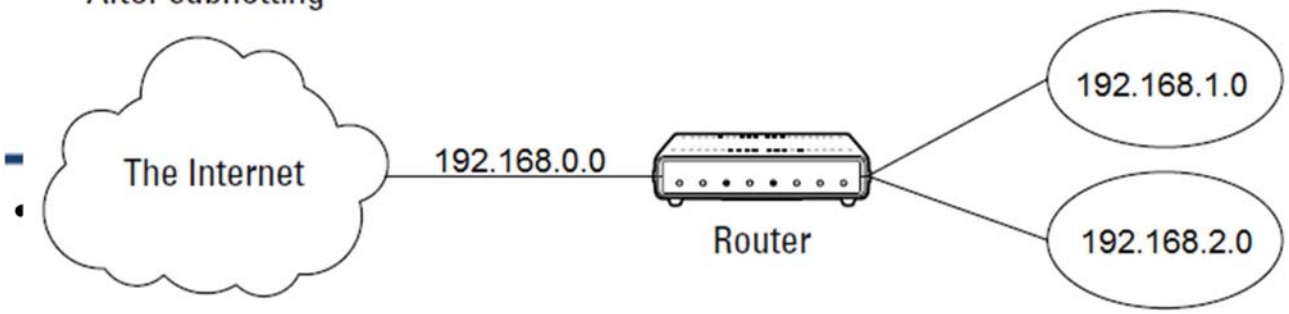
Before subnetting



Router	IP	192	168	0	1
		11000000	10101000	00000000	00000001
	Subnet Mask	11111111	11111111	00000000	00000000
		255	255	0	0
	Network IP	192	168	0	0

PC1	IP	192	168	0	2
		11000000	10101000	00000000	00000010
	Subnet Mask	11111111	11111111	00000000	00000000
		255	255	0	0
	Network IP	192	168	0	0

After subnetting

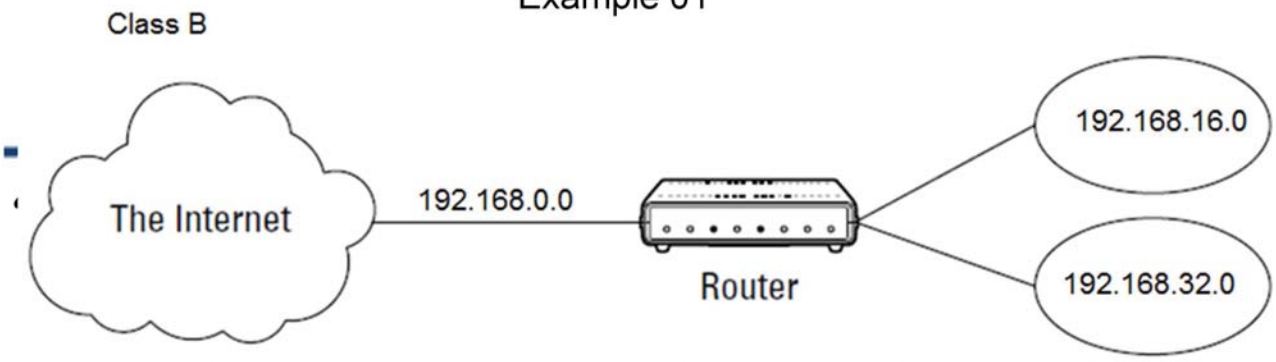


Router	IP	192	168	0	1
		11000000	10101000	00000000	00000001
	Subnet Mask	11111111	11111111	11111100	00000000
		255	255	252	0
	Network IP	192	168	0	0

PC1	IP	192	168	1	1
		11000000	10101000	00000001	00000001
	Subnet Mask	11111111	11111111	11111100	00000000
		255	255	252	0
	Network IP	192	168	0	0

•PC2	IP	192	168	2	1
		11000000	10101000	00000010	00000001
	Subnet Mask	11111111	11111111	11111100	00000000
		255	255	252	0
	Network IP	192	168	0	0

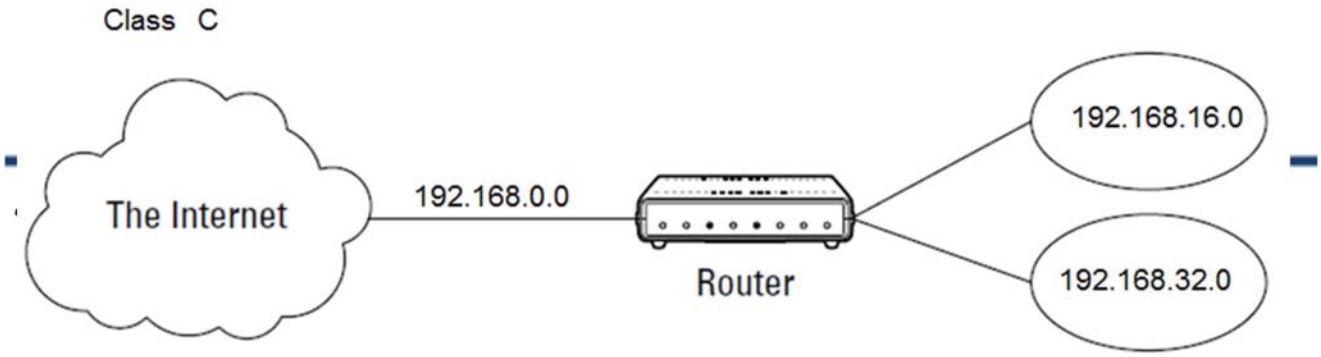
Example 01



Router	IP	192	168	0	1
		11000000	10101000	00000000	00000001
	Subnet Mask	11111111	11111111	00000000	00000000
		255	255	0	0
	Network IP	192	168	0	0

PC1 in sub network 1	IP	192	168	16	1
		11000000	10101000	00010000	00000001
	Subnet Mask	11111111	11111111	00000000	00000000
		255	255	0	0
	Network IP	192	168	0	0

•PC2 PC1 in sub network 2	IP	**192**	**168**	**32**	**1**
		11000000	10101000	00100000	00000001
	Subnet Mask	11111111	11111111	00000000	00000000
		255	255	0	0
	Network IP	192	168	0	0

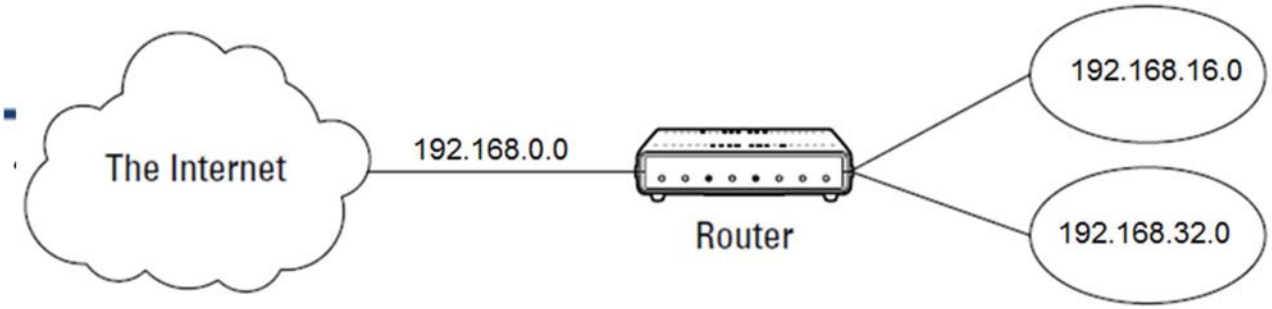


Router	**IP**	**192**	**168**	**0**	**1**
		11000000	10101000	00000000	00000001
	Subnet Mask	11111111	11111111	11111111	00000000
		255	255	255	0
	Network IP	192	168	0	0

PC1	**IP**	**192**	**168**	**16**	**1**
		11000000	10101000	00010000	00000001
	Subnet Mask	11111111	11111111	11111111	00000000
		255	255	255	0
	Network IP	192	168	16	0

•PC2	IP	192	168	32	1
		11000000	10101000	00100000	00000001
	Subnet Mask	11111111	11111111	11111111	00000000
		255	255	255	0
	Network IP	192	168	32	0

Subnetting

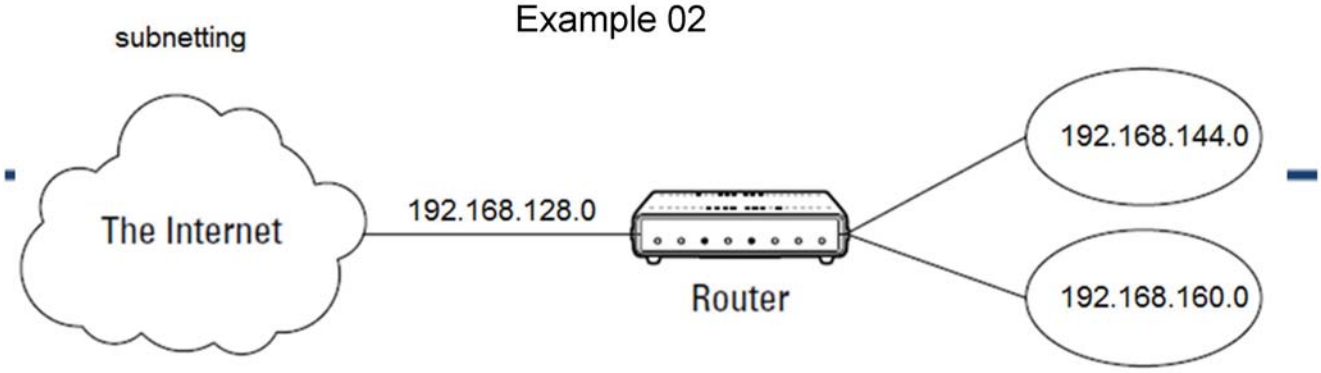


Router	IP	192	168	0	1
		11000000	10101000	00000000	00000001
	Subnet Mask	11111111	11111111	11000000	00000000
		255	255	192	0
	Network IP	192	168	0	0

PC1	IP	192	168	16	1
		11000000	10101000	00010000	00000001
	Subnet Mask	11111111	11111111	11000000	00000000
		255	255	192	0
	Network IP	192	168	0	0

•PC2	IP	192	168	32	1
		11000000	10101000	00100000	00000001
	Subnet Mask	11111111	11111111	11000000	00000000
		255	255	192	0
	Network IP	192	168	0	0

Example 02



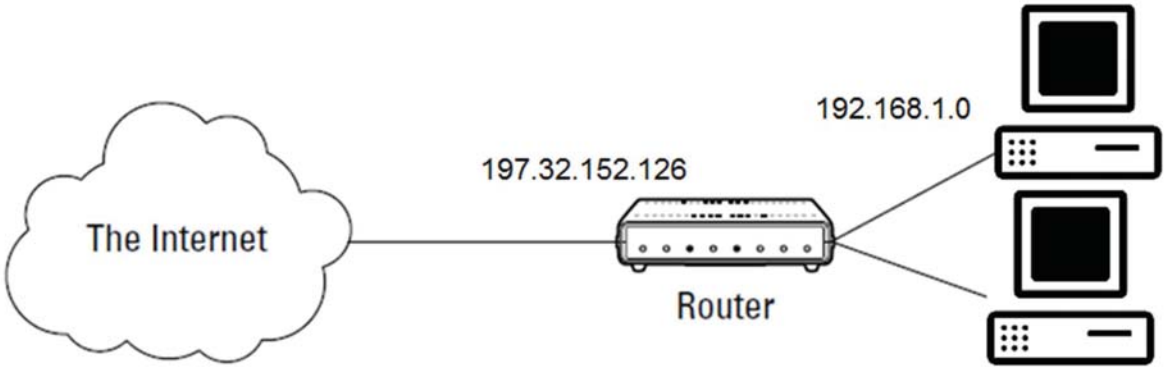
Router	IP	192	168	128	1
		11000000	10101000	10000000	00000001
	Subnet Mask	11111111	11111111	11000000	00000000
		255	255	192	0
	Network IP	192	168	128	0

PC1 on sub network 1	IP	192	168	144	1
		11000000	10101000	10010000	00000001
	Subnet Mask	11111111	11111111	11000000	00000000
		255	255	192	0
	Network IP	192	168	128	0

PC2 on sub network 2	IP	192	168	160	1
		11000000	10101000	10100000	00000001
	Subnet Mask	11111111	11111111	11000000	00000000
		255	255	192	0
	Network IP	192	168	128	0

Private and public addresses

- Any host with a direct connection to the Internet must have a globally unique IP address.
- Not all hosts are connected directly to the Internet.
- Some are on networks that aren't connected to the Internet.
- Some hosts are hidden behind firewalls, so their Internet connection is indirect.



- Several blocks of IP addresses are set aside just for this purpose, for use on private networks that are not connected to the Internet or to use on networks that are hidden behind a firewall.
- Three such ranges of addresses exist, summarized in Table

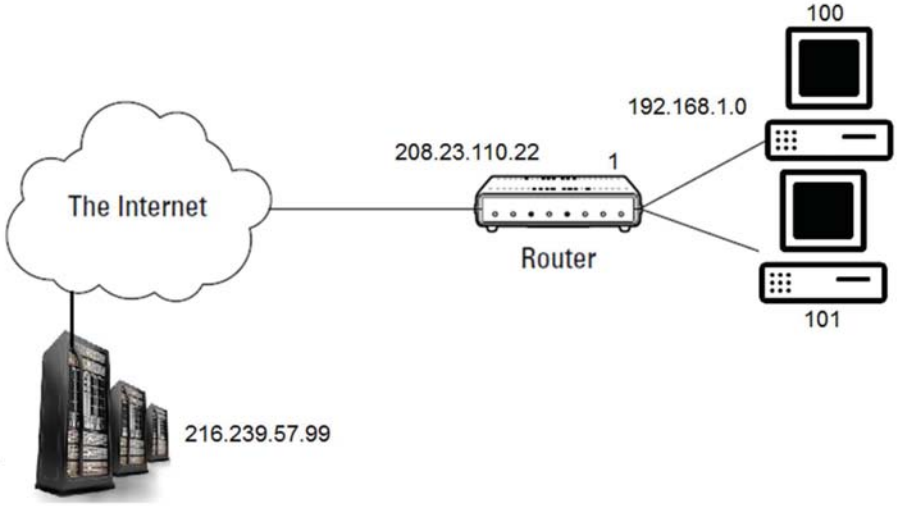
Private Address Spaces

Address Range
10.0.0.1–10.255.255.254
172.16.1.1–172.31.255.254
192.168.0.1–192.168.255.254

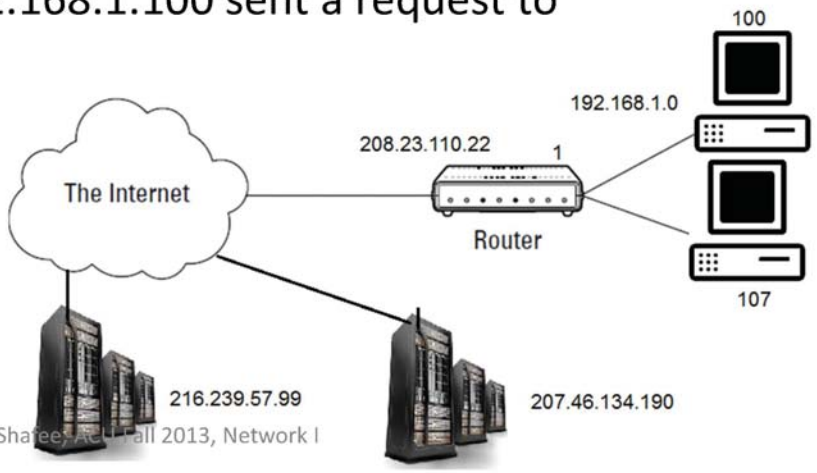
Network Address Translation

- firewalls use a technique called *network address translation* (NAT) to hide the actual IP address of a host from the outside world.
- the NAT device must use a globally unique IP to represent the host to the Internet.
- Behind the firewall, though, the host can use any IP address it wants.
- When packets cross the firewall, the NAT device translates the private IP address to the public IP address and vice versa.

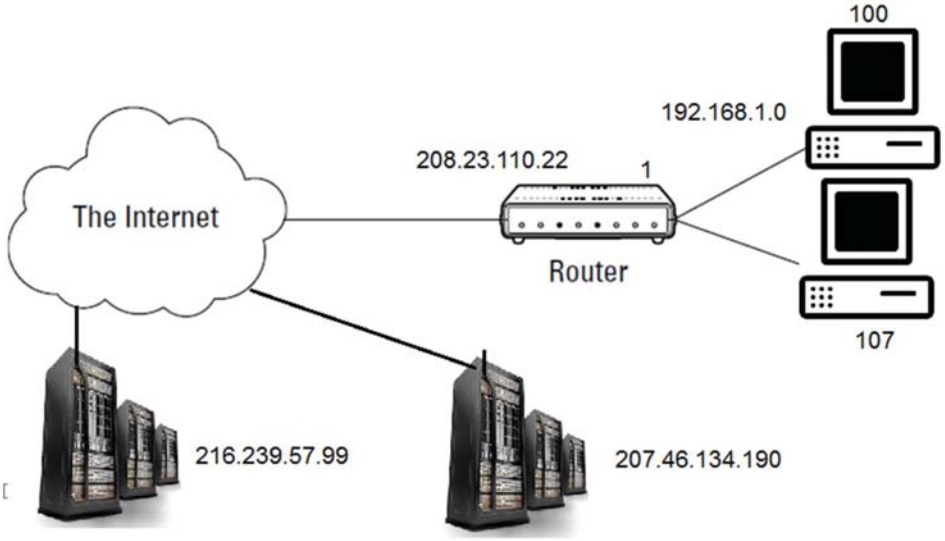
- NAT device can use a single public IP address for more than one host.
- It keeps track of outgoing packets so that it can match incoming packets with the correct host.
- To understand how this works, consider the following sequence of steps:



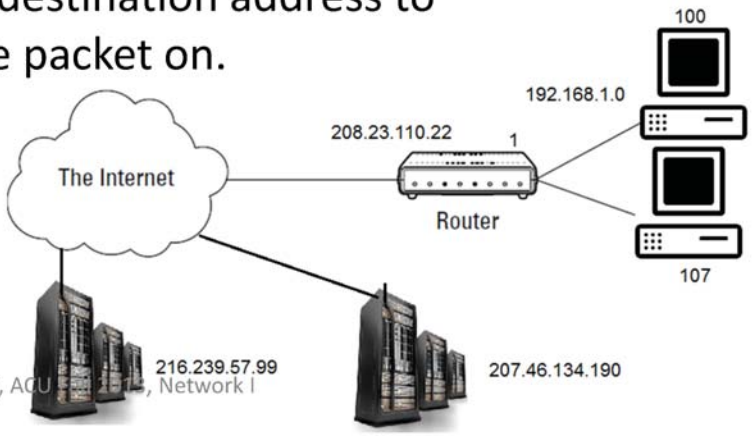
- A host whose private address is 192.168.1.100 sends a request to216.239.57.99, which is www.google.com.
- The NAT device changes the source IP address of the packet to 208.23.110.22, the IP address of the firewall.
- That way, Google will send its reply back to the firewall router. The NAT records that 192.168.1.100 sent a request to 216.239.57.99.



- Now another host, at address 192.168.1.107, sends a request to 207.46.134.190, which happens to be www.microsoft.com. The NAT device changes the source of this request to 208.23.110.22 so that Microsoft will reply to the firewall router. The NAT records that 192.168.1.107 sent a request to 207.46.134.190.



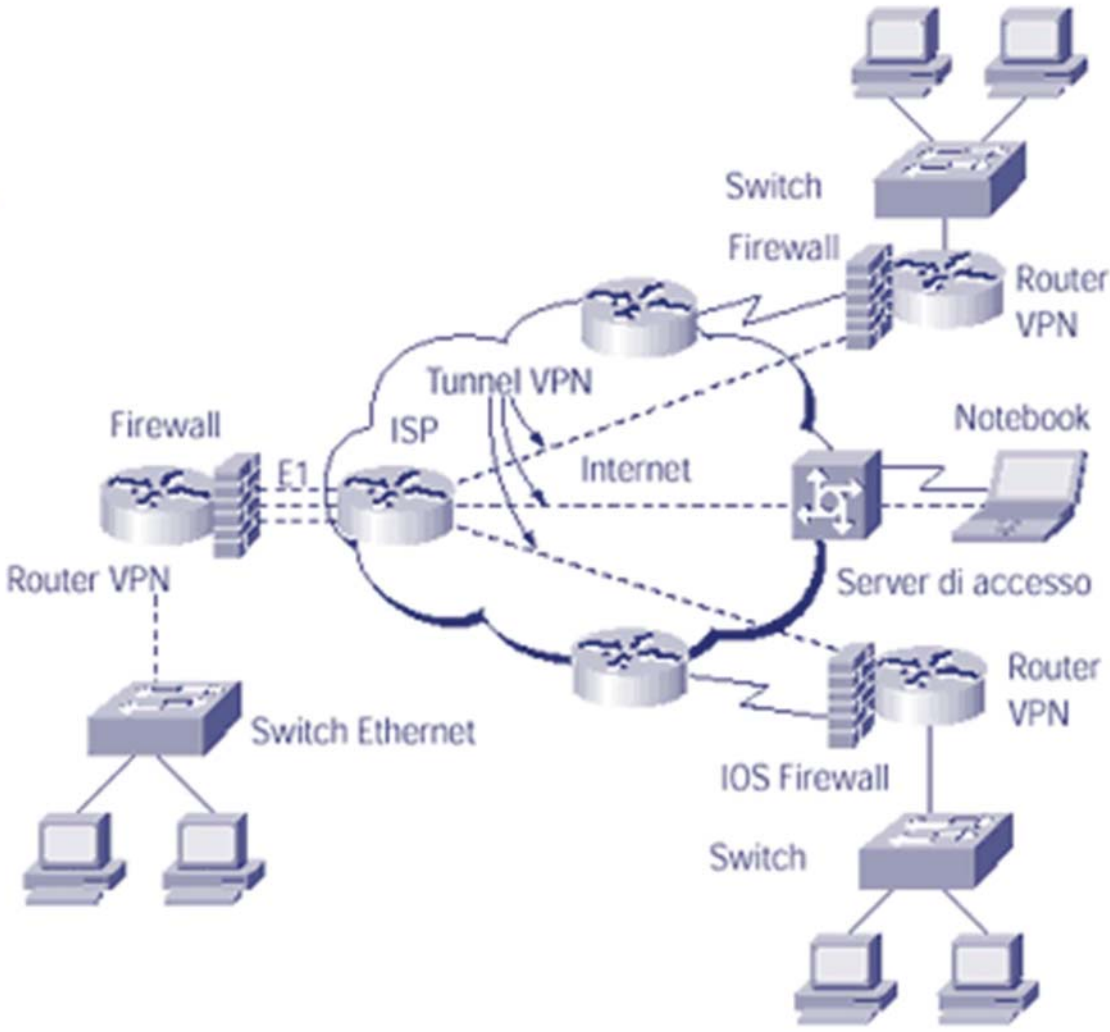
- A few seconds later, the firewall receives a reply from 216.239.57.99. The destination address in the reply is 208.23.110.22, the address of the firewall.
- To determine to whom to forward the reply, the firewall checks its records to see who is waiting for a reply from 216.239.57.99. It discovers that 192.168.1.100 is waiting for that reply, so it changes the destination address to 192.168.1.100 and sends the packet on.



Virtual Private Network (VPN)

- VPN is a private connection between two systems or networks over a shared or public network (typically Internet).
- VPN technology lets an organization securely extend its network services over the Internet to remote users, branch offices, and partner companies.
- In other words, VPN turns the Internet into a simulated private WAN.
- VPN is very appealing since the Internet has a global presence, and its use is now standard practice for most users and organizations.

•



To use the Internet as a private Wide Area Network, organizations may have to address two issues :

- First, networks often communicate using a variety of protocols, such as IPX and NetBEUI, but the Internet can only handle TCP/IP traffic. So VPN may need to provide a way to pass non-TCP/IP protocols from one network to another.
- Second data packets traveling the Internet are transported in clear text. Therefore, anyone who can see Internet traffic can also read the data contained in the packets. This is a problem if companies want to use the Internet to pass important, confidential business information.

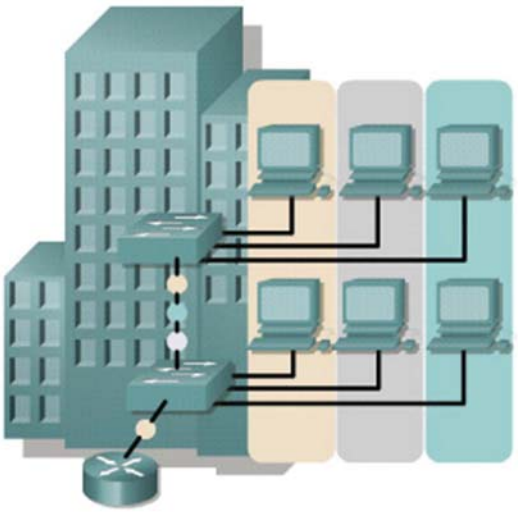
- VPN overcome these obstacles by using a strategy called Tunneling.
- Instead of packets crossing the Internet out in the open, data packets are first encrypted for security, and then encapsulated in an IP packet by the VPN and tunneled through the Internet.
- The VPN tunnel initiator on the source network communicates with a VPN tunnel terminator on the destination network.
- The two agree upon an encryption scheme, and the tunnel initiator encrypts the packet for security.

Advantages

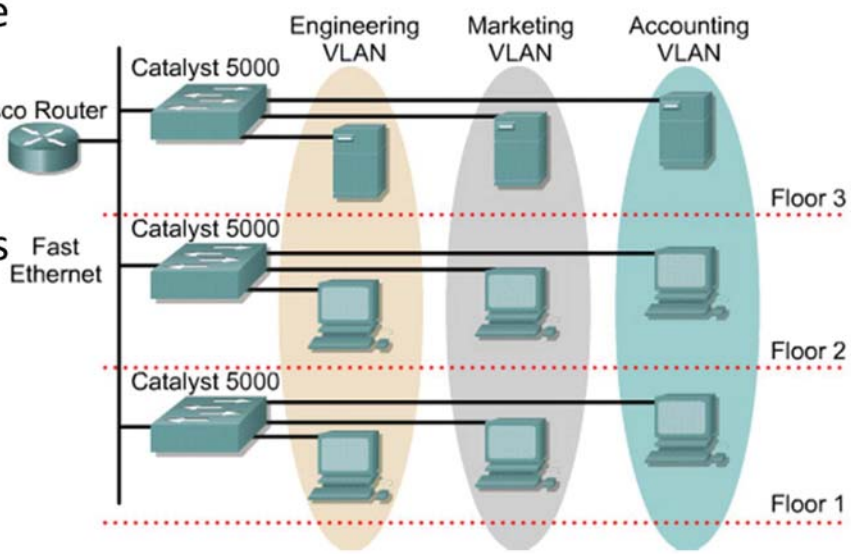
- cost savings, one can avoid having to purchase expensive leased lines to branch offices or partner companies.
- Another benefit of VPN is that it is an ideal way to handle mobile and remote users.

VLANs

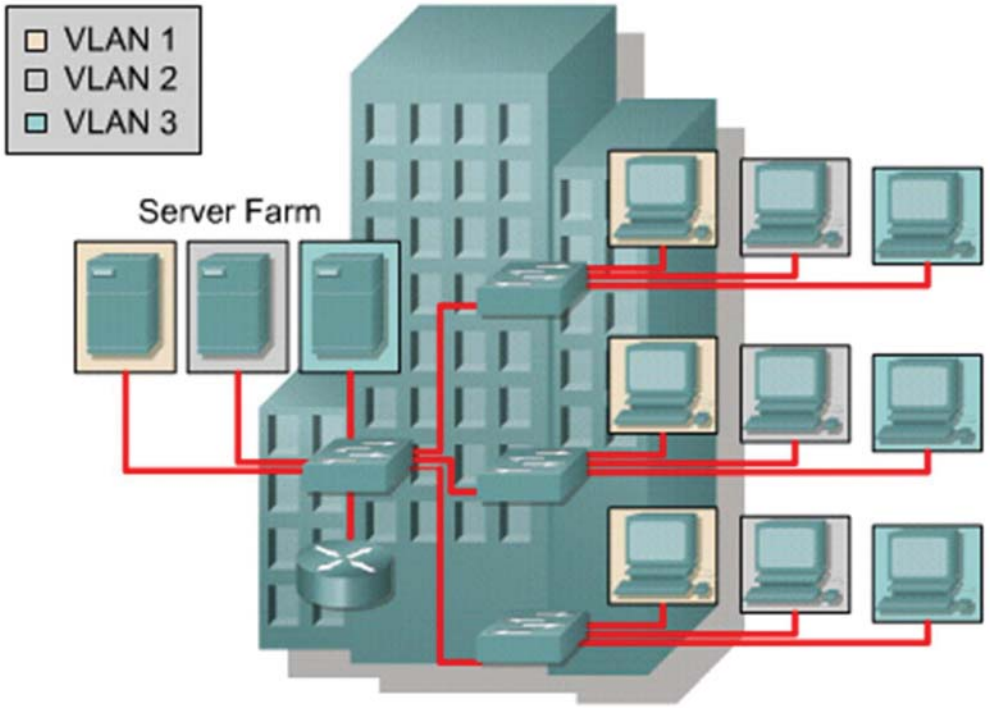
- VLANs logically segment switched networks based on the functions, project teams, or applications of the organization regardless of the physical location or connections to the network.
- All workstations and servers used by a particular workgroup share the same VLAN, regardless of the physical connection or location.
- A workstation in a VLAN group is restricted to communicating with file servers in the same VLAN group.



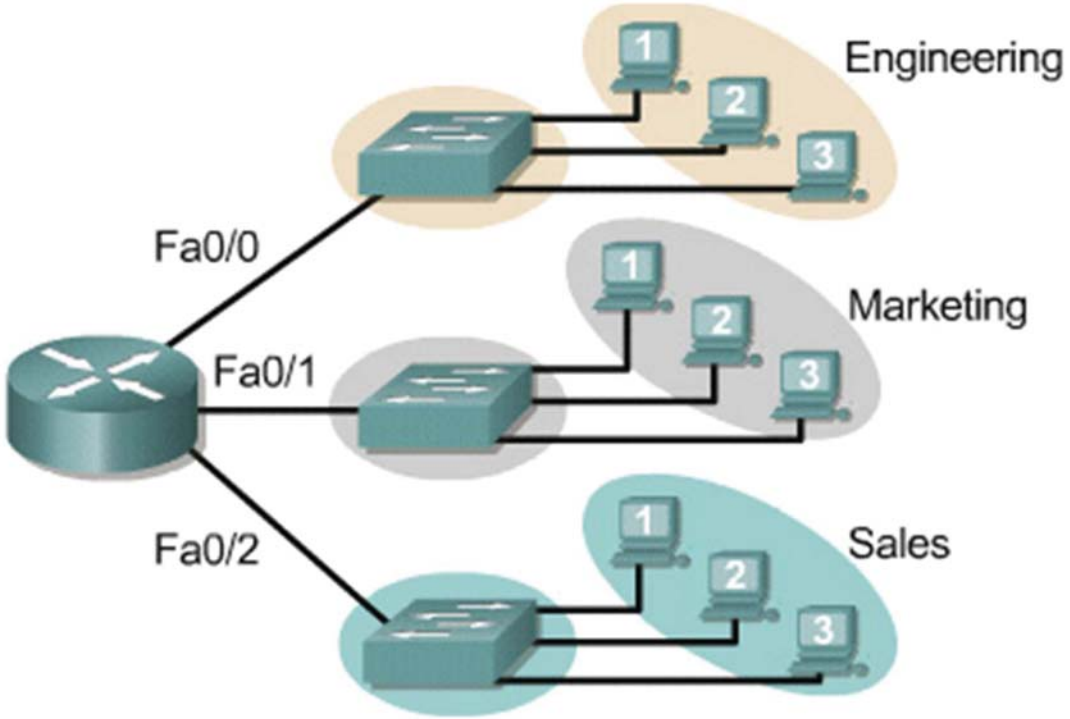
- VLANs function by logically segmenting the network into different broadcast domains so that packets are only switched between ports that are designated for the same VLAN.
- Routers in VLAN topologies provide broadcast filtering, security, and traffic flow management



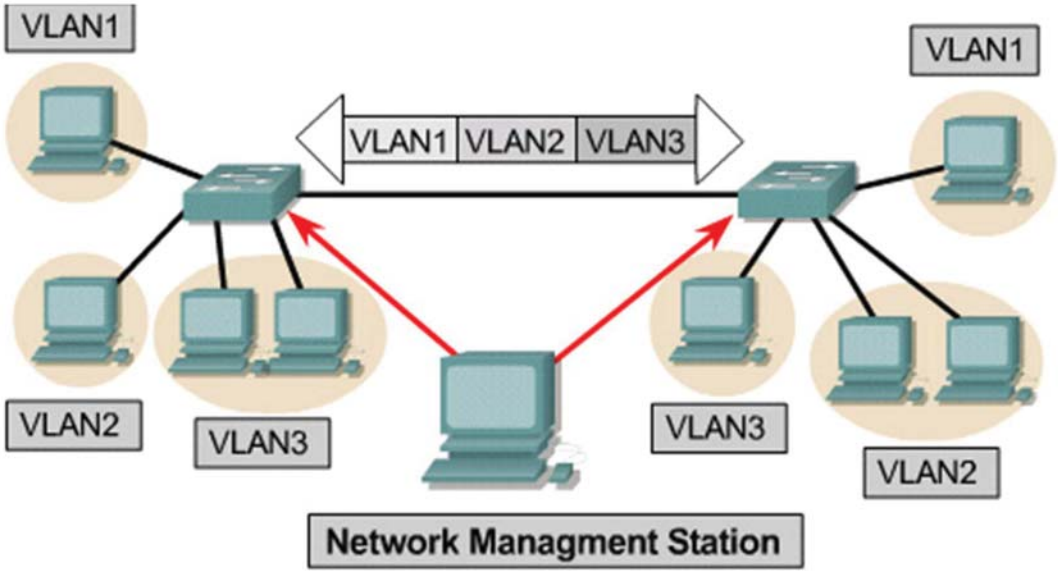
- A VLAN is a broadcast domain created by one or more switches.



- Layer 3 routing allows the router to send packets to the three different broadcast domains.



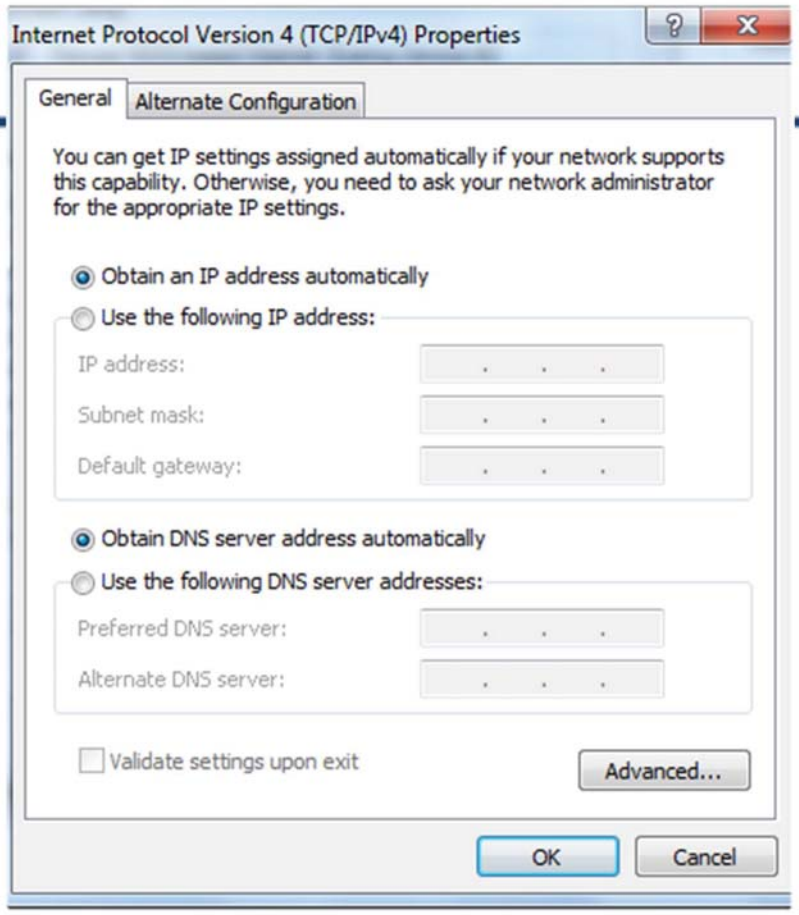
- Each switch port could be assigned to a different VLAN.
- Ports assigned to the same VLAN share broadcasts.
- Ports that do not belong to that VLAN do not share these broadcasts.



Dynamic Host Configuration Protocol (DHCP)

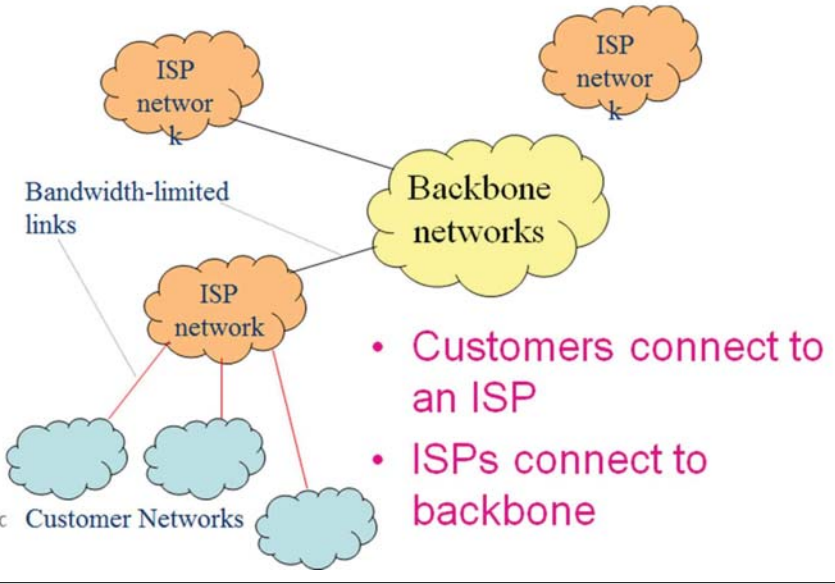
Dynamic Host Configuration Protocol (DHCP) Servers

- Clients in a TCP/IP network must be configured to know their logical network layer IP address
- This IP address can be manually configured or automatically configured using software.
- In a small enterprise, manual configuration is often practical
- In a large enterprise, with hundreds or thousands of clients, manual configuration is not practical
- DHCP servers are used primarily to automate a client IP addressing configuration

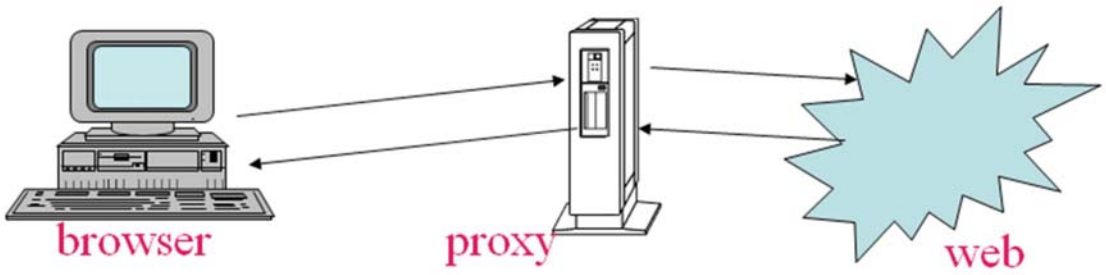


Proxy servers

- Cost of connections is based on bandwidth
- Cost of connection is a major part of network cost
- Organizations only obtain as much bandwidth as they can afford

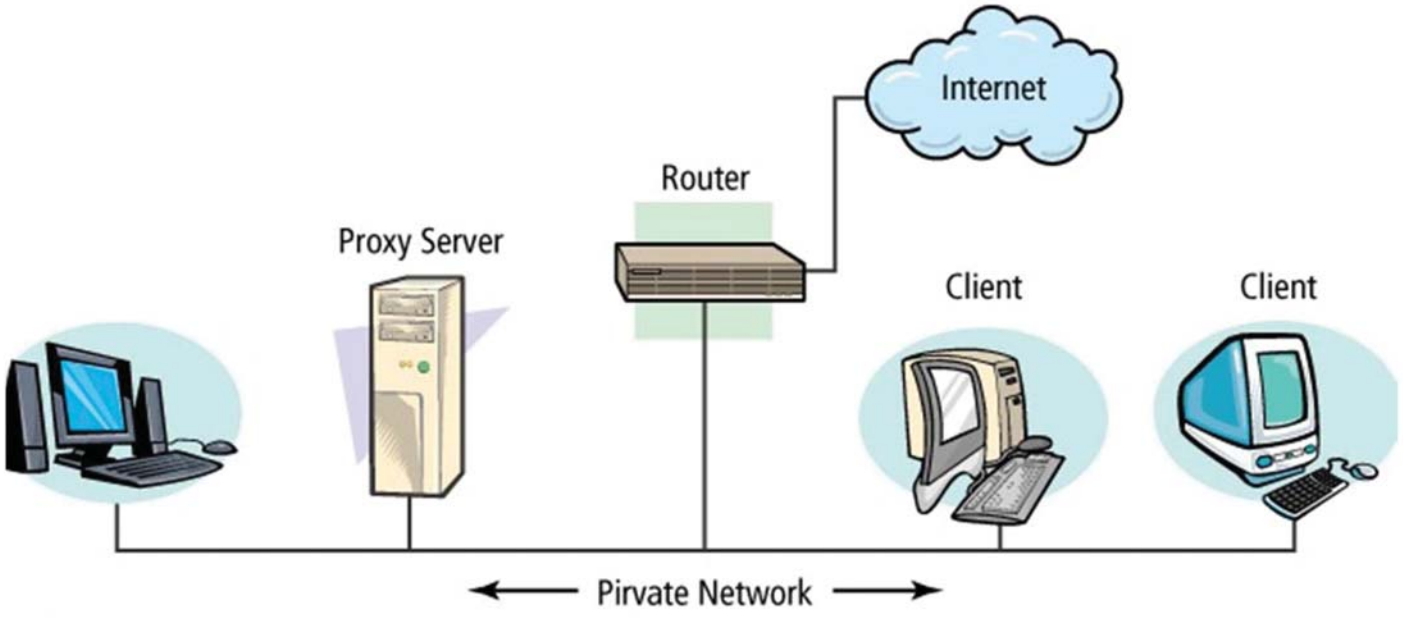


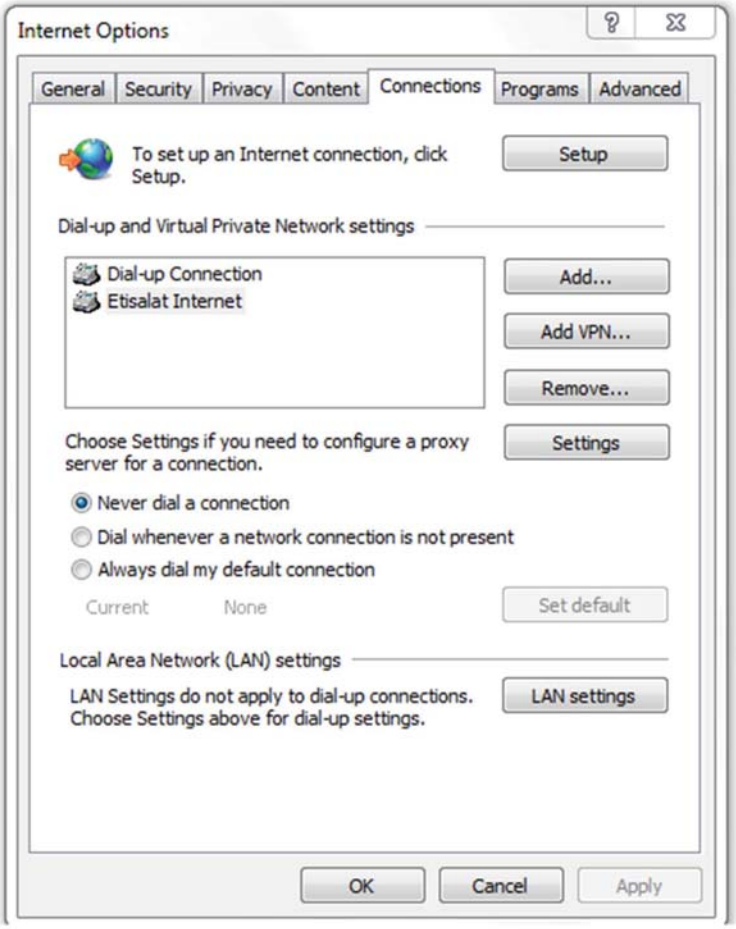
- A proxy is a host which relays web access requests from clients
- Used when clients do not access the web directly

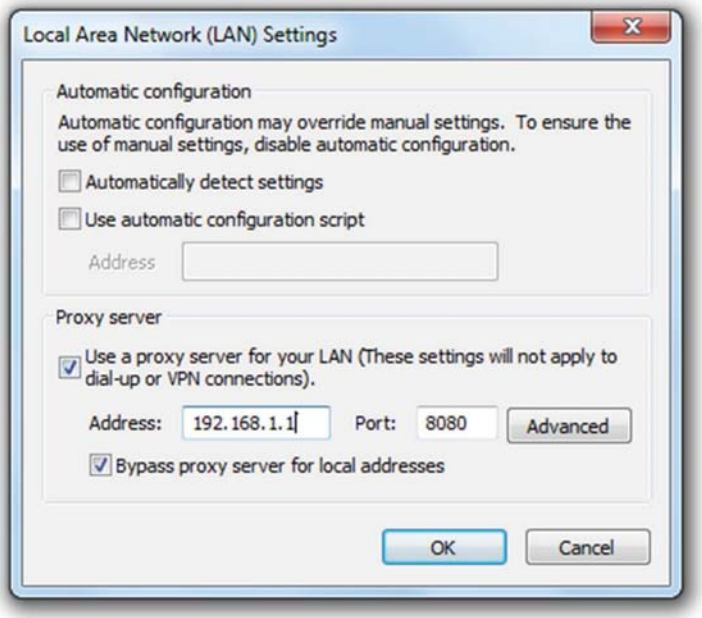


What is Web Caching?

- Storing copies of recently accessed web pages
- Pages are delivered from the cache when requested again
  - Browser caches
  - Proxy caches





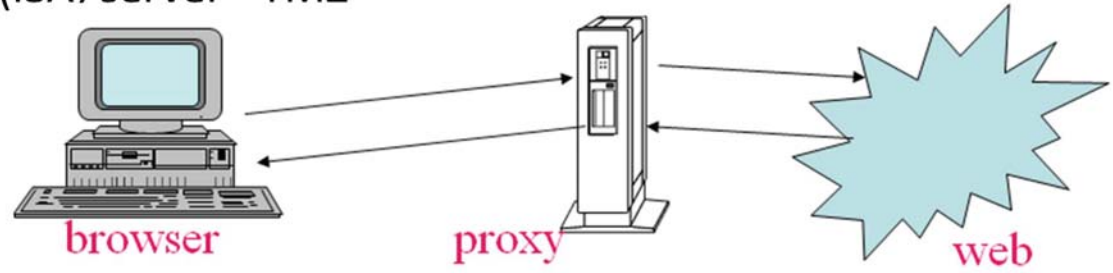


Why Cache?

- Shorter response time
- Reduced bandwidth requirement
- Reduced load on servers
- Access control and logging

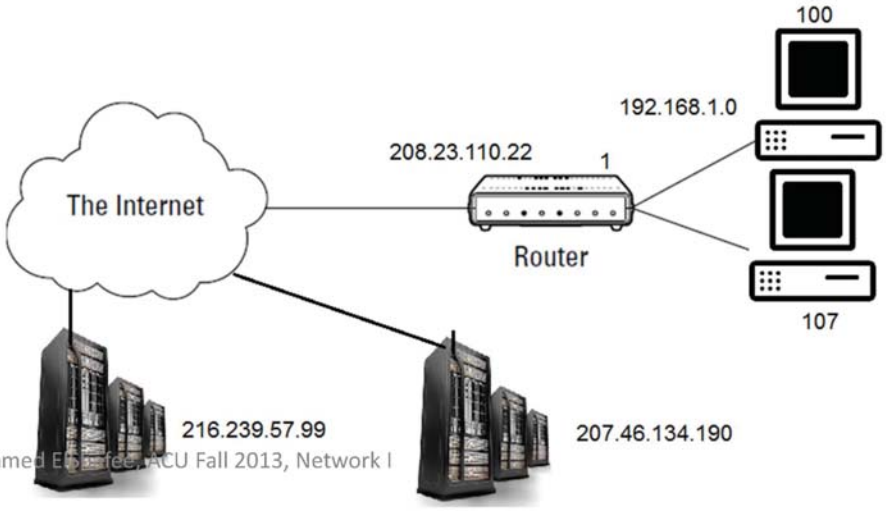
Popular Proxy Caches:

- Apache proxy
- MS proxy (ISA) server - TMZ
- WinProxy
- Squid



Gateway

- Gateways operate at the transport and internetwork layers which use logical addresses in processing messages.
- Gateways connect two or more networks that use the same or different (usually different) network layer protocols.
- Gateways process only those messages explicitly addressed to them.



- Gateways translate one network protocol into another, translate data formats, and open sessions between application programs, thus overcoming both hardware and software incompatibilities.
- A gateway may be a
  - stand-alone microcomputer with several NICs and special software, a
  - Front End Processor (FEP) connected to a mainframe computer, or
  - even a special circuit card in the network server.

Firewalls

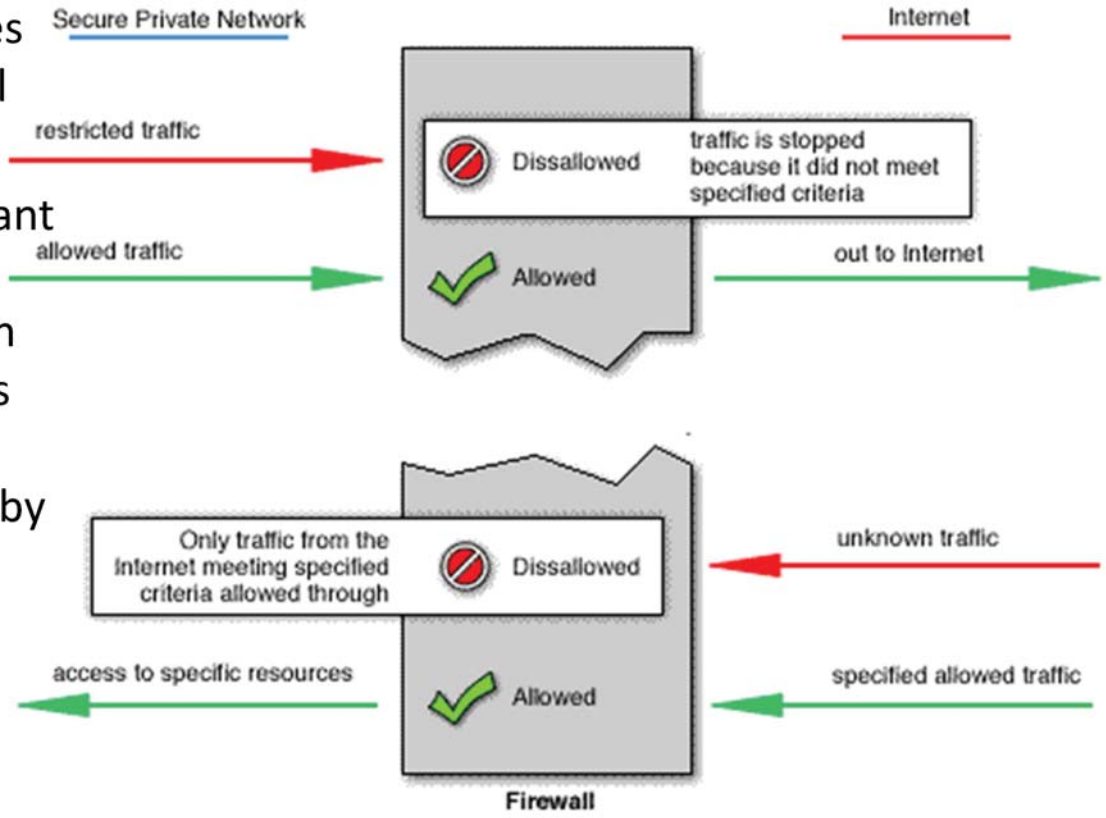
- Firewalls are devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures.

- What can firewalls do?
  - Manage and control network traffic
  - Authenticate access
  - Act as an intermediary
  - Protect resources
  - Record and report on events

- Firewalls operate at Layers 2, 3, 4, and 7 of the OSI model

- How does a firewall work?

deny/grant access based on the rules pre-defined by admin



Firewall Products

- Software
  - ISA Server, Comodo, ZoneAlarm,…
- Appliance
  - Cisco PIX, Checkpoint, SonicWall, WatchGuard,…
- Integrated
  - Multiple security functions in one single appliance: FW, IPS, VPN, Gateway Anti-virus/spam, data leak prevention…

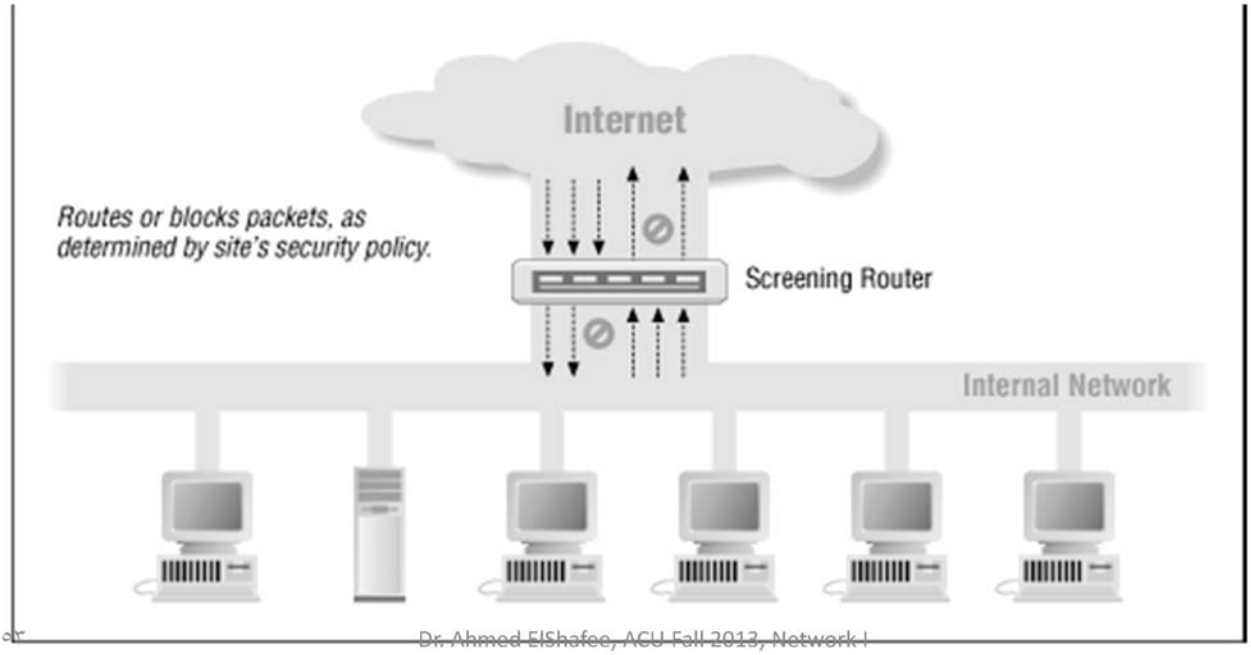
Firewall Technologies

- Host-based (or Personal) FW
  - Windows Firewall, Firestarter,…
- Network firewall
  - (Simple) Packet Filtering
  - Application Firewalls
  - Application-Proxy Gateways
  - Dedicated Proxy Servers
  - Transparent (Layer-2) Firewalls

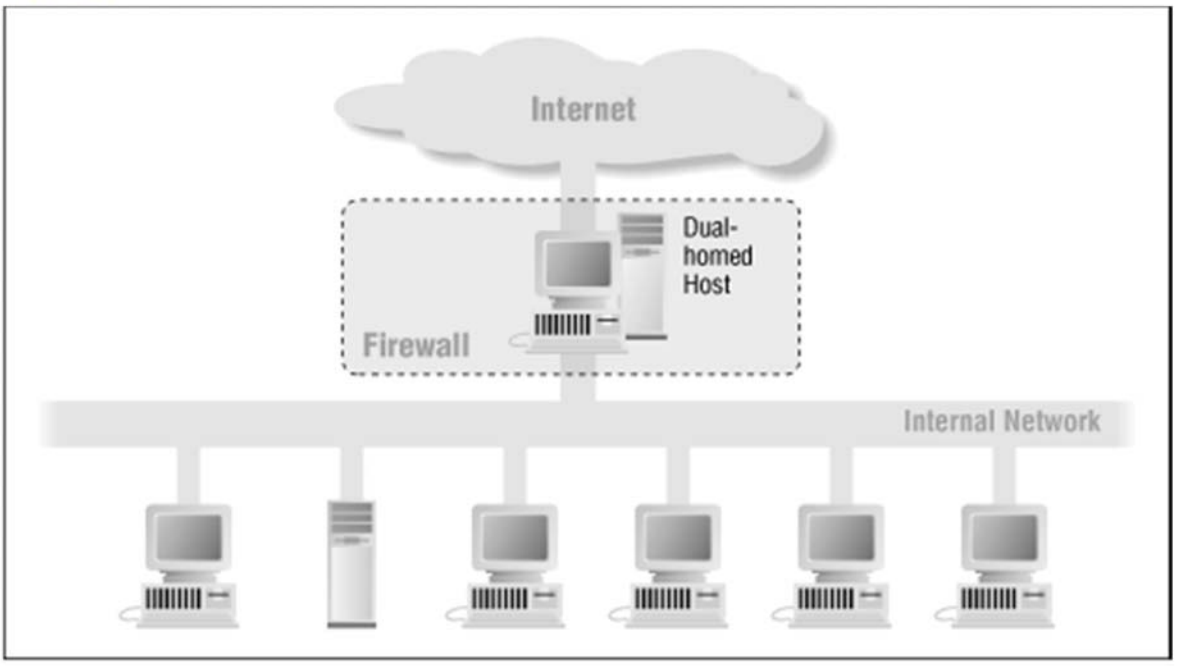
- Others Firewalls technologies
  - NAT (it is actually a routing technology)
  - VPN
  - Network Access Control/Protection (NAC/NAP)
  - Web Application Firewall
  - Firewalls for Virtual Infrastructures
  - Unified Threat Management (UTM)

Firewall Architectures

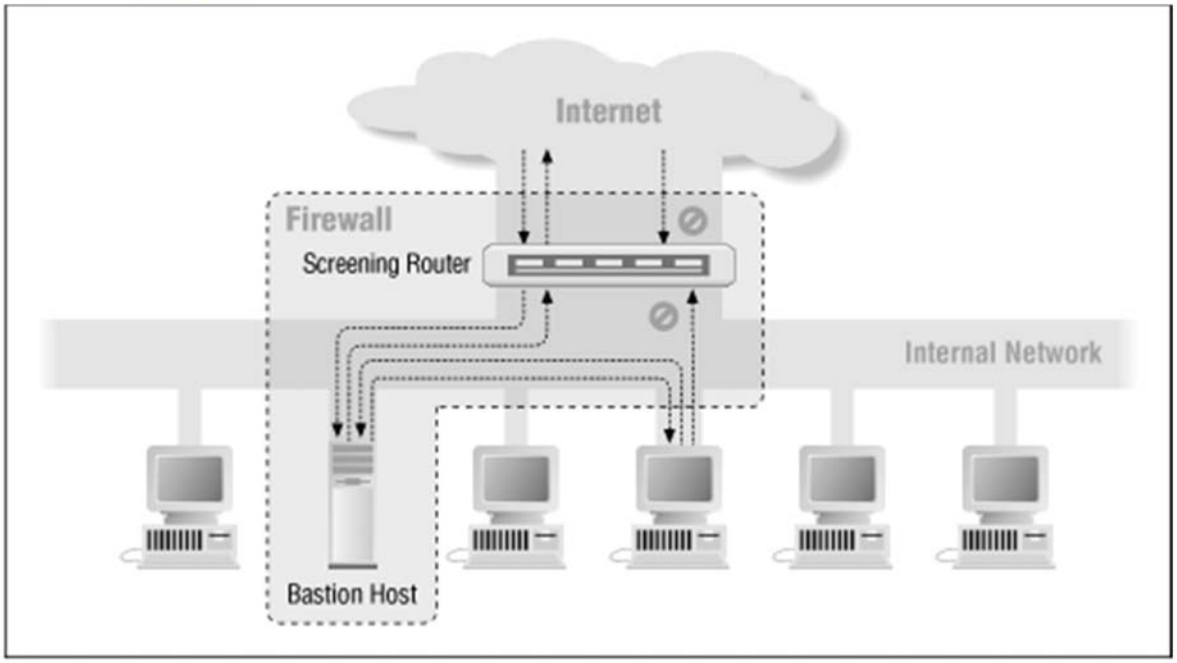
- HW



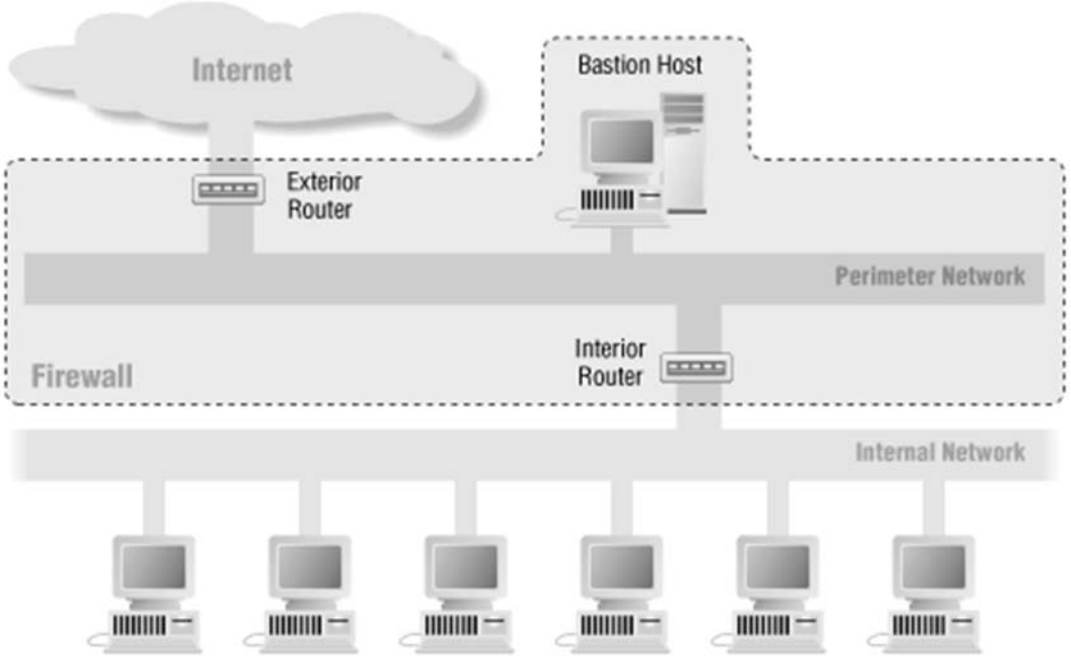
- Server



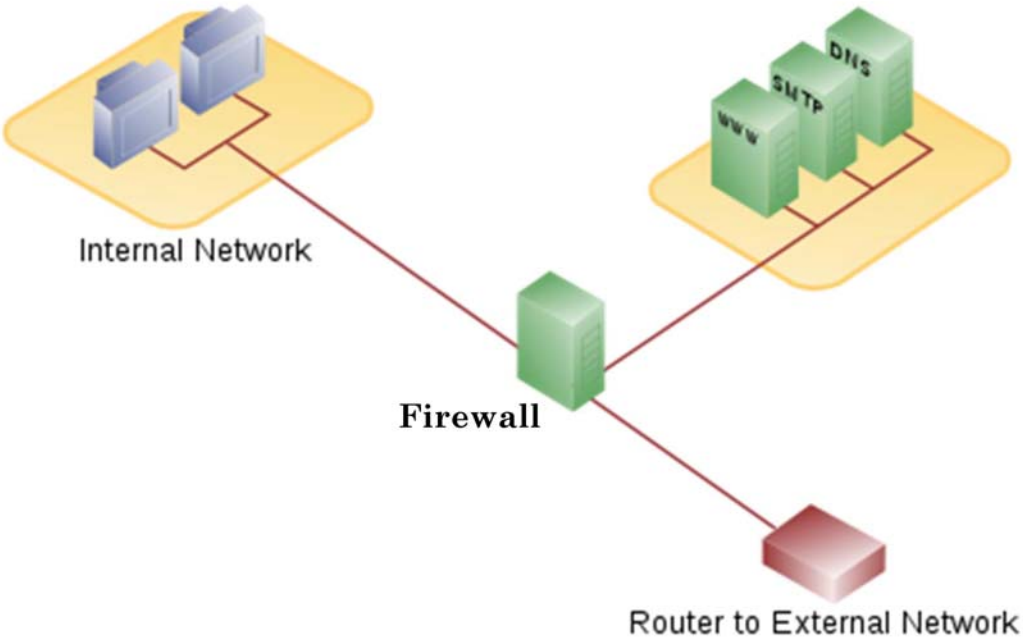
⊙ HW + Server



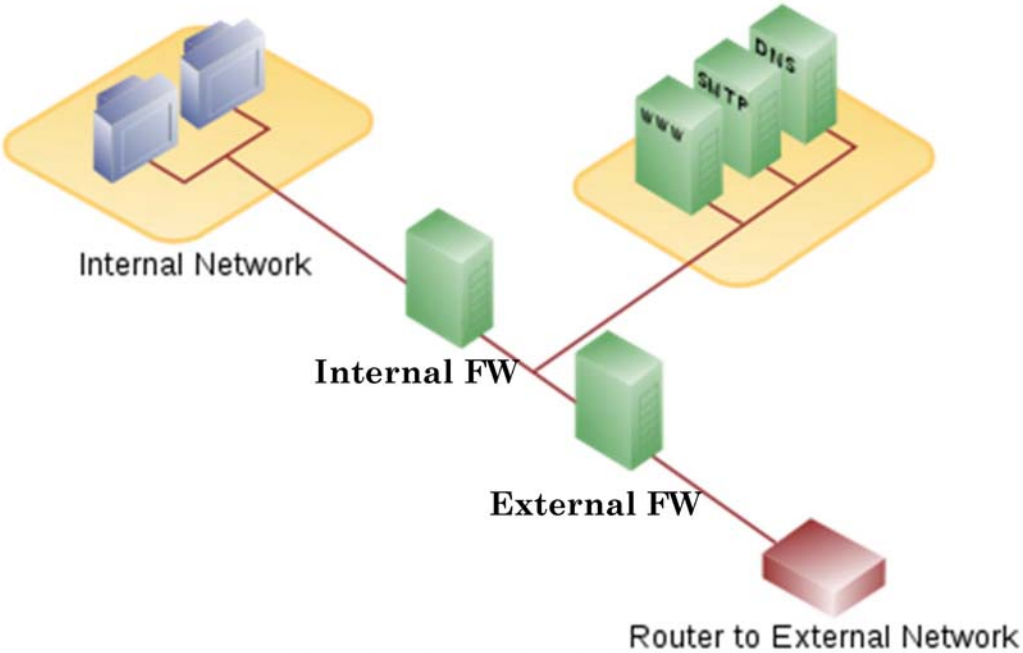
⊙ double HW



- DMZ with single server



- DMZ with dual server



- What a firewall CAN'T protect against:
  - viruses/malwares
  - internal threats (disgruntled workers, poor security policy…)
  - attacks that do not traverse the firewall (social engineering, personal modems or unauthorized wireless connections…)
  - attacks on services that are allowed through the firewall (HTTP, SMTP, FTP…)

Thanks,..

See you next week (ISA),…