Lecture (09)
Internetwork Layer (3)

By:

Dr. Ahmed ElShafee

Agenda

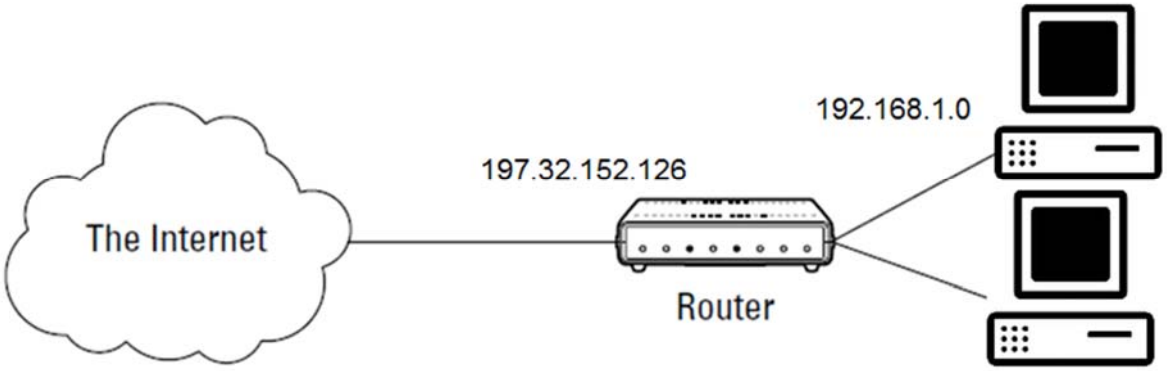
- Private and public addresses
- Network Address Translation
- Virtual Private Network (VPN)
- Virtual LANs

Private and Public addresses

Real IPs

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

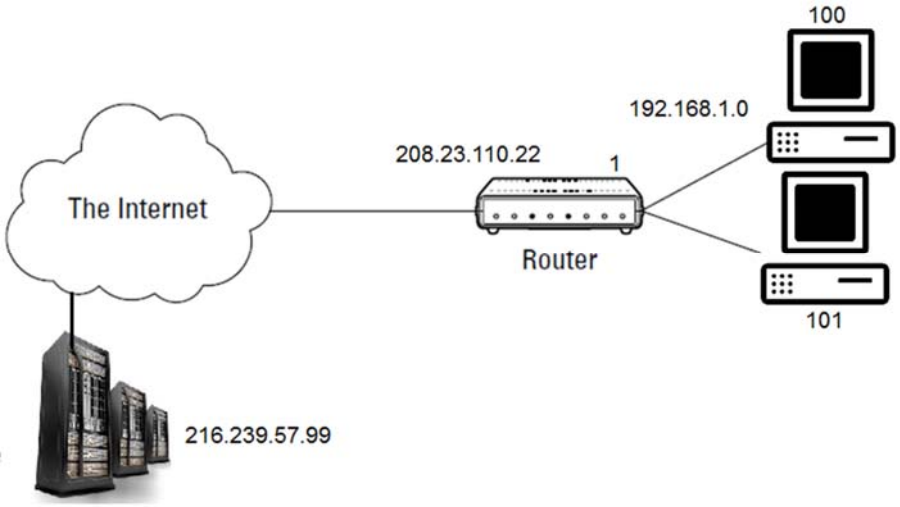
Address Range
10.0.0.1–10.255.255.254
172.16.1.1–172.31.255.254
192.168.0.1–192.168.255.254

NATting

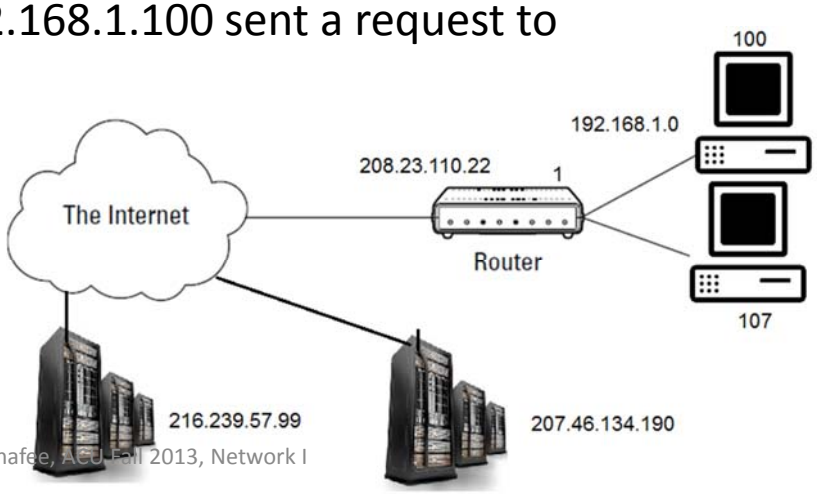
Network Address Translation

- 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.

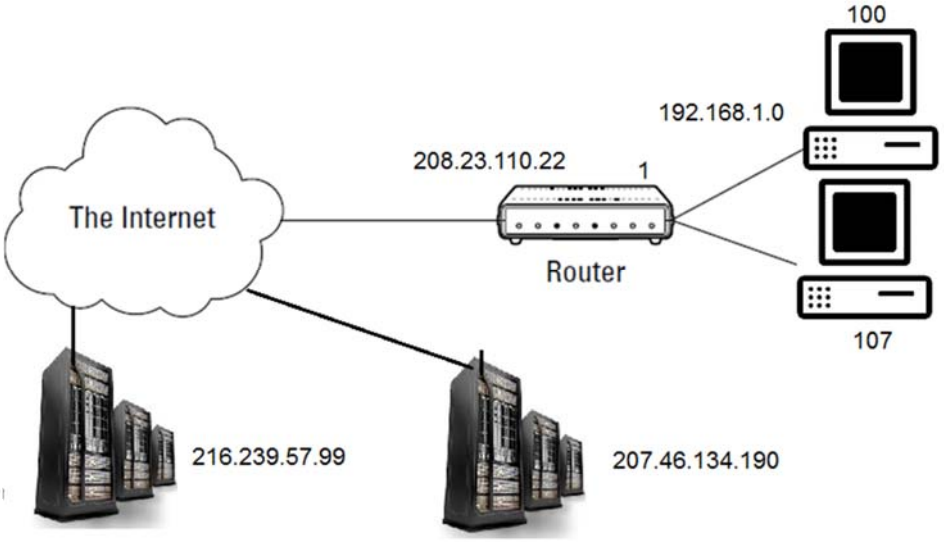
- NAT device can use a single public IP address for more than one host.
- It keeps track of outgoing packets so that it can match incoming packets with the correct host.
- To understand how this works, consider the following sequence of steps:



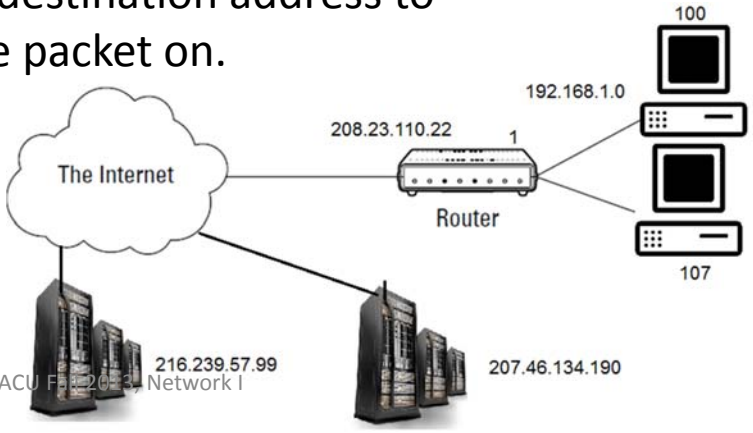
- A host whose private address is 192.168.1.100 sends a request to216.239.57.99, which is www.google.com.
- The NAT device changes the source IP address of the packet to 208.23.110.22, the IP address of the firewall.
- That way, Google will send its reply back to the firewall router. The NAT records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

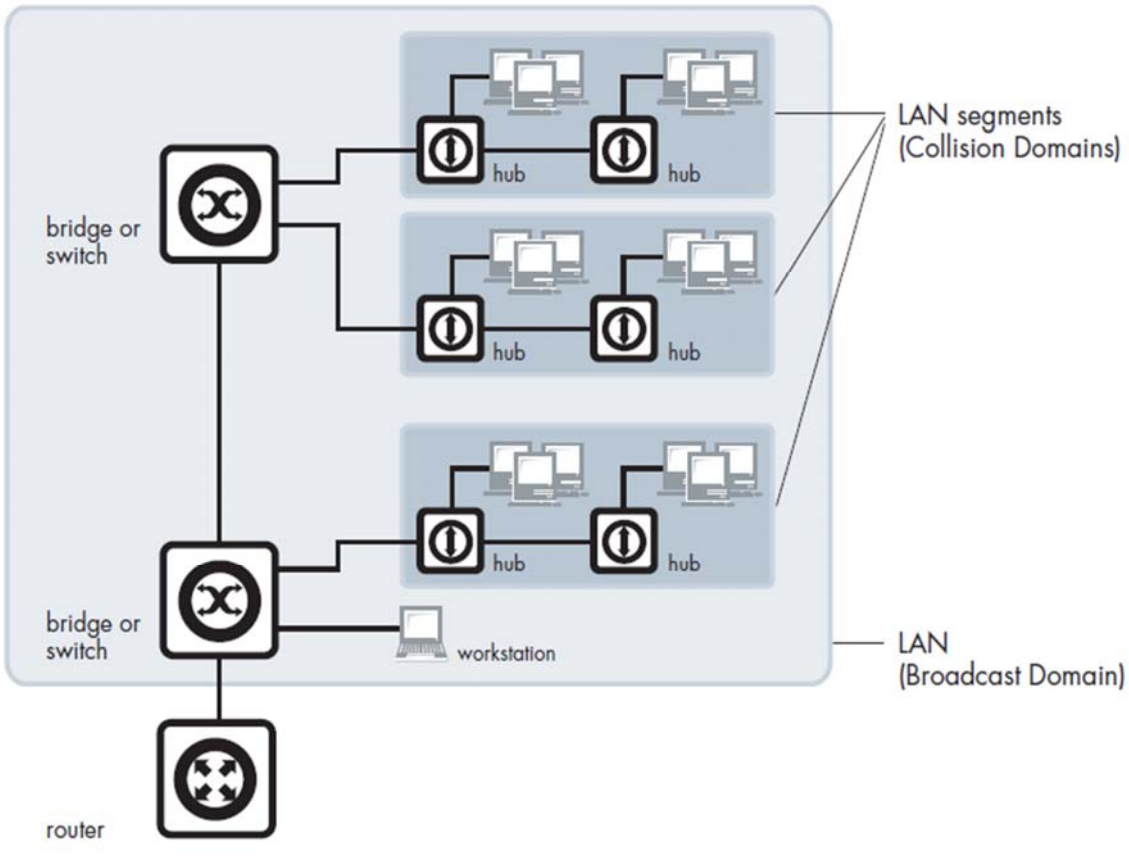


- A few seconds later, the firewall receives a reply from 216.239.57.99. The destination address in the reply is 208.23.110.22, the address of the firewall.
- To determine to whom to forward the reply, the firewall checks its records to see who is waiting for a reply from 216.239.57.99. It discovers 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.



VLANS

Domain terminology

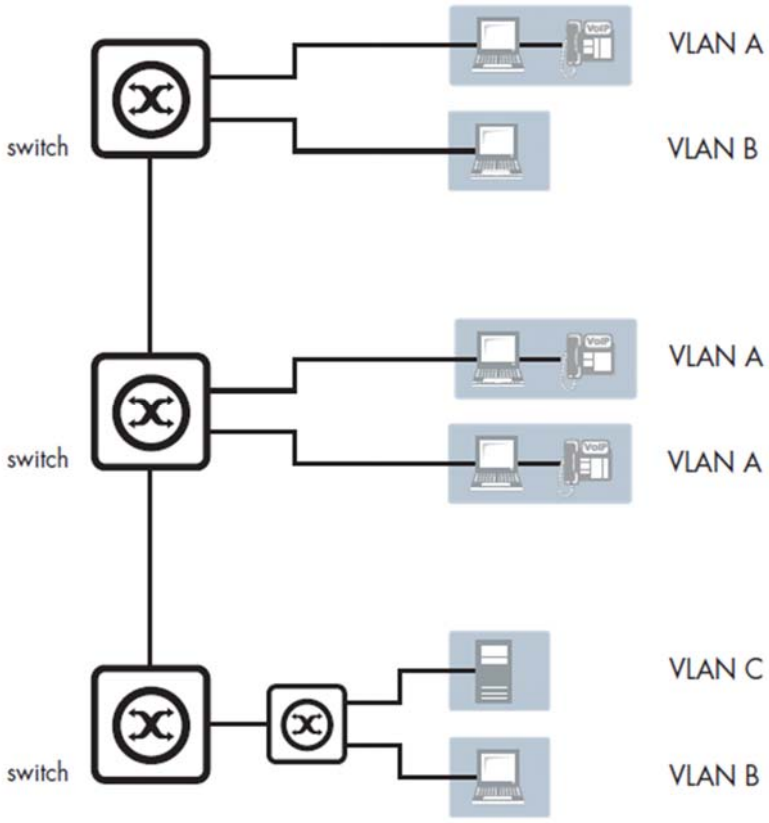


- figure introduces the concept of a **LAN segment**.
- This is also referred to as a **collision domain**, because when a device is trying to send a packet, it can only collide with packets sent by other devices on the same segment.
- each LAN segment consists of all the devices attached to a single switch port—the switch stops packets from different ports from colliding with each other.
- The LAN itself is referred to as a **broadcast domain**, because if any device within the LAN sends out a broadcast packet, it will be transmitted to all devices in that LAN, but not to devices beyond the LAN.

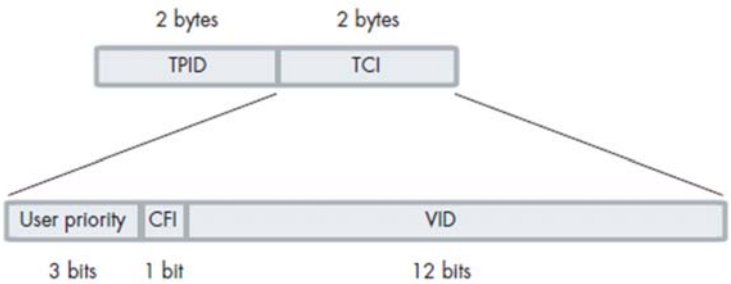
Vlans

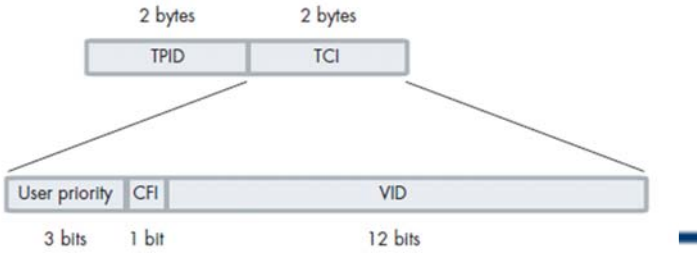
- switch vendors started implementing methods for defining "virtual LANs"—sets of switch ports, usually distributed across multiple switches, that somehow interacted as though they were in a single isolated LAN.
- This way, workstations could be separated off into separate LANs without being physically divided up by routers.
- At about the same time, hubs became less popular and have been largely replaced by L2 switches.
- This has made the whole concept of a collision domain somewhat historical.

- In modern networks, a "**collision domain**" mostly consists of a single device attached to an L2 switch port.
- For example, all the devices in the various areas labelled "VLAN A" all belong to a single virtual LAN—i.e. a single broadcast domain.



- In effect, this just divides a switch up into a set of independent sub-switches.
- **How VLANS work**
- frame tagging, Simply, 4 bytes are inserted into the header of an Ethernet packet.
- This consists of 2 bytes of Tag Protocol Identifier (TPID) and 2 bytes of Tag Control Information (TCI):



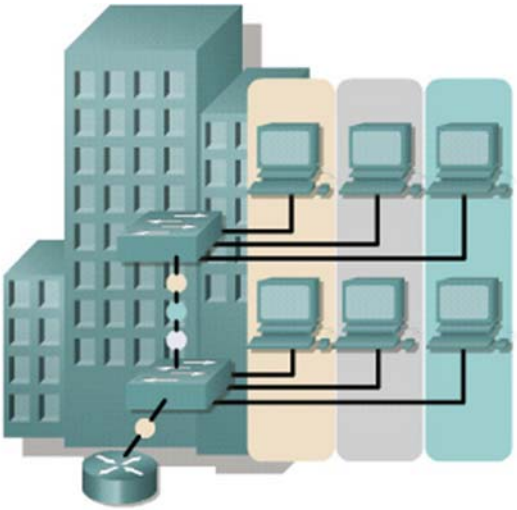


- **TPID** is the tag protocol identifier, which indicates that a tag header is following
- User priority is a 3-bit field that allows priority information to be encoded in the frame. Eight levels of priority are allowed.
- The CFI is a 1-bit indicator that is always set to zero for Ethernet switches.
- CFI is used for compatibility between Ethernet and Token Ring networks.
- the VID field contains the identifier of the VLAN

- **There are only two simple rules:**
- If a port is a tagged member of a VLAN, then any packets sent out that port by that VLAN must have a tag inserted into the header.
- If a tagged packet arrives in at a port, **and** the port is a tagged member of the VLAN corresponding to the VID in the packet's tag, then the packet is associated with that VLAN.

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.



Thanks,..

See you next week (ISA),…